US007185368B2

(12) **United States Patent**
**Copeland, III**

(10) **Patent No.: US 7,185,368 B2**
(45) **Date of Patent: Feb. 27, 2007**

(54) **FLOW-BASED DETECTION OF NETWORK INTRUSIONS**

(75) Inventor: **John A. Copeland, III**, Atlanta, GA (US)

(73) Assignee: **Lancope, Inc.**, Atlanta, GA (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 887 days.

(21) Appl. No.: **10/000,396**

(22) Filed: **Nov. 30, 2001**

(65) **Prior Publication Data**

US 2003/0105976 A1 Jun. 5, 2003

**Related U.S. Application Data**

(60) Provisional application No. 60/265,194, filed on Jan. 31, 2001, provisional application No. 60/250,261, filed on Nov. 30, 2000.

(51) **Int. Cl.**
***G06F 11/30*** (2006.01)

(52) **U.S. Cl.** ..... **726/25**; 726/22; 726/23; 726/26; 713/151; 709/203; 709/224; 709/227; 705/51

(58) **Field of Classification Search** ..... None
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,437,244 | A * | 8/1995 | Van Gilst | 119/73 |
| 5,557,686 | A * | 9/1996 | Brown et al. | 382/115 |
| 5,557,742 | A | 9/1996 | Smaha et al. | |
| 5,621,889 | A | 4/1997 | Lermuzeaux et al. | |
| 5,796,942 | A * | 8/1998 | Esbensen | 713/201 |
| 5,825,750 | A * | 10/1998 | Thompson | 370/244 |
| 5,970,227 | A | 10/1999 | Dayan et al. | |

(Continued)

FOREIGN PATENT DOCUMENTS

WO PCT/US99/29080 6/2000

(Continued)

OTHER PUBLICATIONS

Javitz H S et al.: "The SRI IDES Statistical Anomaly Detector", Proceedings of the Symposium on Research in Security and Privacy US Los Alamitos, IEEE Comp. Soc. Press, v. Symp. 12, pp. 316-326 XP000220803ISBN; 0-8186-2168-0, p. 316, col. 1, line 1, p. 318, col. 1, line 3.*

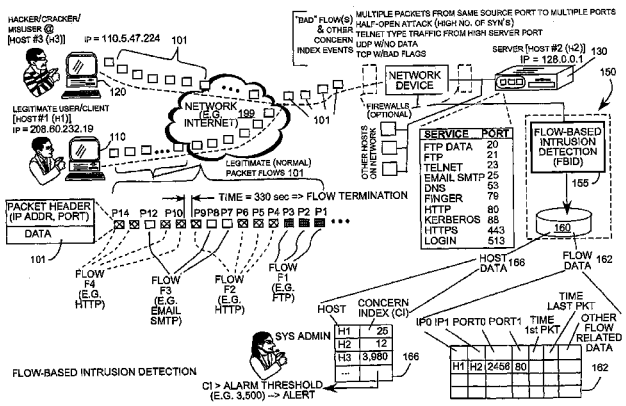
(Continued)

*Primary Examiner*—Nasser Moazzami
*Assistant Examiner*—Ronald Baum
(74) *Attorney, Agent, or Firm*—Morris, Manning & Martin, LLP

(57) **ABSTRACT**

A flow-based intrusion detection system for detecting intrusions in computer communication networks. Data packets representing communications between hosts in a computer-to-computer communication network are processed and assigned to various client/server flows. Statistics are collected for each flow. Then, the flow statistics are analyzed to determine if the flow appears to be legitimate traffic or possible suspicious activity. A concern index value is assigned to each flow that appears suspicious. By assigning a value to each flow that appears suspicious and adding that value to the total concern index of the responsible host, it is possible to identify hosts that are engaged in intrusion activity. When the concern index value of a host exceeds a preset alarm value, an alert is issued and appropriate action can be taken.

**37 Claims, 9 Drawing Sheets**



U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,991,881 | A | 11/1999 | Conklin et al. | |
| 6,119,236 | A * | 9/2000 | Shipley | 713/201 |
| 6,182,226 | B1 | 1/2001 | Reid et al. | |
| 6,275,942 | B1 | 8/2001 | Bernhard et al. | |
| 6,321,338 | B1 | 11/2001 | Porras et al. | |
| 6,363,489 | B1 * | 3/2002 | Comay et al. | 726/22 |
| 6,453,345 | B2 * | 9/2002 | Trcka et al. | 709/224 |
| 6,502,131 | B1 * | 12/2002 | Vaid et al. | 709/224 |
| 6,628,654 | B1 * | 9/2003 | Albert et al. | 370/389 |
| 6,853,619 | B1 * | 2/2005 | Grenot | 370/232 |
| 6,891,839 | B2 * | 5/2005 | Albert et al. | 370/401 |
| 2002/0104017 | A1 * | 8/2002 | Stefan | 713/201 |
| 2002/0133586 | A1 * | 9/2002 | Shanklin et al. | 709/224 |
| 2004/0187032 | A1 * | 9/2004 | Gels et al. | 713/201 |
| 2004/0237098 | A1 * | 11/2004 | Watson et al. | 725/25 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| WO | PCT/US00/29490 | 5/2001 |

OTHER PUBLICATIONS

Lunt T F et al: "Knowledge-based Intrusion Detection", Proceedings of the Annual Artificial Intelligence Systems in Government Conf. US, Washington, IEEE Comp. Soc. Press, vol. Conf. 4, pp. 102-107 XP000040018 p. 102, col. 1, line 1, p. 105, col. 2, line 21.*

Mahoney, M., "Network Traffic Anomaly Detection Based on Packet Bytes", ACM, 2003, Fl. Institute of Technology, entire document, http://www.cs.fit.edu/~mmahoney/paper6.pdf.*

Copeland, John A., et. al., "IP Flow Identification for IP Traffic Carried Over Switched Networks," The International Journal of Computer Telecommunications Networking Computer Networks 31 (1999), pp. 493-504.

Cooper, Mark "An Overview of Intrusion Detection Systems," Zinetica White Paper, (www.xinetica.com) Nov. 19, 2001.

Newman, P., et. al. "RFC 1953: Ipsilon Flow Management Protocol Specification for IPv4 Version 1.0" (www.xyweb.com/rfc/rfc1953.html) May 19, 1999.

Paxson, Vern, "Bro: A System for Detecting Network Intruders in Real-Time," 7th USENIX Security Symposium, Lawrence Berkkeley National Laboratory, San Antonio, TX Jan. 26-29, 1998.

Mukherjee, Biswanath, et. al., "Network Intrusion Detection," IEEE Network, May/Jun. 1994.

"Network-vs Host-Based Intrusion Detection: A Guide to Intrusion Detection," ISS Internet Security Systems, Oct. 2, 1998, Atlanta, GA.

Barford, Paul, et. al. "Characteristics of Network Traffic Flow Anomalies," ACM SIGCOMM Internet Measurement Workshop 2001 (http://www.cs.wisc.edu/pb/ublications.html) Jul. 2001.

Frincke, Deborah, et. al., "A Framework for Cooperative Intrusion Detection" 21st National Information Systems Security Conference, Oct. 1998, Crystal City, VA.

Phrack Magazine, vol. 8, Issue 53, Jul. 8, 1998, Article 11 of 15.

"LANSleuth Fact Sheet," LANSleuth LAN Analyzer for Ethernet and Token Ring Networks, (www.lansleuth.com/features.html), Aurora, Illinois.

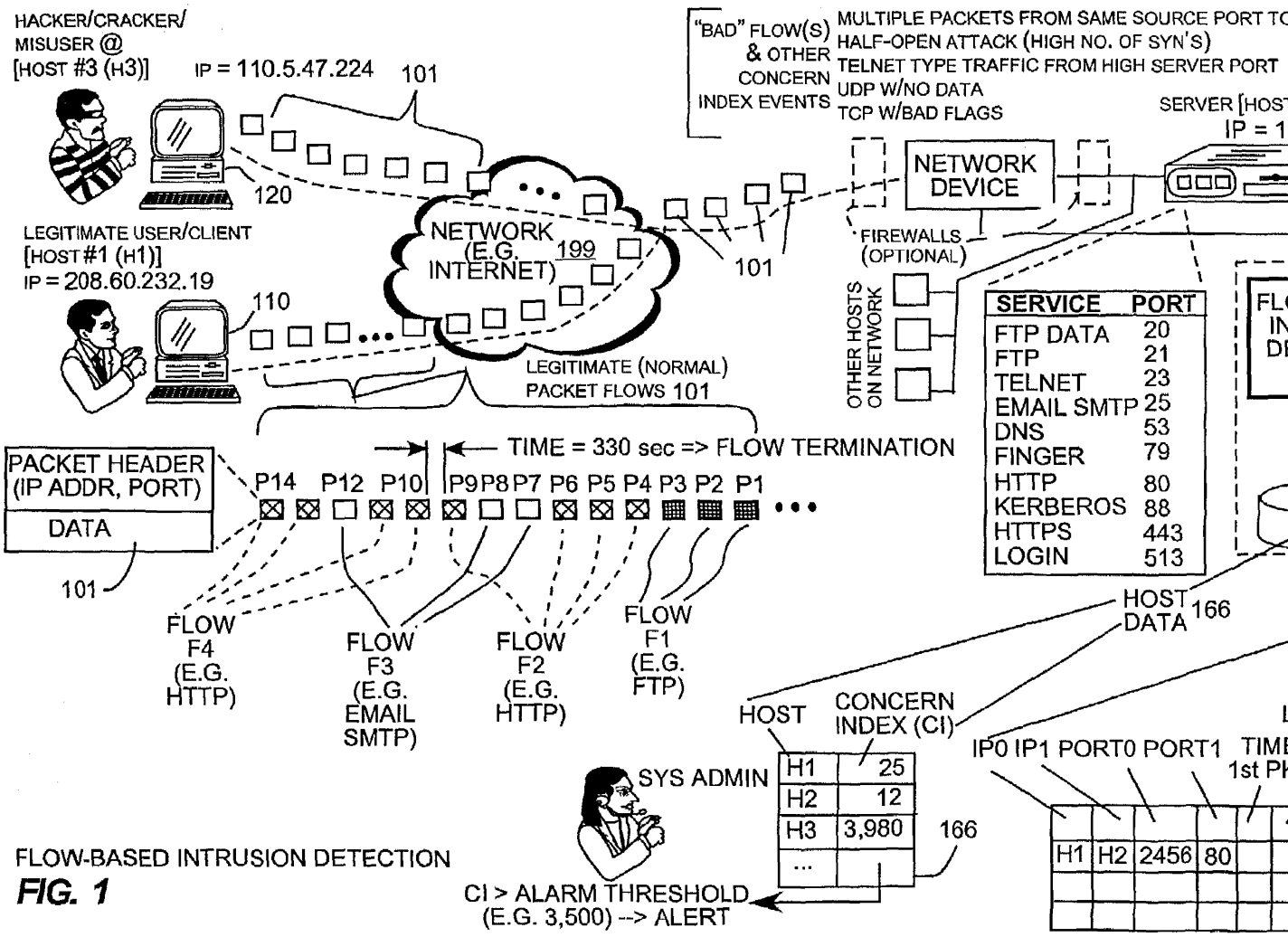
"LANSleuth General Features," (www.lansleuth.com/features.html), Aurora, Illinois.

Copeland, John A., et al, "IP Flow Identification for IP Traffic Carried Over Switched Networks," The International Journal of Computer and Telecommunications Networking Computer Networks 31 (1999), pp. 493-504.

Cooper, Mark "An Overview of Instrusion Detection Systems," Xinetica White Paper, (www.xinetica.com) Nov. 19, 2001.

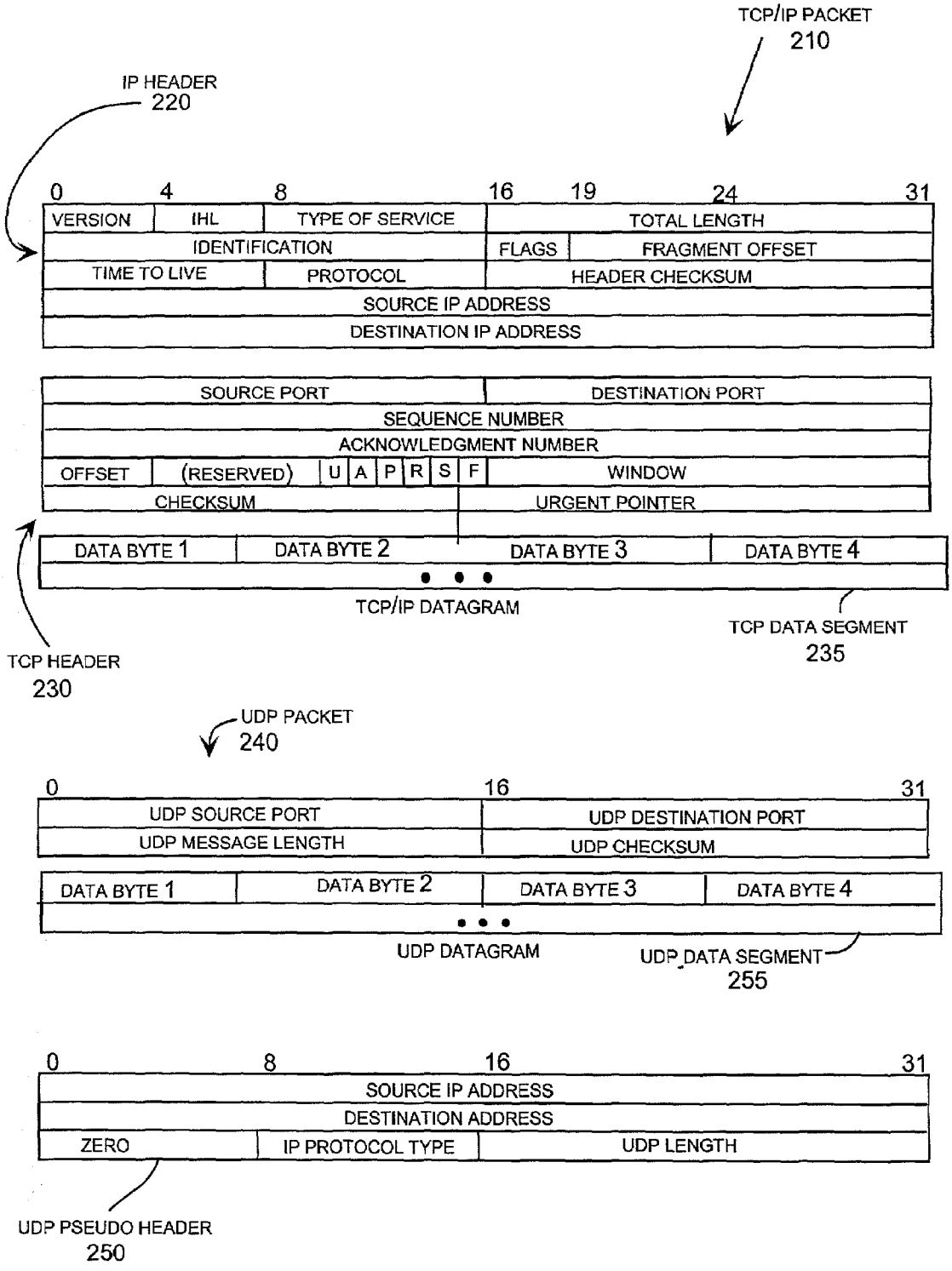
Newman, P., et al. "RFC 1953: Ipsilon Flow Management Protocol Specificaiton for IPv4 Version 1.0" (www.xyweb.com/rfc/rfc1953.html) May 19, 1999.

* cited by examiner




FLOW-BASED INTRUSION DETECTION

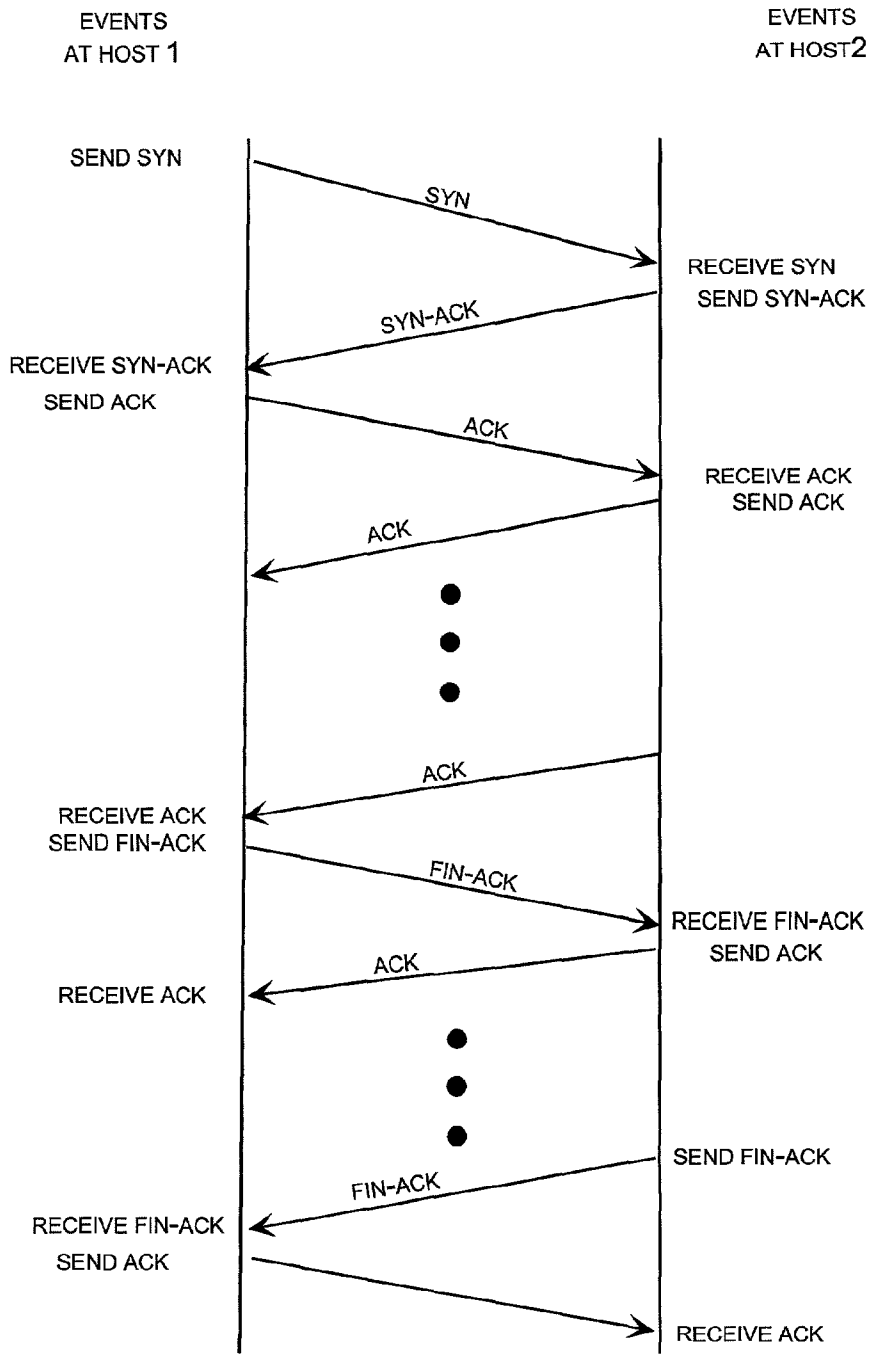
***FIG. 1***




PACKET HEADERS

*FIG. 2*

TCP/IP SESSION
300



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.