# 그리드환경에서 RFID 프라이버시 보호를 위한 확장성있는 태그판별처리 모델 구현

신명숙*, 이준*

# Implementation of Tag Identification Process Model with Scalability for RFID Protecting Privacy on the Grid Environment

Myeong Sook Shin*, Joon Lee*

**요 약**

최근 RFID 시스템의 채택이 다양한 분야에서 빠르게 진행되고 있다. 그러나 RFID 시스템의 대중화를 위해서는 RFID 태그의 정보를 무단으로 획득함으로써 발생할 수 있는 프라이버시 침해 문제를 해결해야 한다. 이 문제를 해결하기 위해서 기존 연구들 중에서 가장 안전한 M. Ohkubo 등의 Hash-Chain 기법이 있다. 그러나 이 기법은 태그를 판별할 때 엄청난 태그 수의 증가로 인해 막대한 계산 능력을 요구하는 문제점이 있다. 따라서 본 논문에서는 프라이버시 보호를 유지하면서 태그판별시간 절감을 위해서 Hash-Chain 기법을 분석하여 그리드 환경으로의 이식한다. 또한 노드별로 SP들을 균등하게 분할하는 태그판별처리 모델을 제안하여 구현하고자한다.

**ABSTRACT**

Recently RFID system has been adopted in various fields rapidly. However, we ought to solve the problem of privacy invasion that can be occurred by obtaining information of RFID Tag without any permission for popularization of RFID system To solve the problems, it is Ohkubo et al.'s Hash-Chain Scheme which is the safest method. However, this method has a problem that requesting lots of computing process because of increasing numbers of Tag. Therefore, in this paper we apply the previous method into the grid environment by analyzing Hash-Chain scheme in order to reduce processing time when Tags are identified. We'll implement the process by offering Tag Identification Process Model to divide SPs evenly by node.

Key Word : RFID, Computational Grid, MPICH-G2, Privacy Protection, Hash-Chain Scheme

## Ⅰ. 서 론

RFID가 산업 전반에 걸쳐 다양하게 적용되기 시작하면서부터 프라이버시에 대한 중요성이 크게 증가되고 있다. 현재 사용되고 있는 RFID[1]는 RFID 시스템이 가지고 있는 특성으로 인하여 사용자 프라이버시 문제[2]를 발생시킨다. 이러한 RFID 시스템에서 프라이버시 침해 문제를 해결하기 위해서는 보안 요건들, 즉 기밀성, 불구분성, 전방 보안성을 모두 만족해야 한다. 또한

* 조선대학교 전자정보공과대학 컴퓨터공학부
(msshin@hanafos.com)

접수일자 : 2009.02.20
완료일자 : 2009.03.13
접수번호 : KIIECT2009-01-16

프라이버시 보호 기법을 적용하게 될 때, 백엔드 서버에서 보장해야 하는 필수 요건은 확장성이다. 확장성이란 처리해야 되는 전체 태그의 개수가 급격히 늘어난다 해도 적절한 시간 안에 태그 판별 작업을 완수할 수 있어야 한다는 의미이다. 일반적으로 프라이버시 보호 기법을 설계하는데 있어서, 안전성을 조금 더 높여주기 위해서는 백엔드 서버에서 처리해야 하는 계산량을 더욱 많이 늘려 주어야 한다. 그러나 백엔드 서버의 계산량이 어느 정도 이상 많아지게 되면 태그를 실시간으로 판별하는 것이 불가능해지기 때문에, 백엔드 서버의 성능 측면에 대한 고려가 반드시 이루어져야만 한다. 따라서 컴퓨터 및 네트워크 성능이 향상됨에 따라 지역적으로 분산되어있는 고성능의 컴퓨터자원의 공유를 통해서, 대규모의 데이터를 계산 처리할 수 있는 방법에 초점을 모으고 있다.

기존 연구들 중에서 프라이버시 보호를 위해 저가의 태그를 이용한 RFID 시스템 환경에서 가장 안전한 기법으로 M. Ohkubo 등의 Hash-Chain 기법[3]을 이용하였다. 그러나 이 기법은 백엔드 서버에서 태그 ID를 판별하기 위하여 모든 태그에 대한 정보를 가지고 순차적으로 판별 과정을 수행한다. 실제로 태그 수의 증가로 인해 막대한 계산 능력을 요구하는 문제점을 가지고 있다. 여기에서 m*n Hash-Chain 계산 테이블에서 해시 시드 값 $s_{1,1}, s_{2,1}, \cdots s_{m,1}$을 SP(Startpoints)라고 하고 n번 연산을 마친 마지막 값, $s_{1,n}, s_{2,n}, \cdots s_{m,n}$을 EP(Endpoints)라고 가정한다.

따라서 기존 계산 작업의 한계를 극복하기 위한 대안으로 지리적으로 분산되어 있는 고성능 컴퓨팅 자원을 네트워크로 상호 연동하여 조직과 지역에 관계없이 가상 집합체들의 자원을 공유하여 대량의 태그 처리를 수행할 수 있는 계산 그리드(Computational Grid)[4]로의 이식 작업이 필요하다.

본 논문에서는 프라이버시 보호를 유지하면서 이러한 대량의 계산 작업을 수행하기 위해서 Hash-Chain 기법의 병행성을 분석하여 계산 그리드 환경으로 이식함으로써 노드별로 SP들을 균등하게 분할하는 태그판별처리 모델을 제안하여 구현한다.

## II. 관련 연구

본 장에서는 RFID 프라이버시 보호를 위한 계산 그리드 환경의 태그판별처리 모델에 적합한 연구들을 소개한다.

### 1. Hash-Chain 기법

M. Ohkubo 등이 제안한 기법[3]으로 그림 1과 같이 일방향 해시 함수를 사용하여 안전한 프라이버시 보호가 보장되는 기법이다.

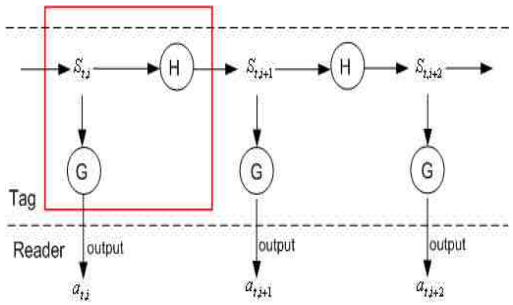


그림 1. Hash-Chain 기법
Fig. 1. Hash-Chain Scheme

백엔드 시스템에는 $ID_t$와 해시 시드 값 $s_{t,1}$이 저장되며 태그에도 동일한 $s_{t,1}$값을 저장하고, 두 개의 해시함수 $H$와 $G$로 구현한다. 리더의 질의에 대해 태그는 $a_{t,i} = G(s_{t,i})$를 수행하여 리더에게 응답하며 자신의 시드 값인 $s_{t,i}$는 $H(s_{t,i})$를 통해 $s_{t,i+1}$ 로 갱신한다. 그러나 이 기법은 서버에서 태그를 판별하기 위한 계산량이 많다는 문제점이 있다.

### 2. 그리드 컴퓨팅

그리드 컴퓨팅[5]은 지리학적으로 분산되어

있는 고성능 컴퓨팅 자원을 네트워크로 연동하여 조직과 지역에 관계없이 가용할 수 있는 컴퓨팅 환경을 말한다. 그리드 시스템은 계산 그리드와 데이터 그리드, 엑세스 그리드로 나눌 수 있다. 계산 그리드는 분산되어 있는 고성능 컴퓨팅 자원을 연결하여 실행함으로써 지금까지 불가능하였던 연구를 수행할 수 있는 환경을 제공하고 High-Throughput 계산 환경을 구축하기 위한 고성능 컴퓨팅 자원을 통합하는 기술이다. 데이터 그리드는 한 곳에 집중된 대량의 데이터를 효율적으로 공유하고, 여러 곳에 분산되어 있는 대량의 데이터 및 데이터베이스에 실시간으로 접근하기 위하여 단계적이고 체계적으로 데이터를 접근 할 수 있게 해주는 기술이며, 액세스 그리드는 동일 분야 연구자들의 공동 연구나 정책 결정을 위한 다양한 분야 연구자들이 원격지에서 접근하여 의견을 교환하고 협력할 수 있는 고성능 협업 환경을 구축하는 기술이다.

3. Globus Toolkit

Globus는 지리적으로 분산된 이종적인 컴퓨팅 자원들을 하나의 가상 컴퓨터처럼 사용 가능할 수 있도록 하는 소프트웨어 기반 구조를 제공한다.

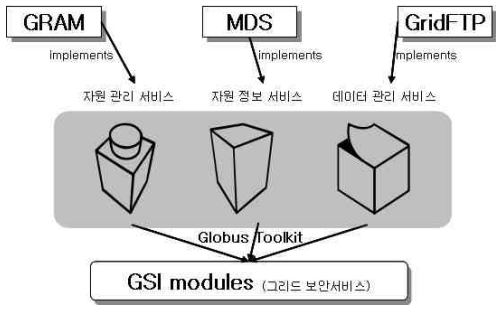


그림 2. Globus 구성 요소

Fig. 2. Globus Configuration Element

Globus 구성 요소는 그림 2와 같이 플랫폼에 직결된 GRAM, MDS, GridFTP, GSI 등 핵심 서비스만 제공하고 응용 프로그램이 자신의 목적에 필요한 서비스를 선택/조합함으로써 다양한 형태의 응용프로그램 및 패러다임 지원한다. 또한 지리적으로 분산된 컴퓨팅 자원들을 하나의 가상 컴퓨터처럼 사용할 수 있도록 소프트웨어 기반 구조를 제공한다.

4. MPICH-G2

MPICH-G는 MPI에 Globus가 제공하는 서비스를 가미함으로서 그리드 컴퓨팅에서의 병렬 프로그래밍 환경의 기초를 구성하였으나, 성능이 기존에 사용하던 벤더들의 MPI에 비해 현저하게 떨어지는 단점이 있어 널리 사용되기에는 큰 부족함이 있었다. 그 후 성능의 향상에 초점을 맞추어 지속적인 연구를 거듭하여 MPICH-G2(Grid-enable MPI Chameleon 2)를 개발하였으며 MPICH-G2는 성능면에서 일반 벤더들의 MPI에 뒤떨어지지 않는다. MPICH-G2는 MPICH-G와 마찬가지로 Globus가 제공하는 많은 서비스를 이용하고 있지만 MPICH-G에서 사용되었던 Nexus를 제거함으로써 많은 성능을 향상 시켰다. Nexus는 여러 개의 프로토콜을 지원하고 자동적인 Data의 변환을 지원하는 등 여러 가지 매력적인 기능으로 오랫동안 MPICH-G의 통신 기반 구조로 사용되었지만 그 외 여러 가지 향상시켜야하는 기능들에 대한 문제로 제거 되었다. MPICH-G2는 모든 통신을 직접적으로 다루도록 재 구현 하였고 이를 통해 Nexus를 사용했을 때 보다 큰 성능의 향상을 가져 왔다[6].

## III. 제안된 방법

기존의 Hash-Chain 기법은 안전한 보안성이 보장되지만 분산 환경에서 엄청난 태그 수의 증가로 인해 막대한 계산 능력을 요구하는 문제점이 있다. 이러한 문제점을 해결하기 위해서 Hash-Chain 기법의 병행성을 분석하여 그리드 환경으로 이식하고, SP들을 균등하게 분할하는 태그판별처리 모델을 제안한다.

1. 그리드 환경으로의 이식

RFID 프라이버시 보호를 위해 적용한 Hash-Chain 기법은 그림 3과 같이 하나의 태그를 판별하기 위한 계산에서, 백엔드 시스템에서는 모든 $1 \leq t \leq m$와 $1 \leq i \leq n$에 대해서 $a'_{t,i} = G(H^{i-1}(s_{t,1}))$를 계산한다.

Hash-Chain 기법에서 SP로부터 EP를 계산하는 과정은 그림 3과 같이 서로 다른 SP에 대해 독립적이다. 즉, 서로 다른 SP로부터 EP를 계산하는 과정에서 서로 간섭이나 종속성이 전혀 없으므로 이 과정은 동시에 수행될 수 있다. 또한 태그 판별 과정도 서로 종속성이 없이 독립적이다.

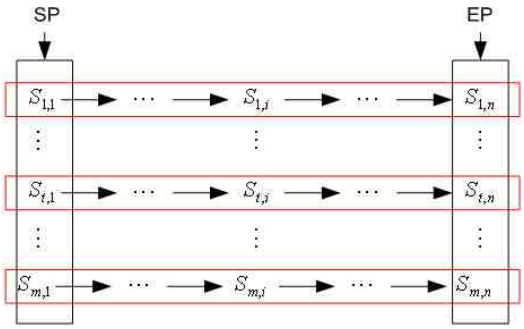


그림 3. 서로 다른 SP에 대해 독립적
Fig. 3. Independence from mutually different SP

본 논문에서는 태그 판별을 위해 막대한 계산 능력을 요구하기 때문에 계산 그리드를 활용하기에 적합하다. 계산 그리드를 이용하여 문제를 해결하기 위해서 소요되는 시간 단축을 위해서 제기된 문제의 병행성을 충분히 분석하여 동시에 수행될 수 있는 작업으로 분할할 수 있어야 한다. 또한 계산 그리드를 이용하여 문제를 해결하기 위해 서는 제기된 문제의 병행성을 분석하여 k개의 노드로 SP들을 균등하게 분할한다. 이를 식으로 나타내면 식 (1)과 같다.

$$SP[i] = \frac{m}{k} \quad (1)$$

여기서 SP[i]는 분할된 SP들의 총수이고, m은 전체 태그 개수이다. 또한 k는 노드 수이며 i는 {1, 2, 3…k}이다. 동시에 수행될 수 있는 노드 수가 많을수록 그리드의 활용도는 높아진다. 그림 4는 계산 그리드 환경에서 k개의 노드로 SP들이 균등하게 분할되는 방법을 나타낸다.

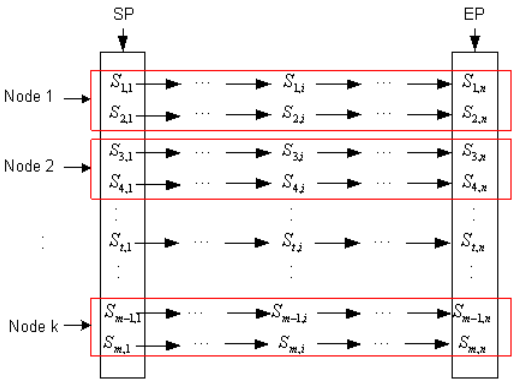


그림 4. 동일한 크기에 따른 균등 분할
Fig. 4. Even Division with Same Size

### 3. 태그판별처리 모델

그리드 환경의 태그판별처리 모델은 그림 5와 같이 역할에 따라 Master와 Slave로 구성된다. Salve는 태그를 판별하는 역할을 한다. Master는 Slave에게 수행할 SP를 균등하게 할당하여 Slave로 전송하고 Slave로부터 생성된 결과를 수집하는 역할을 한다. 즉 Master는 Slave를 관리하는 역할을 한다. 또한 각각의 시스템의 운영체제는 RadHat Linux, 미들웨어는 Globus Toolkit과 MPICH-G2를 탑재하여 사용한다. Master와 Slave 사이는 LAN을 통해 연결되며 메시지 교환을 위해서는 MPI_Recv()와 MPI_Send() 함수를 이용한다.

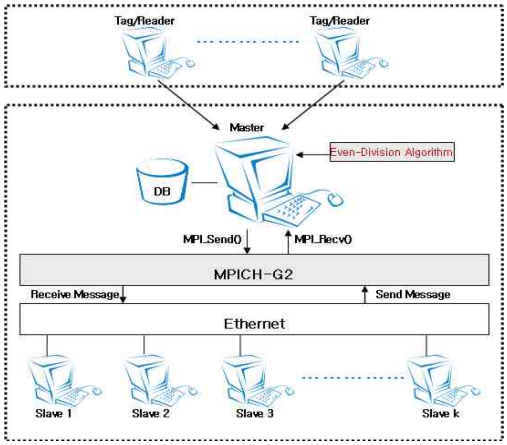


그림 5. 그리드 환경의 태그판별처리 모델
Fig. 5. Tag Identification Process Model of Grid Environment

그림 6은 그리드 환경에서 태그를 판별하는 태그판별처리 모델의 전체적인 흐름을 나타낸다.

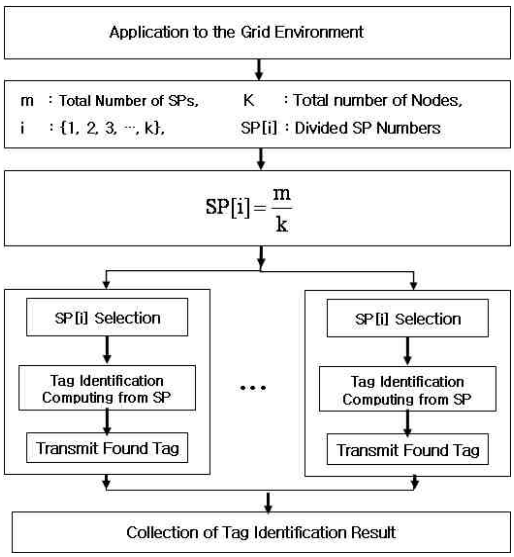


그림 6. 태그판별처리 모델 흐름도
Fig. 6 Flowchart of Tag Identification Process Model

위에서와 같이 백엔드 서버에서의 태그판별시간을 단축하기 위해서는 SP들의 작업을 그리드 환경으로 이식하고 각 노드별로 동시에 수행함으로써 대량의 SP들을 처리할 때 태그판별처리 시간을 단축할 수 있는 모델을 제공한다.

## Ⅳ. 실험 및 분석

### 1. 실험 환경

성능평가를 위한 실험 환경은 표1과 같이 구성된다.

표 1. 구현을 위한 하드웨어 및 소프트웨어 환경
Table. 1 Environment of Software and Hardware for Implement

| 항 목 | | 내 용 |
|---|---|---|
| 하드웨어 | Master | Intel Xeon 5130 2.0G, dual core 4.0GB |
| | Slave1 | Pentium4 2.4G 512M |
| | Slave2 | Pentium4 3.0G 512M |
| | Slave3 | Pentium4 2.8G 512M |
| | Slave4 | Intel Xeon 5130 2.0G, dual core 4.0GB |
| 소프트웨어 | 운영체제 | RadHat Linux 9.0, 커널버전 : 2.4.20-8) |
| | 미들웨어 | Globus Toolkit 2.2.2 |
| | MPI | MPICH-G2 |
| | 언 어 | C |

여기서 제안 모델은 Master와 Slave로 구성된다. Master 역할을 하는 기계는 Intel Xeon 5130 2.0G, dual core 4.0GB 기계를 사용한다. Master와 Slave는 LAN을 통해 연결되며 Hash-Chain 연산을 하여 태그를 판별하는데 이용한다. 그리고 Hash-Chain 연산에 사용한 일방향 해시 함수는 128bit의 md4, md5를 이용하였으며 검색 방법은 순차 검색을 이용하였다. 또한 그리드 환경에서 메시지 전달은 Master와 Slave 사이의 통신을 위해서 필요하다. 본 논문에서는 Master와 Slave 사이의 통신을 위해 MPICH-G2를 이용하였으며 MPI_Recv()와 MPI_Send() 함수를 이용하여 메시지 교환을 한다.

RFID 태그의 샘플 데이터는 16byte의 시드 값을 갖는 임의의 데이터를 생성하여 사용한다. 전체 태그의 개수 $m$ 즉 SP들을 1000, 2000, 3000, 4000개로 증가시키면서 실험하였고 Hash-Chain

의 길이 $n$은 1000으로 실험하였다. 성능평가 방법은 Hash-Chain 길이(n)은 고정된 상태에서 SP들의 개수와 노드 수를 증가하면서 태그판별시간을 평가하였다. 단 테스트는 각각 100번씩 수행하여 평균으로 산출하였다.

2. 실험 결과

본 논문에서 Hash-Chain 길이(n)는 고정된 상태에서 SP들의 총수를 증가하면서 노드 수 별로 태그판별시간을 평가하였다. SP들의 총수에 따른 수행결과는 그림 7과 같으며, 그림 8은 노드 수에 따른 수행결과를 나타낸다. 이 때 SP들의 총수와 노드 수가 증가할수록 큰 폭으로 태그처리시간이 감소되는 것을 구현 결과를 통해 비교하였다.

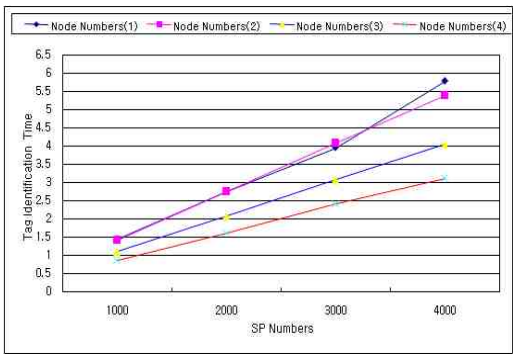


그림 7. SP들의 총수에 따른 수행 결과

Fig. 7 Implement Result by the Total Number of SPs

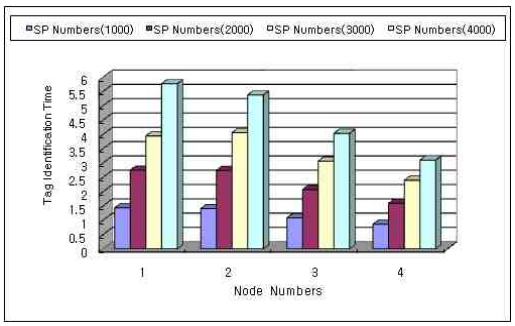


그림 8. 노드 수에 따른 수행 결과

Fig. 8 Implement Result by Node Numbers

본 절에서는 수행시간을 단축하기 위한 방법으로 SP들을 균등하게 분할하는 그리드 환경을 구성하여 다중 노드에서 동시에 수행함으로써 태그판별시간을 단축하였다.

## V. 결론 및 향후 연구

본 논문에서는 프라이버시 보호를 위해 RFID 태그에 적용한 Hash-Chain 기법의 병행성을 분석하여 그리드 환경으로 이식함으로써 노드별로 SP들을 균등하게 분할하는 태그판별처리 모델을 제안하여 구현하였다.

RFID 시스템에서 프라이버시 침해 문제를 해결하기 위해 사용한 Hash-Chain 기법은 백엔드 서버에서의 많은 계산량으로 인해 태그판별시간에 많이 걸리는 문제점 때문에 실제로 활용되기에는 어려움이 있다. 본 논문에서는 이러한 문제의 해결을 위해 먼저 Hash-Chains이 서로 독립적으로 계산이 가능하다는 점을 이용하였다. 또한 태그를 판별하는 과정도 서로 다른 SP들에 대해서 전혀 종속성이 존재하지 않는 점을 이용하여 그리드 환경으로 이식하였다. 따라서 k개의 노드로 m/k개의 해시 시드 값 즉 k개의 노드로 SP들을 균등하게 분할하는 태그판별처리 모델에 적용하여 구현하였다.

구현 결과 Hash-Chain 길이 1000으로 고정된 상태에서 SP들의 개수를 1000, 2000, 3000, 4000으로 증가시키고, 노드 수를 2, 3, 4로 확장하면서 단일 노드에서의 결과와 비교하였다. 성능 결과의 수치 표현을 위해서 노드 수를 4로 고정시키고 SP들의 개수를 1000, 2000, 3000, 4000으로 증가시키면서 단일 노드와 비교하면 각 40%, 42%, 39%, 46%로 성능이 향상되었다. 또한 SP들의 개수를 4000으로 고정시키고 노드 수 2, 3, 4로 확장하면서 단일 노드와 비교하면 각 7%, 30%, 46%로 성능이 향상되었다. 이는 SP들의 개수와 노드 수가 증가할수록 성능이 향상됨을 알 수 있었다.

본 논문에서는 안전한 프라이버시 보호를 위해서 RFID 태그에 Hash-Chain 기법을 이용하

였으며, 태그를 판별하기 위해서 노드별로 SP들을 균등하게 분할하는 태그판별처리 모델을 제안하였다. 이 모델을 구현함으로써 SP들의 개수와 노드 수가 증가할수록 태그판별처리 시간이 감소됨을 보였다. 그러나 이질적인 시스템으로 구성되는 그리드 환경의 특성을 고려하지 않고 작업을 동일한 크기로 분할할 경우 성능을 극대화 시킬 수 없는 한계점이 발생한다. 앞으로의 연구 방향은 그리드 환경으로 구현하는데 있어서 성능을 최적화하기 위한 방법을 연구해 나갈 생각이다.

## 참 고 문 헌

[1] Willam P. Walsh, Research and application of RFID Technology to enhance aviation security, IEEE, 2000.

[2] S. Sarma, S. Weis, D. Engles, "RFID Systems and Security and Privacy Implication," In CHES, vol. 2523 of LNCS, pp. 454-469, August 2002.

[3 ]M. Ohkubo, K. Suzuki, and S. Kinoshita. “Cryptographic approach to “privacy-friendly" tags”. In RFID Privacy Workshop, MIT, USA, 2003.

[4] Hyung-Jun Kim, Sung-up Jo, Yong-won Kwon, So-Hyun Ryu, Yong-je Woo, Chang-Sung Jeong, and hyoungwoo Park, "Fast Parallel Algorithm for Volume Rendering and Its Experiment on Computational Grid", ICCS 2003, INCS 2657, pp. 610-618, 2003.

[5] I. Foster and C. kesselman (eds.) "The Grid: Blueprint for a new Computing Infrastructure," Morgan Kaufman Publishers, 1998.

[6] MPICH-G2, http://www3.niu.edu/mpi

## 저자약력

신 명 숙(Myeong Sook Shin)

2008년 조선대학교 전자정보공과대학 컴퓨터공학과(공학박사)
2005년~현재 조선대학교 전자정보공과대학 컴퓨터공학부 시간강사

<관심분야> 운영체제, 유비쿼터스컴퓨팅, 정보보호

이 준(Joon Lee)

1979년 조선대학교 전자공학과(공학사)
1981년 조선대학교 전자공학과(공학석사)
1997년 숭실대학교 전자계산학과(공학박사)
1982년~현재 조선대학교 전자정보공과대학 컴퓨터공학부 교수

<관심분야> 운영체제, 정보보호, 유비쿼터스컴퓨팅