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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 October 2008 (09.10.2008)

PCT

(10) International Publication Number
WO 2008/121945 A2

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

(21) International Application Number:
PCT/US2008/058866

(22) International Filing Date: 31 March 2008 (31.03.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/909,307	30 March 2007 (30.03.2007)	US
12/059,076	31 March 2008 (31.03.2008)	US

(71) Applicant *(for all designated States except US)*: **NETQOS, INC.** [US/US]; 5001 Plaza On The Lake, Suite 200, Austin, TX 78746 (US).

(71) Applicant and
(72) Inventor *(for all designated States except US)*: **MULLARKEY, Peter** [US/US]; 103 Copper Leaf Road, Austin, TX 78734 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **JOHNS, Michael, C.** [US/US]; 1824 Nelson Ranch Loop, Cedar Park, TX 78613 (US).

(74) Agent: **HULSEY, William, N.**; Hulseyip Intellectual Property Lawyers, P.c., 919 Congress Avenue, Suite 919, Austin, TX 78701 (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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, 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))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *without international search report and to be republished upon receipt of that report*

WO 2008/121945 A2

(54) Title: STATISTICAL METHOD AND SYSTEM FOR NETWORK ANOMALY DETECTION

(57) Abstract: An anomaly detection method and system determine network status by monitoring network activity. A statistics based profile for said network over a period is generated to analyze potentially anomalous network activity to determine if said network activity is anomalous by comparing current activity against the profile. Using the profile as a reference, the anomaly detection system and process estimate and prioritize potentially anomalous network activity based on the probability that the behavior is anomalous. The level of severity that the anomaly detection process uses to determine if an alarm is needed is based on comparing user-adjustable thresholds to the current probability. If the threshold has been breached, the user is alerted, subject to other quality checks. After a reporting cycle concludes, the anomaly detection system and process recompiles the statistics based profile to take into account the information observed in the previous reporting cycle.