Community detection is a hot topic in social networks. The presentation of a different computational paradigm with respect to traditional approaches can be beneficial for researchers to explore new approaches and principles to deal with this problem. The target audience is constituted by all those researchers interested in approaching the problem of community detection with computational models inspired by evolution in nature. No particular background is expected from the audience since the tutorial provides the concepts necessary for understanding the problem.
Abstract

This introductory overview tutorial on social network analysis (SNA) demonstrates through theory and practical case studies applications to research, particularly on social media, digital interaction and behavior records. NodeXL provides an entry point for non-programmers to access the concepts and core methods of SNA and allows anyone who can make a pie chart to now build, analyze and visualize complex networks.
Online social media platforms are severely compromised by the existence of malicious actors such as bots on Twitter, vandals on Wikipedia, fake accounts on Facebook, trolls on Twitter and Slashdot, and spammers who seem to be omnipresent. This tutorial presents methods to identify malicious actors in at least 4 settings: Twitter, Facebook, Slashdot, and Wikipedia. We will look at 4 broad categories of methods: (i) network based techniques where the structure of the social network is used, (ii) text based methods where the linguistic content of posts is examined, (iii) behavior-based methods which study actions of users, and (iv) real-time processes which enable defenders of social media to keep a step ahead of malicious actors. The tutorial will identify commonly used features for classifying actors into malicious vs. benign and will give a brief explanation of different algorithms both specific to social platforms and general algorithms that are platform neutral.