

# 네트워크 통제와 능동형 에이전트 기반의 소프트웨어 라이선스 제어 시스템 설계

박정진<sup>o</sup> 정회영 홍철의 박진섭 신영선  
(주)유비엔씨, 대전대학교

{parkjj<sup>o</sup>, jhy, hush}@ubnc.net, jspark@dju.ac.kr, yhshin@zeus.dju.ac.kr

## Design of Network control and Spontaneous Agent based Software Lisence Control Systems

Jungjin Park<sup>o</sup>, Hoiyoung Jung, Chului Hong, Jinsub Park, Youngsun Shin  
UBNC Corp, Daejon University

### 요 약

최근 인터넷 사용의 증가와 네트워크 통신 속도의 향상으로 인하여, 인터넷을 통한 대용량의 데이터의 전송이 활발하게 이용되고 있다. 이로 인하여 공공기관 및 교육기관, 기업 등에서 사용되고 있는 소프트웨어 중 정식적인 라이선스를 구입하지 않고 사용자들이 개인적으로 인터넷을 통해 불법적으로 다운로드 받아 설치하여 사용하는 사례가 급속하게 증가하고 있다. 본 논문에서는 조직에서 효과적으로 소프트웨어 사용량을 파악하고 사용을 통제함으로써 불법소프트웨어의 사용을 줄일 수 있는 방법으로 능동형 에이전트와 네트워크 통제 방식을 연동한 라이선스 통제 기법을 제안한다.

## 2. 능동형 에이전트의 설계

### 1. 서 론

최근 인터넷의 사용이 급증하고, 네트워크의 통신 속도의 급속한 향상으로 인하여, 인터넷을 통한 대용량 데이터의 전송이 활발하게 이용되고 있다. 이로 인하여 인터넷을 통하여 사용으로 구입하여 사용되어야 하는 각종 상용 콘텐츠가 불법적으로 P2P 공유프로그램, 또는 메신저를 이용한 개인 간의 파일 전송, 파일 공유용 FTP사이트 등 다양한 방법으로 불특정 다수의 사용자들에게 공유되어 사용되고 있다. 이러한 불법 상용 콘텐츠의 불법적인 사용으로 인하여 공공기관 및 교육기관, 기업 등에서는 효과적으로 조직 내의 소프트웨어 라이선스를 관리하기가 어려운 실정이다.

이에 본 논문에서는 클라이언트 시스템에서 시스템 정보와 설치된 소프트웨어 정보를 자동으로 수집하고 분석하는 능동형 에이전트와 에이전트가 수집한 정보를 기반으로 허용되지 않은 상용 소프트웨어를 불법적으로 사용하는 시스템에 대해 네트워크를 제어함으로써 효과적인 라이선스 관리가 이루어질 수 있는 기법을 제안한다.

1장의 서론에 이어 2장에서는 시스템 정보 및 소프트웨어 설치정보를 수집하여 관리 서버로 전송하는 능동형 에이전트 기술에 대하여 설명하고, 3장에서는 능동형 에이전트가 수집한 정보를 바탕으로 불법소프트웨어를 사용하는 시스템의 네트워크 및 소프트웨어 실행을 제한하는 시스템을 제안한다. 그리고 마지막으로 4장에서는 본 논문의 결론을 기술한다.

네트워크 통제를 통하여 시스템의 네트워크를 제어하기 위해서는 기본적으로 에이전트 시스템의 네트워크 정보와 소프트웨어 설치 정보가 요구된다. 능동형 에이전트는 이러한 기본정보를 스캔하여 관리서버로 전송하는 기능을 수행한다.

에이전트는 초기 설치시 실행되면서 에이전트 시스템의 IP 주소, MAC 주소, 운영체제 정보, 서비스팩 버전, 익스플로러의 버전 정보, 시스템 이름, 시스템 워크 그룹, 정보를 전송할 서버의 정보를 생성한다.[1] 시스템 정보 파일의 내용은 다음 그림 1과 같다.

```
sysinfo.ini - 메모장
파일(F) 편집(E) 서식(O) 도움말(H)
[SYSINFO]
MAC=00-0c-29-3a-20-9c
IP=210.107.130.110
OS=Windows2000
OSSP=SP4
IE=6.0.2800.1106
[USERINFO]
MAC=00-0c-29-3a-20-9c
IP=210.107.130.110
HOSTNAME=UBNC-2000
WORKGROUP=(주)유비엔씨
TOPSERVER=210.107.130.107
MIDDLESERVER=210.107.130.107
```

그림 1 에이전트 스캔 시스템 정보

에이전트에서 생성된 시스템 정보는 관리 서버로 전송되어 관리된다. 에이전트의 시스템 정보가 등록되면서 소프트웨어 설치 정보도 함께 관리서버에 전송되어 관리된다. 에이전트에서 전송하는 소프트웨어 정보는 관리서버에서 그림 2와 같이 관리된다.[2][3][4]

id	User_name	SW Name	Exp. Date
10537	00-0c-be-59-ad-14	3D Falling Leaves Full Screen Saver	2006-04-17 오전 1:07:23
6485	00-08-02-60-0E-9C	MyFirewall	2006-03-22 오후 8:20:34
6497	00-08-02-60-0E-9C	Visual Asslat X	2006-03-22 오후 8:20:34
6510	00-08-02-60-0E-9C	OZ Designer 2.5	2006-03-22 오후 8:20:34
6513	00-08-02-60-0E-9C	Rexpert2.5	2006-03-22 오후 8:20:34
8886	00-11-09-E1-9F-C6	SoundMAX	2006-04-03 오전 2:13:11
10538	00-0c-be-59-ad-14	Adobe Acrobat 7.0 Professional - Korean	2006-04-17 오전 1:07:23
6514	00-08-02-60-0E-9C	InstalShield Professional - Standard Edition	2006-03-22 오후 8:20:34
6516	00-08-02-60-0E-9C	AeroScout Engine	2006-03-22 오후 8:20:34
10959	00-0b-cd-b5-06-27	McAfee VirusScan Enterprise	2006-04-18 오전 5:35:06
10650	00-0b-cd-b5-06-27	FMSSetup	2006-04-18 오전 5:35:06
10951	00-0b-cd-b5-06-27	Intel(R) Extreme Graphics Driver	2006-04-18 오전 5:35:06
10639	00-0c-be-59-ad-14	Win7P	2006-04-17 오전 1:07:23
8887	00-11-09-E1-9F-C6	대한민국전자정보인허발급프로그램	2006-04-03 오전 2:13:11
8888	00-11-09-E1-9F-C6	एमआई프로	2006-04-03 오전 2:13:11
9953	00-13-77-18-45-b9	dTomoyo.s 통합 코덱책 식재 (Type 3. 버전 7.0)	2006-04-07 오전 5:34:53
8399	00-06-18-09-9C-01	NetSupport Manager Client	2006-03-31 오전 8:45:16
8400	00-06-18-09-9C-01	ShareIt	2006-03-31 오전 8:45:16
10540	00-0c-be-59-ad-14	All Video Converter 1.9	2006-04-17 오전 1:07:23
8402	00-06-18-09-9C-01	SonySecurity-KO-WACO	2006-03-31 오전 8:45:16
8405	00-06-18-09-9C-01	HP Photo and Imaging 2.1 - Scanjet 2400 Series	2006-03-31 오전 8:45:16
8406	00-06-18-09-9C-01	Java 2 Runtime Environment, SE v1.4.2.05	2006-03-31 오전 8:45:16

그림 2 소프트웨어 저장 정보

능동형 에이전트에서 생성한 정보는 관리 시스템에서 다음 그림 3과 같이 관리된다.

210.107.130.110 정보

시스템 IP: 210.107.130.110 | 시스템 MAC: 00-30-20-7a-23-8e

시스템 모델: LENO-V2000 | BIOS 모델: (O)인텔(R)시

운영체제: Windows 2000 | 서비스 팩: SP3

사용자 부제: 기업용구소 | 사용자 이름: 박종민

사용자 권한: 42-086-A6A8 | 사용자 이메일: d4r@net.com

CPU 정보: Intel Architecture Processor MKC compatible 3200 MHz CPU

RAM 정보: 255 MB

하드 디스크: 2개 (F, G, H, I, J, K)

모뎀 정보: VMware USB L

LAN 정보: VMware Access Point (NIC PC) Adapter

CD-ROM 정보: Generic DVD-R/DL

그림 3 에이전트 시스템 정보

SW 라이선스 관리

번호	SW 이름	라이선스 수	사용자 수	상태	해당자(구분)	수정	삭제
1	Shackelforth	1000	4	정상	(C)구분관리	수정	삭제
2	공공	100	2	정상	대외보안프로그램	수정	삭제
3	한글 오피스 2005	20	2	정상	한글과컴퓨터	수정	삭제
4	VMware Tools	10	2	정상		수정	삭제

그림 4 라이선스 정보 관리

불법 소프트웨어 사용자로 설정된 에이전트 시스템은 네트워크의 통제 대상이 된다. 본 논문에서 네트워크를 통제하는 방식은 두 가지로 제안한다. 첫 번째는 불법 소프트웨어 사용자 에이전트의 네트워크 사용 전체를 차단하는 것이다. 에이전트에서 불법 소프트웨어 사용자를 공지하고 소프트웨어를 삭제할 때까지 네트워크 사용을 차단하는 방식이다. 두 번째는 네트워크 사용 중 웹의 사용만을 제어하는 방식이다. 불법 소프트웨어를 사용하는 에이전트는 웹 브라우저를 통해 인터넷을 사용할 때 정상적으로 사용할 수 없고, 불법 소프트웨어를 삭제하라는 경고 웹페이지를 강제로 보게 되는 방식이다.[5][6]

Adapter selected

NIC 목록

- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0
- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0
- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0

시스템에 있는 NIC 목록

- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0
- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0
- (E)SFPB11-95C7-4E2-9796-6930E1E1A5A0

그림 5 미러링을 위한 랜카드 설정

웹페이지를 강제로 보이기 위해 네트워크 통제시스템은 두개의 랜카드를 사용한다. 하나는 패킷을 미러링 받고, 하나는 패킷을 전송하기 위한 통신 포트 사용한다.

그림 6은 전체 소프트웨어 사용현황과 해당 소프트웨어를 사용하는 에이전트 정보를 보인다. 그림 5는 미러 포트와 통신포트를 지정하는 그림이다.[7]

SW 현황

번호	SW 이름	라이선스 수	사용자 수	정확률	해당자(구분)
1	공공	100	2	0%	(공공)구분
2	SPF	0	2	0%	(공공)구분
3	대한민국전자정보인허발급프로그램	1	1	0%	(공공)구분
4	한글 오피스 2005	1	1	0%	(공공)구분
5	한글 오피스 2005	1	1	0%	(공공)구분
6	한글 오피스 2005	1	1	0%	(공공)구분

번호	IP	시스템명	사용자 수	정확률	운영체제	연속시간
1	210.107.130.110	박종민	기업용구소	기업용구소	WindowsXP	99-60%
2	210.107.130.110	박종민	기업용구소	기업용구소	WindowsXP	99-60%

그림 6 소프트웨어 사용자 현황

또한 에이전트 시스템에 불법 소프트웨어의 사용을 통제하기 위해 강제 실행 차단 정책을 수행한다. 에이전트에서 불법소프트웨어가 삭제되면 에이전트는 설치된 소프트웨어 정보를 갱신하여 관리서버로 불법 소프트웨어 정보가 삭제된 정보를 전송하게 된다. 에이전트로부터 새로운 소프트웨어 설치정보를 전송받은 관리서버 데몬은 네트워크 차단 목록에서 해당 에이전트의 차단 정보를 삭제하고 네트워크 차단 및 소프트웨어 실행 차단 정책을 자동으로 해제한다. 차단목록으로의 추가/제거는 해당 테이블에 트리거(Trigger)를 생성하여 자동으로 추가 및 삭제가 이루어지도록 구현한다.[8]

그림 7은 에이전트에 설정된 소프트웨어 실행 차단 정책 현황을 나타낸다. 소프트웨어 차단 정책은 관리자가 소프트웨어 이름과 실행 프로세스 이름을 지정한다. 설정한 차단 정책은 에이전트로 전송되어 에이전트는 해당 소프트웨어서 클라이언트 시스템에서 실행되면 시스템 사용자에게 관리자에 의해 차단된 소프트웨어임을 알리고 실행되는 프로세스를 Kill하여 실행을 차단하도록 구현했다.[9][10] 실행이 차단되는 프로세스 정보는 관리자에 의해 자유롭게 추가 및 제외가 가능하다.

◎ SAW실행통제

순번	SAW 이름	시스템 프로세스 이름	실행 차단 수	권한 수	차단 해제
1	모놀	cmd.exe	1	2	취소하기
2	인텔 도킹소 2055	cmd.exe	2	1	취소하기
3	Emulnet#2200	cmd.exe	2	1	취소하기

순번	시스템 IP	시스템 MAC	차단 대상	권한
1	210.107.130.110	09-0c-25-3a-25-9c	SP100	하드그룹-1
2	210.107.130.155	09-0c-25-3a-25-9c	SP100	하드그룹-1

그림 7 소프트웨어 실행 통제 정책 현황

4. 결론

본 논문에서는 최근 공공기관, 학교, 기업 등에서 사용되고 있는 소프트웨어가 정품이 아닌 불법적인 공유를 통해 설치되어 사용되는 소프트웨어 설치 정보를 효과적으로 파악하고 이에 능동적으로 대응하는 방법을 제안하였다. 클라이언트 시스템에 에이전트를 설치함으로써 정확한 소프트웨어 설치 현황과 시스템의 네트워크정보 등을 파악할 수 있다. 또한 전체 또는 개별 공지를 통해 불법소프트웨어를 제거를 권고하는 방식으로는 삭제가 어려우므로 네트워크를 강제적으로 통제함으로써 삭제를 또한 높일 수 있다.

불법 상용 소프트웨어의 사용을 줄임으로써 정품 사용을 권장하고 궁극적으로 건전한 소프트웨어 사용문화를 정착시킬 수 있을 것으로 기대된다.

향후 연구 과제로는 본 논문에서는 윈도우 기반의 에이전트를 구현하였다. 이에 윈도우 외의 리눅스 또는 유닉스 계열의 시스템의 에이전트 개발을 통하여 좀더 폭넓게 시스템을 관리할 수 있도록 추가적인 연구가 필요하다.

다.

[참고문헌]

- [1] Seki, N.Shiratori,M.Miyoshi,T.Yamashita, Application of Surface Crack Analysis System 'SCAN' to cracks at hole, ASME-PUBLICATIONS-PVP, Vol.447. 2002
- [2] Wang,X-1.Ge,Y-j.Jiang,J. Research and Foundation on System Info of Signal Processing in Science and Technology of Information Acquisition. INFORMATION AND CONTROL -SHENYANG- Vol.33 No.2. 2004
- [3] 이창훈. 지능형 에이전트 시스템을 위한 변환 에이전트 설계에 관한 연구. 건국기술연구논문지. 1996
- [4] 한승완, 임형석. 이동 에이전트 기반 전자상거래 시스템에서의 안전한 이동 에이전트 전송 프로토콜. 정보처리학회논문지. 2000
- [5] 광인섭, 강홍식. NSAT을 이용한 네트워크 취약성 점검 시스템 설계 및 구현. 인재대학교논문지. 2004
- [6] 윤정모. 소프트웨어 사용권 관리 에이전트 시스템 구현. 서울대학교 논문집. Vol.51 No2. 2000
- [7] 에이전트 이동성을 이용한 원격관리 시스템 구현. 전자정보통신연구소 논문집. Vol.4 No.1. 2001
- [8] 황기태, 김남윤. 윈도우 운영체제에서 불법 소프트웨어 방지 시스템. 한국정보처리학회. 2004
- [9] 윤홍상, 정창렬, 임형권, 고진광. 이동 에이전트를 이용한 네트워크 자원 접근 통제 기법. 한국멀티미디어학회. 1999
- [10] 최준호, 김판구. 네트워크상에서 바이러스 차단을 위한 방화벽 시스템의 설계 및 구현. 한국정보처리학회. 2001