키 분할을 이용한 Low-Cost RFID 시스템 상호 인증 방안에 관한 연구

강 수 영[†] · 이 임 영[††]

요 약

RFID 시스템은 바코드를 대체하기 위한 무선 주파수 식별 기술로 유비쿼터스 환경을 구축하는 핵심 기술이다. RFID 시스템은 인식 속도 및 저장 공간 등 많은 편리성으로 사용이 급증하였지만 저가의 태그가 리더의 쿼리에 의하여 쉽게 동작하기 때문에 태그의 정보 노출에 따른 사용자 프라이버시 침해 문제가 발생하고 있다. 보안을 적용하기 위하여 많은 방식들이 연구되고 있지만 저가의 태그는 5K~10K 게이트 정도의 연산 능력을 가지고 있으며 그 중 250~3K 게이트 정도만을 보안에 할당할 수 있기 때문에 보안 적용이 어려운 실정이다. 따라서 본 방식은 64비트의 키를 분할하여 사용하며 연산을 최대한 줄여 Low-Cost RFID 시스템에 적용할 수 있는 상호 인증 방안에 대하여 제안한다. 기존 방식들은 96비트의 키를 4개로 분할하여 사용하였으나 본 방식은 경량화를 위하여 키 크기를 32비트 줄이고 7번의 통신 횟수를 5번으로 감소시켰다. 또한 두 개의 난수를 생성하는 기존 방식에 비하여 난수 한 개로 보안을 제공하기 때문에 더욱 효율적이라고 할 수 있다. 하지만 XOR 연산만으로 제공되지 못했던 무결성을 위하여 해쉬 함수를 사용하여 제안 방식의 확장을 추가하였다. 확장된 방식은 XOR 연산만을 사용하는 방식들보다 효율성은 제공되지 못하지만 인식 거리가 먼 RFID 시스템에서도 사용할 수 있도록 안전하게 제안된 방식이다.

키워드 : Low-Cost RFID 시스템, 키 분할, 상호 인증

A Study on Low-Cost RFID System Mutual Authentication Scheme using Key Division

Soo-Young Kang[†] · Im-Yeong Lee[††]

ABSTRACT

RFID system is core technology that construct ubiquitous environment for replacement of barcode technology. Use ratio of RFID system rapidly increase because the technology has many good points such as identification speed, storage space, convenience etc. But low-cost tag operates easily by query of reader, so the system happened user privacy violent problem by tag information exposure. The system studied many ways for security application, but operation capability of low-cost tag is about 5K~10K gates, but only 250~3K gates allocated security part. So it is difficult to apply security to the system. Therefore, this scheme uses dividing 64 bits and reduces arithmetic, so proposed scheme provide mutual authentication that can apply to low-cost RFID system. Existing methods divide by 4 and used 96 bits. However, that reduces 32 bits length for lightweight and reduced from communication number of times of 7 times to 5 times. Also, because offer security by random number than existing scheme that generate two random numbers, that is more efficient. However, uses hash function for integrity that was not offered by XOR arithmetic and added extension of proposed scheme. Extended scheme is not offered efficiency than methods that use XOR arithmetic, but identification distance is mode that is proposed secure so that can use in far RFID system.

Key Words : Low-Cost RFID System, Key Division, Mutual Authentication

1. 서 론

유비쿼터스(Ubiquitous) 환경이 조성됨에 따라 RFID의 사용량이 늘고 있다. RFID는 Radion Frequency IDentification의 약어로 바코드를 대체하기 위한 무선 주파수 식별 기술이다. 태그는 전원을 가지고 있어 장거리 인식이 가능한 능동형 태그와 리더로부터 전원을 공급받는 수동형 태그로 분류된다. 능동형 태그는 장거리 인식과 뛰어난 성능에 따라 고가이기 때문에 일반적으로 저가의 수동형 태그를 사용한다. 하지만 수동형 태그라 불리는 Low-Cost RFID 시스템은 리더의 쿼리에 의하여 쉽게 동작하기 때문에 태그에 저장되어 있는 사용자 및 물품의 정보가 노출되어 프라이버시 침해 문제가 발생한다. 이를 보완하기 위하

† 준 회 원 : 순천향대학교 전산학과 석사과정
†† 종신회원 : 순천향대학교 컴퓨터학부 교수
논문접수 : 2007년 2월 28일, 심사완료 : 2007년 8월 23일

여 고유 ID 대신 해쉬된 ID 값을 사용하는 방식, 난수를 생성하여 사용하는 방식, 해쉬 함수를 사용하는 방식 등 많은 연구가 진행되었다. 하지만 해쉬된 ID 값이라 하더라도 ID의 무결성은 제공할 수 있으나 고정된 값이기 때문에 위치 추적에 대한 문제가 발생하였고, 난수를 사용하는 방법은 태그가 R.N.G(Random Number Generation)를 탑재해야 되므로 문제가 되었다. 또한 해쉬 함수를 사용하는 방식은 가장 안전한 방식이지만 5K~10K 게이트 중 250~3K 게이트만을 보안으로 사용해야 되기 때문에 경량화가 필요하게 되었다. 따라서 난수를 리더나 데이터베이스에서 생성하며, 해쉬 함수의 횟수를 줄이고, 경량화를 위한 간단한 연산을 사용하는 방식의 연구가 활발히 진행되고 있다. 또한 상호 인증을 위하여 비밀 키 값을 정당한 객체만이 사전에 공유하고 키 값을 통하여 정당성을 검증한다.

따라서 본 논문에서는 난수를 이용하여 가변적인 값을 생성하고 사전에 안전하게 공유된 비밀 값을 통하여 각 객체들의 정당성을 검증한다. 또한 제안 방식은 간단한 연산(XOR, OR)만을 이용하여 Low-Cost RFID 시스템에서 구현하여 사용할 수 있도록 하였으며, 확장된 방식은 제안 방식에서 제공되지 못했던 무결성을 제공하기 위하여 해쉬 함수를 사용하여 더욱 안전하게 하였다.

본 논문은 2장에서 RFID 시스템에서 발생할 수 있는 보안 위협과 요구 사항에 대하여 제시하고 3장에서는 기존 방식들을 기술하며, 4장에서는 요구 사항을 만족하는 제안 방식에 대하여 기술한다. 5장에서는 제안 방식을 분석하고 6장에서 결론 및 향후 연구 방향을 제시함으로써 끝맺도록 하겠다.

2. 보안 위협 및 보안 요구 사항

RFID 시스템의 태그와 리더는 무선 주파수 통신을 사용하기 때문에 불법적인 제 3자에 의하여 통신 내용이 노출될 수 있으며 획득한 정보를 기반으로 재전송공격 및 트래픽 분석으로 다음 세션에 사용될 값이 노출되거나 사용자의 위치 추적이 가능할 수 있다. 이를 해결하기 위하여 보안 요구 사항을 제기하고 각 요구 사항들을 만족할 수 있도록 해야 한다. 따라서 본 장에서는 이러한 RFID 시스템에서 발생할 수 있는 보안 위협들과 이를 보완하기 위하여 제공되어야 할 보안 요구 사항에 대하여 알아본다.

2.1 보안 위협

무선 주파수 통신을 하는 RFID 시스템은 무선 채널을 이용하기 때문에 불법적인 제 3자의 공격에 취약할 수 있다. 따라서 RFID 시스템에서 발생할 수 있는 공격 유형을 알고 이에 대응할 수 있는 방안을 강구해야 한다. 다음은 RFID 시스템에서 발생할 수 있는 보안 위협에 대하여 기술한 것이다.

◈ 도청(Eavesdropping) : 태그와 리더 간의 통신 채널에서 전송되는 데이터를 불법적인 사용자에게 노출될 수 있으며 도청으로 획득한 데이터를 기반으로 재전송공격 및 트래픽 분석이 가능하다.

◈ 중간자공격(Man-in-the-Middle Attack) : 불법적인 제 3자가 태그와 리더 간의 전송되는 데이터를 획득하여 위조 및 변조하여 전송함으로써 정당한 사용자로 인증 받거나 정당한 사용자가 인증 받지 못하도록 할 수 있다.

◈ 재전송공격(Replay Attack) : 도청으로 획득한 데이터를 정당한 객체에게 재전송하여 정당한 객체로 인증 받거나 동일한 값 획득으로 사용자의 위치 추적을 할 수 있다. 재전송공격으로 안전하기 위해서는 난수나 타임스탬프 등을 사용하여 고정된 값이 출력되지 않도록 해야 한다.

◈ 위치 추적(Tracking Attack) : 태그에서 노출되는 값이 고정되어 있을 경우 정확한 위치는 알 수 없지만 사용자의 추적이 가능하므로 프라이버시가 침해될 수 있다.

2.2 보안 요구 사항

앞서 제기된 RFID 시스템에서 발생할 수 있는 위협 사항들을 해결하기 위하여 만족해야 할 보안 요구 사항들을 기술한다.

◈ 상호 인증(Mutual Authentication) : 통신하는 객체들 간의 정당성을 검증할 수 있어야 한다. 공유한 비밀 값을 확인하여 인증하거나 동일한 값을 생성함으로써 상대방을 인증한다.

◈ 익명성(Anonymity) : 태그에서 노출되는 정보를 획득하더라도 어떠한 태그로부터 전송된 값인지 알 수 없어야 하며 추측할 수 없어야 한다.

◈ 기밀성(Confidentiality) : 비밀 값이나 태그의 ID와 같은 식별 값은 정당한 객체들만이 사전에 안전하게 공유되어야 한다.

◈ 무결성(Integrity) : 무선 통신 채널에서 데이터를 전송할 때 불법적인 제 3자에 의하여 데이터가 위조 및 변조될 수 있다. 이를 방지하기 위하여 암호화 알고리즘이나 해쉬 함수를 사용할 수 있지만 저가의 수동형 태그에서 연산 능력이 낮기 때문에 일반적으로 해쉬 함수를 사용하여 무결성을 제공한다.

3. 기존 연구

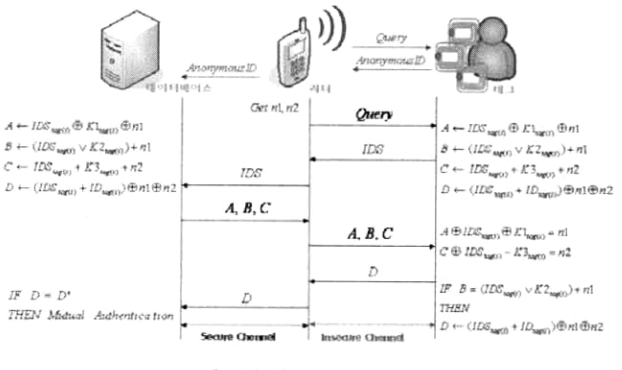
RFID 시스템에서 프라이버시를 보호하기 위하여 많은 연구가 진행되고 있다. 보안을 제공하기 위하여 일반적으로 해쉬 함수를 사용하고 있지만 LMAP, M^2AP, EMAP 방식은 간단한 연산(XOR, OR, AND, ADD)만으로 보안을 제공하는 방안이다. 96비트의 키를 4개로 분할하여 다른 키처럼 사용하며, 매 세션마다 키 값과 메시지를 갱신함으로써 사용자의 위치 추적으로부터 안전하게 하고 재전송공격을 해결할 수 있다. 본 장에서는 기존 방식들에 대하여 기술한다.

3.1 LMAP(Lightweitht Mutual Authentication Protocol)

본 방식은 300 게이트만을 사용하여 보안을 제공할 수 있

는 경량화된 상호 인증 방안으로 96비트의 키를 4개로 분할하고 메시지 4개를 생성하여 리더가 태그에게 A, B, C 메시지를 전송하면 태그는 A, B, C 메시지에 대응되는 D 메시지를 전송함으로써 상호 인증이 제공되는 방식이다[4]. 리더는 태그에게 $Query$를 보내고 태그는 서버에 저장될 때 순서에 해당하는 인덱스 값 $IDS(Index-Pseudonym)$를 리더를 통해 데이터베이스로 전송하게 된다. 데이터베이스는 전송된 IDS를 검색하고 동일한 값이 있을 경우 그 태그의 키 값들과 생성한 두 난수를 이용하여 메시지 A, B, C를 생성하여 태그에게 전송한다. 태그는 A를 이용하여 난수 $n1$을 획득하고 B를 이용하여 난수 $n2$를 획득한다. 또한 B를 생성하여 전송된 값과 동일할 경우 D를 생성하여 데이터베이스로 전송한다. 데이터베이스는 전송된 D와 생성한 D가 일치하면 태그를 인증한다.

하지만 태그에서 난수 검증 과정이 없어서 A를 $A = IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1 \oplus \alpha$로 B를 $B = (IDS_{tag(i)} \vee K2_{tag(i)}) + n1 \oplus \alpha$로 C를 $C = IDS_{tag(i)} + K3_{tag(i)} + n2 \oplus \beta$로 변경했을 경우 태그는 A를 통해 난수를 $n1 \oplus \alpha$로, C를 통해 난수를 $n2 \oplus \beta$로 인식하고 B 검증 후 변경된 두 난수를 이용하여 D를 생성하여 데이터베이스로 전송한다. 데이터베이스는 D 값을 검증할 수 없으므로 정당한 태그라도 인증 받지 못하게 된다. 본 방식의 프로토콜은 (그림 1)과 같고 메시지 생성 방식은 <표 1>에 기술되어 있다.



(그림 1) LMAP 방식

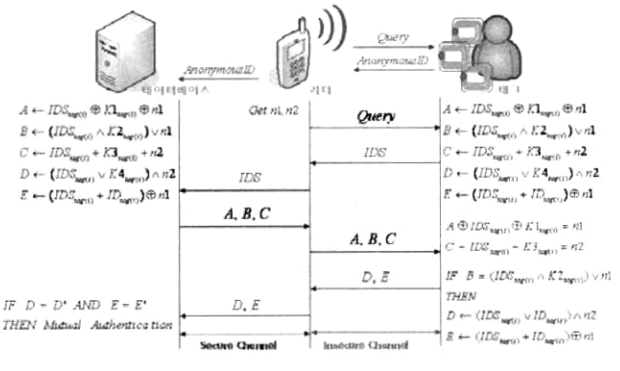
<표 1> LMAP 방식의 메시지 생성 과정과 갱신 과정

메시지 생성 과정	갱신 과정
$A = IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$	$IDS_{tag(i+1)} = (IDS_{tag(i)} + (n2 \oplus K4_{tag(i)})) \oplus ID_{tag(i)}$
$B = (IDS_{tag(i)} \vee K2_{tag(i)}) + n1$	$K1_{tag(i+1)} = K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)} + ID_{tag(i)})$
$C = IDS_{tag(i)} + K3_{tag(i)} + n2$	$K2_{tag(i+1)} = K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)} + ID_{tag(i)})$
$D = (IDS_{tag(i)} + ID_{tag(i)}) \oplus n1 \oplus n2$	$K3_{tag(i+1)} = (K3_{tag(i)} \oplus n1) + (K1_{tag(i)} \oplus ID)$
	$K4_{tag(i+1)} = (K4_{tag(i)} \oplus n1) + (K2_{tag(i)} \oplus ID)$

3.2 M²AP(Minimalist Mutual Authentication Protocol)

본 방식은 LMAP 방식과 동일한 300 게이트만을 사용하였으나 메시지 E를 추가하여 LMAP 방식보다 더 확실하게 데이터베이스를 인증할 수 있는 방식이다[5]. 본 방식도 96비트의 키를 4개로 분할하여 24비트의 키를 이용하고 키는 2^{24}의 안전성을 갖는다. 인덱스에 해당하는 메시지 A, B, C를 태그에게 전송하는 단계는 LMAP 방식과 같으며 단지 메시지 생성 방식과 키 및 IDS 갱신 방식이 다르다. 또한 태그는 A, B, C를 전송받고 메시지 B 검증 후 메시지 D와 E를 생성하여 데이터베이스로부터 인증 받는다.

하지만 A, C를 검증할 수 있는 방안이 없으므로 악의적인 제3자가 난수를 변경할 수 있으며 태그가 메시지를 검증할 수 없으므로 데이터베이스를 인증하지 못하며, 데이터베이스는 메시지 D와 E가 올바로 전송되어야 태그를 인증하므로 상호 인증을 제공할 수 없다. 본 방식의 프로토콜은 (그림 2)와 같으며 메시지 생성 과정 및 키와 IDS 갱신 과정은 <표 2>와 같다.



(그림 2) M²AP 방식

<표 2> M²AP 방식의 메시지 생성 과정과 갱신 과정

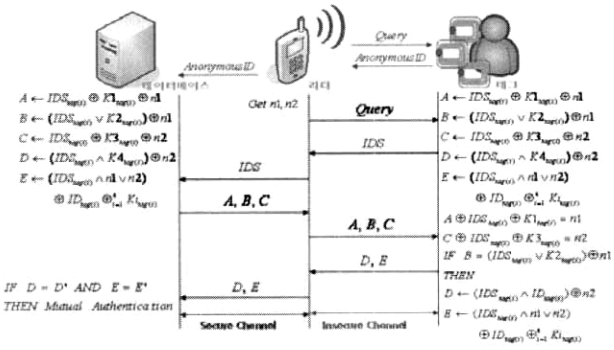
메시지 생성 과정	갱신 과정
$A = IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$	$IDS_{tag(i+1)} = (IDS_{tag(i)} + (n2 \oplus n1)) \oplus ID_{tag(i)}$
$B = (IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$	$K1_{tag(i+1)} = K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)} + ID_{tag(i)})$
$C = IDS_{tag(i)} + K3_{tag(i)} + n2$	$K2_{tag(i+1)} = K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)} + ID_{tag(i)})$
$D = (IDS_{tag(i)} \vee K4_{tag(i)}) \wedge n2$	$K3_{tag(i+1)} = (K3_{tag(i)} \oplus n1) + (K1_{tag(i)} \oplus ID)$
$E = (IDS_{tag(i)} + ID_{tag(i)}) \oplus n1$	$K4_{tag(i+1)} = (K4_{tag(i)} \oplus n1) + (K2_{tag(i)} \oplus ID)$

3.3 EMAP(Efficient Mutual Authentication Protocol)

본 방식은 LMAP 방식과 M²AP 방식보다 효율성을 더 증가시킨 방식으로 150 게이트만을 사용하여 보안을 제공하는 효율적인 인증 방식이다[3]. 메시지 E에서 분할된 4개 키들의 XOR 연산 시그마 값($K1 \oplus K2 \oplus K3 \oplus K4$)을 생성하여 모든 키 값이 XOR 연산되도록 하는 방식이다. LMAP 방식과 M²AP 방식은 4개의 키 중 하나의 키와 연산을 하였지만 본 방식에서는 4개의 키 값을 모두 XOR 연산하기 때문에 키 값을 더 확실하게 검증할 수 있다. 또한 96비트의 ID를 반으로 분할하여 1~48비트의 ID와 49~96비트까지의 ID를 사용함으로써 두 개의 식별 값을 사용하는 효과를 가져 오며, 안전한 함수 $f()$에 키 값을 입력하여 생성된 출력 값을 사용함으로써 안전성을 높이고 있다.

앞에 기술된 두 방식에 비하여 더 안전하며 효율적이지만, 난수 검증 과정이 없어 데이터 위조 및 변조가 가능하

며 한 세션 후 4개의 키 값과 *IDS*가 갱신되기 때문에 비동기가 발생했을 경우 위치 추적의 문제가 발생하며 사용자 익명성이 제공되지 못한다. 본 방식의 프로토콜은 (그림 3)과 같으며 메시지 생성 과정 및 키와 *IDS* 갱신 과정은 <표 3>과 같다.



(그림 3) EMAP 방식

〈표 3〉 EMAP 방식의 메시지 생성 과정과 갱신 과정

메시지 생성 과정	갱신 과정
$A = IDS_{tag(i)} \oplus K1_{tag(i)} \oplus n1$	$IDS_{tag(i+1)} = (IDS_{tag(i)} + (n2 \oplus n1)) \oplus ID_{tag(i)}$
$B = (IDS_{tag(i)} \wedge K2_{tag(i)}) \vee n1$	$K1_{tag(i+1)} = K1_{tag(i)} \oplus n2 \oplus (K3_{tag(i)} + ID_{tag(i)})$
$C = IDS_{tag(i)} + K3_{tag(i)} + n2$	$K2_{tag(i+1)} = K2_{tag(i)} \oplus n2 \oplus (K4_{tag(i)} + ID_{tag(i)})$
$D = (IDS_{tag(i)} \vee K4_{tag(i)}) \wedge n2$	$K3_{tag(i+1)} = (K3_{tag(i)} \oplus n1) + (K1_{tag(i)} \oplus ID)$
$E = (IDS_{tag(i)} \wedge n1 \vee n2) \oplus ID_{tag(i)} \oplus^{4} K1_{tag(i)}$	$K4_{tag(i+1)} = (K4_{tag(i)} \oplus n1) + (K2_{tag(i)} \oplus ID)$

4. 제안 방식

기존 방식들은 상호 인증을 위하여 96비트의 키를 4개로 분할하여 사용하였으며 리더에서 두 개의 난수를 생성하여 보안을 제공하였다. 본 방식은 64비트의 키를 2개로 분할하여 기존 방식에 비해 사용되는 키를 24비트에서 32비트로 8비트 늘리고, 전체 키 크기는 128비트에서 96비트로 32비트 줄인다. 또한 기존 방식은 난수를 2개 생성하였으나 제안 방식은 1개만 생성함으로써 효율성을 제공하고 있다. Key^{32} Division 방식은 기존 방식들과 마찬가지로 경량화 연산(XOR, OR)만으로도 보안을 제공할 수 있는 방안이다. 하지만 수동형 공격뿐만 아니라 능동형 공격자에 대해서도 보안을 제공해야하기 때문에 충돌성이 없는 안전한 해쉬 함수를 이용하여 Hash-based Key^{32} Division 방식으로 보완하였다. 본 장에서는 보안 위협을 막고 요구 사항들을 만족할 수 있는 안전하고 효율적인 방식을 제안한다.

4.1 가정 사항

제안 방식은 다음과 같은 일반적인 RFID 시스템에서의 가정 사항을 기반으로 한다.

◈ 리더와 태그 간의 통신 채널은 무선 통신 구간으로 불안전한 채널로 구성되어 있으며 리더와 데이터베이스 간의 통신 채널은 SSL/TLS와 같이 안전한 채널로 구성되어 있다.

◈ 64비트의 키 값과 태그의 식별 정보는 정당한 객체(태그, 리더, 데이터베이스)만이 안전하게 사전 공유한다.

◈ 리더는 R.N.G(Random Number Generator)를 탑재하고 있어 매 세션 다른 난수를 생성할 수 있다.

◈ Hash-based Key^{32} Division 방식에서 통신 객체들(태그, 리더, 데이터베이스)은 안전한 해쉬 함수를 가지고 있어 해쉬 값을 생성할 수 있다.

4.2 시스템 계수

본 제안방식은 다음의 시스템 계수를 사용한다.

◈ Ki : 64비트의 키를 2개로 분할한 후 i번째 키 값 $(i = 1, 2)$

◈ ID : 태그마다 다른 식별 값으로 한 태그는 하나의 ID를 저장

◈ $metaID$: 태그 ID를 해쉬한 값 $H(ID)$

◈ r : 리더의 R.N.G에서 매 세션 다르게 생성하는 난수

◈ V_1 : 첫 번째 가변적인 값 $K_1 \vee r$

◈ V_2 : 두 번째 가변적인 값 $K_2 \vee r$

◈ Kr_1 : 첫 번째 키 값과 난수의 XOR 연산한 값 $K1 \oplus r$

◈ Kr_2 : $metaID$와 V_1의 XOR 연산한 값 $metaID \oplus V_1$

◈ Kr_3 : 태그 ID와 V_2의 XOR 연산한 값 $ID \oplus V_2$

◈ H_1 : 해쉬 값 1로 $metaID$와 V_1을 해쉬한 값 $H(metaID \| V_1)$

◈ H_2 : 해쉬 값 2로 ID와 V_2를 해쉬한 값 $H(ID \| V_2)$

4.3 제안 방식

본 장에서는 앞서 기술한 보안 위협을 막고 요구사항을 만족할 수 있는 방안에 대하여 제안한다.

4.3.1 Key^{32} Division 방식

Key^{32} Division 방식은 Low-Cost RFID 시스템에서 구현할 수 있도록 제안된 방식으로 XOR 연산과 OR 연산만으로 보안을 제공하며 64비트의 키를 두 개로 분할하여 32비트의 키를 사용하는 방식이다. 기존 방식들보다 전체 키 크기는 96버트에서 64비트로 32비트 작아지고 사용되는 키는 24비트에서 32비트로 8비트 커지기 때문에 32비트의 저장 공간의 효율과 키 생성 개수가 2^{24}에서 2^{32}로 많아짐으로써 안전성이 더 높아진 방식이다.

단계 1. 리더는 통신을 시작하기 위하여 R.N.G에서 난수 r을 생성하고 64비트의 키를 분할하여 1~32비트의 첫 번째 키 $K1$과 난수 r을 XOR 연산하여 생성한 Kr_1을 태그에게 전송한다.

$$Kr_1 = K1 \oplus r$$

단계 2. 태그는 리더로부터 Kr_1을 전송받고 태그의 $K1$을 XOR 연산하여 r을 획득한다. 태그는 획득한 r과 $K1$을 OR

연산을 하여 V_1을 생성하고, $metaID$와 V_1을 XOR 연산하여 생성한 Kr_2을 리더에게 전송한다.

$$Kr_1 \oplus K1 = r$$
$$V_1 = K1 \vee r$$
$$Kr_2 = metaID \oplus V_1$$

단계 3. 리더는 태그로부터 Kr_2를 전송받고 통신 시작 시 생성한 r을 Kr_2와 연접하여 데이터베이스로 전송한다.

단계 4. 데이터베이스는 전송 받은 r과 $K1$을 OR 연산하여 V_1'를 생성하고 전송 받은 Kr_2에 V_1'를 XOR 연산하여 $metaID'$를 획득한다. 데이터베이스는 획득한 $metaID'$와 동일한 $metaID$가 저장되어 있을 경우 태그를 인증하고, $metaID$에 해당하는 ID를 획득한다. 또한 $K2$와 r을 OR 연산하여 V_2를 생성하고 획득한 ID를 XOR 연산하여 Kr_3를 생성한 후 리더로 전송한다.

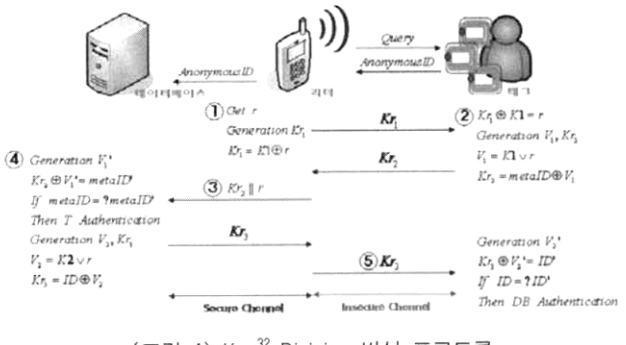
$$K1 \vee r = V_1'$$
$$Kr_2 \oplus V_1' = metaID'$$
$$metaID = ?metaID'$$
$$V_2 = K2 \vee r$$
$$Kr_3 = ID \oplus V_2$$

단계 5. 태그는 Kr_3를 전송받고 $K2$와 r을 OR 연산하여 V_2'를 생성한 후 Kr_3와 XOR 연산하여 ID'를 획득한다. 태그는 저장되어 있는 ID와 동일한 ID'가 획득되었을 경우 데이터베이스를 인증하고 상호 인증을 제공한다.

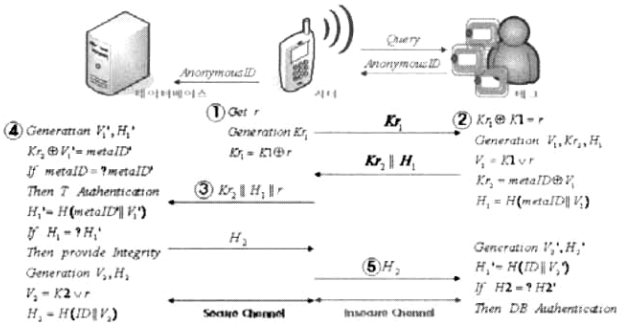
$$V_2' = K2 \vee r$$
$$Kr_3 \oplus V_2' = ID'$$
$$ID = ?ID'$$

4.3.2 확장된 제안 방식

제안 방식은 XOR 연산과 OR 연산을 사용하여 수동형 공격에는 안전하지만 전송 도중 메시지를 위조 및 변조하는 능동형 공격자에 대해서는 보안을 제공하지 못한다. 따라서 확장된 방식은 해쉬 함수를 사용함으로써 데이터가 전송되는 도중 위조 및 변조되지 못하도록 하며 능동형 공격자에 대해서 안전한 방식이다.



(그림 4) Key[32] Division 방식 프로토콜



(그림 5) Hash-based Key[32] Division 방식 프로토콜

단계 1. 리더는 통신을 시작하기 위하여 R.N.G에서 난수 r을 생성하고 64비트의 키를 분할한 뒤 첫 번째 키인 $K1$과 r을 XOR 연산하여 Kr_1을 생성한다.

$$Kr_1 = K1 \oplus r$$

단계 2. 태그는 리더로부터 Kr_1을 태그의 $K1$을 Kr_1에 XOR 연산하여 r을 획득한다. 태그의 $K1$과 획득한 r을 OR 연산하여 V_1을 생성하고 태그의 $metaID$와 XOR 연산하여 Kr_2를 생성한다. 또한 데이터 무결성을 위하여 $metaID$와 V_1을 해쉬하여 H_1을 생성하고 Kr_2와 H_1을 리더에게 전송한다.

$$Kr_1 \oplus K1 = r$$
$$V_1 = K1 \vee r$$
$$Kr_2 = metaID \oplus V_1$$
$$H_1 = H(metaID \| V_1)$$

단계 3. 리더는 태그로부터 Kr_2와 H_1을 전송받고 통신 시작 시 생성한 r을 Kr_2, H_1과 연접하여 데이터베이스로 전송한다.

단계 4. 데이터베이스는 전송 받은 r과 $K1$을 OR 연산하여 V_1'를 생성하고 전송된 Kr_2와 V_1'를 XOR 연산하여 $metaID'$를 획득한다. 데이터베이스는 획득한 $metaID'$와 동일한 $metaID$가 저장되어 있을 경우 태그를 인증하고, $metaID$에 해당하는 ID를 획득한다. 또한 $metaID'$와 V_1'를 해쉬하여 H_1'를 생성하고 전송된 H_1과 비교하여 값이 동일할 경우 무결성을 검증한다. 데이터베이스는 인증 결과 값을 생성하기 위하여 $K2$와 r을 OR 연산하여 V_2를 생성하고 ID와 V_2를 해쉬한 H_2를 리더에게 전송한다.

$$V_1' = K1 \vee r$$
$$Kr_2 \oplus V_1' = metaID'$$
$$metaID = ?metaID'$$
$$H_1 = ?H(metaID' \| V_1)$$
$$V_2 = K2 \vee r$$
$$H_2 = H(ID \| V_2)$$

단계 5. 태그는 리더를 통해 전송된 H_2를 검증하기 위하

여 태그에 저장되어 있는 $K2$와 r을 OR 연산하여 V_2'를 생성한다. ID와 V_2'를 해쉬한 값과 전송된 H_2를 비교하여 두 값이 일치하면 데이터베이스를 인증하여 상호 인증이 이루어진다.

$$V_2' = K2 \vee r$$
$$H_2 = ?H(ID \| V_2)$$

5. 제안 방식 분석

제안 방식은 2장에서 제기되었던 보안 요구 사항을 만족할 수 있는지에 대하여 분석할 것이다. 또한 2006년 Low-Cost RFID 시스템을 기반으로 연구되었던 LMAP 방식, M^{2}AP 방식, EMAP 방식과 제안 방식을 비교함으로써 제안 방식은 효율성을 더 높일 수 있으며 확장된 제안 방식은 기존 방식들보다 효율성은 떨어져 현재 구현은 난해하지만 향후 태그의 연산 능력이 증가되면 사용자가 안전하게 RFID 시스템을 사용할 수 있도록 고안된 방식이다. 본 장에서는 기존 방식들과 제안 방식을 비교하여 분석한다.

5.1 보안 위협에 따른 안전성

제안 방식은 앞의 2장에서 기술한 보안 위협에 따라 그 안전성을 검증할 수 있다. 보안 위협으로는 도청, 중간자공격, 재전송공격, 위치 추적 네 가지 위협 사항을 제기하였으며 이를 보완할 수 있는 정도에 따라 제안 방식의 안전성을 평가할 수 있다.

◈ 도청(Eavesdropping) : 무선 통신 채널이기 때문에 불법적인 제 3자에 의하여 통신 내용은 도청될 수 있지만 XOR 연산 및 OR 연산을 통하여 트래픽 분석을 막음으로써 중요 값은 획득할 수 없다. 기존 방식들과 제안 방식들은 리더와 태그 간에 통신하는 데이터를 제 3자에게 모두 노출되어 도청이 가능하다.

◈ 중간자공격(Man-in-the-Middle Attack) : 기존의 방식에서 리더가 태그에게 보내는 메시지의 난수 $n1$을 $n1 \oplus \alpha$로 변경하고 난수 $n2$를 $n2 \oplus \beta$로 변경하여 전송할 수 있으며 난수 검증 과정이 없어 중간자 공격이 가능하다. Key^{32} Division 방식도 전송되는 데이터에 다른 값을 XOR 연산할 수는 있지만 검증 과정이 있으므로 데이터 변조를 알 수 있다. Hash-based Key^{32} Division 방식은 해쉬 값을 함께 전송하여 중간자가 데이터를 변조할 수 없도록 하였다.

◈ 재전송공격(Replay Attack) : 기존 방식에서는 각 라운드마다 두 개의 난수 $n1$과 $n2$를 사용하여 재전송공격을 막고 있으며, 기존 방식에서는 각 라운드마다 한 개의 난수 r을 사용하여 재전송공격에 안전하다.

◈ 위치 추적(Tracking Attack) : 기존 방식에서는 두 개의 난수 $n1$과 $n2$를 이용하여 가변적인 값을 생성하고 위치 추적으로부터 안전할 수 있으며, 제안 방식에서는 난수 r과 XOR 연산을 하여 값이 매 세션 변경되므로 위치 추적으로부터 안전하다.

5.2 보안 요구 사항 만족에 따른 안전성

2장에서 제시한 보안 요구 사항 만족 여부에 따른 안전성을 평가하여 제안 방식을 분석한다. 앞서 도출한 보안 요구 사항을 최대한 만족할 수 있어야 하며 어떤 값으로 인하여 요구 사항들이 만족될 수 있는지 분석한다. <표 4>에서 요구 사항이 만족하는지 그리고 어떤 요인으로 인하여 제공되고 제공되지 않는지에 대하여 나타낸다.

◈ 상호 인증(Mutual Authentication) : 기존 방식에서 난수 메시지 A에 중간자가 α를 XOR 연산하고 B에 β를 XOR 연산하여 태그에게 전송하면 태그는 난수 검증과정이 없으므로 $n1$을 $n1 \oplus \alpha$로, $n2$를 $n2 \oplus \beta$로 알고 두 난수 $n1 \oplus \alpha$과 $n2 \oplus \beta$를 이용하여 응답 메시지 $D(,E)$를 생성하여 전송함으로써 데이터베이스는 태그를 인증하지 못한다. 하지만 Key^{32} Division 방식에서는 데이터베이스가 Kr_2를 검증하여 $metaID'$를 획득하고 데이터베이스에 획득한 식별 정보와 동일한 값이 있으면 태그를 인증하고 Kr_3를 전송한다. 태그는 Kr_3를 검증하여 획득한 ID'와 자신의 ID가 동일하면 상호 인증을 제공한다. Hash-based Key^{32} Division 방식에서는 XOR 연산된 Kr_2와 H_1을 데이터베이스에서 검증하고 획득한 $metaID'$가 저장되어 있으면 태그를 인증한다. 태그는 데이터베이스로부터 전송된 H_2'와 생성한 $H(ID \| V_2')$를 비교하여 두 값이 동일하면 상호 인증을 제공한다.

◈ 익명성(Anonymity) : Key^{32} Division 방식은 난수와 연산을 통하여 태그의 ID와 분할된 키 $K1$이 노출되지 못하도록 $K1 \oplus r$과 $metaID \oplus V_1 (V_1 = K1 \vee r)$을 사용함으로써 키 값이 노출되지 못하도록 하고 $ID \oplus V_2 (V_2 = K2 \vee r)$을 사용함으로써 태그의 ID가 노출되지 못하도록 하여 익명성을 제공한다. Hash-based Key^{32} Division 방식도 Key^{32} Division 방식과 동일하게 난수가 사용되며, Kr_1, Kr_2, H_1을 사용함으로써 키 값의 노출을 막고 H_2를 사용함으로써 태그의 ID가 노출되지 못하도록 하여 사용자 익명성을 제공한다.

◈ 기밀성(Confidentiality) : 태그와 데이터베이스는 64비트의 키와 태그의 ID, ID를 해쉬한 $metaID$를 정당한 객체만이 공유하고 있으며 불법적인 제 3자가 알 수 없도록 난수와의 연산을 통해 중요 값을 노출시키지 않아 기밀성을 제공하고 있다.

◈ 무결성(Integrity) : Key^{32} Division 방식은 XOR 연산과 OR 연산만으로 수동형 공격자에 대하여 보안을 제공하는 Low-Cost RFID 시스템을 위한 인증 방안이다. 하지만 Kr_2가 전송되는 도중 Kr_2'로 변경되어 전송되었을 경우 데이터베이스는 Kr_2를 검증할 수 없으며 정당한 태그라도 인증 받을 수 없다. 따라서 무결성이 제공되지 못한다. 하지만 Hash-based Key^{32} Division 방식은 Kr_2가 전송되는 도중 위조 및 변조되는 것을 막기 위하여 H_1을 함께 전송하여 무결성을 제공한다. 불법적인 제 3자가 Kr_2'를 전송한다 하더라도 Kr_2에서 획득한 $metaID'$와 저장되어 있던 V_1을 해쉬한 값이 H_1과 일치

하지 않으며 전송되는 도중 위조 및 변조가 발생했다는 것을 인식하고 태그에게 다시 쿼리를 전송한다.

〈표 4〉 보안 위협 및 보안 요구 사항에 따른 비교 분석표

	LMAP	M^2AP	EMAP	K^{32} Division 방식	Hash-based K^{32} Division 방식
도청	X	X	X	X	X
	도청은 가능 *IDS* 노출	도청은 가능 *IDS* 노출	도청은 가능 *IDS* 노출	중요 값 노출 불가능	중요 값 노출 불가능
중간자 공격	X	X	X	△	O
	난수 변조 가능 $n1 \rightarrow n1 \oplus \alpha$ $n2 \rightarrow n1 \oplus \beta$	난수 변조 가능 $n1 \rightarrow n1 \oplus \alpha$ $n2 \rightarrow n1 \oplus \beta$	난수 변조 가능 $n1 \rightarrow n1 \oplus \alpha$ $n2 \rightarrow n1 \oplus \beta$	변조가 가능하나 변조 시 확인 가능	데이터 위조 및 변조 불가능
재전송 공격	O	O	O	O	O
	난수 사용 키, 메시지 갱신	난수 사용 키, 메시지 갱신	난수 사용 키, 메시지 갱신	난수 사용	난수 사용
위치 추적	O	O	O	O	O
	난수 사용 키, 메시지 갱신	난수 사용 키, 메시지 갱신	난수 사용 키, 메시지 갱신	난수 사용	난수 사용
상호 인증	X	X	X	O	O
	일방향 인증	일방향 인증	일방향 인증	상호 인증 제공	상호 인증 제공
익명성	△	△	△	O	O
	IDS 노출	*IDS* 노출	*IDS* 노출	난수 사용	난수 사용
기밀성	O	O	O	O	O
	K1, *K2*, *K3*, *K4*, *ID*	*K1*, *K2*, *K3*, *K4*, *ID*	*K1*, *K2*, *K3*, *K4*, *ID*	*K1*, *K2*, *ID*, *metaID*	*K1*, *K2*, *ID*, *metaID*
무결성	X	X	X	△	O
	난수 검증 불가 $n1, n2$	난수 검증 불가 $n1, n2$	난수 검증 불가 $n1, n2$	변조는 가능하나 변조 시 확인 가능	해쉬함수 사용
효율성	O	O	O	O	X
	⊕, ∨, ∧,	⊕, ∨, ∧,	⊕, ∨, ∧,	⊕, ∨	2회 $H(\ )$

〈표 5〉 효율성 및 안전성에 따른 비교 분석표

	LMAP	M^2AP	EMAP	K^{32} Division 방식	Hash-based K^{32} Division 방식
XOR(⊕)	5/session	3/session	11/session	3/session	2/session
OR(∨)	1/session	2/session	2/session	1/session	1/session
AND(∧)		2/session	2/session	-	-
ADD(+)	2/session	1/session	-		-
SUB(−)	1/session	2/session			
Function	-		함수 $f(\ )$ 1/session	-	해쉬 함수 1/session
전체 키 길이	96bit/4	96bit/4	96bit/4	64bit/2	64bit/2
분할 키 길이	24bit	24bit	24bit	32bit	32bit
태그 저장 공간	6ℓ *ID*, *IDS*, *K* *K2*, *K3*, *K*	6ℓ *ID*, *IDS*, *K* *K2*, *K3*, *K*	6ℓ *ID*, *IDS*, *K* *K2*, *K3*, *K*	4ℓ bit *ID*, *K1*, *K2* *metaID*	4ℓ bit *ID*, *K1*, *K2*, *metaID*
총 통신 횟수	7 pass	7 pass	7 pass	5 pass	5 pass
키 조합 개수 (안전성)	2^{24}	2^{24}	2^{24}	2^{32}	2^{32}

또한 <표 5>에서는 기존 방식들과 제안 방식들의 효율성 및 안전성을 비교하기 위하여 한 세션 당 사용되는 연산들의 횟수와 사용되는 키 길이 및 분할된 키 길이 등에 대하여 비교 분석하였다. 태그의 저장 공간은 저장하고 있는 한 필드를 1ℓbit라고 했을 때 저장하고 있는 데이터 공간을 의미한다. 비록 하나의 키가 기존 방식에서는 4개로, 제안 방식에서는 2개로 분할되어 있지만 키들을 각각 저장해야하기 때문에 따로 따로 필드별로 저장되어 있어야 한다. 또한 통신 횟수는 RFID 시스템에서 데이터를 전송하는 횟수를 의미하며, 기존 방식에서는 리더와 태그 간의 4번의 통신과 리더와 데이터베이스 간의 3번의 통신을 합하여 총 통신 횟수가 7회이다. 그러나 Key^{32} Division 방식과 Hash-based Key^{32} Division 방식은 태그와 리더간의 3번의 통신과 리더와 데이터베이스 간의 2번의 통신을 합하여 총 5회의 통신 횟수를 갖는다. 통신 횟수가 감소할수록 한 세션 당 소요되는 시간은 감소하며 시간적 효율을 제공한다. 키 조합 개수는 사전 공격 및 Brute Force 공격과 같이 키를 유추하는 공격을 당할 경우 키 값이 노출되기까지의 계산해야하는 횟수로 키 길이가 길어질수록 시도해야할 경우의 수가 증가하여 키 값의 안전성을 높일 수 있다. 기존 방식에서는 24비트의 키를 사용하여 2^{24}개의 키를 생성하는 과정에서 키 값이 노출될 수 있으나 Key^{32} Division 방식과 Hash-based Key^{32} Division 방식에서는 2^{32}개의 키를 생성하였을 경우 노출될 수 있어 키 노출에 대하여 더욱 안전하게 하였다.

6. 결 론

유비쿼터스의 핵심 기술인 RFID 시스템은 리더의 신호에 의하여 쉽게 동작하기 때문에 태그에 저장되어 있는 정보가 쉽게 노출되어 프라이버시 침해 문제가 대두되어 왔다. 따라서 본 방식은 64비트의 키를 두 개로 분할하고 난수와 카운트 값을 사용하여 보안을 제공한다. 제안 방식은 XOR 연산 및 OR 연산으로 키 값과 식별 값을 노출시키지 않기 때문에 수동형 공격자에 대하여 보안을 제공한다. 하지만 데이터를 위조 및 변조하는 능동형 공격자에 대해서는 보안을 제공할 수 없기 때문에 확장된 제안 방식은 해쉬 함수를 사용하여 능동형 공격자에 대하여 보안을 제공한다. XOR 연산된 값과 해쉬 값을 연접하여 전송함으로써 데이터가 전송 도중 위조 및 변조되지 않았음을 확인할 수 있다. 하지만 현재 사용되고 있는 Low-Cost RFID 시스템에 적용하기는 구현의 어려움을 겪을 것이다. Low-Cost RFID 시스템은 5K~10K 정도의 게이트를 가지고 있지만 단지 250~3K 게이트 정도만을 보안에 할당할 수 있다. 따라서 해쉬 함수를 경량화해야 하고, 경량화 된 보안을 사용하면서도 안전할 수 있는 방안에 대하여 연구해야 할 것이다. 경량화와 보안의 절충안을 적용할 수 있다면 RFID 시스템의 가장 큰 취약점인 프라이버시 침해 문제를 해결할 수 있을 것이며, RFID 시스템의 사용을 대중화할 수 있는 발판이 될 것이다.

참 고 문 헌

[1] D. Henrici and P. Muller. Hash-based Enhancement of Location Privacy for Radio-Frequency Identication Devices using Varying Identiers. In PERSEC'04, pp. 149-153, 2004.

[2] I. Vajda and L. Buttyan. Lightweight Authentication Protocols for Low-Cost RFID tags. In UBICOMP'03, 2003.

[3] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-cost RFID Tags," OTM Federated Conferences and Workshop: IS Workshop, 2006.

[4] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags," Workshop on RFID Security, 2006.

[5] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags," International Conference on Ubiquitous Intelligence and Computing-UIC'06, 2006.

[6] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," In Security in Pervasive Comp, pp. 201-212, 2004.

[7] S. Weis. "Security Parallels between People and Pervasive Devices," In PERSEC'05, pp.105-109, 2005.

강 수 영

e-mail : bbang814@sch.ac.kr

2006년 2월 순천향대학교 정보기술공학부 학사

2006년 3월~현재 순천향대학교 전산학과 석사 과정

관심분야 : RFID 보안, OTP 보안

이 임 영

e-mail : imylee@sch.ac.kr

1981년 8월 홍익대학교 전자공학과 학사

1986년 3월 오사카대학 통신공학전공 석사

1989년 3월 오사카대학 통신공학전공 박사

1989년 1월~1994년 2월 한국전자통신 연구원 선임연구원

1994년 3월~현재 순천향대학교 컴퓨터학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안