Security and Communication Networks

Special Issue on

Characterization and Detection of Fakes, Spammers, and Bots in Social and Communication Networks

CALL FOR PAPERS

Nowadays, online social networks, and, in general, communication networks, are a crucial component in the public sphere, enhancing communications, fostering discussions, and influencing the public perception for a myriad of issues. On the one hand, this represents an unprecedented communication opportunity. On the other hand, however, social and communication networks have become the ideal stage for the proliferation of fictitious and malicious accounts, including bots and botnets. Indeed, recent studies highlighted the existence of large groups of fake accounts, spammers, and bots that are purposely created to carry out scamming and phishing attacks, share viruses and malwares, post fake news and unsolicited spam, advertise events and products of doubtful legality, sponsor public and political characters, and, ultimately, interfere with legitimate network traffic and lead to a bias within the public opinion.

Efficient detection of such malicious nodes in social and communication networks has thus become one of the most pressing contemporary challenges. However, the task presents many fundamental issues, including, firstly, the difficulties related to the construction of large ground-truth datasets for training and testing detection techniques, secondly, the advanced characteristics of modern malicious nodes that make them hardly distinguishable from legitimate ones, and, thirdly, the advanced communication strategies put in place by bots and botmasters in order to escape detection.

Because of these issues, much research and experimentation are needed for the characterization and the detection of scammers, compromised and fake accounts, spammers, and bots. This special issue thus focuses on authentication techniques, access control mechanisms, network traffic analysis, and novel detection techniques for malicious nodes in a social and communication network. Particular emphasis should be given to the design of flexible and scalable techniques capable of dealing with different types of malicious nodes in large-scale analyses. We also encourage studies assessing the consequences of malicious actions. Finally, novel approaches to the collection and annotation of large ground-truth datasets are also welcomed.

Potential topics include but are not limited to the following:

- Authentication techniques to discriminate between legitimate and malicious nodes
- Access control mechanisms that prevent data disclosure hosted in social and communication networks to possible bots
- Machine learning-based detection techniques for malicious nodes
- Network analysis techniques for characterization and detection of malicious nodes
- Online behavioral modeling for the detection of anomalous behaviors
- Techniques for detecting groups of synchronized and coordinated malicious nodes
- Techniques for detecting evolving/evading malicious nodes

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

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

Lead Guest Editor
Maurizio Tesconi, IIT-CNR, Pisa, Italy
maurizio.tesconi@iit.cnr.it

Guest Editors
Stefano Cresci, IIT-CNR, Pisa, Italy
stefano.cresci@iit.cnr.it

Roberto Di Pietro, Hamad Bin Khalifa University, Doha, Qatar
rdipietro@hbku.edu.qa

Mueen Abdullah, University of New Mexico, Albuquerque, USA
mueen@unm.edu

Submission Deadline
Friday, 18 January 2019

Publication Date
June 2019