Core Identification and Attack Strategies Against Regenerative Complex Networks

W. Guo and X. Lu

Modeling enemy networks in a way that reveals their key entities and links is important when disrupting complex networks with high redundancy. In this paper, we examine how best to attack such networks under a limited ground intelligence constraint. The key modeling contribution is to include both the heterogeneity of the node functions and the dynamics of recuperation after destruction. Through identifying the core nodes, the results show that ground intelligence should focus on locating and attacking high degree nodes, yielding a 41% reduction in conflict length over random opportunistic targeting and a 23% reduction over specialist targeting. Even when difficult to replace specialists are considered, targeting high degree nodes that can recuperate quickly, remains the most effective method of attack. The impact is to allow military forces to more effectively target enemy nodes that will cause functional paralysis and create further collapses.

Introduction

Conflict Against Complex Organisations

The war on terror has dominated western military engagement in the last 15 years. In total, the war on terror is set to exceed the relative cost of the Second World War. Prolonged military engagement against complex transnational organisations is challenging. The location of key entities are often hidden and require ground intelligence to slowly reveal and target over a short time window. Despite the lack of precise spatial-temporal information of the entities, complex network models can still be constructed based on knowledge of the entities and their connections [1]. Unlike traditional organisations that have a spanning tree structure, complex networks typically have high levels of redundancy at both the functional and topological level [2]. Even the removal of one key entity will often see its functionality restored by other existing or new entities (recuperation). The inability to simultaneously target most of the key entities, coupled with the network's resilience against removal attacks, has greatly contributed to long costly wars. Unlike resilient telecommunication networks (i.e., the Internet [3]), terrorist network nodes have varying functions and can recuperate at different rates. Inspired by a similar complexity in ecology networks [4, 5], this paper will examine how to target such networks.

Methods of Disruption and Contribution

Methods aimed at disrupting the operation of networks need to be tailored towards the nature of the network. For example, conventional surgical strikes, which are aimed at disrupting hierarchical organisations; can be ineffective against networks with a high level of redundancy. Over the past decade, a number of research outputs have focused on using complex network theory to model terrorist organisations, including: microscopic terrorist cells (i.e., the 9/11 network [1]), as well as macroscopic terror networks [6]. However, existing models have been simplistic in that they are mainly focused on *static statistical metrics* such as the overall network's connectivity (link density) or each node's betweenness (path importance) [7]. What has been lacking in the research is a focus on the *dynamics* and *heterogeneity* of terrorist networks, such that new nodes and links are able to form for the purpose of compensating the loss of existing ones. This ability to heal (recuperate) can cause traditional surgical strikes to be even less effective against enemy networks with built in redundancies. This paper will model more realistic enemy networks by adding heterogeneous functions and rates of recuperation. These dynamic features complement the static and statistical measures used in complex network theory to form a more heterogeneous and dynamic model.

Methodology

Dynamic Heterogeneous Network Model

In this short paper, we examine a relatively small terror network based on the 9/11 attack and include all known support nodes [1]. The 9/11 network is chosen because it is well understood and has the same complexity features as larger terrorism networks such as the Al-Qaeda, the Taliban, and ISIS. The 9/11 network comprises of $N = 36$ nodes and $L = 190$ links, which has high levels of topological redundancy when compared to a spanning tree structure (minimum of $L = N - 1 = 35$ links). Each node is assigned a functional skill value s_n to represent its contribution to the overall network. To give a more *general understanding* of how different complex networks behave under removal attacks, we also create a number of parallel networks that have the same N and L parameters [2]: (a) a *rewired* network to maximize topological redundancy; (b) a *small-world* network to create uniform number of hops to connect two nodes; (c) randomized *ecology food web* found in nature; and (d) the *Erdos-Renyi (ER)* network model to benchmark results.

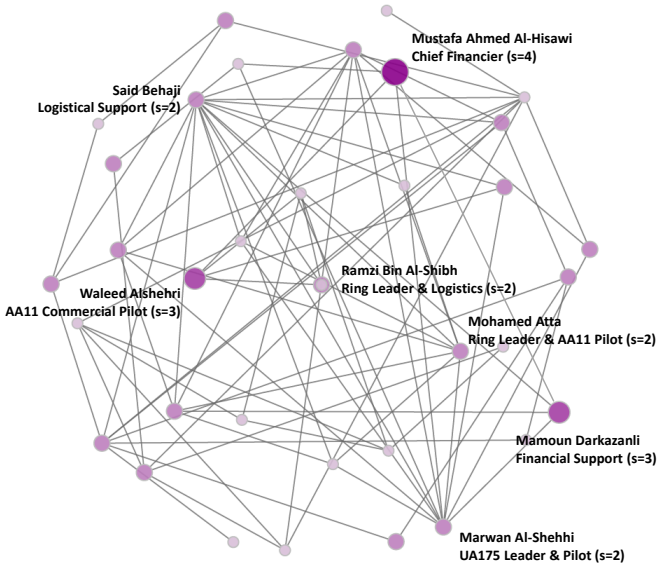

Fig. 1 *9/11 Terrorist Network and Known Associates with Key Nodes Labelled.*

In terms of network heterogeneity, nodes can be generally classified as *specialists* and *generalists* [7]. The distinction is important in terms of how replaceable these nodes are if removed. We define a generalist as having no special skill sets and can be replaced quickly $s_n = 1$. We define specialists have special skill sets and we classify them into three levels ($s_n = [2, 3, 4]$). For this initial study, we define the rate of recuperation r_n as linearly $\propto s_n$ and the percentage of links recuperated as p. It has been argued that complex enemy organisations have leadership nodes that can be easily replaced due to the bottom-up dynamics of such organisations [8]. Conversely, removing nodes with rare technical skill sets that require years to train can be more effective [9]. Fig. 1 shows the 9/11 network with key nodes labelled with their function and the assigned value s_n. Notice how the nodes with the highest skill value s_n do not necessarily have a high degree (d, number of links).

Disruption Strategies

We assume that we cannot removal all the nodes simultaneously due to limited ground intelligence on the nodes' location. We assume we can only get intelligence in one of two manners: 1) random opportunistic intelligence, or 2) targeted intelligence (i.e., identify a node of interest and obtain the location for removal). Hence, the removal process is used in this paper is *sequential removal* of nodes. We measure the robustness of the network and the success of the disruption strategy as: how many removals (X) are required until no links remain between nodes [10]. We consider 3 attack strategies with 500 Monte-Carlo iterations per result:

- Random Opportunity: remove nodes in accordance to emerging ground intelligence or opportunities;
- Highest Degree: remove nodes in accordance to nodes that have the highest degree, implying the node is either a commander or an important communication or logistic hub;
- Highest Specialist: remove nodes in accordance to nodes that have the lowest recuperation rate, disrupting both the function of the network and the rate of overall functional and topological recovery;

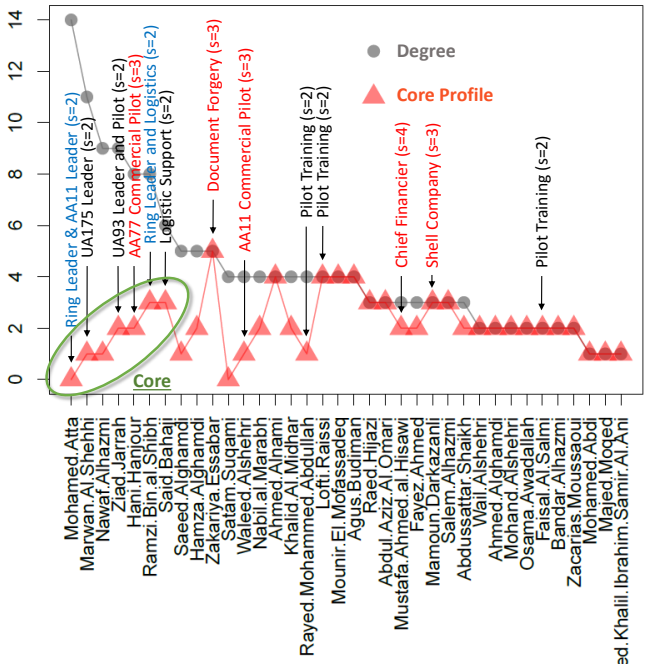

Fig. 2 *Degree and Core Profiling for the 9/11 Terror Network. Specialists are labelled with their corresponding functions and the skill value s_n.*

Table 1: Static Network: Mean No. of Removals before Collapse.

No Recuperation			
Network Type	**Random**	**Degree**	**Specialist**
9/11	27.5	16	21
Rewired	27.5	18.3	23
Small-World	32.0	25.7	27
Food-Web	27.9	18.5	23
Erdos-Renyi (ER)	31.7	25.6	27

Results

Core Identification

The degree (d) of a node in a complex network is defined as the number of links it has with other nodes. The core and periphery are terms associated with nodes which are deemed to have a high and low degree respectively. The core can be found through a recent core-profiling method [11] (as shown in Fig. 2), where it the number of connections each node has with a node that has a higher degree. By ranking the plot in Fig. 2 in descending degree value, the first C nodes before the core profiling value reaches a local maximum is defined as the core (i.e., the first 6-7 names) [11]. Referring to the body of evidence found in the official 9/11 report [12], we can see that this core corresponds to the ring leaders and crucial members of the terrorist group, most of them directly in what became known as the Hamburg Cell. Mohamed Atta (highest degree $d = 14$) is the operational ring leader of the 9/11 operation and received most of the funding and instructions from senior figures Al-Qaeda (including bin Laden).Yet, the key specialist skills reside mostly outside the core nodes. For example, the chief financier M. Ahmed Al-Hisawi and the financial support shell company owned by Darkazanli both have a relatively low degree ($d = 3$).

Robustness to Disruption

In Table 1, we can see two cases: (i) a static heterogeneous network with no recuperation, and (ii) a dynamic heterogeneous network with recuperation that is dependent on the skill of the node $r_n \propto s_n$. We first observe that the robustness (number of removals required for collapse) of the 9/11 network is 12-15% lower than the equivalent complex network models (i.e., rewired, small-world, food-web, and ER). In particular, it is high susceptible to high degree removal strategy, whereby its robustness is 36% lower than the equivalent ER model. We also note that when there is no opportunity for the enemy network to recuperate, due to reasons such as rapid attacks or denial of resources, the high degree removal strategy is superior to removing highly skilled specialists. Compared to random opportunity removal, high degree removal is up to 38% more effective.

Table 2: Dynamic Network: Mean No. of Removals before Collapse.

With Recuperation Rate r and Link Restored p		
Dynamic Network Type	**Degree**	**Specialist**
9/11 ($r = 15s, p = 0.4$)	24	26
9/11 ($r = 15s, p = 0.4$)	25	27
9/11 ($r = 15s, p = 0.6$)	26	30
9/11 ($r = 15s, p = 0.7$)	27	33
9/11 ($r = 15s, p = 0.8$)	28	69

When recuperation is considered (Table 2), we observe two key results. First of all, we note that the number of removals required to achieve collapse is at least 25% higher. The second observation is that we notice degree targeting is largely insensitive to the increased recuperation effects. As the link recuperation ratio p increases by 100%, the number of removals required only increases by 16%, whereas the specialist targeting removal number increases by 165%. Despite recent suggestions that specialist removal can be more effective [9], we have shown that targeting high degree nodes remains the most effective method of attack and is largely insensitive to varying recuperation rates that depends on the specialists' skill level.

Conclusions

In this paper, we have considered how best to attack a complex network through surgical node removal, under an operational constraint of one removal per attack. The results suggest that targeting high degree nodes is still the most effective method for both the static and dynamic network models, even when difficult to replace specialists are considered. The algorithms developed in this paper can be used to identify key military targets and estimate the length of military conflicts. The algorithm itself can be integrated into existing battle and war simulation platforms.

Weisi Guo (*School of Engineering, University of Warwick, UK*)
Corresponding Author Email: weisi.guo@warwick.ac.uk

Xueke Lu (*School of Electronic Engineering and Computer Science, Queen Mary University of London, UK*)

References

1 V. Krebs, "Mapping Networks of Terrorist Cells," *Connections*, vol. 24, 2002.
2 G. Chen, X. Wang, and X. Li, *Fundamentals of Complex Networks: Models, Structures and Dynamics*. Wiley, 2005.
3 H. Zhou and R. Mondragon, "Redundancy and robustness of AS-level Internet topology and its models," *IET Electronics Letters*, vol. 40, 2004.
4 J. Memmott, N. M. Waser, and M. V. Price, "Tolerance of Pollination Networks to Species Extinctions," *Proceedings of the Royal Society of London, Series B: Biological Sciences*, vol. 271, 2004.
5 D. Garlaschelli, G. Caldarelli, and L. Pietronero, "Universal Scaling Relations in Food Webs," *Nature*, vol. 423, 2003.
6 I. Moon and K. M. Carley, "Modeling and Simulating Terrorist Networks in Social and Geospatial Dimensions," *IEEE Intelligent Systems*, vol. 22, 2007.
7 J. Bascompte, P. Jordano, C. Melian, and J. Olesen, "The Nested Assembly of Plant-Animal Mutualistic Networks," *Proceedings of the National Academy of Sciences (PNAS)*, vol. 100, 2003.
8 R. Marion and M. Uhl-Bien, "Complexity Theory and Al-Qaeda: Examining Complex Leadership," *Emergence*, vol. 5, 2003.
9 P. Klerks, "The network paradigm applied to criminal organisations," *Connections*, vol. 24, 2001.
10 J. A. Dunne, R. J. Williams, and N. D. Martinez, "Network Structure and Biodiversity Loss in Food Webs: Robustness Increases with Connectance," *Ecology Letters*, vol. 5, 2002.
11 A. Ma and R. Mondragon, "Rich-Cores in Networks," *PLOS ONE*, vol. 10, 2015.
12 T. Kean and L. Hamilton, "9/11 Commission Report (Chapter 5)," National Commission on Terrorist Attacks Upon the United States, Technical Report, 2004.