# 유비쿼터스 환경에서의 안전하고 효율적인 이종 RFID 관리 기법

## (A Secure and Efficient Management Scheme based Heterogeneous RFIDs for Ubiquitous Environments)

서 대 희 † 백 장 미 †† 조 동 섭 †††
(Dae-Hee Seo) (Jang-Mi Baek) (Dong-Sub Cho)

**요 약** 센서 네트워크 기술로서 스마트 태그 기술을 이용한 RFID 기술이 최근 각광을 받고 있다. 그러나 누구든지 태그 정보를 쉽게 읽어 볼 수 있는 점, 태그와 리더기 간의 상호 인증 문제, 저렴한 가격의 스마트 태그 구현을 위하여 보안적인 구현의 커다란 제약이 존재하는 등 유비쿼터스 컴퓨팅 환경에서 적용하기엔 여전히 문제점들이 발생되고 있다. 따라서 제안방식은 사용자 주변의 신뢰된 RFID 태그를 기반으로 RF 네트워크에서 요구되는 다양한 서비스와 관련된 보안과 효율성을 향상시키기 위해 기존 논문에서 인증만을 위해 사용하던 수동형 RFID 태그를 이용해 임시 그룹을 설정하여 동적인 환경에 다양한 서비스를 제공하기에 적합한 관리 방식을 제안하였다. 또한 RFID 관리 방식에서 RFID 그룹화, 서비스별 임시 그룹 설정, 보안 서비스를 제공하며, 통신의 효율성을 향상 시켰다.

**키워드** : 유비쿼터스 환경, 상호 인증, RFID 관리, 수동형 RFID 태그

***Abstract*** RFID technology using the smart tag technology as a part of the sensor network is currently in the spotlight. But there are still many problems in applying the technology in a ubiquitous environment, including at the point when anybody can read the tag information and the authentication between the tag and the reader, and security problems in very low-cost smart tag implementation. The proposed scheme is designed to enhance security and efficiency related to various services required in RF networks, based on the reliable peripheral devices for users of passive RFID tag. Using passive RFID tag, which has been applied to authentication transactions in existing papers, this study also proposed an appropriate management scheme that is suitable for a dynamic environment and setting a temporary group to provide various services. also proposed scheme is support RFID grouping, temporary group of service and security servicce, improved efficiency of communication.

**Key words** : Ubiquitous Environment, Mutual Authentication, RFID Management, Passive RFID Tag

## 1. 서 론

유비쿼터스 환경에서는 사물에 대한 전산 환경을 부여하기 위해 소형화된 디바이스가 사용되고 이와 관련된 연구는 매우 큰 의미를 가질 수 있다. 따라서 유비쿼터스 환경을 구체화하기 위해서는 소형화된 디바이스에 대한 연구가 반드시 요구되고 있으며, 국내외적으로 RFID(Radio Frequency IDentification)를 핵심 요소기술로 규정하고 이에 대한 연구를 추진 중에 있다. 그러나 기존의 RFID 태그에 대한 연구는 바코드 체계를 대체하기 위한 초기 연구이며, 사용자 프라이버시 보호는 단순한 인증 과정만을 수행함으로써 인증 이후의 문제점을 고려하지 않아 많은 문제점을 내포하고 있다. 따라서 기존의 RFID 연구에서 고려되지 않았던 인증 이후

† 정 회 원 : 이화여자대학교 컴퓨터공학과 교수
dhseo@ewha.ac.kr
†† 정 회 원 : 순천향대학교 컴퓨터공학부
bjm1453@sch.ac.kr
††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
dscho@ewha.ac.kr
논문접수 : 2008년 11월 19일
심사완료 : 2009년 5월 12일

Copyright©2009 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.
정보과학회논문지: 정보통신 제36권 제4호(2009.8)

의 다양한 고려사항을 만족하는 차별화된 보안 프로토콜에 대한 연구를 수행이 반드시 요구된다[1,2].

따라서 본 논문에서는 안전한 RFID 인증 과정 이후 다양한 수동형 RFID 태그들이 동일한 RF 네트워크에 공존할 경우 각각의 RFID 태그들을 임시 그룹화하여 해당되는 RFID 태그들에 제공하고 이를 관리 할 수 있는 안전하고 효율적인 형태의 네트워크 관리 기법을 제안하고자 한다.

이에 2장에서는 유비쿼터스 환경에서 사용되는 RFID 기술에 대한 일반적인 개요를 기술하고, 3장에서는 기존의 RF 인증 및 관리 연구에 대해 분석하고 보안 취약성을 분석하고자 한다. 4장에서는 이종 RFID 태그를 위한 안전하고 효율적인 네트워크 관리 방식의 보안 요구사항을 제안하고 5장에서는 4장에서 제시한 보안 요구사항을 만족할 수 있는 안전하고 효율적인 이종 RFID 관리 기법 제안한다. 6장에서는 기존 연구와 제안 방식을 비교분석한 뒤 마지막으로 7장에서 결론 및 향후 연구 방향을 제시하도록 한다.

## 2. 기술 개요

본 장에서는 유비쿼터스 환경에서 정보보호의 필요성과 핵심 요소 기술로 제시되고 있는 RFID 태그에 대한 일반적인 개요를 기술하고자한다.

### 2.1 소형 디바이스에 대한 보안의 필요성

유비쿼터스 환경은 개체마다 많은 정보를 갖고 있으며 이에 대한 정보를 수집 분석하여 필요한 서비스를 자동적으로 처리해주는 능동형 환경으로써 필연적으로 개인의 정보를 어떻게 보호할 것이며, 어떠한 방법으로 서비스를 안전하게 제공할 것인지에 대한 연구가 반드시 요구된다[3,4].

그러나 기존의 연구는 단순한 개체의 인증을 통한 연구가 이루어지고 있는 실정으로, 유비쿼터스 환경이 구현되었을 때 나타날 수 있는 다양한 형태의 보안 연구가 미흡한 실정이다. 현재 유비쿼터스 환경에서 공격자들에 대한 정확한 형태를 파악할 수 없는 상태에서 적용되는 기술의 보안적 취약점은 어떠한 형태로 사용자 프라이버시 정보를 침해 할지 예측하기 매우 어렵다[5,6].

따라서 다양한 보안 요구사항과 이를 만족하는 보안 프로토콜 개발은 안전한 유비쿼터스 환경에 매우 절실히 요구되는 사항이다.

### 2.2 RFID 시스템의 개요

RFID 시스템은 판독 및 해독 기능을 하는 RF 리더기와 정보를 제공하는 RFID 태그로 구성된 무선통신 시스템이다. RFID 태그는 사람, 자동차, 화물 등에 개체를 식별하는 정보를 부가하는 시스템으로 그 부가 정보를 무선 통신 매체를 이용함으로써 기존에 오프라인으로 이루어지는 다양한 어플리케이션을 자동화할 수 있으며 그 특징은 다음과 같다[5,7,8].

- 편리한 사용과 여러 태그를 동시에 인식이 가능
- 고속 인식이 가능하여 시간적인 효율성이 가능
- 시스템 특성이나 환경 여건에 따라 손쉬운 적용
- 비접촉식의 특성에 따른 반영구적 사용과 유지보수에 대한 경제성이 우수
- OTP(One Time Programming)로 RFID 태그를 프로그램 하여 데이터 위조 및 변조에 대한 보안성 제공
- 시스템 확장이 용이
- 양방향 인식이 가능

RFID 기술은 원거리에서도 물리적인 접촉 없이 인식이 가능하고, 여러 개의 정보를 동시에 판독하거나 수정할 수 있는 장점 때문에 바코드를 대체하거나 보완할 수 있는 기술로서 현재 유통분야뿐 아니라 물류, 교통, 보안 가전 분야로의 적용이 나날이 확대되고 있다[5,7-10].

## 3. 기존 방식 분석

RFID 태그와 관련된 기존 연구는 최근 많은 연구가 진행되고 있으며, 이와 관련된 기존 연구는 해쉬 기반, 재암호화 기반, XOR 기반으로 나누어 분석하면 다음과 같다.

### 3.1 RFID 인증 방식 분석

① Hash Lock Scheme은 MIT에 의해 제시된 방식으로 낮은 가격을 고려한 방식이다. 각각의 개체는 해쉬 함수를 가지고 있다고 고려된다. 그러나 단지 전송 데이터에 대한 동의와 리더기가 가지고 있는 ID의 전송을 통해 인증 과정을 수행한다[1,9,11-13]. 따라서 본 방식은 낮은 가격과 고정된 Meta ID를 기반으로 제안된 방식이지만 공격자가 공개된 Meta ID를 통해 RFID 태그에 대한 공격이 가능하다. 이후 제안된 Randomized Hash Lock Scheme은 해쉬락 방식의 확장된 형태이다. 이 방식의 경우 기존 해쉬락 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[14,15]. 그러나 본 방식은 RFID 태그의 출력 정보가 액세스마다 매번 바뀌어 ID에 대한 유추가 어려운 방식이다. 또한 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. Hash-Chain Scheme은 일본의 NTT에서 제안된 방식으로써 안전한 해쉬 함수

를 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[16,17].

그러나 데이터베이스 서버에 대한 정보의 분할과 더불어 기밀성 측면에서의 안전성은 고려되지 않았다. 이는 초기 데이터 전송 이후의 전송 데이터에 대한 PFS (Perfect Forward Secrecy)를 제공할 뿐이다. 따라서 해쉬 체인 방식의 경우 해쉬 체인을 생성하기 위한 초기 값 전송 시 기밀성 서비스와 확장성 부분에서 문제성 및 고유한 ID와 비밀정보 초기 값에 대한 대응 저장으로 인해 발생할 수 있는 후방향성 서버의 안전성에 문제점을 지적할 수 있다.

② Universal Re-encryption scheme : Satio 등에 의해서 제안한 방식으로 유니버셜(Universal) 재암호화 방식을 사용한다. 유니버셜 재암호화 방식이란, 재암호화 과정이 일어날 때 공개키 없이 임의의 랜덤 값을 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[18,19].

- 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 랜덤 값 $\triangle = \{(\alpha_1^{m_1}, \beta_1^{m_1}),(\alpha_1^{m_2},\beta_1^{m_2}),.....,(\alpha_1^{m_{2i}},\beta_1^{m_{2i}})$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 랜덤 값 갱신 : RFID 태그는 리더로부터 받은 one-time 랜덤 값에 대해 다음과 같은 갱신한다. 우선, RFID 태그와 리더는 비밀 정보 S를 공유한다. 데이터베이스는 RFID 태그에게 새로운 one-time 랜덤 값 $\triangle'$과 X를 다음과 같이 생성하여 전송한다.

$$\triangle' = \{(\alpha_1^{m_1'},\beta_1^{m_1'}),(\alpha_1^{m_2'},\beta_1^{m_2'}), ..., (\alpha_1^{m_{2i}'},\beta_1^{m_{2i}'})\},$$
$$X = h(S, I, \triangle')$$

RFID 태그는 새로 받은 값들을 이용하여 h(S, i, $\triangle'$)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 랜덤 값 $\triangle'$으로 기존의 랜덤 값들을 갱신한다. One-time 랜덤 값을 사용하는 프로토콜이다.

③ HB Authentication protocol(XOR based Scheme) : 최근에 Crypto 학회에 RFID 시스템의 프라이버시 보호에 대한 방식이 제안되었다. 이 방식은 Juels에 의해 제안된 방식으로 1 비트로 상대방을 인증하는 방식이다[12,18,20]. 제안된 방식은 HB 프로토콜이라 표기하며 과정은 다음과 같다.

우선, RFID 태그와 리더 간에 비밀 값 x를 공유한 상태에서 리더가 태그를 인증하게 된다. 태그가 리더에게 $\alpha$ 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 $a \cdot x$값을 받은 $z$값과 같은지를 확인한다. 1 비트로 인증을 하기 때문에 r번 반복하여 정확성을 높인다. 하지만 이러한 경우에도 공격자가 a의 비트 길이 k번만큼 세션을 도청할 경우 비밀 정보 x에 대해 알 수 있기 때문에 $\eta \in (0, \frac{1}{2})$라는 확률로 $\nu$값을 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[18,21].

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

제안된 HB+방식은 능동적인 공격에 안전하게 설계하기 위해서 b라고 하는 값을 태그가 선택하여 전송하도록 하였다[13,22]. 그러므로 공격자가 자신에게 유리한

표 1 기존 RFID 인증 방식 분석

| 방식 | ACIN | 채널보안 | 그룹 보안 서비스 | 그룹에 대한 관리 | 구현의 효율성 (수동형 태그 기반) |
|---|---|---|---|---|---|
| Hash Lock Scheme | AI만 만족 | 전방향 채널 | 비제공 | None | 가능 |
| Randomized Hash Lock Scheme | ACI 만족 | 전방향 채널 | 비제공 | None | 어려움 |
| Hash-Chain Scheme | ACI 만족 | 전방향 채널 | 비제공 | None | 가능 |
| Re-encryption scheme | ACI 만족 | 전방향 채널 | 비제공 | None | 어려움 |
| HB Authentication protocol | AI 만족 | 전방향 채널 | 비제공 | None | 가능 |

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

값 a를 생성하여 공격을 시도할지라도 b 값으로 인해 비밀값 y에 대한 정보를 얻을 수 없기 때문에 안전하다고 제시되고 있으나 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[23].

### 3.2 RFID 관리 방식 분석

① 수동형/능동형 RFID 태그 관리 방식

수동형/능동형 RFID 태그 관리 방식에 대한 연구는 2005년 KISC에서 제안된 RFID 관리 방식으로 수동형과 능동형 RFID 태그를 기반으로 그룹 서비스와 더불어 불법 RFID 태그에 대한 블록 서비스를 제시하는 방식이다. 그러나 본 방식의 경우 다음과 같은 취약성을 내포하고 있다[23].

- 그룹에 대한 관리 : 제안된 방식은 수동형과 능동형 RFID 태그들에 대한 관리 서비스를 구분하여 제시하였다. 그러나 수동형 태그로 네트워크를 구성할 경우 인증 레벨의 설정시 초기 인증 과정에서만 수행하고 이를 기반으로 후방향성 데이터베이스 서버에서 제시한 모든 서버들을 저장한 상태에서 그룹에 대한 서비스가 가능하다. 따라서 제안된 방식은 비인가 된 RF 리더기로부터 RF 태그의 안전성을 보장할 수 없으며, 이를 위한 보안 서비스가 제공되지 않는다.
- 구현의 효율성 : RFID 태그 인증 시스템을 구성하고자 할 경우 현재 RFID 태그의 물리적 한계성 때문에 발생할 수 있는 적용의 문제점을 해결 할 수 있어야 한다. 여기에서 가장 중요한 점은 낮은 가격의 태그에 적용이 가능한지의 여부이며, 이는 하드웨어적 구성에 초점이 맞추어지게 된다.

② SIP 기반의 RFID 관리 시스템

본 연구는 2007년에 SIP 기반으로 RFID 태그를 관리하는 SRMS(SIP-based RFID Management System) 시스템이다. 제안 방식은 쉬운 구현과 3G에서의 IMS (IP Multimedia Subsystem)를 목적으로 상호 운용성을 보장한다. 특히, EPC(Electronic Product Code)를 기반으로 SRMS Name Server와 SUA(Surrogate User Agent)를 이용해 RFID의 위치정보를 관리하는 중앙 집중형 시스템이다[5,24]. 그러나 본 방식의 경우 다음과 같은 보안 취약성을 내포하고 있다.

- ACIN : 본 논문에서는 기본적인 RFID 통신에서 요구되는 보안 서비스를 제공하지 않는다. 따라서 RFID 통신에서 요구되는 기본적인 보안 요구사항 뿐만 아니라 후방향 데이터베이스 서버에서 제공되는 정보에 대한 보안 서비스를 제공하지 않는다.
- 그룹 보안 서비스 : SIP 방식은 각각의 RFID 태그들에 대한 서비스를 개별화 서비스를 제공한다. 따라서 RFID 태그들의 개수가 증가할 경우 각각의 후방향 데이터베이스 서버에서는 보다 효율적인 관리를 위해 그룹 서비스가 요구되며 이를 위한 보안 서비스가 추가되어야 한다. 그러나 본 방식에서는 이에 대한 서비스를 제공하지 못하는 취약성이 내포되고 있다.
- 그룹에 대한 관리 : 본 방식은 위치 추적을 위해 EPC, 타임 스탬프, IP 주소를 기반으로 SIP 방식을 이용하여 위치를 등록한 뒤 이를 역추적 하는 방식을 제공한다. 그러나 본 방식의 경우 후방향성 데이터베이스 서버가 각각의 도메인을 저장해야 하고 각 도메인마다 별도의 서버를 구축함으로써 하나의 RFID 태그를 위한 비용 증가와 더불어 그룹에 대한 서비스를

표 2 기존 RFID 관리 방식 분석

| 방식 | ACIN | 채널 보안 | 그룹 보안 서비스 | 그룹에 대한 관리 | 구현의 효율성 (수동형 태그 기반) |
|---|---|---|---|---|---|
| 수동형/능동형 RFID 태그 관리 방식 | ACI 만족 | 전방향 채널 | 제공 | 제한적 제공 | 어려움 |
| SIP 기반 방식 | N 만족 | 전방향 채널 | 비제공 | None | 쉬움 |

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

제공하지 못함으로써 발생하는 네트워크의 효율성 저하를 문제로 지적할 수 있다.

## 4. 보안 요구사항 분석

수동형 RFID 태그에 대한 안전하고 효율적인 네트워크 관리 프로토콜을 구성할 경우 다음과 같은 보안 요구사항을 제시할 수 있다.

- ACIN : 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.
- 그룹 보안 서비스 : 단일한 RFID 태그만을 고려할 경우 다양한 RFID 태그들이 공존하는 환경에서 RFID 태그들에 그룹과 서비스를 규정하는 방식이 요구된다. 특히, 그룹의 경우 임시성을 가진 인증 및 관리 서비스는 RFID 태그들이 서로 다른 서비스를 요구할 경우 네트워크의 효율성을 저하시키지 않으면서 효율적으로 관리할 수 있는 그룹 보안 서비스이므로 이를 위한 방식을 제공해야 한다.
- 그룹에 대한 관리 : 임시적인 네트워크를 신뢰할 수 있는 후방향 데이터베이스 서버를 기준으로 자유롭게 생성하고 이를 삭제할 수 있어야 한다. 이를 위해서는 후방향성 데이터베이스 서버에서 그룹 관리에 대한 별도의 관리 방식과 서비스 형태를 규정해야 한다.
- 구현의 효율성 : RFID 태그 인증 시스템을 구성하고자 할 경우 현재 RFID 태그의 물리적 한계성 때문에 발생할 수 있는 적용의 문제점을 해결 할 수 있어야 한다. 여기에서 가장 중요한 점은 낮은 가격의 태그에 적용이 가능한지의 여부이며, 이는 하드웨어적 구성에 초점이 맞추어지게 된다.

## 5. 유비쿼터스 환경에서의 안전하고 효율적인 이종 RFID 관리 기법 제안

유비쿼터스 환경에서 소형화된 디바이스로 대표되는 서로 다른 기능의 수동형 RFID 태그들이 동일한 공간에 존재할 수 있다. 따라서 다양한 RFID 태그들이 네트워크를 구성하고 서비스를 관리할 수 있는 별도의 관리 방식이 요구된다. 이에 본 논문에서는 이종 RFID들에 대한 안전하고 효율적인 관리를 위해 다음과 같은 시나리오를 제시하고자 한다.

- 일반적인 WPAN(Wireless Personal Area Network)과 같은 크기의 작은 네트워크 공간에서 다양한 서비스를 제공하는 RFID 태그들이 공존하는 환경이다.
- 다양한 RFID들이 동일한 공간에 존재할 경우(물류, 유통, 우체국 등) 서로 다른 RFID들의 관리가 요구된다.
- 각각의 RFID들은 사용자들과의 안전한 인증 과정 이후 서로 다른 RFID들 간의 안전한 통신을 수행한다.
- 구성된 네트워크는 RF(Radio Frequency) 통신이 가능한 링크를 제공하며, 끊김없는 네트워크 통신이 가능하다.

### 5.1 제안 방식 시나리오

제안 방식은 다양한 RFID들을 소유하고 있는 다수의 사용자들이 무선 RF 네트워크를 기반으로 개인의 프라이버시 정보에 기반한 서비스를 RFID 태그를 통해 후방향 데이터베이스 서버로부터 전송받고자 할 경우 이를 위한 RFID 태그들의 관리와 사용자 프라이버시 보호를 위한 지속적인 관리 서비스를 수행하는 과정으로서 제안 방식의 흐름도는 그림 1과 같다.

① 사용자는 소유하고 있는 RFID 태그들과의 안전한 인증과정을 수행하고 그 결과를 후방향성 데이터베이스 서버에 등록한다.

② 서비스의 형태에 따라 사용자가 소유하고 있는 RFID 태그들을 분류하고 이를 위한 임시 그룹 초기화 단계를 수행한다.

③ 후방향성 데이터베이스 서버는 서비스에 따른 임시 그룹을 설정한다.

④ 임시 그룹으로 설정된 RFID 태그들은 안전한 통신 과정을 통해 임시 그룹을 위한 내부 인증과정을 수행하고 후방향 데이터베이스 서버로부터 서비스를 제공 받는다.

⑤ 임시 그룹에 대한 서비스가 종료될 경우 임시 그룹 정보에 대한 내용을 후방향 데이터베이스 서버는 삭제하고 이를 처리한다.

제안 방식의 시나리오에서 각각의 개체에 대한 정의는 다음과 같다.

- 사용자 : RFID 태그를 소유하고 있는 개체로써, 후방향성 데이터베이스 서버와 RFID 태그의 안전한 인증 과정을 수행한 후 제공받고자 하는 서비스를 요청하고 제공받는 개체.
- RFID 태그 : RFID 태그는 사용자가 소유하는 하드웨어 개체로써 사용자 프라이버시 정보를 내장하고 있으며, RF 리더기를 통해 후방향성 데이터베이스에 대한 인증뿐만 아니라 후방향성 데이터베이스에서 제공하는 서비스를 사용자에게 제공하는 개체.
- 후방향성 데이터베이스 서버 : RF 통신이 가능한 네트워크 기반의 이종 RFID들과 사용자들을 관리하고 서비스에 대한 요청이 있을 경우 서비스를 생성하고 관리하는 무선 RF 네트워크상의 신뢰 개체.

### 5.2 시스템 계수

다음은 안전하고 효율적인 이종 RFID 태그들의 관리

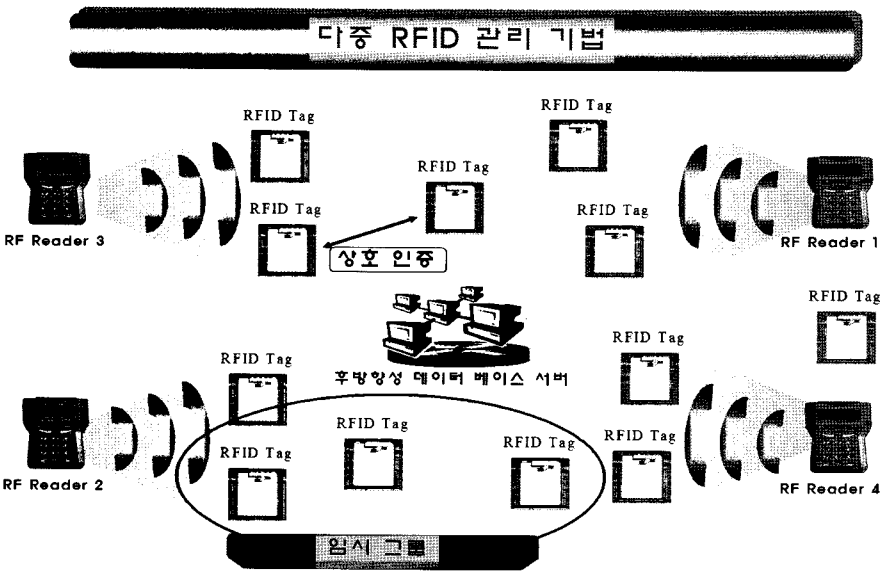


그림 1 제안방식 시나리오

방식을 위한 시스템 계수를 기술한다.

(* : D(후방향성 데이터베이스 서버), R(RF 리더기), T(RFID 태그))

$h_R()$, $h()$ : 리더기에 내장된 안전한 일방향 해쉬 함수, RFID 태그에 저장된 안전한 일방향 해쉬함수

$t_*$ : 타임 스탬프

$k$ : 후방향성 데이터 베이스 서버와 RFID 태그가 공유한 비밀키

*DID*, *RID* : 후방향성 데이터베이스 서버와 RF 리더기의 ID

$\oplus$ : eXclusive OR

$n$, $g$ : 공개 계수($n=pq$, $p$:소수, $q=q|p-1$)

$m_i$, $c_i$ : 후방향성 데이터베이스 서버에서 규정한 서비스 고유값인 $m_i$는 생성된 서비스를 위한 중간값인 $c_i$와 일대일 대응값($i=1,2,3,...,N$)

### 5.3 제안방식에서 사용되는 RFID 하드웨어 특성

본 논문에서 제안하는 RFID 태그의 하드웨어 특성은 다음과 같다.

- Standard Protocol : ISO 15693
- Carrier Frequency : 13.56MHz
- Baud Rate : 26Kbps
- Anti Collision : 50chips/s
- Unique Serial Number : 64bit
- EEPROM memory size : 8 bytes block
- Cryptographic Authentication : 160bits key length

### 5.4 가정 사항

안전하고 효율적인 이종 RFID 태그들의 관리 방식을 위한 가정 사항은 다음과 같다.

① RF 통신이 가능한 네트워크에 다수의 RFID 태그들을 소유하고 있는 서로 다른 사용자들이 존재한다.

② RFID 통신을 위해서 신뢰할 수 있는 후방향성 데이터베이스와 RFID 태그와 통신이 가능한 RF 리더기가 존재한다.

③ 후방향성 데이터베이스 서버와 RFID 태그는 공통된 해쉬 함수 $h_R()$과 $h()$를 공유한다.

④ 후방향성 데이터베이스 서버와 RF 리더기는 공통된 해쉬함수 $h_R()$을 공유한다.

⑤ 후방향성 데이터베이스 서버의 ID인 DID, RF 리더기의 ID인 RID는 모든 구성 개체에게 공개되어 있다.

⑥ RF 네트워크에 참여하는 모든 개체는 동기화가 이루어진 상태이다.

### 5.5 제안 프로토콜

제안 방식은 특수한 무선 RF 통신 환경에서 다수의 사용자가 RFID 태그들을 소유하고 이를 이용해 후방향성 데이터베이스 서버로부터 안전하고 효율적인 형태의 네트워크 관리를 통해 서비스를 제공받는 방식이며, 다음과 같은 흐름으로 구성된다.

**Step 1.** RFID 태그의 인증 및 등록

① RF 리더기는 RFID 태그에 통신 요청 Query와 $v_R$을 전송한다.

$$v_R = h_R(t_R)$$

② RFID 태그는 통신 요청 Query와 $v_R$을 수신한 후 후방향성 데이터베이스 서버와 공유한 키 $k$를 이용

해 임시 인증 정보인 TID(Temporary ID)를 생성한 뒤 이를 RF 리더기에 전송한다.

$$TID = h(k \| DID \| v_R)$$

③ RF 리더기는 $TID$를 수신한 뒤 $ID_R$을 다음과 같이 계산하여 $TID$, $v_R$, $ID_R$을 후방향성 데이터베이스 서버에 전송한다.

$$ID_R = (RID \oplus t_R)$$

④ RF 리더기로부터 전송된 $TID$, $v_R$, $ID_R$를 수신한 후방향성 데이터베이스 서버는 다음과 같은 검증 과정을 수행한다.

<검증 과정>

- 후방향성 데이터베이스 서버는 공개된 RID를 기반으로 $ID_R$을 검증한다. 검증이 올바른 경우 전송된 $v_R$과 $TID$와 후방향성 데이터베이스 서버에서 계산한 $v_R'$, $TID'$을 다음과 같이 비교 검증한다.

$$v_R' = h_R(t_R') \stackrel{?}{=} v_R,\ TID' = h(k \| DID \| v_R') \stackrel{?}{=} TID$$

검증이 올바르지 않는 경우 RFID 태그 인증 및 등록 중단 메시지를 RF 리더기에 전송하며, 재전송을 요구한다.

검증이 올바른 경우 후방향성 데이터베이스 서버는 랜덤수 $r_D (\in_U Z_n)$를 생성하고 다음을 계산하여 RF 리더기에 $ID_{T_1}$, $H_D$, $r_D$, $t_D$를 전송한 후 RFID 태그와 공유했던 비밀키 $k$를 갱신한다.

$$ID_{T_1} = h(k \| t_D \| r_D)$$

$$H_D = h_R(r_D \| t_D)$$

$$k_1 \leftarrow k \oplus t_D$$

⑤ $ID_{T_1}$, $H_D$, $r_D$, $t_D$를 수신 받은 RF 리더기는 $r_D$, $t_D$의 무결성을 검증하기 위해 $H_R = h_R(r_D' \| t_D')$를 계산하여 $H_R \stackrel{?}{=} H_D$임을 확인한다. 검증이 올바른 경우 $ID_{T_1}$, $r_D$, $t_D$를 RF 태그에 전송한다.

⑥ RFID 태그는 RF 리더기로부터 전송된 $ID_{T_1}$을 검증하고 검증이 올바른 경우 다음과 같이 $k$를 갱신한다.

$$k_1 \leftarrow k \oplus t_D$$

후방향성 데이터베이스와의 인증 및 등록 메시지 과정을 종료한다.

**Step 2.** 서비스 형태에 따른 그룹 초기화

각각의 RFID 태그들은 후방향 데이터베이스 서버에 자신의 서비스 형태를 등록하는 과정을 수행하며, 본 Step에서는 다수의 RFID들 중에서 $RFID_1$에 대한 설명만을 기술한다.

① 후방향성 인증서버는 랜덤하게 선택된 $\alpha_D \in_U Z_n$ ($n$과 서로소인 랜덤수)를 생성하여 $c_i$를 계산하고 각각의 $c_i$를 이용해 $V_i$를 생성한 후 $(V_1, m_1), (V_2, m_2), \ldots, (V_i, m_i)$를 모든 RFID 태그들에 브로드 캐스팅한다.

$$c_i = m_i^{\alpha_D} \bmod n$$

$$V_i = c_i \oplus t_{D_1}$$

② 임의의 RFID 태그 1은 후방향 데이터베이스 서버로부터 브로드 캐스팅된 $m_i$로부터 현재 RFID 태그 1이 제공받고자 하는 서비스를 선택한 후 (2개의 서비스($m_2$, $m_3$)를 선택할 경우) $V_2$, $V_3$(선택된 서비스 $m_2$, $m_3$에 해당되는 $V$)를 이용해 $d_{T_2}$, $d_{T_3}$를 계산 한 뒤 $d_{T_2}$, $d_{T_3}$, $t_T$를 RF 리더기에 전송한다.

$$d_{T_2} = h(V_2 \oplus k_1 \oplus t_T)$$

$$d_{T_3} = h(V_3 \oplus k_1 \oplus t_T)$$

③ $d_{T_2}$, $d_{T_3}$를 수신한 RF 리더기는 Step 1 과정에서 생성된 $ID_R$을 이용해 $s_R$을 계산한 뒤 $s_{R_{(2,3)}}$, $d_{T_2}$, $d_{T_3}$, $t_T$를 후방향성 데이터베이스 서버에 전송한다.

$$s_{R_{(2,3)}} = h_R(ID_R \| d_{T_2} \| d_{T_3})$$

④ 후방향성 데이터베이스 서버는 RF 리더기로부터 전송된 $s_{R_{(2,3)}}$을 검증한다.

<검증 과정>

$V_2' = c_2 \oplus t_{D_1}$, $V_3' = c_3 \oplus t_{D_1}$, $d_2' = h(V_2' \oplus k_1 \oplus t_T')$, $d_3' = h(V_3' \oplus k_1 \oplus t_T')$를 계산한 뒤 $s_{R_{(2,3)}}' = h_R(ID_R \| d_{T_2}' \| d_{T_3}')$일 때 $s_{R_{(2,3)}} = s_{R_{(2,3)}}'$이면 전송된 값을 안전하게 저장한다.

이상의 과정이 올바른 경우 후방향성 데이터베이스 서버는 $RFID_1$에 대한 서비스 형태를 임시그룹 A에 등록하고 임시 그룹에 대한 비밀 정보 값인 $\tau_1$을 생성한다.

$$d_{D_2} = V_2 \oplus t_{D_1} \oplus t_T$$

$$d_{D_3} = V_3 \oplus t_{D_1} \oplus t_T$$

$$\tau_1 = h((k_1 \| t_T) \oplus (d_{D_2} \| d_{D_3}))$$

생성된 임시 정보값 $\tau_1$을 seed 값으로 하여 해쉬 체인을 생성하고 $h^2(\tau_1)$를 생성하고 이를 임시 그룹에 대한 $RFID_1$의 비밀 값으로 저장한 뒤 RF 리더기에 $h_D$, $t_{D_1}$, $h_{D_1}$을 전송한다.

$$h_D = h(d_{D_2} \| d_{D_3} \| t_T)$$

$$h_{D_1} = h_R(h_D \| t_{D_1})$$

※ 단일 해쉬체인(Hash Chain)은 seed 값 $x$를 기반으로 일방향 해쉬함수 $h()$를 이용한 계산 값들의 체인인 $h_1(x), h_2(x), \ldots, h_i(x), \ldots, h_n(x)$를 의미한다. 여기에서 $h_i(x)$는 $x$에 해쉬함수를 $i$번 반복 적용한 값으로 $h_i(x)$로부터 $h_{i+1}(x)$를 계산할 수 있으나 $h_{i-1}(x)$를 계산할

수 없다. 이는 일방향성 해쉬 함수의 특성에 기인한다.

⑤ $h_D$, $t_{D_1}$, $h_{D_1}$을 수신한 RF 리더기는 $h_{D_1}$의 무결성을 검증하고 검증이 올바른 경우 $h_D$, $t_{D_1}$을 $RFID_1$에 전송한다.

⑥ $RFID_1$은 $h_D$, $t_{D_1}$을 수신한 후 다음을 검증하여 전송 정보에 대한 무결성과 임시 정보 데이터를 확인한다.

<검증 과정>

- $RFID_1$에서 선택한 서비스에 따른 $V_2$, $V_3$를 이용해 $d_{T_2}$, $d_{T_3}$를 계산한다.

$$d_{T_2} = V_2 \oplus t_{D_1} \oplus t_T,\ d_{T_3} = V_3 \oplus t_{D_1} \oplus t_T$$

계산된 $d_{T_2}$, $d_{T_3}$를 기반으로 $h_D$의 무결성을 검증하고 검증이 올바른 경우 $\tau_1'$을 계산하여 임시 그룹 정보의 $\tau_1$을 생성하고 이를 안전하게 저장한다.

$$\tau_1 = h((k_1 \| t_T) \oplus (d_{T_2} \| d_{T_3})) = \tau_D$$

**Step 3.** 임시 그룹 설정

후방향성 데이터베이스 서버는 Step 2에서 $RFID_1$의 비밀 정보 $\tau_1$를 기반으로 하여 같은 서비스를 요구하는 $RFID$ 태그들이 일정한 개수 이상이거나, 동일한 서비스에 대한 빈도가 높을 경우 해당 $RFID$ 태그들의 임시 그룹을 위한 과정을 수행한다.

① 후방향성 데이터베이스 서버는 동일한 서비스를 요구하는 $RFID$ 태그들($RFID_1$, $RFID_2$, $RFID_3$)의 비밀정보를 $(\alpha_1, \alpha_2, \alpha_3)$으로 정의하고 임시 그룹 설정을 위한 요청 메시지를 RF 리더기에 전송하고, RF 리더기는 이를 $RFID_1$, $RFID_2$, $RFID_3$에 각각 전송한다.

② RF 리더기로부터 전송받은 $RFID_1$은 임시 그룹키 정보 $K_{G_{key_1}}$을 다음과 같이 계산하여 $ID_{T_1}$, $v_{T_1}$을 RF 리더기에 전송한다.

$$K_{G_{key_1}} = h(k_1 \| t_D)$$

$$v_{T_1} = h_R(\tau_1 \| K_{G_{key_1}} \| t_{T_1})$$

③ $ID_{T_1}$, $v_{T_1}$을 전송받은 RF 리더기는 $t_{R_1}$을 생성하여 $ID_{T_1}$, $v_{T_1}$, $t_{R_1}$을 후방향성 데이터베이스 서버에 이를 전송한다.

④ 후방향성 데이터베이스 서버는 RF 리더기로부터 전송받은 $ID_{T_1}$, $v_{T_1}$, $t_R$을 기반으로 $RFID_1$으로부터 전송된 정보를 검증한다.

<검증 과정>

$K_{G_{key_1}}' = h(k_1 \| t_D)$를 계산하여 $K_{G_{key_1}}' \stackrel{?}{=} K_{G_{key_1}}$를 검증하고 $v_{T_1}$의 무결성을 확인한다.

이상의 과정은 $RFID_2$, $RFID_3$와 동일하게 수행하고 이상의 검증 과정이 올바른 경우 후방향성 데이터베이스 서버는 각각의 $RFID$ 태그들에게서 전송된 정보를 이용해 $RFID_1$을 위한 임시 그룹 $A(RFID_1, RFID_2, RFID_3)$를 설정하고 이에 대한 그룹키를 생성하여 $v_{D_2}$, $h_{D_2}$, $t_{D_2}$를 RF 리더기에 이를 전송한다.

$$v_{D_2} = (h(K_{G_{key_2}} \oplus k_2) \| h(K_{G_{key3}} \oplus k_3)) \oplus h(\alpha_1 \| ID_{T_1})$$

$$TK_{AGroup} = v_{D_2} \oplus v_{T_1}$$

$$h_{D_2} = h_R(TK_{AGroup} \| v_{D_2} \| t_{D_2})$$

⑤ RF 리더기는 전송된 $v_{D_2}$, $h_{D_2}$, $t_{D_1}$에서 ② 과정에서 $RFID_1$으로부터 전송되었던 $v_{T_1}$을 이용해 $v_{D_2} \oplus v_{T_1} = TK_{AGroup}'$, $h_{R_2}' = h_R(TK_{AGroup}' \| v_{D_2} \| t_{D_2}) \stackrel{?}{=} h_{D_2}$를 확인한다. 검증이 올바른 경우 $v_{D_2}$, $t_{D_2}$를 $RFID_1$에 전송한다.

⑥ $v_{D_2}$, $t_{D_2}$를 전송받은 $RFID_1$은 다음의 검증 과정을 통해 임시 그룹 A의 그룹키 $G_{key}$를 생성한다.

$$x_{T_1} = h(\alpha_1 \| ID_{T_1})$$

$$(v_{D_2} \oplus x_{T_1}) \| h(K_{G_{key_1}} \oplus k_1) =$$

$$(h(K_{G_{key_2}} \oplus k_2) \| h(K_{G_{key3}} \oplus k_3)) \| h(K_{G_{key_1}} \| k_1)) = G_{key}$$

이상의 과정을 $RFID_2$, $RFID_3$도 동일하게 수행하여 $G_{key}$를 획득한다.

**Step 4.** 임시 그룹의 통신 단계

다음은 서비스 등록 이후 임시 그룹이 완료된 $RFID$ 태그들이 동일한 형태의 서비스를 제공받기 위해 후방향성 데이터베이스 서버에 서비스를 요청하는 단계이다.

① $RFID_1$은 서비스 요청을 위해 $S_{request}$, $ID_{T_1}$, $w_{T_1}$, $t_{T_2}$를 RF 리더기에 전송한다.

$$w = h(G_{key} \| t_{T_2})$$

② RF 리더기는 다음을 계산하여 $ID_{T_1}$, $w_R$을 후방향성 데이터베이스 서버에 전송한다.

$$w_R = h_R(w_{T_1})$$

③ 후방향성 데이터베이스 서버는 $ID_{T_1}$을 DB 테이블에서 검색하여 해당 $RFID$ 태그에 해당되는 $G_{key}$를 확인하고 이에 해당되는 서비스(ex: $m_2$) $S_{responce_{m_2}}$를 RF 리더기에 전송한다.

④ RF 리더기는 $S_{responce_{m_2}}$를 $RFID_1$에 전송한다.

**Step 5.** 임시 그룹의 삭제

임시 그룹으로 형성된 $RFID$ 태그들이 임의의 개수 이하가 될 경우 현재 형성된 임시 그룹을 삭제하는 과정을 후방향성 데이터베이스 서버는 수행한다.

① 후방향성 데이터베이스 서버는 임시 그룹 형성을 위

해 저장한 *RFID* 태그들의 임시 그룹 정보 $K_{G_{temp}}^{T}$ 의 정보를 DB 테이블에서 추출한다.

② 후방향성 데이터베이스 서버에서 추출된 값에서 임시 그룹 A에 해당되는 *RFID* 태그들에 그룹 삭제에 대한 메시지를 멀티 캐스트 한다.

$$D_{group_A} = (ID_{T_1} \| ID_{T_2} \| ID_{T_3})$$

③ 멀티 캐스트된 정보를 수신한 *RFID*태그들은 자신이 포함된 임시 그룹의 상태를 확인하고 임시 그룹에 대한 정보 삭제를 수신한다.

이상의 과정으로 동일한 공간에 이종 *RFID* 태그들을 위한 안전하고 효율적인 네트워크 관리 방식을 수행한다.

## 6. 제안 방식 분석

본 장에서는 제안된 이종 RFID 태그들을 위한 안전하고 효율적이 네트워크 관리 방식을 기존 방식과 비교 분석하고자 한다.

### 6.1 안전성 분석

① ACIN : 제안된 방식은 서로 다른 서비스를 제공하는 수동형 RFID 태그들이 동일한 공간에 존재할 경우에 초기 후방향성 데이터베이스 서버와 공유한 키 $k$를 기반으로 임시적인 RFID 태그의 ID인 *TID*를 생성하고 인증 과정을 수행한다. 또한 타임 스태프 $t$를 이용해 재전송 공격에 안전성을 유지할 수 있으며, 안전한 해쉬 함수 $h()$를 이용해 전송 데이터의 무결성을 보장할 수 있다. 그러나 전송 데이터의 기밀성과 부인 봉쇄 서비스는 제공하지 않는다.

② 채널 보안 : RFID 태그 인증 프로토콜에서 초기 쿼리에 대한 수정 공격이나 전송 데이터의 무결성 보장을 위해서 공유한 키 $k$를 이용해 초기 쿼리에 대한 수정 공격이 수행된다 할지라도 타임스탬프 $t$와의 계산을 통해 생성된 *TID*가 시간 함수에 따라 변화되어 초기 쿼리에 대한 수정 공격에 안전성을 유지할 수 있을 뿐만 아니라 인증 및 관리 프로토콜에서 전송 정보의 무결성 보장을 위해 사용되는 RFID 태그의 하드웨어적 특성인 160bit의 키 길이를 갖는 해쉬 함수의 이용이 가능하다.

③ 그룹 보안 서비스 : 제안된 방식은 기존의 단일한 RFID 태그만을 고려한 인증 방식과 비교하여 보았을 경우 안전성 측면에서 동일한 형태의 서비스를 제공한다. 그러나 인증 이후의 확장된 형태의 RFID 관리 측면에서 분석하였을 경우 서비스 형태에 따른 고유값은 $c$에 의해 임시적인 그룹을 설정하고 RFID 태그와 초기 공유한 키 $k$를 이용해 이를 검증함으로써 함으로써 동일한 서비스를 제공받는 RFID 태그들에 대한 안전한 보안 서비스를 제공하였다.

④ 그룹에 대한 관리 : 제안된 방식은 서비스가 다양하게 변화할 수 있는 동일한 환경의 이종 RFID 태그들을 고려하기 위하여 임시적인 그룹을 생성하고 서비스가 종료될 경우 후방향성 데이터베이스 서버에서 이를 삭제함으로써 그룹에 대한 관리가 보다 효율적으로 이루어지도록 하였다.

⑤ 구현의 효율성 : 제안된 방식은 수동형 RFID 태그를 기반으로 구성함으로써 현재의 RFID 태그의 물리적인 한계성을 고려한 방식이다. 따라서 낮은 가격의 태그에 대한 적용이 가능할 뿐만 아니라 구체적인 하드웨어적 구성을 제시함으로써 보다 현실적인 구현이 가능하다.

### 6.2 성능 분석

동일한 환경의 다양한 RFID들이 존재할 경우 하나의 후방향성 데이터·베이스 서버에서 이를 관리함으로써 하나의 $a$-ary 트리 형태로 구성될 수 있다. 하나의 네트워크에서 RF 리더기의 수를 $N$이라 하고 임시 그룹 통신을 수행하는 RF 리더기의 수를 $RF(w)$이라고 할 때 height $h$는 $\log_a RF$이다.

이에 메시지의 수에 따른 텀(term)에서의 통신비용을 $M^{tree}(w)$라 정의할 때에 전체 비용은 $M^{tree}(w) \le hN(w)$이다. 그러나 RFID 네트워크에서 height h는 일반적으로 3을 의미하므로 전체 비용은 $M^{tree}(w) \le 3N(w)$로 정의할 수 있다. 따라서 후방향성 데이터베이스 서버에서 임시 그룹을 위한 공개 메시지에 대한 내용은 최소 3개 이상의 메시지를 활용한다. 이에 전체 비용 $M^{tree}(w) \le \sum_{i=1}^{h} a^i = \frac{a}{a-1}(RF-1)$로 정리할 수 있으며, 최소 $M^{tree}$에 대한 값은 $\min(3N(w), \frac{a}{a-1}(RF-1))$이며 최대값 $M_{\max}^{tree}(w)$는 $\frac{a}{a-1}(RF-1)$로 정리할 수 있다. 제안된 방식의 전체 통신비용 $M^{tree}$는 $a=3$, $RF$가 10일때 $M^{tree}(w) \le 13.5$이며, 최소 $M^{tree}$는 $\min(3N(w),18))$, 최대 $M_{\max}^{tree}(w)$는 13.5이다.

BFT(Byzantine Fault Tolerance) 방식에서 제시한 알고리즘을 기반으로 $m$개의 악의적인 RFID 태그가 존재할 경우 네트워크 토폴로지(그리드, 트리)에 상관없이 각각의 공통된 인증 메시지를 최소한 $m+1$개 전송 받았을 때의 통신비용을 $M^{mc}(w) \ge (m+1)N(w)$로 정의하고 있다. 따라서 *RFID* 태그의 개수를 10개이고 악의적인 RFID 태그가 이의 10%임을 가정할 때 가정할 경우 $\log_3 10 \approx 2$이고 $\frac{a}{a-1}RF = 15$이므로 $m$개의 악의적인 RFID 태그가 존재할 경우의 최소 통신비용 $M^{mc} \ge 11N(w)$

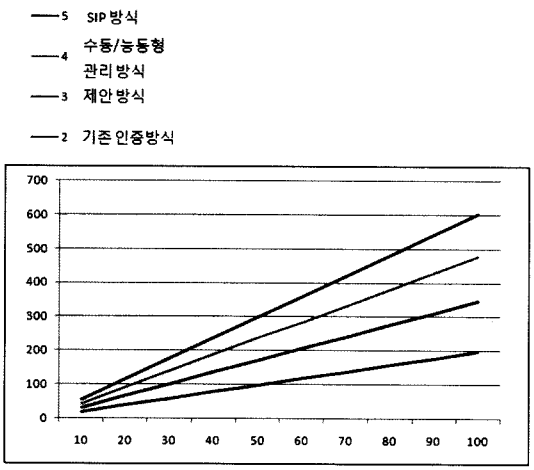


그림 2 전체 통신비용

가 된다. 따라서 제안 방식과 기존 방식에 대한 통신 비용을 그림 2와 같이 분석하였다. 그림 2와 같이 기존의 단일한 인증 방식에 비해서는 통신 횟수 증가에 따라 비용이 상승되어 비효율적이나 관리적인 측면에서 SIP 방식 및 수동형 관리 방식과 비교할 경우 전체 통신비용이 저하되는 효율성을 갖는다.

## 7. 결 론

유비쿼터스 환경을 구체화하기 위한 핵심적인 기술은 네트워크 분야 이외에 소형화된 디바이스를 이용한 인증 기술을 제시할 수 있다. 특히, RFID는 기존의 바코드 체계를 대체할 새로운 기술로 많은 각광을 받고 있으며, 이에 대한 연구는 매우 활발히 이루어지고 있으나 RFID의 특성상 저전력 수동적 형태의 구성으로 인해 사용자 프라이버시 보호에 대한 문제를 내포하고 있어 이를 보완하기 위한 연구가 절실히 요구되는 실정이다. 국외에서는 MIT를 중심으로 RFID에 대한 연구의 중요성을 인식하고 보안성이 강화된 연구를 활발히 진행하고 있으나 RFID 태그에 대한 인증 이후의 다양한 네트워크의 적용과 이를 위한 관리적인 차원에서의 연구는 매우 미흡한 실정이다. 따라서 본 논문에서는 동일한 환경에서 다양한 RFID 태그가 공존할 경우 발생할 수 있는 보안 취약성을 보완하기 위하여 수동형 RFID 태그 기반의 안전하고 효율적인 형태의 네트워크 관리 방식을 제안하였다. 특히, 안전한 RFID 태그 인증 이후에 동일한 서비스를 제공 받고자 하는 RFID 태그들을 임시 그룹화하여 후방향성 데이터베이스 서버에서 동일한 서비스를 제공할 수 있도록 하였다. 이는 기존의 연구에서 고려하지 않았던 RF 네트워크의 새로운 방식이라 할 수 있다. 향후 본 논문에서 고려하지 않았던 탈퇴 RFID 태그 및 공격자 RFID 태그에 대한 안전성 확보 및 네트워크 구성시 발생할 수 있는 통신 효율성을 향상시키기 위한 추가적인 연구가 이루어질 예정이다.

## 참 고 문 헌

[1] Avoine G., and Oechslin P., "RFID Traceability: A Multilayer Problem," Financial Cryptography - FC'05, LNCS, Springer, 2005.

[2] RFID Journal. Gillette to Purchase 500 Million EPC Tags, http://www.rfidjournal.com

[3] Bono, S., Green, M,., Stubblefield, A., Julels, A., Rubin, A., and Szydlo, M., "Security Analysis of a Cryptographically-Enabled RFID Device," In USENIX Security, 2005. (Available at http://rfidanalysis.org/.)

[4] Castro, Miguel and Barbara Liskov, "Practical Byzantine Fault Tolerance," Operating Systems Design and Implementation, 1999, (http://www.pmg.lcs.mit.edu/~castro/osdi99_html/osdi99.html)

[5] Junichiro S., Jae-Cheol R and Kouichi S., "Enhancing privacy of Universal Reencryption scheme for RFID Tags," *EUC 2004*, vol.3207 LNCS, pp.879-890, Dec. 2004.

[6] MIT Auto-ID Center. http://www.autoidcenter.org

[7] Su-Mi L., Young-Ju H., Dong-Hoon L., and Jong L., "Efficient Authentication for Low-Cost RFID systems," *ICCSA05*, vol.3480 LCNS, pp.619-629, May 2005.

[8] 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/spcrfid.pdf

[9] Dimitriou T., "A lightweight rfid protocol to protect against traceability and cloning attacks," *IEEE*, SECURECOMM, 2005.

[10] Gilbert, H., Sibert, H., and Robshaw, M., "An Active Attack Against a Provably Secure Lightweignt Authentication Protocol," Preliminary Version, 2005.

[11] Hung-Yu Chien and Che-Hao Chen, "Mutula authentication protocol for RFID conforming to EPC Class 1 Generation 2 Standards," *Computer Standards & Interfaces*, vol.29, pp.254-259, Feb., 2007.

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

[13] Sanjay E.Sarma, "Towards the five-cent Tag," Technical Report MIT-AUTOID-WH006, MIT Auto ID Center, 2001. Available from http://www.autoidcenter.org

[14] Juels A., "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.
[15] Juels A., "Authentication Pervasive Devices with Human Protocols," Crypto 2005, Aug. 205.
[16] Jeong-kyu Y., Ren K., and Kwan-gio K., "Security and Privacy on Authentication Protocol for Low-cost RFID," Symposium on Cryptography and Information Security, Jan., 2005.
[17] Ohkubo M., Suzuki K., and Kinoshita S., "Cryptographic Approach to "Privacy-Friendly" Tag" RFID Privacy Workshop@MIT, Nov, 2003.
[18] Bringer J., Chabanne H., and Dottax E., "HB++ : a Lightweight Authentication Protocol Secure Against Some Attacks," IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU, 2006.
[19] Henrici D., and Paul M., "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," PerSee'04 at IEEE PerCom. pp.149-153, 2004.
[20] Jules A., and Pappu R., Squealing E., "Privacy protection in RFID-enabled banknotes, In processing of Financial Cryptography," FC'03, vol.2742 LNCS, pp.103-121, Sep 2003.
[21] D.N. Duc, J. Park, H. Lee and K. Kim, "Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning," The 2006 Symposium on Cryptography and Information Security, 2006.
[22] Katz J., and Ji-Sun S., "Prallel and Concurrent Security of the HB and HB+ Protocols," Cryptology ePrint Archive : Report 2005/461 (to appear in the preceedings of Eurocrypt 2006).
[23] D-H, Seo, I-Y Lee, "A Study on Authentication and Management Scheme of RFID Tag for Ubiquitous Environment," *Journal of the Korean Institute of Information Security and Criptology*, vol.16, no.2, pp.81-94, 2006.
[24] Kideok Cho, Sangheon Pack, Taekyoung Kwon, and Yanghee Choi, "SRMS: SIP-based RFID Management System," in *Proc. IEEE International Conference on Pervasive Services (ICPS) 2007*, Istanbul, Turkey, July 2007.

서 대 희
2003년 순천향대학교 대학원 전산학과 졸업(석사). 2006년 순천향대학교 대학원 전산학과 졸업(박사). 2007년 Post-Doc of Howard University. 2008년 현재 이화여자대학교 연구교수. 관심분야는 네트워크 보안, 근거리 무선 통신 보안, 보안성 평가, 유비쿼터스 컴퓨팅

백 장 미
2003년 순천향대학교 대학원 전산학과 졸업(석사). 2006년 순천향대학교 대학원 전산학과 졸업(박사). 2007년 Post-Doc of Howard University. 2008년 현재 순천향대학교 시간강사. 관심분야는 임베디드 시스템, u-Healthcare, 네트워크 관리, 유비쿼터스 컴퓨팅

조 동 섭
1981년 서울대학교 전기공학과 졸업(석사). 1986년 서울대학교 컴퓨터공학과 졸업(박사). 1985년~현재 이화여자대학교 컴퓨터학과 교수. 1996년~1997년 미국 Univ. of California, Irvine Dept, of ECE Visiting Scholar. 관심분야는 임베디드 보안, 웹서비스 아키텍처, 휴먼 컴퓨팅, 웹서버 엔지니어링