Journal of Korea Multimedia Society Vol. 10, No. 5, May 2007(pp. 623-630)

난수를 이용하여 동기화를 제공하는 RFID 프라이버시 보호 기법에 관한 연구

강수영[†], 이임영[††]

요 약

IT 기술의 발전으로 사용자 편의성 요구에 따라 빠른 속도로 유비쿼터스(Ubiquitous) 환경이 조성되고 있다. 유비쿼터스 환경에서는 서비스 제공을 위한 개개인 식별이 중요하기 때문에 RFID(Radio Frequency IDentification) 기술을 핵심적으로 사용하고 있다. RFID란 무선 주파수 인식 기술로 리더의 신호에 의하여 태그가 저장하고 있는 정보를 제공하여 사용자를 식별할 수 있는 기술이다. 높은 인식률과 빠른 인식 속도 등 많은 장점을 가지고 있지만 무선 통신으로 인하여 불법적인 사용자로부터의 도청이 가능하며, 리더의 신호에 의하여 태그가 쉽게 동작하기 때문에 사용자 정보 노출에 대한 문제가 발생하고 있다. 이를 해결하기 위하여 많은 연구가 진행되고 있지만 저가의 수동형 태그에 적용할 수 있는 보안에는 한계가 있기 때문에 일반적으로 해쉬 함수 및 난수를 이용하며, 한 세션에 사용된 값들을 갱신하여 다음 세션에 사용함으로써 보안을 제공하고 있다. 따라서 본 방식은 난수를 이용하여 사용자 프라이버시를 보호하고 값을 갱신하지 않고 가변적인 값을 생성함으로써 동기화를 제공할 수 있도록 하였다.

A Study on Privacy Protect Scheme of RFID Provide Synchronization using Random Number

Soo-Young Kang[†], Im-Yeong Lee[††]

ABSTRACT

With the development in IT technology and with growing demands of users, a ubiquitous environment is being made. Because of individuals identification is important in ubiquitous environment, RFID technology used frequently. RFID, a technology that radio frequency identification, reader send signer, then tag provide user information. RFID has various strengths, such as high recognition rates, quick recognition speed, but Eavesdropping is possible and problem that user information is revealed happens. To solve this, study is proceeded with activity, but, because of low-cost passive tag is limited operation capability, usually used hash function and random number. Also updates value that is used to present session and uses in next session. Therefore, this scheme protects user privacy using random number. And this sheme can offer synchronization by creating variable value without updating value.

Key words: RFID(RFID), Random Number(난수), Synchronization(동기화), Privacy Protect(프라이버시 보호)

1. 서 론

IT 기술의 발전으로 사용자 편의성 요구에 따라 빠른 속도로 유비쿼터스(Ubiquitous) 환경이 조성되고 있다. 유비쿼터스 환경에서는 편재되어 있으며 통신 가능한 디바이스를 요구하게 되고 유비쿼터스

※ 교신저자(Corresponding Author) : 강수영, 주소 : 충남 아산시 신창면 읍내리 순천향대학교(608-743), 전화 : 041) 542-8819, FAX : 041)530-1548,
E-mail : bbang814@sch. ac.kr

접수일 : 2006년 10월 27일, 완료일 : 2007년 3월 23일
[†] 학생회원, 순천향대학교 전산학과
[††] 종신회원, 순천향대학교 컴퓨터학부
(E-mail : imylee@sch.ac.kr)

컴퓨팅의 차세대 핵심 요소로서 무선 주파수 식별 기술 RFID(Radion Frequency IDentification)가 큰 관심을 모으고 있다. RFID 수동형 태그는 동일 표준을 사용하는 리더에게 전원을 공급받아 태그에 저장되어 있는 정보를 제공하게 된다. 일반 사용자가 태그를 부착한 물건을 소지할 경우 리더의 신호에 의해 쉽게 태그가 동작하기 때문에 물건의 정보가 악의적인 제 3자에게 쉽게 노출된다는 문제점이 발생하고 있다. RFID 사용자 프라이버시 침해 문제를 해결하기 위하여 인증 받지 못한 리더가 악의적인 목적으로 태그의 정보를 얻고자 할 경우 태그는 이에 응답하지 않아야 하며 정당한 리더가 태그의 정보를 요청할 경우 위조 및 변조되지 않은 정확한 정보를 제공할 수 있도록 해야 한다. 또한 태그가 응답 값을 전송할 때 가변적인 값을 전송함으로써 사용자의 익명성을 제공할 수 있어야 하며 위치 추적으로부터 안전하도록 할 수 있는 방안에 대하여 연구를 진행해야 한다[1,2,3].

본 논문에서는 난수와 타임스탬프를 이용하여 사용자의 프라이버시를 보호 방안에 대하여 제안한다. 일반적인 RFID 환경을 기반으로 연구되었으며 리더로부터 전원을 공급받는 수동형 태그를 사용하기 때문에 임의의 수를 생성하는 의사난수생성기(R.N.G : Random Number Generator)와 타임스탬프를 생성할 수 있는 타이머가 리더에 탑재되어 있다.

기존의 방식들을 기반으로 하여 본 방식을 제안하였으며 2장에서는 RFID 시스템에서의 발생할 수 있는 보안 위협과 요구 사항에 대하여 제시하고 3장에서는 기존 RFID 보안에 관한 연구에 대하여 알아보며, 4장에서는 앞의 내용을 토대로 설계된 제안 방식에 대하여 서술한다. 5장에서는 2장에서 도출한 보안 요구 사항에 따라 제안 방식을 분석하고 마지막으로 6장에서는 결론 및 향후 연구 방향에 대하여 서술하여 본 방식의 방향을 끝으로 마치도록 한다.

2. 보안 위협 및 보안 요구 사항

RFID 시스템은 태그, 리더, 데이터베이스로 나눌 수 있다. 세 객체가 통신하는 과정이 올바르게 이루어지기 위해서는 데이터 전송에 있어서 위조 및 변조를 막아 데이터가 안전하게 전송되어야 한다. 따라서 본 장에서는 이러한 RFID 시스템에서 발생할 수 있는 보안 위협들과 이를 보완하기 위하여 제공되어야 할 보안 요구 사항에 대하여 기술한다.

2.1 보안 위협

무선 주파수 통신을 하는 RFID는 무선 채널을 이용하기 때문에 많은 공격에 취약할 수 있다. 따라서 RFID에서 발생할 수 있는 공격 유형을 알고 이에 대응할 수 있는 방안에 대하여 강구해야 한다. 다음은 RFID시스템에서 발생할 수 있는 보안 위협이다.

◈ 도청(Eavesdropping) : 태그와 리더 간의 통신 채널에서 전송되는 데이터를 불법적인 사용자에게 노출할 수 있기 때문에 도청에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 중요 값을 유추할 수 없도록 해야 한다.

◈ 트래픽 분석(Traffic Analysis) : 도청으로 획득한 정보를 조합하여 다음 세션의 값을 추측하거나 중요 값을 획득할 수 없어야 한다. 매 세션에 전송되는 데이터들의 트래픽이 일정하지 않도록 해야 한다.

◈ 재전송공격(Replay Attack) : 도청으로 획득한 데이터를 다시 전송하여 획득하고자 하는 값을 유추하거나 획득할 수 없어야 한다.

◈ 위치 추적(Tracking Attack) : 태그에서 매 세션 고정된 값이 노출될 경우 사용자의 정확한 위치는 모르더라도 추적이 가능하여 프라이버시를 침해할 수 있다.

2.2 보안 요구 사항

앞에 기술된 보안 위협 사항들을 해결하기 위하여 다음은 RFID에서 제공되어야 할 보안 요구 사항에 관하여 기술한다.

◈ 인증(Authentication) : 시스템에 속하여 통신하는 각 객체들은 다른 객체들로부터 정당성을 검증받아야 한다. RFID 시스템은 태그, 리더, 데이터베이스로 구성되어 있으며 일반적으로 각 개체들 간에 상호 인증이 제공되어야 한다.

◈ 익명성(Anonymity) : 태그에서 노출된 정보를 획득하더라도 어떠한 태그로부터 전송된 값인지 알 수 없어야 하며 추측 불가능해야 한다. 고정된 식별 값을 사용할 경우 익명성을 제공할 수 없으므로 중요 값을 쉽게 노출시키지 말아야 하며 가변적인 값을 사용함으로써 고정되지 않은 값을 전송해야 한다.

◈ 무결성(Integrity) : 전송되는 데이터들은 무선 채널에서 전송되기 때문에 불법적인 사용자에 의하여 위조 및 변조될 가능성을 가지고 있다. 이를 해결하기 위하여 전송되는 데이터가 전송 도중에 위조 및 변조되지 못하도록 연산 및 암호화를 함으로써 데이터의 무결성을 제공해야 한다.

◈ 기밀성(Confidentiality) : 보안 프로토콜에서 사용되는 값들 중 노출되지 않아야 할 값들은 정당한 객체들만이 공유해야 한다. 통신에 사용되는 비밀 값이나 태그의 ID는 정당한 객체들만이 공유해야 한다.

◈ 효율성(Efficiency) : 수동형 태그는 연산 능력이 미비하므로 암호화하는데 있어서 경량화 되도록 해야 한다.

앞서 기술한 보안 위협에 대응할 수 있는 방안에 대하여 논의되어야 하며 이를 해결하고 보안 요구사항들을 만족할 수 있는 프라이버시 보호 기법을 제안해야 한다.

3. 기존 연구 동향

RFID에서 프라이버시를 보호하기 위해서 기존에 많은 보안 프로토콜이 제안되어 왔다[4,5]. 초기 RFID 보안 기술로써 2003년 MIT에서 제안된 Hash-Lock 기법을 기반으로 하여 RFID 보안에 관한 연구는 더욱 활발하게 진행되고 있다. 본 장에서는 임의의 난수를 생성하여 사용자 프라이버시를 보호하는 기존 기법들에 관하여 분석하고 취약점을 도출하여 이를 해결할 수 있는 방안을 논의한다.

3.1 Randomized Hash-Lock 기법

본 방식은 MIT에서 저가의 태그에서 구현 가능하도록 제안된 Hash-Lock 기법의 식별 값 metaID가 고정되어 있기 때문에 발생하는 위치 추적을 해결하기 위하여 제안된 방식이다[6]. Hash-Lock 기법에서는 키 값을 해쉬한 metaID가 고정되어 있기 때문에 이를 해결하는 방식으로 리더의 질의에 대해 태그는 난수를 생성하여 태그의 식별 값과 연접 후 해쉬한 값을 전송함으로써 보안을 제공하며 갱신 값이 없어서 동기화 문제가 발생하지 않는다. 하지만 수동형 태그에서 의사난수생성기를 탑재해야하기 때문에 효율성이 다소 미흡하다.

3.2 Hash-Based ID Variation 기법

본 방식은 태그의 식별 값을 다양하게 사용하며 가변 ID를 생성하여 사용자 프라이버시를 보호하는 기법이다[7,8]. 난수가 데이터베이스에서 생성되어 효율성을 제공하지만 마지막 세션이 비정상적으로 종료되었을 경우 같은 H(ID)가 노출되므로 위치 추적이 가능하며 비동기화 문제가 발생한다는 문제점을 가지고 있다.

3.3 Low-Cost Authentication 기법

본 방식은 앞서 기술된 Hash-based ID Variation 기법을 기반으로 취약점을 개선하여 제안된 방식이다[9]. Hash-based ID Variation 기법에 비하여 연산이 간단해 졌으며 반으로 나누어 인증 받는 방법이 기존 연구들과 차별화 된 특징이다. 하지만 마지막 통신이 비정상적으로 종료되었을 경우 동일한 난수로 재전송공격을 시도하면 같은 R 값이 생성되어 위치 추적이 가능하며 갱신 값으로 인한 비동기화 문제가 발생한다는 문제점이 발생된다.

3.4 Mutual Authentication 기법

본 방식은 기존 방식들과는 차별화 된 환경에서 제안된 방식이다[3]. 일반적으로 태그와 리더 간의 통신 채널이 무선으로 연결되어 있어 불안전하다고 보는 반면 이 방식에서는 리더와 데이터베이스 간의 통신 채널도 무선 통신 채널로 구성된 환경을 기반으로 제안되었다. 보안 강화를 위한 여러 가지 키 갱신과 식별 값 갱신 과정이 추가되어 효율성은 미흡하지만 각 객체들 간의 인증으로 인하여 무선 네트워크에서의 활용에 있어서는 많은 장점을 갖는다. 하지만 마지막 세션이 비정상적으로 종료되었을 경우 키 값과 ID 값이 갱신되지 않기 때문에 위치 추적 문제가 발생하고 키 값과 ID의 갱신에 대한 비동기화가 발생할 수 있다.

4. 제안 방식

기존 방식들을 살펴보면 사용자 프라이버시 침해 문제를 해결하기 위하여 난수를 이용하여 위치 추적으로부터 안전하게 하고 사용되는 값을 갱신시킴으로써 보안을 제공하고 있다. 하지만 무선 채널에서

데이터가 전송되기 때문에 각 객체들 간의 비동기화 문제가 발생했을 경우 정당한 사용자라 할지라도 인증에 실패할 수 있다. 따라서 본 방식은 난수를 사용하여 사용자를 위치 추적으로부터 안전하고 타임스탬프를 이용하여 재전송공격으로부터 안전하게 하였다. 또한 값을 갱신시키지 않고 난수와 타임스탬프를 이용하여 가변적인 값을 생성하기 때문에 비동기화를 해결할 수 있는 방식이다.

4.1 가정 사항

제안 프로토콜은 다음과 같은 가정 사항을 제시한다.

◈ RFID 프라이버시 보호 제안 기법 1에서 태그와 리더 간의 통신 채널은 무선 통신을 이용하므로 불안전한 채널로 구축되어 있으며 리더와 데이터베이스 간의 통신 채널은 SSL/TLS와 같은 안전한 통신 채널이다.

◈ RFID 프라이버시 보호 제안 기법 2에서 태그와 리더 간의 통신 채널뿐만 아니라 데이터베이스와 리더 간의 통신 채널도 불안전한 통신 채널이다.

◈ 리더는 의사난수생성기를 탑재하고 있으며 매 세션 다른 난수를 생성한다.

◈ S_V 값들은 비밀 값으로 정당한 객체들 간에 안전한 채널에서 공유한다.

4.2 시스템 계수

본 제안 방식에서는 다음과 같은 시스템 계수를 이용한다.

◈ ID : 태그의 고유 식별 값으로 갱신되지 않는 고유한 값

◈ $metaID$: 태그의 식별 값을 해쉬한 값으로 $H(ID)$ 값

◈ S_V : Secret Value로 정당한 객체(태그, 리더, 데이터베이스)만이 사전에 공유한 값

◈ r : 리더에서 생성한 난수 값

◈ TS : 리더에서 생성한 타임스탬프 값

◈ $\triangle r$: 난수 r과 타임스탬프 TS의 차 연산한 값

◈ V_1 : Variable Value 1로 $r \oplus S\_V$ 값

◈ V_2 : Variable Value 2로 $TS \oplus S\_V$ 값

◈ V_3 : Variable Value 3으로 $\triangle r \oplus metaID$ 값

◈ H_1 : Hash Value 1로 $H(r \| TS)$ 값

◈ H_2 : Hash Value 2로 $H(r \| metaID)$ 값

◈ H_3 : Hash Value 3으로 $H(ID \| S\_V \| TS)$ 값

◈ E_1 : 암호화된 값으로 $E_{s\_v}[r \| TS \| metaID]$ 값

◈ E_2 : 암호화된 값으로 $E_{s\_v}[r \| TS \| ID]$ 값

◈ $E_{s\_v}[\ ]$: 대칭키 암호 알고리즘을 사용하여 S_V로 암호화

4.3 RFID 프라이버시 보호 제안 기법

태그에서 고정된 값이 노출될 경우 사용자 위치 추적되므로 프라이버시가 침해 문제가 발생 하였다. 이를 해결하기 위하여 난수와 타임스탬프를 사용하여 태그의 노출 값을 가변하게 생성함으로써 프라이버시를 보호한다. 또한 기존의 방식들은 가변적인 값을 생성하기 위하여 난수를 사용하였으나 동일한 난수 발생 시 값이 고정되므로 위치 추적이 가능하므로 값들을 갱신하여 보안을 제공하려 하였다. 하지만 불안전한 채널에서 데이터 전송을 하기 때문에 전송도중 위조 및 변조 될 경우 정당한 태그라도 다음 세션에서 인증 받지 못하는 비동기화 문제가 발생할 수 있다. 따라서 본 방식은 난수와 타임스탬프를 사용하여 사용자 프라이버시를 보호하고 태그의 ID나 비밀 값을 갱신하지 않고 가변적인 값을 생성함으로써 비동기화를 해결할 수 있다. 난수를 사용한 기존 방식들에 비하여 효율성은 덜 제공하지만 훨씬 안전하고, 동기화를 제공함으로써 정당한 태그에 대한 인증이 모두 제공된다.

가. RFID 프라이버시 보호 제안 기법 1

본 제안 방식은 태그와 리더 간의 무선 주파수 통신으로 불안전한 통신 채널을 사용한다. 태그와 데이터베이스 간의 상호 인증을 제공하며 값을 갱신시키지 않고 난수와 타임스탬프를 이용하기 때문에 동기화 문제가 발생하지 않는 사용자 프라이버시 보호 기법이다.

단계 1. 리더는 통신을 시작하기위하여 R.N.G (Random Number Generation)에서 난수 r를 생성하고 타이머에서 통신 시작 시간인 타임스탬프 TS를 생성한다. 사전에 공유한 비밀 값 S_V에 r과 TS를 각각 XOR 연산하여 V_1과 V_2를 생성하고, 무결성 검증을 위한 해쉬 값H_1을 생성한다. 리더는 생성한 V_1과 V_2, H_1을 태그에게 전송한다.

$$V_1 = r \oplus S\_V$$
$$V_2 = TS \oplus S\_V$$
$$H_1 = H(r \| TS)$$

단계 2. 태그는 전송받은 V_1과 V_2에 사전에 공유한 S_V를 XOR 연산하여 r과 TS를 획득하고, r과 TS을 해쉬하여 $H(r \| TS)'$를 생성한다. 전송된 H_1과 $H(r \| TS)'$를 비교하여 일치할 경우 r과 TS가 전송되는 도중 위조 및 변조되지 않았다는 것을 검증한다. 검증이 되었을 경우 r과 TS의 차 값인 $\triangle r$과 $H(ID)$인 $metaID$를 XOR 연산하여 V_3를 생성하고 r과 $metaID$의 무결성을 검증하기 위한 해쉬 값 H_2를 생성하여 리더에게 전송한다.

$$V_1 \oplus S\_V = r$$
$$V_2 \oplus S\_V = TS$$
$$H_1 = ?H(r \| TS)'$$
$$V_3 = \triangle r \oplus metaID$$
$$H_2 = H(r \| metaID)$$

단계 3. 리더는 태그로부터 전송된 값 $V_3 \| H_2$에 통신 시작 시 생성한 r과 TS를 연접하여 데이터베이스에 전송한다.

단계 4. 데이터베이스는 전송받은 r과 TS의 차 값인 $\triangle r$을 생성하여 V_3에 XOR 연산하여 $metaID'$를 획득한다. r과 $metaID$가 전송되는 도중 위조 및 변조되지 않았는지를 확인하기 위하여 해쉬 값 $H(r \| metaID)$를 생성하여 전송된 H_2와 비교한다. 두 값이 일치하면 r과 $metaID$의 무결성을 확인하고, 획득한 $metaID'$가 데이터베이스에 저장되어 있는지 확인한다. 동일한 값이 있을 경우 태그를 인증하고 $metaID$에 해당하는 ID를 획득한다. 데이터베이스는 획득한 ID와 S_V, TS를 해쉬하여 H_3를 생성하여 리더에게 전송한다.

$$V_3 \oplus \triangle r' = metaID'$$
$$metaID = ?metaID'$$
$$H_3 = H(TS \| S\_V \| ID)$$

단계 5. 리더는 전송받은 H_3를 태그에게 전송하고 태그는 통신 시작 시 리더로부터 전송받은 TS와 S_V, 고유한 ID를 해쉬하여 $H(TS \| S_V \| ID)'$를 생성한다. 태그는 전송받은 H_3와 $H(TS \| S_V \| ID)'$을 비교하여 동일할 경우 데이터베이스를 인증하여 상호 인증이 완료된다.

$$H_3 = ?H(TS \| S\_V \| ID)'$$

나. RFID 프라이버시 보호 제안 기법 2

본 제안 방식은 모바일 환경에서 적용 가능한 방식으로 리더가 고정되어 있지 않은 환경을 고려하였다. 본 방식은 리더와 데이터베이스 간의 채널이 불안전한 채널일 경우 암호화 알고리즘을 사용하여 데이터의 위조 및 변조를 막고 각 객체 간의 인증을 제공하는 방식이다. 난수와 타임스탬프를 이용하여 프라이버시를 보호하며 비동기화에 안전한 방식이다. 단계 1과 단계 2, 단계 6은 RFID 프라이버시 보호 제안 기법 1과 동일하다.

단계 3. 리더는 r과 TS의 차 값 $\triangle r$을 생성하여 V_3에 XOR 연산하여 $metaID$를 획득한다. r과 획득한 $metaID$를 해쉬하여 $H(r \| metaID)'$를 생성하고 전송된 H_2와 비교하여 동일할 경우 r과 $metaID$의 무결성을 검증하고 태그를 인증한다. 리더는 r과 TS, 획득한 $metaID$를 S_V로 암호화하여 E_1을 생성하고 r과 TS와 함께 데이터베이스로 전송한다.

$$V_3 \oplus \triangle r = metaID$$

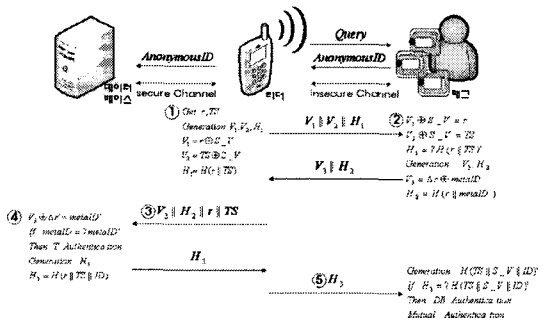

그림 1. RFID 프라이버시 보호 제안 기법 1

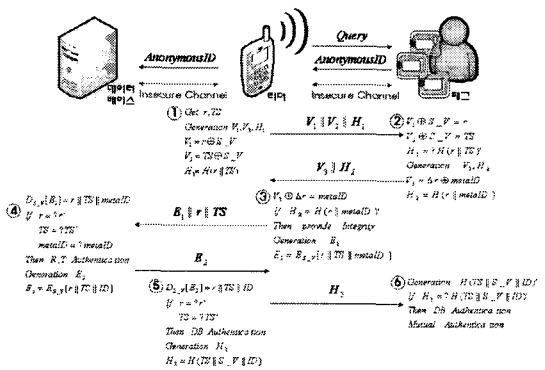

그림 2. RFID 프라이버시 보호 제안 기법 2

$$H_2 = ?H(r \| metaID)'$$
$$E_1 = E_{S\_V}[r \| TS \| metaID]$$

단계 4. 데이터베이스는 비밀 값 S_V로 E_1을 복호하여 r', TS', $metaID'$를 획득한다. 리더로부터 전송된 r과 r'를 비교하고, TS와 TS'를 비교하여 데이터의 무결성을 검증하고 올바르게 복호가 되었기 때문에 리더를 인증하고 저장하고 있는 $metaID$ 중 획득한 $metaID'$가 있을 경우 태그를 인증한다. 데이터베이스는 $metaID$에 해당하는 ID를 획득하고 r, TS, ID를 해쉬하여 E_2를 생성하여 리더에게 전송한다.

$$D_{S\_V}[E_1] = r \| TS \| metaID$$
$$r = ?r', \quad TS = ?TS'$$
$$E_2 = E_{S\_V}[r \| TS \| ID]$$

단계 5. 리더는 전송받은 E_2를 복호하여 r, TS, 태그의 ID를 획득하고 올바른 r과 TS가 전송되었을 경우 무결성을 확인하고 S_V를 통하여 데이터베이스를 인증한다. 인증이 되었을 경우 TS와 S_V, 획득한 태그 ID를 해쉬하여 생성한 H_3를 태그에게 전송한다.

$$D_{S\_V}[E_2] = r \| TS \| ID$$
$$r = ?r', \quad TS = ?TS'$$
$$H_3 = H(TS \| S\_V \| ID)$$

5. 제안 방식의 고찰

제안 방식의 분석은 2장에서 언급한 RFID의 보안 위협과 요구 사항에 따라 분류하여 분석한다. 본 방식은 각각의 보안 위협을 막을 수 있으며 요구 사항을 최대한 만족할 수 있도록 제안 되었으며 이를 분석한다.

5.1 보안 위협에 따른 안전성

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

◈ 도청(Eavesdropping) : 태그와 리더는 무선 주파수 통신을 하기 때문에 불안전한 통신 채널로 악의적인 제 3자에 의한 도청이 가능하다. 도청은 가능하지만 비밀 값과의 XOR 연산을 수행하여 중요 값이 노출되지 않게 해야 하며 도청된 데이터를 이용하여 다른 값을 추출할 수 없도록 해야 한다.

◈ 트래픽 분석(Traffic Analysis) : 도청된 데이터를 매 세션 수집하여 다른 값을 추출해 내거나 중요 값을 추측해내는 공격 유형으로 본 제안 방식에서는 사전에 공유한 비밀 값에 의존되어 있기 때문에 비밀 값을 모르는 악의적인 제 3자는 도청된 데이터들의 트래픽을 분석한다 할지라도 획득하고자 하는 값을 획득할 수 없다. 하지만 비밀 값이 노출되었을 경우 모든 값이 노출될 수 있다는 문제점을 가지고 있다.

◈ 재전송공격(Replay Attack) : 난수와 타임스탬프가 매 세션 다른 값이 생성되므로 도청한 데이터를 재전송한다 할지라도 고정된 값이 출력되지 않으며, 재전송공격으로부터 안전하기 위하여 난수와 타임스탬프의 차 값인 Δr 값을 사용하므로 재전송공격에 더욱 안전하다.

◈ 위치 추적(Tracking Attack) : 태그가 노출하는 값이 고정되어 있는 경우 태그를 소지하고 있는 사용자나 태그가 부착되어 있는 물품의 위치 추적이 가능하다. 본 방식에서는 난수를 사용하여 가변적인 값을 생성하며 통신 시작 시간인 타임스탬프를 이진 데이터로 생성하기 때문에 매 통신 시 가변적인 값을 생성하여 위치 추적의 문제를 해결한다.

5.2 보안 요구 사항 만족에 따른 안전성

본 장에서는 2장에서 기술한 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.

◈ 인증(Authentication) : 제안 기법 1에서는 데이터베이스가 r과 TS의 차를 XOR 연산하여 $metaID'$를 획득하여 저장하고 있는 $metaID$ 중 동일한 값이 있으면 태그를 인증한다. 태그는 TS와 S_V, ID를 해쉬한 값과 H_3을 비교하여 동일할 경우 데이터베이스를 인증하여 상호 인증을 제공한다. 제안 기법 2에서는 데이터베이스가 E_1에서 획득한 $metaID'$와 동일한 $metaID$가 저장되어 있을 경우 태그를 인증하고 올바른 r과 TS를 통하여 S_V를 검증하고 리더를 인증한다. 리더는 E_2를 복호하여 올바른 난수와 타임스탬프를 획득하면 S_V를 기반으로 데이터베이스와 태그를 인증한다. 태그는 TS와 S_V, ID를 해쉬하여 H_3와

표 1. 보안 위협 및 보안 요구 사항에 따른 비교표

	Randomized-Hash Lock 기법	Hash-based ID Variation 기법	Low-Cost 기법	Mutual Authentication 기법	RFID 프라이버시 보호 제안 기법 1	RFID 프라이버시 보호 제안 기법 2
도청	가능	가능	가능	가능	가능	가능
트래픽 분석	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	불가능	불가능
재전송 공격	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	불가능	불가능
위치 추적	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	비정상적 종료시 가능	불가능	불가능
인증	상호인증 제공	상호인증 제공	상호인증 제공	상호인증 제공	상호인증 제공	상호인증 제공
익명성	비정상적 종료시 제공 못함	비정상적 종료시 제공 못함	비정상적 종료시 제공 못함	비정상적 종료시 제공 못함	제공	제공
무결성	제공	제공	제공	제공	제공	제공
기밀성	제공	제공	제공	제공	제공	제공
효율성	미흡	제공	제공	제공	미흡	미흡
비동기화	발생	발생	발생	발생	발생 안함	발생 안함

동일한 값이 생성될 경우 S_V에 기반하여 리더를 인증하고 올바른 ID로 데이터베이스를 인증한다.

◈ 익명성(Anonymity) : 태그에서 노출되는 $meta\ ID$에 난수와 타임스탬프의 차 값인 Δr을 XOR 연산하여 어떤 태그의 $metaID$인지 모르게 하였다. 또한 XOR 연산만으로 위조될 수 있기 때문에 $metaID$와 ID의 해쉬 값을 사용하여 익명성을 제공한다.

◈ 무결성(Integrity) : RFID 태그는 보안을 제공해야 하지만 연산 능력이 제한되어 있기 때문에 해쉬 함수를 사용하여 보안을 제공하고 있다. MD5나 SHA-1과 같은 해쉬 함수를 사용함으로써 전송되는 데이터가 전송 도중 위조 및 변조되지 않았다는 것을 증명할 수 있다.

◈ 기밀성(Confidentiality) : 사전에 정당한 객체들만이 비밀 값 S_V를 공유하고 있으며 데이터 전송에 있어서 비밀 값과의 XOR 연산을 통하여 정당성을 검증받을 수 있다. 또한 태그의 식별 값 ID와 $metaID$ 및 중요 값도 정당한 객체만이 공유하고 있기 때문에 기밀성을 제공한다.

◈ 효율성(Efficiency) : 본 방식은 해쉬 함수를 3회 사용하고 있어 저가의 수동형 태그에서 현재 구현하는 데에는 어려움이 있으며 리더는 R.N.G 이외에 타이머를 탑재하고 암호화 알고리즘을 수행해야 하므로 효율적인 측면을 더욱 보완해야 할 것이다.

6. 결 론

유비쿼터스 환경이 조성됨에 따라 핵심 기술로 RFID가 큰 비중을 차지하고 있다. 그러나 리더의 전원 공급에 의하여 쉽게 동작하여 태그의 정보 및 사용자의 정보를 쉽게 노출하여 사용자의 프라이버시 침해 문제가 발생되고 있다. 이 문제를 해결하기 위하여 리더에서 난수와의 연산으로 가변적인 값을 생성하여 사용함으로써 프라이버시를 보호하는 방식이 연구되고 있다. 기존의 난수를 사용하는 방식은 동일한 난수 값이 발생되었을 경우 재전송공격이 가능하기 때문에 값들을 갱신하여 사용하고 있다. 하지만 본 방식은 난수와 타임스탬프를 사용하여 매 세션 값을 다른 값으로 재전송공격에 안전한 방식이다. 또한 값을 갱신하지 않기 때문에 불안전한 채널에서의 비동기화를 해결할 수 있는 안전한 방식이다. 동기화가 제공되지 못했을 경우 정당한 사용자라 할지라도 인증을 받지 못하는 경우가 발생하기 때문에 동기화 제공이 중요하다. 또한 태그에서는 값을 갱신하는 과정이 필요 없으므로 계산적인 효율을 제공할 수 있다. 하지만 저가의 수동형 태그는 250~3K 게이트 정도를 수용하고 있으며 이 중 150 게이트 정도만 보안을 적용하는데 사용할 수 있기 때문에 연산 능력에 대한 문제가 발생하고 있다. 본 방식 또한 해쉬

연산을 3회 사용하고 있기 때문에 구현을 하는데 있어서 경량화에 대한 과제를 해결해야 할 것이다. 효율성 문제를 해결한다면 유비쿼터스 환경에서 사용자 프라이버시를 보호하며 안전하게 RFID를 사용할 수 있을 것이다.

참 고 문 헌

[1] A. Juels, Revest and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Conference on Computer and Communications Security-ACM CCS*, pp. 103-111, Oct. 2003.

[2] D. Henrici and P. Mullerm, "Hash-Based Enhancement of Location Privacy For Radio-Frequency Identification Devices Using Varying Identifiers," *Workshop on Pervasive Computing and Communications Security-PerSec*, pp. 219-224, Mar. 2004.

[3] Jeongkyn Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim, "Mutual Authentication Protocol for Low-Cost RFID," *Encrypt Workshop*, Jul. 2005.

[4] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic Approach to 'Privacy-Friendly' Tags," *RFID Privacy Workshop*, Nov. 2003.

[5] S. Weis, "Security and Privacy in Radio-Frequency Identification Devices," *Masters Thesis*, May 2003.

[6] S. Weis, S. Sarma, and D. Engels, "RFID systems and security and privacy implications," *Cryptographic Hardware and Embedded Systems-CHES*, pp. 454-469, Aug. 2002.

[7] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy aspects of low-cost radio frequency identification systems," *International Conference on Security in Pervasive Computing*, pp. 201-212, Mar. 2003.

[8] 유성호, 김기현, 황용호, 이필중, "상태기반 RFID 인증 프로토콜," 한국정보보호학회 논문지, 제14권, 6호, pp. 57-68, 2004.

[9] 황영주, 이수미, 이동훈, 임종인, "유비쿼터스 환경의 Low-Cost RFID 인증 프로토콜", 한국정보보호학회 하계학술대회, 제14권, 제1호, pp. 109-114, 2004.

강 수 영

2006년 2월 순천향대학교 정보기술공학부 졸업

2006년 3월~현재 순천향대학교 전산학과 석사 과정

관심분야 : RFID 보안, OTP 보안

이 임 영

1981년 8월 홍익대학교 전자공학과 졸업

1986년 3월 오사카대학 통신공학전공 석사

1989년 3월 오사카대학 통신공학전공 박사

1989년 1월~1994년 2월 한국전자통신연구원 선임연구원

1994년 3월~현재 순천향대학교 컴퓨터 학부 교수

관심분야 : 암호이론, 정보이론, 컴퓨터 보안