Network Algorithms for Homeland Security, or How to find a Small Hidden Group in a Large Communication Network

Mark Goldberg
joint work with J. Baumes, M. Magdon-Ismail, and W. Wallace
{baumej,goldberg,magdon}@cs.rpi.edu, wallaw@rpi.edu
Rensselaer Polytechnic Institute

Abstract

A small group of *actors* in a large communication network, when attempting to coordinate some hostile (terrorist) activity, generally need to *plan* their activity and *conceal* their planning. They may camouflage their planning using encryption and the anonymity offered by a vast background communication; they will not trust any outsider with the details of their planning. How can we detect such activity *without* semantic analysis of the communication data?

We describe models and efficient algorithms for detecting groups, functioning in communication networks, that attempt to hide their planning–*hidden groups*. We show how to extend the algorithm efficiently when the exact time-interval during which the group members communicate is not known. Generalizing to less restrictive patterns of hidden group communications leads to an NP-complete problem. We discuss heuristic approaches to this problem.

As expected, we find that if the background communications are dense or more structured, then the hidden group is harder to detect. Surprisingly, we also find that when the hidden group is non-trusting (secretive), it is *easier* to detect that group.