UPnP 환경에서 안전한 비동기 메시지 통신 서비스 구현

박희만[O*] 이영록* 이형효** 노봉남*
*전남대학교 정보보호협동과정
**원광대학교 정보전자상거래학부
hareup@lsrc.jnu.ac.kr[O], {yrlee,bongnam}@jnu.ac.kr*, hlee@wonkwang.ac.kr**

Implementation of Secure and Asynchronous Message Communication Service in UPnP Environment

Heeman Park[O*], Younglok Lee*, Hyonghyo Lee**, Bongnam Noh*
*Dept. of Information Security, Chonnam National University
**Div. of Information and EC, Wonkwang University

요 약

유비쿼터스 환경에서는 개체가 특별히 소비자를 지정하지 않고 메시지를 송신하는 것과 같은 메시지 전송방법을 자주 사용하게 된다. 이런 통신 방법으로 기존에는 N:1 클라이언트/서버 통신 방법을 기반기술로 하였으나 컴퓨팅 기기들이 점점 산재되고, 기기들의 이동성 또한 증가되면서, 이러한 통신 모델은 여러 형태의 분산 컴퓨팅 환경에 적용하기에는 불충분하게 되었다. 유비쿼터스 컴퓨팅 환경을 포함한 오늘날의 많은 분산 컴퓨팅 환경에서는 여러 응용들의 메시지 상호작용을 위해 간접 통신 모델을 사용하고 있다. 전통적인 통신 모델을 사용하는 대신에 같은 간접 통신 모델을 이용하면, 분산 환경에서의 응용들 사이의 결합도를 감소시키고 많은 정적인 요구들을 제거할 수 있는 이점이 있다. 본 논문에서는 신뢰할 수 있는 유비쿼터스 환경을 만들기 위해 UPnP 기반의 안전한 메시지 통신 서비스를 설계하고 구현한다. 구현된 서비스는 내용기반의 검색이 가능하고, SPKI/SDSI 인증서를 이용하여 정당한 권한을 지닌 제공자와 소비자만이 메시지를 주고받을 수 있도록 한다.

1. 서 론

유비쿼터스 컴퓨팅 환경에서는 네트워크에 연결이 자주 끊기는 응용들이 출현하게 된다. 이들 응용들은 특별히 소비자를 지정하지 않고 메시지를 송신하거나 메시지 생산자와는 관계없이 특정 메시지만을 받아들이는 것과 같은 메시지 전송방법을 자주 사용하게 된다. 이들 응용들은 기존의 연결된 네트워크 컴퓨팅 환경에서처럼 직접적이고 결합적인 통신을 하기에는 많은 제약들이 있다. 이들 응용들은 네트워크 사이를 이동하기도 하고, 어느 순간 전원이 방전되어 네트워크상에서 사라지기도 하며, 단일 처리 운영체제에서 네트워크에 연결된 응용이 초점을 잃음으로써 연결이 끊길 수도 있다. 따라서 응용간의 통신에도 이와 같은 동적인 특성을 반영하여 응용간의 통신에도 간접적이고 분리된 통신을 제공하여야 한다. 상호 작용하는 응용들 간의 분리와 간접성을 획득하는 가장 일반적인 방법은 제3의 메시지 통신 서비스를 이용하는 것이다.

연결이 자주 끊길 수 있는 응용을 위해서 메시지 통신 서비스는 메시지 소비자를 위해 에이전트와 같은 역할을 해야 한다. 그리고 메시지 소비자가 메시지를 수신할 준비가 되었을 때 전달해 줄 수 있어야 한다. 또한 메시지 생산자의 입장에서 메시지 소비자에 대한 정보를 알지 못하더라도 메시지를 발행할 수 있어야하며, 메시지 소비자 또한 메시지 생산자에 대한 정보를 모르더라도 메시지를 수신하는데 문제가 없어야 한다. 메시지 소비자는 자신이 받은 메시지 중에서 원하는 정보를 찾기 위해 많은 시간을 소비할 필요 없이 원하는 메시지만을 수신할 수 있어야 한다. 마지막으로 이러한 일련의 메시지 전달 과정은 안전해야 한다는 것이다.

본 논문에서는 신뢰할 수 있는 유비쿼터스 환경을 만들기 위해 UPnP 기반의 안전한 메시지 통신 서비스를 설계하고 구현한다. 구현된 메시지 통신 서비스는 내용기반의 검색을 가능하게 하고, 정당한 권한을 지닌 제공자와 소비자만이 메시지를 주고받을 수 있도록 한다. 메시지 통신 서비스에 인증과 인가 기능을 제공하기 위해 SPKI/SDSI 인증서를 이용한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 본 연구에 선행한 유비쿼터스 환경에서의 메시지 서비스들의 특징을 기술한다. 3장에서는 UPnP 환경에서 안전하게 메시지를 전달하는 메시지 서비스의 구현을 보여준다. 마지막으로 5장에서는 구현된 시스템에 대한 분석과 결론을 기술한다.

2. 관련연구

UPnP에는 서비스와 그 서비스를 이용하는 클라이언트들간에 비동기 알림을 위한 UPnP 이벤팅 프로토콜이 있다. 이벤팅 프로토콜은 서비스의 모든 상태 변수를 한번에 관심있는 소비자에게 알려주는 프로토콜이다. 하지만 서비스의 상태변수외의 다른 메시지를 주고 받을 수 있는 방법을 제공하지는 못한다. 또한 메시지를 주고받는

생산자와 소비자간에는 단단한 결합을 가지고 있어서, 소비자는 같은 타입의 메시지를 받아 들이기 위해 모든 생산자에 결합을 유지하고 있어야만 한다.

유비쿼터스 컴퓨팅 환경에서의 미들웨어에는 Gaia, M3-RTE, Aura[1,2,3] 등이 있다. 이들 미들웨어들은 비슷한 구조의 이벤트 서비스들을 포함하고 있지만, 모두 보안을 고려하지는 않았다. 대표적으로 Gaia의 이벤트 서비스는 서로 다른 개체들 사이에서 분리된 통신을 제공하기 위한 모델을 제공한다. Gaia 이벤트 서비스는 Orbacus-Corba[4]의 기초적인 이벤트 서비스를 사용하여 통신한다. Gaia의 이벤트 서비스는 OMG(Object Management Group)의 COS(Common Object Service)[5] 모델의 pull기반의 이벤트 전달과 push 기반의 이벤트 전달 모두를 위한 인터페이스를 가지고 있다. Gaia의 이벤트 서비스는 채널 카테고리를 만들고, 그 카테고리와 관련된 채널들을 검색하며, 특정 카테고리와 관련된 채널들을 만들거나 지우기도 한다. 모든 Gaia 컴포넌트들은 스페이스의 상태 변화를 알기위해서 이벤트 서비스를 이용하고 그에 상응한 반응을 한다.

이렇듯 Gaia의 이벤트 통신은 이벤트 공급자와 이벤트 소비자들이 이벤트 서비스라는 중간매체를 이용하여 서로에게 메시지를 전달한다. 중간매체인 이벤트 서비스를 이용함으로써 직접통신에서 크게 나타났던 이벤트 공급자와 이벤트 소비자 간의 결합도를 낮추었고, 서로에 대한 정보에 의존하지 않고서도 통신을 할 수 있다. 하지만 네트워크상에서 전달되는 메시지의 순서를 장담할 수 없으며, 통신의 복잡성이 증가하게 된다. 또한 채널의 생성은 이벤트 서비스가 채널을 중앙 관리해야 하는 단점이 있고, 하나의 채널은 하나의 이벤트 타입을 전송하는 통로이므로 채널을 이용하는 이벤트 제공자와 소비자 사이에는 이벤트 타입에 대한 의존성이 발생하게 된다.

3. 안전한 메시지 통신 서비스

본 논문에서는 UPnP[6] 환경에서 컴포넌트를 사이에 안전하게 메시지를 주고 받을 수 있도록 메시지 통신 서비스를 구현한다. 구현한 메시지 통신 서비스는 메시지 생산자와 소비자의 낮은 결합도 제공하는 서비스로 메시지 소비자는 메시지 생산자에 대한 정보를 알지 못하여도 원하는 메시지를 받을 수 있고, 메시지 생산자는 소비자의 정보를 모르고도 메시지를 생산하고 전송할 수 있다.

또한 유비쿼터스 컴퓨팅 환경에서 송수신 되는 메시지에는 사용자의 컨텍스트 정보 등의 개인 프라이버시와 기타 비밀스러운 내용이 담겨져 있을 수 있다. 이러한 보안상의 문제로 메시지는 인증되어지고 권한이 있는 정당한 사용자에게만 전달되어야 한다. 하지만 에드혹과 같은 유비쿼터스 환경에서는 온라인 서버가 없을 수도 있으므로, 기존에 네트워크 환경에서 적용하던 인증과 접근제어 방법을 그대로 적용할 수는 없다. 본 논문에서는 이 문제를 해결하고자 SPKI/SDSI(Simple Public Key Infrastructure / Simple Distributed Security Infrastructure) 인증서를 사용하였다.

그림 1은 안전한 메시지 통신 서비스(SecMS: Secure Message Communication Service)의 구조를 나타낸다. MCS(Message Communication Service)는 메시지 생산자가 메시지를 발행하면 그 메시지에 구독 신청한 메시지 소비자에게 비동기적으로 메시지를 전달한다. 그리고

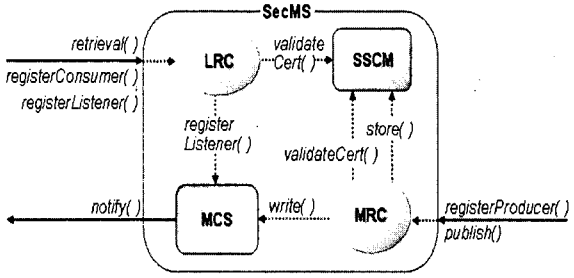

그림 1 안전한 메시지 통신 서비스

메시지 소비자가 연결이 끊겼던 기간 동안 받지 못했던 메시지를 검색할 수 있도록 메시지를 유효기간동안 저장하는 기능을 수행한다. 또한 메시지 소비자가 자신에게 맞는 필터를 붙일 수 있도록 한다.

SSCM(SPKI/SDSI Certificate Manager)는 UPnP 보안 모델에 기술된 인증서 검증 도구와 같은 것으로 메시지 소비자와 생산자가 SecMS에 대해 정해진 연산을 수행할 수 있는 권한이 있음을 증명한 인증서 경로를 검증하는 역할을 수행한다. SSCM도 마찬가지로 "Certificate Chain Discovery" 알고리즘을 포함하고 있다.

LRC(Listener Registration Controller)는 메시지 소비자가 메시지 구독요청시 메시지를 비동기적으로 받기 위한 리스너를 MCS에 등록할 책임을 지고 있으며, 메시지 소비자가 메시지를 검색할 때 정당한 사용자인지를 검사한다. LRC는 메시지 소비자에게서 받은 메시지 타입과 인증서 묶음을 SSCM에게 보내 권한 검사를 의뢰하고, 그 반환 값을 통해 메시지 소비자의 등록여부를 결정한다.

ERC(event Registration Controller)는 메시지 생산자를 등록하고 관리할 책임이 있고, 생산자가 메시지를 발행할 때 정당한 사용자인지를 검사한다.

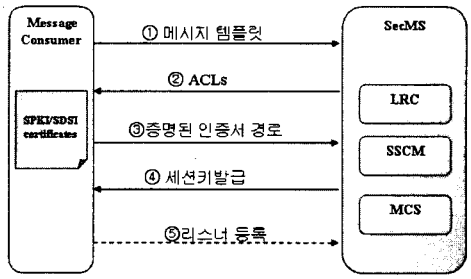

그림 2 메시지 소비자 등록 절차

메시지 소비자가 원하는 메시지에 대해 구독신청을 하기 위해서는 자신이 해당 메시지에 대한 정당한 구독 권한이 있음을 증명해야만 한다. 그림 2는 메시지 소비자가 자신이 구독하기 원하는 메시지에 대한 권한 증명과

SecMS에 등록하는 절차이다. ①메시지 소비자는 자신이 구독하기를 원하는 메시지에 대한 템플릿을 작성하고, SecMS에게 메시지 템플릿에 관련된 ACL(Access Control List)을 요구한다. ②SecMS는 메시지 템플릿에 해당하는 ACL들을 메시지 소비자에게 반환한다. ③메시지 소비자는 "Certificate Chain Discovery" 알고리즘을 통하여 앞서 가져온 ACLs과 비교하여 자신이 구독 권한이 있음을 증명하는 인증서 경로를 만들어 낸다. SecMS는 인증서 경로를 SSCM을 통해서 권한이 있음을 검증한다. ④SecMS는 세션키를 발급하고 ⑤구독권한이 증명된 메시지 소비자는 유효시간동안 메시지 검색과 메시지 구독신청이 가능하다.

메시지 생산자 또한 메시지 소비자와 유사한 방법으로 메시지 발행 권한을 증명하고 메시지를 발행한다.

4. 시스템 분석 및 결론

SecMS는 분리된 통신과 간접적 정보 전달이 가능하다. SecMS는 메시지 소비자와 메시지 생산자 사이에서 메시지의 중계 역할을 하면서 둘 사이에 분리된 통신을 가능케 한다. 분리된 통신으로 메시지 소비자들은 메시지 생산자에 대한 정보를 모르고도 필요한 메시지를 얻을 수 있다. 메시지 생산자의 입장에서도 마찬가지다.

SecMS에서 메시지 소비자는 자신이 요구한 메시지 템플릿을 통해 필터링된 내용기반의 메시지 수신이 가능하다. 메시지 템플릿에는 원하는 메시지 수신이 가능하도록 메시지 소비자가 정의할 수 있으며 SecMS는 정의된 템플릿에 맞는 메시지만을 통지한다. 관심 없는 메시지에 대한 필터링은 개발 횟수와 처리비용면에서 매우 경제적이고, 네트워크 부하를 줄일 수 있는 이점이 있다.

SecMS는 메시지를 저장할 수 있다. 연결끊김 기기들에게 메시지나 통지 배달을 위해서는 메시지 저장을 위한 지속 데이터 저장소가 요구된다. 이동기기가 연결이 끊겨있는 동안에 이동기기를 위해 온 메시지들이 있다면 이 메시지를 저장하고 관리한다. 이렇게 관리된 메시지는 메시지 소비자가 다음에 다시 연결을 하고 검색을 통해 가져갈 수 있게 된다.

SecMS는 메시지 유효기간 설정이 가능하다는 것이다. 메시지 서비스의 메시지 저장기능은 다른 한편으로 저장된 메시지의 폭증을 가져올 수 있는데, 이를 막기 위해 메시지마다 유효기간을 기술할 수 있다. 메시지 유효기간은 SecMS에 메시지가 저장되어 있을 최대 시간이다. 그 시간이 지나면 메시지는 SecMS에서 지워진다. 이 기능은 저장된 메시지의 폭증을 막을 수도 있지만, 메시지 유효기간 설정의 주체가 메시지 생산자라는 점에서 의미없는 메시지가 서버에 계속 남아 있음으로 해서 가져올 수 메시지 무결성의 문제를 유효기간의 자유로운 설정으로 해결할 수 있는 장점이 있다.

마지막으로 SecMS는 메시지 소비자와 메시지 생산자가 UPnP 서비스 보안 모델에서 제시한 바와 같은 방법으로 메시지 통신을 위해서 자신들이 메시지 수신과 메시지 발행권한이 있음을 증명하고 검증받는 절차를 거치고 안전한 메시지 통신을 한다.

[참고문헌]

[1] Manuel Román, Christopher K. Hess, Renato Cerqueira, Anand Ranganathan, Roy H. Campbell, and Klara Nahrstedt: Gaia:A Middleware Infrastructure to Enable Active Spaces. *In IEEE Pervasive Computing* 74-83, Oct. Dec. 2002

[2] A. Rakotonirainy, J.Indulska, W.W Loke, A.Aaslavsky: Middleware for Reactive Components: An Integrated Use of Context, Roles, and Event Based Coordination, *Lecture Notes In Computer Science*, Vol. 2218 . 77-98

[3] J. P. Sousa and D. Garlan: Aura:an architectural framework for user mobility in ubiquitous computing environments. *In Proceedings of the 3rd Working IEEE/IFIP Conference on Software Architecture*, Montreal, Canada, Aug. 2000

[4] Object-Orientated Concepts Inc , "ORBacus for C++ and Java".Versions 3.0, 1998.

[5] Object Management Group, "The Common Object Request Broker : Architecture and Specification" , 2.0 ed., July 1995.

[6] UPnP Forum, UPnP Device Architecture, Dec. 2003

[7] UPnP Forum, Device Security, Nov. 2003