정적인 TTP 기반의 안전하고 효율적인 이기종 네트워크 관리 기법에 관한 연구☆

A Study on Secure and Efficient Heterogenous Network Management Scheme based on Static TTP

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

요 약

최근의 이기종 네트워크 관리에 대한 연구는 단순히 PKI를 이용한 방식으로 이루어지고 있는 실정이며, 실제 이기종 네트워크가 구현되었을때 나타날 수 있는 다양한 형태의 보안 연구가 미흡하다. 따라서 다양한 보안 요구사항과 이를 만족하는 보안 관리 프로토콜 개발은 안전한 이기종 네트워크 환경에 매우 절실히 요구되는 사항이다. 본 논문에서는 기존의 연구에서 고려사항으로 제시되었던 보안적 사항을 만족하는 이기종 네트워크의 안전하고 효율적인 관리 방식을 제시한다. 제시된 방식은 사용자의 프라이버시 보호를 위해 정적인 중앙 개체와 중간 개체를 이용해 상호 인증과정을 수행하고 사용자들간의 통신이 필요한 경우 1-out-2 분실 통신로를 이용해 암호 통신을 수행함으로써 안전성 뿐만 아니라 통신의 효율성까지 고려한 방식이다.

특히, TTP를 기반으로 이기종 네트워크에서 요구되는 다양한 서비스와 관련된 보안과 효율성을 높이기 위한 방식으로 기존 논문에서 전자 상거래에 사용하던 모바일 단말기를 이용해 다양한 서비스를 제공하고 임시 그룹을 설정하여 동적인 환경에 적합한 관리 방식을 제안하였다.

Abstract

Recent heterogeneous network management researches on information security, however, deal only with simple management using PKI and could not sufficiently address the different kinds of security problems that could arise in a heterogeneous network. Thus, various security requirements should first be satisfied and a security management protocol should first be developed to achieve a secure heterogeneous network. Hence, in this paper, various secure and effective heterogeneous network management that address security issues, which were merely a consideration in existing studies, are proposed. The proposed scheme for the protection of the user privacy is the central object and static middle objects of the process used to mutual authentication. also if communication between users is required 1-out-2 oblivious transfer to communicate by using secret communication, as well as the effectiveness and security conscious approach.

Specially The proposed scheme is designed to enhance security and efficiency related to various services required in heterogeneous network, based on the reliable peripheral devices for TTP. Using Mobile device, which has been applied to electronic commerce transactions in existing schemes, this study also proposed an appropriate management scheme that is suitable for a dynamic environment and setting a temporary group to provide various services.

☞ Keyword : Ubiquitous Environment, Heterogeneous Network Security, Secure Network Management, User Authentication, 유비쿼터스 환경, 이기종 네트워크 보안, 안전한 네트워크 관리, 사용자 인증

1. 서 론

새로운 u-지식 사회에서의 기반이 되는 유비쿼터

* 정 회 원 : 이화여자대학교 연구교수
dhseo@ewha.ac.kr
** 정 회 원 : 순천향대학교 시간강사
bjm1453@sch.ac.kr
*** 정 회 원 : 이화여자대학교 컴퓨터학과 교수
dscho@ewha.ac.kr(교신저자)
[2008/03/31 투고 - 2008/04/08 심사 - 2008/08/09 심사완료]
☆이 논문은 2008년도 2단계 두뇌한국(BK)21 사업에 의하여 지원되었음

스 컴퓨팅 환경은 사용자를 중심으로하는 주변 상황이나 환경을 네트워크가 지능적으로 파악하여 사용자 네트워크를 최적화 한다. 그러나 사용자가 자유스럽게 컨텐츠를 사용하고 접근하기 위해서는 다양한 네트워크에서 사용자 프라이버시 보호에 대한 안전성이 우선 되어야 한다[1][2].

특히, 이기종 환경에서 사용자들이 공존할 경우 사용자들간의 통신 뿐만 아니라 이기종 환경의 특수성이 기인한 안전한 통신 과정을 수행해야한다. 그러나 최근의 연구들은 주로 그룹 통신의 효율성을 위한 Internet2 기반의 IP 멀티캐스트, 오버레이 멀티캐스트(overlay multicast)에 대한 연구가 활발히 진행되고 있다. 따라서 효율성 뿐만 아니라 사용자 프라이버시 정보의 안전성 확보를 위한 연구가 시급히 요구된다[3].

이는 유비쿼터스 환경에서 안전한 통신에 기반해 효율성 높은 관리 방식을 다양한 그룹 통신들이 적용할 수 있을 뿐만 아니라 사용자의 안전성까지 확보될 수 있어 안전한 u-지식사회 구축을 위해 반드시 요구되는 연구이다. 따라서 본 논문에서는 안전한 u-지식사회를 위해 이기종 네트워크 환경에서 사용자 프라이버시 보호를 위한 안전한 통신과 관리 방식에 대한 연구를 수행하고자 한다.

본 논문의 2장에서는 유비쿼터스 컴퓨팅 환경과 이기종 네트워크의 개요에 대해 기술하고 3장에서는 기존의 이기종 네트워크 환경의 네트워크 관리 방식에 대해 분석하고 안전하고 효율적인 네트워크 관리 방식을 위한 보안 요구사항을 제시한다. 4장에서는 3장에서 제시한 보안 요구사항을 기준으로 기존 연구를 분석하고 5장에서 이기종 환경의 안전하고 효율적인 네트워크 관리 방식에 대해 제안한다. 6장에서는 기존 방식과 제안 방식을 보안 요구사항에 기반해 비교 분석한 뒤 마지막으로 7장에서 결론을 맺고자 한다.

2. 유비쿼터스 컴퓨팅과 이기종 네트워크의 개요

유비쿼터스 네트워크는 휴대전화 및 PDA, 노트북등을 가지고 실내 및 실외에 관계없이 통신이 가능한 네트워크 환경을 의미한다. 따라서 모바일 디바이스가 근거리에서 인터넷 망 또는 주변 네트워크에 언제 어디서든 통신하고 빠른 시간에 네트워크를 형성하기 위한 기술들이 요구되고 있다[4][5].

특히, 이기종 네트워크는 다수의 RAN(Radio Access Networks)이 여러 가지 구조를 가지고 있다. 즉, CCN(Common Core Network)을 기반으로 여러 네트워크 기능과 연산 기능들이 하나의 네트워크에 공존하는 형태이며, 서로 다른 RANs들의 상호 운용 뿐만 아니라 특성들간의 연동을 통해 무선 제어 기술을 제공한다. 일반적으로 무선 통신은 물리적으로 데이터 링크를 제공한다. RANs들간이 통신은 같은 CCN을 기반으로 수행된다. 이것은 네트워크 효율성이 향상되고 오버헤드가 감소하는 특징을 가질 수 있다. 중요한 것은 서로 다른 RANs가 한곳에 집중되는 것이다. 최근의 이기종 네트워크에 관련된 연구는 IP(Internet Protocol) 레벨에서의 이동성 지원을 위한 Mobile IP에 대한 연구와 이웃 노드들간의 핸드오프 및 QoS(Quality of Service) 연구가 주류를 이루고 있다[5][6].

그러나 이기종 네트워크 환경에서 사용자의 프라이버시가 보호되지 않는다면 최상의 네트워크에 최적의 서비스를 제공받고자 하는 사용자의 요구를 만족시킬 수 없다. 따라서 이기종 네트워크 환경을 고려한 안전한 형태의 네트워크 관리 구조에 대한 연구가 시급한 실정이다.

3. 이기종 네트워크 보안 사항

본 장에서는 이기종 네트워크에서 보안의 필요성과 관리 구조에서의 보안 요구사항에 대해 논하고자 한다.

3.1 이기종 네트워크에서 보안의 필요성

유비쿼터스 네트워크는 사용자의 프라이버시 뿐

만 아니라 비즈니스를 포함한 사회 전반을 변화 시킬 수 있는 가장 큰 핵심 요소 기술이다.

유비쿼터스 환경의 특성상 모든 컴퓨터와 사물이 하나로 연결된 네트워크로서 누구든지 사용자의 정보에 접근할 수 있다. 이와 같이 고도화된 네트워크 환경의 보안적 취약점은 고의적인 제 3자의 공격자로부터 정보 도용을 통한 프라이버시 침해로 이어질 수 있다[1][7]. 또한 유비쿼터스 네트워크에서의 보안 기술은 하드웨어적으로 제한된 시스템에서 제공해야 하기 때문에 일반적인 인터넷 환경에서 제공되는 보안 서비스 보다 구현하기 어려운 측면도 있다.

이기종 네트워크는 네트워크 환경의 다양한 변화에 따라 보안과 서비스가 동적으로 제공될 수 있으며, 이는 유비쿼터스 네트워크와 같은 다양한 네트워크 환경에 공존하는 환경에서 핵심 요소 기술 중 하나이다. 따라서 유비쿼터스 네트워크 환경에서 안전성 확보를 위해서는 독립적인 형태의 네트워크 안전성 뿐만 아니라 다양한 네트워크 환경이 공존하는 이기종 네트워크 환경의 안전성도 반드시 고려되어야 한다.

따라서 새로운 유비쿼터스 컴퓨팅 환경에서 이기종 네트워크의 기술적인 효율성과 더불어 안전성에 대한 문제가 선행되지 않는다면 여러 가지 사회적인 문제가 발생될 수 있다.

3.2 이기종 네트워크 관리의 보안 요구사항 분석

이기종 네트워크를 구성하는 각 개체들중 최종 개체는 사용자 프라이버시 정보와 밀접한 연관을 지닌 개체이다. 특히, 최종 개체는 각 정보 시스템과의 연계성을 통해 사용자 주변의 정보를 자율적으로 수집하고 관리하는 요소이다. 따라서 안전하고 효율적인 형태의 네트워크 구성을 위해서는 다음과 같은 보안 요구사항을 제시할 수 있다.

- 상호 인증 : 안전한 상호 인증은 비밀값에 기반한 인증 정보를 통해 생성되어야하며, 이를 통해 전체적인 네트워크의 안전성을 유지할 수 있어야 한다.
- 기밀성과 무결성 : 네트워크 구성 개체간에 사용자 프라이버시 정보를 전송할 경우 전송되는 데이터에 대한 기밀성과 무결성을 제공하여 안전성을 유지할 수 있어야 한다.
  * 개체들간 내부 통신의 기밀성 : 네트워크 내부에서 통신은 공격자로부터 안전성을 유지할 수 있도록 기밀성을 제공해야 한다. 따라서 새로운 노드들의 참가/탈퇴에 따라 비인가된 노드들에 대한 네트워크 안전성을 보장해야 한다.
  * 전송 데이터에 대한 기밀성과 무결성 : 이기종 네트워크에서 데이터의 전송과 수신에서 전송 메시지의 기밀성과 무결성을 제공하지 않는다면 개인 프라이버시 정보에 매우 취약한 서비스이므로 전송 데이터에 대한 보안 서비스가 반드시 요구된다.
- 공격자에 대한 안전성 : 이기종 네트워크가 구성될 경우 공격자 혹은 비인가된 제 3자에 의한 인가된 노드들의 안전성을 유지할 수 있어야 한다. 네트워크의 안전성은 내부 공격자 뿐만 아니라 외부 공격자에 대한 안전성을 확보하기 위해서 신뢰된 개체로부터의 안전성을 유지할 수 있어야 한다.
- 참가 노드의 계산 효율성 : 공개키를 이용한 네트워크 관리 방식에서 각 구성 개체들간의 안전한 통신과 관리를 위해서는 비밀 통신이 필요한 개체들만 통신에 참여해야 한다. 특히, 공개키를 이용하는 특성상 보안키 생성등에 요구되는 오버헤드가 전체적인 네트워크의 효율성에 영향을 미쳐서는 안된다.
- 네트워크 관리의 효율성 : 보안 서비스의 연산량 증가로 인해 네트워크 전체의 효율성을 저해해서는 안된다. 따라서 안전성과 효율성이 고루 갖춘 네트워크 관리 방식이 요구된다.

- 관리 정책의 일관성 : 이기종 네트워크의 안전성을 유지시키기 위해서는 신뢰된 개체에 기반한 일관적인 관리가 요구된다.

4. 기존 방식 분석

본 장에서는 기존의 이기종 네트워크 관리 기법에 대해 3장에서 제시한 보안 요구사항을 기반으로 분석하고자 한다.

4.1 Threshold 공개키 방식

본 논문은 1999년 Zhou외 1명이 제안한 방식으로 threshold 공개키 관리 방식을 이용하였다. 제안된 방식은 공개키가 모든 노드에게 알려지고 비밀키는 threshold 방식을 사용해 n개의 노드가 비밀 공유하는 방식이다. 본 방식의 특징은 각 노드가 선택된 특정 노드에 의해 공유한 비밀키를 이용해 상호 인증을 수행하는 방식이다[8]. 그러나 본 방식의 경우 다음과 같은 취약성을 내포하고 있다.

① 관리 방식의 정책 : 각 노드들중에 누가 n개의 노드를 선택할 것인가에 대한 문제점이 발생된다. 즉, 인가되지 않은 노드가 비밀키를 공유하는 노드로 선택될 경우 보안 정책상 문제가 발생될 수 있다. 따라서 신뢰된 개체에 의한 보안 관리의 일관성이 요구된다.

② 상호 인증 : 한 개의 노드는 공개키 서명이 필요한 때를 인지해야 하며, threshold 수에 대하여 특정 노드가 n개의 선택한 노드를 요청할 경우 공개키 서명이 필요한지를 확인할 수 있는 방법이 없다. 따라서 상호 노드들간의 인증이 반드시 요구되며, 이를 위해서 별도의 노드간의 상호 인증 방식이 필요하다.

③ 네트워크 관리의 효율성 : Threshold 값의 사용에 따른 네트워크의 가용성과 강건성의 문제이다. 만약 threshold 값이 클 경우 가용성이 감소하지만 강건성은 증가할 것이다. 따라서 안전성과 효율성을 유지할 수 있어야 한다.

4.2 향상된 Threshold 공개키 방식

제안된 방식은 4.1의 threshold 공개키 방식의 공정성과 가용성을 향상시킨 방식으로 제안되었으며 모든 노드들은 공개키 기관의 역할을 수행한다. 만약 노드의 인증이 요구될 경우 threshold 수를 배포받은 노드들은 각 이웃 노드들과의 통신을 통해 인증 요소를 갱신하거나 생성한다[7]. 그러나 향상된 threshold 공개키 방식은 다음과 같은 보안 취약성을 내포하고 있다.

① 네트워크의 효율성 : 제안된 방식은 참여 노드들이 공개키 기관로써의 역할을 수행함으로써 참여 노드들의 계산 효율성은 네트워크 구성 개체 수가 증가할수록 참여 노드들의 리소스는 매우 큰 오버헤드가 발생하게 된다.

② 외부 공격자에 대한 안전성 : 공격자는 많은 인증 정보들을 선택할 수 있는 충분한 형태의 리소스를 획득할 수 있다. 네트워크의 구성상 공격자는 해당 노드들의 개인키와 공개키 정보들을 충분하게 획득할 수 있어 이를 기반으로 새로운 공격의 보안 취약성이 발생한다.

4.3 ID-Based 방식

2004년에 Deng외 1명이 제안된 ID-Based 네트워크 관리 방식은 모든 노드들이 초기화 상태에서 협력하여 공개키/개인키 쌍을 생성하게 된다. ID-Based 방식은 각각의 노드들의 유일한 IP 주소를 가지고 있거나 인증 정보를 가지고 네트워크에 참여함을 가정함으로써 각 노드들이 시스템의 비밀키 일부만을 공유하고 그 응답으로 인증정보를 전송하는 방식으로 이루어진다. 초기화 과정에서 각 노드들은 반드시 적어도 t개의 이웃 노드들과 연결해야 하며, t개의 노드들은 개인 비밀키를 생성하기

위해 공동적인 연산을 수행하여 이를 안전하게 전송하는 방식이다[2]. 그러나 본 방식의 경우 다음과 같은 취약성을 내포하고 있다.

① 노드들의 효율성 : 각각의 노드들이 이웃 노드들에 비밀키 생성에 참여함으로써 전체 네트워크에 참여하는 노드들의 연산 효율성이 저하될 뿐만 아니라 네트워크 효율성을 저하시키는 문제점이 발생한다.

② 상호 인증 : 각 노드들은 비밀키 생성을 위해 자신의 주변에 노드들을 검색해야 한다. 그러나 안전한 상호 인증 과정 없이 주변의 모든 노드들을 검색하여야 하므로 노드들에 대한 프라이버시 보호가 어렵다는 단점이 존재한다.

③ 임시적인 보안 키 사용 : 본 방식의 경우 t개의 노드들과의 통신을 위해 임시적인 공개키를 사용한다. 그러나 임시적인 공개키에 대한 생성은 각 노드들이 생성하며, 이를 기반으로 개인키 생성에 대한 값을 전송한다. 따라서 각 노드들 간의 상호 인증과 더불어 안전한 통신을 위한 세션키 설립 과정이 요구된다.

5. 이기종 네트워크에서의 안전하고 효율적인 그룹 통신 방식 제안

본 논문에서는 이기종 네트워크에서의 안전하고 효율적인 그룹 통신을 위한 방식을 제안한다. 제안 방식은 정적인 중앙 개체(TTP : Trust Third Party)를 기반으로 서로 다른 사용자 n명이 상호 인증을 요구할 경우 초기 분배된 비밀값을 이용해 인증 정보를 생성하고 중간 개체가 이를 검증하여 n명의 사용자들에 대한 인증이 가능한 방식이다. 따라서 제안 방식은 다음과 같은 가정사항을 기반한다.

- 최종 단말은 이동성을 제공해야하며, 중간 개체와 중앙 개체는 이동성이 없는 신뢰 개체이며, 안전한 통신로를 갖는다.
- 중앙 개체의 공개키 PU_K, 중간 개체의 공개키 $PU_{\lambda I}$는 모든 개체에게 공개되어 있다.

5.1 시스템 계수

다음은 이기종 네트워크 환경에서 안전하고 효율적인 네트워크 관리 방식을 제안하기 위한 시스템 계수를 기술한다.

p, q : 두 소수p, q ($|p|$=1024bit and $|q|$=160bit, $q|p-1$)

g : 위수 $g(_P(g)=q)$

$P()$: 확률 함수 (확률분포 $D=(U,P)$, U는 non-empty set, $u\in U$, $P[u]\in[0,1]$, $\sum_{u\in U} P[u]=1$, $X_i = U\rightarrow\chi_i$)

s, w, x, r : 임의의 랜덤수 ($s,w,x\in {}_RZ_q^*$)

F : Finite field

a : 비밀통신을 위한 비밀값

X_i : $b_{i1},\ldots,b_{im}\in X_i$

$E()$, $D()$: 암호화, 복호화 알고리즘

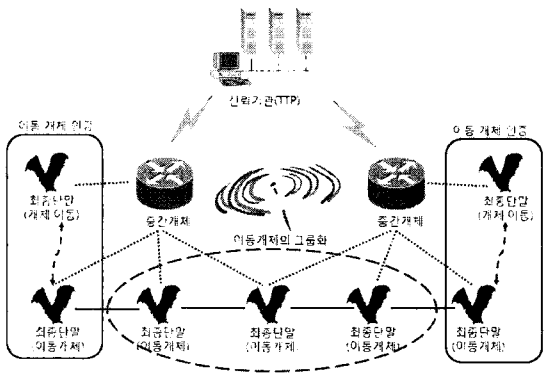
$G()$: 공개 함수

c : $_R\{0,1\}^k$

$H()$: 안전한 해쉬 함수

5.2 제안 방식 시나리오

제안 방식은 이기종 네트워크 환경에서 정적인



(그림 1) 제안방식 시나리오

신뢰기관인 TTP과 중간 개체를 기반으로 최종 단말인 이동개체들로 이루어질 경우 이동 개체들이 이동시 TTP와 중간 개체의 신뢰된 통신을 통해 안전한 인증을 수행하고 이를 그룹화한다. 따라서 이동 개체들간의 상호 인증을 통해 이기종 네트워크의 안전하고 효율적인 관리 방식이며, (그림 1)과 같이 도식화 할 수 있다.

5.3 제안 프로토콜

이기종 네트워크 환경에서 안전하고 효율적인 네트워크 관리 구조를 위해 제안 방식은 다음과 같은 흐름을 갖는다.

[단계 1] 중앙 개체로부터 할당받은 독립적인 랜덤수와 상호 독립적인 값을 생성을 위한 초기 설정 과정
[단계 2] 중간 개체와 중앙 신뢰 개체의 통신
[단계 3] 이동 개체들의 그룹 초기화
[단계 4] 임의의 개체들간의 상호인증을 위한 통신

〔단계 1〕 초기 설정 과정

단계 1은 초기 설정 과정으로서 중앙 개체로부터 할당받은 상호 독립적인 값을 이동개체에서 생성하며 이는 다음과 같다.

① 각각의 이동 개체들은 서로 독립적인 랜덤 값인 $X_1,...,X_n$과 $g_1,....,g_n$의 함수를 중앙 개체로부터 사전에 안전한 과정을 거쳐 저장하고 다음과 같은 상호 독립적인 값을 갖게 된다.

$$g_1(X_1),...,g_n(X_n)$$

Proof . U가 X의 집합일때 X는 랜덤한 값을 갖는다. 만약 X가 실수의 부분집합일때 X는 실수 랜덤값을 갖는다. 만약 $X: U \rightarrow X$가 랜덤 값을 갖는다면 $f: X \rightarrow Y$가 함수일 경우 $f(X) := f \circ X$도 랜덤값을 갖는다. $i = 1,....,n,$ 일 경우 y_i가 $g_i(X_i)$의 임의의 값일 경우 $\chi_i = g_i^{-1}(y_i)$로 정리할 수 있다.

$$P[g_1(X_1) = y \wedge ... \wedge g_n(X_n) = y_n]$$

$$= P[(\bigvee_{x_1 \in \chi_1}$$

$$= P[\bigvee_{x_1 \in \chi_1}$$

$$= \sum_{x_1 \in \chi_1} ... \sum_{x_n \in \chi_n} P[X_1 = x_1 \wedge ... \wedge X_n = x_n]$$

$$= \sum_{x_1 \in \chi_1} ... \sum_{x_n \in \chi_n} P[X_1 = x_1]...P[X_n = x_n]$$

$$=(\sum_{x_1 \in \chi_1} P[X_1 = x_1])...(\sum_{x_n = \chi_n} P[X_n = x_n])$$

$$= P[\bigvee_{x_1 \in \chi_1} \quad ...P[\bigvee_{x_n \in \chi_n}$$

$$= P[g_1(X_1) = y_1]...P[g_n(X_n) = y_n]$$

② 중앙 신뢰 개체는 생성된 $(y_1,....,y_n)$를 중간 신뢰 개체에 전송한다. 전송 후 중간 신뢰 개체는 $y_i \in y_n$을 선택하여 다음과 같은 공개키 PU를 생성한다. (이동 개체 1의 경우 공개키는 PU_1, 개인키는 y_1이다.)

$$PU_i = g^{-y_i} (\mathrm{mod} p)$$

③ 중간 개체는 생성된 공개키 PU_i를 공개함으로써 <단계 1>의 초기 설정 과정을 종료한다.

〈단계 2〉 중간 개체와 중앙 개체의 통신 단계

단계 2는 이동 개체들이 랜덤하게 이동하였을 경우 주변의 개체들과의 인증을 위한 비밀값 생성과 이를 기반으로 중간 개체와 중앙 개체의 통신 과정으로 다음과 같다.

① 임의의 이동 개체들 n개(n=3일 경우)가 상호 인

증이 요구될 경우 임의의 개체 1은 사전에 전송 받은 g_1을 기반으로 Y_1을 생성한 후 a_1을 계산하여 이를 중간개체에 전송한다.

$$Y_1 = X_1^x,\ a_1 = X_1^w$$

② 중간 개체는 a_1을 전송 받은 후 c를 중앙 개체와 이동 개체 1에 전송한다.

③ 이동개체 1은 c를 기반으로 $S = w - cx$를 계산 후 V를 중간 개체에 전송한다.

$$V = E_{g_1}(S)$$

③ 중간 개체는 V를 중앙 개체에 전송하고 중앙 개체는 다음의 과정을 거쳐 검증을 수행한다.

$$a_1 = g_1^S Y_1^c$$

이상의 과정은 상호인증을 요구하는 모든 이동 개체들이 같은 과정으로 수행한다.

〈단계 3〉 : 임의의 이동 개체들간의 그룹 초기화 단계

중앙 개체와 임의의 이동 개체들간의 비밀값에 기반한 통신 단계를 수행하며 이는 다음과 같다.

① 이동 개체 1은 <단계 2>에서 중앙 개체와 공유한 (a_1)을 공개키 PU_T으로 암호화하여 다음을 중간 개체에 전송한다.

$$V = E_{PU_T}(a_1 \| TS)$$

② 중간 개체는 이동 개체 1로부터 전송된 V를 중앙 개체에 전송한 후 임의의 그룹 A로 이동 개체 1의 공개키를 등록한다.

③ V를 전송받은 중앙 개체는 개인키 y_T로 복호화한 뒤 a_1을 확인한 뒤 그 결과를 중간 개체에 전송한다.

④ 중간 개체는 그룹 A에 이동 개체 1이 등록되었음을 전송한다.

$$Reg\_Message$$

이상의 과정을 거쳐 중앙 개체는 이동 개체의 인증 정보를 확인하고 중간 개체는 해당 이동 개체를 임의의 그룹화하여 이를 관리한다.

〈단계 4〉 임의의 개체들간의 상호 인증을 위한 통신 단계

단계 4는 임의의 개체들간의 상호 인증을 위한 통신 단계이며, 임의의 개체는 총 3개로 구성되며 다음은 임의의 이동 개체 1에서 임의의 이동 개체 2, 3과의 상호 인증을 위한 통신 과정이다.

① 이동 개체 1은 임의의 중간 개체에 전송할 랜덤 값 (r_{1_1}, r_{1_2})를 생성한후 이를 공개키로 암호화하여 중간 개체에 V_1, TS를 전송한다.

$$V_1 = E_{PU_M}(r_{1_1}, r_{2_1})$$

② 중간 개체에서는 임의의 이동 개체 1로부터 V_1 확인하고 (r_{1_1}, r_{2_1})를 임시 저장하고 γ_i와 x_{γ_i} $(\gamma_i = \{0, 1\},\ x_{\gamma_i} \in {}_U Z_n)$를 선택하고 ω와 TS를 이동 개체 1에 전송한다.

$$w = E_{K_{PU_1}}(x_{\gamma_1}) + r_{1_1} \bmod n$$

③ 이동 개체 1은 $x_{\gamma_1} = D_{K_{y_1}}(w - r_{1_1} \bmod n)$을 검증한 뒤 <단계 3>의 그룹 초기화 단계에서 중앙 개체와 공유한 a_1을 이용하여 $c_{r_{1_1}}$과 $c_{r_{1_2}}$를 다음과 같이 계산하여 중간 개체에 전송한다. (M_0와 M_1은 임의의 이동 개체들간의 상호 인증을 위한 메시지)

$$c_{r_{1_1}} = E_{a_1}(M_0) + x_{\gamma_1} \bmod n,$$
$$c_{r_{1_2}} = E_{a_1}(M_1) + x_{\gamma_2} \bmod n$$

④ c_{r_1}을 전송받은 중간 개체는

$E_{a_1}(M_0) = c_{r_{1_1}} - x_{\gamma_1} \bmod n$을 계산하여 $E_{a_1}(M_0)$을 중앙 개체에 전송한다.

⑤ 중앙 개체는 $E_{a_1}(M_0)$를 복호화한 뒤 상호 인증 메시지 M_0를 중간 개체에 전송한다.

⑥ 중간 개체는 중앙 개체로부터 전송된 M_0를 임시 저장하고 이동 개체 1로부터 전송된 $E_{a_1}(M_0) = c_{r_{1_1}} - x_{\gamma_1} \bmod n$을 비교한 뒤 올바른 경우 <단계 3>에서 설정된 임시 그룹의 인증 정보 등록하며, 이동 개체 2와 3에 인증 결과를 전송한 뒤 이동 개체 1과의 통신을 종료한다.

6. 제안 방식 분석

본 장에서는 3장에서 제시한 보안 요구사항을 기반으로 제안 방식을 분석하고자 한다.

6.1 안전성 분석

제안된 방식은 이기종 네트워크 환경에서의 안전성을 확보하기 위한 보안 요구사항을 기반으로 하여 다음과 같은 분석할 수 있다.

- 상호 인증 : 제안 방식에서는 중앙 개체로부터 할당받은 독립적인 값인 $g_1(X_1),...,g_n(X_n)$으로 임의의 공개키 $PU(=g^{-y_i}(\bmod p))$를 생성하고 이를 기반으로 $ZKIP$의 검증 이후 분실 통신로를 통해 상호 인증된 통신을 수행한다.
- 기밀성과 무결성 : 제안된 방식은 사용자의 프라이버시 정보를 전송할 경우 데이터의 기밀성과 무결성을 다음과 같이 제공하여 전송 데이터에 대한 안전성을 유지한다.

  ※ 개체들간 내부 통신의 기밀성 : 개체들간의 내부 통신은 변형된 1-out-2 분실 통신로를 이용해 $c_{r_{1_1}} = M_0 + x_{\gamma_1} \bmod n$과 $c_{r_{1_2}} = M_1 + x_{\gamma_2} \bmod n$을 수신한 개체가 공개키 서명을 통해 $M_1 = c_{r_{1_1}} - x_{\gamma_1} \bmod n$을 획득한다. 획득된 메시지는 중간 개체와의 통신에서 상호 인증된 개체들만이 이를 확인할 수 있다.

  ※ 전송 데이터에 대한 기밀성과 무결성 : 이기종 네트워크에서 데이터의 전송과 수신 과정에서 전송 메시지의 기밀성과 무결성은 중앙 개체로부터 생성된 PU와 $ZKIP$을 이용해 기밀성을 유지하며, 안전한 해쉬 함수를 통해 무결성을 제공한다.
- 참가 노드의 계산 효율성 : 제안된 방식은 사전에 서로 독립적인 값인 $X_1,...,X_n$과 $g_1,...,g_n$ 함수를 중앙의 신뢰된 개체로부터 안전하게 전송받은 후 이를 기반으로 독립적인 값을 생성하게 된다. 이는 중앙 신뢰 개체에 전송하고 난 후 중간 개체들이 독립적인 공개키를 생성하여 사용하게 된다. 즉, 독립적인 공개키 생성에 각 노드들은 비밀값을 생성하게 되지만 실제 공개키 연산은 중간 개체들을 활용함으로써 참여 노드들에 대한 효율성을 높이도록 하였다.
- 공격자에 대한 안전성 : 이기종 네트워크가 구성될 경우 공격자는 전송 정보와 개체의 물리적인 공격등을 통해 사용자 프라이버시 침해를 위한 공격 행위를 수행하게 된다. 전송 정보에 대한 안전성은 ACI(Authentication, Confidentiality, Integrity)를 제공하고 있으며, 본 논문에서 개체의 물리적인 안전성과 부인봉쇄 서비스는 고려하지 않았다.
- 네트워크 관리의 효율성 : 제안된 방식은 신뢰된 중앙 개체와 중간 개체에서 공개키와 관련된 연산을 수행함으로써 최종 노드들에 대한 계산적 효율성을 확보했을 뿐만 아니라 통신의 효율성을 위해 1-out-2분실 통신로를 통해 통신 방식의 효율성까지 고려하였다.

6.2 효율성 분석

효율성 측면에서 제안방식은 전체 네트워크의 효율성을 높이기 위해서 1-out-2 분실 통신 방식을 변형하여 제안하였다.

이동 개체의 상호인증을 위한 메시지 $c_{r_{1_1}} = E_{a_1}(M_0) + x_{\gamma_1} \bmod n$과 $c_{r_{1_2}} = E_{a_1}(M_1) + x_{\gamma_2} \bmod n$는 중간 개체를 거쳐 중앙 개체에서 이를 확인할 수 있다. 따라서 중간 개체는 상호 인증 메시지의 정당성만을 확인할 수 있어 인증 정보에 대한 중앙 집중형 관리 방식이다.

이는 이기종 네트워크의 구성 개체들간의 안전한 통신 과정을 위해 통신 횟수의 효율성을 위해 신뢰된 개체가 네트워크 통신에 참여함으로써 안전성 뿐만 아니라 전체 네트워크의 효율성을 증가시키고자하였다. 그러나 본 논문에서는 안전성 향상을 위해 다양한 암호 알고리즘과 이산대수 방식을 사용함에 따라 계산량의 비효율성은 여전히 내포하고 있어 다양한 적용성을 저해하는 요소로 될 수 있다. 또한 변형된 1-out-2 분실 통신 방식을 이기종 네트워크에서 사용될 경우 다양한 네트워크간의 통신에서 연속적인 메시지가 모두 소실될 확률이 높아져 통신의 문제점을 내포한다.

〔표 1〕 제안 방식 비교 분석

보안 요구사항		Threshold 방식	향상된 Threshold 방식	ID-Based 방식	제안 방식
상호인증		△	O	△	O
기밀성과 무결성	개체들간 내부 통신의 기밀성	O	O	△	O
	전송 데이터에 대한 기밀성과 무결성	O	O	O	O
공격자에 대한 안전성		O	×	O	O
참가 노드의 계산 효율성		O	△	×	O
네트워크 관리의 효율성		×	×	O	O
관리 정책의 일관성		×	O	O	O

[X : 취약, △ : 보통, O : 안전]

이상의 내용을 기존방식과 비교해 볼 경우 [표 1]과 같이 정리할 수 있다.

7. 결론

유비컴퓨팅 환경의 무선 네트워크 기술은 향후 사용자들에게 아주 많은 편리함을 제공해 줄 수 있는 신기술임에도 불구하고 보안적인 사항이 고려되지 않는다면, 악의적인 목적을 가진 사용자들에 의한 개인 프라이버시 침해와 같은 공격적 취약점을 도출 시킬 수 있다.

유비컴퓨팅 환경의 이기종 네트워크는 다양한 네트워크가 공존할 수 있는 유비컴퓨팅 환경의 특성상 다양한 형태로 존재할 수 있는 네트워크 구조이다. 따라서 이기종 네트워크에서의 안전성이 확보되지 않을 경우 사용자 프라이버시 침해 뿐만 아니라 안전한 u-지식사회 구축이 어려워진다. 이에 본 논문에서는 안전한 u-지식사회 구축을 위해 유비컴퓨팅 환경의 이기종 네트워크의 안전하고 효율적인 형태의 네트워크 관리 방식을 제안하였다. 제안된 방식은 이동 개체들의 안전성 확보를 위해 다양한 보안 요구사항을 만족할 수 있는 안전성과 효율성을 고루 갖춘 방식을 제안하였다. 그러나 제안된 방식에서는 성능 평가를 위한 정량적 지표에 대한 정의나 평가가 이루어지지 않아 실제 적용시 발생할 수 있는 네트워크 효율성에 대해서는 평가가 이루어지지 않았다. 따라서 제안된 방식은 유비컴퓨팅 환경에서 다양한 네트워크 환경이 공존하는 구조에서 안전성과 효율성이 요구되는 환경에 적용될 수 있으나 보안적인 사항 뿐만 아니라 네트워크의 효율성까지 확보할 수 있도록 추가적인 보안 요소를 정의하고 이를 기반으로 정량적 지표의 평가를 향후 연구에서 추진하고자 한다.

참 고 문 헌

[1] Capkun S, Buttyan L, Hubaux JP, "Self-organized public-key management for mobile ad hoc

networks," IEEE Transaction on Mobile Computing 2003; 2(1): pp52-64, 2003.

[2] Deng H and Agrawal DP, "TIDS: threshold and identity-based security scheme for wireless ad hoc networks," Ad Hoc Networks 2004; 2(3): pp291-307, 2004.

[3] Yuh-Min Tseng, "A heterogeneous-network aided public-key management scheme for mobile ad hoc networks," International Journal of Network Management 2007, pp3-15, 2007.

[4] Brett C. Tjaden, Lonnie R. Welch and Shawn D. Ostermann, David Chelberg, "INBOUNDS: The Integrated Network-Based Ohio University Network Detective Service", 4th World Multi conference on Systemics, Cybernetics and Informatics (SCI 2000) and 6th International Conference on Information Systems Analysis and Synthesis (ISAS 2000), pp23-26, 2000.

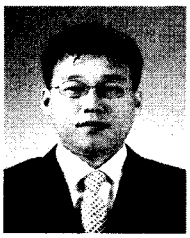
[5] http://www.crhc.uiuc.edu/EASY/Papers/robinson-easy01.pdf

[6] Gang W and Mitsuhiko M, "MIRAI Architecture for Heterogeneous Network," IEEE Communication Magazine, pp126-134, 2002.

[7] Kong J, Zerfos P, Luo H, Lu S and Zhang L, "Providing roubst and ubiquitous security support for mobile ad hoc networks," In IEEE Ninth International Conference on Network Protocols (ICNP'01), pp251-260, 2001.

[8] Zhou L and Haas Z, "Securing, ad hoc networks". IEEE Networks 1999; 13(6): pp23-60, 1999.

◐ 저 자 소 개 ◑



서 대 희(Seo Dae-Hee)
2003년 순천향대학교 대학원 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2007년 Post-Doc of Howard University
2008년 현재 이화여자대학교 연구교수
관심분야 : 네트워크 보안, 근거리 무선통신 보안, 보안성 평가, 유비쿼터스 컴퓨팅
E-mail : dhseo@ewha.ac.kr

백 장 미(Baek Jang-Mi)
2003년 순천향대학교 대학원 전산학과 졸업(석사)
2006년 순천향대학교 대학원 전산학과 졸업(박사)
2007년 Post-Doc of Howard University
2008년 현재 순천향대학교 시간강사
관심분야 : 임베디드 시스템, 유비쿼터스 네트워크, 유비쿼터스 컴퓨팅
E-mail : bjm1453@sch.ac.kr

조 동 섭(Cho Dong-Sub)
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
관심분야 : 임베디드 보안, 웹서비스 아키텍처, 휴먼컴퓨팅, 웹서버 엔지니어링
E-mail : dscho@ewha.ac.kr