(12) International Application Status Report

Received at International Bureau: 19 June 2018 (19.06.2018)
Information valid as of: 27 November 2018 (27.11.2018)
Report generated on: 16 September 2019 (16.09.2019)

(10) Publication number:
WO2018/224670

(43) Publication date:
13 December 2018 (13.12.2018)

(26) Publication language:
English (EN)

(21) Application Number:
PCT/EP2018/065212

(22) Filing Date:
08 June 2018 (08.06.2018)

(25) Filing language:
English (EN)

(31) Priority number(s):
17175330.4 (EP)

(31) Priority date(s):
09 June 2017 (09.06.2017)

(31) Priority status:
Priority document received (in compliance with PCT Rule 17.1)

(51) International Patent Classification:
H04L 12/24 (2006.01); H04L 12/26 (2006.01)

(71) Applicant(s):
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street London EC1A 7AJ (GB)
(for all designated states)

(72) Inventor(s):
SERVAJEAN, Maximilien; Ground Floor, Faraday Building 1 Knightrider Street London EC4V 5BT (GB)
CHENG, Yipeng; Ground Floor, Faraday Building 1 Knightrider Street London EC4V 5BT (GB)

(74) Agent(s):
BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY; INTELLECTUAL PROPERTY DEPARTMENT
Ground Floor, Faraday Building 1 Knightrider Street London EC4V 5BT (GB)

(54) Title (EN): ANOMALY DETECTION IN COMPUTER NETWORKS

(54) Title (FR): DÉTECTION D'ANOMALIE DANS DES RÉSEAUX INFORMATIQUES

(57) Abstract:

(EN): A method of anomaly detection for network traffic communicated by devices via a computer network, the method comprising: clustering a set of time series, each time series including a plurality of time windows of data corresponding to network communication characteristics for a device; training an autoencoder for each cluster based on time series in the cluster; generating a set of reconstruction errors for each autoencoder based on testing the autoencoder with data from time windows of at least a subset of the time series; generating a probabilistic model of reconstruction errors for each autoencoder; and generating an aggregation of the probabilistic models for, in use, detecting reconstruction errors for a time series of data corresponding to network communication characteristics for a device as anomalous.

(FR): L'invention concerne un procédé de détection d'anomalie pour un trafic de réseau communiqué par des dispositifs par l'intermédiaire d'un réseau informatique, le procédé consistant à : regrouper un ensemble de séries chronologiques, chaque série chronologique comprenant une pluralité de fenêtres temporelles de données correspondant à des caractéristiques de communication de réseau pour un dispositif ; former un autocodeur pour chaque groupe sur la base d'une série chronologique dans le groupe ; générer un ensemble d'erreurs de reconstruction pour chaque autocodeur sur la base du test de l'autocodeur avec des données provenant de fenêtres temporelles d'au moins un sous-ensemble de la série chronologique ; générer un modèle probabiliste d'erreurs de reconstruction pour chaque autocodeur ; et générer une agrégation des modèles probabilistes pour, lors de l'utilisation, détecter des erreurs de reconstruction pour une série chronologique de données correspondant à des caractéristiques de communication de réseau pour un dispositif comme anormales.

International search report:
Received at International Bureau: 06 August 2018 (06.08.2018) [EP]

International Report on Patentability (IPRP) Chapter II of the PCT:

Not available

(81) Designated States:

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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, SA, 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

European Patent Office (EPO) : 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

African Intellectual Property Organization (OAPI) : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG

African Regional Intellectual Property Organization (ARIPO) : BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW

Eurasian Patent Organization (EAPO) : AM, AZ, BY, KG, KZ, RU, TJ, TM