그리드 컴퓨팅을 위한 NAT 프락시

김은성*, 박형우*, 이상산*, 정진욱**
*한국과학기술정보연구원 슈퍼컴퓨팅센터
**성균관대학교 정보통신및컴퓨터공학부
e-mail : eskim74@hpcnet.ne.kr

NAT Proxy for Grid Computing

Eun-Sung Kim*, Hyung-Woo Park*, Sang-San Lee*, Jin-Wook Chung**
*Supercomputing Center, Korea Institute of Science & Technology Information
**School of Information Communication & Computer Engineering, Sungkyunkwan University

요 약

그리드란 지리적으로 분산된 컴퓨터, 데이터베이스, 과학장비 등을 초고속 네트워크를 통하여 연결하여 가상의 슈퍼컴퓨터로 활용하고자 하는 노력으로 탄생하였다. 이러한 그리드를 가능하게 하는 소프트웨어 기반 구조로 글로버스 미들웨어가 있다. 본 논문에서는 방화벽으로 구성된 네트워크 환경에서 글로버스를 사용할 때의 여러 가지 문제점들을 고찰하고 기존 해결 방안을 살펴보았다. 또한 기존 방안에서 해결하지 못하는 NAT 방화벽에서의 문제점을 해결하기 위해서 GSI 권한위임 메커니즘을 확장하여 NAT 프락시를 제안하였다. 이 NAT 프락시를 통하여 NAT 방화벽으로 구성된 네트워크 환경에서도 글로버스를 사용할 수 있을 것으로 기대한다.

1. 서론

산업사회가 고도화됨에 따라 필요한 컴퓨터 등 IT 자원의 필요성은 급격히 증가하고 있으나, 한정된 자원으로 인하여 다수의 사용자가 필요한 자원을 충분히 사용하는 것은 매우 제한적으로 이루어지고 있다. 실제적으로 컴퓨팅 자원은 국가적으로 매우 다양하게 분포되어 있으며, 이들의 사용량은 지역별, 연별, 월별, 시간별로 매우 다르게 나타난다. 주로 주간보다 야간에 사용률이 적으며 봄, 가을이 여름, 겨울보다 사용률이 크게 나타난다. 만약 이러한 차이와 사용률을 국가적으로 효율적으로 관리하여 활용한다면 매우 큰 경제적 효과를 얻을 수 있으며, 지역별로 한정된 자원의 한계를 뛰어넘어 대용량, 초고속의 거대문제(Grand Challengeable Problem)에 도전할 수 있게 된다. 더불어 지역 및 국가간 정보화 격차 해소에 크게 기여할 수 있게 될 것이다.

자원의 공유와 공동 활용은 인터넷이 보편화되고 네트워크의 성능이 급격히 향상됨에 따라 가능하게 되었다. 과거에는 동일한 컴퓨팅 자원들을 통합하는 NOW(Network Of Workstations), PC 클러스터링 기술에 노력하여 왔으나, 최근에는 자원 통합에 있어서 동일 기종의 컴퓨터들 뿐만이 아니라 이기종 컴퓨팅 자원들과 대용량 저장 장치, 다양한 고성능 연구 장비들이 포함되고 있다. 이렇게 분산된 자원을 연결해 하나의 시스템처럼 사용하고자 하는 노력을 메타컴퓨팅, 또는 P2P(Peer to Peer) 슈퍼컴퓨팅이나 그리드(GRID)라고 부른다.[1]

그리드 환경은 하이 엔드 기반의 IT(정보기술)로서 과거에는 불가능했던 5T(BT(생명공학 기술), NT(나노기술), ET(환경 기술), ST(항공우주 기술), TT(전통제조산업 기술)) 분야의 거대문제를 해석 가능하게 하였으며, 그 결과를 연구 현장에 적용하여 신기술을 개발하도록 하였다. 이것은 매우 가치 있는 일로서 국가 경쟁력 제고에 큰 영향을 줄 수 있다.

본 논문에서는 그리드 환경을 구축하는 인프라 미들웨어인 글로버스(Globus)를 방화벽으로 구성된 네트워크 환경에서 사용할 때의 문제점들을 고찰하고 이를 해결하기 위한 기존 방안들에 대해서 살펴본다. 또한 기존 방법들이 해결하지 못하고 있는 NAT(Network Address Translation) 방화벽에서 글로버스를 사용하기 위한 메커니즘을 제시하고자 한다.

2. 그리드와 글로버스 프로젝트

그리드란 여러 조직에 의해서 소유되고 관리되는

하이 엔드 컴퓨터, 네트워크, 데이터베이스와 과학 장비의 통합적이고 협력적인 사용을 가능하게 하는 기반 구조를 말한다. 그리드 환경에서 사용되는 그리드 어플리케이션으로는 다음과 같은 것들이 있다.[1][10]

- 분산 슈퍼컴퓨팅(*distributed supercomputing*)
- 지능형 과학장비(smart instruments)
- 데스크탑 슈퍼컴퓨팅(desktop supercomputing)
- 원격 가상몰입(teleimmersion)

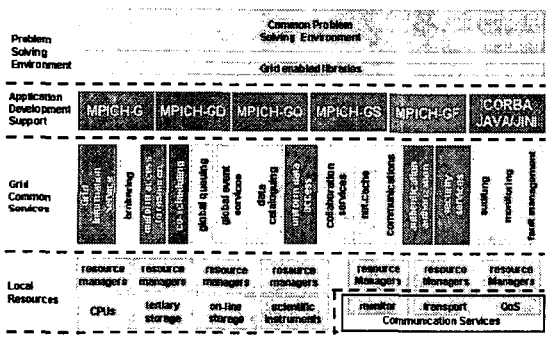
이러한 어플리케이션들은 자주 많은 양의 데이터와 컴퓨팅을 요구하고 조직간의 안전한 자원 공유를 요구하기 때문에 현재의 인터넷과 웹 기반 구조로는 쉽게 처리될 수 없다. 따라서 이를 지원하기 위한 새로운 소프트웨어 기반 구조가 요구된다.

글로버스 프로젝트는 과학 기술 분야의 컴퓨팅에 그리드 개념의 어플리케이션이 가능하도록 하는데 초점을 둔 연구 개발 프로젝트이다. 이 프로젝트는, 웹이 사람들에게 정보에 대해 생각하는 방법을 변화시켰듯이 사람들이 계산(computation)에 대해 생각하는 방법을 변화시키려 하고 있다.[4][10]

글로버스 메타컴퓨팅 툴킷은 글로버스 프로젝트의 결과물의 일환으로서 그리드 환경과 그리드 기반 어플리케이션을 구현하는 것을 용이하게 해주는 미들웨어 소프트웨어이다. 이 시스템은 글로벌 컴퓨팅 환경을 위한 소프트웨어 기반 구조를 구성하기 위해서 통신, 자원 배치, 자원 스케줄링, 인증, 네트워크 정보, 데이터 액세스와 같은 기본 메커니즘을 제공한다. 또한 글로버스 메타컴퓨팅 툴킷은 다음과 같은 영역의 문제를 해결하기 위한 툴들과 라이브러리들을 포함하고 있다.

- 보안(Security)
- 통신(Communication)
- 정보 기반 구조(Information Infrastructure)
- 장애 검출(Fault Detection)
- 자원 관리(Resource Management)
- 이식성(Portability)
- 데이터 관리(Data Management)

다음 <그림 1>은 글로버스 메타컴퓨팅 툴킷의 구조를 보여준다.



<그림 1> 글로버스 메타컴퓨팅 툴킷의 구조

글로버스 메타컴퓨팅 툴킷은 오픈 아키텍처, 오픈 소스 소프트웨어 툴킷이다. 따라서 많은 프로젝트와 개발자들이 이 툴킷의 개발에 참여하고 있다.

3. 그리드 환경에서의 방화벽

글로버스 메타컴퓨팅 툴킷은 앞에서 설명한 바와 같이 그리드 환경을 구성하기 위한 다양한 기본 메커니즘을 제공하고 있다. 이 툴킷에서 사용되는 통신 메커니즘은 globus I/O 와 넥서스 통신 라이브러리에 의해서 제공된다. globus I/O 는 어플리케이션 프로그래머들에게 보안, 비동기 통신, QoS 를 지원하는 TCP, UDP, IP multicast, 파일 I/O 서비스를 제공하며 넥서스는 다양한 통신 프로토콜과 특성에 대해 단일한 API 를 제공하는 멀티메소드(multimethod) 통신을 지원한다. 하지만 이 모듈들은 표준 TCP 통신 메커니즘을 이용하기 때문에 글로버스 메타컴퓨팅 툴킷은 다음과 같은 문제점들을 가진다.[3]

① 방화벽 문제 : 글로버스 서버는 방화벽을 통해서 이용될 수 없다
② 사설 IP 문제 : 사설 IP 를 가지는 컴퓨팅 서버는 이 사설 IP 를 인식할 수 없는 다른 서버와 통신할 수 없다.

현재 이를 해결하기 위한 다양한 노력들이 진행되고 있으며 이를 구체적으로 살펴보면 다음과 같다.

첫번째로 글로버스 메타컴퓨팅 툴킷을 개발하고 있는 팀에서는 방화벽 문제를 해결하기 위해서 컴퓨팅 서버가 방화벽 내에 있을 때 [표 1]과 같은 포트를 열어둘 것을 권고하고 있다.[12]

[표 1] 글로버스 네트워크 포트

어플리케이션	글로버스 버전	네트워크 포트
Gatekeeper	1.1.3 and later	2119/tcp
GRIS	1.1.3 and later	2135/tcp, 2135/udp
GIIS	1.1.3 and later	Site-selected
GridFTP	All	2811/tcp(control)
GSI-enabled SSH	All	22/tcp
MyProxy	All	7512/tcp

[표 1]에 있는 모든 TCP 포트는 사용자 영역(>1024) 위에 리턴 연결을 가지기 때문에 이에 대한 포트도 추가적으로 열어주어야 한다. 하지만 globus I/O, GridFTP 데이터 채널과 넥서스 모두 이를 동적으로 생성해주기 때문에 방화벽에 적절한 포트를 열어줄 수가 없다. 이러한 문제를 해결하기 위해서 글로버스 팀에서는 *GLOBUS_TCP_PORT_RANGE* <*min,max*> 환경 변수를 사용하도록 하고 있다. 이 환경 변수를 설정해 놓으면 globus I/O, GridFTP 데이터 채널과 넥서스 모두 이 포트 범위 안에서 리턴 연결을 생성한다. 따라서 방화벽 관리자는 추가적으로 이 범위의 포트를 열어놓으면 된다. 이러한 해결책은 일반적인 방화벽에서는 잘 동작하지만 NAT 방화벽을 이용하는 경우에는 상호 인증 문제로 잘 동작하지 않는다.[2][12]

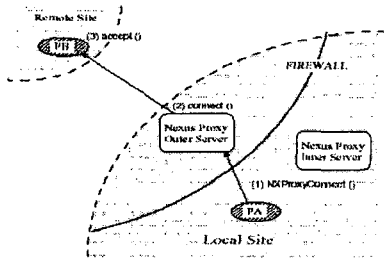
두 번째로 넥서스 프락시(Nexus Proxy)를 이용하는

것이다. 이 넥서스 프락시는 SOCKS 와 유사한 구조를 가지며 방화벽 문제와 사설 IP 문제를 해결하기 위해서 TCP 통신을 중계하는 기능을 제공한다. 즉, 넥서스 프락시 서버는 방화벽 밖에서 실행되고 미리 방화벽을 통과하도록 허락된 포트를 통하여 클라이언트의 요청을 받아서 이를 중계해준다. 이러한 기능을 제공하기 위해서 넥서스 프락시는 [표 2]와 같은 함수들을 정의한다.[3]

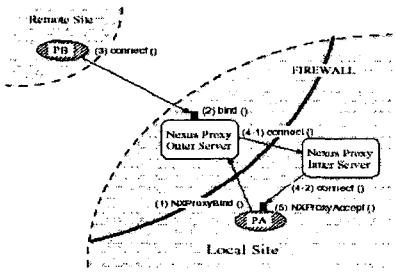
[표 2] 넥서스 프락시 라이브러리 함수

함수	설명
NXProxyConnect()	넥서스 프락시 외부 서버로 연결 요청을 보내고 클라이언트가 목적지 프로세스와 통신할 수 있는 파일 지시자를 반환한다.
NXProxyBind()	넥서스 프락시 외부 서버로 바인드 요청을 보내고 클라이언트가 요청을 감시할 수 있는 파일 지시자를 반환한다.
NXProxyAccept()	연결 요청을 수신한다.

<그림 2>와 <그림 3>은 넥서스 프락시의 통신 메커니즘을 보여준다.



<그림 2> 넥서스 프락시(active connection)



<그림 3> 넥서스 프락시(passive connection)

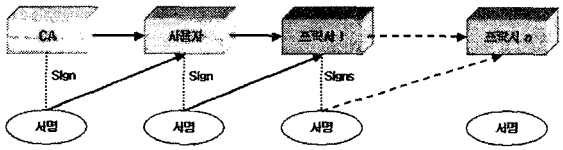
이와 같은 넥서스 프락시는 방화벽 문제와 사설 IP 문제는 해결할 수 있지만 아직 완벽한 구현이 이루어지지 않아서 직접 현장에서 사용하기에는 어려움이 많다. 또한 넥서스 프락시도 NAT 방화벽을 지원하지 못하고 있다.

4. 그리드를 위한 NAT 지원 메커니즘

NAT 방화벽 뒤에서 글로버스 서비스를 설정하려 할 때의 문제점은 컴퓨팅 노드의 게이트키퍼 인증서에 사용되는 이름이 방화벽의 이름과 같지 않다는 것이다. NAT 는 자신이 보호하는 네트워크 내의 호스트의 IP 를 외부에 감춘다. 따라서 이 NAT 방화벽 내에 있는 컴퓨팅 노드에 연결하려고 하는 클라이언트는 실제 컴퓨팅 노드의 IP 에 연결하는 것이 아니라 NAT 방화벽의 IP 로 연결하게 된다. 이러한 상황에서 클라이언트가 자신이 연결하려고 하는 IP 의 리버스 룩업(reverse lookup)을 통해서 얻은 이름과 게이트키퍼의 인증서에 있는 이름이 동일할 것을 요구하기 때문에 상호 인증 에러가 발생하게 되어서 통신이 이루어지지 않게 된다. 이 때 게이트키퍼의 인증서에 NAT 방화벽의 이름을 넣으면 외부 사용자는 글로버스 서비스를 이용할 수 있게 된다. 하지만 이러한 경우 내부 사용자는 상호 인증 에러로 글로버스 서비스를 이용할 수 없게 된다.[11]

위에서 설명한 문제를 해결하기 위해서 본 논문에서는 GSI(Grid Security Infrastructure)의 권한위임(delegation) 메커니즘의 확장을 통한 NAT 프락시로 NAT 방화벽 문제를 해결하고자 한다.

GSI 의 권한위임 메커니즘은 사용자가 자신을 인증하기 위하여 패스워드를 입력하는 횟수를 줄이기 위한 것이다. 즉, 사용자를 대신하는 프락시라는 것을 생성하여 여러 개의 자원에 대한 요구가 있을 때 사용자가 자신을 인증하기 위하여 여러 번 패스워드를 입력하는 것을 피하게 한다. 사용자가 프락시를 생성하면 프락시는 새로운 공개키를 포함하는 새로운 인증서와 새로운 비밀키를 가진다. 즉, 자신을 구별할 수 있는 새로운 서브젝트 네임(subject name)을 가지게 된다. 새로운 인증서는 소유자의 신원을 포함하며 그것이 프락시의 것이라는 것을 표현하기 위해 약간 수정된다. 이 새로운 인증서는 CA(Certification Authority)가 아니라 사용자에 의해서 인증된다. 또한 이 인증서는 자신이 유효한 시간값을 가진다. <그림 4>는 이러한 권한위임 과정을 나타낸다.



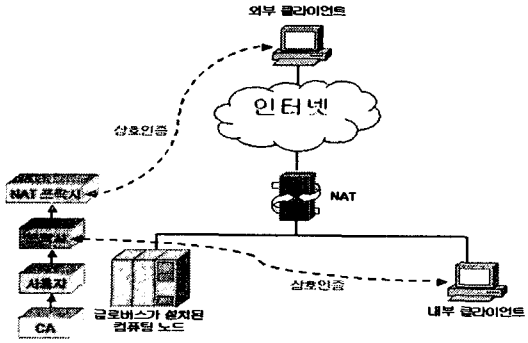
<그림 4> 권한위임 과정

프락시가 생성되면 사용자는 패스워드를 입력하는 것 없이 상호 인증을 위해서 프락시의 인증서와 비밀키를 사용할 수 있다.

프락시가 사용될 때의 상호 인증 프로세스는 약간 다르다. 인증을 수행하는 곳에서는 프락시의 인증서 뿐만 아니라 소유자의 인증서도 받는다. 상호 인증을 하는 동안 소유자의 공개키는 프락시의 인증서에 있는 서명을 검증하기 위해서 사용되고 CA 의 공개키는 소유자의 인증서에 있는 서명을 검증하기 위해서 사용된다. 이러한 과정은 소유자를 통해서, CA 로부터 프락시까지 신뢰 사슬을 생성하게 한다. 따라서 상호 인증에 성공하게 된다[12].

이러한 메커니즘을 이용하여 본 논문에서는 NAT

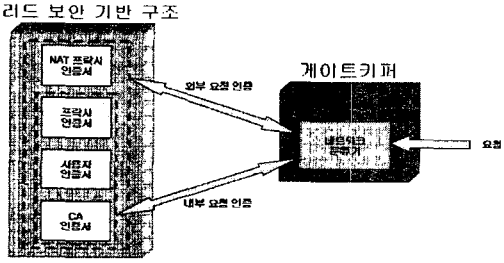
프락시를 제안한다. <그림 5>는 NAT 프락시 메커니즘을 보여준다.



<그림 5> NAT 프락시

NAT 프락시는 사용자가 생성한 프락시가 생성하는 프락시이다. 이 프락시의 서브젝트 네임은 NAT 방화벽의 이름이다. 즉, 이 NAT 프락시가 NAT 방화벽의 이름을 가지고 있기 때문에 앞에서 설명한 상호 인증 문제를 해결할 수 있다. 이러한 프락시를 도입함으로써 NAT 방화벽 외부에 있는 클라이언트와 NAT 방화벽 내부에 있는 컴퓨팅 노드간의 상호 인증이 이루어지게 된다. 결국 사용자가 생성한 프락시는 내부 네트워크의 인증을 위해서 사용되고 이 프락시가 생성한 NAT 프락시는 외부 네트워크의 인증을 위해서 사용된다.

NAT 프락시의 생성은 이미 프락시의 권한위임 메커니즘이 규정되어 있기 때문에 수월하게 구현될 수 있을 것이다. 하지만 외부 네트워크 트래픽과 내부 네트워크 트래픽을 구별하는 것은 현재 글로버스에 구현되어 있지 않으므로 외부 네트워크 트래픽은 NAT 프락시로 연결해주고 내부 네트워크 트래픽은 사용자가 생성한 프락시로 연결해주는 메커니즘(네트워크 분류기)이 게이트키퍼에 추가되어야 한다. <그림 6>은 이러한 메커니즘을 나타낸다.



<그림 6> NAT 지원을 위한 게이트키퍼 확장

본 논문에서 제안한 NAT 프락시 메커니즘을 통해서 NAT 기반 방화벽에서도 글로버스를 이용한 그리드 환경을 구축할 수 있을 것으로 기대된다.

5. 결론

메타컴퓨터 혹은 메타컴퓨팅이라는 이름으로도 불리는 그리드는 네트워크를 통해서 서로 연결된 컴퓨팅 자원을 사용자가 개인용 컴퓨터를 이용하듯이 사용할 수 있도록 하자는 개념에서 출발했다. 다시 말해 그리드는 네트워크로 연결된 가상의 슈퍼컴퓨터를 말하는 것이다. 이와 같은 그리드는 현재 협업 업무에서부터, 컴퓨터를 이용한 정밀 실험, 원격 데이터세트의 검색, 원격 소프트웨어의 사용, 데이터 중심의 컴퓨팅, 대형 시뮬레이션, 무수한 변수가 사용되는 연구 등에 사용할 수 있을 것으로 기대되고 있으며, 이미 많은 프로젝트가 시작된 상태다.[13]

본 논문에서는 이러한 그리드를 구축하는데 핵심적인 요소인 글로버스 미들웨어에 대해서 살펴보고 이를 방화벽으로 구성된 네트워크 환경에서 사용할 때의 여러 가지 문제점들을 고찰하고 해결 방안들을 살펴보았다. 그리고 현재 NAT 방화벽을 지원하지 못하는 그리드 환경을 위해 GSI 의 권한위임 메커니즘을 확장하여 NAT 프락시를 제안하였다.

향후 과제로는 제안된 NAT 프락시의 실제 구현을 통해서 이의 효용성을 테스트하고 이를 더욱 개선하기 위한 방안을 연구하고자 한다.

참고문헌

[1] I. Foster, C. Kesselman, S. Tuecke. "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International J. Supercomputer Applications, 15(3), 2001.

[2] M. Baker, H. Ong and G. Smith, "A Report on Experiences operating the Globus Toolkit through a Firewall", University of Portsmouth, 2001.

[3] Y. Tanaka, M. Hirano, M. Sato, H. Nakada, and S. Sekiguchi, "Resource Manager for Globus-based Wide-area Cluster Computing", 1st IEEE International Workshop on Cluster Computing (IWCC'99), pp.237-244, 1999.

[4] I. Foster, C. Kesselman, "Globus: A Metacomputing Infrastructure Toolkit", Intl J. Supercomputer Applications, 11(2):115-128, 1997.

[5] I. Foster, J. Geisler, W. Nickless, W. Smith, S. Tuecke, "Software Infrastructure for the I-WAY High Performance Distributed Computing Experiment", Proc. 5th IEEE Symposium on High Performance Distributed Computing, pp. 562-571, 1997.

[6] R. Butler, D. Engert, I. Foster, C. Kesselman, S. Tuecke, J. Volmer, V. Welch. "A National-Scale Authentication Infrastructure", IEEE Computer, 33(12):60-66, 2000.

[7] I. Foster, C. Kesselman, G. Tsudik, S. Tuecke, "A Security Architecture for Computational Grids", Proc. 5th ACM Conference on Computer and Communications Security Conference, pp.83-92, 1998.

[8] I. Foster, N. T. Karonis, C. Kesselman, S. Tuecke, "Managing Security in High-Performance Distributed Computing", Cluster Computing, 1(1):95-107, 1998.

[9] K. Czajkowski, I. Foster, N. Karonis, C. Kesselman, S. Martin, W. Smith, S. Tuecke, "A Resource Management Architecture for Metacomputing Systems", Proc. IPPS/SPDP '98 Workshop on Job Scheduling Strategies for Parallel Processing, pp.62-82, 1998.

[10] http://www.globus.org/

[11] http://www.globus.org/security/overview.html

[12] http://www.globus.org/security/v1.1/firewalls.html

[13] http://www.zdnet.co.kr