선행적 인증 정보 서비스에 기반한 그리드 보안 시스템

권영도**, 서명구*, 장경일*, 남성진*, 박규석***
경남대학교 컴퓨터공학과

A GRID Security System based on Proactive Authentification Information Service

Myung Goo Seo, Kyung Il Jang, Sung Jin Nam,
Young Do Kweon, Kyoo Seok Park
Dept. of Computer Engineering, KyungNam University

요 약

지리적으로 분산되어 있는 이기종의 분산 컴퓨팅 자원과 대규모 데이터를 효과적으로 활용하기 위해서 최근에 GRID 컴퓨팅 환경에 대한 연구가 매우 활성화되고 있다. 이러한 GRID 환경을 구현하기위해 필요한 부분중의 하나가 사용자와 자원간의 인증에 관련된 문제이다. 현재 Globus Toolkit은 PKI(Public Key Infrastructure)를 기본으로 하는 보안정책을 사용하고 있다. 이 정책은 인증과정에 적지않은 오버헤드가 발생되는 문제점을 가지고 있다. 이에 본 논문에서는 사용자와 자원간의 직접적인 인증으로 인해 발생하는 성능상의 비효율성을 줄이기 위해 사용자가 자원에 접속하기전 AIS서버(Authentification Information Server)를 이용하여 미리 인증을 거친후, 자원에 접근할 때는 기 발급된 식별자로 인증 될 수 있도록 처리해주는 메커니즘을 제안한다.

중심어 : 그리드(Grid), 글로버스 툴킷(Globus Toolkit), 인증(Authentication)

1. 서론

인터넷이 보편화되고 컴퓨터 및 네트워크의 성능이 향상되면서 각 분야별로 컴퓨터를 이용하는 양상이 변하고 있다. 그와 동시에 WWW(World Wide Web)의 출현과 엄청난 성공에 힘입어 지금까지는 연구 분야로만 있었던 컴퓨팅 파워의 공유뿐만아니라 나아가 네트워크로 연결될 수 있는 모든 것을 공유하고자 하는 노력이 진행되고 있다. 이런 노력은 단순히 로컬(local) 자원의 공유가 아닌 광대역 통신망을 활용한 공유로 확대되어 동일 기종 컴퓨터뿐 아니라 이기종 컴퓨팅 자원과 대용량 저장장치, 다양한 고성능 연구장비가 포함되는 통합 환경을 이루게 되었으며, 이것을 GRID(그리드)라고 한다[1]. GRID는 사용자가 어떤 큰 문제를 해결하고자 할 때, 마치 단일 시스템을 쓰듯이 전 세계에 펼쳐져 있는 자원들을 사용할 수 있도록 해준다. 이 사항이 이루어지기 위해서는 필수적으로 자원의 이질성이나 보안 문제, 자원 상태를 관리 및 제어하기 위한 미들웨어를 필요로 한다. 현 시점에서 Globus Toolkit[3]은 이러한 기능을 수행해주는 가장 보편적으로 사용되고 있는 GRID 미들웨어로서 기존의 시스템이나 네트워크 정책과 강력한 호환성을 가진다[2]. 하지만 현재 GRID는 완전히 그 틀이 정립되어 있는 상태가 아니므로 그에 따른 GRID 미들웨어도 그 기능이 완벽히 구현되지 않았다[3]. 이에 본 논문에서는 GRID 미들웨어 중 하나인 Globus Toolkit의 사용자 인증 부분에서 발생할 수 있는 성능상의 문제점과 해결 방안을 제안한다. 본 논문의 구성은 다음과 같다. 2절에서는 관련 연구를 기술하고, 3절에서 Globus Toolkit 상에서 제공되는 보안과 인증에 관련된 사항을 설명하며, 4절에서는 AIS 서버를 추가한 Globus 인증 메커니즘을 제안한다. 그리고 마지막으로 5절에서는 결론 및 향후 과제에 대하여 기술한다.

2. 관련연구

2.1 GRID Middleware

미들웨어는 사용 가능 자원을 사용자에게 하나의 시스템처럼 보이도록 하여야 한다. GRID 미들웨어는 프로세스 관리, 자원들의 동시 사용, 저장장치의 접근, 정보 보안, 사용자 인증, 네트워크 QoS, 자원예약 등의 서비스를 제공한다. 현재 진행되고 있는 미들웨어

관련 프로젝트는 Globus[4], Legion[5], Condor[6], Cactus[7]등이 있다. Globus는 GRID 서비스를 위한 하나의 독립적인 서비스 요소들로 구성되어 있다.

Legion은 다양한 컴퓨팅 자원과 네트워크를 연결해 단일 시스템과 같은 모양을 내는 객체 지향 메타시스템이며, Condor는 분산된 워크스테이션을 통합해 사용할 수 있게 하는 고처리율(High-throughput) 컴퓨팅 환경이다. 또한, Cactus는 GRID 환경에서 과학기술 분야 연구를 위한 문제 해결 환경으로 구조가 모듈화된 미들웨어이다. 이런 GRID 미들웨어의 개발을 위해서는 다양한 이기종 컴퓨팅 자원 이용에 따른 정보의 호환성 문제, 자원 관리의 어려움, 애플리케이션 개발의 어려움, 시스템 개발시 통합의 어려움 등의 문제점이 존재한다. 이를 해결하기 위해 GRID 미들웨어의 표준화가 진행되고 있다.[1]

2.2 RSL(Resource Specification Language)

RSL은 Globus상에서 전달되는 자원 명세(Resource requirements)와 작업 환경(Job configuration)을 표현하는 언어이다[10]. 자원 명세에는 자원의 타입, 필요 노드 개수, 메모리 등이 포함되고 작업 환경에는 실행 프로그램의 이름과 위치, 인수, 환경 변수 등이 포함된다.

2.3 광역 자원 관리자(DUROC, Dynamically-Updated Request Online Co-Allocator)

DUROC은 세분화된 RSL(Multi-request RSL)을 파싱해 각 세부 작업단위로 나눠 분배하고 작업이 동시에 실행되도록 하는 기능과 각 세부작업을 모니터링하고 그 결과를 취합하는 기능을 제공하는 Agent이다[1].

3. Globus Toolkit

3.1 Globus Toolkit의 구성

Globus Toolkit은 미국 ANL(Argonne National Lab.)에서 개발한 그리드 미들웨어이다[3]. 현재 Globus Toolkit이 보편적으로 사용되고 있는 이유는 GRID에서 필요로 하는 다양한 서비스를 분리될 수 없는 단일 시스템이 아닌 독립적인 요소로서 제안하며 기존에 각 시스템 및 네트워크의 관리 정책이나 운영 도구들을 무시하지 않고 각 요소들과 협력해 GRID를 구축해 나가기 때문이다. 이 Globus Toolkit은 크게 4가지 부분으로 나눌 수 있다[4].

1. GSI(Grid Security Infrastructure)
   Globus의 보안을 담당하는 부분으로써 PKI와 SSL에 기반을 두고 있으며 Single Sign-on 기능을 지원한다.
2. MDS(Metacomputing Directory Service)
   각 자원의 정보를 수집하는 GRIS(Grid Resource Information Service)서버와 수집된 자원의 정보를 통합하는 GIIS(Grid Index Information Service)서버에서 수집해 제공하는 정보를 저장하고 서비스하는 저장소의 기능을 수행한다.
3. GASS(Globus Access to Secondary Storage)
   Execution Node상에 있는 파일의 처리나 접근, 데이터의 분산 저장을 담당한다.
4. GRAM(Grid Resource Allocation Management)
   client의 접근에 대한 인증과 Execution Node상의 자원의 할당과 관리를 담당한다. Gatekeeper와 Job Manager로 구성된다.

그림 1은 Globus Toolkit의 자원 관리 아키텍처를 보여 주고 있다.

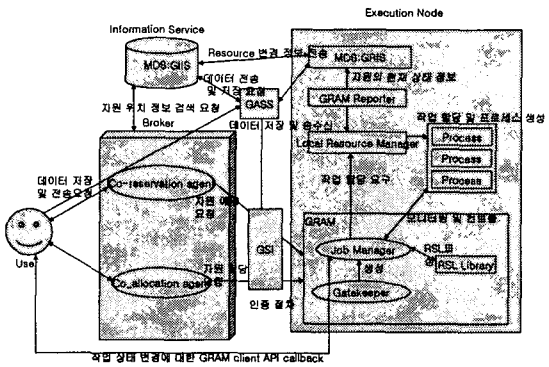

그림 1. Globus Toolkit 자원 관리 아키텍처

3.2 Globus Toolkit의 보안과 인증

현재 Globus Toolkit 상의 보안은 PKI(Public Key Infrastructure)와 SSL(Secure Socket Layer) 프로토콜을 이용해 구현된 GSI가 담당하고 있다[8]. GSI의 가장 두드러진 기능은 단일 인증 기능(Single Sign-On)과 권한 위임(delegation)이다. 단일 인증 기능은 Client에서 Execution Node상의 자원을 사용하기 위해 거쳐야 하는 인증단계를 한번의 인증으로 간소화한 기능이다. 위의 단일 인증 기능이 제공하는 보안 서비스로는 인증(Authentication), 허가(Authorization), 계정관리(Accounting), 부인방지(Audit), 무결성(Integrity)등이 있다[9]. 권한 위임은 Execution Node상에 전달된 작업 처리를 위한 자원이 부족할 때 다른 Execution Node의 자원을 요청할

수 있도록 하는 절차를 작업 요청자의 또 다른 인증 과정을 거치지 않고 기존에 가지고 있던 인증을 통해서 진행될 수 있도록 하는 기능이다. 이 과정은 그림 2에 나타나 있다[11].

① 우선 사용자는 자신의 키와 인증서를 이용하여 사용자 프록시(user proxy)를 만들고 이를 이용하여 자원에 접근하게 된다.
② 프록시와 원격지의 GRAM과의 인정 과정을 거치면 process를 사용할 수 있게 되고 작업을 진행할 수 있게 된다.
③ 만일 site1의 자원만으로 작업이 진행되기 어려우면 사용자에게 site2의 자원 사용 인증을 요청하지 않고 사용자 프록시로부터 받은 인증 자료를 통해서 위임받은 권한으로 site1의 process는 site2의 인증을 통과하게 된다.
④ site2의 GRAM을 통해 다시 필요한 작업에 대한 process를 생성하여 작업을 완수할 수 있게 된다.

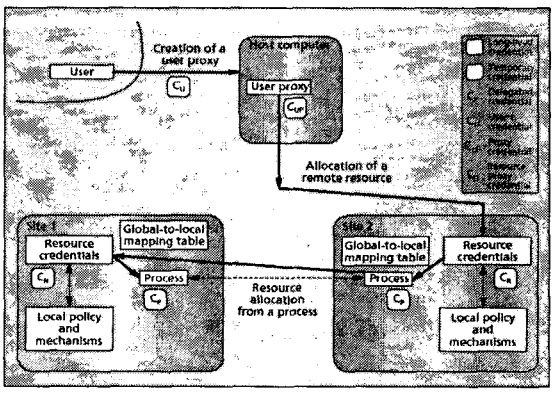

그림 2. GSI의 사용자 인증과 권한의 위임 과정

Globus에서 사용자가 컴퓨팅 자원에 대한 요청을 수행할 때 사용자와 계산 자원 사이에 상호 인증(Mutual authentication)이 일어난다[9]. 상호 인증을 위해 사용자와 Execution Node상에는 몇 가지 인증서가 존재한다. Gatekeeper 인증서, 사용자 인증서, 사용자 Proxy 인증서, 프로세스 인증서가 그 것이다[11].

3.3 Globus Toolkit상의 문제점

현재 GSI를 이용한 인증방법은 자원 사용자가 각각의 Execution Node에 접근할 때 마다 인증을 받아야 할당된 자원을 사용할 수 있게 되어 있다. 이런 과정을 거치면서 자원 사용자가 자원을 필요한 자원을 획득하는 과정에 많은 시간을 소요하게 되므로 비효율적이며. 그에 대한 측정값은 표1과 같다[13].

표 1은 GIS에서 자원을 가진 Node를 검색하여 작업을 진행하기까지의 각 진행 상태마다 소비되는 시간을 측정한 자료이다. DUROC에서 하나의 Execution Node상의 GRAM에 인증을 거치는 과정에 드는 비용이 0.5초로 나와있다. 만일 한 작업을 처리하는데 필요한 Node가 늘어나면 늘어날수록 인증에 소비되는 비용이 엄청나게 늘어나게 될 것이다.

4. 제안 메카니즘

본 논문에서는 현재 사용되고 있는 자원 사용자와 GRAM간의 인증 절차를 거치지 않고 인증에 대한 정보를 별도로 관리하는 AIS(Authentication Information Server)를 두어 자원을 가진 Node를 검색할 시에 그에 대한 인증까지 될 수 있도록 하는 방법을 제안한다.

4.1 AIS의 구성

AIS는 기본적으로 두 가지 서비스, GAIS(Grid Authentication Information Service)와 GAIIS(Grid Authentication Index Information Service)로 나뉜다. GAIIS는 AIS서버상에 존재하면서 각 자원에 대한 인증 권한 ID를 저장한다. GAIS는 각 Execution Node상에 존재하면서 자원에 대한 인증 권한 ID를 GAIIS에게 수시로 변경시켜 전송한다.

4.2 RSL의 확장

기존의 RSL field에는 인증 관련사항이 포함되어 있지 않다. 본 논문에서는 AIS에서 받아온 각 자원에 대한 인증과 관련하여 Gramid, Brokerid, Authid Field를 RSL에 추가한다. Gramid는 자원이 위치한 Gram의 식별자를 나타내며, Brokerid는 자원이 위치한 Broker 식별자를 나타내고, Authid는 GRAM에 인증을 거치지 않고 통과하기 위해 필요한 식별자이다. 이에 대한 형태는 다음과 같이 표현된다.

표 1. 자원 할당에 대한 성능 테스트 결과

operation	latency(s)
initgroups()	0.7
authentication	0.5
misc.	0.01
fork()	0.001

사용자로부터 전송된 RSL 문서 내용.

```
....
&(count=5)(executable=myprog)
....
```

Broker를 통과하여 세분화된 RSL 문서 내용.

```
.....
+(&(Gramid=#GI1)(count=3)(executable=myprog)
    (Brokerid=#BI1)(Authid=sn200110))
 (&(Gramid=#GI2)(count=2)(executable=myprog)
    (Brokerid=#BI1)(Authid=sn211012))
.....
```

4.3 Globus 사용자 인증 과정

본 논문에서 제안한 개선된 사용자 인증 시스템의 구성도는 그림 3과 같으며 다음과 같이 진행된다.

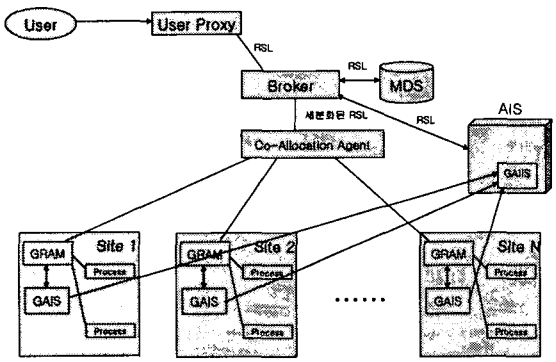

그림 3. 인증 진행 구성도

① 사용자와 Broker간의 인증이 이루어지면 Broker는 MDS에 사용자가 요청한 작업을 위한 자원들의 위치 정보 검색을 요청한다.

② 검색된 자원의 위치 정보가 Broker에게 전송된다.

③ Broker는 전송받은 자원의 위치 정보를 사용해서 AIS서버에 그 자원에 대한 인증 정보를 요청한다.

④ AIS서버는 요청에 대한 자원을 검색해서 그 자원에 해당하는 각 인증을 위한 정보를 Broker에게 전송한다.

⑤ Broker는 MDS와 AIS로부터 전송받은 정보들을 세분화된 RSL로 구성한다.

⑥ Co-Allocation Agent에 의해 각 Site별로 작업은 분할하여 전송한다.

⑦ 보안을 위하여 확장된 RSL정보를 GRAM의 Gatekeeper가 전송받아 인증절차 수행여부를 결정한다.

5. 결론 및 향후 과제

GRID는 지리적으로 분산된 자원을 네트워크로 연결된 사용자가 마치 단일 컴퓨터처럼 자원과 데이터를 공유하여 사용할 수 있도록 구성되어진 환경이다. 이를 위해서는 사용자와 자원간의 다양한 보안 요구사항이 필요하게 된다. 그러나, 현재 이러한 요구사항을 만족할 만한 메커니즘이 제안되지 않았기 때문에 현재 표준으로 제정되어 운영되고 있는 기술을 바탕으로 이들을 통합하고 새로운 프로토콜을 확장하고 그리드 보안 요구사항을 만족하도록 구성하고 있다. 본 논문에서는 기존의 인증 방법에 대한 성능 관련 문제점을 분석하고 그의 보완을 위해 AIS 서버와 RSL의 확장을 그 해결방안으로 제시하였다.

추후 본 논문에서 제시한 AIS 서버의 구현과 RSL Field의 확장에 관한 설계 및 구현이 요구된다.

[참고 문헌]

[1] 월간 마이크로 소프트웨어 2002. 7

[2] Ian Foster, Carl Kesselman, Steven Tuecke , "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", International J. Supercomputer Applications, 15(3), 2001.

[3] Grid Service Requirements, http://www.epcc.ed . ac.uk/enacts/gridservice.pdf

[4] Globus Project, http://www.globus.org

[5] Legion Project, http://www.cs.virginia.edu/~legio n

[6] Condor Project, http://www.cs.wisc.edu/co ndor

[7] Cactus, http://www.cactuscode.org

[8] Grid Security Infrastructure, http://www.globu s.org/Security

[9] Ian Foster, Carl Kesselman, Gene Tsudik, Steven Tuecke, "A Security Architecture for Computional Grids", http://www.globus.org/research/papers.html

[1 0] http://www-fp.globus.org/gram/gram_rsl_param eters.html

[11] Grid Security infrastricture(KISTI 슈퍼컴퓨팅 센터 슈퍼컴퓨팅 연구실), http://testbed.gridcenter . or.kr/seminar/seminar2/sangwan.ppt

[12] P. D. Coddington, L. Lu, D. Webb, A. L. Wendlborn, "Extensible Job Managers for Grid Computin

g",
http://www.globus.org/research/papers.html
[13] CHAPTER-6 Resource Co-Allocation in Comp
utational Grids,
http://vega.icu.ac.kr/~highnet/gmc /g
mc.html