(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.[8]
H04L 12/56 (2006.01)

(45) 공고일자 2006년01월31일
(11) 등록번호 10-0548154
(24) 등록일자 2006년01월24일

(21) 출원번호 10-2003-0037549
(22) 출원일자 2003년06월11일

(65) 공개번호 10-2004-0106727
(43) 공개일자 2004년12월18일

(73) 특허권자 (주)엔텔스
서울특별시 강남구 청담동 41-2 금하빌딩 15층

(72) 발명자 심재희
서울특별시광진구광장동577번지현대파크빌1012-303호

유건우
서울특별시강남구신사동518-17평화빌라102호

김상희
경기도구리시수택동대림한숲아파트103-1715호

(74) 대리인 이경란

심사관 : 신성길

(54) 유무선 통신망에서의 패킷 전송 제어 및 패킷 과금 데이터생성을 위한 방법 및 장치

요약

본 발명은 네트워크를 통해 소스 IP 주소 및 목적지 IP 주소를 포함하는 패킷 데이터를 수신하여 공유 메모리에 저장하는 패킷 데이터 입력부와, 당해 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하여, 패킷 데이터가 필터링 규칙을 만족하면 삭제(delete)하는 필터링부와, 필터링 규칙을 만족하지 않는 경우 패킷 데이터를 목적지 IP 주소로 전송하는 패킷 데이터 출력부와, 필터링 규칙을 만족하지 않는 경우 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량, 사용자 정보를 분석하는 프로토콜 분석부와, 프로토콜 분석부에 의해 분석된 정보를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 데이터 저장부를 포함하는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치에 관한 것으로서, 통신 사업자에게 필수 기능인 패킷 서비스 제어 기능과 과금 데이터 생성 기능을 하나의 장치에서 통합하여 수행할 수 있으므로 시스템 구축시 비용 절감 및 시스템 단순화가 가능하다.

대표도

도 2b

색인어

패킷, 필터링, 프로토콜, 과금, TCP

명세서

도면의 간단한 설명

도 1a는 종래 기술에 따른 유선 인터넷 환경에서의 과금 처리 방법을 나타낸 도면.

도 1b는 종래 기술에 따른 무선 인터넷 환경에서의 과금 처리 방법을 나타낸 도면.

도 2a는 본 발명의 바람직한 일 실시예에 따른 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면.

도 2b는 본 발명의 바람직한 일 실시예에 따른 패킷 서비스 장치의 블록 구성도.

도 2c는 본 발명의 바람직한 일 실시예에 따른 공유 메모리 운용에 대한 개념도.

도 3a는 본 발명의 바람직한 다른 실시예에 따른 무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면.

도 3b는 본 발명의 바람직한 또 다른 실시예에 따른 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면.

도 3c는 본 발명의 바람직한 다른 실시예에 따른 무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면.

도 4는 본 발명의 바람직한 일 실시예에 따른 패킷 서비스 장치에서 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법을 수행하는 과정을 나타낸 순서도.

도 5a는 본 발명의 바람직한 일 실시예에 따른 송신단의 TCP 상태도.

도 5b는 본 발명의 바람직한 일 실시예에 따른 수신단의 TCP 상태도.

도 5c는 본 발명의 바람직한 일 실시예에 따른 TCP 연결 흐름과 각 단계별 상태를 나타낸 도면.

도 5d는 본 발명의 바람직한 다른 실시예에 따른 동시 접속(Simultaneous-Open) 또는 동시 해제(Simultaneous-Close)의 경우 TCP 연결 흐름과 각 단계별 상태를 나타낸 도면.

<도면의 주요 부분에 대한 부호의 설명>

210 : 패킷 서비스 장치

250 : 패킷 데이터 입력부

255 : 데이터 전송 및 필터링부

260 : 프로토콜 분석부

265 : 데이터 저장 및 통계 처리부

270 : 패킷 데이터 출력부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치에 관한 것으로, 특히 하나의 장치를 이용하여 패킷 서비스 제어 및 사용자의 패킷 사용량 측정을 가능하게 하는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

과학 기술의 발전과 경제 수준의 향상은 통신 기기의 개발과 광범위한 보급을 가능하게 하였다. 또한 통신 기기의 보급은 원격지에 위치한 사용자간에 유무선 통신망을 통한 데이터의 송수신을 가능하게 하였다.

그리고, 사용자의 입장에서 이와 같은 유무선 데이터의 송수신(예를 들어, 유료 데이터 수신 등)을 위해 일정 비용의 지불을 하여야 하는 경우가 있으며, 서비스 제공자의 입장에서 서비스 이용에 대한 과금을 수행하기 위해 사용자의 사용량 데이터를 저장 및 관리할 필요가 있다. 또한, 최근에는 악의의 사용자들이 원활한 통신 서비스 수행, 웹 서버 접속 억제 등의 목적으로 해킹(hacking), 서비스 거부(DOS : Denial of Service) 공격 등을 행하는 경우가 있으므로 이에 대한 방지책(패킷 서비스 제어 등)의 수립도 요청되고 있다.

종래의 유무선 통신망에서 적용되는 패킷 서비스 제어 방법은 방화벽(Firewall)을 사용하여 소스 IP(Source IP)와 목적지 IP(Destination IP)를 비교하여 해당 패킷(Packet)의 전송 여부를 결정하는 방법이 주로 적용되고 있었다. 또한, 과금 데이터 생성을 위해 사용자의 패킷 데이터 송수신량을 측정하기 위한 방법으로 유선 인터넷에서는 가입자가 접속한 컨텐츠 서버에 저장된 해당 사용자의 사용 컨텐츠 기록(즉, 사용자 접근 로그)을 이용하는 방법이 적용되고 있었으며, 무선 인터넷의 경우에는 해당 가입자가 사용한 총 패킷량 정보를 이용하는 방법이 적용되고 있었다.

그러나, 종래의 패킷 서비스 제어 방법은 방화벽(Firewall)에서 소스 IP(Source IP) 주소와 목적지 IP(Destination IP) 주소만을 비교하여 패킷의 전송여부를 결정하는 방법이므로, 서비스 거부 (DOS : Denial of Service) 공격과 같이 IP 주소만으로 비교가 불가능한 해킹에 대처할 수 있는 방법을 제공할 수 없었다. 또한, TCP/IP 프로토콜(Protocol) 상위에 위치하는 응용 프로토콜을 기준으로 패킷의 전송여부를 결정해야 되는 상황에서도 처리할 방법을 제공하지 못하는 문제점이 있었다.

그리고, 상술한 바와 같이 종래의 과금 데이터 생성(사용량 검출) 방법의 경우, 유선 인터넷에서는 컨텐츠 서버에서 컨텐츠별 사용자 사용 로그를 저장한 후, 외부의 과금서버에서 이 사용 로그를 과금의 기본자료로 사용하는 방법이 적용되고 있었다. 그러나, 이러한 방법은 새로운 컨텐츠 서버가 신규로 생성될 때마다 외부의 과금서버는 신규 컨텐츠 서버와도 연동처리를 해야 함으로써, 신속하고 유연한 과금처리 작업 수행이 어려운 문제점이 있었다.

또한, 무선 인터넷의 경우 이루어지는 종래의 과금 데이터 생성(사용량 검출) 방법은 외부의 과금 서버가 사용자가 망에 로그인 된 후 사용한 총 패킷량 정보만을 패킷교환기에서 제공받아 과금 처리 업무를 수행하는 방법이었다. 그러나, 이러한 방법은 과금 서버가 제공받는 정보는 총 패킷량 정보로 제한되므로 각 서비스별로 다양한 과금 체계의 적용이 용이하지 않은 문제점이 있었다.

또한, 종래의 패킷 서비스 제어 기능과 과금 데이터 생성 기능은 통신 사업자의 경우 필수적인 기능이므로 각각의 기능을 수행하는 독립된 장치를 각각 다른 위치에 구비하여 사용하고 있었다. 그러나, 이는 통신 사업자에게 있어 이중의 비용 지출 및 관리 체계의 복잡성을 유발시키는 요인으로 작용되고 있었다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명의 목적은 데이터 패킷 분석을 통해 소스(Source) 및 목적지(Destination) IP 경로 추적 기능, IP 주소별/네트웍별 프로토콜 분석 기능, TCP/IP 레벨의 프로토콜 분석뿐 아니라 응용 프로토콜에서의 분석을 통한 패킷 접근제어를 통해 서비스 거부(DOS : Denial of Service) 공격과 같은 해킹 여부를 탐지하여 대처할 수 있는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

본 발명의 다른 목적은 패킷 서비스 제어 기능뿐 아니라 실시간 패킷 사용량 및 패킷 사용량 분포에 대한 실시간 모니터링 기능을 제공하며, 실시간 패킷 사용량 정보를 이용하여 통계 작업 및 네트워크 용량 산정을 가능하게 하는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

본 발명의 또 다른 목적은 사용자 단말기로부터 패킷 교환기까지는 무선 데이터 통신 구간이고, 패킷 교환기부터 컨텐츠 서버까지는 유선 데이터 통신 구간으로 분리된 경우에도, 하나의 장치를 통해 유무선 인터넷의 과금 처리를 위한 과금 기초 데이터를 생성할 수 있어 설치 및 운용의 편의성을 증진시키고 유무선 통합 환경의 단일화된 데이터 과금 솔루션을 제공할 수 있는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

본 발명의 또 다른 목적은 프로토콜 분석을 통한 컨텐츠의 내용 및 컨텐츠별 패킷량 정보를 동시에 검출할 수 있도록 하는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

본 발명의 또 다른 목적은 통신 사업자에게 필수 기능인 패킷 서비스 제어 기능과 과금 데이터 생성 기능을 하나의 장치에서 통합하여 수행할 수 있도록 하는 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치를 제공하는 것이다.

발명의 구성 및 작용

상기 목적들을 달성하기 위하여, 본 발명의 일 측면에 따르면, 패킷 서비스 장치에 있어서, 네트워크를 통해 패킷 데이터를 수신하여 공유 메모리에 저장하는 패킷 데이터 입력부-여기서, 상기 패킷 데이터는 적어도 소스 IP 주소(Source IP Address), 목적지 IP 주소(Destination IP Address)를 포함함-와, 상기 공유 메모리에 저장된 상기 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하여, 상기 패킷 데이터가 상기 필터링 규칙을 만족하면 삭제(delete)하는 필터링부와, 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 상기 목적지 IP 주소를 이용하여 전송하는 패킷 데이터 출력부와, 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량, 사용자 정보를 분석하는 프로토콜 분석부와, 상기 프로토콜 분석부에 의해 분석된 정보를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 데이터 저장부를 포함하는 것을 특징으로 하는 패킷 서비스 장치가 제공된다.

또한, 본 발명에 따른 패킷 서비스 장치는 상기 데이터 저장부에 저장된 정보를 이용하여 과금 기초 데이터를 생성하는 통계 처리부를 포함하되, 상기 과금 기초 데이터는 실시간 통계 및 분석 정보를 포함하는 것을 특징으로 할 수 있다.

또한, 본 발명에 따른 패킷 서비스 장치는 상기 패킷 데이터가 프로토콜의 특성으로 인해 단편화(fragmentation)된 경우, 상기 프로토콜 분석부에서 분석할 수 있도록 논리적으로 하나의 패킷 데이터로 재조립하는 패킷 데이터 재조립부를 더 포함할 수 있다.

그리고, 상기 프로토콜 분석부는 상기 패킷 데이터의 종류에 따라 특화된 복수개의 프로토콜 분석부로 이루어진 것을 특징으로 할 수 있다.

또한, 본 발명에 따른 패킷 서비스 장치는 송신단으로부터 수신단으로 SYN 패킷 데이터가 전송되고, 상기 수신단에서 상기 전송단으로 상기 SYN 패킷 데이터에 상응하는 ACK 패킷 데이터가 전송된 후에만 상기 수신단의 TCP 상태를 SYNRCVD 상태로 추측하는 것을 특징으로 할 수 있다.

상기 공유 메모리는 환형 큐의 형태인 경우, ReadStart 값과 NextRead 값을 동일하게 설정함으로써 쓰기 가능 영역을 최대화할 수 있는 것을 특징으로 하며, 상기 공유 메모리의 운용 알고리즘은 균형 이진 트리(Balanced-Binary-Tree) 알고리즘인 것을 특징으로 할 수 있다.

본 발명의 다른 측면에 따르면, 유무선 인터넷 서비스 시스템에 포함된 패킷 서비스 장치가 송신단으로부터 수신된 패킷 데이터를 수신단으로 전송 여부를 제어하는 방법에 있어서, 네트워크를 통해 패킷 데이터를 수신하는 단계-여기서, 상기 패킷 데이터는 적어도 소스 IP 주소(Source IP Address), 목적지 IP 주소(Destination IP Address)를 포함함-와, 상기 수신된 패킷 데이터를 공유 메모리에 저장하는 단계와, 상기 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하는 단계와, 상기 패킷 데이터가 상기 필터링 규칙을 만족하는 경우, 상기 패킷 데이터를 삭제(delete)하는 단계와, 상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 상기 목적지 IP 주소를 이용하여 전송하는 단계와, 상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량, 사용자 정보를 분석하여 과금 기초 데이터를 생성하는 단계와, 상기 과금 기초 데이터를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 단계와, 과금 수행 장치로부터 상기 과금 기초 데이터의 제공 요청이 수신되는 경우, 상기 과금 기초 데이터를 네트워크를 통해 상기 과금 수행 장치로 전송하는 단계를 포함하는 것을 특징으로 하는 패킷 서비스 제어 방법이 제공되고, 당해 패킷 서비스 제어 방법의 수행을 가능하게 하는 시스템, 장치 및 기록매체가 제공된다.

본 발명에 따른 패킷 서비스 제어 방법에서 상기 패킷 서비스 장치는 송신단으로부터 수신단으로 SYN 패킷 데이터가 전송되고, 상기 수신단에서 상기 전송단으로 상기 SYN 패킷 데이터에 상응하는 ACK 패킷 데이터가 전송된 후에만 상기 수신단의 TCP 상태를 SYNRCVD 상태로 추측하는 것을 특징으로 할 수 있다.

또한, 본 발명에 따른 패킷 서비스 제어 방법에서 적용되는 상기 필터링 규칙은 상기 패킷 데이터에 상응하는 소스 IP 주소(Source IP Address) 및 목적지 IP 주소(Destination IP Address)가 필터링되어야 할 IP 주소로서 이미 등록된 IP 주소와 일치하는지 여부, 상기 패킷 데이터에 오류가 존재하는지 여부, 상기 패킷 데이터가 해킹 의도를 포함하고 있는지 여부, 바이러스(Virus)에 감염된 패킷 데이터인지 여부 중 적어도 어느 하나를 검사하기 위한 것일 수 있다.

또한, 본 발명에 따른 패킷 서비스 제어 방법은 상기 패킷 데이터가 프로토콜의 특성으로 인해 단편화(fragmentation)된 경우, 상기 프로토콜 분석부에서 분석할 수 있도록 논리적으로 하나의 패킷 데이터로 재조립하는 단계를 더 포함할 수 있다.

도 1a는 종래 기술에 따른 유선 인터넷 환경에서의 과금 처리 방법을 나타낸 도면이고, 도 1b는 종래 기술에 따른 무선 인터넷 환경에서의 과금 처리 방법을 나타낸 도면이다.

도 1a를 참조하면, 사용자 단말기(110)와 하나 이상의 컨텐츠 서버(120a, 120b, 120c, ..., 120n - 120으로 통칭함)는 네트워크를 통해 결합되어 있다.

사용자 단말기(110)는 이동 통신 단말기, 개인 휴대 단말기(PDA : Personal Digital Assistant), 노트북 컴퓨터 등과 같이 네트워크를 통해 컨텐츠 서버(120)에 접속할 수 있는 장치이면 아무런 제한없이 적용 가능하다.

도 1에 도시된 바와 같이, 유선 인터넷 환경에서 사용자가 임의의 컨텐츠 서버(120)에서 제공하는 유료 컨텐츠를 이용하기 위하여 사용자 단말기(110)를 이용하여 당해 컨텐츠 서버(120)에 네트워크를 통해 접속을 시도한다.

이후, 해당 사용자가 당해 컨텐츠 서버(120)에서 제공하는 유료 컨텐츠를 이용한 경우, 컨텐츠 서버(120)는 해당 사용자의 유료 컨텐츠 이용 정보를 사용자 접근 로그에 기록하여 관리한다.

이후, 통신 사업자(즉, 유선 인터넷 접속 서비스 제공자)가 미리 지정된 시점에서 해당 사용자에 상응하여 과금을 수행하고자 하는 경우, 유선 인터넷 접속 서비스 시스템에 포함된 접근 로그 수집 장치(130)는 네트워크를 통해 결합된 하나 이상의 컨텐츠 서버(120)로부터 사용자 접근 로그를 수집한다.

이 경우, 각각의 컨텐츠 서버(120)에서 관리하는 사용자 접근 로그의 포맷이 상이한 경우에는 표준 형식의 사용자 접근 로그로 변경을 수행하여 해당 사용자의 유료 컨텐츠 이용에 대한 과금을 수행한다.

그러나, 이와 같은 종래의 과금 처리 방법은 네트워크를 통해 결합된 컨텐츠 서버(120)의 수가 많은 경우, 접근 로그 수집 장치가 다수의 컨텐츠 서버(120)에 접속하여야 하고, 또한 각 컨텐츠 서버(120)별로 접속 방식이 상이할 수 있으므로 다양한 인터페이스 방법을 구비하여야 하는 문제점이 있었다.

도 1b에는 종래 기술에 따른 무선 인터넷 환경에서의 과금 처리 방법이 도시되어 있다.

도 1b를 참조하면, 무선 인터넷 서비스를 이용할 수 있는 사용자 단말기(110)와 하나 이상의 컨텐츠 서버(120a, 120b, 120c, ..., 120n - 120으로 통칭함)는 네트워크를 통해 결합되어 있다.

무선 인터넷 환경에서 사용자가 무선 인터넷 서비스를 이용하고자 하는 경우, 우선 사용자 단말기(110)는 무선통신 장비(140)를 경유하여 패킷 교환기(150)에 접속된다. 무선통신망의 데이터 패킷을 유선 인터넷 패킷으로 변환해서 네트워크(인터넷망)를 통해 컨텐츠 서버(120)에 접속할 수 있도록 하는 패킷 교환기(150)에는 WCDMA 환경인 경우 게이트웨이 지피알에스 서포트 노드(GGSN : Gateway GPRS Support Node), 서빙 지에스엠 서포트 노드(SGSN : Serving GSM Support Node) 등이, 무선 랜 환경인 경우 억세스 포인트(AP : Access Point) 등이 포함될 수 있다.

또한, 패킷 교환기(150)가 무선통신망의 데이터 패킷을 유선 인터넷 패킷으로 변환해서 네트워크(인터넷망)를 통해 컨텐츠 서버(120)에 접속할 수 있도록 하기 위하여 패킷 변환을 수행하는 과정에서, 각 사용자별로 패킷 사용량을 주기적으로 과금 로그 수집장치(160)(예를 들어, AAA 장치)로 전송하게 된다.

그리고, 통신 사업자는 무선 데이터 통신에 대한 과금처리를 할 경우, 과금 로그 수집장치(160)에 저장된 사용자별 패킷 사용량을 이용하여 과금을 수행하게 된다. 이 경우 패킷 사용량에 비례하는 단순화된 과금정책만을 수행할 수 있을 뿐, 다양한 서비스별 과금정책을 수행할 수 없는 한계를 가지게 된다.

도 2a는 본 발명의 바람직한 일 실시예에 따른 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면이고, 도 2b는 본 발명의 바람직한 일 실시예에 따른 패킷 서비스 장치의 블록 구성도이며, 도 2c는 본 발명의 바람직한 일 실시예에 따른 공유 메모리 운용에 대한 개념도이다.

도 2a를 참조하면, 본 발명에 따른 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성은 사용자 단말기(110), 유선 인터넷 서비스 시스템, 패킷 서비스 장치(210), 하나 이상의 컨텐츠 서버(120a, 120b, 120c, ..., 120n - 이하 120으로 통칭함)를 포함한다. 다만, 유선 인터넷 서비스 시스템은 본 발명의 요지와 다소 관련성이 떨어지는 사항이므로, 유선 인터넷 서비스를 가능하게 하는 일종의 네트워크로 표시하기로 하며, 패킷 서비스 장치(210)는 유선 인터넷 서비스 시스템에 포함된 하나의 장치일 수 있다. 그리고, 사용자 단말기(110), 패킷 서비스 장치(210), 컨텐츠 서버(120)는 네트워크를 통해 상호 결합된다.

도 2a에 도시된 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 참조할 때, 사용자 단말기(110)와 컨텐츠 서버(120)간에 송수신되는 모든 패킷 데이터는 패킷 서비스 장치(210)를 경유함을 알 수 있다.

즉, 본 발명에 따른 패킷 서비스 장치(210)가 사용자 단말기(110)와 컨텐츠 서버(120)간에 송수신되는 패킷 데이터의 특성을 분석할 수 있다면, 해당 패킷 데이터를 사용자 단말기(110) 또는 컨텐츠 서버(120)로 전송할 것인지 여부, 해당 패킷 데이터의 송수신과 관련한 과금 데이터 생성이 가능함을 쉽게 이해할 수 있을 것이다. 따라서, 상술한 기능을 수행할 수 있는 본 발명에 따른 패킷 서비스 장치(210)를 이용하면, 통신 사업자는 종래의 유선 인터넷 환경에서 반드시 필요시 되던 과금로그 수집장비(도 1a의 130 또는 도 1b의 160)를 구비할 필요가 없게 된다.

또한, 패킷 서비스 장치(210)는 송수신되는 패킷에 관련된 정보(예를 들어, 패킷의 근원지, 패킷의 개수, 패킷의 분포 및 통계, 패킷의 내용 등)를 분석할 수 있으므로, 단순히 소스 IP(source IP), 목적지 IP(destination IP)만을 조회해서 패킷의 전송여부를 결정하는 기존의 방화벽(firewall)과는 달리 보다 효과적으로 당해 패킷 데이터의 외부 전송 여부를 결정할 수 있다. 결과적으로, 만일 당해 패킷이 송신 거부로 결정된 패킷이라면 전송 거부를 통해 효율적인 패킷 데이터 관리(Intelligent Packet Flow Management)가 가능하게 된다.

그리고, 본 발명에 따른 패킷 서비스 장치(210)가 다양한 요소(예를 들어, 응용 프로토콜의 특정 항목의 값이 필터링 규칙에 등록된 값으로 설정되어 있는지 여부, 특정 소스 IP(Source IP)에서 하나의 목적지(Destination)로 동일한 패킷이 전송되는 회수가 임계치로 설정한 횟수를 넘는지 여부 등)를 이용하여 해당 패킷 데이터의 전송 여부를 판단하므로, 서비스 거부(DOS : Denial of Service) 공격 등의 경우에도 네트워크를 안정적으로 운영할 수 있다.

또한, 본 발명에 따른 패킷 서비스 장치(210)는 네트워크 모니터링을 위해 네트워크를 통해 송수신되는 패킷 데이터의 크기별, 송수신 패킷 데이터의 개수별, 프로토콜별 현황 자료 등을 실시간으로 제공할 수 있다.

또한, 도 2a에는 하나의 패킷 서비스 장치(210)만이 존재하는 것처럼 도시되었으나, 실제로는 로드 밸런싱(Load Balancing), 대량의 처리 능력 등의 목적을 위해 다수의 패킷 서비스 장치(210)를 포함하는 패킷 서비스 장치 그룹으로 구성할 수도 있다. 이와 같이, 유선 인터넷 서비스 시스템에 패킷 서비스 장치 그룹이 포함되는 경우에는 패킷 서비스 장치(210) 상호간에 정상적으로 동작하는지 여부를 검사하도록 하여, 정상적으로 동작하는 패킷 서비스 장치(210)에서만 패킷 데이터를 전송하도록 하여 전체 시스템의 운용 효율성을 증진시킬 수 있다.

본 발명에 따른 패킷 서비스 장치(210)의 기능을 간략히 설명하면 다음과 같다.

먼저, 사용자의 조작에 의해 사용자 단말기(110)가 유선 인터넷에 접속하는 경우, 사용자 단말기(110)로부터 전송되는 모든 패킷 데이터는 패킷 서비스 장치(210)를 통해 목적지 주소로 전송된다. 이 과정에서 패킷 서비스 장치(210)는 사용자 단말기(110)로부터 수신된 패킷 데이터의 소스 IP(Source IP) 정보를 이용하여 해당 사용자가 누구인지를 인지한 후, 발신자 포트 정보를 이용하여 IP, TCP, UDP 프로토콜에서 나누어진 패킷을 재조합한 후 응용 프로토콜로 분석하여 각종 네트워크 정보, 해당 컨텐츠의 내용 및 패킷의 총량을 알아낼 수 있다. 또한, 상술한 정보를 주기적으로 패킷 서비스 장치(210) 내부에 저장함으로써 서비스별, 서버별, 사용자별 통계자료 또는 당해 사용자에 대한 과금 기초 자료로 사용할 수 있도록 한다.

이하, 도 2b를 참조하여 본 발명에 따른 패킷 서비스 장치(210)에 대해 설명하기로 한다.

도 2를 참조하면, 본 발명에 따른 패킷 서비스 장치(210)는 패킷 데이터 입력부(250), 데이터 전송 및 필터링부(255), 프로토콜 분석부(260), 데이터 저장 및 통계 처리부(265), 패킷 데이터 출력부(270)를 포함한다.

패킷 데이터 입력부(250)는 사용자 단말기(110)로부터 네트워크를 통해 패킷 데이터를 수신하여 데이터 전송 및 필터링부(255)로 전송하는 기능을 수행한다. 즉, 패킷 데이터 입력부(250)는 패킷 서비스 장치(210)가 운용되는 플랫폼에 따라 NIC(Network Interface Card)가 소켓(Socket), DLPI(Data Link Provider Interface) 또는 패킷 서비스 장치를 위한 전용 프로토콜 디바이스 드라이버 등의 방법으로 패킷 데이터를 수신한 후, 수신된 패킷 데이터를 데이터 전송 및 필터링부(255)로 전달하는 기능을 수행한다. 특히, 본 발명에 따른 패킷 서비스 장치 전용의 프로토콜 디바이스 드라이버는 수신된 패킷 데이터를 OS의 커널 영역(Kernel Area)으로부터 데이터 전송 및 필터링부(255)를 위한 공유 메모리 등에 직접 복사를 하므로, 다른 방식의 패킷 수신 방법보다 월등한 성능을 가지게 된다. 그리고, 당해 패킷 데이터들은 커널의 기능을 이용하여 사용자 메모리로 직접 복사하여 후속 처리를 하게 하거나, 커널 영역과 사용자 영역에서 동시에 접근할 수 있는 공유메모리를 통해 직접 패킷 데이터를 기록하여 후속 처리를 하게 된다.

일반적으로 공유 메모리란 일반 운영체계에서 사용하는 읽기 및/또는 쓰기 방식에 의한 것보다 프로그램 프로세스들이 데이터를 더 빠르게 교환할 수 있도록 하는 방법에 관한 것을 의미한다. 예를 들어, 클라이언트 프로세서가 전달한 데이터를 서버 프로세스가 수정 후 다시 클라이언트에게 되돌려주는 경우를 설명하면 다음과 같다.

클라이언트가 운영 체계의 버퍼를 사용하여 출력 파일에 기록하면, 서버는 버퍼로부터 그 파일을 자신의 작업 공간 내로 읽어들이며, 이때 공유 메모리의 지정된 공간을 사용하면, 시스템 서비스를 사용하지 않고서도 데이터가 양쪽 프로세스에 의해 직접 액세스될 수 있도록 할 수 있다.

데이터를 공유 메모리에 집어넣기 위해, 클라이언트는 세마포어 값을 확인한 후에 공유 메모리에 액세스하여 데이터를 기록하며, 그 후 대기하고 있는 데이터가 있다는 사실을 서버에게 알려주기 위해 세마포어 값을 재설정한다. 서버는 공유 메모리에 입력 데이터가 있는지를 알기 위하여 세마포어 값을 주기적으로 확인하게 된다. 차례대로, 서버 프로세스는 공유 메모리 공간에 데이터를 다시 기록하고, 세마포어를 사용하여 데이터가 읽혀질 준비가 되었다는 사실을 클라이언트에게 알리게 된다.

이하, 도 2c에 도시된 공유 메모리 운용에 관한 개념도를 이용하여 본 발명에 따른 패킷 서비스 장치(210)의 성능 향상 방법에 대해 설명한다.

상술한 바와 같이, 본 발명에 따른 패킷 서비스 장치(210)의 각 요소들(components)은 공유 메모리를 통해 서로 통신을 하게 되며, 대부분의 경우 데이터 오염 방지, 데드락 방지 등을 위해 세마포어, 뮤텍스 등과 같은 OS에서 제공되는 락(Lock)과 관련된 기능들을 사용하게 된다.

그러나, 대부분의 경우 이런 기능들은 매우 느리게 동작하므로 전체적으로 시스템 속도를 저하시키는 원인이 되기도 한다.

따라서, 본 발명에 따른 패킷 서비스 장치(210)는 락(Lock) 기능의 사용을 최소화하는 아래와 같은 방법을 이용함으로써 패킷 서비스 장치(210)의 성능을 향상시킨다.

도 2c에 도시된 바와 같이, 본 발명에 따른 패킷 서비스 장치(210)의 공유메모리는 기본적으로 환형 큐의 형태를 띄고 있으며, 데이터를 기록할 때마다 'WritePosition'이 증가하게 된다. 그리고, 데이터는 'ReadStart' 앞의 위치까지 기록할 수 있으며, 데이터를 읽을 때마다 'NextRead'가 증가하게 된다.

'ReadStart'와 'NextRead' 간의 영역은 공유 메모리에서 보호되는 공간이므로, 공유 메모리의 데이터를 유지하기 위해 당해 공유 메모리를 사용하는 컴포넌트들은 별도의 데이터의 복사 작업이 제한된다.

그러나, 당해 영역의 데이터가 더 이상 필요없는 경우 그 크기만큼 'ReadStart'의 값을 증가시켜 그 영역만큼의 데이터를 이후에 추가적으로 쓸 수 있도록 할 수 있다. 예를 들어, 당해 영역 전부가 필요없는 경우 'Read Start'의 값을 'NextRead'의 값과 같도록 설정한다면 공유 메모리의 전체영역을 쓰기 가능 영역으로 만들 수도 있는 것이다.

이와 같은 공유 메모리 운용상의 특징으로 'Pool' 단위로 읽기 작업을 수행하도록 하고, 공유메모리를 쓰는 쪽에서 참조하는 변수들과 읽는 쪽에서 참조하는 변수들이 확연히 구분되도록 함으로써, 상술한 락(Lock)이 필요한 횟수를 획기적으로 줄일 수 있고, 결과적으로 패킷 서비스 장치의 전체적인 성능이 향상될 수 있다.

다시 도 2b를 참조하면, 패킷 서비스 장치(210)에 포함된 데이터 전송 및 필터링부(255)는 패킷 데이터 입력부(250)로부터 패킷 데이터를 수신하여, 패킷 재조합(IP 프로토콜, TCP 프로토콜, UDP프로토콜로 나누어진 패킷의 재조합), TCP/IP Protocol들(IP, TCP, UDP, ICMP)은 데이터의 정합성 체크를 위한 체크섬(checksum) 오류 검사, 필터링 규칙에 따라 수신된 패킷을 무시하거나, 전송하는 기능을 수행한다. 또한, 데이터 전송 및 필터링부(255)는 응용 프로토콜 레벨에서의 정확한 패킷 분석을 위해 프로토콜 분석부(260)로 패킷을 전송하는 기능을 수행한다. 데이터 전송 및 필터링부(255)는 각각의 기능별로 별도의 수단으로 분리되어 구성될 수 있음은 당연하다.

프로토콜 분석부(260)는 응용 프로토콜별로 데이터 패킷을 분석하여, 패킷의 총량과 컨텐츠의 내용을 분석하는 기능을 수행한다. 프로토콜 분석부(260)는 각 용도에 따라 복수 개로 구성할 수 있음은 당연하다. 예를 들어 HTTP는 제1 프로토콜 분석부에서, WAP은 제2 프로토콜 분석부에서, DNS는 제3 프로토콜 분석부에서 각각 독립된 프로그램을 이용하여 분석 및 처리하도록 할 수 있다. 프로토콜 분석부(260)의 프로그램들은 패킷의 소스 IP(Source IP), 목적지 IP(Destination IP), 포트 정보, 사용자 정보, 해당 URL이나 요청한 파일의 이름 및 크기, 패킷의 재전송 여부 등을 분석 및/또는 추출하고, 추출된 정보를 데이터 저장 및 통계 처리부(265)로 전송한다.

프로토콜 분석부(260)는 패킷 서비스 장치(210)가 동작하는 환경 또는 운용자의 설정에 따라 처리할 수 있는 프로토콜 분석 컴포넌트를 패킷 서비스 장치(210)의 동작을 중단하지 않은 상태에서 추가 및/또는 삭제할 수 있다. 그리고, WAP, HTTP, FTP 등의 표준 프로토콜뿐 아니라 동작 환경 등에 따라 특화 또는 수정된 표준 프로토콜들도 유무선 환경에 따라 적절하게 적용되어, 원하는 정보를 추출하여 데이터 출력부(270)를 통해 목적지로 전송할 수 있다. 이때, 추출 가능한 정보로는 총 사용량, 세션별 사용량, 프로토콜별 사용량, 이상 패킷 용량 등과 같이 패킷 자체에서 얻을 수 있는 여러 가지 통계 정보 외에, 프로토콜별 흐름과 데이터 패턴 등을 분석해 얻어지는 정보 등이 있다.

데이터 저장 및 통계 처리부(265)는 프로토콜 분석부(260)에서 생성된 정보를 표준 포맷 형태로 저장하는 기능, 실시간 통계 및 분석 기능을 제공한다. 따라서, 통신 서비스 사업자는 데이터 저장 및 통계 처리부(265)의 기능을 통해 프로토콜 분석부(260)에 의해 분석 및/또는 검출된 정보를 과금, 시스템 용량 확장 등을 위한 기초 자료로 활용할 수 있다. 데이터 저장 및 통계 처리부(265)는 각각의 기능별로 별도의 수단으로 분리되어 구성될 수 있음은 당연하다.

본 발명에 따른 패킷 서비스 장치(210)의 데이터 저장 및 통계 처리부(265)는 운용자의 설정과 동작환경에 따라 주기적으로 또는 외부 컴포넌트 등에서 요구가 있을 때 각 컴포넌트에서 유지하고 있는 패킷/세션 등에 관한 상태나 로그정보들을 미리 지정된 형태로 가공하여 디스크에 저장할 수 있다. 이때 상태 정보 또는 로그 정보들이 가공되는 형태는 운용자가 직접 분석할 수 있는 형태, 다른 소프트웨어 또는 하드웨어 프로토콜 분석 장비에서 사용할 수 있는 형태 등일 수 있다. 또한, 데이터 저장 및 통계 처리부(265)는 디스크에 저장된 데이터를 기초로 각종 통계정보를 생성하여 관리자 화면을 통해 디스플레이될 수 있는 자료를 생성하게 된다.

패킷 데이터 출력부(270)는 패킷 데이터 입력부(250)로부터 수신한 패킷 데이터를 지정된 목적지로 전송하는 기능, 데이터 저장 및 통계 처리부(265)에 표준 포맷 형태로 저장된 데이터를 외부 과금서버로 전송하는 기능을 수행한다. 만약 특정 패킷 데이터가 데이터 전송 및 필터링부(255)에 의해 필터링된 경우라면 해당 패킷 데이터는 패킷 데이터 출력부(270)에 전송되지 않으며, 결과적으로 해당 패킷 데이터는 목적지까지 전송되지 않는다.

도 3a는 본 발명의 바람직한 다른 실시예에 따른 무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면이고, 도 3b는 본 발명의 바람직한 또 다른 실시예에 따른 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면이고, 도 3c는 본 발명의 바람직한 다른 실시예에 따른 무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템의 전체 구성을 나타낸 도면이다.

앞서 도 2a를 참조하여 본 발명에 따른 패킷 서비스 장치(210)의 배치예를 설명하였으나, 그 외에도 도 3a 내지 도 3c에 도시된바와 같은 다양한 형태로 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템을 구성할 수 있다.

도 3a에 도시된 무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템에서의 패킷 서비스 장치(210)의 배치 형태는 도 2a에 도시된 유선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성 시스템에서의 패킷 서비스 장치(210)의 배치 형태와 유사한 형태이므로 이에 대한 설명은 생략하기로 한다.

또한, 본 발명에 따른 패킷 서비스 장치(210)는 도 3b 및 도 3c에 도시된 바와 같이 라우터(310)(또는 스위치 허브 등)에 병렬로 결합되도록 구성될 수도 있다.

도 3b 및 도 3c에 도시된 바와 같이 패킷 서비스 장치(210)를 배치하는 경우, 라우터(310)(또는 스위치 허브 등)에서 해당 패킷 데이터를 지정된 목적지로 전송하면서 동시에 해당 패킷 데이터를 패킷 서비스 장치(210)로 전송하게 된다. 그리고, 패킷 서비스 장치(210)는 수신된 패킷 데이터를 분석 및 통계 처리하게 되며, 분석 및 통계 처리된 정보를 저장한다.

도 2a 및 도 3a에 도시된 바와 같이 패킷 서비스 장치(210)를 배치하는 경우와 달리, 도 3b 및 도 3c에 도시된 바와 같이 패킷 서비스 장치(210)를 배치하면 라우터(310)로부터 전송된 패킷 데이터가 이미 목적지를 향해 전송 중이므로 패킷 서비스 장치(210)에 의한 패킷 데이터 전송 여부에 대한 제어는 불가능할 수 있다. 물론, 라우터(310)에서 패킷 서비스 장치(210)로부터 전송 허가 정보를 수신한 후 해당 패킷 데이터를 전송하도록 하는 경우라면 패킷 데이터 전송 여부에 대한 제어가 가능함은 당연하다.

또한, 도 3b 및 도 3c에 도시된 바와 같이 패킷 서비스 장치(210)를 배치함으로써 패킷 데이터 전송 여부에 대한 제어가 불가능한 경우일지라도, 그 외의 모니터링, 통계 및 과금자료 생성이 기능은 앞서 설명한 바와 동일하게 수행할 수 있다.

또한, 도 3b 및 도 3c에 도시된 바와 같이 패킷 서비스 장치(210)를 배치하면 패킷 서비스 장치(210)의 장애시에도 네트워크를 통하는 패킷 데이터의 송수신 과정에는 아무런 장애가 없으므로 통신 사업자가 사용자에게 중단없는 서비스를 제공할 수 있음은 당연하다.

도 4는 본 발명의 바람직한 일 실시예에 따른 패킷 서비스 장치에서 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법을 수행하는 과정을 나타낸 순서도이다.

앞서 설명한 바와 같이, 도 4의 각 단계는 패킷 서비스 장치(210)를 구성하는 각 수단(component)에서 개별적으로 수행될 수 있으나, 이해의 편의를 위해 패킷 서비스 장치(210)에서 수행하는 것으로 통칭하여 설명하기로 한다.

도 4를 참조하면, 단계 410에서 패킷 서비스 장치(210)는 네트워크를 통해 사용자 단말기(110) 또는 컨텐츠 서버(120)로부터 패킷 데이터를 수신한다. 그리고, 수신된 패킷 데이터는 공유 메모리(예를 들어, 입력 버퍼(Input Buffer) 등)에 저장된다.

단계 415에서 패킷 서비스 장치(210)는 단계 410을 통해 수신한 패킷 데이터가 미리 지정된 필터링(Filtering) 규칙에 만족하는지 여부를 검사한다.

이때, 미리 지정된 필터링 규칙은 당해 패킷 데이터에 상응하는 소스 IP 주소(Source IP Address) 및 목적지 IP 주소(Destination IP Address)가 필터링되어야 할 IP 주소로서 이미 등록된 IP 주소와 일치하는지 여부, 체크섬(checksum), 패리티 검사(parity check) 등을 통해 패킷 데이터에 오류가 존재하는지 여부, 서비스 거부 (DOS : Denial of Service) 공격 등과 같은 해킹 의도가 존재하는지 여부, 바이러스(Virus)에 감염된 패킷 데이터인지 여부 등을 검사하기 위한 것으로, 상술한 필터링 규칙을 만족하는 경우에는 문제있는 패킷 데이터인 것으로 판단하여 목적지로 전송되지 않도록 한다.

단계 415의 검사 결과로 당해 패킷 데이터가 미리 지정된 필터링 규칙을 만족하는 경우에는 단계 420으로 진행하여 당해 패킷 데이터를 삭제한 후 단계를 종료한다. 물론 신규 패킷 데이터가 수신되는 경우에는 단계 410부터 다시 진행한다.

그러나, 단계 415의 검사 결과로 당해 패킷 데이터가 미리 지정된 필터링 규칙을 만족하지 못하는 경우에는 패킷 서비스 장치(210)는 단계 425 및 단계 430을 동시에 진행한다.

즉, 패킷 서비스 장치(210)는 단계 425에서 당해 패킷 데이터를 목적지 IP 주소(Destination IP Address)로 전송함과 동시에 단계 430에서 단계 410을 통해 수신된 패킷 데이터의 재조합을 수행한다. 물론, 단계 425의 동작은 앞서 설명한 도 2a 및 도 3a의 구성을 가지는 경우에 해당되는 것이며, 도 3b 및 도 3c와 같이 구성되는 경우는 단계 425는 별도의 라우터(310)에 의해 수행될 수 있다.

단계 430에서 수행되는 재조합 과정은 IP, TCP, UDP 등 프로토콜의 특성으로 인해 단편화(fragmentation)된 패킷 데이터를 이후 응용 프로토콜에서 분석할 수 있도록 하기 위해 논리적으로 하나의 패킷 데이터로 구성하는 것이다. 다만, 당해 패킷 데이터가 재조립이 불필요한 경우에는 단계 430은 생략될 수 있음은 당연하다. 그리고, IP 패킷의 경우 재조립이 필

요하면 버퍼(예를 들어, Hash-Tree 버퍼 등)에 보관하여 추후 들어오는 패킷들을 재조립하게 되며, 재조립이 완료된 IP 패킷들과 재조립이 필요없는 패킷들은 헤더(Header)에 포함된 정보에 따라 ICMP, TCP, UDP 등의 처리를 하게 된다. 특히, TCP의 경우 세션 관리를 해야하는데 이 역시 Hash-Tree 알고리즘이 이용될 수 있으며, 이를 통해 해당 패킷 데이터가 어떤 세션에 연관된 패킷인지 판단하게 된다. TCP/IP 또는 상위 프로토콜들을 관련된 패킷들끼리 재조립하거나 세션 관리 등의 목적을 위해 데이터 삽입, 삭제, 검색 등의 기능이 필요함은 당연하며, 이때 종래에는 Hash-List 알고리즘이 많이 사용되고 있었다. 그러나, Hash-List 알고리즘은 특정 키 군(Set)이 몰려서 삽입될 경우 Hash의 기능이 떨어지게 되어 최악의 경우 하나의 Hash-List에 자료가 전부 몰리게 되고, 결과적으로 검색시 걸리는 시간이 굉장히 길어지는 단점이 있었다. 따라서, 본 발명에 따른 패킷 서비스 장치(210)는 Hash-List 구조가 아닌, Hash-Tree구조에 따른 버퍼 운용 알고리즘을 사용한다. 즉, Hash의 각 노드에 대해 List가 아닌 균형 이진 트리(Balanced-Binary-Tree) 알고리즘을 도입하여, 하나의 Hash 노드에 자료가 몰리더라도 그 영향을 최소화하였다.

본 발명에 따른 패킷 서비스 장치(210)가 TCP 연결을 맺고 있는 사용자 단말기(110) 및 컨텐츠 서버(120)간의 접속 상태를 추정하고 유지 관리하는 방법에 대해서는 이후 도 5a 내지 도 5d를 참조하여 상세히 설명하기로 한다.

단계 435에서 패킷 서비스 장치(210)는 단계 430을 통해 재조합된 패킷 데이터에 대한 분석 작업을 수행한다. 패킷 서비스 장치(210) 내에 다수의 프로토콜 분석부(260)가 포함될 수 있음은 앞서 설명한바와 같다. 이는 네트워크를 통해 전송되는 패킷의 프로토콜은 HTTP, WAP, FTP, TELNET, RTP, RTCP 등과 같이 여러 가지가 존재하며, 이에 대한 처리방식도 각각의 특성상 서로 상이하기 때문이다. 따라서, 패킷 서비스 장치(210)는 각각의 패킷 데이터를 효과적으로 처리하기 위해서는 HTTP, WAP, FTP 등의 상이한 프로토콜별로 해당 프로토콜 전용의 응용 프로토콜 분석부(260)가 존재할 필요가 있다. 그리고, 프로토콜 분석부(260)에서는 사용자 정보, 패킷 사용량 정보, 컨텐츠 정보 등을 추출하는 동작을 수행한다.

단계 440에서 패킷 서비스 장치(210)는 단계 435를 통해 추출된 정보를 이용하여 분석 데이터 저장 및 통계 처리를 수행한다. 이때, 패킷 서비스 장치(210)는 각 서비스별, 사용자별, 서버별 통계 등과 같이 필요로 하는 통계정보를 생성하고, 생성된 통계 정보를 저장 장치에 저장한다.

이후, 외부 장치(또는 동일한 인터넷 서비스 시스템 내의 다른 장치)로부터 기초 과금 데이터 제공 요청이 수신되는 경우, 단계 445에서 패킷 서비스 장치(210)는 단계 440을 통해 저장되고 통계 처리된 정보를 네트워크를 통해 당해 외부 장치로 전송한다.

이와 같이 본 발명에 따른 패킷 서비스 장치(210)는 패킷 데이터 전송 제어 기능 및 과금 기초 데이터 생성 기능을 동시에 수행할 수 있다.

즉, 본 발명에 따른 패킷 서비스 장치(210)는 운용자의 설정과 동작 환경에 따라, 분석 가능한 항목들을 점검한 후 미리 지정된 필터링 규칙(즉, 특정 패턴)을 만족하는 패킷들을 무시(예를 들어, 방화벽(Firewall), 네트워크 침임 탐지 및 방지 시스템(NIDS : Network Intrusion Detection & Prevention System) 등의 기능 수행)의 기능하거나, 수신된 패킷 데이터를 목적지 주소로 전송할 수 있다. 또한, 관리자가 관리자 단말기를 이용하여 직접 분석할 수 있는 형태, 다른 소프트웨어 또는 하드웨어 프로토콜 분석 장비에서 사용할 수 있는 형태로 패킷 로그를 가공하여 외부 네트워크 또는 디스크에 저장 할 수 있다.

도 5a는 본 발명의 바람직한 일 실시예에 따른 송신단의 TCP 상태도(TCP State Diagram)이고, 도 5b는 본 발명의 바람직한 일 실시예에 따른 수신단의 TCP 상태도(TCP State Diagram)이고, 도 5c는 본 발명의 바람직한 일 실시예에 따른 TCP 연결 흐름과 각 단계별 상태를 나타낸 도면이며, 도 5d는 본 발명의 바람직한 다른 실시예에 따른 동시 접속(Simultaneous-Open) 또는 동시 해제(Simultaneous-Close)의 경우 TCP 연결 흐름과 각 단계별 상태를 나타낸 도면이다.

본 발명에 따른 패킷 서비스 장치(210)는 송신단(사용자 단말기(110) 또는 컨텐츠 서버(120))으로부터 임의의 패킷 데이터를 수신하여 수신단(컨텐츠 서버(120) 또는 사용자 단말기(110))으로 전송하는 과정을 수행하는 장치이다.

따라서, 송신단에서 수신단으로 TCP 연결을 위한 SYN 플래그(Flag)가 세팅된 패킷을 전송한 경우라도, 패킷 서비스 장치(210)는 송신단이 SYNSENT, 수신단이 SYNRCVD(SYN-RECEIVED)의 상태라고 추측할 수는 없다.

이는 송신단에서 패킷 서비스 장치(210)까지는 유효하게 패킷 데이터가 수신되었고, 또한 패킷 서비스 장치(210)에서 해당 패킷 데이터를 수신단으로 오류없이 전송했을지라도 수신단이 네트워크상의 오류 등으로 해당 패킷 데이터를 정상 처리하지 못하는 경우도 있으며, 이러한 경우에는 수신단의 TCP 상태(state)가 SYNRCVD이 아니기 때문이다.

따라서, 본 발명에 따른 패킷 서비스 장치(210)는 특정 패킷 데이터 하나(예를 들어, SYN 플래그가 세팅된 TCP 패킷)가 전송된 것만으로 양쪽의 TCP 상태(state)를 판단하고, 바로 다음에 수신단쪽에서 SYN과 ACK이 정상적으로 세팅된 패킷 데이터가 송신단쪽으로 전달될 경우에만, 이전의 SYN 플래그가 세팅된 TCP 패킷이 정상적으로 수신단에서 처리되었다고 판단한 후, 양쪽의 상태를 유지하게 되는 것이다.

따라서, 본 발명에 따른 패킷 서비스 장치(210)는 일정 단계에서는 송신단 및/또는 수신단을 SYNRCVD_R, CLOSE_R, ESTABLISHED_R 등과 같이 *_R의 이름을 가진 상태(즉, 후보 상태(Ready State) - 실제 상태 천이가 일어나기 전 상태)로 관리한다.

그리고, 이하에서 도 5a 내지 도 5d에 도시된 도면을 설명함에 있어, 이해의 편의를 위해 도 5a 내지 도 5d에 도시된 도면을 함께 설명하기로 하며, 또한 도 5a 내지 도 5d에 도시된 도면간에 관련성 있는 단계를 동일한 참조번호를 적용하여 함께 설명하기로 한다. 다만, 도 5a 및 도 5b의 송신단(Sender)과 수신단(Receiver)의 구분은 특정 패킷 데이터를 송신 또는 수신한 주체를 의미하는 것으로서, 도 5c 및 도 5d의 CP(Connection Point)-A 또는 CP-B를 특정하는 것은 아니다. 따라서, 이하에서는 송신단 또는 수신단이라는 용어대신 CP-A 또는 CP-B라는 용어를 사용하기로 한다.

먼저, 도 5a 내지 도 5c를 참조하면, 단계 510은 CP-A에서 연결을 초기화하기 위해 순서번호를 동기화한 SYN 패킷을 CP-B로 전송하는 단계이다. 이 경우 종래의 패킷 데이터 중계 장치는 SYN 패킷을 CP-A에서 CP-B로 전송한 후에는 CP-B가 SYNRCVD 상태인 것으로 추측한다. 그러나, 이와 같이 추측하는 것은 상술한 문제점 때문에 본 발명에 따른 패킷 서비스 장치(210)에는 적용되지 않는다. 따라서, 패킷 서비스 장치(210)는 CP-B로부터 단계 520을 통해 SYN|ACK 패킷 데이터가 수신될 때까지 수신단의 상태를 예비상태인 SYNRCVD_R로 추측하는 것이다.

단계 520을 통해 SYN|ACK 패킷 데이터가 CP-B로부터 CP-A로 전송되면, 패킷 서비스 장치는 CP-A가 ESTABLISHED_R 상태인 것으로 추측하고, 단계 530을 통해 ACK 패킷 데이터가 CP-A로부터 CP-B로 전송(즉, 확인응답 번호가 유효함)되면 CP-A와 CP-B가 ESTABLISHED 상태인 것으로 추측한다.

이는 이후의 단계에서도 동일하게 적용된다. 즉, 단계 540을 통해 CP-A로부터 FIN 패킷 데이터가 CP-A로부터 CP-B로 전송(즉, 송신측이 데이터 전송을 종료함)한 경우, 패킷 서비스 장치(210)는 현재 CP-A의 상태가 CLOSE_R 상태인 것으로 추측한다. 그리고, 단계 540을 통해 ACK 패킷 데이터가 CP-B로부터 CP-A로 전송되면 CP-A가 CLOSED 상태인 것으로 추측하며, CP-B가 CLOSED 상태로 전환되는 방법도 이와 같다.

다음으로, 도 5a, 도 5b 및 도 5d를 참조하여 CP-A와 CP-B간에 SYN 패킷 데이터를 동시에 전송한 경우에 패킷 서비스 장치(210)에서 CP-A와 CP-B의 상태를 추측하는 방법에 대해 설명한다.

단계 510에서 CP-A가 CP-B로 SYN 패킷 데이터를 전송함과 동시에 단계 560을 통해 CP-B가 CP-A로 SYN 패킷 데이터를 전송한 경우, 패킷 서비스 장치(210)는 단계 510의 SYN 패킷 데이터 전송에 의해 CP-A는 SYNSENT 상태, CP-B는 SYNRCVD_R 상태로 추측한 후, 단계 560의 SYN 패킷 데이터 전송에 의해 CP-A 및 CP-B가 SYNRCVD_SO 상태인 것으로 추측한다.

이후, CP-A와 CP-B는 각각 상대방으로부터 수신한 SYN 패킷 데이터에 대한 응답으로 SYN|ACK 패킷 데이터를 전송하면, 패킷 서비스 장치(210)는 단계 570에서 CP-A 및 CP-B가 ESTABLISHED 상태인 것으로 추측한다.

그리고, 이후 CP-A 및 CP-B가 CLOSED 상태로 되는 과정은 상술한 내용으로서 쉽게 이해할 수 있으므로 별도의 설명은 생략한다.

본 발명은 상기 실시예에 한정되지 않으며, 많은 변형이 본 발명의 사상 내에서 당 분야에서 통상의 지식을 가진 자에 의하여 가능함은 물론이다.

발명의 효과

상술한 바와 같이 본 발명에 따른 유무선 통신망에서의 패킷 전송 제어 및 과금 데이터 생성을 위한 방법 및 장치는 데이터 패킷 분석을 통해 소스(Source) 및 목적지(Destination) IP 경로 추적 기능, IP 주소별/네트웍별 프로토콜 분석 기능, TCP/IP 레벨의 프로토콜 분석뿐 아니라 응용 프로토콜에서의 분석을 통한 패킷 접근제어를 통해 서비스 거부(DOS : Denial of Service) 공격과 같은 해킹 여부를 탐지하여 대처할 수 있다.

또한, 본 발명은 패킷 서비스 제어 기능뿐 아니라 실시간 패킷 사용량 및 패킷 사용량 분포에 대한 실시간 모니터링 기능을 제공하며, 실시간 패킷 사용량 정보를 이용하여 통계 작업 및 네트워크 용량 산정을 가능하게 한다.

또한, 본 발명은 사용자 단말기로부터 패킷 교환기까지는 무선 데이터 통신 구간이고, 패킷 교환기부터 컨텐츠 서버까지는 유선 데이터 통신 구간으로 분리된 경우에도, 하나의 장치를 통해 유무선 인터넷의 과금 처리를 위한 과금 기초 데이터를 생성할 수 있어 설치 및 운용의 편의성을 증진시키고 유무선 통합 환경의 단일화된 데이터 과금 솔루션을 제공할 수 있다.

또한, 본 발명은 프로토콜 분석을 통한 컨텐츠의 내용 및 컨텐츠별 패킷량 정보를 동시에 검출할 수 있다.

또한, 본 발명은 통신 사업자에게 필수 기능인 패킷 서비스 제어 기능과 과금 데이터 생성 기능을 하나의 장치에서 통합하여 수행할 수 있도록 하여 비용 절감 및 시스템 단순화가 가능하다.

(57) 청구의 범위

청구항 1.

패킷 서비스 장치에 있어서,

네트워크를 통해 패킷 데이터를 수신하여 공유 메모리에 저장하는 패킷 데이터 입력부-여기서, 상기 패킷 데이터는 적어도 소스 IP 주소(Source IP Address), 목적지 IP 주소(Destination IP Address)를 포함함-;

상기 공유 메모리에 저장된 상기 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하여, 상기 패킷 데이터가 상기 필터링 규칙을 만족하면 삭제(delete)하는 필터링부;

상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 상기 목적지 IP 주소를 이용하여 전송하는 패킷 데이터 출력부;

상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량 및 사용자 정보를 분석하는 프로토콜 분석부;

상기 프로토콜 분석부에 의해 분석된 정보를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 데이터 저장부를 포함하는 것을 특징으로 하는 패킷 서비스 장치.

청구항 2.

제1항에 있어서,

상기 데이터 저장부에 저장된 정보를 이용하여 과금 기초 데이터를 생성하는 통계 처리부

를 더 포함하되,

상기 과금 기초 데이터는 실시간 통계 및 분석 정보를 포함하는 것

을 특징으로 하는 패킷 서비스 장치.

청구항 3.

제1항에 있어서,

상기 패킷 데이터가 프로토콜의 특성으로 인해 단편화(fragmentation)된 경우, 상기 프로토콜 분석부에서 분석할 수 있도록 논리적으로 하나의 패킷 데이터로 재조립하는 패킷 데이터 재조립부

를 더 포함하는 것을 특징으로 하는 패킷 서비스 장치.

청구항 4.

제1항에 있어서,

상기 프로토콜 분석부는 상기 패킷 데이터의 종류에 따라 특화된 복수개의 프로토콜 분석부로 이루어진 것

을 특징으로 하는 패킷 서비스 장치.

청구항 5.

제1항에 있어서,

상기 패킷 서비스 장치는 송신단으로부터 수신단으로 SYN 패킷 데이터가 전송되고, 상기 수신단에서 상기 전송단으로 상기 SYN 패킷 데이터에 상응하는 ACK 패킷 데이터가 전송된 후에만 상기 수신단의 TCP 상태를 SYNRCVD 상태로 추측하는 것

을 특징으로 하는 패킷 서비스 장치.

청구항 6.

제1항에 있어서,

상기 공유 메모리는,

환형 큐의 형태인 경우, ReadStart 값과 NextRead 값을 동일하게 설정함으로써 쓰기 가능 영역을 최대화할 수 있는 것

을 특징으로 하는 패킷 서비스 장치.

청구항 7.

제6항에 있어서,

상기 공유 메모리의 운용 알고리즘은 균형 이진 트리(Balanced-Binary-Tree) 알고리즘인 것

을 특징으로 하는 패킷 서비스 장치.

청구항 8.

유무선 인터넷 서비스 시스템에 포함된 패킷 서비스 장치가 송신단으로부터 수신된 패킷 데이터를 수신단으로 전송 여부를 제어하는 방법에 있어서,

네트워크를 통해 패킷 데이터를 수신하는 단계-여기서, 상기 패킷 데이터는 적어도 소스 IP 주소(Source IP Address), 목적지 IP 주소(Destination IP Address)를 포함함-;

상기 수신된 패킷 데이터를 공유 메모리에 저장하는 단계;

상기 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하는 경우, 상기 패킷 데이터를 삭제(delete)하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 상기 목적지 IP 주소를 이용하여 전송하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량, 사용자 정보를 분석하여 과금 기초 데이터를 생성하는 단계;

상기 과금 기초 데이터를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 단계;

과금 수행 장치로부터 상기 과금 기초 데이터의 제공 요청이 수신되는 경우, 상기 과금 기초 데이터를 네트워크를 통해 상기 과금 수행 장치로 전송하는 단계

를 포함하는 것을 특징으로 하는 패킷 서비스 제어 방법.

청구항 9.

제8항에 있어서,

상기 패킷 서비스 장치는 송신단으로부터 수신단으로 SYN 패킷 데이터가 전송되고, 상기 수신단에서 상기 전송단으로 상기 SYN 패킷 데이터에 상응하는 ACK 패킷 데이터가 전송된 후에만 상기 수신단의 TCP 상태를 SYNRCVD 상태로 추측하는 것

을 특징으로 하는 패킷 서비스 제어 방법.

청구항 10.

제8항에 있어서,

상기 필터링 규칙은 상기 패킷 데이터에 상응하는 소스 IP 주소(Source IP Address) 및 목적지 IP 주소(Destination IP Address)가 필터링되어야 할 IP 주소로서 이미 등록된 IP 주소와 일치하는지 여부, 상기 패킷 데이터에 오류가 존재하는지 여부, 상기 패킷 데이터가 해킹 의도를 포함하고 있는지 여부, 바이러스(Virus)에 감염된 패킷 데이터인지 여부 중 적어도 어느 하나를 검사하기 위한 것

을 특징으로 하는 패킷 서비스 제어 방법.

청구항 11.

제8항에 있어서,

상기 패킷 데이터가 프로토콜의 특성으로 인해 단편화(fragmentation)된 경우, 상기 프로토콜 분석부에서 분석할 수 있도록 논리적으로 하나의 패킷 데이터로 재조립하는 단계

를 더 포함하는 것을 특징으로 하는 패킷 서비스 제어 방법.

청구항 12.

패킷 서비스 제어 방법을 수행하기 위해 패킷 서비스 장치에 의해 실행될 수 있는 명령어들의 프로그램이 유형적으로 구현되어 있으며, 상기 패킷 서비스 장치에 의해 판독될 수 있는 기록매체에 있어서,

네트워크를 통해 패킷 데이터를 수신하는 단계-여기서, 상기 패킷 데이터는 적어도 소스 IP 주소(Source IP Address), 목적지 IP 주소(Destination IP Address)를 포함함-;

상기 수신된 패킷 데이터를 공유 메모리에 저장하는 단계;

상기 패킷 데이터가 미리 지정된 필터링(filtering) 규칙을 만족하는지 여부를 검사하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하는 경우, 상기 패킷 데이터를 삭제(delete)하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 상기 목적지 IP 주소를 이용하여 전송하는 단계;

상기 패킷 데이터가 상기 필터링 규칙을 만족하지 않는 경우, 상기 패킷 데이터를 응용 프로토콜별로 분석하여 패킷의 총량, 사용자 정보를 분석하여 과금 기초 데이터를 생성하는 단계;

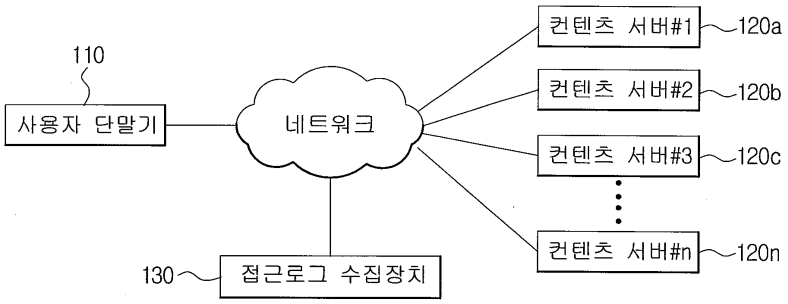
상기 과금 기초 데이터를 미리 지정된 표준 포맷 형태로 변환하여 저장하는 단계;

과금 수행 장치로부터 상기 과금 기초 데이터의 제공 요청이 수신되는 경우, 상기 과금 기초 데이터를 네트워크를 통해 상기 과금 수행 장치로 전송하는 단계

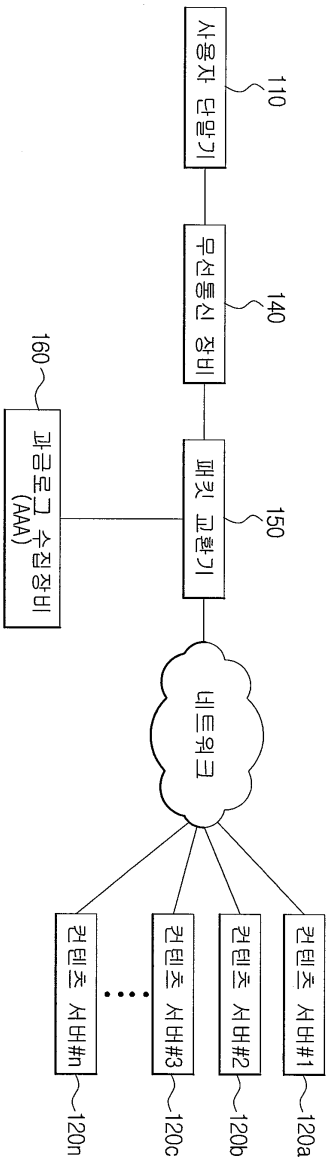
를 실행할 수 있는 프로그램을 기록한 기록매체.

도면

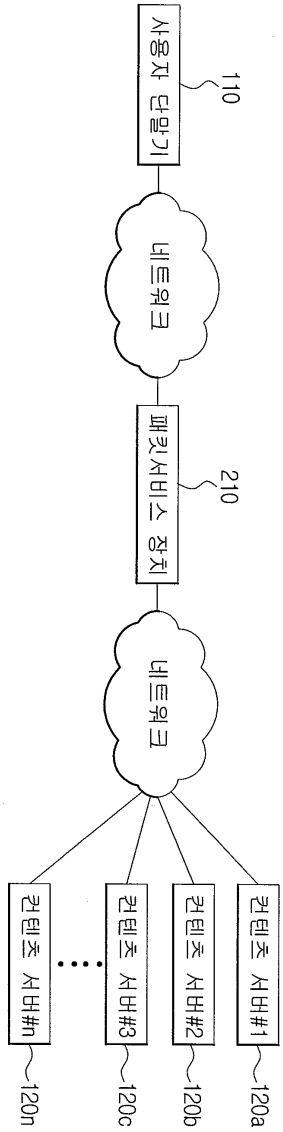
도면1a



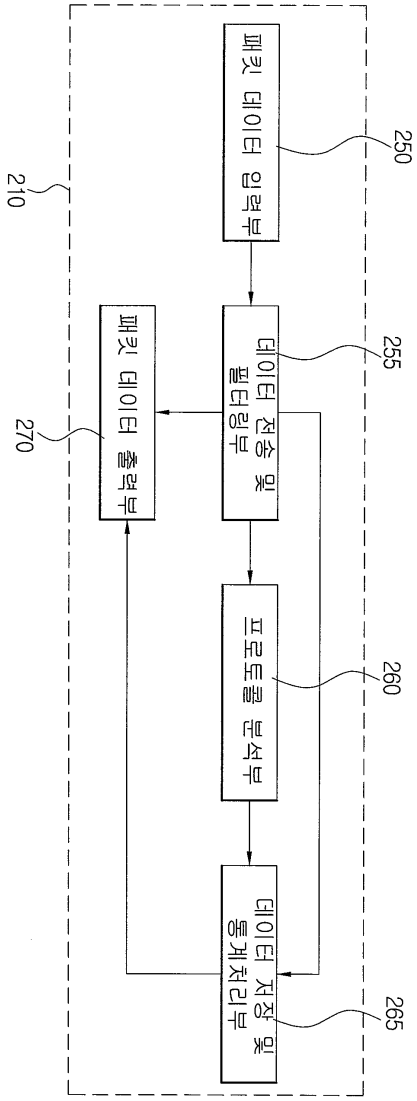
도면1b


사용자 단말기
110
무선통신 장비
140
160
과금로그 수집장비 (AAA)
패킷 교환기
150
네트워크
컨텐츠 서버#n
120n
컨텐츠 서버#3
120c
컨텐츠 서버#2
120b
컨텐츠 서버#1
120a

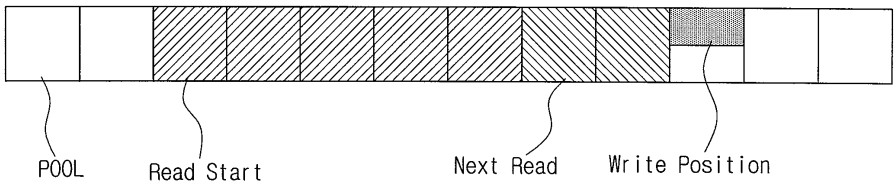
도면2a


사용자 단말기
110
네트워크
패킷서비스 장치
210
네트워크
컨텐츠 서버#n
120n
컨텐츠 서버#3
120c
컨텐츠 서버#2
120b
컨텐츠 서버#1
120a

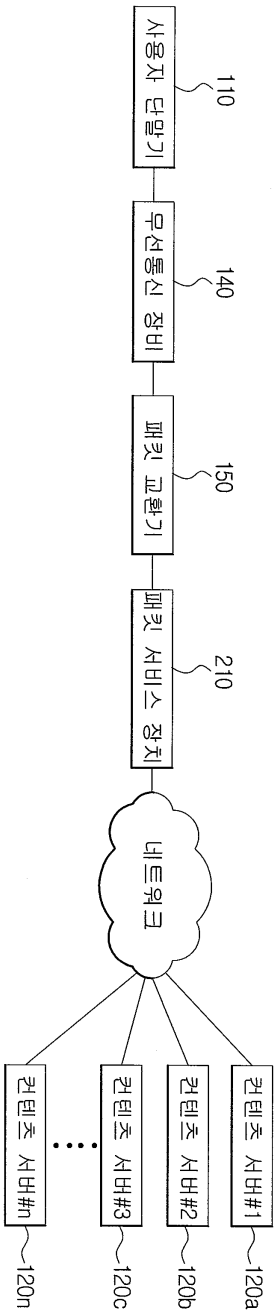
도면2b


210
패킷 데이터 입력부
250
데이터 전송 및 필터링부
255
패킷 데이터 출력부
270
프로토콜 분석부
260
데이터 저장 및 통계처리부
265

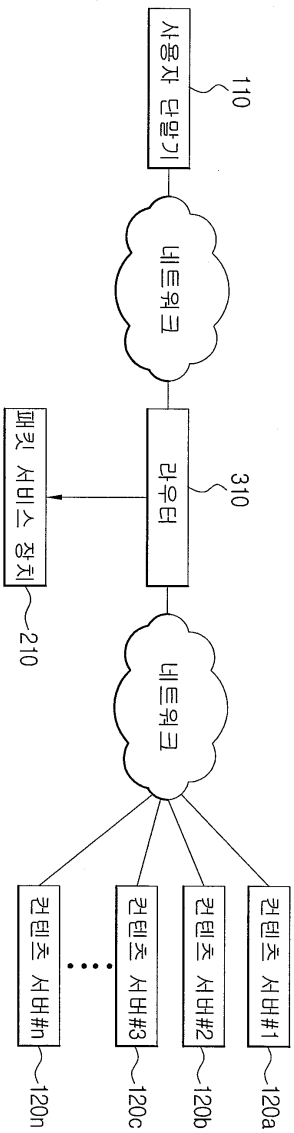
도면2c


POOL
Read Start
Next Read
Write Position

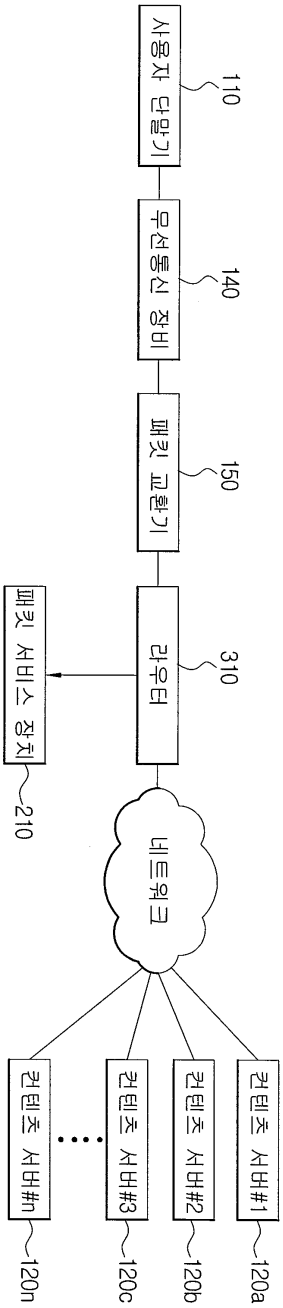
도면3a


사용자 단말기
110
무선통신 장비
140
패킷 교환기
150
패킷 서비스 장치
210
네트워크
컨텐츠 서버#1
120a
컨텐츠 서버#2
120b
컨텐츠 서버#3
120c
컨텐츠 서버#n
120n

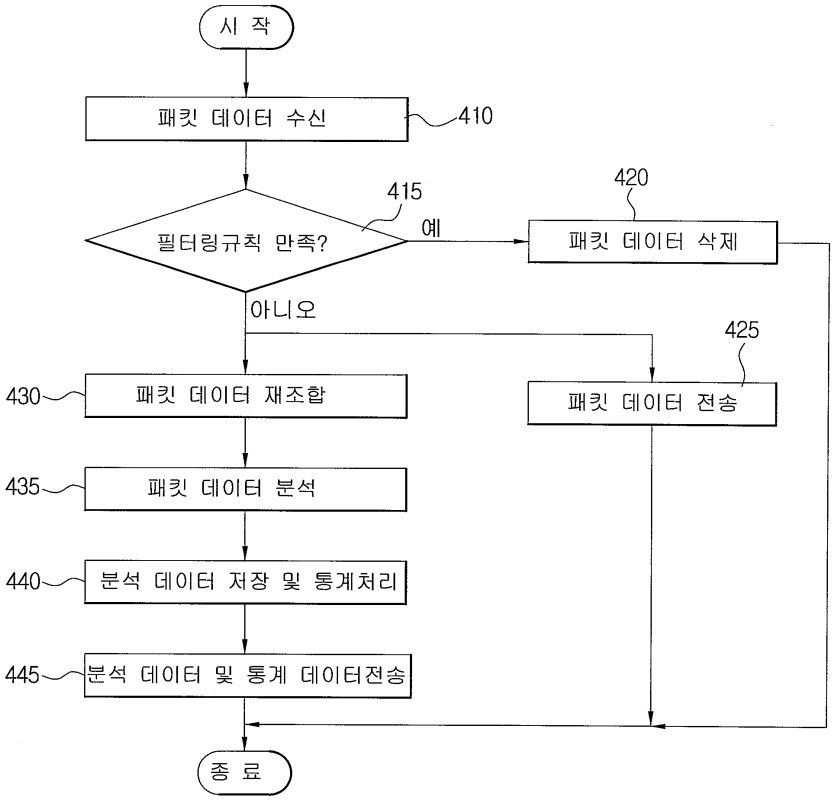
도면3b


사용자 단말기
110
네트워크
라우터
310
패킷 서비스 장치
210
네트워크
컨텐츠 서버#1
120a
컨텐츠 서버#2
120b
컨텐츠 서버#3
120c
컨텐츠 서버#n
120n

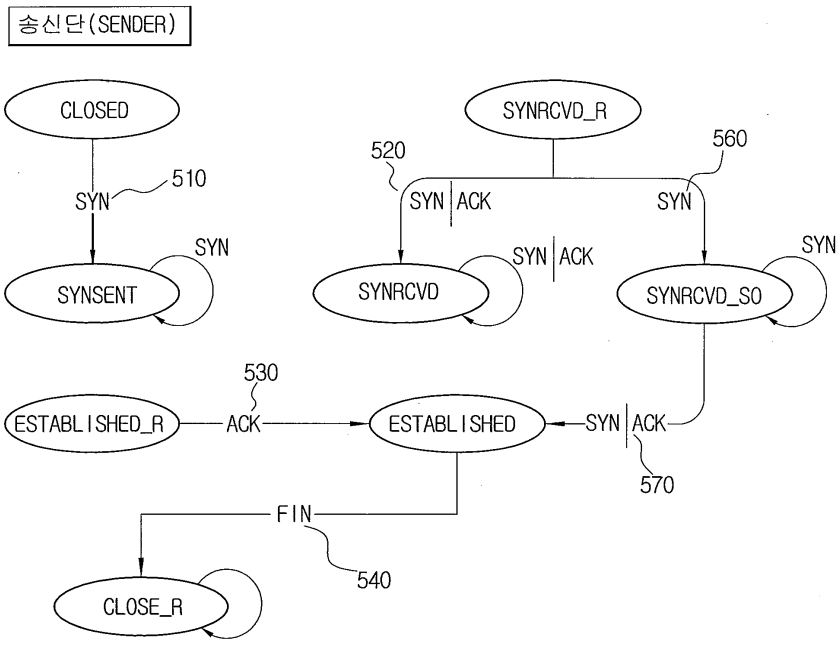
도면3c


사용자 단말기
110
무선통신 장비
140
패킷 교환기
150
라우터
310
패킷 서비스 장치
210
네트워크
컨텐츠 서버#n
120n
컨텐츠 서버#3
120c
컨텐츠 서버#2
120b
컨텐츠 서버#1
120a

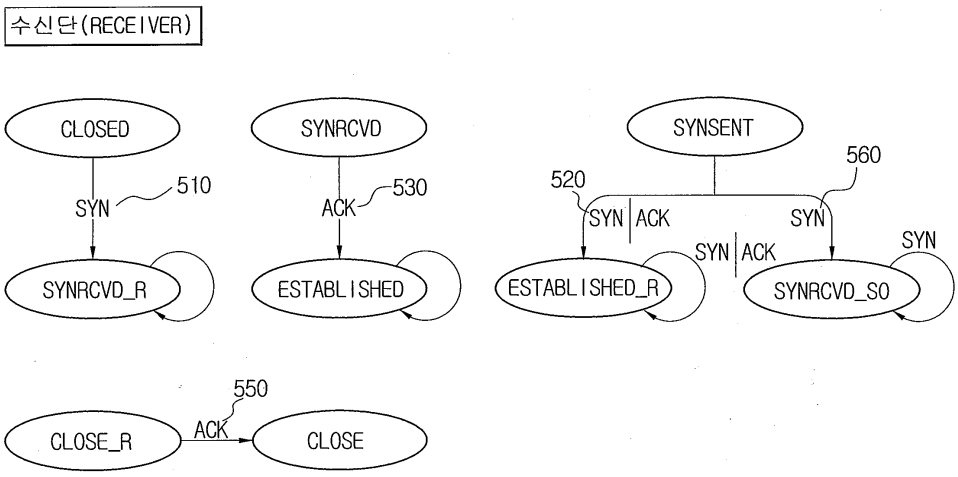
도면4


시 작
패킷 데이터 수신
410
415
필터링규칙 만족?
예
420
패킷 데이터 삭제
아니오
425
430
패킷 데이터 재조합
패킷 데이터 전송
435
패킷 데이터 분석
440
분석 데이터 저장 및 통계처리
445
분석 데이터 및 통계 데이터전송
종 료

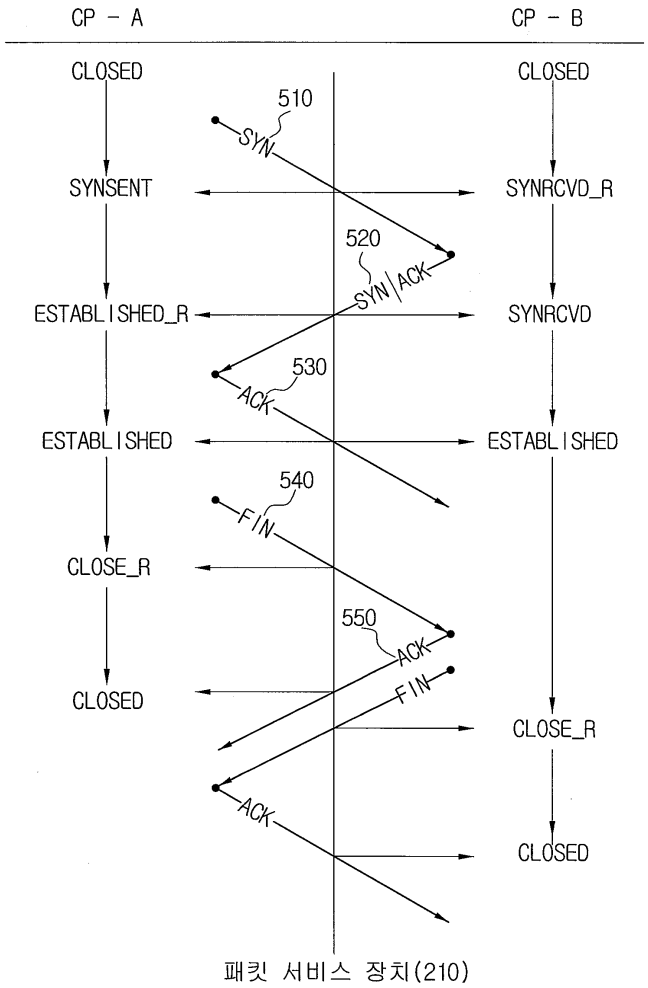
도면5a


송신단(SENDER)
CLOSED
SYN
510
SYN
SYNSENT
SYNRCVD_R
520
SYN | ACK
560
SYN
SYN | ACK
SYNRCVD
SYN
SYNRCVD_SO
530
ESTABLISHED_R
ACK
ESTABLISHED
SYN | ACK
570
FIN
540
CLOSE_R

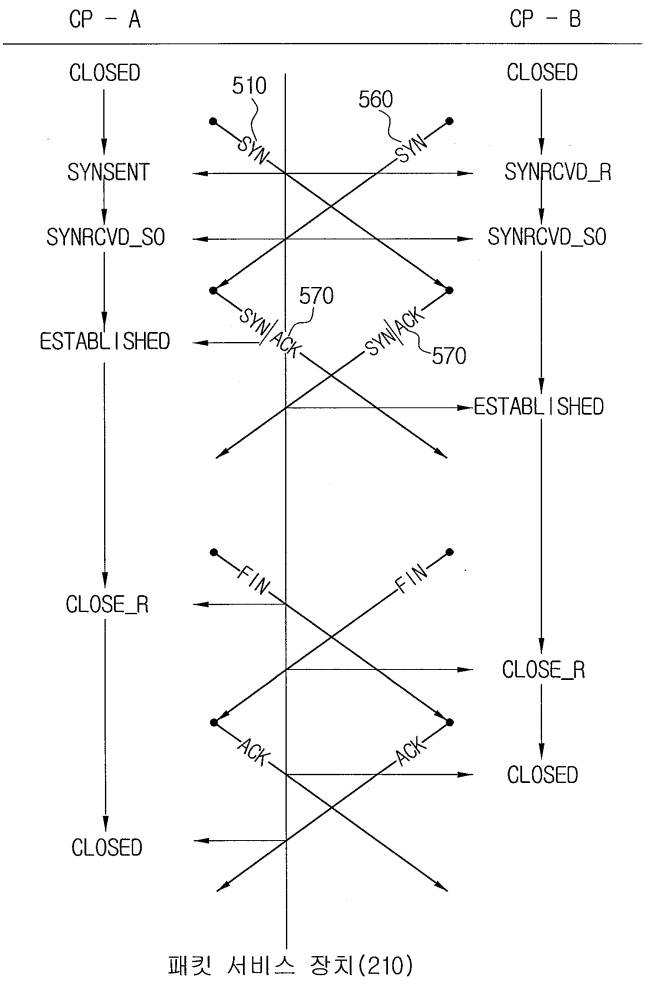
도면5b


수신단(RECEIVER)
CLOSED
SYN
510
SYNRCVD_R
SYNRCVD
ACK
530
ESTABLISHED
SYNSENT
520
SYN | ACK
560
SYN
ESTABLISHED_R
SYN | ACK
SYN
SYNRCVD_SO
550
ACK
CLOSE_R
CLOSE

도면5c


CP - A
CP - B
CLOSED
CLOSED
510
SYN
SYNSENT
SYNRCVD_R
520
SYN | ACK
ESTABLISHED_R
SYNRCVD
530
ACK
ESTABLISHED
ESTABLISHED
540
FIN
CLOSE_R
550
ACK
FIN
CLOSED
CLOSE_R
ACK
CLOSED
패킷 서비스 장치(210)

도면5d


CP - A
CP - B
CLOSED
CLOSED
510
560
SYN
SYN
SYNSENT
SYNRCVD_R
SYNRCVD_SO
SYNRCVD_SO
570
SYN|ACK
SYN|ACK
570
ESTABLISHED
ESTABLISHED
FIN
FIN
CLOSE_R
CLOSE_R
ACK
ACK
CLOSED
CLOSED
패킷 서비스 장치(210)