US 20040090923A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2004/0090923 A1

Kan et al. (43) Pub. Date: May 13, 2004

(54) NETWORK MONITORING SYSTEM RESPONSIVE TO CHANGES IN PACKET ARRIVAL VARIANCE AND MEAN

(76) Inventors: **Chao Kan**, Frisco, TX (US); **Aziz Mohammed**, Plano, TX (US); **Wei Hao**, Richardson, TX (US); **Jimin Shi**, Plano, TX (US)

Correspondence Address:
ALCATEL USA
INTELLECTUAL PROPERTY DEPARTMENT
3400 W. PLANO PARKWAY, MS LEGL2
PLANO, TX 75075 (US)

(21) Appl. No.: **10/412,127**

(22) Filed: **Apr. 11, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/424,495, filed on Nov. 7, 2002.

Publication Classification

(51) **Int. Cl.**[7] **H04J 1/16**

(52) **U.S. Cl.** **370/252**; 370/329

(57) **ABSTRACT**

A network monitoring system **(10)** for monitoring a network along which network traffic flows in a form of packets. The system comprises circuitry **(36, 42)** for receiving a packet communicated along the network and for determining whether the received packet satisfies a set of conditions. The system further comprises circuitry **(36/30, 46)**, responsive to a determination that the received packet satisfies the set, for determining a measure, wherein the measure is determined over a defined time interval and comprises a ratio of packet arrival variance and a mean of packets arriving during the time interval and for comparing the measure to a threshold. Lastly, the system comprises circuitry **(36, 52)**, responsive to the measure exceeding the threshold, for adjusting network resources.

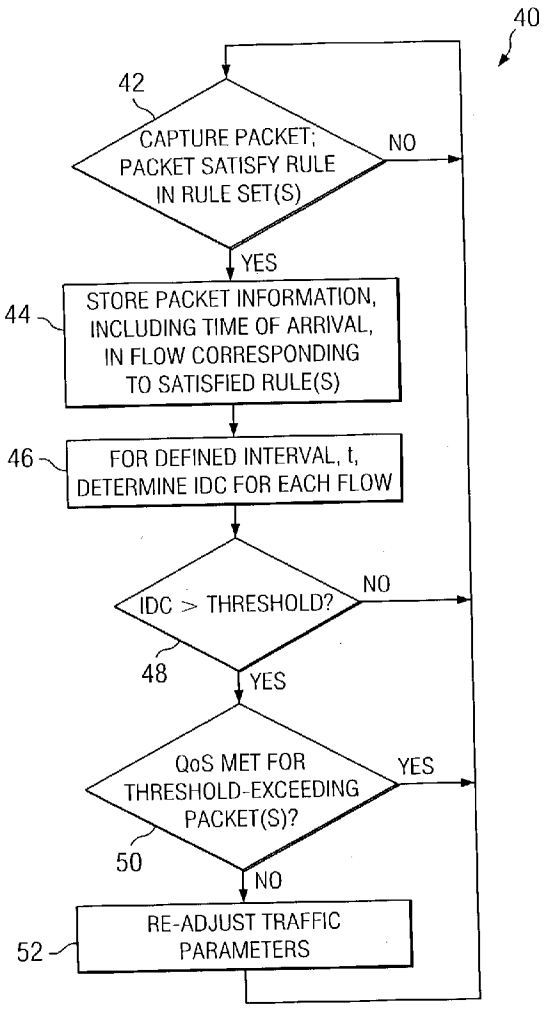


FIG. 1

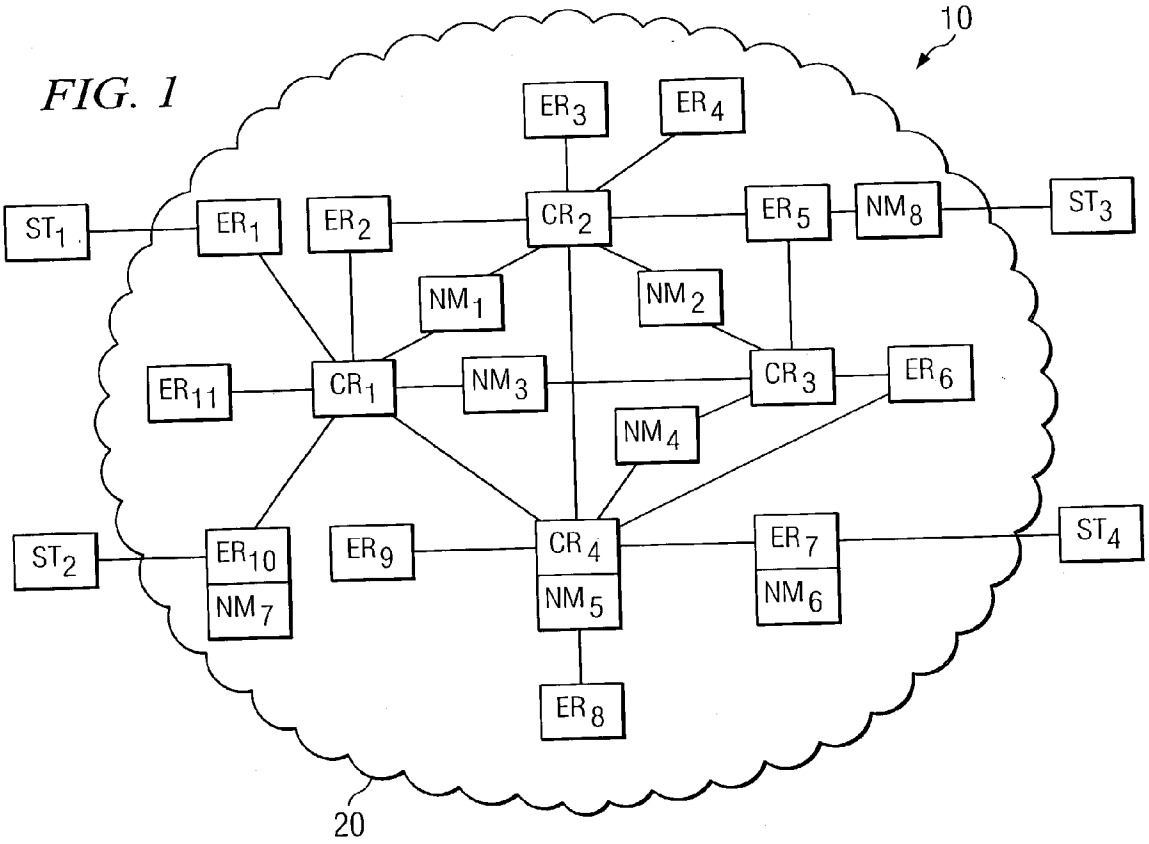
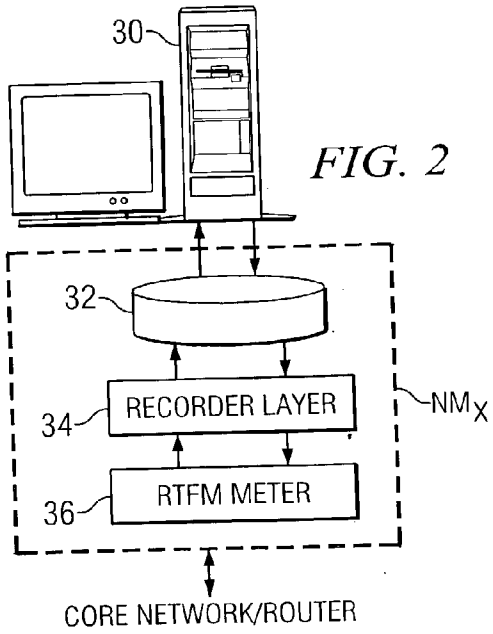


FIG. 2



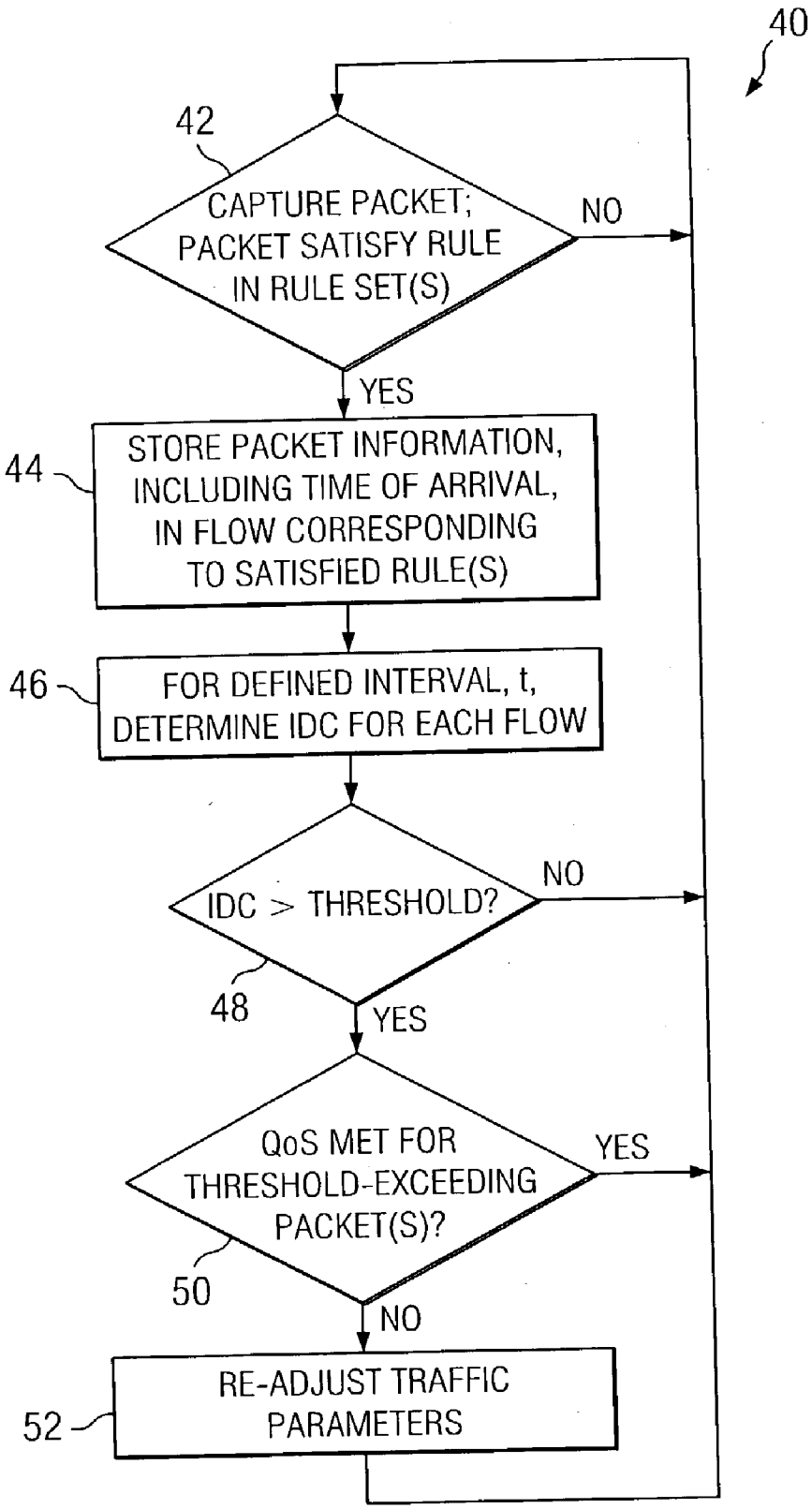


FIG. 3

NETWORK MONITORING SYSTEM RESPONSIVE TO CHANGES IN PACKET ARRIVAL VARIANCE AND MEAN

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit, under 35 U.S.C. §119(e)(1), of U.S. Provisional Application No. 60/424,495, filed Nov. 7, 2002, and incorporated herein by this reference.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable.

BACKGROUND OF THE INVENTION

[0003] The present embodiments relate to computer networks and are more particularly directed to a system for monitoring network performance and correcting network congestion by evaluating changes in packet arrival variance relative to mean packet arrival.

[0004] As the number of users and traffic volume continue to grow on the global Internet and other networks, an essential need has arisen to have a set of mechanisms to monitor network performance and to take corrective measures in response to falling performance. Such performance may be evaluated in various forms, including but not limited to detecting and troubleshooting network congestion. Network congestion results from mismatches between network capacity and network demand. The mismatch may be a long-term one, or at instantaneous time scales. Further, network capacity may appear to be ample when using tools that look at long-term traffic averages; however these approaches are not always suitable because a more subtle problem may arise with short bursts of packets, or peak demand. With congestion analyses mechanisms, the reliability and availability of the network nodes (e.g., IP routers) and the given internet paths can be evaluated. This is especially true for Internet Service Providers ("ISPs") seeking to comply with the Service Level Agreements ("SLAs") that they are now providing to customers. Additionally, such a need is prevalent for the underlying internet protocol ("IP") networks in the Internet.

[0005] The Internet is also evolving towards an advanced architecture that seeks to guarantee the quality of service ("QoS") for real-time applications. QoS permits the controlling of what happens to packets when there is congestion in a network, or more precisely when there is insufficient network capacity to deliver all of the offered load without any noticeable queuing delays. One type of QoS framework seeks to provide hard specific network performance guarantees to applications such as band-width/delay reservations for an imminent or future data flow. Such QoS is usually characterized in terms of ability to guarantee to an application-specified peak and average band-width, delay, jitter and packet loss. Another type is to use Class-of-Service ("CoS") such as Differentiated Services ("Diff-Serv") to represent the less ambitious approach of giving preferential treatment to certain kinds of packets, but without making any performance guarantees.

[0006] During the QoS process to provide services better than the traditional best effort, network congestion detection often becomes the starting point for the network performance analysis. In the past, a number of congestion detection and control schemes have been investigated in data networks. One congestion detection scheme uses the transport-layer protocols to infer congestion from the estimated bottleneck service time or from changes in throughput or end-to-end delay, as well as from packet drops. Specifically, the Internet has traditionally relied on mechanisms in the Transport Control Protocol ("TCP"), such as sliding window control and retransmission timer deficiencies to avoid congestion. TCP operates to seek excess bandwidth by increasing transmission rates until the network becomes congested and then reducing transmission rate once congestion occurs. A few limitations arise from this approach. First, TCP congestion detection at a first node requires an acknowledgement from a second node, that is, the increased transmission is continued until no acknowledgement is received from the second node; thus, a feedback communication is required from another node and that feedback also utilizes bandwidth on the network. Second, in its effort to identify bandwidth, TCP necessarily causes the very congestion which it then seeks to minimize, where the congestion is caused as the TCP increases the bandwidth to a point that exceeds the network capacity. Another type of congestion detection scheme is to involve network components such as routers in the entire process. As most network congestion occurs in routers, they may be considered an ideal position to monitor network load and congestion and respond thereto in a control scheme. Such network-based congestion control uses explicit signaling between routers to provide feedback congestion information to a transmitting router, where the transmitting router may then alter its behavior in response to the feedback, or an overall scheme can change the packet processing within one or more routers so as to reduce congestion. In any event, this latter scheme also requires a form of feedback from a recipient router, thereby increasing traffic on the network to accommodate the feedback and also requiring the reliance of the transmitting router on the integrity of a different router.

[0007] In view of the above, there arises a need to address the drawbacks of the prior art, as is accomplished by the preferred embodiments described below.

BRIEF SUMMARY OF THE INVENTION

[0008] In the preferred embodiment, there is a network monitoring system along which network traffic flows in a form of packets. The system comprises circuitry for receiving a packet communicated along the network and for determining whether the received packet satisfies a set of conditions. The system further comprises circuitry, responsive to a determination that the received packet satisfies the set, for determining a measure and circuitry for comparing the measure to a threshold, wherein the measure is determined over a defined time interval and comprises a ratio of packet arrival variance and a mean of packets arriving during the time interval. Lastly, the system comprises circuitry, responsive to the measure exceeding the threshold, for adjusting network resources.

[0009] Other aspects are also described and claimed.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

[0010] **FIG. 1** illustrates a block diagram of a network system **10** into which the preferred embodiments may be implemented.

[0011] **FIG. 2** illustrates a block diagram of each network monitor NM_1 through NM_8 of **FIG. 1**.

[0012] **FIG. 3** illustrates a flow chart of the operation of each network monitor NM_1 through NM_8 of **FIG. 2**.

DETAILED DESCRIPTION OF THE INVENTION

[0013] **FIG. 1** illustrates a block diagram of a system **10** into which the preferred embodiments may be implemented. System **10** generally includes a number of stations ST_1 through ST_4, each coupled to a network **20** via a router, and each operable to send packets as a source or receive packets as a destination. By way of example, network **20** is an internet protocol ("IP") network such as the global Internet or other IP-using network, where each station and IP networks in general are well known in the art. One skilled in the art should appreciate that the use of the IP protocol is by way of illustration, and many of the various inventive teachings herein may apply to numerous other protocols, including by way of examples asynchronous transfer mode ("ATM"), token ring, Novell, Apple Talk, and still others. In any event, returning to network **20** as an IP network, and also by way of an example, each station ST_x may be constructed and function as one of various different types of computing devices, all capable of communicating according to the IP protocol. Lastly and also by way of example, only four stations ST_x are shown so as to simplify the illustration and example, where in reality each such station may be proximate other stations (not shown) and at a geography located at a considerable distance from the other illustrated stations.

[0014] Continuing with **FIG. 1**, along the outer periphery of network **20** are shown a number of edge routers ER_1 through ER_{11}, while within network **20** are shown a number of core routers CR_1 through CR_4. The terms edge router and core router are known in the art and generally relate to the function and relative network location of a router. Typically, edge routers connect to remotely located networks and handle considerably less traffic than core routers. In addition and due in part to the relative amount of traffic handled by core routers, they tend to perform less complex operations on data and instead serve primarily a switching function; in other words, because of the tremendous amount of throughput expected of the core routers, they are typically hardware bound as switching machines and not given the capability to provide operations based on the specific data passing through the router. Indeed, core routers typically do not include much in the way of control mechanisms as there could be 10,000 or more connections in a single trunk. Further, typically core routers do not involve their operations with TCP related items and instead deal at the IP level and below. In contrast, edge routers are able to monitor various parameters within data packets encountered by the respective router. In any event, the various routers in **FIG. 1** are shown merely by way of example, where one skilled in the art will recognize that a typical network may include quite a different number of both types of routers. Finally, note that each core router CR_x and each edge router ER_x may be constructed and function according to the art, with the exception that preferably selected ones of those routers may include additional functionality for purposes of traffic congestion detection and response based on packet arrival variance and mean as described later. In addition, selected routers may be further constructed to respond to the traffic congestion detection that the router determines as well as in response to the traffic congestion detection of another router in network **20**. Moreover, in one approach, core routers may be configured to respond differently than edge routers in the case of detecting traffic congestion.

[0015] Completing the discussion of **FIG. 1**, note that the various stations, edge routers, and core routers therein are shown connected to one another in various fashions and also by way of example. Such connections are intended to illustrate an example for later discussion of the preferred operation and also to reflect a general depiction of how networks are generally established. Thus, each station ST_x is shown connected to a single edge router ER_x, where that edge router ER_x is connected to one or more core routers CR_x. The core routers CR_x, also by way of example, are shown connected to multiple ones of the other core routers CR_x. By way of reference, the following Table 1 identifies each station and router shown in **FIG. 1** as well as the other device(s) to which each is connected.

TABLE 1

station or router	connected nodes
ST_1	ER_1
ST_2	ER_{10}
ST_3	ER_5
ST_4	ER_7
ER_1	ST_1; CR_1
ER_2	CR_1; CR_2
ER_3	CR_2
ER_4	CR_2
ER_5	ST_3; CR_2; CR_3
ER_6	CR_3; CR_4
ER_7	ST_4; CR_4
ER_8	CR_4
ER_9	CR_4
ER_{10}	ST_2; CR_1
ER_{11}	CR_1
CR_1	ER_1; ER_{11}; ER_{10}; ER_2; CR_2; CR_3; CR_4
CR_2	ER_2; ER_3; ER_4; CR_1; CR_3; CR_4; ER_5
CR_3	ER_5; ER_6; CR_2; CR_1; CR_4
CR_4	ER_7; ER_8; ER_9; CR_1; CR_2; CR_3; ER_6

[0016] Given the various illustrated connections as also set forth in Table 1, in general IP packets flow along the various illustrated paths of network **20**, and in groups or in their entirety such packets are often referred to as network traffic. In this regard and as developed below, the preferred embodiments operate to identify and respond to congestion in such network traffic. Finally, note that **FIG. 1** may represent a simplified version of a network or the Internet in that only a few stations and routers are shown, while one skilled in the art will readily appreciate that the inventive concepts in this document may be applied to a larger number of stations, routers, and the network interconnectivity between those devices.

[0017] **FIG. 1** also illustrates a number of network monitors NM_1 through NM_8 according to the preferred embodi-

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.