사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템

(A Multi-Agent Scheme Considering User's Mobility RFID based on Knowledge Management System)

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

요 약 유비쿼터스 컴퓨팅의 핵심 기술로 무선 Ad Hoc네트워크가 거론되고 있으며, 센서 네트워크의 일환인 스마트 태그 기술이 최근 활발히 논의되고 있다. 따라서 이에 관한 보안을 검토하여 보는 것도 향후 전개될 유비쿼터스 컴퓨팅에서의 현실화를 앞당길 수 있다. 따라서 센서 네트워크의 일환인 스마트 태그 기술을 이용한 RFID 기술이 최근 각광을 받고 있다.

특히, 다양화된 정보를 관리하는 지식 관리시스템에 RFID 태그를 적용할 경우 정보의 이동성과 관리의 편의성을 제공할 수 있어 차세대의 능동형 지식 관리 서비스를 사용자에게 제공하는 장점이 있다. 따라서 본 논문에서는 기존의 지식 관리시스템과는 차별화된 형태의 이동성을 고려한 지식 관리 시스템의 안전한 구성 방식을 제안하고자 한다. 제안 방식은 멀티 에이전트에서 사용자의 인증과 권한 정보를 설정하고 사용자 정보에 기반을 둔 그룹화를 통해 사용자의 이동성을 고려한 지식 서비스를 제공하며, 지속적인 정보 제공을 위하여 서비스의 가용성을 보장한다.

키워드 : 유비쿼터스 환경, 지식 관리 시스템, RFID 태그, 멀티 에이전트, 가용성

Abstract The Wireless Ad Hoc network is discussed as a core technology for ubiquitous computing, and the smart tag technology is currently being actively discussed as a part of the sensor network. Thus, considering its security may advance the realization of ubiquitous computing. RFID (Radio Frequency Identification) technology using the smart tag technology as a part of the sensor network is currently in the limelight. In particular, when RFID is applied to a knowledge management system managing various data, data mobility and management convenience are ensured and automated knowledge service can be provided to users. Accordingly, this paper to proposed a secure scheme for mobility knowledge management systems using multi-agents differentiated from the existing knowledge management systems. Specifically, the proposed scheme designates user's authentication and privilege information in multi-agents and provides effective knowledge service through grouping based on user information. Moreover, even user's movement, the proposed scheme ensures service availability and provides continuous information through communication with multi-agent systems.

Key words : Ubiquitous Environment, Knowledge Management System, RFID Tag, Multi Agent, Availability

·본 연구는 2009년도 2단계 두뇌한국(BK) 21 사업에 의하여 지원되었음

† 정 회 원 : 한국전자통신연구원 선임 연구원
dhseo@etri.re.kr
†† 정 회 원 : 순천향대학교 컴퓨터학부 시간강사
bjm1453@sch.ac.kr
††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
dscho@ewha.ac.kr

논문접수 : 2009년 7월 9일
심사완료 : 2009년 12월 16일

정보과학회논문지: 정보통신 제37권 제2호(2010.4)

1. 서 론

인터넷의 급속한 발전은 유비쿼터스 환경으로의 전환을 가져왔으며, 이를 기반으로 비즈니스 모델화가 활발히 진행되고 있다. 특히, 수많은 다양한 정보들이 생성되고 폐기되는 가운데 사용자의 정보 욕구가 증대되어 가면서 많은 정보들을 보다 효율적으로 관리하고 제공받기 위한 지식 관리 시스템이 중요시되고 있다. 지식 관리 시스템은 주로 기업에서 활용되고 있으며, 기업 경영을 지식이라는 관점의 전환에서 활발히 적용되고 있으며, 기존의 기업정보 서비스는 정형화된 정보만을 관리한다. 따라서 이를 통해 주된 의사 결정이나 인적 자원에 정보를 제공하는 것을 목적으로 수행되어 왔으며, 비정형화된 데이터를 자산 내에 축적, 활용함으로써 보다 효율적인 기업의 의사 결정과 정보의 관리를 목적으로 한다[1].

그러나 사용자 주변의 통신 기기의 다변화와 정보의 다양성에 의해 수동적으로 정보만을 제공받던 사용자들이 정보의 욕구 증대와 더불어 능동적으로 정보의 생성, 배포, 폐기에 이르는 생명주기에 직접적으로 참여가 이루어짐에 따라 기업적인 형태가 아닌 공개적인 형태의 지식 관리 시스템에 대한 연구가 시급히 요구되고 있다. 또한 공개된 지식 관리 시스템의 특성상 비인가 된 공격자에 대한 안전성 확보뿐만 아니라 자동화된 서비스를 통해 사용자의 프라이버시 보호와 능동적인 서비스는 사용자 중심의 유비쿼터스 환경에서 절실히 요구되는 서비스이다.

이에 본 논문에서는 RFID(Radio-Frequency Identification)를 이용한 멀티 에이전트를 기반으로 하는 안전하고 효율적인 형태의 지식 관리 시스템을 제안하고자 한다. 본 논문의 2장에서는 지식 관리 시스템과 RFID의 개요에 대해서 기술하고, 3장에서는 기존의 지식 관리 시스템에 대한 취약성과 보안 요구사항을 설명한다. 4장에서는 RFID를 이용한 지식 관리 시스템의 멀티 에이전트를 제안하고 5장에서는 3장에서 제시한 보안 요구사항을 기반으로 기존 방식과의 비교 분석을 수행한 뒤 6장에서 결론 및 향후 연구 방향을 제시하고자 한다.

2. 기술 개요

본 장에서는 유비쿼터스 환경에서 지식 관리 시스템과 RFID의 개요에 대해서 기술하고자 한다.

2.1 유비쿼터스 환경에서 지식 관리 시스템의 개요

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[1].

특히, 새로운 컴퓨팅 환경에서 정보의 다양성은 사용자의 프라이버시와 같이 중요하고 필수적인 정보뿐만 아니라 모든 사용자들이 공유할 수 있는 공개적인 정보도 포함되어 있다. 따라서 모든 정보들에 대해서 정보의 재사용뿐만 아니라 정보를 관리하고 저장 및 합법적인 재사용을 통해 보다 효율적으로 지식을 공유할 수 있도록 하는 것이 지식 관리 시스템이다.

지식 관리 시스템은 처음 미국의 캐너기멜론대학의 ZOG 연구에 결과를 기반으로 제안된 시스템으로 기업 내부에서 비정형화된 정보를 기반으로 내부 사용자들의 의견 교환을 통해 최종적인 결과를 도출하기 위한 인적 관리 시스템에서 시작되었다. 그러나 연구들은 주로 개별적인 지식을 체계화하고 보다 효율적인 공유가 이루어지는데 목적이 있는 반면 이로 인해 발생할 수 있는 보안적인 문제점이나 새로운 환경에의 적용성에 대해서는 고려되지 않고 있다. 따라서 능동적인 사용자가 중심이 되는 유비쿼터스 환경에서는 사용자의 프라이버시 보호를 위한 별도의 서비스와 더불어 자동화된 지식 서비스를 제공하기 위한 체계적인 구조가 반드시 요구된다.

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 있다.

RFID는 현재 저주파(125khz)·고주파(13.56MHz)의 전자태그 중심으로 60cm이내 근거리에서는 출입통제, 교통카드 등에 인식기능(Identification)중심으로 사용되고 있으며, 극초단파(433MHz, 900MHz) 대역에서는 유통·물류 분야를 중심으로 활성화가 이루어지고 있다. 따라서 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 확대되고 있다[2].

3. 기존 방식 및 보안 요구사항 분석

본 장에서는 기존의 지식 관리 시스템에 대해서 분석하고 새로운 환경에 적합한 지식 관리 시스템이 제공해야 하는 요구사항을 제시하고자 한다.

3.1 PBKM 방식

본 논문은 Shouhuai Xu(외 1명)이 제안한 방식으로 안전한 지식 관리를 위한 PBKM(Privacy-preserving

and Breaching-aware Knowledge Management)이다. 제안된 방식은 표준 보안 메커니즘과 같이 접근제어, 사용자 프라이버시 보호를 제공하고 각각의 지식 자원에 의한 연결성을 갖고 하위 개체와의 상호 호환성을 제공하는 프레임워크이다. 특히, 제안된 프레임워크는 각각의 컴포넌트별로 상호 연결성과 기존이 보안 서비스 및 데이터 마이닝 기술 등을 갖고 있으며, 이를 통해 각각의 정보에 대해서 분류와 안전한 서비스가 가능하도록 하였다. 관리적인 측면에서 PBKM은 다양한 규칙을 규정하고 상호 연결성을 갖는 하위 개체에 서로 다른 정책을 부여함으로써 안전한 지식 관리가 가능하도록 하였다[3]. 그러나 본 방식의 경우 다음과 같은 보안 취약성을 내포하고 있다.

① 적용의 한계성 : 제안된 방식은 특수한 형태의 컴포넌트를 제시하고 이를 기반으로 PBKM 메커니즘을 제안하였다. 제안된 컴포넌트는 트리나 규칙을 기반으로 개체를 관리하는 컴포넌트와 각각의 그룹들에 대한 자동화된 규칙을 적용하는 컴포넌트, 상호 그룹간의 안전성 확보를 위한 보안 컴포넌트를 기존의 지식 관리 시스템에 추가하였다. 그러나 이는 기존의 지식 관리 시스템에 범용적으로 적용될 수 없으며, 각각의 모든 개체 및 구성을 새롭게 해야 되는 한계성이 있다. 따라서 범용적으로 사용이 가능한 개체로 구성되어야 한다.

② 그룹 관리의 효율성 : 제안된 방식은 멀티 파티 프로토콜을 기반으로 각각의 사용자들에 대한 안전성 확보를 제공하였다. 즉, 그룹 $P_i \in P_1,...,P_m$ ($m \le l$, l은 지식 관리 시스템에서 선택된 그룹, $P_1,...,P_l$)에서 $f: x_1,...,x_l \mapsto k_1,...,k_l$ 일 때 $k_i (1 \le i \le l)$에 대한 안전한 출력($P_i(k_i = \perp)$)을 통해, 각 그룹들 간의 정보를 제공받도록 하였다.

그러나 사용자의 이동성이 활발한 경우 그룹들간의 통신 및 초기화가 빈번히 발생되고 이를 위해서는 별도의 키 설립 및 그룹 관리 과정이 요구된다. 따라서 그룹 관리의 효율성을 제공하기 위한 새로운 형태의 관리 프로토콜이 요구된다.

③ 서버에 대한 안전성 : PBKM의 지식 서버는 정보를 요구하는 사용자로부터 추가적인 서비스가 요구될 경우 지식 관리 서버로부터 정보를 추출하거나 학습을 통하여 제공한다. 사용자의 요구 정보 K에 대하여 f_K를 지식 서비스라고 하고 공격자에 의해 정의된 정보 K'에 대응되는 서비스를 $f_{K'}$이라고 한때 $\Pr(f_{K'}'(.) = f_K(.)) > \sigma$ (σ는 K의 지식 단계, α는 중요 레벨 등급)이며, $0 \le \sigma \le 1$, $0 \le \alpha \le 1$일 때 $\Pr(f_{K'}'(.) = f_K(.))$이다. 따라서 지식 관리 서버는 모든 개체로부터 안전성을 확보해야 하지만 이를 위한 별도의 보안 서비스가 제공되지 않는 취약성이 있다.

④ 관리 개체의 안전성과 효율성 : 지식 관리 시스템에서 사용자는 자동화되고 안전한 형태의 서비스를 제공받고자 한다. 따라서 지식 관리 시스템에서 사용되는 함수들에 대한 안전성 확보와 더불어 프로토콜의 안전성 확보는 전체적인 지식 관리 시스템의 관리를 위해서 반드시 요구된다. 또한 관리적인 측면에서 효율성을 제공하기 위한 그룹 형태의 관리와 서비스를 제공해야 한다. 그러나 본 방식에서는 그룹에 대한 안전성과 관리의 효율성을 위한 그룹에 대한 서비스가 제공되지 않는다.

3.2 CTP 방식

본 방식은 기밀성, 신뢰성, 프라이버시 보호(Confidentiality, Trust and Privacy)를 제공하는 SKM(Secure Knowledge Management)을 제안하였다. 제안 방식은 접근 제어 기술을 기반으로 신뢰적인 관리 방식을 통해 프라이버시 제어를 제공하는 지식 관리 시스템이다. CTP 방식은 RBAC(Role-Based Access Control) 방식을 이용하여 통신의 기밀성을 보장하고 제어 방식을 RBAC에 적용하는 UCON(RBAC and Usage Control)을 통해 신뢰적인 관리와 각 개체들 간의 협상에서 발생할 수 있는 보안 위협에 대해서 안전성을 유지하도록 하였다. 또한 개체간의 협상과 관리를 위해서 안전한 키를 설정하고 이를 기반으로 지식 공유와 통신의 안전성을 제공한다[4]. 그러나 본 방식의 경우 다음과 같은 보안 취약성을 내포하고 있다.

① 키의 생성과 분배 : 제안된 방식은 안전한 지식 관리 시스템을 위하여 TN(Trust-Negotiation)을 기반으로 각각의 파티별(사용자 혹은 프로세스) 웹 기반 트랜잭션에 초점을 맞추었다. 그러나 시멘틱 웹과 데이터 마이닝 기술을 기반으로 정보를 획득하고 정보를 가공시 별도의 P3P(Platform for Privacy Preferences)가 요구되며, 안전한 통신을 위한 보안 키 설정을 제공하지 못한다. 따라서 데이터 형식이나 활용에 따라 개인 프라이버시 정보가 요구되는 정보일 경우 안전성 확보를 위한 키 생성 및 분배가 반드시 요구된다.

② 보안 정책 : CTP 방식은 RBAC과 UCON을 어떻게 지식 관리에 적용하고 활용할 것인지에 대해서 제안하였다. 그러나 TN을 다양한 구조에 적용시 발생할 수 있는 보안 문제로 발생할 수 있는 문제에 대해서는 고려되지 않았다. 특히, CTP 방식에서 가장 중요한 RBAC을 서로 다른 그룹에 적용시키고자 할 경우 발생할 수 있는 정책적 고려가 이루어지지 않았으며, 이로 인해 발생할 수 있는 보안 취약성도 논의되지 않았다.

③ 통신 및 저장 데이터의 안전성 : 제안된 방식은 시멘틱 웹과 데이터 마이닝을 통해 사용자에게 지식 정보를 제공하고자 하였다. 그러나 제공되는 데이터의 무결성과

데이터별 사용자의 프라이버시 보호를 위해 요구되는 통신의 안전성을 제공하지 못할 뿐 아니라 획득된 데이터들의 다양한 특성을 고려한 저장 데이터의 보안 서비스를 제공하지 못한다.

3.3 향상된 SKM 방식

본 방식은 델파이를 이용해 SKM을 제안하기 위하여 21개의 요구사항을 제시하고 영역별, 그룹별, 사용자별 중요성이 있는 프로세스를 정의하였다. 각각의 요구사항은 사용자 프라이버시 중심의 유/무선 형태의 서비스가 제공될 때 정책과 서비스에 대한 보안 요구사항으로써 각각의 보안 요구사항에 대하여 제공해야 하는 필요성과 정의를 기술하였으며, 이를 델파이로 구현하여 효율성을 분석하였다[5]. 그러나 본 방식의 경우 다음과 같은 취약성을 내포하고 있다.

① 키의 생성과 분배 : 제안된 방식은 각각의 보안 요구사항에 따라 키의 생성에 따른 효율성 및 사용자별, 요구하는 지식에 따라 별도의 키의 사용으로 안전성을 제공하고자 하였다. 그러나 각각의 생성된 키를 그룹 혹은 사용자에 따라 안전하게 분배하고 이를 관리하는 서비스를 제공하지 못한다. 따라서 키의 생성과 더불어 각각의 키에 사용을 위한 사용자의 키 분배 서비스를 제공해야 한다.

② 보안 정책 : 향상된 SKM 방식은 기존의 CTP 방식[4]의 프레임워크를 기반으로 하여 사전에 모든 정보에 대한 정책이 이루어진 상태를 가정으로 이루어진다. 그러나 새로운 사용자 혹은 새로운 형태의 지식 서비스가 이루어지고자 할 경우 이를 위한 정책의 설립과 환경에 따른 정책의 다양성을 적용시킬 수 없다. 따라서 유비쿼터스 컴퓨팅과 같은 새로운 환경에 유동적인 보안 정책을 적용시킬 수 없는 취약성을 내포하고 있다.

③ 그룹 보안 서비스 : 향상된 SKM 방식은 각각의 그룹에 대한 보안 서비스를 제공하지 않는다. 특히, 확장된 형태의 SKM에서 사용자들의 그룹화와 그룹에 대한 보안 서비스는 전체적인 SKM의 안전성 확보에 반드시 요구된다. 그러나 본 방식에서는 그룹에 대한 보안 서비스를 제공하지 않는 취약성이 있다.

3.4 보안 요구사항 분석

다음은 RFID를 이용한 이동성 지식 관리 시스템의 멀티 에이전트를 구성할 때 요구되는 보안 요구사항을 분석하고자 한다.

① 키의 생성과 분배 : 지식 관리 시스템을 제공하기 위하여 참여하는 모든 개체와의 통신은 안전한 키의 설정을 통해 이루어져야 한다. 따라서 각각의 개체들은 안전한 키 생성과정과 분배 과정을 통해 생성된 키를 통신 및 저장 데이터의 안전한 보안 서비스에 활용할 수 있어야 한다.

② 통신 및 저장 데이터의 안전성 : 안전한 지식 관리 시스템에 참여하는 모든 개체들 간의 통신은 안전하게 생성된 키를 기반으로 이루어져야하며, 통신 개체들 및 데이터들의 인증, 기밀성, 무결성을 보장할 수 있어야 한다.

③ 보안 정책 : 서로 다른 지식 관리 서버들뿐만 아니라 각각의 개체들 간의 서로 다른 보안 정책을 유동성 있게 적용할 수 있어야 하며, 데이터의 특징별로 서로 다른 보안 정책을 유지함으로써 사용자의 프라이버시 보호와 안전한 서비스를 유지할 수 있는 정책을 수립해야 한다.

④ 그룹 보안 서비스 : 다양한 사용자들의 그룹화를 통한 관리의 효율성을 증대시킬 수 있어야 한다. 또한 각각의 그룹의 속성에 따라 서로 다른 안전한 보안 서비스를 제공할 수 있어야 한다.

⑤ 관리 개체의 안전성 : 지식 관리 시스템을 제공하는 관리 개체의 안전성은 저장 데이터의 안전성뿐만 아니라 사용자의 프라이버시 정보의 안전성 확보에도 반드시 요구되는 요구사항이다.

⑥ 그룹 관리의 효율성 : 전체적인 사용자들을 속성별로 그룹화하고 그룹들을 효율적으로 관리하기 위한 별도의 그룹 보안 및 관리 서비스가 요구된다. 이는 다양한 사용자들에 대한 관리 방식의 효율성과 더불어 구성된 그룹들에 대한 효율성 확보를 위해 제공되어야한다.

⑦ 적용성 : 안전한 지식 관리 시스템이 특정 환경에 구애받지 않고 다양한 환경에 적용성을 가질 수 있어야 하며, 새로운 환경뿐만 아니라 서로 다른 지식 관리 시스템과의 상호 운용성을 제공해야 한다.

4. 사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템 방식

제안 방식은 지식 관리 시스템에서 사용자들을 위한 멀티 에이전트를 이용하여 RFID 태그와 상호 인증 과정을 수행하고 각 사용자들에 대한 속성을 기반으로 사용자들을 그룹화하고 해당 그룹에 따른 지식과 보안 서비스를 제공한다.

4.1 시나리오

사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템의 시나리오는 다음과 같다.

① 이동성 지식 관리 시스템의 멀티 에이전트들에 대한 초기화 과정을 수행한다.

② 이동 사용자가 소유하고 있는 RFID 태그들은 이동성 지식 관리 시스템과 안전한 인증과정을 수행하고 그 결과를 에이전트에 등록한다.

③ 멀티 에이전트에서는 서비스의 형태에 따라 사용자가 소유하고 있는 RFID 태그들을 분류하고 이를 위한

임시 그룹 초기화 단계를 수행한다.

④ 이동 사용자가 지식 서비스를 제공 받는 과정에서 다른 셀로 이동하였을 경우 해당 사용자에 대한 지속적인 서비스를 제공한다.

⑤ 임시 그룹에 대한 서비스가 종료될 경우 임시 그룹 정보에 대한 내용을 지식 관리 시스템은 삭제하고 이를 처리한다.

4.2 시스템 계수

다음은 사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리를 위한 시스템 계수를 기술한다.

(* : aa(권한정보 에이전트), M(지식 관리 시스템), ma: 이동 에이전트, T(RFID 태그, $T_1, T_2, \ldots, T_U, \ldots T_n$), R: RF 리더기($R_1, R_2, \ldots, R_n$), AMS(Agent Management Server), ANS(Agent Name Server)

ID_* : 개체의 ID

M_{aa}, M_{ma} : 권한 정보 에이전트와 이동 에이전트의 초기 생성 메시지

$h_{key}()$, $h()$: 안전한 keyed 해쉬 함수, 안전한 해쉬 함수

t_* : 타임스탬프

E_* : 암호화 알고리즘

S_* : 공개키 서명 알고리즘

al : 권한 설정 정보

r_* : 의사 난수

(p_*, q_*) : 개체의 공개키, 개인키쌍

$\oplus$: eXclusive OR

n, g : 공개 계수($n = pq$)

4.3 가정 사항

사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템을 위한 가정 사항은 다음과 같다.

① 일반적인 WPAN(Wireless Personal Area Network)과 같은 크기의 작은 네트워크 공간에서 다양한 지식 서비스를 제공받고자 하는 이동 사용자들이 RFID 태그들을 소유하고 있는 환경이다.

② RFID 통신을 위해서 신뢰할 수 있는 지식 관리 시스템과 RFID 태그와 통신이 가능한 RF 리더기가 존재하며, 각각의 개체들은 동기화 된다.

③ 지식 관리 서버는 g^i를 생성하고 $g^{i_{aa}}$는 AMS, $g^{i_{ma}}$는 ANS에 안전하게 사전 분배하며 $g^i = g^{i_{aa}} + g^{i_{ma}}$이다.

④ 지식 관리 서버를 이용하고자하는 이동 사용자들은 RFID 태그를 사전에 등록하고 (g^{I_s}, g^{I_s})를 안전하게 분배받는다.

⑤ 지식 관리 서버와 RF 리더기 공유키 k_{MR}을 안전하게 공유한다.

4.4 사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템 제안

제안 방식은 다음과 같은 흐름으로 구성된다.

[Step 1] 멀티 에이전트의 초기화

- 권한 정보 에이전트의 초기값 생성

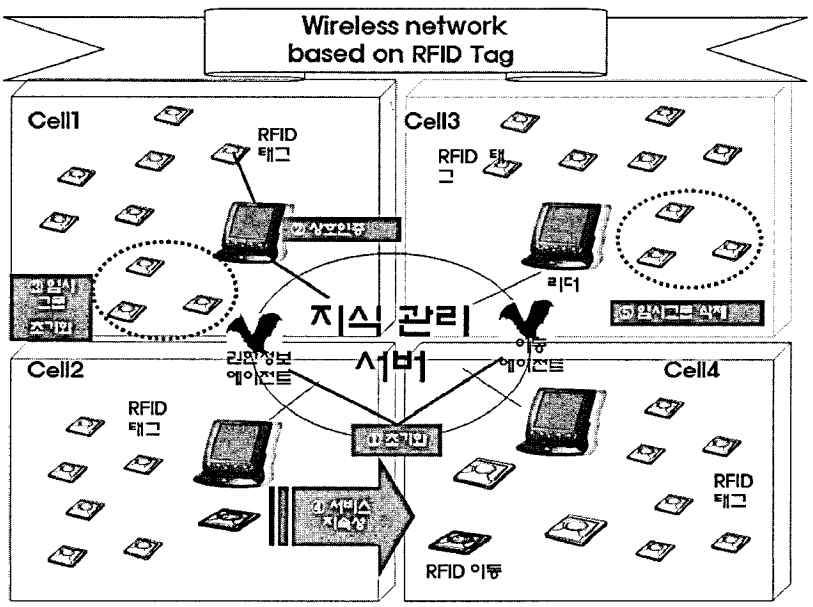

그림 1 지식 관리 시스템에서 RFID 이동성을 고려한 멀티 에이전트 방식 시나리오

① 멀티 에이전트 시스템의 AMS는 권한 정보 에이전트의 초기값 생성을 위해 다음을 생성한 후 이를 지식 관리 시스템에 전송한다.

$$ID_{aa},\ M_{aa},\ g^{i_{ma}}$$

② 지식 관리 시스템은 권한 정보 에이전트의 ID_{aa}, M_{aa}를 DB에 저장하고 $g^{i_{ma}}$를 기반으로 권한 정보 에이전트의 초기 값을 생성한다.

$$M_M^1 = H(M_{aa}\|ID_{aa}) \oplus H(g^{i_{ma}}\|t_M)$$

$$k_M^1 = g^{i_{ma}*r_M} \bmod n$$

$$Z_M^1 = \frac{g^{i_{ma}*r_M}}{(k_K^1 + H(M_{aa}))} mod n$$

$$M_{code_{aa}} = E_{p_t}(M_M^1\|Z_M^1\|M_{aa}\|t_M)$$

생성된 권한 정보 에이전트의 초기값 $M_{code_{aa}}$를 멀티 에이전트 시스템의 AMS에 할당한다.

- 이동 에이전트의 초기값 생성

① AMS 이동 에이전트의 초기값 생성을 위해 다음을 계산하여 지식 관리 시스템에 이를 전송한다.

$$ID_{ma},\ M_{ma},\ g^{i_{ma}}$$

② 지식 관리 시스템은 AMS로부터 전송받은 ID_{ma}, M_{ma}, $g^{i_{ma}}$를 기반으로 다음을 계산하여 이동 에이전트의 초기값을 생성한다.

$$M_M^2 = H(M_{ma}\|ID_{ma}) \oplus H(g^{i_{ma}}\|t_M)$$

$$k_M^2 = g^{i_{ma}*r_M} \bmod n$$

$$Z_M^2 = \frac{g^{i_{ma}*r_M}}{(k_K^2 + H(M_{ma}))} mod n$$

$$M_{code_{ma}} = E_{p_t}(M_M^2\|Z_M^2\|M_{ma}\|t_M)$$

생성된 이동 에이전트의 초기값 $M_{code_{ma}}$을 AMS에 전송하고 AMS는 이를 이동 에이전트의 초기값으로 등록한다.

[Step 2] RFID와 지식 관리 시스템과의 상호 인증

다음은 이동 사용자들이 소유하고 있는 RFID 태그들과 지식 관리 시스템과의 상호 인증 과정이다.

① 이동 사용자의 RFID 태그는 지식 정보를 제공받기 위한 메시지와 v_T, t_T를 RF 리더기에 전송한다.

$$v_T = H(g^{i_{s_1}}\|t_T)$$

② RF 리더기는 지식 관리 서버와 공유한 키 k_{MR}을 기반으로 RFID 태그의 임시 태그 정보를 다음과 같이 생성하여 지식 관리 시스템에 TID_{R_1}, v_T, t_T를 전송한다.

$$TID_{R_1} = H_{k_{MR}}(ID_R\|v_T)$$

③ 지식 관리 시스템은 TID_{R_1}, v_T, t_T을 수신한 후 TID_{R_1}을 검증한다.

<검증 과정>

- 지식 관리 서버는 공개된 ID_R, 사전에 사용자부터 등록된 i_{s_1}을 기반으로 TID_R를 검증한다.

$$v_T' = H(g^{i_{s_1}}\|t_T) = v_T$$

$$TID_{R_1}' = H_{k_{MR}}(ID_R'\|v_T') = TID_{R_1}$$

검증이 TID_{R_1}에 대한 검증이 올바르지 않는 경우 RF 리더기에 상호 인증 초기화 메시지를 전송하며, RF 리더기는 RFID 태그에 상호인증 메시지를 재요청한다.

검증이 올바른 경우 지식 관리 서버는 다음을 계산하여 RF 리더기에 TID_M^1, v_M, t_M을 전송한다.

$$TID_M^1 = H(g^{i_{s_1}}\|g^{i_{s_1}}\|t_M)$$

$$v_M = H(g^{i_{s_1}}\|t_M)$$

④ RF 리더기는 지식 관리 시스템으로부터 전송된 TID_M^1, v_M으로 TID_R를 계산하여 TID_M^1, TID_{R_2}, t_M을 RFID 태그에 전송한다.

$$TID_{R_2} = H_{k_{MR}}(ID_R\|v_M)$$

⑤ RFID 태그는 RF 리더기로부터 전송된 TID_M^1, TID_{R_2}, t_M으로 다음의 과정을 거쳐 전송 데이터를 검증한다.

<검증 과정>

$v_M' = H(g^{i_{s_1}}\|t_M)$이면 $TID_M^1 = H(g^{i_{s_1}}\|g^{i_{s_1}}\|t_M) = TID_M^1{}'$이다.

검증이 올바른 경우 RFID 태그와 지식 관리 시스템과의 상호 인증 과정을 종료하고 RFID 태그와 지식 관리 서버는 다음과 같은 세션키 sk_{MT}를 생성하고 RFID 태그에 대한 인증 정보인 v_T를 AMS에 전송한다.

$$sk_{MT} = H(v_T \oplus v_M \oplus TID_{R_1} \oplus TID_{R_2})$$

[Step 3] 서비스 형태에 따라 RFID 태그의 분류 및 임시 그룹 초기화

다음은 사용자가 요구하는 서비스 형태에 따라 RFID 태그들을 분류하고 이들에 대한 속성으로 임시 그룹을 초기화하는 과정을 수행한다.

① 지식 정보 시스템에서는 RFID 태그들로부터 정보 전송을 요청 받는다.

Service_Request

② RFID 태그들로부터 정보 전송 요청을 받은 지식 정보 시스템은 동일한 서비스가 있을 경우(ID_{T_1}, ID_{T_2}, ID_{T_3}) 다음의 정보를 ANS에 전송한다.

$$h_{T_1} = H_{sk_{MT_1}}(ID_{T_1}\|v_{T_1}\|t_{T_1}),\ h_{T_2} = H_{sk_{MT_2}}(ID_{T_2}\|v_{T_2}\|t_{T_2}),$$

$$h_{T_3} = H_{sk_{MT_3}}(ID_{T_3}\|v_{T_3}\|t_{T_3})$$

③ ANS는 RFID 태그들(ID_{T_1}, ID_{T_2}, ID_{T_3})의 정보인 h_{T_1}, h_{T_2}, h_{T_3}를 수신하고 전송 정보의 무결성을 검증한

후 s_{ANS}를 계산하여 RFID 태그에서 요구하는 서비스에 대한 권한 정보 생성을 위하여 AMS에 s_{ANS}, t_{ANS}를 전송한다.

$$s_{ANS} = H(h_{T_1}) \oplus H(h_{T_2}) \oplus H(h_{T_3}) \oplus Service$$

AMS에 전송 이후 ANS는 이동 사용자들의 임시 그룹화를 통해 관리하기 위하여 $TGID_{T_1T_2T_3}$를 계산하여 ANS의 개인키로 서명한 뒤 이동 에이전트의 고유값과 임시그룹 정보들을 지식 관리 시스템에 전송한다.

$$TGID_{T_1T_2T_3} = H(ID_{T_1} \oplus v_{T_1}) \| H(ID_{T_2} \oplus v_{T_2}) \| H(ID_{T_3} \oplus v_{T_3})$$

$$Sig_{ANS} = S_{q_{ANS}}((M_{code_{ms}} \| TGID_{T_1T_2T_3}) \| Service)$$

④ AMS는 ANS로부터 전송된 s_{ANS}, t_{ANS}를 수신한 후 지식 관리 시스템으로부터 해당 서비스의 Sig_{ANS}를 요청하고 이를 전송받은 후 ANS의 공개키로 서명을 확인한다. 서명 확인 후 $M_{code_{ms}}$, $TGID_{T_1T_2T_3}$를 $Service$에서 요구되는 권한 정보(al)를 다음과 같이 생성하고 이를 지식 관리 시스템에 전송한다.

$$Sig_{AMS} = S_{q_{AMS}}(M_{code_{ms}} \| al_1 \| TGID_{T_1T_2T_3})$$

⑤ 지식 관리 시스템은 ANS와 AMS로부터 전송된 Sig_{ANS}, Sig_{AMS}를 일대일 대응하여 저장한다.

<권한 설정>

- 권한 1(al_1) : 해당 서비스에 대해여 그룹 및 단일 개체에 모든 권한을 부여하여 서비스의 재가공, 배포가 가능한 권한
- 권한 2(al_2) : 해당 서비스를 그룹내에서만 읽고, 쓰고, 수정할 수 있는 권한
- 권한 3(al_3) : 해당 서비스를 그룹 및 단일 서비스에 대한 읽기 기능만 가능한 권한

[Step 4] 사용자 이동에 따른 서비스의 지속성 보장

사용자가 다른 셀로 이동하였을 때 서비스의 지속성을 보장하기 위하여 이동한 사용자의 RFID 태그에 서비스를 제공하는 단계이다.

① 이동 사용자의 RFID 태그 ID_{T_U}는 서비스의 지속성을 보장받기 위하여 이동한 셀의 RF 리더기(ID_{R_2})에 다음을 계산하여 ID_{T_U}, h_{T_U}, v_{T_U}, t_{T_U}와 제공 받고자 하는 서비스 정보를 전송한다.

$$h_{T_U} = H_{sk_{MT_U}}(v_{T_U} \| t_{T_U}),\ \text{Service\_information}$$

② 서비스 정보와 ID_{T_U}, h_{T_U}, v_{T_U}, t_{T_U}를 전송받은 RF 리더기(ID_{R_2})는 RFID 태그에 대한 서비스 지속성 보장을 위하여 지식 관리 시스템에서 공개한 Sig_{AMS}, 서비스 정보, ID_{T_U}, v_{T_U}, t_{T_U}와 h_{R_2}를 계산하여 ANS에 전송한다.

$$h_{R_2} = H_{k_{MR}}(h_{T_U} \| t_{T_U})$$

③ ANS는 RF 리더기(ID_{R_2})로부터 전송받은 Sig_{AMS}, Service_Information, ID_{T_U}, v_{T_U}, t_{T_U}, h_{R_2}를 기반으로 다음의 검증 과정을 수행한다.

<검증 과정>

RF 리더기(ID_{R_2})로부터 전송된 ID_{T_U}를 확인하고 ID_{T_U}와 공유한 세션키 sk_{MT_U}를 이용해 h_{T_U}'을 생성한 뒤 h_{R_2}의 무결성을 검증한다.

$h_{T_U}' = H_{sk_{MT_U}}(v_{T_U} \| t_{T_U})$이고 $h_{R_2}' = H_{MR}(h_{T_U}' \| t_{T_U}) = h_{R_2}$이면 서비스 지속성을 요구하는 ID_{T_U}의 권한 정보인 s_{ANS}를 확인한다.

$s_{ANS} \oplus Service \oplus H(h_{T_U}) = H(h_{T_4}) \oplus H(h_{T_5})$인 h_{T_4}와 h_{T_5}를 추출하고 이를 기반으로 $TGID_{T_4T_5T_U} \oplus H(ID_{T_U} \oplus v_{T_U}) = H(ID_{T_4} \oplus v_{T_4}) \oplus H(ID_{T_4} \oplus v_{T_4})$임을 검증한다.

검증이 올바른 경우 ANS의 서명값 Sig_{ANS}를 지식 관리 시스템에 전송한다.

④ 지식 관리 시스템은 Sig_{ANS}와 일대일 대응되는 Sig_{AMS}를 추출한 뒤 권한 정보를 확인하고 이에 해당되는 서비스를 RF 리더기 ID_{R_2}를 통해 이동 사용자에게 이를 전송한다.

[Step 5] 임시 그룹에 대한 서비스 종료 및 임시 그룹 정보 삭제

동일한 형태의 서비스가 종료 될 경우 해당 임시 그룹에 대한 정보를 삭제하고 이를 지식 관리 시스템에서 초기화하는 과정이다.

① 지식 관리 시스템은 임시 그룹에 대한 서비스가 종료 될 경우 해당 서비스 그룹에 대한 초기화를 위하여 멀티 에이전트 시스템의 AMS와 ANS에 그룹 초기화 메시지를 전송한다.

② AMS는 이동 에이전트의 초기화 값을 제외하고 임시 그룹 정보($TGID$)와 권한 정보(al)을 삭제한 후 Sig_{AMS}를 초기화한다.

③ ANS는 해당 서비스와 임시 그룹 정보 메시지를 삭제하고 서명값을 초기화한다.

④ 멀티 에이전트 시스템은 AMS와 ANS에서 설정한 에이전트의 초기값을 검증하고 검증이 올바른 경우 지식 관리 시스템에 그 결과를 전송한다.

⑤ 지식 관리 시스템은 멀티 에이전트의 검증에 대한 결과를 수신하고 Sig_{AMS}와 Sig_{ANS}를 삭제한다.

이상의 과정을 통해 사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템이 구성된다.

5. 제안 방식 분석

본 장에서는 제안된 사용자의 이동성을 고려한 멀티 에이전트 방식의 RFID 기반 지식 관리 시스템을 기존 방식과 비교 분석하고자 한다.

5.1 안전성 분석

① 키의 생성과 분배 : 지식 관리 시스템을 제공하기 위하여 참여하는 모든 개체와의 통신은 안전한 키의 설정을 통해 이루어져야 한다. 향상된 SKM 방식과는 차별화된 형식으로 사용자별, 요구하는 지식에 따라 별도의 키를 생성한다. 즉, 사용자에 따라 $sk_{MT} = H(v_T \oplus v_M \oplus TID_{R_1} \oplus TID_{R_2})$를 계산하여 Keyed 해쉬 함수의 키로 사용함으로써 상호 통신의 안전성을 유지하였으며, 요구되는 지식에 따라 임시 그룹을 설정하여 각각의 사용자들이 동일한 서비스를 받고자 할 경우 멀티 에이전트 시스템의 *AMS*와 *ANS*에서 서명된 *Sig*값에 임시 그룹에 대한 내용과 에이전트의 안전한 초기값을 공개함으로써 사용자들에 대한 안전한 관리가 가능한 키의 생성과 분배가 이루어지도록 하였다. 또한 CTP 방식에서의 취약성인 안전한 보안 키 설정을 위하여 안전한 상호 인증 과정을 제안함으로써 키 생성 및 분배 과정의 안전성을 보장하였다.

② 통신 및 저장 데이터의 안전성 : 제안방식은 모든 개체들 간의 통신들의 안전성 확보를 위하여 각각의 사용자들에 따라 별도의 세션키 sk를 이용하였으며, 서비스의 제공자인 지식 관리 시스템과 사용자의 RFID 태그에 대한 상호 인증을 통해 통신상의 기밀성과 무결성을 보장하도록 하였다.

③ 보안 정책 : 제안 방식에서는 사용자가 요구하는 지식 서비스의 형태와 사용자에 따라 서비스 권한 정보(al)을 임시 그룹화 하여 설정함으로써 권한 정보의 형태에 따라 지식 서비스를 차별화 할 수 있도록 하였다. 또한 사용자의 프라이버시 보호를 위하여 멀티 에이전트 시스템의 초기화 값을 *AMS*와 *ANS*의 서명값에 포함시켜 공개함으로써 안전한 서비스가 유지되고 이를 검증할 수 있도록 하였다.

④ 그룹 보안 서비스 : 다양한 사용자들이 동일한 서비스를 요구할 경우 제안 방식에서는 임시 그룹인 *TGID*를 설정하고 이를 임시 그룹화 하여 지식 관리 서버에서 관리함으로써 서로 다른 지식 서비스에 대한 효율적인 관리가 가능하도록 하였으며, 그룹 서비스의 안전성 보장을 위하여 *TGID*를 멀티 에이전트의 초기 값들과 함께 서명하여 공개함으로써 모든 사용자들이 서비스에 따른 임시 그룹을 확인할 수 있을 뿐만 아니라 안전한 에이전트의 보호를 위한 초기 값의 검증을 통해 그룹들의 권한 및 서비스 정보가 비인가 된 제 3자에 의해 불법적으로 수정되는 취약성을 보완하였다.

⑤ 관리 개체의 안전성 : 지식 관리 시스템에 저장된 정보들은 이동 사용자의 디바이스 정보를 이용한 안전한 해쉬 함수값(h) 혹은 계산된 중간값(v)을 이용함으로써 지식 관리 서버의 관리 개체의 저장 데이터에 대한 안전성을 보장한다.

⑥ 그룹 관리의 효율성 : 제안 방식에서는 각 사용자들이 요구하는 서비스의 형태에 따라 동일한 서비스가 요구될 경우 이를 임시 그룹화 하여 관리할 수 있는 방안을 제안하였다. 따라서 이는 다양한 사용자들의 효율적인 관리뿐만 아니라 서비스의 효율성을 증대시킬 수 있다.

⑦ 적용성 : 제안 방식에서는 소형 디바이스로 대표되는 RFID 태그를 기반으로 안전한 형태의 지식 관리 시스템을 제안하였다. 특히, 멀티 에이전트 시스템은 안전한 초기값의 생성하고 이를 기반으로 사용자에 서비스를 제공할 때 발생할 수 있는 환경적 변화에 유동적으로 적용이 가능한 방식으로 지식 서비스 시스템의 효율성 뿐만 아니라 다양한 환경에 적용할 수 있는 적용성을 보장한다.

이상의 내용을 기존 방식과 비교할 경우 표 1과 같이 정리할 수 있다.

5.2 성능 분석

제안 방식은 송신자와 수신자간 비슷한 사이즈의 메시지에 대한 확률을 기반으로 분석하고자 한다. 사용자가 푸아송 분포(poisson distribution)를 공통적으로 가

표 1 제안방식 보안 분석

방식 / 요구사항	PBKM 방식	CTP 방식	향상된 SKM 방식	제안 방식
키의 생성과 분배	○	×	△	○
통신 및 저장 데이터의 안전성	○	×	○	○
보안 정책	△	×	△	○
그룹 보안 서비스	△	△	×	○
관리 개체의 안전성	△	△	○	○
그룹 관리의 효율성	×	○	○	○
적용성	×	○	○	○

(×: 위험, △: 취약, ○: 안전)

정할 경우 지속시간 T, $P(X=i)=e^{-\lambda_1 T}\frac{(\lambda_1 T)^i}{i!}$일 때 독립적인 사용자간의 참여 시간 $P(X=i, Y=j)=P(x=i)P(y=j)=e^{-\lambda_1 T-\lambda_2 T}\frac{(\lambda_1 T)^i(\lambda_1 T)^j}{i!j!}$이면 $P(|X-Y|\le\delta)=\Sigma_1 P(i,i)+\Sigma_i P(i,i+1)+\ldots+\Sigma_i P(i,i+\delta)+\Sigma_i P(i,i-1)+\ldots+\Sigma_i P(i,i-\delta)$이다[6]. 따라서 서로 사용자들간의 서로 다른 초기화 과정의 λT로부터 일반적인 사용자의 메시지의 평균 메시지 T라 할 경우 독립적인 사용자의 경우 서로 다른 λ 값을 가지고 있으며 비슷한 메시지에 대한 확률은 매우 낮다.

제안 방식에서는 임시 그룹 설정을 위하여 독립적인 사용자들간의 메시지를 설정함으로 만약 두 명의 독립적인 사용자가 임시 그룹으로 설정될 경우 이동 사용자(RFID 1)의 $\lambda_1 T=5$, 이동 사용자($RFID_2$)가 $\lambda_2 T=10$일 경우 확률 $P(|X-Y|\le 2)$이다. 따라서 기존 방식에서 동일한 메시지($P(|X-Y|\le 1)$)를 전송함으로써 향상된 형태의 메시지 효율성을 지닐 수 있다.

또한 RFID 태그의 인증 과정에서의 RFID 태그만을 고려한 해쉬 연산을 통해 서비스의 지속성을 제공 받을 수 있는 초기값 v를 계산함으로써 기존 방식과는 차별화된 형태의 서비스가 가능하다. 특히, 메시지에 따른 통신 비용 측면에서 전체적인 통신 비용을 $M^{tree}(w)$라 정의할 때에 전체 비용은 $M^{tree}(w)\le hN(w)$으로 정의할 수 있으며 공개 메시지의 내용은 멀티 에이전트의 메시지 2개 이상의 활용과 최소 M^{tree}는 $\min(2N(w), \frac{a}{a-1}(R-1))$, 최대값은 $M^{tree}_{\max}(w)$는 $\frac{a}{a-1}(R-1)$로 정의할 수 있다. (a: $a-ary$ 트리, R: RF 리더기 수, height h : $\log_a R$) 따라서 제안 방식은 멀티 에이전트를 이용하여 통신을 수행함으로 전체적인 통신 비용 M^{tree}는 $a=4$이고 RF가 4일 때 $M^{tree}(w)\le 4$이며, 최소 M^{tree}는 $\min(2N(w), 4)$이며, 최대 $M^{tree}_{\max}(w)$는 4이다.

그림 2는 RFID 태그의 인증 과정에서 메시지에 따른 통신 비용 측면을 RFID 태그의 인증만을 고려한 방식 및 기존의 KMS 방식을 기준으로 제안 방식을 비교하였을 때 통신 효율성을 계산한 결과이다. 이상의 결과를 기준으로 기존의 RFID 태그 인증 방식과 비교해볼 때 멀티 에이전트 개체의 포함으로써 RFID 인증만을 비교할 경우 효율성이 저하되나 기존의 지식 관리 시스템보다 효율적인 형태의 관리가 가능하다.

6. 결 론

최근 유비쿼터스 환경으로 변화하는 가운데 다양한 정보들이 사용자들에게 제공되고 활용되고 있으며, 사용자의 이동성 보장과 소형화된 디바이스로 대표되는 RFID의 활용은 실생활을 유비쿼터스 환경으로 전환하는데 핵심적인 요소로 대표되고 있다. 특히, 다양화된 지식 서비스를 사용자에게 안전하면서도 효율적인 형태로 제공하기 위한 다양한 연구가 진행되고 있으나 사용자의 이동성 확보를 비롯하여 다변화 되는 공격 환경에 안전성과 관리적인 효율성에 대해 미흡한 실정이다.

따라서 본 논문에서는 사용자의 이동성을 고려한 지식 서비스가 가능한 네트워크 관리 방식을 제안하였다. 제안 방식은 멀티 에이전트 기술을 이용하여 사용자의 그룹화와 서비스의 지속성을 위한 방식을 제안하였으며, 기존의 연구에서 고려되지 않았던 다양한 보안 요구사항과 효율성을 만족한다.

그러나 본 방식은 임시 그룹에서 탈퇴한 사용자에 대한 네트워크의 안전성과 계산량 증가 및 고려사항에 따른 특수한 네트워크 적용의 문제점과 일반적인 RFID 태그의 안전성을 위한 다양한 보안 요구사항을 고려하지 않는 문제점이 여전히 내포하고 있으며 이를 위해서 향후 추가적인 연구가 이루어질 예정이다.

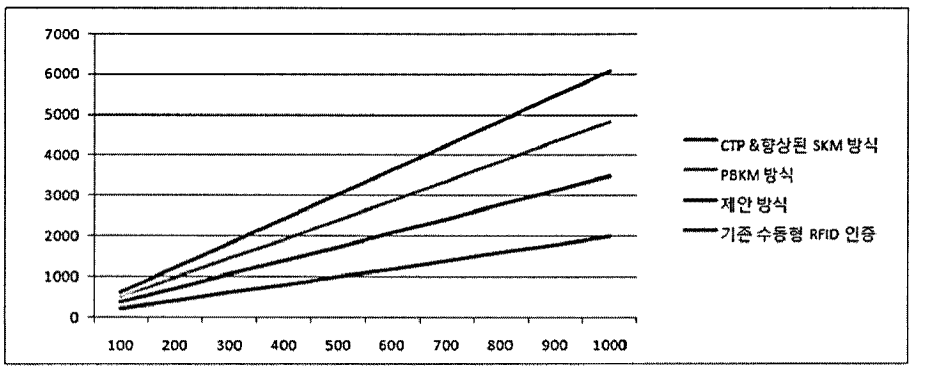

그림 2 제안 방식의 효율성 분석

참 고 문 헌

[1] Insu Park, Jinkyu Lee, H. Raghav Rao, Shmbhu J. Upadhyaya, "Emerging Issues for Secure Knowledge Management-Results of Delphi Study," *IEEE Trans.*, vol.36, no.3, pp.421-428, 2006.

[2] 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.

[3] S. Xu and W. Zhang, "PBKM: A secure knowledge management framework," in *Proc. Workshop Secure Knowledge Management (SKM)*, pp.207-212, 2004.

[4] S. Upadhyaya, H. R. Rao, and G. Padmanabhan, "Secure knowledge management," in Encyclopedia of Knowledge Management, E. D. Swartz, Ed. Hershey, PA: Idea Group Publishing, pp.795-801, 2005.

[5] Guofe Gu, Junjie Zhang, and Wenke Lee, "Botsniffer:Detecting Botnet Command and Control Channels in Network Traffic," Network&Distributed System Security Symposium, pp.269-286, 2008.

[6] A. Ferrari, G. Letac, J.-Y. Tourneret, "Exponential families of mixed Poisson distributions," *Journal of Multivariate Analysis*, volume 98, Issue 6, pp.1283-1292, 2007.

서 대 희

2003년 순천향대학교 전산학과 졸업(석사). 2006년 순천향대학교 대학원 전산학과 졸업(박사). 2006년~2007년 Howard University Post-Doc. 2007년 5월~2007년 12월 한국정보보호진흥원 위촉선임연구원. 2008년 7월~2009년 9월 이화여자대학교 컴퓨터공학과 연구교수. 2009년 10월~현재 한국전자통신연구원 SW콘텐츠단 지식정보보호부 인프라보호팀 선임연구원. 관심분야는 정보보호, 네트워크 보안, 소형 디바이스 보안, 오버레이 네트워크, 공격자 추적

백 장 미

2003년 순천향대학교 전산학과 졸업(석사). 2006년 순천향대학교 대학원 전산학과 졸업(박사). 2006년~2007년 Howard University Post-Doc. 2007~현재 순천향대학교 컴퓨터학부 강사. 관심분야는 임베디드 시스템, 모바일 헬스케어, 지능형 소프트웨어, 지식관리 시스템

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, 휴먼컴퓨팅, 웹서버 엔지니어링