RFID/USN에서의 EXOR과 해쉬 함수를 이용한 인증 프로토콜†

(An Authentication Protocol using the EXOR and the Hash Function in RFID/USN)

신진섭*, 박영호*
(Jin-Seob Shin, Young-Ho Park)

요 약 언제 어디서나 네트워크에 접근하여 경제적이고 편리하게 정보를 교환할 수 있는 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 본 논문은 유비쿼터스 환경을 실현하기 위한 기술 중 하나인 RFID 태그 시스템에서의 프라이버시 보호 방법에 관한 것으로 RFID의 특성에 적합한 인증 프로토콜을 제안한다. 제안한 프로토콜은 RFID의 태그에서 연산량을 줄이기 위하여 EXOR과 해쉬 연산만을 수행하게 하며, 기존의 방식들에 비하여 안전성을 향상시킨다.

핵심주제어 : 인증 프로토콜, 유비쿼터스, RFID, 해쉬 함수, 보호

Abstract The essential factor of ubiquitous is security technology to properly prepare making possible network access, economic and convenient information exchange. This paper proposes an authentication protocol for RFID as one technology to realize such an ubiquitous. The proposed protocol used only the EXOR and the hash function operations reduces operations at RFID tag, which improves stability compared to existing protocols.

Key Words : Authentication Protocol, Ubiquitous, RFID, Hash Function, Security

1. 서 론

유비쿼터스 환경에서는 각 디바이스들이 생활의 곳곳에 널리 퍼져 있고 이러한 디바이스를 통해서 어느 곳에서나 정보의 이동이 용이하다. 이것은 어디에서던지 정보가 유출될 수 있음을 의미한다. 따라서 유비쿼터스 환경이 제대로 갖추어지기 위해서는 보안 기술이 필수적인 요소이다. 기존의 디바이스보다 작고, 경량이며, 값싸고, 이동 가능한 디바이스를 필요로 하는 유비쿼터스 컴퓨팅 및 네트워크 환경에서는 기존의 보안 기술을 그대로 적용하기는 어렵다. 그러므로 정보 보호 기술의 핵심인 암호 기술도 유비쿼터스 환경에 적합한 형태로 발전되어야 한다[1,2].

RFID/USN(radio frequency identification/ ubiquitous sensor setwork) 환경에서의 공격 대상은 기존의 컴퓨터에 저장된 정보 또는 통신 정보만이 아닌 개인이 소유한 모든 물체 단위까지 침해 범위가 확대될 수 있기 때문에 RFID/USN 서비스 활성화에 심각한 장애 요인이 될 수 있다. 예를 들어, 태그가 부착된 소비자의 물건에 대한 추적을 통해 소비자의 위치 추적이 가능하며, 개개인이 가지고 다니는 물건들을 소비자 모르게 비밀리에 목록화하여 악

† 이 논문은 상주대학교 2007년도 학술연구지원금에 의해 연구되었음.
교신저자 : 박영호 (yhpark@sangju.ac.kr)
* 상주대학교 전자전기공학부

용할 수 있다. 또한 태그가 출입 통제 시스템에 사용될 경우 악의적인 리더가 태그의 정보를 쉽게 읽어들이고, 여기서 얻은 정보를 이용하여 태그를 위조하는 것이 가능하다. 이것은 태그의 정보에 대한 인증되지 않은 접근에서 비롯된다. 만약 태그의 메모리에 민감한 데이터가 저장되어 있다면 이것은 심각한 보안 문제를 야기될 수 있다[2,3].

현재 RFID/USN에서의 이러한 보안 문제를 해결하기 위한 다양한 연구가 진행되고 있다. 이러한 연구의 일환으로 RFID 시스템에서 사용자 프라이버시를 위해 kill tag, faraday cage, active jamming, blocker tag 등과 같은 물리적 레벨의 대응기법[4]과 hash lock[5], 재암호화[6,7] 등과 같이 암호 기술을 이용한 보호 기법이 제안되고 있다. Hash lock의 unlocking 방식은 RFID 태그에서 연 산량을 줄이기 위하여 고안되었으며, 키 관리가 요구되며 사용자 추적이 용이하다는 단점이 있다. 이러한 사용자 추적을 방지하기 위하여 randomized hash lock 방식을 제안하였다. 이 방식은 초당 100~200개의 태그를 읽어야 하는 많은 개수의 태그를 읽어야 하고 많은 해쉬 연산을 수행해야 한다는 단점이 있다. 두 방식은 리더기와 데이터베이스 간에 데이터가 평문으로 통신된다는 문제점도 있다.

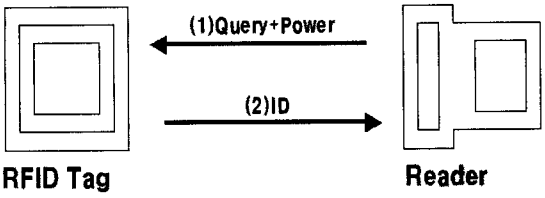
본 논문에서는 이러한 문제점들을 극복할 수 있는 새로운 인증 프로토콜을 제안한다. 본 프로토콜은 RFID의 태그에서 연산량을 줄이기 위하여 EXOR과 해쉬 연산만을 수행하게 하였으며 기존의 방식들에 비하여 안전성을 향상시킨다.

2. RFID 시스템의 특성

RFID 태그는 무선 통신용 안테나와 IC 칩을 조합한 저가의 소형 장치이다. 태그에 질의를 발생시켜, RFID 태그 메모리에 쓰여 있는 ID를 읽어내는 무선 장치를 리더라 부른다[5].

리더에 의해 질의를 할 때, 전원도 함께 보내며, 이 경우 RFID 태그 자신에는 전원이 필요 없다. 이 때문에 RFID 태그는 장차 바코드를 대신하는 식별 기능으로 활용될 것이다. 바코드와 같이 폭 넓은 이용을 위해서는 RFID 태그 크기는 0.4mm×0.4mm 이하로 종이에 심을 수 있을 정도로 얇은 것이 바람직하다. 따라서 RFID 태그의 계산 능력은 제한되어, RFID 태그라 복잡한 능력을 처리하는 것은 곤란하다. 또한 전파를 이용하는 특성상, RFID 태그와 리더 사이에 주고받는 내용을 쉽게 도청 할 수 있다.

RFID 태그에는 몇 종류가 있으며, 통신거리, 메모리 종류, 전원의 유무에 의해 분류된다. 우선, 통신거리로는 밀접형(0~수mm), 근접형(수mm~수10cm) 및 원격형(수10cm~수m)이 있다. 메모리에는 read only형, read/write형 그리고 write once read many 형이 있다. 쓰기 가능한 메모리를 탑재한 경우, RFID 태그의 ID 정보를 reader/writer라 부르는 무선통신 장치에 의해 써넣기가 가능하며, RFID 태그의 전원에는 능동형과 수동형으로 구분된다. 능동형은 RFID 태그에 전원을 내장하고 있고, 수동형은 리더로부터 전원을 얻는다. 태그와 리더를 이용한 개인정보 식별 시스템을 RFID 시스템이라 부른다.



<그림 1> 일반적인 RFID 시스템

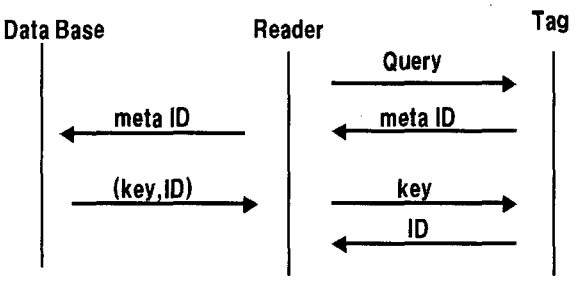
일반적으로 RFID 태그와 리더사이에 주고받는 절차를 그림 1에 보인다. RFID 시스템을 이용하면 상품의 포장을 개방하지 않아도 상자 속에 태그가 부착된 상품인식이 가능하기 때문에 상품의 재고 관리나 물류 관리에 이용된다. 태그는 상품에 붙여져 있으며, 바코드 같은 기능이 부여되어 있으므로 도난 방지 역할을 기대할 수 있다. 또한 상품 구입 후에도 RFID 시스템은 소비자에 편리한 기능을 준다. 예를 들면, 리더가 부착된 냉장고가 태그에 부착된 식료품의 유통 기한을 감시한다든지, 양복장에 보관되고 있는 옷에서 양호한 조합을 제공하는 것이 가능하게 될 것이다. 유럽중앙은행은 유로 지폐에 RFID 태그를 심는 것을 제안하고 있다. RFID 태그 ID와 지폐에 인쇄된 일련번호를 조합한 식별을 이용하면, 위조 방지 및 가짜 금융차용의 억제를 기대할 수 있다.

3. Hash lock

3.1 Hash lock의 locking 프로토콜

리더 R은 램덤한 key를 선택하고, meta ID 값으로 hash(key)를 계산한다. 리더 R은 meta ID를 태그 T에 기록하고 이때 T는 잠긴 상태(locked state)에 들어가며, 리더 R(meta ID ,key)은 저장한다[5].

3.2 Hash lock의 unlocking 프로토콜



<그림 2> Hash lock의 unlocking 프로토콜

리더 R은 태그 T에게 T의 meta ID를 질의 한다. 리더 R은 데이터베이스에서 (meta ID,key)를 조사하고, 리더 R은 T에게 key를 전송하고, 만약 hash (key)와 meta ID가 일치 하면, T는 잠긴 상태에서 빠져 나온다(unlock). 일방향 해시 함수의 역함수 계산 어려움에 기반한 hash lock 방식은 인가받지 않은 리더기가 태그 콘텐츠 읽는 것을 방지 할 수 있다.

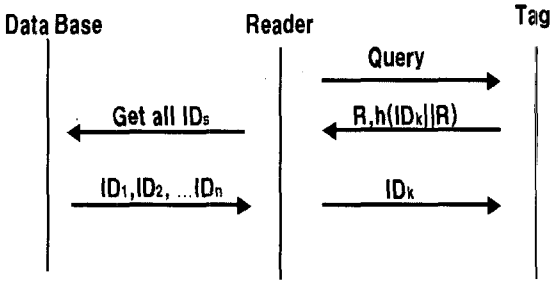
위장(spoofing)은 방어하지 못하지만 탐지는 가능하다. 공격자는 태그에게 meta ID를 요구한 후에 재전송 공격(replay attack)에서 합법적 리더기에게 태그를 위장하는 것이 가능하다. 그러면 합법적 리더기는 위장된 태그에게 키를 주게 된다. 그러나 리더기는 태그의 콘텐츠(일반적으로 태그의 ID)를 체크하여 백엔드 데이터베이스로부터 적절한 meta ID인지를 검증할 수 있다.

Hash lock 태그에 해시함수의 구현만을 요구하고, 백앤드에 키 관리를 요구한다. 이러한 요구 조건은 가까운 장래에 경제적인 것이 될 수 있다. 그러나 위 방식에서는 meta ID가 식별자처럼 사용되기 때문에 사용자 추적(tracking of individuals)이 가능하다.

4. Randomized hash lock

Hash lock 기법에서 가능했던 사용자 추적을 방지하기 위한 방식이다. 태그는 인가되지 않은 사용자에 의한 질의에 대하여 예상 가능한 응답을 하지 않지만, 합법적인 리더기에 의해서는 여전히 식별 가능해야 하는 방식이다. 이 기법에서는 태그에 일 방향 해시 함수와 함수 발생기(PRNG)가 구축되어 있어야 한다.

합법적인 리더기는 태그를 스캔하기 전에 "knows what she owns"를 가정한다. 태그를 lock 상태로 만드는 것은 프로토콜이 필요 없는 간단한 과정이나, 태그를 unlock 상태로 하는 프로토콜은 필요하다. 태그를 unlock 상태로 하는 프로토콜은 그림 3과 같다 [5].



<그림 3> Randomized hash lock의 unlocking 프로토콜

리더는 태그에게 질의를 보내면 태그는 랜덤한 값 R을 생성하여 $hash(ID||R)$ 값을 계산하고, 태그 T는 R에게 $(R, hash(ID||R)$을 전송한다. 리더는 알려진 ID_i값에 대해 $hash(ID_i||R)$을 계산하고, 그 값이 $hash(ID_i||R) \equiv hash(ID_i||R)$을 만족하는 ID_i를 찾는다면, 리더는 태그에게 ID_i를 전송한다. 만약 ID_i와 ID가 일치한다면, 태그는 잠긴 상태에서 빠져나온다.

이 방식은 초당 100~200개의 태그를 읽어야 하는 수많은 개수의 태그를 소유한 환경에서는 비현실적이다. 그러나 상대적으로 적은 수의 태그 사용자를 갖는 환경에서는 가능한 방식이다. 소매상점은 일반 사용자에 비해서 위치 프라이버시와 연관성이 적기 때문에 소매상인들은 hash lock기법을 적용하고, 구매

하는 소비자에게는 randomized hash lock 기법을 적용한다.

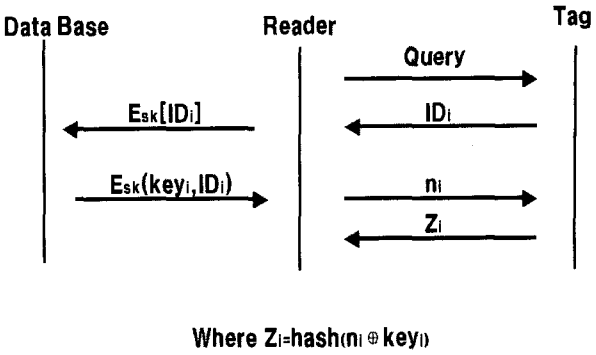
한 가지 문제는 합법적인 리더기들이 어떻게 그들의 태그를 알게 되느냐는 것이다. 물건이 팔렸을 때, 그것의 ID도 반드시 같이 전송되어야 한다. 그렇지 않으면 새로운 소유주가 태그를 읽을 수 없다. 새로운 소유주가 자신의 태그에 접근하는 한 가지 방식이 마스터 키를 사용하는 것이다.

위 방식이 충분히 현실적이지만 이론적으로 완벽하지는 않다. 이는 일방향 함수의 정의가 역함수 계산의 어려움만을 의미하기 때문이다. ID 비트가 노출되지 않음을 보장하기 위해서 보다 강한 프리미티브의 사용이 가능하다. 각 태그는 리더기와 유일한 비밀키를 공유한다고 하고, PRF(pseudo random function) 앙상블(ensemble)을 지원한다고 가정하면, 이론적으로 ID 비트 노출 방지가 가능하다. 구현상의 문제로 PRF 앙상블을 대칭키 암호보다 아주 적은 자원으로 구현 가능하냐의 문제가 발생하는데, PRF 앙상블의 최소 하드웨어 복잡도는 open problem이다.

5. 제안한 RFID/USN에서의 인증 프로토콜

RFID/USN에서의 보안 기술이 적용되지 않으면 개인 프라이버시 등 다양한 위협에 노출될 수 있다. 이러한 보안 문제를 해결하기 위하여 많은 연구가 진행되고 있으며 Hash lock[5] 방식이 대표적인 방식이다. Hash lock의 unlocking 방식은 RFID 태그에서 연산량을 줄이기 위하여 고안되었으나 키 관리가 요구되며 사용자 추적이 용이하다는 단점이 있다. 이러한 사용자 추적을 방지하기 위하여 randomized hash lock 방식을 제안하였다. 이 방식은 리더기가 초당 100~200개의 태그를 읽어야 하고 많은 해쉬 연산을 수행해야 한다는 단점이 있다. 또한, 두 방식은 리더기와 데이터베이스 간에 데이터가 평문으로 통신된다는 문제점도 있다.

본 논문에서는 이러한 문제점들을 극복할 수 있는 새로운 인증 프로토콜을 그림 4와 같이 제안한다.



<그림 4> 제안한 RFID/USN에서의 인증 프로토콜

본 방식에서는 RFID 데이터베이스와 리더 간의 세션 키가 설정 되어 있다고 가정하며 각 태그의 비밀키는 데이터베이스에 등록되어 있다고 가정한다. 프로토콜은 다음과 같이 수행된다.

1) 리더는 태그에게 질의를 보낸다.
2) 태그는 자신의 ID_i를 리더에게 전송한다.
3) 리더는 데이터베이스와 설정된 세션 키를 사용하여 태그의 ID_i를 암호화하여 $E_{SK}[ID_i]$ 데이터베이스에게 전송한다.
4) 데이터베이스는 수신된 $E_{SK}[ID_i]$을 세션 키를 사용하여 복호한 후 ID_i 태그의 비밀키를 세션 키를 사용하여 암호화한 값 $E_{SK}[key_i, ID_i]$을 리더에게 전송한다.
5) 리더는 수신한 $E_{SK}[key_i, ID_i]$을 복호하여 ID_i의 비밀 키 key_i를 저장하고 태그에게 랜덤 값 n_i을 전송한다.
6) 태그는 수신한 랜덤 값 n_i와 자신의 비밀키를 EXOR한 결과를 해쉬한 값 $Z_i = hash(n \oplus key_i)$를 리더에게 전송한다.
7) 리더는 Z_i를 계산하여 수신한 값과 같으면 태그를 인증한다.

본 프로토콜은 RFID의 태그에서 연산량을 줄이기 위해서 EXOR과 해쉬 연산만을 수행하게 하였으며 기존의 방식들에 비하여 안전성을 향상시켰다. 본 논문에서는 제안한 프로토콜은 패스워드 추측공격(password guessing attack), 메시지 재전송 공격(message replay attack), 위장공격(impersonate on

attack)의 측면에서 안전성 분석을 한다.

[패스워드 추측공격] 패스워드 추측공격은 온라인과 오프라인 패스워드 추측 공격은 인증 실패 횟수를 계산함으로써 쉽게 탐지되고 조치될 수 있으므로, 오프라인 패스워드 추측 공격에 대해서만 고려한다. 제안한 프로토콜에서 패스워드를 획득하기 위해서 공격자가 통신 메시지로부터 패스워드를 유추해야 하는데, 태그에 이미 암호화키가 내장되어 있으며 데이터베이스와 리더기 간의 메시지는 세션키로 암호화 되어 전송되므로 안전하게 전송된다. 따라서 제안한 프로토콜은 패스워드 추측공격으로부터 안전하다.

[메세지 재전송 공격] 만약 공격자가 태그가 이전에 획득한 메시지 ID_i, n_i와 Z_i를 가지고 정당한 태그로 가장하고 리더에게 ID_i를 전송하더라도 리더는 새로운 랜덤수 n_j를 전송하므로 이전에 획득한 메시지 Z_i로부터 키를 알 수 없으므로 정당한 Z_j를 계산할 수 없다. 공격자가 키 key_i를 모르면 제안한 프로토콜에서의 메시지 재전송 공격은 성공하지 못한다. 그러므로 제안된 프로토콜은 메시지 재전송 공격으로부터 안전하다.

[위장공격] 적법한 사용자나 공격자가 타인을 위장하기 위해서는 위장하고자 하는 사용자의 패스워드나 이로부터 유도된 검증자를 알아야 한다. 패스워드 추측 공격에서 기술한 것처럼 해쉬함수의 일방향성으로 인해 이들을 알아내는 것이 불가능하고 또한 메시지 재전송 공격으로도 키를 유추할 수 없으므로 제안한 프로토콜은 위장공격 으로부터 안전하다.

프로토콜의 성능 평가는 계산비용과 통신비용을 측정 비교 할 수 있다. 계산비용은 랜덤 값, EXOR 연산, 비대칭키 연산, 대칭키 연산, 해쉬 연산의 개수로 측정하고, 통신비용은 메시지 전송회수로 측정을 한다. 계산 비용 중에서도 비대칭키 연산은 다른 연산에 비해 수행시간이 매우 길기 때문에 이들 연산의 횟수가 프로토콜의 성능에 매우 큰 영향을 미친다. 표 1은 제안된 프로토콜의 연산 성능을 나타낸 것이다.

<표 1> 제안된 프로토콜의 성능 평가

비교요소 / 프로토콜		계산 비용					통신 비용
		랜덤 정수	EXOR 연산	비대칭키 연산	대칭키 연산	해쉬 연산	메시지 전송 횟수
제안된 프로토콜	태그	0	1	0	0	1	6
	리더	1	1	0	1	1	
	DB	0	0	0	1	1	

제안한 프로토콜은 연산 시간이 많이 소요되는 비대칭키 연산은 사용하지 않으며 데이터베이스와 리더기간에 대칭키 연산이 이루어진다. 연산량이 제한되어야 하는 태그에서는 EXOR와 해쉬 연산이 한 번씩 이루어지므로 부하가 적으며 리더에서도 EXOR, 해쉬 연산, 랜덤 수 발생 및 대칭 키 연산이 한 번씩 이루어지므로 부하가 많이 걸리지 않는다.

6. 결 론

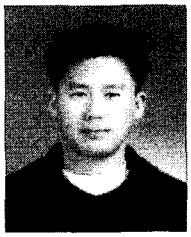
유비쿼터스 환경은 차세대 IT 기술로서 미래에 많은 편리함을 가져다 줄 것으로 기대된다. 실생활에 많은 편리함을 주는 만큼 악의적인 공격자로 인해서 개인의 정보 유출과 프라이버시 침해 등 다양한 부작용이 나타날 것이므로 정보 보호가 필요하다.

본 논문에서는 유비쿼터스 환경을 실현하기 위한 기술 중의 하나인 RFID 시스템에서의 RFID 태그의 특성을 고려한 RFID 태그와 리더 사이의 인증 프로토콜을 제안하였다. 제안된 프로토콜은 RFID의 태그에서 연산량을 줄이기 위해서 EXOR과 해쉬 연산만을 수행하게 하였으며 기존의 방식들에 비하여 안전성을 향상시켰다. 본 논문에서는 제안된 프로토콜의 안전성을 분석하기 위하여 패스워드 추측공격, 메시지 재전송 공격, 위장공격의 측면에서 분석을 하였다.

참 고 문 헌

[1] 남택용, 장종수, 손승원,"유비쿼터스 환경에서의 개인정보 보호 기술," 전자통신동향분석, 제20권,

제 1호, pp.54-62, 2005년 2월
[2] 신진섭, 박영호, "RFID/USN에서의 인증 프로토콜에 관한 연구," 한국정보보호학회영남지부 학술발표논문집, pp.21-25, 2007년 2월
[3] 김동석, "u-센서 네트워크 구축을 위한 정책 추진 방향," 전파지 116호, 2004년 1월/2월
[4] A. Juels, R. L. Rivest and M. Szydlo, "The Blocker Tag: Selective Block-ing of RFID Tags for Consumer Pfivacy," ACM, CCS03, pp.103-111, 2003.
[5] S. Weis et al., "Security and Privacy Aspects of Low-cost Radio Frequency Identification Systems," Security and Pervasive Computing, LNCS2802, pp.201-212, 2003.
[6] P. Golle et al., "Universal Re-encryption for Mix-nets," CT-RSA, LNCS2964, pp.163-178, 2004.
[7] A. Juels and R. Pappu, "Squealing Euros: Privacy Protection in RFID-enabled Banknotes," Financial Cryptography, LNCS2742, pp.103-121, 2003.



신 진 섭 (Jin-Seob Shin)

- 2005년 2월 상주대학교 전자전기공학부(공학사)
- 2007년 2월 상주대학교 대학원 전자전기공학과(공학석사)
- 관심분야: 정보보안, 이동통신

박 영 호 (Young-Ho Park)

- 종신회원
- 1989년 2월 경북대학교 전자공학과(공학사)
- 1991년 2월 경북대학교 대학원 전자공학과(공학석사)
- 1995년 8월 경북대학교 대학원 전자공학과(공학박사)
- 1996년 3월 ~ 현재 상주대학교 전자전기공학부 교수
- 2003년 8월 ~ 2004년 7월 Oregon State University 방문 교수
- 관심분야 : 정보보안, 광통신, 등