유휴 멀티 e-Science 그리드 자원 공유를 위한 통합 자원 접근 제어

(An Integrated Access Control for Sharing of E-Science Grid Resources)

정 임 영 † 정 은 진 †† 염 헌 영 †††
(Im Y. Jung) (Eunjin Jung) (Heon Y. Yeom)

요 약 본 논문은 e-Science 그리드 자원 공유를 위한 가볍고 솔기없는 통합 자원 접근제어를 제안한다. 그리드 컴퓨팅에 기반한 e-Science는 고가의 과학 실험 장비를 포함하는 그리드 자원을 원격조정하고 이로부터 얻은 데이타를 고성능 컴퓨터를 통해 처리하는 총체적인 도메인을 구성하여 과학자들의 연구를 돕는다. 그런데, 많은 사용자들이 그리드 자원을 이용할 때, 사용자가 소속된 e-Science 그리드에서 자원이 부족할 경우, 원하는 자원을 이용하기 위해 기다리거나 자원이용을 포기할 수 있다. 이런 경우, 적절한 보상 하에 타 그리드의 유휴 자원을 이용할 수 있으면 자원제공자와 사용자 모두에게 도움이 될 수 있다. 그런데, e-Science 그리드는 개개 그리드 단위로 특정 과학응용을 연구하는 과학자들의 사용편의를 위해, 가상 조직(Virtual Organization-VO)에 특화된 자원 접근정책이 운영되고 있기 때문에, 자원의 공유가 결코 쉬운 문제가 아니다. 본 논문은 e-Science 그리드 사용자가 복수 개 타 그리드의 공유자원을 이용할 때, 전체 그리드 차원의 자원접근정책 통합을 위한 선협정(Service Level Agreement-SLA)이 필요없어 가볍고, 사용자가 소속 그리드의 자원을 이용하는 것과 같은 과정으로 추가적인 등록이 필요하지 않아 솔기없는 새로운 통합 자원 접근 제어를 제안한다.

키워드 : e-Science 그리드, 그리드자원공유, 통합자원접근제어

Abstract This paper proposes a light-weight, seamless integrated access control for global e-Science resource sharing. E-Science, based on Grid Computing, was designed to help scientists to remotely control and process the Grid resources such as high-end equipments and remote machines. As many researchers engage in the e-Science Grids, the researchers in a grid often have to wait for or give up use of the Grid resources, even when there are idle resources in other Grids. In this case, provided that proper compensation is given, Grid resource sharing is helpful both for the researchers and the Grids which provide their resources. But, sharing Grid resources globally is not simple, as each e-Science Grid is especially designed for resource sharing in its Virtual Organization(VO) and already has its unique access control policy for its resources. This paper proposes a new integrated access control for e-Science Grid resource sharing. The access control is light-weight without any priori service level agreement(SLA)s among the Grids which share their resources and seamless because the users can use the resources shared as the ones belonging to their Grids without their additional registration to the other Grids.

Key words : e-Science Grid, Grid resource sharing, an integrated access control for Grid resource sharing

· 본 논문은 서울대학교 공학연구소의 지원을 받은 것이다.

† 정 회 원 : 서울대학교 컴퓨터공학부
iyjung@dcslab.snu.ac.kr
†† 정 회 원 : Univ. of Iowa 컴퓨터사이언스 교수
ejjung@cs.uiowa.edu
††† 종신회원 : 서울대학교 컴퓨터공학부 교수
yeom@snu.ac.kr

논문접수 : 2008년 5월 26일
심사완료 : 2008년 8월 29일

Copyright@2008 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.

정보과학회논문지: 시스템 및 이론 제35권 제10호(2008.10)

1. 서 론

과학 연구의 경우, 고도의 연산 자원이나 대용량의 데이타 처리를 필요로 하는 경우가 일반적이나, 연구 기관별로 이를 충족시킬 만한 고도의 컴퓨팅 인프라를 갖춘다는 것은 매우 어려운 일이다. E-Science[1]는 그리드 컴퓨팅[2]을 기반으로 지리적으로 분산된 고가의 연구 자원을 원격 조작을 통해 이용하여 과학 연구의 생산성을 향상시키는 것을 목표로 한다. 공유의 대상이 되는 자원은 슈퍼컴퓨터, 클러스터와 같은 연산 자원뿐 아니라 첨단 장비, 기존 연구 데이타, 인적 자원을 망라한다. 그러나, e-Science 그리드에서 효율적인 자원 공유는 결코 쉬운 문제가 아니다. e-Science 그리드는 개개 그리드 단위로, 관련 가상조직[2]의 자원공유를 목적으로 설계되고 운영되고 있다. e-Science 그리드의 사용자가 많아지고, 기사용자가 많은 양의 자원을 오랜 시간 이용해야 하는 경우, 타 그리드에 유휴자원이 있는데도, 다른 사용자들은 자신이 속한 그리드의 가용자원이 없어서 자원이용을 대기하거나 또는 대기 시간이 긴 경우는 자원이용을 포기해야 하는 경우가 생기게 된다. 그림 1은 분산 성능 테스트 프레임워크인 DiFerP를 이용해서, GT3.2[3]에서 그리드 서비스 요청(Load)에 따른 응답시간(Response Time)과 요청 해결 부분(Throughput)을 그래프화 한 것[4]이다. 그리드 상에서 서비스 이용요청이 점점 많아질 때 이를 만족시켜줄 가용자원이 없는 경우, 서비스 응답시간 지연이 심해짐을 알 수 있다.

그렇지만, 자원부족이 생길 때마다 고가의 자원을 각 그리드가 계속 자체 보충하는 것은 현실적으로 힘들고 합리적이지 않다. 따라서, 기존 그리드 자원으로 그리드 사용자의 요구를 효율적으로 충족시키기 위해, 전체 그리드 자원의 공유는 필요한 일이다. 이를 위해서는, 먼저 각 그리드의 자발적인 유휴자원의 공유를 유도할 수 있는 방안과 그리드의 자원을 공정하고 안전하게 공유할 수 있는 믿을 만한 자원 이용 메커니즘을 찾아야 한다.

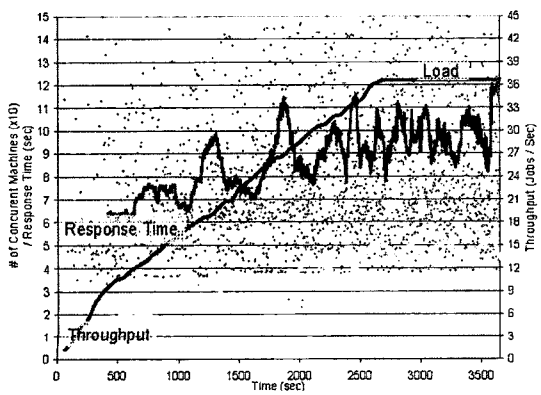

그림 1 GT3.2 서비스 객체의 생성 : Response Time, Throughput, Load

현재, 고가의 유휴자원 공유를 유도하기 위한 유인기제(incentive mechanism)가 그리드 컴퓨팅에 도입되어 많은 논의가 진행 중이다. 그런데, 경제논리를 적용한 자원이용 가격의 책정 및 거래 메커니즘에 관한 논의는 활발한 반면, 공유를 위한 각 그리드의 보안정책을 수용하는, 그리드 자원 접근에 대한 총체적인 호환성 문제는 상대적으로 많은 논의가 되고 있지 못하다. 현재 그리드 자원 공유를 위해 도입된 유인기제들이 Peer-to-Peer (P2P) 시스템에서의 유인기제와 거의 같은 형태로서, 그리드 환경에 바로 적용되기에는 적절하지 않다. E-Science 그리드는 가상조직을 통한 자원접근제어가 가능하기 때문에, P2P시스템에 비해서 더 강한 신원관리(identity management)를 가정할 수 있다. P2P시스템이 일반적으로 한 종류의 자원공유-즉, Gnutella[5], BitTorrent[6], KaZaa[7]들에서의 파일공유 또는 SETI [8]에서의 CPU 공유-를 목적으로 하는 반면, 그리드 시스템의 경우, 컴퓨팅 리소스, 첨단 장비, 데이타 저장소 등 다양하고 보다 가치가 높은 자원이 공유되기 때문에 각 자원 별로 통제되는 접근허가가 다르다.

그리드 간의 자유로운 자원 공유를 위해서는, 그리드 자원에 접근할 수 있는 각 그리드 가상조직의 보안정책이 호환되어 서로를 신뢰할 수 있어야 한다. 그런데, e-Science 그리드는 기본적으로 특정과학응용에 대해 이의 이용자들만을 주 대상으로 모든 보안 정책이 설계되는 특수 도메인이다. 어떤 한 그리드의 가상조직 멤버들이 속한 그리드 자원에 대한 접근권한 설정은 각 그리드 고유의 정책에 따르게 된다. 그리고, 자격기반자원접근(Role Based Access Control-RBAC)에 기반할 경우, 각 그리드가 정한 자격(role)과 이에 따른 권한 설정은 일반적으로 상이하다. E-Science에서 다루는 데이타는 주로 연구자들의 실험데이타로서 그 보안이 특히나 중요하다. 따라서, e-Science 그리드 자원은 완전한 개방 시장(open market)으로서의 기능이 아닌 통제된 개방 시장으로서 자원공유가 가능해야 할 필요가 있다. 그리고, 각 그리드에서의 자격의 의미(semantic)가 같지를 않으며, 이 자격들에 대한 자원 접근 허가도 다르게 제공이 되기 때문에, 간단히 자격만을 통합하여 이 자격에 따른 자원 접근 허용 정책을 그대로 적용 할 수가 없다. 굳이 성격이 다른 자격기반자원접근제어를 통합하는 경우는, 특정 그리드 간의 빈번한 자원공유를 위한 필요성을 제외하면, 굳이 통합의 이득이 없어진다.

이에, 본 논문은 e-Science 그리드의 한 응용인 HVEM Grid [9]를 중심으로, 사용자가 속한 그리드에 가용자원이 없을 경우, 여러 유휴 그리드에 소속된 자원

들을 공유하기 위한 자원접근제어에 대한 해법으로, 가볍고 솔기없는 새로운 통합자원접근제어를 자격기반 자원접근제어 기반에서 제안한다.

논문의 구성은, 2장에서는 그리드 시스템에서의 자원 공유 논의를 살펴본다. 또한, 자원 공유를 위한 보안 시스템 및 그리드 인프라에서의 보안 메커니즘에 대한 논의도 같이 살펴보고, 기존 논의의 문제점과 미비점을 짚어볼 것이다. 3장에서는 e-Science Grid의 한 응용 예인 HVEM Grid의 자원 및 서비스을 기준으로, 그리드 자원접근제어, 그리고 자원 공유를 위한 조건을 기술한다. 4장에서는 HVEM Grid를 중심으로 멀티 공유자원 이용을 위한 새로운 통합접근제어 메커니즘을 제안을 한다. 5장에서는 제안된 그리드 공유자원 통합접근제어 메커니즘의 보안성을 분석하고, 기존의 그리드 자원 통합접근제어 제안과의 효율성을 비교한다. 그리고, 6장의 결론으로 본 논의는 마무리된다.

2. 관련연구

분산 시스템의 특징을 가지는 그리드의 자발적인 자원 공유를 이끌어내기 위한 유인기제[10]는 일정한 기준에 의해 자원 제공에 대한 보상을 지급하는 것이다. 현재까지 그리드 자원 관리 시스템에 활발히 도입된 유인기제들은 P2P 시스템에서의 유인기제와 거의 같은 형태들이다. 경매를 통한 그리드 자원의 할당을 Catallaxy paradigm[11]으로 제안한 CatNets[12] 프로젝트와 열린 그리드 시장을 위한 그리드 미들웨어를 제안한 SORMA 프로젝트[13]의 경우, 효율적인 자원 이용정책만 조명될 뿐, 인증 및 공유자원 접근제어 등의 거래를 위한 보안 구조는 빠져있다. 은행의 개념을 도입한 그리드 계정 서비스를 제시하는 GridBank[14]의 경우도, 자원 거래 메커니즘 외에는 X.509를 비롯한 그리드 인프라의 기본 정책 및 메커니즘을 이용한다고만 간단히 언급하고 있다. 그리드 가상조직들의 협동을 위한 보안 메커니즘을 미들웨어 측면에서 제시한 NAREGI 프로젝트[15]에서는 가상조직 간의 인증서 발급기관(Certificate Authority-CA)과 인증서 등록기관(Registration Authority-RA)들은 서로 신뢰관계가 있다는 가정 하에 VOMS [16]를 이용하고 사용자 프락시를 통해 다른 그리드 자원을 사용하는 도식을 따른다. 즉, 이미 서로를 잘 알고 있는 가상 조직들 간은 계약 하에 새로운 정책을 정해서 서로의 자원을 자유롭게 이용할 수 있는 구조가 된다. 그런데, 유휴자원을 이용하는 모든 그리드 간에 사전에 협정(SLA)을 맺어서 서로의 자원을 공유하기 위한 보안규정을 정하는 일은 확장성이 부족하고, 공유정책에 변화가 생기면 보안 협정을 갱신해야 하는 문제가 있다[17-19]. 또한, 자원을 공유하는 그리드들을 위한 통합 정책의 유지 관리를 위해 제3의 신뢰기관을 필요로 하는 부분은 분산 자원을 이용하는 컴퓨팅의 경우 대중적인 해법이 아니다[18].

자원을 공유하는 그리드 간에 완전히 새로운 정책을 선협정으로 정하지 않고, 각 그리드의 기존 정책을 호환시켜보자는 논의도 있다. 즉, 그리드 간의 공유자원 접근을 위한 자격 호환성은 대개 그리드 간에 비슷한 자격을 정의하고 이에 대한 자원 접근을 제어한다는 가정 하에 사용자가 속한 그리드와 자원을 제공하는 그리드 양자 간의 타협 논의로 국한되어왔다[17]. 그러나, 어떤 e-Science 그리드에서의 자격이 다른 그리드에서 같은 이름을 가진다고 이 자격의 의미가 같다고 가정하고, 이 자격에 대한 권한을 기계적으로 통합해서 자원 접근을 제한하는 것은 일반적으로 무리한 가정이 된다. 이는 비교적 장기적인 공동연구를 위해 제휴를 맺은 몇몇 그리드를 넘어서 전체 그리드의 유휴자원을 공유의 대상으로 볼 때는 더더욱 무리한 가정이 된다. 또한, 자격 및 이에 관련된 자원 접근 제어 정책의 변화를 포용할 수 있는 메타정책(meta-policy)을 정하자는 논의[20]도 있다. 그러나, 전체를 포괄하는 메타정책을 먼저 수립해야 하며, 각 그리드 정책에 변화가 생길 때마다 메타 정책과의 호환성 시험을 통해서 메타정책에 부합이 되도록 조정을 하는 과정이 필수이다. 결국, 이 메타정책이 전체 그리드의 정책을 포괄하는 구조가 아닌 이상, 이에 부합되는 자격기반 접근 제어 구조를 가지는 그리드 도메인에 유용하고 그 외의 도메인에는 적용하기 힘든 부분이 있다.

따라서, 본 논문은 어떤 그리드 사용자가 자신이 속한 그리드에 가용 자원이 없을 때, 외부 그리드의 유휴자원을 임시로 사용하는 일반적인 경우를 대상으로, 추가적인 장치 및 새로운 정책이나 제3의 신뢰기관의 필요가 없고, 또 새로운 등록 과정 등의 추가 절차가 필요 없는, 거래정보공유의 보안이 보장되는 자격기반접근제어에 기반한 가볍고 솔기없는 멀티 그리드 공유자원 접근 제어 메커니즘을 제안한다.

3. E-Science 그리드 자원 접근 제어

3.1 자원, 서비스 및 접근 제어

그림 2는 HVEM Grid System을 나타낸다. HVEM Grid 사용자들은 원격조정서버(Telecontrol Server)를 통해 초고압전자현미경(High Voltage Electronic Microscope-HVEM)[21]을 원격으로 조작할 수 있으며, 원하는 시료의 사진을 찍을 수가 있다. 찍은 사진은 데이타그리드(DataGrid)[22]에 저장될 수 있고, 이 이미지를 데이타그리드로부터 가져와서 계산그리드(Computation Grid)의 계산자원제공자를 통해 3차원 이미지로 만들어

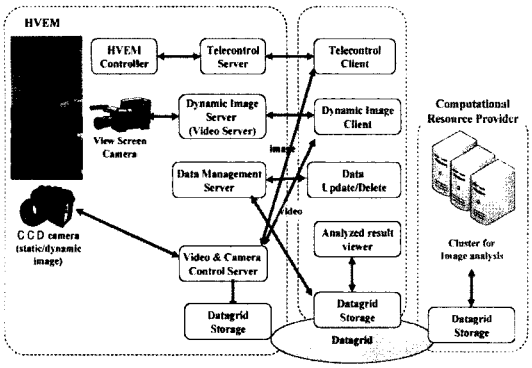

그림 2 HVEM Grid System

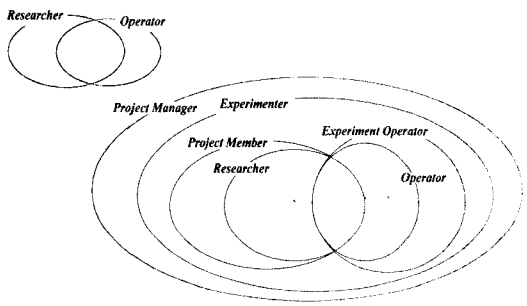

그림 3 HVEM Grid의 자격 계층도식(Role Hierarchy)

다시 데이타그리드에 저장할 수 있다. 과학 실험 및 고가의 실험기기 보안을 목적으로, HVEM Grid에의 접근은 먼저 X.509에 기반한 인증서를 통한 사용자 인증을 하게 되고, 실제 자원의 이용은 다시 HVEM Grid 내에서 사용자들에게 정의한 자격기반자원접근제어[23-25]에 따른다. 즉, 사용자는 HVEM Grid의 일원이 됨으로써 자원에 접근할 수 있는 자격을 부여받게 되는데, 그리드의 자원은 이 자격에 대한 접근 권한으로 제어된다. 그림 3은 HVEM Grid의 권한 설정을 보여준다. 크게 연구자(researcher)와 오퍼레이터(operator)가 있고, 이들은 HVEM 실험을 통해 나온 데이타 정리를 위해 프로젝트(project) 및 실험(experiment) 등의 체계를 갖추게 되면, 이에 따라 각 실험에 대해 프로젝트 매니저(Project Manager)와 실험자(Experimenter) 등의 세부자격을 갖추게 되고 데이타그리드 및 계산그리드의 자원접근 권한이 다르게 설정이 된다. HVEM Grid의 경우 공유대상이 되는 자원은 데이타그리드와 계산그리드이다.

3.2 E-Science 그리드 유휴 자원 공유를 위한 조건

E-Science 그리드 상의 자원 공유가 공평하고 빠르고 용이하게 제공되기 위해서는 다음의 조건이 만족되어야 한다.

- 기존 그리드의 자원접근제어 정책은 되도록 수정하지 않고 자원 공유가 가능해야 한다.

그리드 간 자원 공유 계약을 일일이 체결하려면 기존의 자원접근제어정책을 수정해야 하고, 게다가 한번 수정하고 나면 갱신 비용이 높아지게 된다. 각 그리드가 정한 자격과 자원 접근 정책을 모두 조율하고, 이를 유지하고 각 그리드 자격이나 자원접근정책에 변화가 생기면 갱신하는데 많은 비용이 들기 때문이다. 자원공유에 참여하는 그리드의 수가 늘수록 그 비용은 비례해서 증가하게 되므로, 특히 단기 자원공유를 위해서는, 서비스수준계약이나 기타 자원 공유에 대한 계약을 되도록 하지 않는 방향이 바람직하다.

- 자원을 제공하는 그리드에서 허용되지 않는 자원 접근은 그리드 간 자원공유 시에도 허용되지 않아야 한다.

그리드 사용자들에게 허용되지 않는 자원 접근은 자원 공유 시에 허용되지 않도록 보장이 되어야 자발적인 자원 공유를 유도할 수 있다.

- 자원공유를 원하는 그리드 사용자는 할당받은 자원의 양 및 사용권한은 보장받되, 그 이상을 제공받지 않아야 한다.

그리드 사용자는 할당받은 자원이용은 보장받아야 하고, 전체 그리드 자원 공유의 공정성을 기하기 위해 그 이상은 제공받지 않아야 한다.

3.3 멀티 그리드 유휴 자원 공유 시나리오

본 논의는 장기 협약을 통한 그리드 자원 공유는 논외로 하고, 여러 그리드 유휴자원을 임시로 이용하는 경우를 논의의 대상으로 한다. 그리고, 한 곳 이상의 그리드에서 공유자원을 제공받을 때 통합 자원접근권한설정에 대해 논한다.

그림 4는 멀티 그리드 자원공유의 한 시나리오를 보여준다. 그리드 A에 속하는 사용자 A[a]가 자신이 속한 그리드에서 필요한 자원을 이용할 수 없어서 공유자원을 제공하는 타 그리드 B, C, D, E, F, G에 자원이용요

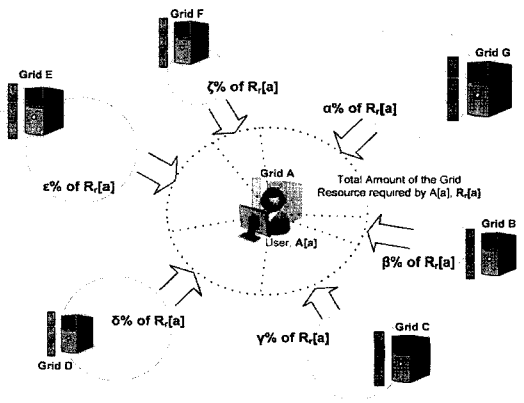

그림 4 유휴 공유 자원 이용 시나리오

청을 하는 경우이다. A[a]가 필요로 하는 자원은 A에서 허가받은 R_r[a]이나, 이를 한 그리드에서만 제공을 받을 수가 없어서, 각 그리드로부터, R_r[a]의 α%, β%, γ%, δ%, ε%, ζ% 만큼씩을 요청하는 경우를 나타낸다.

4. 멀티 그리드 공유 자원 통합 접근제어

기본적으로 그리드 공유자원을 사용하는 사용자는 자신이 속한 그리드의 자원이 부족해서 공유자원을 사용하는 것이고, 영구적이 아닌 임시로 사용하는 것이기 때문에, 사용자가 속한 그리드에서 자원 할당 및 제어정책을 따르는 것이 타당하다. 따라서, 본 논의는 사용자가 속한 그리드에서의 사용자에게 적용하는 자격기반 자원 접근제어에서 기술한 자원할당 및 제어정책을 이 사용자가 다른 그리드의 자원을 이용할 때도 기본적으로 적용되도록 한다. 그리고, 사용자가 실제 할당받는 타 그리드 자원은 그 위에 자원 제공자의 자원공유 제한정책이 반영된 가상자격기반제어(Virtual RBAC)을 통해서 가능하도록 한 메커니즘을 제안한다. 기본적으로는 사용자가 속한 그리드의 자격기반접근제어를 따라 타 그리드 자원을 이용하지만, 자원을 제공하는 타 그리드가 외부인이 공유자원 사용시에 적용하는 자원접근제어 정책이 있다면 이를 반영한 새로운 자격 및 이에 따른 권한이 정의되어야 하고, 이는 임시로 존재하게 되는 새로운 자격기반접근제어가 되기 때문에 가상자격기반제어가 된다. HVEM Grid를 비롯한 e-Science 그리드의 경우 공유자원을 이용하기 위해서는 먼저 인증절차를 거쳐야 한다. 그리고, 사용자의 자격에 따라 공유자원 이용에 제약이 가해진다. 따라서, 본 장에서는 e-Science 그리드의 공유자원 이용을 위한 인증부터 데이타그리드 공유자원 이용과 계산 그리드 공유자원 이용을 위한 자격기반자원접근제어의 호환성 메커니즘을 기술한다.

4.1 그리드 자원 공유를 위한 준비

자원을 공유하는 그리드들은 멀티캐스트 그룹을 이뤄, 자신이 제공하는 공유자원에 대한 정보를 주기적으로 멀티캐스트한다. 이 정보는 가용공유자원의 종류와 양, 사용기간 만료된 자원 및 사용자에 대한 준실시간(near realtime) 정보이다. 이는 각 그리드 사용자들에게 실시간으로 제공되어, 자신이 원하는 자원을 어떤 그리드에서 제공받을 수 있는지를 알 수 있도록 한다. 또한, 이 정보로, 각 그리드는 사용자 각각의 자원할당량과 자원 사용권한을 관리할 수 있다. 각 그리드들은 이미 공개키 시스템(PKI)기반의 개인키, 공개키를 가지고 있고, 각 그리드의 공개키는 이미 자원을 공유하는 그리드 간에 이미 다 알고 있고, 그리드 간의 통신채널은 안전하다고 가정한다.

4.2 그리드 사용자 인증

자원을 제공하는 그리드와 공유를 요청하는 그리드 간에는 다음과 같은 거름망(filter)을 거쳐, 그리드 A에 속한 사용자 a인 A[a]가, 임대한 그리드 자원 사용에 대한 가상 자격(Virtual Role)을 부여받고, 자원을 제공하는 그리드는 이 자격에 대한 가상 자원 접근 정책을 결정하게 된다.

A[a]는 반드시 자신이 속한 그리드 A를 통해서만 타 그리드 자원을 사용할 수 있고, 그리드 A는 이미 할당된 타 그리드의 A[a]에 대한 자원할당량을 뺀 A[a]의 총 자원 할당량과 자격권한을 조정하게 된다. 그림 5와 6은 A[a]가 타 그리드의 자원을 요청하는 과정과 다 쓴 자원을 반납하는 과정을 시간의 흐름에 따른 프로토콜로 나타낸 것이다.

그림 5에서, 자원을 공유하는 그리드에 접속할 수 있는 것은 각 사용자가 속한 그리드 포털을 통해서이다. A[a]가 그리드 A의 포털에 자신의 인증서로 접속해서 타그리드에 필요한 자원의 양과 사용기간을 요청한다. 이 때, 이 할당자원을 공유할 사용자 및 그룹의 리스트를 같이 보내게 된다. 실제 그 요청은 A[a]를 대신해서 A가 타 그리드에 하게 되는데, 이 때, A는 자신의 인증서와 A[a]의 A에서의 권한 및 자원할당량을 자신의 개인키로 사인을 해서 같이 보내게 된다. 각 그리드에서는 그리드 A에게 제공하는 공유자원에 대한 사용제약이 있으면 이를 적용시킨 후 A[a]에 대한 가상 자격 rv_X(A[a])를 자신의 개인키로 사인을 해서 A에 보내게 된다. 즉, B에서 보내온 것이면 rv_B(A[a]), D에서 보내온 것이면 rv_D(A[a])라 명명된다. 이 가상자격에는 각 그리드에서의 자원할당량과 이에 따른 제약조건, 그리고 사용 가능한 시간이 명시된다. A는 이 가상 자격을 A[a]에는 전달하여 할당 가능한 자원의 양과 이의 이용에 대한 제약을 알려준다. A[a]가 이를 받아들여 사용하게 되면, A는 A[a]의 가상 자격들을 하나의 가상자격으로 통합 명명된 rv_A(A[a])를 자원을 사용하는 그리드에 전송하게 된다. 이는 각 그리드마다 자격 명명이 달라서, 접근하는 그리드가 다르면 다른 가상자격 명명으로 매번 접근해야하는 문제를 해결하게 된다. 이후, A[a]는 공유자원사용 유효기간 동안은 타 그리드에서 rv_A(A[a])로 관리되게 된다. 사용 유효기간이 다가오면 자원을 공유했던 각 그리드는 이에 대한 경고를 A를 통해 A[a]에게 보내게 되는데, 갑작스런 자원회수로 인한 데이타 손실을 막기 위해서이다. 사용 유효기간 전의 자원 반납의 경우는 그림 6과 같이 우선 A[a]의 자원접근 가능여부를 확인한다. 공유자원을 제공하는 그리드는 접근하는 A[a]와 A를 인증서로 확인하고, A[a]의 할당자원을 체크한다. 할당 자원에 접근허가가 되는 경우는 자진 반납이 가능한데, A[a]에 부여되었던 자원을 회수하

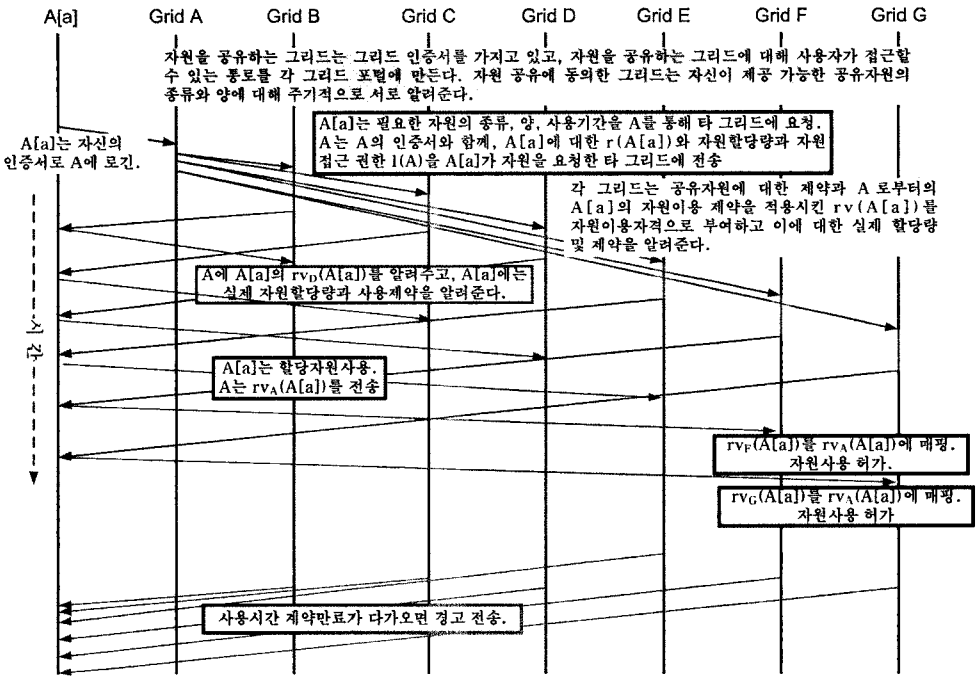

그림 5 공유 자원 요청 과정

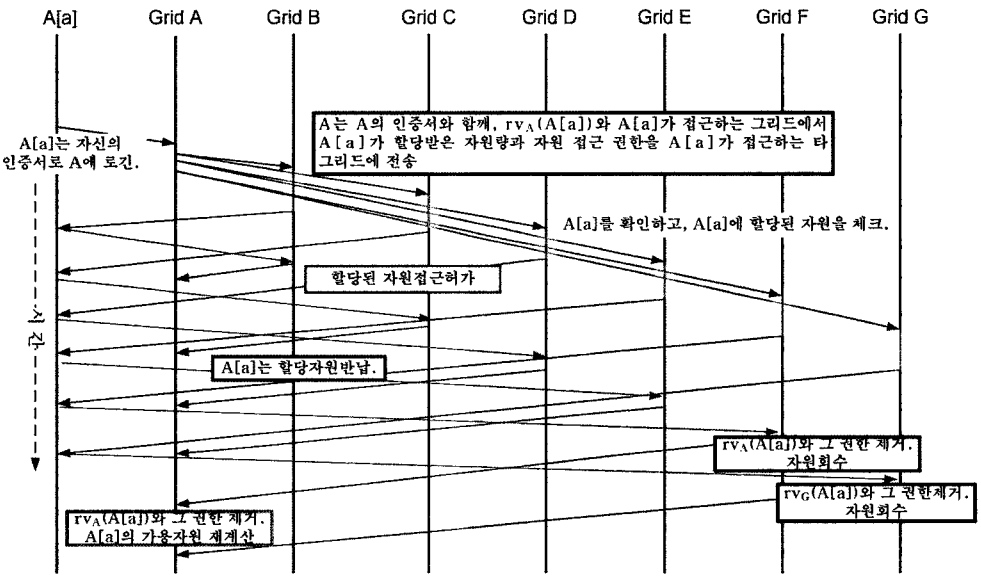

그림 6 공유자원 반납 과정

고, A[a]의 가상 자격과 그 권한을 없애는 일로 마무리가 된다. 자진 반납의 절차를 거치지 않으면, 기간 종료와 함께 자동으로 자원이 회수된다.

4.2.1 자원을 제공하는 그리드의 거름망(filter)

각 그리드가 사용자 A[a]에 대해 자신의 자원을 제공해주는 메커니즘은 거의 비슷하다. 따라서, 자원을 제공하는 그리드 B를 중심으로 자원 제공자의 거름망에 대해 기술한다.

- 사용자 인증

자원 공유를 원하는 A[a]가 자신의 인증서를 제시하

는 경우, 그리드 B는 A[a]가 정당한 그리드 A의 사용자이고 A의 가상조직에 속한다는 것을 확인한다. 또한, 그리드 B는 A의 인증서와 A에서 보내오는 A[a]에 대한 자원 할당 규칙을 보고 A[a]가 그리드 A의 정당한 사용자로서 A에 속하는지에 대한 것을 확인한다. 사용자 개인과 사용자가 속하는 그리드에 대한 인증이 동시에 이뤄지기 때문에, 어떤 그리드에도 속하지 않은 사용자는 기본적으로 그리드 자원을 공유할 수가 없다. 자원을 공유하는 그리드 간에는 사용자 각각에 대한 세부적인 공유 자원 사용 규칙에 대해서는 선협약을 하지 않는다.

- 공유자원 할당

  사용자 별로 할당되는 공유자원은 사용자가 소속된 그리드에서 일차적으로 사용자의 자격에 따라 할당량이 결정이 되고, 이차적으로 사용자가 소속된 그리드의 할당량 및 자원접근권한을 보고 자원을 제공하는 그리드에서 실제 공유가능한 자원을 할당해 준다. 이 때, A[a]가 요구하는 자원양이 현재 B에서 제공해 줄 수 있는 양보다 크면 요구를 거절한다. 즉, A[a]의 요구량을 $R_r^B(A[a])$, A[a]가 A에서 할당 받을 수 있는 자원의 양을 $R_a^A(A[a])$, B에서 공유를 위해 제공하는 전체 양을 R_a^B라고 하면, $R_a^B - R_r^B(A[a]) \geq 0$, $R_a^A(A[a]) \geq R_r^B(A[a])$여야 한다. 만족이 되는 경우는 B는 A에게 A[a]의 자원할당을 통보하게 되고, A[a]는 이 자원을 이용할 수 있게 된다. B가 제공하는 공유자원의 양은 주기적으로 멀티캐스트 되지만, 실시간 자원 사용상황은 아니기 때문에, 실제 자원 할당 시에 자원 사용요구는 거절될 수 있다.

- 가상 자격 및 가상 자원접근제어 설정

  공유되는 자원의 양을 정하고 이를 할당 시, 단기의 자원 임대 기간 동안 이 자원에 대한 접근을 통제하기 위해 이 사용자에 대한 가상 자격을 결정하고 이에 따른 권한 설정을 자원을 제공해주는 그리드에서 하게 된다.

그림 7에서 보여주듯이, A에서의 A[a]의 자격 r(A[a])는 공유자원을 제공하는 그리드 X의 자원공유정책을 반영한 $vr_X(A[a])$로 가상 자격이 정해지게 된다. A는 A[a]의 A에서의 자격 r(A[a])를 A[a]가 접근하는 그리드 들에 알려주면, 각 그리드는 이를 바탕으로 제공하는 공유자원을 사용할 A[a]에 대한 가상 자격을 알려주게 되는데, 예를 들면, 그리드 D는 가상자격 $vr_D(A[a])$를 A에 알려주게 되고, 그리드 B는 $vr_B(A[a])$를 알려주는 식이 된다. A[a]는 자신이 원하는 양과 조건이 만족이 되는 그리드 자원을 요청하고 사용하게 되는데, 이 때 A는 A[a]가 정해진 기간에 사용하는 공유 그리드 자원들에 대해 그 명명된 통합가상자격이 $vr_A(A[a])$로 접근

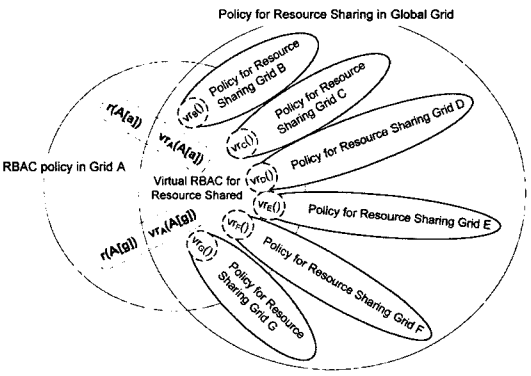

그림 7 그리드 자원 공유 시 설정되는 가상 자격 및 자원 접근제어

을 할 것임을 A[a]가 접근하는 각 그리드에 알려주게 된다. $vr_A(A[a])$를 받은 그리드 B는 $vr_B(A[a])$를 $vr_A(A[a])$로 그 명명을 바꾸게 되고, 그리드 D는 $vr_D(A[a])$를 $vr_A(A[a])$로 그 명명을 바꿔서 이후 $vr_A(A[a])$로 접근한 사용자에 대한 자원 제공을 적절히 해주게 된다. 이는 각 그리드에서의 A[a]에 대한 자격 명명을 통일하는 것이고, 각 그리드에서의 $vr_A(A[a])$의 권한은 다르게 된다. A의 그룹 g에 대해서도 같은 가상 자격 설정이 가능하다. 이 가상 자격은 자원 임대 기간 동안에만 유효하고, 기간이 지나면 경고 후에 없어지게 된다. 지정된 기간 안에 할당받은 자원에 접근하는 경우는 그림 8과 같다. A[a]가 자원을 할당받을 때, 이 기간 안에 할당받은 A[a]의 자원에 접근할 수 있는 l(A)를 같이 제출하게 되는데, 이 속에는 A의 사용자 및 그룹리스트가 들어있다. 즉, l(A)를 통해서 알려지게 되는 A[b]의 공유자원에의 접근 권한이 있고, A에서의 A[b]가 그 공유자원을 사용할 권한이 있는 경우에만 접근이 가능하고, 그렇지 않으면 접근 이 허용되지 않는다. 그림 8에서 A[b]는 A에서의 자격 r(A[b])와 이 자격에 대해 A에서 허용한 자원접근권한에 의해서 그리드 N에서 A[a]가 할당받은 자원을 공유하게 된다. l(A)는 A[a]가 A에게 제출을 하고, A가 A[b]의 권한을 검토해서 공유자원을 제공하는 그리드에 제출을 하게 된다.

다음 절에서는 HVEM Grid에서 자원 공유 시 구체적으로 적용이 되는 예를 살펴본다.

4.3 HVEM 데이타 그리드 공유

데이타 그리드에서 데이타 읽기의 경우는 이미 발표된 연구결과가 대상이 되는데, 이는 HVEM Grid의 모든 사용자들에게 개방이 되고, 개방되지 않은 데이타의 경우는 발표되지 않은 실험 데이타로 HVEM 실험 관련 인들에게만 읽기가 허용이 된다. 이 데이타에 대한 쓰기나 수정은 이 데이타를 입력한 본인과 HVEM 실험이

속한 프로젝트 매니저만이 할 수 있는 일로 자격에 따른 데이타그리드 접근 제어를 하고 있다.

HVEM Grid에서는 기본적으로, 데이타 그리드 자원의 공유를 허용하는 외부 그리드 사용자들에게는 HVEM Grid 내부 사용자들과 같이, 발표된 데이타만이 열람되도록 하고, 공동연구로 인해 필요한 특별한 데이타에 대한 접근 정책은 공동연구를 진행하는 그리드 간의 협약을 통해 공유가 이루어지도록 한다. 공동연구를 위한 공유의 경우는 단기적인 유휴자원 공유의 개념을 벗어나는 경우로서 본 논의에서는 논외로 한다.

데이타 저장소로의 데이타 그리드를 공유하는 경우, 자원을 제공하는 그리드는 일정 영역의 저장소를 빌려주게 된다. 즉, 각 공유자원은 사용가능한 양과 기간으로 정의될 수 있다. 이 때, 공유 자원을 사용하기 위한 기본 과정은 그림 5, 6의 도식과 같고, 이미 공유 자원에 저장된 데이타에 대한 그리드 사용자의 접근과정은 그림 8의 도식과 같다. 그리드 B의 데이타그리드에 대해 자원공유를 요청할 때, 그리드 A의 사용자 A[a]가 자료 공유를 원한다면, 그림 5에서 자원을 할당받을 때 A[a]가 B에서 획득한 자원에 접근할 수 있는 그리드 A에서 정의된 실험 그룹 또는 프로젝트 그룹과 이 그룹의 접근권한을 B에 I(A)의 형태로 제공해야 한다. 여기에 기술되지 않은 그룹의 멤버나 개인은 접근할 수 없게 된다. 그리드 A에서 정의된 그룹은 B의 자원 공유 정책에 의해 그 권한이 축소 될 수 있고, B에서는 가상그룹(Virtual Group)으로 관리가 된다. 이 그룹에 속하는 그룹원들이 A[a]가 획득한 B의 자원에 대해 접근이 허용되면 더 이상의 A에서의 자격에 관계없이 A[a]가 B에서 획득한 자원에 대해 B가 정한 가상자격에 따라 접근이 가능하다. 접근 허용 그룹은 공유를 할당받은 공간에 대한 접근 허가를 정의받게 되고, 이 속의 특정 데이타에 대한 접근허가는 기본적으로 정의되지 않는다. 특정 데이타에 대한 접근제어는, 사용자가 할당받은 영역 속에 저장되는 데이타의 속성을 저장 시에 정할 수 있다. 즉, e-Science 그리드에 저장되는 실험 데이타 중, 저장자 만이 접근 가능한 사설(private), 가상 그룹 멤버들에 의해 읽기 접근이 가능한 공개(public)로 구분해서 저장을 하게 된다.

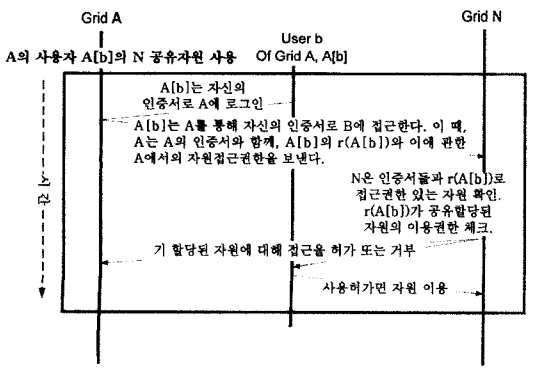

그림 8 공유자원에의 접근

4.4 HVEM 계산 그리드 공유

계산 그리드의 경우는, 처리 용량이 큰 프로그램을 실행시킬 수 있는 컴퓨팅 자원을 사용하는 것으로써, 이를 이용할 수 있는 권한 역시 사용자가 속한 그리드 도메인의 자격기반접근제어에 따르며, 자원을 제공하는 그리드 정책이 같이 적용된 사용권한 설정이 이뤄지게 된다. 사용자가 원하는 자원요구량 역시 사용자가 속한 그리드에서 할당받은 양을 기준으로 다른 그리드 자원을 이용할 수 있게 된다. 컴퓨팅 자원은 각 사용자에게 기본 프로그램을 기준으로 몇 대에서 어느 정도 기간을 사용할 수 있는지를 기준으로 할당되게 된다. 이를 기준으로 타 그리드의 자원을 이용할 수 있다. 계산 그리드의 경우도 그룹에 대해 자원을 할당받은 것이면, 할당받은 사용기간 안에 A[a]가 지정한 그룹원들이 같이 할당받은 자원을 사용할 수 있으나, 개인이 할당받은 경우는 개인만이 사용권이 있게 된다. 자원의 요청 및 반납은 그림 5, 6에 따르고, 할당된 기간 내에 공유자원에의 접근은 그림 8을 따른다.

5. 분석 및 평가

이 장에서는, 제안된 e-Science 그리드 자원공유를 위한 통합자원접근 메커니즘를 타 제안에 대해 그 성능을 분석하고 보안 타당성을 기술한다.

5.1 성능 평가

서로 다른 자원접근정책을 운영하는 그리드 간의 자원공유를 위해서는 이들 정책의 호환성을 어떻게든 제공해 주어야 한다. 기존 연구는 자원공유 전에 선협정을 통해서 그 기반을 마련하는가 그렇지 않은 다른 방법을 사용하는가에 따른 접근방법이 양분이 되며, 편의상 본 제안을 A라 두고 기존 제안을 이 성격에 따라 B, C로 구분하여 명명한다.

B : 자원을 공유하는 전체 그리드 간에 공유자원 접근을 위한 선협정을 자원 공유 전에 미리 맺는 경우이다. 이 경우는 각 그리드 간의 연결통로(cross link)를 이용하는 SERAT를 제안한 경우가 해당[19]이 되는데, 이 연결통로를 정하는 과정이 선협정을 맺는 과정과 같다. 또한, 사용자의 신용장(credential)에 기반한 각 그리드 간의 자격을 대응(mapping)시키는 경우도 이에 해당이 된다[17]. 그리고, 분산 선협정 관리(B-a)를 하는가 중앙집중식 관리(B-b)를 하는가에 따라 비용이 다르게 산출될 수 있다.

C : 그리드 간 자원공유를 위한 자격호환에 대한 선협정은 맺지 않는 경우이다. 대신 각 그리드 정책의 호환을 위한 메타정책을 정하고 이에 따라 자원공유를 하는 경우가 해당된다[13].

본 제안의 부담(overhead)과 성능은 다음과 같은 e-Science 그리드의 자원 공유상황 하에서 평가가 될 수 있다.

- 각 그리드에서 제공할 수 있는 자원의 종류와 양은 알 수 있다고 가정한다.
- 공유자원을 제공하는 그리드는 그룹을 이루어 이 그룹에 속하는 그리드들은 서로 간의 인증이 가능하다고 가정한다.
- 공유자원에 대한 정책은 자원을 제공하는 그리드 단위로 바뀔 수 있고, 자원을 공유하는 그리드는 추가 및 제거될 수 있다.
- 각 그리드 내의 정책 변화로 그리드 사용자의 자격 및 자원 접근제한설정은 달라질 수 있다.

성능 평가를 위해 표 1과 같은 기호를 사용한다.

표 1 성능평가를 위한 표기

I	공유자원을 이용하는 사용자의 수
L	한 사용자가 요청하는 자원을 제공하는 그리드 수
P	자격 및 권한 단순 매칭 및 비교 비용
M	통신 비용
n	자원을 공유하는 그리드의 수
a	각 그리드 상의 자격의 수
b	각 그리드 상의 자격이 가질 수 있는 권한 수
c	메타정책이나 통합 자원 접근 정책의 자격 수
d	메타정책이나 통합 자원 접근 정책의 자격이 가질 수 있는 권한의 수
α ($0 \le \alpha \le 1$)	정책의 변화가 생긴 그리드, 새로운 공유자원을 제공하는 그리드 혹은 더 이상 자원을 공유하지 않는 그리드의 비율

그리고, 다음의 세 가지 경우에 대해 평가를 한다.

- 그리드 간의 자원 공유를 위한 준비 비용
  - A는 공유자원을 이용하기 위한 준비비용이 없다.
  - B는 상이한 그리드 보안 체계에 대한 선협정 비용이 든다. 이는 분산 선협정 관리(B-a)를 하는가 중앙집중식 관리(B-b)를 하는가에 따라 다음 식 (1), 식 (2)의 비용으로 각각 계산된다.

$$ {}_nC_2*a*b*a*b*P \quad (1) $$

$$ {}_{(n-1)}C_1*c*a*d*b*P \quad (2) $$

  - C는 자원공유에 참여하는 그리드 전체에 적용되는 메타정책을 수립하고 각 그리드가 각각의 정책을 메타 정책에 대응을 시키는 비용이 든다. 정상적인 대응이 되는 경우는 인증서를 발급하게 된다.

$$ {}_nC_1*c*a*d*b*P \quad (3) $$

- 한 그리드의 사용자가 외부 그리드 공유자원을 이용할 때 드는 비용
  - A는 사용자의 인증서와 소속 그리드에서의 자원접근권한으로 타 그리드에서 공유자원 할당을 결정하게 된다. 자원이용 요청이 있을 때, 각 그리드에서 외부 사용자에 대한 자원이용권한 결정에 대한 비용이 B와 C에 대해 더 들게 된다. 공유를 요청한 그리드 내부에서 사용자가 원하는 자원을 줄 수 있는지 심사를 하게 되고, 이에 대한 결과를 보고 사용자는 그 자원을 쓸 것인지를 최종 결정하고 그 자원을 이용하면, 사용자의 가상 자격을 어떻게 설정을 하면 되는지에 대한 결과를 주어야 하기 때문에, 공유자원을 원하는 사용자 I에 대해서는 식 (4)의 비용이 들게 된다. 앞 부분은 그림 5의 프로토콜 상의 가상자격 협상 비용이고, 뒷 부분은 각 그리드에서 I가 속한 그리드에 대한 전체 공유자원 할당 정책을 사용자가 요청한 자원에 할당하는 비용이다. 즉, 각 그리드 단위로 적용하는 제약을 각 사용자의 요청에 대해 적용을 시키는 비용이 들게 된다. 이후, 사용자 각각에 대한 자원할당이 이뤄지게 된다.

$$ I*L*(2P+3M) + I*L*P \quad (4) $$

  - B는 사용자의 인증서로 이미 체결된 협약에 의한 사용자의 자격과 권한을 확인하고 각 그리드의 정책에 호환되는 권한으로 자원의 이용을 허락하게 된다.

$$ I*L*(P+2M) \quad (5) $$

  - C는 메타정책에 호환이 되는 정책을 가진다는 인증서와 외부 그리드에서 이용할 수 있는 외부 인터페이스(export interface)를 사용자가 제시를 하면 이를 통해 외부 자원을 이용하게 된다.

$$ I*L*(P+2M) \quad (6) $$

- 공유자원을 제공하는 그리드에 변화가 있는 경우에 대한 비용
  - A는 그리드 상에 어떤 변화가 생기더라도 그로 인해 드는 비용은 없다. 실제 사용자가 공유자원을 이용할 때 그 권한은 구체적으로 결정이 되는 사항이기 때문에, 계속 관리를 해야하는 전체 구조는 없다.
  - B는 자원을 공유하는 그리드의 정책변화, 자원공유에 새로 참여하는 그리드, 더 이상 자원공유를 하지 않는 그리드에 대응하는 선협정을 자원을 공유하는 그리드 간에 다시 맺어야 한다.
    - 그리드 정책의 변화 및 자원공유에 새로 참여하는 그리드가 있는 경우

$$ {}_{n\alpha}C_1*{}_{n(1-\alpha)}C_1*a*b*a*b*p + {}_{n\alpha}C_2*a*b*a*b*p \quad (7) $$

$$ {}_{n\alpha}C_1*c*d*a*b*p \quad (8) $$

식 (7), 식 (8)은 각각 (B-a)와 (B-b) 경우에 대한

비용이다.

- 더 이상 자원공유를 하지 않는 경우

$$n(1-\alpha)C_2*a*b*a*b*p \quad (9)$$

$$(n(1-\alpha)-1)C_1*c*d*a*b*p \quad (10)$$

식 (9), 식 (10)은 각각 (B-a)와 (B-b) 경우에 대한 비용이다.

- C는 메타정책에는 변화가 없고, 변화가 있는 그리드에서 메타정책과 호환이 되는 정책을 수립했다는 인증서를 다시 만들어야 하고, 그리드 정책의 외부 인터페이스도 다시 만들어야 한다.

- 그리드 정책의 변화 및 자원공유에 새로 참여하는 그리드가 있는 경우

$$n\alpha C_1*c*d*a*b*p \quad (11)$$

- 더 이상 자원공유를 하지 않는 경우

$$n(1-\alpha)C_1*c*d*a*b*p \quad (12)$$

위의 준비비용, 공유자원 이용비용 및 공유자원을 제공 그리드의 변화를 수용하는 비용, 세 가지 경우를 모두 고려한 비용은 다음과 같다.

A		$I*L*(2P+3M) + I*L*P$
B	a	${}_nC_2*a*b*a*b*P + I*L*(P+2M) + {}_{n\alpha}C_1*n(1-\alpha)C_1*a*b*a*b*P + {}_{n\alpha}C_2*a*b*a*b*P$} (or ${}_{n(1-\alpha)}C_2*a*b*a*b*P$)
	b	${}_{(n-1)}C_1*c*a*d*b*P + I*L*(P+2M) + {}_{n\alpha}C_1*c*d*a*b*P$ (or ${}_{(n(1-\alpha)-1}C_1*c*d*a*b*P$)
C		${}_nC_1*c*a*d*b*P + I*L*(P+2M) + {}_{n\alpha}C_1*c*d*a*b*P$ (or ${}_{n(1-\alpha)}C_1*c*d*a*b*P$)

그리고, 각 경우에서 공통부분을 제거한 비용을 분석해보면 다음과 같다. A는 공유자원을 사용하는 사용자 수와 이 사용자가 얼마나 많은 그리드의 자원을 사용하는가에 민감한 경우가 된다. 반면 B와 C는 각 그리드에 속한 자격과 그 자격에 따르는 권한 수, 자원을 공유하는 전체 그리드 수, 또 자원을 공유하는 그리드의 변화에 상당히 영향을 많이 받는 비용구조가 된다.

표 2 시뮬레이션 환경

	그림 9, 10, 11	그림 12, 13, 14
L	1과 10 사이에서 무작위 선택	
P	0.02	
M	0.1	
a(c)	5	
b(d)	10	
α	0	0.2부터 1까지 변화

다음의 그림 9에서 그림 14까지는 이를 시간비용으로 나타낸 시뮬레이션 결과로 보여준다. 시뮬레이션 시, 표 1에서의 기호 값들은 표 2로 나타내었다. WinXP, Pen 4 3.00GHz, 1G RAM의 환경에서, 트리 매칭 프로그램과 TCP/IP통신의 처리시간의 측정으로, 실험에서는 자격 및 권한의 비교 비용 P는 0.02, 이에 대한 분산 그리드 객체들의 통신 비용은 0.1로 두었다. 즉, 프로세서와 통신 환경에 따라 P는 M은 절대적인 값이 아니라 비교 비용에 대한 통신비용의 비로서 그 값을 나타낸 것으로 50배의 차이가 나는 처리 및 통신 환경을 가정했다. E-Science 그리드는 전세계에 구축되어 있고, 이들 간의 통신 비용은 원 거리의 경우는 한 그리드 내에서의 비교 비용보다 훨씬 크게 된다. P와 M은 편의상 이를 초단위로 가정한다. 그리고, HVEM 그리드를 예로 들면, 프로젝트 매니저, 실험자, 프로젝트 멤버, 실험 그룹원, 그 외 일반 연구자, 실험그룹원인 오퍼레이터와 일반 오퍼레이터 들의 7개의 자격이 있고, 이들 각각이 허용받을 수 있는 세부권한은 데이타그리드, 계산그리드, HVEM 원격제어 및 포털 서비스에서 10개 이상이 된다. E-Science 그리드의 자격 및 권한의 수는 그리드 서비스의 수가 늘어나고 자원의 수가 늘면서 그 제어사항이 더 늘어나는 것이 일반적이다. 본 실험에서는 각 그리드의 자격은 5로 고정하고 이에 대한 권한 값은 10으로 두었다. 그리고, 편의상 메타정책이나 통합정책의 자격 및 권한도 같은 값으로 두었다. 보통은 사용자가 필요로 하는 자원은 거의 한 두 군데 그리드에서 제공이 되는 것이 일반적이기 때문에, 한 사용자가 필요로 하는 자원들이 속하는 그리드의 수는 최대 10이내로 제한을 두었다. 그리고, 실험의 모든 값들은 100번의 실행 평균값들이다.

그림 9는 공유자원을 사용하는 사용자의 수가 1부터 96까지 증가하고, 공유자원을 제공하는 전체 그리드 수가 또한 10부터 100까지 증가할 때, A의 메커니즘을 따를 때의 공유자원이용 비용을 나타낸 것이다. 그래프는 10부터 90까지만 나타내었다. 그림 10과 그림 11은 각각 B-a, B-b, C의 비용을 나타낸 것이다. 괄호 속의 숫자는 자원을 공유하는 그리드의 수를 나타낸다. 이 모든 경우는 자원을 공유하는 그리드 상의 변화가 전혀 없는 상태로 α 값은 0이 되는 경우들이다. A와 B, C는 시간비용으로 그려지는 y축의 값의 범위가 일단 다름을 알 수 있다. 자원을 공유하는 그리드 수의 증가는 B와 C 메커니즘의 초기비용의 증가를 유도하게 되어, 초기비용이 없는 A에 비해 그 비용이 높아진다. 이는 이 실험에서는 고정시킨 자격과 권한의 수가 늘어나면 더욱더 커지는 양상을 보여주게 된다. B-b와 C의 경우는 통합정책을 운영하는 경우로서 비슷한 비용을 보여주게 된다. 분산 정책을 유지하는 B-a에 비해 낮은 비용이 드는 경우이긴 하나, 본 실험에는 고려하지 않은 통합정책을 운영하기 위한 중앙서버나 메타정책을 먼저 수립해야 하는 추가 부담이 있다.

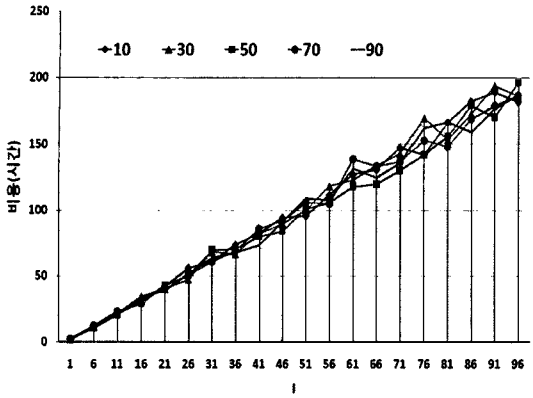

그림 9 그리드 수(n)에 대한 사용자(I) 증가에 따른 A의 비용

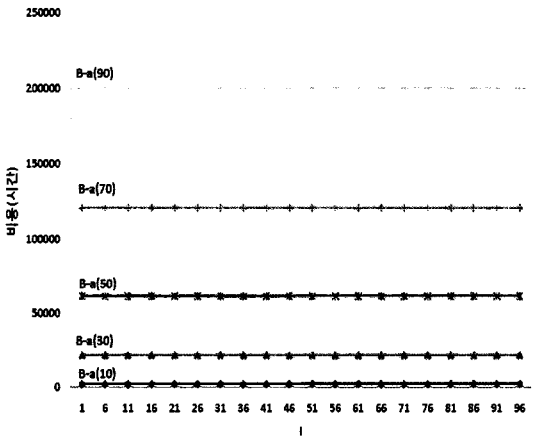

그림 10 그리드 수(n)에 대한 사용자(I) 증가에 따른 B-a의 비용

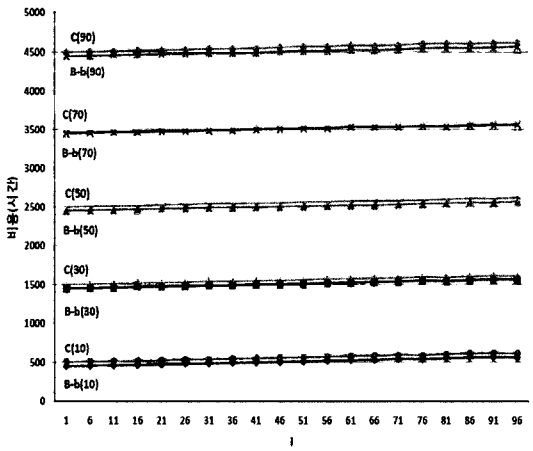

그림 11 그리드 수(n)에 대한 사용자(I) 증가에 따른 B-b와 C의 비용

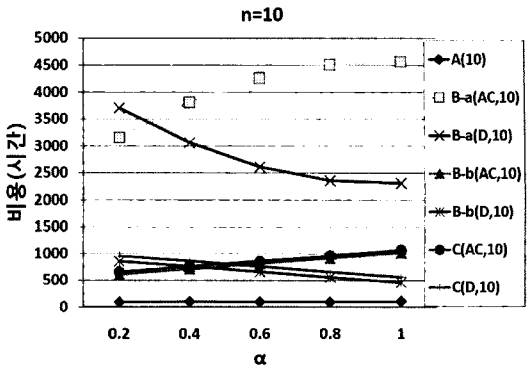

그림 12 α에 따른 비용 분석 (n=10)

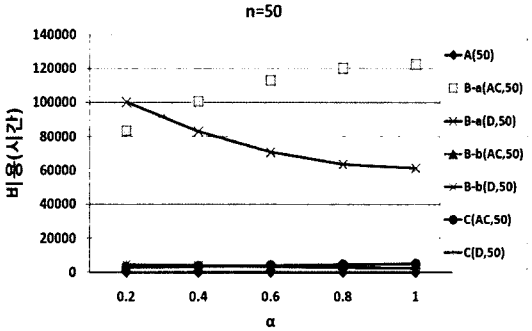

그림 13 α에 따른 비용 분석 (n=50)

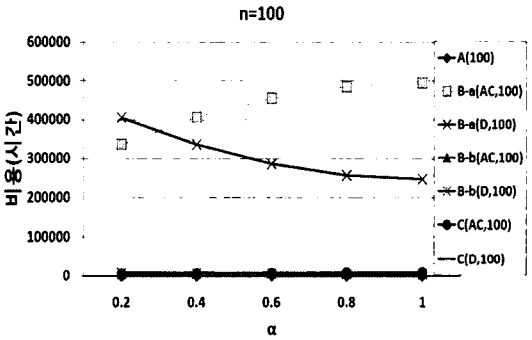

그림 14 α에 따른 비용 분석 (n=100)

그림 12, 13, 14는 공유자원을 사용하는 사용자의 수를 50으로 고정하고 공유자원을 제공하는 그리드 상의 변화로 인해 통합정책 역시 변화해야 하는 경우에 대한 실험을 보여준다. 전체 자원을 공유하는 그리드 중 변화가 일어난 그리드의 비율을 변화시키고 전체 그리드의 수를 변화시킬 때 어느 정도의 비용이 발생하게 되는지에 대한 결과들이다. A의 경우는 그리드의 수나 변화가 일어난 그리드의 비율에 무관하기 때문에 고정된 아주 작은 값을 보여주고 있다. 그러나, B와 C의 경우는 자

원을 공유하는 그리드 수가 많을수록 그 비용은 상당히 증가하는 양상을 보여준다. 그래프에서 괄호 속의 숫자는 자원을 공유하는 그리드의 수를 나타내고, AC는 새로이 자원을 공유하는 그리드가 추가가 되는 경우와 기존 그리드 상의 정책변화가 생긴 경우를 나타낸다. D는 자원을 공유하던 그리드가 더 이상 자원을 공유하지 않는 경우를 나타낸다. AC의 경우는 이미 자원을 공유하는 그리드들과 정책 통합의 필요가 있기 때문에 이 비율이 증가하면 비용이 따라서 증가한다. 반면, D의 경우는 더 이상 자원을 제공하지 않는 그리드를 배제하고 남은 그리드들의 정책통합이 일어나는 경우기 때문에, 이 비율이 증가하면 남은 그리드 들의 수가 적어지기 때문에 비용이 줄어들게 된다.

본 제안은 자원공유에 참여하는 모든 그리드 간에 상이한 정책호환을 위한 선협정이 필요하지 않으며, 이를 대체하는 메타정책을 또한 필요로 하지 않는다. 또한, 각 그리드의 정책변화에 둔감한 장점이 있게 된다. 상이한 과학분야의 연구지원 목적을 가지는 e-Science 그리드의 자원 공유는 서로 간의 공동연구나 협력을 위한 전체 그리드 자원의 세부적인 공유를 위한 협정이 굳이 필요하지 않은 경우이다. P2P의 성격이 강한 일반 데스크톱 그리드와는 달리 e-Science 그리드 자체 자원의 보안이 중요하고 일반적으로 공유될 수 있는 자원이 계산그리드나 데이타그리드로 제한되는 경우지만, 고가의 고성능 자원으로서 유휴분은 공유가 될 수 있기 때문이다.

따라서, e-Science 그리드의 유휴자원을 활용하기 위한 본 제안은 다음의 특징을 만족한다.

- 가벼운(light-weight) 접근제어 메커니즘

  E-Science 그리드 공유자원은 이용자가 속한 그리드의 자원을 이용할 수 없을 때, 차선으로 기간을 정해 필요한 자원만큼만 사용하는 임시적인 것이기 때문에, 전체 그리드의 자원접근 제어정책을 항상 알 필요가 없다. 대신, 사용자가 자원을 요구해서 사용할 당시만 그리드 간에 자원을 요청하는 사용자의 자원접근제어에 대한 합의를 하면 되기 때문에, 이를 위해 임시의 가상 자격과 이에 따른 자원접근제어 정책을 정하게 된다. 그리드의 모든 사용자가 공유자원을 원하는 경우는 결국은 그리드 간 선협정을 통해 자격호환성을 미리 정하는 것과 같은 비용이 들지만, 그렇지 않은 경우에 대해서는 그리드 간 자격호환성 유지를 위해 드는 비용은 없는 경우가 된다. 이 유지 비용은 그리드의 내부정책의 변화에 민감한 만큼, 적은 비용이 아니다.

- 솔기없는 자격기반자원접근제어(Seamless RBAC) 통합 메커니즘

  타 그리드의 공유자원 접근에 있어, 본 메커니즘은 사용자가 소속 그리드에 접근할 때와 같은 순서를 밟게 되고, 가상자격만 획득하게 되면, 타 그리드에는 유효기간 동안 그 자격으로 출입이 가능하다. 따라서, 중앙기관에 의한 사용자 등록 관리가 필요 없고, 자원을 공유하는 그리드 간에만 서로의 인증서로 확인을 하고 신뢰가 확보되면 된다. 사용자 입장에서는 소속된 그리드에서 접근제어를 받듯이 공유자원을 제공받는 쪽에서 자신의 소속 그리드에서의 자격으로 서비스를 받으면 된다. 또한 타 그리드의 자원 이용에 있어 추가적인 인증이나 자격획득을 위한 등록과정이 추가되지 않는 솔기없는 자원접근제어를 보장받게 된다.

5.2 보안 분석

타 그리드 자원의 공유를 위해서 사용자의 접근제어는 다음의 두 항목들을 보장해야 하는데[17,19,26], 본 논문에서 제시된 메커니즘은 다음과 같이 보장을 하게 된다.

- 보안원리(Security Principle)

  한 그리드에서 허용되지 않는 자원 접근은 안전한 그리드 간 자원 공유 시에 허용되지 않아야 한다는 원리이다. 이에 대해 본 제안에서는 공유자원을 요청하는 사용자나 그룹은 소속 그리드에서 자신의 자격에 관련해서 접근이 허용되지 않는 자원은 공유자원 접근 시에도 허용되지 않는다. 모든 자원접근제한은 소속 그리드에서 부여한 권한에 의존하고, 여기에 공유자원을 제공하는 그리드의 자원접근제어정책이 반영이 되기 때문이다.

- 자율원리(Autonomy Principle)

  한 그리드에서 허용되는 접근 자원은 안전한 그리드 간 자원 공유 시에도 그대로 허용되어야 한다는 원리이다.

  이에 대해 본 제안은 사용자의 소속 그리드에서 접근 허용이 되는 자원은 기본적으로 공유자원에서도 허용이 된다. 기본적으로 본 제안은 사용자가 속한 그리드의 자원접근제한 정책을 따르기 때문이다. 다만, 공유자원을 제공하는 그리드의 자원관리 특성상 정책적인 제한을 둘 수 있어, 사용자가 소속 그리드에서 획득한 자원이용권한에 일률적인 제한이 가해질 수 있다. 이를 받아들일 것인가 다른 공유자원을 찾을 것인가는 또한 사용자가 결정을 할 수 있는 사항이다. 따라서, 사용자는 공유자원을 제공하는 여러 그리드를 놓고 자신이 원하는 만큼의 자원을 제공하는 그리드의 자원을 사용대가를 지불하고 이용할 수가 있다.

본 논문에서 제안하는 그리드 자원 공유를 위한 통합 자원접근제어 메커니즘은 이상과 같이 임시로 사용할 공유 자원접근제어의 호환성을 보장하는데, 보다 가벼운 메커니즘으로 부담이 적고, 사용자가 소속 그리드 자원을 이용하는 것과 같은 편의를 제공받게 한다.

6. 결 론

본 논문은 통합 그리드 자원 접근제어 메커니즘을 e-Science의 한 응용인 HVEM Grid를 기반으로 제시했다. e-Science 그리드의 닫힌 자원 운영정책은 자발적인 그리드 자원공유를 유인기제로 이끌어낸다고 하더라도 실질적으로는 다른 그리드와의 자원 공유를 힘들게 하는 요소가 된다. 가장 대표적인 걸림돌은 각 e-Science 그리드의 독자적인 자원 접근 제어 정책이다. 중요한 과학 연구 데이타와 장비들이 존재하는 e-Science 그리드에서, 두 그리드 간의 완전한 자원 공유는 공동 연구를 통한 양 그리드 간의 협약으로 장기적으로 이뤄질 수 있다. 그러나, 일반적인 e-Science 그리드의 유휴자원 이용은, 사용자가 속한 그리드에서 가용자원이 없을 때 자발적으로 자신의 자원을 제공하는 타 그리드의 자원을 임시로 이용하는 경우가 된다. 이런 경우는 그리드의 모든 사용자의 자원 접근 정책을 다 알 필요가 없고 두 그리드 간의 자원공유 규약을 유지, 갱신하는 비용을 낭비할 필요가 없다. 따라서, 본 논의에서는 e-Science 그리드 자원 공유를 위해, 각 그리드의 자원 접근 정책을 수용하면서 자원 공유의 용이성을 지원할 수 있는 가볍고, 솔기없는 자격기반자원접근제어 메커니즘을 제안하여, 연구자들의 자유로운 그리드 자원 공유 요구가 만족될 수 있도록 했다.

향후, e-Science 자원 공유를 위한 구체적인 유인기제를 HVEM Grid를 기반으로 연구하고, 자원 공유를 위한 전반적인 인증 보안도 연구할 것이다.

참 고 문 헌

[1] e-Science Definition, http://e-Science.ox.ac.uk/public/general/definitions.xml, *Oxford e-Science Centre*

[2] Foster, I. and Kesselman, C. and Tuecke, S., "The anatomy of the grid : Enabling scalable virtual organizations," *Intl., J. Supercomputer Applications*, 2001.

[3] Globus Toolkit 3.2, http://www.globus.org/toolkit/

[4] Catalin Dumitrescu, Ian Foster and Ioan Raicu, "A Scalability and Performance Evaluation of a distributed Usage SLA-based Broker in Large Grid Environments," Technical Paper, University of Chicago.

[5] Gnutella Protocol, http://www9.limewire.com/developer/gnutella_protocol_0.4.pdf

[6] BitTorrent Guide, http://www.dessent.net/btfaq/

[7] Jian Liang, Rakesh Kumar and Keith W. Ross, "Understanding KaZaA," http://cis.poly.edu/~ross/papers/UnderstandingKaZaA.pdf

[8] SETI@Home: The Search for Extraterrestrial Intelligence Project, http://setiathome.berkeley.edu/

[9] Hyuck Han, Hyungsoo Jung, Heon Y. Yeom, Hee S. Kweon, and Jysoo Lee, "HVEM Grid: Experiences in Constructing an Electron Microscopy Grid," *The Eighth Asia Pacific Web Conference*, Jan. 2006, Harbin, China (Also published in LNCS 3841, pp.1159-1162)

[10] Ricahrd T. B. Ma, Sam C. M. Lee, John C. S. Lui, and David K. Y. Yay, "Incentive Resource Distribution in P2P Networks," *In Proc. IEEE International Conference on Distributed Computing Systems*, 2004.

[11] Oscar Ardaiz, Felix Freitag, Leandro Navarro, Torsten Eymann, and Michael Reinicke, "CatNet - Catallactic Mechanisms for Service Control and Resource Allocation in Large Scale Application-Layer Networks," *Workshop on Global and Peer-to-Peer Computing on Large Scale Distributed Systems, 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid*, 2002.

[12] "CatNet Project," http://research.ac.upc.edu/catnet/

[13] "SORMA Project," http://www.sorma-project.eu/

[14] Alexander Barmouta, and Rajkumar Buyya, "GridBank: A Grid Accounting Services Architecture (GASA) for Distributed Systems Sharing and Integration," *International Parallel and Distributed Processing Symposium (IPDPS'03)*, 2003.

[15] Japan NAREGI project, http://www.naregi.org

[16] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell' Agnello, A. Frohner, A. Gianoli, K. Lrentey, and F. Spataro, "VOMS: an Authorization System for Virtual Organizations," *in 1st European Across Grids Conference*, February 2003.

[17] Ajith Kamath, Ramiro et.al, "User-Credential Based Role Mapping in Multi-domain Environment," *Proceedings of the Privacy, Security, Trust (PST)*, 2006.

[18] Catalin Dumitrescu, Ian T. Foster, "GRUBER: A Grid Resource Usage SLA Broker," *Euro-Par* 2006.

[19] Mohamed Shehab, Elisa Bertino and Arif Ghafoor, "SERAT: SEcure Role mApping Technique for Decentralized Secure Interoperability," *In Proc. ACM Symposium on Access Control, Models and Technologies(SACMAT'05)*, Sweden, June, 2005, Eilat, Israel, (Also published in LNCS 4360, pp. 175-190).

[20] Belokosztolszki, A. and Moody, K., "Meta-Policies for Distributed Role-Based Access Control Systems," *Third International Workshop on Policies for Distributed Systems and Networks*, 2002.

[21] ARM 1300s, 기초과학지원연구원 소속, http://www.kbsi.re.kr

[22] Im Young Jung, In Soon Cho, Heon Y. Yeom, Hee S. Kweon and Jysoo Lee, "HVEM DataGrid: Implementation of a Biologic Data Management System for Experiments with High Voltage Electron Microscope," *Distributed, High-Performance and Grid Computing in Computational*

Biology (GCCB 2006), Jan. 2007.
[23] David F. Ferraiolo and Richard Kuhn, "Role-Based Access Control," *Proceedings of the 15th NIST-NSA National Computer Security Conference*, 1992.
[24] D Ferraiolo, J Cugini, DR Kuhn, "Role based access control : features and motivations," *ACM Transactions on Information and System Security (TISSEC)*, 1995.
[25] DF Ferraiolo, R Sandhu, S Gavrila, DR Kuhn, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, 2001.
[26] L. Gong and X. Qian, "Computational Issues in Secure Interoperation," *IEEE Transaction on Software and Engineering*, Vol. 22, No. 1, Jan., 1996.

정 임 영

1993년 포항공과대학교 화학과 학사. 1999년 서울대학교 전산과학과 학사. 2001년 서울대학교 컴퓨터공학부 석사. 2004년~현재 서울대학교 컴퓨터공학부 박사과정 관심분야는 분산시스템, 분산컴퓨팅, 그리드 컴퓨팅, e-Science 그리드, 시스템 보안

정 은 진

1999년 서울대학교 전산과학과 학사. 2002년 Univ. Texas at Austin 석사. 2006년 Univ. Texas at Austin 박사. 2006년~현재 Univ. of Iowa 조교수. 관심분야는 보안, 분산시스템, 알고리즘, 네트웍

염 헌 영

1984년 서울대학교 계산통계학과 학사 1986년 Texas A&M Univ. 전산학 석사. 1992년 Texas A&M Univ. 전산학 박사. 1993년~현재 서울대학교 컴퓨터공학부 교수. 관심분야는 분산시스템, 결함내성, 운영체제, 데이타베이스 시스템, 그리드 컴퓨팅