情報保護學會論文誌
第19卷 第5號, 2009. 10

유비쿼터스 오피스 네트워크에서의 Main/Sub 디바이스 인증/인가 프로토콜*

문 종 식,† 이 임 영‡
순천향대학교 컴퓨터학부

Main/Sub Device Authentication and Authorization Protocol in Ubiquitous Office Network*

Jong-Sik Moon,† Im-Yeong Lee‡
Division of Computer Science and Engineering, Soonchunhyang University

요 약

현대사회는 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 정보사회라는 새로운 문화적 변환기를 맞이하고 있으며, 다양한 서비스 및 디바이스의 발전을 가져오고 있다. 그러나 보안 측면에서 고려해야 할 요구사항은 더욱 복잡해지고 다양화되고 있으며, 기존의 매체나 프로토콜이 갖고 있는 보안 취약성을 그대로 내포하게 된다. 유비쿼터스 오피스 네트워크 환경에서 이동성을 제공하는 디바이스는 상대적으로 컴퓨팅 능력이 낮아 기존에 개발된 보안 기능의 탑재가 어려우므로 단말 해킹, 바이러스 공격, 정보유출 등 다양한 공격이 시도될 가능성이 높다고 할 수 있다. 이에 대한 대책으로 제안된 PKI 인증 기술은 유비쿼터스 오피스 네트워크 서비스 제공 구조인 멀티도메인 환경에 적용하기에 적합하지 않으며, 변형된 인증체계 개발이 필요하다. 따라서 본 논문에서는 아이디 기반 공개키 방식 및 인가 티켓을 이용하여 안전하고 효율적인 로밍과 Main 디바이스 인증/인가 기술 및 Sub 디바이스 티켓을 이용한 인증/인가 기술에 관한 연구를 통하여 안전성과 효율성을 제공할 수 있다.

ABSTRACT

In modern society, as the rapid development of IT technology combined with the computer-based high-speed communication networks makes it possible to provide a wide spectrum of services and devices, we have been confronting a new cultural transformation era, referred to as the information society. However, the requirements to be considered in security aspect have became more complicated and diversified, and there remains the same security weaknesses as in the existing media or protocol. Particularly, the office network device with roaming is susceptible to the different kinds of attacks such as terminal hacking, virus attacks, and information leakage because the computing capacity is relatively low and the loading of already developed security functions is difficult. Although developed as one solution to this problems, PKI security authentication technology isn't suitable for multi-domain environments providing uonments proffice network service, and so the development of a novel authentication system is needed. Therefore, in this paper researched the roaming and device authentication/auth for multitechnology using an ID-based public key, authorization ticket, and Sub-device ticket with a purpose to contribute to the development of the secured and efficient technology.

Keywords: Authentication, Authorization, Device, Office Network

접수일(2009년 7월 27일), 게재확정일(2009년 9월 1일)
* 본 연구는 교육과학기술부와 한국산업기술진흥원의 지역혁신인력양성사업으로 수행된 연구결과임.

† 주저자, comnik528@sch.ac.kr
‡ 교신저자, imylee@sch.ac.kr

I. 서 론

네트워크 및 디바이스의 발전과 방송·통신·네트워크·서비스 등 다양한 분야의 기술들이 융합되어 u-지식사회로의 빠른 이동 등 IT 기술이 전반적인 환경에서 변화를 가져오고 있다. 이러한 환경에서 기존의 네트워크 인프라는 홈 네트워크 및 오피스 네트워크로 발전하고 있으며, 오피스 네트워크 기술은 유선뿐만 아니라 무선 측면에서도 빠른 발전을 이루고 있다. 또한 기존의 기술들이 홈 네트워크 및 오피스 네트워크 환경에 집약되어 통합 서비스를 제공해 나가는 방향으로 많은 연구가 진행되고 있다. 그러나 언제 어디서나 컴퓨팅이 가능한 유비쿼터스 컴퓨팅 사회에서는 개인의 컴퓨팅 환경 의존도가 증가함에 따라 사이버공격뿐만 아니라 오피스 네트워크 및 오피스 디바이스의 취약성을 이용하여 사내 오피스 네트워크에 대한 불법적인 접근이 가능하다. 따라서 오피스 디바이스에 대한 안전성 확인을 통해 정당한 사내 오피스 디바이스만 오피스 네트워크에 접근할 수 있어야 한다. 또한 정당하지 않은 디바이스의 서비스 이용을 차단하기 위해 다양한 보안기술 및 오피스 네트워크 서비스를 제공받는 디바이스에 보안기술을 적용하여 정당한 디바이스를 통해서만 서비스를 제공받을 수 있게 하는 한 단계 강화된 보안의 필요성이 제기되고 있다[1-8]. u-지식사회 오피스 네트워크로의 진화는 다양한 서비스 도메인에서 디바이스 이동이 증가될 것이며, 오피스 디바이스간의 협업에 의한 새로운 서비스가 증가할 것이다. 이와 같은 기술의 진화에 따라 u-지식사회 환경에서 안전한 이동과 끊김 없는 서비스를 제공할 수 있도록 경량화된 오피스 디바이스 인증/인가 기술이 필요하다. 따라서 본 논문에서는 오피스 네트워크 환경에서 다양한 서비스의 요구사항을 고려하여 Main/Sub 디바이스 인증/인가 기술에 관한 연구를 진행하여 안전성과 효율성을 높이고자 하였다. 본 논문에서 정의하고 있는 Main 디바이스는 사내에서 일반적으로 사용하는 개인용 컴퓨터 및 노트북 등 연산능력 및 컴퓨팅 파워가 충분한 디바이스를 의미한다. 그리고 Sub 디바이스는 Main 디바이스 사용자가 소유한 연산능력이 낮고 저전력 디바이스이며, 이동 중 사용할 수 있는 스마트 폰, PDA 등과 같은 네트워크 접속이 가능한 디바이스이다. 본 논문의 구성은 다음과 같다. 2장에서는 디바이스 인증/인가 기술동향 및 보안 요구사항에 대하여 기술하고, 기반 기술을 설명한다. 3장에서는 기존연구를 분석하고, 4장에서는 안전한 Main/Sub 디바이스 인증/인가 기술을 제안한다. 5장에서는 제안 방식을 요구사항 및 효율성에 맞추어 분석하고, 마지막으로 6장에서는 결론 및 향후 연구 방향을 제시하고자 한다.

II. 연구 배경

본 장에서는 오피스 네트워크에서의 보안 요구사항에 대하여 분석하고 기반 연구가 되는 겹선형 쌍함수의 개요에 대하여 설명한다.

2.1 보안 요구사항 및 오피스 네트워크 요구사항

기존의 유선 네트워크와는 다르게 오피스 네트워크에서는 기존의 일반적인 보안 요구사항과 정당하지 않은 제 3자의 공격에 따른 요구사항을 고려해야 한다. 또한 자신의 오피스 네트워크 내에서 제공하는 서비스 외에 다른 사업자가 제공하는 오피스 네트워크로 이동하여 서비스를 제공받을 수 있기 때문에 그에 대한 요구사항도 고려해야 한다.

2.1.1 보안 요구사항

- 기밀성: 오피스 네트워크 환경에서 통신되는 데이터는 정당한 객체만이 확인할 수 있어야 한다. 데이터의 출처와 목적지, 횟수, 길이, 또는 통신 선로상의 트래픽 특성에 대하여 공격자로부터 불법적인 획득으로 비밀 값을 노출되지 않도록 해야 한다.
- 무결성: 오피스 네트워크 디바이스간의 통신 및 서버간의 통신에 있어 네트워크를 통해 전송되는 데이터가 위·변조 되거나 삭제되지 않도록 해야 한다.
- 인증: 오피스 네트워크 서비스를 이용하고자 접근하는 디바이스가 전송한 메시지 또는 인증정보의 출처가 정확히 확인되고, 그 실체의 신분이 거짓이 아닌 정당한 디바이스라는 것을 검증할 수 있어야 한다.
- 접근제어: 오피스 네트워크 서비스의 모든 접근 행위에 대해 그 권한을 명백히 구분해 허가되지 않은 디바이스의 접근 시도를 사전에 차단할 수 있도록 하는 통제가 필요하다.

2.1.2 제 3자의 공격에 따른 요구사항

- 도청 공격: 오피스 네트워크를 통해 전송되는 데이

터가 제 3의 공격자에게 노출될 수 있기 때문에 도청 공격에 안전하기 위해서는 제 3자가 데이터를 획득하더라도 비밀 값을 유추할 수 없도록 해야 한다.

- 재전송 공격: 오피스 네트워크에서 전송되는 데이터를 제 3자가 획득하여 메시지를 재전송함으로써 인증 받거나 서비스를 제공 받는 것을 막을 수 있어야 한다.
- 패스워드 추측 공격: 오피스 네트워크상에서 악의적인 제 3자가 전송되는 메시지를 분석하여 패스워드를 추측할 수 있다. 따라서 통신 중에 전송 되는 메시지를 분석하여 패스워드를 추측하는 것을 막아야 한다.

2.1.3 오피스 네트워크에서의 요구사항

- 빠른 로밍 인증: 사내 오피스 네트워크 환경에서 다른 서비스 제공자가 제공하는 사외 오피스 네트워크의 서비스를 이용하고자 이동할 경우, 인증에 소요되는 시간이 오래 걸리게 되면 끊김 없는 서비스를 제공할 수 없다. 따라서 이동 디바이스에게 끊김 없는 서비스를 제공하기 위해서는 인증 소요시간이 짧으며, 경량화된 인증에 대한 고려가 필요하다.
- 오피스 인증 서버의 오버헤드: 다른 사업자가 제공하는 오피스 네트워크 서비스를 이용할 경우, 원격지에서 오피스 인증 서버로 전송되는 인증 요청이 빈번하게 일어나면 오피스 인증 서버의 오버헤드가 발생할 수 있다. 따라서 사내 오피스 네트워크 인증 서버로 요청되는 인증 및 접근을 감소시키거나 분산시켜 오버헤드를 줄이는 방안에 대한 고려가 필요하다.
- Main/Sub 디바이스 사용: 오피스 네트워크 환경에서는 개인 PC 및 노트북 등을 이용하여 서비스를 제공받을 것이다. 그러나 사용자는 이러한 고성능의 Main 디바이스 이외에 저전력, 소형화의 Sub 디바이스를 이용하여 서비스를 제공받고자 할 것이며, 사내 네트워크 이외에 다른 네트워크로 이동하면서도 서비스를 제공받을 수 있어야 한다. 따라서 Main 디바이스 이외에 Sub 디바이스를 이용하는 방식을 고려해야 한다.

2.2 겹선형 쌍함수

겹선형 쌍함수(Bilinear Pairing)[9-11]는 타원곡선 상의 이산대수 문제를 유한체상의 이산대수 문제로 축소시켜 그 어려움을 줄여 타원곡선 암호시스템을 공격하는 도구로 원래 제안되었다. 최근에는 공격 도구가 아닌 정보보호를 위한 암호학적 도구로 사용되고 있으며, 겹선형 쌍함수는 다른 말로 겹선형 사상(Bilinear Map)이라 한다. 이 절에서는 다음과 같은 표기법을 사용하며, 이 사상의 정의는 다음과 같다.

- q : 매우 큰 소수
- G_1 : 위수가 q인 타원곡선 위의 덧셈군
- G_2 : 위수가 q인 유한체 위의 곱셈군
- $P, Q, R \in {}_RG_1$
- $a, b, c \in {}_RZ_q^*$
- $e: G_1 \times G_1 \rightarrow G_2$ 겹선형 사상

[정의 1] 다음과 같은 특성을 만족하는 $e: G_1 \times G_1 \rightarrow G_2$를 사용하는 Admissible Bilinear Map이라 한다.

- 겹선형(Bilinear): 임의의 P, Q, R에 대하여 다음이 성립해야 한다.
  - $e(P, Q+R) = e(P, Q) \cdot e(P, R)$
  - $e(P+Q, R) = e(P, R) \cdot e(Q, R)$
  - $e(aP, bQ) = e(P, Q)^{ab}$
- 비퇴화성(Non-Degenerate): G_1의 모든 쌍 P, Q에 대하여, $e(P, Q)$는 G_2의 항등원이 아니어야 한다.
- 계산가능성(Computable): 임의의 P, Q에 대하여 $e(P, Q)$를 계산할 수 있는 효율적인 알고리즘이 존재해야 한다.

겹선형 사상의 특성에 의해 다음이 성립한다.

$$e(aP, bQ) = e(P, bQ)^a = e(aP, Q)^b$$
$$= e(P, Q)^{ab} = e(abP, Q) = e(P, abQ)$$

이 사상 때문에 타원곡선 상에서 D-H 결정 문제는 다음과 같이 정의 된다.

$$e(aP, bQ) = e(cP, P) \Rightarrow ab = c$$

따라서 겹선형 사상을 암호학적 도구로 사용하는 많은 암호프로토콜에서는 다음 문제의 어려움에 기반하고 있다.

[정의 2] (BDHP, Bilinear Diffie-Hellman Problem) G_1의 원소 P, aP, bP, cP가 주어졌을 때,

$e(P, P)^{abc}$를 계산하는 문제를 말한다.

이 문제는 타원곡선 이산대수 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP로부터 a를 계산할 수 있으면 $e(bP, cP)^a$를 통해 $e(P, P)^{abc}$를 계산할 수 있다. 뿐만 아니라 이 문제는 타원곡선 D-H 문제를 해결할 수 있으면 해결할 수 있다. 예를 들어 aP, bP로부터 abP를 계산할 수 있으면 $e(abP, cP)$를 통해 $e(P, P)^{abc}$를 계산할 수 있다.

III. 기존 연구

기존에 연구된 디바이스 인증/인가 방식 중 Inter-Domain 디바이스 인증/접근제어 방식과 S/Key 기반 홈 디바이스 인증 방식을 분석하면 다음과 같다.

3.1 Inter-Domain 디바이스 인증/접근제어 방식

Inter-Domain 디바이스 인증/접근제어 방식은 효율적인 통신과 사용자 편의를 위해 Two-layer PKI 기반 디바이스 인증과 접근제어 방식을 제안하였다[12,13]. 이 방식에서의 Two-layer는 글로벌 PKI layer와 지역적 PKI layer이며, 글로벌 PKI layer는 기존의 PKI 모델을 사용하였다. Inter 홈 네트워크의 디바이스 등록과 인증을 위해서 글로벌 PKI layer를 사용하였으며, 각 종단 디바이스 인증을 위해 지역적 PKI layer를 사용하였다. Inter-Domain 디바이스 인증/접근제어 방식은 안전성과 효율성 그리고 Multi-Domain 디바이스 인증 프로토콜로 사용자의 편의성을 제공하며, Attribute Mapping Certificate를 사용하여 접근제어 방식의 편의성을 제공한다. 그러나 PKI 기반 방식을 사용함으로써 계산량의 효율성이 떨어지며, Root CA와 홈 게이트웨이에 오버헤드가 발생한다. 또한 Manufacturer의 추가로 인해 통신량이 증가되는 단점이 있다. 다음은 Inter-Domain 디바이스 인증/접근제어 방식에서 사용되는 시스템 계수이다.

- $GCert_X$: Global CA가 X에게 발행한 X.509 인증서
- $CCert_{XY}$: Domain X가 domain Y에게 발행한 cross domain 인증서
- $LCert_{XY}$: Home 게이트웨이 X가 Y에게 발행한 local 디바이스 인증서
- N_X: 재전송 공격을 막기 위해 X가 생성한 난수

From → To	Message
1: $D \rightarrow H$	*Registration request*
2: $H \rightarrow D$	N_H
3: $D \rightarrow H$	$(D_{ID}, N_D, N_H)K_{MD}$
4: $H \rightarrow M$	$(D_{ID}, N_D, N_H)K_{MD}, (N_H, N_D, SecretID)K_{H^{-1}}, Gcert_H$
5: $M \rightarrow H$	$(K_H, N_D)K_{MD}, DevInfo, (N_H, DevInfo)K_{M^{-1}}, Gcert_M$
6: $H \rightarrow D$	$(K_H, N_D)K_{MD}, Lcert_{HD}$

[그림 1] 디바이스 등록 프로토콜

From → To	Message
1: $C \rightarrow H_S$	$N_C, Lcert_{H_C C}$
2: $H_S \rightarrow H_C$	$Gcert_{H_S}$
3: $H_C \rightarrow H_S$	$Gcert_{H_C}, Ccert_{H_C H_S}$

[그림 2] Inter-domain 결합 프로토콜

From → To	Message
1: $C \rightarrow H_S$	$N_C, Lcert_{H_C C}$
2: $H_S \rightarrow C$	$Ccert_{H_C H_S}, (N_C)K_{H_S^{-1}}, AttMappingCert$

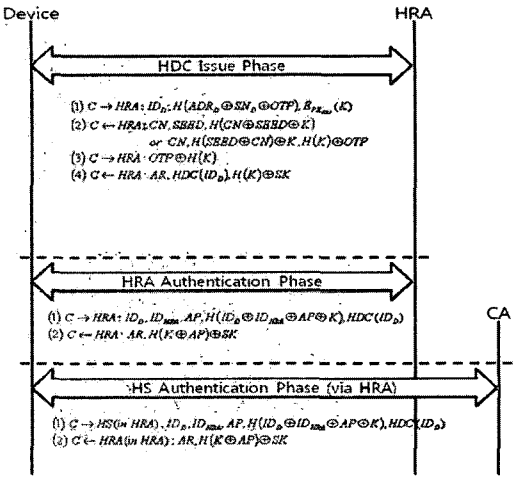
[그림 3] Inter-domain 디바이스 인증 프로토콜

- K_{XY}: X와 Y가 공유한 대칭키, K_X : X의 공개키
- $(\ )K_{XY}$: 대칭키 K_{XY}를 이용한 암호화, $(\ )K_X$: X의 공개키를 사용한 암호화
- $(\ )K_{X^{-1}}$: X의 개인키를 사용한 서명
- M: 제작사 서버, D: 디바이스, H: 홈 게이트웨이
- C: 클라이언트 디바이스, S: 서비스 디바이스, H_X: X가 속해있는 홈 게이트웨이
- X_{ID}: X의 아이디

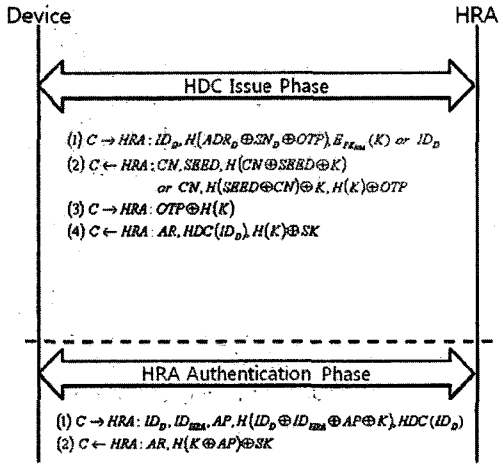
본 방식에서의 등록, 결합, 인증에 대한 프로토콜은 [그림 1], [그림 2], [그림 3]과 같다.

3.2 S/Key 기반 홈 디바이스 인증 방식

S/key 기반 홈 디바이스 인증 방식[14,15]은 홈 네트워크 보안의 기본적이고 본질적 요소의 홈 디바이스 인증을 소개하며, 스마트 홈 네트워크에서 안전한 무선 접근을 위해 S/Key 기반 외부 홈 인증 방식과 내부 홈 인증 방식을 제안하여, 홈 네트워크 서비스 사용자의 편의성 및 안전성을 제공하였다. 그러나 Exclusive OR 연산으로 계산량의 감소는 가져왔으나 통신로 상의 도청으로 인해 비밀정보의 유출 및 재전송 공격에 취약하며 HDC(Home Device Certificate) 발행단계로 인한 통신량이 증가되는 단점을 가지고 있다. 본 방식의 내부 및 외부 인증 프로토콜은 [그림 4], [그림 5]와 같다. 다음은 S/Key 기반



〔그림 4〕 외부 홈 인증 프로토콜



〔그림 5〕 내부 홈 인증 프로토콜

홈 디바이스 인증 방식의 시스템 계수이다.

- *HRA*: Home RA
- *HS*: Home RA에서의 홈 서비스
- ID_X: X의 아이디
- *SN*: 시리얼 번호
- *OTP*: 일회용 패스워드
- *CN*: 카운트 넘버
- *AR*: 인증 결과 값
- *SK*: 세션키
- *HDC*: 홈 디바이스 인증서
- *ADR*: 디바이스의 주소

IV. Main/Sub 디바이스 인증/인가 제안 방식

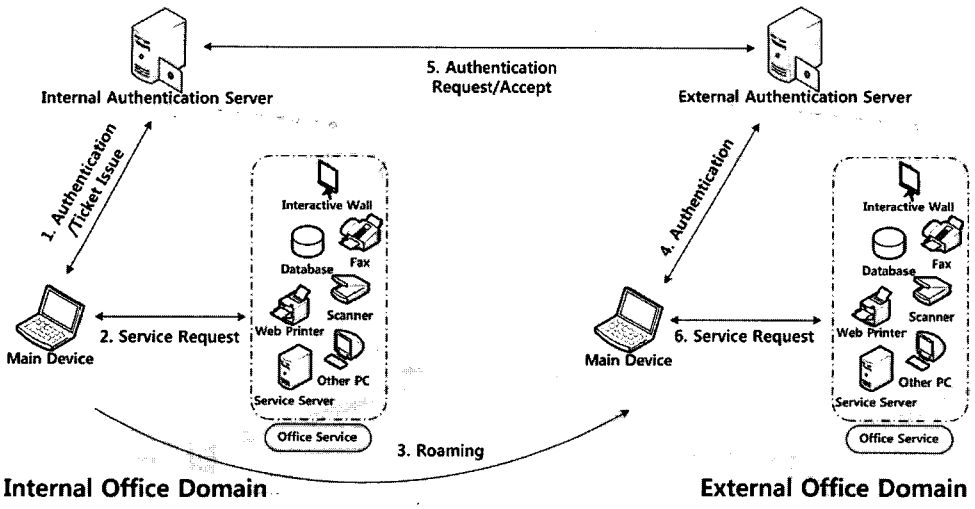
디바이스 인증 기술 중 PKI 인증 기술은 단일 도메인의 개체 간 상호인증을 위해 제 3자인 공인 인증기관의 서명확인을 통해 인증을 받는 방식이므로 유비쿼터스 오피스 서비스 제공 구조인 멀티도메인 환경에 적용하기 위해서는 추가 기술개발이 필요하며 센서 디바이스에 응용하기에 연산량 등의 문제가 있어 적용하기 어렵다. 따라서 유비쿼터스 오피스 네트워크 멀티도메인 환경에 호환 적용이 가능한 변형된 인증체계 개발이 필요하며, 제안 방식은 이를 해결하고자 Main 디바이스 로밍 및 인증/인가 프로토콜과 Sub 디바이스 티켓을 이용한 인증/인가 프로토콜을 제안하였다.

Main 디바이스 로밍 및 인증/인가 프로토콜은 유비쿼터스 오피스 네트워크 환경에서 사내 오피스 네트워크에서 서비스를 제공받던 디바이스가 사외 오피스 네트워크로 이동하였을 때 사내 오피스 인증 서버로부터 발급받은 인가 티켓을 기반으로 서비스를 지속적으로 제공 받을 수 있다. Sub 디바이스 티켓을 이용한 인증/인가 프로토콜은 오피스 네트워크 환경에서 Main 디바이스가 인증을 요청하고 티켓을 발행받으면 인가 티켓을 기반으로 오피스 네트워크 서비스를 제공받을 수 있다. 또한 Main 디바이스 외에 연산능력 및 컴퓨팅 파워가 부족한 Sub 디바이스를 가지고 서비스를 제공받자 할 때 Sub 디바이스 인가 티켓을 Main 디바이스가 사내 오피스 인증 서버로부터 발행받아 분배해주면 Sub 디바이스는 티켓을 가지고 오피스 네트워크 서비스를 제공받을 수 있다. 이와 같은 방식으로 경량화된 아이디 기반 인증/인가를 제공할 수 있으며, 안전성과 효율성을 제공할 수 있다.

4.1 Main/Sub 디바이스 인증/인가 방식 시스템 계수

본 논문에서 제안하는 2가지 프로토콜이 사용하는 시스템 계수는 다음과 같다.

- *: 각각의 개체 (*MD*: Main 디바이스, *SD*: Sub 디바이스, *IOAS*: 사내 오피스 인증 서버, *EOAS*: 사외 오피스 인증 서버, *HOS*: 사내 오피스 서비스 개체, *EOS*:사외 오피스 서비스 개체)
- ID_*: *의 아이디
- ID_{SD_i}: Sub 디바이스의 아이디(i=1, 2, 3, …, $n(1 \le n \le 10)$)
- *PIN*: 디바이스의 식별번호



〔그림 6〕 Main 디바이스 로밍 및 인증/인가 방식 전체 흐름도

- *OTP*: 일회용 패스워드
- g: 곱셈군 Z_n^*의 생성자
- $h()$: 안전한 일방향 해쉬 함수
- *CT*: OTP 입력 값으로 *MD*와 *IOAS*! 간에 동기화 되어 있는 카운터
- *TS*: OTP 입력 값으로 *MD*와 *IOAS* 간에 동기화 되어 있는 시간 값
- e: $G_1 \times G_1 \rightarrow G_2$ 겹선형 사상
- $E_*[\,]$: *의 키로 암호화
- $Sign_*$: *의 개인키로 서명
- *KS*: 신뢰된 개체들 간에 공유한 대칭키
- *Service_key*: 인증 서버와 서비스 개체 간의 공유한 대칭키
- KU_*: *의 아이디 기반 공개키
- KR_*: *의 아이디 기반 개인키

4.2 Main 디바이스 로밍 및 인증/인가 방식

Main 디바이스 로밍 및 인증/인가 방식은 유비쿼터스 오피스 네트워크 환경에서 개인용 컴퓨터 및 노트북 등의 디바이스가 안전하고 효율적으로 오피스 서비스를 이용할 수 있는 방식이다. 이와 같은 시나리오는 사내에서 사외로의 출장 및 본사에서 지사로의 파견 등이 있을 수 있으며, 사내에서 사내로 이동할 경우도 이에 해당한다. 디바이스가 서비스를 제공받고자 할 때, 오피스 인증 서버로부터 인증을 받고 인가 티켓을 발급받아 오피스 네트워크 서비스 개체에게 인가 티켓을 제시하여 서비스를 제공받을 수 있다. 또한 디바이스가 사내 오피스 네트워크 외에 사외 오피스 네트워크 서비스를 이용할 경우 사외 오피스 인증 서버로 사내 오피스 인증 서버에서 발급받은 인가 티켓을 제시하고 인증을 받으면 서비스를 제공받을 수 있다(〔그림 6〕 참조). Main 디바이스 로밍 및 인증/인가 프로토콜은 사내 오피스 네트워크에서 인증 및 티켓 발행 단계와 사외 오피스 네트워크 로밍 시 인증 단계로 이루어진다. Main 디바이스와 사내 오피스 네트워크 인증 서버 간 공유한 대칭키 및 동기화 값은 디바이스 등록 시 분배 및 설정 되었다고 가정하며, 대칭키는 안전성을 위해 일정한 주기로 갱신한다.

4.2.1 사내 오피스 네트워크에서 인증 및 티켓 발행 단계

본 단계에서는 Main 디바이스가 오피스 서비스를 제공받기 위해 사내 오피스 인증 서버에게 인증을 요청하고, 사내 오피스 인증 서버는 Main 디바이스의 정당성을 검증한 후 사내 및 사외 오피스 네트워크에서 사용할 수 있는 인가 티켓을 발행한다. Main 디바이스는 발행받은 인가 티켓을 기반으로 사내 오피스 서비스 및 사외 오피스 서비스를 제공받을 수 있다.

Step 1. Main 디바이스(*MD*)와 사내 오피스 인증 서버(*IOAS*)는 서로 공유한 대칭키(*KS*) 및 아이디를 입력 값으로 각각 아이디 기반 공개키(*KU*)/개인키(*KR*) 쌍을 생성한 후, Main 디바이스는 인증을 위한 일회용 패스워드(*OTP*)를 생성한다. 일회용 패스워드

는 디바이스의 식별번호, 공유한 대칭키, 공유한 카운터 값과 동기화 시간 값을 XOR 연산하여 해쉬한 값이다.

$$MD: KU_{MD} = ID_{MD},\ KR_{MD} = ID_{MD} \cdot g^{KS},\ OTP = h(PIN \oplus KS \oplus CT \oplus TS) \quad (1)$$

$$IOAS: KU_{IOAS} = ID_{IOAS},\ KR_{IOAS} = ID_{IOAS} \cdot g^{KS} \quad (2)$$

Step 2. Main 디바이스는 인증을 받기위해 생성한 일회용 패스워드와 공유한 카운터 값을 사내 오피스 인증 서버의 공개키로 암호화하여 Main 디바이스의 아이디 및 사내 오피스 인증 서버의 아이디와 함께 인증 서버에게 전송한다.

$$MD \rightarrow IOAS :: ID_{MD},\ ID_{IOAS},\ E_{KU_{IOAS}}[OTP,\ CT] \quad (3)$$

Step 3. 사내 오피스 인증 서버는 전송된 값 중 암호화된 값을 복호화한 후, Main 디바이스가 전송한 값을 검증하기 위해 서버에 저장되어 있는 디바이스의 식별번호, 대칭키, 카운터 값, 시간 값을 XOR 연산하여 일회용 패스워드(OTP')를 생성한다. 생성한 일회용 패스워드와 Main 디바이스가 전송한 일회용 패스워드를 비교하여 값이 일치하면 정당한 Main 디바이스로 인증한다.

$$IOAS: OTP' = h(PIN \oplus KS \oplus CT \oplus TS) \quad (4)$$

$$OTP' \stackrel{?}{=} OTP \quad (5)$$

Step. 4. Main 디바이스의 인증이 완료되면 사내 오피스 인증 서버는 Main 디바이스가 사내 오피스 서비스를 이용하거나 사외 오피스 네트워크로 접근할 때 인증 값으로 사용할 수 있는 인가 값(*Authorization Value*)과 인가 티켓(*Authorization Ticket*)을 생성한다. 인가 값은 사내 오피스 인증 서버의 개인키, Main 디바이스의 아이디, 공유한 대칭키를 입력 값으로 하여 ABM(Admissible Bilinear Map)을 기반으로 생성한다. 인가 티켓은 Main 디바이스의 아이디, 사내 오피스 인증 서버의 아이디와 생성한 인가 값을 해쉬하여 사내 오피스 인증 서버의 개인키로 서명한 값으로 구성한다.

$$Authorization\ Value = e(KR_{IOAS},\ ID_{MD} \cdot KS) \quad (6)$$

$$Authorization\ Ticket = ID_{MD},\ ID_{IOAS},\ Sign_{IOAS}[h(Authorization\ Value)] \quad (7)$$

인가 티켓은 Main 디바이스가 오피스 서비스를 이용하고자 할 때, 사내 오피스 인증 서버에게 인증을 요청하지 않고 티켓을 이용하여 바로 서비스를 이용할 수 있어 인증 서버의 오버헤드를 줄일 수 있다. 또한 사내 오피스 네트워크에서 사외 오피스 네트워크 및 다른 네트워크 이동하였을 때 티켓을 제시하여 인증을 제공받을 수 있다.

Step 5. 사내 오피스 인증 서버는 생성한 인가 값과 인가 티켓을 Main 디바이스의 아이디 기반 공개키로 암호화하여 Main 디바이스에게 전송한다.

$$IOAS \rightarrow MD: E_{KU_{MD}}[Authorization\ Value,\ Authorization\ Ticket] \quad (8)$$

Step 6. Main 디바이스는 사내 오피스 인증 서버로부터 전송받은 값을 복호화하고 인가 값을 검증하기 위해 자신의 개인키, 사내 오피스 인증 서버의 아이디, 공유한 대칭키를 ABM을 이용하여 인가 값(*Authorization Value'*)을 생성한다. 생성한 인가 값과 전송된 인가 값을 비교하여 값이 일치하면 인가 값이 정당한 오피스 인증 서버로부터 전송된 것을 확인할 수 있다. 또한 인가 티켓의 서명을 복호화하여 생성한 인가 값을 해쉬한 값과 비교하여 티켓을 정당성을 검증한다. 인가 값을 검증하는 수식을 풀어서 표기하면 다음과 같다.

$$Authorization\ Value' = e(KR_{MD}, ID_{IOAS} \cdot KS) \quad (9)$$

$$Authorization\ Value' \stackrel{?}{=} Authorization\ Value \quad (10)$$

$$Authorization\ Value = e(KR_{IOAS},\ ID_{MD} \cdot KS) \quad (11)$$

$$e(KR_{MD},\ ID_{IOAS} \cdot KS) = e(KR_{IOAS},\ ID_{MD} \cdot KS) \quad (12)$$

$$e(ID_{MD} \cdot g^{KS},\ ID_{IOAS} \cdot KS) = e(ID_{IOAS} \cdot g^{KS},\ ID_{MD} \cdot KS) \quad (13)$$

$$a = ID_{MD},\ b = ID_{IOAS},\ P = g^{KS},\ Q = KS \quad (14)$$

$$e(aP,\ bQ) = e(P,\ Q)^{ab} \quad (15)$$

$$Authorization\ Value' = e(aP,\ bQ) = e(P,\ Q)^{ab} \quad (16)$$

$$Authorization\ Value = e(bP,\ aQ) = e(P,\ Q)^{ba} \quad (17)$$

$$Authorization\ Value' = Authorization\ Value \quad (18)$$

Step 7. 사내 오피스 인증 서버는 Main 디바이스가 서비스를 이용할 때 서비스 개체로부터 인증을 받을 수 있도록 Main 디바이스의 아이디와 인가 티켓을 오피스 서비스 개체(데이터베이스, 웹 프린터, 서비스 서버 등)와 공유한 서비스키로 암호화하고, 서명하여 서비스 개체들에게 브로드캐스팅 한다.

$$IOAS \rightarrow HOS\ Broadcasting :\\ Sign_{IOAS}[E_{Service\_key}[ID_{MD},\ Authorization\ Ticket]] \quad (19)$$

Step 8. 오피스 서비스 개체는 브로드캐스팅 된 값을 복호화하고 사내 오피스 인증 서버의 서명을 검증한 후 Main 디바이스 아이디와 인가 티켓을 인덱스화 시켜 저장한다.

Step 9. Main 디바이스는 사내 오피스 서비스를 이용하고자 할 때 인증 서버에게 인증을 거쳐 서비스를 제공받지 않고 오피스 서비스 개체에게 티켓을 제시한다. 오피스 서비스 개체는 저장되어 있는 Main 디바이스의 아이디와 인가 티켓을 전송된 티켓과 검증하여 일치하면 서비스를 제공한다.

$$MD \rightarrow HOS :\ E_{KU_{HOS}}[Authorization\ Ticket] \quad (20)$$

$$HOS :\ Service\ Accept \quad (21)$$

4.2.2 사외 오피스 네트워크 로밍 시 인증 단계

본 단계에서는 Main 디바이스가 사내 오피스 네트워크에서 사외 오피스 네트워크로 로밍 하였을 때, 사내 오피스 인증 서버로부터 발급받은 인가 티켓을 제시하여 인증을 받고 서비스를 지속적으로 제공받을 수 있다.

Step 1. Main 디바이스(*MD*)는 사외 오피스 네트워크 서비스를 제공받기 위해 사외 오피스 인증 서버(*EOAS*)에게 사내 오피스 인증 서버(*IOAS*)로부터 발급받은 인가 티켓을 사내 오피스 인증 서버의 공개키로 암호화하여 디바이스의 아이디와 사내 인증 서버의 아이디를 전송한다.

$$MD \rightarrow EOAS :\\ ID_{MD},\ ID_{IOAS},\ E_{KU_{EOAS}}[Authorization\ Ticket] \quad (22)$$

Step 2. 사외 오피스 인증 서버는 전송 받은 값을 사내 오피스 인증 서버에게 전달한다. 사내 오피스 인증 서버는 자신의 아이디 기반 개인키로 전송받은 값을 복호화하여 인가 티켓을 검증하여 값이 일치하면 Main 디바이스가 사외 오피스에서 서비스를 이용할 수 있도록 인가 티켓을 서명하고 사외 오피스 인증 서버에게 전송한다.

$$EOAS \rightarrow IOAS :\\ ID_{MD},\ Sign_{EOAS}[E_{KU_{IOAS}}[Authorization\ Ticket]] \quad (23)$$

$$IOAS :\\ Authorization\ Ticket' \stackrel{?}{=} Authorization\ Ticket \quad (24)$$

$$IOAS \rightarrow EOAS :\ Access\_Accept,\\ Sign_{IOAS}[E_{KU_{EOAS}}[Authorization\ Ticket]] \quad (25)$$

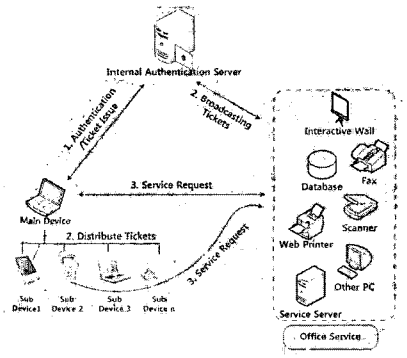
Step 3. 사외 오피스 인증 서버는 전송받은 티켓을 사외 오피스 서비스 개체에게 브로드 캐스팅 한다. 오피스 서비스 개체는 브로드캐스팅 된 값을 복호화하고 사외 오피스 인증 서버의 서명을 검증한 후 Main 디바이스 아이디와 인가 티켓을 인덱스화 시켜 저장한다.

$$EOAS \rightarrow HOS\ Broadcasting :\\ Sign_{EOAS}[E_{Service\_key}[ID_{MD},\ Authorization\ Ticket]] \quad (26)$$

Step 4. Main 디바이스는 사외 오피스 서비스를 이용하고 자 할 때 사내 오피스 서비스 이용시와 같이 티켓을 제시하고 서비스를 제공받을 수 있다.

4.3 Sub 디바이스 티켓을 이용한 인증/인가 프로토콜

Sub 디바이스 티켓을 이용한 인증/인가 방식은 유비쿼터스 오피스 네트워크 환경에서 서비스를 제공받는 사용자가 컴퓨팅 파워가 우수한 Main 디바이스를 주로 이용할 것이나, 이동 및 편리성을 제공하는 소형 디바이스를 이용하여 서비스를 제공받을 수 있다. 사용자는 하나의 Main 디바이스 외에 연산능력 및 컴퓨팅 파워가 부족한 Sub 디바이스를 이용하여 서비스를 제공받고자 할 때, 매번 인증 서버로부터 인증을 받고 서비스를 제공받지 않고 Sub 디바이스 인가 티켓을 Main 디바이스가 인증 서버로부터 발행 받아 분배해주면 티켓을 가지고 오피스 네트워크 서비스를 제공받을 수 있다([그림 7] 참조). Sub 디바이스 티켓을 이용한 인증/인가 프로토콜은 오피스 네트워크에서 Main 디바이스 인증 및 Sub 디바이스 인증/인가 단계로 구성되며, Main 디바이스와 사내 오피스 인



(그림 7) Sub 디바이스 티켓을 이용한 인증/인가 방식 전체 흐름도

증 서버간 공유한 대칭키 및 동기화 값들은 사전에 분배되었다고 가정한다.

4.3.1 Main 디바이스 인증 및 Sub 디바이스 인증/인가 단계

본 단계는 Main 디바이스가 사내 오피스 인증 서버에게 Sub 디바이스의 인가 티켓을 발급받아 Sub 디바이스들에게 티켓을 분배한다. Sub 디바이스는 분배 받은 티켓으로 서비스를 이용할 때 인증 서버에게 인증을 거치지 않고 바로 서비스를 제공받을 수 있다.

Step 1. Main 디바이스(*MD*)는 Sub 디바이스 티켓을 발급받기 위해 사용자가 소유한 Sub 디바이스(*SD*)들의 아이디(ID_{SD_i})와 일회용 패스워드(*OTP* : 4.2.1절 Step 1 참조)를 암호화하여 사내 오피스 인증 서버(*IOAS*)에게 전송한다.

$$MD \rightarrow IOAS : ID_{MD},\ E_{KU_{IOAS}}[ID_{SD_1} \| ID_{SD_2} \| \ldots \| ID_{SD_n},\ OTP] \quad (27)$$

Step 2. 사내 오피스 인증 서버는 Main 디바이스로부터 전송받은 값을 복호화한 후, 값을 검증하기 위해 서버에 저장된 디바이스의 식별번호, 대칭키, 카운터 값, 시간 값을 XOR 연산하여 일회용 패스워드(*OTP'*)를 생성한다. 생성한 일회용 패스워드와 전송한 일회용 패스워드를 비교하여 값이 일치하면 정당한 디바이스로 인증한다.

$$IOAS : OTP' = h(PIN \oplus KS \oplus CT \oplus TS) \quad (28)$$

$$OTP' \stackrel{?}{=} OTP \quad (29)$$

Step 3. 사내 오피스 인증 서버는 인증이 완료되면 Sub 디바이스가 서비스를 이용할 때 인증 값으로 사용할 수 있는 Sub 디바이스 인가 값(*SD Authorization Value*)과 Sub 디바이스 인가 티켓(*SD Authorization Ticket*)을 생성한다.

$$SD\ Authorization\ Value = e(KR_{IOAS},\ h(ID_{SD_1} \| ID_{SD_2} \| \ldots \| ID_{SD_n}) \cdot KS) \quad (30)$$

$$SD\ Authorization\ Ticket = ID_{MD},\ ID_{IOAS},\ Sign_{IOAS}[h(SD\ Authorization\ Value)] \quad (31)$$

Step 4. 사내 오피스 인증 서버는 Main 디바이스의 아이디 기반 공개키로 암호화하여 Main 디바이스에게 전송한다.

$$IOAS \rightarrow MD : E_{KU_{MD}}[SD\ Authorization\ Value,\ SD\ Authorization\ Ticket] \quad (32)$$

Step 5. Main 디바이스는 Sub 디바이스 인가 값과 Sub 디바이스 인가 티켓을 검증한다 (검증 수식은 4.2.1절의 Step 6 참조).

$$SD\ Authorization\ Value' = e(h(ID_{SD_1} \| ID_{SD_2} \| \ldots \| ID_{SD_n}) \cdot g^{KS},\ ID_{IOAS} \cdot KS) \quad (33)$$

$$SD\ Authorization\ Value' \stackrel{?}{=} SD\ Authorization\ Value \quad (34)$$

Step 6. Main 디바이스는 티켓의 검증이 완료되면, Sub 디바이스에게 각각 Sub 디바이스 인가 티켓을 분배한다.

Step 7. 사내 오피스 인증 서버는 오피스 서비스 개체에게 Sub 디바이스 인가 티켓과 Main 디바이스의 아이디, Sub 디바이스의 아이디를 브로드캐스팅 한다. 오피스 서비스 개체는 브로드캐스팅 된 값을 복호화하고 사내 오피스 인증 서버의 서명을 검증한 후 Main 디바이스 아이디, Sub 디바이스의 아이디 및 인가 티켓을 인덱스화 시켜 저장한다.

$$IOAS \rightarrow MD : Sign_{IOAS}[E_{Service\_key}[ID_{MD},\ ID_{SD_1} \| ID_{SD_2} \| \ldots \| ID_{SD_n},\ SD\ Authorization\ Ticket]] \quad (35)$$

Step 8. Sub 디바이스는 사내 오피스 서비스를 이용하고 자 할 때, 사내 오피스 서비스 개체에게 Sub 디바이스 티켓을 제시하고 인증 받아 제공받을 수 있다.

V. 제안 방식의 분석

제안 방식의 프로토콜을 요구사항에 맞추어 분석하고, 통신량 및 연산량을 분석한다. 또한 총 통신 횟수 및 초기 인증 통신 횟수 등을 통해 비용 분석과 오버헤드를 비교 분석한다.

5.1 안전성 및 요구사항 분석

제안 방식을 2장의 로밍 및 디바이스 인증/인가 요구사항에 맞추어 분석하면 다음과 같으며 〔표 1〕은 기존 방식과 제안 방식의 비교표이다.

- 기밀성 : 제안 방식은 이동 및 통신 중에 외부의 공격으로부터 안전하기 위하여 대칭키 방식(*KS*)과 아이디 기반 공개키(*KU*) 방식을 사용하여 암호화하며, 서명을 통하여 안전성을 제공한다.
- 무결성 : 전송된 데이터의 변경 및 수정에 대한 검증이 가능하기 위해 해쉬 함수를 이용하며, 서명을 통한 메시지의 무결성을 제공한다.
- 인증 : 사외의 오피스 네트워크에서 사내의 오피스 네트워크로 접근하거나 서비스를 지속받기 위해 인가 값(*Authorization Value*) 및 인가 티켓(*Authorization Ticket*)을 기반으로 디바이스를 인증할 수 있다. 또한 티켓을 발행받기 위한 초기 인증 시 일회용 패스워드(*OTP*)를 사용함으로써 디바이스를 인증할 수 있으며, 디바이스는 사내 오피스송한 인가 값과 전송한 인가 검증함으로써 상호인증을 제공할 수 있다.
- 도청공격 및 재전송 공격 : 대칭키 및 아이디 기반 공개키 암호 방식을 통한 도청공격을 원천봉쇄 할 수 있으며, 일회용 패스워드 및 동기화 되어 있는 카운터와 시간 값 사용으로 재전송 공격으로부터 안전하다.
- 패스워드 추측 공격 : 제안 방식은 일회용 패스워

〔표 1〕 기존 방식과 제안 방식의 요구사항 분석표

	Inter-domain 디바이스 인증/접근제어 방식	S/Key 기반 디바이스 인증 방식	Main/Sub 디바이스 인증/인가 방식
기밀성	대칭키/공개키 암호 방식	XOR 방식 및 해쉬 함수 안전성에 근거	대칭키/아이디 기반 공개키 암호 방식
무결성	서명 검증	해쉬 함수	해쉬 함수와 서명 검증
인증	상호인증(*Nonce*를 이용한 Challenge-response)	일회용 패스워드	일회용 패스워드와 인가 값으로 Main/Sub 디바이스 인증
접근제어	인증서 기반 접근제어	인증서를 통한 접근제어	티켓을 소유한 디바이스만 서비스에 접근 가능
도청공격	도청을 통한 *SecretID*와 N_H 획득 가능	카운터 값과 *Seed* 값 획득 가능	메시지 암호화를 통한 도청공격 원천 봉쇄
재전송 공격	*Nonce* 사용으로 공격 방어	일회용 패스워드 사용으로 방어	일회용 패스워드, 카운터, 시간 값 사용으로 방어
패스워드 추측 공격	패스워드 사용 안함	도청공격을 통한 메시지 획득으로 추측 가능	패스워드 추측 불가
빠른 로밍 인증	로밍 고려하지 않음	홈 디바이스 인증서 발행으로 통신량 증가 및 연산량 증가	인가 티켓을 기반으로 빠른 로밍 인증 제공
인증 서버의 오버헤드	PKI 기반 공개키 방식 사용으로 디바이스 개수 증가 시 오버헤드 발생	용도별 인증서 증가로 인한 오버헤드 증가	아이디 기반 공개키 방식 사용으로 연산량 및 통신량 감소를 통한 인증 서버의 오버헤드 감소
디바이스의 다양성	여러 디바이스 사용이 가능하나 디바이스 마다 인증서 발행	여러 디바이스 사용이 가능하나 디바이스 마다 인증서 발행	Sub 디바이스를 이용한 서비스 제공 방안 적용

드 생성 시 카운터 값과 시간 값을 동시에 사용하고 대칭키를 입력 값으로 하는 일회용 패스워드를 사용함으로써 패스워드를 추측하기 어렵다.

- 빠른 로밍 인증 : 디바이스가 로밍 시 끊김 없는 서비스를 제공하기 위해 제안 방식은 인가 티켓을 기반으로 빠른 인증을 제공할 수 있다. 또한 로밍 및 인증을 제공하기 위하여 아이디 기반 공개키 방식을 이용하였으며, 사외 오피스 인증 서버에게 인가 티켓을 전송해줌으로써 안전하고 효율적으로 인증을 제공할 수 있다.
- 인증 서버의 오버헤드 : 유비쿼터스 환경 및 디바이스의 연산능력을 고려하여 인증서 기반의 공개키 방식을 사용하지 않고 아이디 기반 공개키 방식을 사용하여 디바이스의 연산량을 줄였으며, 또한 통신량의 감소로 인하여 디바이스와 인증 서버의 로드를 줄였다. 그러나 지수승 연산에 대한 사항은 향후 고려해야 할 것으로 사료된다.
- Main/Sub 디바이스 사용 : 제안 방식은 서비스를 제공받는 Main 디바이스 외에 사용자가 보유한 Sub 디바이스를 이용한 서비스 제공방안에 대하여 제안하였다. Sub 디바이스는 인가 티켓을 기반으로 사내 서비스 이용 및 로밍을 통한 사외 서비스 이용을 고려하여 다양한 서비스 모델을 제시하였다.

5.2 통신량 및 연산량 분석

기존 방식과 제안 방식의 통신량 및 디바이스 연산량을 분석한 결과는 〔표 2〕와 같다. 제안 방식은 Main 디바이스 인증/인가와 Sub 디바이스 인증/인가 방식을 각각 분석하였다. 제안 방식은 인증, 로밍, 티켓 발행 등 모든 단계를 포함하여 로밍을 고려하지 않은 기존 방식 보다 통신량을 줄였으며, 초기 인증 횟수 역시 상호 인증을 제공하면서 2회로 감소시켰다. 암호화 연산은 디바이스의 연산만을 분석하였으며 복호화 연산도 포함하여 분석하였다. S/Key 디바이스 인증 방식 보다 제안 방식이 암호화 연산은 많으나, PKI 연산 보다 연산량이 적은 아이디 기반 공개키 연산이기 때문에 기존 방식에 비해 암호화 연산량이 적다. 또한 S/Key 디바이스 인증 방식은 암호화 연산 사용을 줄이고 해쉬 연산 및 XOR 연산을 통하여 경량화를 시켰으나, 안전성 측면에서 강도가 떨어진다.

5.3 비용 분석

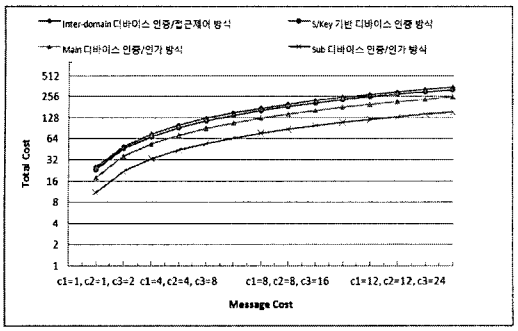
홈 네트워크 및 오피스 네트워크에서 통신량 및 연산량에 따른 통신비용은 중요하며 모바일 네트워크 일 경우, 그 중요성은 더욱 커진다. 따라서 제안 방식과 기존 방식의 비용 분석을 위해 〔표 2〕의 총 통신 횟수 및 초기 인증 통신 횟수와 암호화 연산 횟수를 수식으로 정의하여 비교한다. 인증 횟수의 감소 및 암호화 연산 횟수에 따른 비용을 비교하기 위해 다음과 같은 시스템계수 및 비용 산출 수식을 정의한다.

- t : 총 통신 횟수
- a : 초기 인증 통신 횟수
- e : 암호화 연산 횟수
- c_1 : 통신 메시지 비용
- c_2 : 인증 메시지 비용
- c_3 : 암호화 연산 비용
- $Total\ Cost = (t-a)\times c_1 + a\times 2c_2 + e\times c_3$

통신 메시지 비용(c_1) 및 인증 메시지 비용(c_2)은 1

〔표 2〕 통신량 및 디바이스 연산량 분석표

	Inter-domain 디바이스 인증/접근제어 방식	S/Key 기반 디바이스 인증 방식	Main 디바이스 인증/인가 방식	Sub 디바이스 인증/인가 방식
총 통신 횟수	11 회 (Inter domain)	19 회 (인증서 발급 단계 포함)	8 회 (로밍 단계 포함)	5 회
초기 인증 통신 횟수	2 회	4회 (상호 인증)	2 회 (상호 인증)	2 회 (상호 인증)
암호화 연산 (복호화 연산 포함)	7 회 (PKI 기반 공개키 연산)	2 회 (PKI 기반 공개키 연산)	5 회 (ID 기반 공개키 연산)	3회 (ID 기반 공개키 연산)
해쉬 연산	-	16 회	1 회	2 회
지수승 연산	-	-	1 회	-
Pairing 연산	-	-	1 회	1 회



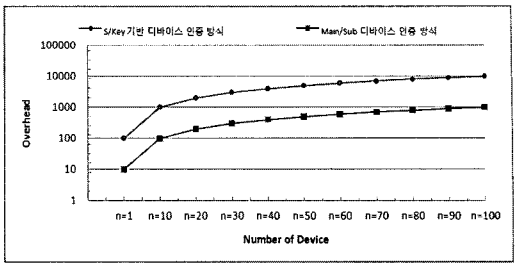
〔그림 8〕 메시지 비용에 따른 비용 분석

씩 증가하고, 암호화 연산 비용(c_3)는 2씩 증가하는 것으로 가정한다. 이는 인증 메시지를 생성하는 비용보다 암호화 연산에 드는 비용이 더 높을 것으로 가정한 것이다(암호화 연산은 지수승 연산 및 암호 알고리즘을 통한 암호화 메시지를 생성하기 때문에 비용이 높은 것으로 가정). 통신량 및 디바이스 연산량 분석표에서 나타난 수치를 수식에 적용하여 계산하면 Inter-domain 디바이스 인증/접근제어 방식의 비용은 $Total\ Cost = 9c_1 + 2c_2 + 14c_3$와 같다. S/Key 기반 디바이스 인증 방식과 제안 방식도 동일한 방법으로 수식을 정의하여 메시지 비용에 따른 통신비용을 분석하여 그래프로 나타내면 〔그림 8〕과 같다. 분석 결과를 보면 제안 방식 모두 기존 방식보다 비용 측면에서 좋은 성능을 보인다. S/Key 기반 디바이스 인증 방식은 암호화 연산 보다 해쉬 및 XOR 연산 안전성에 근거하고 있기 때문에 차이가 적으나, 암호화 연산을 적용하면 제안 방식과의 편차는 더욱 클 것으로 예상된다.

5.4 오버헤드 분석

제안 방식과 기존 방식의 디바이스 인증 방식을 디바이스의 증가에 따른 홈 도메인의 인증 서버(홈네트워크 인증 서버, 사내 오피스 인증 서버 등과 같이 디바이스가 소속된 네트워크 인증 서버) 오버헤드 연산을 통해 비교한다. Inter-domain 디바이스 인증/접근제어 방식은 로밍을 고려하지 않았으므로 오버헤드 비교분석에서 제외하고, S/Key 기반 디바이스 인증 방식과 비교를 통한 오버헤드 분석을 진행한다. 오버헤드 비교를 위한 시스템 계수 및 수식은 다음과 같다.

- n : 디바이스의 수($n = 1, 10, 20, \ldots, 100$)
- m : 인증 서버로 요청되는 메시지의 수



〔그림 9〕 디바이스 증가에 따른 오버헤드 분석

- r : 디바이스가 접근을 시작하여 세션이 끝날 때 까지 이동한 횟수(10회로 가정)
- OH : 홈도메인의 인증서버에 발생되는 오버헤드
- $OH = n \times m \times r$

디바이스의 수는 1부터 10씩 증가하는 것으로 가정하며, 디바이스가 접근을 시작하여 세션이 끝날 때 까지 이동한 횟수 r은 10회로 가정한다. S/Key 기반 디바이스 인증 방식을 수식에 적용하여 계산하면, 예를 들어 홈 인증 서버에 등록되어 있는 디바이스가 100대, 총 이동 횟수는 10회이고, 이동할 때 마다 홈 인증 서버로 인증을 요청하므로 오버헤드는 $OH = 100*10*10 = 10000$이 된다. 그러나 제안 방식은 동일한 가정 하에서, 초기에 사외 오피스 네트워크로 이동하였을 때만 사내 오피스 인증 서버로 인증을 요청하므로 총 이동 횟수 10회 중 1회만 홈 인증 서버로 접근하게 되어 $OH = 100*1*10 = 1000$이 된다. 그러므로 디바이스의 수가 증가함에 따라 S/Key 기반 디바이스 인증 방식과 제안 방식을 비교하면 오버헤드가 감소하는 것을 볼 수 있다. 〔그림 9〕는 이상의 오버헤드를 분석한 결과이다.

VI. 결 론

현대사회는 IT 기술의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 정보사회라는 새로운 문화적 변환기를 맞이하고 있으며, 다양한 서비스 및 디바이스의 발전을 가져오고 있다. 그러나 보안 측면에서 고려해야 할 요구사항은 더욱 복잡해지고 다양화될 것이며, 기존의 매체나 프로토콜이 갖고 있는 보안 취약성을 그대로 갖는다. 또한 네트워크와 디바이스의 급속한 발달과 초고속망을 통한 인터넷 및 컴퓨터의 보급으로 인해 오피스 디바이스의 사용영역 및 서비스가 확장되고 있다. 그러나 기존에 사용되던 네트워크 기반의 사이버공격 기술이 오피스 네트워크

에 그대로 적용될 수 있는 문제점을 갖고 있기 때문에 IP 네트워크상에서의 다양한 문제 등 기존 해킹공격에 대한 오피스 디바이스 보호 대책이 미비한 실정이다.

따라서 본 연구에서는 유비쿼터스 환경에서 오피스 네트워크간 로밍, Main 디바이스 인증/인가 및 Sub 디바이스 티켓을 이용한 인증/인가에 관한 연구를 진행하였다. 오피스 네트워크간 로밍 및 디바이스 인증/인가 프로토콜은 빠른 로밍 인증 및 경량화된 인증/인가 방식을 위하여 아이디 기반 공개키 방식 및 Admissible Bilinear Map 기반 인가 티켓을 이용하였다. 또한 사용자가 소유한 Main 디바이스 외에 연산능력 및 컴퓨팅 파워가 부족한 Sub 디바이스를 이용하여 서비스를 제공받기 위해 Sub 디바이스 인가 티켓을 이용하는 연구를 진행하였다. 이와 같은 방식을 통해 사내 오피스 인증 서버의 오버헤드 및 통신 횟수를 줄일 수 있으며, 안전성과 효율성을 제공할 수 있다.

향후 TTA에서 표준화한 외부 인증서 기반 인증/인가 및 댁내 인증서 기반 인증/인가 구조에 적합한 디바이스 인증/인가 방식에 대한 연구가 필요할 것으로 사료된다. 그리고 Main 디바이스 및 Sub 디바이스의 로밍에 따른 이기종 네트워크에서의 인증/인가에 관한 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] 김도우, 한종욱, 정교일, "홈디바이스 인증/인가 기술 동향," 주간기술동향, 통권 1329호, pp. 1-11, 2008년 1월.

[2] 이윤경, 한종욱, 정교일, "홈네트워크 보안 표준화 동향," 전자통신동향분석, 22(1), pp. 73-82, 2007년 2월.

[3] "홈네트워크에 적용 가능한 홈 디바이스 인증서 프로파일," TTAS.KO-12.0052, 2007년 12월.

[4] 이선영, 임강빈, 배광진, 정태영, 한종욱, "디바이스 인증 및 인가에 기반한 유비쿼터스 홈네트워크 프라이버시 대책," 정보보호학회논문지, 18(5), pp. 125-131, 2008년 10월.

[5] 김재곤, 김구수, 엄영익, "홈 네트워크 환경에서 다중 도메인을 지원하는 공유키 및 공개키 기반의 이동 에이전트 인증 기법," 정보보호학회논문지, 14(5), pp. 109-119, 2004년 10월.

[6] 지준웅, 김지홍, 김창규, "권한인증서를 이용한 도메인간의 사용자 인증방안," 정보보호학회논문지, 18(6A), pp. 75-83, 2008년 12월.

[7] 이원진, 전일수, "홈네트워크 상에서 속성기반의 인증된 키교환 프로토콜," 정보보호학회논문지, 18(5), pp. 49-57, 2008년 10월.

[8] 홍승필, 이철수, "유비쿼터스 컴퓨팅 환경내 개인정보보호 프레임워크 적용 방안," 정보보호학회논문지, 16(3), pp. 157-164, 2006년 6월.

[9] A. Shamir, "Identity-based crypto systems and signature schemes," CRYPTO '84, LNCS 196, pp. 47-53, 1985.

[10] P.S.L.M. Barreto, B. Libert, N. McCullagh, and J.J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps," ASIACRYPT 2005, LNCS 3788, pp. 515-532, 2005.

[11] T. Goriparthi, M.L. Das, and A. Saxena, "An improved bilinear pairing based remote user authentication scheme," Computer Standards & Interfaces, vol. 31, no. 1, pp. 181-185, Jan. 2009.

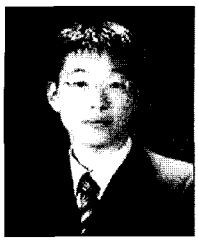
[12] J.B. Hwang, H.K. Lee, and J.W. Han, "Efficient and User Friendly Inter-Domain Device Authentication/Access Control for Home Networks," EUC 2006, LNCS 4096, pp. 131-140, 2006.

[13] J.B. Hwang and J.W. Han, "A Security Model for Home Networks with Authority Delegation," ICCSA 2006, LNCS 3983, pp. 360-369, 2006.

[14] D.G. Lee, I.S. You, S.C. Kim, Y.K. Lee, J.W. Han, and K.I. Chung, "Intelligent Home Network Authentication SKey-Based Home Device Authentication," ISPA 2007 Workshops, LNCS 4743, pp. 214-223, 2007.

[15] Y.K. Lee, D.G. Lee, and J.W. Han, "Home Device Authentication Method based on PKI," Proceedings of the Future Generation Communication and Networking (FGCN 2007), vol. 2, pp. 7-11, 2007.

〈著者紹介〉



문 종 식 (Jong-Sik Moon) 정회원
2006년 2월: 순천향대학교 정보기술공학부 졸업
2008년 2월: 순천향대학교 컴퓨터학과 석사
2008년 3월 ~ 현재: 순천향대학교 컴퓨터학과 박사과정
〈관심분야〉 AAA, IPTV 보안, 디바이스 인증

이 임 영 (Im-Yeong Lee) 종신회원
1981년 2월: 홍익대학교 전자공학과 졸업
1986년 2월: 오사카대학 통신공학전공 석사
1989년 2월: 오사카대학 통신공학전공 박사
1985년 ~ 1994년: 한국전자통신연구원 선임연구원
1994년 ~ 현재: 순천향대학교 컴퓨터학부 교수
〈관심분야〉 암호이론, 정보이론, 컴퓨터 보안