제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

SSL을 이용한 Mobile CORBA 환경에서의 보안

강석태*, 김은규*, 정연진*, 이성룡*, 이광모*
*한림대학교 컴퓨터공학과
e-mail:stkang@cie.hallym.ac.kr

Security in Mobile CORBA Environment Using SSL

Seok-Tae Kang*, Eun-Gyu Kim*, Yeon-Jin Jung*, Sung-Ryong Lee*, Kwang-Mo Lee*
*Dept of Computer Engineering, Hallym University

요약

인터넷의 사용이 활발해지면서 이동 중에도 인터넷을 이용 정보를 얻거나 쇼핑을 하려는 사람들이 늘어남에 따라 Mobile Network이나 Mobile 환경에서의 보안이 요구되고 있다. 이 논문에서는 Architecture for Location Independent CORBA Environment (ALICE)구조에 기반을 둔 Mobile CORBA 환경에서 Mobile Host(MH)와 Mobile Gateway(MG)간의 통신 시 전파 특성상 보안에 취약하여 정보유출의 우려가 있다. 그래서 현재 공개키 방식으로 널리 쓰이는 SSL(Secure Socket Layer)을 이용 무선에서의 보안을 제안한다.

1. 서론

무선 통신 기능을 갖춘 이동전화가 대중화 되면서 사람들은 걸어 다니면서도 인터넷을 통해 쇼핑을 하거나 필요한 컨텐츠를 제공 받고 싶어 하는 욕구가 늘어나고 있다. 그러나 이동통신기기의 특성상 많은 용량의 메모리, 대형화면을 가질 수 없기 때문에 작은 용량의 애플리케이션을 요구 하고 있다.

OMG에서 정의한 CORBA의 패러다임은 CORBA 객체는 어떤 플랫폼에서도 실행가능하며, 네트워크 상의 어디든지 위치할 수 있으며, 어떤 언어든지 작성할 수 있다, 이를 이용하여 이질적인 분산환경에서 객체지향 응용을 구현하기 위한 기반구조이다.

이런 CORBA를 응용한다면 이동통신기기에서 다양한 애플리케이션을 구현하거나 사용할 수가 있을 것이다.

무선에서 송수신 되는 자료는 전파를 통해 공중으로 브로드캐스트(Broadcast)되는 특성으로 인해 주고받아지는 데이터가 다른 곳으로도 전달될 수 있다 그러나 SSL을 이용 한다면 지정된 수신자만이 수신된 데이터를 해독하여 이용할 수 있어 보안이 용이하다.

CORBA 자체에서도 보안관련 서비스를 제공하나 인트라넷이 아닌 인터넷으로 확대되어 나간다면 그러한 자체적인 보안서비스가 아닌 현재 신뢰할 수 있는 공인기관에 의한 보안으로 바뀌어 가야 할 것이다.

여러 가지 다양한 애플리케이션을 구현하기위해서 OMG의 CORBA를 무선통신에 적용시키는 것이 가장 이상적이다. CORBA를 적용한 연구가 몇 가지 있으나 그중에서 Architecture for Location Independent CORBA Environment(ALICE)는 MH 상에서 동작하는 CORBA 객체들이 표준 CORBA 응용들과 IIOP를 통해 통신할 수 있고, CORBA상의 다양한 분산환경의 모든 부분에 상위 응용계층과 연계한 세션 계층을 이용하여 구현하는 접근방식으로 이동환경의 문제를 해결했고, SSL 이용하여 무선구간인 MH와 MG 간의 보안문제를 해결했다.

2. 관련연구

2.1. ALICE

CORBA ORB는 일반적으로 IIOP를 사용하여 통신한다. IIOP는 일종의 객체 지향 프로토콜로, 다른 프로그래밍 언어로 쓰여진 분산 프로그램이 인터넷을 통해 서로 통신할 수 있도록 한다. 즉, IIOP는 ORB 간의 통신을 위한 일반 규약인 GIOP(General Inter-ORB Protocol)를 TCP/IP에서 동작하도록 정의한 것이다. CORBA 표준에서는 IIOP를 필수적으로 지원하도록 규정하고 잇다. 이러한 IIOP를 이동환경에서 수행 가능하도록 확장한다면, mobile CORBA 구현이 가능하게 될 것이다. 그렇지만, 현재 IIOP를 포함한 표준 CORBA 기술은 모바일 컴퓨팅 환경에서 사용되도록 설계되지 않았다. 이 모

바일 컴퓨팅 환경에서 CORBA를 사용하는 것은 하드웨어 이동성과 무선망의 특성에 의해 몇 가지 문제를 일으킬 수 있다. 이러한 문제를 해결하기 위한 구조로 ALICE를 비롯한 Mobile CORBA와 관련된 구조가 제시되었다. 그중 ALICE 구조는 응용계층과 연계한 세션 계층에서 이동성에 따른 문제를 해결하도록 하고, 기존 IIOP 표준을 수용하면서, 이동성에 따른 문제를 해결하는 별도의 계층을 제안하였다. 따라서 기존의 TCP나 IIOP의 별다른 수정 없이 Mobile CORBA 환경을 구현 할 수 있는 장점을 가진다.

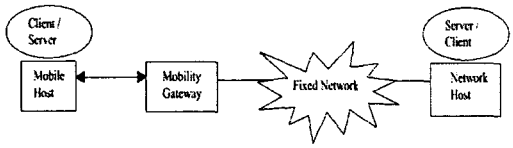

그림 1. 모바일 통신 구조

ALICE는 계층적인 접근법을 택하여 기존의 TCP/IP 구조와 표준 IIOP 메시지 구조를 유지하면서 별도의 세션 계층으로 이동 환경에 따른 여러 가지 문제점을 해결하도록 하고 있다. 또한, 유선 네트워크와 무선 호스트 사이에 MG가 마치 유선망과 무선 망 사이의 다리 역할을 하도록 하여 신뢰할 수 없고 낮은 대역폭을 가지고 무선망의 문제들을 해결한다.

ALICE의 구조는 클라이언트나 서버가 존재하는 고정된 네트워크와 MH 사이에 MG를 두도록 하는 것이다. 여기에서 MG의 중요한 역할은 MH에 대한 통신 요청을 받아서 MH에게 적절하게 전달해 주는 것이다. 또 다른 역할은 상위 계층에 대해서 주소 번역과 재전송과 같은 역할을 하게 된다.

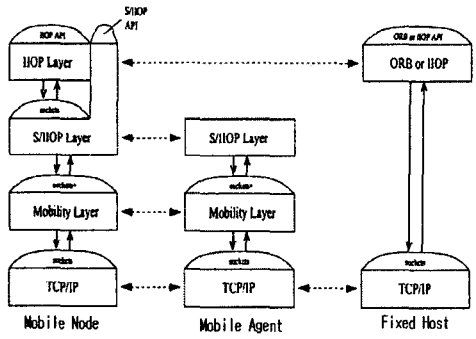

그림 2. ALICE 구조

ALICE의 각 계층 구조를 살펴보면, MH 상에는 IIOP 계층이 가장 상위 계층으로 존재하고, 하위 계층인 TCP/IP 계층과 IIOP 계층 사이에 S/IIOP 계층과 이동성 계층이 있다. MG상에는 S/IIOP계층이 있어 MH의 S/IIOP계층과 논리적 연결을 맺고, 이동성 계층과 TCP/IP 계층 또한 MH상의 이동성 계층, TCP/IP 계층과 각각 논리적 연결을 맺는다. 고정 호스트는 일반적인 유선망에서와 마찬가지로 IIOP계층과 TCP/IP 계층을 가지고 있고, TCP/IP 계층은 MG와 IIOP계층은 MH와 논리적 연결을 맺게 된다. IIOP 계층은 이동성과 관계없이 CORBA 표준 IIOP 프로토콜을 구현한 계층이다. 이 계층은 응용계층에서 다른 CORBA응용이나 IIOP로 적용된 객체들과 서로 통신할 수 있도록 한다. 이것은 TCP/IP나 이동성 계층, S/IIOP 계층 위에 직접 제공될수 있도록 하는 표준 소켓 인터페이스로 구현되어야 한다.

CORBA와 IIOP는 클라이언트 프로그램이 항상 요구하고 서버 프로그램이 클라이언트의 요구를 기다리는 클라이언트/서버 모델을 가정한다. 클라이언트가 네트워크 상 어딘가에 있을 어떤 프로그램에 대해 처리요구를 하려면, 그 프로그램의 주소를 가져야 하는데, 이 주소를 IOR (Interoperable Object Reference 이라고 부른다. IIOP를 이용할 때, 주소는 적어도 한 쌍의 호스트이름과 포트 번호로 구성되어있다.

GIOP는 프로그램이 IOR과 연결하여 서버가 응답을 보내도록 한다. CDR (Common Data Representation 은 자료를 표준 방식으로 교환하도록 한다.

Mobility 계층은 상위 계층에 이동성 정보를 제공하기 위해서 두 가지 종류의 callback함수를 도입한다. MH가 MG에 연결될 때 새로이 연결되는 게이트웨이 주소를 등록하게 된다. MG가 변경될 때 이 callback 함수를 실행하게 될 것이다. 이 정보를 이용해서 S/IIOP 계층은 현재 MH의 연결 지점을 알 수 있다. MH 상의 S/IIOP 계층은 현재 네트워크 연결정보를 이용하여 SIOR을 만든다. MG에는 기본 포트가 있어 새로운 객체가 생성되는지 항상 listen() 하고 있다. MH에서 IOR이 생성되었을 때 MH의 호스트이름과 포트번호의 쌍은 MG의 그것과 교체되는 것을 swizzled 라고 한다. MH는 이 포트를 알고 있어서 새로운 객체 레퍼런스를 생성할 때 기본 포트를 통해서 "Swizzling"을 하게 된다. MH에 있는 객체를 호출하기 위해서는 클라이언트는 해당 객체에 대한 SIOR을 가지고 있어야 한다.

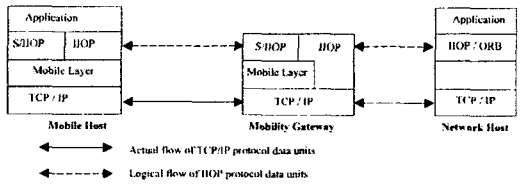

그림 3. 계층 구조

3. SSL(Secure Socket Layer)

SSL은 미국의 Netscape사에 의해 개발되었고, IETF(Internet Engineering Task Force)에서 SSL을 표준화하여 TLS를 개발하였다. 현재 사용되는 웹 브라우저는 모두 SSL와 TLS를 지원한다.

현재 무선인터넷 보안방식으로 TLS와 SSL을 기반

으로 하는 WTLS와 SSL 두 방식이 있다.

SSL은 인터넷상에서 신용카드번호나 온라인 뱅킹 데이터와 같이 중요한 정보를 전송할 때 가장 많이 사용되는 보안방법이다. SSL은 기밀성, 무결성, 사용자 인증, 부인봉쇄의 보안서비스를 제공한다.

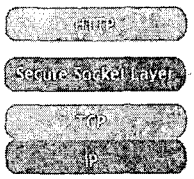

그림 4. SSL 구조

SSL은 128비트 암호화를 제공한다. 128비트란 실제로 모든 암호화된 트랜잭션에 의해 생성되는 '키'의 길이를 나타낸다. '0' 또는 '1'로 나타내는 키 값의 개수가 총 128개라는 뜻으로 암호를 설정할 수 있는 모든 경우의 수는 2^{128}이고 암호를 해독할 수 있는 확률은 $\frac{1}{2^{128}}$이 된다. 현재 40, 48, 56비트 암호체계는 해킹 기술에 의해 깨질 수 있음이 밝혀졌으나 128비트 암호체계는 안전함을 인정받고 있다.

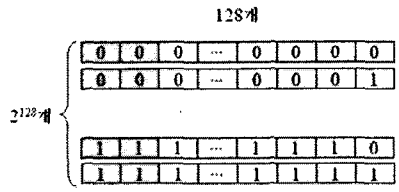

그림 5. 128비트

3.1. 인증방식

SSL은 공개키 인증방식을 사용한다. SSL이 지원하는 공개키 인증서는 서버 쪽은 DH, RSA, DSA, RSA암호화 인증서를 지원하고, 클라이언트 쪽은 DH, RSA 또는 DSA 인증서를 지원할 수 있다.

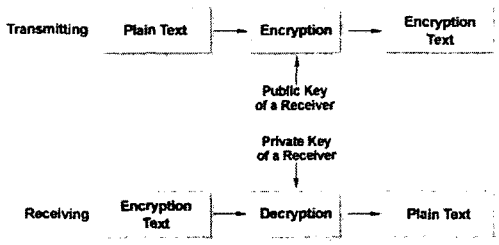

그림 6. 공개키 암호 방식

3.2. 인증모드

SSL은 세 가지 인증모드(Authentication Mode)를 지원한다. 익명모드(Anonymous), 서버 인증모드(SA, Server Authenticated), 클라이언트-서버 인증 모드(MA, Mutual Authenticated)를 지원한다. SSL에서 인증모드는 서버가 선택할 수 있도록 규정하고 있다.

3.3. 알고리즘

암호 알고리즘은 정해진 것 없이 여러 가지 알고리즘을 지원하면서 실행과정에서 이들은 선택적으로 사용할 수 있게 되어있다. 알고리즘의 선택은 클라이언트가 사용가능한 암호 알고리즘 리스트를 보내고, 서버가 이들 중에서 선택하는 방법이다.

지원하는 알고리즘으로는 해쉬함수의 경우 MD5, SHA-1을 지원하고, 비밀키 암호 알고리즘은 DES, 3DES, RC4등이 있다. 키 교환 알고리즘으로는 RSA 공개키 암호 알고리즘, DH 키 교환 알고리즘을 지원한다. 클라이언트 또는 서버의 인증서가 전자서명 인증서인 경우에는 키 교환 알고리즘에 사용할 수 있는 값을 생성한 후, 이 값을 전자서명을 통하여 서명한 후 보내는 방법을 사용한다.

4. 설계

Mobile 네트워크에서는 MobileNode(또는 MH) 와 MobileAgent(또는 MG)간의 통신 시 터널링을 하게 되어있다. 터널링 방법으로는 IP-in-IP, Minimal, GRE등이 있다 그러나 이러한 방법들은 보안을 위해 사용되는 것이 아니라 CN(Correspondent Node)에서부터 MN까지 Mobile 네트워크를 통할 때 거기에 적합하도록 패킷을 바꿔주는 역할을 한다.

터널링에 SSL을 더한다면 보안적인 면에서는 아주 뛰어날 것이다. 또한 MH 이동시 MG 간의 경로최적화 핸드오프가 된다는 가정 하에 구성을 해보았다.

CORBA는 IIOP를 통해 통신을 하는데 ALICE 역시 모바일을 지원하기 위한 Mobile 계층이 더 추가된 형식이고 TCP/IP를 기반으로 하기 때문에 SSL도 변형이나 수정 없이 SSL을 조합할 수 있다. 그림 7은 ALICE 계층 구조에 SSL을 더한 형태를 보여주고 있다.

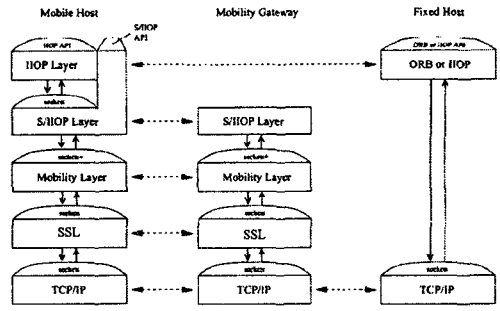

그림 7. ALICE + SSL

SSL은 상위 레벨 프로토콜 대신에 TCP/IP 프로토콜을 사용하여 SSL 사용 가능한 클라이언트와의 인증을 통해 SSL 사용 가능한 서버로 접속하는 것을

허가한다. 또한 서버가 인증을 통해 클라이언트와 통신하는 것을 허가하게 된다. 이로 인해 암호화 연결이 설정된 두개의 기계(server, client)가 서로 통신을 하게 된다.

SSL 계층은 SSL 레코드, SSL 핸드쉐이크 와 두개의 서브 프로토콜을 포함한다.

SSL 레코드는 데이터를 보내는데 사용하기 위한 포맷을 정의하고 SSL 핸드쉐이크는 SSL 연결이 설정되어있을 때, SSL 사용 가능한 서버와 클라이언트 사이의 메시지들을 교환하기 위해서 SSL 레코드를 사용한다.

5. 결론 및 향후 연구과제

현재 빠른 속도로 무선 단말기기가 보급되고 있고 IMT-2000이 상용서비스를 시작하였다. 이런추세로 보면 머지않아 무선 단말기를 소지한 사용자의 욕구가 늘어나고 무선인터넷에 접속을 하는 접속자의 수도 기하급수적으로 증가 할 것이다. ALICE+SSL은 무선에서의 이기종간의 효율적인 통신을 담당할 것이고, 보안의 문제에서도 효과를 볼 수 있을 것이다.

나아가 유선에서 진행되고 있는 PKI처럼 무선 PKI로 발전할 수 있어야 할 것이다.

6. 참고 문헌

[1] Mads Haahr, Raymond Cunningham and Vinny Cahill, "Supporting CORBA Applications in a Mobile Environment", Mobicom '99 Seattle Washington USA.

[2] Charles E. Perkins, "Mobile Networking Through Mobile IP", IEEE Internet Computing, January 1998.

[3] Netscape Communications Corporation, http://wp.netscape.com/security/techbriefs/ssl.html

[4] "CORBA Specification", http://www.omg.org

[5] 임경식, "이동인터넷 기술", http://www.krnet.or.kr/krnet99/tut/T331332/index.htm, KRNet99 컨퍼런스 특강, 1999년 6월.

[6]김병철, "무선인터넷 특강" 충남대학교 정보통신공학부 자료, 2001.

[7] X. Zhao, C. Castelluccia, and M. Baker, "Flexible Network Support for Mobile Hosts", ACM/Kluwer journal on Mobile Networks and Applications (MONET) Special Issue on Management of Mobility in Distributed Systems, volume 6, number 2, March/April 2001.

[8] 신혜령, 이형우, 김주호, "Mobile CORBA 환경에서 게이트웨이간의 경로최적화 핸드오프", 정보과학회논문지 제29권 제3호, p224~232, 2002. 6.

[9] SoftForum, http://www.softforum.co.kr