홈 네트워크 환경에서의 이동 에이전트 인증 기법 및 도메인 관리 기법 설계

김재곤*, 김구수*, 엄영익*
*성균관대학교 컴퓨터공학과
e-mail : {angel77, gusukim, yieom}@ece.skku.ac.kr

Design of Mobile Agent Authentication and Domain Management Scheme in Home Network Environment

Jae-Gon Kim*, Gu Su Kim*, Young Ik Eom*
*Dept. of Computer Engineering, Sung Kyun Kwan University

요 약

홈 네트워크 환경은 댁내의 가전 기기들을 원격 접속 및 원격 제어가 가능하도록 연결한 네트워크 환경이다. 이동 에이전트는 네트워크 상에서 스스로 이동하면서 사용자 또는 다른 개체 대신 행동 할 수 있는 프로그램으로서 홈 네트워크 환경에서 원격 상호작용과 네트워크 부하를 줄이고 서비스를 제공할 수 있다. 이를 위해서는 서비스를 요청한 개체 및 서비스 주체에 대한 인증과정이 필요하다. 본 논문에서는 홈 네트워크 환경에서의 이동 에이전트 인증을 위한 다음 세 가지의 사항을 고려한다. 첫 째, 홈 네트워크 디바이스의 제한적인 성능, 둘 째, 홈 네트워크 디바이스의 이동성, 셋 째, 이동 에이전트의 코드 및 상태 정보 이동성. 이들에 대한 고려를 통하여 홈 네트워크 환경에 적합한 도메인 관리 기법과 인증기법을 설계한다.

1. 서론

홈 네트워크 환경은 댁내의 가전 기기들을 원격 접속 및 원격 제어가 가능하도록 연결한 네트워크 환경이다[1]. 이동 에이전트는 이동 능력을 갖는 에이전트 프로그램으로서 홈 네트워크 환경에서 원격 상호작용과 네트워크 부하를 줄일 수 있을 것으로 기대되고 있다[2]. 이동 에이전트의 서비스가 홈 네트워크에서 실현되기 위해서는 이동 에이전트 인증 기술이 필요하다. 본 논문에서는 홈 네트워크 환경에서의 이동 에이전트 인증을 위한 고려 사항들을 분석하고 이를 바탕으로 홈 네트워크 환경에 적합한 도메인 관리 기법 및 인증 기법을 설계한다.

2 절에서는 관련 연구 내용을 설명하고, 3 장에서는 제안 도메인 관리 기법과 인증 기법을 설명하고, 4 장에서는 제안 인증 기법의 신뢰성을 증명하고, 5 장에서는 결론 및 향후 계획을 설명한다.

2. 관련 연구

2.1 홈 네트워크 미들웨어

홈 네트워크 미들웨어는 다양한 플랫폼 상에서 동작하는 홈 네트워크 기기들 간에 상호 운영성을 제공하고 홈 네트워크 환경에 필요한 서비스들을 제공한다. 홈 네트워크 미들웨어는 보안을 유지하고 사생활을 보호하기 위해서 보안 서비스를 제공한다. 보안 서비스를 제공하는 홈 네트워크 미들웨어로는 UPnP, Jini, HAVi 등이 있다[3,4,5].

2.2 이동 에이전트 플랫폼

이동 에이전트는 네트워크 상에서 스스로 이동하면서 사용자를 대신하여 행동할 수 있는 프로그램을 말한다. 이동 에이전트 플랫폼은 그러한 이동 에이전트가 실행되는 환경이다[6].

2.3 홈 네트워크 환경에서의 이동 에이전트 인증

이동 에이전트 인증은 에이전트를 전송하는 플랫폼이 수신 플랫폼의 신원을 확인하고, 수신 플랫폼이 송신 플랫폼과 전송 받을 에이전트의 신원을 확인하는 것이다[7].

이동 에이전트 인증 기법은 그 동안 많은 연구가 있어 왔다. 그러나 홈 네트워크 환경에서의 이동 에이전트 인증 기법에 대한 연구는 현재까지 부족한 실정이다. 본 논문에서는 홈 네트워크 환경에서 이동 에이전트 인증을 수행할 경우에 고려해야 하는 사항들을 분석한다. 이를 기반으로 홈 네트워크 환경에 적절한 도메인 관리 기법 및 인증 기법을 제안한다.

** 이 논문은 2003년도 한국학술진흥재단의 지원에 의하여 연구되었음(KRF-2003-041-D20420).

3. 제안 기법

3.1 고려 사항

홈 네트워크 환경에서의 이동 에이전트 인증에서 다음의 세가지 사항이 고려 되어야 한다.

첫 째, 홈 네트워크 환경에서 사용되는 디바이스들은 일반적으로 데스크 탑 컴퓨터보다 제한적인 성능을 갖는다. 또한 자체 전원을 이용하는 디바이스의 경우 소모하는 전력을 최소화 하여 기능을 수행 할 수 있어야 한다. 따라서 이동 에이전트 인증은 디바이스의 성능이 저하되지 않도록 가능한 적은 비용을 들여서 이루어 져야 한다.

둘 째, 홈 네트워크 환경에서 사용되는 디바이스 중에서는 이동성을 갖는 디바이스가 있다. 이동 에이전트가 방문자 디바이스의 플랫폼에서 홈 구성원의 디바이스로 이주되는 경우와 그 반대의 경우에 대한 인증 구조가 있어야 한다.

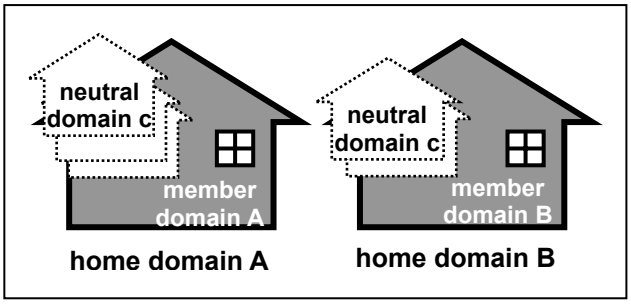
셋 째, 이동 에이전트는 코드와 상태 정보를 가지고 플랫폼 간을 이주하기 때문에 언제라도 플랫폼에 의해 에이전트가 보유하고 있는 정보가 유출, 수정, 도용될 가능성을 가지고 있다. 따라서 이동 에이전트 인증은 이러한 사항들을 고려해야 한다.

본 논문에서는 홈 도메인 내부에서는 비밀키 기반 인증 기법을 적용하고, 에이전트가 홈 도메인 밖으로 이주할 경우에는 공개키 기반 인증 기법을 적용한다. 비밀키 기반 인증 기법을 사용하는 이유는 비밀키 기반 인증 기법이 공개키 기반 인증 기법에 비하여 적은 비용이 들기 때문이다. 동일한 도메인에 등록 되어 있는 플랫폼들은 동일한 비밀키를 이용하여 같은 도메인에 소속되어있는 플랫폼인지 확인한다. 다음 절에서는 이러한 인증 기법을 사용하기 위한 도메인 관리 기법, 키 배포 방법, 인증 알고리즘을 설명한다.

3.2 도메인 관리

홈 네트워크 환경에서 도메인의 경계는 물리적인 홈으로 나뉘어 질 수 있다. 그러나 비밀키를 공유하는 영역으로서 도메인을 사용하기 위해서는 홈이라는 물리적인 구분으로 도메인을 나누는 것 외에 가상의 논리적인 도메인을 설정하는 것이 필요하다.

본 논문에서는 홈의 물리적인 영역과 일치하는 논리적 도메인을 멤버 도메인이라고 한다. 그리고 각 도메인들 간의 합의에 의하여 만들어진 논리적인 도메인을 중립 도메인이라고 한다. (그림 1)은 홈 도메인과 멤버 도메인 그리고 중립 도메인을 보인다.



(그림 1) 홈 도메인, 멤버 도메인, 중립 도메인

각각의 집은 홈 도메인을 의미한다. 회색으로 칠해진 집 모양의 내부는 홈 도메인의 멤버 도메인이다. 각각의 홈 도메인은 여러 개의 중립 도메인을 가질 수 있다.

홈 도메인을 관리하기 위하여 HDMS(Home Domain Management Server)를 둔다. HDMS 는 홈 도메인내의 플랫폼들을 관리하고 다른 HDMS 들과 협상하여 중립 도메인을 만든다. 멤버 도메인의 멤버 플랫폼 및 에이전트는 멤버 비밀키를 이용하여 인증을 수행한다. 방문자 디바이스의 플랫폼 및 에이전트는 중립 도메인 내에서 중립 도메인 비밀키를 이용하여 인증을 수행한다. 멤버 에이전트가 방문자 디바이스상의 플랫폼으로 이주하기 위해서는 중립 도메인의 비밀키를 가지고 있어야 한다. 반대로 방문자 플랫폼의 에이전트가 홈 도메인의 멤버 플랫폼에 이주하기 위해서는 홈 도메인에서 사용되고 있는 중립 도메인의 비밀키를 가지고 있어야 한다. 각 플랫폼에서는 인증이 이뤄진 중립 도메인의 종류에 따라 각기 다른 권한을 부여한다.

(그림 1)의 각 홈 도메인은 같은 이름의 중립 도메인 c 를 가지고 있다. 두 중립 도메인은 같은 이름을 가지고 있지만 서로 다른 비밀키를 사용한다. 홈 도메인 A 에 참가하는 홈 도메인 B 의 플랫폼 P_B 는 공개키 기반 인증을 수행하고 홈 도메인 A 의 HDMS 로부터 중립 도메인의 비밀키를 할당 받는다. 이후부터 P_B 는 중립 도메인 c 의 멤버로서 동작한다. 이러한 방법을 사용 함으로써 홈 도메인 안에서 멤버 도메인 비밀키를 공개하지 않으면서도 방문자 디바이스의 플랫폼과 에이전트를 비밀키를 이용하여 인증 할 수 있게 된다. 이러한 방법의 또 한가지 장점은 각 도메인이 독자적으로 비밀키를 관리할 수 있게 된다는 것이다.

3.3 키 분배 및 에이전트 초기화

본 절에서는 3.2 절에서 설명한 도메인 관리 기법을 기반으로 하여 플랫폼이 홈 도메인 및 중립 도메인에 등록하여 비밀키를 분배 받는 방법을 설명하고 에이전트가 보유하게 되는 정보에 대하여 설명한다.

(알고리즘 1)에서 플랫폼의 홈 도메인 등록 방법을 설명한다.

$P \rightarrow HDMS : P_{ID} \parallel KUp$
$HDMS : Save <P_{ID}, KUp> in member domain$
$platform directory$
$C = E_{KUp}[K_M]$
$HDMS \rightarrow P : C$
$P : K_{PM} = D_{KRp}[C]$

(알고리즘 1) 홈 도메인 등록 알고리즘

P 는 도메인에 등록하고자 하는 플랫폼이며, P_{ID} 는 플랫폼의 ID 를 의미한다. KUp, KRp 는 플랫폼의 공개키와 개인키이다. K_M 은 멤버 도메인 비밀키를 의미한다. 플랫폼은 별도의 사용자 인증 과정을 거쳐 자신의 공개키를 HDMS 에게 등록하고, HDMS 는 해당 공개키를 이용하여 멤버 도메인 비밀키를 플랫폼에게 전달한다.

(알고리즘 2)에서 플랫폼의 중립 도메인 등록 방법을 설명한다.

```
P : C = E_KRp[ P_ID || n ]
P → HDMS : neutral domain name || P_ID || n || C
HDMS → home network CA : P_ID
Home network CA → HDMS : KUp
HDMS : P_ID' || n' = D_KUp[ C ]
        If( P_ID == P_ID' && n == n' )
            Save <P_ID> in "neutral domain name" neutral
            domain platform directory
            C = E_KUp[ K_N ]
HDMS → P : C
P : K_PN = D_KRp[ C ]
    Save < "neutral domain name", K_PN> in
    neutral domain secret key directory
```

(알고리즘 2) 중립 도메인 등록 알고리즘

neutral domain name 은 플랫폼이 참여하려는 중립 도메인의 이름이다. n 은 임의의 난수값이다. K_N 은 중립 도메인 비밀키이며 K_{PN} 은 플랫폼이 보유하게 되는 중립 도메인 비밀키이다. HDMS 는 플랫폼을 공개키 기반 인증 방법을 이용하여 인증한다. 인증이 성공적으로 이루어 지면 HDMS 는 플랫폼에게 중립 도메인의 비밀키를 배포한다. 이후부터 플랫폼은 중립 도메인의 멤버로서 동작한다.

(알고리즘 3)은 에이전트 생성시 에이전트 초기화 알고리즘을 설명한다.

```
HP : M_A = H[ Code of Agent ]
     AMAT = E_Kpm[ M_A ]
     AIDAT = E_KRp[ M_A ]
```

(알고리즘 3) 에이전트 초기화 알고리즘

(알고리즘 3)의 M_A 는 에이전트의 코드 부분에 대한 메시지 다이제스트이다. 이를 사용 함으로써 에이전트 코드의 불법적인 수정을 발견하고 암호화된 인증 토큰의 도용을 방지한다. AMAT(Agent Member domain Authentication Token)는 M_A를 멤버 도메인 비밀키로 암호화한 값으로서 에이전트의 멤버 도메인 인증에 사용된다. AIDAT(Agent Inter Domain Authentication Token)는 M_A 를 에이전트를 생성한 플랫폼의 비밀키로 서명한 값으로서 에이전트의 다중 도메인간 인증에 사용된다.

(알고리즘 4)는 에이전트가 중립 도메인에 참여할 때에 설정 되는 인증 정보를 설명한다.

```
P : M_A = H[ Code of Agent ]
    ANDN = neutral domain name
    ANAT = E_Kpn[ M_A ]
```

(알고리즘 4) 에이전트 중립 도메인 참여시 인증 정보 설정 알고리즘

ANDN(Agent Neutral Domain Name)은 에이전트가 참여한 중립 도메인의 이름이다. ANAT(Agent Neutral domain Authentication Token)은 에이전트 코드의 메시지 다이제스트를 중립 도메인의 비밀키로 암호화한 값으로서 중립 도메인 내부 이주 시에 사용되는 인증 토큰이다.

3.4 에이전트 인증

본 절에서는 이동 에이전트의 단일 도메인 내부 이주시의 인증 방법과 다중 도메인간 이주시의 인증 방법을 설명한다.

(알고리즘 5)에서 에이전트의 단일 도메인 내부 이주시의 인증 방법을 설명한다.

```
A → P : domain name || M_A || AT
P: Find <K_D> of domain name in domain secret key
    directory
  M_A' = E_KD[ AT ]
   If(M_A == M_A' && MA' == H[Code of Agent])
      authentication success
   else
      authentication failure
```

(알고리즘 5) 도메인 내부 인증 알고리즘

A 는 이주하는 이동 에이전트이며 P 는 목적지 플랫폼이다. AT(Authentication Token)는 멤버 도메인 내부 이주의 경우는 AMAT 의 값이 되며 중립 도메인 내부 이주의 경우는 ANAT 의 값이 된다. K_D 는 domain name 에 해당하는 도메인의 비밀키이다. 이동 에이전트는 도메인 인증 토큰과 에이전트 코드의 메시지 다이제스트를 전송한다. 플랫폼은 해당하는 인증 토큰의 도메인 비밀키를 찾아내어 인증토큰을 복호화한다. 본 인증 알고리즘은 멤버 도메인과 중립 도메인 구분 없이 동일하게 적용된다.

(알고리즘 6)에서 다중 도메인간 인증 알고리즘을 설명한다.

```
A → P : HP_ID || HD_ID || M_A || AIDAT
P → HomeNetworkCA : HP_ID
HomeNetworkCA → P : KUp
P : M_A' = E_KUp[AIDAT ]
    if(M_A' == M_A   && MA' == H[Code of Agent])
       authentication success
       If( HD_ID != PHD_ID or
           HD_ID != CD_ID )
          join neutral domain, goto <algorithm 4>
    else
       Authentication failure
```

(알고리즘 6) 다중 도메인간 인증 알고리즘

HP_{ID} 는 에이전트의 홈 플랫폼 ID 이며 HD_{ID} 는 에이전트의 홈 도메인 ID 이다. PHD_{ID} 는 플랫폼의 홈 도메인 아이디이며 CD_{ID} 는 플랫폼이 현재 참여해 있는 홈 도메인 ID 이다. 에이전트는 이주할 플랫폼에 홈 플랫폼 ID 및 홈 도메인 ID 를 전송한다. 플랫폼은 해당하는 공개키를 홈 네트워크 CA 에게서 받아서 AIDAT 에 되어있는 서명을 확인한다. 인증이 성공하면 에이전트가 이주한 도메인이 홈 도메인이 아니거나 플랫

폼과 에이전트의 홈 도메인이 서로 다르면 (알고리즘 4)의 중립 도메인 참여단계로 들어 간다.

4. 제안 인증 기법의 신뢰성 증명

본 절에서는 여러 가지 공격에 대하여 본 인증 기법의 신뢰성을 증명한다.

경우 1: 중립 도메인의 구성원인 에이전트가 멤버 도메인의 구성원으로 인증을 시도하기 위해 중립 도메인 인증 토큰을 멤버 도메인의 인증 토큰인 것처럼 속여서 플랫폼에 전송한다. 그러나 중립 도메인과 멤버 도메인의 비밀키는 서로 다르므로 복호화된 값이 같지 않게 되므로 인증에 실패한다.

A : $ANAT = E_{KN}[M_A]$
A → P : "member" || M_A || ANAT
P : $M_A' = D_{KM}[ANAT]$
$M_A \neq M_A'$
∴ authentication fail

경우 2: 홈 도메인의 멤버 에이전트가 HDMS 로부터 방문자 플랫폼이 참여해 있는 중립 도메인의 비밀키를 할당 받는다. 멤버 에이전트는 방문자 플랫폼으로 이주하여 방문자 플랫폼의 홈 도메인 멤버처럼 행동하고자 한다. 그러나 방문자 플랫폼도 마찬가지로 홈 도메인 멤버 비밀키와 방문자 도메인 비밀키를 구분하여 가지고 있으므로 인증에 실패하게 된다.

HDMS → A : K_N
A : $ANAT = E_{KN}[M_A]$
A → P : "member" || M_A || ANAT
P : $M_A' = D_{KM}[ANAT]$
$M_A \neq M_A'$
∴ authentication fail

경우 3: 악의를 가진 에이전트가 홈 도메인의 멤버 플랫폼의 인증 토큰을 가로채어, 마치 자신이 멤버 도메인의 비밀키로 암호화된 인증 토큰을 가지고 있는 것처럼 속일 수 있다. 그러나 인증 토큰을 사용하는 에이전트의 코드 부분이 다르기 때문에 인증토큰의 복호화된 값과 에이전트 코드의 메시지 다이제스트가 다르게 되므로 인증에 실패한다.

A : AMAT' = AMAT of other member agent
A → P : "member" || M_A || AMAT'
P : $M_A' = D_{KM}[AMAT']$
$M_A' \neq H[$ Code of A $]$
∴ authentication fail

경우 4: 외부 도메인에서 홈 도메인으로 에이전트가 이주할 경우 에이전트가 가지고 있는 AIDAT 에 에이전트를 생성한 플랫폼의 서명이 되어있지 않으면 다중 도메인간 인증이 수행되지 않는다. 따라서 다중 도메인간 인증에 실패한 에이전트는 중립 도메인 비밀키를 할당 받는 것 역시 불가능해 진다.

A → P : HP_{ID} || HD_{ID} || M_A || AIDAT
P → HomeNetworkCA : HP_{ID}
HomeNetworkCA → P : KUp
P : $M_A' = E_{KUp}[AIDAT]$
$M_A \neq M_A'$
∴ authentication fail
∴ fail to allocate ANAT

5. 결론 및 향후 계획

본 논문에서는 홈 네트워크 환경에서의 이동 에이전트 인증을 수행하기 위해 중립 도메인 및 멤버 도메인이라는 논리 도메인 계층을 두었다. 이러한 도메인 관리 기법을 통하여 홈 도메인에 방문자 디바이스가 있는 경우를 다룰 수 있는 비밀키 기반 인증 기법을 설계 할 수 있었다. 비밀키 기반 인증 기법을 공개키 기반 인증 기법과 같이 사용함으로써 인증에 사용되는 비용을 줄일 수 있다.

향후 본 논문에서 제안한 인증 기법을 실제 이동 에이전트 플랫폼을 통해 구현할 계획이다. 또한 본 논문에서 제안한 인증 기법을 기반으로 홈 네트워크 환경에서의 이동 에이전트 플랫폼 접근 제어 기법을 설계할 계획이다.

6. 참고문헌

[1] Bill Rose, "Home Networks: A standards Perspective.", IEEE Communication Magazine, p.78 – 85, December 2001

[2] Jeong-Joon Yoo and Dong-Ik Lee. "Scalable Home Network Interaction Model Based on Mobile Agents.", Proceeding of the PerCom'03, p.543 – 546, March 2003

[3] Call Ellison, "Device Security 1: Service Template For UPnP Device Architecture 1.0", www.upnp.org, November 2003

[4] Sun Microsystems Inc, "AR - Jini™ Architecture Specification", www.jini.org.

[5] HAVi Inc, "The HAVi Specification version 1.1", www.havi.org, May 2001

[6] Neeran M.Karnik and Anand R.Tripathi, "Agent Server Architecture for the Mobile-Agent System.", Proceedings of the PDPTA'98, p.66 – 73, July 1998

[7] Shimshon Berkovits, Joshua D. Guttman and Vipin Swarup, "Authentication for Mobile Agents.", Mobile Agents and Security LNCS, p.114 – 136, 1998