

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
24 August 2023 (24.08.2023)



(10) International Publication Number
WO 2023/158786 A1

(51) International Patent Classification:

G06N 3/094 (2023.01) G06N 3/045 (2023.01)
G06N 3/08 (2023.01) G06N 3/0464 (2023.01)
G06N 3/0985 (2023.01) G06N 20/00 (2019.01)

(21) International Application Number:

PCT/US2023/013290

(22) International Filing Date:

17 February 2023 (17.02.2023)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/311,620 18 February 2022 (18.02.2022) US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventors: **CHEN, Huiyuan**; 919 S Winchester Blvd., San Jose, California 95128 (US). **WANG, Fei**; 34155 Siward Dr., Fremont, California 94555 (US). **YANG, Hao**; 2046 Wendover Lane, San Jose, California 95121 (US).

(74) Agent: **PREPELKA, Nathan, J.** et al.; The Webb Law Firm, One Gateway Center, 420 Ft. Duquesne Blvd., Suite 1200, Pittsburgh, Pennsylvania 15222 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, 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, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI,

(54) Title: METHOD, SYSTEM, AND COMPUTER PROGRAM PRODUCT FOR GENERATING ROBUST GRAPH NEURAL NETWORKS USING UNIVERSAL ADVERSARIAL TRAINING

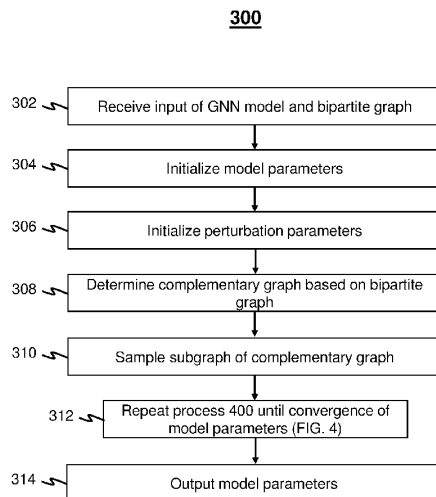


FIG. 3

(57) Abstract: Described are a method, system, and computer program product for generating robust graph neural networks using universal adversarial training. The method includes receiving a graph neural network (GNN) model and a bipartite graph including an adjacency matrix, initializing model parameters of the GNN model, initializing perturbation parameters, and sampling a subgraph of a complementary graph based on the bipartite graph. The method further includes repeating until convergence of the model parameters: drawing a random variable from a uniform distribution; generating a universal perturbation matrix based on the subgraph, the random variable, and the perturbation parameters; determining Bayesian Personalized Ranking (BPR) loss by inputting the bipartite graph and the universal perturbation matrix to the GNN model; updating the perturbation parameters based on stochastic gradient ascent; and updating the model parameters based on stochastic gradient descent. The method further includes, in response to convergence of the model parameters, outputting the model parameters.

[Continued on next page]

SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, KM, 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))*