



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0120823
(43) 공개일자 2010년11월17일

(51) Int. Cl.

H04L 12/26 (2006.01) H04L 12/56 (2006.01)

H04W 24/00 (2009.01) H04W 88/04 (2009.01)

(21) 출원번호 10-2009-0039656

(22) 출원일자 2009년05월07일

심사청구일자 2009년05월07일

(71) 출원인

충남대학교산학협력단

대전광역시 유성구 궁동 220번지 충남대학교

(72) 발명자

이영석

대전 유성구 관평동 대덕테크노밸리 8단지 금성백
조아파트 809-602

손현구

대전 유성구 궁동 474-7 308호

(74) 대리인

김원준

전체 청구항 수 : 총 9 항

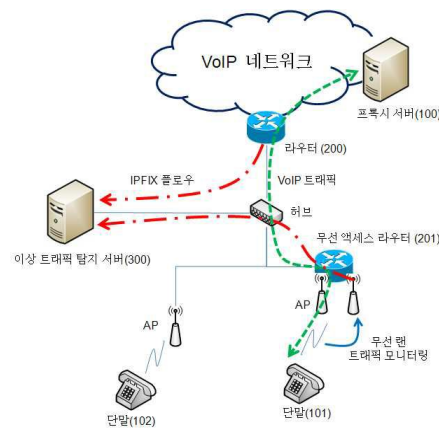
(54) 플로우 데이터를 이용한 VoIP 응용 이상 트래픽 탐지 방법

(57) 요약

본 발명은 네트워크상의 트래픽 모니터링을 통해 SIP/RTP를 이용하는 VoIP의 응용 이상 트래픽을 탐지하는 방법 및 장치에 관한 것으로, 보다 구체적으로 (A) 전송되는 VoIP 플로우의 IP 패킷을 라우터 또는 무선 라우터에서 캡처하여 SIP 메시지와 RTP 트래픽을 분류하는 단계; (B) 분류된 SIP 메시지와 RTP 트래픽의 헤더 정보를 추출하는 단계; (C) 추출된 정보를 데이터베이스에 저장하는 단계; 및 (D) 추출된 정보와 데이터베이스에 저장된 정보로부터 SIP 이상 트래픽과 RTP 이상 트래픽의 발생을 판정하는 단계;를 포함하는 VoIP 응용 이상 트래픽의 탐지 방법 및 이를 위한 장치에 관한 것이다.

본 발명에 의하면 네트워크 상에서 VoIP 트래픽의 관찰을 통해 VoIP 응용 이상 트래픽 탐지가 가능하므로 보다 효율적인 인터넷 텔레포니 서비스의 제공이 가능하며 이상 트래픽의 사전 차단에 유용할 것으로 기대된다.

대표도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호 C1090-0801-0016 / 2008-1463

부처명 정보통신연구진흥원 / 한국과학기술원

연구관리전문기관

연구사업명 대학 IT 연구센터 육성지원사업 / IT 핵심 기술개발 사업

연구과제명 해킹·바이러스 대응기술 연구 / 초정밀 측정 및 분석 기술 연구

기여율

주관기관 충남대학교

연구기간 2003.8.1~2011.8.31 / 2008.3.1~2013.2.28

특허청구의 범위

청구항 1

(A) 라우터상에서 VoIP 플로우의 IP 패킷으로부터 SIP 메시지와 RTP 트래픽을 분류하는 단계;

(B) 분류된 SIP 메시지와 RTP 트래픽의 헤더 정보를 추출하는 단계;

(C) 상기 (B) 단계에서 추출된 정보를 데이터베이스에 저장하는 단계; 및

(D) 상기 (B) 단계에서 추출된 정보로부터

a) VoIP 플로우의 SIP 메시지가 BYE 메시지인 경우,

상기 데이터 베이스에서 상기 BYE 메시지와 같은 CALL-ID와 4-tuple 정보를 갖는 INVITE 메시지와 OK 메시지의 미디어 세션 정보로부터 BYE 메시지 발생 후 1~5초 사이에 음성 트래픽이 발생하면 BYE DoS 이상 트래픽으로 판정하며,

b) RTP 트래픽 대해

① 상기 데이터베이스에서 동일 4-tuple을 갖는 RTP 트래픽을 검색하여 SSRC가 바뀐 적이 있거나, ② 플로우 내의 최대, 최소, 플로우의 처음 및 마지막 순서번호를 비교하여, i) 처음 순서번호 > 마지막 순서번호이고, 최소 순서번호 < 처음 순서번호 이거나 최대 순서번호 > 마지막 순서번호 또는 ii) 처음 순서번호 < 마지막 순서번호이고, 최소 순서번호 > 마지막 순서번호 이거나 최대 순서번호 < 처음 순서번호이면 플러딩 이상 트래픽이 발생한 것으로 판정하는 단계;

를 포함하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 2

제 1 항에 있어서,

상기 (A)단계의 라우터가 무선라우터인 경우,

(B) 단계에서 802.11의 헤더 정보를 추가로 추출하고,

(D) 단계에서 VoIP 플로우의 SIP 메시지가 CANCEL 메시지인 경우,

① 상기 CANCEL 메시지와 같은 상기 데이터베이스에서 CALL-ID와 4-tuple 정보를 갖는 INVITE 메시지를 검색하여 MAC 주소가 서로 다르거나, ② CANCEL 메시지와 CANCEL 메시지 이전 패킷의 802.11 MAC 순서번호의 차이가 5보다 작은 경우 CANCEL DoS 이상 트래픽으로 판정하는 것을 추가로 포함하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 3

제 1 항 또는 제 2 항에 있어서,

상기 (D) 단계에서 이상 트래픽으로 판정된 경우 해당 플로우를 시각화하는 단계를 추가적으로 포함하는 VoIP 이상 트래픽의 탐지 방법.

청구항 4

제 1 항 또는 제 2 항에 있어서,

상기 단계 (B)에서 추출되는 정보는 IETF IPFIX 표준 형태인 것을 특징으로 하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 5

제 1 항 또는 제 2 항에 있어서,

상기 SIP 메시지의 헤더정보는 메시지 종류, Call-ID, 음성 트래픽의 연결 정보 및 코덱 정보인 것을 특징으로 하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 6

제 1 항 또는 제 2 항에 있어서,

상기 RTP 트래픽의 헤더정보는 순서번호 및 SSRC 정보인 것을 특징으로 하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 7

제 2 항에 있어서,

상기 802.11의 헤더정보는 순서번호 및 출발지와 목적지의 MAC 주소 정보인 것을 특징으로 하는 VoIP 응용 이상 트래픽의 탐지 방법.

청구항 8

제 1 항 또는 제 2 항의 방법에 의해 VoIP 응용 이상 트래픽을 탐지 및 모니터링하기 위한 장치로서,

(A) 단말기와 프록시 서버 사이의 경로에 존재하는 라우터 또는 무선라우터에서 VoIP 트래픽에 대한 모니터링을 실시하며, (a) 네트워크의 IP 패킷을 캡처하여 VoIP 트래픽의 SIP 메시지와 RTP 트래픽을 분류하는 SIP/RTP 트래픽 탐지부; (b) 분류된 SIP 메시지, RTP 트래픽과 802.11의 헤더 정보를 추출하는 SIP/RTP 트래픽 분석부; (c) 분석된 헤더정보로부터 SIP/RTP 플로우 테이블을 생성하는 SIP/RTP 플로우 생성부; 및 (d) 생성된 SIP/RTP 플로우 테이블로부터 IPFIX 플로우를 생성하고 전송하는 IPFIX 플로우 전송부;로 이루어진 VoIP 트래픽 탐지 및 분석 장치;와

(B) (a) 상기 VoIP 트래픽 탐지 및 분석 장치로부터 전송된 IPFIX 플로우를 수신하는 IPFIX 플로우 수신부; (b) 수신된 IPFIX 플로우를 분석하여 SIP/RTP 트래픽의 헤더정보를 저장하는 데이터베이스; 및 상기 SIP/RTP 트래픽 정보와 데이터베이스에 저장되어 있는 정보를 비교하여 VoIP 응용 이상 트래픽 여부를 판단하는 VoIP 응용 이상 트래픽 탐지부;로 구성되는 VoIP 응용 이상 트래픽 탐지 서버로 이루어지는 것을 특징으로 하는 VoIP 응용 이상 트래픽 탐지 장치.

청구항 9

제 8 항에 있어서,

상기 VoIP 응용 이상 트래픽 탐지 서버는 상기 VoIP 응용 이상 트래픽 탐지부에서 이상 트래픽으로 판정된 경우 해당 플로우를 시각화하는 VoIP 응용 이상 트래픽 시각화부를 추가로 포함하는 것을 특징으로 하는 VoIP 응용 이상 트래픽 탐지 장치.

명 세 서

발명의 상세한 설명

기술 분야

[0001] 본 발명은 네트워크상의 트래픽 모니터링을 통해 SIP/RTP를 이용하는 VoIP의 응용 이상 트래픽을 탐지하는 방법에 관한 것이다.

배경 기술

[0002] VoIP(Voice over internet protocol) 기술이라 함은 인터넷 프로토콜(IP)을 이용하는 사용자 간에 음성 트래픽의 전송을 통하여 전화 서비스를 할 수 있는 것을 지칭한다. 즉, 기존 공중교환전화망인 PSTN(public switched telephone network)망을 통해 이루어졌던 음성데이터의 전송을 디지털 형태로 인터넷 상에서 전송하는 것이다. 지난 1995년 보컬텍이 인터넷폰을 상용화한 이후 주목받기 시작한 VoIP기술은 국제전화 사업자들이 통신요금인하를 위해 경쟁적으로 도입하면서 보편화되고 있다. 국내에서는 새롭기술이 1999년 1월 5일 국내 PC사용자들을 대상으로 인터넷무료전화 다이얼패드 서비스를 개시한 이후 인터넷폰 이용자가 기하급수적으로 증가하고 있다. 국내 VoIP 서비스 시장은 2009년까지 연평균 성장률 54%를 기록해 2009년에는 9689억원 규모를 형성할 것으로 전망된다.

[0003] VoIP 서비스는 쌍방간의 접속을 통한 미디어 서비스이므로 연결을 맺기 위한 규약(프로토콜)이 필요하다. 또한 VoIP 서비스는 인터넷뿐만 아니라 사설 IP 기반망, 공중 전화망(PSTN), 또는 이들의 복합망에서도 연동되어야 하기 때문에 기술 및 프로토콜의 표준화가 중요하다. 가장 널리 사용하고 있는 연결 프로토콜의 표준은 ITU-T(Internation Telecommunication)에서 개발한 H.323 와 IETF(Internation Engeneering Task Force)에서 개발하는 SIP(Session Initiation Protocol)를 들 수 있다. 이 중, SIP는 1999년에 IETF의 공식 표준으로 채택되면서 현재 VoIP 전화 호출을 위한 신호 메시지를 전달하는 프로토콜로 널리 사용되고 있으며 차세대 VoIP 신호 방식으로 각광받고 있다. SIP는 H.323보다 연결을 맺는 과정이 간단하고 HTTP처럼 패킷의 헤더정보가 일반 텍스트로 되어 있어 쉽게 인터넷 환경에 적용할 수 있으며, 연결 부하가 적다는 이점이 있다.

[0004] RTP(Real-time Transport Protocol)는 인터넷에서 음성 또는 동영상 등의 스트리밍 트래픽을 전송할 수 있는 응용 계층 프로토콜이다. 즉, SIP는 연결의 맺고 끊음을 담당하는 반면 RTP는 음성과 영상 등의 멀티미디어 데이터의 전송을 담당한다. RTP는 신뢰성은 없으나 빠르게 데이터를 전달할 수 있는 UDP라는 수송 프로토콜 위에서 실행되며 실시간 응용에 필수적인 시간 정보 및 매체의 동기화 기능을 제공한다.

[0005] 이와 같이 VoIP 서비스는 SIP와 RTP가 역할을 나누어 맡고 있기 때문에 VoIP 트래픽은 SIP 메시지와 RTP 트래픽을 포함한 트래픽을 지칭하며, VoIP 응용 이상 트래픽 역시 SIP 기반의 이상 트래픽과 RTP 기반의 이상 트래픽으로 나눌 수 있다. SIP 이상 트래픽은 연결과 관련된 이상 트래픽으로서, 사용자가 전화를 걸 때 이 전화에 대하여 강제로 연결을 취소시키는 CANCEL DoS(Denial of Service) 이상 트래픽과 사용자간 통화 중 하나 또는 양측 사용자의 통화를 강제로 종료시키는 BYE DoS 이상 트래픽을 들 수 있다. 이러한 SIP 이상 트래픽은 하나의 패킷만으로 사용자 간의 VoIP 서비스를 무력화시킬 수 있는 폐해가 있다. RTP 이상 트래픽은 연결은 정상적으로 이루어지지만, 실질적인 통화에 문제점이 있는 것으로 보통 유효하지 않은 RTP 패킷을 다량으로 보냄으로써 음성 통화 품질을 저하시키거나 임의의 데이터 삽입으로 이상한 소리를 재생하게 하는 RTP 플러딩 공격에 의한 이상 트래픽이다. 또한 최근의 VoIP 서비스는 무선 인터넷 환경에서도 지원을 하기 때문에 무선 환경에서 공격자가 정상 VoIP 트래픽을 스니핑하여 이상 트래픽의 생성이 가능하므로 이에 대한 탐지 방법이 필요하다. 보다 원활한 VoIP를 이용한 인터넷 텔레포니 서비스를 제공하기 위해서는 VoIP 이상 트래픽을 유발하는 트래픽을 효율적으로 탐지하는 것이 필요하다.

[0006] 현재 사용되고 있는 이상 트래픽 탐지 방법은 일반 네트워크 상에서 DoS 웹, 바이러스 등의 이상 트래픽 탐지 기능만을 제공하며 VoIP 서비스를 대상으로 한 이상 트래픽 탐지에 적합하도록 구성되어 있지 않기 때문에 종래 기술에 의한 이상 트래픽 탐지 방법만으로는 VoIP 환경에서 발생하는 이상 트래픽을 효과적으로 탐지하기 어렵다. 따라서, VoIP 서비스에서 이상 트래픽 탐지에 대한 방법의 개발이 요구된다.

발명의 내용

해결 하고자하는 과제

- [0007] 이러한 문제점을 해결하기 위한 본 발명이 이루고자 하는 기술적 과제는 일반 네트워크 환경과는 특이한 VoIP 서비스 환경에서 VoIP 응용 이상 트래픽을 효과적으로 탐지할 수 있는 방법 및 그 장치를 제공하는 것이다.
- [0008] 본 발명은 또한 최근 급증하고 있는 무선 인터넷을 이용한 VoIP 서비스 환경에서 일어날 수 있는 응용 이상 트래픽에 대한 탐지 방법을 제공하는 것이다.

과제 해결수단

- [0009] 상기 기술적 과제를 달성하기 위한 본 발명은 (A) 라우터상에서 VoIP플로우의 IP 패킷으로부터 SIP 메시지와 RTP 트래픽을 분류하는 단계; (B) 분류된 SIP 메시지와 RTP 트래픽의 헤더 정보를 추출하는 단계; (C) 상기 (B) 단계에서 추출된 정보를 데이터베이스에 저장하는 단계; 및 (D) 상기 (B) 단계에서 추출된 정보와 데이터베이스에 저장된 정보로부터 a) VoIP 플로우의 SIP 메시지가 BYE 메시지인 경우, 상기 데이터베이스에서 상기 BYE 메시지와 같은 CALL-ID와 4-tuple 정보를 갖는 INVITE 메시지와 OK 메시지의 미디어 세션 정보로부터 BYE 메시지 발생 후 1~5초 사이에 음성 트래픽이 발생하면 BYE DoS 이상 트래픽으로 판정하며, b) RTP 트래픽 대해 ① 동일 4-tuple을 갖는 RTP 트래픽을 검색하여 SSRC가 바뀐 적이 있거나, ② 플로우 내의 최대, 최소, 플로우의 처음 및 마지막 순서번호를 비교하여, i) 처음 순서번호 > 마지막 순서번호이고, 최소 순서번호 < 처음 순서번호이거나 최대 순서번호 > 마지막 순서번호 또는 ii) 처음 순서번호 < 마지막 순서번호이고, 최소 순서번호 > 마지막 순서번호이거나 최대 순서번호 < 처음 순서번호이면 플러딩 이상 트래픽이 발생한 것으로 판정하는 것에 의해 이상 트래픽과 RTP 이상 트래픽의 발생을 판정하는 단계;를 포함하는 VoIP 응용 이상 트래픽의 탐지 방법에 관한 것이다.
- [0010] 상기 VoIP 서비스가 무선 인터넷 환경에서 이루어지는 경우 (B) 단계에서 802.11의 헤더정보를 추가로 추출하여 스니핑에 의한 CANCEL DoS 이상 트래픽의 발생을 추가로 탐지한다.
- [0011] 또한, 상기 (D) 단계에서 이상 트래픽으로 판정된 경우 해당 플로우를 시각화하는 단계를 추가적으로 포함하여 VoIP 이상 트래픽을 탐지할 수 있다.
- [0012] 본 발명은 또한 상기 방법에 의해 VoIP 응용 이상 트래픽을 탐지하기 위한 장치로서, (A) 단말기와 프록시 서버 사이의 경로에 존재하는 라우터 또는 무선라우터에서 VoIP 트래픽에 대한 모니터링을 실시하며, (a) 네트워크의 IP 패킷을 캡처하여 VoIP 트래픽의 SIP 메시지와 RTP 트래픽을 분류하는 SIP/RTP 트래픽 탐지부; (b) 분류된 SIP 메시지, RTP 트래픽과 802.11의 헤더 정보를 추출하는 SIP/RTP 트래픽 분석부; (c) 분석된 헤더정보로부터 SIP/RTP 플로우 테이블을 생성하는 SIP/RTP 플로우 생성부; 및 (d) 생성된 SIP/RTP 플로우 테이블로부터 IPFIX 플로우를 생성하고 전송하는 IPFIX 플로우 전송부;로 이루어진 VoIP 트래픽 탐지 및 분석 장치;와 (B) (a) 상기 VoIP 트래픽 탐지 및 분석 장치로부터 전송된 IPFIX 플로우를 수신하는 IPFIX 플로우 수신부; (b) 수신된 IPFIX 플로우를 분석하여 SIP/RTP 트래픽의 헤더정보를 저장하는 데이터베이스; 및 상기 SIP/RTP 트래픽 정보와 데이터베이스에 저장되어 있는 정보를 비교하여 VoIP 응용 이상 트래픽 여부를 판단하는 VoIP 응용 이상 트래픽 탐지부;로 구성되는 VoIP 응용 이상 트래픽 탐지 서버로 이루어지는 것을 특징으로 하는 VoIP 응용 이상 트래픽 탐지 장치에 관한 것이다.
- [0013] 상기 VoIP 응용 이상 트래픽 탐지 서버는 상기 VoIP 응용 이상 트래픽 탐지부에서 이상 트래픽으로 판정된 경우 해당 플로우를 시각화하는 VoIP 응용 이상 트래픽 시각화부를 추가로 포함하여 이루어질 수 있다.

효 과

- [0014] 이상에서 설명한 바와 같이, 본 발명에 따르면 네트워크 상에서 VoIP 트래픽의 관찰을 통해 VoIP 응용 이상 트래픽 탐지가 가능하므로 보다 효율적인 인터넷 텔레포니 서비스의 제공이 가능하다. 또한, VoIP 서비스 제공자 뿐만 아니라 인터넷 서비스 제공자도 VoIP 응용 이상 트래픽을 탐지할 수 있어 이상 트래픽의 사전 차단에 유용

할 것으로 기대된다.

발명의 실시를 위한 구체적인 내용

- [0015] 이하 도면을 참조하여 본 발명을 상세하게 설명한다. 그러나, 이들은 예시적인 목적일 뿐 본 발명이 이에 한정되는 것은 아니다.
- [0016] 도 1은 단말(101)과 단말(102)사이 VoIP 트래픽의 흐름을 개략적으로 보여준다. 도 1을 참조하면 단말(101)과 단말(102)는 프록시 서버(100)를 통하여 서로 VoIP 트래픽을 전송한다. 이때, 단말(101)에서 전송하는 트래픽은 무선 액세스 라우터(201)과 라우터(200)을 통하여, 단말(102)에서 전송하는 트래픽은 라우터(200)을 통하여 프록시 서버(100)에 전송되는 것으로 도시하였으나 이는 예시적인 것으로 단말(101)(102)가 모두 무선라우터를 거치거나 라우터를 거쳐 데이터를 전송할 수 있음은 당연하다.
- [0017] 본 발명은 (A) 전송되는 VoIP 플로우의 IP 패킷을 라우터 또는 무선 라우터에서 캡처하여 SIP 메시지와 RTP 트래픽을 분류하는 단계; (B) 분류된 SIP 메시지와 RTP 트래픽의 헤더 정보를 추출하는 단계; (C) 추출된 정보를 데이터베이스에 저장하는 단계; 및 (D) 추출된 정보와 데이터베이스에 저장된 정보로부터 SIP 이상 트래픽과 RTP 이상 트래픽의 발생을 판정하는 단계;를 포함하는 VoIP 응용 이상 트래픽의 탐지 방법에 관한 것이다.
- [0018] 이 때 SIP 메시지는 출발지/목적지 포트번호를 5060을 사용하는 것으로 가정한다. 상기 (B) 단계의 SIP 메시지의 헤더 정보는 메시지 종류, Call-ID, 음성 트래픽의 연결 정보 및 코덱 정보를 포함한다. 상기 메시지의 종류는 SIP 메시지가 어떤 역할을 하는 지에 대한 것을 나타내며 INVITE 메시지, BYE 메시지, ACK 메시지, CANCEL 메시지, REGISTER 메시지 및 OPTION 메시지로 나눌 수 있다. Call-ID는 사용자가 VoIP 응용을 사용할 때 생성되는 ID이다. 또한, 음성 트래픽 연결정보는 전화 연결 요청 후 사용자간 음성 트래픽 통신을 위한 출발지/목적지의 IP 주소와 포트번호를 나타내고, 코덱 정보는 음성 트래픽 전송시 사용되는 음성 압축 방법을 나타낸다.
- [0019] RTP 트래픽의 헤더로부터는 순서번호와 SSRC 정보를 추출한다. RTP 헤더의 순서번호는 RTP 패킷이 전송될 때마다 하나씩 점증적으로 증가하며, SSRC 정보는 사용자가 음성 통화를 하는 동안 그 통화에 대해 동기화를 하기 위하여 사용되는 값으로 정상적인 통화의 경우 통화가 유지되는 동안에는 바뀌지 않는다.
- [0020] 상기 단계 (B)에서 추출된 정보는 IETF IPFIX(IP Flow Information eXport) 표준 형태인 것이 바람직하다. IETF IPFIX는 라우터 또는 무선 액세스 라우터를 통하여 수신된 IP 패킷을 플로우로 분류하여 플로우 생성시간, 종료시간, 패킷수, 바이트수 등의 값을 유동적으로 관리하는 IP 플로우 측정 및 전송에 관한 표준이다.
- [0021] 또한 본 발명의 VoIP 이상 트래픽 탐지 방법에서는 (D)에서 이상 트래픽이 발생한 것으로 판정되는 경우 이를 시각화하는 단계를 추가로 포함하여 이상 트래픽 탐지를 가능하게 하고, 더 나아가 이 트래픽에 대하여 차단을 수행할 수 있도록 하는 것이 바람직하다.
- [0022] 도 2 내지 도 4는 상기 (D)의 VoIP 응용 이상 트래픽을 판정하는 구체적인 방법을 설명하는 순서도이다.
- [0023] 먼저, 도 2는 VoIP 응용에 사용자간의 음성 통화에서 한 사용자의 통화를 강제로 종료시키는 BYE DoS 이상 트래픽을 탐지하는 것을 보여주는 도면이다. 본 도면은 음성 트래픽 연결 정보를 습득하는 부(510)와 음성 트래픽의 시간 정보 검사부(520)으로 구성되어 있다. 음성 트래픽 연결 정보를 얻는 것은 BYE 메시지와 같은 CALL-ID와 4-tuple(출발지/목적지 IP 주소와 포트번호)정보를 가지는 INVITE와 OK 메시지를 모니터링한 결과에서 음성 통화 연결 정보를 가져온다. 이 연결 정보를 이용하여 음성 트래픽의 시간 정보 검사부(520)에는 같은 연결 정보를 가지는 RTP 트래픽이 라우터에서 모니터링된 시간을 검사한다. 이때 BYE 트래픽이 발생한 후 소정 시간 뒤에도 RTP 트래픽이 모니터링될 경우 이는 의도되지 않는 BYE 트래픽이 발생한 것으로 볼 수 있으므로 BYE DoS 이상 트래픽이 발생한 것으로 판단한다. 상기 소정 시간은 서비스 상태에 따라 적절하게 응용되어야 함은 당연하지만 BYE 트래픽 전송 후 1~5초 사이에도 음성 트래픽이 탐지된다면 RTP 이상 트래픽이 발생한 것으로 판단하

는 것이 바람직하다.

- [0024] 도 3은 VoIP 응용에서 음성 트래픽 전송시 사용되는 RTP 트래픽을 이용한 플러딩 이상 트래픽을 탐지하는 것을 보여주는 도면이다. 본 도면은 RTP 헤더의 SSRC 값 검사부(610), RTP 헤더의 순서번호 계산부(620), 순서번호 비교부(630, 640)로 구성된다. RTP 헤더의 SSRC 검사부(610)는 모니터링된 RTP 플로우에서 SSRC의 변경 여부를 검사한다. SSRC 정보는 정상적인 통화의 경우 통화가 유지되는 동안에는 바뀌지 않으므로 모니터링된 RTP 플로우 내에서 SSRC 값이 변경된 적이 있었다면 이상 트래픽이 발생한 것이다.
- [0025] 한편, SSRC 값이 변경된 적이 없다고 하더라도 공격자가 SSRC 값을 임의로 정상 RTP 트래픽에서 사용되는 값과 동일하게 설정하여 사용할 가능성이 있으므로 RTP 순서번호를 이용하여 추가로 이상 트래픽 발생을 탐지할 필요가 있다. RTP 헤더의 순서번호 계산부(620)는 플로우 내의 첫 패킷의 순서번호와 마지막 패킷의 순서번호 차이를 계산한다. 순서번호의 차이가 0보다 작으면 플로우 내에서 순서번호가 65535까지 사용되고, 다시 0부터 사용된 것이므로 순서번호 차이가 0보다 클 때와는 순서번호 비교를 서로 다르게 적용해야 한다. 따라서 순서번호 비교부에서 (630)은 순서번호 차이 계산시 0보다 작을 경우에 비교하는 방법을 나타내고, (640)은 순서번호 차이 계산시 0보다 큰 경우에 비교하는 방법을 나타낸다. (630)의 비교부에서는 RTP 플로우에서 최소 순서번호가 마지막 순서번호보다 크거나 최대 순서번호가 처음 순서번호보다 작을 경우 이상 트래픽으로 탐지한다. (640)의 비교부에서는 RTP 플로우에서 최소 순서번호가 처음 순서번호보다 작거나 최대 순서번호가 마지막 순서번호보다 클 경우 이상 트래픽으로 탐지한다.
- [0026] 한편 무선 인터넷 환경에 의한 VoIP 서비스의 경우에는 무선 환경에서 공격자가 정상 VoIP 트래픽을 스니핑하여 이상 트래픽의 생성이 가능하기 때문에 802.11의 헤더정보를 추가로 비교할 필요가 있다. 도 4는 무선 인터넷에 의한 VoIP 서비스 환경에서 VoIP 응용에 사용자의 전화를 취소시키는 CANCEL DoS 이상 트래픽에 대하여 VoIP 트래픽을 모니터링한 결과를 이용하여 탐지하는 것을 보여주는 순서도이다. 본 도면에서 CANCEL DoS 이상 트래픽 탐지는 출발지 MAC 주소 검사부(410)와 802.11 MAC 헤더의 순서번호를 이용한 검사부(420)로 구성된다.
- [0027] 탐지된 SIP 메시지의 헤더 정보로부터 SIP 메시지가 CANCEL 메시지로 판명되면, 데이터베이스로부터 본 SIP 메시지와 같은 CALL-ID와 4-tuple(출발지/목적지 IP 주소와 포트번호)을 가지는 INVITE 메시지를 검색하여 CANCEL 메시지와 INVITE 메시지의 802.11 헤더 정보로부터 추출한 출발지 MAC 주소를 비교한다. 정상적인 CANCEL 메시지의 경우에는 전화를 거는 UAC(User Agent Client)가 CANCEL 메시지를 보낸 것이므로 INVITE 메시지와 CALL 메시지의 출발 MAC 주소가 일치할 것이므로, MAC 주소가 일치하지 않는다면 VoIP 응용 이상 트래픽에 의한 것으로 판단한다.
- [0028] 상기 MAC 주소가 일치한다고 하더라도 무선 랜 환경에서 공격자가 정상 트래픽의 출발지 MAC 주소를 그대로 복사하여(스니핑)하여 이상 트래픽을 생성할 가능성이 있으므로, 802.11 MAC 헤더의 순서번호를 이용한 검사부(420)에서는 이 순서번호를 이용하여 추가적으로 CALL DoS 이상 트래픽 탐지를 수행한다. 보다 구체적으로 출발지 MAC 비교 검사부(410)에서 둘의 MAC 주소가 동일할 경우, CANCEL 메시지의 이전 IP 패킷의 순서번호와 비교를 통하여 순서번호의 차이가 소정의 값 이상이면 CANCEL DoS 이상 트래픽이 발생한 것으로 간주한다. 상기 순서번호의 차이는 네트워크 환경에 따라 적절히 조절될 수 있으므로 5 정도의 값을 사용하는 것이 바람직하다. 순서번호의 차이가 5 정도의 값으로 설정한 이유는 CANCEL 패킷과 이전의 IP 패킷사이에 단말과 액세스 포인트 사이에 IP 계층을 사용하지 않는 패킷이 존재하기 때문이다. 이들 패킷은 802.11 환경에서 송수신되는 패킷으로써 802.11 MAC 헤더만 존재한다.
- [0029] 본 발명은 또한 전술한 방법에 의한 VoIP 응용 이상 트래픽 탐지 및 모니터링을 위한 장치에 관한 것으로, 본 발명의 장치는 (A) 라우터 또는 무선 라우터에서 VoIP 트래픽을 탐지하고 그로부터 SIP 메시지와 RTP 트래픽의 헤더 정보를 추출하는 VoIP 트래픽 탐지 및 분석 장치와 (B) VoIP 트래픽 탐지 및 분석 장치로부터 얻어진 정보로부터 VoIP 응용 이상 트래픽의 발생 여부를 판정하고, 이를 시각화하는 VoIP 응용 이상 트래픽 탐지 서버로 이루어진다. 도 1은 전체적인 시스템을, 도 5와 도 6은 VoIP 트래픽 탐지 및 분석 장치와 VoIP 응용 이상 트래픽 탐지 서버를 각각 개략적으로 보여준다.
- [0030] 먼저 도 5의 VoIP 트래픽 탐지 및 분석장치는 단말기와 프록시 서버 사이의 경로에 존재하는 라우터 또는 무선 라우터에서 VoIP 트래픽에 대한 모니터링을 실시하며, (a) 네트워크의 IP 패킷을 캡처하여 VoIP 트래픽의 SIP

메시지와 RTP 트래픽을 분류하는 SIP/RTP 트래픽 탐지부(210); (b) 분류된 SIP 메시지, RTP 트래픽과 802.11의 헤더 정보를 추출하는 SIP/RTP 트래픽 분석부(220); (c) 분석된 헤더정보로부터 SIP/RTP 플로우 테이블을 생성하는 SIP/RTP 플로우 생성부(230); 및 (d) 생성된 SIP/RTP 플로우 테이블로부터 IPFIX 플로우를 생성하고 전송하는 IPFIX 플로우 전송부(240);로 이루어진다.

[0031] SIP/RTP 플로우 생성부(230)에서는 트래픽 모니터링이 되는 네트워크로 인터페이스로부터 트래픽을 수집하고, 이들 트래픽 중 SIP와 RTP 트래픽에 대한 플로우 테이블을 관리한다. 수집된 SIP/RTP 트래픽이 새로운 플로우이면 테이블을 생성하고, 기존에 저장된 플로우가 존재하면 일부 테이블의 값을 업데이트 한다. 생성부에서 사용되는 플로우 테이블은 이들 트래픽의 IP 주소, 포트번호 및 SIP와 RTP 헤더 정보등이 포함된다. 플로우 테이블에 저장된 정보는 IPFIX 플로우가 생성되기 전 일정시간 동안 유지된다. IPFIX 플로우 전송부(240)에서는 상기 일정 시간 후 플로우 테이블에 저장된 정보를 이용하여 IPFIX 플로우를 생성하며, 플로우 테이블의 정보는 삭제된다. 생성된 IPFIX 플로우는 IPFIX 플로우 전송부(240)를 통해 VoIP 응용 이상 트래픽 탐지 서버(300)로 전송된다.

[0032] 도 3은 VoIP 응용 이상 트래픽 탐지 서버의 구조를 보여주는 도면으로 (a) VoIP 트래픽 탐지 및 분석 장치로부터 전송된 IPFIX 플로우를 수신하는 IPFIX 플로우 수신부(310); (b) 수신된 IPFIX 플로우를 분석하여 SIP/RTP 트래픽의 헤더정보를 저장하는 데이터베이스(320); 및 상기 SIP/RTP 트래픽 정보와 데이터베이스에 저장되어 있는 정보를 비교하여 VoIP 응용 이상 트래픽 여부를 판단하는 VoIP 응용 이상 트래픽 탐지부;로 구성되는 VoIP 응용 이상 트래픽 탐지 서버로 이루어지는 것을 특징으로 하는 VoIP 응용 이상 트래픽 탐지 장치에 관한 것이다.

[0033] 상기 VoIP 응용 이상 트래픽 탐지 서버는 상기 VoIP 응용 이상 트래픽 탐지부에서 이상 트래픽으로 판정된 경우 해당 플로우를 시각화하는 VoIP 응용 이상 트래픽 시각화부를 추가로 포함하여 이루어질 수 있다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 실시예에 따른 SIP/RTP를 이용하는 VoIP 응용 이상 트래픽 탐지를 위한 대략적인 도면이다.

[0035] 도 2는 본 발명의 실시예에 따른 VoIP 응용에서 사용자 간의 음성 통화 중 한 사용자의 통화를 강제로 종료시키게 하는 BYE DoS 이상 트래픽 탐지 알고리즘이 적용된 흐름도이다.

[0036] 도 3은 본 발명의 실시예에 따른 VoIP 응용에 사용자 간의 음성 통화 품질을 낮추는 피해를 유발하는 RTP 플러딩 이상 트래픽 탐지 알고리즘이 적용된 흐름도이다.

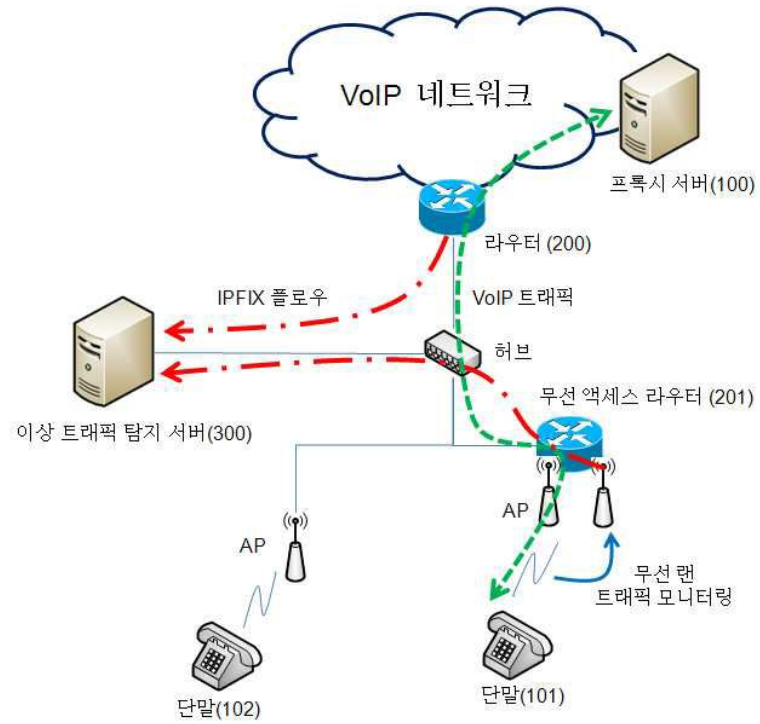
[0037] 도 4는 본 발명의 실시예에 따른 VoIP 응용에 전화 취소 피해를 유발하는 CANCEL DoS 이상 트래픽 탐지 알고리즘이 적용된 흐름도이다.

[0038] 도 5는 본 발명의 VoIP 응용 이상 트래픽 탐지 장치의 일 실시예에 의한 VoIP 트래픽 탐지 및 분석 장치를 보여주는 개략도이다.

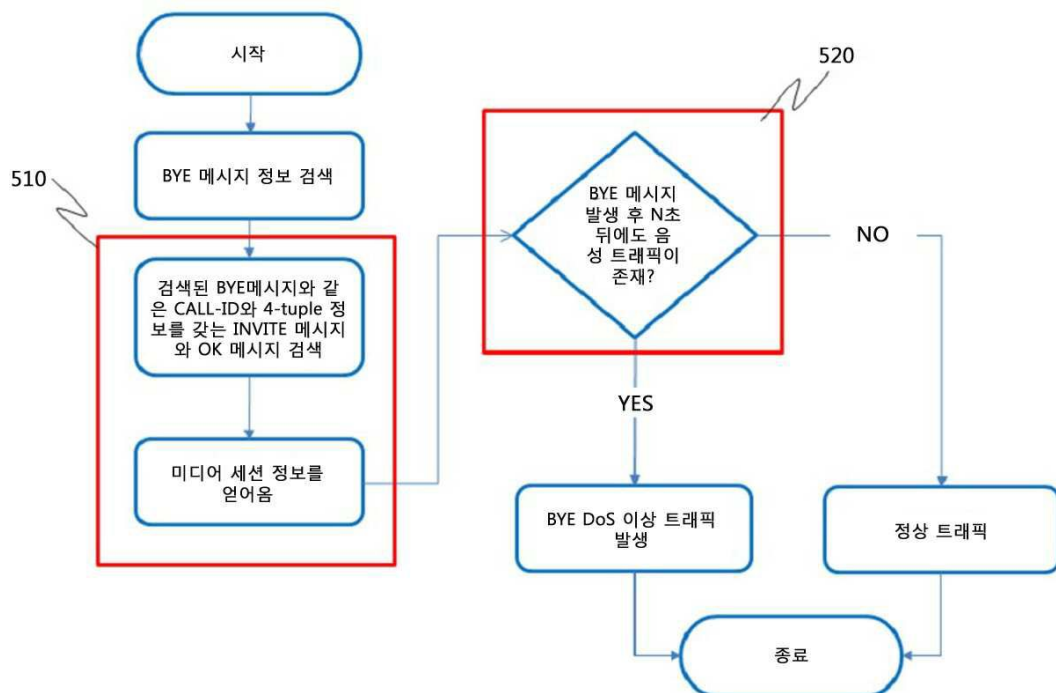
[0039] 도 6은 본 발명의 VoIP 응용 이상 트래픽 탐지 장치의 일 실시예에 의한 VoIP 응용 이상 트래픽 탐지 서버를 보여주는 개략도이다.

도면

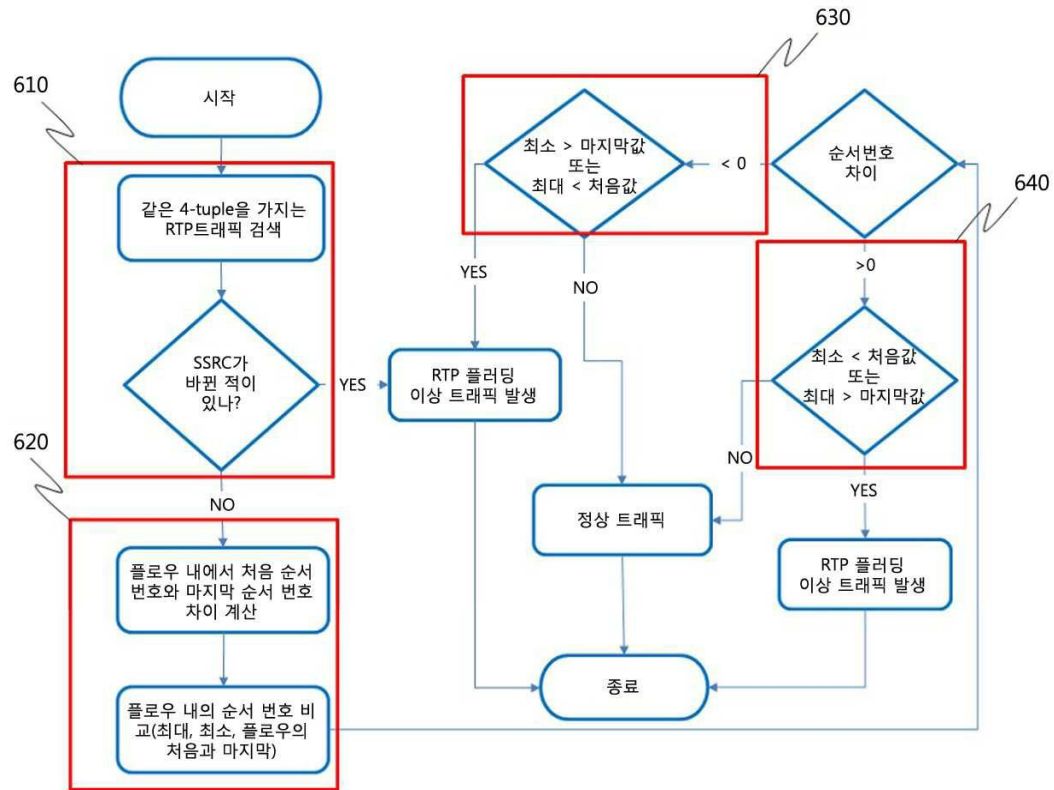
도면1



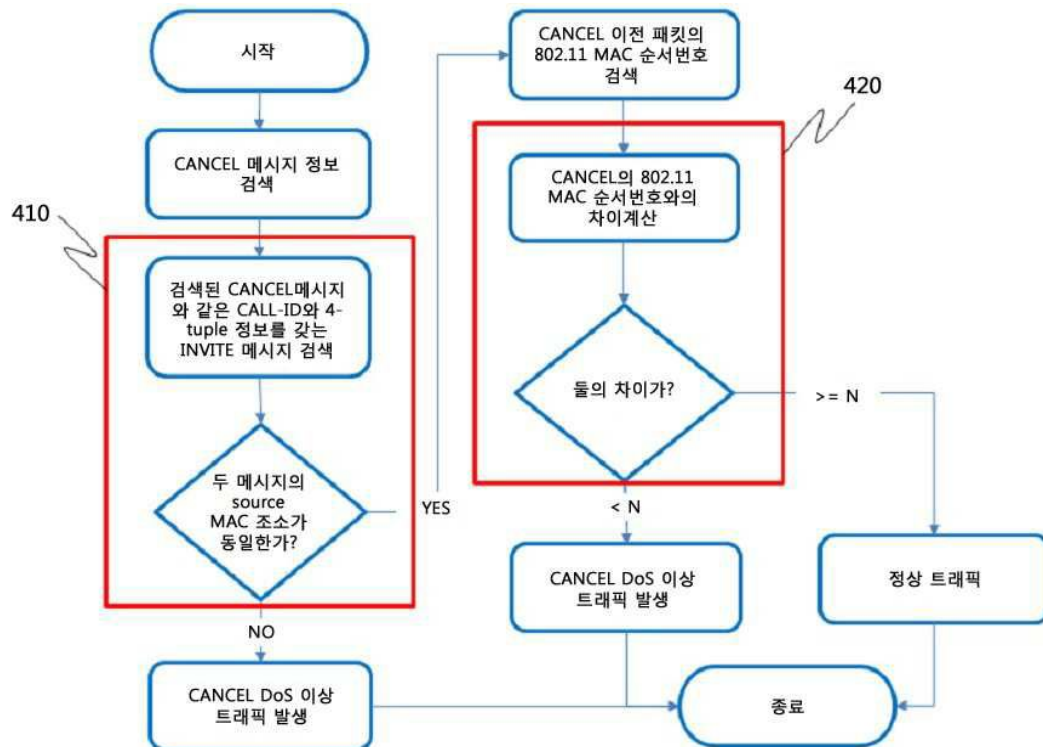
도면2



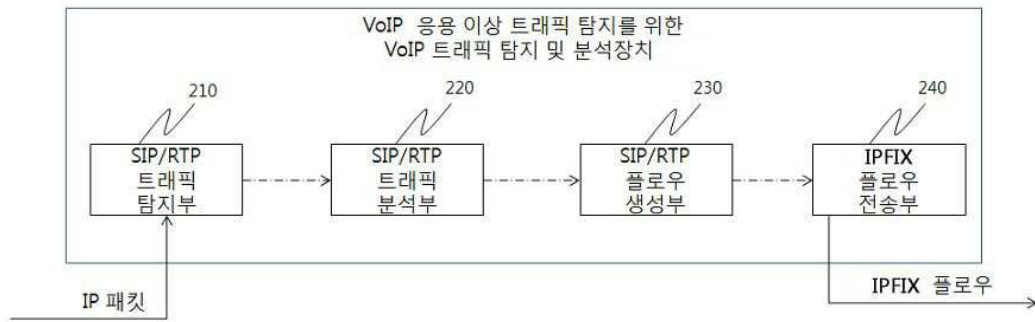
도면3



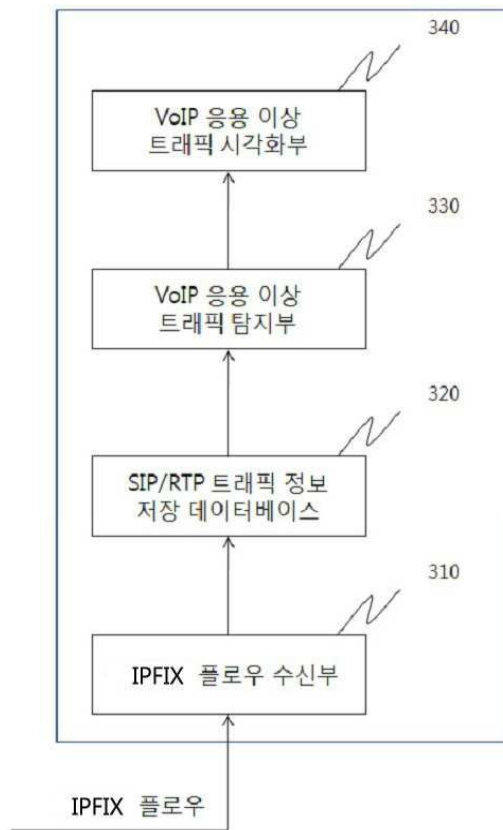
도면4



도면5



도면6



VoIP 응용 이상 트래픽 탐지 서버