韓國컴퓨터情報學會 論文誌
第16卷 第4號, 2011. 04.

2011-16-4-3-7

재카운터를 이용해 오류를 수정하는 경량화 RFID 인증 프로토콜 설계

오 기 욱*

A Design of Lightweight RFID Authentication Protocol Errors Correction Using Re-Counter

Gi Oug OH*

요 약

수동형 태그는 능동형 태그와는 다르게 연산처리가 뒤떨어지며 많은 연산처리는 힘들다. 본 논문에서 제안한 프로토콜은 수동형 태그에서 연산을 줄이지만 보안 인증에 안전하도록 개선한 인증 알고리즘으로 재카운터를 이용하여 리더가 태그를 읽을 때 오류가 발생하여도 계속 같은 값을 반환하는 다른 시스템과 달리 새로운 값을 반환하고 태그의 연산 부분을 리더 혹은 후위시스템에서 처리하도록 RFID 보안 프로토콜을 개선하였다. 그리고 RFID 인증 프로토콜이 보장해야 할 기본적인 보안사항들을 만족하도록 하였으며 태그의 실제 정보를 악의적인 방법을 통해 불법적으로 획득하더라도 실제 정보가 아닌 암호화된 정보가 노출이 되어 정보의 획득이 힘들고 연속적으로 태그 정보를 읽더라도 읽을 때마다 태그의 정보가 변경되기 때문에 위치 추적성등에 안전한 프로토콜이다.

▸ 키워드 : RFID 인증, 경량화, 재카운터, 위치 추적성

Abstract

Passive tags are inferior to active tags in processing efficiency, so they have difficulty in large volume processing. The proposed protocol reduces the volume of computation in passive tags and, at the same time, improves authentication for enhanced safety and security. That is, different from existing RFID protocols that return the same value even if an error happens when the reader reads a tag, the improved RFID security protocol returns a new value using a re-counter and processes the computation part of a tag in the reader or in a back end system. Even if the information of a tag is acquired by an malicious way, it is not actual information but encrypted information that is not usable. In addition, even if tag information is read in sequence, it is changed in each read, so the protocol is safe from Location Tracking.

▸ Keyword : RFID Authentication, Lightweight, Re-Counter, Location Tracking

• 제1저자 : 오기욱 • 교신저자 : 오기욱
• 투고일 : 2011-02-09, 심사일 : 2011-03-18, 게재확정일 : 2011-04-04
* 안양대학교 교양학부(Division of Liberal Arts)

www.kci.go.kr

Ⅰ. 서 론

RFID(Radio Frequency IDentification)는 후위시스템과 리더 그리고 태그들로 구성되어 있다. RFID 시스템에서 비보호 구간인 리더와 태그간의 무선 주파수 통신은 정보 노출, 사용자의 위치추적(Location Tracking), 위조나 서비스 장애와 같은 보안 및 사용자 프라이버시(Privacy) 침해등 심각한 문제를 발생한다[1,2].

RFID의 전자 태그는 능동형(Active)과 준수동형(Semi-Passive), 수동형(Passive)으로 분류한다[2,3]. 능동형 태그는 전원과 연산장치를 가지고 있어 자원을 효율적으로 사용할 수 있으며 많은 계산을 필요로 하는 보안 알고리즘을 적용할 수 있다. 또한 전파의 전달범위가 크고 넓기 때문에 자신의 정보를 인증 받은 리더와 인증 받지 않은 리더에게도 자신의 정보를 전달한다. 반면, 수동형 태그는 자신의 정보를 리더에게 보내기 위한 필요 전원을 갖고 있지 못하기 때문에 리더로부터 전원을 받고, 정보의 전달범위도 매우 짧다. 수동형 태그는 태그의 가격이 2센트 이하로 바코드를 대신할 수 있도록 구성되어 있기 때문에 능동형 태그와 같이 복잡한 보안 알고리즘을 적용하기 힘들다. 제한적인 연산 처리를 하는 수동형 태그에서 여러 번 계산을 필요로 하거나 태그 내에 난수 생성기를 적용한 결과 태그 성능이 높아지도록 유도하고 있다. 이런 결과로 수동형 태그의 값이 비싸지게 되고 심지어 수동형 태그가 아닌 능동형 태그의 사용을 유도하고 있는 실정이다. 따라서 바코드를 대신하려는 개발목적에 알맞은 수동형 태그에 적용할 수 있는 보안 알고리즘의 개발이 필요하다.

RFID 시스템은 RF 통신을 사용하는 특성 때문에 태그의 정보를 쉽게 획득할 수 있고 실제로 허가 받지 않고 누구나 리더만 있으면 정보 획득이 가능하다. 따라서 리더와 태그는 암호화된 정보 교환이 필요하며 교환되는 정보가 누출되더라도 정상적인 거래 당사자 아닌 비 인가자들이 정보의 내용을 알거나 교환되는 정보를 사용하지 못하도록 암호화 되어있어야 한다[3].

RFID 시스템은 리더와 후위 시스템사이는 보안(Secure) 채널이고 리더와 태그사이는 비 보안(InSecure)채널이라 한다[2, 5].

기존 연구들을 보면, 태그의 구성이 수동형 보다는 능동형에 가깝도록 보안 알고리즘을 설계하여서 단순하고 강력한 보안 알고리즘 보다는 복잡한 보안 알고리즘을 적용하였다. 또한 보안 안전성 문제를 해결하기 위해 RFID 시스템의 다양한 인증 알고리즘들이 제안되었으나 많은 제안이 해시함수와 난수 생성기를 이용해 난수를 발생시킨 복잡한 알고리즘들이 제안되었으며 태그의 정보를 리더가 한 번에 읽어 인증되는 시스템에 국한되어 있다. 그렇기 때문에 태그 정보를 읽을 때 오류가 발생되면 후위시스템으로 정보를 넘겨주지 못하거나 또는 계속 같은 정보를 반환하기 때문에 사용자 혹은 공격자들이 태그의 정보를 알 수 있거나 위치트래킹 공격을 피할 수 없는 단점이 발생하였다.[2, 4, 6].

본 논문에서는 보안 채널간의 암호 인증보다 비보호 채널간의 채널 즉, 리더와 태그의 관계에서 태그의 계산을 낮추어 수동형 태그에 적용 가능한 보안 알고리즘을 제시하고 리더가 태그의 정보를 한 번에 읽지 못하고 여러 번 시도하여 태그의 정보를 읽는 경우에도 태그에 영향을 주지 않고 변화된 암호화 값을 전송하여 리더와 후위 시스템에서 처리할 수 있는 비보호 채널 상에 안전한 RFID 인증 프로토콜을 제안한다.

제안한 프로토콜은 리더에서 생성된 난수를 태그에서 태그 아이디와 연접(AND, ||)하고 카운터를 생성하여 태그의 정보를 읽을 때마다 카운터의 값을 증분하기 때문에 위치 트래킹(Location Tracking)문제점을 회피 할 수 있다. 카운터는 카운터의 값이 작으면 태그의 정보 값이 중복될 수 있으나 카운터의 값이 충분하면 거의 중복되지 않기 때문에 카운터의 값을 이용할 수 있다. 또한, 리더가 태그의 정보를 한 번에 읽지 못하고 여러 번에 걸쳐 읽더라도 리더에서 읽은 횟수만큼을 계산하여 후위 시스템에서 처리하여 태그의 정보를 알 수 있도록 하였으며, 태그에서 난수를 생성하지 않아 태그의 연산 오버헤드와 연산처리 부담을 줄였다.

Ⅱ. 관련연구

1. 기존 프로토콜 분석

본 절에서는 RFID 프로토콜 해시함수를 이용하는 프로토콜들을 간단히 살펴보고, 후위시스템에서 태그 아이디를 검색하고 인증할 때 사용하는 해시연산의 비효율성을 분석한다. 사용자의 위치트래킹 같은 프라이버시문제와 재전송공격 및 도청공격과 같은 RFID 프로토콜들의 보안문제들을 해결하기 위해 여러 가지 기법들이 제안되었다. 보안기법들은 비트연산(XOR) 기반, 해시함수 기반, 재 암호화, 그레이코드들과 같이 소프트웨어를 이용한 암호학적 접근기법과 태그 무효화(kill), Active Jamming과 같은 물리적인 접근기법으로 분류된다[2, 3, 7]. 본 절에서는 암호학적 접근기법으로 해시함수를 사용하는 프로토콜들을 살펴보았다.

www.kci.go.kr

2. 해시 체인 프로토콜

Okubo등에 의해 제안된 해시체인 프로토콜은 두 개의 해시 체인함수를 이용하여 리더의 질의(Query)를 태그가 매 세션마다 다른 응답을 전송하고 인증하는 프로토콜로 [그림 1]과 같이 서로 다른 두 개의 해시함수를 이용하여 리더의 질의를 태그가 응답하여 Ai, i, G(Si) 정보를 생성하여 리더로 전달하고, DB에서 G(Si)에 대한 i번의 인증연산을 수행한 후 인증된 아이디를 리더에게 전달한다.

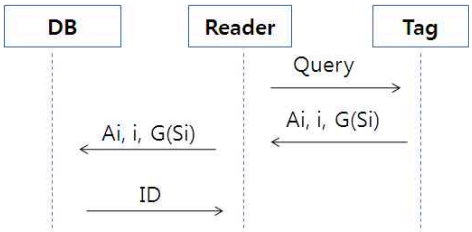

그림 1. 해시 체인 프로토콜
Figure 1. Hash Chain Protocol

해시 체인 프로토콜의 단점은 리더의 질의에 대해 항상 같은 응답을 하므로 공격자가 태그의 응답 Ai와 i를 알 수 있어 Ai와 i를 재전송하는 경우 정당한 태그로 위장할 수 있으므로 재전송 공격과 스푸핑 공격에 취약하다[2, 3]. 해시 락이나 랜덤 해시 락 프로토콜들처럼, 데이터베이스에서 태그검색과 태그 인증 경우 i번의 G(Si) 연산을 수행해기 때문 데이터베이스에서 태그검색과 태그 인증할 때 n번의 계산횟수에 대한 비효율성의 문제가 발생한다.

3. 상호인증을 위한 RFID 프로토콜

상호인증을 위한 RFID 프로토콜을 제안한 [7]은 공개된 채널 상에 송수신되는 모든 통신 메시지의 인증과 무결성을 위해 단방향 해시 함수를 사용하였다. 프로토콜을 보면 상호인증을 수행한 후에 데이터베이스와 태그가 다음 세션을 위해 태그에 존재하는 태그 아이디를 새로운 태그 아이디로 갱신하도록 단계를 진행함으로 전 방향 안전성을 제공할 수 있도록 하였다.

표 1. 단계별 동작과정
Table 1. Step Operation Process

단계	동 작 과 정
[단계1]	Reader -> Tag : Query, R
[단계2]	Tag -> Reader : T, h(ID ‖ R ‖ T)
[단계3]	Reader -> DB : R, h(K ‖ R), T
[단계4]	DB -> Reader : h(K ‖ R ‖ T)⊕Info, h(K ‖ R ‖ T ‖ Info), h(ID ‖ T)
[단계5]	Reader -> Tag : h(ID ‖ T)
[단계6]	Tag -> h(ID ‖ T)

프로토콜의 동작과정은 [단계 6]으로 표 1과 같이 구성되어 있다. 상호인증을 위한 프로토콜은 태그에서의 연산 및 태그에서 난수생성기를 통해 난수를 생성하며 데이터베이스에서의 연산이 복잡하기 때문에 과부하가 발생되며 태그의 인식시간도 태그가 증가할수록 늘어난다는 단점이 있다.

4. ID 검색 개선을 위한 상호인증 프로토콜

아이디(ID) 검색개선을 위한 상호인증 프로토콜을 제안한 [8]은 단방향 해시함수를 이용하여 암호화하였으며, 데이터베이스에서 태그 아이디를 검색하는데 소요되는 시간을 개선하고 해시 연산량에 따른 과부하를 줄이고자 태그에서 난수를 생성하지 않고 처리하도록 하였다. 또 다른 상호인증 프로토콜보다 상호인증 프로토콜의 동작과정을 줄임으로 복잡도를 줄였다. 표 2는 아이디 검색 개선을 위한 상호인증 프로토콜의 동작과정이다.

표 2. 단계별 동작과정
Table 2. Step Operation Process

단계	동 작 과 정
[단계1]	Reader -> Tag : Query, R
[단계2]	Tag -> Reader : I, h(ID ‖ I ‖ R)
[단계3]	Reader -> DB : R, I, h(K ‖ R), h(ID ‖ I ‖ R)
[단계4]	DB -> Reader : Inew=h(ID ‖ I ‖ T), IDnew = h(ID ‖ I ‖ R ‖ T), h(K ‖ R ‖ T)⊕Info, h(K ‖ R ‖ T ‖ Info), h(ID ‖ T ‖ R)
[단계5]	Reader -> Tag : T, h(ID ‖ R ‖ T), h(K ‖ R ‖ T)⊕Info, h(K ‖ R ‖ T ‖ Info)
[단계6]	Tag : T, h(ID ‖ R ‖ T)

단계별 동작과정 프로토콜은 [단계 6]의 동작과정으로 구성되어 있으며 DB에서 비효율성을 줄이기 위해 공유비밀 정보 I를 이용한다. I는 태그의 공유비밀정보로 데이터베이스로부터 발급받아 태그에 저장하여 이용한다. I와 태그 아이디를 매핑하여 정당한 관계인지를 체크함으로써 전방향 안전성을

www.kci.go.kr

제공한다. 그러나 이 프로토콜은 연산과정을 줄임에도 불구하고 태그에서의 연산 과부하에 따른 부담을 줄이지 못하였다.

III. 제안하는 RFID 상호인증 프로토콜

비보호 채널에서 태그의 연산을 기존 방식보다 줄임으로 경량화된 인증 프로토콜을 개선하였으며 리더가 수동형 태그의 정보를 한 번에 읽지 못하고 여러 번에 걸쳐 읽을 경우에 피할 수 없는 프라이버시 침해를 회피할 수 있도록 구성하였으며 정당한 사용자인 경우에 사용자가 원하는 정보를 획득할 수 있도록 개선된 인증 프로토콜을 제안한다. 또 태그에서 수행되는 해시함수의 연산 횟수와 다른 연산횟수를 줄임으로 용량이 작은 수동형 태그에서도 적용할 수 있도록 하였으며 처리과정에 필요한 태그의 연산을 리더와 후위시스템에서 처리하도록 하였다.

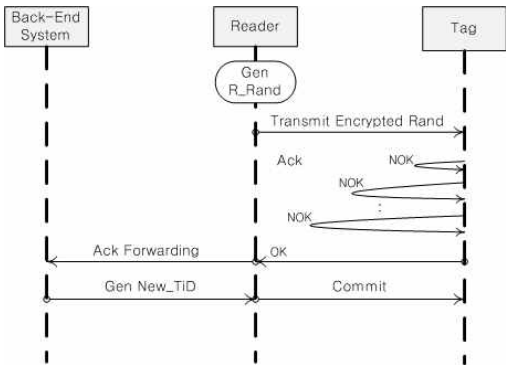

그림 2 인증 프로토콜 순차 다이어그램
Figure 2. Authentication Protocol Sequence Diagram

그림 2는 제안한 프로토콜 인증과정을 순차 다이어그램으로 표현한 것으로 리더에서 난수를 생성한 다음 생성된 난수를 해시함수를 이용하여 암호화한 후 암호화된 정보를 태그에 보낸다. 태그에서는 카운터(Cnt)를 이용하여 리더로 읽을 때마다 위치추적을 할 수 없도록 카운터의 값을 증분한다. 증분된 카운터 값과 해시함수로 암호화된 난수 값 그리고 태그 자체의 아이디 값(TiD)을 연접하여 해시 함수로 암호화하여 리더에게 보낸다. 리더는 자신이 생성한 난수(R_Rand)값과 태그로부터 전달 받은 해시함수로 암호화된 값 그리고 증분된 카운터 값을 보호 채널을 이용하여 후위시스템으로 보낸다. 후위시스템은 리더로부터 전달 받은 값과 태그로부터 전달 받은 값을 역으로 계산하여 두 개의 값이 같은지를 비교연산 한다. 두 값이 같으면 태그의 정보를 데이터베이스에서 검색하여 처리하고 만약 두 값이 다르면 태그 정보 처리를 종료한다.

그림 3은 제안한 인증 프로토콜로서 태그에서 난수를 생성하지 않는다. 제안 인증 프로토콜은 후위시스템에 있는 데이터베이스의 인증을 위해 리더에서 생성한 난수(R_Rand)를 전달받아 해시함수를 이용하여 암호화 한다. 이와 같이 암호화 하는 이유는 첫 번째로 태그의 전방향 안전성을 위해 태그의 새로운 태그 아이디를 갱신할 때 사용하기 위한 것이고, 두 번째로 후위 시스템의 데이터베이스에서 새롭게 갱신된 태그 아이디를 전달하는 과정을 줄이고자 하기 때문이다.

그림 3은 제안한 인증 프로토콜로 리더가 태그의 정보를 읽을 때 한 번도 읽기 오류가 발생하지 않고 한 번에 태그의 정보를 읽는 경우를 나타낸 것이며, 그림 4는 리더가 태그의 정보를 한 번에 읽지 못하고 여러 번 읽기 과정을 통해 태그의 정보를 읽어 처리하는 것을 나타내었다.

정상적인 공격에 대하여 안전성을 만족하는 그림 3의 각 단계별 처리 절차에 대한 동작원리는 다음과 같다.

[단계 1] 리더 -> 태그

리더에서 태그에게 질의(Query)와 리더에서 생성된 난수를 해시함수로 이용하여 보안처리 한 값을 태그에게 전송한다.

[단계 2] 태그 -> 리더

태그에서 카운터를 증분한다. 카운터는 리더가 태그의 정보를 읽을 때마다 증분한다. 카운터는 리더가 매번 읽을 때마다 증분하기 때문에 위치 트래킹을 피할 수 있다. 태그 아이디와 카운터, 리더에서 넘어온 보안 처리된 난수값을 해시함수로 암호화하여 리더로 전송한다.

[단계 3] 리더 -> 후위 시스템

리더는 태그에서 넘어온 카운터와 리더에서 발생한 난수 값 그리고 해시함수를 이용하여 암호화한 값 H(TiD||Cnt||H(R_Rand))를 후위시스템에 전송한다. 후위시스템은 리더에서 넘어온 난수 값을 해시함수를 이용하여 암호화하고 함께 넘어온 카운터 값과 암호화 한 값인 H(TiD||Cnt||H(R_Rand))이 서로 맞는지를 검증한다. 따라서 후위 시스템에서 연산을 통해 만들어진 값과 리더에서 넘어온 값이 맞으면 후위 시스템의 데이터베이스에서 해당하는 정보를 찾아 리더에게 보내주고 두 값이 맞지 않으면 해당하는 정보가 없기 때문에 시스템을 종료하거나 해당하는 정보가 없음을 알려준다.

www.kci.go.kr

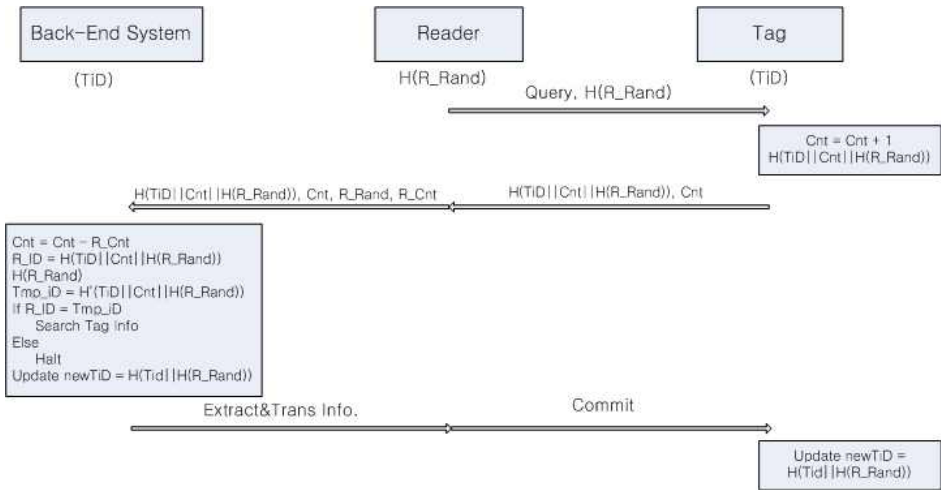

그림 3. 제안한 RFID 인증 프로토콜
Figure 3. Proposed RFID Authentication Protocol

[단계 4] 리더 -> 태그

리더는 후위시스템에서 확인(Commit)정보를 받아서 태그에 넘겨주고 새로운 태그 아이디(New_TiD) 생성 정보를 태그로 전송한다. 태그 는 리더로부터 확인정보를 받고 자신의 새로운 아이디를 생성하여 리더로부터 받은 아이디와 자신이 생성한 아이디를 비교하여 새로운 아이디로 갱신한다. 만약, 비교한 두 값이 같지 않으면, 인증은 실패한 것으로 간주하여 과정을 중지한다. 이 정보는 태그가 가지고 있는 정보를 조합해서 만들었고 후위 시스템 역시 태그의 정보를 조합해서 만들었기 때문에 같은 새로운 아이디로 갱신할 수 있다.

그림 4는 리더가 태그의 정보를 한 번에 읽지 못하고 여러 번 읽기 절차를 통하여 태그의 정보를 처리하는 과정을 나타

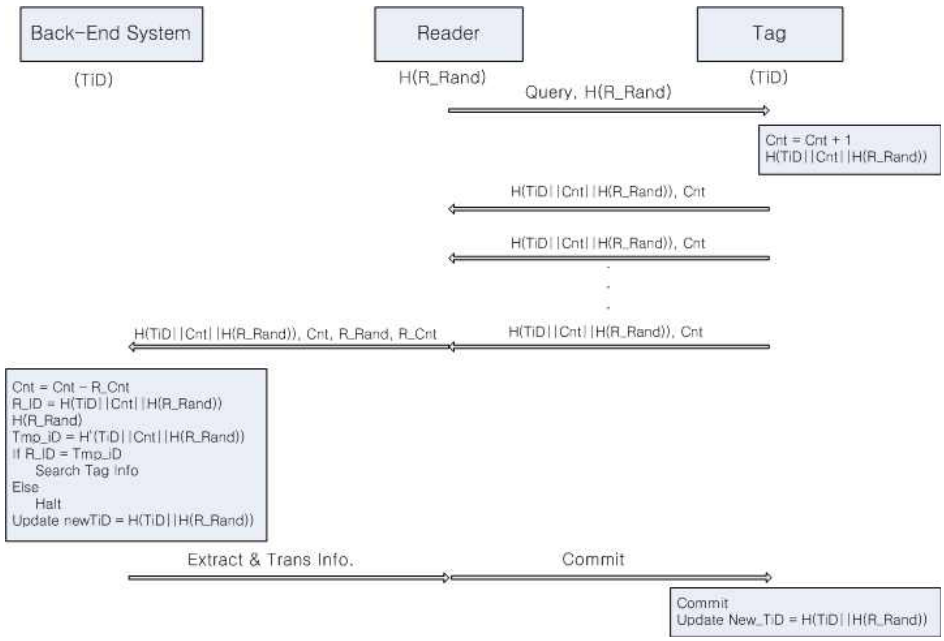

그림 4. 읽기 오류 처리하는 제안한 RFID 인증 프로토콜
Figure 4. Proposed RFID authentication protocol processing a read error

www.kci.go.kr

낸 것으로 제안한 RFID 인증 프로토콜이 읽기 오류가 발생했을 때 처리하는 단계를 나타내었다. 한 번에 읽기를 성공하는 제안된 RFID 인증 프로토콜은 [단계 4]를 통하여 모든 절차를 끝내지만 읽기 오류가 발생한 경우에도 마찬가지로 [단계 4]중 리더가 여러 번 읽는 경우를 추가하여 모든 절차를 끝낼 수 있다. 즉, 이 경우 [단계 2]에서 태그에서 리더로 넘어오는 정보가 카운터의 증분으로 인해 계속 변경되어 다른 정보가 넘어오지만 카운터 값도 함께 넘어오기 때문에 후위 시스템에서 검증을 할 수 있다. 물론 검증하는 부분이 태그의 카운터 값과 리더의 재카운터 값(R_Cnt)을 후위시스템에서 계산해주기 때문에 읽기 오류 발생한 경우나 읽기 오류가 발생하지 않은 경우 모두 처리할 수 있다.

Ⅳ. 제안 프로토콜 분석

비보호 채널에서 기존의 RFID 보안 프로토콜과 제안한 RFID 보안 프로토콜간의 도청 공격, 재전송 공격, 트래픽 분석, 위치 트래킹 공격, 서비스 거부 공격, 전 방향 안전성과 같은 안전성에 대한 평가와 성능분석을 하였으며, 태그 아이디 검색 및 인증할 때 RFID 인증 프로토콜에서 해시 연산 횟수에 따른 해시 계산량을 개선한 RFID 프로토콜의 효율성을 분석한다.

1. 제안 시스템의 안전성 분석

제안한 프로토콜에 대해서 전방향 안전성과 도청 공격, 재전송 공격, 스푸핑 공격, 트래픽 분석 공격, 위치 트래킹 공격, 서비스 거부 공격 등에 대한 안전성 평가 분석을 하였다.

1) 재전송 공격(Replay Attack)

리더에서 난수를 생성하여 해시 함수로 암호화 한 값을 태그로 보내고 태그에서는 매번 읽을 때마다 증분한 카운터 값이 리더의 난수 값과 함께 연산된다. 그리고 비인가 리더가 태그의 정보를 읽더라도 매번 다른 값이 반환되기 때문에 제안 프로토콜은 재전송 공격에 안전하다.

2) 스푸핑 공격(Spoofing Attack)

공격자가 변하지 않는 태그 아이디 값을 획득한다면 공격자는 스푸핑 공격을 수행할 수 있다. 하지만 제안한 프로토콜에서는 정보 획득자가 정당하게 태그 아이디 값을 획득해야만 정당한 값을 획득할 수 있다. 공격자가 리더에서 계속 오류를 발생시켜 하나의 태그 아이디 값을 획득하더라도 태그에 존재하는 카운터가 증분되어 태그 아이디 값이 변동되기 때문에 정확한 태그의 정보를 획득할 수 없다. 리더에서 발생하는 난수의 값을 해시 함수를 이용하여 태그에 전송하고 태그에서는 카운터 값과 같이 재차 해시함수를 이용하여 암호화하기 때문에 해독하기 힘들고 리더가 태그의 정보를 획득할 때마다 변동하는 값으로 인해 태그 아이디 값이 계속적으로 변한다. 따라서 스푸핑 공격에 의해 정당한 태그 정보를 획득하는 것은 불가능하므로 스푸핑 공격에 안전하다.

3) 도청 공격(Eavesdropping Attack)

공격자는 리더에서 태그로 전송되는 모든 값을 도청할 수 있다. 그러나 리더에서 생성한 난수를 해시함수로 암호화하여 태그에 전달하고 태그에서는 카운터와 태그 아이디를 해시 함수를 이용하여 암호화하여 리더에게 전달하기 때문에 실제 내용을 알 수 없다. 공격자는 리더에서 생성되어 암호화되어진 난수가 태그에서 재차 해시함수로 암호화되어 변화된 값을 도청하기 때문에 내용을 전혀 알 수 없지만 보호 채널간의 정상적인 후위시스템과 연결된 리더에서는 암호화되지 않은 난수 값을 전송한다. 따라서 후위시스템에서 해시함수로 암호화를 수행하여 값을 인증하기 때문에 정당한 정보를 인증할 수 있게 된다. 따라서 공격자의 도청공격에 안전하다.

4) 위치트래킹공격(Location Tracking Attack)

위치 트래킹 분석은 리더로 태그의 정보를 읽을 때마다 반복하여 같은 정보를 읽을 수 있기 때문에 위치 트래킹 공격을 할 수 있지만 제안한 프로토콜은 리더로 태그를 읽을 때마다 카운터의 값이 증분되고 태그 아이디와 리더에서 전송한 해시 함수로 암호화한 난수 값을 다시 해시 함수로 암호화하기 때문에 읽을 때 마다 값이 변경된다. 따라서 같은 리더가 태그의 정보를 다시 읽을 때에도 한 태그에서 같은 정보가 발생하지 않기 때문에 위치 트래킹 공격에 안전하다. 물론 다른 리더로 태그 정보를 읽을 때도 매번 태그 정보가 바뀌기 때문에 동일한 태그 정보를 리턴 받지 않는다. 따라서 사용자의 프라이버시를 보호할 수 있는 위치 트래킹 공격에 안전하다.

5) 서비스거부 공격(Denial of Service Attack)

제안 프로토콜에서는 매 세션마다 데이터베이스와 태그간에 상호인증을 한다. 만약 태그에 서비스 공격을 하면 태그는 자신의 카운터 값만을 증분하고 해시 연산을 수행하는 처리를 수행하기 때문에 태그에서 서비스 거부공격을 수행할 만큼의 많은 연산량을 요구하지 않는다. 또 태그를 이용하여 리더에 서비스 공격을 수행하더라도 리더에서 발생하는 특정 난수 값을 검증하기 때문에 서비스 거부 공격을 하지 못한다. 그리고 후위 시스템에 서비스 거부 공격을 하더라도 태그의 정보와 리더에서 넘어온 정보가 같은지를 비교 검증하여 다르면 바로

www.kci.go.kr

종료를 하기 때문에 제안 프로토콜은 서비스 거부 공격에 안전하다.

6) 트래픽 분석 공격(Traffic Analysis Attack)

태그가 리더가 읽을 때마다 같은 값을 전송한다면, 태그의 위치를 쉽게 파악할 수 있다. 따라서 태그에서 리더로 넘어오는 정보가 매번 같지 않고 다를 경우에 트래픽 분석을 할 수 없다. 제안 프로토콜은 리더에서 생성한 난수를 해시함수로 암호화한 다음 태그에게 전송하고 태그에서 암호화된 난수 값과 증분한 카운터의 값 그리고 태그의 아이디를 재차 해시함수로 암호화한다. 암호화 한 값은 리더가 같은 태그를 읽더라도 읽을 때마다 암호화 값이 바뀌기 때문에 태그의 이동 경로를 추적할 수 없으며 트래픽 분석공격에 안전하다.

7) 상호 인증(Mutual Authentication)

리더에서 생성된 난수를 해시함수를 이용하여 암호화 한 후에 태그에 전송하면 태그는 카운터와 태그 아이디 그리고 암호화된 난수를 다시 해시함수를 이용하여 암호화한 후 리더로 전송한다. 태그로부터 전송된 정보를 리더는 자신이 발생한 난수와 태그의 카운터 그리고 세 개의 값을 암호화하여 모두 후위 시스템에 전송한다. 태그에서 전송된 값인 H(TiD ‖ Cnt ‖ R_Rand))와 후위 시스템에서 역으로 계산하여 계산된 값이 태그에서 전송된 값이 같은지를 비교하여 상호 인증한다. 만약 전송 받은 값 H(TiD ‖ Cnt ‖ R_Rand))과 리더에서 전송받은 카운터 값 그리고 난수 값을 역으로 계산한 값이 같지 않으면 서로 상호 인증되지 않았기에 시스템을 종료한다.

8) 전방향 안전성(Forward Security)

기존의 많은 RFID 인증프로토콜들은 매 세션마다 동일한 하나의 태그 아이디만을 이용하여 상호인증을 수행한다. 따라서 폐기되거나 사용중지된 태그로부터 리더와 태그간의 교류된 과거 전송정보를 알 수 있기 때문에 정보의 무결성과 기밀성 보장이 힘들다. 제안한 RFID 인증 프로토콜은 후위시스템과 태그간의 상호인증 후에 태그의 아이디를 새롭게 생성한다. 그러므로 기존에 태그 정보를 알더라도 새롭게 생성된 정보는 기존 태그 정보와 다르며, 기존의 태그 정보를 가지고 있더라도 태그가 소유한 정보를 추적할 수 없어 전방향 안전성을 보장한다.

위과 같이 RFID 보안 인증 안전성 항목인 재전송 공격, 스푸핑 공격, 도청 공격, 위치 트래킹 공격, 서비스 거부 공격, 트래픽 분석 공격, 상호인증, 전방향 안전성에 대한 안전성 분석을 통해 본 논문에서 제안한 프로토콜이 RFID 보안인증에 안전함을 보였으며 사용자 프라이버시를 보호할 수 있음을 보여주었다.

표 3. 안전성 분석
Table 3. Safety Analysis

공격유형 \ 프로토콜	[2]	[7]	[8]	제안프로토콜
재전송 공격	X	O	O	O
스푸핑 공격	X	O	O	O
도청 공격	X	O	O	O
위치 추적 공격	O	O	O	O
서비스거부 공격	O	O	O	O
트래픽 분석 공격	O	O	O	O
상호 인증	O	O	O	O
전방향 안전성	X	O	O	O

표 3은 기존에 제안된 RFID 인증 프로토콜들과 본 논문에서 제안한 프로토콜에 대해 RFID 보안 인증 안전성 항목을 비교하여 나타내었다.

2. 효율성 분석

태그 아이디 검색 및 인증 시 사용되는 해시함수 연산을 후위 시스템에서 처리하고 태그에서 해시함수 연산을 제한하여 다른 인증 프로토콜보다 효율성을 높였다. 제안 프로토콜은 태그의 경량화에 목적을 두고 있기 때문에 태그에서의 연산보다는 리더나 후위 시스템에서 연산을 수행하였다. 태그에서는 해시함수를 이용한 해시연산은 한번만 사용하였으며 리더에서 리더 자신이 발생시킨 난수 값에 해시연산을 하여 암호화된 값을 태그에 넘겨주었다. 그리고 후위시스템에서 태그의 해시연산과 리더의 해시연산을 수행하여 리더에서 넘어온 값들이 맞는지 검증연산을 수행하였다.

표 4는 제안 프로토콜과 비교 프로토콜간의 후위 시스템과 리더 및 태그에서 사용되는 해시 연산, XOR 연산 및 난수 생성횟수 그리고 저장량에 대해서 비교 평가 하였다.

제안 프로토콜은 표 4에서 보듯이 태그에서 한 번의 해시연산과 카운터를 통해 자신의 정보를 암호화했으며, 리더에서 생성된 난수를 이용하여 상호인증을 한다. 후위시스템에서 태그 아이디와 리더에서 생성된 난수를 해시 연산을 통하여 암호화된 두 값을 XOR 연산을 하여 태그에 전달하므로 전방향 안전성을 제공한다. 따라서 기존의 RFID 인증 프로토콜보다 연산단계와 횟수를 줄임에도 불구하고 앞 절에서 열거한 RFID 보안인증 공격들에 안전함을 보이며, 태그에서도 계산을 현저히 줄였음을 알 수 있다.

www.kci.go.kr

표 4. 제안한 프로토콜과 기존 프로토콜간의 연산비교
Table 4. Comparison of computation between the proposed protocol and existing protocols

연산 종류 \ 시스템 객체		[7]	[8]	제안프로토콜
해시 연산	후위시스템	n+5	7	3
	Reader	3	3	1
	Tag	3	4	1
XOR 연산	후위시스템	1	0	0
	Reader	1	0	0
	Tag	0	0	0
Rand 생성 횟수	후위시스템	0	0	0
	Reader	1	1	1
	Tag	1	0	0
‖ 연산	후위시스템	0	10	2
	Reader	0	3	0
	Tag	0	4	2

‖ : 연접연산, Rand : 난수

성능분석으로는 RFID 인증 프로토콜 구성요소간의 계산요소에 대한 연산량과 상호 인증과 정보 전송을 위한 계산 오버헤드를 평가하였다.

계산 오버헤드를 위해서 해당 프로토콜에서 사용되는 연산 종류와 횟수를 계산하여 처리하였다. 표 5는 시스템 구성요소간의 연산량을 계산하여 표시한 것으로 태그와 리더간의 통신 스텝 및 리더와 후위시스템간의 통신 스텝 수 그리고 통신 시 전송되는 메시지 크기를 계산하여 각 구성요소간의 전송 메시지 연산량과 통신횟수를 정리하였으며 리더와 태그 간에 한 번의 해시 연산과 한 번의 쿼리 그리고 한 번의 난수를 이용하여 태그에게 메시지를 전달함으로 연산량을 간단하게 처리하였다.

표 5. 제안 RFID 시스템 구성요소 간 연산량
Table 5. The volume of computation among the components of the proposed RFID system

연산 종류	연산량 및 통신횟수
Reader에서 Tag로의 전송 메시지	1Q +1R +1h
Tag에서 Reader로의 전송 메시지	1h +Cnt
Reader에서 후위시스템으로 전송 메시지	1R +2h +Cnt +R_Cnt
Reader와 Tag간의 통신 라운드	2 최대(R_Cnt)
Reader와 후위시스템간의 통신 라운드	2
Tag ID 검색횟수	n

Q : 질의 수, h :해시연산 횟수,
R : 난수, Cnt : 카운터, R_Cnt : 반복 카운터

RIFD 시스템에서 오버헤드는 계산오버헤드와 저장오버헤드 그리고 통신오버헤드로 구분하지만 그림 5는 기존의 인증 프로토콜과 제안한 인증 프로토콜간의 계산오버헤드를 계산하였다.

그림 5. 제안프로토콜과 기타프로토콜에 대한 계산오버헤드
Figure 5. Computation overhead for proposed protocol and other types of protocol

결론적으로, 제안한 RFID 인증 프로토콜은 표 3, 4, 5 와 그림 5에서 알 수 있듯이 다양한 공격에 안전할 뿐만 아니라 시스템 구성요소간의 상호인증, 전방향 안전성을 제공하고 태그의 계산 오버헤드도 개선하였음을 알 수 있으며, 태그에서 계산처리 할 부분을 리더와 후위시스템에서 처리하도록 하였다. 즉, 계산 능력이 낮은 수동형 태그에 알맞도록 태그 암호화와 연산처리에 대해 안전성과 효율성을 높였음을 알 수 있다.

Ⅴ. 결론

본 제안 논문은 RFID 시스템의 보안 요구사항을 만족하는 경량화된 상호 인증 프로토콜이다. 태그의 연산처리 부분을 리더와 후위시스템에서 처리하도록 하였으며 태그에서 난수를 생성하지 않고 리더에서 생성된 난수를 해시연산을 이용하여 암호화 된 값을 태그에서 카운터 증분과 해시연산을 통해 암호화하였다. 태그에서 연산 처리에 대한 부담을 감소함에도 불구하고 태그 소유자의 위치 프라이버시가 보장되고 스푸핑 공격과 재전송 공격 그리고 트래픽 분석공격에 안전성을 갖는다.

본 논문은 태그의 정보를 한 번에 읽는 경우와 한 번에 읽지 못하는 경우 모두 처리하도록 카운터의 값을 리더가 재 카운터(R_Cnt)하여 후위시스템에게 넘겨줌으로 두 가지 경우를 모두 처리하도록 하였으며 RFID 시스템의 공격방법인 재

www.kci.go.kr

공격 전송, 사용자 프라이버시 보호공격 및 다른 공격에 더 안전한 경량화된 프로토콜을 제안하였다.

향후 과제로는 제안한 프로토콜의 시뮬레이션이나 구현을 통해, 제안한 프로토콜이 보다 경량화된 태그 환경에서 얼마나 사용 가능성이 높은지와 태그 프라이버시도 함께 보장됨을 증명할 수 있는 모델을 연구하고자한다.

참고문헌

[1] Yong-zhen Li, Hyung-Jin Mun, Yoon-su Jeong, Sang-ho Lee, "Mutual Authentication Protocol Of The Low-cost RFID Using Random Partial ID", The journal of Korea Information and Communication Society, 2006-7, Vol.31 No.7C.

[2] S. Wies, S.Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", Security in Pervasive Computing 2003, LNCS 2802, pp.201-212, 2003.

[3] Gi Oug Oh " A RFID secure Protocol and System Design Using Gray Code" Graduate School Soongsil University. Doctoral Thesis, 2007.

[4] K.Ree, J.Kwak, S. Kim and D.Won, "Cha -llenge-Response Based on RFID Authentication Protocol for Distributed Database Environment", SPC'05, LNCS 3450, pp.70-84, 2005.

[5] Jeongkyu Yang, Kui Ren, Kwangjo Kim, "Security and Privacy on Authentication Protocol for Low-cost RFID", SCIS 2005.

[6] Hung Yu Chien, Che Hao Chen, "Mutual aut -hentication protocol for RFID conforming to EPC Class 1 Generation 2 standards", Computer Standards & Interfaces 29, pp.254-259, 2007.

[7] Eun-Jun Yoon, Kee-Young Yoo, "A Design of RFID Mutual Authentication System based on Open Channel", The journal of Korea Information and Communication Society, 2009-10, Vol. 34 No. 10, pp946-954.

[8] Mi-Og Park, Gi Oug Oh "RFID Mutual Authentication Protocol on Insecure Channel for Improvement of ID Search", Journal of The Korea Society of Computer and Information, 2010-10, Vol 15 No 10, 1598-849X

저 자 소 개

오 기 욱

1991: 경원대학교 전자계산학과 공학사.

1993: 숭실대학교 컴퓨터학과 공학석사.

2007: 숭실대학교 컴퓨터학과 공학박사

현 재: 안양대학교 교양학부 조교수

관심분야: RIFD, USN, 보안

Email : ohgiug@paran.com

www.kci.go.kr

www.kci.go.kr