(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 November 2013 (21.11.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/173000 A3

(51) International Patent Classification:
G06N 5/04 (2006.01)

(21) International Application Number:
PCT/US2013/035943

(22) International Filing Date:
10 April 2013 (10.04.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/646,590	14 May 2012 (14.05.2012)	US
61/683,274	15 August 2012 (15.08.2012)	US
61/748,217	2 January 2013 (02.01.2013)	US
13/773,247	21 February 2013 (21.02.2013)	US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; Attn: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121 (US).

(72) Inventors: **GUPTA, Rajarshi**; 5775 Morehouse Drive, San Diego, California 92121 (US). **WEI, Xuetao**; 5775 Morehouse Drive, San Diego, California 92121 (US). **GATHALA, Anil**; 5775 Morehouse Drive, San Diego, California 92121 (US). **SRIDHARA, Vinay**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agent: **COLE, Nicholas Albert**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

[Continued on next page]

(54) Title: ON-DEVICE REAL-TIME BEHAVIOR ANALYZER

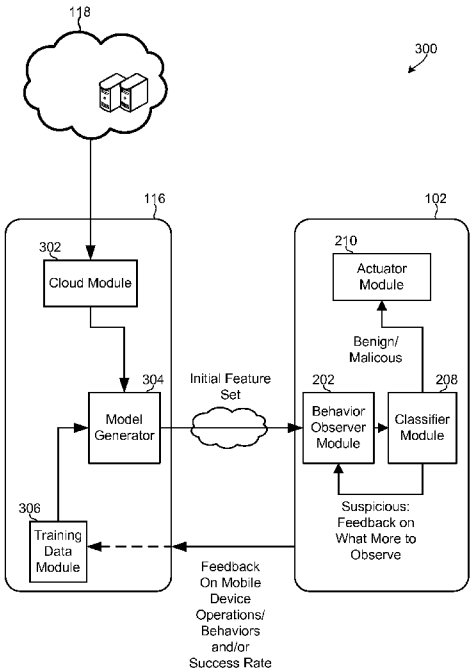

FIG. 3

(57) Abstract: Methods, systems and devices for generating data models in a communication system may include applying machine learning techniques to generate a first family of classifier models using a boosted decision tree to describe a corpus of behavior vectors. Such behavior vectors may be used to compute a weight value for one or more nodes of the boosted decision tree. Classifier models factors having a high probably of determining whether a mobile device behavior is benign or not benign based on the computed weight values may be identified. Computing weight values for boosted decision tree nodes may include computing an exclusive answer ratio for generated boosted decision tree nodes. The identified factors may be applied to the corpus of behavior vectors to generate a second family of classifier models identifying fewer factors and data points relevant for enabling the mobile device to determine whether a behavior is benign or not benign.

WO 2013/173000 A3

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
9 January 2014

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/035943

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06N5/04
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	A. SHABTAI: "Malware detection on mobile devices", PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON MOBILE DATA MANAGEMENT (MDM'2010), 23 May 2010 (2010-05-23), pages 289-290, XP031692994, DOI: 10.1109/MDM.2010.28 the whole document ----- -/--	1-27

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 October 2013	07/11/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Douarche, Nicolas

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/035943

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Y.-B. LU, S.-C. DIN, C.-F. ZHENG, B.-J. GAO: "Using multi-feature and classifier ensembles to improve malware detection", JOURNAL OF CHUNG CHENG INSTITUTE OF TECHNOLOGY, vol. 39, no. 2, November 2010 (2010-11), pages 57-72, XP55086345, ISSN: 0255-6030 the whole document ----	1-27
X	P. NATESAN, P. BALASUBRAMANIE: "Design of two stage filter using enhanced adaboost for improving attack detection rates in network intrusion detection", INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY & SECURITY, vol. 2, no. 2, April 2012 (2012-04), pages 349-358, XP55086347, ISSN: 2249-9555 the whole document ----	1-27