(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년03월30일
(11) 등록번호 10-0949808
(24) 등록일자 2010년03월19일

(51) Int. Cl.
H04L 12/24 (2006.01) *G06F 15/00* (2006.01)
(21) 출원번호 10-2007-0126650
(22) 출원일자 2007년12월07일
심사청구일자 2007년12월07일
(65) 공개번호 10-2009-0059669
(43) 공개일자 2009년06월11일
(56) 선행기술조사문헌
KR1020070097485 A*
EP1096756 A1
JP2004146973 A
KR1020040055196 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
한국전자통신연구원
대전 유성구 가정동 161번지
(72) 발명자
문용혁
인천 계양구 작전2동 우암센스뷰 101동 1003호
나재훈
대전 서구 삼천동 가람아파트 12-1301
(뒷면에 계속)
(74) 대리인
한양특허법인

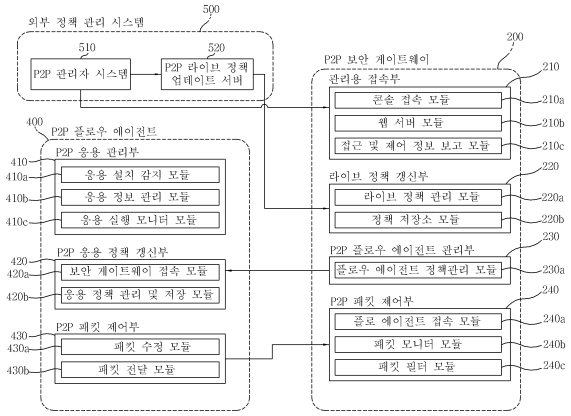
전체 청구항 수 : 총 21 항 심사관 : 천대녕

(54) P 2 P 트래픽 관리 장치 및 그 방법

(57) 요 약

본 발명은 P2P 트래픽 관리 장치 및 그 방법에 관한 것으로, P2P 플로우 에이전트가 실행 중인 응용 프로그램을 모니터링하며 P2P 응용 프로그램을 추출하고, 설정된 정책에 따라 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하여 전송하면, P2P 보안 게이트웨이가 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 가하는 것을 특징으로 한다.

대 표 도 - 도5



(72) 발명자

유재호

경기 성남시 분당구 야탑동 68번지 첨단기술연구센터 406호

장종수

대전 유성구 전민동 엑스포아파트 303-903

권혁찬

대전 서구 내동 5 벽산맑은아침아파트 104-1802

고선기

대전 서구 내동 롯데아파트 109-1204

구자범

서울 동작구 사당동 163-5

이 발명을 지원한 국가연구개발사업

과제고유번호	2005-S-090-03
부처명	정보통신부 및 정보통신연구진흥원
연구사업명	IT성장동력기술개발
연구과제명	유무선 IPv6 기반 P2P 네트워크 정보보호 기술 개발
주관기관	한국전자통신연구원
연구기간	2007-03-01 ~ 2008-02-28

특허청구의 범위

청구항 1

암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하는 시스템에 있어서,

실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하여 전송하는 P2P 플로우 에이전트; 와

상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 수행하는 P2P 보안 게이트웨이를 포함하는 P2P 트래픽 관리 시스템.

청구항 2

청구항 1에 있어서,

도메인 관리자로부터 입력되는 신규 정책을 감지하고, 감지된 신규 정책 및 운영 규칙을 상기 보안 게이트웨이로 제공하는 라이브 정책 업데이트 서버를 더 포함하는, P2P 트래픽 관리 시스템.

청구항 3

청구항 2에 있어서,

상기 감지된 신규 정책을 상기 보안 게이트웨이로 제공함에 있어,

i) 상기 라이브 정책 업데이트 서버가 네트워크 내의 적어도 하나의 상기 보안 게이트웨이로 상기 감지된 신규 정책을 전송하는 제1 라이브 정책 업데이트 방법, 또는 ii) 상기 라이브 정책 업데이트 서버가 하나의 보안 게이트웨이로 상기 감지된 신규 정책을 전송하고, 이를 수신한 상기 하나의 보안 게이트웨이가 네트워크 내의 나머지 보안 게이트웨이로 상기 신규 정책을 전송하는 제2 라이브 정책 업데이트 방법을 이용해, 상기 감지된 신규 정책을 상기 보안 게이트웨이로 전송하는 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 4

청구항 1에 있어서,

상기 패킷에 대한 제어는,

패킷의 선별적 통과, 대역폭 제한, 패킷 폐기, 우선순위 변경, 및 서비스 차등화 중 적어도 하나인 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 5

청구항 4에 있어서,

상기 패킷의 선별적 통과 및 상기 대역폭 제한의 경우에는, 상기 패킷으로부터 상기 응용 식별 정보를 제거하거나 또는 언인캡슐레이션(Unencapsulation)시켜 네트워크로 전송하는 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 6

청구항 1에 있어서,

상기 P2P 플로우 에이전트는,

P2P 응용 프로그램을 실행을 감지하는 경우, 상기 P2P 응용 프로그램의 프로세스 실행 정보를 이용하여 P2P 응용 프로그램 정보를 획득하고, 상기 획득한 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하며, 상기 P2P 응용 프로그램의 프로세스로부터 패킷을 생성하여 전송하고자 하는 시도가 탐지되면, 상기 획득한 정책에 따라 상기 패킷에 대해 제어를 수행하는, P2P 트래픽 관리 시스템.

청구항 7

청구항 2에 있어서,

상기 P2P 보안 게이트웨이는,

상기 라이브 정책 업데이트 서버로부터 정책 내역을 수신하고, 수신한 정책 내역의 신규성 및 상기 정책 내역의 버전이 기존에 운영 중인 정책과 충돌되는지 여부를 검증하며, 검증 결과에 따라 정책 저장소에 저장된 데이터를 업데이트하는 라이브 정책 갱신부를 포함하는 P2P 트래픽 관리 시스템.

청구항 8

청구항 3에 있어서,

상기 라이브 정책 업데이트 서버는,

상기 도메인 관리자로부터 입력되는 신규 정책을 수신하고, 수신한 신규 정책이 기존의 기본 정책과 위배되는지 여부를 체크하고, 체크 결과에 따라 입력된 신규 정책을 새로운 기본 정책으로 설정하고, 상기 제1 라이브 정책 업데이트 방법 또는 상기 제2 라이브 정책 업데이트 방법 중 어느 방법으로 업데이트를 수행할 것인지 결정하여, 결정된 업데이트 방법을 이용해 상기 P2P 보안 게이트웨이로 상기 신규 정책을 전송하는, P2P 트래픽 관리 시스템.

청구항 9

청구항 8에 있어서,

상기 P2P 보안 게이트웨이는,

상기 라이브 정책 업데이트 서버로부터 상기 제2 라이브 정책 업데이트 방법을 통해 신규 정책을 수신한 경우, P2P 방식을 통해 네트워크 내의 다른 P2P 보안 게이트웨이들로 상기 신규 정책을 전송하고,

이를 수신한 네트워크 내의 상기 다른 P2P 보안 게이트웨이들은, 수신한 신규 정책의 버전 및 기존의 정책과의 충돌 여부를 검증하고, 검증 결과에 따라 내부의 정책 저장소 모듈을 업데이트하는 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 10

청구항 9에 있어서,

상기 P2P 보안 게이트웨이는,

신규 정책 내역이 적절히 반영되었는지 인지하고, 적용된 신규 정책 내역이 상기 P2P 플로우 에이전트에 반영될 필요성이 있는지 판단하여, 필요성이 있는 경우 상기 신규 정책의 버전을 P2P 플로우 에이전트용으로 간소화하여 변환하고, 버전 변환된 상기 정책을 상기 P2P 플로우 에이전트로 전송하는 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 11

청구항 10에 있어서,

상기 P2P 플로우 에이전트는,

상기 P2P 보안 게이트웨이로부터 상기 정책을 수신하고, 수신한 정책의 포맷, 버전, 및 기존의 정책과의 충돌 여부를 검증하여, 검증 완료된 정책을 운용에 반영하고, 상기 정책의 검증 완료 여부를 상기 P2P 보안 게이트웨이로 통보하는 것을 특징으로 하는, P2P 트래픽 관리 시스템.

청구항 12

암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하기 위해 P2P 보안 게이트웨이와 상호 연동하는 P2P 플로우 에이전트에 있어서,

실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프

로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하는 P2P 플로우 에이전트.

청구항 13

청구항 12에 있어서,

신규 P2P 응용 프로그램의 설치를 감지하는 응용 설치 감지 모듈;

상기 감지된 신규 P2P 응용 프로그램을 저장하고, 기 설치된 P2P 응용 프로그램 관련 정보에 대한 조회 및 반환을 수행하는 응용 정보 관리 모듈; 및

P2P 응용 프로그램의 실행 여부 및 패킷 생성을 모니터링하여 보고하는 응용 실행 모니터 모듈을 포함하는 P2P 플로우 에이전트.

청구항 14

청구항 13에 있어서,

상기 응용 실행 모니터 모듈로부터 패킷 생성 감지를 보고받은 경우, 상기 생성된 패킷을 가로채어, 관련 정책 내역에 따라 상기 패킷에 제어를 수행하고, 제어된 패킷을 상기 P2P 보안 게이트웨이로 전송하는 P2P 패킷 제어부를 더 포함하는 P2P 플로우 에이전트.

청구항 15

암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하기 위해 P2P 플로우 에이전트와 상호 연동하는 P2P 보안 게이트웨이에 있어서,

상기 P2P 플로우 에이전트에서 감지된 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 조회된 관련 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자가 추가되고, 상기 응용 식별자가 추가되어 상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 수행하는, P2P 보안 게이트웨이.

청구항 16

청구항 15에 있어서,

상기 P2P 플로우 에이전트로부터 제어된 P2P 패킷을 수신하고, 수신한 P2P 패킷으로부터 응용 식별자 및 관련 정보를 추출하여 P2P 트래픽인지 여부를 판별하고, 상기 응용 식별자 및 관련 정보를 이용해 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 P2P 패킷 필터링의 제어를 수행하는 P2P 패킷 제어부; 와

네트워크 상의 라이브 정책 업데이트 서버로부터 정책 내역을 수신하고, 수신한 정책 내역이 신규한지 여부 및 상기 정책 내역의 버전이 기존에 운영 중인 정책과 충돌되는지 여부를 검증하며, 검증 결과에 따라 정책 저장소에 저장된 데이터를 업데이트하는 라이브 정책 갱신부를 포함하는 P2P 보안 게이트웨이.

청구항 17

암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하는 방법에 있어서,

P2P 플로우 에이전트가 실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하여 전송하는 단계; 와

P2P 보안 게이트웨이가, 상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 수행하는 단계를 포함하는 P2P 트래픽 관리 방법.

청구항 18

청구항 17에 있어서,

상기 P2P 플로우 에이전트가 각 패킷에 응용 식별자를 추가하여 전송하는 단계는,

상기 P2P 플로우 에이전트가, P2P 응용 프로그램을 실행을 감지하는 경우, 상기 P2P 응용 프로그램의 프로세스 실행 정보를 이용하여 P2P 응용 프로그램 정보를 획득하고, 상기 획득한 P2P 응용 프로그램 정보를 이용해 관련 정책을 조회하는 단계; 와

상기 P2P 플로우 에이전트가, 상기 P2P 응용 프로그램의 프로세스로부터 패킷을 생성하여 전송하고자 하는 시도를 탐지하면, 조회된 상기 정책에 따라 상기 패킷에 대해 제어를 수행하는 단계를 포함하는, P2P 트래픽 관리 방법.

청구항 19

청구항 17에 있어서,

라이브 정책 업데이트 서버가, 도메인 관리자로부터 입력되는 신규 정책을 감지하고, 감지된 신규 정책 및 운영 규칙을 상기 보안 게이트웨이로 제공하는 단계를 더 포함하는, P2P 트래픽 관리 방법.

청구항 20

청구항 19에 있어서,

상기 P2P 보안 게이트웨이가, 상기 라이브 정책 업데이트 서버로부터 정책 내역을 수신하고, 수신한 정책 내역이 신규한지 여부 및 상기 정책 내역의 버전이 기존에 운영 중인 정책과 충돌되는지 여부를 검증하는 단계; 와

상기 검증 결과에 따라 상기 P2P 보안 게이트웨이의 정책 저장소에 저장된 데이터를 업데이트하는 단계를 더 포함하는, P2P 트래픽 관리 방법.

청구항 21

청구항 19에 있어서,

상기 라이브 정책 업데이트 서버가, 상기 도메인 관리자로부터 입력되는 신규 정책을 수신하고, 수신한 신규 정책이 기존의 기본 정책과 위배되는지 여부를 체크하고, 체크 결과에 따라 입력된 신규 정책을 새로운 기본 정책으로 설정하고, 상기 P2P 보안 게이트웨이로 상기 신규 정책을 전송하는 단계를 더 포함하는, P2P 트래픽 관리 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 P2P 트래픽 관리 장치 및 그 방법에 관한 것으로, 좀 더 구체적으로는 네트워크상에서 피어 투 피어(Peer-to-Peer, 이하 P2P) 응용 서비스 또는 응용 프로그램을 통해 송수신되는 암호화된 패킷을 인지하고 정보의 유해성 또는 불법성 여부에 근거한 도메인 정책에 따라 P2P 트래픽을 선별적으로 통과, 차단, 제어하기 위한 P2P 보안 게이트웨이와 P2P 플로우 에이전트 상호 협력 모델 기반의 P2P 유해 트래픽 탐지 및 그 제어에 관한 것이다.

[0002] 본 발명은 정보통신부의 IT성장동력핵심기술개발사업의 일환으로 수행한 연구로부터 도출된 것이다(과제관리번호: 2005-S-090-03, 과제명: 유무선 IPv6 기반 P2P 네트워크 정보 보호 기술 개발(Development of P2P Network Security Technology based on Wired/Wireless IPv6 Network)).

배 경 기 술

[0003] 기존의 P2P 네트워크는 분산된 컴퓨팅 자원(컴퓨터 자체 또는 파일, 소프트웨어 등의 논리 자원 등)을 활용하여 상업적으로는 냅스터, 베어쉐어, 라임와이어, 모피어스, 위니, 푸르나, E-Donkey 또는 연구적으로는 Gnutella,

Kazaa, BitTorrent, Pastry, Chord 등과 같이 파일, 음악, 동영상 등의 멀티미디어 자원의 공유를 원활하게 하는 기술적 수단으로 사용 및 연구되어 대중의 넓은 지지와 범용적 사용자층을 확보한 바 있다. 또한, SATI@HOME와 같이 실험적 목적으로 프로세서 사이클, 저장 공간, 데이터베이스 등의 분산된 자원을 이용하여 대단위 컴퓨팅 시스템을 구축하는 등의 학술적 용도로 사용되어 왔다.

[0004] 그러나 근래에 들어 Pure P2P 아키텍처에 서버를 적절히 포함시킨 하이브리드 P2P 아키텍처를 제공하는 P2P 프레임워크 중 Kazaa를 기반으로 하는 SKYPE와 같은 P2P VoIP 서비스 및 JOOST와 같이 차세대 TV를 표방하는 P2P 스트리밍 서비스가 인터넷으로 제공되고 있어, 통상적으로 MP3와 같은 음악 파일 정도를 공유하거나 메시징 서비스 정도의 응용 서비스로 인식되어 온 P2P 네트워크 응용에 대한 인식 전향의 필요성이 대두되고 있다.

[0005] 이와 같이 일반적으로 P2P 응용 서비스 또는 응용 프로그램은, P2P 방식의 네트워크 프로토콜을 이용하여 상호 통신하거나, 클라이언트와 서버의 역할을 동시에 수행하는 피어들로 구성된 네트워크에 참여하는 네트워크 어플리케이션 또는 썬마이크로시스템즈(Sun Microsystems)의 JXTA와 같은 P2P 프레임워크를 기반으로 동작하는 네트워크 애플리케이션으로 정의될 수 있으며, 다양한 네트워크 규모 하에서 응용의 목적에 따라 파일공유, VoIP, 동영상 스트리밍, 분산 컴퓨팅 등의 각기 다른 용도로 적용될 수 있다.

[0006] P2P 응용 서비스 또는 응용 프로그램에서는, 경우에 따라 P2P 네트워크에 참여하는 컴퓨터를 노드(Node), 피어(Peer), 호스트(Host) 등으로 기존의 컴퓨터 과학 또는 네트워크 분야 용어와 구분없이 사용하지만, 피어라는 용어로 명확히 구분 짓는 것이 중앙 서버 없이 서비스를 제공하거나 사용하는 두 가지 기능을 모두 취하는 P2P 기술의 특징을 제대로 반영하는 것이라 할 것이다.

[0007] P2P 네트워크에서는 기존의 분산 컴퓨팅 환경에서 고려될 수 있는 보안 취약성(중간자 공격(Man in the middle attack), 서비스 거부 공격(Denial of Service), 바이러스(Insertion of Virus), 웜(Warm), 스파이웨어(Spyware), 스팸(Spamming)) 뿐만 아니라 피어의 자유로운 참여 및 탈퇴, 신규 아이디의 저비용, 비제한적 생성 그리고 피어 식별자 검증 구조의 부재 등의 특성으로 인해 P2P 네트워크만의 고유한 보안 요구사항들(White Washing, ID Spoofing, Sybil Attack, Eclipse Attack, Storage & Retrieval Attack, Privacy Violation) 을 갖게 되었다.

[0008] 그러나 현존하는 P2P 네트워크의 가장 심각한 보안 취약성은 대용량 P2P 트래픽(특히, 파일 공유를 위한 P2P 네트워크)의 유통이라는 특성에 기인한다고 할 수 있다. P2P 파일 공유 네트워크는 이미, 전체 네트워크 트래픽 양의 60% ~ 80% 이상을 점유할 정도로 급성장하였다. 또한, CISCO사는 최근 2007년 보고서를 통해 2011년에 P2P 트래픽은 현재의 4배 이상에 달할 것으로 관측하는 전망을 발표한 바 있다. 이는 실제 인터넷을 구성하는 네트워크 장비의 대부분이 P2P 네트워크 트래픽을 처리하는 데 많은 프로세싱 능력을 소비하고 있다는 것을 의미하며, 나아가 이로 인해 네트워크 병목 현상(Bottleneck)이나 폭주(Congestion) 등이 빈번하게 발생되는 문제가 초래되고 있다. 또한 대부분의 인터넷 서비스 업체(ISP: Internet Service Provider)는 P2P 트래픽 처리로 인한 큰 비용적 손실을 감수하고 있는 것으로 보고되고 있다. P2P 사용자가 점차 늘어나고, 많은 응용 서비스가 P2P 네트워크를 기반으로 제공될수록 이와 같은 문제점의 심각성은 더욱 심화될 것이다.

[0009] 특히, 최근 P2P 네트워크를 이용한 응용 서비스 및 응용 프로그램이 새로운 콘텐츠 유통 구조 또는 콘텐츠 전달 네트워크(Content Delivery Network)를 형성하고 있어 불법자료의 유통, 기밀자료의 전파, 악성코드를 포함한 첨부 파일의 전달 등에 대한 사전 탐지 및 차단 등의 보안 요구 사항이 크게 요구되고 있고, P2P 기술이 다양한 응용 서비스를 위한 기본 네트워크 모델로서 활발히 활용되고 있는 추세이며, 그에 따라 종전에 비해 인터넷 트래픽 점유율을 보다 높여갈 것으로 예상되기 때문에, 이에 대한 보안 대책이 필요하다.

[0010] 이러한 문제점과 관련하여, 일반적인 네트워크 응용 서비스가 유발시키는 트래픽 폭증 또는 병목현상 등을 해결하기 위한 휴리스틱(Heuristic) 방안으로, “트래픽 양과 시간 임계치(Traffic Volume Threshold and Time Threshold)에 기반한 방법론"이 일반적으로 네트워크 장비(방화벽(Firewall), 침입탐지시스템(IDS: Intrusion Detection System), 침입방지시스템(Intrusion Prevention System))에 적용되어 왔으나, P2P 네트워크의 경우 그 기술 규격(프로토콜 또는 프레임워크) 및 실제 서비스 운용 시 발생하는 네트워크 상태가 매우 가변적이므로, 상기 방법론은 유해 P2P 트래픽을 탐지하거나 P2P 응용 서비스를 인지하여 이를 제어하는 방안으로 적절하지 못하다.

[0011] 네트워크 트래픽을 선별적으로 탐지하여 이를 제어하는 방법론으로는, 상기 방법론을 포함하여 크게 6가지로 구분될 수 있으며, 현재의 IDS 및 IPS와 같은 상용 네트워크 보안 장비의 경우 주로 “시그니쳐(Signiture)” 혹은 그와 유사한 방법론을 채택하여 P2P 네트워크를 차단하고자 노력하고 있다.

[0012] 그 중 먼저 패킷 인스펙션(Packet Inspection) 방법론에 대해 살펴보면, 이 기법은 "비상태형 패킷 인스펙션(Stateless Packet Inspection)"과 "상태형 패킷 인스펙션(Stateful Packet Inspection)"으로 나뉠 수 있다. 전자의 경우 유입되는 패킷별로 서비스 포트 또는 헤더의 특정 필드 값을 보고 간단히 판단하는 방법이며, 개별 패킷 단위로 판별하기 때문에 여러 패킷을 조합해야만 판별할 수 있는 네트워크 이상 징후에 대한 탐지가 불가능하고, P2P 응용 서비스에서 흔히 사용되는 포트 이동(Port Shifting), 랜덤 포트(Random Port) 등과 같은 이슈(Issue)에 대해서는 취약한 단점이 존재한다. 또한 후자는 특정 네트워크 트래픽을 구별할 수 있도록 사전에 트래픽에 대한 역 엔지니어링(Reverse Engineering) 또는 패킷 기술 규격 분석 등의 작업을 통해 생성된 시그니쳐를 토대로 네트워크 장비를 거쳐가는 트래픽을 검토하는 기법을 의미한다. 시그니쳐 데이터베이스와 유입되는 패킷의 유형을 비교하기 위해서는 패킷의 헤더뿐만 아니라 페이로드를 모두 검토해야 하므로(계층 7 상에서만 비교 작업이 이뤄진다고 할지라도) 네트워크 장비에 대단히 많은 오버헤드(Overhead)가 발생하게 되는 단점이 있고, 네트워크 응용 서비스별로 별도의 시그니쳐가 요구되며, 하나의 시그니쳐 생성을 위한 분석 과정에 많은 시간과 경비가 소비되는 등의 문제점이 약점으로 지적될 수 있다.

[0013] 패킷 인스펙션이 정형적인 패턴(Pattern)에 근간을 둔 기법이라면, 휴리스틱 방법론은 네트워크 응용 서비스의 운용 특성이나 응용 서비스가 발생시키는 트래픽 자체의 행동양식(Traffic Behavior)에 따라 판단의 근거를 설정하는 기법이라 할 수 있다. 이 방법에서는 "플로우 레벨 행동양식(Flow Level Behavior)"과 "트랜잭션 레벨 행동양식(Transaction Level Behavior)", 두 가지 기법으로 분류될 수 있다. 전자는 패킷의 "Inter-Arrival Time, Inter-Packet Difference, Duration of Flow, Packet Size" 등에 관한 평균, 분포, 편차 등과 같은 실험 통계치에 근거하여 특정 P2P 트래픽을 감지하고자 하는 방안이다. 후자는 패킷의 크기 또는 플로우의 방향과 같은 각 패킷의 속성의 상태 전이로부터 특성을 추출하여 P2P 트래픽을 인지하고자 하는 방법론이다. 그러나 상기 기술한 두 가지 휴리스틱 방법론은 P2P 네트워크의 규모가 클수록, 모니터링 기간이 길수록, 또한 지리적으로 분산된 많은 피어를 대상으로 실험할수록 보다 P2P 트래픽을 탐지하기에 적합한 통계치의 추출이 가능 할뿐만 아니라, 네트워크를 구성하는 피어가 유발시키는 예측 불가능한 행동 패턴에 따라 네트워크의 상태가 대단히 가변적일 수 있으므로, P2P 트래픽 탐지율에 대한 보장성이 떨어진다. 또한 해당 기법은 기술적 선도성은 있으나 일부 연구자의 소규모 P2P 네트워크를 대상으로 한 논문 연구사례로서만 제안되고 있는 실정이기 때문에 그 실효성에 대한 적극적이고 체계적인 검증이 추가적으로 요구되고 있어, 상용 네트워크 장비로의 실시는 고려되지 않고 있다.

[0014] 그 외 여섯째 방법론으로 "피어 행동 유형(Peer Behavior)"(특히, UDP 패킷 크기 또는 연결을 맺는 횟수, 연결을 맺는 방법(IP 주소 및 포트 개수 등)) 등에 의존한 단편적인 탐지 규칙(Rule)들이 제안되고 있으나, 적극적인 실시예가 전무하며, 실시 예에 따른 탐지율에 관한 명확한 결과 데이터가 존재하지 않고 있다.

[0015] 참고적으로 상기 기술된 기법 각각은 다른 방법론과 병합될 수 있으며, 개별적으로 휴리스틱 특성을 포함하도록 확장될 수 있어 다른 방식의 기술적 구분 및 정의가 가능할 수 있다.

[0016] 이상 기술한 모든 방법론은 대다수의 상용 P2P 네트워크의 각기 다른 기술 규격과 운용시 발생하는 가변성에 대한 문제점으로 인해 보편적으로 안정화되고 의미 있는 P2P 트래픽 탐지율을 제공하고 있지 못하고 있다. 무엇보다도 P2P 트래픽 또는 P2P 응용 서비스의 탐지를 어렵게 만드는 주요 원인은 바로 암호화된 P2P 패킷(Encrypted P2P Packet)의 등장이다. 대표적으로 SKYPE, BitTorrent, JOOST 등의 P2P 응용 서비스가 제어 패킷(Control or Signal Packet)은 물론, 모든 데이터 패킷을 암호화하여 전달하는 기술 규격을 따르고 있어, 기존의 단순 매칭 기법이나 정형화된 패턴에 의존한 방법론의 사용으로는 패킷에 대한 검사가 불가능하므로, P2P 트래픽 여부에 관한 판별이 사실상 어렵고, 경험론적 휴리스틱에 근간을 둔 방법론 역시 대규모 실험 사례를 통한 실효성 검증이 미비하며, 페이로드에 대한 직접적인 분석보다는 단편적인 패킷 전송의 외형적 특성이나 유형을 분석하는 데 그치고 있어 그 실시예를 찾아보기 힘들다.

발명의 내용

해결 하고자하는 과제

[0017] 살펴본 바와 같은 문제점을 고려할 때, 피어 행동 유형에 근거한 방법론을 제외하고는 대부분의 기존 기법이 주로 네트워크상에서 패킷을 분석하여 트래픽의 유입을 제어를 수행하고자 하는 측면이 강하다고 할 수 있다. 따라서 P2P 트래픽 제어의 주요한 방안으로 "피어와 네트워크 장비간의 상호 작용을 기반으로 하는 모델"과 같은 보다 명시적인 방법론을 통해서만 암호화된 P2P 패킷의 탐지 및 이의 제어가 가능할 것이다.

[0018] 본 발명은 상술한 문제점을 해결하기 위한 것으로, 헤더 또는 페이로드에 대한 조사가 불가능한 암호화된 P2P

패킷을 생성하여 송수신하는 P2P 응용 서비스 또는 응용 프로그램을 선별적으로 인지하여 제어하는 P2P 트래픽 관리 장치 및 그 방법을 제공하는 것을 목적으로 한다.

과제 해결수단

[0019] 본 발명의 일 측면에 따른 P2P 트래픽 관리 시스템은, 암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하기 위한 것으로, 실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하여 전송하는 P2P 플로우 에이전트와 상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 가하는 P2P 보안 게이트웨이를 포함한다.

[0020] 상기 시스템은, 도메인 관리자로부터 입력되는 신규 정책을 감지하고, 감지된 신규 정책 및 운영 규칙을 상기 보안 게이트웨이로 제공하는 라이브 정책 업데이트 서버를 더 포함할 수 있다.

[0021] 상기 감지된 신규 정책을 상기 보안 게이트웨이로 전송함에 있어, i) 상기 라이브 정책 업데이트 서버가 네트워크 내의 적어도 하나의 상기 보안 게이트웨이로 상기 감지된 신규 정책을 전송하는 제1 라이브 정책 업데이트 방법, 또는 ii) 상기 라이브 정책 업데이트 서버가 하나의 보안 게이트웨이로 상기 감지된 신규 정책을 전송하고, 이를 수신한 상기 하나의 보안 게이트웨이가 네트워크 내의 나머지 보안 게이트웨이로 상기 신규 정책을 전송하는 제2 라이브 정책 업데이트 방법을 이용해 전송하는 것을 특징으로 한다.

[0022] 상기 패킷에 대한 제어는, 패킷의 선별적 통과, 대역폭 제한, 패킷 폐기, 우선순위 변경, 및 서비스 차등화 중 적어도 하나인 것을 특징으로 한다.

[0023] 상기 패킷의 선별적 통과 및 상기 대역폭 제한의 경우에는, 상기 패킷으로부터 상기 응용 식별 정보를 제거하거나 또는 언인캡슐레이션(Unencapsulation)시켜 네트워크로 전송하는 것을 특징으로 한다.

[0024] 상기 P2P 플로우 에이전트는, P2P 응용 프로그램을 실행을 감지하는 경우, 상기 P2P 응용 프로그램의 프로세스 실행 정보를 이용하여 P2P 응용 프로그램 정보를 획득하고, 상기 획득한 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하며, 상기 P2P 응용 프로그램의 프로세스로부터 패킷을 생성하여 전송하고자 하는 시도가 탐지되면, 상기 획득한 정책에 따라 상기 패킷에 대해 제어를 수행한다.

[0025] 상기 P2P 보안 게이트웨이는, 상기 라이브 정책 업데이트 서버로부터 정책 내역을 수신하고, 수신한 정책 내역의 신규성 및 상기 정책 내역의 버전이 기존에 운영 중인 정책과 충돌되는지 여부를 검증하며, 검증 결과에 따라 정책 저장소에 저장된 데이터를 업데이트하는 라이브 정책 갱신부를 포함한다.

[0026] 상기 라이브 정책 업데이트 서버는, 상기 도메인 관리자로부터 입력되는 신규 정책을 수신하고, 수신한 신규 정책이 기존의 기본 정책과 위배되는지 여부를 체크하고, 체크 결과에 따라 입력된 신규 정책을 새로운 기본 정책으로 설정하고, 상기 제1 라이브 정책 업데이트 방법 또는 상기 제2 라이브 정책 업데이트 방법 중 어느 방법으로 업데이트를 수행할 것인지 결정하여, 결정된 업데이트 방법을 이용해 상기 P2P 보안 게이트웨이로 상기 신규 정책을 전송한다.

[0027] 상기 P2P 보안 게이트웨이는, 상기 라이브 정책 업데이트 서버로부터 상기 제2 라이브 정책 업데이트 방법을 통해 신규 정책을 수신한 경우, P2P 방식을 통해 네트워크 내의 다른 P2P 보안 게이트웨이들로 상기 신규 정책을 전송하고, 이를 수신한 네트워크 내의 상기 다른 P2P 보안 게이트웨이들은, 수신한 신규 정책의 버전 및 기존의 정책과의 충돌 여부를 검증하고, 검증 결과에 따라 내부의 정책 저장소 모듈을 업데이트하는 것을 특징으로 한다.

[0028] 상기 P2P 보안 게이트웨이는, 신규 정책 내역이 적절히 반영되었는지 인지하고, 적용된 신규 정책 내역이 상기 P2P 플로우 에이전트에 반영될 필요성이 있는지 판단하여, 필요성이 있는 경우 상기 신규 정책의 버전을 P2P 플로우 에이전트용으로 간소화하여 변환하고, 버전 변환된 상기 정책을 상기 P2P 플로우 에이전트로 전송하는 것을 특징으로 한다.

[0029] 상기 P2P 플로우 에이전트는, 상기 P2P 보안 게이트웨이로부터 상기 정책을 수신하고, 수신한 정책의 포맷, 버전, 및 기존의 정책과의 충돌 여부를 검증하여, 검증 완료된 정책을 운용에 반영하고, 상기 정책의 검증 완료 여부를 상기 P2P 보안 게이트웨이로 통보하는 것을 특징으로 한다.

[0030] 본 발명의 다른 측면에 따른 P2P 플로우 에이전트는, 암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리하기 위해 P2P 보안 게이트웨이와 상호 연동하며, 실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가한다.

[0031] 상기 P2P 플로우 에이전트는, 신규 P2P 응용 프로그램의 설치를 감지하는 응용 설치 감지 모듈; 상기 감지된 신규 P2P 응용 프로그램을 저장하고, 기 설치된 P2P 응용 프로그램 관련 정보에 대한 조회 및 반환을 수행하는 응용 정보 관리 모듈; 및 P2P 응용 프로그램의 실행 여부 및 패킷 생성을 모니터링하여 보고하는 응용 실행 모니터 모듈을 포함하며, 상기 생성된 패킷을 가로채어, 관련 정책 내역에 따라 상기 패킷에 대해 제어를 수행하고, 제어된 패킷을 상기 P2P 보안 게이트웨이로 전송하는 P2P 패킷 제어부를 더 포함할 수 있다.

[0032] 본 발명의 또 다른 측면에 따른 P2P 보안 게이트웨이는, 상기 P2P 플로우 에이전트에서 감지된 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 조회된 관련 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자가 추가되고, 상기 응용 식별자가 추가되어 상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 수행한다.

[0033] 상기 P2P 보안 게이트웨이는, 상기 P2P 플로우 에이전트로부터 제어된 P2P 패킷을 수신하고, 수신한 P2P 패킷으로부터 응용 식별자 및 관련 정보를 추출하여 P2P 트래픽인지 여부를 판별하고, 상기 응용 식별자 및 관련 정보를 이용해 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 P2P 패킷 필터링의 제어를 수행하는 P2P 패킷 제어부와 네트워크 상의 라이브 정책 업데이트 서버로부터 정책 내역을 수신하고, 수신한 정책 내역이 신규한지 여부 및 상기 정책 내역의 버전이 기존에 운영 중인 정책과 충돌되는지 여부를 검증하며, 검증 결과에 따라 정책 저장소에 저장된 데이터를 업데이트하는 라이브 정책 갱신부를 포함한다.

[0034] 본 발명의 또 다른 측면에 따른 P2P 트래픽 관리 방법은, 암호화된 P2P 트래픽이 송수신되는 네트워크상에 존재하는 P2P 트래픽을 관리에 관한 것으로, P2P 플로우 에이전트가 실행 중인 응용 프로그램을 모니터링하여 P2P 응용 프로그램의 실행을 감지하고, 해당 P2P 응용 프로그램의 프로세스 실행 정보와 P2P 응용 프로그램 정보를 이용해 관련 정책 내역을 조회하여 조회된 정책 내역에 따라, 상기 응용 프로그램에 의해 발생되는 각 패킷에 응용 식별자를 추가하여 전송하는 단계; P2P 보안 게이트웨이가, 상기 P2P 플로우 에이전트로부터 유입되는 패킷을 모니터링하여 상기 응용 식별자가 포함된 패킷을 추출하고, 추출된 응용 식별자를 이용해 관련 정책을 조회하여 획득하고, 획득한 정책에 따라 상기 패킷에 대해 제어를 수행하는 단계를 포함한다.

효 과

[0035] 본원발명은, P2P 보안 게이트웨이 및 P2P 플로우 에이전트 상호 협력 모델을 이용하여 다양한 P2P 네트워크 및 P2P 아키텍처를 이용하는 범용의 응용 서비스 또는 응용 프로그램이 발생시키는 암호화된 트래픽을 탐지하고 이를 정책에 따라 제어함으로써, P2P 패킷의 헤더 또는 페이로드를 관찰하여 이를 분석할 필요가 없어짐으로 인해 IP 패킷 필터링 기법에 의존한 방법론에 비해 오버헤드를 크게 줄일 수 있으며, P2P 응용에 따른 별도의 시그니쳐 분석 및 개발로 인한 시간 및 비용의 손실을 줄일 수 있다. 또한, 플로우 분석 통계자료에 근거한 방법론이 잠재적으로 내포하는 정량적 수치 변동 가능성에 따른 오탐율을 최소화할 수 있어 명시적으로 P2P 응용을 제어할 수 있다는 장점을 제공한다.

발명의 실시를 위한 구체적인 내용

[0036] 본 발명은, P2P 네트워크 패킷 분석만을 통해 P2P 트래픽 탐지 기법을 제공하려는 종래의 기법 및 장치와는 달리 피어 측에 P2P 플로우 에이전트를 탑재하고 네트워크상에는 P2P 보안 게이트웨이를 설치하여 상호 연계를 통해 P2P 응용 프로그램 및 서비스의 설치 및 운용을 인지하고 패킷 생성 및 전달 시 이와 같은 상호 협력 모델을 기반으로 P2P 트래픽을 탐지하여 정책에 따라 효과적으로 P2P 트래픽을 제어하는 절차를 수행함으로써, 본 발명에서 목적하는 암호화된 P2P 트래픽의 탐지 및 제어를 쉽게 달성할 수 있다.

[0037] 이하, 본 발명의 바람직한 실시예를 도면을 참조하면서 설명하기로 한다.

[0038] 먼저, 도 1 내지 도 3을 통해 본 발명이 적용되는 네트워크 구성과 P2P 보안 서비스 구조에 대해 구체적으로 설

명하고자 한다.

[0039] 도 1은 본 발명이 적용되는 P2P 네트워크 구성도로서, 전체 P2P 보안 서비스 구조를 P2P 보안 서비스 도메인을 중심으로 도시하고 있다.

[0040] 본 발명에 따른 P2P 네트워크는, 라이브 정책 업데이트 서버(100), P2P 보안 게이트웨이(200), 도메인 관리자(300), P2P 보안 서비스 도메인을 구성하는 적어도 하나의 P2P 플로우 에이전트(400)를 포함하여 구성된다.

[0041] 하나의 논리적인 P2P 보안 서비스 도메인에 존재하는 각 피어에는 P2P 플로우 에이전트(400) 서비스(소프트웨어 모듈)가 탑재되어 있으며, 게이트웨이 네트워크 장비에는 P2P 보안 게이트웨이(200) 데몬(소프트웨어 모듈)이 설치되어 있다. 도 1을 참조하면, P2P 보안 게이트웨이(200)를 중심으로 라이브 정책 업데이트 서버(100), 도메인 관리자(300) 및 P2P 보안 서비스 도메인이 상호 연결을 맺고 있는데, 이와 같은 관계는 인터넷을 중심으로 지리적으로 분산되어 있는 각각의 P2P 보안 게이트웨이(200)에 확대 적용될 수 있는 구조적 특성을 갖는다.

[0042] 여기서, P2P 보안 서비스 도메인이라 함은 사내망을 구성하는 워크그룹(Work group), 서브넷 마스크(Subnet Mask)로 구분되는 하위 네트워크, 이더넷(Ethernet)으로 구성된 소단위의 임의 네트워크, 동일 정책이 적용되는 논리적인 단위의 네트워크 영역, 물리적으로 근접한 거리에 위치한 피어들로 구성된 그룹 및 P2P 서비스망의 하위 네트워크(Sub-Network) 등과 같은 다양한 의미로 고려될 수 있다.

[0043] 또한, 본 네트워크 구성에서 알 수 있듯이, 네트워크 장비에 대한 관리 또는 정책의 갱신을 위한 경우를 제외하고는 P2P 서비스 자체의 경우 별도의 중앙 서버가 존재하지 않는 환경을 고려한다. 즉, P2P 플로우 에이전트(400)는 실제 P2P 네트워크에 참여하여 통상적인 P2P 응용 서비스를 이용하는 주체(Servant)로서의 역할을 수행하고, P2P 보안 게이트웨이(200)는 네트워크 장비로서 P2P 응용 서비스를 이용할 때 발생하는 P2P 트래픽에 대한 탐지 및 제어를 담당하게 되며, 라이브 정책 업데이트 서버(100) 및 도메인 관리자(300)는 P2P 보안 게이트웨이(200)의 동작을 네트워크 환경 및 P2P 응용 서비스의 조건 변화에 맞게 조율하는 관리부(Management Domain)의 역할을 수행하게 된다.

[0044] 도 2는 도 1에 도시된 구성요소 간의 구체적인 연관 관계 및 상호 작용에 대해서 도시하고 있다.

[0045] 도 2에는 크게 P2P 보안 정책 도메인, P2P 보안 서비스 도메인 및 P2P 보안 관리 도메인의 총 3개의 영역이 존재한다.

[0046] 우선, P2P 보안 정책 도메인은 라이브 정책 업데이트 서버(100)와 도메인 관리자(300)를 포함하며, P2P 보안 서비스 도메인은 P2P 플로우 에이전트(400)를 탑재하고 있는 피어를 포함하고, P2P 보안 관리 도메인은 P2P 보안 게이트웨이(200)로 구성된다.

[0047] 이하에서는, 각 구성요소가 개별적인 역할을 수행함에 있어, P2P 응용 서비스 인식 및 트래픽 탐지/제어를 위해 네트워크에 연결된 다른 구성요소와 관련하여 기능하는 동작 및 그 결과에 대해서 기술한다.

[0048] 도메인 관리자(300)는 하나의 P2P 보안 게이트웨이(200)에 의해 운용되는 지역 망(Local Network) 서비스 규칙을 결정하고, 개별적인 네트워크 장비를 대상으로 결정된 정책을 적용(Enforcement)하는 역할을 수행한다. 또한 도메인 관리자(300)는 P2P 보안 게이트웨이(200)의 정책을 변경하거나 시스템 유지/보수를 수행하기 위해 접근할 수 있다. 접근에 따른 인증 및 권한 검증에 대한 사항은 네트워크 보안 및 컴퓨터 과학의 통상적인 기법에 준하며 한 방법에 국한되지 않고 다양한 기법에 의해 실시될 수 있다.

[0049] 적어도 하나의 P2P 보안 게이트웨이(200)에 의해 관찰되는 여러 지역 망의 정책을 결정하고 이를 네트워크 상황에 따라 망 전체의 P2P 보안 게이트웨이(200)에 적용하기 위해서, 도메인 관리자(300)는 해당 정책에 대한 명세서(Description)를 라이브 정책 업데이트 서버(100)에 제공한다. 라이브 정책 업데이트 서버(100)가 신규 또는 갱신된 정책 사항의 전파를 지시받게 되면, 각 개별 P2P 보안 게이트웨이에 접근하여 정책 사항의 업데이트를 통보하고 관련 명세서를 전달한다. 보다 상세한 정책 업데이트 방법에 대해서는, 도 3, 4 및 9를 통해 추후에 설명하기로 한다.

[0050] P2P 트래픽 탐지 및 제어를 위해 적합한 정책 및 동작 내역을 탑재한 P2P 보안 게이트웨이(200)는 통상적으로 P2P 응용 서비스가 발생하는 트래픽에 의해 발생할 수 있는 보안 취약점을 탐지하여 해결하는 P2P 보안 관리 도메인으로서의 역할을 수행하게 된다.

[0051] 이하에서는, 구체적으로 정책 적용이 어떻게 이뤄지는지 살펴보기로 한다.

[0052] P2P 보안 게이트웨이(200)가 적용된 정책을 토대로 원활하게 동작하기 위해서는 P2P 보안 서비스 도메인에 위치

한 P2P 플로우 에이전트(400)와의 동일한 운용 규칙을 공유하여 상호 협력할 수 있도록 하는 사전 조율 작업이 필수적이다. 이러한 사전 조율 작업은 기본적으로 P2P 보안 게이트웨이(200)에 탑재된 정책 및 운용 규칙이 변경될 때 발생할 수 있으며, P2P 네트워크 운용 특성에 따라 동적으로 이뤄질 수 있다.

[0053] 끝으로, 피어의 P2P 응용 서비스에 의해 발생되는 P2P 패킷은 P2P 플로우 에이전트(400)를 통해 P2P 보안 게이트웨이에 전달되며, P2P 보안 게이트웨이(200)는 탑재된 정책에 따라, 예를 들어, 통과(250), 대역폭 제한(252) 및 폐기(254) 등의 절차를 수행할 수 있다.

[0054] 적용 가능한 패킷 제어 절차의 범주는 상술한 바에 국한되지 않으며, 정책 고안자 및 네트워크 운용 계획자에 의해 다양하게 설계 및 사용될 수 있을 것이다.

[0055] 도 3은 본 발명에 따른 정책의 실시간 업데이트를 수행하기 위한 바람직한 일 실시예에 따른 중앙 서버 기반의 라이브 정책 업데이트 방법을 도시한다.

[0056] 도 3을 참조하면, 통상적으로 도메인 관리자(300)로부터 라이브 정책 업데이트 서버(100)로 신규 정책 및 운영 규칙을 전송하면, 라이브 정책 업데이트 서버(100)는 이를 감지하여 즉시 또는 기 정의한 정책 갱신 시간에 맞추어 신규 또는 갱신 정책을 각 P2P 서비스 도메인을 담당하고 있는 P2P 보안 게이트웨이(200)에 전송한다.

[0057] 따라서, 본 실시예에 따른 라이브 정책 업데이트 모델은, 정책 갱신에 따라 전달되어야 하는 데이터 크기 및 갱신 P2P 보안 게이트웨이(200)에 수에 따라 갱신에 따르는 시간 및 비용이 결정되는 특성을 가지게 된다.

[0058] 여기서, 도 4와 같은 변형된 실시예 형태의 라이브 정책 업데이트 모델을 추가적으로 고려해 볼 수 있다.

[0059] 도 4는 본 발명에 따른 정책의 실시간 업데이트를 수행하기 위한 바람직한 일 실시예에 따른 P2P 네트워크 기반의 라이브 정책 업데이트 방법을 도시한다.

[0060] 도 4를 살펴보면, 종래의 정책 업데이트 방식이 도 3과 같이 중앙 라이브 정책 업데이트 서버(100)에 의존하여 갱신된 정책 또는 데이터가 전송된 반면, 본 실시예에 따른 정책 업데이트 방법은 이미 갱신된 정책 또는 데이터를 포함한 네트워크 장비 즉, P2P 보안 게이트웨이(200-1)에서 업데이트되지 않은 다른 P2P 보안 게이트웨이(200-2, 200-3, 200-4)로 해당 정책 및 데이터를 P2P 형태로 전달하는 모델을 채택하고 있다.

[0061] P2P 보안 게이트웨이(200) 상호 간의 정책 업데이트를 위한 통신은 TTL(Time-To-Live) 등의 수치를 이용하여 무제한적인 데이터 전파 또는 루프(Loop) 등의 불필요한 채널 구조를 갖지 않도록 실시할 수 있으며, 상호 인증을 위해 별도의 중앙 인증 서버를 두거나 또는 자체 생성한 암호화 키(Self-Generated Cryptography Key) 및 제 3자를 경유하는 Web-of-Trust 등의 신뢰 모델 이용하는 방안을 고려할 수 있으며, 바람직한 실시예는 이에 국한되지 않는다.

[0062] 또한 P2P 보안 게이트웨이(330b)에서 다른 P2P 보안 게이트웨이(200-2, 200-3, 200-4)의 정책 버전을 체크하여 최신의 정책으로 갱신되는 과정 및 그 외 P2P 보안 게이트웨이 상호간의 P2P 네트워크 기반의 라이브 정책 업데이트에 따른 고려 사항은 통상적인 네트워크 정책 업데이트 방법에 준하여 실시될 수 있다.

[0063] 그러므로, 본 발명에서는 네트워크 상황 및 비용 요소에 따라 두 모델 중 하나를 택하여 라이브 정책 업데이트를 수행할 수 있는 운용상의 장점을 제공할 수 있다.

[0064] 지금까지, 본 발명이 적용되는 네트워크 구성을 중심으로 본 발명의 기술적 특성에 대해 개략적으로 설명하였다.

[0065] 다음으로, 도 5를 통해 각 네트워크 구성요소 중 P2P 플로우 에이전트와 P2P 보안 게이트웨이의 세부 구성에 대해 살펴보고자 한다.

[0066] 도 5는 본 발명에 따른 P2P 플로우 에이전트와 P2P 보안 게이트웨이의 세부 블록 구성을 나타낸다.

[0067] 본 발명에 따른 P2P 보안 게이트웨이(200)는 연계 시스템으로서 외부 정책 관리 시스템(500)과 연결되어 구성된다. P2P 플로우 에이전트(400)는 크게 P2P 응용 관리부(410), P2P 응용 정책 갱신부(420), 및 P2P 패킷 제어부(430)를 포함한다.

[0068] P2P 응용 관리부(410)에서는, 응용 설치 감지 모듈(410a)을 통하여 신규로 설치를 시도하는 P2P 응용 프로그램 및 서비스를 인식하고, 설치가 종료된 P2P 응용에 대한 정보를 응용 정보 관리 모듈(410b)을 통해 레지스트리 및 프로그램 설정 파일 등으로부터 추출하여 저장하고 이를 관리한다.

[0069] 또한, 응용 실행 모니터 모듈(410c)은 상시로 P2P 응용 프로그램 수행을 모니터링하다가 P2P 응용 프로그램의

실행이 감지되면, 해당 P2P 응용 프로그램에 대한 정보를 응용 정보 관리 모듈(410b)에 요청하며, 해당 결과를 P2P 응용 정책 갱신부(420)의 응용 정책 관리 및 저장 모듈(420b)에 전달하여 실행중인 P2P 응용 프로그램에 대한 적절한 정책 내역을 조회한다.

[0070] 조회된 정책 내역을 바탕으로 해당 P2P 응용 프로그램에서 발생되는 패킷을 제어하기 위해 P2P 패킷 제어부(430)의 패킷 수정 모듈(430a)은 P2P 응용 프로그램에 대한 식별 정보, 예를 들어, P2P 응용 프로그램명, 프로그램 식별코드, 사용자 ID, Peer ID 등을 바람직한 실시예로서 패킷의 IP 옵션 필드에 추가하거나 또는 P2P 플로우 에이전트(400)에서 본래의 패킷을 P2P 응용 식별 정보를 포함한 별도의 헤더로 인캡슐레이션(Encapsulation)하는 등의 기법을 사용하여 패킷을 수정하는 기능을 담당하고, 패킷 전달 모듈(430b)은 수정된 패킷을 P2P 보안 게이트웨이(200)에 전송한다.

[0071] P2P 보안 게이트웨이(200)는 크게, 관리용 접속부(210), 라이브 정책 갱신부(220), P2P 플로우 에이전트 관리부(230), 및 P2P 패킷 제어부(240)를 포함한다.

[0072] P2P 플로우 에이전트(400)로부터 수신된 패킷은, P2P 패킷 제어부(240)의 플로우 에이전트 접속 모듈(240a)에 최초로 전송되며, 패킷 모니터 모듈(240b)을 통해 해당 패킷의 P2P 응용 식별 정보가 감지된다. 추출된 식별 정보는 우선 라이브 정책 갱신부(220)의 정책 저장소 모듈(220b)에 질의되고, 조회된 결과에 따라 패킷 필터 모듈(240c)을 통해 적절한 정책이 수행(통과, 대역폭 제한, 차단, 우선순위 변경, 서비스 차등화 등)된다.

[0073] 다음으로, 외부 정책 관리 시스템(500)의 P2P 관리자 시스템(510)은 관리 목적에 따라 두 가지 방식을 통하여 P2P 보안 게이트웨이(200)에 접근할 수 있는데, 첫째, P2P 관리자 시스템(510)은 관리용 접속부(210)의 콘솔 접속 모듈(210a)에 직접 연결하여 명령어 줄(Command Line) 환경에서 P2P 보안 게이트웨이(200) 운용에 필요한 사항을 점검하거나 변경하여 적용할 수 있다. 둘째 P2P 관리자 시스템은(510)은 종래의 HTTP 또는 HTTPS 등의 웹 프로토콜을 이용하여 관리용 접속부(210)의 웹 서버 모듈(210b)에 연결될 수 있으며, 본 연결을 유지하며 접근 및 제어 정보 보고 모듈(210c)을 통하여 P2P 보안 게이트웨이(200)의 운용 및 관리 정보를 열람할 수 있다.

[0074] 한편, 외부 정책 관리 시스템(500)의 P2P 관리자 시스템(510)을 통해 설계 및 작성된 신규 정책 내역이 P2P 라이브 정책 업데이트 서버(520)에 전달되면, 변경 정책을 P2P 보안 게이트웨이에 적절히 갱신하여 이를 P2P 응용 탐지 및 트래픽 제어에 사용하기 위해 라이브 정책 갱신부(220)에 연결한다. 신규 정책 내역을 수신한 라이브 정책 관리 모듈(220a)은 정책의 버전 확인을 거쳐 정책 저장소 모듈(220b)로 해당 사항을 전달하는 역할을 수행한다. 정책 저장소 모듈(220b)은 해당 내역을 저장하고 관리하며 조회 요청 시 관련 결과의 제공을 담당한다.

[0075] 또한, P2P 보안 게이트웨이(200)에서 변경된 정책 사항을 동일하게 P2P 플로우 에이전트(400)에 적용할 필요성이 발생할 경우 P2P 응용 정책 갱신부(420)의 보안 게이트웨이 접속 모듈(420a)은 P2P 플로우 에이전트 관리부(230)의 플로우 에이전트 정책관리 모듈(230a)과 별도의 연결을 맺고 P2P 플로우 에이전트(400)에 적합하게 수정된 관련 정책 내역을 전달한다. 이와 같은 과정은 P2P 보안 게이트웨이(200)의 자체적인 판단에 준하여 푸쉬(Push) 모델로 수행되거나 또는 P2P 플로우 에이전트가 주기적으로 폴링(Polling)하여 정책 갱신 시기를 탐지하는 풀(Pull) 모델 등의 형태로 실시되는 것이 바람직하다. 이후 응용 정책 관리 및 저장 모듈(420b)은 버전 체크 등의 검증 절차를 통해 신규로 적용될 정책임을 확인하고 이를 저장 및 P2P 플로우 에이전트(400) 운용에 반영한다.

[0076] 또한, 신규 반영된 정책은 업데이트와 동시에 P2P 보안 게이트웨이(200) 및 P2P 플로우 에이전트(400)의 운용에 실시간 반영됨을 원칙으로 하는 것이 바람직하다.

[0077] 여기서, P2P 보안 게이트웨이와 플로우 에이전트 상호 협력 모델을 통한 P2P 유해 트래픽 탐지 방법 및 그 제어 기법을 주요하게 구성하는 P2P 플로우 에이전트(400) 및 P2P 보안 게이트웨이(200)의 바람직한 실시예로서 제시한 도 5의 상세 블록들은 상기 내용에 국한되지 않으며, 네트워크 계획자 또는 정책 관리자의 별도의 요구사항에 따라 보다 세분화되거나 다양한 모듈을 신규 탑재할 수 있을 뿐 아니라 여러 모듈의 기능을 모두 관장하는 보다 큰 범위의 모듈로 통합될 수도 있다.

[0078] 이하에서는, 본 발명에 따른 P2P 트래픽 관리 방법의 동작 흐름을 설명하기로 한다. 통상적으로 이해될 수 있는 기술 부분에 대한 설명은 피함으로써 본 발명이 갖는 동작의 특성을 명확히 제시하고자 한다.

[0079] 도 6은 본 발명에 따른 P2P 플로우 에이전트에서의 기본 정책 부여 과정의 일 실시예를 보여준다.

[0080] 즉, 도 6에서는 최초로 탑재된 피어에서 신규로 등록되는 P2P 프로그램을 인지하고 이에 관한 정보를 저장 관리하며 기본 정책을 부여하는 과정을 나타내고 있다.

[0081] P2P 플로우 에이전트 서비스가 최초로 시작되면(S601), 프로세스 신규 등록 모니터링이 기본적으로 수행되고(S602), 만약 응용 프로그램이 신규 설치 중에 있는 것으로 판단되면(S603의 Yes), P2P 응용 프로그램 설치를 감지하고(S604), 신규 응용 프로그램 설치가 완료될 때까지 대기한다(S605). 신규 응용 프로그램 설치가 종료되면, 해당 응용 프로그램의 설치시 운영 체제에 기록한 관련 설정 내역을 추적하여 저장하며(S606), 임시 응용 식별자를 부여하고 기본 정책을 부여한다(S607).

[0082] 본 발명의 바람직한 실시예에 따르면, 도 6에 나타난 절차는 P2P 플로우 에이전트 서비스가 종료될 때까지 지속적으로 수행된다.

[0083] 도 7은 본 발명의 일 실시예에 따라, P2P 플로우 에이전트와 P2P 보안 게이트웨이간 실시간 모니터링 절차를 통한 P2P 응용 프로그램 인지, P2P 패킷 수정 및 전송 과정에 대해 나타내고 있다.

[0084] P2P 플로우 에이전트 서비스가 시작되면(S701), P2P 플로우 에이전트(400)는 수행중인 프로세스를 실시간 모니터링하며(S702), 만약 P2P 응용이 실행중인 것으로 판별되면(S703의 Yes), 해당 프로세스에 대한 실시간 실행 정보(예를 들어, 프로세스 이름, 프로세스 아이디, 네트워크 대역폭 사용량, CPU 점유율 등)를 조회 및 획득하고(S704), 이에 대한 정보를 근거로 P2P 응용 프로그램 설치시 획득하여 저장한 응용 정보를 조회하는데(S705), 이는 실행 중인 프로세스가 P2P 응용 프로그램의 인스턴스(Instance)인지 여부를 감지하기 위해 필요한 절차다.

[0085] 이때, 프로세스에 대한 해당 정보가 존재하면(S706의 Yes), 이어서 해당 프로세스와 관련된 P2P 응용 정책이 존재하는지 여부를 조회한다(S707). 정책의 존재 유무를 판별하여(S708), 정책이 존재할 경우(S708의 Yes) 해당 P2P 응용 정책을 획득하고(S709), 만약 관련 정책이 부재일 경우에는 기본 정책 적용을 결정하며 이를 획득한다(S710). P2P 플로우 에이전트는 P2P 응용 프로그램이 패킷을 네트워크로 전송하고자 하는지 여부를 판별하고(S711), P2P 패킷 전송 시도가 감지되면(S712), 해당 패킷을 가로채고 응용 종료될 때까지 상기와 같이 획득된 정책 내역을 기준으로 P2P 응용을 식별할 수 있는 정보를 추가하는 등의 수정을 가한다(S713).

[0086] 본 실시예에 따른 절차는 P2P 플로우 에이전트 서비스가 종료될 때까지 지속적으로 수행되는 것이 바람직하다.

[0087] 도 8은 본 발명의 일 실시예에 따라, P2P 플로우 에이전트와 P2P 보안 게이트웨이간 P2P 응용 패킷 탐지를 통한 P2P 트래픽 제어 과정을 P2P 보안 게이트웨이의 동작을 중심으로 도시한 플로우차트다.

[0088] 우선, P2P 보안 게이트웨이 데몬이 시작되면(S801), P2P 플로우 에이전트로 유입되는 패킷은 실시간으로 모니터링되며(S802), 만약 P2P 응용 식별자가 포함된 패킷이 발견되면(S803의 Yes), 패킷에서 P2P 응용 관련 정보를 추출하고(S804), 응용 관련 정보에 포함된 P2P 응용 식별자를 이용하여 P2P 라이브 정책을 조회하고(S805), 정책 존재 유무를 판별한다(S806). 만약 정책이 존재하면(S806의 Yes) 해당 P2P 라이브 정책을 획득한다(S810). 그러나 정책이 존재하지 않을 경우에는(S806의 No), 관련 정책을 획득하기 위해 정책 업데이트 설정을 확인하는데(S807), 업데이트가 가능할 경우는 P2P 라이브 정책 업데이트 서버(100)로 관련 P2P 응용 프로그램에 대한 운용 및 제어 지침을 포함한 신규 정책 내역을 요청하지만(S809), 업데이트가 불가능하거나 적절한 신규 정책 내역을 P2P 라이브 정책 업데이트 서버(100)에서 제공하지 못하는 경우에는 기본 정책 적용을 결정하고(S808), 기본 정책을 P2P 라이브 정책으로서 획득한다(S810).

[0089] 다음으로, 획득된 정책의 종류에 따라(S811), 패킷 통과(S812), 대역폭 제한(S813) 및 패킷 폐기(S814) 등의 정책을 수행할 수 있는데, 특히 패킷 통과(S812) 및 대역폭 제한(S813)의 경우에는, 전송되는 패킷으로부터 P2P 응용식별과 관련한 정보를 제거하거나 언인캡슐레이션(Unencapsulation)시켜 인터넷과 같은 통상적인 네트워크를 경유하여 목적지에 전달될 수 있도록 한다(S815).

[0090] 한편, 상술한 과정을 거친 후에도 P2P 보안 게이트웨이 데몬이 계속 수행되고 있는 경우(S816의 No)에는 상술한 바와 같은 과정을 지속적으로 반복하는 것이 바람직하다.

[0091] 도 9는 본 발명에 따른 P2P 라이브 정책 업데이트 과정의 동작 흐름을 나타내고 있다.

[0092] 본 실시예에서는, P2P 보안 게이트웨이(200) 및 P2P 플로우 에이전트(400)를 신규 정책 내역을 수신하여 갱신될 대상으로 고려한다.

[0093] P2P 라이브 정책 업데이트 서버(100)에 정책 변경 사항이 발생하면(S901), 업데이트 방법 선택 절차가 진행된다(S902). 업데이트 방법으로는, P2P 라이브 정책 업데이트 서버를 통한 중앙 서버 기반의 라이브 정책 업데이트(S903) 또는 복수의 P2P 보안 게이트웨이간의 상호 연결을 통한 P2P 네트워크 기반의 라이브 정책 업데이트(S904)가 있는데, 선택된 업데이트 방법에 의해 신규 정책을 획득한다(S903 또는 S904).

[0094] 여기서, 업데이트 방법의 선택은 P2P 서비스 네트워크 유지보수시 고려될 수 있는 OPEX(Operation Expenditure), CAPEX(Capital Expenditure) 등의 요소를 감안하여 네트워크 관리자에 의해 결정되거나, P2P 보안 관리 도메인을 구성하는 P2P 보안 게이트웨이의 규모를 기준으로 하는 별도의 알고리즘에 따라 결정될 수 있다.

[0095] 두 방법 중 한 가지 방법을 통해 획득된 신규 정책을 적용하기에 앞서, P2P 보안 게이트웨이(200)는 기존 정책과의 충돌 여부를 검사한다(S905). 만약 정책 충돌이 발생한다면 기존의 정책이 유지되고(S906), 그렇지 않을 경우에는, 수신된 신규 정책 내역을 P2P 보안 게이트웨이(200)의 정책 저장소로 전송하여, 정책 충돌 검사가 완료되었음을 알리며 동시에 업데이트를 요청한다(S907)). 여기서, 정책 저장소에 저장된 신규 정책은 P2P 보안 게이트웨이 데몬에 실시간 적용되어(S908), 운용되는 것이 바람직하다.

[0096] 만약 P2P 보안 게이트웨이가, 수신한 신규 정책 내역을, 인접한 다른 P2P 보안 게이트웨이로 전달할 필요가 있다고 판단하면(S909의 Yes), 다른 P2P 보안 게이트웨이와 일대일 상호 연결을 맺어 정책 버전의 사전 검증 절차를 수행하고, 검증에 문제가 없을 경우 정책 내역의 전달을 시도하며(S911), 신규 정책 내역을 수신하는 P2P 보안 게이트웨이는 상술한 절차를 반복하여 저장소에 신규 정책을 갱신한다. 만약, 수신측 P2P 보안 게이트웨이가 정책 업데이트 전파의 마지막 피어라면 P2P 방식의 업데이트 전파는 여기에서 종료될 것이다.

[0097] 그렇지 않을 경우(S909의 No), P2P 플로우 에이전트가 탑재하고 있는 정책 내역의 변경이 필요한지 여부를 타진하여(S910), 업데이트가 필요한 경우(S910의 Yes), P2P 보안 게이트웨이는 P2P 플로우 에이전트에 연결하여(S912), P2P 응용 관리 정보 및 신규 정책 추가 또는 갱신을 요구한다(S913). P2P 플로우 에이전트의 정책 변경이 필요하지 않은 경우(S910의 No)는, P2P 정책 업데이트 과정이 모두 종료된다.

[0098] 상술한 과정은 P2P 라이브 정책 업데이트 서버의 직접적인 요청에 따라 시작되거나, 기 정의한 주기적 업데이트 시간에 따라 이뤄질 수도 있으며, 또는 P2P 보안 게이트웨이의 주기적인 정책 갱신 여부 확인을 통해 시작될 수 있으며, 그 바람직한 실시예는 이에 국한되지 않는다.

도면의 간단한 설명

[0099] 도 1은 본 발명이 적용되는 P2P 네트워크 구성도로서, 전체 P2P 보안 서비스 구조를 P2P 보안 서비스 도메인을 중심으로 도시한 도면.

[0100] 도 2는 도 1에 도시된 구성요소 간의 구체적인 연관 관계 및 상호 작용에 대해서 도시한 도면.

[0101] 도 3은 본 발명에 따른 정책의 실시간 업데이트를 수행하기 위한 바람직한 일 실시예에 따른 중앙 서버 기반의 라이브 정책 업데이트 방법을 도시한 도면.

[0102] 도 4는 본 발명에 따른 정책의 실시간 업데이트를 수행하기 위한 바람직한 일 실시예에 따른 P2P 네트워크 기반의 라이브 정책 업데이트 방법을 나타낸 도면.

[0103] 도 5는 본 발명에 따른 P2P 플로우 에이전트와 P2P 보안 게이트웨이의 세부 블록 구성을 나타낸 도면.

[0104] 도 6은 본 발명에 따른 P2P 플로우 에이전트에서의 기본 정책 부여 과정의 일 실시예를 나타낸 도면.

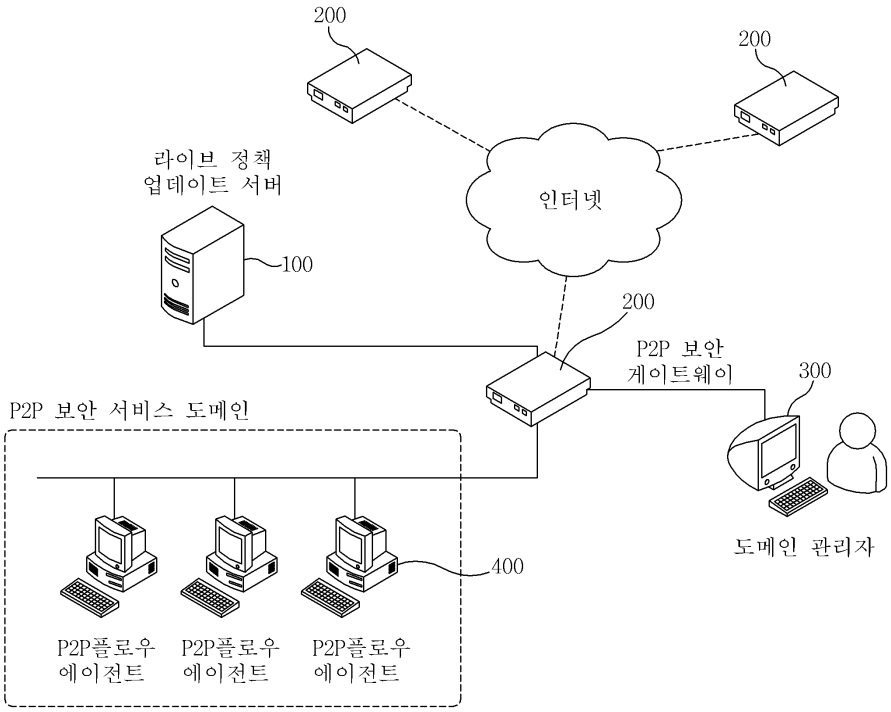
[0105] 도 7은 본 발명의 일 실시예에 따라, P2P 플로우 에이전트와 P2P 보안 게이트웨이간 실시간 모니터링 절차를 통한 P2P 응용 프로그램 인지, P2P 패킷 수정 및 전송 과정에 대해 나타낸 도면.

[0106] 도 8은 본 발명의 일 실시예에 따라, P2P 플로우 에이전트와 P2P 보안 게이트웨이간 P2P 응용 패킷 탐지를 통한 P2P 트래픽 제어 과정을 P2P 보안 게이트웨이의 동작을 중심으로 도시한 플로우차트.

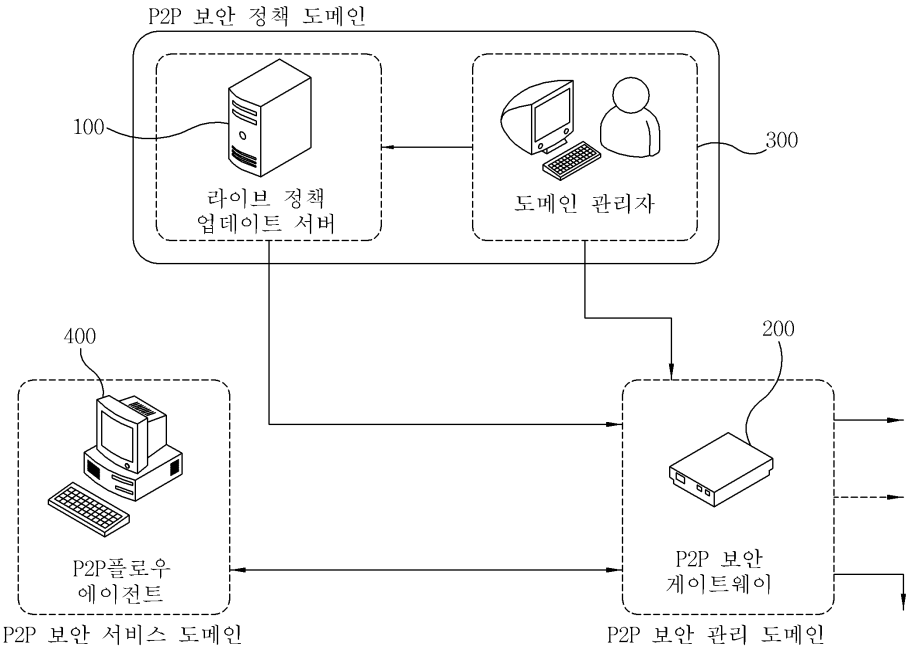
[0107] 도 9는 본 발명에 따른 P2P 라이브 정책 업데이트 과정의 동작 흐름을 나타낸 도면.

도면

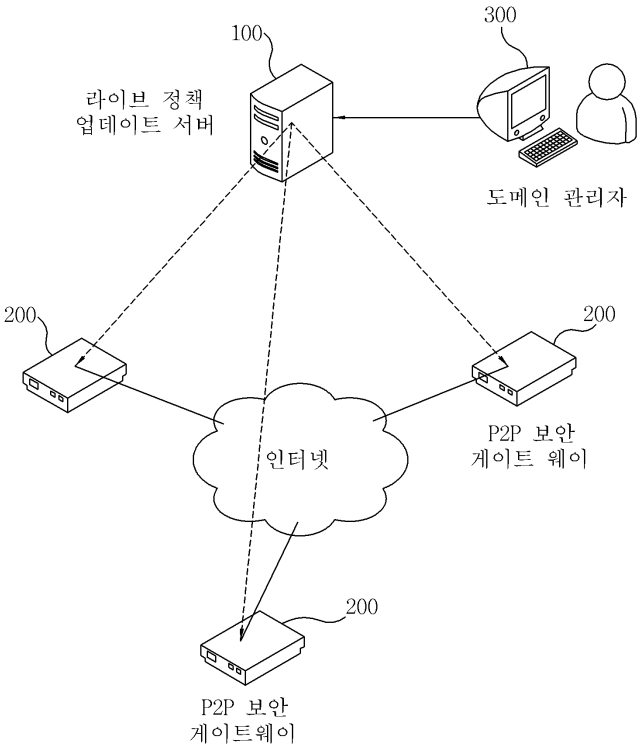
도면1


200
200
라이브 정책
업데이트 서버
인터넷
100
200
P2P 보안
게이트웨이
300
P2P 보안 서비스 도메인
400
도메인 관리자
P2P플로우
에이전트
P2P플로우
에이전트
P2P플로우
에이전트

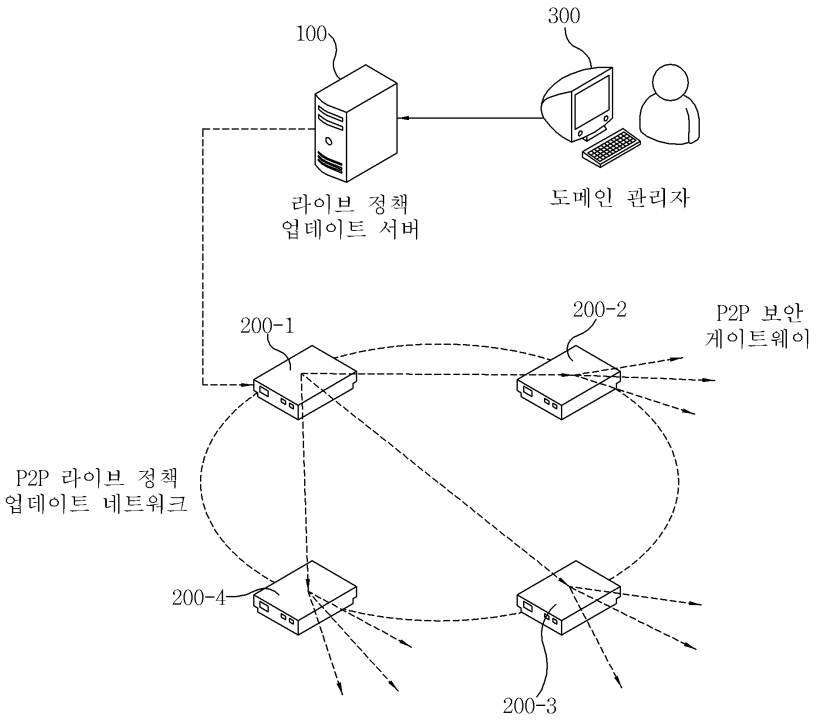
도면2


P2P 보안 정책 도메인
100
라이브 정책
업데이트 서버
도메인 관리자
300
400
200
P2P플로우
에이전트
P2P 보안
게이트웨이
P2P 보안 서비스 도메인
P2P 보안 관리 도메인

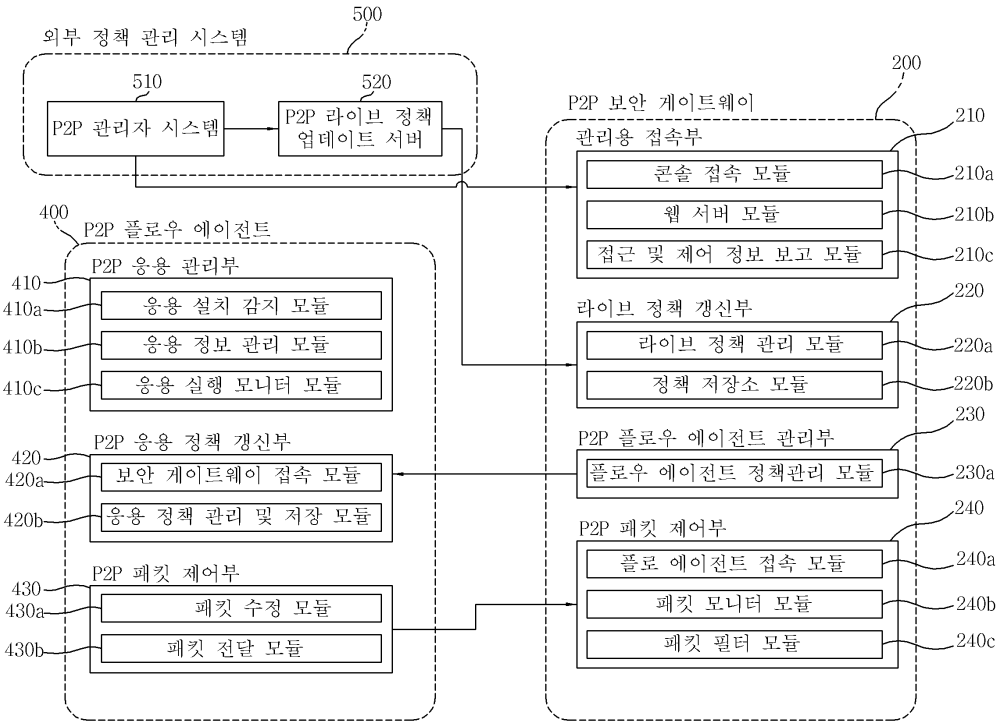
도면3


100
300
라이브 정책
업데이트 서버
도메인 관리자
200
200
인터넷
P2P 보안
게이트 웨이
200
P2P 보안
게이트웨이

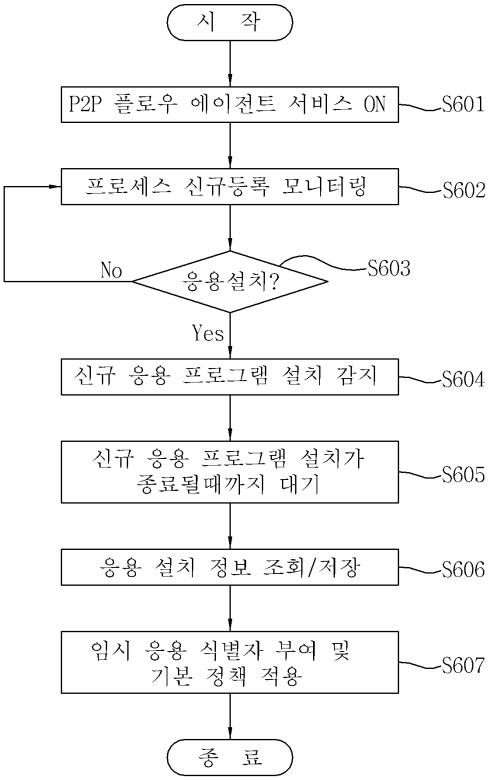
도면4


100
300
라이브 정책
업데이트 서버
도메인 관리자
200-1
200-2
P2P 보안
게이트웨이
P2P 라이브 정책
업데이트 네트워크
200-4
200-3

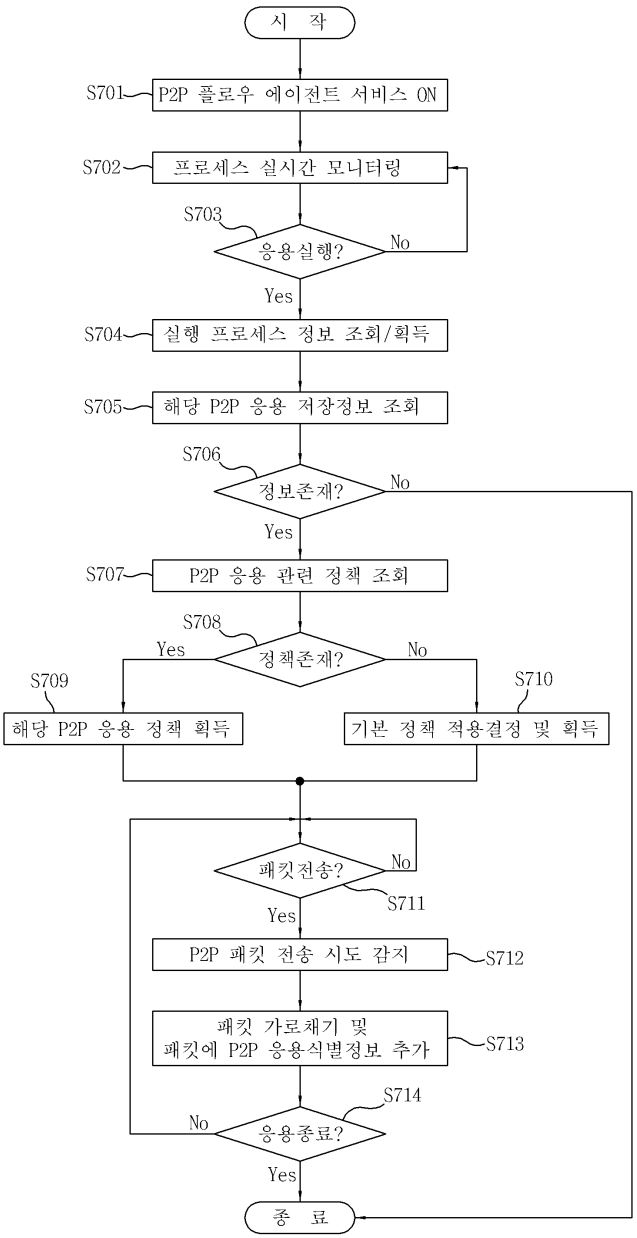
도면5


외부 정책 관리 시스템
500
510
P2P 관리자 시스템
520
P2P 라이브 정책 업데이트 서버
P2P 보안 게이트웨이
200
관리용 접속부
210
콘솔 접속 모듈
210a
웹 서버 모듈
210b
접근 및 제어 정보 보고 모듈
210c
라이브 정책 갱신부
220
라이브 정책 관리 모듈
220a
정책 저장소 모듈
220b
P2P 플로우 에이전트 관리부
230
플로우 에이전트 정책관리 모듈
230a
P2P 패킷 제어부
240
플로 에이전트 접속 모듈
240a
패킷 모니터 모듈
240b
패킷 필터 모듈
240c
400
P2P 플로우 에이전트
P2P 응용 관리부
410
410a
응용 설치 감지 모듈
410b
응용 정보 관리 모듈
410c
응용 실행 모니터 모듈
P2P 응용 정책 갱신부
420
420a
보안 게이트웨이 접속 모듈
420b
응용 정책 관리 및 저장 모듈
P2P 패킷 제어부
430
430a
패킷 수정 모듈
430b
패킷 전달 모듈

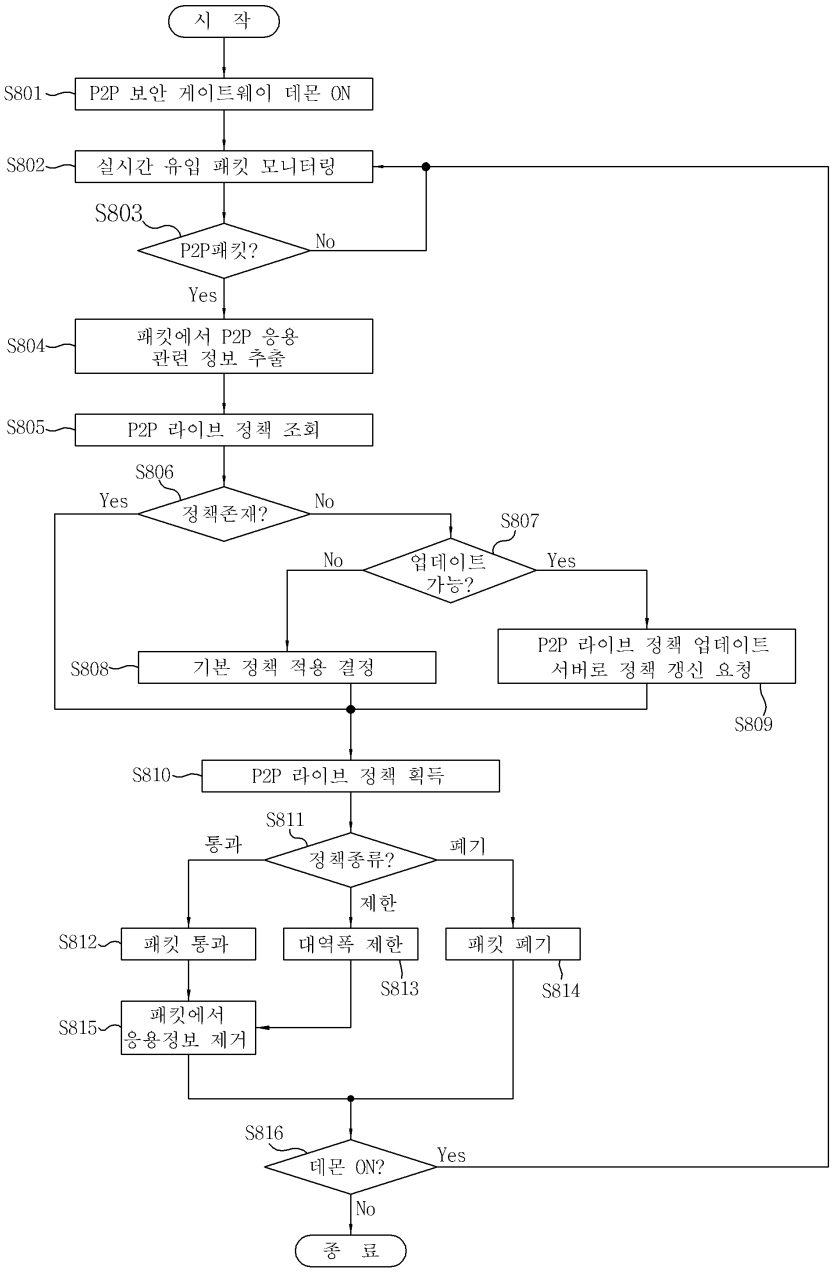
도면6


시 작
P2P 플로우 에이전트 서비스 ON
S601
프로세스 신규등록 모니터링
S602
No
응용설치?
S603
Yes
신규 응용 프로그램 설치 감지
S604
신규 응용 프로그램 설치가 종료될때까지 대기
S605
응용 설치 정보 조회/저장
S606
임시 응용 식별자 부여 및 기본 정책 적용
S607
종 료

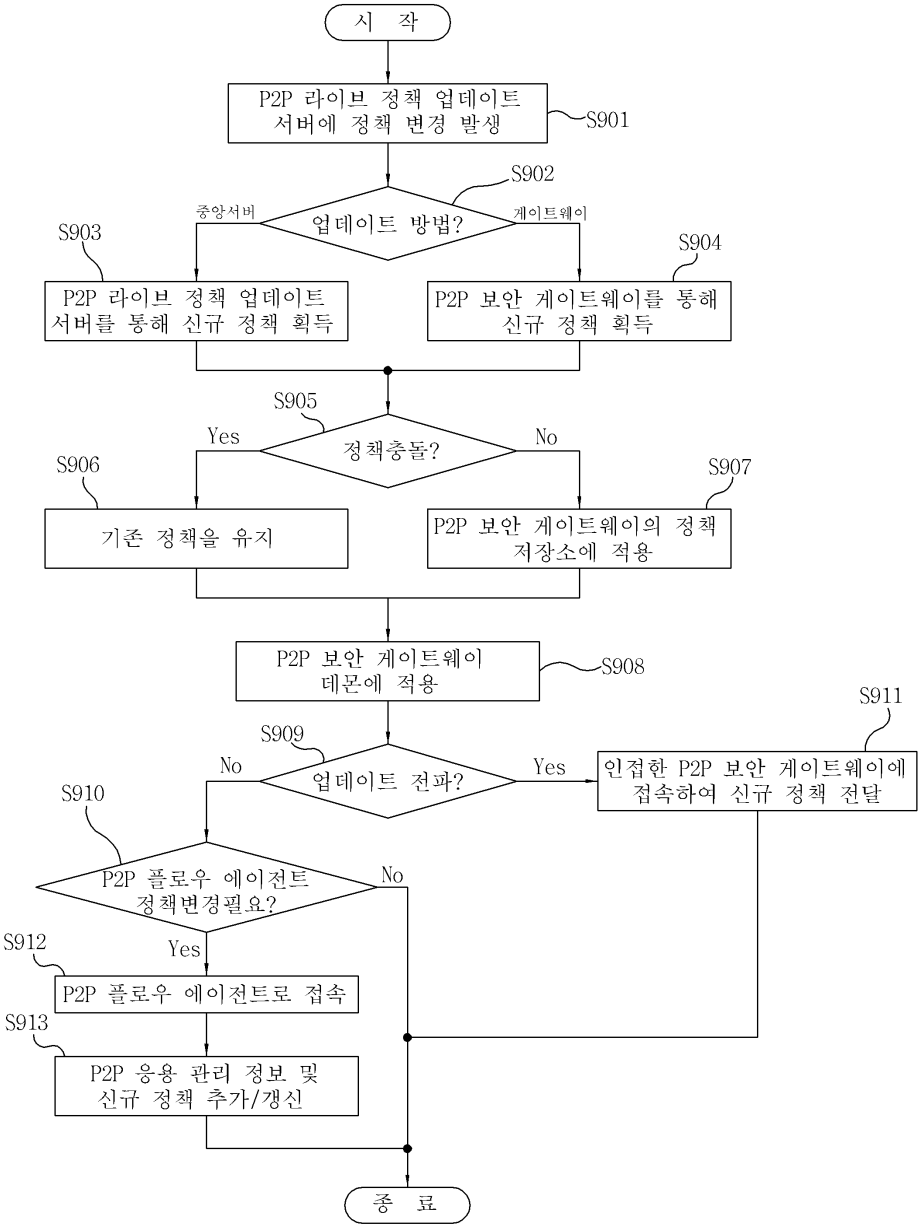
도면7


시 작
S701
P2P 플로우 에이전트 서비스 ON
S702
프로세스 실시간 모니터링
S703
응용실행?
No
Yes
S704
실행 프로세스 정보 조회/획득
S705
해당 P2P 응용 저장정보 조회
S706
정보존재?
No
Yes
S707
P2P 응용 관련 정책 조회
S708
정책존재?
Yes
No
S709
해당 P2P 응용 정책 획득
S710
기본 정책 적용결정 및 획득
패킷전송?
No
S711
Yes
P2P 패킷 전송 시도 감지
S712
패킷 가로채기 및
패킷에 P2P 응용식별정보 추가
S713
S714
No
응용종료?
Yes
종 료

도면8


시 작
S801
P2P 보안 게이트웨이 데몬 ON
S802
실시간 유입 패킷 모니터링
S803
P2P패킷?
No
Yes
S804
패킷에서 P2P 응용 관련 정보 추출
S805
P2P 라이브 정책 조회
S806
Yes
정책존재?
No
S807
No
업데이트 가능?
Yes
S808
기본 정책 적용 결정
P2P 라이브 정책 업데이트 서버로 정책 갱신 요청
S809
S810
P2P 라이브 정책 획득
S811
통과
정책종류?
폐기
제한
S812
패킷 통과
대역폭 제한
S813
패킷 폐기
S814
S815
패킷에서 응용정보 제거
S816
데몬 ON?
Yes
No
종 료

도면9


시 작
P2P 라이브 정책 업데이트 서버에 정책 변경 발생
S901
S902
업데이트 방법?
중앙서버
게이트웨이
S903
P2P 라이브 정책 업데이트 서버를 통해 신규 정책 획득
S904
P2P 보안 게이트웨이를 통해 신규 정책 획득
S905
정책충돌?
Yes
No
S906
기존 정책을 유지
S907
P2P 보안 게이트웨이의 정책 저장소에 적용
P2P 보안 게이트웨이 데몬에 적용
S908
S909
업데이트 전파?
No
Yes
S911
인접한 P2P 보안 게이트웨이에 접속하여 신규 정책 전달
S910
P2P 플로우 에이전트 정책변경필요?
No
Yes
S912
P2P 플로우 에이전트로 접속
S913
P2P 응용 관리 정보 및 신규 정책 추가/갱신
종 료