Complexity

Special Issue on
Advances in Complex Systems and Their Applications to Cybersecurity

WILEY | Hindawi

CALL FOR PAPERS

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.

A complex system can be defined as any system in which its parts and interactions together represent a specific behaviour, such that an analysis of all its constituent parts cannot explain the behaviour. In general, cyber systems can be considered as complex adaptive system and could be analyzed by means of the same principles of complexity science, inspired by systems thinking and natural science.

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 number of attacks in order to protect systems and information.

Complexity is a cross-disciplinary journal focusing on the rapidly expanding science of complex adaptive systems. The purpose of the journal is to advance the science of complexity. Nowadays IT systems are designed by thousands of individuals with different backgrounds and technological knowledge. This fact introduces a strong human element in the design of cyber systems and makes them particularly vulnerable as computer break-ins are caused by the sum of different circumstances rather than a standalone vulnerability. This special issue is to publish high-quality research papers as well as addressing recent advances on complex systems applied under the frame of cybersecurity, all of them with a holistic approach to the problem. Articles may deal with such methodological themes as chaos, genetic algorithms, cellular automata, neural networks, and evolutionary game theory. Original, high-quality contributions that are not published or that are not currently under review by other journals or peer-reviewed conferences are sought.

Potential topics include but are not limited to the following:

- Machine learning for data mining in cybersecurity
- Machine learning for security of cyber-physical systems
- Supervised and unsupervised learning for intrusion detection
- Security chaos engineering
- Adaptive defense of network infrastructure
- Secure Internet of things
- Intelligent control and monitoring of critical systems
- Genetic algorithm applied to biometric security
- Complex systems in cryptography
- Application of neural networks to secure Internet of things
- Developments for improving the security of blockchain
- New cryptographic primitives including postquantum scenario
- Network security, connectivity, cellular automata, and graphs
- High dimensional and convolutional linear systems

Authors can submit their manuscripts through the Manuscript Tracking System at https://mts.hindawi.com/submit/journals/complexity/acsa/.

Papers are published upon acceptance, regardless of the Special Issue publication date.

Lead Guest Editor
Fernando Sánchez Lasheras, University of Oviedo, Oviedo, Spain
sanchezfernando@uniovi.es

Guest Editors
Danilo Comminiello, Sapienza University of Rome, Rome, Italy
danilo.comminiello@uniroma1.it

Alicja Krzemień, Central Mining Institute, Katowice, Poland
akrzemien@gig.eu

Submission Deadline
Friday, 7 December 2018

Publication Date
April 2019