Hindawi
Complexity
Volume 2019, Article ID 3261453, 2 pages
https://doi.org/10.1155/2019/3261453

Editorial

Advances in Complex Systems and Their Applications to Cybersecurity

Fernando Sánchez Lasheras,[1] **Danilo Comminiello**,[2] **and Alicja Krzemień**[3]

[1]*Mathematics Department, University of Oviedo, c/Federico García Lorca 18, 33007 Oviedo, Spain*
[2]*Department of Information Engineering, Electronics and Telecommunications (DIET), Sapienza University of Rome, Via Eudossiana 18, 00184 Rome, Italy*
[3]*Department of Risk Assessment and Industrial Safety, Central Mining Institute, Plac Gwarków 1, 40166 Katowice, Poland*

Correspondence should be addressed to Fernando Sánchez Lasheras; sanchezfernando@uniovi.es

Received 25 February 2019; Accepted 25 February 2019; Published 4 June 2019

Cybersecurity is one of the fastest growing and largest technology sectors and is increasingly being recognized as one of the major issues in many industries, so companies are increasing their security budgets in order to guarantee the security of their processes. Successful menaces to the security of information systems could lead to safety, environmental, production, and quality problems.

One of the most harmful issues of attacks and intrusions is the ever-changing nature of attack technologies and strategies, which increases the difficulty of protecting computer systems. As a result, advanced systems are required to deal with the ever-increasing complexity of attacks in order to protect systems and information.

This special issue received several contributions, 5 of which have been accepted for publication.

In the article "Effect of the Sampling of a Dataset in the Hyperparameter Optimization Phase over the Efficiency of a Machine Learning Algorithm" by N. DeCastro-García et al., the authors investigate on the use of different partitions of a dataset in the hyperparameter optimization phase over the efficiency of a machine learning algorithm. Nonparametric inference has been used to measure the rate of different behaviors of the accuracy. A level of gain is assigned to each partition allowing authors to study patterns and allocate whose samples are more profitable. The statistical analyses were carried out over five cybersecurity datasets.

In the article "Detection of Jihadism in Social Networks Using Big Data Techniques Supported by Graphs and Fuzzy Clustering" by C. Sánchez-Rebollo et al., the authors performed an analysis of Twitter messages to detect the leaders orchestrating terrorist networks and their followers. A big data architecture is proposed to analyze messages in real time in order to classify users according to different parameters like level of activity, the ability to influence other users, and the contents of their messages. Graphs have been used to analyze how the messages propagate through the network and fuzzy clustering techniques were used to classify users in profiles. The Algorithms test was performed with the help of public database from Kaggle and other Twitter extraction techniques.

In the article "Delving into Android Malware Families with a Novel Neural Projection Method" by R. V. Vega et al., the authors proposed the application of unsupervised and supervised machine-learning techniques to characterize Android malware families. More precisely, a novel unsupervised neural-projection method for dimensionality-reduction, namely, Beta Hebbian Learning (BHL), was applied to visually analyze such malware. Additionally, well-known supervised Decision Trees (DTs) are also applied to improve characterization of such. The proposed techniques are validated when facing real-life Android malware data by means of the well-known and publicly-available Malgenome dataset.

In the article "Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol" by H. A. Moretón et al., the authors proposed the creation of classification

models that can feed an Intrusion Detection System using a dataset containing frames under attacks of an Internet of Things (IoT) system that uses the MQTT protocol. Two kinds of methods are applied: ensemble methods and recurrent networks, achieving very satisfactory results.

Finally, in the article "Practical Employment of Granular Computing to Complex Application Layer Cyberattack Detection" by R. Kozik et al., the authors propose a novel approach to the detection of cyberattacks taking inventory of the practical application of information granules. Also, the feasibility of utilizing Granular Computing (GC) as a solution to the most current challenges in cybersecurity is researched. Promising results have been shown on a benchmark dataset.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

The editorial team would like to express appreciation to all authors for their valuable contributions and to all reviewers for their valuable comments. In addition, the editors would like to thank the Complexity Journal's Editorial Board for their valuable help and support regarding this special issue.

Fernando Sánchez Lasheras
Danilo Comminiello
Alicja Krzemień