1 Background

The paradigm of dark networks offers nothing more than a collection of traditional SNA measures and methods focused on identifying actors embedded in so-called light networks with the their centralities. Once central actors are identified it is still not clear whether that actor is a bad actor or not. Thus it is SNA without proper alignment to the task at hand and does not offer specific explanatory tools for combating bad behavior.

The goal of dark network literature would be to identify risk of global effects under specific continuous actor behaviors and to identify actors whose changing behavior if they turn dark becomes problematic.

2 Methodology

Take a network already filled with data. Our goal is to rewire that network while maintaining the same degree sequence and calculating a centrality distribution's entropy and the consequent loss or gain in entropy from said re-wiring.

This will be the Entropy of Centrality given the degree distribution. The re-wiring can be done based on specific agent behaviors, and the entropy, our sufficient statistic, represents the amount of surprise/change in centrality based on said rewiring. What we'll be able to understand is the information loss, given degree distribution, of the centrality distribution and we can explore that space.

The method can be modified to only include missing links or addition of links.

The initial idea contained a permutation test, but for a permutation test to occur I need to control for structure given some trait/attribute distribution. For example, if we swap the degree (permute) to some other output, like the amount of money, and measure the entropy of that money distribution then I can understand how each network loses or gains information from that change.

QAP controls for structure in that it takes an input and an output, but if I relabel I'm just moving the centralities. It doesn't quite do the job I want it to. But degree sequence re-wiring, controls the degree distribution while letting us understand the effect of structure given modification of links, and of nodes. But it will only work, as is for bond percolation, not site percolation.

Let's review the psuedocode:

2.1 Expected Results

The methodology as simple as it is provides an empirical method to test the relative surprise in edge deletion under the assumption that this ”surprise” is a unique characteristic of the network's structure and topology. This can guide policy-making in a general sense and provides us with a scalar measure to quantify the sensitivity of the whole network to changes.

Additionally, instead of random rewiring, one can institute specific agent-based rewiring behaviors more in line with expected human behavior. For example, rewiring only edges where senders or received possess a large number of edges (high degree), mimicking what one may expect when an adversary attempts to ”hide” the leader of an organization. Another example may be rewiring edges that belong to bridge nodes (the messenger) that could be serving as critical junctures between one sub-group and another. The later example would be best considered in the context of a network with some dynamical messaging process.

Finally, though not fully explored in literature, we can assign, based on our permutations a relative entropy attribute to each node/agent. Targeting policy-makers can, knowing that their resources are limited, redirect resources to ensure that targets that could ”surprise” the network more will be suitably targeted.

3 Policy Implications

In the absence of direct knowledge about the placement and activity condition of a bad actor, reliance on the dark network framework leaves much to be desired. Specifically, there's very little that distinguishes the framework from traditional SNA as developed as early as the 1970s, and with today's predictive power generated from black box machine learning algorithms that can crunch many simultaneous features of large quantities of data, the paradigm seems uninvigorated.

Network targeting policy in the context of incomplete and/or manipulated information should be focused on the surprise effect of an actor relative to the whole network. This is especially the case when intelligence collection is limited or can easily be corrupted.

I believe that this newly developed framework at minimum provides an empirically sound method for analysis, and in the best of circumstances can begin to reveal powerful explanatory effects when studying the adversary.

4 Mathematics

We rely on a number of mathematical results from existing literature:

Common Centralities:

Given a graph G(ε,ν) with nodes ν = {1,N} with number of nodes N and set $\varepsilon \in \nu$ x ν with number of edges M. We will assume that it is a simple network, unweighted, undirected, and with no self-loops. We also define an adjacency matrix such that:

$$A_{ij} = \begin{cases} 1, & \text{(i,j)} \in \varepsilon \\ 0, & \text{otherwise} \end{cases}$$

Since we constrain our network to simple undirected edges, we define our degree sequence to be some set $D = D_1, D_2, D_3, ..., D_N$ where $D_1 ... D_N = \sum A_{1j}, A_{2j}, ..., A_{Nj}$.

Following from this we can begin to define several centrality distributions:

4.1 Centralities

Closeness centrality:

Closeness is nodal measure that identifies how close a node is to the remainder of the network by measuring the reciprocal of distances d_{ij} from every node i to every node j. A continuous measure, the p.d.f of this measure gives the probability of a node i possessing a value $C(i)$. A normalized version of the measure exists that ensures $\sum C(i) = 1$.

$$C(i) = \frac{1}{\sum_j d_{ij}} \tag{1}$$

$$C(i) = \frac{N}{\sum_j d_{ij}} \quad \text{for the normalized version} \tag{2}$$

Another centrality measure that is popular in the so-called Dark Networks community

References