한국산학기술학회논문지
Vol. 12, No. 2 pp. 901-908, 2011

안전한 그리드 응용을 위한 정책기반의 보안 기능 설계

조영복[1], 유미경[1], 이상호[1*]
[1]충북대학교 전자계산학과

Design of a Policy-based Security Mechanism for the Secure Grid Applications

Young-Bok Cho[1], Mi-Kyung You[1] and Sang-Ho Lee[1*]
[1]Dpartment of Computer Science, Chungbuk University

요 약 그리드 시스템의 SKY@Home에 적용된 통합 보안 모듈은 보안 기술을 좀 더 보완함으로써 그리드 시스템에 최적화된 보안모듈을 개발함으로써 보안성을 향상시켰다. 그러나, 현재 구현된 통합 보안 모듈은 Firewall, IDS, 바이러스 등을 제공하는 통합 모듈이지만 생성된 로그분석이나 룰 편집이 수작업으로 이루어져 관리자의 역할이 중요하게 작용된다. 따라서 관리자의 작업 처리가 원활하게 이루어지지 않을 경우 자원제공 PC들은 최신의 자료를 업데이트하기가 어렵다. 이러한 문제점을 해결하기 위해서 자료를 자동 갱신 하는 방법을 개선할 필요가 있다. 제안모델의 안전한 그리드 응용을 위한 정책기반 시스템의 자원제공 PC는 통합 보안 모듈을 적용함으로써 외부의 침입으로부터 클라이언트가 손쉽게 보안 기술을 활용하여 대처할 수 있다. 또한 자원제공 PC에서 사용되는 통합 보안 모듈은 추가적인 장비의 구입, 설치, 추가 비용이 없으므로 구현 비용이 현재 사용되는 보안 기술보다 적게 소요된다. 기존 제안 방식에서 제공되는 다양한 기법으로 인한 시스템 자원 낭비를 줄이고자 그리드시스템에 최적화되도록 제안 시스템을 자원제공 PC에 적용함으로써 유효자원이 기존 방식보다 최대 20% 증가할 수 있어 침입탐지 및 예방, 바이러스 치료 등의 절차에 따라 악의적 공격을 대처하는 동시에 시스템의 가용성, 신뢰성, 무결성 및 기밀성이 전체적으로 향상됨을 보였다.

Abstract For the available grid environmental realization, the resource supply PC must have to provide an appropriate security function of their operation environments. SKY@HOME is a kind of the grid computing environments. If this has not supervised by administrator handling smoothly, it is inherently vulnerable state to the security level of the grid environments, because the resource supply PC is not update a security function without delay. It is also have the troublesome problems which have to install of an additional security program for support the appropriate security. This paper proposes an integration security model on the policy-based that provides an update each level according to the situation of the resource supply PC for improving its problems as a security aspect of the SKY@HOME. This model analyzes the security state of the resource supply PC respectively, and then the result is available to provide an appropriate security of the resource supply PC using an integration security model. The proposed model is not need additionally to buy and install the software, because it is provided the security management server oriented service. It is also able to set up the suit security function of a characteristic of the each resource supply PC. As a result, this paper clearly show the participation of resource supply PC improved about 20%.

Key Words : Grid System, P2P, SKY@Home, Grid Security Policy, Grid Agent

---

본 논문은 2009년도 충북대학교 학술 연구 지원 사업의 연구비 지원에 의해 연구되었음
*교신저자 : 이상호(shlee@cbnu.ac.kr)
접수일 10년 12월 10일 수정일 11년 01월 14일 게재확정일 11년 02월 10일

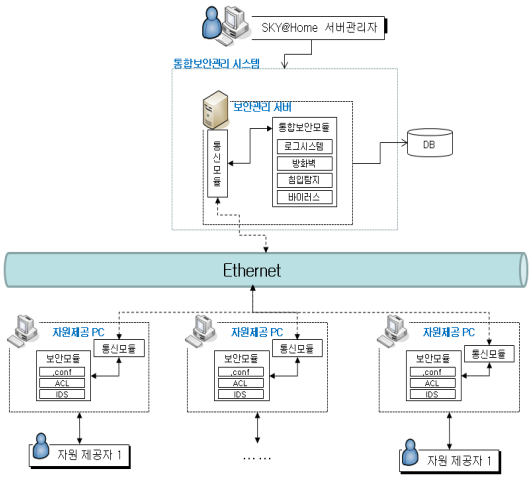
1. 서론

최근 산업사회가 고도화됨에 따라 인터넷상에 존재하는 많은 컴퓨팅 자원을 초고속 네트워크와 연동하여 다양한 분야에 활용하는 그리드 서비스가 각광받고 있다. 그리드 서비스는 자원 활용측면에서 고성능, 대용량의 IT 자원을 충분히 활용할 수 있고, 지역적으로 분산되어 있는 컴퓨터 자원을 이용하기 때문에 매우 효율적인 컴퓨팅 환경이다[1,3,4]. 그러나 일반적인 그리드 환경은 이런 환경을 구성하는 PC들(자원제공 PC)의 안전성을 보장하지 못한다. 자원제공 PC는 인터넷기반 분산컴퓨팅의 불특정 다수로 구성되어 보안 위협이 내 · 외부에 항상 존재한다[1,2,5]. 그러나 자원제공 PC의 관리자는 자신의 자원을 제공하는 입장으로 작업의 신뢰도와 안전성을 보장 받길 원한다. 그리드컴퓨팅 환경에서 신뢰도와 안전성이 보장되지 않는다면 그리드 컴퓨팅을 위한 자원제공 PC의 통신참여율이 낮아지고 유휴자원은 감소하게 된다[6,7,11,12]. 현재 개발된 침입탐지, 감내기술은 주로 보안관리 서버측면에서 활용 가능한 것으로 다양한 기법이 사용되고 있으나, 구현 비용이 높고 많은 장비가 필요하므로 유지보수 및 확장이 용이하지 않은 문제점을 갖는다[8,9,13]. 이와 같은 문제들을 해결하기 위해 이 논문에서는 그리드 컴퓨팅 플랫폼 중 하나인 SKY@Home을 중심으로, 사용자 입장에서 정책기반의 보안기능을 제공함으로 보다 신뢰성이 보장된 그리드 서비스가 가능하도록 하였다. SKY@Home에 적용될 정책기반의 통합보안 모델은 그리드 컴퓨팅에 참여한 자원제공 PC에 방화벽(Firewall), 침입탐지시스템(IDS), 바이러스(Virus)와 같은 보안 프로그램을 자율적으로 정책서버에서 통합관리 지원한다. 또한 각 자원제공 PC의 시스템 환경에 적합한 사용자 중심의 보안정책을 제공한다. 따라서 그리드 컴퓨팅의 신뢰성을 높이고 자원제공PC의 컴퓨팅 참여율을 높였다. 또한 SKY@Home의 데이터 암호화 방식을 부분 암호화 기법을 사용해 전체적인 시스템 효율을 향상시켰다. 이 논문의 구성은 2장에서는 그리드 컴퓨팅 시스템 SKY@Home과 SKY@Home의 보안 취약성, 3장에서는 안전한 그리드 응용을 위한 정책기반의 통합보안모델 설계, 4장에서는 설계된 시스템의 실험 및 평가와 5장에서는 결론 및 향후 연구를 기술한다.

2. 관련연구

2.1 그리드 컴퓨팅 시스템 SKY@Home

그리드(Grid)는 분산되어 있는 컴퓨터들을 네트워크로 연결해 각각의 컴퓨터가 가지고 있는 자원을 공유하는 서비스이다. 국내에서는 정보통신부의 지원으로 한국과학기술정보연구원(KISTI)의 슈퍼컴퓨팅센터를 중심으로 인터넷 기반 분산 컴퓨팅 환경구축사업으로 Korea@Home이 개발 되었다. 이는 단일 컴퓨터로는 수행하기 어려운 대량의 정보처리를 분산 처리를 통해 결과를 얻고자 하는 그리드 미들웨어이다. 이후 MEC KOREA사는 Korea@Home을 기술이전 받아 새롭게 생산한 것이 SKY@Home이다. 이는 트래픽 양 및 서버 의존도 감소, 플랫폼 사용의 편리성을 증대한 그리드 미들웨어로, 시스템 구성은 분산응용 제공자, 플랫폼 서버, 자원제공 PC등으로 구성된다. 자원제공 PC 관점에서 작업처리는 자원제공 PC의 자발적 참여가 기반이 되어야 하며, 초기 웹페이지 접속을 통해 에이전트 프로그램을 다운받을 수 있다. 에이전트는 자원제공 PC에 프로그램 설치 이후, CPU 사용이 없을 때, 서버로 작업 데이터를 요청한다. 에이전트는 서버에서 응용작업을 다운받아 변조여부를 확인 후 분산응용 작업을 수행한다. 응용작업의 결과는 후처리 과정으로 작업결과의 검증 및 압축단계를 거친 후 서버로 업로드 된다. 마지막으로 서버에서는 작업결과의 변조여부 판별과 인증과정을 수행하고, 데이터베이스에 자원정보를 전송해 대용량 응용관리 서버에 저장 된다[8]. 그림 1은 SKY@Home의 구성도를 도식화한 것이다.



[그림 1] SKY@Home의 구성도

2.2 SKY@Home의 취약성

SKY@Home의 분산 컴퓨팅 기술은 국내·외의 우수한 초고속 인터넷 망과 유휴 PC자원의 첨단 연구개발 과정에 활용함으로써 편리성과 효율성을 제공한다. SKY@Home은 보안성을 제공하기위해 기본적으로 인증

서발급 및 폐기기능을 가지며 데이터 전송, 기밀성, 부인봉쇄, 위변조 방지기능을 제공한다. 그러나 이런 보안성 제공을 위해서는 서버관리자에 의한 로그분석과 룰 관리 및 ACL 편집기능을 수행하는 서버관리자에 매우 의존적인 방법으로 동작된다. 기존 SKY@Home처럼 서버 관리자에 의존적으로 자원제공 PC의 보안성을 제공한다면, 그리드 컴퓨팅에 참여하는 유휴자원인 자원제공 PC입장에서는 매우 불안하다. 자원제공 PC는 자신의 컴퓨터를 그리드 컴퓨팅에 일부 사용할 수 있도록 지원하는 과정에서 자신의 컴퓨터가 바이러스나 해킹 툴로 부터 안전하길 바란다. 만약 안전성을 보장받지 못할 경우 자원제공 PC는 불안감으로 그리드 컴퓨팅 참여를 거부하게 되고, 이런 상황이 지속되면 유휴자원이 감소되어 그리드 컴퓨팅 전체의 신뢰성이 감소되는 문제점을 갖는다. 또한 기존 SKY@Home은 보안성을 제공하기 위한 방법으로 암호화작업을 수행한다. 그러나 암호화 작업으로 인한 서버의 부하가 심각한 상태이다. 서버의 부하는 그리드 컴퓨팅의 신뢰도를 감소시키는 요인이 되고 있다.

3. 안전한 그리드 응용을 위한 정책기반의 통합보안 모델설계

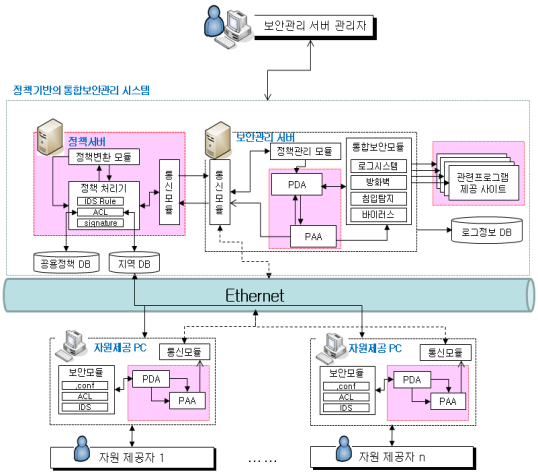
이 절에서는 안전한 그리드 응용을 위한 정책기반의 통합보안 모듈 프레임워크를 설계한다. 정책 기반의 통합보안 모델은 자원제공 PC를 대상으로 서버 관리자와 독립적으로 정책기반의 통합보안 에이전트가 바이러스, 침입탐지 등을 분석하고 각각의 자원제공 PC에 적합한 보안성을 보안 정책에 의해 제공한다.

3.1 통합보안 모델 개요

제안 모델은 보안관리 서버, 정책서버와 다수의 자원제공 PC로 구성된다. 정책 서버(Policy Server)는 공용정책과 지역정책 데이터베이스를 기반으로 자원제공 PC에서 제공될 보안 정책을 설정한다. 보안관리 서버는 자원제공 PC에서 생성된 로그분석, ACL 추가/수정/삭제 등의 기능을 담당하는 정책관리 모듈과 정책서버에 저장된 보안 등급을 유지하기 위한 통합보안 모델의 설치파일을 서비스하는 Policy Decision Agent(PDA)와 Policy Action Agent(PAA)로 구성된다. 또한 보안관리 서버의 통합보안 모듈은 자원제공 PC로 참여한 컴퓨터에 동작되고 있는 보안관련 프로그램의 정보를 관리하며, 자원제공 PC의 보안모듈과 연동되어 주어진 정책에 맞는 보안관련 프로그램을 자동 실행시키는 기능을 수행한다.

3.2 정책기반의 통합보안 모델 설계

정책기반의 통합보안 모델은 기존 SKY@Home를 확장한 모델 그림 2와 같다. 기존 모델에 정책서버와 PDA,PAA 에이전트를 추가하여 서버관리자와 독립적으로 자원제공 PC의 보안상태를 분석하고 주어진 보안정책에 맞는 최소의 보안성을 유지함으로 그리드 컴퓨팅의 유휴자원의 안전성을 보장한다.



[그림 2] 제안 모델 구성도

그림 2와 같이 보안관리 서버의 정책관리 모듈은 자원제공 PC가 통신에 참여시 자원제공 PC의 보안성과 안전성을 확인하기 위해 정책관리 모듈의 PDA가 자원제공 PC의 실행 프로세서를 분석한다. 실행프로세스 확인을 위해 제안 모델에서는 자원제공 PC가 유휴자원으로 참여하면 자동으로 정책관리모듈에서 PDA 에이전트가 실행되어 윈도우 상에 실행되는 프로세스를 확인한다. 실행프로세서 확인은 GetWindowText() 함수를 이용하고 실행프로세서 분석은 CreateToolhelp32Snapshot(), Process32First(), Process32Next()를 사용해 자원제공 PC에서 실행중인 프로세서들을 확인한다. 또한 자원제공 PC를 실시간으로 보안관리 서버에서 방화벽, 침입탐지 프로그램 및 백신 프로그램의 버전을 분석하여 시스템 사양에 적합한 최신 프로그램이 동작되도록 제공한다. 전체적인 처리과정은 다음과 같다.

① 자원제공 PC가 통신 참여를 요청함

② 보안관리 서버의 통합보안모듈이 동작

③ 자원제공 PC의 실행 프로세스 확인(자원제공 PC의 보안 상태 분석)
㉠ 백신버전 확인
㉡ 방화벽 버전 확인
㉢ 침입탐지 버전확인

④ if 자원제공 PC 실행 프로세스 버전 정책서버 rule의 버전보다 낮을 경우
㉠ 백신 사이트 접속 → 버전 업그레이드
㉡ 방화벽 사이트 접속 → 버전 업그레이드
㉢ 침입탐지 사이트 접속 → 버전 업그레이드

⑤ 자원제공 PC실행 프로세스 확인

⑥ 보안관리 서버에게 ⑤결과 전달

3.2.1 보안관리 서버

보안관리 서버는 정책관리 모듈과 통합보안모듈로 구성된다. 정책관리 모듈은 서버관리자와 독립적으로 자원제공PC에서 제공되어야 할 기본적인 보안성을 관리할 수 있도록 PDA, PAA로 구성된 에이전트가 동작된다. 통합보안모듈은 자원제공 PC들의 보안성을 제공하기위해 보안도구의 설치유무를 판단하고, 동작중인 보안프로그램 버전정보를 분석하여 정책서버에서 제시하는 기본적인 보안성이 제공되는지 판단한다. 만약 정책서버에서 정의된 보안수준이하인 경우 통합보안 모듈은 보안프로그램을 제공하는 웹에 접속하여 보안 관련프로그램을 다운로드할 수 있다. 이렇게 설치된 보안 프로그램은 자원제공 PC의 안전성을 제공하기 위해 실시간으로 검색하여 자원제공 PC의 보안성을 유지한다.

3.2.2 정책 서버

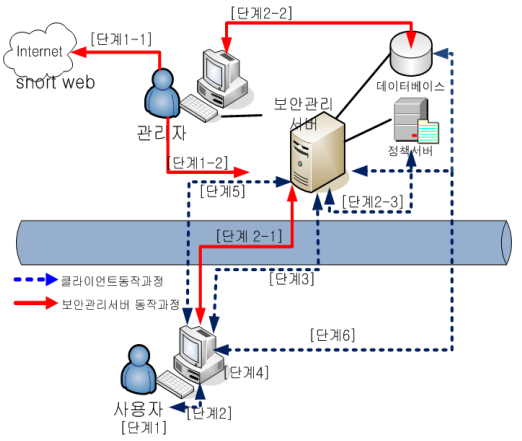
정책 서버는 정책결정이나 처리를 위한 정책 처리기로 구성된다. 정책처리기에서 실시간으로 이더넷 상에 흐르는 패킷을 Pcap 라이브러리의 무작위 모드(Promiscuous Mode)로 Snort를 통해 탐지해 새로운 침입에 대한 룰을 추가하고 자원제공 PC들에게 새롭게 갱신된 룰을 전달한다.

3.2.3 자원제공 PC

자원제공 PC는 보안모듈이 동작되어 자원제공 PC에서 동작중인 IDS 룰 정보와 IDS log 정보를 분석한다. 자원제공 PC는 보안관리 서버의 요청에 의해 통합보안 모듈이 동작되면 자원제공 PC의 정책서버 룰을 기준으로 최신버전 보안 프로그램 설치 및 업그레이드를 수행한다. 자원제공 PC에서 설치 및 업그레이드된 프로그램의 버전정보를 conf파일로 데이터베이스에 전달된다.

3.3 정책기반의 통합보안 모델 동작

보안관리 서버의 정책기반 통합보안 모델의 처리과정은 파일자동 업데이트, 로그분석과 ACL 편집과정, 정책관리로 구성된다. 그림 3는 정책기반의 통합보안 모델의 동작과정을 도식화한 것이다.



[그림 3] 통합보안 모델의 동작과정

그림 3에서 보안관리 서버의 동작과정은 다음과 같다.

[단계 1-1] : 관리자는 snort사에 접속하여 최신파일을 다운로드 받아 이전버전의 파일을 업데이트한 후 보안관리 서버의 보안 파일을 업데이트.
[단계 1-2] : .conf 파일에 있는 IDS.exe버전 정보와 IDS Rule 버전 정보를 업데이트
[단계 2-1] : 자원제공 PC의 IDS 로그를 관리자가 스캔하여 정책서버의 룰 정보와 보안관리 모델의 보안성을 확인. (만약 IDS 로그 분석을 통해 보안 문제가 발생할 경우 발생될 경우 로그를 룰에 추가하고 보안 문제를 해결)
[단계 2-2] : 관리자는 자원제공 PC의 Signature Rule을 통해 서비스를 신규 희망하거나 탈퇴할 경우 PAA는 자원제공 PC의 Signature를 추가/삭제.
[단계 2-3] : 정책서버의 ACL을 추가, 삭제, 수정 할 수 있도록 편집하는 단계로 자원제공 PC의 ACL을 업데이트.

그림 3에서 자원제공 PC의 보안측면의 동작 과정은 다음과 같다.

[단계 1] : 자원제공 PC의 전원 ON.
[단계 2] : 보안관리 서버의 통합보안 모듈의 자동실행.

```
{ m_AutoStartups.reserve( 30 );
  LPCTSTR    lpctszAutorunKeyPath=_T(SOFTWARE₩₩Micro
   soft₩₩Windows₩₩CurrentVersion₩₩Run₩₩");
    m_hLocalMachineAutostartupKey  =  GetRegKey(HKEY_L
     OCAL_MACHINE,lpctszAutorunKeyPath );
    ASSERT( m_hLocalMachineAutostartupKey );
    m_hCurrentUserAutostartupKey = GetRegKey(HKEY_CUR
     RENT_USER,lpctszAutorunKeyPath );
    ASSERT( m_hCurrentUserAutostartupKey );}
```

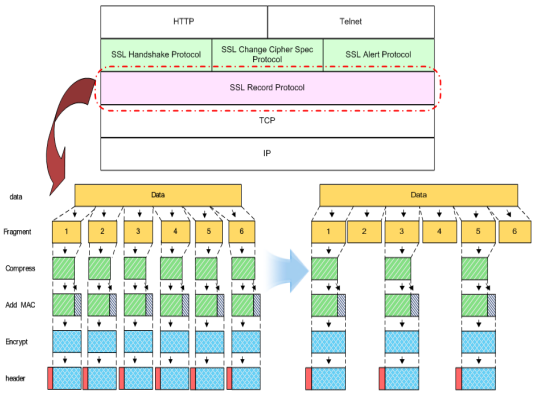
[단계 3] : PDA는 실행중인 프로세스 분석을 통해 실행중인 보안관련 프로그램의 버전확인, 백신실행 여부 등 결과를 PAA로 전달.

```
if (stricmp(pe32.szExeFile, szPath) == 0){
  HANDLE hProcess == NULL;
  if(hProcess==OpenProcess(PROCESS_TERMINATE,  FALSE,
    pe32.th32ProcessID))    {
          TerminateProcess ( hProcess, 0 );
          CloseHandle ( hProcess );     }}
```

[단계 4] : PAA는 분석결과를 기반으로 패치정보가 존재할 경우 패치하고 방화벽과 침입탐지 프로그램을 자동 실행.
[단계 5] : 사용자의 이벤트 처리를 통해 필요한 보안관련 프로그램의 설치 및 업그레이드 실행한 후 conf파일의 버전정보를 업데이트
[단계 6] : 종료명령과 함께 로그 이벤트를 저장 후 보안관리 서버로 전달하여 자신의 로그정보 삭제.

3.4 SKY-SSL부분암호화

기존 SKY@Home은 데이터 암호화/복호화에 따른 시스템 부하가 가중되어 시스템 자원을 효율적으로 관리하기 어렵다. 또한 암/복호화를 사용하기위해서는 openSSL 라이브러리를 별도로 설치하도록 요구한다. 따라서 제안 논문에서는 모든 데이터는 짧은 전송처리 시간과 시스템 부하를 낮출 수 있는 방으로 부분 암호화 방법을 적용하였다. 암호화 되지 않은 데이터의 일부분은 XOR연산을 통해 보안성을 보장한다.



[그림 4] 부분암호화 방법

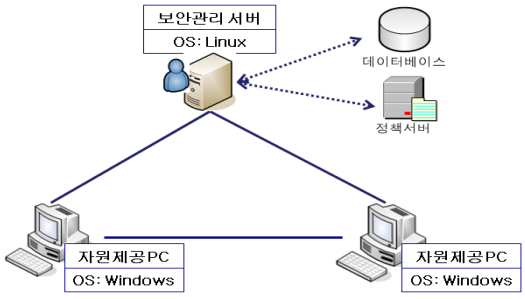
그림 4는 부분 암호화 방법으로 난수를 통한 랜덤비트열에 따라 암호화 데이터와 비암호화 데이터를 분류하여 전송함으로 평문전송시보다 빠르게 데이터 전송이 가능하여 그리드 컴퓨팅 환경의 효율성을 향상시킨다.

4. 평 가

제안 모델의 효율성과 안전성 및 기술개발의 타당성을 검증하기 위해 다음과 같은 실험환경을 구축하고 실험운영을 통한결과를 기반으로 평가한다.

4.1 운영 환경

운영 환경은 그림 5와 같이 개선된 정책기반의 통합보안모듈이 장착된 SKY@Home을 위한 플랫폼 구축을 위해 보안관리 서버와 데이터베이스, 정책 서버 및 자원제공 PC들로 구성한다.



[그림 5] 보안관리 서버와 자원제공 PC간 동작 모델

그림 5의 운영 환경은 SKY@Home을 위한 플랫폼 구현을 위해 표 1과 같이 구성한다.

[표 1] 운영환경

	보안관리 서버	데이터베이스	정책 서버	자원제공 PC1	자원제공 PC2
수량	1	1	1	1	1
OS	Fedora 2.6.18-1	MySQL	WS 2000	Windows XP	Windows XP
컴파일러	GCC4.1.1	×	×	×	×
메모리	2G	2G	1G	1G	512M
CPU	3.0	-	3.0	3.0	2.6
XYSSL	0.9	-	0.9	0.9	0.9
포트	6001	6001	6001	6001	6001

실제 그리드 환경에서는 자원제공 PC로 참여하는 각 컴퓨터들의 환경이 서로 다르게 구성된다. 따라서 실험환경에서 자원제공PC의 환경을 서로 다르게 구성하였다. 또한 서로 다른 환경의 자원제공 PC에 적합한 보안정책을 실행할 수 있도록 실험 환경을 구성하여 운영한다.

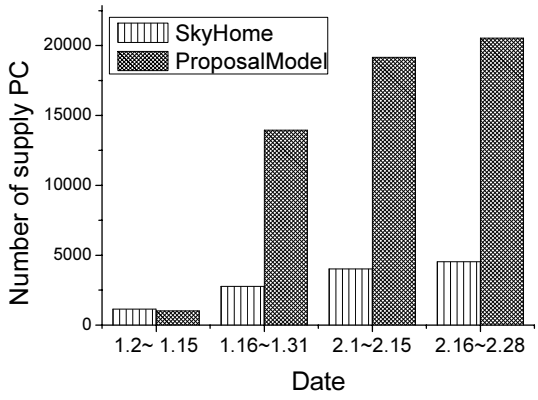
4.2 운영

(주)MEC코리아는 테스트베드를 기존 Sky@Home 그리드환경과 정책기반의 보안관리 서버를 이용한 그리드 환경을 구축하여 (주)MEC코리아 오창 그리드연구소에서 2009년 1월2일~2월 28일까지 설치 운영하였다. 운영은 기존 Sky@Home서버와 정책기반의 보안관리 기능이 탑재된 제안 모델을 구현하여 운영하였다. 표 2는 각 기간별로 그리드 컴퓨팅에 자원제공 PC로 참여한 그리드 컴퓨팅 참여율을 조사한 결과이다.

[표 2] 자원제공 PC의 참여율

구분 / 일자	Sky@Home 서버	정책기반의 통합 보안관리 서버	참여율
1.2~ 1.15	1,145대	1,351대	18%
1.16~1.31	2,769대	3,946대	19%
2.1~2.15	4,021대	21,165대	19%
2.16~2.28	4,724대	20,543대	23%

운영기간 중 그리드 환경에 참여하는 자원제공PC의 참여율을 분석한 결과 표 2과 같다. 자원제공 PC의 참여율은 정책기반의 보안관리 서버를 이용한 그리드 환경이 기존 Sky@Home 서버보다 평균 20%향상 되었다. 또한 자원제공 PC의 관리자의 도움 없이 자원제공 PC의 보안 프로그램을 자동 업데이트를 통해 안전성을 높여 자원제공 PC로부터 신뢰성을 확보했기 때문이다. 그림 6은 자원제공 PC의 기간별 통신 참여율을 도식화 한 것이다.



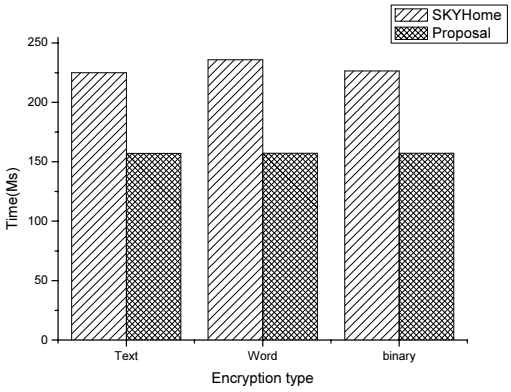
[그림 6] 자원제공 PC의 통신 참여율

표 2와 같은 환경을 운영할 때 기존 Sky@Home과 제안 모델에서 전송 데이터를 전체암호화해서 전달하는 방법과 부분 암호화 알고리즘을 사용해 전달될 때 데이터 전송 시간을 표 3으로 나타낸 것이다.

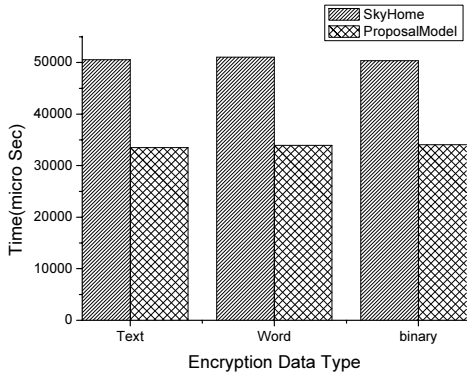
[표 3] 전체암호화와 부분암호화의 데이터 전송 시간

		sky@home		제안방식	
		16K	2MB	16K	2MB
server	Text	225.0	50567.4	157.0	33495.6
	Word	235.8	51032.4	157.2	33959.8
	binary	226.4	50378.8	157.2	34036.6
client	Text	257.2	58076.4	195.0	39048.8
	Word	255.0	61664.4	195.0	40133.8
	binary	255.6	59306.6	195.2	39857.0

그림 7과 그림 8은 제안 방법과 기존 방법에서 데이터 암호화시 소요되는 시간을 도식화 하여 나타낸 것이다.



[그림 7] 16K 데이터암호화



[그림 8] 2MB 데이터암호화

실험결과 전체 암호화보다 부분 암호화를 통해 데이터를 전달하게 되면 16K 데이터의 경우 약 24%, 2MB 데이터의 경우 약 32% 데이터 전달시간이 빠르다. 실험 결과와 같이 전체데이터암호화를 위한 서버 부하를 부분 암호화를 사용함으로 서버부하를 줄임으로 전체 그리드 컴퓨팅의 신뢰성을 향상시킨다.

4.3 평가

정책기반의 통합보안 모델은 기존 SKY@Home 시스템에서 제공받지 못했던 보안문제를 해결함으로써 보다 안전한 SKY@Home 플랫폼을 제공한다. 표 2는 SKY@Home과 정책기반의 통합보안 모델의 기능을 각 보안관리 서버와 자원제공 관점에서 비교 분석한 결과를 보여준다. 정책기반의 통합보안 모델은 기존 SKY@Home보다 안전하게 자원제공 PC를 통신에 참여시키고, 참여하는 자원제공 PC들마다 각 환경에 맞는 보안정책이 적용됨으로써 더 높은 신뢰 수준으로 자신의 PC를 그리드 시스템에 참여 시킬 수 있다.

5. 결론 및 향후 연구

정책기반의 통합보안 모델은 SKY@Home 플랫폼에서 자원제공 PC의 보안관련 프로그램을 통합적으로 관리함으로 보안에 대한 부담을 줄이고, 각 PC마다 서로 다른 수준별 보안정책을 운영 관리할 수 있도록 지원한다. 정책기반의 통합보안 모델은 그리드 환경의 자원제공 PC를 외부 침입으로부터 안전할 수 있도록 보안기술을 활용하여 대처할 수 있고, 각 자원제공 PC마다 수준별 보안정책을 제공한다. 또한 제안모델은 추가적인 장비의 구입, 설치, 추가비용 없이 현재 사용되는 시스템에 이식이 가능하다. SKY@Home 플랫폼에서 정책기반의 통합보안 모델을 사용할 경우, 자원제공 PC의 참여율을 기존방식보다 최대 20% 증가하였다. 정책기반의 통합보안 모델은 침입탐지 및 예방, 바이러스 치료, 방화벽 등의 절차에 따라 악의적 공격에 빠른 대처와 예방이 가능하고, 동시에 시스템의 가용성, 신뢰성, 무결성 및 기밀성 측면에서도 안전하기 때문이다. 향후 각 자원제공 PC마다 수준별 정책 설정을 효율적으로 지원할 수 있는 방안 등에 대한 연구가 수행되어야 할 것이다.

참고문헌

[1] 허의남, “글로벌 신경망, 그리드(GRID) 기술,” Oracle Korea Magazine vol.39 no.3, pp.38-45, 2004.

[2] 윤훈주, “유비쿼터스와 그리드컴퓨팅,” 경영과컴퓨터 통권345호 pp.127-129, 2005.

[3] 함재균, 명훈주, 김형진, 이종숙 , “웹 서비스를 통한 그리드의 진화,” 인터넷정보학회지 제6권 제2호 ,pp.53-60, 2005.

[4] Srisan E and Uthayopas P,"Heuristic Scheduling with Partial Knowledge under Grid Environment", Proc, of the 2nd International Symposium on Communications and Information Technology, pp144-453, 2002

[5] TTA, “The Evolution from Open Grid Service Infrastructure to Web Service Resource Framework,” TTA Standard, pp 56-62 Dec. 2005.

[6] I.Foster. C,Kesselman and S. Tuecke,"The Anatomy of the Grid:Enabling Scalable Virtual Organizations", Jourral of the International Supercomputer Applications, vol. 15, no. 3, pp 200-222. 2001.

[7] I. Foster, C. Kesselman, "Globus: A Metacomputing Infrastructure Toolkit" Intl. J. Supercomputer Application, 1997.

[8] S.Venkataramaiah and J.Subhlok,"Performance Estimation for Scheduling on Shared Networks," Proc of the 9th Workshop on Job Scheduling Stategies for Parallel Processing, pp 148-165, Jun 2003.

[9] I. Foster, C. Kesselman, , "The Globus Project : A Status Report" Computers and the humanities Volume 9, Number 6, pp 291-298, 2006.

[10] 김주한, “웹서비스 보안 기술의 표준화 및 시장 동향,” 전자통신동향분석, 제20권 제1호, 2. pp.43-53, 2005.

[11]강경우, 박형우, “Grid 연구 개발 동향” , 한국정보과학회지 20권 2호 pp.25-30, 2002.

[12] Yuri Demchenko “Security Architecture for Open Collaborative Environment,” LNCS 3470, pp 1011-1302, Feb. 2005.

[13] 김상대, 김승우 퍼지 방위각 추정기를 이용한 세 개의 전 방향 바퀴 구조의 이동로봇시스템의 개발” 한국산학기술학회논문지 v11,n10. pp 3873-3879. 2010.

[14] 김진수, “무선 센서 네트워크에서 에너지 소모 모델의 임계값을 고려한 클러스터링 기법”, 한국산학기술학회 논문지 v11.no10. pp 3950-3957. 2010.

조 영 복(Young-Bok Cho) **[정회원]**

- 2006년 2월 : 충북대학교 전자계산학과 (이학석사)
- 2006년 3월 ~ 현재 : 충북대학교 전자계산학과 박사과정

<관심분야>
센서네트워크, 라우팅, 클러스터링, 정보보안

유 미 경(Mi-Kyung You) **[준회원]**

- 1987년 2월 : 부산대학교 공과대학 전자공학과 (공학학사)
- 2010년 3월 ~ 현재 : 충북대학고 전자계산학 석사과정

<관심분야>
무선 센서네트워크, 보안, 정보통신

이 상 호(Sang-Ho Lee) **[정회원]**

- 1989년 2월 : 숭실대학교 대학원 전자계산학과 (Ph. D)
- 1981년 2월 ~ 현재 : 충북대학교 전자정보대학 교수

<관심분야>
컴퓨터 네트워크, 정보보호, 데이터 통신