# P2P에서의 안전한 정보 공유 모델 : IAA 기반 접근방식

진홍태*, 김동성*, 박종서*

*한국항공대학교 컴퓨터공학과

e-mail: {jhongtae, dskim, jspark}@mail.hangkong.ac.kr

# Secure Information Sharing Model in P2P: IAA based Approach

Hong Tae Jin*, Dong Seong Kim*, Jong Sou Park*

*Department of Computer Engineering, Hankuk Aviation Univ.

## 요 약

본 논문에서는 P2P(Peer-to-Peer) 환경에서 효율적이고 안전하게 정보를 공유할 수 있는 시스템 구조를 제안한다. 기존의 Server-Client 환경에 비해 P2P 환경이 네트워크를 확장시키고 병목 현상을 줄일 수 있는 방안으로 떠오르게 됨에 따라 그에 따른 보안 문제도 필수적으로 고려해야 할 사항이 되었다. 따라서 P2P 환경에서도 안전하게 정보를 공유할 수 있고, 각 Peer들의 정보를 보호해 줄 수 있는 보안 기술이 필요하다. 본 논문에서 제안하는 시스템은 IAA(Intelligent Automation Agent)를 이용한 접근방식을 제공함으로서, 다른 시스템에 응용 가능하고 보안 환경의 변화에 민첩하게 유기적으로 대처할 수 있는 통합된 관리 방법을 제시한다.

## I. 서론

### 1. P2P의 등장 배경

18개월마다 컴퓨터 칩의 성능이 2배로 되면서 가격이 절반으로 떨어진다는 '무어의 법칙'은 개인 PC의 기능이 서버와 대등한 수준으로 급속히 발전하고 있는 현재의 상황을 잘 묘사하고 있다[1]. 바로 이러한 클라이언트 PC 기능 향상과 급속한 가입자망의 확대, 초고속 인터넷 환경 등이 P2P의 등장을 가속화 시켰다. Client-Server 방식의 기존 네트워크에서는 서버 집중식으로 서버의 역할이 강조되었다. 즉, 기존의 서버 집중식 네트워크 구조에서 나타날 수 있는 트래픽 집중이라는 한계를 클라이언트 상호간 분산·협력이라는 새로운 개념으로 해결하려는 시도가 결국에는 P2P를 등장시켰다고 할 수 있다. P2P란 컴퓨터와 컴퓨터를 직접 연결해 서버 없이도 사용자간 파일을 공유할 수 있는 기술을 말한다[2]. 초고속 통신망의 보급으로 인한 인터넷 대역폭의 광대역, 고속화와 인터넷 사용자들의 PC가 고성능화 되어 감에 따라 기존의 서버 집중식 모델의 한계성과 비용이 드러나게 되었다. 또한 현재의 PC 처리속도, 메모리 그리고 하드디스크의 용량이 지속적으로 증가하는 추세여서, 이제 개인의 PC가 서버의 역할을 충분히 수행하는 단계에 도달했기 때문에 P2P 환경으로의 필요성이 나타나게 되었다.

### 2. P2P 보안의 필요성

표 1. 2003년 9월 바이러스 통계

| 구분 | 2002 | 2003 | | | | | | | | | | | | 2003년 총계 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | |
| 바이러스 | 9,308 | 1,098 | 975 | 785 | 487 | 539 | 304 | 925 | 832 | 522 | | | | 7,060 |
| 인터넷 웜 | 27,021 | 1,361 | 1,320 | 2,557 | 2,350 | 3,704 | 1,854 | 1,185 | 9,748 | 15,662 | | | | 43,741 |
| 트로이목마 (or 변종이) | 1,687 | 1,284 | 878 | 419 | 309 | 304 | 491 | 411 | 334 | 387 | | | | 4,809 |
| 가짜(Hoax) | 13 | 0 | 16 | 10 | 5 | 3 | 5 | 6 | 4 | 2 | | | | 57 |
| 조크(Joke) | 111 | 5 | 1 | 6 | 3 | 0 | 0 | 3 | 1 | 2 | | | | 21 |
| 기타 | 537 | 11 | 50 | 42 | 52 | 59 | 248 | 20 | 120 | 86 | | | | 688 |
| 합계 | 38,677 | 3,757 | 3,238 | 3,797 | 3,186 | 4,611 | 3,522 | 2,550 | 11,059 | 20,661 | | | | 56,376 |

표 1은 2003년 9월에 발생한 바이러스, 웜 발생 피해 증가 현황을 나타낸다[3]. 기존에는 한 서버 혹은 호스트 대상으로 컴퓨터 바이러스나 해킹을 하던 방식에서 이제는 호스트 네트워크 기반으로 해킹기술이 발전하고 또한 바이러스와 통합된 사이버 테러 기술이 등장함으로 인한 피해가 증가하

고 있다. P2P 구조를 사용함으로써 네트워크를 확장시키고 병목현상을 감소시킬 수 있다. 그러나 기존의 Client-Server 모델에서 서버에 집중되었던 보안 문제가 각 Peer로 확대됨에 따라서 각 Peer들에서의 해킹이나 바이러스 등에 대한 보안 문제를 고려해야 한다. 또한 네트워크가 확대됨에 따라 엔트로피가 증가하면 혼잡도가 커지는 것처럼 네트워크 보안에 위협을 주는 취약성이 더욱 확대되므로, 네트워크 상에서의 보안도 고려해야 한다. P2P기술은 차세대 인터넷으로 중요하지만 만일 보안문제가 해결되지 않은 상태에서 적용된다면, 웜이나 바이러스 등으로 인해 더 많은 피해를 줄 수 있을 것이다. 한때 gnutella에서는 P2P에서 작동하는 웜바이러스가 발견되었는데, 이러한 바이러스는 P2P 구조의 특성상 순식간에 번식하게 된다는 점에서 심각한 보안 위협 요소로 작용할 수 있다[4]. 그러므로 P2P구조가 활성화 되기 위해서는 반드시 보안문제가 해결되어야 한다.

# II. P2P 환경에서의 안전한 정보 공유 모델

## 1. P2P에서 사용되는 3가지 모델

P2P 환경에서 현재 사용되고 있는 모델들을 살펴보면 다음과 같다[5].

가. 순수한 P2P

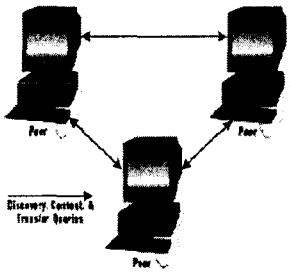


그림 1 순수한 P2P 구조

이 방식은 그림 1과 같이 중앙서버의 의존 없이 작동하기 때문에 검색엔진과 같은 모듈들은 개별 클라이언트들이 구동한 프로그램에 설치된다. 또한 네트워크에 접속된 Peer를 동적으로 찾으며 통신 방식은 파일업로드/다운로드, Online 수행, 요청/응답 등의 데이터 전달 등이 있다. 특징으로는 기존의 Client-Server의 관습적 통신방법을 탈피하였다는 것과, 사용자가 규칙 및 자신의 네트워크 환경을 설정할 수 있고, 상호 대칭적인 의사소통이 가능하다는 것이다. 그러나 Peer들에 대한 검색이 네트워크 상에서 이루어지기 때문에 효율적으로 많은 수의 Peer들을 조회할 수 없다는 단점이 있다.

나. 조회/ Lookup/ 컨텐트 제공 기능을 갖는 P2P

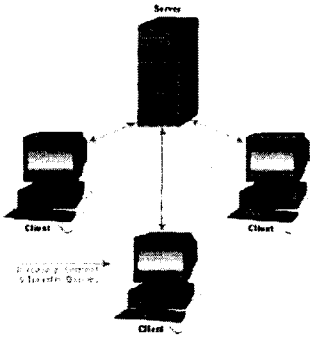


그림 2 조회/ Lookup/ 컨텐트 제공 기능을 가진 P2P 구조

이 방식에서는 그림 2와 같이 서버는 전형적인 Client-Server 구조 같은 지배권을 가진다. 따라서 Peer의 요청을 들어주는 모든 것은 서버에 존재하며 모든 자원이 중앙의 데이타베이스에 저장된다. 단점으로는 많은 요청이 쇄도할 때 서버가 느려지고, 데이터 관리, 저장, 모든 요청을 서버가 처리하므로 많은 비용이 소모된다. 또한 단일지점에 기인한 고장 발생 가능성이 높기 때문에, 이는 전체 시스템에 부정적인 영향을 미칠 수 있다.

다. 간단한 조회기능 서버를 갖는 P2P

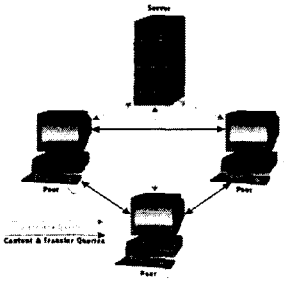


그림 3 간단한 조회기능 서버를 갖는 P2P 구조

이 방식은 기존의 순수 P2P 방식과 서버를 갖는 P2P 방식의 장점들을 혼합한 구조로 그림 3과

같이 서버는 접속하는 Peer에게 이미 접속된 Peer의 이름을 제공하는 것에 한정된 기능을 하므로 단지 Peer들로 하여금 접속된 Peer들의 목록을 제공함으로써 Peer들을 도와준다. 그러므로 접속을 수립하는 것과 통신을 수행하는 것은 각각의 Peer들의 몫이다. 따라서 기존의 순수한 P2P 모델에 비해서 많은 수의 Peer들을 조회할 수 있는 가능성이 높다는 특징을 갖기 때문에, 최근들어 많은 P2P 모델이 이 유형을 따르고 있다.

## 2. 안전한 P2P 제안 모델

### 1) 보안 정책이 결합된 정보 공유 기법

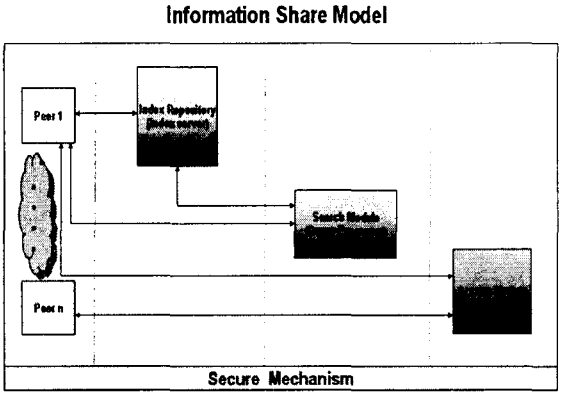


그림 4 P2P 환경에서 보안 정책이 결합된 정보 공유 기법

본 논문에서는 몇 가지 P2P 모델 중 순수한 P2P 모델에 비해서 우월하고 많은 수의 Peer들을 조회할 수 있는 가능성이 높아 현재 가장 많은 P2P 모델이 사용하고 있는 간단한 조회 기능을 갖는 서버(인덱스 서버)를 갖는 P2P 방식(그림 3 참조)을 사용한다. P2P 환경에서 기본적으로 정보를 공유하는 메커니즘은 다음과 같다. 우선 Peer1이 P2P 환경에 참여하게 되면 기본적으로 인덱스 서버에 자신의 ip와 공유 데이터 목록을 등록하게 된다. 그러면 Peer1이 원하는 데이터를 찾기 위해 찾고자 하는 데이터의 이름을 입력하게 되고 Search Module을 통해 인덱스 서버를 검색한 후, 최종적으로 Peer1이 원하는 데이터를 가지고 있는 상대방 Peer의 ip를 반환하게 된다. 그러면 Peer1은 자신의 찾고자 하는 데이터를 가지고 있는 Peer와 Access Module을 통해 직접 통신하여 데이터를 공유하는 방법을 사용하고 있다. 본 논문에서는 다음과 같이 보안 메커니즘을 결합하여 기존의 P2P 환경을 더욱 개선시켜 안전한 정보 공유를 하고자 한다.

### 2) 제안 모델의 구조 및 구성요소

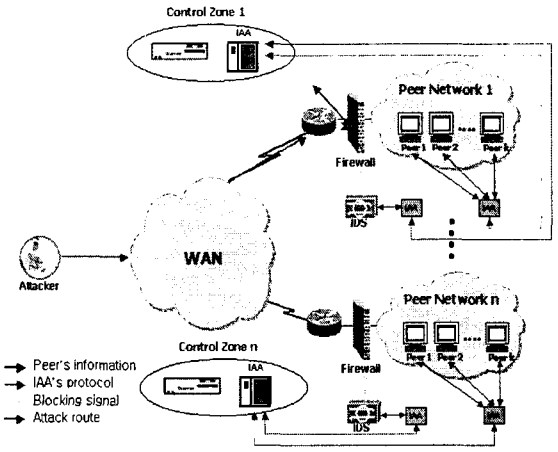


그림 5 제안된 안전한 P2P 모델

본 논문에서 제안하는 IAA(Intelligent Automation Agent)기반의 P2P 정보 공유 방식은 그림 5와 같이 기존의 IDS(Intrusion Detection System), 방화벽 등을 관리하는 각각의 IAA를 탑재 함으로서 IAA끼리의 프로토콜을 통해 자신의 Peer Network의 전체 시스템 상태를 관리하는 통합 관리 보안 메커니즘이다[6][7]. 실제적으로 IAA가 각각의 Peer들의 시스템 상태와 IDS 상태 및 로그 기록을 전달해주는 각각의 IAA들과의 프로토콜을 통한 통신으로 시스템들의 상태 정보를 관리하기 때문에, 침입이나 바이러스 등의 여러 보안 위협 요소들로부터 적절한 정책들을 알려줄 수 있는 안전한 P2P 환경을 구축해준다. 그렇기 때문에 각각의 Peer Network에 속해 있는 모든 Peer들의 관리 방식은 독립적인 IAA들의 관리 영역으로서, 통합된 관리 방식을 제공한다.

### 3) 운용 메커니즘

먼저 시스템을 침입하려는 악의의 목적을 가진 사람(Attacker)이 공격(Denial Of Service, Buffer Overflow 공격, 바이러스 유포 등)을 시도하려고 할 때, IDS에서 이를 감지한 후에 IDS는 방화벽으로 그 공격에 맞는 정책을 방화벽(Firewall)으로 전달해준다. 그러면 방화벽은 그 정책에 따라 그러한 공격에 부합된 침입을 탐지하여 적절한 대응(특정 포트 차단 등)을 하게 된다. IAA(Intelligent Automation Agent)는 IDS의 상태를 체크해주는 것과 각각의 Peer들의 상태를 관리해주는 두 가지 기능을 제공하며 이들은 Control Zone에 있는 중앙 IAA와 IAA's protocol을 이용하여 서로의 정

보를 공유하며 통신한다. 스캐너는 자신이 속해 있는 네트워크 내의 모든 Peer들의 시스템 상태를 항상 스캐닝한다. 이상 유무가 발견되면 이것은 즉시 중앙의 IAA 데이터 베이스로 전달되고 적절한 정책이 Peer들을 관리하는 IAA를 통해 취해진다. 이와 같은 일련의 과정들은 실시간으로 IAA들의 적절한 협업 과정을 통해서 이루어지기 때문에 침입과 같은 상태를 적절하게 복구하고 대책을 마련할 수 있도록 한다.

4) 본 제안 모델의 장점 및 단점

IAA(Intelligent Automation Agent) 기반의 P2P 정보 공유 방식은 통합된 여러 환경을 관리하는 각각의 Agent들이 존재하기 때문에 P2P 방식이 아닌 다른 환경에도 응용이 가능하고 IAA가 자신들만의 고유한 프로토콜을 사용하여 통신하기 때문에 내부 네트워크 자체의 보안 효과를 가져온다. 또한 전체 네트워크의 상태가 IAA를 통해 항상 모니터링 되므로 공격 탐지 뿐 아니라 네트워크의 이상 유무가 발생할 때 즉각적인 대응이 가능하다. 그러나 기존의 공격 패턴 정보가 들어있는 IDS 데이터 베이스에 의존해서 외부 네트워크 공격을 탐지하므로 기존에 알려지지 않은 새로운 공격 기법이나 바이러스 등에 쉽게 내부로의 침입을 허용할 수 있고 또한, 각각의 시스템들을 실시간으로 모니터링 해야 하므로 이를 이용하는 프로세스에 과부하가 걸릴 수 있다.

## III. 결론 및 향후 연구

본 논문에서는 IAA를 통해 보안 메커니즘을 구현한 P2P 환경에서의 안전한 정보 공유 모델을 제안하였다. IAA를 이용하여 P2P 환경에서 해킹이나 바이러스 등의 위협으로부터의 공격을 차단할 수 있는 메커니즘을 제시하였으며 이를 적용할 경우의 장단점에 대해서 고려해 보았다. 앞으로 개선해야 할 부분은 단점으로 지적되었던 알려지지 않은 공격 패턴에 대해 이를 탐지하는 방법과 실시간으로 시스템 정보를 모니터링하는 IAA의 프로세스 과부하를 줄이는 방법에 대한 연구가 필요하다. 또한 P2P 방식 뿐 아니라 여러 다양한 곳에 응용할 수 있는 방법에 대한 연구가 필요하다.

## Acknowledgements

본 연구는 인터넷 정보검색(IRC) 지역 연구센터(RRC)와 대학 IT 연구센터 육성지원사업의 연구결과로 수행되었음.

## 참고문헌

[1] http://www.terms.co.kr/MooresLaw.htm, 텀즈, "Moore's Law"

[2] David Barkai, Peer-to-Peer Architecture Group, Microcomputer Research Lab and Intel Corporation, "An Introduction to Peer-to-Peer Computing", Intel®Devloper -UPDATEMagazine, pp. 1-7, February 2000.

[3] http://www.certcc.or.kr, "Certcc-Kr", 2003년 9월 바이러스 통계

[4] http://home.ahnlab.com, "안철수 연구소", P2P와 악성 코드

[5] Kant, K., Iyer, R., and Tewari, V.;"A framework for classifying peer-to-peer technologies", Cluster Computing and the Grid 2nd IEEE/ACM International Symposium CCGRID2002 , 21-24, pp. 338 -345, May 2002.

[6] Xiaolin Pang; Catania, B.; Kian-Lee Tan; "Securing your data in agent-based P2P systems", Database Systems for Advanced Applications, 2003. (DASFAA 2003). Proceedings. Eighth International Conference on , 26-28, pp. 55 -62, March 2003.

[7] S. D. Chi, J. S. Park, K. C. Jung, J. S. Lee, "Network Security Modeling and Cyber-attack Simulation Methodology", Lecture Notes on Computer Science series, 6th Australian Conf. On Information Security and Privacy, Sydney, July, 2001.