US007664048B1

(12) **United States Patent**
Yung et al.

(10) **Patent No.: US 7,664,048 B1**
(45) **Date of Patent: Feb. 16, 2010**

(54) **HEURISTIC BEHAVIOR PATTERN MATCHING OF DATA FLOWS IN ENHANCED NETWORK TRAFFIC CLASSIFICATION**

(75) Inventors: **Weng-Chin Yung**, Folsom, CA (US); **Mark Hill**, Los Altos, CA (US); **Anne Cesa Klein**, Cupertino, CA (US)

(73) Assignee: **Packeteer, Inc.**, Cupertino, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 870 days.

(21) Appl. No.: **10/720,329**

(22) Filed: **Nov. 24, 2003**

(51) **Int. Cl.**
H04L 12/26 (2006.01)

(52) **U.S. Cl.** **370/253**; 370/235; 370/252; 709/224

(58) **Field of Classification Search** 370/223, 370/224, 229, 230, 231, 236.1, 238, 235, 370/253, 252; 709/224, 226, 233, 235, 246
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,914,650	A	4/1990	Sriram	
5,828,846	A	10/1998	Kirby	
6,003,077	A	12/1999	Bawden	
6,023,456	A	2/2000	Chapman	
6,038,216	A *	3/2000	Packer	370/231
6,046,980	A *	4/2000	Packer	370/230
6,122,670	A *	9/2000	Bennett et al.	709/236
6,144,636	A *	11/2000	Aimoto et al.	370/229
6,219,050	B1	4/2001	Schaffer	
6,285,660	B1	9/2001	Ronen	
6,363,056	B1	3/2002	Beigi	
6,397,359	B1	5/2002	Chandra	
6,584,467	B1	6/2003	Haught	
6,591,299	B2 *	7/2003	Riddle et al.	709/224
6,625,648	B1	9/2003	Schwaller	
6,628,938	B1	9/2003	Rachabathuni	
6,681,232	B1	1/2004	Sistanizadeh	
6,690,918	B2	2/2004	Evans	
6,701,359	B1	3/2004	Calabrez	
6,738,352	B1	5/2004	Yamada	
6,798,763	B1	9/2004	Kimura	
6,894,972	B1	5/2005	Phaal	
7,010,611	B1 *	3/2006	Wiryaman et al.	709/232
7,120,931	B1	10/2006	Cheriton	
7,154,416	B1	12/2006	Savage	
7,155,502	B1	12/2006	Galloway	
7,193,968	B1	3/2007	Kapoor	
7,215,637	B1	5/2007	Ferguson	
7,224,679	B2	5/2007	Solomon	

(Continued)

OTHER PUBLICATIONS

Pazos, C.M. et al., "Flow Control and Bandwidth Management in Next Generation Internets" IEEE, Jun. 22, 1998, pp. 123-132.*

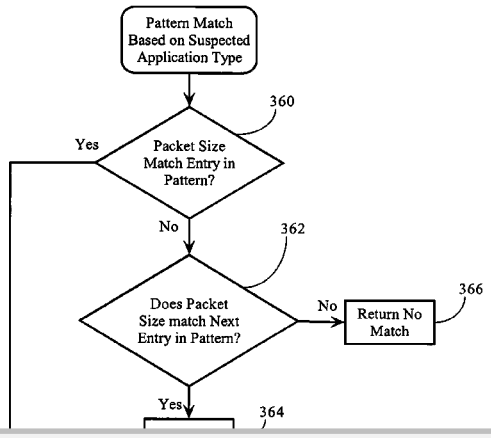
(Continued)

Primary Examiner—Donald L Mills
(74) *Attorney, Agent, or Firm*—Baker Botts L.L.P.

(57) **ABSTRACT**

Methods, apparatuses and systems facilitating enhanced classification of network traffic that extends beyond analysis of explicitly presented packet attributes and holistically analyzes data flows, and in some implementations, related data flows against known application behavior patterns to classify the data flows. Implementations of the present invention facilitate the classification of encrypted or compressed network traffic, or where the higher layer information in the data flows are formatted according to a non-public or proprietary protocol.

31 Claims, 11 Drawing Sheets



U.S. PATENT DOCUMENTS

7,292,531	B1	11/2007	Hill
7,296,288	B1	11/2007	Hill
7,324,447	B1	1/2008	Morford
7,385,924	B1	6/2008	Riddle
7,554,983	B1	6/2009	Muppala
2002/0122427	A1	9/2002	Kamentsky
2002/0143901	A1	10/2002	Lupo
2003/0035385	A1	2/2003	Walsh
2003/0112764	A1	6/2003	Gaspard
2003/0185210	A1	10/2003	McCormack
2004/0125815	A1	7/2004	Shimazu
2006/0045014	A1	3/2006	Charzinski

OTHER PUBLICATIONS

Ye, Guanhua et al., "Using explicit congestion notification in stream control transmisson provided in networks", IEEE, May 19-22, 2003, pp. 704-709.*

Yung, U.S. Appl. No. 10/917,952, entitled: Examination of connection handshake to enhance classification of encrypted network traffic, Aug. 2004.

* cited by examiner

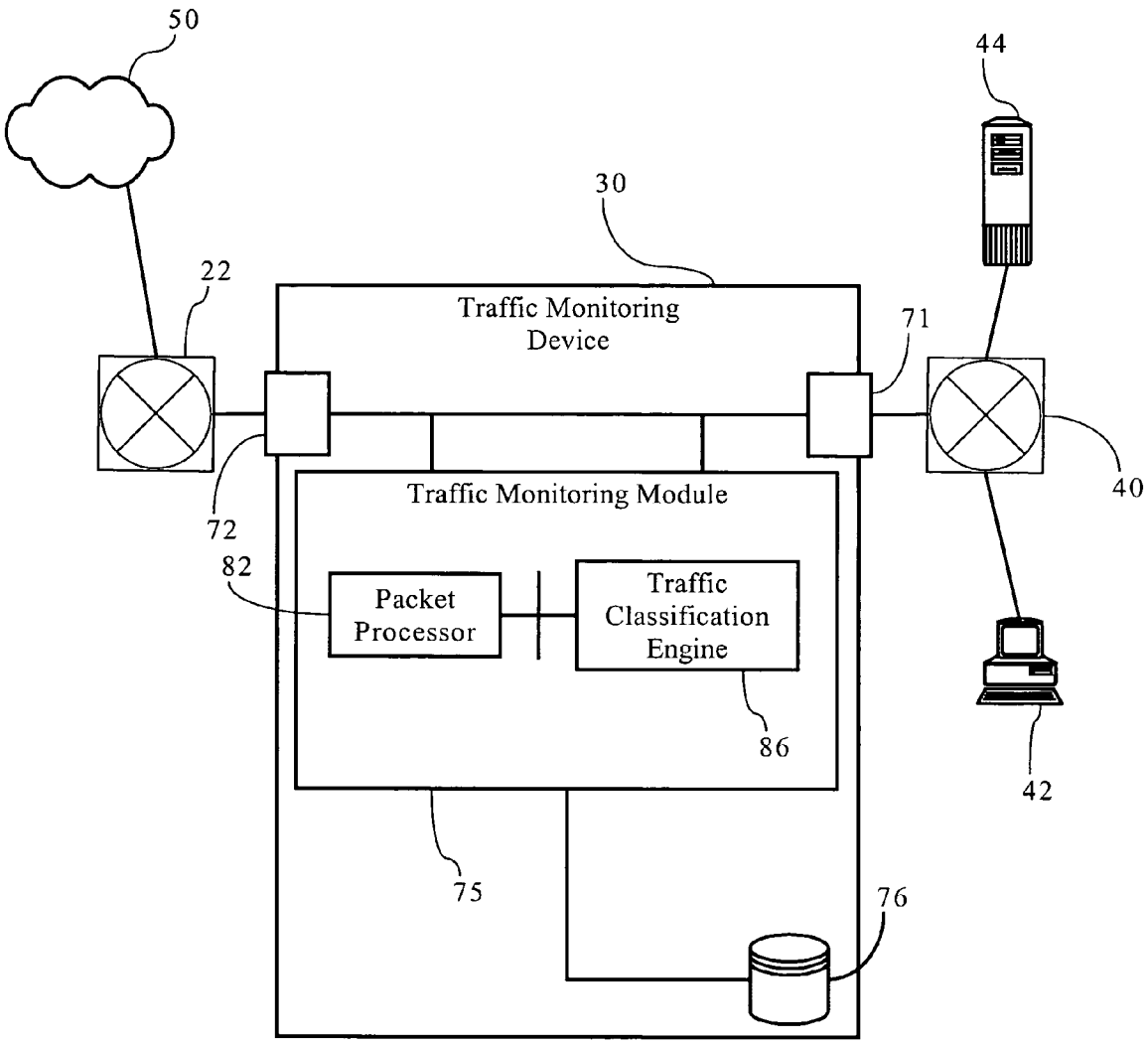


Fig._1

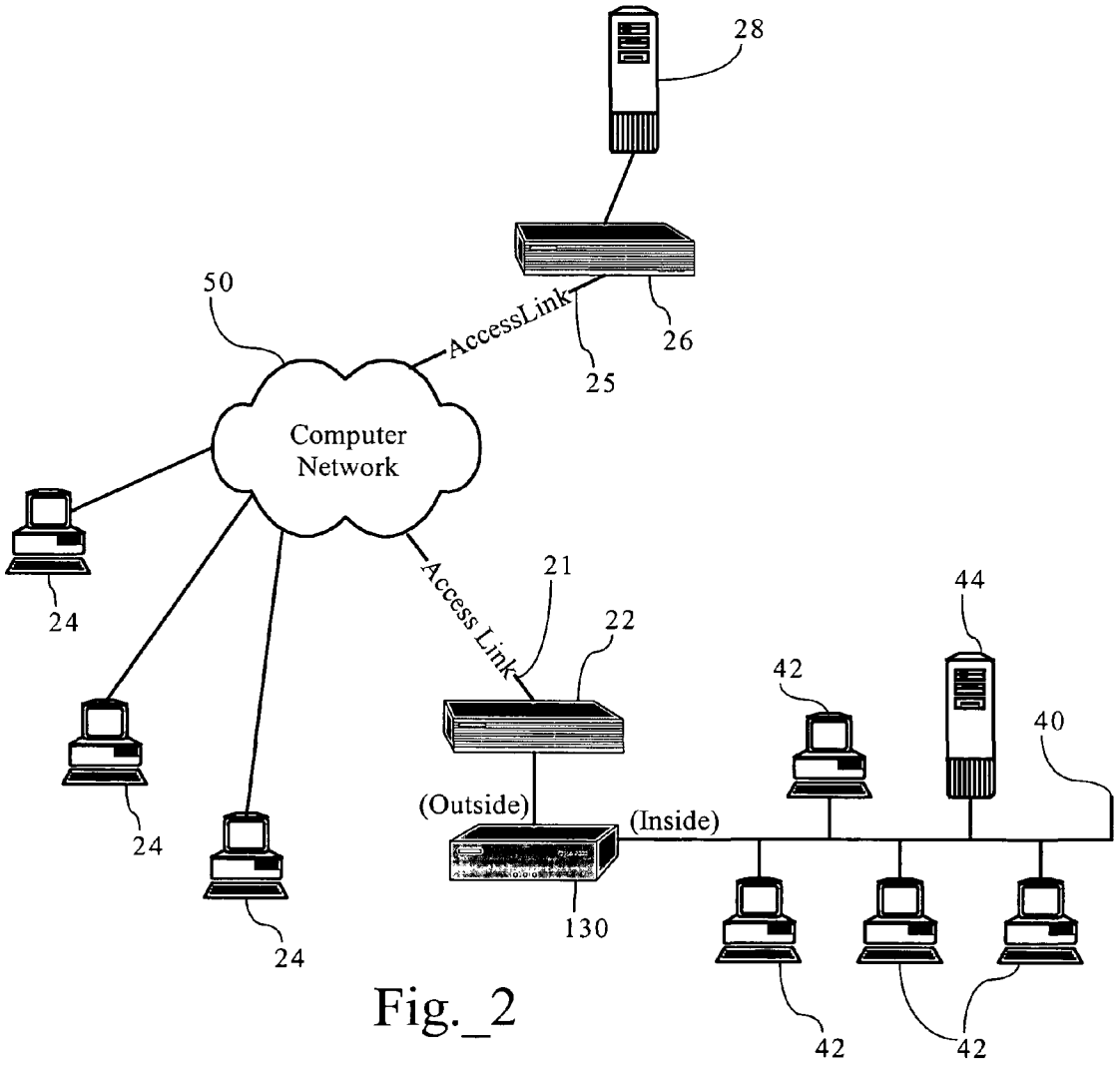


Fig._2

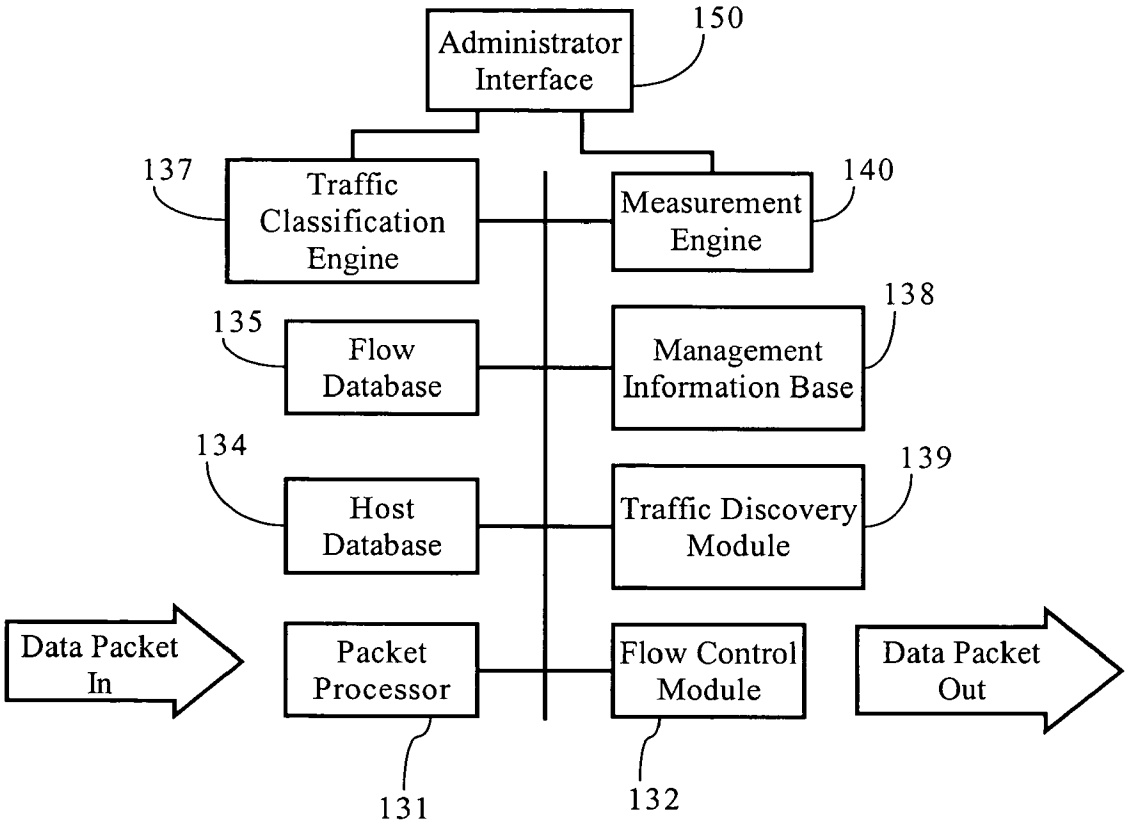


Fig._3

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.