(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl.[7]
H04L 12/26
H04L 29/06

(11) 공개번호 10-2005-0085604
(43) 공개일자 2005년08월29일

(21) 출원번호 10-2005-7010742
(22) 출원일자 2005년06월11일
번역문 제출일자 2005년06월11일
(86) 국제출원번호 PCT/CA2003/000724
국제출원일자 2003년05월14일
(87) 국제공개번호 WO 2004/056063
국제공개일자 2004년07월01일

(30) 우선권주장 60/433,032 2002년12월13일 미국(US)

(71) 출원인 시터시아 네트웍스 코포레이션
캐나다 브리티시 콜롬비아 브이6앤 2에스4 밴쿠버 웨스트 36 애비뉴 3708

(72) 발명자 맥이삭 개리 론느
캐나다 브리티시 콜롬비아 브이6앤 2에스4 밴쿠버 웨스트 36애비뉴 3708

(74) 대리인 박장원

심사청구 : 없음

(54) 상관함수를 사용하여 네트워크 공격을 검출하기 위한네트워크 대역폭 이상 검출 장치 및 방법

요약

통신 시스템에서 대역폭 이상들을 검출하는 방법은 제 1 시간 기간에 제 1 방향에서 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 단계와, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하는 단계와, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호을 생성하는 단계를 포함한다.

대표도

도 3

색인어

대역폭 이상 검출, DDoS,

명세서

기술분야

본 발명은 일반적으로 컴퓨터 네트워크 및 보안, 분산 서비스 거부 공격(Distributed Denial of Service attacks)에 관한 대역폭 남용에 관한 것이고, 그리고 더욱 상세하게 네트워크 대역폭 이상 검출 장치, 방법, 신호 및 매체에 관한 것이다.

배경기술

고속 개인 인터넷 접속 그리고 상업, 오락 및 교육을 위한 월드 와이드 웹 사용의 급속한 확장은 광역 사용자 커뮤니티에 상당한 장점을 제공한다. 웹 기반 정보 서비스들에 대한 저비용의 광범위하면서도 연속적인 이용가능성은 공공 및 교육 서비스에 대한 액세스를 제공하는 포탈들에 대한 새로운 사업 모델에서부터 인터넷 커뮤니티의 모든 사용자들에게 사상과 정보를 빠르고 자유롭게 교환하는 범위에 이르기까지 발전을 가능하게 했다.

인터넷이 대중에게 매우 광범위하게 이용가능하기 때문에, 인터넷 운용에 기본적인 네트워크 프로토콜 특성들의 다양한 유해한 이용들에 의해 붕괴되기 쉽다. 유해한 이용들은 특정 운용 시스템이나 애플리케이션을 타켓(target)으로하는 전염성 컴퓨터 바이러스의 생성과 전파, 패킷 브로드캐스팅과 TCP/IP 접속 확립과 같은 네트워크 프로토콜 피처들의 남용, 그리고 네트워크-접속된 컴퓨터 시스템들에의 침입을 포함한다.

상기 유해한 이용들의 가해자들은 종종 컴퓨터 운용 시스템 결점 및 허술한 액세스 제어 비밀번호의 선택과 같은 시스템 구성에 있어서 인간의 오류를 이용한다. 시스템 관리자 및 사용자들은 프로시저(procedure) 변경, 소프트웨어 패치의 적용과 같은 방법으로 컴퓨터 시스템의 취약점을 최소화할 수 있다. 소프트웨어 버그들은 끊임없이 출현하고, 사용자 구성 에러들이 제공되며, 공격자들은 시스템에서의 기존에 알려지지 않은 약점들을 밝혀내거나 새로운 방법으로 현행 공격 소프트웨어를 수정할 것이다.

보안 컴퓨터 시스템조차도 인터넷 접속이 중단되기 쉽다. 인터넷 웹 사이트들, 도메인 네임 서버 및/또는 코어 라우터들의 사용자에게 심각한 혼란을 야기할 수 있는 유해한 인터넷 활동의 한가지 유형은 소위 "분산 서비스"(DDoS) 공격을 포함한다. 이러한 공격들은 방어하기가 매우 어려운바, 이는 인터넷 자체의 운용에 기초적인 기능들을 사용하기 때문이다.

DDoS 공격들은 인터넷 전반에 퍼져있는 서로 다른 수많은 컴퓨터 시스템들의 통합되어 상기 통합된 컴퓨터들상에 드론 소프트웨어 에이전트(drone software agent)들을 설치함에 특징이 있다. 상기 통합된 공격 시스템들은 수십, 수백 혹은 수천 개의 컴퓨터들일 수 있다. 상기 트론 소프트웨어 에이전트는 통합된 컴퓨터들 각각이 동시에 패킷들의 범람을 개시하도록 한다. 상기 패킷들은 선택된 타겟 시스템으로 향하도록 한다. 상기 패킷들은, 예컨대, 모두 타겟 시스템으로 향하는 전송 제어 프로토콜(TCP), 사용자 데이터그램 프로토콜(UDP) 및/또는 인터넷 제어 메시지 프로토콜(ICMP) 패킷들의 연속적인 스트림들을 포함한다. 상기 프로토콜들은 인터넷 엔지니어링 태스크 포스("IETF") RFC 표준 1122에 기재되고 그리고 RFC 문서에 관련된 인터넷 층과 전송 층에서 구현된다.

통합된 컴퓨터 시스템에 의해 생성된 들어오는 패킷들을 처리하는 것은 타켓 컴퓨터 시스템의 자원을 매우 많이 소모하여 정상 요청들을 서비스할 수 없게된다. 종종 이러한 유형의 서비스 거부 공격은 확장된 시간 기간 동안 유지될 수 있고, 상기 공격 동안에 타켓 서버를 이용 불가능하게 한다. 게다가, 타겟 시스템으로 향하는 모든 패킷들의 범람은 타겟 시스템 인접하여 위치한 라우터들의 패킷 프로세싱 능력을 과부하 할 수 있다. 따라서, 분산 서비스 거부 공격은 컴퓨터 시스템(공격에 대해 직접 타겟이 되지 않음)의 사용자들에게 영향을 미친다.

DDoS 공격들은 그들에 대한 소스의 추적이 매우 어렵다. 대부분 경우에, 범람하는 패킷들에서 발견되는 상기 소스 인터넷 프로토콜(IP) 어드레스들은 거짓이며, 즉, 거짓 값으로 대체되어 있으므로, 근원 시스템의 진실한 실체에 대한 어떠한 정보도 제공하지 않는다.

분산 서비스 거부 공격들에 사용되는 소프트웨어 에이전트들의 상세한 설명은 카네기-멜론 대학 소프트웨어 엔지니어링 연구회(Carnegie-Mellon Software Engineering Institute)에 의해 운영되는 컴퓨터 비상 대응 팀(CERT) 웹 사이트, "CERT Advisory CA-2000-0 1 Denial-of-Service Developments"에서 개시된다.

알려진 드론 에이전트들의 징후를 식별하고 및/또는 드론이 공격에 사용되는 패킷들의 소스 어드레스를 속이는 능력을 제한하는 몇 가지 수단들을 제공하는 일부 시스템들이 존재한다. 예컨대, 1997년 2월 25일 발행된 미국 특허 번호 5,606,668인 제목 "System for Securing Inbound and Outbound Data Packet Flow in a Computer Network"에 설명된 것과 같은 패킷 필터링 방화벽들(firewall)이 일정 패킷들이 특정 컴퓨터 혹은 네트워킹 도달하기 전에 차단하는데 사용될 수 있다. 패킷 필터링 방화벽은 상기 방화벽에서 수신된 각 패킷의 헤더의 내용을 조사하고 규정을 적용하여 상기 패킷들로 무엇이 행해졌는지를 결정한다. 방화벽에 많은 규정이 적용될수록 성능은 떨어지고 방화벽 유지는 증가한다. 그러나, 패킷 필터링 방화벽은 DDoS에 대한 효과적인 방어를 제공하지 못하는바, 이는 상기 방화벽 자체가 들어오는 패킷들에 의해 압도될 수 있기 때문이다.

침입 검출 시스템들은 컴퓨터 시스템이 포함되었는지를 결정하는데 사용될 수 있다. 미국 특허 번호 6,088,804인 제목 "Adaptive System and Method for Responding to Computer Network Security Attacks"은 모조된 공격 징후들(예컨대, 바이러스 패턴들)을 학습하는 적응성 신경 네트워크 기술과 에이전트들을 사용하는 이러한 하나의 시스템을 설명한다. 상기 시스템의 단점은 실제 공격 징후들이 모조된 징후들과 유사하지 않고 훈련하지 않은 새로운 징후들은 전혀 검출되지 않는다. 미국 특허 번호 5,892,903인 제목 "Method and Apparatus for Detecting and Identifying Security Vulnerabilities in an Open Network Computer Communication System"에 개시된 다른 시스템은 알려진 취약점에 대해 컴퓨터들과 네트워크 소자들을 테스트하고 네트워크 관리자에 의한 행동에 대한 보고를 제공한다. 그러나, 상기 시스템은 알려진 취약점들과 취약한 소자의 상세한 컴퓨터-시스템-특정 설명들에 대한 데이터베이스가 필요하다. 게다가, 상기 종래 기술 시스템 구현들은 통합된 컴퓨터상의 공격 징후들을 식별하기 위해 운용 시스템 특정과 패킷 내용 특정 정보에 의존한다. 침입 검출 시스템들의 개요가 Debar 등에 의한 논문 "Towards a Taxonomy of Istrusion-Detection Systems, Computer Networks 31:805-822"에 개시되어 있다.

통합되기 쉽고 그리고 다른 컴퓨터 시스템들에 대해 DDoS 공격들을 개시하는데 사용될 수 있는 인터넷 컴퓨터 시스템들은 언제나 존재한다. 상기 끊임없이 진화하는 환경에서, 침입 검출 시스템들은 검출 능력들에 있어 자연스럽게 뒤쳐진다. 암호화 기술 및 다른 은폐 방법들은 드론 에이전트들의 검출을 회피하고 그리고 유해한 사용자, 매스터 이이전트와 드론 에이전트 사이의 통신 차단을 회피하기 위해 공격 가해자들에 의해 사용된다.

일반적으로, 공격의 타겟으로부터 공격의 소스에 이르는 경로를 발견하는 쉬운 방법은 없다. 소스 시스템들의 위치를 찾아내는 것은 시간 소모적인 프로세스로서, 시스템과 라우터의 운용 기록 및 광범위한 휴먼 통신(human communication)에 대한 상세한 조사와 영향을 받은 당사자들 사이에 증거를 교환하기 위한 협력을 포함한다. 이러한 문제를 해결하고자하는 하나의 시스템이 WO/01/46807에 개시된다. 그러나, 상기 시스템은 복수의 인터넷 서비스 제공자들(ISPs)에 속하는 라우터에 대한 자동 액세스와 라우터 소프트웨어에 대한 상당한 변경들을 필요로 한다. 이러한 액세스 레벨은 경쟁하는 ISP들 사이에 존재하지 않을 것이다.

네트워크 보안과 침입 검출에 대한 분야의 종래 기술은 이상 네트워크 데이터 트래픽을 검출하기 위해 패킷 내용들의 조사와 고 레벨 프로토콜 분석(higher level protocol analysis)(예컨대, TCP 층 접속 핸드세이킹(handshaking)과 흐름 식별)에 초점을 두었다. 이러한 시스템들 및 방법들은 데이터 링크를 이동하는 모든 패킷들에 대한 세밀한 조사를 포함하고 상당한 프로세싱과 메모리 자원들뿐 아니라 네트워크 관리자에 의한 더욱 복잡한 구성을 필요로 한다.

현재의 방법들은 DDoS 공격들의 타겟들 혹은 ISP 코어 라우터들을 보호하는데 주목한다. 상기 방법들은 자동 혹은 사용자 제어 방식으로 소스에 인접한 유해한 대역폭 소모의 공격을 빠르게 검출하지 못하고 그리고 네트워크 트래픽에서 이상 변경들을 즉시 검출하지 못하며, 상기 공격을 마운트하는 상부 층 네트워크 프로토콜들에 무관하다.

발명의 상세한 설명

본 발명은 데이터 통신 시스템에서 대역폭 이상들을 검출하는 방법을 제공함으로써 상기 문제에 대처한다. 상기 방법은 네트워크상의 분산 서비스 거부 공격의 결과로서 발생하는 유형의 대역폭 이상들을 검출할 수 있다. 매우 기본적인 형태로, 상기 방법은 제 1 시간 기간에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 단계와, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하는 단계와, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 단계를 포함한다.

서비스 거부 공격 신호를 생성하는 단계는 상기 상관 값이 기준 값보다 작으면 상기 서비스 거부 공격 신호를 생성하는 단계를 포함한다. 서비스 거부 공격 신호를 생성하는 단계는 상기 상관 값이 상기 기준 값보다 작은지 여부를 결정하는 단계를 포함한다.

상기 방법은 트래픽 측정값들의 제 1 세트에 응답하여 상기 제 1 트래픽 파형을 발생하는 단계를 포함한다. 상기 제 1 트래픽 파형을 발생하는 단계는 트래픽 측정값들의 상기 제 1 세트를 이산 웨이브렛 변환(discrete wavelet transform)하는 단계를 포함한다. 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들이 사용된다. 이산 웨이브렛 변환은 상기 제 1 트래픽 파형을 나타내는 제 1 성분을 생성한다. 상기 상관 값을 생성하는 단계는 상기 제 1 성분과 상기 기준 파형을 상관하는 단계를 포함한다.

상기 동일한 프로세서 회로가 상기 제 1 트래픽 파형을 발생하고 상기 제 1 트래픽 파형과 상기 기준 파형을 상관하는데 사용된다.

상기 방법은 상기 제 1 방향에서 데이터를 모니터링하고 이에 응답하여 트래픽 측정값들의 상기 제 1 세트를 생성하는 단계를 포함한다.

트래픽 측정값들의 상기 제 1 세트를 생성하는 단계는 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성하는 단계를 포함한다.

프로세서 회로는 상기 제 1 트래픽 파형을 생성하고 이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하도록 통신 인터페이스와 통신하는데 사용된다.

상기 제 1 방향에서 데이터를 모니터링하는 단계는 상기 제 1 방향에서 패킷들을 계수하는 단계 및 옥텟들을 계수하는 단계 중 적어도 하나를 포함한다.

상기 제 1 트래픽 파형을 생성하는 프로세서 회로는 트래픽 측정값들을 나타내는 값들을 수신하기 위해 패킷 계수기(counter) 및 옥텟 계수기 중 적어도 하나와 통신하도록 구성된다. 상기 프로세서 회로는 상기 패킷 계수기 및/또는 상기 옥텟 계수기를 구현하도록 구성된다.

상기 방법은 상기 제 1 방향에서 상기 데이터를 수동적으로 모니터링하는 단계를 더 포함한다.

상기 방법은 상기 서비스 거부 공격 신호에 응답하여 연산자를 신호하는 단계를 더 포함한다.

상기 방법은 상기 서비스 거부 공격 신호에 응답하여 상기 네트워크로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 단계를 더 포함한다.

상기 방법은 제 2 시간 기간에 상기 데이터 통신 시스템상의 제 2 방향에서 데이터 볼륨의 시 분배를 나타내는 제 2 트래픽 파형을 수신하고, 그리고 상기 상관 값을 생성하기 위해 상기 제 2 트래픽 파형을 상기 기준 파형으로 사용하는 단계를 더 포함한다.

상기 방법은 트래픽 측정값들의 제 1 및 제 2 세트들에 응답하여 각각 네트워크상의 제 1 및 제 2 방향에서 트래픽을 나타내는 상기 제 1 및 제 2 트래픽 파형들을 생성하는 단계를 포함한다.

상기 제 1 및 제 2 트래픽 파형들을 생성하는 단계는 트래픽 측정값들의 상기 제 1 및 제 2 세트들 각각을 이산 웨이브렛 변환하는 단계를 포함한다. 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들이 사용된다. 이산 웨이브렛 변환은 제 1 트래픽 파형을 나타내는 제 1 성분과 제 2 트래픽 파형을 나타내는 제 2 성분을 생성한다. 상기 상관 값을 생성하는 단계는 상기 제 1 및 제 2 성분들을 상관하는 단계를 포함한다.

상기 방법은 상기 상관 값을 생성하는데 사용되는 트래픽 파형 생성기를 프로세서 회로에 구현하는 단계를 포함한다.

상기 방법은 상기 제 1 및 제 2 방향에서 데이터를 모니터링하고 이에 응답하여 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 생성하는 단계를 포함한다.

트래픽 측정값들을 생성하는 단계는 상기 제 1 및 제 2 방향에 대해 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성하는 단계를 포함한다.

상기 방법은 이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하도록 통신 인터페이스와 통신하기 위해 프로세서 회로가 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 한다.

모니터링 단계는 상기 제 1 및 제 2 방향 각각에서 패킷들 및 옥텟들 중 적어도 하나를 계수하는 단계를 포함한다.

상기 방법은 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 나타내는 값들을 수신하도록 패킷 계수기 및/또는 옥텟 계수기와 통신하기 위해 프로세서 회로가 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 한다.

상기 방법은 상기 프로세서 회로가 상기 패킷 계수기 및 상기 옥텟 계수기 중 적어도 하나를 구현하도록 하는 단계를 포함한다.

상기 방법은 상기 제 1 및 제 2 방향에서 데이터를 수동적으로 모니터링하는 단계를 포함한다.

상기 방법은 상기 서비스 거부 공격 신호에 응답하여 연산자를 신호하는 단계를 더 포함한다.

상기 방법은 상기 서비스 거부 공격 신호에 응답하여 상기 네트워크로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 단계를 더 포함한다.

상기 제 1 및/또는 제 2 트래픽 파형들은 제 1 및 제 2 방향에서 데이터 볼륨의 제 1 및 제 2 시 분배(time distribution) 각각의 통계 측정을 나타낸다.

본 발명의 다른 양상에 따르면, 데이터 통신 시스템에서 대역폭 이상들을 검출하는 장치가 제공된다. 상기 장치는 제 1 시간 기간에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 설비와, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하는 설비와, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 설비를 포함한다.

본 발명의 다른 양상에서, 데이터 통신 시스템에서 대역폭 이상들을 검출하도록 프로세서 회로에 지시하는 코드들로 인코딩된 컴퓨터 판독가능 매체가 제공되는바, 상기 대역폭 이상 검출은 상기 프로세서 회로가 제 1 시간 기간에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하고, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하고, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하도록 함으로써 이루어진다.

본 발명의 또 다른 양상에서, 데이터 통신 네트워크에서 대역폭 이상들을 검출하도록 프로세서 회로에게 지시하는 코드들로 인코딩된 컴퓨터 판독가능 신호가 제공되는바, 상기 대역폭 이상 검출은 상기 프로세서 회로가 제 1 시간 기간에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하고, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하고, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하도록 함으로써 이루어진다.

본 발명의 다른 양상에서, 데이터 통신 시스템에서 대역폭 이상들을 검출하는 장치가 제공된다. 상기 장치는 제 1 시간 기간에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하고, 상기 제 1 트래픽 파형과 기준 파형의 상관관계를 나타내는 상관 값을 생성하고, 그리고 상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하도록 구성된 프로세서 회로를 포함한다.

상기 프로세서 회로는 상기 상관 값이 기준 값보다 작은지 여부를 결정하고 그리고 상기 상관 값이 상기 기준 값보다 작으면 상기 서비스 거부 공격 신호를 생성하도록 구성된다.

상기 장치는 트래픽 측정값들의 제 1 세트를 수신하고 이에 응답하여 제 1 트래픽 파형을 생성하는 제 1 트래픽 파형 생성기를 더 포함한다. 상기 제 1 트래픽 파형 생성기는 트래픽 측정값들의 제 1 세트를 이산 웨이브렛 변환함으로써 상기 제 1 트래픽 파형을 생성하도록 구성된다. 상기 제 1 트래픽 파형 생성기는 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들을 사용하도록 구성되고 그리고 상기 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분을 생성하도록 구성된다.

상기 프로세서 회로는 상기 제 1 성분과 기준 파형을 상관함으로써 상기 상관 값을 생성하도록 구성되나.

상기 프로세서 회로는 상기 제 1 트래픽 파형 생성기를 구현하도록 구성된다.

상기 장치는 상기 제 1 방향에서 데이터를 모니터하고 이에 응답하여 트래픽 측정값들의 제 1 세트를 생성하는 통신 인터페이스를 더 포함한다. 상기 통신 인터페이스는 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성한다. 상기 프로세서 회로는 이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되며, 상기 값들은 트래픽 측정값들의 제 1 세트를 나타낸다.

상기 통신 인터페이스는 상기 제 1 방향에서 데이터의 패킷들 및 옥텟들 각각을 계수하는 패킷 계수기와 옥텟 계수기 중 적어도 하나를 포함한다. 상기 프로세서 회로는 상기 패킷 계수기와 상기 옥텟 계수기 중 적어도 하나에 의해 생성된 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되며, 상기 값들은 네트워크 트래픽 측정값들의 제 1 세트를 나타낸다.

상기 프로세서 회로는 상기 통신 인터페이스를 구현하도록 구성된다.

상기 장치는 상기 제 1 방향에서 데이터를 수동적으로 모니터하고 그리고 상기 통신 인터페이스에 제 1 방향에서 데이터의 사본을 제공한다.

상기 장치는 상기 서비스 거부 공격 신호에 응답하여 연산자를 신호하는 신호 디바이스를 포함한다.

상기 장치는 상기 서비스 거부 공격 신호에 응답하여 상기 네트워크로부터의 데이터의 전송 및 수신 중 적어도 하나를 제어하는 통신 제어 디바이스를 포함한다.

상기 프로세서 회로는 제 1 시간 기간에 데이터 통신 네트워크에서 제 2 방향에서 데이터 볼륨의 시 분배를 나타내는 제 2 트래픽 파형을 수신하고, 그리고 상관 값을 생성하기 위해 상기 제 2 트래픽 파형을 상기 기준 파형으로 사용하도록 구성된다.

상기 장치는 트래픽 측정값들의 제 1 및 제 2 세트들을 수신하고 이에 응답하여 상기 제 1 및 제 2 트래픽 파형들을 생성하는 트래픽 파형 생성기를 더 포함하거나, 혹은 트래픽 측정값들의 상기 제 1 및 제 2 세트들에 응답하여 상기 제 1 및 제 2 트래픽 파형들을 각각 생성하도록 제 1 및 제 2의 별개의 트래픽 파형 생성기를 이용할 수 있다.

상기 트래픽 파형 생성기(들)는 트래픽 측정값들 각각을 이산 웨이브렛 변환하여 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 구성된다.

상기 트래픽 파형 생성기(들)는 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 값들을 사용하도록 구성되고, 그리고 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분과 상기 제 2 트래픽 파형을 나타내는 제 2 성분을 생성하도록 구성된다.

상기 프로세서 회로는 상기 제 1 및 제 2 성분들을 상관함으로써 상기 상관 값들을 생성하도록 구성된다.

상기 프로세서 회로는 상기 트래픽 파형 생성기(들)를 구현하도록 구성된다.

상기 장치는 상기 제 1 및 제 2 방향에서 데이터를 모니터하고 이에 응답하여 각각 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 생성하는 통신 인터페이스를 더 포함한다.

상기 통신 인터페이스는 상기 제 1 및 제 2 방향 각각에 대해 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성한다. 상기 프로세서 회로는 각 방향에 대해 이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하기 위해 통신 인터페이스와 통신하도록 구성되며, 상기 값들은 각각 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 나타낸다.

상기 통신 인터페이스는 상기 제 1 및 제 2 방향 각각에 대해 데이터의 패킷 및 옥텟을 각각 계수하는 패킷 계수기 및 옥텟 계수기 중 적어도 하나를 포함한다. 상기 프로세서 회로는 상기 패킷 계수기와 상기 옥텟 계수기 중 적어도 하나에 의해 생성된 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되며, 상기 값들은 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 나타낸다.

상기 프로세서 회로는 상기 통신 인터페이스를 구현하도록 구성된다.

상기 장치는 상기 제 1 및 제 2 방향에서 데이터를 수동적으로 모니터하고 상기 데이터의 사본을 상기 통신 인터페이스에 제공하는 수동 모니터를 더 포함한다.

상기 장치는 상기 서비스 거부 공격 신호에 응답하여 연산자를 신호하는 신호 디바이스를 포함한다.

상기 장치는 상기 서비스 거부 공격 신호에 응답하여 네트워크로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 통신 제어 디바이스를 포함한다.

어떤 경우, 상기 발명은 상기 데이터 트래픽을 데이터 트래픽 파형으로 해석하고 상기 데이터 트래픽 파형의 특성을 분석함으로써 전송된 데이터 트래픽의 이상 레벨의 개시를 검출하는 방법을 제공한다. 일 실시예에서, 데이터 트래픽 파형은 주파수와 볼륨(즉, 복수의 시간 기간들 각각에서 양방향 컴퓨터 네트워크 링크상의 특정 위치에서 관찰되는 데이터 트래픽의 유닛들 갯수)을 기록함으로써 샘플링된다.

DDoS 공격을 검출하고 그 다음 무력화하는 것의 장점(바람직하게 DDoS 에이전트들로 감염된 개개의 컴퓨터들의 레벨에서)은 유해한 네트워크 트래픽을 생성하는 시스템들의 발신 통신을 차단함으로써 얻어진다. 본 명세서의 상기 방법 및 장치는 소스 컴퓨터들상의 잠재적인 DDoS 에이전트들에 근접한 네트워크의 에지에서 혹은 근처에서 대역폭 사용을 모니터링하도록 사용된다. 본 발명에 따른 장치 및 방법은 예컨대 부분별 이더넷 스위치들, 라우터, 혹은 개인용 방화벽 하드웨어 및 방화벽 소프트웨어의 요소로서 합체될 수 있다.

도면의 간단한 설명

본 발명의 전술한 양상들 및 다른 양상들은 이들의 특정 실시예들에 대한 하기의 설명들과 이들을 묘사하는 첨부 도면들로부터 더욱 명백해질 것이지만, 본 발명의 예시에 지나지 않는다. 도면은 다음과 같다.

도 1은 본 발명의 일 실시예에 따라 대역폭 이상 검출기를 이용하는 데이터 통신 시스템의 도식적인 다이어그램이다;

도 2는 데이터 통신 시스템에서 데이터 트래픽을 나타내는 트래픽 측정값들의 제 1 세트의 그래프 표현이다;

도 3은 도 1에 도시된 상기 통신 시스템의 네트워크 서브시스템의 블록 다이어그램이다;

도 4는 서비스 거부 공격과 연관되지 않은 데이터에 대해서 도 1의 데이터 통신 시스템상의 제 1 및 제 2 방향에서 데이터 볼륨의 시 분배를 나타내는 제 1 및 제 2 파형들을 나타내는 그래프이다;

도 5는 본 발명의 일 실시예 및 이의 대체 실시예에 따른 프로세서 회로의 블록 다이어그램이다;

도 6은 서비스 거부 공격에 연관된 데이터에 대해서 도 1의 데이터 통신 시스템상의 제 1 및 제 2 방향에서 데이터 볼륨의 시 분배를 나타내는 제 1 및 제 2 파형들을 나타내는 그래프이다;

도 7 및 도 8은 도 5에 도시된 프로세서 회로에 의해 실행되는 방법의 흐름 다이어그램이다.

실시예

도 1에서 본 발명의 제 1 실시예에 따른 시스템(10)이 도시된다. 상기 시스템은 컴퓨터들의 네트워크(12)를 포함하는바, 상기 컴퓨터 네트워크들은 인트라넷 혹은 인터넷과 같은 데이터 통신 시스템(14)과, 그리고 예컨대 개인용 컴퓨터(18), 제 1 서버 컴퓨터(20), 제 2 서버 컴퓨터(22) 및 네트워크 서브-시스템(24)과 같은 네트워크 디바이스들을 포함하는 복수의 노드들(16)을 구비한다. 본 실시예에서, 상기 네트워크 서브시스템은 대역폭 이상 검출기(26)와 네트워크 노드(28)를 포함하며, 상기 네트워크 노드(28)는 서브 네트워크 및/또는 일반적으로 컴퓨터 네트워크에 연결되는 복수의 디바이스들 중 어느 하나를 포함한다. 이러한 디바이스들은, 예컨대, 서버 컴퓨터, 고객 컴퓨터, 라우터, 브리지, 멀티-포트 브리지(이더넷 스위치), 허브, ATM 스위치, 및 무선 액세스 포인트들을 포함하는바, 이에 한정되지 않는다. 상기 데이터 통신 시스템(14)은 구내 정보 통신망(LAN) 혹은 인터넷과 같은 광역 통신망을 나타내는 사이트에 접속할 수 있다.

시스템(10)의 정상 동작 동안에, 네트워킹된 디바이스들(16)은 서로 통신한다. 예를 들면, 고객 컴퓨터(18)는 서버 컴퓨터들(20 혹은 22) 또는 상기 데이터 통신 시스템(14)에 연결된 다른 고객 컴퓨터들과 통신할 수 있다. 이런 모든 경우에, 네트워킹된 디바이스들(16) 사이의 통신은 수 개의 데이터 전송 프로토콜들을 사용한다. 이러한 프로토콜들은, 예컨대, 네트워크 프로토콜들의 OSI 7 계층에 따라 분류될 수 있다. 상기 프로토콜들은, 예컨대, TCP/IP 프로토콜 슈트로부터 프로토콜들을 포함한다.

고객 컴퓨터(18)와 네트워크 서브 시스템(24)에 관련된 월드 와이드 웹 서버와 같은 서버 컴퓨터(30) 사이의 일반적인 상호작용은 고객 컴퓨터(18)의 서버 컴퓨터(30)에 대한 프로토콜 접속을 초기화하는 단계를 포함한다(즉, 서버 컴퓨터(30)에 상대적인 전송 및 수신 방향에서). 그 다음, 복수의 데이터 패킷이 고객 컴퓨터(18)와 서버 컴퓨터(30) 사이에서 이동한다. 최종적으로, 프로토콜 접속은 고객 컴퓨터(18) 혹은 서버 컴퓨터(30)에 의해 종료된다. 복수의 고객 컴퓨터들과 복수의 서버 컴퓨터들 사이의 이러한 복수의 프로토콜 접속들은 네트워크상에서 패킷 이동이 집합되도록 한다. TCP/IP 프로토콜 슈트에 대한 이러한 프로세스의 상세한 설명은 출판사 Prentice-Hall, 저자 Stallings의 1998년 출판된 High-speed Networks: TCP/IP and ATM Design Principles에 개시된다. 일반적으로, 네트워킹된 디바이스 각각은 다른 네트워킹된 디바이스에 전송을 위해 데이터 통신 시스템(14)으로 데이터 패킷들을 전송하고 그리고 네트워킹된 각 디바이스는 네트워킹된 다른 디바이스에서 생성된 데이터 패킷들 데이터 통신 시스템(14)으로부터 수신한다.

데이터 통신 시스템(14)상에서 하나의 네트워킹된 디바이스와 다른 네트워킹된 디바이스 사이에서 진행되는 정상 통신들은 일반적으로 전송 및 수신 방향들에서 "버스티(bursty)"로 나타난다. 서비스 거부 공격에 의해 발생하는 것과 같은 대역폭 이상들은 넌-버스트(non-burst), 혹은 솔리드(solid)들로 나타난다. 전송 방향에서 고객 컴퓨터(18)와 서버(30) 사이의 정상 통신의 예시(40)가 도 2에 도시된다. 정상 데이터 트래픽에 대해서 수신 방에서도 유사한 활동들이 관찰된다. 전송 방향에서 서비스 거부 공격에 관련된 데이터 볼륨의 예시(41)가 도 2에 도시된다. 수신 방향에서 유사한 활동들이 관찰되지 않는다.

도 1에 도시된 실시예에서, 상기 네트워크 서브시스템(24)에 대해 상대적인 적어도 하나의 방향에서 이동하는 데이터 패킷들을 모니터하고 그리고 상기 방향에서 분산 서비스 거부 공격이 검출되면 서비스 거부 공격 신호(denial of service attack signal)를 생성하는데 대역폭 이상 검출기(26)가 사용된다. 상기 서비스 거부 공격 신호는 연산자를 신호하는 신호 디바이스를 활성화하는데 사용되고 및/또는 상기 서비스 거부 공격 신호에 응답하여 상기 네트워크로부터의 데이터의 전송 및 수신 중 적어도 하나를 제어하는 통신 제어 디바이스를 활성화하는데 사용된다.

도 3에서 예시적인 대역폭 이상 검출기(26)의 실시예가 도시되고, 그리고 본 예시에서는 데이터 통신 시스템(14)과 네트워크 노드(28)에 위치한 별개의 디바이스로 도시된다. 상기 대역폭 이상 검출기(26)는 데이터 통신 시스템(14)의 임의의 곳에 위치할 수 있는바, 상기 위치에서 상기 검출기(26)는 네트워킹된 임의의 두 개의 디바이스 사이에 전송되는 데이터 트래픽을 샘플링할 수 있어야 한다. 그러나, 대역폭 이상 검출기(26)가 잠재적인 분산 서비스 거부 공격 에이전트에 인접한 네트워크의 에지에서 혹은 근처에서 위치할 때 장점이 있으며, 예컨대, 부분별 통신 룸에서 이더넷 스위치들과 함께 위치할 수 있다.

설명 목적으로, 데이터 통신 시스템(14)과 대역폭 이상 검출기(26) 사이의 링크(42)가 도시되며, 상기 링크(42)는 제 1 전송 데이터 라인(44)과 제 1 수신 데이터 라인(46)을 구비한다. 유사하게, 제 2 링크(48)가 상기 대역폭 이상 검출기(26)와 상기 네트워크 노드(28) 사이에 제공되며 제 2 전송 데이터 라인(50)과 제 2 수신 데이터 라인(52)을 포함한다. 상기 제 1 수신 데이터 라인(46)은 네트워크 노드(28)로 향하는 데이터를 데이터 통신 시스템(14)으로부터 수신한다. 상기 제 2 전송 데이터 라인(50)은 네트워크 노드(28)에 의해 전송되고 상기 데이터 통신 시스템(14)으로 향하는 데이터를 이동한다.

상기 실시예에서, 상기 전송 데이터 라인들(44 및 50)상에서 이동하는 데이터는 네트워크상의 제 1 (전송) 방향에서 이동하는 것으로 간주하고 그리고 수신 데이터 라인들(46 및 52)상에서 이동하는 데이터는 제 2(수신) 방향에서 이동하는 것으로 간주한다.

상기 대역폭 이상 검출기(26)는 별개의 디바이스로 도시되었으나 자체로 네트워크 노드로 기능하는 장치에 합체될 수 있다. 예를 들면, 상기 대역폭 이상 검출기는, 예컨대, 라우터, 브리지, 멀티-포트 브리지, 허브, 무선 액세스 포인, 케이블/DSL 모뎀, 방화벽, 혹은 ATM 스위치에 합체될 수 있다.

상기 실시예에서, 대역폭 이상 검출기(26)는 상기 제 1 링크(42)에 대한 접속을 위해 네트워크 측 링크 접속(62)과 상기 네트워크 노드(28)에 대한 접속을 위해 노드 측 접속(64)을 구비하는 수동 모니터링 디바이스(60)를 포함한다. 상기 수동 모니터링 디바이스(60)는 상기 전송 라인(50)에 나타나는 각 데이터의 사본을 공급하는 적어도 하나의 출력(본 예시에서 출력(66))을 또한 포함한다. 상기 수동 모니터링 디바이스(60)는 적어도 하나의 방향(이번 경우에는 전송 방향)에서 데이터의 사본을 탭오프(tap off)한다. 일반적으로, 수동 모니터링 디바이스(60)는 상기 제 1 방향에서 데이터를 수동적으로 모니터하고 상기 제 1 방향에서 데이터의 사본을 다른 디바이스에서 이용가능하게 한다. 이번 애플리케이션에 사용되는 일반적인 수동 모니터링 디바이스는 캘리포니아주 서니베일의 Net Optics Corporation에 의해 제공된다.

상기 대역폭 이상 검출기(26)는 통신 인터페이스(70)를 더 포함하는바, 상기 통신 인터페이스는, 예컨대, 이더넷 인터페이스 칩, 스위치 프로세서, 혹은 보안 프로세서와 같은 네트워크 인터페이스 칩을 포함한다. 대안적으로, 상기 통신 인터페이스(70)는, 예컨대, 이산 로직 회로 및/또는 프로세서 회로를 포함하는 다른 소자들에 의해 구현될 수 있다.

상기 실시예에서, 상기 통신 인터페이스(70)는 레지스터를 구비하는 이더넷 인터페이스 칩을 포함하는바, 상기 레지스터는 인터넷 엔지니어링 태스크 포스 RFC #3144(Internet Engineering Task Force RFC #3144)에 나열된 것과 같은 이더넷 원격 모니터링 프로토콜 표준의 이더넷 통계 그룹의 특성에 관련된 값들을 제공한다. 특히, 상기 통신 인터페이스(70)는 옥텟 계수기(73) 및 패킷 계수기(75)의 옥텟 레지스터(72) 및 패킷 레지스터(74) 중 적어도 하나를 포함한다. 상기 통신 인터페이스(70)는 상기 전송 데이터 라인(50)상의 데이터 유닛들의 사본을 수신하기 위해 수동 모니터링 디바이스(60)의 출력(66)과 통신하는 입력(76)을 포함하며, 그리고 상기 데이터 유닛들의 계수를 보유하며, 그리고 특정 시간 기간 동안(본 명세서에서 샘플 시간으로 불림)에 상기 데이터 유닛들로부터 이러한 데이터 유닛들에 관련된 옥텟들의 갯수와 패킷들의 캣수를 결정한다. 상기 실시예에서, 상기 통신 인터페이스(70)는 연속적인 1/1024 초 간격 동안에 전송 데이터 라인(50)상의 옥텟들 및 패킷들의 갯수를 계수하도록 설정되고 그리고 각 간격의 끝에서 관련된 계수 값들로 상기 옥텟 레지스터(72)와 패킷 레지스터(74)를 로드(load)한다. 따라서, 각 1/1024 초마다, 새로운 계수 값이 옥텟 레지스터(72)와 패킷 레지스터(74)에서 이용가능하다. 따라서, 상기 통신 인터페이스(70)는 트래픽 측정값들을 생성하기 위해 상기 전송 라인상의 데이터를 샘플링함으로써 제 1 방향에서 데이터를 모니터한다. 일정 시간 기간 혹은 윈도우 동안(예컨대, 120초)에 모집된 상기 복수의 트래픽 측정값들은 트래픽 측정값들의 제 1 세트들로 불린다.

상기 대역폭 이상 검출기(26)는 트래픽 파형 생성기(80)를 더 포함하는바, 상기 트래픽 파형 생성기(80)는 트래픽 측정값들의 상기 제 1 세트를 수신하고 이에 응답하여 상기 전송 방향에서 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 생성한다. 상기 제 1 트래픽 파형 생성기(80)는 트래픽 측정값들의 상기 제 1 세트에 대한 웨이브렛 분석을 수행하기 위해 트래픽 측정값들의 상기 제 1 세트를 이산 웨이브렛 변환함으로써 상기 제 1 트래픽 파형을 생성하도록 구성된다.

웨이브렛 분석은 시간 기준의 범위에서 주파수의 급격한 변화의 검출을 가능하게 한다. 이산 웨이브렛 변환은 선택된 웨이브렛 함수를 사용하여 일련의 연속적인 로패스 및 하이패스 필터링 연산들의 적용을 포함하여 본래 데이터 트래픽 신호의 근사(approximation) 및 세밀한(detail) 성분들을 생성한다. 본 발명에서 이러한 목적으로 사용되는 일 예시적인 웨이브렛 함수는 Haar 웨이브렛이다. 매틀랩 웨이브렛 툴박스와 사용자의 가이드를 포함하는 상업적 소프트웨어 패키지들은 이산 웨이브렛 변환을 이용하여 신호들의 일반적인 목적 분석을 위한 유틸리티들을 제공한다.

다양한 서로 다른 계수들이 이산 웨이브렛 변환에 사용되고 그리고 이산 웨이브렛 변환에서 Haar 웨이브렛 필터를 사용하는 것은 제 1 트래픽 파형 생성기(80)가 트래픽 측정값들의 제 1 세트의 평활(smooth) 및 세부(detail) 성분들을 생성하도록 한다. 본 실시예에서, 오직 평활 성분만이 관심 대상이고 평활 성분은 제 1 트래픽 파형을 나타낸다.

도 4에서, 평활 성분이 120초 동안 점선 윤곽(82)으로 시간에 대한 크기 값으로 도시되어 있다. 도 3에 도시된 제 1 트래픽 파형 생성기(80)는 샘플링된 120 초 윈도우 동안 각 시간에 관련된 복수의 크기 값들로서 제 1 트래픽 파형을 나타내어, 트래픽 측정값들의 제 1 세트를 생성한다. 따라서, 제 1 트래픽 파형은 제 1 시간 기간 동안에 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시분배를 나타낸다.

다시 도 3에서, 대역폭 이상 검출기(26)는 대역폭 이상들(84)을 검출하기 위해 검출기를 더 포함한다. 이러한 검출기(26)는 제 1 트래픽 파형과 기준 파형을 수신하고 그리고 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값들을 생성한다. 상관 값이 기준을 만족하면, 서비스 거부 공격 신호가 생성된다.

도 3 및 도 5에서, 검출기(84)는 프로세서 회로(69)에서 구현되는바, 상기 프로세서 회로는 예를 들면 개인용 컴퓨터 시스템의 일부이다. 프로세서 회로는 CPU(71), RAM(73), 및 ROM(75)을 포함하고 그리고, 예를 들면, 통신 인터페이스(70)를 더 포함한다. 대안적으로, 프로세서 회로(69)는 스위치, 라우터, 브리지 혹은 데이터 통신 시스템에 연결가능한 임의의 장치일 것이다. 검출기(84)를 구현하는 동일한 프로세서 회로(69)는 제 1 트래픽 파형 생성기(80)와 통신 인터페이스(70)를 구현하도록 사용된다. 대안적으로, 통신 인터페이스(70), 제 1 트래픽 파형 생성기(80) 및 검출기(84)의 임의의 조합은 다양한 서로 다른 프로세서 회로 조합들을 사용하여 구현될 수 있다. 검출기(84)를 구현하는 프로세서 회로(69)는 그것이 생성하는 상관 값이 기준 값보다 작은지 여부를 결정하고 그리고 상관 값이 상기 기준 값보다 작은 경우에 서비스 거부 공격 신호를 생성하도록 구성된다. 서비스 거부 공격 신호를 생성하도록 하는 추가의 기준이 이용될 수 있는바, 예컨대, 상관 값이 일정 시간 동안에 기준 값 이하의 값으로 유지되는지를 결정하거나, 혹은 일정 시간 동안에 기준 값 아래로 상관 값이 많이 하락하는지 여부를 결정하는 것이다.

제 1 트래픽 파형과의 상관에 사용되는 기준 파형은 기저장된 파형이거나 혹은 대안적으로 수신 데이터 라인(46)상에서의 제 2 방향에서 데이터 유닛들의 모니터링에 의해 생성되는 트래픽 측정값들의 제 2 세트에 응답하여 생성되는 제 2 트래픽일 수 있다. 이러한 경우에, 수동 모니터링 디바이스(60)는 수신 데이터 라인(46)상의 데이터 유닛들의 사본을 통신 인터페이스(70)에 제공하는 제 2 출력(86)을 갖도록 구성된다. 게다가, 통신 인터페이스(70)는 옥텟 계수기(89)와 패킷 계수기(91)의 제 2 이더넷 통계 옥텟 레지스터(88)와 제 2 이더넷 통계 패킷 레지스터(90)와 함께 구성되는바, 이는 소정의 1/1024번째 초(즉, 옥텟 및 패킷들이 전송 방향에서 계수되는 동일한 시간 기간 동안에)에서 수신 데이터 라인(46)상의 옥텟 및 패킷 숫자들을 각각 나타내는 계수 값들을 유지하기 위함이다. 대안적으로, 통신 인터페이스(70)는 별개의 칩 혹은 프로세서 회로로서 구성될 수 있다. 수신 데이터 라인(46)을 모니터링함으로써 생성되는 트래픽 측정값들은 트래픽 측정값들의 제 2 세트에 축적되고 그리고, 제 1 트래픽 파형 생성기(80)와 동일하게, 상기 제 2 세트는 제 2 트래픽 파형 생성기(92)에 제공되어 도 4에 (94)로 도시된 바와 같이 제 2 트래픽 파형을 생성하는바, 이는 제 1 트래픽 파형과 상관되는 기준 파형으로서 기능한다. 대안적으로, 트래픽 측정값들의 제 1 및 제 2 세트들은 일반적으로 동일한 시간 기간 동안에 축적되어 제 1 및 제 2 트래픽 파형들을 생성한다(즉, 제 1 파형 생성기는 다중화된다).

소정의 제 1 및 제 2 트래픽 파형들을 가지고, 검출기(84)는 제 1 및 제 2 트래픽 파형들의 상관관계를 나타내고 더욱 상세하게, 전송 파형과 수신 파형 사이의 상관관계를 나타내는 도 4에 도시된 값 0.69와 같이 상관 값을 생성한다. 그 다음, 검출기는 상관 값 0.69가 0.6과 같은 소정의 값보다 큰지 여부를 결정하고, 만약 그렇다면, 동일한 시간 기간 동안에 전송 및 수신 데이터 볼륨 사이에 양질의 상관관계가 존재하여 서비스 거부 공격이 발생하지 않았음을 나타내는 서비스 거부 공격 신호 비활성을 설정한다.

도 6에서, 만약 제 1 및 제 2 파형이 (101) 및 (102)에 도시된 것과 같다면, 검출기는 0.12와 같은 상관 값을 생성할 것이고 상기 장치는 상기 상관 값이 소정의 값 0.6보다 작음을 결정하여 서비스 거부 공격과 일치하는 상관관계가 발생하였음을 나타내는 서비스 거부 공격 신호 활성을 설정할 것이다. 다시 도 3에서, 서비스 거부 공격 신호는, 예를 들면, 스위치 혹은 네트워크 노드(28)에서의 프로세서 회로를 방해하는데 사용되어 서비스 거부 공격을 중단하도록 스위치 혹은 네트워크 노드(28)가 데이터 통신 시스템(14)에 액세스하는 것이 거부된다. 대안적으로 혹은 추가로, 서비스 거부 공격 신호는 알람, 깜빡거리는 빛, 음성 신호 혹은 운용자가 인식할 수 있는 다른 자극에 의해 운용자에게 제공되어 운용자가 서비스 거부 공격이 발생하였음을 인식하도록 한다.

도 5에서, 본 명세서에 기재된 시스템의 대안적인 구현은 다른 인터페이스(100)와 함께 구현된다. 상기 인터페이스(100)는 수동 모니터링 디바이스(60)로부터 수신된 데이터 유닛들을 위해 프로세서 회로(69)로 통하는 경로를 단순히 제공하고 그리고 상기 프로세서 회로(69) 자체는 소정의 샘플링 간격에서 전송 및 수신 라인들 중 어느 하나 혹은 양쪽상에 나타나는 패킷들 및/또는 옥텟들의 숫자를 계수하는 기능을 계속 수행하는데 사용된다. 이러한 기능들을 수행하기 위해 프로세서 회로(69)에 지시하는 코드는 프로세서 회로에 EPROM과 같은 컴퓨터-판독 가능 매체(ROM(75)의 일부를 형성할 수 있음)에 제공되는 컴퓨터 판독 가능 명령어들로서 제공되며, 혹은 콤팩트 또는 플로피 디스크 그리고 프로그램가능 ROM(상기 ROM(75)의 일부를 형성할 수 있음)에 저장되어 프로세서 회로(69)에 저장될 수 있다. 대안적으로 혹은 추가로, 본 발명의 실시예에 따른 기능들을 수행하도록 프로세서 회로(69)에 지시하는 코드들은 상기 코드들(예컨대 수신 라인상의 수신된 판독 데이터 패킷들에 의해 제공되는 것과 같은)로 인코딩된 컴퓨터 판독 가능 신호의 수단으로 프로세서 회로에 공급된다.

본 발명의 대안적인 실시예를 구현하는데 사용되는 코드 블럭들을 나타내는 블럭들을 포함하는 흐름 챠트가 도 7에 도시된다. 임의의 소정의 블럭에 표시된 기능을 구현하는데 사용되는 실제 코드는 예를 들면 C, C++ 및/또는 어셈블러에 의해 쓰여진다.

상기 실시예에서, 프로세서 회로(69)는 블록(130)에 의해 옥텟 및 패킷 계수 레지스터, 어레이, 인덱스, 상태 표시, 플래그, 제어 레지스터들을 포함하는 다양한 계수기들과 레지스터들을 초기화하도록 지시받는다. 그 다음, 블록(131)은 프로세서 회로(69)가 수동 모니터링 디바이스(60)와 통신하여 수동 모니터링 디바이스가 전송 및 수신 라인상의 패킷들을 수동적으로 모니터링하는지 여부를 결정하도록 지시한다. 만약 그렇지 않다면, 상기 프로세스는 종료된다.

만약 수동 모니터링 디바이스(60)가 작동한다면, 블록(132)은 프로세서 회로(69)에게 계수기들을 초기화하도록 지시한다.

그 다음, 블록(129)은 프로세서 회로(68)에게 제 1 및 제 2 어레이들에 트래픽 측정값들의 제 1 및 제 2 세트들을 채우도록 지시한다. 이렇게 하기 위해, 블록(129)은 상기 어레이들을 채우기 위한 루프를 구현하기 위해 협동하는 두 개의 주요 기능 블록들을 포함한다. 상기 제 1 기능 블록(133)은 프로세서 회로(69)에게 인덱스 값(i)이 소정의 값(윈도우사이즈-1,

여기서 윈도우사이즈는 트래픽 데이터의 제 1 및 제 2 세트들에서 성분들의 갯수를 일컫는다)으로 계산된 기준 값 이하인지 여부를 결정하도록 지시한다. 최종적으로, 윈도우사이즈 값은 트래픽 데이터의 제 1 및 제 2 세트들의 입수 기간의 길이를 나타낸다.

블록(134)은 프로세서 회로(69)에게 제 1 및 제 2 어레이들 현재 패킷 혹은 옥텟 계수기 값들 그리고 상기 전송 및 수신 라인들을 위한 연관된 타임스탬프 값들을 입수하고 저장하고, 인덱스(i)를 증분시키고 그리고 프로세서를 블록(133)으로 회귀시킨다. 따라서, 제 1 및 제 2 어레이들은 숫자들 쌍들의 어레이들이며, 상기 제 1 숫자는 계수기 값이 관계하는 시간 간격을 나타내고 그리고 제 2 숫자는 상기 시간에 관련된 계수기 값을 나타낸다. 제 1 및 제 2 어레이들은 윈도우사이즈의 길이를 구비한 제 1 및 제 2 패킷벡터들로 불린다.

블록(135)은 프로세서 회로(69)에게 제 1 및 제 2 어레이들을 읽어서 어레이에 있는 모든 값들이 0인지를 결정하도록 지시한다. 만약 그렇다면, 프로세서 회로는 다시 블록(131)으로 회귀하여 수동 모니터가 여전히 활성화되었는지 여부를 결정하고 계수 값들을 다시 수집하도록 지시된다.

블록(136)은 상기된 파형 생성기 기능을 구현하고 그리고 프로세서 회로(69)에게 제 1 및 제 2 패킷 벡터들을 이산 웨이브렛 변환을 사용하여 웨이브렛 분석하여 상기 전송 및 수신 방향들 각각에 대해서 근사값 및 세부 값들을 생성하도록 지시한다. 근사값은 데이터 트래픽 측정들의 큰 척도(high-scale)의 저주파 성분을 나타낸다. 큰 척도는 오랜 시간 윈도우 동안에 데이터 트래피 측정들을 보기위해 신호들을 필터링하는 웨이브렛의 "늘여짐"을 일컫는다. 세부 값들은 입력 데이터 트래픽 측정들의 작은 척도(low-scale)의 고주파 성분들이다. 작은 척도는 짧은 시간 윈도우 동안에 데이터 트래픽 측정들을 보기 위해 데이터 트래픽 측정들을 필터하는 웨이브렛의 "압축"을 의비한다.

그 다음, 본 실시예에서, 블록(137)은 프로세서 회로(69)에게 이산 웨이브렛 변환에 의해 생성된 현재 및 과거 세부 값들에 대한 분산 크기를 계산하도록 지시한다. 예를 들면, 하나의 분산 크기는 표준 편차에 사용된다. 분산 크기는 세부 값들의 세트의 표준 편차를 나타내는 단일 숫자이다.

그 다음, 블록(138)은 프로세서 회로(69)에게 블록(136)에서 생성된 근사값을 전송 라인상의 정상 데이터 트래픽에 대한 근사값의 상한을 나타내는 근사임계값(AppxThreshold value)과 비교하도록 지시한다.

만약 근사값이 근사임계값을 초과하면, 블록(139)은 프로세서 회로(69)에게 서비스거부사건계수값(DoSEventCount value)을 0으로 설정하도록 지시한다.

도 8에서, 만약 근사값이 근사임계값 이상이면, 블록(141)은 프로세서 회로(69)에게 근사값 및 세부 분산 크기를 저장하도록 지시한다.

근사값 및 세부 분산 크기 값들의 저장은 이러한 값들의 축정의 효과 혹은 이러한 값들의 표현을 갖는다. 상기 값들의 세트들은 각 시간 기간 동안에 데이터 통신 시스템에서 제 1 및 제 2 방향에서 데이터 볼륨의 시 분배의 제 1 및 제 2 통계 측정들을 나타내는 제 1 및 제 2 트래픽 파형들을 나타낸다.

블록(142)은 프로세서 회로(69)에게 근사값이 근사임계값 이상이면 서비스거부사건계수값을 증분하도록 지시한다. 블록(142)은 프로세서 회로에게(69) 제 1 및 제 2 방향에 대해 저장된 근사값들 서로가 상관하도록 하여 제 1 상관 값(r1)을 생성하고, 그리고 제 1 및 제 2 방향에 대해서 저장된 분산 값들 서로가 상관하도록 하여 제 2 상관 값(r2)을 생성하도록 지시한다. 상관 값 계산의 예시들이 1967년 Snedecor, G.W.와 W.G. Cochran의 Statistical Methods에 개시되어 있다. r1 및 r2가 각각 기준을 만족하면, 즉 둘중 하나 혹은 둘 모두가 기준 상관 값 혹은 값들보다 작을때, 서비스거부사건계수값은 증분된다. 시간 t1에서 시간 t2까지 수신 라인 근사와 분산 값들 사이의 차이의 절대값에 대한 시간 t1에서 시간 t2까지 전송 라인 근사와 분산 값들 사이의 차이의 절대값의 비율이 안정한 값을 유지할 때와 같은 다른 기준이 서비스거부사건계수값의 증분 여부를 표시하기 위해 사용될 수 있다. 이러한 안정한 값은 사용자 정의 혹은 정상 데이터 트래픽 파형이 나타날 때의 기간 동안에 과거 측정들에 기초한다. 전송 라인 데이터 트래픽과 수신 라인 데이터 트래픽 사이의 상관 정도는, 예컨대 대안적으로, Earl의 The Fuzzy Systems Handbook(제 2판)에 기재된 것과 같은 퍼지 집합 소속 함수(fuzzy set membership function)에 의해 측정된다.

세부 값들에 관련된 분산의 변동 값들은 정상 데이터 트래픽을 나타내는데 반해, 상기 전송 라인상의 데이터 트래픽으로부터 유발된 세부 값들의 높고 상대적으로 일정한 분산 크기는 이상 대역폭 소모를 나타낸다. 전송 라인 데이터로부터 유발된 근사 및 세부 값들의 변동은 실질적으로 동일한 시간 간격 동안에 수신 랑니상에서 측정된 데이터로부터 유발된 근사 및 세부 값들의 변동과 일반적으로 양의 상관(positively correlate)된다.

전송 및 수신 라인들에 대한 근사 및 세부 값들의 변동들의 상관에 있어서, 전송 및 수신 데이터가 동일한 시간 동안에 측정될 필요는 없다. 근사 및 세부 값들은 평활 값들이기 때문에, 데이터가 동시에 측정되지 않았더라도 상관을 검출할 수 있다. 그러나, 전송 및 수신 라인들에 대한 데이터 계수 값 샘플들은 정상 네트워크 트래픽 움직임 동안에 이런 평활 값들에서 상관을 검출하기 위해 서로 충분히 근접한 시간에 샘플링되어야 한다.

블록(142) 후에, 블록(143)은 프로세서 회로(69)에게 서비스거부사건 계수값이 서비스거부임계값(DoSThreshold) 이상인지 여부를 결정하도록 지시하고, 만약 그렇다면, 블록(145)이 프로세서 회로에게 플래그 혹은 신호 제어 레지스터와 같은 상태 표시자를 참 혹은 활성 값으로 설정하여 서비스 거부 공격 신호가 발생하도록 지시하게 한다. 신호 제어 레지스터는 서비스 거부 공격 신호를 나타내는 디지털 신호의 상태를 제어하도록 기능하는 레지스터이거나, 혹은 프로세서 회로가 스위치 제어 회로와 같은 제어 컴퓨터 혹은 프로세서 회로에게 서비스 거부 공격 메세지를 보내도록 하는 프로세서 회로의 루틴의 호출을 초기화한다. 제어 컴퓨터는 연산자를 신호하거나 전송하거나 혹은 수신 라인들상의 데이터 흐름을 방해하거나 이용가능한 대역폭을 축소함으로써 서비스 거부 공격을 막는다.

만약 서비스거부공격계수값이 서비스거부공격임계값 미만이면, 블록(144)은 프로세서 회로(69)에게 상태 표시자를 거짓 혹은 불활성 값으로 설정하여 서비스 거부 공격 신호가 발생하지 않도록 지시한다. 임계값은 연산자에 의해 정의되거나 혹은 특정 시간 간격 동안(수초, 수분, 수시간..)에 측정된 정상 데이터 트래픽 파형들로부터 유발된 평균값에 기초한다. 예를 들면, 연산자는 근사임계값을 6.0으로, 세부 분산 임계값을 0.30으로, 그리고 서비스거부임계값을 전송 라인 대역폭 남용 검출에 대한 5사건으로 설정할 수 있다. 근사임계값 및 서비스거부임계값과 같은 모든 연산자 구성가능한 파라미터들은, 예를 들면, 호스트 컴퓨터 혹은 CPU(71) 자체에 의해 실행된 사용자 인터페이스에 의해 보내진 메세지를 통해 도 5에 도시된 CPU(71)에서 수신될 수 있다.

본 발명의 특정 실시예들이 설명되고 도시되었지만, 이러한 실시예들은 본 발명의 설명으로서만 고려되고 첨부된 청구항들에 따라 해석되는 본 발명을 한정하지 않는다.

(57) 청구의 범위

청구항 1.

데이터 통신 시스템에서 대역폭 이상들 검출 방법으로서,

제 1 시간 기간에 상기 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 단계와;

상기 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값을 생성하는 단계와; 그리고

상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 2.

제 1항에 있어서,

상기 서비스 거부 공격 신호를 생성하는 단계는 상기 상관 값이 기준 값보다 작을 때 상기 서비스 거부 공격 신호를 생성하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 3.

제 2항에 있어서,

상기 서비스 거부 공격 신호를 생성하는 단계는 상기 상관 값이 상기 기준 값보다 작은지 여부를 결정하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 4.

제 1항에 있어서,

제 2 시간 기간에 상기 데이터 통신 시스템에서 제 2 방향의 데이터 볼륨의 시 분배를 나타내는 제 2 트래픽 파형을 수신하는 단계와; 그리고

상기 상관 값을 생성하기 위해 상기 제 2 트래픽 파형을 상기 기준 파형으로 사용하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 5.

제 1항에 있어서,

트래픽 측정값들의 제 1 세트에 응답하여 상기 제 1 트래픽 파형을 생성하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 6.

제 5항에 있어서,

상기 제 1 트래픽 파형을 생성하는 단계는 트래픽 측정값들의 상기 제 1 세트를 이산 웨이브렛 변환하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 7.

제 6항에 있어서,

트래픽 측정값들의 상기 제 1 세트를 상기 이산 웨이브렛 변환하는 단계는 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들을 사용하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 8.

제 6항에 있어서,

상기 제 1 트래픽 파형을 생성하는 단계는 상기 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분을 생성하도록 하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 9.

제 8항에 있어서,

상기 상관 값을 생성하는 단계는 상기 제 1 성분과 상기 기준 파형을 상관하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 10.

제 8항에 있어서,

상기 제 1 트래픽 파형을 생성하고 그리고 상기 제 1 트래픽 파형과 상기 기준 파형을 상관하도록 프로세서 회로를 사용하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 11.

제 1항에 있어서,

상기 제 1 트래픽 파형은 상기 제 1 방향에서 데이터 볼륨의 시 분배의 통계적 척도를 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 12.

제 5항에 있어서,

상기 제 1 방향에서 데이터를 모니터링하고 그리고 이에 응답하여 트래픽 측정값들의 상기 제 1 세트를 생성하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 13.

제 12항에 있어서,

트래픽 측정값들의 상기 제 1 세트를 생성하는 단계는 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 14.

제 13항에 있어서,

이더넷 통계 그룹의 상기 특성을 나타내는 상기 값들을 수신하도록 통신 인터페이스와 통신하기 위해 프로세서 회로가 상기 제 1 트래픽 파형을 생성하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 15.

제 12항에 있어서,

상기 제 1 방향에서 상기 데이터를 모니터링하는 단계는 상기 제 1 방향에서 패킷들을 계수하는 단계 및 옥텟들을 계수하는 단계 중 적어도 한 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 16.

제 15항에 있어서,

트래픽 측정값들의 상기 제 1 세트를 나타내는 값들을 수신하도록 패킷 계수기 및 옥텟 계수기 중 적어도 하나와 통신하기 위해 프로세서 회로가 상기 제 1 트래픽 파형을 생성하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 17.

제 16항에 있어서,

상기 프로세서 회로가 상기 패킷 계수기 및 상기 옥텟 계수기 중 적어도 하나를 구현하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 18.

제 12항에 있어서,

상기 제 1 방향에서 상기 데이터를 수동적으로 모니터링하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 19.

데이터 통신 방법으로서,

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 단계와;

제 12항의 상기 데이터 통신 시스템 방법과; 그리고

상기 서비스 거부 신호에 응답하여 연산자를 신호하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 방법.

청구항 20.

데이터 통신 방법으로서,

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 단계와;

제 12항의 상기 데이터 통신 시스템 방법과; 그리고

상기 서비스 거부 신호에 응답하여 상기 데이터 통신 시스템으로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 방법.

청구항 21.

제 4항에 있어서,

트래픽 측정값들의 제 1 및 제 2 세트들에 응답하여 상기 데이터 통신 시스템상의 상기 제 1 및 제 2 방향에서의 트래픽을 각각 나타내는 상기 제 1 및 제 2 트래픽 파형을 생성하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 22.

제 21항에 있어서,

상기 제 1 및 제 2 트래픽 파형들은 상기 데이터 통신 시스템의 제 1 및 제 2 방향들에서 데이터 볼륨의 제 1 및 제 2 시분배의 제 1 및 제 2 통계적 척도들을 각각 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 23.

제 21항에 있어서,

상기 제 1 및 제 2 트래픽 파형들을 생성하는 단계는 트래픽 측정값들의 상기 제 1 및 제 2 세트들 각각을 이산 웨이브렛 변환하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 24.

제 23항에 있어서,

트래픽 측정값들의 상기 제 1 및 제 2 세트들을 상기 이산 웨이브렛 변환하는 단계는 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들을 사용하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 25.

제 23항에 있어서,

상기 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분과 상기 제 2 트래픽 파형을 나타내는 제 2 성분을 생성하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 26.

제 25항에 있어서,

상기 상관 값을 생성하는 단계는 상기 제 1 및 제 2 성분들을 상관하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 27.

제 25항에 있어서,

상기 상관 값을 생성하는데 사용되는 프로세서 회로에 트래픽 파형 생성기를 구현하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 28.

제 21항에 있어서,

상기 제 1 및 제 2 방향에서 데이터를 모니터링하는 단계와; 그리고

이에 응답하여 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 각각 생성하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 29.

제 28항에 있어서,

트래픽 측정값들의 상기 제 1 및 제 2 세트들을 생성하는 단계는 상기 제 1 및 제 2 방향에 대해 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 각각 나타내는 값들을 생성하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 30.

제 29항에 있어서,

이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하도록 통신 인터페이스와 통신하기 위해 프로세서 회로가 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 31.

제 28항에 있어서,

상기 데이터를 모니터링하는 단계는 상기 제 1 및 제 2 방향 각각에서 패킷 계수기들 및 옥텟 계수기들 중 적어도 하나를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 32.

제 28항에 있어서,

트래픽 측정값들의 상기 제 1 및 제 2 세트들을 나타내는 값들을 수신하도록 패킷 계수기와 옥텟 계수기 중 적어도 하나와 통신하기 위해 프로세서 회로가 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 33.

제 32항에 있어서,

상기 프로세서 회로가 상기 패킷 계수기 및 상기 옥텟 계수기 중 적어도 하나를 구현하도록 하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 34.

제 28항에 있어서,

상기 제 1 및 제 2 방향에서 상기 데이터를 수동적으로 모니터링하는 단계를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 방법.

청구항 35.

데이터 통신 방법으로서,

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 단계와;

제 1항의 상기 데이터 통신 방법과; 그리고

상기 서비스 거부 신호에 응답하여 연산자를 신호하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 방법.

청구항 36.

데이터 통신 방법으로서,

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 단계와;

제 1항의 상기 데이터 통신 방법과; 그리고

상기 서비스 거부 신호에 응답하여 상기 데이터 통신 시스템으로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 단계를 포함하는 것을 특징으로 하는 데이터 통신 방법.

청구항 37.

데이터 통신 시스템에서 대역폭 이상들 검출 장치로서,

제 1 시간 기간에 상기 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 수단과;

상기 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값을 생성하는 수단과; 그리고

상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 수단을 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 38.

데이터 통신 시스템에서 대역폭 이상들을 검출하도록 프로세서 회로에 지시하는 코드들이 인코딩된 컴퓨터 판독 가능 매체로서, 상기 대역폭 이상들의 검출은:

제 1 시간 기간에 상기 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 단계와;

상기 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값을 생성하는 단계와; 그리고

상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 판독 가능 매체.

청구항 39.

데이터 통신 시스템에서 대역폭 이상들을 검출하도록 프로세서 회로에 지시하는 코드들이 인코딩된 컴퓨터 판독 가능 신호로서, 상기 대역폭 이상들의 검출은:

제 1 시간 기간에 상기 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하는 단계와;

상기 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값을 생성하는 단계와; 그리고

상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하는 단계를 포함하는 것을 특징으로 하는 컴퓨터 판독 가능 매체.

청구항 40.

데이터 통신 시스템에서 대역폭 이상들 검출 장치로서,

제 1 시간 기간에 상기 데이터 통신 시스템에서 제 1 방향의 데이터 볼륨의 시 분배를 나타내는 제 1 트래픽 파형을 수신하고;

상기 제 1 트래픽 파형과 기준 파형 사이의 상관관계를 나타내는 상관 값을 생성하고; 그리고

상기 상관 값이 기준을 만족하면 서비스 거부 공격 신호를 생성하도록 구성된 프로세서 회로를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 41.

제 40항에 있어서,

상기 프로세서 회로는 상기 상관 값이 기준 값보다 작으면 상기 서비스 거부 공격 신호를 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 42.

제 41항에 있어서,

상기 프로세서 회로는 상기 상관 값이 상기 기준 값보다 작은지 여부를 결정하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 43.

제 40항에 있어서,

상기 프로세서 회로는 제 2 시간 기간에 상기 데이터 통신 시스템상의 제 2 방향에서 데이터 볼륨의 시 분배를 나타내는 제 2 트래픽 파형을 수신하고; 그리고

상기 상관 값을 생성하기 위해 상기 제 2 트래픽 파형을 상기 기준 파형으로 사용하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 44.

제 40항에 있어서,

트래픽 측정값들의 제 1 세트를 수신하고 이에 응답하여 상기 제 1 트래픽 파형을 생성하는 제 1 트래픽 파형 생성기를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 45.

제 44항에 있어서,

상기 제 1 트래픽 파형 생성기는 트래픽 측정값들의 상기 제 1 세트를 이산 웨이브렛 변환 함으로써 상기 제 1 트래픽 파형을 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 46.

제 45항에 있어서,

상기 제 1 트래픽 파형 생성기는 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들을 사용하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 47.

제 45항에 있어서,

상기 제 1 트래픽 파형 생성기는 상기 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분을 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 48.

제 47항에 있어서,

상기 프로세서 회로는 상기 제 1 성분과 상기 기준 파형의 상관함으로써 상기 상관 값을 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 49.

제 44항에 있어서,

상기 프로세서 회로는 상기 제 1 트래픽 파형 생성기를 구현하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 50.

제 40항에 있어서,

상기 제 1 트래픽 파형은 상기 제 1 방향에서 데이터 볼륨의 시 분배의 통계적 척도를 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 51.

제 44항에 있어서,

상기 제 1 방향에서 데이터를 모니터하고 이에 응답하여 트래픽 측정값들의 상기 제 1 세트를 생성하는 통신 인터페이스를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 52.

제 51항에 있어서,

상기 통신 인터페이스는 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 53.

제 52항에 있어서,

상기 프로세서 회로는 이더넷 통계 그룹의 특성을 나타내는 상기 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되며,

상기 값들은 트래픽 측정값들의 상기 제 1 세트를 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 54.

제 51항에 있어서,

상기 통신 인터페이스는 상기 제 1 방향에서 데이터의 패킷들 및 옥텟들 각각을 계수하는 패킷 계수기와 옥텟 계수기 중 적어도 하나를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 55.

제 54항에 있어서,

상기 프로세서 회로는 상기 패킷 계수기와 상기 옥텟 계수기 중 적어도 하나에 의해 생성된 값들을 수신하도록 상기 통신 인터페이스와 통신하도록 구성되며,

상기 값들은 트래픽 측정값들의 상기 제 1 세트를 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 56.

제 55항에 있어서,

상기 프로세서 회로는 상기 통신 인터페이스를 구현하도록 구성되는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 57.

제 51항에 있어서,

상기 제 1 방향에서 상기 데이터를 수동적으로 모니터하고 그리고 상기 제 1 방향에서 상기 데이터의 사본을 상기 통신 인터페이스에 제공하는 수동 모니터를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 58.

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 데이터 통신 장치로서,

제 51항의 상기 장치와; 그리고

상기 서비스 거부 신호에 응답하여 연산자를 신호하는 신호 디바이스를 포함하는 것을 특징으로 하는 데이터 통신 장치.

청구항 59.

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 데이터 통신 장치로서,

제 51항의 상기 장치와; 그리고

상기 서비스 거부 신호에 응답하여 상기 데이터 통신 시스템으로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 통신 제어 디바이스를 포함하는 것을 특징으로 하는 데이터 통신 장치

청구항 60.

제 43항에 있어서,

트래픽 측정값들의 상기 제 1 및 제 2 세트들을 수신하고 이에 응답하여 상기 제 1 및 제 2 트래픽 파형을 생성하는 트래픽 파형 생성기를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 61.

제 60항에 있어서,

상기 제 1 및 제 2 트래픽 파형들은 상기 데이터 통신 시스템에서 상기 제 1 및 제 2 방향에서 데이터 볼륨의 제 1 및 제 2 시 분배의 제 1 및 제 2 통계적 척도들을 각각 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 62.

제 60항에 있어서,

상기 트래픽 파형 생성기는 트래픽 측정값들의 상기 제 1 및 제 2 세트들 각각을 이산 웨이브렛 변환함으로써 상기 제 1 및 제 2 트래픽 파형들을 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 63.

제 62항에 있어서,

상기 트래픽 파형 생성기는 상기 이산 웨이브렛 변환에서 Haar 웨이브렛 필터 계수들을 사용하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 64.

제 62항에 있어서,

상기 트래픽 파형 생성기는 상기 이산 웨이브렛 변환에 의해 상기 제 1 트래픽 파형을 나타내는 제 1 성분과 상기 제 2 트래픽 파형을 나타내는 제 2 성분을 생성하도록 구성되는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 65.

제 64항에 있어서,

상기 프로세서 회로는 상기 제 1 및 제 2 성분들을 상관함으로써 상기 상관 값을 생성하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 66.

제 64항에 있어서,

상기 프로세서 회로는 상기 트래픽 파형 생성기를 구현하도록 구성된 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 67.

상기 60항에 있어서,

상기 제 1 및 제 2 방향에서 데이터를 모니터하고 이에 응답하여 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 각각 생성하는 통신 인터페이스를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 68.

제 67항에 있어서,

상기 통신 인터페이스는 상기 제 1 및 제 2 방향 각각에 대해 원격 모니터링 프로토콜에서 이더넷 통계 그룹의 특성을 나타내는 값들을 생성하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 69.

제 68항에 있어서,

상기 프로세서 회로는 상기 제 1 및 제 2 방향 각각에 대해 이더넷 특성 그룹의 특성을 나타내는 상기 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되고,

상기 값들은 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 각각 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 70.

제 67항에 있어서,

상기 통신 인터페이스는 상기 제 1 및 제 2 방향 각각에 대해 데이터의 패킷들 및 옥텟들 각각을 계수하는 패킷 계수기와 옥텟 계수기 중 적어도 하나를 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 71.

제 67항에 있어서,

상기 프로세서 회로는 상기 패킷 계수기와 상기 옥텟 계수기 중 적어도 하나에 의해 생성된 값들을 수신하기 위해 상기 통신 인터페이스와 통신하도록 구성되고,

상기 값들은 트래픽 측정값들의 상기 제 1 및 제 2 세트들을 나타내는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 72.

제 67항에 있어서,

상기 프로세서 회로는 상기 통신 인터페이스를 구현하도록 구성되는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 73.

제 67항에 있어서,

상기 제 1 및 제 2 방향에서 상기 데이터를 수동적으로 모니터하고 그리고 상기 데이터의 사본을 상기 통신 인터페이스에 제공하는 수동 모니터를 더 포함하는 것을 특징으로 하는 데이터 통신 시스템에서 대역폭 이상들 검출 장치.

청구항 74.

데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 데이터 통신 장치로서,

제 40항의 상기 장치와; 그리고

상기 서비스 거부 공격 신호에 응답하여 연산자를 신호하는 신호 디바이스를 포함하는 것을 특징으로 하는 데이터 통신 장치.

청구항 75.

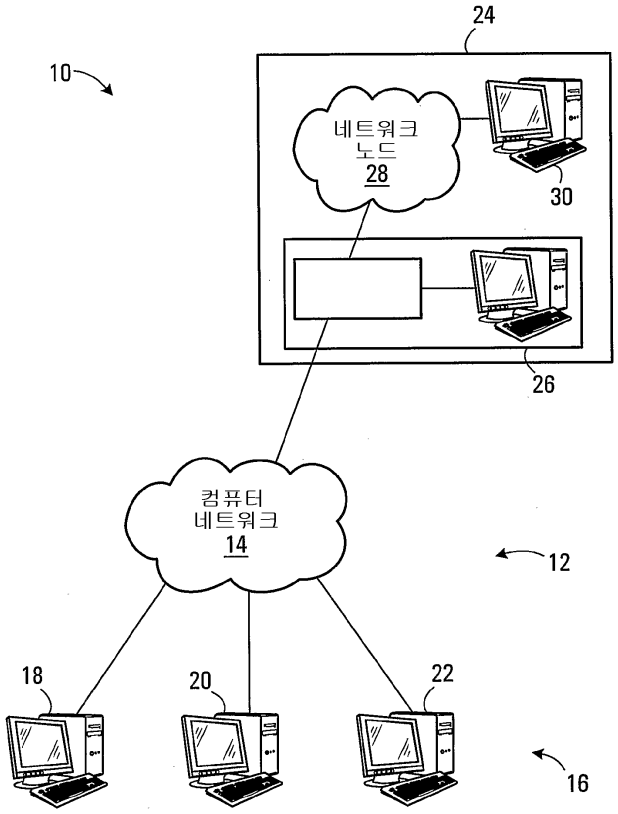
데이터 통신 시스템으로부터 데이터를 전송 및 수신하는 데이터 통신 장치로서,

제 40항의 상기 장치와; 그리고

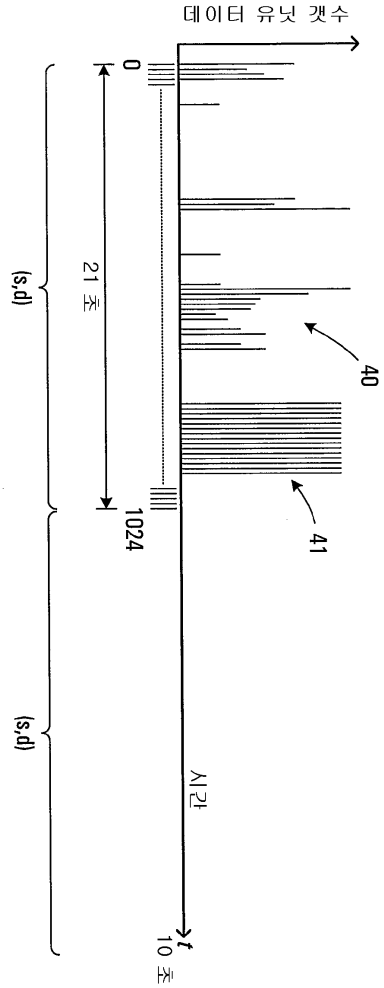
상기 서비스 거부 공격 신호에 응답하여 상기 데이터 통신 시스템으로부터 데이터의 전송 및 수신 중 적어도 하나를 제어하는 통신 제어 디바이스를 포함하는 것을 특징으로 하는 데이터 통신 장치.

도면

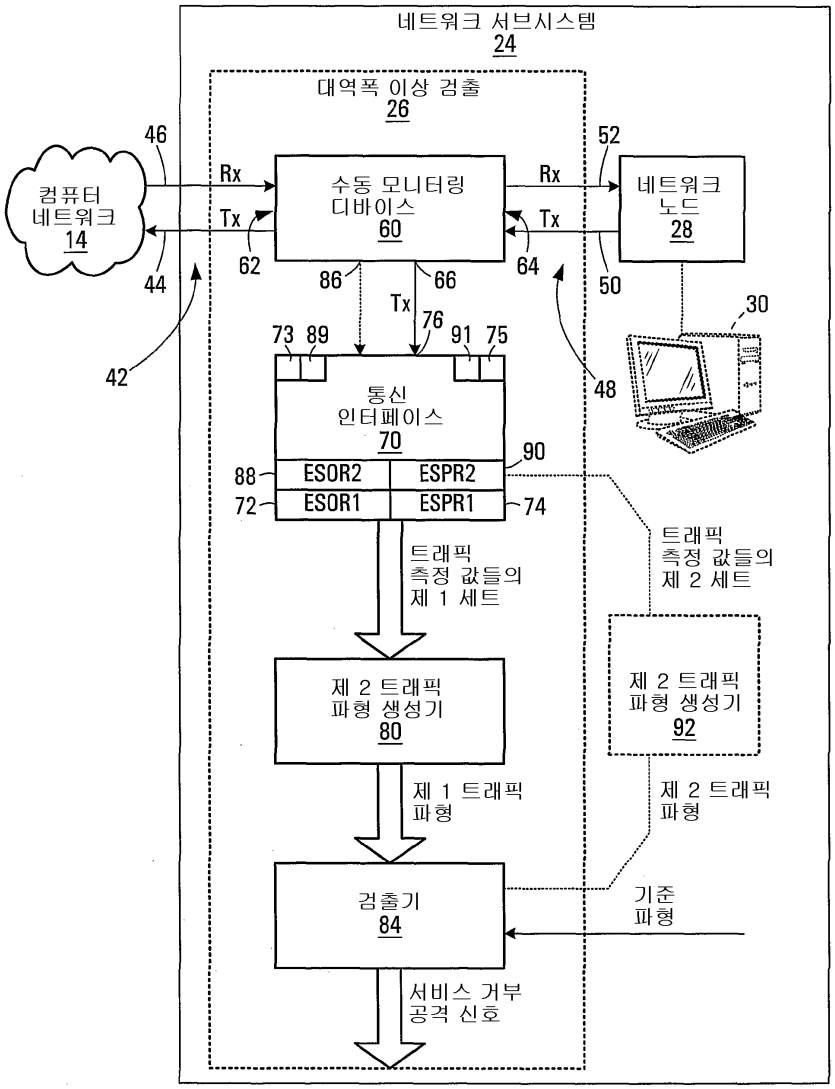
도면1



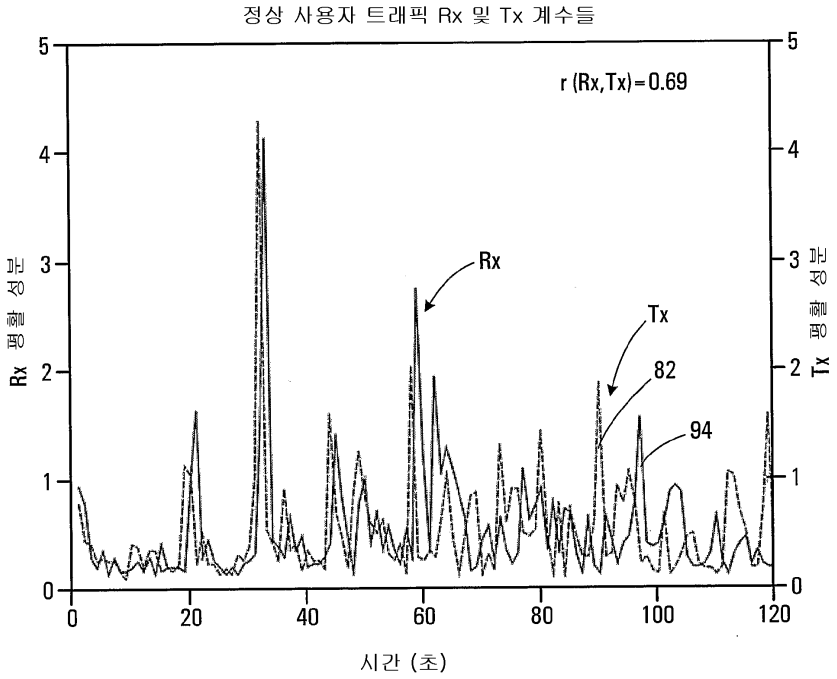
도면2



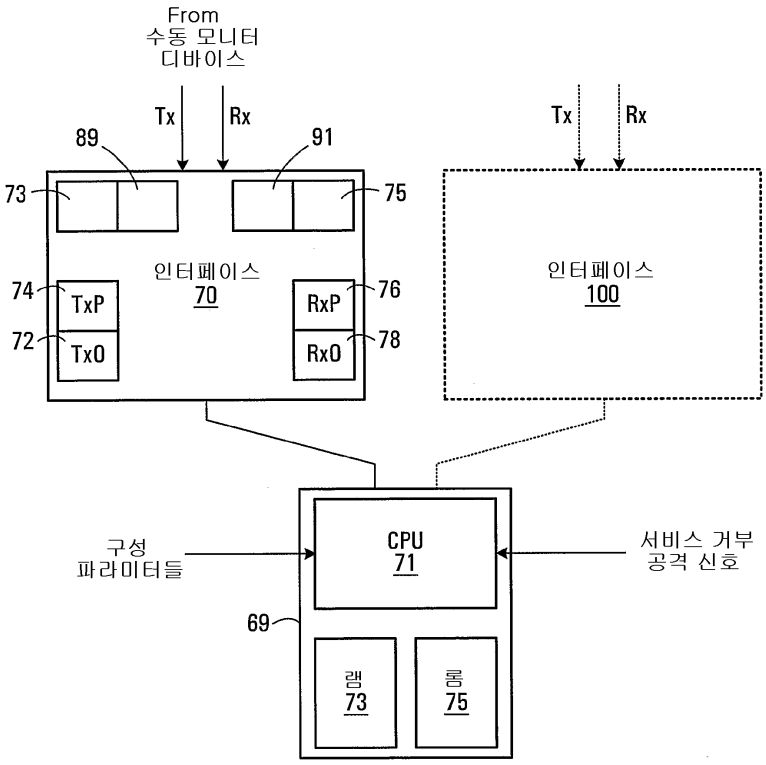
도면3


네트워크 서브시스템
24
대역폭 이상 검출
26
46
52
컴퓨터
네트워크
14
Rx
Tx
수동 모니터링
디바이스
60
Rx
Tx
네트워크
노드
28
62
64
44
50
86
66
Tx
76
30
73
89
91
75
42
48
통신
인터페이스
70
90
88
ESOR2
ESPR2
72
ESOR1
ESPR1
74
트래픽
측정 값들의
제 1 세트
트래픽
측정 값들의
제 2 세트
제 2 트래픽
파형 생성기
80
제 2 트래픽
파형 생성기
92
제 1 트래픽
파형
제 2 트래픽
파형
검출기
84
기준
파형
서비스 거부
공격 신호

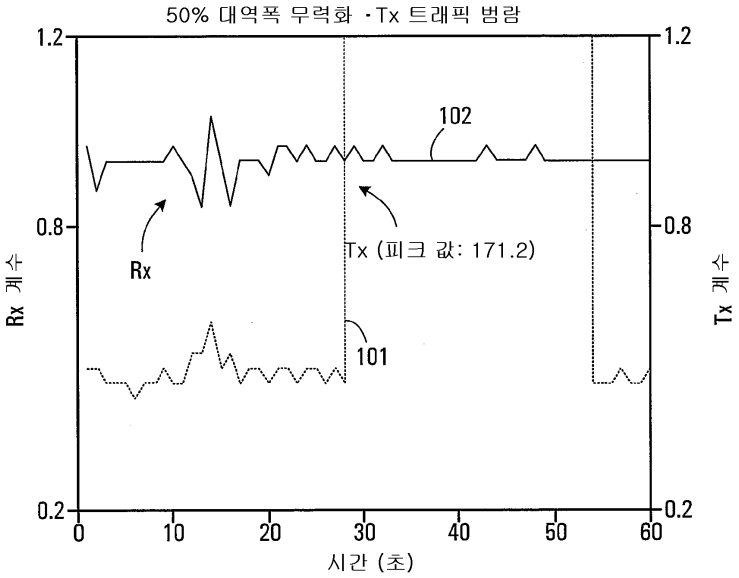
도면4


정상 사용자 트래픽 Rx 및 Tx 계수들
r (Rx,Tx)=0.69
Rx
Tx
82
94
Rx 평활 성분
Tx 평활 성분
시간 (초)
0
20
40
60
80
100
120
1
2
3
4
5

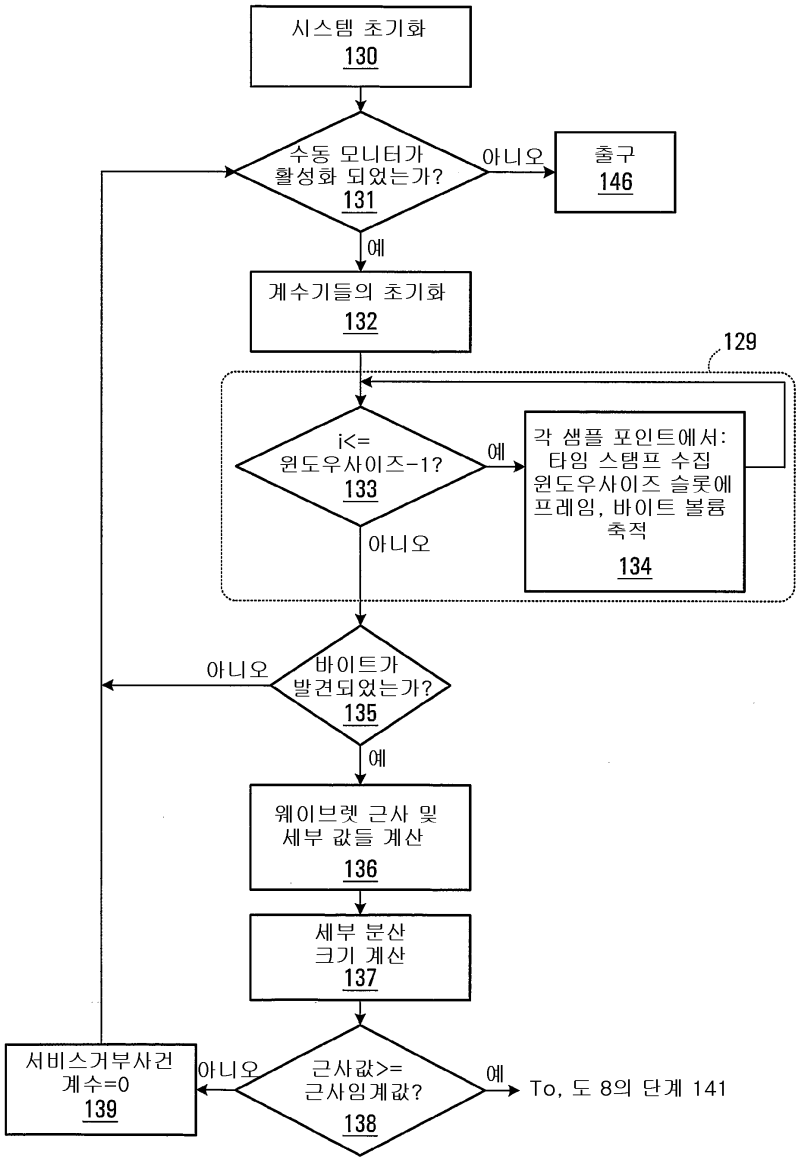
도면5


From
수동 모니터
디바이스
Tx
Rx
89
91
73
75
인터페이스
70
74
TxP
72
TxO
RxP
76
RxO
78
Tx
Rx
인터페이스
100
구성
파라미터들
CPU
71
서비스 거부
공격 신호
69
램
73
롬
75

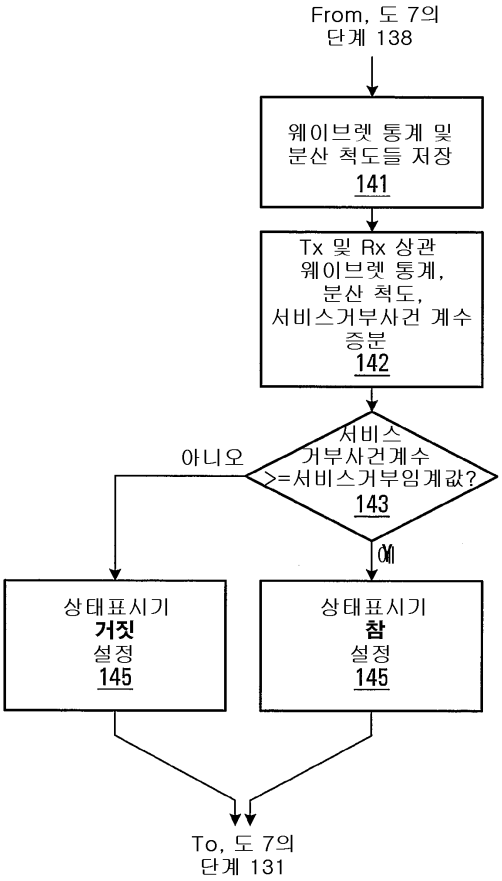
도면6


50% 대역폭 무력화 - Tx 트래픽 범람
1.2
0.8
0.2
Rx 계수
Tx 계수
102
Rx
Tx (피크 값: 171.2)
101
0
10
20
30
40
50
60
시간 (초)

도면7


시스템 초기화
130
수동 모니터가 활성화 되었는가?
131
아니오
출구
146
예
계수기들의 초기화
132
129
i<= 윈도우사이즈-1?
133
예
각 샘플 포인트에서: 타임 스탬프 수집 윈도우사이즈 슬롯에 프레임, 바이트 볼륨 축적
134
아니오
바이트가 발견되었는가?
135
아니오
예
웨이브렛 근사 및 세부 값들 계산
136
세부 분산 크기 계산
137
근사값>= 근사임계값?
138
예
To, 도 8의 단계 141
아니오
서비스거부사건 계수=0
139

도면8


From, 도 7의
단계 138
웨이브렛 통계 및
분산 척도들 저장
141
Tx 및 Rx 상관
웨이브렛 통계,
분산 척도,
서비스거부사건 계수
증분
142
서비스
거부사건계수
>=서비스거부임계값?
143
아니오
예
상태표시기
거짓
설정
145
상태표시기
참
설정
145
To, 도 7의
단계 131