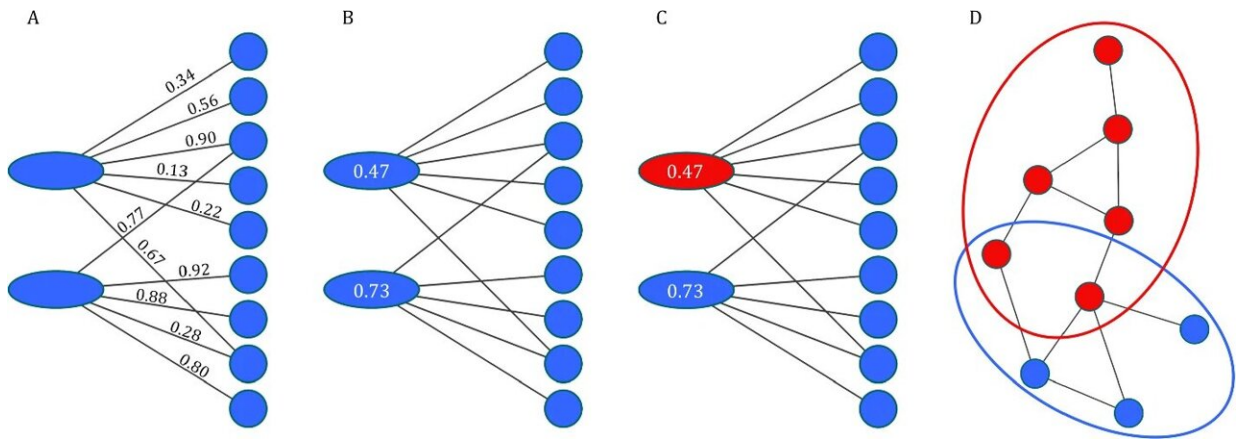
Cyber researcher pioneers method to track groups of anomalous users

January 9 2023



Algorithm overview. **A** After constructing the bipartite network, we created a link-predictor based on its topological features and predict edges' existence. **B** For each community-representing vertex, we aggregate the predicted probabilities into meta-features, for example, averaging them. **C** We rank them by the meta-features. **D** We fetch the corresponding original communities and manually examine them. Credit: *Neural Processing Letters* (2023). DOI: 10.1007/s11063-022-11103-1

Malicious or fictitious users on internet networks have become the bane of the internet's existence. While many bemoan their increasing frequency, few have developed methods to track and expose them. A Ben-Gurion University of the Negev researcher has developed a new method to detect groups of anomalous users.

Their findings were just published in *Neural Processing Letters*.

"The advantage of this study is that we can detect anomalous groups of users (such as groups of fake profiles) rather than single users. Uncovering groups of fake profiles is a challenging and less explored task," says Dr. Michael Fire, head of the Data4Good Lab and a member of the Department of Software and Information Systems Engineering.

An anomalous user community might be one that is promoting violent behavior or extremism, one that is spreading fake news, but it could potentially also help locate hot spots during pandemics, the researchers wrote.

One of the advantages of their method, which they named Co-Membership-based Generic Anomalous Communities Detection Algorithm (CMMAC), is that it is not restricted to a single type of network.

"Our method is generic. Therefore, it can potentially work on different types of social media platforms. We tested it on several different types of networks, such as Reddit and Wikipedia (which is also a type of social network)," explains Dr. Fire.

After testing their method on randomly generated networks and real-world networks, they found that it outperformed many other methods in a range of settings.

"Our method is based solely on network structural properties. That makes our method independent of vertices' attributes (the connections between users online). Thus, it is agnostic to the domain. When comparing our algorithm with other algorithms, it performed better on simulation and real-world data in many cases. It successfully detected groups of anomalous users' communities who presented peculiar online

activity," says Dr. Fire.

Additional researchers include Shay Lapid, an MA student, and Dima Kagan, a Ph.D. student, in Dr. Fire's lab.

More information: Shay Lapid et al, Co-Membership-based Generic Anomalous Communities Detection, *Neural Processing Letters* (2023). DOI: 10.1007/s11063-022-11103-1