유비쿼터스 컴퓨팅을 위한 신뢰그룹 관리

박종열* 이동익* 홍순좌** 박중길** 이진석**
*광주과학기술원
**국가보안기술연구소
jypark@kjist.ac.kr

Trusted Group Management for Ubiquitous Computing

Jongyoul Park*, Dong-Ik Lee*, Soon-Jwa Hong** , Joong-Gil Park**, Jin-Seok Lee**
*Kwang-Ju Institute of Science and Technology
**National Security Research Institute

요 약

유비쿼터스 컴퓨팅은 그 발전배경에 있어서 이동성을 강조하고 있다. 개인의 휴대 단말은 점차 작고 잘 보이지 않게 되면서 주변의 컴퓨팅 자원을 활용하는 위탁컴퓨팅 모델이 부각되고 있다. 하지만 개인의 휴대 단말이 악의적인 네트워크 환경이나 위탁컴퓨터에 대해서는 무기력한 것이 사실이다. 이를 보완하기 위해서는 휴대 단말이 신뢰할 수 있는 신뢰 그룹에게 원하는 작업을 위탁할 수 있어야 하고 서버 그룹과 클라이언트 그룹 사이의 서로 다른 기능을 제공해야 한다. 논문은 유비쿼터스 컴퓨팅 환경에서 휴대 단말인 클라이언트들이 신뢰할 수 있는 신뢰 서버들을 효율적으로 관리할 수 있는 비 대칭형 그룹 관리 시스템을 설계하고 제안한다.

1. 서론

유비쿼터스 컴퓨팅의 개념은 Xerox Park 의 Mark Weiser[1]에 의해서 처음 제안 되었으며 일반적으로는 다음과 같은 특징을 갖는다 [2].

- ✓ 산재하고, 쉽게 접근 가능하고, 때로는 보이지 않는 컴퓨팅 디바이스들
- ✓ 이동이 쉽고 때로는 환경에 내장되어 있는 것들
- ✓ 산재된 통신 구조에 연결된 것들

위의 특징에서도 알 수 있듯이 많은 컴퓨터들이 서로 연결되어 있고, 사용자는 그 컴퓨터들을 실제로 인지하지 않아도 자신이 원하는 작업을 언제 어디서나 서비스 받을 수 있는 컴퓨팅 환경을 말한다.

뛰어난 성능의 PDA의 등장과 무선랜, 블루투스, 적외선 통신과 같은 무선 통신 기술이 발전하면서 유비쿼터스 컴퓨팅 기술은 차세대 컴퓨팅 환경으로서의 확고부동한 자리를 점하게 되었다. 유비쿼터스 컴퓨팅을 실현하기 위한 많은 기술들 중에 사용자의 인터페이스는 기존의 시스템과 많은 부분에서 다르다. 이동이 쉽고 사용자가 특별히 인지하지 않아도 되는 특징은 많은 기능을 모두 포함하는 기존의 범용 컴퓨터와는 다른 작은 특성화된 컴퓨터를 요구하게 되었다. 이러한 작은 컴퓨터들은 사용자가 필요로 하는 모든 프로그램과 기능을 갖추는 것은 비효율적이다. 따라서 유비쿼터스 컴퓨팅 환경에서 사용자는 주위에 산재되어 있는 컴퓨팅 자원을 필연적으로 이용하게 되고 이 과정에서 이동 코드 기술이 주로 활용된다[3,4].

주위의 컴퓨팅 자원을 활용하는 위탁 컴퓨팅 환경은 수행 환경 자체가 악의적일 수 있기 때문에 보안 문제가 크게 강조되고 있다[3,5]. 이러한 문제를 해결하기 위해서는 클라이언트가 자신의 작업을 믿고 위탁할 만큼 신뢰하는 서버들의 목록을 별도 관리해야 한다.

본 논문에서는 사용자가 산재된 다수의 유비쿼터스 컴퓨터들 중에서 자신의 프로그램을 안전하게 위임할 수 있는 인증된 서버들을 찾는 것을 목적으로 한다.

2. 관련 연구와 문제점

클라이언트에 의해서 특정 서버가 신뢰를 인정 받기 위해서는 클라이언트와 서버 사이의 신뢰 관계가 성립되어야 한다. 유비쿼터스 환경에서 클라이언트와 서버 사이의 신뢰관계는 다음과 같이 분류할 수 있다.

1. **최상위 신뢰 등급**: 신뢰 수준이 가장 제한적인 등급으로 자신이 절대적으로 신뢰하는 서버들의 목록으로 구성되며, 일반적으로는 사용자의 개인 서버가 전형적인 경우이다.

2. **보통 수준의 신뢰 등급**: 일반적인 용도의 컴퓨팅 환경에서 사용하는 신뢰 수준으로 유비쿼터스 네트워크에서 정의하고 관리되는 신뢰 수준을 나타낸다.
3. **최하 수준의 신뢰 등급**: 최종 사용자에 의해서 수행되고 수집되는 모든 정보가 비밀을 요하기 보다는 빠른 수행을 필요로 하는 수준의 신뢰 수준으로, 특별한 보호 기능을 요하지 않는다.

위와 같은 3가지 분류에서 최상위 신뢰등급과 최하 수준의 신뢰등급은 별도의 관리를 필요로 하지 않다. 반면 보통 수준의 신뢰 등급은 사용자에 의해서 지정된 그룹 혹은 유비쿼터스 네트워크에서 정의하고 있는 신뢰도 높은 그룹이다. 이들은 지리적으로 광범위하게 분산되어 있고 규모면에서 상당히 큰 규모를 가진다.

지금까지 그룹의 구성원들 사이의 비밀정보를 공유하기 위해 많은 연구들이 진행되어 왔다. 특히 암호학적 방법을 찾기 위한 방법이 많은 연구되었다[6]. 암호학적 방법은 뛰어난 보안성을 가지고 있지만, 유비쿼터스 컴퓨팅 환경에서 대규모 그룹을 대상으로 사용하기에는 아직 성능상의 제한을 가지고 있다. 반면 대규모의 그룹을 대상으로 하는 시스템에서는 텍사스 대학의 키 그래프를 이용한 방법이 상당히 효율적인 것으로 알려져 있다[7]. 키 그래프를 이용한 방법은 그룹의 구성원을 일정한 기준에 의해서 소규모 서브 그룹으로 분리하여 관리하는 방법으로 새로운 구성원의 추가와 삭제 시에 빠른 적용이 가능하기 때문에 대규모 그룹을 대상으로 하는 경우에 적합하다.

키 그래프를 이용한 방법은 기존의 개별적으로 키를 분배하던 방식을 서브그룹단위로 키 분배와 갱신을 하여 작업의 양과 시간을 대폭 축소 하였다. 위 방법은 통신의 내용을 그룹 외부로의 유출을 막는 비밀성에 중점을 두고 있다. 반면 유비쿼터스 컴퓨팅에서의 신뢰 그룹의 관리는 클라이언트의 프로그램을 안전하게 수행해줄 인증된 시스템을 찾는 것을 목적으로 한다. 따라서 그룹 통신과 유비쿼터스 컴퓨팅 환경에서의 신뢰 그룹 사이에는 차이점이 존재하며 내용은 다음과 같다.

	그룹 통신	신뢰 그룹
구성원의 관계	대등	비대칭 (서버 와 클라이언트)
과거내용	공개불가	공개가능 (요청 메시지만 공개)
목적	비밀통신	시스템 인증

표 1 그룹통신과 그룹관리

이밖에 인증서를 이용한 방법도 가능하다[8]. 신뢰 그룹으로 판정된 시스템에게 인증서를 부여하고 클라이언트는 인증서를 가진 서버에게 프로그램을 위탁할 수 있다. 하지만 인증서를 이용한 방법은 서버의 목록이 변경되면 인증서의 폐기까지 변경이 불가능하고

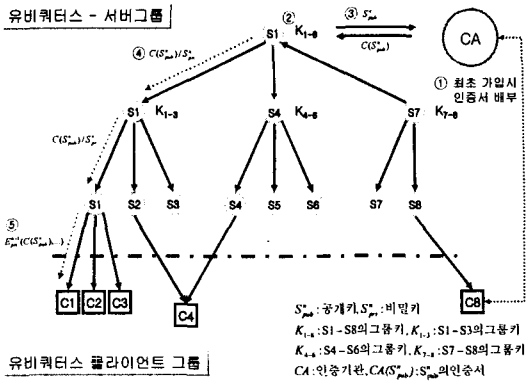

그림 1 유비쿼터스 컴퓨팅을 위한 그룹 관리

클라이언트에서는 폐기목록을 검색하는 등의 추가 작업이 필요하다. 더욱이 유비쿼터스 컴퓨팅에서의 위탁 컴퓨팅 모델은 특정 서버가 안전한가를 검사하는 것이 아니고 위탁 요청 메시지를 유비쿼터스 네트워크에 흘려 보내고 권한을 가진 서버[1]가 요청 메시지를 해독하여 요청을 처리하는 방식으로 인증서만을 이용한 방법은 적합하지 않다.

3. 유비쿼터스 컴퓨팅을 위한 그룹 관리 시스템

본 논문에서는 키 그래프를 이용한 그룹 통신 방법을 변형하여 유비쿼터스 환경에 적합한 신뢰 그룹 관리 시스템을 설계한다. 기존의 키 그래프를 직접 이용한 방법의 경우는 작업을 위탁하는 클라이언트와 위탁 받는 서버가 동등한 구조를 가지고 있다. 반면 유비쿼터스 컴퓨팅에서 신뢰 그룹은 두가지 구성원으로 나뉘어 진다. 신뢰 서버들로 구성된 서버 그룹과 클라이언트들로 구성된 클라이언트 그룹이다. 이들의 특징은 다음과 같다.

- ✓ **서버 그룹**: 많은 컴퓨팅 자원을 가지고 있으며 항상 네트워크에 연결되어 있다. 클라이언트 그룹에 강한 신뢰를 심어주기 위해서 구성원의 관리가 철저하고 그들 사이에 그룹 키를 공유한다.
- ✓ **클라이언트 그룹**: 적은 컴퓨팅 자원을 가지고 있으며 때에 따라서는 오프라인으로 작업을 하기도 한다. 신뢰 그룹의 구성원이기는 하지만 다른 사용자에게 신뢰를 심어줄 필요는 없다.

따라서 위의 두 그룹은 서로 달리 관리 되어야만 한다. 본 논문에서는 그림1과 같이 두 그룹을 구분하였고 각각 비밀키 와 공개키를 배분한다.

제안된 시스템에서는 신뢰 그룹 전체를 총괄하는 인증기관(CA)의 존재를 가정한다. 인증기관은 서버 그룹의 구성원을 결정 하고 클라이언트에게 인증서를 발급해 준다. 유비쿼터스 컴퓨팅환경에서 인증기관은

[1] 그룹키를 아는 서버만 클라이언트의 요청 메시지를 해독할 수 있다.

기업, 개인, 네트워크 제공자(Network Provider), 정부기관 등 다양한 형태가 될 수 있다.

그림1은 그룹의 공개키와 비밀키의 분배과정을 그린 것으로 각 단계별 설명은 다음과 같다.

① 클라이언트가 새로 그룹의 구성원이 되면 인증기관으로부터 신규 인증서(자신의 공개키)를 발급 받는다.

② 서버 그룹의 구성원이 변경되어 서버 그룹의 그룹키 $K_{1\text{-}8}$ 을 새로 생성하는 경우 공개키/비밀키를 같이 생성한다.

③ 서버 그룹은 인증기관으로부터 공개키의 인증서를 발급 받는다.

④ $K_{1\text{-}8}$, 비밀키, 공개키 인증서를 서버 그룹에 전송한다.

⑤ 클라이언트 그룹에 전송할 공개키 인증서를 이전 클라이언트 그룹의 비밀키로 암호화 해서 전송한다.

그림 2 공개키 분배과정

즉 서버 그룹의 그룹 키는 기존의 키 그래프를 이용하는 경우와 동일한 방법으로 관리가 되며, 클라이언트 그룹에게는 인증서 기반의 제한된 공개키만을 제공한다. 여기서 **" 제한된 공개키"** 란 공개키를 모두에게 공개하는 것이 아니라 그룹의 구성원이 된 클라이언트들에게만 공개한다는 의미이다. 공개키를 제한적으로 배포하기 위해서 서버 그룹에서 클라이언트에게 새로운 공개키를 배포할 때 이전 비밀키 S_{pri}^{n-1}로 암호화 하여 전송한다. 이전 공개키 S_{pub}^{n-1}를 아는 클라이언트는 쉽게 새로운 공개키를 얻을 수 있다.

만약 클라이언트가 오랜 기간 동안 오프라인으로 작업을 하거나 가입 후 처음으로 키를 배분 받는 경우라면 그룹의 인증서버로부터 발급 받은 인증서로 별도의 인증 과정을 거치게 된다.

4. 시스템 특징 및 안전성 분석

제안한 시스템은 유비쿼터스 컴퓨팅 환경에서 비대칭적 구조의 그룹을 효과적으로 관리하기 위해 제안하였다. 클라이언트 그룹에 속한 디바이스들은 자신이 중요한 작업을 위탁하고자 할 경우 자신이 가지고 있는 공개키로 암호화하여 유비쿼터스 네트워크에 전송한다. 유비쿼터스 네트워크는 요청 작업을 처리할 수 있는 서버를 선택하고 그 서버가 클라이언트가 신뢰하는 그룹에 속한 경우라면 요청 메시지를 복호화하여 서비스하겠지만 그렇지 못한 경우에는 서비스 제공이 실패하게 된다.

서버 그룹과 클라이언트 그룹은 서로 다른 키를 가지게 된다. 이 과정에서 서버 그룹과 클라이언트 그룹 사이에 발생 가능한 공격은 두가지 형태가 있다. 하나는 새로 분배되는 공개키 S_{pub}^{n}을 알아내는 것이고, 다른 하나는 키를 분실하거나 오랜 기간 오프라인 이여서 새로운 공개키를 받지 못한 경우이다.

- **새로운 공개키 S_{pub}^{n}을 알아 내는 방법**: 공개키 S_{pub}^{n}의 인증서를 이전 비밀키 S_{pri}^{n-1}로 암호화하기 때문에 이전 그룹 외에 새로운 공개키를 알 수 없다.
- **완전히 새로운 공개키를 발급 받는 경우**: 인증기관에서 별도로 전송하는 공개키를 발급 받기 위해서는 인증기관의 인증서나 인증기관의 인증과정을 거쳐야 하기 때문에 외부에 유출되지 않는다.

5. 결론

본 논문은 유비쿼터스 컴퓨팅에서 적은 컴퓨팅 자원을 가지는 유비쿼터스 디바이스들이 자신을 작업을 신뢰할 수 있는 서버에게 위탁할 수 있도록 신뢰 서버 그룹의 효율적인 관리 방법과 이를 이용하기 위한 클라이언트 그룹의 구성에 관한 방법을 제안하였다. 제안한 방법은 신뢰 서버들 사이에 동일한 그룹키를 가지고 있어 클라이언트들이 언제 어느 서버와도 통신을 할 수 있는 가상의 신뢰 공간을 제공하게 된다. 앞으로 악의를 가진 클라이언트가 신뢰 서버에 대한 공격을 감행하는 경우에 대한 보완 연구를 계속 진행한 예정이다.

6. 참고문헌

[1] M. Weiser, " The Computer for the 21st Century," Sci. Amer., Sept.,1991.

[2] NIST, http://www.nist.gov/pc2001/

[3] R. K. Balan, J. Flinn, M. Satyanarayanan, S. Sinnamohideen, H. Yang, "The Case for Cyber Foraging," In Proceedings of the 10th ACM SIGOPS European workshop, Saint-Emilion, France, September 2002.

[4] R. Campbell, D. Sturman, T. Tock, "Mobile Computing, Security and Delegation," the International Workshop on Multi-Dimensional Mobile Communications, 1994.

[5] J. Park, D. Lee, H. Kim, I. Jang, J. Park, "Virtual private computing for thin client against malicious surrogate", Spring Korea Information Science Society Conference, 2003.

[6] Mignotte, M., " How to share a secret?," Cryptography - Proceedings of the Workshop on Cryptography, Burg Feuerstein, Germany, p. 371. Springer-Verlag, Berlin, 1983.

[7] C. Wong, M. Gouda, S. Lam, " Secure group communications using key graphs," IEEE/ACM Transactions on Networking, Volume. 8, Issue 1, p. 16-30, Feb. 2000.

[8] M. Naor, K. Nissim, " Certificate Revocation and Certificate Update," Proceedings 7th USENIX Security Symposium, San Antonio, Texas, 1998.