DAFTAR PUSTAKA

Aldweesh, A., Derhab, A., Emam, A.Z., 2020. Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems 189. https://doi.org/10.1016/j.knosys.2019.105124

Aljawarneh, S., Aldwairi, M., Yassein, M.B., 2018. Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model. Journal of Computational Science 25, 152–160. https://doi.org/10.1016/j.jocs.2017.03.006

Alotaibi, S.D., Yadav, K., Aledaily, A.N., Alkwai, L.M., Yousef Dafhalla, A.K., Almansour, S., Lingamuthu, V., 2022. Deep Neural Network-Based Intrusion Detection System through PCA. Mathematical Problems in Engineering 2022. https://doi.org/10.1155/2022/6488571

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Adna N Anwar, 2020. TON-IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access 8, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862

Breiman, L., 2001. Random Forest. Machine Learning 45, 5–32. https://doi.org/10.1017/CBO9781107415324.004

Caville, E., Lo, W.W., Layeghy, S., Portmann, M., 2022. Anomal-E: A Self-Supervised Network Intrusion Detection System based on Graph Neural Networks.

Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P., 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys and Tutorials 21, 2671–2701. https://doi.org/10.1109/COMST.2019.2896380

Chen, H., Zhang, H., Si, S., Li, Y., Boning, D., Hsieh, C.J., 2019. Robustness verification of tree-based models. Advances in Neural Information Processing Systems 32.

Chen, T., Guestrin, C., 2016. XGBoost: A scalable tree boosting system. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 13-17-Augu, 785–794. https://doi.org/10.1145/2939672.2939785

Chowdhury, R.N., Chowdhury, M.M., Chowdhury, S., Islam, M.R., Ayub, M.A., Chowdhury, A., Kalpoma, K.A., 2020. Parameter Optimization and Performance Analysis of State-of-the-Art Machine Learning Techniques for Intrusion Detection System (IDS). ICCIT 2020 - 23rd International Conference on Computer and Information Technology, Proceedings. https://doi.org/10.1109/ICCIT51783.2020.9392683

Debicha, I., Bauwens, R., Debatty, T., Dricot, J.M., Kenaza, T., Mees, W., 2023. TAD: Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. Future Generation Computer Systems 138, 185–197. https://doi.org/10.1016/j.future.2022.08.011

Duan, G., Lv, H., Wang, H., Feng, G., 2022. Application of a Dynamic Line Graph

Neural Network for Intrusion Detection with Semisupervised Learning. IEEE Transactions on Information Forensics and Security. https://doi.org/10.1109/TIFS.2022.3228493

Gamage, S., Samarabandu, J., 2020. Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications 169. https://doi.org/10.1016/j.jnca.2020.102767

Geurts, P., Ernst, D., Wehenkel, L., 2006. Extremely randomized trees. Machine Learning 63, 3–42. https://doi.org/10.1007/s10994-006-6226-1

Goodfellow, I., Bengio, Y., Courville, A., 2016. Deep Learning. MIT Press, London, England.

Gowdhaman, V., Dhanapal, R., 2022. An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing 26, 13059–13067. https://doi.org/10.1007/s00500-021-06473-y

Guo, G., 2022. An Intrusion Detection System for the Internet of Things Using Machine Learning Models. 2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering, ICBAIE 2022 332–335. https://doi.org/10.1109/ICBAIE56435.2022.9985800

Hamilton, W.L., Ying, R., Leskovec, J., 2017. Inductive representation learning on large graphs. Advances in Neural Information Processing Systems 2017-Decem, 1025–1035.

He, Y., Shen, Z., Cui, P., 2021. Towards Non-I.I.D. image classification: A dataset and baselines. Pattern Recognition 110. https://doi.org/10.1016/j.patcog.2020.107383

Hindy, H., Brosset, D., Bayne, E., Seeam, A.K., Tachtatzis, C., Atkinson, R., Bellekens, X., 2020. A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems. IEEE Access 8, 104650–104675. https://doi.org/10.1109/ACCESS.2020.3000179

Hu, B., Kamiya, K., Takahashi, K., Nakao, A., 2021. Multi-hop Graph Embedding for Botnet Detection. 2021 IEEE Global Communications Conference, GLOBECOM 2021 - Proceedings. https://doi.org/10.1109/GLOBECOM46510.2021.9685712

Ibitoye, O., Shafiq, O., Matrawy, A., 2019. Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks. 2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings. https://doi.org/10.1109/GLOBECOM38437.2019.9014337

Injadat, M.N., Moubayed, A., Nassif, A.B., Shami, A., 2020. Systematic ensemble model selection approach for educational data mining. Knowledge-Based Systems 200. https://doi.org/10.1016/j.knosys.2020.105992

Jamalipour, A., Murali, S., 2022. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey. IEEE Internet of Things Journal 9, 9444–9466. https://doi.org/10.1109/JIOT.2021.3126811

Jiang, W., 2022. Graph-based deep learning for communication networks: A survey. Computer Communications 185, 40–54. https://doi.org/10.1016/j.comcom.2021.12.015

Ke Guolin, Qi Meng, Thomas Finley, Taifeng Wang, Wei Chen, Weidong Ma,

Qiwei Ye, Tie-Yan Liu, 2017. Lightgbm: A highly efficient gradient boosting decision tree. Advances in neural information processing systems 30.

Kilincer, I.F., Ertam, F., Sengur, A., 2022. A comprehensive intrusion detection framework using boosting algorithms. Computers and Electrical Engineering 100. https://doi.org/10.1016/j.compeleceng.2022.107869

Kingma, D.P., Ba, J.L., 2015. Adam: A method for stochastic optimization. 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings 1–15.

Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B., 2019. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems 100, 779–796. https://doi.org/10.1016/j.future.2019.05.041

Kuang, K., Cui, P., Athey, S., Xiong, R., Li, B., 2018. Stable prediction across unknown environments. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 1617–1626. https://doi.org/10.1145/3219819.3220082

Kumar, A., Shridhar, M., Swaminathan, S., Lim, T.J., 2022. Machine learning-based early detection of IoT botnets using network-edge traffic. Computers and Security 117. https://doi.org/10.1016/j.cose.2022.102693

Lan, J., Lu, J.Z., Wan, G.G., Wang, Y.Y., Huang, C.Y., Zhang, S.B., Huang, Y.Y., Ma, J.N., 2022. E-minBatch GraphSAGE: An Industrial Internet Attack Detection Model. Security and Communication Networks 2022. https://doi.org/10.1155/2022/5363764

Lawal, M.A., Shaikh, R.A., Hassan, S.R., 2020. An anomaly mitigation framework for iot using fog computing. Electronics (Switzerland) 9, 1–24. https://doi.org/10.3390/electronics9101565

Li, J., Sun, P., Hu, Y., 2020. Traffic modeling and optimization in datacenters with graph neural network. Computer Networks 181. https://doi.org/10.1016/j.comnet.2020.107528

Lian, W., Nie, G., Jia, B., Shi, D., Fan, Q., Liang, Y., 2020. An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning. Mathematical Problems in Engineering 2020. https://doi.org/10.1155/2020/2835023

Lin, C.H., Lin, Y.C., Wu, Y.J., Chung, W.H., Lee, T.S., 2021. A Survey on Deep Learning-Based Vehicular Communication Applications. Journal of Signal Processing Systems 93, 369–388. https://doi.org/10.1007/s11265-020-01587-2

Little, M.A., Badawy, R., 2019. Causal bootstrapping.

Liu, Y., Mu, Y., Chen, K., Li, Y., Guo, J., 2020. Daily Activity Feature Selection in Smart Homes Based on Pearson Correlation Coefficient. Neural Processing Letters 51, 1771–1787. https://doi.org/10.1007/s11063-019-10185-8

Lo, W.W., Layeghy, S., Sarhan, M., Gallagher, M., Portmann, M., 2022. E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT, in: Noms.

Makuvaza, A., Jat, D.S., Gamundani, A.M., 2021. Deep Neural Network (DNN) Solution for Real-time Detection of Distributed Denial of Service (DDoS)

Attacks in Software Defined Networks (SDNs). SN Computer Science 2. https://doi.org/10.1007/s42979-021-00467-1

Manzano Sanchez, R.A., Zaman, M., Goel, N., Naik, K., Joshi, R., 2022. Towards Developing a Robust Intrusion Detection Model Using Hadoop–Spark and Data Augmentation for IoT Networks †. Sensors 22. https://doi.org/10.3390/s22207726

Mulyanto, M., Faisal, M., Prakosa, S.W., Leu, J.S., 2021. Effectiveness of focal loss for minority classification in network intrusion detection systems. Symmetry 13, 1–16. https://doi.org/10.3390/sym13010004

Nasiri, H., Alavi, S.A., 2022. A Novel Framework Based on Deep Learning and ANOVA Feature Selection Method for Diagnosis of COVID-19 Cases from Chest X-Ray Images. Computational Intelligence and Neuroscience 2022. https://doi.org/10.1155/2022/4694567

Nemcovsky, Y., Zheltonozhskii, E., Baskin, C., Chmiel, B., Bronstein, A.M., Mendelson, A., 2022. Adversarial robustness via noise injection in smoothed models. Applied Intelligence. https://doi.org/10.1007/s10489-022-03423-5

Nguyen, D.D., Le, M.T., Cung, T.L., 2022. Improving intrusion detection in SCADA systems using stacking ensemble of tree-based models. Bulletin of Electrical Engineering and Informatics 11, 119–127. https://doi.org/10.11591/eei.v11i1.3334

Petković, M., Kocev, D., Džeroski, S., 2020. Feature ranking for multi-target regression. Machine Learning 109, 1179–1204. https://doi.org/10.1007/s10994-019-05829-8

Pujol-Perich, D., Suarez-Varela, J., Cabellos-Aparicio, A., Barlet-Ros, P., 2022. Unveiling the potential of Graph Neural Networks for robust Intrusion Detection. Performance Evaluation Review 49, 111–117. https://doi.org/10.1145/3543146.3543171

Purnama, S.R., Istiyanto, J.E., Amrizal, M.A., Handika, V., Rochman, S., Dharmawan, A., 2022. Inductive Graph Neural Network with Causal Sampling for IoT Network Intrusion Detection System. IEEE.

Saba, T., Rehman, A., Sadad, T., Kolivand, H., Bahaj, S.A., 2022. Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering 99. https://doi.org/10.1016/j.compeleceng.2022.107810

Sarhan, M., Layeghy, S., Moustafa, N., Portmann, M., 2021. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST 371 LNICST, 117–135. https://doi.org/10.1007/978-3-030-72802-1_9

Sarhan, M., Layeghy, S., Portmann, M., 2022. Towards a Standard Feature Set for Network Intrusion Detection System Datasets. Mobile Networks and Applications 27, 357–370. https://doi.org/10.1007/s11036-021-01843-0

Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q., 2018. A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence 2, 41–50. https://doi.org/10.1109/TETCI.2017.2772792

Snoek, J., Larochelle, H., Adams, R.P., 2012. Practical Bayesian optimization of machine learning algorithms. Advances in Neural Information Processing Systems 4, 2951–2959.

Thang, D.C., Dat, H.T., Tam, N.T., Jo, J., Hung, N.Q.V., Aberer, K., 2022. Nature vs. Nurture: Feature vs. Structure for Graph Neural Networks. Pattern Recognition Letters 159, 46–53. https://doi.org/10.1016/j.patrec.2022.04.036

Wei, G., Zhao, J., Feng, Y., He, A., Yu, J., 2020. A novel hybrid feature selection method based on dynamic feature importance. Applied Soft Computing Journal 93. https://doi.org/10.1016/j.asoc.2020.106337

Xiao, Q., Liu, J., Wang, Q., Jiang, Z., Wang, X., Yao, Y., 2020. Towards network anomaly detection using graph embedding. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12140 LNCS, 156–169. https://doi.org/10.1007/978-3-030-50423-6_12

Xu, H., Mannor, S., 2010. Robustness and generalization. COLT 2010 - The 23rd Conference on Learning Theory 503–515.

Yang, L., Shami, A., 2020. On hyperparameter optimization of machine learning algorithms: Theory and practice. Neurocomputing 415, 295–316. https://doi.org/10.1016/j.neucom.2020.07.061

Zeng, Z.R., Peng, W., Zeng, D., 2022. Improving the Stability of Intrusion Detection with Causal Deep Learning. IEEE Transactions on Network and Service Management. https://doi.org/10.1109/TNSM.2022.3193099

Zhang, T., Shan, H.R., Little, M.A., 2022. Causal GraphSAGE: A robust graph method for classification based on causal sampling. Pattern Recognition 128. https://doi.org/10.1016/j.patcog.2022.108696