Hands on Case Study: Applying Dynamic Network Analysis to Temporal Netflow Data

Geoffrey Dobson

gdobson@andrew.cmu.edu
June 13, 2018

Overview

- Graduate
- Apply for jobs
- Land a new job
- Get direction from your customer
- Do your job (the hands on part)
This job sounds perfect!
Land a new job

<table>
<thead>
<tr>
<th>Company</th>
<th>BAE Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Title</td>
<td>Senior Researcher, Network Science</td>
</tr>
<tr>
<td>Workcenter</td>
<td>Cyber Situational Awareness Cell</td>
</tr>
<tr>
<td>Job Description</td>
<td>Apply network science techniques and expertise to the Cyber Situational Awareness Cell of a multibillion dollar international corporation</td>
</tr>
</tbody>
</table>

Get direction from your customer

“We have thousands of computers connected all over the world, and we know all about them…but we don’t know how the network is behaving!!!.....HELP!”

Source: Youtube
Do your job

• Collect Netflow data
• Conduct Dynamic Network Analysis
• Gain better Cyber Situational Awareness
Collect Netflow Data

1. Go to thumb drive -> DAY 3 - Basic Analysis -> Data -> net flow data
Collect Netflow Data

2. Create New Folder on Desktop called “Unzipped”

3. Go to Thumb drive and right click on each zip file, and extract to Unzipped Folder

4. Open Import Wizard and select Table of network links
Collect Netflow Data

5. Name the Meta Network

Collect Netflow Data

6. Browse to files
Collect Netflow Data

7. Configure input data

- Import Data into OA
  - Select the file containing the data with column headers.
  - Optional: Select and enter the required information.
  - Optional: Define network labels and attributes based on the columns.

8. Uncheck "Create a dynamic meta-network.." and Finish
Understand your data

- Describe your network data:
  - Undirected single mode network
  - Agent by Agent meta network
  - Bipartite graph
  - Flow records per day?
    - ~200,000
  - Links per day?
    - ~ 130,000
  - Nodes per day?
    - ~ 22,000

Perform Dynamic Network Analysis

1. Create a dynamic meta-network
Perform Dynamic Network Analysis

2. Fill in Date field

Example date strings were 2001 (i.e., the year 2001), 2001-07 (i.e., July 2001), 2001-07-01 (i.e., January 1, 2001 as 01/01/2001), 2001-01-07-08 01 (i.e., January 1, 2001 at 8:01 AM minus one hour from UTC).

3. Click Measure Charts
Perform Dynamic Network Analysis

4. Select the Dynamic Meta Network

Perform Dynamic Network Analysis

5. Select Custom: Density and Network Centralization, Total Degree, Click Run
Perform Dynamic Network Analysis

6. Add Measure, then view various results

Perform Dynamic Network Analysis

6. continued
Gain Cyber SA

- What could huge increase in Total Degree Centralization mean?
  - Malicious Scanning?
  - Cyber Attack?
  - Systems connecting to external update server?

More Analysis?

- Keep library of known nodes and compare against?
- Other measures that could provide better SA?
  - Weighted density?
  - In degree centralization on nodes inside the network?
    - Could identify targeted attacks
- Periodicity? Days of the week, etc