해시체인기반의 경량화 RFID 인증 프로토콜

윤근영* · 김동성* · 박종서*

요 약

해시 체인 기반의 여러 RFID 인증 프로토콜들이 제안되었다. 상태기반 인증 프로토콜과 시도 응답기반 인증 프로토콜은 위치추적 공격, 스푸핑 공격, 재전송 공격, 트래픽 분석 공격에는 안전하지만 DoS 공격에는 취약하고, 위치 추적과 서비스 거부 공격에 강한 RFID 인증 프로토콜은 위치추적 공격, 스푸핑 공격, 재전송 공격, DoS 공격에는 안전하지만 트래픽 분석 공격에는 취약하다. 본 논문에서는 이런 문제점들을 보완하기 위해 해시체인 인증 프로토콜과 위치 추적과 서비스 거부 공격에 강한 RFID 인증 프로토콜의 장점을 결합하여 좀 더 안정적이며 경량화된 RFID 인증 프로토콜을 제안한다. 제안 프로토콜의 보안성을 분석한 결과 위치추적 공격, 스푸핑 공격, 재전송 공격, 트래픽 분석 공격, DoS 공격 측면에서 안전한 것으로 나타나며 이외의 서버와 태그 내부에서의 연산량이 경량화된 RFID 인증 프로토콜임을 보인다.

A Lightweight RFID Authentication Protocol Based on Hash Chain

Keun-Young Youn* · Dong Seong Kim* · Jong Sou Park*

ABSTRACT

It has been proposed that several RFID authentication protocols based on hash chain. Status based authentication protocol and challenge-response based authentication protocol are secured against location tracking attacks, spoofing attacks, replay attacks, traffic analysis attacks but are vulnerable to Dos attacks. RFID authentication protocol with strong resistance against traceability and denial of service attack is secured against location tracking attack, spoofing attacks, replay attacks, DoS attacks but are vulnerable to traffic analysis attacks. The present study suggests a more secure and lightweight RFID authentication protocol which is combining the advantages of hash-chain authentication protocol and RFID authentication protocol with strong resistance against traceability and denial of service attack. The results of the secure analysis for a proposed protocol are illustrated that it is secured against location tracking attacks, spoofing attacks, replay attacks, traffic analysis attacks, Dos attacks and is a lightweight operation between server and tag.

Key words : RFID, Authentication protocol, Lightweight, Information Security

* 한국항공대학교 컴퓨터공학과

1. 서 론

RFID(Radio Frequency Identification) 시스템은 무선 주파수를 이용해 물리적 접촉 없이 개체에 대한 정보를 읽거나 기록하는 자동인식기술 시스템이다[1]. 바코드에 비해 저장능력이 뛰어나고, 비 접촉식이기 때문에 리더와의 시야확보를 고려할 필요도 없으며 인식 속도가 빨라 물류시스템에서 바코드를 대체할 인식 시스템으로 많은 연구가 진행되고 있다. 그러나 RFID 시스템이 물리적인 접촉 없이도 인식이 가능하다는 것은 보안이나 개인 프라이버시 침해에 대한 문제 등이 발생하게 된다는 뜻이 된다. 예를 들어 Tag의 정보를 식별 가능한 상태에서 보내질 경우 도청에 의해 쉽게 노출이 될 수 있다. 이를 바탕으로 위치추적, 트래픽 분석 공격 등이 가능하며 이로 인해 이 Tag가 부착된 물건을 구입하는 소비자의 개인 프라이버시가 침해될 수 있다[2].

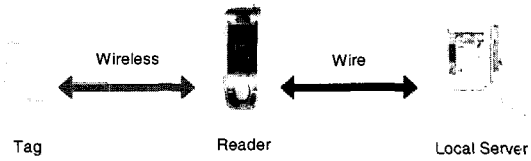
RFID 태그가 광범위하게 활용될 경우에 개인의 구매 패턴 및 선호도뿐만 아니라 물품 보유현황, 위치정보 등 개인 정보와 관련된 사항을 분석할 수 있다는 점에서 정보 침해 가능성이 존재한다[3]. 따라서 RFID 시스템의 안전한 운영과 보급의 확산을 위해 보안 방안이 필요하다.

그러나 RFID 시스템은 낮은 연산능력과 제한된 용량 등의 하드웨어적인 제한 때문에 높은 연산능력과 많은 용량이 필요한 기존의 통신환경에서 사용하는 보안 방법을 그대로 적용하기에는 힘들다[5]. 그래서 기존의 보안 방법론을 분석하고 적용 가능한 기술을 도입하여 효과적인 보안 시스템을 구성하는 것이 필요하다[3].

본 논문에서는 RFID 포핸드 보안을 위한 기존의 인증 프로토콜을 분석하고 이를 개선하기 위한 경량화 된 인증 프로토콜을 제안하고 검증한다. 초기에는 대부분 해시 기반의 인증 프로토콜이 제안되었다. 이 인증 프로토콜들은 DoS 공격, 위치추적 공격 등에 취약점을 지니고 있어 이를 개선하기 위해 해시 체인기반 인증 프로토콜[10], 상태기반 인증 프로토콜[2], 시도응답기반 인증 프로토콜[6], 위치 추적과 서비스 거부 공격에 강한 RFID 인증 프로토콜[5]이 제안되었다. 이 프로토콜들은 위치추적 공격, 스푸핑 공격, 재전송 공격, DoS 공격에는 안전하지만 트래픽 분석 공격에는 취약하다. 본 논문에서는 이런 문제점들은 보완하기 위해 해시체인 인증 프로토콜[10]과 위치 추적과 서비스 거부 공격에 강한 인증 프로토콜[5]의 장점을 결합하여 좀 더 안정적이며 경량화 된 RFID 인증 프로토콜을 제안하고 안정성 분석을 수행하고자한다.

2. 관련 연구

아래 (그림 1)은 기본적인 RFID의 네트워크 구조를 나타낸다.



(그림 1) RFID 시스템의 개략적 구조

리더와 서버간은 유선환경이므로 유선 환경에서 구현된 보안요소들을 적용시킬 수 있으나, 태그와 리더간은 무선 환경이므로 태그의 제한된 요소들로 인해 기존 방법을 응용한 더욱 효과적인 보안 방법을 필요로 하게 되었다. 태그와 리더간의 통신에서 보안요소를 적용하기 위해서는 양측 모두 암호화 연산을 사용할 수 있는 능력이 필요하지만. 현재의 수동형 RFID 태그에서는 이런 능력을 수행하기에는 힘들다[3].

2.1 해시 기반 인증 프로토콜

RFID의 무선구간에서의 인식거리가 확장되면서 도청의 위험과 불법적인 리더에 대한 위험이

더욱 커졌다. 단순한 도청만으로는 정보를 파악하거나 태그가 부착된 사물을 식별할 수 없어도 지속적인 도청을 통해 태그를 추적할 수 있으므로, 이에 대한 방지가 필요하게 된다. 특히, 수동형 태그는 연산능력이 부족하고 존재에 대해 미리 파악하기 힘들기 때문에 도청 위험이 크다.

불법적인 리더로 부터의 접근을 막기 위해 상대방을 인증하려면, 상대방의 인증정보를 유지해야 한다. 불법적인 리더를 태그가 식별하여 응답하기 어렵기 때문에 태그의 연산에 의한 서버의 리더 인증 형식을 통해 리더를 인증해야 하며, 인증된 리더만이 태그에 대해 접근할 수 있는 권한을 가진다[3]. 그러므로 제안되는 대부분의 기술형태는 직접적으로 태그가 리더를 인증 처리하는 것 보다 서버에 저장된 태그 정보를 기반으로 이루어지며, 리더는 서버로의 접근 권한을 갖고 있어야만 원하는 태그에 대한 식별 정보를 얻을 수 있다[3]. 또한 해시 메커니즘 자체로 주고받는 정보의 위조 방지가 가능하며 재사용 공격을 방지하기 위해 랜덤 값인 nonce 등을 이용해 재사용 여부에 대한 식별이 가능하도록 한다. 이 때 사전에 성공한 세션에서 사용한 해시의 키 값을 알고 있어야만 현재 세션에서의 인증이 가능하며 이전 세션 해시 키 값은 현재의 인증 처리를 위한 검증 정보로만 사용되어짐으로 최소한의 정보를 통한 안전한 보안 인증 요구사항을 만족하게 한다[7].

태그와 리더는 정보 교환을 위해 상대방에 대한 인증이 필요하고, 인증 정보를 유지해야 한다. 하지만 제한된 능력을 가진 태그가 불법적인 리더를 구별해 내기란 힘든 일이다. 그렇기 때문에 태그 연산에 의한 리더 인증이 아닌 서버에 의한 리더 인증의 형식으로 리더를 인증해야 한다[3].

태그와 리더간의 인증 프로토콜을 위해 초기에 제안되었던 프로토콜들은 대부분 해시기법을 사용하였다. <표 1>에서 보는바와 같이 제안된 프로토콜들은 재전송 공격에는 안전하나 Dos 공격, 위치추적 공격 등에 취약하다고 나타났다.

〈표 1〉 해시기반 인증 프로토콜에 대한 보안적인 취약점

인증기법	보안취약점
해시기반 ID변형 인증 프로토콜[8]	• 스푸핑 공격가능 • 위치추적 공격가능 • Dos 공격가능
개선된 해시기반 ID변형 인증 프로토콜[9]	• 위치추적 공격가능 • Dos 공격가능
해시체인 인증 프로토콜[10]	• 재전송 공격가능 • 스푸핑 공격가능 • Dos 공격가능 • 두 개의 서로 다른 해시 함수 사용으로 태그 가격 상승 • 많은 계산량 요구

최근의 RFID 인증 프로토콜은 Henrici의 해시기반 ID변형 인증 프로토콜[8]과 OhKubo의 해시-체인 인증 프로토콜[10] 두 방법을 기반으로 발전된 인증 프로토콜 연구가 활발하며, 많은 논문들이 OhKubo의 해시체인 인증 프로토콜[10]을 바탕으로 취약점을 해결한 인증 프로토콜들이 제안되고 있다.

해시를 기반으로 한 여러 인증프로토콜이 제안되었지만 재전송 공격에 안전하면 위치추적이나 스푸핑 공격에 취약하든가 위치추적이나 트래픽 분석 공격에 안전하다면 재전송 공격이나 스푸핑 공격에는 취약하다. 그러나 해시 락[1], 외부 재암호화[12]등의 이전 프로토콜들 보다는 취약점이 적고 좀 더 안전한 프로토콜들로 제안된 프로토콜들이다.

2.2 취약점 분석에 따라 제안된 프로토콜

해시 체인 인증 프로토콜을 기반으로 하여 위치추적 공격, 스푸핑 공격, 재전송 공격 등에 안전한 인증 프로토콜들이 <표 2>와 같이 제안되었다. 하지만 여전히 서버에 대한 DoS 공격이나, 트래픽 분석 공격 등에는 취약했다.

〈표 2〉 취약점 분석에 따라 제안된 인증 프로토콜에 대한 보안적인 취약점

인증 기법	보안 취약점
상태기반 인증 프로토콜[2]	• DoS 공격가능
시도 응답 기반 인증 프로토콜[6]	• DoS 공격가능
위치추적, 서비스 거부 공격에 강한 인증 프로토콜[5]	• 트랙픽분석 공격 가능

해시 체인 인증 프로토콜[10]을 기반으로 하는 것이 제안 프로토콜들의 공통점이며 Hash나 랜덤수, XOR등의 비교적 크기가 작은 연산 방법들을 이용한다.

상태기반 인증 프로토콜[2]은 해시체인 인증 프로토콜[10]의 가장 큰 취약점인 위치추적 공격에 대한 취약점을 보안하였다. 서버에서의 연산이 간단하고 Flag를 두어 이전 인증 세션의 정상 종료 여부를 확인하며 서버에서의 연산이 간단하다는 이점을 가진다. 그러나 서버에 대한 물리적인 DoS 공격에 대해서만 고려하여 불법적인 리더가 쓰레기 메시지들을 보내 계속적인 레코드 검색을 하게 만든다면 DoS 공격에 노출이 될 수 있게 된다.

시도응답 인증 프로토콜[6]은 해시체인 인증 프로토콜[10]의 위치추적 공격과 스푸핑 공격에 대한 취약점을 보안하였다. 리더와 태그가 각각 랜덤 수를 발생시키고 태그에서 랜덤 수 생성 시 비밀키를 사용하여 세션마다 정보가 달라지게 되므로, 재전송 공격과 스푸핑 공격에 안전할 수 있다. 하지만 이전 세션의 정상적인 종료여부를 고려하지 않고, 서버에서 단순한 정보들의 비교만으로 인증을 하여 DoS 공격에 노출되어 있다.

위치추적과 서비스거부 공격에 강한 인증 프로토콜[5]은 정보 노출과 위치추적 문제에 중점을 두었다. 서버에서의 DoS 공격에 대한 취약점을 보안하였고, 이전 세션의 정상 종료 여부를 SFlag로 구분하여 각각에 대해 다른 연산을 수행하고, 위치 추적 공격에 대한 취약점을 보안하였다. 하지만 태그와 서버에서 많은 연산이 일어나며 많은 가정 하에 제안되어 도청에 노출될 경우에 대한 대안이 없이 도청에 의한 트래픽 공격에는 노출되어 있다.

3. 제안 프로토콜

다양한 인증 프로토콜들이 제시되고는 있지만 대부분 해시 체인 기반의 인증 프로토콜을 바탕으로 변형되어 여러 공격에 대한 취약점을 보안하거나, 너무 많은 가정 하에 제안되는 경우이며 태그의 연산량을 많이 필요로 하는 방법들이다.

태그에 대한 연산량을 줄이려면 이전 인증세션 종료여부를 체크하는 과정이나, RSA 알고리즘, Knapsack 알고리즘 등의 복잡한 연산 알고리즘은 사용할 수 없다. 또한, 이전 인증세션 종료여부에 따른 연산을 생각하지 않거나, 간단하게만 이루어지는 연산은 보안에 취약한 알고리즘이 될 수 있다.

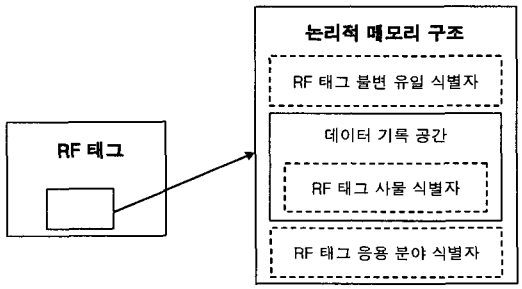
반대로, 이전 인증세션 종료여부에 대해 각각에 서로 다른 연산을 하거나, 복잡한 연산은 보안에는 안전할 수 있지만, 태그의 연산량의 증가 등의 문제를 발생시킨다. 태그에서 안정성을 보장하려면 이전 인증세션의 종료여부에 대해 확인을 해야 하며, 연산이 간단해 지면서도 안정적이어야 한다. 이에 다음과 같은 프로토콜을 제안한다.

3.1 태그 구조

태그가 스스로 불법적인 리더를 구별해 내기는 힘들기 때문에 태그는 서버를 통해 불법적인 리더의 공격을 구별해 내야 한다.

(그림 2)은 RFID 태그 식별자에 대한 개념도이다[4]. 태그 불변 유일 식별자(일명 태그 ID)는 특정 RFID 태그를 항상 고유하게 구별하기 위한 목적으로, 태그의 IC 생산자 또는 태그 제조자에 의해 태그에 고정 기록되는 태그 식별자이다. 즉 RF 태그 불변 유일 식별자는 태그의 IC 제조 시점이나

태그 제조 시점에 결정되는 식별번호로 어떤 응용 분야나 공간 및 상황에 대해서도 유일한 식별을 보장한다는 특징을 가진다. RF 태그 불변 유일 식별자는 하나 이상의 RFID 리더의 다수 안테나 설정환경에서 특정 RFID 태그를 완벽하게 인식하기 위해 사용할 수 있다. 또한 RFID 태그의 생산 절차와 그 생명주기 동안의 추적을 위해서, 또는 RFID 태그가 부착된 아이템을 추적하기 위해 사용하는 ID이다.



(그림 2) RFID 태그 식별자 개념도

RF 태그 사물 식별자(일명 Item ID)는 RF 태그가 부착된 사물을 고유하게 구별하기 위한 목적으로 RF 태그이용자가 결정하여 RF 태그의 메모리에 기록될 수 있는 식별자이다.

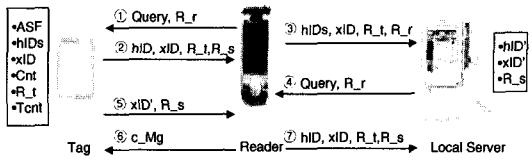
태그ID와 ItemID를 이용하여 인증을 한다면, ItemID는 제품에 사용할 때 마다 바뀌므로, 재사용성도 보장될 뿐만 아니라 두 개의 ID로 해시와 XOR 연산 등을 통해 좀더 안전한 인증 프로토콜 모델이 만들어 질 수 있다.

3.2 제안 프로토콜의 구성 및 인증 과정

이 논문에서는 전체적인 Tag와 서버에서의 연산량은 줄이면서도 좀 더 안전한 인증 프로토콜을 제안하고자 한다.

3.2.1 기본 구조와 매개변수

제안하는 인증 프로토콜은 (그림 3)과 같은 구조를 가진다.



(그림 3) 제안 프로토콜 기본 구조

[사용 매개변수]

- ASF(Authentication Session Flag)
  : 이전 세션의 정상종료 여부를 나타낸다. 정상적으로 종료되었을 경우 '0'이 되고, 비정상적으로 종료되었을 경우 '1'이 된다.
- hIDs(hash IDs)
  : 태그ID와 ItemID를 count 변수와 함께 연접하여 해시 한다. 다른 태그들과의 구별을 위해서 사용한다.
- xID(XOR ID)
  : 해시된 hIDs들을 랜덤 수와 XOR 연산을 하여 사용 한다.
- cnt(count)
  : 이전 세션이 정상 종료되었다면 저장되어있던 cnt사용하고, 이전 세션이 비정상 종료되었다면 랜덤한 새로운 변수를 생성한다. 정상적으로 종료시 바뀐 값을 저장해 둔다.
- R_t(Random_tag), R_r(Random_reader), R_s (Random_server)
  : 각각 태그, 리더, 서버에서 생성하는 랜덤 숫자이다.
- Tcnt(Transaction Count)
  : 세션이 시작하면서 생성되어 시도한 횟수에 대해 증가한다.
- c_Mg(Confirm Message)
  : 태그와 서버간의 인증이 정상적으로 이루어졌음을 알리는 메시지이다.

안전한 인증을 위해 태그, 리더, 서버가 각각 랜덤 수를 발생시키고, 해시 함수와 XOR 연산을 사용한다. 또한, ASF를 이용해 이전 세션의 정상, 비정상 종료여부를 파악하며, Tcnt 변수를 이용해 DoS공격을 대비한다.

3.2.2 인증과정 알고리즘

(1) 리더는 태그에 대한 정보를 얻기 위해 Query를 태그로 보내야 한다. 이런 경우 태그는 불법적인 리더의 접근인지 합법적인 리더의 접근인지 판별을 해야 한다. 그러나 힘들기 때문에 Local Sever와의 인증 프로토콜을 이용하여 합법적인 리더일 때만 정보를 제공하게 된다. 그래서 리더는 태그로 Query를 보낼 때, 랜덤 수 R_r을 생성하여 Query와 함께 태그로 전달한다.

(2) 태그는 인증세션을 시작하기 이전에 이전 인증에 대해 정상적인 종료인지 비정상적인 종료인지에 대해 ASF를 이용해 확인한다. 이전 세션이 정상적으로 종료되었다면 저장되어 있던 cnt를 이용해 hIDs와 xID를 연산하여, 리더와 태그가 생성한 랜덤 수와 함께 서버로 보낸다. 이전 세션이 비정상적으로 종료되었을 경우, Tcnt를 통해 세션 종료 시까지 접근 횟수를 count 하여 max_count가 되면 DoS 공격으로 간주하고 현재의 세션에 대해 종료한다.

(3) 정상적으로 서버에 정보가 도착하면, 서버는 이미 연산되어 저장된 hIDs'를 검색한다. hIDs'가 검색되지 않으면, 공격으로 간주하고 현재의 세션을 종료하고, hIDs'가 검색되면 태그가 보낸 R_t, R_r을 이용해 검색된 hIDs'와 xID'를 만들어 낸다. 만들어진 xID'와 태그가 보낸 xID가 같으면 서버의 랜덤 수인 R_s를 생성하여 xID'와 R_s를 태그로 전송하고, 같지 않으면 공격으로 간주하고 세션을 종료한다.

(4) 정상적으로 xID'와 R_s를 받으면 c_Mg를 서버로 보내 정상적인 인증이 되었다고 판단하여 인증 세션을 종료하고, 정상적으로 xID'와 R_s를 받지 못하면 공격으로 간주하고 세션을 종료한다.

(5) 서버는 태그로부터 c_Mg를 받으면 정상적인 인증 세션이 이루어졌다고 판단하고 바뀐 hIDs'를 Update한뒤 세션을 종료하고, c_Mg를 받지 못하면, 공격으로 간주하고 세션을 종료한다.

4. 보안에 대한 안전성 분석

본 장에서는 제안 프로토콜 보안에 대한 안정성을 분석하고 기존에 제안되었던 Ohkubo의 해시 체인기반 인증 프로토콜[10], 상태기반 인증 프로토콜[2], 시도 응답기반 인증 프로토콜[6]

〈표 3〉 기존 인증 프로토콜들과 제안 인증 프로토콜에 대한 비교

	해시체인기반 프로토콜[10]	상태기반 프로토콜[2]	시도-응답기반 프로토콜[6]	위치추적 서비스 공격에 강한 프로토콜[5]	제안 프로토콜
위치추적 공격	안전	안전	안전	안전	안전
스푸핑 공격	취약	안전	안전	안전	안전
재전송 공격	취약	안전	안전	안전	안전
DOS 공격	취약	취약	취약	안전	안전
트래픽 분석 공격	안전	안전	안전	취약	안전
태그 계산 정도	h2	h3	h2, R1	h2, R1(2)	h1, R1
DB계산량	비밀값 갱신횟수*ID	$\sqrt{ID}$	ID	not	not

위치 추적과 서비스 거부 공격에 강한 인증 프로토콜[5]들을 분석하여 좀 더 안정적이고 좀 더 효율적인 인증 프로토콜과 비교하여 우수성을 보인다. <표 3>을 통해 기존의 인증 프로토콜과 제안 인증 프로토콜들을 비교하여 요약하였다.

4.1 위치추적 공격에 관한 안전성

위치 추적 공격은 도청을 이용하여 태그의 정보를 감시함으로써 일어날 수 있다. 이를 방지하기 위해 상태기반 인증 프로토콜[2]과 위치 추적과 서비스 거부 공격에 강한 인증 프로토콜[5]은 태그 내에서의 랜덤 수인 R_t를 생성하여 매 세션마다 응답을 바꾸어 전송하게 된다. 그렇게 되면 위치추적을 하기 위해 매 세션마다 바뀌는 랜덤수를 알아야 하는데 이는 불가능 하게 된다. ASF를 사용해 이전 세션에 대한 정상 종료 여부를 확인하고, cnt의 이용으로 hIDs가 매 세션마다 변하게 되므로 ID가 노출된다고 해도 랜덤 수들을 모두 예상하거나 연산하여 위치 추적 공격을 할 수는 없다.

4.2 스푸핑 공격에 관한 안전성

불법적인 리더가 정상적인 리더인 것처럼 속이고 공격을 할 수 있지만, 랜덤 수를 알아내야만 연산이 가능하므로, 시도 응답 인증 프로토콜의[6] 연산과 같이 리더와 태그에서의 랜덤 수들을 모두 추측하기란 불가능하다. 또한, 불법적인 리더가 정당한 리더로 가정하여, Query와 R_r을 추측하여 보낸다고 해도 cnt와 서버가 발생시키는 랜덤 수 R_s를 추측하여 다시 연산된 메시지를 보내야 하므로 이런 스푸핑 공격은 불가능하다.

4.3 재전송 공격에 관한 안전성

불법적인 리더나 공격자가 도청을 통해 재전송 공격을 하려고 하면, 매 세션마다 바뀌는 랜덤 수들을 알아야 하는데 랜덤 수들은 매 세션마다 달라질 뿐 아니라 시도 응답 인증 프로토콜의[6] 연산과 같이 리더가 생성하는 R_r를 이용하므로 공격자는 서로 다른 응답이 동일한 태그에서 전송하는 것인지 알 수가 없다. 또한 Tag의 cnt와 서버의 R_s를 추측하여 매 세션마다 바뀌는 정보를 재전송하기는 어려우며 만약 태그에서 전송하는 메시지를 도청하여 이에 대한 응답을 추측하여 보낸다고 해도, 추측하여 연산하는 시간이 굉장히 짧아야 하므로 이는 불가능하다. 또한 서버는 새로 연산된 xID'와 서버에서 발생시킨 랜덤 수 R_s를 태그로 보내 인증이 되었다는 것을 확인하고 태그는 이 c_Mg를 서버에 보내 메시지를 받지 못했을 경우 재전송 공격으로 판단하여 현재 세션을 종료하여 재전송 공격에 안전할 수 있다.

4.4 DoS 공격에 관한 안전성

서버의 연산은 위치 추적과 서비스 거부 공격에 강한 인증 프로토콜[5]과 유사하게 서버 내에 이미 연산되어진 hIDs'가 저장되어 해시 연산을 따로 하지 않아 공격자가 해시 연산을 수행할 수 없다. 또한 전달되어진 랜덤변수와 저장되어진 hIDs'로 XOR 연산하여 Tag의 연산과 같지 않을 경우 이에 대해 공격으로 간주하고 확인된 hIDs에 대해서만 연산하기 때문에, 서버에 존재하지 않는 잘못된 메시지나 공격이 들어오면 연산이나 검색을 하지 않게 된다. 그렇기 때문에 DoS 공격에 대해 안전할 수 있다. 또한 태그에서는 Tcnt 변수를 사용하여 시도횟수를 count하여 max_Tcnt에 도달하면 현재 세션을 종료시켜 태그에 대한 DoS 공격에 대해서도 안전할 수 있다.

4.5 트래픽 분석 공격에 관한 안전성

무선 환경을 이용한 불법적인 도청을 완전히 차단하기에는 아직까지는 큰 어려움이 따른다. 그래서 RFID 보안에서는 Forward Security를 보장

하여야 한다. 그렇게 된다면 도청한 정보가 어떠한 불법적인 이유로도 쓰일 수 없으므로, 도청에 의한 다양한 공격들에 대해서 안전하게 된다. 또한 도청만으로는 서로 달리 생성되는 모든 랜덤 수들의 추측하여 연산하기 어렵고 매번 바뀌는 태그의 응답을 모두 추측할 수 없으며 추측하여 연산한다 하더라도 이에 따른 연산이 짧은 시간 내에 이루어 질 수 없어 도청에 의한 정보를 이용한 불법적인 리더의 위치 추적이나 태그의 이동경로에 따른 프라이버스 침해 등에 공격은 불가능하다.

본 논문에서 제안하는 인증 프로토콜은 보안 안정성을 제공할 뿐만 아니라 태그와 서버의 연산량을 감소시키는 효과를 가진다. 또한 상태기반 인증 프로토콜[2]와 위치 추적과 서비스 거부 공격에 강한 인증 프로토콜[5] 같이 이전 인증 세션의 정상적인 종료 여부에 대해서도 고려하였다, 태그내부의 ID들을 사용하여 추가되거나 늘어나는 용량이 필요 없는 재사용성을 제공한다.

5. 결 론

RFID 인증 프로토콜에서는 위치추적 공격, 스푸핑 공격, 재전송 공격, DoS 공격, 트래픽 분석 공격 등의 취약점에 안전하면서도 적은 연산량으로 인증 과정을 수행해야 한다.

본 논문에서는 태그와 서버의 연산량을 줄이면서도 안정성을 보장할 수 있으며 재사용성도 가진 RFID 인증 프로토콜 모델을 제안하고, 이 프로토콜에서 일어날 수 있는 공격들에 대한 안정성을 분석하였다. 위치 추적공격, 스푸핑 공격, 재전송 공격, DoS 공격, 트래픽 분석 공격에 대한 안전성도 검증하였다.

향후 연구로 이 프로토콜의 안정성에 대해 좀 더 객관적으로 평가하기 위해 모델 체킹 기반의 분석을 수행할 것이다. 또한, 태그와 리더, 서버 내부의 연산량에 대해 세부 분석을 수행할 것이다.

참 고 문 헌

[1] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy As pects of Low-Cost Radio Frequency Identification System", Security in Pervasive Computing 2003, LNCS 2802, 2004.

[2] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜", 정보보호학회 논문지 제14권, 제6호, 2004.

[3] 노병희, 고현봉외 12명, 전자식별(RFID)보급 활성화를 위한 역기능 및 정보보호대책연구, 한국전산원, 2004.

[4] 유승화, 유비쿼터스 사회의 RFID, 전자신문사, 2005.

[5] 강전일, 양대헌, "위치 추적과 서비스 거부공격에 강한 RFID 인증 프로토콜", 인하대학교 정보통신대학원, 한국정보보호학회 논문지 제15권, 제4호, 2005.

[6] 이근우, 오동규, 곽진, 오수현, 김승주, 원동호, "분산 서버환경에 적합한 Challenge-Response 기반의 안전한 RFID 인증 프로토콜", 성균관대학교, 정보처리학회논문지, 제12-C권, 제3호 2005.

[7] 서운석, 신순자, 구자동, 임진수, "유비쿼터스 컴퓨팅 환경에서 보안 및 인증서비스 방향연구", 한국전산원, 2004.

[8] D. Henrici, and P. Muller, "Hash-based Enhancement of Location Privacy for Radio -frequency Identifiers", Procedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Work shops(PERCOMW'04), IEEE, 2004.

[9] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 한국정보보호학회 하계정보보호학술대회 논문집 Vol. 14, No. 1, 2004.

[10] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-Chain Based Forward-Secure Privacy Protection Scheme for Low-Cost RFID", Proceedings of the SCIS 2004, 2004.

[11] Miyako Ohkubo, Koutarou Suzuki, Shingo Kinoshita, "Cryptographic Approach to "Privacy-Friendly", "Tags", RFID Privacy Workshop MIT, 2003.

[12] A. Juels. and R. Pappu, "Squealing Euros : Privacy protection in RFID-enabled banknotes", Financial Cryptography'03, LNCS 2742, Springer-Verlag Heidelberg, 2003.

윤 근 영

2004년 한국항공대학교 컴퓨터 공학과 졸업

2004년~현재 한국항공대학교 컴퓨터공학과 석사 과정

김 동 성

2001년 한국항공대학교 전자 공학과 (공학사)

2003년 한국항공대학교 컴퓨터 공학과(공학석사)

2003년~현재 한국항공대 학교 컴퓨터공학과 박사 과정

박 종 서

1983년 한국항공대학교 항공통신 공학과(공학사)

1986년 North Carolina State Univ. 대학원(공학 석사)

1994년 Pennsylvania State Univ. 대학원(공학박사)

1996년~현재 한국항공대학교 컴퓨터공학과 부교수