情報保護學會論文誌
第16卷 第2號, 2006. 4

유비쿼터스 환경을 위한 RFID 태그의 인증과 관리에 관한 연구

서 대 희,† 이 임 영‡
순천향대학교

A Study on Authentication and Management Scheme of RFID Tag for Ubiquitous Environment

Dae-Hee Seo,† Im-Yeong Lee‡
Division of Information Technology Eng. Soonchunhyang University

요 약

최근 새로운 형태의 네트워크 환경인 유비쿼터스 컴퓨팅에 대한 연구가 활발하게 진행되고 있다. 본 논문에서는 유비쿼터스 환경을 구현하기 위한 핵심적인 기술을 Ad hoc 네트워크와 스마트 태그 기술로 규정하고, 스마트 태그와 관련한 RFID 태그의 보안 서비스에 대한 연구를 수행하고자 한다. 이는 RFID 태그가 유비쿼터스 컴퓨팅과 관련된 인프라에 적용되기 위해서는 중요한 몇가지 기술적인 요소와 구조가 고려되어야 하며, RFID 태그의 보안성이 기술적인 측면의 핵심중에 하나로 규정되기 때문이다. 특히, 안전한 유비쿼터스 환경을 구현하기 위해 RF 통신을 수행하는 수동형 RFID 태그의 경우 태그 가격의 경제성을 보장하는 보안 서비스 및 이를 관리할 수 있는 기술적인 사항과 능동형 RFID 태그에 적용이 가능한 보안 서비스 및 네트워크 관리 기술이 절실히 요구되는 실정이다. 따라서 본 논문에서는 수동형 RFID 태그를 기반으로 구성된 네트워크에서 안전한 인증 후 태그 서비스에 따른 인증 레벨을 설정하여 동일한 서비스를 제공할 경우 이를 관리하는 프로토콜과 능동형 RFID 태그로 이루어진 네트워크에서 현재 위치 및 서비스 등록 과정을 수행하여 불법적인 RFID 태그에 대한 보안 서비스 뿐만 아니라 서비스를 단일 서비스와 그룹 서비스로 구분해 안전한 통신 방식을 제안하고자 한다.

ABSTRACT

This study, in particular, aims to regulate the core techniques of ubiquitous computing, such as the use of an ad hoc network and the smart-tag technique, and to look more closely into RFID Tag's smart-tag-related security service. The study aims to do so because several important technical factors and structures must be taken into account for RFID Tag to be applied in the ubiquitous-computing-related infrastructure, and the security of the tag is considered one of the core technologies. To realize secure ubiquitous computing in the case of the passive-tag-performing RF communication, a less costly security service, the technical items needed to carry this out, a security service to be applied to passive tags, and network management techniques are required. Therefore, the passive-tag-based network, as the authentication level is established based on the secure authentication of each tag and the service that the tag delivers in the passive-tag-based network, and as the same service and authentication levels are applied, and the active-tag-based network system proposed herein is not merely a security service against illegal RFID tags by performing a current-location and service registration process after the secure authentication process of the active RFID tag, but is also a secure protocol for single and group services, is proposed in this study.

Keywords : *유비쿼터스 환경, 인증, 관리, RFID 태그*

접수일: 2005년 12월 13일; 채택일: 2006년 3월 9일
† 주저자, patima@sch.ac.kr
‡ 교신저자, imylee@sch.ac.krr

Ⅰ. 서 론

인터넷 및 이동전화로 대표되는 정보통신 기술의 발전은 생활 패턴 자체를 변화 시켜 가정, 학교, 사무실을 비롯한 모든 환경에서 정보를 습득 및 서비스를 제공받는 환경으로의 변화를 가져왔다. 특히, 새로운 서비스 제공을 위해 지속적인 연구와 발전은 계속되고 있으며, 이러한 발전의 특징은 다양한 무선 통신 기술의 개발에 있다.

최근 주목받고 있는 무선 기술중 차세대 무선 통신기술로써 인정받으며, 유비쿼터스 컴퓨팅과 같은 사용자 중심의 차세대 네트워크 구조에 적용 가능한 기술이 RFID(Radio Frequency Identification)이다.

RFID는 무선 통신을 이용해 원격으로 정보를 인식하는 기술로써 기존의 오프라인에서 대표적으로 활용되고 있는 바코드 체계를 대체할 수 있어 개인 생활은 물론 산업 전반에 많은 응용 서비스가 가능하여 최근 많은 연구 개발이 이루어지고 있다[6].

기존 RFID 시스템에 대한 연구는 RF 리더기와 RFID 태그를 중심으로 이루어지는 보안 관계에 연구의 초점이 맞추어져 있다. 그러나 RFID 태그가 보편화된 서비스로 이루어질 경우 많은 보안 취약성이 발생할 수 있으며, 이를 위한 안전한 네트워크 형태의 구성과 관리에 대한 연구는 수행되지 않고 있다.

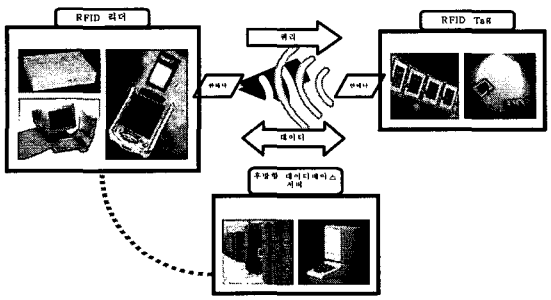


그림 1. 일반적인 RFID 시스템

따라서 본 논문의 2장에서는 일반적인 RFID 시스템의 개요에 대해 기술하고, 3장에서는 RFID 태그의 연구 방향에 대한 문제점과 기존 방식에 대한 보안 취약성을 분석하고 RFID 태그 기반의 인증 및 관리 시스템에서 만족해야 하는 보안적인 요구사항을 제시하고자 한다. 4장에서는 3장에서 제시한 보안 요구사항을 만족하는 안전하고 효율적인 RFID 태그 인증 기술과 관리 방식에 대해 제안하고, 5장에서는제안 방식을 분석한 뒤 마지막으로 6장에서는 결론을 맺도록 한다.

2. 기술 개요

RFID 시스템은 판독 및 해독 기능을 하는 RF 리더기와 정보를 제공하는 RFID 태그로 구성된 무선통신 시스템이다. RFID 태그는 사람, 자동차, 화물등에 개체를 식별하는 정보를 부가하는 시스템으로 그 부가 정보를 무선 통신 매체를 이용함으로써 기존에 오프라인으로 이루어지는 다양한 어플리케이션을 자은 일반적인 RFID 시스템의 구성도이다.

- 편리한 사용과 여러 태그를 동시에 인식
- 고속 인식이 가능하여 시간적인 효율성
- 시스템 특성이나 환경 여건에 따라 손쉬운 적용
- 비접촉식의 특성에 따른 반영구적 사용과 유지보수에 대한 경제성
- OTP(One Time Programming)로 태그를 프로그램하여 데이터 위조 및 변조에 대한 보안성
- 시스템의 확장
- 양방향 인식

3. RFID 관련 연구 분석 및 보안 요구사항

본 장에서는 RFID 시스템의 연구 방향에 대한 문제점과 기존 방식의 보안 취약성을 분석하고 수동형과 능동형 RFID 태그 기반의 인증 및 관리 시스템에서 요구되는 보안 요구사항에 대해 논하고자 한다.

3.1 RFID 연구 동향과 문제점

RFID와 관련된 연구는 주로 하드웨어적 경량화와 더불어 안전한 서비스를 위한 보안 연구가 중심을 이루고 있다. 특히, 보안과 관련된 연구는 2003년 12월에 MIT에서 개최된 RFID Privacy Workshop에서 많은 연구 결과가 발표 되었으며, RSA 연구소에서도 RFID의 중요성을 인식하고 이와 관련된 연구를 추진중에 있다. 현재의 RFID 보안에 대한 연구의 초점은 RFID 태그와 RF 리더기를 중심으로 이루어지는 인증에 그 초점이 맞추어져 있다. 따라서 안전한 인증 이후의 발생되는 문제점들에 대한 연구는 매우 미흡한 실정이다. RFID 태그의 적용

에 대한 연구는 NTT에서 제시한 해쉬 체인 방식을 이용해 인증을 수행한 뒤 단순한 비트의 확장을 통한 EPC(Electronic Product Code)로의 적용만을 수행함으로써 RFID 태그의 안전한 인증 이후의 문제점들에 대해서는 고려되지 않았다.

RFID 태그가 실제 환경에서 사용되기 위해서는 인증과 같은 보안 요구사항이 매우 중요한 요소로 고려될 수 있으나 안전한 인증 이후에 이를 어떻게 관리하는가 역시 매우 중요한 요구사항으로 제시될 수 있다.

이에 본 연구에서는 기존 연구의 연장선상에서 RFID 태그의 안전한 인증 이후 이를 관리할 수 있는 안전하고 효율적인 방식에 대한 연구의 중요성을 인식하고 이에 대한 연구를 수행하고자 한다.

3.2 RFID 시스템의 기존 연구 분석

RFID 태그와 관련된 연구는 최근 유비쿼터스 컴퓨팅과 관련하여 많은 주목을 받고 있으며, 이와 관련된 기존 연구를 해쉬 기반, 재암호화 기반, XOR 기반으로 나누어 분석하면 다음과 같다.

(가) Hash Lock Scheme : MIT에 의해 제시된 방식으로 낮은 가격을 고려한 방식이다. 각각의 개체는 해쉬 함수를 가지고 있다고 고려되며, 다음과 같은 방식으로 진행된다. 먼저 RF 리더기는 키 K를 각각의 RFID 태그에 전송하며, RFID 태그는 Meta ID를 계산한다. (Meta ID = Hash(K)) RF 리더기는 쿼리를 RFID 태그에 전송하고 RFID 태그는 이에 대한 응답 메시지로 Meta ID를 전송한다. RF 리더기는 사전 분배한 키와 Meta ID의 연계성을 고려하여 이를 검증한 뒤 검증 결과가 올바른 경우 그에 대한 응답 메시지를 RFID 태그에 전송한다. 이 방식의 경우 단지 전송 데이터에 대한 동의와 리더기가 가지고 있는 ID의 전송을 통해 인증 과정을 수행한다[1,5].

따라서 본 방식은 낮은 가격과 고정된 Meta ID를 기반으로 제안된 방식이지만 공격자가 공개된 Meta ID를 통해 RFID 태그에 대한 공격이 가능하다.

(나) Randomized Hash Lock Scheme : MIT에서 제시된 방식으로 해쉬락 방식의 확장된 형태이다. 이 방식의 경우 기존 해쉬 락 방식과는 달리 RFID 태그가 안전한 해쉬 함수와 랜덤 생성기까지 가지고 있다고 가정한다. 각각의 RFID 태그는 랜덤 수를 생성하여 이를 입력 값으로 안전한 해쉬 값을 생성한다. (r은 랜덤 수, C=H(ID||r)), RFID 태그는 C와 r을 리더기에 전송한다. RF 리더기는 전송된 데이터를 후방향 데이터 베이스에 전송한다. 데이터 베이스는 해쉬 함수를 이용해 전송된 r과 각각의 ID를 대응하여 저장한다. 데이터 베이스에서는 ID와의 연관성을 통해 C와 ID를 검증한다[1,6].

본 방식은 RFID 태그의 출력 정보가 엑세스 마다 매번 바뀌어 ID에 대한 유추가 어려운 방식이다. 그러나 이와 같은 방식의 경우 RFID 태그의 위치에 대한 추적 정보를 제공한다. 특히, RFID 태그의 비밀정보와 위치 정보가 관계된다면, 전방향성 보안 사항을 만족할 수 없다. 추가적으로 해쉬 함수는 낮은 가격의 RFID 태그에 적용될 수 있으나 의사난수 생성기와 같은 경우에는 사실적으로 구현이 불가능하다.

(다) Hash-Chain Scheme : 일본의 NTT에서 제안된 방식으로써 안전한 해쉬 함수를 이용하여 해쉬 체인을 생성한다. 해쉬 체인값을 생성하기 위한 초기 값은 RFID 태그와는 무관한 값이며, 이를 기반으로 안전한 해쉬 체인 값을 생성하여 상호 인증을 수행하는 방식이다. 본 방식의 경우 기존의 EPC(Electronic Product Code)에 확장된 방식의 EPC를 제안하였으며, PFS(Perfect Forward Secrecy)와 구분 불가능성을 만족하는 방식이다[12].

그러나 데이터 베이스 서버에 대한 정보의 분할과 더불어 기밀성 측면에서의 안전성은 고려되지 않았다. 이는 초기 데이터 전송 이후의 전송 데이터에 대한 PFS를 제공할 뿐이다. 따라서 해쉬 체인 방식의 경우 해쉬 체인을 생성하기 위한 초기 값 전송시 기밀성 서비스와 확장성 부분에서 문제성 및 고유한 ID와 비밀정보 초기값에 대한 대응 저장으로 인해 발생할 수 있는 후방향성 서버의 안전성에 문제점을 지적할 수 있다.

④ Universal Re-encryption scheme : Satio 등

에 의해서 제안한 방식으로 유니버셜(Universal) 재암호화 방식을 사용한다. 유니버셜 재암호화 방식이란, 재암호화 과정이 일어날 때 공개키 없이 임의의 랜덤값을 사용하여 재암호화가 이루어지는 방식이다. 하지만, RFID 태그의 정보에 재암호화 과정이 여러 번 일어나더라도, 단 한 번의 복호화 과정으로 원래의 메시지를 복원할 수 있다. 이 방식은 다음의 재암호화 방식에 기반하며 그 과정은 키 생성, 암호화, 복호화, 재-암호화 4단계로 이루어진다[9,15].

- 키 생성 : 데이터베이스는 비밀키 x, 공개키 y (y=gx)를 생성한다.
- 암호화 : 정당한 데이터베이스는 다음과 같이 RFID 태그의 정보(m)를 암호화하여 RFID 태그의 메모리에 안전하게 저장한다. ($C=[(\alpha_0, \beta_0);(\alpha_1,\beta_1)]$) = $[(my^{k_0}, g^{k_0});(y^{k_1}; g^{k_1})]$)
- 복호화 : 리더의 질의를 받은 RFID 태그는 자신의 암호문 C를 데이터베이스에 전송한다.

데이터베이스는 암호문 C에서 m1(m1= $\alpha_1/\beta_1^{\infty}$)을 확인하고, m1이 1이면, m0(m0= $\alpha_0/\beta_0^{\infty}$)을 메시지로 받아들인다.

- 재-암호화 : 재암호화 방식은 외부기기가 대신 수행하며, RFID 태그로부터 전송받은 암호문을 변경하여 RFID 태그에게 전송한다. RFID 태그는 데이터베이스로 저장하고 있는 one-time 랜덤값 $\Delta = \{(\alpha_1^{m_1},\beta_1^{m_1}),(\alpha_1^{m_2},\beta_1^{m_2}),.....,(\alpha_1^{m_{2n}},\beta_1^{m_{2n}})$과 자신의 암호문 C를 사용하여 다음과 같이 재암호화 값을 리더에게 전송한다.

  $C' = [(\alpha_0', \beta_0');(\alpha_1', \beta_1')] = [(\alpha_0\alpha_1^{m_1}, \beta_0\beta_1^{m_1});$
  $(\alpha_0\alpha_1^{m_2}, \beta_0\beta_1^{m_2})]$

- One-time 랜덤값 갱신 : RFID 태그는 리더로부터 받은 one-time 랜덤값에 대해 다음과 같은 갱신한다. 우선, RFID 태그와 리더는 비밀 정보 S를 공유한다. 데이터베이스는 RFID 태그에게 새로운 one-time 랜덤값 Δ'과 X를 다음과 같이 생성하여 전송한다.

  $\Delta' = \{(\alpha_1^{m_1'},\beta_1^{m_1'}),(\alpha_1^{m_2'},\beta_1^{m_2'}),\quad ...,(\alpha_1^{m_{2n}'},$
  $\beta_1^{m_{2n}'})\}$, X = h(S, I, Δ')

RFID 태그는 새로 받은 값들을 이용하여 h(S, i, Δ')를 계산하고, 이 값이 데이터베이스로부터 받은 값 X와 동일한지 비교한다. 두 값이 같으면, RFID 태그는 전송된 메시지가 공격자에 의해서 변조되지 않고, 정확하게 전송되었다고 인식하게 된다. 그래서 새로운 one-time 랜덤값 Δ'으로 기존의 랜덤값들을 갱신한다. One-time 랜덤값을 사용하는 프로토콜이다.

⑤ HB Authentication protocol(XOR based Scheme) : 최근에 Crypto 학회에 RFID 시스템의 프라이버시 보호에 대한 방식이 제안되었다. 이 방식은 Juels에 의해 제안된 방식으로 1비트로 상대방을 인증하는 방식이다[12,15]. 제안된 방식은 HB 프로토콜이라 표기하며 과정은 다음과 같다.

우선, RFID 태그와 리더 간에 비밀값 x를 공유한 상태에서 리더가 태그를 인증하게 된다. 태그가 리더에게 α 값을 전송하고 RFID 태그는 $z = a \cdot x$값을 생성하여 전송한다. 이 값을 생성하는 과정은 내적을 사용한다. 즉, z = a1 ⋯ ak * x1 ⋯ xk = a1 * x1 + ⋯ +ak * xk이다. 리더는 그 값을 받고 자신이 저장하고 있는 x값과 a값을 이용하여 생성한 a·x값을 받은 z값과 같은지를 확인한다. 1비트로 인증을 하기 때문에 r번 반복하여 정확성을 높인다. 하지만 이러한 경우에도 공격자가 a의 비트길이 k번만큼 세션을 도청할 경우 비밀값 x에 대해 알 수 있기 때문에 $\eta \in (0, \frac{1}{2})$라는 확률로 ν값을 XOR하여 전송한다. 이 과정에서는 리더는 태그로부터 받은 $z = a \cdot z \oplus \nu$값의 정확성은 r번 반복하여 그 값이 $\eta \cdot r$보다 적게 틀린 경우 정당한 태그로 받아들인다[37].

위에 제안된 방식은 수동적인 공격자에 대해서 안전할 수 있으나 공격자가 a값을 자신에 유리한 값으로 선택하여 리더에게 전송한다면 응답값 z에서 x에 대한 값을 알아 낼 수 있다. 따라서 Jules는 능동적인 공격에 안전한 HB+방식을 제안하였다. 이 방식은 리더와 RFID 태그 간에 추가적으로 y라고 하는 비밀값을 서로 저장하고 이전 방식과 달리 b라는 랜덤값을 태그가 전송하는 방식이다.

제안된 HB+방식은 능동적인 공격에 안전하게 설계하기 위해서 b라고 하는 값을 태그가 선택하여 전송하도록 하였다[37]. 그러므로 공격자가 자신에게

유리한 값 a를 생성하여 공격을 시도할지라도 b 값으로 인해 비밀값 y에 대한 정보를 얻을 수 없기 때문에 안전하다고 저자는 주장하고 있다. 그러나 제안된 방식은 1비트의 값으로 태그를 인증하는 것이기 때문에 인증하는 것이기 때문에 다수의 태그를 관리하는 환경에서는 오류 발생의 확률이 많다. 그러므로 다수의 태그의 정보를 다루는 환경에서 사용하기에는 부적합하며 이 방식은 안전성 측면에서 취약성을 갖는다[37].

표 1. 기존 RFID 인증 방식 분석

방식	ACIN	채널보안	새로운 서비스 생성 및 조회	안전한 상태획득
해쉬락 방식	AI만 만족	전방향 채널	비제공	None
향상된 해쉬락 방식	ACI 만족	전방향 채널	비제공	None
해쉬 체인 방식	ACI 만족	전방향 채널	비제공	None
재암호화 방식	ACI 만족	전방향 채널	비제공	None
XOR 방식	AI 만족	전방향 채널	비제공	None

{ACIN(Authentication, Confidentiality, Integrity, Non-repudiation)}
* None : 서비스를 제공하지 않음

3.3 RFID 태그의 인증 및 관리 프로토콜 보안 요구사항

RFID 태그의 안전하고 효율적인 인증 및 관리 프로토콜을 구성할 경우 다음과 같은 보안 요구사항을 제시할 수 있다.

- ACIN (Authentication, Confidentiality, Integrity, Non-repudiation) : 일반적인 통신로상에서 요구되는 기본적인 보안 서비스를 제공해야 한다.
- 채널 보안 : RFID 태그 인증 프로토콜은 초기 쿼리에 대한 수정 공격이나 전송 데이터와의 무결성 뿐만 아니라 안전한 통신을 위한 전방향성 채널 보안 서비스가 요구된다.
- 불법 RFID 태그에 대한 취약성 : RFID 태그를 기반으로 네트워크를 형성하였을 경우 불법 RFID 태그에 대한 접근으로부터 네트워크 보안 서비스를 제공할 수 있어야 한다.
- 그룹 보안 서비스의 확장성 : 단일한 RFID 태그에 대한 서비스만을 고려할 경우 RFID 태그의 개수가 증가함에 따라 리더기의 효율성이 저하되어 RFID 태그 기반의 네트워크 구성시 전체 네트워크 효율성을 저하 시킬 수 있는 요인이 된다. 따라서 단일한 RFID 태그 인증 서비스를 수행한다 할지라도 이를 기반으로 네트워크를 구성할 경우 효율성을 고루 갖출 수 있는 그룹 보안 서비스를 제공해야 한다.
- 구현의 효율성 : RFID 태그 인증 시스템을 구성하고자 할 경우 현재 RFID 태그의 물리적 한계성 때문에 발생할 수 있는 적용의 문제점을 해결할 수 있어야 한다. 여기에서 가장 중요한 점은 낮은 가격의 태그에 적용이 가능한지의 여부이며, 이는 하드웨어적 구성에 초점이 맞추어지게 된다.

4. 제안방식

본 논문에서는 수동형 RFID 태그와 능동형 RFID 태그로 구성된 네트워크에서 다양한 형태의 네트워크 관리 방식을 제안하고자 한다. 수동형 RFID 태그를 기반으로 구성된 네트워크에서는 안전한 인증 후 태그 서비스에 따른 인증 레벨을 설정하고 동일한 서비스를 제공할 경우 이를 관리하는 프로토콜과 능동형 RFID 태그로 이루어진 네트워크에서는 불법적인 RFID 태그에 대한 보안 서비스와 서비스 형태에 따른 관리 방식을 제안하고자 한다.

4.1 수동형 RFID 태그 기반 인증 및 관리 프로토콜 제안

수동형 RFID 태그 기반의 네트워크 구성시 각 RFID 태그의 안전한 인증 방식과 생성하는 서비스에 따라 인증 레벨을 설정하여 서비스를 구분하고 이를 관리할 수 있는 방식을 제안하고자 한다.

수동형 RFID 기반 인증 및 관리 방식은 다음과 같은 가정을 기반으로 수행된다.

① 모든 RFID 태그는 수동형 전력 공급 형태를 갖는 스마트 태그로써 초기 접속을 위한 데이터베이스의 DID(후방향 데이터베이스의 ID)를 저장한다.

② RF 리더기와 데이터베이스와는 유선으로 연결되어 있으며, 신뢰된 개체이다.

③ RFID 태그는 사전에 $C_T = H(x_T)$ 를 계산하여 RF 리더기와 후방향 데이터 베이스 서버에 이

를 안전하게 전송하고 RF 리더기와 후방향 데이터 베이스 서버는 C_T를 안전하게 저장한다.

가. 시스템 계수

다음은 본 제안 방식에서 사용되는 시스템 계수이다.

* (후방향 데이터베이스 : D, RF 리더기 : R, RFID 태그 : $T(T_1, T_2, ..., T_n)$)

DID, RID : 데이터 베이스, RF 리더기의 ID

TID_T : RFID 태그의 ID

r_* : *에서 생성된 의사난수

H() : 안전한 해쉬 함수

Cnt_i : RFID 태그 기반의 네트워크를 구성하는 개체가 공유하는 동기화된 카운터 정보로써 후방향 데이터베이스에 의해 동기화 된다. (i=1,2,3,....,n)

x_T : RFID 태그의 초기 정보 (태그의 물리적 주소, 생성시간 등이 포함된 정보)

$F()$: RF 리더기와 후방향 데이터베이스에서 공유하고 있는 랜덤 함수

M : 서비스 메시지

T_* : 타임 스탬프

AL_j^i (Authentication Level) : 인증 레벨 (j는 태그 번호, i는 인증 레벨)

나. 제안방식 프로토콜

수동형 RFID 태그 기반의 안전한 인증과 네트워크 관리 프로토콜은 다음과 같은 과정으로 수행된다.

1) 초기 인증 프로토콜

통신을 요구하는 모든 RFID 태그와 통신을 수행하는 과정으로 RFID 태그 1과의 통신은 다음과 같다.

① RF 리더기는 RFID 태그 1에 통신 Query를 전송한다.

② RFID 태그 1은 DID와 C_{T_1}을 RF 리더기에 전송한다.

③ RF 리더기는 랜덤 수 r_R을 생성하여 RID, C_R, r_R을 후방향 데이터베이스에 전송하고 C_R을 전송하고 C_{T_1}의 대응 테이블에 C_R을 저장한다.

$$C_R = r_R \oplus C_{T_1}$$

④ 후방향 데이터베이스는 랜덤수 r_D를 생성하고 이를 기반으로 후방향 데이터베이스와 RF 리더기의 랜덤수 확인을 위한 L을 다음과 같이 계산한 후 RFID 태그 1로부터 사전에 등록된 C_{T_1}을 이용해 C_D를 생성하며, r_R과 r_D는 C_{T_1}의 일대일 대응 테이블로 저장한다.

$$L = H(r_R \| r_D)$$
$$C_D = r_R \oplus r_D \oplus C_{T_1}$$

후방향 데이터베이스는 L과 C_D를 RF 리더기에 전송한다.

⑤ RF 리더기는 데이터 베이스로부터 전송된 (L, C_D)에서 ③ 과정에서 저장된 C_R을 이용해 r_D를 추출하고 β_1, α_1을 계산하여 β_1, α_1, C_R을 RFID 태그 1에 전송한다. 전송 후 β_1, α_1, L을 일대일 대응 테이블로 저장한다.

$$\beta_1 = H(r_R \| Cnt_1) \ , \ \alpha_1 = F(L \| Cnt_1)$$

⑥ RFID 태그 1은 β_1, α_1, C_R을 수신한 뒤 C_R을 기반으로 β_1을 검증하고 올바른 경우 α_1을 임시 저장한 뒤 이벤트 종결 메시지와 Z_1을 계산하여 RF 리더기에 전송하고 이를 대응 테이블에 저장한다.

$$Z_1 = TID_{T_1} \oplus \beta_1$$

⑦ RF 리더기는 Z_1에서 TID_{T_1}을 추출하여 후방향 데이터베이스에 TID_{T_1}, Cnt_1을 전송하고 후방향 데이터베이스는 Cnt_1을 TID_{T_1}과 일대일 대응 테이블로 저장한다. (그림 2 참조)

2) 서비스 생성에 따른 인증 레벨 프로토콜

서비스 생성에 따른 인증 레벨 프로토콜은 초기화 프로토콜을 진행한 뒤 RFID 태그 정보에 대한 인증 레벨을 설정하는 과정이다. (RFID 태그 1과의 설정과정)

① RF 리더기는 RFID 태그 1에 Query를 전송한다.

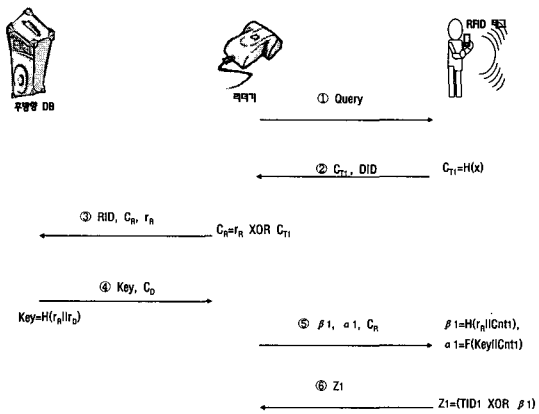


그림 2. 초기화 프로토콜

② RFID 태그 1은 Z_1과 서비스 생성 메시지 M을 RF 리더기에 전송한다.

③ RF 리더기는 초기 인증 프로토콜의 ⑤에서 저장된 α_1과 전송된 Z_1을 데이터 베이스에 전송한다.

④ α_1, Z_1을 전송받은 데이터 베이스는 전송 정보에 대한 검증과정을 수행한 뒤 올바른 정보일 경우 TID_1에 해당되는 RFID 태그 1의 인증 레벨 정보를 다음과 같이 생성한다.

- 검증 과정 : 초기 인증 프로토콜에서 저장된 대응 테이블을 검색하여 TID_{T_1}에 대응 저장된 r_R, r_D을 추출해 β_1', α_1'을 생성하여 $\beta_1=\beta_1'$, $\alpha_1'=\alpha_1$, $Z_1'=Z_1$ 검증
- 인증 레벨 정보 AL(Authentication Level) 생성 : 후방향 데이터베이스는 인증 레벨 정보의 중간값 생성을 위해 랜덤 수 r_{D_1}을 생성한 후 A_1^i를 계산한다. 생성된 A_1^i로부터 인증 레벨 정보 AL_1^i를 계산 한 뒤 후방향 데이터베이스의 타임스탬프 T_D와 함께 RF 리더기에 이를 전송한다. (RFID 태그 1에 해당되는 인증 정보 생성의 경우, 생성된 AL_1^i는 C_{T_1}의 일대일 대응 테이블로 저장된다.)

$$A_1^i = H(r_{D_1}) \| Z_1,\ AL_1^i = H(A_1^i)\ \ (i=1,2,3)$$

- AL_1^1 : 초기화 과정이 수행된 RFID 태그에 대해서만 자동 접근이 허용된다. 인증되지 않은 태그의 경우 1) 과정이 요구된다.
- AL_1^2 : 초기화 과정이 수행된 RFID 태그라 할지라도 1) 과정이 재수행된다.
- AL_1^3 모든 장비에 대해 개방적이다. 인증이 필요하지 않으며, 개체에 대한 접근이 자동적으로 허용된다.

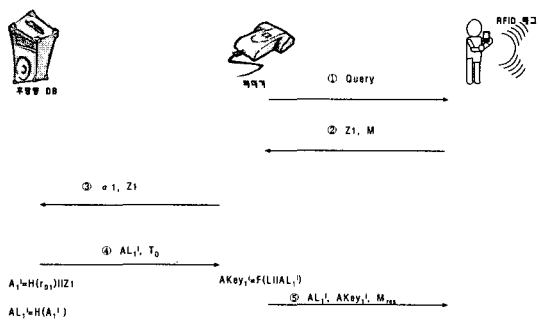


그림 3. 서비스 생성에 따른 인증 레벨 설정 과정

⑤ RF 리더기는 서비스 생성 메시지 M에 대한 응답 메시지 M_{res}를 생성하고 RFID 태그 1에 대한 인증 레벨 정보 AL_1^i, 인증 레벨 키 AKey_1^i, M_{res}를 RFID 태그 1에 전송한다. 전송된 AKey_1^i는 AL_1^i와 일대일 대응 저장된다.

$$AKey_1^i = F(L \| AL_1^i)\ \ (i=1,2,3)$$

3) 동일한 서비스에 대한 관리

동일한 서비스와 인증 레벨을 갖는 RFID 태그의 서비스 요청이 있을 경우 다음과 같은 수행과정을 거쳐 동일한 서비스에 대한 관리를 데이터 베이스에서 수행한다.

① RF 리더기는 j개의 임의의 RFID 태그들에 Query를 전송한다.

② j개의 RFID 태그들은 서비스를 요청하는 Service Request와 $(Z_1,....,Z_j)$, $(AL_1^1,....,AL_j^i)$을 RF 리더기에 전송한다.

③ j 개의 RFID 태그들로부터 전송된 Service Request, $(Z_1,....,Z_j)$, $(AL_1^1,....,AL_j^i)$에서 동일한 Service Request를 요구하는 RFID 태그가 일정 개수 이상일 경우 전송된 Z에서 TID를 추출하여 대응 테이블 검색을 통해 해당되는 RFID 태그들의 (AL_1^1,AL_2^1,AL_3^1), (Z_1,Z_2,Z_3), $(AKey_1^1,AKey_2^1,AKey_3^1)$를 데이터 베이스에 전송한다. (동일한 서비스를 요구하는 RFID 태그가 TID_{T_1}, TID_{T_2}, TID_{T_3}일 경우)

④ 동일한 태그들의 서비스 요청에 따른 (AL_1^1, AL_2^1, AL_3^1), (Z_1, Z_2, Z_3), $(AKey_1^1, AKey_2^1, AKey_3^1)$ 을 전송받은 데이터 베이스는 임시 그룹서비스 TGS(Temporary Group Service), 임시 그룹키 G_{Key} 를 생성한다. 임시 그룹 서비스를 위해 RFID 태그의 Z는 데이터베이스에 저장된 r_R과 Ctt를 기반으로 검증할 수 있다. 검증이 올바른 경우 해당 TID에 대응되는 r_D의 값을 이용해 G_{Key} 를 생성한다.

$$TGS = H((AKey_1^1 \oplus TID_1) \| (AKey_2^1 \oplus TID_2) \| (AKey_3^1 \oplus TID_3))$$

$$G_{key} = H(r_D \oplus r_D' \oplus r_D'')$$

생성된 임시 그룹키 G_{Key}를 RF 리더기에 전송한다. 데이터 베이스는 저장된 TID들을 임시 그룹화하여 이를 TGS라 명명한다.

⑤ RF 리더기는 데이터 베이스 서버로부터 전송된 G_{Key}를 임시 저장하고, ② 과정의 RFID 리스트에 해당되는 RFID 태그에 G_{Key}를 멀티 캐스트 방식으로 할당한다. (그림 4 참조)

4.2 능동형 RFID 태그 인증 및 관리 프로토콜 제안

능동형 RFID 태그의 안전한 인증 과정 후 현재 위치 및 서비스 등록 과정을 수행하여 불법적인 RFID 태그에 대한 보안 서비스뿐만 아니라 단일 서비스와 그룹 서비스를 위한 안전한 관리 프로토콜을 제안하고자 한다. (그림 5참조)

가. 가정사항

① RFID 태그는 능동형 전력 공급이 가능한 태그로써 안전한 해쉬 함수와 암호화 함수, 의사 난수 생성기를 이용한 연산이 가능하다.

② 초기 RFID 태그는 후방향 데이터 베이스로부터 $HWID_{T_1}$, PW_{T_1}을 안전한 경로를 통해 할당받는다. (RFID 태그 1의 경우)

③ 후방향 데이터 베이스는 RFID 태그 1에 할당된 $HWID_{T_1}$ 에 대응되는 PW_{T_1}을 안전하게 저장하고 이를 RF 리더기에 안전하게 전송한다. RF 리더기는 모든 $HWID_T$ 와 PW_T를 일대일 대응 저장한다.

④ PW_0는 H($HWID_{T_1}$) + H(PW_{T_1})으로 구성되며, RF 리더기는 일대일 대응 테이블로 안전하게 저장한다.

⑤ RF 리더기는 실제적인 연산이 수행되는 개체이며, 후방향 데이터 베이스 서버는 초기 RFID 태그에 대한 정보 전송만을 수행한다.

⑥ RFID 태그 1은 초기 위치 정보(L_{T_1})을 사전에 RF 리더기로부터 전송받아 저장한다.

나. 시스템 계수

본 제안 방식에서 사용되는 시스템 계수는 다음과 같다.

* (R : RF 리더기, T : RFID 태그($T_1, T_2, ..., T_n$), BT : Black Tag)

$HWID_T$: RFID 태그의 고유한 하드웨어 주소값

PW_{T_1} : 후방향 데이터 베이스와 RF 리더기에 안전하게 저장된 값으로 RFID 태그 1이 초기 등록한 $HWID_{T_1}$ 에 대응되는 패스워드 정보

TID_T , RID : RF 태그의 ID, RF 리더기의 ID

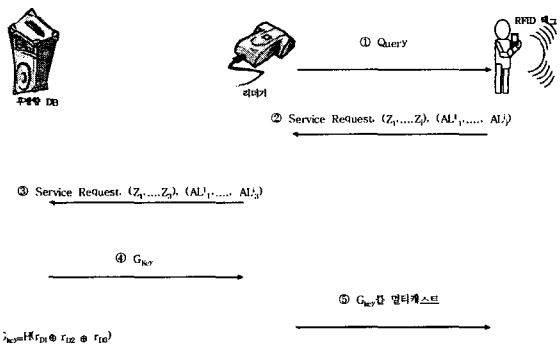


그림 4. 동일한 서비스에 대한 관리 과정

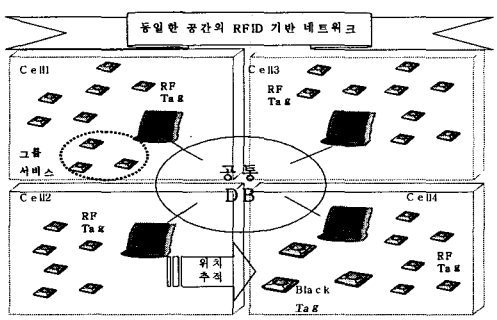


그림 5. 제안방식 시나리오

r_* : *에서 생성된 의사난수

t_j : RF 리더기와 RFID 태그가 공유한 식별 회수 (j=1,2,3,.....,n)

$H()$: 안전한 해쉬 함수

T_* : 각 개체의 타임 스탬프

L_T : RFID 태그의 위치정보 (타임 스탬프, 생성장소)

$Trace$: RF 리더기의 위치 정보

$E()$: 암호화 알고리즘

다. 세부 프로토콜

다음은 각 단계별 세부 프로토콜 과정을 기술한다.

1) 초기 등록 및 키 분배 단계

초기 등록 및 키 분배 단계는 RFID 태그 1이 RF 리더기에 초기 등록하고 키를 분배하는 과정이다. (그림 6 참조)

① RFID 태그 1은 초기 등록된 고유한 하드웨어 주소 값인 $HWID_{T_1}$을 이용해 W_{T_1}을 계산하여 RF 리더기에 전송한다.

$$W_{T_1} = H(HWID_{T_1})$$

② RF 리더기는 RFID 태그 1에서 후방향성 데이터 베이스로부터 사전에 분배받은 W_{T_1}에 대응되는 PW_{T_1}을 이용해 PW_0'을 생성하여 이를 기반으로 저장된 PW_0와의 검증 과정을 수행한다.

$$W_{T_1} + H(PW_{T_1}) = H(HWID_{T_1}) + H(PW_{T_1}) = PW_0'$$

$$PW_0' = PW_0$$

검증결과 전송된 W_{T_1}이 올바른 경우 PW_{T_1}을 PW_{T_1}'으로 갱신한 뒤 V와 r_R을 생성하여 RFID 태그 1에 전송한다.

$$V = H(PW_0), \quad Key = H(PW_0 \| HWID_{T_1})$$

$$PW_1' = E_{Key}(H(PW_{T_1})) + t_1$$

③ RFID 태그 1은 RF 리더기로부터 전송된 V를 사전에 저장된 $HWID_{T_1}$과 PW_{T_1}으로 검증하고 올바른 경우 r_R을 이용해 Z_{T_1}을 계산하고 Z_{T_1}, Y를 RF 리더기에 전송한 후 이를 저장한다.

$$Z_{T_1} = H(r_R \oplus PW_{T_1}), \quad Y = TID_{T_1} \oplus Z_{T_1}$$

④ RF 리더기는 RFID 태그 1로부터 전송된 Z_{T_1}을 검증한 뒤 올바른 경우 Y에서 TID_{T_1} RF 리더기는 현재 RFID 태그 1의 위치를 확인하기 위하여 위치 정보를 생성하고 이에 대한 서비스를 등록하는 단계이다. (그림 7 참조)을 추출해 PW_0에 일대일 대응 테이블로 저장하고 프로토콜 종료 메시지를 RFID 태그 1에 전송한다.

⑤ RFID 태그 1은 프로토콜 종료 메시지를 전송 받은 후 새로운 패스워드 정보인 PW_{T_1}'을 새로운 패스워드로 설정한다.

$$PW_{T_1}' = E_{Key}(H(PW_{T_1})) + t_1$$

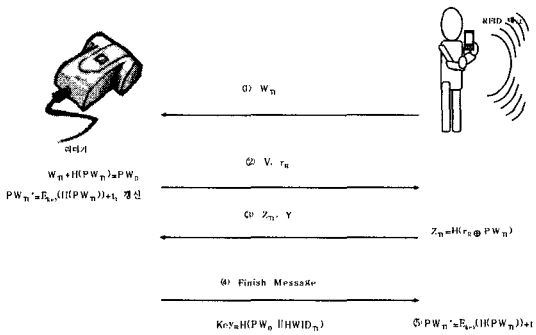


그림 6. 초기 등록 및 키 분배 단계

2) 위치 및 서비스 등록 단계

① RF 리더기는 RFID 태그 1에 대한 현재 위치 정보 획득을 위한 요청 메시지를 전송한다.

② RFID 태그 1은 RF 리더기로부터 전송된 메시지를 수신한 후 의사난수 r_{T_1}을 생성하고 다음을 계산하여 RF 리더기에 TID_{T_1}, r_{T_1}, h_{T_1}을 전송한다.

$$h_{T_1} = H(TID_{T_1} \| r_{T_1})$$

③ TID_{T_1}, r_{T_1}, h_{T_1}을 수신한 RF 리더기는 Trace와 TID_{T_1}의 $HWID_{T_1}$을 후방향 데이터베이스에서 검색하여 검증한뒤 올바른 경우 X_R과 Z_R을 계산하여 RFID 태그 1에 X_R,

Z_R을 전송한다. 전송 후 TID_{T_1}의 L_{T_1}에 대한 정보를 대응 테이블로 저장한다.

$P = H(L_{T_1} \| Trace)$ $X_R = H(P \| HWID_{T_1})$,
$Z_R = H(TID_{T_1} \| L_{T_1} \| X_R)$

④ RFID 태그 1은 암호 통신을 위한 NKey를 초기 등록 및 키 분배 단계의 ③에서 RF 리더기에 전송한 Z_{T_1}을 이용해 계산한다. (RF 리더기로부터 전송된 X_R과 Z_R은 RFID 태그 1에 저장된다.)

$NKey = H(Z_{T_1} \| HWID_{T_1})$

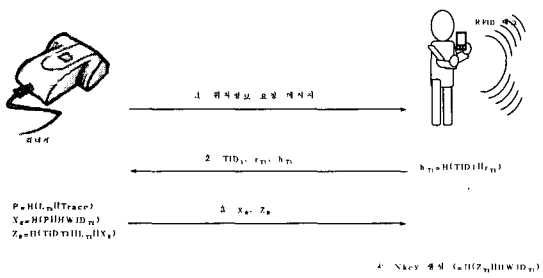


그림 7. 위치 및 서비스 등록 단계

3) 불법 RFID 태그에 대한 보안 서비스

불법적인 RFID 태그를 본 논문에서는 Black 태그라고 하며, Black 태그가 위치 및 서비스 단계에서 RF 리더기에 확인 될 경우 다음의 과정을 수행한다.(그림 8 참조)

① Black 태그는 접속 요청 메시지와 W_{Black}을 RF 리더기에 전송한다. (초기 등록 및 키 분배 단계의 ①참조)

② Black 태그로부터 접속 요청 메시지를 수신한 RF 리더기는 초기 등록 및 키 분배 단계의 ②에서 등록된 $HWID_T$ 인지 검증한 후 (RF 리더기의 등록되지 않는 $HWID_T$ 일 경우) 서비스 요청 메시지에 대한 응답 메시지를 송신한다.

③ Black 태그는 L_{BT}, X_{BT}, Z_{BT}, TID_{BT} 를 RF 리더기에 송신한다.

$X_{BT} = H(L_{BT} \| TID_{BT} \| HWID_{BT})$
$Z_{BT} = H(L_{BT} \| TID_{BT} \| X_{BT})$

④ RF 리더기는 Black 태그의 TID와 위치정보 메시지인 L_{BT}를 전송 받고 Black 태그의 Z_{BT}을 검증한다. 검증이 올바른 경우 Black 태그에 대한 정보(TID_{BT}, L_{BT})를 브로드캐스팅하고 Black 태그 리스트에 해당 태그에 대한 정보를 등록한다.

4) 인증된 단일 RFID 태그의 서비스 제공

인증된 RFID 태그 1이 서비스를 요구할 경우 RF 리더기는 단일 서비스 토큰(SToken)을 생성하여 이를 RFID 태그 1에 전송한 뒤, 안전한 서비스를 제공한다. (RFID 태그 1의 경우)

① RFID 태그 1은 접속 요청 메시지를 RF 리더기에 전송한다.

② RFID 태그 1로부터 접속 요청 메시지를 수신한 RF 리더기는 서비스 정보 요청 메시지를 RFID 태그 1에 송신한다.

③ RFID 태그 1은 RF 리더기로부터 전송된 서비스 정보 요청 메시지를 수신한 뒤 임의의 난수 r_{T_1}'과 타임 스탬프 T_{T_1}을 기반으로 V_{T_1}을 다음과 같이 계산하고 이를 RF 리더기에 전송한다.

$V_{T_1} = E_{NKey}(r_{T_1}' \| T_{T_1})$

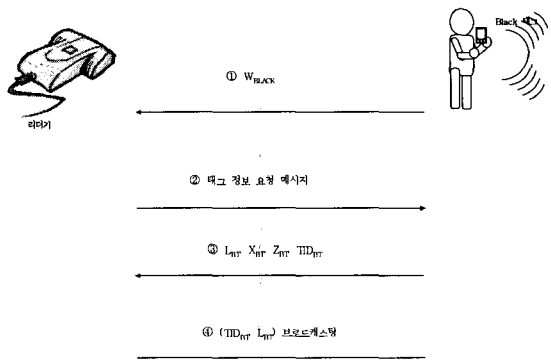


그림 8. 불법 RFID 태그에 대한 보안 서비스

④ V_{T_1}을 수신한 RF 리더기는 서비스 정보 요청 메시지에 대한 단일 서비스 토큰을 생성하고 V_R, RID와 같이 RFID 태그 1에 전송한다. 전송 이후 RF 리더기는 r_{R_1}과 $SToken_R$을 TID_{T_1}의 일대일 대응 테이블로 저장한다.

$V_R = E_{NKey}(r_{R_1})$, $SToken_R = E_{NKey}(r_{T_1}' \| r_{R_1} \| RID)$

- RFID 태그 1은 V_R을 복호화하여 $STOken_R$을 검증함으로써 그 정당성을 확인할 수 있다.

5) 그룹 서비스 제공

단일 서비스를 제공하는 단일 서비스 토큰이 일정 개수 이상 RF 리더기에 전송되어 서비스를 제공 받고자 할 경우 다음과 같은 그룹 서비스를 제공한다.

① j 개의 RFID 태그들은 서비스 요청 메시지와 $(STOken_{1,\ldots,j} STOken_j)$, $(TID_{T_1},\ldots,TID_{T_j})$를 RF 리더기에 전송한다.

② 단일 서비스 토큰들을 전송받은 RF 리더기는 일정 개수 이상의 동일한 서비스 요청 메시지가 전송될 경우 다음과 같이 그룹 서비스 토큰을 생성하여 각각의 RFID 태그에 전송함으로써 동일한 서비스를 요구하는 RFID 태그들을 위한 임시 그룹 서비스를 제공한다. (TID_{T_1}, TID_{T_2}, TID_{T_3}의 RFID 태그가 동일한 서비스 요청 메시지가 전송될 경우, 각 단일 서비스 토큰을 복호화하여 r_R을 추출한 뒤 이를 기반으로 그룹서비스 토큰을 생성한다.)

$$GToken = E_{NKey}(H(STOken_1 \| STOken_2 \| STOken_3) \| (r_{R_1} \oplus r_{R_2} \oplus r_{R_3}) \| RID)$$

이상의 과정을 거쳐 RFID 태그 기반의 안전한 형태의 네트워크 관리 방식이 수행된다. 그림 9는 4)~5)의 과정을 나타낸다.

5. 제안 방식 분석

본 장에서는 제안방식의 분석을 통해 기존 방식과의 차별성을 기술하고자 한다.

5.1 안전성 분석

제안 방식은 기존 방식과 비교해볼 때 다음과 같은 보안적 특징을 갖는다.

가) 수동형 RFID 태그 기반의 인증 및 관리 기법의 보안 분석

① ACIN(Authentication, Confidentiality, Integrity, Non-repudiation) : 제안 방식은 사전 공유된 RFID 태그의 고유값 x_T와 안전한 해쉬 함수 H()를 통해 인증과 무결성에 대한 보안 서비스를 제공해 준다. 기밀성 측면에서는 의사난수를 통해 인증 권한을 설정함으로써 안전성을 유지하고자 하였으나, 부인봉쇄 측면에서는 여전히 문제성을 지니고 있다.

② 채널 보안 : 제안된 방식은 전방향 채널에 대한 보안 사항을 β, α를 검증한 뒤 인증 레벨 AL을 기반으로 제공한다. 또한 RFID 태그와 RF 리더기 사이에 전송되는 정보의 수정 공격에 대해 랜덤 수 r_R과 안전한 해쉬함수 H(), 랜덤 함수 $F()$를 기반으로 안전성을 제공한다.

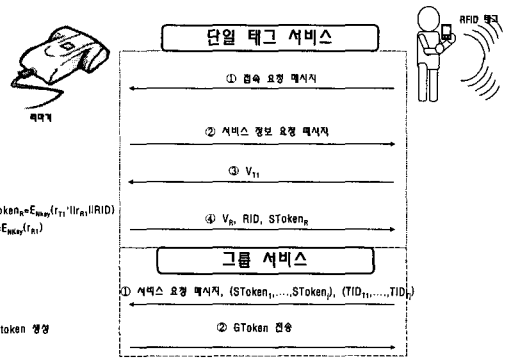


그림 9. 단일한 RFID 태그와 그룹 서비스 과정

③ 불법 RFID 태그에 대한 서비스 : 수동형 RFID 태그 기반 방식의 경우 불법 RFID 태그에 대한 보안 서비스를 제공하지 못한다.

④ 그룹 서비스로의 확장성 : 제안된 방식은 인증 레벨과 임시 그룹 설정을 통해 그룹 서비스로의 확장이 가능하다.

⑤ 구현의 효율성 : 수동형 RFID 태그의 인증 및 관리 방식은 1개의 해쉬 함수만으로 구성이 가능하다. 따라서 1,000 게이트를 1 Cent로 계산하였을 때 해쉬 함수는 2,000 게이트로 구성이 가능한 수동형 RFID 태그로의 구성이 가능하다. 따라서 기존 방식과 비교해볼 때 효율적인 구성 방식이다.

나) 능동형 태그 기반의 인증 및 네트워크 관리 기법

① ACIN : 제안된 방식의 경우 기존 방식과 비교 분석해 볼 때 인증 및 무결성 서비스를 안전한 해쉬 함수 기반으로 제공한다. 그러나 기존 방식에서 고려되지 못했던 기밀성을 위해 리더기에서 암호화된 서비스 토큰인 Token(단일서비스 토큰 $STOken = E_{NKey}(r_{T_1}' \| r_{R_1} \| RID)$, 그룹 서비스

토큰 GToken = $E_{Nkey}(H(SToken) \| r_R \| RID)$)을 이용함으로써 어플리케이션 서비스를 위한 데이터의 기밀저장 서비스를 제공할 수 있다.

② 채널 보안 : 제안된 방식은 리더기에서의 암호화를 통해 RFID 태그에 전송되는 정보의 기밀성을 보장하였다. 따라서 기존 방식과 같은 전방향 채널의 기밀성 서비스를 제공할 수 있도록 하였으며, 전송되는 정보에 대한 무결성 제공을 위해 해쉬 함수를 이용한 방식을 제시하였다.

③ 불법 RFID 태그에 대한 보안 서비스 : 제안된 방식은 기존 방식에서 고려되지 않았던 Trace 정보인 $X_{BT} = H(L_{BT} \| TID_{BT} \| HWID_{BT})$ 를 이용해 불법 RFID 태그가 접근시 이동 경로를 추적할 수 있을 뿐 아니라 이에 대한 접근 제한 서비스를 위해 Black 태그에 대한 내용을 주변 리더기에 브로드캐스팅하고 이에 대한 정보를 유지하도록 하였다.

④ 그룹 서비스로의 확장성 : 제안 방식의 경우 RFID 태그 기반의 네트워크 형성시 효율성을 높이기 위해 단일 및 그룹 서비스 토큰을 이용한 방식을 제안하였다. 서비스 토큰은 *HWID* 기반의 인증 수

표 2. RFID 태그의 인증 및 관리 방식 안전성 분석

방식	ACIN	채널보안	그룹 보안 서비스의 확장성	불법 RFID 태그 에 대한 보안 서비스	구현
해쉬락 방식	AI	전방향	None	None	가능
향상된 해쉬락 방식	ACI	전방향	None	None	어려움
해쉬 체인 방식	ACI	전방향	None	None	가능
재암호화 방식	ACI	전방향	None	None	가능
XOR 방식	AI	전방향	None	제공	가능
제안방식 I	ACI	전방향	제공	None	가능
제안방식 II	ACI	전방향	제공	제공	매우 어려움

* ACIN(Authentication, Confidentiality, Integrity, Non-repudiation)
* None : 서비스를 제공하지 않음

행후 임시적인 그룹 서비스를 위해 제공할 수 있어 리더기에 대한 효율성을 높이고자 하였다.

⑤ 구현의 효율성 : 능동형 제안 방식의 경우 고가의 RFID 태그 기반의 다양한 보안 서비스를 위해 여러 가지 알고리즘을 포함하는 방식을 제안하였다. 따라서 수동형 방식에 비해 매우 비효율적인 구현적 특징을 제시할 수 있다.

5.2 효율성 분석

제안방식은 3장에서 분석한 기존 방식과 비교해 볼 때 다음과 같은 효율성을 갖는다.

- 패스 수 : 해쉬락 방식은 6번의 핸드쉐이크 과정을 수행하고 향상된 해쉬 락 방식의 경우 5번의 핸드쉐이크를 기반으로 수행되며, 해쉬 체인 방식은 4 패스로 진행된다. 수동형 RFID 태그를 기반으로한 제안 방식은 초기 등록 및 인증 과정은 7번의 핸드쉐이크로 수행된다. 재암호화 방식과 XOR 방식의 경우 5회와 4회의 패스수로 이루어진다. 따라서 패스 수로 비교해 볼 때 향상된 기존 방식보다 패스수의 증가를 들 수 있다. 그러나 능동형 RFID 태그 기반의 제안방식은 각 방식보다 효율적인 4번의 핸드쉐이크를 통해 인증 서비스를 제공함으로써 해쉬락과 향상된 해쉬락 방식보다는 높은 형태의 패스 효율성을 제공한다.
- 연산량 : 수동형 RFID 태그 기반 방식의 경우 RFID 태그를 기준으로 초기 등록 및 인증 과정을 수행하는 과정에서 2번의 해쉬 연산을 수행한다. 재암호화 방식과 XOR 방식의 경우 암호화 연산 및 랜덤수 연산으로 인증이 이루어진다. 따라서 해쉬락 방식, 해쉬 체인 방식과 같은 효율성을 제공할 수 있으나, 향상된 해쉬락 방식이나 XOR 방식과 비교해 볼 경우 비효율적인 랜덤수를 사용하지 않기 때문에 연산량에서 효율적이라고 제시할 수 있다. 능동형 RFID 태그 기반의 제안방식은 향상된 해쉬 락 방식과 XOR 방식에서 제시했던 랜덤 수 생성기를 RFID 태그가 내장되어 있음을 가정하였을 때 인증 과정에서 랜덤수 생성이 아닌 암호화 연산을 수행함으로서 인증 과정만을 구분하여 비교할 때 보다 효율적이라 제시할 수 있다.
- 사용알고리즘 : 수동형 RFID 태그 제안방식의 사용 알고리즘은 해쉬 알고리즘 1개로 구현되는 특징을 갖는다. 따라서 기존 방식과 비교해볼때 보다 높은 형태의 효율성을 제공한다고 할 수 있다. 또한 900MHz 대역에서 설계된 프로토콜로 활용될 경우 사용되는 해쉬 알고리즘 하나만으로

구성이 가능함으로, 가격대 효율측면에서 높은 특징을 제공해 준다. 능동형 RFID 태그를 기반으로 구성된 제안방식의 경우 기존 방식에서 고려되지 않았던 다양한 보안 서비스와 연산량을 부여함으로써 해쉬함수와 더불어 랜덤 수 생성기와 암호화 함수 내장을 가정하였다. 따라서 기존 향상된 해쉬 락 방식과 비교 분석할 경우 수동형 RFID 태그에 대한 높은 보안 서비스제공에 따른 취약성을 능동형 RFID 태그 형태로 구성 가능하게 하였다.

- 구현 여부 : 수동형 태그 기반의 제안방식은 랜덤 수 생성기를 대신해 카운터 정보를 사용함으로써 구현에 대한 가능성이 높다할 수 있다. 그러나 능동형태그 기반의 제안방식의 경우 랜덤 수 생성기와 안전한 해쉬 함수 및 암호화 함수를 포함함으로써 높은 보안 서비스를 제공할 수 있는 반면 구현에 대한 비현실성을 제시할 수 있다.

표 3. 제안방식의 효율성 분석

방식	패스	연산량(RFID기준)	사용 알고리즘	구현
해쉬락 방식	6	해쉬연산 2번	해쉬 알고리즘 1개	저가형
향상된 해쉬락 방식	5	랜덤수 연산 1번 해쉬연산 1번	RNG 1개 해쉬 암고리즘 1개	고가형
해쉬 체인 방식	4	해쉬연산 2번	해쉬알고리즘 2개	저가형
재암호화 방식	5	암호화 연산 1번 해쉬 연산 1 번	암호화알고리즘1개 RNG 1개	고가형
XOR 방식	4/5	XOR 연산 2번/ 랜덤수 연산 1번 XOR 연산 1번	RNG 1개 해쉬알고리즘 1개	저가형
제안방식 I	6	해쉬 연산 3번	해쉬 알고리즘 1개	저가형
제안방식 II	4	해쉬 연산 2번 암호화 연산 1번	RNG 1개 해쉬 알고리즘 1개 암호 알고리즘 1개	고가형

6. 결 론

본 논문에서는 차세대 IT 기반 환경인 유비쿼터스 컴퓨팅 기술의 적용을 위해 다양한 연구와 상용화가 추진중에 있는 무선 통신기술중에서 RF 통신을 기반으로 한 수동형과 능동형 RFID 태그의 인증 및 관리에 대한 연구를 수행하였다. 특히, 유비쿼터스 환경과 같은 사용자 중심의 네트워크 형성을 위해서는 소형 개체 기술이 반드시 요구되고 이와 더불어 사용자의 프라이버시를 보호할 수 있는 보안 기술에 대한 연구가 절실히 필요한 시점에서 매우 의미 있는 연구를 수행하였다. 그러나 제안된 방식의 경우 여전히 프로토콜 수정 공격이나 물리적 공격 및 다양한 네트워크 공격에는 취약할 수 있다. 따라서 향후 연구 방향으로는 보다 다양한 보안 위협에 대한 보완사항과 더불어 보다 현실적인 RFID 태그에 대한 보안 서비스를 위한 프로토콜이 연구되어야 할 것으로 사료된다.

참 고 문 헌

[1] Stephen A. Weis, "Security and Privacy in Radio-Frequency Identification Devices", Masters Thesis. MIT. May, 2003.

[2] Stephen A. Weis, Sanjay E.Sarma, Ronald L. Rivest and Daiel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", First International Conference on Security in Pervasive Computing, 2003. http://theory.lcs.mit.edu/ sweis/spc-rfid.pdf

[3] Sanjay E.Sarma, "Towards the five-cent Tag", Technical Report MIT-AUTOID-WH-006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org

[4] Sanjay E.Sarma, Stephen A. Weis and Daiel W. Engels, "Radio-Frequency Identification : Secure Risks and Challenges", RSA Laboratories Cryptobytes, vol. 6, no.1, pp.2-9. Spring 2003

[5] Sanjay E.Sarma, Stephen A. Weis and Daiel W. Engels, "Radio-frequency identification systems", In Proceeding of CHES '02, pp454-469. Springer-Verlag, 2002. LNCS no. 2523.

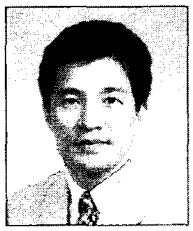
[6] D. Henrici and Paul Muller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," PerSee'04 at IEEE PerCom. pp. 149~153, 2004.

[7] A. Jules and R. Pappu. Squealing euros, "Privacy protection in RFID-enabled

bank-notes, In processing of Financial Cryptography," FC'03, vol.2742 LNCS, pp.103~121, Sep 2003.
[8] A. Juels, "Minimalist cryptography for Low-Cost RFID Tag," In The Fourth International Conference on Security in Communication Networks-SCN 2004, vol. 3352 LNCS, pp.149~164, Sep 2004.
[9] A. Juels, "Authentication Pervasive Devices with Human Protocols," Crypto 2005, Aug 205. (http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/ pdfs/lpn.pdf)
[10] S. Junichiro, R. Jae-Cheol and S. kouichi, "Enhancing privacy of Universal Re-encryption scheme for RFID Tags," EUC 2004, Vol. 3207 LNCS, pp.879~890, Dec 2004.
[11] L. Su Mi, H. Young Ju, L. Dong Hoon and L.Jong "Efficient Authentication for Low-Cost RFID systems," ICCSA05, vol. 3480 LCNS, pp.619~629, May 2005.
[12] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, "Cryptographic Approach to "Privacy-Friendly" Tag" RFID Privacy Workshop@MIT, Nov, 2003
[13] MIT Auto-ID Center. http://www.autoidcenter.org
[14] RFID Journal. Gillette to Phurchase 500 Millin EPC Tags, http://www.rfidjournal.com
[15] 조태남, 이상호, "(2,4)-트리를 이용한 그룹키 관리*", 한국정보보호학회 논문지 ,Vol11, No1, pp77-89, 2001.
[16] 박영호, 이경현, "이동네트워크 환경에서의 그룹키 관리구조*", 한국정보보호학회 논문지, Vol12, No.2, pp89-100, 2002.
[17] 권정옥, 황정연, 김현정, 이동훈, 임종인, "일방향 함수와 XOR을 이용한 효율적인 그룹키 관리 프로토콜:ELKH", 한국정보보호학회 논문지 Vol.12, No.6, pp93-112, 2002.
[18] 이상원, 천정희, 김용대, "Pairing을 이용한 트리 기반 그룹키 합의 프로토콜", 한국정보보호학회 논문지, Vol.13, No.3, pp101-110, 2003.
[19] 박영희, 정병천, 이윤호, 김희열, 이재원, 윤현수, "Diffie-Hellman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜", 한국정보보호학회 논문지, Vol13, No.5, pp3-15, 2003.
[20] 최은영, 이동훈, "RFID 정보보호 기술 동향," 정보처리학회 학회지, pp.75-83, 2005.

〈著者紹介〉

서 대 희 (Dae-Hee Seo) 학생회원
2003년 2월: 순천향대학교 전산학 전공 석사
2004년 3월~현재: 순천향대학교 전산학과 박사과정
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안



이 임 영 (Im-Yeong Lee) 정회원
1981년 8월: 홍익대학교 전자공학과 졸업
1986년 3월: 오사카대학 통신공학 전공 석사
1989년 3월: 오사카대학 통신공학 전공 박사
1989년 1월~1994년 2월: 한국전자통신연구원 선임연구원
1994년 3월~현재: 순천향대학교 정보기술공학부 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안