지문 인식을 이용한 Peer to Peer Network 보안 모델의 설계

박정재, 구하성
한서대학교대학원 전산학과

A Design of Peer-to-Peer Network Security Model using Fingerprint Recognition

Jung-Jae Park, Ha-Sung Koo
Dept. of Computer and Information, Hanseo University

요 약

본 논문은 현재까지 제시되어진 peer to peer network model들을 정리하고 대표적인 peer to peer network model에 지문인식을 적용하여 개인에 대한 신원 인증 절차를 수행함으로써 보안에 대한 새로운 해결책을 제안하였다 기존의 peer to peer network model은 개인 대 개인간의 효율적인 network검색 기능과 분산 computing 환경을 제공하지만 보안에 관해서는 아직까지도 많은 연구가 필요하다. 본 연구에서는 기존의 peer to peer network model들에 지문인식을 사용한 새로운 보안 model을 설계하였다.

1. 서론

P2P(peer-to-peer)는 각 컴퓨터가 동등한 능력을 가지고 있어, 어떤 컴퓨터에서라도 통신 세션을 시작할 수 있는 통신 모델을 지칭한다. P2P를 동등계층 통신이라고도 부르는데, 네트웍에 연결되어 있는 모든 컴퓨터들이 서로 대등한 동료의 입장에서 데이터나 주변장치 등을 공유할 수 있다는 의미를 담고 있다. 이 개념과 대비되는 다른 모델로는 클라이언트-서버 모델이나 마스터-슬레이브 모델 등이 있다[1]. P2P 네트워크는 클라이언트-서버 네트워크 모델과 비교하여 전용 서버가 존재하지 않으며, 모든 워크 스테이션은 클라이언트가 될 수 있고 동시에 서버도 될 수 있다[2].

P2P 네트워크는 노드 간의 메시지를 전달할 경우 서버를 거치지 않고 두개의 노드 사이를 직접 연결하여 전달한다. 만약 다른 노드로 직접연결을 하여 메시지를 전달할 경우 인증이 이루어 지지 않는 보안의 취약점을 가지고 있다. 이러한 이유로 허용되지 않은 사용자가 특정 노드에 접근할 수 있는 문제점이 있으며, 본 연구에서는 지문인식을 통한 인증으로 이를 해결한다. 기존의 P2P 네트워크를 구현한 대표적인 제품인 그누텔라 네트워크를 분석하고 지문을 이용한 생체 인식 인증을 통해 해결할 수 있는 방법을 제안하고자 한다.

본 논문의 구성은 2장에서 P2P 네트워크의 개

념과 구조에 대해서 기술하고, 3장에서는 그누텔라 네트워크에 대한 분석과 보안의 문제점에 대하여 살펴보며, 4장에서는 지문 인식의 일반적 개념과 인증에 대해 설명한다. 5장에서는 지문을 이용한 P2P 모델의 인증 처리를 제안하며, 마지막으로 6장에서는 결론과 앞으로의 연구 방향을 기술하였다

2. P2P 네트워크의 개념과 구조

일반적으로 P2P 네트워크 모델은 다음과 같은 내용을 가지고 있다.

1. 다른 피어의 찾기 : P2P 네트워크의 피어들을 스스로 찾아내는 모델이다. 일반적으로 클라이언트-서버 네트워크 모델에서는 서버에 등록된 클라이언트가 서버에게 질의를 요청하여 클라이언트를 찾았다. P2P 네트워크는 브로드캐스팅 혹은 검색 알고리즘을 사용하여 스스로 피어들을 찾고 공유된 자원을 검색한다.
2. 컨텐츠의 피어의 검색 : 하나의 피어가 원하는 컨텐츠를 요청하고 요청에 해당하는 결과값을 전달한다.
3. 다른 피어들의 컨텐츠 공유 : 공유되어진 컨텐츠를 다른 피어들에게 요청하여 찾아낼 수 있다

위의 내용들을 기반으로 다음과 같은 P2P 네트워크 구조를 만들어 낼 수 있다[3].

2.1 일반적인 P2P모델

A, B, C의 컴퓨터로 구성되어진 일반적 P2P모델의 예를 보자.

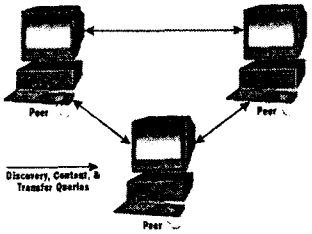

그림 1. 일반적인 P2P 네트워크 구성도

A, B, C 3개의 컴퓨터 모두 클라이언트와 서버로 동작할 수 있다. A가 서버가 되는 순가 B는 클라이언트가 될 수 있고, C와 B가 서버가 되는 순가 A가 클라이언트가 될 수 있다. 즉 각각의 컴퓨터가 필요에 따라 얼마든지 클라이언트와 서버로 사용할 수 있다는 것이 P2P 네트워크의 특징이다. 이것은 인터넷 상에서 포털 서비스 등을 통해 서비스를 제공받는 수직적 방식과 달리 네트워크에 연결된 모든 사람의 PC로부터 수평적인 정보를 제공 받을 수 있다.

2.2 간단한 검색 서버와 P2P

이 구조는 간단한 P2P모델과 비슷하게 동작하지만 그림 2에서처럼 다른 피어들을 찾기 위한 중앙서버가 있다.

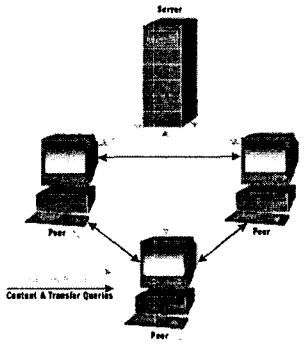

그림 2. 간단한 검색 서버와 P2P

이 모델은 피어의 로그온 타임을 통지하여 피어들간에 컨텐츠를 검색할 수 있게 중앙 서버에서 참여중인 다른 피어들의 목록들을 받는다. 이렇게 받은 목록들은 다른 피어에게 검색을 요청하기 위해 접근할 때 사용한다.

2.3. 검색, 룩업 서버와 P2P

그림 2와 비슷한 구조를 갖고 있으며 검색 서버에 컨텐츠 룩업 서비스를 포함하여 확장하였다. 이것은 피어들의 목록들을 받아만 오는 것이 아니라 컨텐츠를 일반적인 주기마다 찾기 서버로 전송한다. 피어는 특정 컨텐츠를 찾기 위해서 중앙 서버에 요청할 질의를 전송한다. 중앙 서버는 클라이언트들에게 질의를 전송하여 그에 대한 결과와 클라이언트의 목록을 요청 피어에게 전송한다. 전송된 결과값으로 각 피어에게 직접 접근 하여 컨텐츠를 가져온다.

이 모델은 네트워크를 통한 질의의 요청횟수가 증가 함에 따라서 서버의 병목현상이 발생한다. 하지만 컨텐츠의 전송은 피어간 직접 연결로 처리하기 때문에 서버 병목현상을 클라이언트-서버 모델보다 줄일 수 있다.

3. P2P 네트워크의 구현

일반적인 P2P 네트워크 모델을 구현한 것은 그누텔라이다.

3.1 일반적인 P2P의 구현 예

일반적 P2P 구현의 예로써 그누텔라가 있다. 그누텔라는 fully-distributed information-sharing technology이다[4]. 각각의 그누텔라 노드들이 분산된 정보를 공유하고 있는 파일 공유 기술이다. 웹에서 서비스를 받거나 정보를 얻으려면 서버의 주소를 알아야 하거나 검색엔진을 통해 서버의 주소를 알아내어야만 한다. 하지만 그누텔라는 수많은 그누텔라의 노드 중의 하나만 알아도 네트웍 속의 수 많은 정보 혹은 파일들을 찾을 수 있다. 물론 그 수많은 정보를 몇 개의 서버만이 관리하고 그 서버를 이용하여 찾을 수 있다.

3.2 그누텔라의 동작 원리

그누텔라는 기본적으로 다른 노드에 대한 정보를 가지고 있으며, 만약 노드에 대한 정보가 없다면 사용자가 하나 이상의 노드에 대한 최소한의 정보를 가지고 있어야 한다. 대부분의 그누텔라 프로그램은 다른 노드에 대한 정보를 캐쉬에 저장하고 있다. 프로그램이 실행 되면 먼저 캐쉬에 있는 정보를 통해 그누텔라 네트워크에 연결이 된다. 아래의 그림 3, 4는 새로운 노드가 연결되기 전에 그누텔라 네트워크와 새로운 노드가 연결된 후의 그누텔라 네트워크를 나타냈다.

그림 4에서 새로운 노드와 연결된 세 개의 노드는 캐쉬에서 임의로 선택된 세 개의 노드들이다. 새로운 노드가 그누텔라 네트워크에 연결됨으로써 서로 분리되어 있던 두개의 그누텔라 네트워크로 연결이 된다. 이렇게 연결된 그누텔라 네트워크 피어들은 서로

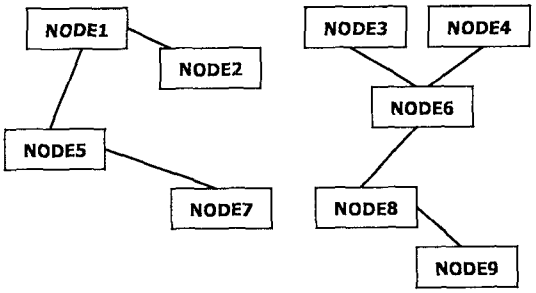

그림 3. 새로운 노드가 연결되기 전 네트워크 구조

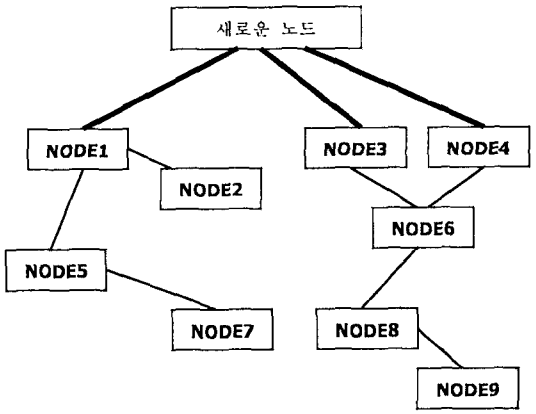

그림 4. 새로운 노드가 연결된 후 네트워크 구조

자료를 전송하고 받게 된다. 이때 각 피어들은 각각의 GUID(Global Unique IDentifier)와 TTL을 이용하여 브로드케스팅으로 위치를 알리거나 질의를 요청한다. 피어들간의 직접연결을 하여 자료를 전송하거나 받는다. 이에 대한 메시지 전송헤더는 표1과 같다[3].

<표 1> 그누텔라 네트워크 헤더

Byte	Summary	Description	
0-15	GUID	Global Unique Identifier	
16	Payload Descriptor	Value	Function
		0x01	Ping
		0x02	Pong
		0x40	Push Request
		0x80	Query
		0x81	Query Hits
17	TTL	Time to Live, 메시지가 한 번씩	

		전달될 때 마다 1씩 감소하며 0이 되면 메시지는 사라진다.
18	Hops	메시지가 전달된 회수(한 번 전달될 때 마다 1씩 증가한다.
19-22	Payload Length	Payload의 크기

4. 지문 인식의 일반적 개념

컴퓨터 네트워크가 점점 발전함에 따라 일상 업무 뿐만 아니라 보안을 유지하여야 하는 정보들도 네트워킹 환경에서 주고 받을 필요성이 증가하고 있다. 이의 해결 방법으로 많은 정보 보호 기술이 개발되고 있으며, 그 중 하나의 방법으로 신체의 특성을 이용하는 생체측정학 역시 매우 중요한 기술 분야로 발전되고 있다. 지문은 입력의 편리성과 데이터의 불변성 그리고 도용이 힘들기 때문에 신체측정의 여러 분야 중 가장 활발하게 발전되고 있으며 가장 많이 상용화되고 있다.

4.1. 특징점 추출

다양한 조건 및 잡음이 섞인 지문 화상으로부터 그 지문의 특성을 규정 지울 수 있는 융선의 특이점은 그림 5에 나타내었다.

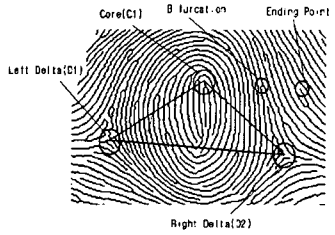

그림 5. 지문에서의 특이점

위의 그림에서 단점은 융선이 시작되거나 끝나는 점이며, 분기점은 융선이 갈라지는 곳이며, 중심점은 지문의 융선중 방향이 가장 급격하게 변하는 곳이며, 삼각주는 융선의 흐름이 세 방향으로 나뉘어지는 곳을 말한다.

4.2 지문의 매칭기술

지문 매칭 알고리듬은 특징점이 추출되고 난 뒤 이루어지는 단계로서 지문에 가장 특화된 알고리듬이다. 일반적인 경우 1:1 매칭시에는 타인을 본인으로 판단하는 TYPE I ERROR가 0%에 가까운 성능을 가져야 하며, 1:many인 경우 타인을 본인으로 판단하는 경우에는 관대하나 본인을 본인으로 판단하지 못하는 TYPE II ERROR에는 매우 엄격한 오류 허용률을 가져야 한다. 또한, 1:1인 경우 본인 비교만 이루어지는 형식으로서 특징점의 모든 분포를 고려해 단계별로 비교하지만 1:many 인 경우 100만 이상의 지문을 매칭하기 위해서는 가능한한 매칭의 전처리 단계에서 단순 비교하여 후보군을 줄여야 한다. 이런 견지에서 분류를 이용하며, 매칭의 전처리 단계에서 특정 후보군을 제외시키는 알고리듬의 설계가 요구된다. 일반적으로 매칭 알고리듬은 특징점간의 기하적으로 구성된 그래프 패턴의 비교 산정과 특징점의 x축과 y축의 위치와 특징점과 융선과의 비교를 통해 특징점의 방향 성분을 추출하여 이용한다. 아래의 그림 6은 지문영상으로부터 추출된 그래프 패턴의 예이다.

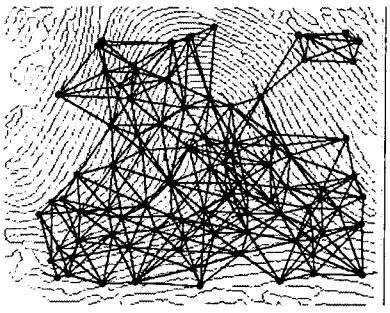

그림 6. 특징점의 기하학적인 구조

5. 지문을 이용한 P2P 모델의 인증 처리

일반적인 P2P 네트워크 모델에서 자료의 전송이 피어간에 직접 연결로 처리 되어 각 피어가 자신에게 들어오는 사용자에 대하여 인증 처리를 할 수 없다. 본 장에서는 지문 인식 인증 시스템을 P2P 네트워크 모델에 추가함으로써 보안 문제를 해결한다.

5.1 로컬 피어의 인증 처리

로컬 피어에서 사용자를 등록할 때에는 사용자

이름과 그에 해당하는 지문데이터를 입력 받아야 한다. 입력 받은 데이터는 지문 데이터는 KISA에서 제안한 SEED 암호화 알고리즘으로 암호화되어 저장한다[8].

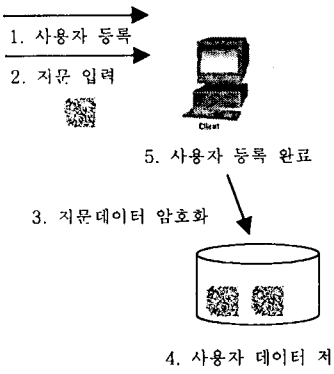

그림 7. 로컬 피어의 사용자 등록

그림 7은 로컬 피어에서의 사용자 등록 순서이다. 사용자 정보로 입력 받은 사용자 이름은 PUID(Private User Identifier)로 저장되어 로컬에서의 인증처리 혹은 피어간의 인증처리를 할 경우 사용자 식별에 사용되어 진다. 로컬 피어에서 사용자 인증을 받는 과정은 그림 8에 나타내었다.

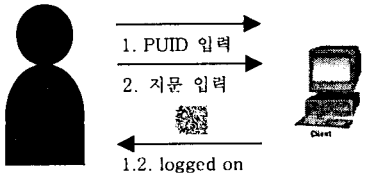

그림 8. 로컬 피어의 사용자 인증

5.2 피어간의 인증 처리

피어간의 인증 처리를 하기 위해서는 기존의 그누텔라 네트워크 헤더와 메시지에 추가할 메시지가 있다. 기존의 그누텔라 네트워크는 피어를 알리는 방법으로 GUID를 사용하고 있다. 지문 인식을 이용한 인증을 하기 위해서는 피어를 찾는 것 외에 사용자를 식별할 수 있어야 한다. 즉 GUID와 함께 해당 피어의 사용자들을 식별할 수 있는 PUID(Private User IDentifier)가 있어야 한다. GUID와 PUID의 조합으로 사용자에 대한 FPVUID(Finger Printer Verification Universal unique IDentifier)를 만들어 낸다. FPVUID를 이용하여 피어의 위치와 사용자를 식별한 후, 지문을 이용하여 사용자를 인증 한다.

<표 2> 그누텔라 변경된 네트워크 헤더

Byte	Summary	Description	
0-15	FPVUID(GUID)	Finger Printer Verification Universal unique Identifier (GUID)	
16	Payload Descriptor	Value	Function
		0x01	Ping
		0x02	Pong
		0x40	Push Request
		0x80	Query
		0x81	Query Hits
		0x90	User Register Request
		0x91	User Register
		0x92	Finger Print Auth Request
		0x93	Finger Print Auth
17	TTL	Time to Live, 메시지가 한 번씩 전달될 때 마다 1씩 감소하며 0이 되면 메시지는 사라진다.	
18	Hops	메시지가 전달된 회수(한 번 전달될 때 마다 1씩 증가한다.	
19-22	Payload Length	Payload의 크기	
23	FPVUID (PUID)	각 피어의 사용자 Number	

<표 3>User Register Request 메시지

Bytes	Summary	Description
0-15	FPVUID(GUID+ PUID)	등록 피어 유저의

		FPVUID
16-31	Nonce Data	암호화된 랜덤 데이터

<표 4>User Register 메시지

Bytes	Summary	Description
0-1	Port	자신이 쓰고 있는 IPv4 Port 번호
2-5	IP Address	자신의 IPv4 IP Address
5-255	Finger Data	등록할 암호화된 지문 데이터

<표 5>Finger Print Auth Request 메시지

Bytes	Summary	Description
0-15	FPVUID(GUID+ PUID)	인증할 피어의 사용자 FPVUID
16-31	Nonce Data	암호화된 랜덤 데이터

<표 6>Finger Print Auth 메시지

Bytes	Summary	Description
0-1	Port	자신이 쓰고 있는 IPv4 Port 번호
2-5	IP Address	자신의 IPv4 IP Address
16-31	Nonce Data	암호화된 랜덤 데이터

표 2는 그누텔라 네트워크의 헤더에 피어간 사용자 인증을 위해 추가된 기능이다. 인증관련 Function 메시지 네 개와 전체 헤더에서 PUID를 나타내는 1Byte를 추가 시킴으로써 사용자 식별과 인증 기능을 위한 메시지를 추가했다. 기존의 그누텔라 네트워크와의 호환을 위해서 GUID 필드는 변화 되지 않는다. PUID와 GUID 조합으로 FPVUID를 만들며 각 피어 당 255명의 사용자를 등록할 수 있다. 표 3 과 표 4는 사용자를 피어에 등록시키는데 사용되는 메시지이다. 표 5와 표 6은 사용자를 지문 인식을 이용하여 인증하는데 사용되는 메시지이다.

5.2.1 피어간 사용자 등록

지문을 이용한 P2P 네트워크 인증을 처리하기 위해서 각 피어간의 사용자를 식별해야 한다. 사용자를 식별하기 위해선 피어들은 인증할 사용자를 등록 한다. 등록과 인증과정은 Microsoft Windows NT에서 사용되었던 NTLM인증과정을 기반으로 처리하였다. NTLM이란 윈도우 제품군의 보안 프로토콜이다[9]. 그림 9는 피어간의 등록 과정 이다. 그림 9의 1번은

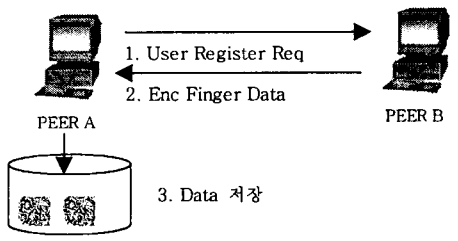

그림 9. 피어간 사용자 등록

User Register Request 메시지를 전달해 피어를 찾아 FPVUID와 피어간의 확인 데이터로 쓰일 Nonce(임의의 랜덤한 128bit 데이터)를 전송한다. 2번에서 자신의 Port와 IP Address 전달하고, SEED로 암호화된 지문 데이터를 Nonce로 암호화 하여 전송한다. 전송되어진 지문 데이터는 Nonce로 복호화하여 저장한다.

5.2.2 피어간 사용자 인증

피어간 인증 처리는 특정 사용자가 접근할 경우 접근 사용자가 누구인지 판별해 내는 것이다. 사용자를 판별하기 위해 지문 인증을 사용하여 인증한다. 지문 인증을 하기 위해서는 사용자 등록 작업이 선행 되어져야 한다. 그림 10은 지문을 이용한 인증과정 이다. 피어 B가 피어 A에게 사용자 인증 요청을 한다. FPVUID로 인증할 피어와 사용자를 찾고 Nonce를 전송한다. 피어 A는 FPVUID중 PUID를 보고 해당 사용자를 찾고 사용자의 암호화된 지문데이터로 Nonce를 암호화 하여 Nonce를 피어 B에게 전송한다. 그 동안 피어 B는 FPVUID를 사용하여 자신의 PEERDB에서 해당 사용자의 암호화된 지문데이터를 찾아 피어 A와 같이Nonce를 암호화 시킨다. 피어 A에서 암호화 되어진 Nonce Data가 전송되면 피어 B의 암호화된 Nonce데이터와 비교하여 같은지를 판별하여 인증하여 판별한다.

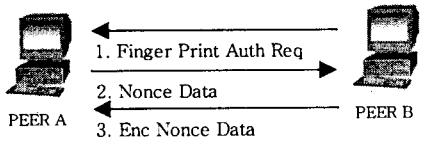

그림 10. 피어간 사용자 인증

전체 과정을 나타낸 것이 그림 11과 같다.

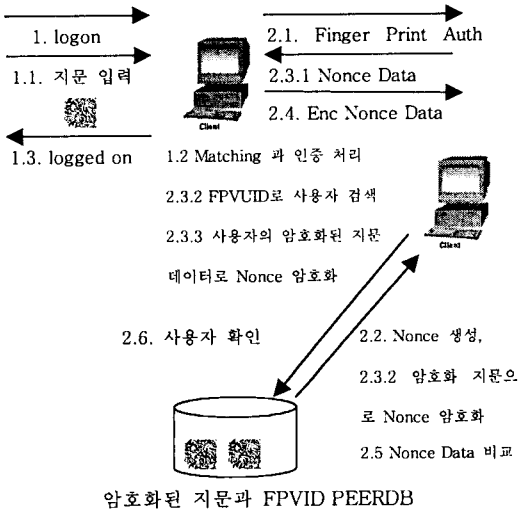

그림 11. 지문을 이용한 P2P의 새로운 인증 처리

6. 결론 및 연구 방향

지문은 사람의 신체의 특성을 이용하는 것으로 도용이 거의 불가능하다는 장점을 가지고 있으므로 최근 들어 많이 연구되어지는 정보 보호 학문의 한 분야이다. P2P 네트워크에 관한 논의가 활발해지는 요즘 지문 인식을 이용한 개인간 인증부분에 관한 연구는 충분한 가치가 있다고 생각된다. 지문 인식을 이용한 인증은 현재 P2P 네트워크의 취약점인 사용자 판별과 인증에 관한 문제와 악의를 갖는 사용자가 특정 피어에 접근하는 것을 해결하고 제안하였다. P2P 네트워크 모델의 장점으로 인해 현재 많은 상용화 제품들이 나오고 있다. 이러한 제품 중에서 가장 대표적인 그누텔라 모델에 지문 인증을 적용함으로써 보다 좋은 보안 환경을 갖게 설계하였으며, 지문의 특수성으로 사용자는 더욱 편한 인증 처리를 할 수 있는 장점을 갖게 되었다.

향후 연구로는 각 P2P 네트워크 모델에 지문 인식을 이용한 인증을 삽입하여 확장해 나갈 것이며, 병목현상의과 부하를 줄일 수 있는 방법에 대한 연구가 더 필요하다.

6. 참고 문헌

[1] Bob Knighten "Peer to Peer Computing," Intel Developer Forum, Fall, 2000

[2] Backgrounder "Peer to Peer Technology," Intel Corporation, August, 2000

[3] Lance Olson ".NET P2P Writing Peer-to-Peer Networked Apps with the Microsoft .NET Framework," MSDN Magazine, February, 2001

[4] 이진원, 이승학 "Ktella," 2001

[5] A. K. Hrechak, "Automated Fingerprint Recognition Using Structural Matching," Pattern Recognition, 23, 1990.

[6] FBI's Manual, The Science of Fingerprints, U.S. Goverment Printting Office, Washington, D.C., 1963.

[7] B. M. Mettre, " Fingerprint Image Analysis for Automatic Identification," Machine Vision and Applications, 6, 1993

[8] 이홍섭, 박성준, 외 5명 " A Design and Analysis of SEED," 한국정보보호센터, 12, 1998

[9] Jeffrey Richter, Jason D. Clark, Programming Server-Side Applications for Microsoft Windows 2000, Microsoft Press Ltd, p.537-539, 2000