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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012063 A3

(51) International Patent Classification⁷: G06F 11/30

(21) International Application Number: PCT/US2003/023877

(22) International Filing Date: 30 July 2003 (30.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/208,485 30 July 2002 (30.07.2002) US

(71) Applicant: ASGARD HOLDING, LLC [US/US]; 305 S. Andrews Avenue, Suite 505, Ft. Lauderdale, FL 33301 (US).

(72) Inventor: DAY, Christopher, W.; 11433 N.E. 6th Avenue, Biscayne Park, FL 33161 (US).

(74) Agent: GREENBERG, Steven, M.; Christopher & Weisberg, P.A., 200 East Las Olas Boulevard, Suite 2040, Fort Lauderdale, FL 33301 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

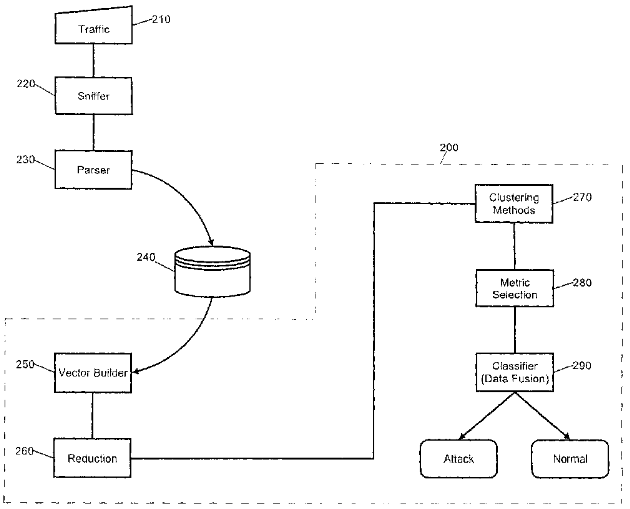
— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 8 April 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: INTRUSION DETECTION SYSTEM



(57) Abstract: An intrusion detection system (IDS). An IDS which has been configured in accordance with the present invention can include a traffic sniffer for extracting network packets from passing network traffic; a traffic parser configured to extract individual data from defined packet fields of the network packets; and, a traffic logger configured to store individual packet fields of the network packets in a database. A vector builder can be configured to generate multi-dimensional vectors from selected features of the stored packet fields. Notably, at least one self-organizing clustering module can be configured to process the multi-dimensional vectors to produce a self-organized map of clusters. Subsequently, an anomaly detector can detect anomalous correlations between individual ones of the clusters in the self-organized map based upon at least one configurable correlation metric. Finally, a classifier can classify detected anomalous correlations as one of an alarm and normal behavior.

WO 2004/012063 A3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/23877

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30
US CL : 713/200;709/224,229;706/ALL
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)
U.S. : 713/200;709/224,229;706/ALL

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
EAST; CONTINUITY DATA;INVENTOR NAME SEARCH;USPAT;US-PGPUB;EPO;JPO;DERWENT;IBM-TDB

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,088,804 (HILL et al) 11 JULY 2000 - Col. 4 lines 38-41; Col. 5 lines 39-45; 46-49; Col. 6 lines 9-24,14-22,23-32;Col. 7 lines 35-39 and 47-48; Fig. 1 and Fig. 3.	1 - 18
A	US 5,311,593 (CARMI) 10 May 1994 - see entire document	1 -18
A	US 5,414,833 (HERSHEY et al) 09 May 1995 - see entire document	1 - 18

□ 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 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 05 January 2004 (05.01.2004)	Date of mailing of the international search report 25 FEB 2004
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. (703) 305-3230	Authorized officer Peggy Harrod VINCENT TRANS Telephone No.703- 305-3900

Continuation of Item 4 of the first sheet:
The title of the invention is not descriptive. A new title is reqired that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "INTRUSION DETECTION SYSTEM USING NEURAL NETWORKS".

Continuation of B. FIELDS SEARCHED Item 3:
IDS INTRUSION NEAR DETECTION VECTOR;ANOM$6;PACKET NEAR FIELD;HILL ADAPTIVE;UNSUPERVISED NEAR LEARN $3;COMPETITIVE NEAR NEUAL NEAR NETWORK;SELF NEAR ORGANIZ$3 NEAR MAP