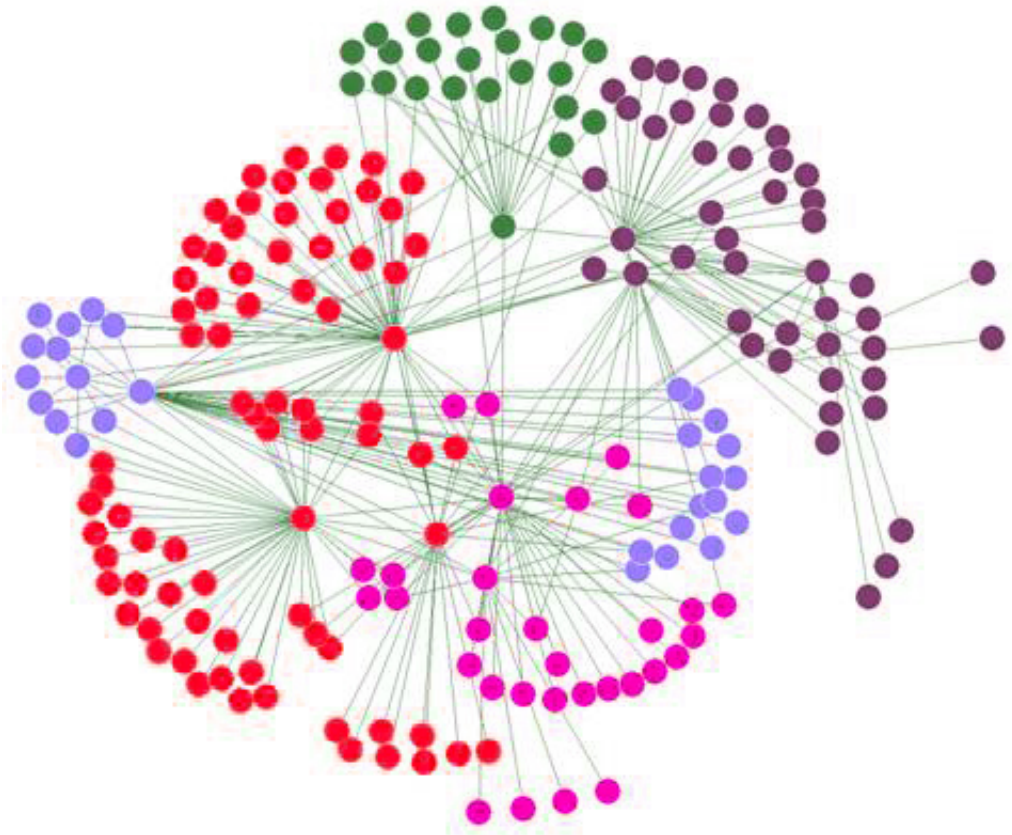
Researchers develop algorithm to locate fake users on many social networks

April 17 2018



Social network diagram. Credit: Daniel Tenerife/Wikipedia

Ben-Gurion University of the Negev (Beer-Sheva, Israel) and University of Washington (Seattle) researchers have developed a new generic method to detect fake accounts on most types of social networks, including Facebook and Twitter.

According to a new study in *Social Network Analysis and Mining*, the new method is based on the assumption that fake accounts tend to establish improbable links to other users in the networks.

"With recent disturbing news about failures to safeguard user privacy, and targeted use of social media by Russia to influence elections, rooting out fake users has never been of greater importance," explains Dima Kagan, lead researcher and a researcher in the BGU Department of Software and Information Systems Engineering. "We tested our algorithm on simulated and real-world data sets on 10 different social networks and it performed well on both."

The algorithm consists of two main iterations based on machine-learning algorithms. The first constructs a link prediction classifier that can estimate, with high accuracy, the probability of a link existing between two users. The second iteration generates a new set of meta-features based on the features created by the link prediction classifier. Lastly, the researchers used these meta-features and constructed a generic classifier that can detect fake profiles in a variety of online social networks.

"Overall, the results demonstrated that in a real-life friendship scenario we can detect people who have the strongest friendship ties as well as malicious users, even on Twitter," the researchers say. "Our method outperforms other anomaly detection methods and we believe that it has considerable potential for a wide range of applications particularly in the cyber-security arena."

The Ben-Gurion University researchers previously developed the Social Privacy Protector (SPP) to help users evaluate their friends list in seconds to identify which have few or no mutual links and might be "fake" profiles.

More information: Dima Kagan et al, Generic anomalous vertices

detection utilizing a link prediction algorithm, *Social Network Analysis and Mining* (2018). DOI: 10.1007/s13278-018-0503-4

Provided by American Associates, Ben-Gurion University of the Negev