US008693348B1

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

(10) **Patent No.: US 8,693,348 B1**
(45) **Date of Patent: Apr. 8, 2014**

(54) **SYSTEMS AND METHODS FOR CONTENT TYPE CLASSIFICATION**

(71) Applicant: **Fortinet, Inc.**, Sunnyvale, CA (US)

(72) Inventors: **Shaohong Wei**, Sunnyvale, CA (US); **Zhong Qiang Chen**, Sunnyvale, CA (US); **Ping Ng**, Milpitas, CA (US); **Gang Duan**, San Jose, CA (US)

(73) Assignee: **Fortinet, Inc.**, Sunnnyvale, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **14/087,847**

(22) Filed: **Nov. 22, 2013**

Related U.S. Application Data

(63) Continuation of application No. 13/795,283, filed on Mar. 12, 2013, which is a continuation of application No. 13/409,141, filed on Mar. 1, 2012, now Pat. No. 8,639,752, which is a continuation of application No. 12/503,100, filed on Jul. 15, 2009, now Pat. No. 8,204,933, which is a continuation of application No. 11/357,654, filed on Feb. 16, 2006, now Pat. No. 7,580,974.

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

(52) **U.S. Cl.**
CPC ***H04L 43/18*** (2013.01)
USPC **370/241**

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

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,361,379	A	11/1994	White	
6,157,955	A	12/2000	Narad et al.	
6,608,816	B1	8/2003	Nichols	
6,665,725	B1	12/2003	Dietz et al.	
7,006,502	B2	2/2006	Lin	
7,082,102	B1	7/2006	Wright	
7,095,715	B2	8/2006	Buckman et al.	
7,242,681	B1 *	7/2007	Van Bokkelen et al.	370/389
7,420,992	B1	9/2008	Fang et al.	
7,580,974	B2	8/2009	Wei et al.	
7,945,522	B2	5/2011	Mcgovern et al.	
8,204,933	B2	6/2012	Wei et al.	
8,639,752	B2	1/2014	Wei et al.	
2003/0012147	A1	1/2003	Buckman et al.	
2004/0002930	A1	1/2004	Oliver et al.	
2004/0261016	A1	12/2004	Glass et al.	
2005/0249125	A1 *	11/2005	Yoon et al.	370/252
2006/0112043	A1	5/2006	Oliver et al.	
2006/0229902	A1	10/2006	Mcgovern et al.	
2006/0239273	A1	10/2006	Buckman et al.	
2007/0192481	A1	8/2007	Wei et al.	
2008/0052326	A1	2/2008	Evanchik et al.	
2009/0268617	A1	10/2009	Wei et al.	

(Continued)

OTHER PUBLICATIONS

"U.S. Appl. No. 11/357,654, 312 Amendment filed Jun. 23, 2009", 5 pgs.

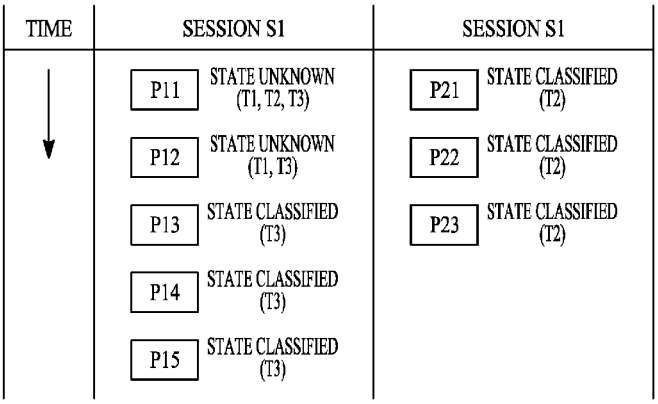
(Continued)

Primary Examiner — Kevin C Harper
(74) *Attorney, Agent, or Firm* — Schwegman Lundberg & Woessner, P.A.

(57) **ABSTRACT**

Various embodiments illustrated and described herein include systems, methods and software for content type classification. Some such embodiments include determining a potential state of classification for packets associated with a session based at least in part on a packet associated with the session that is a packet other than the first packet of the session.

20 Claims, 7 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2012/0023557	A1*	1/2012	Bevan et al.	726/4
2012/0163186	A1	6/2012	Wei et al.	
2013/0258863	A1	10/2013	Wei et al.	

OTHER PUBLICATIONS

"U.S. Appl. No. 11/357,654, Non-Final Office Action mailed Sep. 18, 2008", 10 pgs.
"U.S. Appl. No. 11/357,654, Notice of Allowance mailed Mar. 23, 2009", 10 pgs.
"U.S. Appl. No. 11/357,654, Response filed Dec. 18, 2008 to Non-Final Office Action mailed Sep. 18, 2008", 8 pgs.
"U.S. Appl. No. 11/357,654, Response to Rule 312 Communication mailed Jul. 23, 2009", 2 pgs.
"U.S. Appl. No. 12/503,100, Final Office Action mailed Jun. 9, 2011", 12 pgs.
"U.S. Appl. No. 12/503,100, Non-Final Office Action mailed Oct. 18, 2010", 12 pgs.
"U.S. Appl. No. 12/503,100, Notice of Allowance mailed Feb. 17, 2012", 13 pgs.
"U.S. Appl. No. 12/503,100, Response Filed Feb. 9, 2012 to Final Office Action Jun. 9, 2011", 8 pgs.
"U.S. Appl. No. 12/503,100, Response filed Mar. 18, 2011 to Non Final Office Action mailed Oct. 18, 2010", 10 pgs.
"U.S. Appl. No. 12/503,100, Supplemental Notice of Allowability mailed Apr. 25, 2012", 9 pgs.
"U.S. Appl. No. 13/409,141, Non Final Office Action mailed Aug. 8, 2013", 6 pgs.
"U.S. Appl. No. 13/409,141, Notice of Allowance mailed Sep. 18, 2013", 9 pgs.
"U.S. Appl. No. 13/409,141, Response filed Sep. 3, 2013 to Office Action mailed Aug. 8, 2013", 5 pgs.
"Application U.S. Appl. No. 13/409,141, Supplemental Notice of Allowability mailed Dec. 20, 2013", 5 pgs.

* cited by examiner

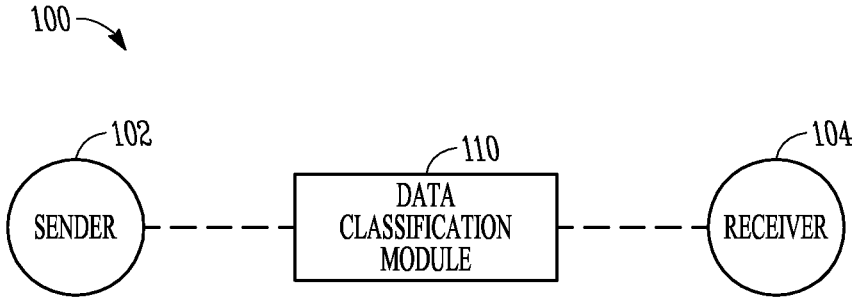


FIG. 1

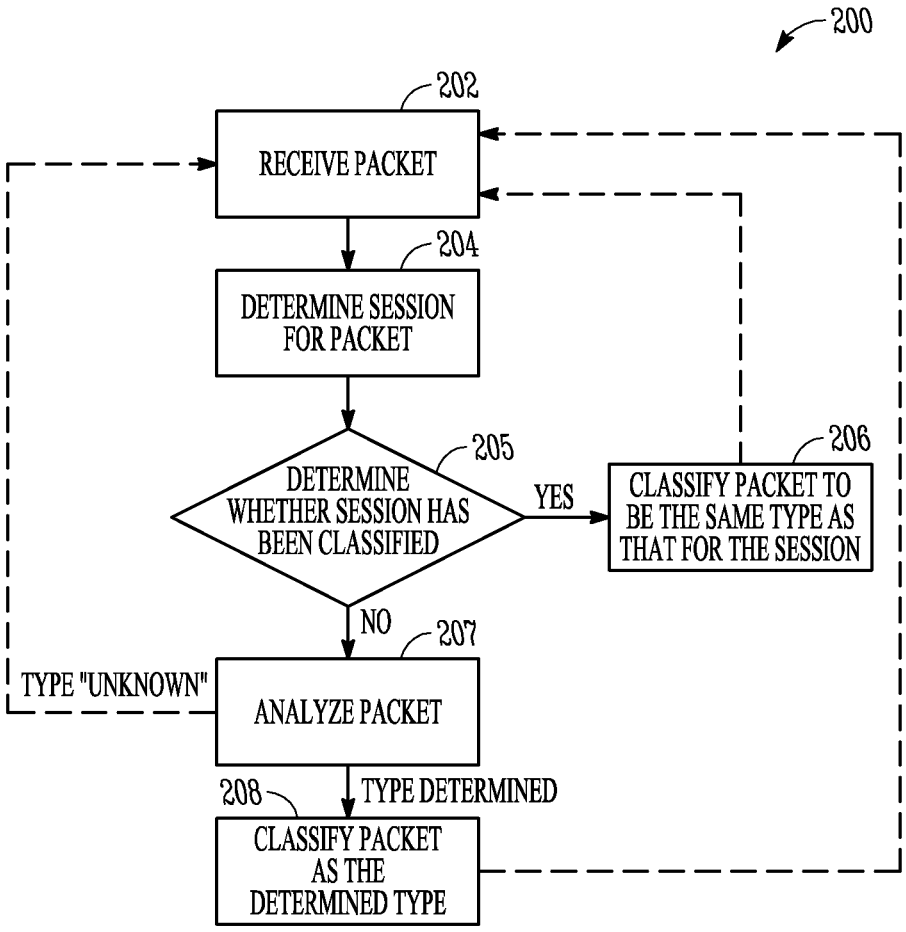


FIG. 2

Example 1: TCP traffic

#	direction	packet_size	port	using proxy	(p,s) matchs skype
1	C --> S	14	!80/!443	no	unknown
2	S --> C	28-36	!80/!443	no	unknonwn
3	C --> S	14	!80/!443	no	Yes (confirm)

FIG. 3A

Example 2: TCP traffic

#	direction	packet_size	port	using proxy	(p,s) matchs skype
1	C --> S	16	80	no	unknown
2	S --> C	14	80	no	unknown
3	C --> S	28-36	80	no	unknown
4	S --> C	14	80	no	Yes

FIG. 3B

Example 3: TCP traffic

#	direction	packet_size	port	using proxy	pattern	(p,s) mat
1	C --> S	72	443	no	|80 46 01 03 01 00 2d|	unknown
2	S --> C	93	443	no	|16 03 01 00 4a 02|	unknown
3	C --> S	14	443	no	N/A	yes (co

FIG. 3C

Example 4: UDP traffic:

#	direction	packet_size	port	pattern(3rd byte)	(p,s) matchs s
1	C --> S	18/27	>1024	0x02	unknown
2	S --> C	>10	>1024	0x02/0x07	yes

FIG. 3D

Example 5: normal Yahoo login, through port 80
protocol: TCP; client (C): 192.168.5.186:1734; server (S): 216.155.193.1

#	direction	pattern	classifier(p,s, yahoo)
1	C --> S	|YMSG| + ver_number + pkt_len test	session is Yahoo! candidate However, without server_side packet, the classifier returns "unknown"
2	S --> C	|YMSG| + ver_num	Confirmed. The content type is marked as Yahoo!

FIG. 3E

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.