초경량 RFID 인증 프로토콜 연구 동향

이길제* · 윤은준** · 유기영***

1. 서 론

RFID 기술은 물류, 항만, 의료, 교육 등 다양한 환경의 사물에 부착된 태그(Tag)로부터 전파를 이용하여 사물의 정보 및 주변 환경을 인식하여 각 사물의 정보를 수집, 저장, 가공, 추적함으로써 사물 에 대한 측위, 원격 처리, 관리 및 사물 간 정보 교환 등 다양한 서비스를 제공하며, 기존에 이용되고 있는 바코드에 대한 불편한 점을 개선하고 물품 관리 및 운송을 보다 효율적으로 관리하기 위해 제안되었다.

이러한 RFID는 기본적으로 정보를 제공하는 태그(Tag)와 태그로부터 받은 정보를 판독 및 해독 기능의 판독기(Reader), 그리고 수신 받은 데이터를 처리하는 데이터베이스 시스템으로 구성되어 물품 관리 및 여러 응용 분야에서 네트워크화 및 지능화함으로써 보안, 안전, 환경 등 다양한 분야에 혁신을 가져다주었다[1-6].

RFID는 크게 능동형(active)태그와 수동형(passive)태그로 분류된다. 능동형 태그는 태그 자체에 내부 배터리와 송신 장치를 내장하고 있어 스스로 연산과 송신할 수 있다. 433MHz, 916.5MHz, 그리고 2.45GHz 대역의 주파수를 사용하고 있으며, 능동형 RFID 리더와 태그는 단일 주파수 대역 FSK 신호를 이용하며, 반이중 방식으로 리더와 태그 간 통신을 한다. 능동형 RFID태그는 자체 전력을 가지고 있어 수동형보다 비교적 긴 인식거리를 가지고 있어, 공항 또는 항만의 관리 시스템에 주로 사용하고 있다. 수동형 태그는 태그 자체에 베터리가 없고 리더가 보내는 특정 주파수를 받아 그 에너지를 이용해 리더에게 자신의 내부 메모리에 저장된 정보를 전송한다. 따라서 전자파 세기에 따라 태그의 인식 범위가 제한되게 된다.

이런 이유들로, 능동형 태크의 경우 인증이나 보안 프로토콜에서 암호학적으로 많은 연산이 발생하여도 무리 없이 처리되지만, 수동형의 경우

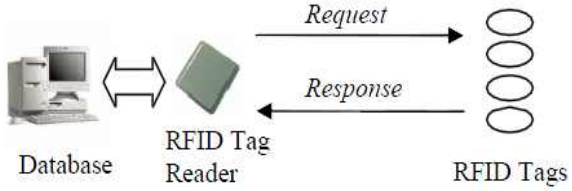

그림 1. RFID 통신 모델[1]

※ 교신저자(Corresponding Author) : 유기영 주소 : 대구광역시 북구 산격3동 경북대학교(702-701), 전화: 053)950-5553, E-mail : yook@knu.ac.kr
* 경북대학교 전기전자컴퓨터공학부 박사과정
(E-mail: vilelkj@infosec.knu.ac.kr)
** 경일대학교 사이버보안학과 교수
(E-mail : ejyoon@kiu.ac.kr)
*** 경북대학교 컴퓨터공학과 교수
※ 이 논문은 지식경제부 및 한국산업기술평가관리원의 산업융합원천기술개발사업(정보통신)[10041145, 자율군집을 지원하는 웰빙형 정보기기 내장 소프트웨어 플랫폼 개발]과 중소기업청에서 지원하는 2012년도 산학연공동기술개발사업 C0032042의 연구수행으로 인한 결과물임.

복잡한 연산이 불가능하게 되어, 초경량 RFID 인증 프로토콜에 대한 연구가 활발히 진행되어진다[1-6].

최근에는 EPCglobal(Electronic Product Code global: 월마트 및 P&G 등 RFID시스템 글로벌 사용자단체가 중심이 되어 RFID 분야에 실질적인 대중성을 보유한 사실표준을 제정하는 민간표준화기구)을 중심으로 프로토콜 등의 표준화가 활발히 진행 중이며, EPC-Global Class 1 Gen2-UHF 프로토콜 SPEC에서는 Kill password 및 Access password를 제공하고 있다[3,4]. Kill password의 경우, 안전성은 뛰어나지만, 태그를 재사용하지 못하는 단점이 있다. 또한 태그에 접근 및 통신을 위해 Access password와 간단한 프로토콜을 제공하고 있으나, 보안상 취약점이 있다.

EPC-Global Class 1 Gen 2에서 제공하는 프로토콜에서는 EPC를 암호화 하지 않고 전송하고 있으며, 태그와 리더 간 상호인증을 제공하지 않는 등 여러 가지 문제점들이 존재하며, 이를 해결할 수 있는 인증 기법의 도입이 필요하다.

이를 위하여 RFID의 다양한 공격 방법들을 살펴보고, 다양한 공격에도 강인하고 효율적인 초경량 RFID 인증 프로토콜에 대해 살펴보고, 향후 전망을 예상해본다.

2. RFID 공격 기법

RFID 시스템의 리더와 태그는 공개된 채널에서 통신하기 때문에 인터페이스, 리더기, 시스템 공격등 다양한 공격들에 취약하다. 본 장에서는 RFID 시스템의 다양한 공격유형을 파악하고 이에 따른 보안 요구사항을 확인한다[1,4,7-10].

2.1 도청공격(Eavesdropping attack)

RFID 시스템에서 가장 많이 발생하는 공격중의 하나로, 공격자가 태그에 대한 내부 정보(ID)를 몰라도 해당 태그로 위장하여 리더와 태그 사이에서 전송되는 정보를 볼 수 있는 공격이다.

2.2 전파방해 공격(Jamming attack)

전파방해 공격은 태그와 리더 사이 그리고 통신의 가용성과 무결성을 공격하기 위한 고의적인 시도로 강력한 송신기를 통해 수행되어 집니다.

2.3 중계 공격(Relay attack)

잘 알려진 중간자 공격(man-in-the-middle attack)으로, 공격자는 리더와 태그 사이에서 받은 정보를 자신의 것으로 교체하는 공격이다.

2.4 재전송 공격(Replay attack)

공격자가 과거에 리더와 태그 사이에 통신한 내용들을 도청한 후 이를 재전송하여 합법적인 태그, 리더 또는 DB로 인증을 받으려는 공격이다.

2.5 위치추적

리더의 연속적인 요청에 태그의 동일한 응답으로부터 태그의 위치를 추적하는 방법으로, 태그와 리더 사이의 통신 메시지 내용을 가변적으로 하여 태그의 식별자(ID)를 추적(Trace)할 수 없게 한다.

2.6 트래픽 분석 공격(Traffic Analysis Attack)

공격자가 도청을 통해서 얻은 내용을 분석하여 리더의 질의에 대한 태그의 응답을 예측하여 Tag의 이동경로를 추적할 수 있는 공격이다.

2.7 스푸핑 공격(Spoofing Attack)

스푸핑 공격은 공격자가 정당한 태그로 위장하

여 리더로부터 인증에 필요한 정보를 획득하거나, 정당한 리더로 위장하여 태그 또는 DB로부터 인증에 필요한 정보를 획득하거나, 또는 정당한 DB로 위장하여 리더로부터 인증에 필요한 정보를 획득하여 이를 이용하여 정당한 태그, 리더 또는 DB로 인증 받는 공격이다.

2.8 서비스거부 공격(Denial of Service Attack)

서비스 거부 공격은 리더, 태그 또는 DB가 정당한 통신 상대방의 인증 요청임에도 불구하고 공격자에 의한 많은 계산이 요구되는 데이터를 송신하여, 이전 세션에서 갱신되는 값들을 올바른 값으로 갱신되지 못하도록 방해하는 등 리더, 태그 또는 DB가 정상적인 서비스와 기능을 수행 하지 못하도록 하는 공격이다.

2.9 전방향 안전성(Forward Secrecy)

공격자에게 현재 세션에서 DB와 태그간에 공유된 비밀키 값이 누출되더라도 해당 비밀 값을 이용하여 과거에 사용된 비밀 값을 유도하거나 메시지 무결성을 저해하지 않아야 하는 보안성을 의미한다. 즉, 폐기된 태그를 공격자가 쉽게 획득하여 부채널 공격(Side-Channel Attack)등을 통해 태그 내에 저장된 비밀키 값을 얻을 수 있다. 따라서, DB와 태그는 상호인증을 수행 후 다음 세션을 위해 서로의 비밀 값을 안전하게 갱신하여 트래픽 분석 공격이나 위치 트래킹 공격 등을 방어할 수 있어야 한다.

이러한 공격들을 막기 위해서는 암호학적 기법을 사용하여 전송되는 데이터의 무결성, 가용성, 기밀성 등을 보장하여야하며, 경량화된 방법이 필요하다.

3. 초경량 RFID 인증 방법

3.1 XOR 기반의 일회용 암호

2003년 Juels[11]이 처음 제안하였으며, 리더 또는 DB 서버는 각 태그에서 생성하는 랜덤 키에 대한 목록을 가지고 있고, 리더와 태그 사이에 여러 메시지를 전달하면서 동일한 키를 리스트에서 찾아냅니다. 이 때, 태그는 리더에게 ID를 전송하지만, 인증을 위해 리더와 태그 사이에 불필요한 메시지 전달을 필요로 한다. 또한, 키 리스트의 안전성을 보장하기 위해 태그와 리더는 키 리스트를 갱신해야합니다. 이 방법은 위치 추적 공격에 대해 안전하지만, 데이터 프라이버시 보장과 전방향 안전성에 대해서는 제공하지 않습니다.

3.2 외부 재암호화 기법

외부 재암호화 기법은 2006년 이 등[12]에 의해 제안되었으며, 사용자의 요청이 있을 때, 리더가 외부 장치로부터 전송된 데이터를 재암호화 하여, 공격자는 도청을 하여도 다음 세션까지 태그에 대한 정보를 얻기 힘듭니다. 하지만, 각 태그의 암호화된 ID를 새로 갱신하는데 어려움을 가지며, 사용자의 개인 정보를 보호하지는 못한다.

3.3 해쉬 체인 기반 기법

Ohkubo[13] 등에 의해 해쉬를 기반으로 하는 인증 프로토콜이 제안 되었으며, 프라이버시와 태그 정보의 갱신이 쉬워졌다. 해쉬 체인 기법은 태그의 두 가지 방법으로 통신을 이용한다. 프로토콜에서 랜덤한 수를 생성하지 않아도 태그의 정보를 보호하고 위치 추적 공격을 막을 수 있다. 하지만, 중계 공격과 전방향 안전성을 만족하지는 않는다.

3.4 차단자 태그 기법

2003년 Juels[14] 등이 제안하였으며, RFID 리더를 혼란 시켜 태그의 데이터 송신을 무효화함으로써 개인이나 상품에 관한 데이터를 추적할 수 없게 설계한 통신방해 기술이다. 이 기법은 이진 트리 기반의 충돌 방지 기법에 사용된다.

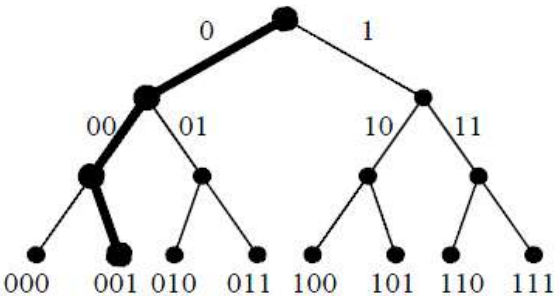

그림 1. 이진 트리 기반의 충돌 방지 프로토콜[1]

3.5 확장 해쉬 락 기법

2004년 Weis[15]가 해쉬 락과 확장된 해쉬 락 기법으로 제안한 인증 기법으로, 해쉬락 기법은 키 k를 해쉬하여 metaID를 생성하고 이 정보를 이용한다. 하지만, metaID를 통한 위치추적 및 도청공격에 취약하다. 확장된 해쉬 락 기법은 태그에서 생성한 랜덤한 수를 이용해 metaID를 생성하여 안전한 인증과 중계공격을 방어할 수 있다. 하지만, ID가 노출될 경우 위치추적이 가능하고, 공격자의 리더가 합법적인 리더로 위장할 수 있다. 따라서, 이 기법 또한 RFID 보안 요구조건과 전방향 안전성을 제공하지는 못한다.

3.6 Ultra lightweight 기법

Lopez 등이 해쉬를 이용한 방법에서 벗어나 XOR, OR, AND, 모듈러 연산을 이용한 보안과 프라이버시를 제공하는 lightweight 기법으로 LMAP[16](lightweight Mutual Authentication Protocol), M2AP[17] (Minimalist Mutual-Authentication Protocol), EMAP[18](Efficient Mutual Authentication Protocol) 방법을 연달아 발표하였다. 4가지의 키와 300게이트 그리고 96비트의 ID를 이용하여 태그 식별을 위한 IDS(Index-pseudonym)을 생성한다. 제안된 프로토콜들은 비트연산인 XOR, AND, OR와 모듈러(modular) 연산을 사용한 것으로 매우 간단하게 동작한다. 그 과정은 그림 3,4,5와 같다.

▪ Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$ $B=(IDS_{tag(i)} \vee K2_{tag(i)})+n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2$ $D=(IDS_{tag(i)}+ID_{tag(i)})) \oplus n1 \oplus n2$

▪ Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus K4_{tag(i)})) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

그림 3. LMAP 기법[16]

▪ Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$ $B=(IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2$ $D=(IDS_{tag(i)} \vee K4_{tag(i)})) \wedge n2$

$E=(IDS_{tag(i)}+ID_{tag(i)})) \oplus n1$

▪ Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus n1)) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

그림 4. M2AP 기법[17]

▪ Message generation process

$A=IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$ $B=(IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$

$C=IDS_{tag(i)}+K3_{tag(i)}+n2$ $D=(IDS_{tag(i)} \vee K4_{tag(i)})) \wedge n2$

$E=(IDS_{tag(i)} \wedge n1 \vee n2) \oplus ID_{tag(i)} \oplus_{i=1}^{4} Ki_{tag(i)}$

▪ Key renewal process

$IDS_{tag(i+1)}=(IDS_{tag(i)}+(n2 \oplus n1)) \oplus ID_{tag(i)}$

$K1_{tag(i+1)}=K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)}+ID_{tag(i)})$

$K2_{tag(i+1)}=K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)}+ID_{tag(i)})$

$K3_{tag(i+1)}=(K3_{tag(i)} \oplus n1)+(K1_{tag(i)} \oplus ID_{tag(i)})$

$K4_{tag(i+1)}=(K4_{tag(i)} \oplus n1)+(K2_{tag(i)} \oplus ID_{tag(i)})$

그림 5. EMAP 기법[18]

하지만 제안된 프로토콜은 리더의 요청에 태그는 항상 IDS로 응답하여 ID까지 유출될 수 있을 뿐만 아니라. 비동기화(de-synchronization) 공격과 적극적 및 수동적인 공격에 취약하였다[19].

4. 최근 초경량 RFID 연구 현황 및 결론

최근 초경량 RFID 시스템에 대한 연구가 활발해 짐에 따라 저연산의 다양한 기법들이 소개되고 있다.

초기 초경량 기법으로 Lopez등이 제안한 LMAP, M2AP, EMAP 기법은 저연산에 메모리 효율성도 뛰어났지만, 리더의 요청에 의한 태그의 동일 메시지 전송으로 인한 취약점을 가졌다. 이를 해결하기 위해 2007년에 Chien[20]은 제안한 상호인증과 태그 익명성을 제공하는 새로운 초경량 상호인증 프로토콜인 SASI를 제안하였다. 그러나 Sun 등[21]은 SASI가 비동기화 공격에 저항할 수 없음을 보였고, Cao 등[22]은 SASI에 대해 중간자 공격을 하여 리더와 태그가 비동기화됨을 보였으며, Phan[23]은 태그 추적 공격을 위해 SASI에서 사용한 비트단위 OR 연산의 불균형성을 이용하였다. 2009년에 Peris-Lopez 등[24]은 SASI의 영향을 받아 새로운 프로토콜인 Gossamer 프로토콜을 제안하였으나 2010년 Targa 등[25]은 Gossamer가 비동기화 공격에 취약함을 보였다. 아주 최근에 Tian 등[26]은 XOR 연산, 회전(rotation) 연산, 그리고 순열(permutation) 연산을 사용하여 저가의 RFID 태그를 위한 초경량 인증 프로토콜인 RAPP를 제안하고, RAPP가 다양한 보안공격으로부터 안전함을 주장하였다. 특히 Tian 등[26]이 제안한 RAPP에서 초경량 RFID 인증 프로토콜 분야에서는 처음으로 순열(permutation) 연산인 $Per()$ 연산을 정의하고 이를 사용하였다. 그들이 정의한 $Per()$ 연산의 정의는 다음과 같다.

[정의] A와 B는 각각 다음과 같은 l 비트의 문자열이라 가정한다.

$A = a_1 a_2 \cdots a_l,\ a_i \in \{0,1\},\ i = 1,2,\cdots,l$

$B = b_1 b_2 \cdots b_l,\ b_i \in \{0,1\},\ i = 1,2,\cdots,l$

B의 해밍웨이트(Hamming weight)를 $w(B)$라고 표현하고, $w(B)$가 $m(0 \le m \le l)$이면

$b_{k_1} = b_{k_2} = \cdots\ b_{k_m} = 1$,

$b_{k_{m+1}} = b_{k_{m+2}} = \cdots\ b_{k_l} = 0$, 여기서

$1 \le k_1 < k_2 < \cdots < k_m \le l$ 이고

$1 \le k_{m+1} < k_{m+2} < \cdots < k_l \le l$ 이다.

그렇다면 B에 대한 A의 순열 연산, $Per(A,B)$는 다음과 같다.

$$Per(A,B) = a_{k_1} a_{k_2} \cdots a_{k_m} a_{k_l} a_{k_{l-1}} \cdots a_{k_{m+2}} a_{k_{m-1}}$$

[예제] $X = 01001010$이고 $Y = 01110101$ 이라면 $Per(X,Y) = 10000110$가 된다. 그림 6은 예제의 연산과정을 알기 쉽게 도시하고 있다.

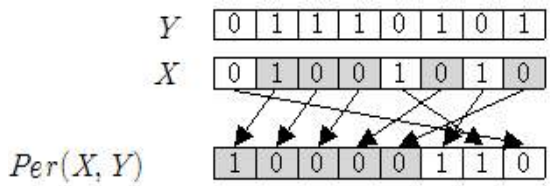

그림 6. $Per(X,Y)$의 연산

RAPP는 저가의 태그, 리더, 그리고 백엔드(back-end) 데이터베이스의 세 개체를 포함한다. 리더와 백엔드 데이터베이스는 유선이든 무선이든 안전한 통신채널에 의해 통신하는 반면에 리더와 태그의 통신 채널은 무선이며 보안 공격에 취약하다. RAPP에서 태그 내의 연산을 위해 $Per()$ 연산과 더불어 XOR 연산 및 회전연산인 $Rot()$ 연산을 사용하였다. 태그는 L 비트의 고

표 1. 초경량 RFID 인증 프로토콜의 비교

비교요소 \ 프로토콜	LMAP [16]	M^{2}AP [17]	SASI [21]	Gossamer [24]	RAPP [26]
태그 추적 공격	취약	취약	취약	안전	안전
비동기화 공격	취약	취약	취약	취약	취약
디스클로즈 공격	취약	취약	취약	안전	안전
필요 저장공간	6L*	6L	7L	7L	5L
사용된 연산	$\oplus, +, \vee$	$\oplus, +, \vee, \wedge$	$\oplus, +, \vee, Rot$	$\oplus, +, Rot_2, Mixbits$	$\oplus, Rot, Per$

(L은 아이디나 비밀키의 길이)

유한 아이디, ID와 네 개의 요소, $\{IDS, K_1, K_2, K_3\}$를 가지고 있다. 여기서 IDS는 태그의 의사아이디(pseudonym)이며 K_1, K_2, K_3는 비밀키이다. 비동기화(de-synchronization) 공격을 막기 위해 백엔드 데이터베이스는 각 태그의 이사아이다와 비밀키에 대해 이전(old) 값, $\{IDS^{old}, K_1^{old}, K_2^{old}, K_3^{old}\}$와 새로운(new) 값, $\{IDS^{new}, K_1^{new}, K_2^{new}, K_3^{new}\}$를 유지한다. RAPP는 크게 인증단계와 업데이트 단계로 구분되며 그 세부적인 수행 과정을 그림 7에 요약하였다.

하지만 RAPP 또한 저자의 주장과는 달리 비동기화 공격에 대한 취약점을 여전히 가지고 있다. 공격자는 리더와 태그가 주고받는 메시지, (A,B)와 (D,E)를 몰래 캡쳐함과 동시에 메시지 (D,E)가 태그로 전송되는 것을 차단시킨다. 그렇게 하면 리더의 IDS^{new}과 $K_1^{new}, K_2^{new}, K_3^{new}$는 갱신되지만 태그의 정보는 변하지 않게 되어 비동기 공격이 가능하다.

다시 말해 위와 같은 초경량 RFID 인증 기법들[20-26]은 표 1의 결과와 같이 여전히 태그 추적 저항 공격, 비동기화 공격, 서비스 거부 공격, 중계 공격, 재전송 공격, 전방향 안전성 등 다양한 RFID 공격 및 요구사항에 대해 해결해야할 부분이 남아있다. 결론적으로 초경량 RFID 인증 프로토콜에 대한 다양한 효율성 분석과 보안성 향상을 위한 연구는 계속적으로 필요하며 이와 같은 개선 연구 수행을 통해 RFID 및 NFC 기반 응용 시스템의 보안성을 높일 수 있을 것이다.

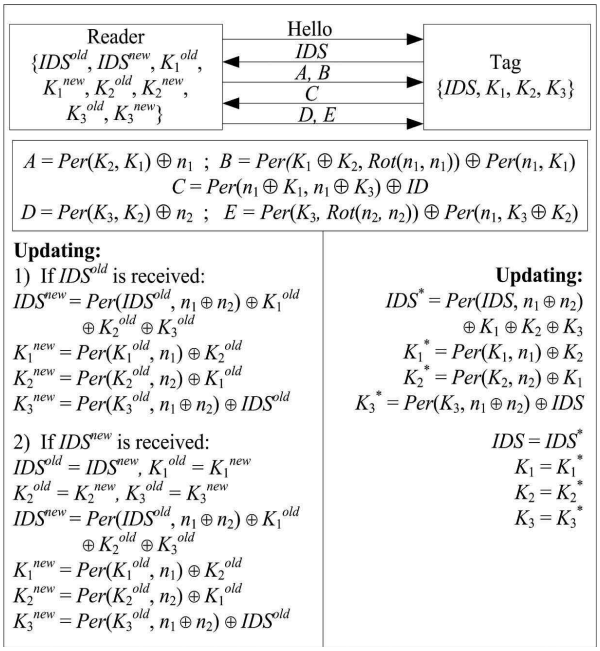

그림 7. RAPP 프로토콜[21]

참 고 문 헌

[1] Irfan Syamsuddin, Song Han, Vidyasagar Potdar, and Tharam Dillon, "A Survey on Low-cost RFID Authentication Protocols," International Journal of Computer Systems Science and Engineering, Sep. 2010

[2] 윤은준, 하경주, 유기영, "견고한 행렬기반 RFID

상호인증 프로토콜," 한국통신학회논문지, Vol. 33, No.11, Nov. 2008.
[3] 최길영, 성낙선, 모희숙, 박찬원, "RFID 기술 및 표준화 동향, "전자통신동향분석, 제22권, 제3호, June 2007.
[4] 윤은준, 유기영, "공개 채널 기반의 RFID 상호인증 시스템 설계," 한국통신학회논문지, Vol.34, No.10, Oct. 2009.
[6] F. Klaus, "RFID handbook," Second Edition, Jone Willey & Sons, 2003.
[7] 최은영, 최동희, 임종인, 이동훈, "저가형 RFID 시스템을 위한 효율적인 인증 프로토콜," 정보보호학회논문지 15권 5호, pp. 59-71, 2005.
[8] 김배현, 유인태, "반사공격에 안전한 RFID 인증 프로토콜," 한국통신학회논문지 32권 3호, pp. 348-354, 2007.
[9] 이재강, 오세진, 정경호, 이창희, 안광선, "시프트 연산과 난수를 이용한 가변적 대칭키 기반의 RFID 상호인증 프로토콜," 한국통신학회논문지, Vol.37B, No.05, May. 2012.
[10] S. Han, V.potdar, and E. Chang, "Mutual Authentication Protocol for RFID Tags Based on Synchronized Secret Information with Monitor," ICCSA 2007, LNCS 4707, pp. 227-238, 2007.
[11] Ari Juels, "Minimalist Cryptography for Low-Cost RFID Tags," Security in Communication Networks In Security in Communication Networks, Vol.3352, pp. 149-164, 2003.
[12] S. Lee, H. Lee, T. Asano, and K. Kim, "Enhanced RFID Mutual Authentication Scheme based on Synchronized Secret Information," AUTO-ID Labs White Paper, WPHARDWARE 032, 2006.
[13] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Hash-chain based forward-secure privacy protection scheme for low-cost RFID," Proceedings of the SCIS 2004, pp. 719-724, 2004.
[14] A. Juels, R. L. Rivest, M Szydlo "The blocker tag: selective blocking of RFID tags for consumer privacy," In Proceedings of 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 103-111, 2003.
[15] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, "Security & Privacy Aspects of Low-Cost Radio Frequency Identification Systems," Security in Pervasive Computing, LNCS no. 2802, pp. 201-212, 2004.
[16] Peris-Lopez, P., Hernandez-Castro, JC., Juan, E.T. and Arturo,R., "LMAP: A Real Lightweight Mutual Authentication Protocol for Lowcost RFID tags" Workshop on RFID Security -- RFIDSec 06, July 2006.
[17] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan and Ribagorda, Arturo,"M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags", Lecture Notes inComputer Science, 912--923, Springer-Verlag, Sep-2006.
[18] Peris-Lopez, Pedro and Hernandez-Castro, Julio Cesar and Estevez-Tapiador, Juan M. and Ribagorda, Arturo, "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags", OTM Federated Conferences and Workshop: IS Workshop -- IS'06, 2006, 4277 Lecture Notes in Computer Science, P-352-361, November 2006.
[19] T.Li, G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols," IFIP SEC 2007, May 2007.
[20] H.Y. Chien, "SASI: a new ultralightweight RFID authentication protocol providing strong authentication and strong integrity," IEEE Trans. Dependable and Secure Computing, Vol.4, No.4, pp. 337-340. Dec. 2007.
[21] H.-M. Sun, W.-C. Ting, and K.-H. Wang, "On the security of Chien's ultralightweight RFID authentication protocol," IEEE Trans. Dependable and Secure Computing, Vol.8, No.2, pp. 315-317, 2011.
[22] T. Cao, E. Bertino, and H. Lei, "Security analysis of the SASI protocol," IEEE Trans.

Dependable and Secure Computing, vol. 6, no. 1, pp. 73-77, 2009.

[23] R. C.-W. Phan, "Cryptanalysis of a new ultra-lightweight RFID authentication protocol-SASI," IEEE Trans. Dependable and Secure Computing, Vol.6, No.4, pp. 316-320, 2009.

[24] P. Peris-Lopez, J. Hernandez-Castro, J. Tapiador, A. Ribagorda, "Advances in ultra-lightweight cryptography for low-cost RFID tags: Gossamer protocol," Information Security Applications, pp. 56-68, 2009.

[25] D. Tagra, M. Rahman, S. Sampalli, "Technique for preventing DoS attacks on RFID systems," 18th international conference on software telecommunications and computer networks-SoftCOM'10, IEEE Computer Society, 2010.

[26] Y. Tian, G. Chen, and J. Li, "A New Ultralightweight RFID Authentication Protocol with Permutation," IEEE Communications Letters, Vol.16, No.5, May 2012.

이 길 제

- 2000년~2007년 경일대학교 컴퓨터공학과 학사
- 2007년~2010년 경북대학교 정보통신학과 석사
- 2010년~현재 경북대학교 전기전자컴퓨터공학과 박사과정
- 관심분야 : 암호학, 정보보호, 스테가노그라피, 인증 프로토콜

윤 은 준

- 1988년~1995년 경일대학교 학사
- 2001년~2003년 경일대하교 컴퓨터공학과 석사
- 2003년~2007년 경북대학교 컴퓨터공학과 박사
- 2007년~2008년 수성대학교 컴퓨터정보계열 전임강사
- 2009년~2011년 경북대학교 전자전기컴퓨터공학부 계약교수
- 2011년~현재 경일대학교 사이버보안학과 교수
- 관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네트워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜

유 기 영

- 1972년~1976년 경북대학교 수학교육학과 학사
- 1976년~1978년 한국과학기술원 컴퓨터공학과 석사
- 1987년~1992년 Rensselaer Polytechnic Institute. Computer Science 박사
- 1978년~1987년 경북대학교 공과대학 전자공학과 교수
- 1987년~1992년 Rensselaer Polytechnic Institute. Dept. of computer TA
- 1987년~현재 경북대학교 컴퓨터공학과 교수
- 관심분야 : 암호학, 정보보호, 유비쿼터스보안, 네크워크보안, 데이터베이스보안, 스테가노그라피, 인증프로토콜