US010652111B2

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

(10) **Patent No.: US 10,652,111 B2**
(45) **Date of Patent: May 12, 2020**

(54) **METHOD AND SYSTEM FOR DEEP PACKET INSPECTION IN SOFTWARE DEFINED NETWORKS**

(71) Applicant: **ORCKIT IP, LLC**, Newton, MA (US)

(72) Inventors: **Yossi Barsheshet**, Ashdod (IL); **Simhon Doctori**, Gan-Yavne (IL); **Ronen Solomon**, Ranat-Gan (IL)

(73) Assignee: **ORCKIT IP, LLC**, Dover, DE (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 306 days.

(21) Appl. No.: **15/126,288**

(22) PCT Filed: **Apr. 21, 2015**

(86) PCT No.: **PCT/US2015/026869**
§ 371 (c)(1),
(2) Date: **Sep. 15, 2016**

(87) PCT Pub. No.: **WO2015/164370**
PCT Pub. Date: **Oct. 29, 2015**

(65) **Prior Publication Data**

US 2017/0099196 A1 Apr. 6, 2017

Related U.S. Application Data

(60) Provisional application No. 61/982,358, filed on Apr. 22, 2014.

(51) **Int. Cl.**
H04L 12/26 (2006.01)
H04L 12/64 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 43/028*** (2013.01); ***H04L 12/6418*** (2013.01); ***H04L 43/026*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC . H04L 43/026; H04L 12/6418; H04L 43/028; H04L 49/70; H04L 69/161
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

2010/0208590 A1* 8/2010 Dolganow H04L 43/026 370/235
2010/0212006 A1 8/2010 Dolganow et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 2672668 A1 12/2013

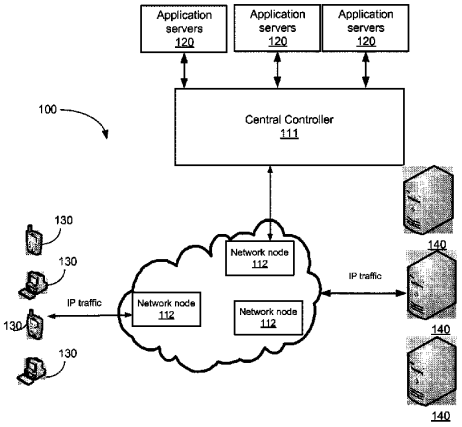
OTHER PUBLICATIONS

Supplementary Search Report of EP 15783292 dated Nov. 7, 2017.
(Continued)

Primary Examiner — Jae Y Lee
Assistant Examiner — Jean F Voltaire
(74) *Attorney, Agent, or Firm* — May Patents Ltd. c/o Dorit Shem-Tov

(57) **ABSTRACT**

A method for deep packet inspection (DPI) in a software defined network (SDN). The method includes configuring a plurality of network nodes operable in the SDN with at least one probe instruction; receiving from a network node a first packet of a flow, the first packet matches the at least one probe instruction and includes a first sequence number; receiving from a network node a second packet of the flow, the second packet matches the at least one probe instruction and includes a second sequence number, the second packet is a response of the first packet; computing a mask value respective of at least the first and second sequence numbers indicating which bytes to be mirrored from subsequent packets belonging to the same flow; generating at least one
(Continued)



mirror instruction based on at least the mask value; and configuring the plurality of network nodes with at least one mirror instruction.

54 Claims, 6 Drawing Sheets

(51) **Int. Cl.**
H04L 12/851 (2013.01)
H04L 12/931 (2013.01)
H04L 29/06 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 47/2483*** (2013.01); ***H04L 49/70*** (2013.01); ***H04L 69/161*** (2013.01)

(58) **Field of Classification Search**
USPC 370/389
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

2011/0264802 A1 10/2011 Dolganow et al.
2013/0329764 A1 12/2013 Chesla et al.
2014/0052836 A1* 2/2014 Nguyen H04L 45/306 709/223
2015/0124812 A1* 5/2015 Agarwal H04L 45/24 370/392
2016/0020998 A1* 1/2016 Bifulco H04L 45/64 370/235
2016/0197831 A1* 7/2016 De Foy H04L 45/7453 370/392
2016/0219080 A1* 7/2016 Huang H04L 63/20

OTHER PUBLICATIONS

Seugwon Shin et al, "Fresco: Modular Composable Security Services for Software-Defined Networks", NDSS Symposium 2013, Apr. 23, 2013, pp. 1-16 XP055422187.
International Search Report of PCT/US2015/026869 dated Aug. 6, 2015.
Minlan Yu et al, "Scalable flow-based networking with DIFANE", Proceedings of the ACM SIGCOMM 2010 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, New Delhi, India, Aug. 30-Sep. 3, 2010, ACM, pp. 351-362 XP058189957.

* cited by examiner

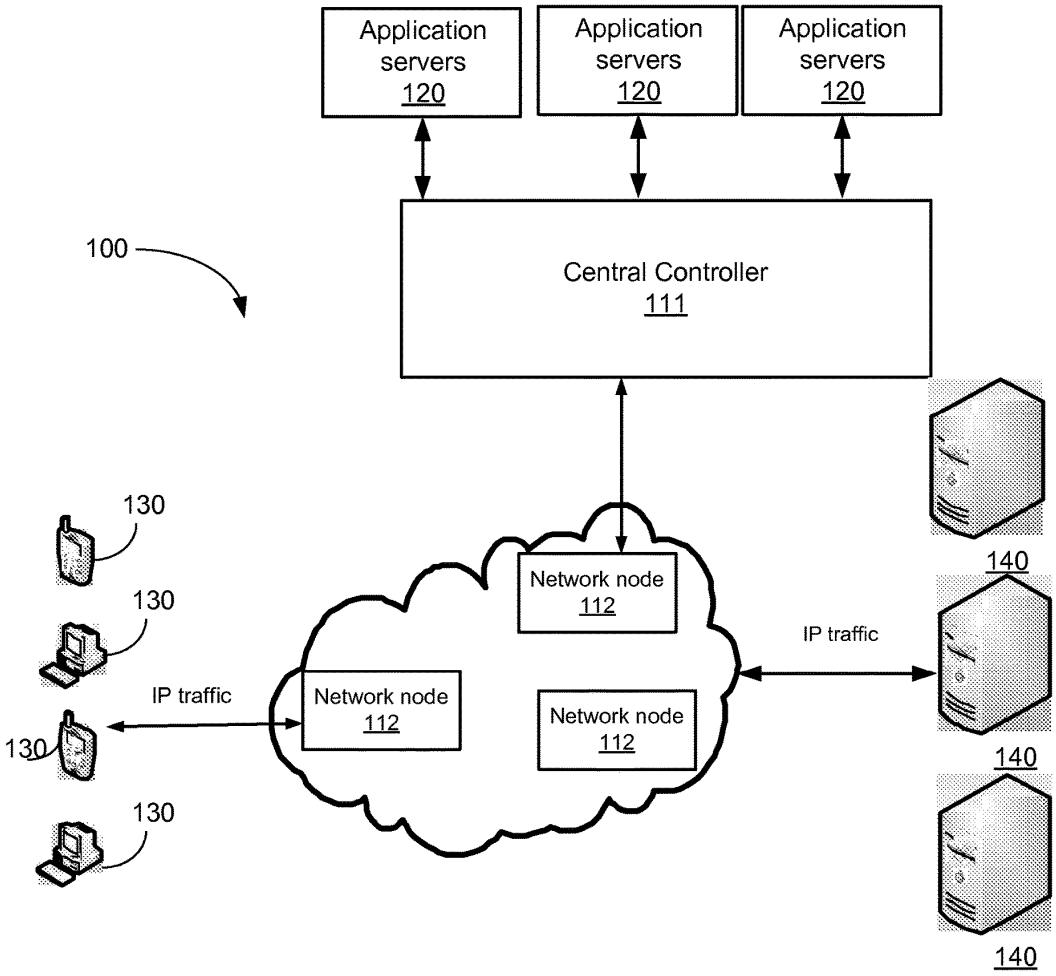


FIG. 1

200

KEY **210**					DATA **220**								
Client IP address	Server IP address	Client source TCP port	Server destination TCP port	IP protocol number	Flow ID	Client→ Server sequence number M	Server→ Client sequence number N	state	Creation timestamp	Client→ Server Hit counter X [bytes]	Server → Client Hit counter Y [bytes]	Client→ Server data buffer	S C b
192.1.1.1	209.1.4.4	15431	21	6	1	0xf46d5c34	0x3c98b9ab	ACK	15:32:13				

FIG. 2

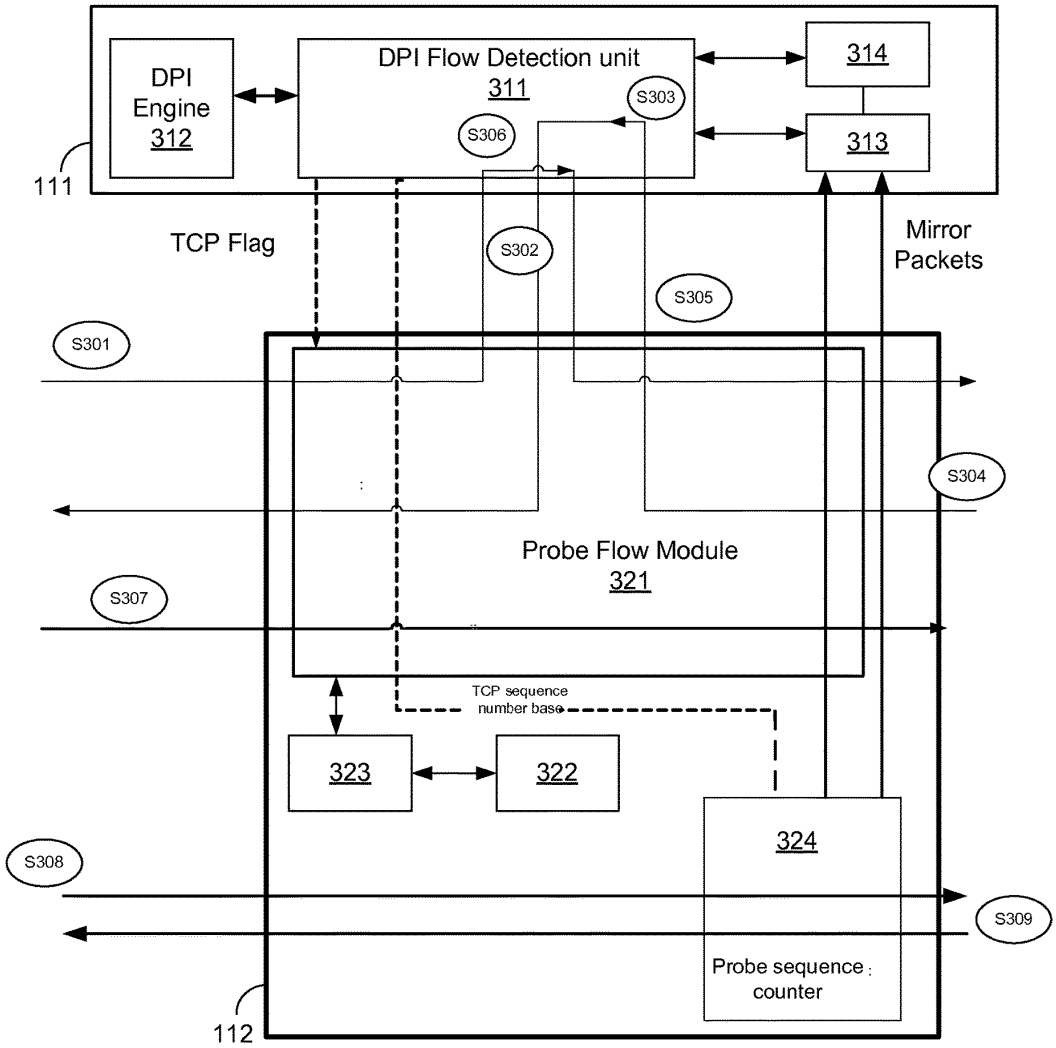


FIG. 3

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.