Neural Computing and Applications (2022) 34:20447–20448
https://doi.org/10.1007/s00521-022-07908-9

EDITORIAL

Cybersecurity applications of computational intelligence

Álvaro Herrero[1] · Emilio Corchado[2] · Michal Wozniak[3] · Sung Bae-Cho[4] · Slobodan Petrović[5]

Received: 29 September 2022 / Accepted: 29 September 2022 / Published online: 12 October 2022

Computational Intelligence (CI) has been revealed as one of the most promising technologies to solve some complex problems. An increasing number of such problems are taking place in the cybersecurity domain. Hence, cybersecurity applications of CI are becoming more popular. This special issue presents some of these cutting-edge applications presented at the 13th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2020). Extended versions of selected papers presenting innovations in up-to-date cybersecurity challenges are compiled in this special issue.

Artificial Neural Networks (ANN) are proposed in the first paper for combat Fake News (FN). More precisely, the Bidirectional Encoder Representations from Transformers (BERT) architecture is applied to build a FN detection model. Approaching the problem from the Natural Language Processing perspective, authors study transfer learning as a method to improve the performance of BERT-derived methods in order to boost the identification of FN. The proposal is validated on two open datasets, containing information about news related to different types of information.

The second contribution presents the use of a distributed anomaly detection system to identify the source of the wrong operation of bicomponent materials in wind generator blades. Different Machine Learning models are applied to an industrial facility that obtains carbon fiber as final product. An early diagnosis of any deviation from the normal operation of the system is crucial to take corrective actions. The proposal takes advantage of one-class techniques to implement a distributed system capable of locating anomalies in specific parts of the facility under study. An innovative contribution of this work is the implementation of one-class classifiers to consider the possibility of locating the source of the anomaly.

From a complementary perspective, Flusser et al. detect, by Surrogate ANNs, anomalies in large-scale computer network traffic. These models are applied to the identification of outlying (and thus suspicious) events, outperforming a number of state-of-the-art algorithms such as *k*-Nearest Neighbors (*k*NN). It is achieved by approximating an existing anomaly detector's score function by training a Multi-layer Perceptron (MLP). Algorithms are benchmarked on a dataset provided by Cisco Systems. According to the obtained results, some shallow networks can outperform deep ones when applied to certain datasets.

Finally, adversarial attacks against Deep ANNs area visually analyzed for Dynamic Risk Assessment. Three defense strategies, against adversarial example attacks, have been selected in order to visualize the behavior modification of each one of them in the defended models (composed of both convolutional and dense layers). The behavior of the original and the defended model are compared, representing the target model by a graph in a visualization. This visualization allows identifying the

✉ Álvaro Herrero
ahcosio@ubu.es

Emilio Corchado
escorchado@usal.es

Michal Wozniak
michal.wozniak@pwr.edu.pl

Sung Bae-Cho
sbcho@yonsei.ac.kr

Slobodan Petrović
slobodan.petrovic@ntnu.no

[1] Grupo de Inteligencia Computacional Aplicada (GICAP), Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad de Burgos, Av. Cantabria s/n, 09006 Burgos, Spain

[2] Departamento de Informática Y Automática, Universidad de Salamanca Plaza de La Merced, Salamanca, Spain

[3] Department of Systems and Computer Networks, Faculty of Electronics, Wroclaw University of Science and Technology, Wybrzeze Wyspianskiego, 27, 50-370 Wrocław, Poland

[4] Department of Computer Science, Yonsei University, Seoul 03722, South Korea

[5] Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, P.o. box 191, N-2802 Gjøvik, Norway

vulnerabilities of the model and shows how the defenses try to avoid them. As a result, the proposed visualizations can be useful for improving and optimizing the defenses.

Acknowledgements The guest editors wish to thank Prof John MacIntyre (Editor-in-Chief of the Neural Computing and Applications Journal) for providing the opportunity to edit this special issue. We would also like to thank the reviewers who have thoroughly evaluated the papers and the editorial staff for their support.