Destabilizing Dynamic Networks Under Conditions of Uncertainty

Kathleen M. Carley, kathleen.carley@cmu.edu
Jeffrey Reminga, jreminga@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA.
Steve Borgatti, borgatts@bc.edu
Boston College, Boston, MA.

Abstract—*Managing and controlling knowledge intensive dynamic systems requires being able to estimate, analyze, and evaluate, under conditions of uncertainty, the existing system and the impact of actions, such as changes in personnel or resources on this system. Our approach to this problem is dynamic network analysis. Using a combination of statistical and simulation tools, we analyze the robustness under uncertainty of a series of metrics for identifying key entities whose removal from the network destabilizes the network by degrading performance on one or more dimensions. We examine multiple types of uncertainty, including cases of over and underestimation of the presence of relations among entities. We find that higher levels of information assurance are needed for nodes than edges, and that destabilization even under uncertainty can still be disruptive. An illustrative use of this work includes identification of individuals in a covert network to isolate in order to decrease the networks ability to take action.*

1. INTRODUCTION

Covert networks are dynamic entities. To destabilize these networks it is necessary to trace the chains of relationships connecting individuals, knowledge, resources, tasks, events, locations, etc. as they evolve. Destabilization and surveillance strategies need to be evaluated in the context of evolving networks and missing or incorrect information. To ignore either the dynamics or the information assurance issue is liable to lead to erroneous, and possibly devastatingly wrong, policies. For example, isolating a leader in a cellular network may have the same effect as cutting off the Hydra's head; instead of one you know have many leaders [1]. To facilitate such policies two types of tools are needed. First, we need tools for identifying which actor or actors critical [2]. Second, we need tools for estimating the likelihood that the right entity has been identified, as it is rarely the case that full information is known. We approach these interlinked problems using Dynamic Network Analysis [3]. Dynamic network analysis treats the system as a series of interlocked dynamic and probabilistic networks connecting diverse entities such as people, knowledge and tasks.

Traditionally, social network analysis (SNA) has focused on small, bounded networks, with 2-3 types of links (such as friendship and advice) among one type of node (e.g., actors), at one point in time, with close to perfect information. Although a few studies have considered extremely large networks, or two types of nodes (people and events), or unbounded networks (such as inter-organizational response teams); such studies are the exception to the rule. As such little is known about the extent to which the extant measures scale and still enable actors to be discriminated among in large networks or are robust under varying levels of information assurance. Further, what little work has been done on dynamic networks suggests that traditional SNA measures may be less than adequate for discerning critical actors in a complex dynamic environment [4].

What is needed is a dynamic network analysis theory and toolkit. We are working to develop such a tool kit and the associated metrics and decision aids. In this paper, two tools that will form the cornerstone of such a toolkit – DyNet and ORA are used. DyNet is a multi-agent network model of network evolution and destabilization where the destabilization is done under varying levels of information assurance. ORA is a statistical package for locating vulnerabilities in dynamic networks using both traditional SNA measures and new measures designed for the more detailed meta-matrix data [5].

The meta-matrix is a conceptual device where the entities of concern and the relations among them are identified. For this paper, we focus on the entities actors, knowledge and tasks recognizing that other entities such as technology, resources, or events might be added in a more detailed scheme. These entities are connected vis a series of relations shown in table 1. In this paper, we will use these matrices as binary matrices given the focus on the relative impact of social network and dynamic network measures; although, much of our work on ORA deals with non binary data.

Table 1. Meta-Matrix for Dynamic Networks

	Actors	Knowledge	Tasks
Actors	*INT* Interaction or social network	*Fact_Known* Knowledge network	*Prob_Assigned* Assignment network
Knowledge			*Prob_Fact* Needs networks
Tasks			*Task_ Precedence* Precedence network

In this paper, we are using ORA and DyNet to provide initial indicators of the value of isolation destabilization tactics on covert networks. We begin by describing the experimental design used for assessing the robustness of the metrics under varying levels of information assurance, followed by the resultant robustness profiles of selected measures. Then we run a dynamic analysis of the embassy bombing data under no destabilization, destabilization based on degree centrality, and destabilization based on cognitive load. Then we interpret these results in terms of the information assurance information.

2. EXPERIMENTAL DESIGN FOR MEASURE ROBUSTNESS

An important characteristic of a measure is its robustness, or how sensitive a measure is to changes in its input. Our methodology to test measure robustness is a Monte Carlo virtual experiment whereby we repeatedly generate an initial network, introduce error into the network, and then compare the measure values of the initial and perturbed networks.

Parameters

The virtual experiment independent variables and their values are shown in Table 2.

Table 2. Summary of Virtual Experiment

Parameter	**Description**	**Range**
Size	Nodes in the network (size)	10, 25, 50, 100
Density	Density of the network	.01, .02, .05, .1, .3, .5, .7, .9
Type_Error	Type of error in the perturbed network.	Superfluous Edges, Missing Edges, Node Removal
Per_Error	The percentage of nodes/edges that are changed in the initial network given the error type.	0. 1, 5, 10, 25, 50

For each <Size, Density, Type_Error, Per_Error> combination, a Monte Carlo simulation is run in which 100 **initial** networks of size N and density D are generated uniformly at random. Each network is square with edges drawn uniformly at random. Future work will move beyond these ranges of values.

For each of these 100 initial networks, 100 **perturbed** networks are generated by introducing Type_Error of quantity Per_Error into the initial network. The measures for the initial and perturbed networks are then computed and compared.

Error

An initial network is perturbed by one of the following four types of error:

- Superfluous Edges - edges are added uniformly at random to the initial network
- Missing Edges - edges are removed uniformly at random from the initial network
- Missing Nodes - nodes are removed uniformly at random from the initial network.

For the initial results reported in this paper the number of missing edges was set equal to the number of superfluous edges. Further work will remove this assumption.
The amount of error, indicated by the parameter Percent_Error is the percentage of nodes or edges altered when perturbing the initial network.

Measures

We run a series of measures on both the initial and the perturbed network. These measures capture various aspects of what it means for a node to be critical or "key" in a network. We use both standard SNA measures and dynamic network measures. Herein we report on only three such measures – degree centrality, betweenness centrality, and cognitive load. Each of these measures is arguably an indicator of a critical actor [1],[4]. These measures are vector valued, with a single value per actor. In other words, each measure provides a ranking of the actors in terms of their criticality on that measure.

Degree Centrality—The Degree Centrality of a node in a network INT is its degree.

$$Degree\_Centrality_i = \sum_{Individuals\ j \neq i} (INT_{ij} + INT_{ji})$$

Betweenness Centrality—The Betweenness Centrality of node i in a network INT is defined as: across all node pairs excluding i that have a shortest path containing i, the percentage that pass through i. Let SP_{jk} be the shortest sequence of nodes starting with j and ending with k such that

between every node m and the following node n in the sequence, $INT_{mn} = 1$. And, let $CSP_{jki} = 1$ if SP_{jk} contains i and $CSP_{jki} = 0$ otherwise. Using CSP_{jki}, Betweeness Centrality can be defined as follows:

$$Betweenness\_Centrality_i = \frac{\sum_{Individuals\ j \neq i} \sum_{Individuals\ k \neq i,j} CSP_{jki}}{(Num\_Inds - 1)\ (Num\_Inds - 2)}$$

Cognitive Load—The Cognitive Load of node i in a set of networks connecting actors, knowledge, resources, and tasks is defined as the sum of all relations that require cognitive action to be realized. It takes into account the number of other agents, resources, and tasks an agent needs to manage, the difficulty of that management, and the communication needed to engage in such activity. Cognitive load uses not just the interaction network, but also the network linking people to tasks (Prob_Assigned), that linking people to tasks (Fact_Known), the network defining what information is needed for which task (Prob_Fact), and which task needs to be done before which (Task_Precedence).

$$\begin{aligned} Cog\_load = & \sum_{Individuals\ i} (INT_{ij} + INT_{ji}) \\ & + \sum_{\Pr oblems - j} \Pr ob\_Assigned_{ji} + \sum_{Facts - k} Fact\_Known_{ik} \\ & + \sum_{\Pr oblems - j} \sum_{Facts - k} \{\Pr ob\_Assigned_{ji} * \Pr ob\_Fact_{jk}\} \\ & + \sum_{\Pr oblems - h} \sum_{Indivuals - m \neq i} \{\ \Pr ob\_Assigned_{hi} * \\ & \qquad \Pr ob\_Assigned_{hm}\ \} \\ & + \sum_{\Pr oblems - h} \sum_{\Pr oblems - n} \sum_{Indivuals - m \neq i} \{ \\ & \qquad \Pr ob\_Assigned_{hi}\ *\ \Pr ob\_Assigned_{nm}\ * \\ & \qquad (Task\_\Pr ecedence_{hn} + Task\_\Pr ecedence_{nh})\} \\ & + \sum_{\Pr oblems - h} \sum_{Facts - k} \{\Pr ob\_Assigned_{hi} * \Pr ob\_Fact_{hk} \\ & \qquad * \frac{(1 - Fact\_Known_{ik}) * (Num\_Inds - 1)}{\sum_{Indivuals - m \neq i} Fact\_Known_{mk}}\ \} \end{aligned}$$

Note that cognitive load includes degree centrality as it's first term. Further, when all of the networks are random with the same density and size, cognitive load is highly correlated with degree centrality.

Statistics

After introducing the error into the initial network, we run the measure and compare its values with those from the initial network. A variety of statistics are computed. In this paper we report two of these – Pearson's Correlation and top-1. These statistics are computed between the initial network's measure value X and the perturbed network's measure value Y:

Pearson's Correlation—This is the average across all Y perturbations of the standard correlation statistic, computed as: $\frac{Cov(X,Y)}{\sigma_X \sigma_Y}$, where Cov(X,Y) is the co-variance of the vectors X and Y. This captures the extent to which the ranking of the measure on the initial and perturbed matrix are the same. The errors discussed are random and assigned at random to nodes/ties in the network. When these errors systematically impact nodes that are high/low in ranking on some measure more than those that are low/high the correlation between the initially and perturbed will drop. The higher the correlation, the more resilient the measure across information errors, as the percentage error acts like a constant offset for that measure.. Whereas, a low correlation indicates that the measure is not robust to that type of error.

Top-1—This is a very restrictive measure of the accuracy with which the actor that is highest on the measure of concern in the initial network is correctly identified in the perturbed network. It is the percentage of the Y perturbations in which the node labeled highest on measure "Z" is also highest in the initial X network.

Note that when the type of error is Node Removal, the perturbed vector Y has missing nodes, which are treated as missing data in the following manner: the nodes removed from Y are also removed from X and the above statistics are computed with Y and the reduced X.

3. INFORMATION ASSURANCE RESULTS

In general, the higher the percentage error the less like that the top person is correctly identified and the less likely that the overall pattern of the network is correctly discerned. The top-1 measure is slightly more robust for extremely small (size 10) low density (.01) networks; whereas, the Pearson-correlation measure is less robust. Admittedly, such small networks are of little interest and they are the ones where complete information is easiest to locate.

The impact of errors is not linear. For top-1, for both degree and betweenness centrality, we see decreasing effects as the size of the network increases (see e.g., the impact of different levels of node removal on the robustness of degree centrality in Fig. 1.). Further, for top-1, size has a substantially greater impact on measure robustness than density (see tables 3 and 4). Additionally, there is an interaction effect between Percent_Error and size/density. For degree centrality there is no interaction effect due to size and density, whereas there is a slight interaction effect for betweenness. Since in general we may be dealing with large

sparse networks it may be worth expending more effort on locating who is in the network than in tracking down all possible connections.

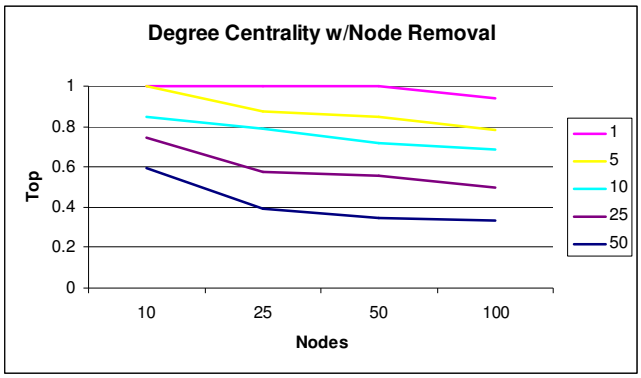

Figure 1. Impact of different percentage of node removal on identification of actor highest in degree centrality

Table 3. Choosing Top-1 Using Degree Centrality

	Node Removal	Edge Removal	Edge Superfluous
Variable	Std.Coeff	Std Coeff	Std Coeff
Per_Error	-1.509***	-1.480***	-1.374***
Size	-0.645***	-0.829***	-0.644***
Density	-0.277***	-0.599***	-0.197
Per_Error ^{2}	0.837***	0.978***	0.980***
Size ^{2}	0.495***	0.586***	0.495***
Density ^{2}	0.243***	0.266*	-0.215*
Per_Error * Size	-0.164***	-0.199***	-0.099
Per_Error * Density	-0.103***	-0.096*	-0.286***
Size * Density	0.033	0.056	0.055
R^2	0.902	0.865	0.858
* <= .05, ** <= .01 *** <= .005			

Finally, we find that in general, for node removal the response surface can be adequately characterized using a second order equation for both degree and betweenness centrality. However, the robustness of the top-1 measure under either edge removal or superfluous nodes is less well characterized by a second order equation suggesting some third order effects. The results suggest that there is a limit to how bad the estimation of the top actor can be, and that using the application of these techniques even on highly incorrect data leads to the accurate location of the key actor more often than would occur by chance (1/number of nodes).

Table 4. Choosing Top-1 Using Betweenness Centrality

	Node Removal	Edge Removal	Edge Superfluous
Variable	Std.Coeff	Std Coeff	Std Coeff
Per_Error	-1.510***	-1.532***	-1.507***
Size	-0.855***	-0.857***	-0.753***
Density	-0.337***	-0.407***	-0.184
Per_Error ^{2}	0.981***	1.030***	1.076***
Size ^{2}	0.613***	0.621***	0.547***
Density ^{2}	0.262*	0.065	-0.249*
Per_Error * Size	-0.243***	-0.211***	-0.101
Per_Error * Density	-0.133***	-0.109*	-0.236***
Size * Density	0.150***	0.112*	0.118*
R^2	0.902	0.863	0.844
* <= .05, ** <= .01 *** <= .005			

As the level of information assurance decreases and more errors are made the overall observed (perturbed) network begins to diverge sharply from the true (initial) network. This can be seen by looking at the correlation measure in Tables 5 and 6. First, we see that the correlation is not a function of the percentage error. There is an indirect effect of percentage error, for both degree and betweenness centrality, where the interaction of error and density further lowers the overall correlation, particularly for errors due to adding or removing edges.

Table 5. Correlation Using Degree Centrality

	Node Removal	Edge Removal	Edge Superfluous
Variable	Std.Coeff	Std Coeff	Std Coeff
Per_Error	-0.368	-0.006	-0.188
Size	1.790***	1.205***	1.323***
Density	1.322***	1.239***	1.604***
Per_Error ^{2}	-0.182	-0.075	0.141
Size ^{2}	-1.351***	-0.774***	-0.967***
Density ^{2}	-0.805***	-0.829***	-1.306***
Per_Error * Size	0.189	-0.264***	0.035
Per_Error * Density	0.055	-0.556***	-0.616***
Size * Density	-0.442***	-0.449***	-0.323***
R^2	0.508	0.658	0.574
* <= .05, ** <= .01 *** <= .005			

Second, we see that where we were less likely to correctly predict the top actor using either degree or betweenness centrality as the size and density of the network increases, we are more likely to achieve a high correlation between the actual and the perturbed network. This suggests that as the size and density of the network grows we will increasingly be able to characterize its overall pattern. Overall, these results show that the response surface for correlation cannot be adequately characterized with a second order equation. Preliminary investigations suggest that a third order equation will be sufficient; however, further determination will

require a much large sample over the space than described herein.

Table 6. Correlation Using Betweenness Centrality

	Node Removal	Edge Removal	Edge Superfluous
Variable	Std.Coeff	Std Coeff	Std Coeff
Per_Error	-0.558***	-0.259	-0.397*
Size	1.830***	1.550***	1.617***
Density	1.644***	1.699***	1.949***
Per_Error ^{2}	-0.060	-0.026	0.266
Size ^{2}	-1.265***	-0.990***	-1.100***
Density ^{2}	-0.978***	-1.148***	-1.486***
Per_Error * Size	0.125	-0.200***	0.010
Per_Error * Density	0.102	-0.392***	-0.540***
Size * Density	-0.531***	-0.538***	-0.464***
R^2	0.724	0.763	0.683
* <= .05, ** <= .01 *** <= .005			

.

We note that the above results are limited in that they do not cover large scale networks. This may not be critical for the top-1 measure where a second order equation is sufficient for characterizing the space, particularly for node removal. If correlation is the issue, then additional analyses and larger networks need to be considered. Further, even for top-1, a slightly better fit might be possible using an explicitly exponential model. Overall, however, these results suggest that as we move to conditions of multiple uncertainties (missing nodes and edges, superfluous nodes due to aliases, etc.) that the overall response surface will become quite complicated. One consequence is that larger networks and a greater portion of the response surface will need to be mapped with simulation. Finally, these results suggest that the ability of the measures to correctly locate the specific actor who is at the top, deteriorates rapidly. Hence, less restrictive measures of metric performance may be called for. This is particularly true as the "top" actors may be hard targets and so a less useful choice.

Note, we have not shown the cognitive load results as when only the social network is permuted (INT) the only portion of cognitive load that changes is the degree centrality portion so its behavior is like that of degree centrality.

4. DESTABILIZATION

We now demonstrate an application of these results to the destabilization of a covert network. Through another project data on the Tanzania embassy bombing was collected (EB data). This is a small data set with information on 16 actors, 8 types of knowledge/resources and 5 tasks - see [4] for details. The overall density of the social network is .12. ORA we identify the most critical or key actors. Wadih al Hage is highest in both degree and betweenness centrality. Whereas, the DNA measures, such as cognitive load, identify Ahmed the German as key. We used DyNet to determine the relative impact of removal of either of these nodes. The results indicate that the removal of Wadih will improve performance, enhance the speed of information diffusion, and maintain the existing resource congruence and so long term performance. Whereas, removal of Ahmed degrades performance, enhances the speed of information diffusion (though not as much as Wadih's removal), and increases resource congruence. Collectively, the combination of changes results in a more rigid less adaptive organizational structure.

We now ask, to what extent are Wadih or Ahmed really the key actors? To do this, we need the best estimate of the fraction missing nodes/edges or superfluous edges. Then these values can be plugged into the response surface mapping equations to generate an error estimate. So, e.g., a if 25% of the nodes are missing then these estimate are only likely to identify the key actor 65% of the time, and if 25% of the edges are missing then the key actor is identified correctly only 57to 59% of the time. Since in fact there are likely to be both missing nodes and missing ties and a smaller number of superfluous ties, the correct identification of the key actor is probably even less likely.

One problem with this application is that a key feature of covert networks is that they are cellular and distributed [6] rather than random. For the EB data, to the extent that there is insufficient data to determine if the network is random or not, then use of errors based on random networks is a reasonable first approximation.

5. CONCLUSIONS

This work demonstrates a procedure for determining the robustness of measures for identifying critical actors in networks and using that information in a dynamic context. Particular attention is placed on the measures degree centrality, betweenness centrality, and cognitive load..

Limitations and Future Work

There are four key limitations to this work. First, the robustness analysis was done using random iid networks. Under such conditions, cognitive load and degree centrality are conceptually similar and so should behave the same in terms of robustness. However, on random iid networks this is likely not to be the case. In deed, even a simple change, such as difference in the density of the task precedence matrix and the social network will engender differences in the robustness profile of centrality and cognitive load. As we move further out to cellular networks, all of the robustness results are likely to change.

Second, the networks that we simulated dynamically were cellular networks. Consequently we were applying robustness indicators assuming random iid networks but

applying them to cellular networks. This is more accurate than using random networks for both portions as this mixed approach let us capture the impact of cultural and organizational factors on the evolving network thus leading to a closer mapping to real data. The key is to ask, given that there are biases in estimating our confidence in the results, how is the bias affecting the conclusion. The distribution of links per node should be more normally distributed and may have a smaller range in random networks than in cellular networks. This difference in distribution when coupled with the nature of cellular networks to be formed of cliques connected through leaders with a broader resource bases and task assignment should mean that SNA centrality measures are less robust under varying level of information assurance than indicated herein and DNA measures, such as cognitive load, are more robust assuming random information errors. Essentially, individuals high in centrality will have fewer links to other entities than will those high in cognitive load; moreover, there is likely to be less variance in observable centrality than on cognitive load across actors. Consequently, these results may be overestimating the ease of correctly identifying the key actors by centrality and underestimating the ease of correctly identifying the key actors by cognitive load. Our next step is to discern the robustness characteristics of the metrics for networks with the same structure as those evolved, with particular attention to cellular networks. When this is done, cognitive load and degree centrality should exhibit different robustness profiles. In future work, the differential impact of the "type of network" on the robustness profile of measures of actor criticality should be considered.

The third limitation has to do with the data used for the evolutionary analysis. The dataset is small particularly in terms of information about tasks and resources. It is likely that were more known here, alternative actors may have been identified as key and the overall system might have appeared easier to destabilize. More generally, the lack of information in terms of tasks and knowledge/resources is diminishing the difference between degree centrality and cognitive load leading them to act similarly. Additional large scale databases are needed to examine this issue.

The final limitation we wish to discuss is the distribution of information errors. In this study, we have examined different kinds of errors; but, in each case the errors were distributed randomly. It is unlikely, however, that this is the case for intelligence operations. Rather, it is likely that the combination of known key actors, available surveillance technology and operatives will combine to generate a very non-random source of errors. Future work should consider the biases in data collection that lead to non-random distributions of error.

Final Comment

These results suggest that likelihood of exactly determining the top actor on any dimension is extremely low with even moderate levels of missing data. Future work should explore whether estimation using cellular rather than random networks can improve on this.

ACKNOWLEDGEMENTS

This paper is part of the Dynamics Networks project in CASOS at CMU. This work was supported in part by the Department of Defense, the Office of Naval Research under grant No. 9620.1.1140071 on Dynamic Network Analysis, DARPA DAAH01-03-C-R111, and the National Science Foundation. Additional support was provided by CASOS – the center for Computational Analysis of Social and Organizational Systems at Carnegie Mellon University (http://www.casos.ece.cmu.edu). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Department of Defense, the Office of Naval Research, Darpa, the National Science Foundation or the U.S. government. Many thanks to Connie Fournelle and ALPHATECH for providing data.

REFERENCES

[1] Carley, Kathleen M. Ju-Sung Lee and David Krackhardt, Destabilizing Networks, *Connections* 24(3):31-34, 2001.

[2] Borgatti, Stephen, "The Key Player Problem," in Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, R. Breiger, K. Carley, & P. Pattison, (Eds.) Comittee on Human Factors, National Research Council,. Pp. 241-252, 2003.

[3] Carley, Kathleen M.,"Dynamic Network Analysis" in Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, R. Breiger, K. Carley, & P. Pattison, (Eds.) Comittee on Human Factors, National Research Council,. Pp. 133-145, 2003.

[4] Carley, Kathleen M., Matthew Dombroski, Max Tsvetovat, Jeffrey Reminga, & Natasha Kamneva, "Destabilizing Dynamic Covert Networks" In Proceedings of the 8th ICCRTS held at the National Defense War College, Washington DC. EBR, Vienna, VA., 2003.

[5] Carley, Kathleen M., "Smart Agents and Organizations of the Future" The Handbook of New Media. Edited by L. Lievrouw & S. Livingstone, Ch. 12 pp. 206-220, Thousand Oaks, CA, Sage, 2002.

[6] Ronfeldt, D. and J. Arquilla, "Networks, Netwars, and the Fight for the Future," First Monday 6(10), September 21, 2001. online: http: //firstmonday.org /issues/issue6_10/ronfeldt/index.htm.