LDAP 인증을 이용한 그리드 네트워크 관리 시스템의 설계

노 민 기*, 하 지 아**, 안 성 진***,
* 한국과학기술정보연구원
** 성균관대학교 정보통신공학부, *** 성균관대학교 컴퓨터공학과,

요 약

그리드는 지리적으로 흩어져 있는 이종의 자원들을 고속 네트워크로 연결하여 협업하기 위한 기반구조이다. 그리드 응용의 수행되기 위해서는 먼저 네트워크의 안정성과 신뢰성이 보장되어야 함으로 네트워크 자원들은 관리되어야 한다. GMA는 대규모 분산된 자원의 모니터링을 위한 효과적인 구조를 제안한다. 본 논문에서는 GMA를 기반으로 실제적이고 전체적인 네트워크 관리를 위한 웹 기반 그리드 네트워크 관리 시스템을 설계하였다. 그리드 네트워크 관리 시스템은 여러 분산된 관리 시스템을 스스로 유지시키면서 연결할 수 있어야 한다. LDAP 인증을 이용하여 시스템 접근에 대해 관리자 인증을 수행하여 그리드 네트워크 관리 시스템의 안정성을 보장한다.

Design of Grid Network Management System using LDAP Authentication

Noh Minki*, Ha Jia**, Ahn Seongjin***,

ABSTRACT

Grid is a infrastructure to connect heterogeneous resources that are scattered over areas with high-speed network and to cooperate with each other. To carry out Grid application, first, network resources should be managed, since the network has to be safe and reliable. GMA suggests an effective architecture for monitoring of resources that are scattered over a wide area. In this paper, basing on GMA, Grid network management system based on web for practical and general network management is designed. Grid network management system has to operate and connect various distributed management system. Using LDAP authentication , as one access system , Grid network management system maintain stability.

1. 서 론

그리드는 분산된 고성능 컴퓨터와 대용량 DB 및 첨단 장비 등의 정보통신자원을 고속 네트워크로 연동하여 상호공유하고 이용할 수 있게 한다.[1] 그리드를 관리하기 위해서는 인프라로 제공되는 초고속네트워크 관리 시스템이 필요하다. 본 논문은 그리드 네트워크의 자원의 상호 운용을 위한 대규모의 분산된 관리 정보를 수집하고 사용할 수 있는 관리 구조인 GGF의 GMA모델을 연구하여 대규모 네트워크의 통합 관리와 효과적인 확장을 가능하게 하는 시스템을 설계하였다.[2] 또한 그리드 네트워크의 구성요소를 가시화하고 대규모의 상이한 자원의 관리를 한 곳에서 가능하게 하는 상황판을 제공하여 모니터링을 통한 성능 및 장애 관리가 가능한 시스템을 설계하였다. 시스템의 구조는 GMA모델에 따라 생산자(Producer)와 소비자(Consumer)로 구성되고, 전체 네트워크의 자원 정보 관리를 위한 디렉토리 서비스를 사용한다. 디렉토리서비스로는 LDAP을 사용한다. 여러 생산자는 해당 네트워크의 관리 정보 제공처로 디렉토리 서비스에 발행하고 자신의 지역 데이터베이스를 이용하여 정보 저장을 수행한다. 소비자는 디렉토리 서비스를 이용하여 그리드 네트워크 생산자들과 자원에 대한 검색으로 연결하여 총체적인 관리를 가능하게 한다.

LDAP은 분산 컴퓨팅 환경에서 유지, 보수가 용이한 분산 디렉토리 서비스의 구축을 가능하게 한다. 인터넷 통신 표준 프로토콜인 TCP/IP 스텍 상에서 동작하므로 향후 인터넷 환경에서 가장 적합한 구조를 갖는 프로토콜로 평가되고 있다.[3] 본 시스템에서는 LDAP에 각 네트워크 관리 시스템의 서브트리를 관리자 인증정보를 저장하여 각 계층에 대한 인증을 수행하였다. 이로써 디렉토리를 사용하는 그리드 네트워크 관리 시스템의 보안을 유지할 수 있다.

2. 관련 연구

2.1 GMA

GGF의 성능 분야에 GMA에서는 그리드 네트워크에 있는 여러 그리드 모니터링 시스템의 상호 작용을 쉽게 이끌 수 있도록 확장성을 고려한 모니터링 구조에 대해서 연구하고 있다. (그림 1)에서와 같이 GMA는 세 개의 구성요소로 이루어져 있다. 디렉토리서비스는 이용 가능한 정보의 발행과 검색을 지원한다. 생산자는 데이터를 제공하는 부분으로 소비자에게 이벤트를 보내고 소비자는 데이터를 받는 부분으로 생산자로부터 이벤트를 요청하고 수신한다. 소비자와 생산자가 이용할 수 있는 관리정보를 이벤트로 구성하여 그에 대한 정보를 디렉토리 서비스에 저장하여 지역적으로 분산되어 있다 해도 두 생산자·소비자 쌍은 원하는 정보를 이벤트형식으로 전송할 수 있다.

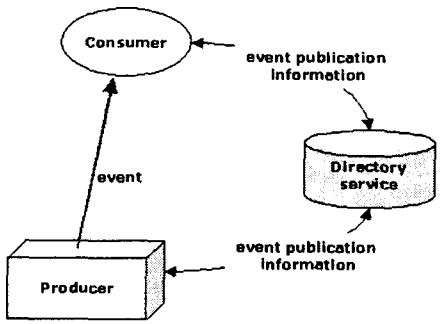

그림 1 GMA 구성요소

위 GMA구조에서 소비자는 관심의 생산자에 대한 발견을 위해 디렉토리 서비스를 이용하며, 생산자는 관심의 소비자를 찾기 위해 디렉토리 서비스를 사용한다. 생산자 소비자는 발견된 구성요소에 연결을 성립한 후 메시지의 전달과 성능 데이터의 전송은 각 소비자/생산

자 쌍 사이에서 디렉토리 서비스의 관련 없이 직접 수행된다.

그리드 환경에서는 수많은 정보 속에서 모니터링이 이루어지므로 네트워크상의 자원의 정보에 대한 검색에 소요되는 지연이 예측할 수 없을 정도가 될 수 있다. 따라서 수집과 탐색에 관련된 오버헤드와 지연에 대해 명확한 지역 내의 제어가 가능해야 한다. (그림 1)에서와 같이 메타데이터를 접근 가능한 공간에 디렉토리서비스에 저장해 두고 통신상에서는 데이터의 생산자와 소비자간에 직접적인 전송이 이루어지도록 함으로써 데이터의 전송과 탐색을 분리하여 대규모 자원에 대한 모니터링을 수행한다.[4]

본 논문에서는 이와 같은 구조를 기반으로 하여 그리드 네트워크 관리시스템에서 총괄적인 관리를 위해서 공통의 디렉토리서비스를 이용하여 네트워크 영역의 관리시스템이 메타정보를 디렉토리서비스에 저장하였다. 관리자는 디렉토리서비스에 접근하여 대규모의 네트워크상에서 탐색과정을 거쳐 해당 관리 시스템에 직접 연결할 수 있다. 연결 후 생산자는 관리자의 요청에 직접 응답하여 관리를 할 수 있게 한다. 이를 통해서 분산된 생산자를 이용하여 관리시스템을 구성하여 전체 네트워크를 관리 할 수 있다.

2.2 LDAP

디렉토리 서비스란 인터넷에 연결되어 있는 호스트 및 인터넷 사용자들에게 디렉토리 형태로 구성된 유용한 데이터를 빠르게 제공하는 것을 말하며 인터넷의 발전과 함께 인터넷 디렉토리 서비스의 기술개발도 빠르게 발전하고 있다. 1980년대 말에 특정분야의 디렉토리 서비스의 이용, 개발 요구가 높아감에 따라 CCITT(International Telegraph and Telephone Consultative Committee, 현재는 ITU이다)와 ISO(International Organization for Standardization) 두 단체가 함께 X.500이라는 디렉토리 서비스 표준을 만들기 시작하였다.

LDAP은 X.500 디렉토리에 대한 TCP/IP에서의 용이한 접속과 구현에 초점을 두고 만들어진 프로토콜이다. LDAP은 데이터 모델 자체가 분산 모델에 기초를 두고 있으며, 주어진 데이터의 쿼리가 인터넷상에 연결된 모든 호스트상의 디렉토리 데이터와의 연동이 되는 구조적 장점과 그 구현이 매우 용이한 장점을 갖고 있다.

LDAPv3의 주요 특징은 아래와 같다.

- LDAPv2의 프로토콜 구성요소들을 모두 제공한다. 이 프로토콜은 X.500에 관한 대부분의 회의/ 발표 비용 없이 TCP나 다른 운반수단으로 곧바로 전달된다.
- 대부분의 프로토콜 자료들은 일반스트링(ordinary string)으로 인코딩이 가능하다.
- 주어진 입력 쿼리에 대하여 정보를 보유하고 있는 서버들이 정보를 요청한 서버에게 참조지시(Referral)기능을 지원한다.
- 공동 보안 서비스(association security services) 제공을 위해 SALS와 TLS 메커니즘을 함께 사용할 수 있다.
- ISO 10646 문자셋을 지원한다.
- 새로운 작업기능의 지원을 위한 확장성을 갖는다.
- 데이터베이스 스키마는 사용자들의 이용을 위해 디렉토리에 기술된다.

디렉토리의 내적인 구조를 정의하는 정보모델을 살펴보면, 디렉토리 객체는 디렉토리 정보의 분산 여부에 관계없이 하나의 엔트리(Entry)에 저장된다. 엔트리는 속성(Attribute)의 집합으로 구성되며, 국가명, 조직명, 우편번호, 직책, 전화번호 등 약 60여 개의 속성 유형을 가지고 있다. 그리고 사용자의 필요에 따라 새로운 속성 유형을 정의할 수 있다. 그러나 속성 유형들은 연속된 정수들로 구성된 고유의 객체 식별자 OID(Object IDentifier)를 사용하며 이는 다른 사용자가 같은 유형의 속성을 방지한다.

DIB(Directory Information Base)는 속성 구분과 매칭규칙을 준수한 엔트리의 집합으로 구

성된 것을 말하며 이들의 모든 엔트리는 UNIX 파일 시스템과 유사한 계층적인 트리 구조로 구성되어지는데 이를 디렉토리 정보 트리 DIT (Directory Information Tree)라고 한다. DIB의 구성은 전체 디렉토리 시스템의 작은 부분이지만 이들의 구축 방법에 따라 전체적인 시스템 규격 작성에 큰 영향을 미친다. [5][6]

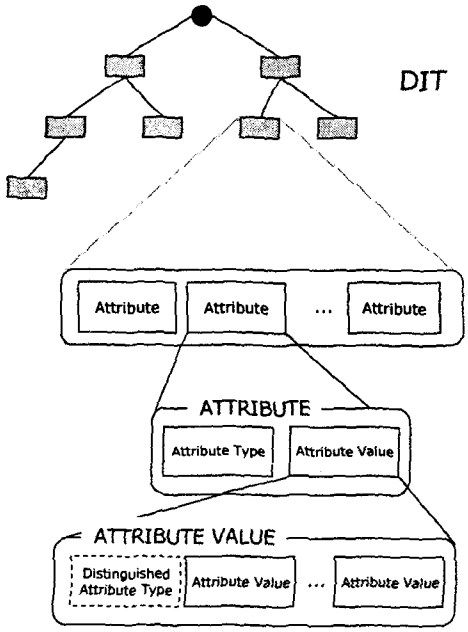

그림 2 LDAP의 DIT와 엔트리 구조

(그림 2)은 DIT와 엔트리의 구조를 보여주고 있다. 모든 엔트리는 특정한 속성을 가진 RDN(Relative Distinguished Name)으로 구성되어 있다. RDN의 역할은 상위 엔트리와 하위 엔트리들을 서로 구분하기 위하여 사용되며 이들의 집합을 DN(Distinguished Name)이라고 부른다. RDN과 DN은 디렉토리 정보를 엑세스하기 위하여 사용되어지므로 고유한 값을 가져야 하며 동시에 디렉토리 사용자가 이해 및 기억하기 용이해야한다.

3. 그리드 네트워크 관리 시스템 설계

그리드 네트워크 관리 시스템을 설계하기 위하여 그리드 네트워크가 지리적으로 이종의 분산되어 있는 자원으로 구성된 것을 고려해야 한다 이를 위해 GGF의 Grid Performance Working Group에서 제안한 GMA(Grid Monitoring Architecture)를 연구하여 이의 개념을 이용하여 시스템에 설계하였다.

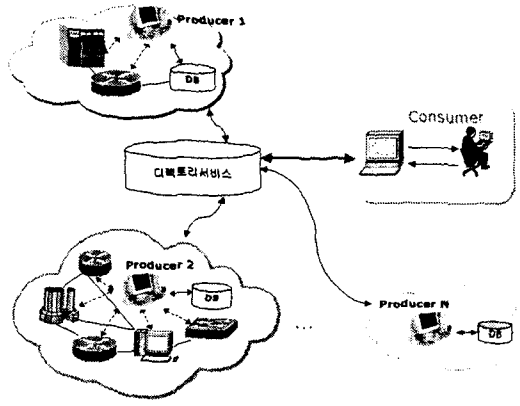

그림 3 전체 시스템

(그림 3)은 전체 시스템 구성도를 나타낸다. 관리 도메인인 네트워크에는 관리정보를 제공하는 여러 생산자(Producer)를 둔다. 그리드의 Web-based 네트워크 관리를 수행하는 소비자(Consumer)를 둔다. 소비자는 디렉토리 서비스를 이용하여 각 생산자 시스템에 연결하여 자원의 관리 정보를 볼 수 있다

여러 생산자는 자신의 연결정보와 관리 네트워크의 장비 및 회선에 대한 메타정보를 디렉토리 서비스에 발행하고 관리 영역의 성능 및 장애 정보를 수집 분석하여 자신의 지역 데이터베이스를 이용하여 정보 저장을 수행한다. 소비자

는 디렉토리 서비스를 이용하여 그리드 네트워크 생산자 시스템의 등록과 삭제를 수행하며 각 생산자의 자원 정보를 분석하여 맵상에 가시화함으로써 총체적인 관리를 가능하게 한다.

3.1 디렉토리서비스

네트워크 자원의 관리 서비스를 공유하기 위해서는 상이한 구성요소의 메타정보를 중앙화하는 것이 필요하다. 모니터링 구성요소들은 제각기 작동하면서 서로 이용할 수 있어야 한다.[7] 디렉토리서비스는 각 구성요소의 존재를 알릴 수 있고 이용할 수 있게 하는 공통의 저장소가 된다.[8]9] 본 논문에서는 LDAP을 이용하였다. 이는 디렉토리에 접근하는 표준화된 프로토콜로 분산된 네트워크 구성요소들을 관리하기 위한 확장성있는 구조를 적용하기 용이하다.

(그림 4)는 본 그리드 네트워크 관리 시스템을 위해 설계한 DIT(Directory Information Tree)이다. 각 네트워크 관리 시스템은 엔트리를 구성하고 관리시스템에 구성되어 있는 생산자r에 대한 정보를 하위 노드에 둔다. 생산자는 하나 또는 다수의 모니터링 정보를 이벤트로 저장한다. 이벤트를 제공하는 생산자 정보를 저장함에 따라 소비자는 원하는 정보를 얻을 수 있다. 이벤트는 그리드의 상이한 모니터링 시스템이 동적으로 구성될 때 호환을 위해 일치성이 유지되어야한다. 이는 NMWG에서 정의하는 부분이 될것이다.[10] 메트릭은 아직 표준화된 부분이 없기 때문에 임의의 네트워크 메트릭을 정의하는 기관을 두어 이벤트 스키마를 저장한다.

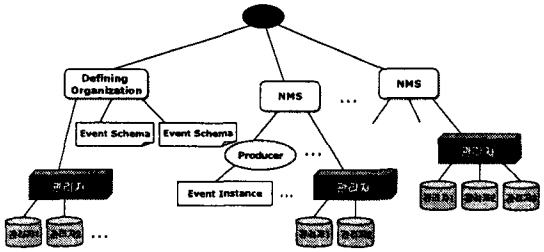

그림 4 디렉토리 구성도

각 네트워크 관리 시스템에는 관리자 정보를 저장하는 서브 DIT를 가진다. 각 네트워크 관리 시스템에 자신의 서브트리에 관리자 정보를 관리하는 엔트리를 두어 자신의 관리자들의 인증정보를 가지게 된다. 관리자를 다루는 DIT의 세부 사항은 값은 (그림 5)와 같다.

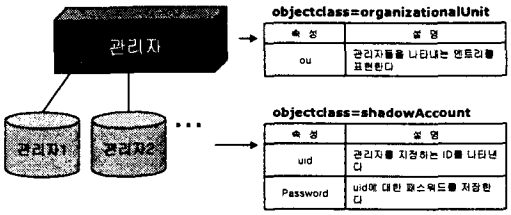

그림 5 관리자 서브트리 구성도

3.2 생산자

생산자는 모니터링 정보를 요청하는 곳에 정보를 제공하는 역할을 수행한다. 생산자는 다음과 같은 모듈로 구성된다.

1) 그리드 네트워크 토폴로지 표시 모듈

그리드 네트워크 구성요소의 토폴로지를 표시하기 위해서는 먼저 구성요소들에 대한 정보를 기록하는 기능을 제공해야 한다. 이를 위해서 자원 추가, 자원 삭제, 자원 병경 기능을 수행하도록 한다.

2) 그리드 네트워크 구성요소의 상태표시 모듈

그리드 네트워크 구성요소의 상태표시를 위해서는 먼저 구성요소의 상태표시 항목을 정의해야 한다. <표 1>은 정의된 수집 항목을 나타낸다. 정의된 상태표시 항목은 소비자 시스템에 의해 생산자 시스템으로 요청되고 생산자 시스템이 디렉토리 서비스를 이용하여 구성요소의

정보를 수집 및 분석하여 이벤트 형식으로 응답하는 기능을 제공한다.

분석은 실시간 분석으로서 소비자 인터페이스의 네트워크 화면(네트워크 맵)에 보여질 장애 정보와 관리자가 관리 대상에 대한 현재의 장애 상황을 실시간으로 분석하려는 항목 요구에 대한 실시간 응답을 처리한다. 이러한 분석 시스템의 분석 결과는 분석 항목에 따라 표, 그래프 등의 형식으로 관리자에게 가시화되는 기능을 제공한다.

<표 1> 수집 항목

장애 관리 정보	설 명
라우팅 에러율	라우터의 수신 패킷 중에 경로 설정 테이블에 없음으로 인해 라우팅을 수행하지 못하는 패킷의 율을 나타낸다.
시스템 메모리 부하율	시스템의 전체 송수신 패킷에 대해서 발생하는 폐기 패킷의 율로 나타낸다.
시스템 패킷 출력율	단위 시간당 시스템(라우터)에 출력되는 IP 패킷 트래픽율이다.
시스템 패킷 전달 실패율	시스템의 수신 패킷에 대해서 경로 설정에 관여하는 패킷에 대해 전달 실패되는 패킷의 율을 나타낸다.
인터페이스 패킷 송신율	인터페이스에 유출입 되는 전체 패킷에 대한 송신 패킷의 율을 나타낸다.
시스템 패킷 전달율	시스템의 수신 패킷에 대해서 경로 설정에 관여하는 패킷의 율로 나타낸다.
에러 수신율	원격지 시스템으로부터 유입되는 프레임의 에러에 의해서 상위 계층 프로토콜로 전송되지 못하는 수신 패킷의 수를 의미한다.
인터페이스 패킷 손실율	인터페이스에서 손실되는 송신/수진 패킷의 율로 나타낸다.
시스템 패킷 손실율	시스템의 IP 계층에서 송수신할 때 손실되는 패킷의 율을 나타낸다.

3) 실시간 장애 정보 제공 모듈

그리드 네트워크 맵을 웹 상에 적용시켜 현재 네트워크 상황을 모니터링 하는 기능을 제공하한다. 여러 시스템들이 이와 유사한 기능을 제공하지만, 웹 상에서 네트워크 맵을 통해 트래픽 정보, 장애 탐지 정보 등을 실시간으로 제공하지 못하고 있다. 본 시스템에서 관리자는 관리 대상이 되는 네트워크 맵 구성을 볼 수 있으며, 마치 고속도로의 트래픽 상황을 CCTV를 통해 보는 것처럼 실시간 장애 현황을 네트워크 맵을 통해 한 눈에 파악할 수 있다.

4) 일정기준(임계값)을 이용한 장애 발생 감지 모듈

관리자가 정의한 일정기준(임계값)에 근거하여 장애발생을 감지한다. <표 2>는 장애 발생 감지 항목을 나타낸다.

<표 2> 장애 발생 감지 항목

임계값 항목	설 명
라우터 메모리 부하율	라우터의 전체 송수신 패킷에 대해서 발생하는 폐기 패킷의 율로 나타낸다.
패킷 전달 실패율	단위 시간당 해당 장비에 출력되는 IP 패킷 트래픽율이다.
데이터 에러율	해당 장비에 입출력 되는 패킷의 에러율이다.
시스템 패킷 손실율	시스템의 IP 계층에서 송수신할 때 손실되는 패킷의 율을 나타낸다.
인터페이스 패킷 손실율	인터페이스에서 손실되는 송신/수신 패킷의 비율로 나타낸다.

생산자가 장애 관리를 위해 수집한 정보로부터 값을 분석하여 관리자가 설정한 임계값을 초과하면 소비자에게 이벤트를 보냄으로써 관리자에게 실시간으로 통보함으로써 유연하게 대처하는 기능이다. 관리자는 임계값을 설정함으로써 장애 정도를 조절하여 효율적인 네트워크 트래픽 관리를 할 수 있다.

5) 트랩데몬을 이용한 실시간 장애 탐지 모듈

네트워크 상에서 장애 발생은 가장 치명적인 문제이다. 이 경우, 먼저 장애가 발생했는지 아닌 지의 장애 발생 여부를 탐지하는 것이 필요하며, 그 다음에는 어디에서 장애가 발생했는지 가능한 한 빨리 장애 위치를 파악하여 관리자에게 통지하거나 시스템 내의 에러나 장애 발생을 일으킬 수 있는 소지가 있는 중요 에러에 대해서는 신속히 관리 시스템에 알릴 필요가 있다. 관리 시스템은 이 에러를 보고 받고 적절한 대응을 하도록 한다. 본 시스템은 지능적인 관리를 통하여 보다 빠르고 정확한 장애 위치 확인 기능을 제공한다.

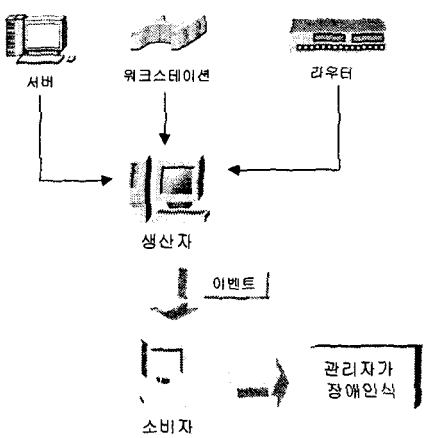

그림 6 실시간 탐지

트랩을 이용한 장애 탐지 과정은 (그림 6)과 같다. 먼저 데몬 프로세스와 같이 관리자의 요청이 없더라도 주기적으로 네트워크의 장애 감시한다. 이때 감시 주기는 관리자가 설정 가능하다. 디렉토리서비스에 정의된 장애 항목에 대해 생산자가 주기적으로 감시하고, 각 장애 항목에 대하여 관리자가 설정한 임계값과 비교를 통하여 장애 진단 여부 파악 및 장애 발생 시 소비자에게 통보한다.

3.3 소비자

소비자는 관리 정보를 요청하여 수신하는 곳이다. 소비자는 디렉토리 서비스를 통하여 모니터링을 하려는 정보의 제공 생산자를 찾아 생산자에 직접 연결하여 이를 요청한다.

각 네트워크 관리시스템의 관리자는 디렉토리에 저장되어 있는 자신의 인증 정보를 이용하여 관리시스템에 접근할 수 있다. 관리자가 관리시스템에 접근하는 과정은 (그림 7)과 같다. 먼저 접근하려는 네트워크 관리시스템의 디렉토리의 서브트리 위치를 구성파일로부터 가져온다. 해당 엔트리에 관리자 목록을 검색하여 인증을 수행한다. 아이디와 패스워드가 인증되면 관리시스템에 접근하여 관리를 수행하게 된다.

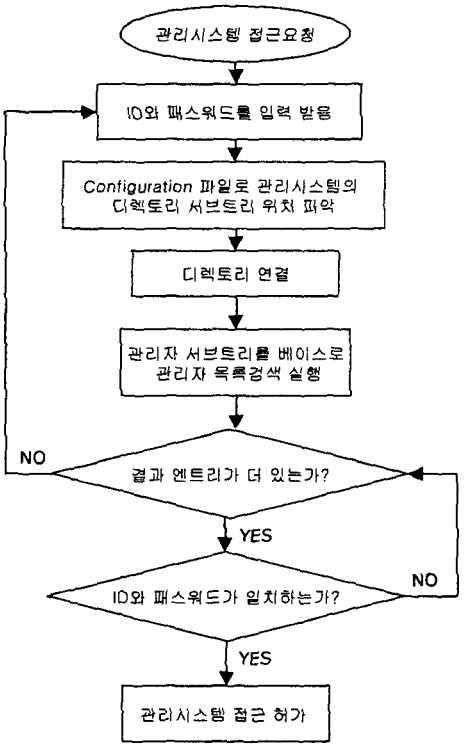

그림 7 관리자 인증과정

4. 결 론

본 논문에서는 GMA 모델을 토대로 그리드 네트워크 자원의 상호 운용을 위한 대규모 분산된 관리 정보를 사용하기 위해 적합한 관리 구조 연구를 수행하여, 그리드 네트워크 관리 시스템을 설계하였다. 생산자와 소비자의 유기적인 관계를 통하여 정보를 송수신하고 그리드 네트워크의 관리를 수행한다. 또한 그리드 네트워크의 구성요소를 가시화하고 대규모의 상이한 자원의 관리를 한 곳에서 제공하여 한눈에 모니터링을 통한 여러 그리드 네트워크의 성능 및 장애를 관리할 수 있는 시스템이다.

그리드 네트워크 관리 시스템을 구성하는 각 관리 영역의 시스템은 해당 관리자에 의해 접근되어야한다. 이를 위해 디렉토리에 해당 관리 시스템의 관리자의 인증정보는 저장하게 하였다. 관리 시스템의 서브트리에 관리자를 나타내는 엔트리를 두어 하위에 관리자 인증정보를 저장한다. 본 논문에서 설계한 그리드 네트워크 관리시스템은 분산된 관리 시스템들에 접근하기 위한 관리자를 인증할 수 있게 되어 그리드 네트워크 관리 시스템의 안정성을 보장한다.

참고문헌

[1] http://www.gridforumkorea.org/

[2] http://www.globalgridforum.org/

[3] A. Croll, E. Packman, "Managing Bandwidth", Prentice Hall, 1999

[4] B.Tierney, R. AYdt, D. Gunter, W. Smith, M. Swany, V. Taylor, R.Wolski. "A Grid Monitoring Architecture." GGF Document

[5] Jim Sermersheim, "Novell's LDAP Developer's Guide", IDG books, 2000

[6] 신정훈, 김희철, 권영직, "인터넷 LDAP 기술과 시험시스템 구축에 관한 연구", 한국정보시스템학회,147-153, 1998

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

[8] S. Fitzgerald, I. Foster, C. Kesselman, G. von Laszewski, W. Smith, S. Tuecke. "A Directory Service for Configuring High-Performance Distributed Computations." Proc. 6th IEEE Symp. HPDC, pp. 365-375, 1997.

[9] K. Czajkowski, S. Fitzgerald, I. Foster, C. Kesselman. "Grid Information Services for Distributed Resource Sharing". Proceedings of the Tenth IEEE International Symposium on HPDC-10, IEEE Press, t 2001.

[10] Bruce Lowekamp, Brian Tierney, "Network Metrics for Grid Applicaitons and Services",

노 민 기

2000년 공주대학원 영상매체전공 (석사)

2000년 ~ 한국과학기술정보연구원 연구전산망

하 지 아

2002년 성균관대학교 전기전자 및 컴퓨터공학부 졸업 (공학사)

2002년 ~ 현재 성균관대학교 정보통신공학부 석사과정

안 성 진

1988년 성균관대학교 정보공학과 졸업 (학사)

1990년 성균관대학교 대학원 정보공학과 졸업 (석사)

1990년 ~ 1995년 한국전자통신연구원 연구전산망 개발실 연구원

1996년 정보통신 기술사 자격 취득

1998년 성균관대학교 대학원 정보공학과 졸업 (박사)

1999년 ~ 현재 성균관대학교 컴퓨터교육과 조교수