情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

RFID를 위한 HB++ 프로토콜의 공격 방법 연구*

신 수 연† , 권 태 경‡
세종대학교

A study of various attacks on the HB++ protocol for RFID*

Sooyeon Shin† , Taekyoung Kwon‡
Sejong University

요 약

RFID 태그의 연산 능력의 제한으로 인해 RFID 시스템은 경량화된 인증 프로토콜을 필요로 하며, 최근 몇 년간 이에 대한 연구가 이루어져왔다. 본 논문에서는 RFID 시스템을 위한 경량화된 인증 프로토콜인 HB 프로토콜과 그 변형 프로토콜들에 대해 살펴보고 해당 프로토콜의 공격에 대해서 살펴본다. 그 중에서도 HB++ 프로토콜에 대한 Piramuthu의 공격이 문제가 있음을 지적하고 안전한 프로토콜을 위한 설정을 제안한다.

ABSTRACT

Lightweight authentication protocols are necessary in RFID systems since a RFID tag has computation constraints. Over recent years, many protocols have been proposed. In this paper, we examine the HB protocol and its variants, and their vulnerabilities to attacks. We analyze the problem of Piramuthu's attack on the HB++ protocol and propose solutions to it.

Keywords: RFID, Authentication, LPN problem, HB protocols

I. 서 론

RFID (Radio Frequency Identification)는 사물과 사람을 자동적으로 식별할 수 있는 유비쿼터스 컴퓨팅 환경의 핵심기술로 현재 이를 상용화하기 위한 연구와 노력들이 지속되고 있다. RFID 시스템의 확산을 위해서는 이를 위한 기반시설 구축과 관련 기술들의 개발 뿐 만 아니라 해당 시스템 구축 시 발생 가능한 사생활 침해와 보안 문제를 해결해야 할 필요가 있다. 학계에서는 이를 위한 보안 기술들이 제안되고 있는데, 이 중에서 휴먼 인증 방식은 사람과 RFID 태그의 계산/연산 능력이 비슷한 것에 착안하여, HCI 분야에서 사용되던 인증 기술을 RFID 시스템에 적용한 것이다. HB 프로토콜[6]은 휴먼 인증을 위해 Hopper과 Blum이 제안한 프로토콜로 암호 프리미티브는 사용하지 않지만, NP-hard급의 LPN (Learning Parity with Noise) 문제에 기반하여 안전성을 제공한다.

2005년 Juels et al.은 RFID 태그의 연산 능력이 사람과 마찬가지로 제한되어 있음을 밝혀내고, 이를 RFID 시스템에 적용시켰다[7]. 뿐만 아니라 능동 공격(active attack)에 취약함을 밝혀내고 이를 개선한 HB+ 프로토콜을 제안하였다. 하지만, 2006년 Katz와 Shin[9], 그리고 Gilbert et al.[4]은 HB 프로토콜과 HB+ 프로토콜의 공격에 성공하였다. 2007년 Bringer et al.은 중간자 공격에 취약한 HB+ 프로토콜의 안전성을 강화하기 위해 순열 함수(permutation fucntion) f와 로테이션(rotation)을 사용하는 HB++ 프로토콜을 제안하였다[2].

접수일(2010년 8월 18일), 게재확정일(2010년 10월 9일)
* 이 논문은 2008년도 세종대학교 교내연구비 지원에 의한 논문임.
† 주저자, shinsy80@sju.ac.kr
‡ 교신저자, tkwon@sejong.ac.kr

Piramuthu는 HB+ 프로토콜로 부터 발생되는 z 값 노출의 문제가 Bringer et al.의 HB++ 프로토콜에도 영향을 미침을 밝혀낸 뒤, 이를 개선한 경량 HB++ 프로토콜을 제안하였다[13]. 2007년 Duc과 Kim은 새로운 확률 변수 γ 추가하여 HB+ 프로토콜을 개선한 HB* 프로토콜을 제안하였으며[3], Munilla와 Peinado는 HB 프로토콜과 HB+ 프로토콜의 중간자 공격을 방어하기 위해 개선된 HB+ 프로토콜인 HB-MP 프로토콜을 제안하였다[12]. 하지만, 여전히 HB*과 HB-MP 프로토콜은 중간자 공격이 가능하며, 심지어 HB-MP 프로토콜은 수동 공격(passive attack)에 취약하다[16]. 2008년 Gilbert et al.은 단일 라운드에서 실행되지만, 저전력 태그에서 두 개의 큰 랜덤이진 행렬 혹은 Toeplitz 행렬을 요구하는 HB# 프로토콜을 제안하였으며[5], Leng et al.은 HB-MP 프로토콜의 취약성을 보완하기 위해, 비밀 키의 로테이션을 랜덤하게 하는 HB-MP+ 프로토콜을 제안하였다[10]. 2009년 Yoon et al.은 HB-MP+ 프로토콜은 복잡한 능동 공격을 방어하기 위한 로테이션을 위한 실제 함수와 트래킹(tracking) 문제를 방지하기 위한 강력한 방법을 가지지 않았음을 지적하고 이를 개선한 HB-MP++ 프로토콜을 제안하였다[16].

본 논문에서는 기존 HB 프로토콜들과 이들의 취약점에 대해 간략히 설명하고, Bringer et al.의 HB++ 프로토콜에 대한 Piramuthu의 공격에 문제가 있음을 밝혀낸 뒤, 안전한 프로토콜을 위한 태그의 상태 전이 및 해밍 무게(Hamming weight) 설정을 제안한다.

본 논문은 다음과 같이 구성된다. 먼저 II장에서는 HB 프로토콜과 그 변형 프로토콜에 대해 간략히 설명하고 이들의 취약점에 대해 설명하고, III장에서는 Piramuthu의 HB++ 프로토콜에 대한 공격과 HB++ 수정 프로토콜에 대해 설명한다. IV장에서는 Piramuthu의 공격에 대한 문제점을 지적하고 안전한 프로토콜을 위한 제안을 하고 V에서는 이 논문의 결론을 맺는다.

II. HB 프로토콜 및 그 변형

2.1 HB 프로토콜

Hopper와 Blum에 의해 제안된 HB 프로토콜은 사람과 컴퓨터 간의 비밀 값인 x를 통해 인증을 시도하는 프로토콜이다[6]. 먼저 컴퓨터는 사람에게 난수 a를 전송하면 사람은 자신의 비밀 값 x와 전송 받은 a 값에 bitwise AND 연산을 한 뒤 해당 결과의 패리티를 다시 컴퓨터에게 전송해 준다. 이 때, 사람은 η만큼의 확률로 잘못된 패리티 값을 컴퓨터에게 전송해 주게 되는데, 컴퓨터는 n 라운드만큼의 프로토콜을 수행했을 때 해당 세션의 패리티 값이 성공 확률이 $1-\eta$ 보다 크다면 적법한 사람임을 인증하게 된다. HB 프로토콜은 주어진 확률 η안에서 비정규적으로 인증 실패를 발생시키는데, 이를 LPN (Learning Parity Noise) 문제라고 부른다. NP-Hard급으로 분류되는 LPN 문제는 정규적인 방법으로 공격되지 않기 때문에 수동 공격에 안전하다.

Juels와 Weis는 HB 프로토콜이 재사용 공격(replay attack)과 같은 능동 공격에 취약함을 밝혀내었다[7]. HB 프로토콜에서 패리티 비트인 결과 값 z는 고정된 비밀 값 x를 제외하면, 리더의 난수인 a에 의해 결정되기 때문에 재사용 공격에 취약할 수밖에 없다. 즉, 정당한 리더로 가장 공격자는 언제든지 태그의 비밀 값 x를 얻어낼 수 있는 결과가 생긴다.

2.2 HB+ 프로토콜

Juels와 Weis는 HB 프로토콜의 취약성을 개선하기 위해, 태그가 리더에게 보내는 은닉 요소(blinding factor) b를 프로토콜 상에 추가한 HB+ 프로토콜을 제안하였다[7]. HB+의 결과 값 z는 리더의 난수 a뿐만 아니라, 태그의 난수 b에도 의존하기 때문에, 재사용 공격을 통해서는 비밀 값을 얻어낼 수 없다.

Gilbert et al.은 HB+ 프로토콜이 중간자 공격에 취약함을 밝혀내었다[4]. 공격자는 리더가 보내는 난수 a를 막은 뒤 한 비트에 영향을 미치는 δ_i와 XOR하여 변조된 값 a'를 태그에게 전송한다. 정상적인 값 a를 수신했을 연산과 $z' = (a' \cdot x) \oplus (b \cdot y) \oplus \nu$를 비교해 봤을 때, 변조된 값을 통한 연산은 $(\delta_i \cdot x)$가 추가된다. 위의 가정에서 공격자는 태그에 대한 리더의 인증 성공/실패를 알 수 있기 때문에, $(\delta_i \cdot x)$의 값을 알아낼 수 있다. 해당 세션의 공격을 k비트만큼 수행하면 비밀 값 x를 쉽게 알아낼 수 있다. 공격자는 알아낸 비밀 값 x를 통해 태그를 복제할 수 있는데, 은닉 요소 b를 항상 0으로만 보냄으로써 비밀 값 y를 무력화 시킨다. 또 다른 방법으로 태그가 리더에게 보내는 은닉 요소 b에 대해서도 중간자 공격을 수행함으로써 비밀

값 y를 알아낸 뒤, 비밀 값 x, y 쌍을 모두 갖는 완벽한 태그를 복제할 수 있다.

2.3 HB++ 프로토콜

Bringer et al.는 HB+ 프로토콜에 대한 중간자 공격을 막기 위해 두개의 추가된 비밀 값 x', y'과 순열 함수 f를 사용하는 HB++ 프로토콜을 제안하였다[2]. 먼저 은닉 요소 b를 전송한 태그는 리더가 보내는 도전(challenge) a에 대해 $z=(a\cdot x)\oplus(b\cdot y)\oplus\nu$와 $z'=f(a)\cdot x'\oplus f(b)\cdot y'\oplus\nu'$을 결과 값으로 전송한다. 해당 프로토콜에서 생성되는 노이즈(noise)인 ν와 ν'은 동일한 확률로 발생하지만 발생하는 순서는 동일하지 않으므로 z와 z'의 성공/실패 여부는 동일하지 않다. HB++ 프로토콜의 한 세션은 z와 z'이 각각 $\eta z, \eta z'$ 보다 작은 확률로 실패 할 때 인증에 성공한다.

Bringer et al.의 HB++ 프로토콜은 f의 사용에도 불구하고, Wagner의 중간자 공격을 통해 비밀 값이 노출됨이 확인되었다. Bringer et al.은 이를 해결하기 위한 방법으로 로테이션을 사용하였다. 즉, 암호화된 값을 비트의 로테이션을 통해 정규적인 암호 값을 추측할 수 없도록 만들어, 최종 HB++ 프로토콜을 제안하였다. 최종 HB++ 프로토콜은 인증을 위한 선행 키 교환 프로토콜과 실제 인증을 위한 프로토콜로 나뉜다. HB++ 프로토콜에서 각 태그들은 키를 비밀 값 x,x',y,y'를 미리 갖지 않는 대신, 키를 도출해 낼 비밀 값 Z를 갖는다. 인증을 위한 키 교환 프로토콜은 각 세션의 인증이 시작될 때마다 이루어지는 과정으로 태그-리더 사이에 난수 B,A를 주고 받은 뒤 이 값들에 대해 해쉬 함수 h를 사용하여 실제 인증에서 사용할 비밀 값 x,x',y,y'을 매번 다르게 생성한다. 또한 첫 번째 HB++에 대한 Wagner의 중간자 공격에 강인한 프로토콜을 만들기 위해 기존 순열 함수 f의 출력 값을 각 라운드에 따라 로테이션 시켜서 (a,δ,δ') 집합을 추측하기 힘들도록 만들었다. 따라서 이를 통한 비밀 값 x와 x'의 추측 공격이 불가능하도록 개선하였다.

III. Priamuthu의 HB++ 수정 프로토콜

3.1 Piramuthu의 공격

Piramuthu는 Juels과 Weis의 HB+ 프로토콜이 중간자 공격과는 다른 방식의 공격에 취약함을 주장하였으며[13], 해당 공격은 다음과 같다.

- 빠른 질의 공격: 해당 공격에서 공격자는, 태그가 새로운 은닉 요소 b를 생성하기 이전에, 새로운 도전 a를 빠르게, 지속적으로 전송함으로써 은닉 요소 b의 난수성을 제거한다. 이를 통해 공격자는 HB+ 프로토콜에 대한 능동 공격이 가능해진다.
- LPN 문제를 풀어내는 공격: 해당 공격에서 공격자는 도전 $a=0$인 값을 보냄으로써, 태그의 응답(response) z값이 항상 $(b\cdot y)$가 되도록 조절한다. 태그가 보내는 은닉 요소 b를 미리 알고 있는 공격자는 지속적인 질의를 통해 (b,z)쌍을 추출하여 y값을 알아낸다.

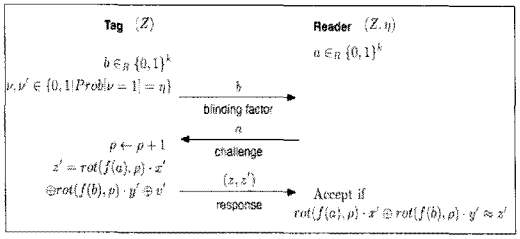
Piramuthu는 또한 두 개의 비밀 값 x',y'가 추가된 Bringer et al.의 HB++ 프로토콜에 대해서도 공격이 가능함을 주장하였다[13]. HB++ 프로토콜에 대한 Piramuthu의 공격은 다음과 같다.

- z값 노출: HB+로부터 기인하는 문제로써 Gilbert et al.의 중간자 공격 또는 위에서 제기한 두 가지 방법(빠른 질의 공격 및 LPN 문제를 풀어내는 공격)을 통해 HB++의 비밀 값 x,y가 노출 될 수 있다. 비밀 값 x,y를 알게 된 공격자는 해당 태그에 대해 불법적인 추적을 할 수 있다.
- 빠른 질의 공격: 해당 공격에서 공격자는 빠른 질의를 통해 은닉 요소 b의 난수성을 제거하고 로테이션 수행에 영향을 미치는 ρ값의 증가를 막음으로써 (b,ρ)값이 변하지 않도록 유지한다.
- 동일한 (b,ρ)상에서 a 변조 공격: 빠른 질의 공격을 통해 (b,ρ)값이 변하지 않게 된다면, 공격자는 다음과 같은 단계를 통해 비밀 값 x',y'을 추출할 수 있다.

1. $a=0$을 전송하여 $rot(f(b),\rho)\cdot y'$ 추출
2. $a=1$을 전송하여 $1\cdot x'\oplus rot(f(b),\rho)\cdot y'$추출
3. 추출한 $rot(f(b),\rho)\cdot y'$와 $1\cdot x'\oplus rot(f(b),\rho)\cdot y'$를 XOR하여 x'값 추출
4. $a=b$를 전송하여 $rot(f(b),\rho)\cdot(x'\oplus y')$ 추출
5. 추출한 $rot(f(b),\rho)\cdot(x'\oplus y')$, $rot(f(b),\rho)\cdot y'$ x'을 통해 y' 추출

3.2 Piramuthu의 HB++ 프로토콜

Piramuthu는 위에서 밝힌 문제인 z값 노출을 회피하고 안전성을 보장하기 위해 Bringer et al.의



〔그림 1〕 Piramuthu의 HB++ 프로토콜의 한 라운드

HB++ 프로토콜에서 z 연산을 뺀 프로토콜을 제안하였다. S. Piramuthu의 개선된 HB++ 프로토콜은 〔그림 1〕과 같다[13].

IV. Piramuthu 공격의 문제점과 개선 방법

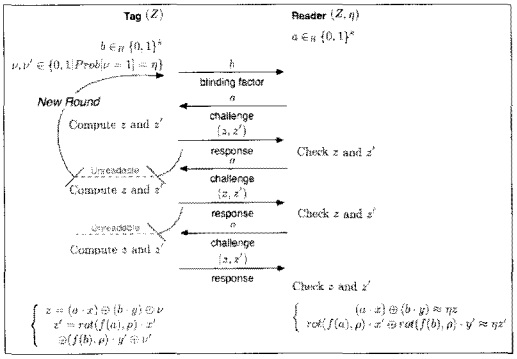
4.1 Piramuthu 공격의 문제점

4.1.1 빠른 질의 공격

Piramuthu는 HB++에 대한 공격을 하기 위해 송신이 빠른 불법적인 리더를 사용한다고 가정하였다. 즉, 공격자는 태그가 새로운 은닉 요소 b를 생성하기 이전에 빠르게 도전 a를 전송함으로써 은닉 요소 b의 난수성을 제거하고 로테이션 수행에 영향을 미치는 ρ의 증가를 막을 수 있다. 결과적으로 공격자는 동일한 (b,ρ)쌍에 대한 질의를 통해 추가 된 비밀 값 x'과 y'의 값을 추출해 낸다. 해당 공격은 〔그림 2〕와 같이 이루어진다. 하지만, Juels는 이는 태그의 동작을 무시한 비정상적인 가정이라고 언급하였다[8]. Gen 2 태그는 다수 리더의 질의에 따른 race condition 방지를 위해 4개의 session을 갖추고 있다. 뿐만 아니라, 특정 command가 동작 할 수 있는 상태를 정해 놓음으로써 비정상적인 command에 대한 응답을 하지 않도록 할 수 있다. 따라서 빠른 송신에 따른 은닉 요소 b의 난수성 제거와 ρ의 증가 방지 가정에는 문제가 있다.

4.1.2 동일한 (b,ρ)상에서 a 변조 공격

Piramuthu는 은닉 요소 b와 ρ값이 변하지 않는 상태에서 a 값을 단순히 변조하여 비밀 값 x', y'을 알아낼 수 있다고 주장하였지만, 이는 계산적으로 불가능하다. $a=0, a=1$을 통해 $rot(f(b),\rho)\cdot y'$과 $1\cdot x'\oplus rot(f(b),\rho)\cdot y'$을 알아낼 수 있지만 공격자가



〔그림 2〕 빠른 질의 공격에서 가정한 상태 전이도

알 수 있는 값은 1비트의 패리티 비트이기 때문에 위 식을 통해서는 x'의 값을 알아낼 수 없다. 이와 동일하게 $a=b$인 도전을 전송하여 알아낸 $rot(f(b),\rho)\cdot(x'\oplus y')$와 이미 추출한 $rot(f(b),\rho)\cdot y'$, x'을 통해서 y'의 값을 추출하는 것도 계산적으로 불가능 하다.

4.1.3 LPN 문제를 풀어내는 공격

Blum et al.은 BKW 알고리즘을 사용하여 HB 프로토콜의 안전성인 LPN 문제에 대한 공격을 시도하였다[1]. BKW 알고리즘은 도청을 통해 알아낸 상당한 크기의 도전-응답 집합 (a_i,z_i)중에서 XOR을 통해 j번째 비트만 1로 채워진 기저벡터 e_j를 생성해 내는 a_i들을 찾아냄으로써 비밀 값 x를 알아낸다. BKW 알고리즘의 간략한 식은 다음과 같다.

1. $a_{i_1}\oplus\cdots\oplus a_{i_2}=e_j$인 $a_{i_1}\sim a_{i_2}$ 집합 검색
2. $(x\cdot e_j)=(x\cdot(a_1\oplus\cdots\oplus a_{i_2}))=(z_1\oplus\cdots\oplus z_{i_2})$

위 식을 통해 공격자는 비밀 값 x의 j비트 값을 확률적으로 알아 낼 수 있다. 해당 알고리즘은 1GB의 메모리를 사용하여 39 비트의 키를 알아낼 수 있다. Levieil et al.은 BKW 알고리즘을 개선한 LF1 알고리즘과 LF2 알고리즘을 제안하였다[11]. LF2 알고리즘은 1/4인 η값과 10000번의 쿼리를 통해 99비트의 키 값을 갖는 LPN 문제를 3GHz의 CPU상에서 1GB의 메모리만 사용하여 30초 만에 해결해 내는 성능을 보였다. BKW와 LF2 알고리즘을 사용했을 때 LPN 문제는 다음 〔표 1〕과 같은 안전성을 갖는다[15].

순열 함수 f와 로테이션을 사용하는 HB++ 프로

〔표 1〕 LPN 문제의 안전성

Key Length	BKW Runtime	LF2 Runtime
32	2^{24}	(2^{24})
64	2^{35}	(2^{28})
96	2^{46}	2^{33}
128	2^{56}	(2^{38})
160	2^{64}	(2^{43})
192	2^{72}	(2^{47})
224	2^{80}	2^{52}
256	2^{88}	(2^{56})
288	2^{96}	(2^{60})

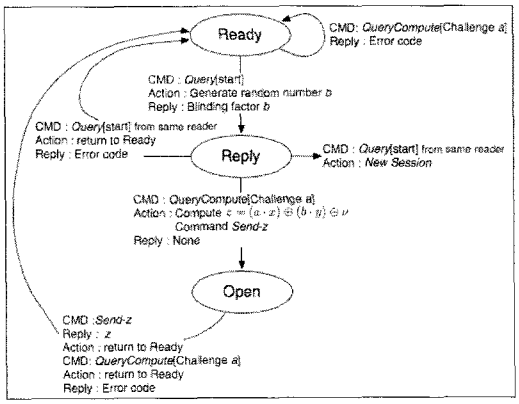
토콜은 암호학적인 안전성을 위해서 100비트 이상의 비밀 키를 쓴다고 가정할 수 있다. 이러한 경우 BKW 및 LF2 알고리즘을 사용하여 LPN 문제를 풀어내려는 시도를 한다고 해도 실제적으로 불가능 하다. Piramuthu는 키의 길이가 커지게 된다면 해당 공격의 수행이 불가능함을 인정하였다[14]. Juels는 HB류의 프로토콜에서 사용할 비밀 키의 길이를 결정하는 문제를 미결 문제로 남겨두었다[8].

4.2 안전한 프로토콜을 위한 제안

4.2.1 단계별 상태 전이 설정

4.1절에서 Piramuthu의 빠른 질의 공격에서 사용한 가정의 문제가 있음을 밝혔다. 인증을 시도하는 태그가 리더의 모든 질의에 대해 무조건 응답하는 것은 문제가 있기 때문에, HB류의 프로토콜을 위한 태그의 상태 전이도를 명확히 할 필요가 있다. 현재 물류 태그의 표준 제정된 Gen 2는 Ready, Arbitrate, Reply, Acknowledged, Open, Secured, Killed의 7개 상태가 있다[17]. 태그는 리더의 명령(CMD: command)이 적법한 상태에 있을 때에만 응답을 함으로써, 태그의 정보를 보호한다. 본 논문은 Gen 2 태그의 상태 전이를 기초로 하여 HB+ 프로토콜을 위한 상태 전이를 〔그림 3〕과 같이 제안한다.

HB+ 프로토콜에서 태그가 은닉 요소 b를 생성하여 응답하기 위해서는 리더의 도전 *start*가 필요하다. 〔Ready〕 상태인 태그가 리더의 도전 *start*를 수신하면 은닉 요소 b를 전송한 뒤 〔Reply〕 상태로 전이된다. 〔Reply〕 상태로 전이된 태그는 리더의 도전 a를 기다리게 되는데, 이 때 다른 리더로부터 도전 *start*가 전송되면 해당 리더를 위한 새로운 세션의 〔Ready〕 상태에서 부터 통신을 시작하고, 같은 리더



〔그림 3〕 HB+ 프로토콜을 위한 태그의 상태 전이도

로부터 도전 *start*가 전송되면 에러 메시지를 전송한 뒤 〔Ready〕 상태로 복귀한다. 리더의 도전 a가 〔Reply〕 상태인 태그에게 정상적으로 전달되면, 태그는 $z=(a\cdot x)\oplus(b\cdot y)\oplus\nu$ 연산을 한 뒤 〔Open〕 상태로 전이된다. 이 때 태그는 Send-z라는 명령을 전달함으로써, 태그가 〔Open〕 상태로 전이된 이후 곧바로 응답 z를 전송할 수 있게 한다. 〔Open〕 상태로 전이된 태그가 응답 z를 전송하기 전에 불법적인 리더의 다른 명령이 전송된다면 에러 메시지를 전송한 뒤 〔Ready〕 상태로 복귀한다. 〔Open〕 상태로 전이된 태그는 응답 z를 전송한 뒤 〔Ready〕 상태로 전이한다. 해당 상태 전이는 리더의 질의에 대한 무조건적인 응답을 제한함으로써 Piramuthu의 빠른 질의 공격을 막을 수 있다.

4.2.2 도전 a의 해밍 무게 설정

Piramuthu는 동일한 (b,ρ) 상에서 도전 a를 0과 1로 전송함으로써 비밀 값 x'을 알아낼 수 있다고 주장하였다. 비록 1비트를 응답하는 HB++ 프로토콜에서는 성취되지 않는 공격이지만, 비밀 값을 빼내기 위해 전송 된 특수한 값에 대한 응답은 공격의 가능성을 열어주는 것이 될 수 있다. HB 프로토콜의 경우 해밍 무게(hamming weight)가 1인 도전 a를 통한 능동 공격이 가능하기 때문에 해밍 무게 설정은 효과적인 공격 방지 기법이 될 수 있다.

$$\frac{k}{4} \le Hamming\ weight \le \frac{3k}{4}$$

본 논문은 HB류의 프로토콜에서 사용할 은닉 요소

〔표 2〕 HB 프로토콜들의 비교표

프로토콜	통신 횟수	연산 횟수	공격에 대한 안전성		
			도청	재사용	중간자 공격
HB	$2R$	$R\times(\cdot)$ $R\times(\oplus)$	O	X	-
HB+	$3R$	$2R\times(\cdot)$ $2R\times(\oplus)$	O	O	X
HB++	$3R+2$	$4R\times(\cdot)$ $4R\times(\oplus)$ $2R\times(f)$ $2R\times(rot)$ $2\times(h)$	O	O	X
HB++ 개선	$3R+2$	$2R\times(\cdot)$ $2R\times(\oplus)$ $2R\times(f)$ $2R\times(rot)$ $2\times(h)$	O	O	O

및 도전의 해밍 무게를 위와 같은 범위로 사용할 것을 제안한다. 길이가 k비트인 비밀 값 중 1로 채워진 비트가 1/4보다 작거나 3/4보다 크다면 해당 신호에 대한 응답을 하지 않게 함으로써 특수한 값을 통한 공격에 대해 안전성을 갖게 한다.

4.3 성능 및 안전성 분석

〔표 2〕는 HB 프로토콜과 그 변형 프로토콜들의 통신, 연산 횟수, 도청, 재사용 공격, 중간자 공격에 대한 안전성에 대한 비교 분석을 보여준다. 표에서 R은 LPN 문제를 위한 라운드 수를 나타내며, HB++ 개선은 Piramuthu의 HB++ 프로토콜과 제안한 기법을 포함한 경우를 나타낸다. 실제로 안전한 프로토콜의 제안은 통신 횟수, 연산 횟수에 영향을 미치지 않으므로 Piramuthu의 HB++ 프로토콜과 동일한 성능을 가진다.

V. 결 론

유비쿼터스 컴퓨팅 환경을 구축하기 위한 센서 및 RFID 태그는 계산능력과 메모리의 한계로 인해 전통적으로 사용하는 암호 프리미티브 사용에 제약이 있다. HB+ 프로토콜은 암호화 프리미티브가 아닌 LPN 문제 발생을 통하여 안전성을 얻기 때문에 자원의 제약이 심한 RFID 태그에서 사용하기에 적합한 프로토콜이다. 하지만 HB+ 프로토콜에 대한 중간자 공격이 발견됨에 따라 이를 수정한 HB++와 HB* 프로토콜이 제안되었다.

본 논문은 Bringer et al.의 HB++에 대한 Piramuthu의 공격이 실행 불가능함을 밝혔다. 뿐만 아니라 빠른 질의를 통한 공격을 막을 수 있는 태그의 상태 전이와 해밍 무게 조절에 대해 제안하였다.

참고문헌

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

〔2〕 J. Bringer, H. Chabanne and E. Dottax, "HB++: a Lightweight Authentication Protocol Secure Against Some Attacks," In Proceedings of IEEE International Conference on Pervasive Services, SecPerU, 2006.

〔3〕 D. N. Duc and K. Kim, "Securing HB+ against GRS 중간자 공격," Proceedings of SCIS 2007, January, 2007.

〔4〕 H. Gilbert, M. Robshaw and H. Sibert, "An Active Attack Against HB+ - A Provably Secure Lightweight Protocol," Cryptology ePrint Archive, Report 2005/237, 2005. http://eprint.iacr.org.

〔5〕 H. Gilbert, M. Robshaw and Y. Seurin, "HB#: Increasing the security and efficiency of HB+." In Proceedings of EUROCRYPT 2008, Springer-Verlag, LNCS 4965, pp. 361-378, 2008.

〔6〕 N. J. Hopper and M. Blum, "Secure Human Identification Protocols," In Proceedings of ASIACRYPT 2001, C. Boyd (Ed.), Springer-Verlag, LNCS 2248, pp. 52-66, 2001.

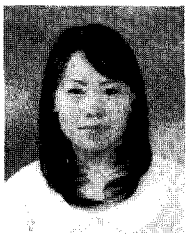
〔7〕 A. Juels and S. A. Weis, "Authenticating Pervasive Devices with Human Protocols," In Proceedings of CRYPTO'05, Victor Shoup (Ed.), Springer-Verlag, LNCS 3261, pp. 293-308, 2005.

〔8〕 A. Juels, Private communication, May, 2007.

〔9〕 J. Katz and J. S. Shin, "Parallel and concurrent security of HB and HB+

protocols," Cryptolgy ePrint archive, Report 2005/461, 2005, http://eprint.iacr.org.
[10] X. Leng, K. Mayes and K. Markantonakis, "HB-MP+ Protocol: An Improvement on the HB-MP Protocol," In Proc. IEEE International Conference on RFID, 2008.
[11] E. Levieil, P. A. Fouque, "An Improved LPN Algorithm," 5th International Conference, Security Cryptography for Networks 2006, Springer-Verlag, LNCS, vol. 4116, pp. 348-359, 2006.
[12] J. Munilla and A. Peinado, "HB-MP: A Further Step in the HB-Family of Light-weight Authentication Protocols," Computer Network, 51(9), pp. 2262-2267, 2007.
[13] S. Piramuthu, "HB and Related Light-weight Authentication Protocols for Secure RFID Tag/Reader Authentication," Proceedings of CollECTeR Europe Conference, June, 2006.
[14] Piramuthu, Private communication, June, 2007.
[15] S. A. Weis, "New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness Testing," MIT Computer Science Ph.D. Thesis, 2006.
[16] B. Yoon, M. Y. Sung, S. Yeon, H. S. Oh, Y. Kwon, C. Kim and K.-H. Kim, "HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System," In IEEE International Conference on RFID, pp. 186-191, 2009.
[17] EPCglobal, "EPCTM Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz," version 1.0.9, January, 2005.

〈著者紹介〉



신 수 연 (Sooyeon Shin) 학생회원
2004년 2월: 세종대학교 컴퓨터공학과 학사
2006년 2월: 세종대학교 컴퓨터공학과 석사
2006년 9월 ~ 현재: 세종대학교 컴퓨터공학과 박사과정
〈관심분야〉 프라이버시 보호기술, 익명성 기술, RFID, 센서 네트워크 등

권 태 경 (Taekyoung Kwon) 종신회원
1992년 2월: 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년 ~ 2000년: U.C. Berkely Post-Doc.
2001년 ~ 현재: 세종대학교 컴퓨터공학과 부교수, 정보보호학회 이사 및 편집위원
〈관심분야〉 암호프로토콜, 네트워크 프로토콜, 센서네트워크 보안, 프라이버시 보호, HCI 보안 등