CALL FOR PAPERS

IEEE Transactions on Sustainable Computing

Special Issue on Sustainable Cyber Forensics and Threat Intelligence

GUEST EDITORS:

- Mauro Conti, University of Padua, Italy. conti@math.unipd.it
- Ali Dehghantanha, University of Salford, UK. a.dehghantanha@salford.ac.uk
- Giuseppe Bianchi, University of Rome Tor Vergata, Italy. giuseppe.bianchi@uniroma2.it
- Tooska Dargahi, CNIT - University of Rome Tor Vergata, Italy. tooska.dargahi@uniroma2.it

TOPIC SUMMARY:

Increasing societal reliance on interconnected digital systems, including smart grids and Internet of Things (IoT), made sustainable detection and investigation of threat actors among highest priorities of any society. Scale and attack surface of modern networks mandate optimized deployment of limited cyber forensics and threat intelligence resources to detect and remove malicious actors in a timely manner. However, timely dealing with such a huge number of attacks is not possible without employment of artificial intelligence and machine learning techniques. When a significant amount of data is collected from or generated by different security monitoring solutions; intelligent big-data analytical techniques are necessary to mine, interpret and extract knowledge out of those data. The emerging field of cyber threat intelligence is investigating applications of artificial intelligence and machine learning techniques to perceive, reason, learn and act intelligently against advanced cyber attacks. Considering that sustainability is a crucial success factor in implementation, installation and deployment of threat intelligence and cyber forensics capacities in modern networks, for this special issue we seek original and high-quality papers in the following topics (but are not limited to):

- Sustainable cyber threat intelligence in IoT, smart grids, and modern networks
- Green digital forensics and cyber investigation
- Sustainability issues and opportunities in cyber investigation and threat intelligence
- Power aware applications for cyber investigation and threat intelligence
- Application of machine learning tools and techniques in cyber threat intelligence
- Theories and models for detection and analysis of advanced persistent threats
- Collective optimization techniques for cyber investigation and threat hunting
- Threat intelligence techniques for detecting, and reacting to advanced intrusion campaigns
- Intelligent forensics tools, techniques and procedures for sustainable computing
- Threat intelligence in cyber security domain utilising big data solutions such as Hadoop
- Resource management and optimization of cyber investigation activities in heterogeneous networks
- Interpretation of cyber threat and forensic data utilising intelligent data analysis techniques
- Infer intelligence of existing cyber security data generated by different monitoring solutions

IMPORTANT DATES:

Submission Deadline: September 1 2017
First round notification: November 1 2017
Revised papers due: December 15 2017
Final notification: January 15 2018
Publication: July-September 2018 (tentative)

SUBMISSION GUIDELINES:

Authors are invited to submit their manuscripts electronically adhering to the *IEEE Transactions on Sustainable Computing* guidelines (https://www.computer.org/web/tsusc/author). Please submit your papers through the online system (https://mc.manuscriptcentral.com/tsusc-cs) and be sure to select the special issue on Digital Forensics and Cyber Threat Intelligence in Sustainable Computing. *Manuscripts should not be published or currently submitted for publication elsewhere.* Please submit only full papers intended for review, not abstracts, to the ScholarOne portal.