

Privilege Management Infrastructure를 이용한 Grid Computing 연구

최현석*, 이재인*, 김지호*, 박세현*, 송오영*

*중앙대학교, 전자전기공학부

A Study of Grid Computing Based on Privilege Management Infrastructure

Hyun Seok Choi*, Jai In Lee*, Ho Ji Kim*, Se Hyun Park*, Oh Young Song*,

School of Electrical & Electronics Engineering Chung Ang Univ.

요 약

본 논문에서는 제안하는 Grid Computing은 PMI(Privilege Management Infrastructure)를 이용하여 효율적으로 컴퓨팅 파워의 분산 관리하고 네트워크의 트래픽을 분산시키는 모델을 제시한다. 또한 Agent 간 통신 및 Agent와 Server 간 통신에서 Soap Protocol과 SSL Protocol을 접목하여 보안 RPC통신을 기반으로 데이터의 무결성과 기밀성을 보장한다. 본 논문에서 제안한 모델은 Agent를 효과적으로 관리하고 네트워크의 트래픽을 감소시킴과 더불어 Grid Computing의 성능이 개선될 것으로 기대된다.

I. 서론

Grid Computing은 다양한 기관과 지역에 걸쳐 분산되어 있는 다양한 종류의 컴퓨팅 자원을 보다 효율적인 방법으로 사용하는 컴퓨팅 방식이다. 1980년대 메타컴퓨팅(metacomputing)이라는 이름으로 시작하였으며 현재 세계 곳곳에 분포되어 있는 컴퓨터, 데이터베이스, 첨단 장비 등을 연결하여 가상의 단일 컴퓨터 만드는 프로젝트를 여러 나라에서 진행 중이다. 이러한 프로젝트에는 나노기술(Nano Technology), 환경기술(Environment Technology), 항공우주 기술(Space technology) 등이 있으며 이러한 문제점을 푸는데 슈퍼컴퓨터를 대신할 수 있게 한다.

현재 미국에서 진행 중인 주요 프로젝트에는 SETI@Home(우주생명체 탐색작업), HGP(인간 게놈지도 작성사업), NASA IPG(항공기 통합 설계) 등이 있으며 유럽에는 기초과학 연구지원사업인 유러피안 데이터 그리드 그리고 산업기술 연구사업인 유로 그리드가 진행 중에 있다. [1]

그리드에는 분산된 컴퓨팅 자원을 한대의 고성능 컴퓨터처럼 사용하는 계산 그리드(Computational Grid), 원격지에 분산된 자료들을

통합하여 분석할 수 있게 해주는 데이터 그리드(Data Intensive Grid), 그리고 이 두 가지 그리드를 통합하여 그룹간에 데이터를 공유하여 협업할 수 있는 액세스 그리드(Access Grid)가 있다. 이 중 가장 많이 연구되고 있는 분야는 계산 그리드(Computational Grid)이다. 계산 그리드에도 고성능 컴퓨터를 동시에 사용하여 주어진 문제를 해결하는 분산 슈퍼 컴퓨팅 그리드와 주어진 시간에 가능한 많은 작업을 처리하는 고처리율 컴퓨팅 그리드가 있다. 본 논문에서의 Grid Computing의 Architecture는 고처리율 컴퓨팅 그리드이다.

그리드는 그 특성상 자원 자원제공자의 Privacy 뿐만 아니라 통신상의 데이터의 기밀성과 무결성이 특히 요구된다. 그러나 다양한 컴퓨팅 자원을 하나로 통일할 수 없고 이를 통일적으로 관리하는데 매우 어렵다. 이러한 관점에서 본 논문에서는 Agent를 효과적으로 관리하고 통신상에 데이터의 기밀성과 무결성 보장을 위해 SOAP(Simple Object Access Protocol), SSL(Secure Socket Layer) 그리고 PMI를 적용하여 좀 더 나은 그리드 개발환경과 더불어 유연한 보안 서비스를 제공하는 그리드 모델을 제시하고자 한다.

II. 기존 Grid Computing

현재 세계에서 진행되고 있는 Grid Computing은 가능한 한 시간에 빠른 처리를 할 수 있는 고 처리율 컴퓨팅 그리드이다. 이러한 그리드는 자원 제공자에게 그리드 서버가 특정 데이터 파일과 그리드 서버와 통신할 수 있고 자원제공자의 Privacy와 데이터의 기밀성과 무결성을 보장해주는 보안 Agent를 제공한다. 특히 가장 많이 사용되고 있는 그리드 미들웨어인 Globus에는 사용자가 사용하는 인증서의 종류는 세 가지이다. GridCA에서 발행하는 사용자 인증서 그리고 프로세서가 실행되고 있을 때 잠시 생성되는 프로세서 인증서, 실제 사용자를 인증하는 사용자 프록시 인증서가 있다. 인증서의 종류가 많으면 그에 따른 인증서 관리가 어려워지게 된다. 즉, 인증서 하나로 해결할 수 있는 문제점을 많은 인증서를 발급함으로써 인증서 관리가 어렵게 된다. 또한 Globus에서는 보안 핵심인 openssl 라이브러리를 사용하지 않고 컨맨드라인 명령을 이용한다는 단점을 가지고 있다. 또한 인증서 발급을 위해 꼭 웹사이트에 들어가야 하는 단점을 가지고 있다.

또한 데이터 관리의 어려움으로 인해 현재 진행 중인 그리드 컴퓨팅 프로젝트들은 대부분은 한 가지 주제를 가지고 프로젝트를 진행 중이다. [2]

III. SOAP 프로토콜을 이용한 RPC(Remote Procedure Call)

본 논문에서는 SOAP 프로토콜을 이용하여 클라이언트의 요청에 따라 이에 응답을 주는 RPC 프로토콜을 적용한다. SOAP은 특정 분산컴포넌트 기술에 의존하지 않는 객체 액세스 프로토콜이다. 이는 XML과 HTTP를 사용하여 플랫폼에 독립적으로 서비스를 할 수 있게 해준다.

분산 환경 하에서 정보교환을 하기 위한 하나의 프로토콜인 SOAP은 다음과 같은 장점을 가지고 있다. 첫째, SOAP은 전송매체로 HTTP를 사용하기 때문에 인터넷에서 널리 사용된다. 둘째, HTTP와 XML을 사용하기 때문에 개발도구나 플랫폼에 구애를 받지 않는다. 이러한 SOAP 프로토콜은 그리드 컴퓨팅 환경에서는 자원제공자의 PC 플랫폼에 상관없이 개발이 가능하다는 장점을 가진다. 따라서 플랫폼 독립적인 SOAP 프로토콜을 사용하는 것은 적절하다. 또한 FTP를 이용하여 데이터를 전송하기 위해서는 또 다른 FTP 모듈을 개발하여야 하지만 SOAP 프로토콜을 이용할 시

에는 데이터 파일을 XML문서에 Binary 데이터 형식으로 집어넣어 전송이 가능하다는 이점이 있다. 또한 SSL을 접목시켜 HTTPS 서비스를 제공하여 SOAP 프로토콜에 전송되는 데이터에 대한 기밀성과 무결성을 보장해 줄 수 있다.[3]

IV. PMI(Privilege Management Infrastructure)

기존 공개키 인증서는 사용자의 신원 확인용으로만 사용되어 지므로 일반적인 환경에서의 접근 권한, 역할, 임무, 직위에 대한 정보의 필요성이 존재하게 된다. 이러한 요구로 인하여 인증서와 유사한 AC를 이용하여 사용자의 권한 등을 인증하게 되는데 이를 PMI 라고 한다. PMI는 AC를 발급, 저장, 유통을 제어하는 권한관리 기반구조로서 공개키 기반구조와 유사한 형태를 지니고 있다. AC 정보 제공을 위해서는 기존 신원 확인용 공개키 인증서의 확장 필드를 이용하며 신원 확인용과 별도의 속성 인증서를 발급한다. PMI의 구성요소로는 PKI의 최상위 인증기관(Root CA)와 대응되는 개념으로 최상위 권한 기관인 SOA(Source of Authority), 하위 CA와 대응되는 하위 권한 기관으로 AA(Attribute Authority) 그리고 속성 인증서 발급 서버인 ACS(Attribute Certificate Server)가 있다. PMI의 기본 구성은 다음과 같이 구성되어 있다.[4]

1) AA

SOA는 PMI 체계에서 최상위의 권한을 가진 관리자이다. 모든 사용자와 하위 관리자들에 대해 모든 서비스와 모든 역할을 할당하거나 폐지할 수 있다. 또한 SOA는 하위 관리자인 AA(Attribute Authority)들을 생성해 각 AA에게 일정 권한을 위임하거나 폐지한다. PAC을 사용해 모든 서비스와 역할의 권한 정보를 직접 관리한다.

2) Privilege Verifier(Validation server)

Privilege Verifier는 사용자의 인증서와 AA가 발행한 사용자의 AC를 검증하는 역할을 한다.

3) End-entity Privilege Holder(Agent)

AC를 사용하며 권한을 인증 받는 최종 사용자이다. [5]

AC는 Version, Holder, Issuer, Signature, serial Number, Validity, Attributes, IssuerUniqueID, extensions 필드로 구성되어 있다.

V. PMI를 이용한 Agent 그룹화 및 Load Balancing

본 논문에서 제안하는 그리드 모델에서는 PMI를 이용하여 Agent의 컴퓨팅 능력에 따라 agent의 레벨을 다음과 같이 나눈다.

- Group Leader Agent : 그리드 서버로부터 받은 작업량에 따라 Worker Agent에게 작업을 분배한다.
- Group CA Agent : 자신의 인증서를 이용하여 Group에 속해 있는 Agent들에게 인증서를 발급한다.
- Worker Agent : Group Leader로부터 작업을 받고 그에 따른 작업을 하고 결과를 Leader에게 전송한다

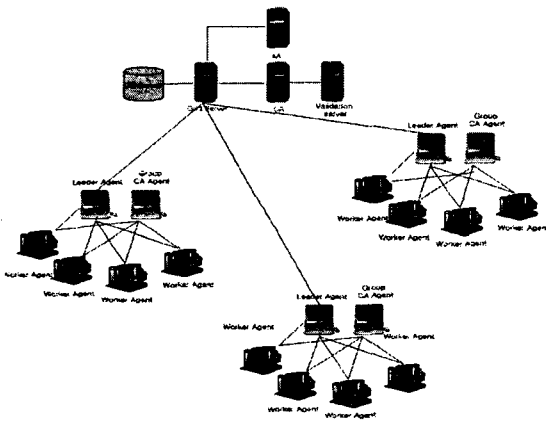


그림 1 제안 모델

다음 그림 2는 Server에 포함되는 모듈을 나타낸 것으로 Agent 그룹화 모듈, 작업 스케줄러 모듈, 그리고 마지막으로 Agent를 인증하는 PKI Server 모듈이 들어간다. Agent 그룹화 모듈은 그룹별 Agent 개수와 Leader Agent와 CA Agent 등을 관리한다. 작업 스케줄러 모듈은 작업을 분배하는 역할을 한다. PKI Server 모듈은 Agent의 인증을 담당하는 모듈로서 Soap Server의 기능을 담당한다. 즉, 그리드 서버의 기능을 최소화함으로써 Agent가 증가하여도 똑같은 질의 서비스를 가능하게 한다.

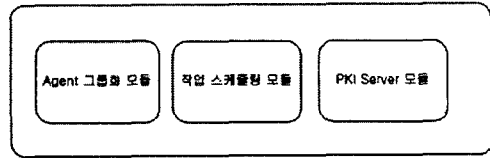


그림 2 Server 모듈

다음 그림 3은 Agent에 대한 모듈에 대한 그림이다. 각 Agent는 Leader Agent가 될 수 있으므로 작업 스케줄러 모듈을 필수적으로 포함해야 하며 PKI Server 기능도 같이 들어 있어야 한다. 즉, Worker Agent의 인증을 해주는 역할을 한다. 그리고 CA 모듈은 CA의 권한을 받은 Agent만이 이 모듈을 활성화 시켜 동작시킨다. 마지막으로 PKI Client 모듈은 PKI 기능과 함께 SOAP client의 기능을 같이 가지고 있다.

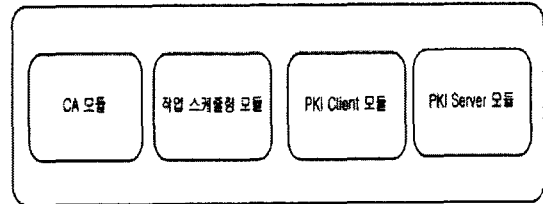


그림 3 Agent 모듈

Leader Agent 또는 CA Agent는 처음 동작 시 그리드 서버에게 권한 인증을 받게 되며 권한 인증을 받으면서 주기적으로 발행하는 Token을 부여받는다. 이 Token은 일정시간동안 유효하며 권한을 가지고 있다는 것을 증명하는 것이다. 다음은 AC를 이용하여 Agent의 권한 검증을 나타낸 것이다.

- ① Agent의 권한을 획득하기 위해 그리드 서버에게 AC 인증서와 사인값을 전송한다.
- ② 그리드 서버는 인증서 사인값을 인증 서버에게 전송하여 권한 검증을 요청한다.
- ③ 인증서버는 전달받은 데이터를 이용하여 Agent에 대한 권한 검증을 하고 이에 대한 결과값을 그리드 서버에게 전송한다.
- ④ 그리드 서버는 Leader Agent임을 확인하고 요청 메시지에 대한 처리를 하여 그 결과를 Agent에게 전송한다.

그림 1처럼 Agent를 그룹화 함으로써 일정의 특화된 작업을 수행할 수 있도록 한다. 즉, 이렇게

함으로써 한 가지 프로젝트만이 아닌 IT, ET, BT 등 다양한 프로젝트를 동시에 수행이 가능하다. 또한 평상시에는 Leader Agent만이 Grid Server와 통신하므로 네트워크의 트래픽을 분산시킬 수 있다는 것이다. 예를 들어, 1시간 안에 데이터가 들어와야 하는 프로젝트를 수행한다고 하면 작업이 분배되고 나서 1시간 안에 모든 작업이 완료되어야 한다. 그렇지만 지금까지와 같이 모든 Agent가 통신을 그리드 서버에게 직접 한다면 트래픽 집중으로 인한 네트워크 장애같은 문제의 소지가 있다. 반면 본 논문에서 제안하는 모델에서는 Leader Agent만이 직접 그리드 서버와 통신을 하므로 트래픽 분산이 되어 Load Balancing이 가능해진다. work agent는 leader agent와 통신을 한다. 따라서 leader agent에게 트래픽 집중의 가능성이 있지만 처음 leader agent를 설정할 시에 이러한 능력을 바탕으로 leader agent를 선정한다. 그러나 트래픽 집중을 해결하기 위해서 그룹을 만드는데 있어서 최소한의 worker agent를 설정한다.

그리드 컴퓨팅 하에서는 자원제공자가 자원제공을 갑자기 중단할 수 있고 네트워크 장애라든지 여러 가지 문제가 일어날 수 있다. 특히 그룹에서 Leader 역할을 맡은 Agent나 CA의 역할을 맡은 Agent가 불시에 꺼졌을 경우 이를 대체하기 위한 수단이 필요하다.

본 제안 모델에서는 이러한 문제점을 풀기 위해 Group의 Leader 꺼졌을 경우 이를 가장 빠르게 감지한 Worker Agent가 그리드 서버에게 보고한다. 보고를 받은 그리드 서버는 새로운 Leader Agent를 선정하고 AA는 자동으로 선정된 Leader Agent의 AC를 갱신하여 발급한다. 반면 Group CA Agent가 꺼졌을 경우는 Path Validation 문제가 발생한다. 이러한 문제점을 해결하기 위해서 처음 CA가 인증서를 발급할 시 Group Agent의 인증서만을 저장하는 것이 아니라 개인키까지 저장을 한다. CA Agent의 개인키를 저장함으로써 CA Agent가 불시에 꺼졌을 경우라도 상위 CA에서 인증서 Path를 형성하여 Worker Agent를 인증할 수 있다. 단 개인키를 서버에 저장하는 방식이 문제의 소지가 있지만 본 논문에서 제안하는 grid computing은 유연한 보안서비스를 제공하는데 그 목적을 두고 있으므로 철저한 서버보안으로 이를 해결한다고 가정한다.

이에 따라 본 논문에서 제안하는 방식은 그리드 서버의 부하를 감소시킴과 네트워크 트래픽을 분산시켜 그리드 컴퓨팅 하에서 발생할 수 있는 보안적인 문제를 유연하게 대처할 수 있다.

VI. 결론

인터넷이 발전하고 모든 작업을 컴퓨터로 사용하고 있는 시대에 들어왔다. 인터넷 사용자의 증가에 따라 컴퓨터 사용 또한 증가하고 있다. 이에 따라 컴퓨터의 남은 자원을 활용하기 위한 연구가 증가하고 있으며 이러한 연구의 핵심은 바로 그리드 컴퓨팅이다. 그리드 컴퓨팅의 연구가 활발해짐에 따라 자원제공자의 Privacy와 통신상에 이동되는 데이터의 기밀성과 무결성이 대두되었다. 이러한 문제점을 해결하기 위해서 본 논문에서는 다음과 같은 세 가지 핵심 기술을 제시하였다. 첫째, 분산환경하에서 플랫폼 독립적인 SOAP 프로토콜을 이용하는 것이다. 둘째, PMI를 이용하여 Agent마다 역할을 준다. 이렇게 함으로써 서버의 부하를 최소한으로 감소시키고 서버에게 집중되는 트래픽을 감소시킬 수 있다. 셋째, Agent를 그룹화하여 그룹에 따라 같은 프로젝트를 수행할 수 있지만 다른 프로젝트 또한 수행할 수 있게 하여 쉽게 다양한 프로젝트 수행을 가능하게 한다.

위의 세 가지 핵심기술을 특징으로 한 그리드 모델은 제안된 새로운 작업 수행 모델을 적용한 Grid Computing은 인터넷 기반 분산 컴퓨팅 환경을 조성하고, 슈퍼컴퓨터 또는 클러스터 시스템의 응용 기술 개발에 도움이 될 것으로 기대한다.

참고문헌

- [1] 이석, "인터넷 컴퓨팅의 생물학 응용 및 BioGrid의 동향", 슈퍼컴퓨팅소식 5권 41-45 페이지 2001년 6월
- [2] <http://globus.org>
- [3] Eric newcomer " Webservice의 이해 " pearson education Korea.
- [4] Andrew Nash and William Duane and Celia Joseph and Derek Brink "PKI:Implementing and Manageing E-security" McGraw-Hill, 2001.
- [5] S. Farrell and R. Housely " An Internet Attribute Certificate Profile for Authentication" RFC 3281, 2002.