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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 December 2013 (12.12.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/184211 A3

(51) International Patent Classification:
G06F 11/00 (2006.01)

(21) International Application Number:
PCT/US2013/031463

(22) International Filing Date:
14 March 2013 (14.03.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/614,148 22 March 2012 (22.03.2012) US

(71) Applicants: **LOS ALAMOS NATIONAL SECURITY, LLC** [US/US]; Los Alamos National Laboratory, LC/IP MS A187, Los Alamos, NM 87545 (US). **IMPERIAL INNOVATIONS LIMITED** [GB/GB]; 52 Princes Gate, Exhibition Road, London SW7 2PG (GB).

(72) Inventors: **NEIL, Joshua, Charles**; 137 Freelove Lane, Jemez Springs, NM 87025 (US). **TURCOTTE, Melissa**; 93 Chandos Avenue, Whetstone, London N20 9EG (GB). **HEARD, Nicholas, Andrew**; 1 Springshaw Close, Sevenoaks, Kent TN13 2QE (GB).

(74) Agents: **LEONARD II, Michael, A.** et al.; LeonardPatel PC, 218 North Lee Street, Suite 320, Alexandria, VA 22314 (US).

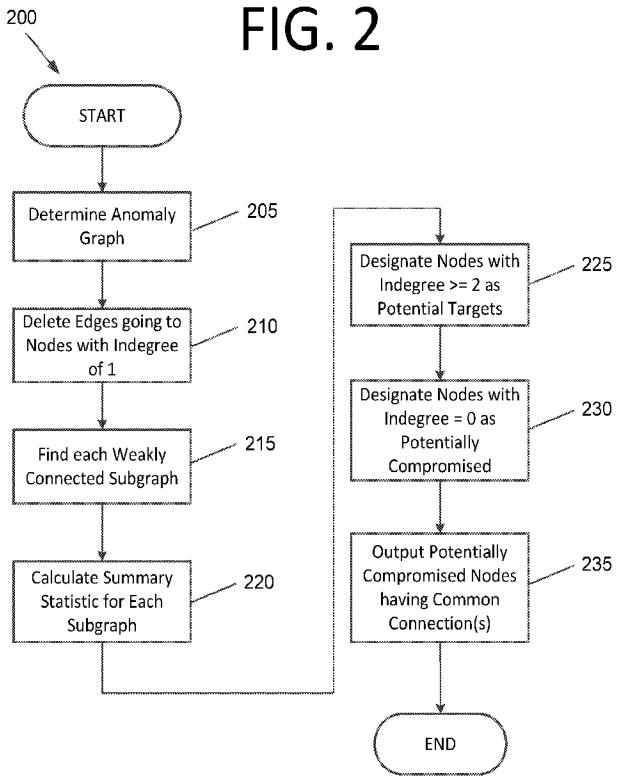
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, 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,

[Continued on next page]

(54) Title: ANOMALY DETECTION TO IDENTIFY COORDINATED GROUP ATTACKS IN COMPUTER NETWORKS

FIG. 2



(57) Abstract: Systems, apparatuses, methods, and computer programs for detecting anomalies to identify coordinated group attacks on computer networks are provided. An anomaly graph of a network including nodes, edges, and an indegree of the nodes in the anomaly graph may be determined. Nodes with an indegree of at least two may be designated as potential targets. Nodes with no incoming connections may be designated as potentially compromised nodes. The designated potentially compromised nodes may be outputted as potentially associated with a coordinated attack on the network when the potentially compromised nodes connect to one or more of the same potential target nodes.

WO 2013/184211 A3

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

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

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:
13 March 2014

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 13/31463

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/00 (2013.01)
USPC - 726/23
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)
IPC (8) - G06F 11/00 (2013.01)
USPC - 726/23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 709/224, 714/26, 714/37, 714/38.14, 714/39, 714/47.1, 714/E11.029, 726/25 (See keywords below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Thomsoninnovation.com; Patbase; Google Scholar; Google Patents; Google.com; Freepatentsonline; ProQuest Dialog
Search Terms: Network, graph, tree, map, node, vertex, edge, link, connection, path, indegree, in-degree, incoming, inbound, ingoing, anomalous, malicious, intrusion, hack, attack, suspicious, behavior, trend, pattern, monitor, zero, no,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 2007/0209074 A1 (COFFMAN), 06 September 2007 (06.09.2007), entire document, especially Abstract; para [0042], [0050]-[0051], [0065]-[0068], [0071], [0091], [0166]	8 ---- 10
X --- Y	US 2005/0044406 A1 (Stute), 24 February 2005 (24.02.2005), entire document, especially Abstract, para [0014]-[0015], [0073]-[0074], [0121]	8 ---- 10
X --- Y	US 2007/0226796 A1 (Gilbert et al.), 27 September 2007 (27.09.2007), entire document, especially Abstract, para [0038], [0048], [0050], [0080], [0137]	8 ---- 10
Y	Neil. "Scan Statistics for the Online Discovery of Locally Anomalous Subgraphs." In: Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy , The University of New Mexico, May, 2011 [retrieved on 28 October 2013 (28.10.2013)] Retrieved from the Internet <URL: http://repository.unm.edu/handle/1928/13885 >, entire document, especially Abstract; Figure 7.5; pages 2-3, 61	10
A	US 2011/0231937 A1 (LIPPMANN et al.), 22 September 2011 (22.09.2011), entire document, especially Abstract, para [0021]-[0023], [0027]-[0028]	1-20
A	US 2010/0192226 A1 (Noel et al.), 29 July 2010 (29.07.2010), entire document, especially Abstract, para [0046], [0057]-[0062]	1-20

☒ Further documents are listed in the continuation of Box C. ☐

* 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
29 October 2013 (29.10.2013)	13 JAN 2014
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 13/31463

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Akoglu et al. "Anomaly Detection in Large Graphs." In: CMU-CS-09-173 Technical Report, School of Computer Science Carnegie Mellon University, Pittsburgh, November, 2009 [retrieved on 28 October 2013 (28.10.2013)] Retrieved from the Internet <URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.188.2619 >, entire document, especially Abstract	1-20
A	Djidjev et al. "Graph Based Statistical Analysis of Network Traffic." In: Proceedings of the Ninth Workshop on Mining and Learning with Graphs. August 2011 [retrieved on 28 October 2013 (28.10.2013)] Retrieved from the Internet <URL: http://csr.lanl.gov/detection/>, entire document, especially Abstract	1-20
A	US 2011/0154119 A1 (WANG et al.), 23 June 2011 (23.06.2011), entire document	1-20
A	US 2004/0133672 A1 (BHATTACHARYA et al.), 08 July 2004 (08.07.2004), entire document	1-20