Clustered EJB 서버의 멀티캐스트 보안 연구

김수형[0] 이경호 김중배
한국전자통신연구원
(lifewsky[0], jjkim, khleesun)@etri.re.kr

A Study of Multicast Security in Clustered EJB Server

Soo-Hyung Kim[0] Kyeong-Ho Lee Joong-Bae Kim
Electronics and Telecommunications Research Institute

요 약

본 논문은 EJB 서버의 클러스터링 지원을 위해 구현된, 가변적인 멤버십 관리와 빈 인스턴스 상태 정보 복제 등의 서비스를 제공하는 멀티캐스트 프레임워크에서, 멀티캐스트 통신의 안전성을 보장하기 위한 멤버십 제어, 키 관리, 데이터 보안, 외부 보안 시스템 연동, 보안 정책 관리 등에 대해 논하며 그 구조와 방법을 제시하고자 한다.

1. 서 론

대부분의 주요 EJB 서버 개발 업체들은 대규모의 요청 처리와 가용성을 제공하기 위해 EJB 서버를 클러스터링 하는 구조와 방법을 제공하고 있다[5]. EJB 서버를 클러스터링 기술들은 클러스터 토폴로지에 따라 다양하겠지만, 필수적으로 빈 인스턴스의 상태 복제, 클러스터링 구성에 따른 적절한 정적/동적 빈 배포, 그리고 클러스터 멤버 관리 등의 기술들이 필요할 것이다. 특히 빈 인스턴스 상태 복제 기술의 경우, 전체 클러스터 멤버들간의 상태 동기화를 위해 멤버들간의 정보 공유 채널이 필요하며, 또한 동적 클러스터 멤버 관리가 지원되기 위해서는 멤버들의 가입과 탈퇴가 즉각적으로 반영되어야 한다[3].

본 연구팀에서는 개발된 EJB 서버의 클러스터링을 지원하기 위해, 클러스터에 참여하는 EJB 서버들의 가변적인 멤버십 관리와 빈 인스턴스 상태 정보 복제의 효율성을 향상 시킬 수 있는 멀티캐스트 프레임워크를 개발하였다[3]. 개발된 멀티캐스트 프레임워크는 클러스터 멤버들, 즉 EJB 서버들, 간의 통신을 주로 담당하며, 클러스터 멤버들의 동적 멤버십 관리를 위한 기능이 추가된 구조를 지니고 있다.

멀티캐스트 통신에서의 잠재적인 보안 위험 유형은 유니캐스트 통신에서 만날 수 있는 보안 위험 유형들과 동일하나, 다수의 통신 대상을 갖는 본질적인 특성 때문에 상대적인 위험은 더 크다 할 수 있다[1]. 특히 EJB 서버들간의 멀티캐스트 통신에서는 비즈니스에서 필요한 정보들이 빈의 상태 정보 변경에 따라 멀티캐스트 통신을 통해 전달 될 수 있기 때문에 보안에 대한 고려사항들은 무시될 수 없다. 방화벽으로 보호되는 내부 망에서 구축된 클러스터 일지라도 내부 사용자의 공격이 있을 수 있으며, 특히 WAN 환경의 구축을 고려한다면 클러스터 멤버들 간의 통신 보안이 필수적이라 할 수 있다.

이러한 이유로, 본 논문은 지금까지 개발된 EJB 서버들의 클러스터링 구조에 멀티캐스트 통신 보안 서비스를 제공하는 멀티캐스트 프레임워크의 보안 구조와 그 방법을 제시하고자 한다.

2. 클러스터드 EJB 서버

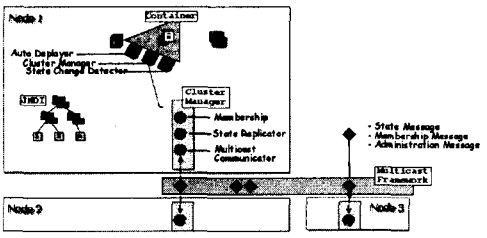

그림 1 Clustered EJB 서버 개념도

클러스터드 EJB 서버는 클러스터 멤버들 간의 빈 상태 정보 복제 메시지 송•수신, 클러스터 멤버 관리, 어플리케이션의 배포, 서버의 상태 모니터링 등을 지원하기 위해 그림 1과 같은 개념적인 구조를 갖는다.

클러스터 매니저는 멤버십 관리, 빈 상태 복제, 멀티캐스트 통신 채널 관리 등의 기능을 수행하는 해당 인스턴스들을 관리하며, 멀티캐스트 프레임워크의 지원하에 전체 클러스터의 멤버십을 구성한다. 멀티캐스트 프레임워크는 JavaGroups 또는 IP Multicast의 멀티캐스트 통신을 지원하는 전송 계층을 관리하고 각각의 서비스에 필요한 메시지들을 구성하여 다른 멤버의 멀티캐스트 프레임워크와 송•수신하는 기능을 제공한다. 그리고 자동 배포자는 멤버십에 가입한 멤버에 대한 어플리케이션의 동적 배포를 지원하며, 상태 변화 감지자는 Stateful 세션 빈 인스턴스의 상태 변화를 감지하여 변화된 상태를 클러스터 매니저의 멀티캐스트 프레임워크를 통해 전달하는 기능을 제공한다.

3. 멀티캐스트 프레임워크

멀티캐스트 프레임워크는 EJB 서버의 클러스터링을 위한 기본 서비스, 즉 멤버십 관리와 서버간 데이터 통신 등과 같은 서비스들을 제공하는데, 이러한 서비스들은 어플리케이션의 배포, 상태 복제, 멤버십 관리, 멤버 모니터링 등을 제공하는 각각의 매니저들에 의해 사용되며, 필요한 정보를 수집•제공하기 위해 클러스터 내 다른 EJB 서버와 끊임 없이 통신한다.

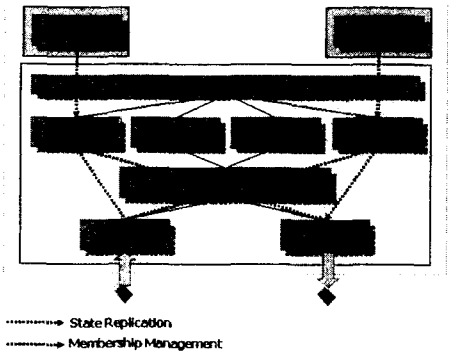

그림 2 멀티캐스트 프레임워크 개략도

클러스터 매니저는 그림 2와 같이, 통신 매니저, 멤버십 매니저, 상태 복제자, 보안 매니저와 같은 멀티캐스트 프레임워크의 주요 기능을 수행하는 매니저 인스턴스들을 관리한다. 각각의 매니저에서 요구되는 초기 설정 값은 클러스터 환경 정의 파일에서 가져오며, 환경 정의 파일은 EJB 서버의 관리자에 의해서 지정되어 멀티캐스트 통신 환경과 클러스터 구성 방법, 보안 정책 등과 같은 정보를 제공 한다.

통신 관리자는 유니캐스트/멀티캐스트 통신 채널을 생성하며, 이 채널을 통해 메시지를 구성하고 송•수신하는 역할을 담당하는데, 멀티캐스트 방법에 따라 신뢰성 있는 멀티캐스트 전송과 그룹 관리 서비스를 제공하는 JavaGroups[6]나 수행 성능 면에서 장점을 갖는 기존의 IP Multicast를 선택적으로 사용할 수 있다. 상태 복제자는 상태 변화 탐지자로부터 의뢰된 빈 인스턴스 상태 변화 정보 리스트를 관리하며 통신 관리자로부터 얻은 채널을 통해 이를 전달한다. 멤버십 관리자는 클러스터를 구성하고 있는 멤버들에 대한 정보를 관리하는데, 멤버들의 가입•탈퇴 정보를 동적으로 관리하기 위해서, JavaGroups를 사용하는 경우에는 JavaGroups의 그룹 관리 서비스를 통해, IP Multicast를 사용하는 경우에는 Heartbeat 메시지 송•수신을 통해 동적 멤버 관리 서비스를 제공한다. 보안 관리자에 대한 설명은 다음 장에서 자세히 설명한다.

3. 멀티캐스트 프레임워크에서의 보안 구조

멀티캐스트 보안의 목적은 정당한 그룹 멤버들이 안전하고 효율적으로 그룹 통신을 할 수 있도록 기밀성과 인증을 제공하는 것이며, 이를 위한 많은 연구가 오래 전부터 진행되어 왔다[1][2][4]. 본 논문에서는 클러스터드된 EJB 서버들 간의 멀티캐스트 통신이라는 제한된 영역에서의 멀티캐스트 보안을 다루고 있으며, 이를 처리하기 위한 EJB 서버 내 멀티캐스트 프레임워크 상에서의 보안 구조는 전체 EJB 서버의 구조적 틀에 적합하도록 구성되어야 한다. 따라서 아래에서 설명되는 구조를 통해 보안 서비스를 제공하고자 한다.

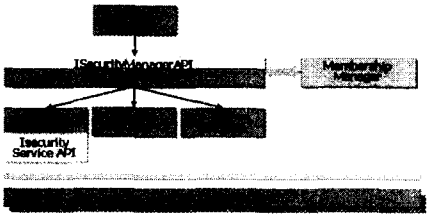

그림 3 보안 매니저의 개략도

멀티캐스트 프레임워크에서 보안 서비스를 제공하기 위해, 본 연구에서는 보안 매니저를 그림 3과 같이 클러스터 매니저를 통해 관리되도록 하였다. 보안 매니저는 보안 서비스 제공자, 보안 정책 관리자, 키 관리자를 하위에 두고 관리한다. 보안 서비스 제공자는 데이터의 암•복호화 및 무결성 확인, 멤버 인증 프로토콜 지원, 외부 보안 시스템과의 연동을 위한 API 제공 등의 서비스를 제공한다. 보안 정책 관리자는 해당 멤버가 참여하고 있는 클러스터 그룹 혹은 하위 그룹의 보안 정책을 관리하며, 신규 멤버의 Security Association을 위한 정보를 관리하고 멀티캐스트 보안의 수준, 키 관리 정책 수행 등의 서비스를 제공한다. 마지막으로 키 관리자는 세션 키를 생성하거나 멤버의 가입/탈퇴 시에 그룹 키를 갱신하는 서비스를 제공한다. 이러한 보안 서비스에 대해 다음 장에서 좀 더 상세히 살펴보도록 한다.

4. 보안 서비스

앞 장에서 설명한 바와 같이, EJB 서버의 클러스터링을 위해 지원되는 멀티캐스트 프레임워크 상에서, 제공되어야 하는 보안 서비스는 크게 멤버 가입/탈퇴 처리와 같은 멤버십 제어, 멀티캐스트 그룹 간의 세션 키 관리, 전송되는 데이터의 보안 및 외부 보안 서비스 연동, 마지막으로 보안 정책에 대한 관리로 정의할 수 있다.

4.1 멤버십 제어

구현된 멀티캐스트 프레임워크에서 클러스터의 멤버 구성은 동적으로 구성될 수 있다. 따라서 클러스터 그룹에 대한 멤버의 가입과 탈퇴를 탐지하는 모듈이 제공되어야 하는데, JavaGroups의 경우에는 그룹 관리 서비스를 통해, IP Multicast의 경우에는 Heartbeats 메시지 송•수신을 통해 구현되었다. 각 멤버들은 멤버십의 변화가 탐지되면 멤버십 관리자에게 이를 통보하고 멤버십 관리를 요청하는데, 멤버십 관리자는 보안 관리자를 통해, 멤버십 제어를 위한 가입/탈퇴 각각에 대해 다음과 같은 보안 작업을 수행한다. 단, 제안하는 멀티캐스트 보안 구조는, 그룹 제어자의 유형에 따른 분류에서, 분산형 구조를 채택하고 있다.

4.1.1 멤버 가입

클러스터에 참여하고자 하는 신규 멤버는 전체 클러스터 멤버에게 멤버십 가입을 요청하고 Kerberos 서버에 의해 인증된 인증 정보와 랜덤 키를 전체 멤버에게 전달한다. 기존 멤버들은 신규 멤버의 인증 정보를 보안 서비스 매니저를 통해 확인하고 키 관리 매니저를 통해 신규 멤버가 전달하는 랜덤 키를 조합하여 새로운 그룹 키를 생성한다. 새로운 그룹 키는 이후의 데이터 보안 서비스에서 사용된다.

위의 멤버 가입 시나리오를 수행하기 위해서, Kerberos 서버는 클러스터에 참여하고자 하는 멤버들의 DB를 구축하고

있어야 하며, 이는 신규 EJB 서버의 셋업 과정에서 이루어져야 한다. Kerberos 서버는 EJB 사용자의 인증을 위해 많이 사용되고 있다.

4.1.2 멤버 탈퇴

클러스터 그룹에 대한 멤버의 탈퇴가, EJB 서버의 고장과 같은 예측할 수 없는 이유로, 탈퇴 멤버의 사전 통보 없이 이루어지는 경우에도 멀티캐스트 프레임워크에서 지원되는 멤버 탈퇴 감지 기능을 통해 전체 멤버에게 통보되도록 설계되었다. 탈퇴를 통보 받은 멤버십 관리자는 키 관리자에게 이 사실을 전달하여 rekeying에 필요한 작업을 수행할 수 있다.

4.2 키 관리

클러스터 멤버들간의 멀티캐스트 세션에 대한 비밀성을 보장하기 위해서는 키에 대한 안전한 관리가 중요하며, 세션 동안의 키에 대한 접근은 인증 받은 멤버들에 의해서만 가능해야 한다. 키 관리 매니저는 안전한 키 관리를 위해, Kerberos 인증을 통해 전달 받은 세션 키를 그룹 키의 생성 시에 사용하도록 하여, 각 서버들이 정당한 인증 과정을 거쳐 그룹에 참여하지 않은 이상에는 그룹 키를 알 수 없도록 한다. 신규 멤버의 참여시에는 신규 멤버가 할당 받은 세션 키와 기존 그룹 키를 사용하여 키를 재생산 함으로써 rekeying을 수행한다. 신규 멤버는 자신의 세션 키와 클러스터 내 멤버로부터 부여 받은 기존 그룹 키를 통해 신규 그룹 키를 생산함으로써 클러스터 참여를 허용 받는다.

키 배포 구조는 중앙 집중형 구조를 고려할 수도 있으나, 현재 개발된 EJB 서버의 멀티캐스트 프레임워크 구조 상 분산형 구조를 채택한다.

4.3 데이터 보안 및 외부 보안 시스템 연동

멀티캐스트 채널을 통해 전달되는 데이터에 대한 무결성 및 기밀성, 그룹 인증, 소스 인증 등을 제공해야 한다. 네트워크를 통해 전달되는 데이터의 보안을 위해 어플리케이션 계층에서의 보안보다는 네트워크 계층에서의 보안이 좀 더 효율적이며 안전하다는 연구가 보편적이지만, 본 연구에서는 IPSec 등과 같은 멀티캐스트 통신의 하위 계층에서의 도움 없이 EJB 서버에서의 멀티캐스트 보안을 다양한 보안 정책에 따라 구축될 수 있도록 하는 것을 목표로 한다.

클러스터드된 EJB 서버들은 빈 인스턴스의 상태 변화를 즉각적으로 반영하여야 하기 때문에 데이터 보안의 정도는 관리자에 의해 명시적으로 지정되어야 하며 보안 정책 관리자는 이런 명시된 정보를 시스템 상에 반영할 수 있어야 한다.

EJB 서버는 사용자의 인증과 역할 관리를 위해 외부 보안 서비스와 연동하여 자주 서비스된다. 본 연구에서는 이처럼 이미 구축된 외부 보안 서비스를 통해 클러스터 멤버에 대한 인증을 수행하는 것을 고려하였으며, 보안을 위해 필요한 다양한 알고리즘에 영향 받지 않도록, 요구되는 공통의 보안 API를 설계하여 플러그인 구조를 채택 하고자 한다.

4.3 보안 정책 관리

클러스터드 EJB 서버의 멀티캐스트 보안은 서버 관리자가 명시한 클러스터링 환경 정보와 보안 정책에 따라 유연성 있게 수행되도록 한다. EJB 서버의 클러스터링 구조는 다양한 토폴로지를 통해 구축될 수 있으며, EJB 서버에서 수행되는 어플리케이션 또한 다양한 업무적 특성을 가질 수 있다. 서버 관리자는 이러한 상황을 고려하여 보안 정책을 수립하고 명시할 수 있어야 한다.

EJB 서버가 방화벽으로 보호되는 내부 망에서 안전하다고 판단되며, 어플리케이션의 특성 상 내부 망의 보안 체계만으로 충분하다고 생각된다면 멀티캐스트에 통신에 대한 보안은 무시되고, 전체 시스템의 효율성만을 제고할 수 있다. 하지만 수행되는 어플리케이션에서 세션 빈의 상태 정보가 중요한 보안 대상이 된다고 판단된다면, 요구되는 보안의 정도에 따라, 데이터 보안의 강도, 그룹 키의 갱신 주기, 멤버십의 제어 정책, 접근 제어 정책에 대한 변화를 적용할 수 있어야 한다. 내부 망의 서버도, 외부 망에서와 같이, 언제든 공격의 대상이 될 수 있기 때문이다.

5. 결론 및 향후 연구

멀티캐스트 통신은 유니캐스트 통신보다 많은 잠재적인 위험 요소들을 가지고 있다. 이러한 위험 요소들로부터 방어하기 위해, 현재까지 많은 멀티캐스트 보안 및 키 관리에 대한 논문들이 있어 왔으나, 다양한 멀티캐스트 환경 하에서는 특별히 어떤 정책과 구조가 옳다고 말할 수는 없다.

본 논문은 EJB 서버의 클러스터링을 위해 구현된 멀티캐스트 프레임워크 상에서 클러스터 멤버들 간의 멀티캐스트 통신에 필요한 보안 구조에 대해 논하였다. 논의된 멀티캐스트 보안 구조에서 제공되어야 하는 보안 서비스는 멤버십 제어, 키 관리, 데이터 보안 및 외부 보안 시스템 연동, 보안 정책 관리이며, 이는 현재 개발되어 있는 클러스터드된 EJB 서버에 적합하도록 설계되었다.

향후, 멤버십 제어에서 요구되는 멤버 가입 및 탈퇴에 대한 프로토콜을 명시적으로 기술하고 검증해야 할 필요가 있으며, 보안 정책에 필요한 요소들을 살펴 보고 각 요소에 의해 EJB 서버에 미칠 영향과 보안 서비스를 통해 요구되는 추가적인 부담이 어느 정도인지 실험을 통해 조사되어야 한다. 또한 네트워크 계층에서의 멀티캐스트 보안이 가능한 시스템에서의 보안 구조를 고려해야 할 것이다.

6. 참고 문헌

[1] Peter S. Kruus, Joseph P. Macker, "Techniques and Issues in Multicast Security," Proc. IEEE MILCOM, 1998.

[2] 은상아, 조태남, 채기준, 이상호, 박원주, 나재훈, "안전한 멀티캐스트 서비스 제공을 위한 효율적인 그룹 관리 메커니즘 및 구조," 한국정보처리학회논문지, VOL. 9-C NO. 3, 2002.

[3] 김수형, 정승욱, 서범수, 노명찬, 김중배, "Clustered EJB 서버에서의 멀티캐스트 프레임워크 연구," 정보처리학회추계학술대회, 2002

[4] M. Moyer, J. Rao, P. Rohatgi, "A Survey of Security Issues in Multicast Communications," IEEE Network Magazine, Nov/Dec, 1999.

[5] Abraham Kang, "J2EE Clustering," http://www.javaworld.net/javaworld/jw-02-2001/jw-0223-extremescale.html, 2001

[6] Bela Ban, "JavaGroups User's Guide," http://www.javagroups.com/javagroupsnew/docs/newuser.zip, 2001