2010

# Group-Based Social Network Characterisation of Hidden Terrorist Networks

Belinda A. Chiera
*University of South Australia*

# GROUP-BASED SOCIAL NETWORK CHARACTERISATION OF HIDDEN TERRORIST NETWORKS

Belinda A. Chiera

School of Mathematics and Statistics
University of South Australia
Mawson Lakes, South Australia
belinda.chiera@unisa.edu.au

## Abstract

*Hidden networks arise in high-dimensional network structures when the hidden network members camouflage their existence by appearing randomly connected to the larger network structure, but in reality ensure they remain in persistent contact with one another over time. This paper takes a first step towards determining how to locate such hidden networks through the novel use of group-based social network metrics to characterise the features of hidden networks. Micro, meso and macro-level network analyses of the September 11 network and a selection of popular simulated terrorist network structures will show that the simulated networks are highly visible whereas the hidden networks display low visibility except at the macro level. Moreover these hidden networks aid to camouflage a highly prominent terrorist network of trusted prior contacts.*

**Keywords:** Hidden networks, group-based social network metrics, betweenness centrality, counter-terrorism.

## INTRODUCTION

The global impact of terrorist-driven tragedies such as September 11, 2001 (United States), October 12, 2002 (Indonesia) and July 7, 2005 (United Kingdom) has served to underscore the alarming reality that catastrophic acts of devastation and destruction can be enacted in any place and at any time. These large-scale attacks were coordinated by small, determined networks of individuals who used a number of stratagems to camouflage their identities and connectivity, including: communications network identity ambiguity through the frequent changing of SIM cards or e-mail addresses; minimising or avoiding contact with outsiders to their own network; and changing the flow of communication between the individuals in their network. The latter tactic was adopted to obfuscate the overall terrorist network structure when network members were forced to use communications technology. Such contrivances give rise to a class of persistently connected *hidden networks*. Hidden networks have a two-level structure encompassing firstly the individuals belonging to the network, followed by the network itself. At the individual level, network members appear randomly connected to the vast background communications network, although not necessarily to one another. At the network level however, a communications path comprising the network members, at the minimum, is preserved to provide an unimpeded communications flow.

Detecting hidden networks is a difficult problem in practice. These networks are small (*e.g.* the September 11 network consisted of 19 terrorists (Krebs, 2002)) and they have limited external connectivity, if any. To date, there has been little work on this emerging area of research. Previous efforts (Baumes et al., 2004) modelled hidden networks as non-random graph structures adopting the appearance of randomness. It was found that hidden networks were detectable up to a particular threshold of background network density, beyond which they became virtually impossible to detect.

Other efforts included using cosmological theory and clustering techniques to detect hidden events that are not directly observable (Maeno and Yukio, 2006). In (Skillicorn, 2004) Singular Value Decomposition was used to detect the presence of unusual correlations as an indicator of terrorist activities. The method was successfully demonstrated using a simulated network containing widespread diffuse correlation, however scalability cannot be ensured unless the data are sparse. In (Chawathe, 2010) a computationally intensive method of detecting frequently occurring graph patterns to identify hidden networks was proposed, coupled with offline data mining and real-time monitoring.

In this paper we take the novel step of using *group-based social network metrics* to characterise the structure of hidden networks as a first step towards locating hidden networks, using the September 11 terrorist network of (Krebs, 2002) as our network structure. We postulate a group-based analysis is relevant since a hidden network is still subject to:

1. ***The existence of communication:*** *to enable information sharing between hidden network members; and*
2. ***Fundamental behavioural roles:*** *such as commencing communication and relaying information across the hidden network. These roles exist irrespective of which individual fulfills them.*

Moreover, hidden networks may be more difficult to detect depending upon whether they are analysed at the micro-, meso- or macro-level. We address this issue by performing a tri-level group-based characterisation of a hidden network at each of these levels.

This paper is outlined as follows. In Section 2 we introduce a collection of group-based social network metrics used for micro-, meso- and macro-level analyses, and discuss one way to determine the expected appearance of a hidden network. In Section 3 we analyse the September 11 terrorist network of (Krebs, 2002) against a collection of simulated network structures to determine the similarities and differences between these networks, including their ease of detectability, when viewed from a group perspective at the micro-, meso- and macro-network levels. Finally, we give our conclusions and future directions in Section 4.

## CHARACTERISING HIDDEN TERRORIST GROUPS USING GROUP-BASED SOCIAL NETWORK METRICS

Social network metrics are typically designed to capture different facets of communication between individuals within a graph-based network structure, and are subsequently reliant upon representing the communications network as a graph consisting of nodes (individuals), and edges (lines of communications between individuals). Although we intend to use group-based social network metrics in this work, we still require a graph-based representation of a communications network. We correspondingly define a graph $\mathcal{G}$, consisting of nodes $v_i \in \mathcal{V}$ and edges $e_{ij} \in \mathcal{E}$ connecting nodes $v_i, v_j$ such that a communications network can be expressed as $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$.

### Micro Level Analysis

For a micro-level analysis we will calculate group degree and group betweenness centralities. Degree centrality captures the number of connections (edges) a person (node) of interest has to other nodes in the network. An individual with high degree centrality would have many connections to others in the network and would thus be highly prominent within the network itself. The group-based equivalent can be similarly interpreted as it captures prominence of a *group* $\mathcal{H}$, to the remainder of the network, $\mathcal{G} - \mathcal{H}$. For a true hidden network we would expect low prominence.

Normalised group degree centrality (NGDC) can be defined as (Everett and Borgatti, 2005):

$$NGDC = \frac{|N(\mathcal{H})|}{|\mathcal{V}| - |\mathcal{H}|} \tag{1}$$

where $N(\mathcal{H})$ is the set of all nodes $v_i \in \mathcal{V}$ such that $v_i \notin \mathcal{H}$ but are adjacent to a member of $\mathcal{H}$.

Betweenness centrality is a social network metric used to identify, for each node (person) in the network, the proportion of all paths of a specific type (*e.g.* shortest paths) in the network that pass through a node of interest. From a social network perspective, the worth of betweenness centrality is in its usage to capture the control of information flow through the network (Wasserman and Faust, 1994). This concept is similarly extended to a group $\mathcal{H}$ to indicate how likely it is a hidden group of interest would appear on a network path of interest and thus their role in information flow throughout the network $\mathcal{G}$. A normalised group-based betweenness centrality (NGBC) metric can be defined as (Everett and Borgatti, 2005)

$$NGBC = \frac{2\sum_{u<v} \frac{g_{u,v}(\mathcal{H})}{g_{u,v}}}{(|\mathcal{V}| - |\mathcal{H}|)(|\mathcal{V}| - |\mathcal{H}| - 1)} \tag{2}$$

where $g_{u,v}$ is the number of shortest paths connecting nodes $u, v \notin \mathcal{H}$, $g_{u,v}(\mathcal{H})$ is the number of shortest paths passing through $\mathcal{H}$ with the maximum possible number being $(|\mathcal{V}|-|\mathcal{H}|)(|\mathcal{V}|-|\mathcal{H}|-1)/2$.

## Meso-Level Analysis

For a meso-level analysis we will compute the total centrality and dyadic contributions of a hidden network based on group degree and group betweenness centrality. Total centrality gauges the contribution each hidden network has on the network structure as a whole, whereas dyadic contributions lend insight into the intra-network effect a hidden network has on the remainder of the network.

If $f$ is a graph-invariant (a centrality measure, *e.g. degree,* depending only on the graph structure) and $\mathcal{G}$ contains a node of interest $\chi$, representing the individuals that form the hidden network, then the induced centrality $C_f$ of $\chi$ is (Everett and Borgatti, 2010):

$$C_f(\chi) = f(\mathrm{G}) - f(\mathrm{G}-\chi)$$

where $\mathcal{G}-\chi$ is the network $\mathcal{G}$ with node $\chi$ deleted. Extending this definition to the difference between induced centralities when node $\chi$ is and is not present, we obtain the so-called total centrality of $\chi$ (Everett and Borgatti, 2010)

$$C_\tau(\chi) = \sum_{j \in \mathcal{V}(\mathcal{G})} C(j) - \sum_{j \in \mathcal{V}(\mathcal{G}-\chi)} C'(j)$$

where $\mathcal{V}(\mathcal{G})$ is the node set defined on $\mathcal{G}$, $C$ is a centrality metric calculated on $\mathcal{G}$ and $C'$ is calculated on $\mathcal{G}-\chi$.

The dyadic contribution of a hidden network is defined in (Everett and Borgatti, 2010) for an adjacency matrix $P$. If $p_{ij} \in P$ is the difference between node $j$'s centrality when $i$ is present and when $i$ is absent ($i$ being the hidden network, $j$ a node in the remainder of the network), then

$$p_{ij} = C_{\mathcal{G}}(j) - C_{\mathcal{G}-i}(j)$$

where $C_{\mathcal{G}}(j)$ is the centrality of node $j$ in $\mathcal{G}$ and $C_{\mathcal{G}-i}(i) = 0$.

## Macro-Level Analysis

Network centralisation metrics (degree, betweenness centrality) can be transformed to obtain a macro-level analysis of a network structure (Borgatti et al., 2002:Wasserman and Faust, 1994)

$$\text{Centralisation} = 100 * \frac{\sum C^* - C_i}{\max \sum C^* - C_i}$$

where $C^*$ is the most central entity in the network $\mathcal{G}$ and $\max \sum C^* - C_i$ is the largest possible centralisation possible computed using a star network structure.

There is an important distinction between centrality and centralisation; centrality reflects the prominence of a group in the network, whereas centralisation refers to the overall cohesion of the network and thus lends itself to macro-analysis. Moreover, centralisation indicates the prominence of a hidden network within a larger network structure which translates to vulnerability, should the hidden network be compromised.

## How "Should" a Hidden Network Look?

In (Lindelauf et al., 2009) a trade-off between a hidden network's need for secrecy versus information flow was analysed to provide an indication of the optimal structure for a hidden network, in a Nash equilibrium sense. The *secrecy* $S$ of the optimally structured hidden group $\mathcal{H}' \in \mathcal{G}$ is (Lindelauf et al., 2009)

$$S(\mathcal{H}') = \sum_{i \in \mathcal{H}'} \alpha_i u_i$$

where $\alpha_i$ is the exposure probability of individual $i$ in $\mathcal{H}'$. An information measure for $\mathcal{H}'$ was also defined (Lindelauf et al., 2009)

$$I(\mathcal{H}') = \frac{n(n-1)}{T(\mathcal{H}')}$$

with $\mathcal{H}'$ being the network structure maximising $S(\mathcal{H}')I(\mathcal{H}')$. This solution was successully applied in (Lindelauf et al., 2009) to the 2002 Jemaah Islamiyah Bali terrorist network. Here we will investigate the applicability of this trade-off to the 9/11 network when compared with using a standard clique-based search approach for detecting hidden network structures.

## TERRORIST NETWORK ANALYSIS

To characterise the group-based structure of hidden networks, we analysed the September 11 network (Krebs, 2002) (hereafter referred to as the 9/11 network), reproduced in Figure (1) with $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\} = \{19,27\}$. A collection of simulated network structures were also produced to determine how the 9/11 network structure differs from, or is similar to, randomly generated network structures of similar size and structure, when viewed at a group level.

Simulated networks were generated as: (i) Erdös Rényi networks with the same node properties as the 9/11 network; (ii) Barabási networks, which replicate power-law connectivity within a network; and (iii) Strogatz-Wallis (or small-world) networks, designed to capture the linking of stranger nodes in a network through mutual acquaintanceships. We generated 1,000 network structures of each type. Erdös Rényi and Strogatz-Wallis networks are popularly used in the literature (Baumes et al., 2006, Baumes et al., 2004) to represent terrorist networks and it is of interest to determine whether they successfully capture the structure of hidden networks when viewed from a group-based perspective.

Further simulated networks were produced using UCINET (Borgatti et al., 2002) such that each randomly generated network possessed the same marginal structure of the original 9/11 network (based on the network adjacency matrix). Again 1,000 of each network type, Krebs975, Krebs500, and Krebs275, were randomly generated. The values of 975, 500 and 275 represent the cut-off probabilities of 0.975, 0.500 and 0.275 respectively, used to determine whether or not a link was randomly generated between two nodes. To facilitate the comparison between the actual and simulated network, we computed normalised centralities for all three levels of analysis.

Four hidden networks were identified within the 9/11 network (Figure (1)) based on the individuals on-board the following flights:

1. ***AA Flight # 77:*** *represented by the orange* ▽ *nodes;*
2. ***UA Flight # 93:*** *represented by the blue* ◊ *nodes;*
3. ***AA Flight # 175:*** *represented by the purple* □ *nodes; and*
4. ***UA Flight # 11:*** *represented by the green* ○ *nodes.*

A fifth hidden network — **Trusted Priors** — was formed from a group of individuals previously known to one another (Atta, Al-Shehhi, Hanjour, Jarrah, S. Alhazmi and N. Alhazmi). A tri-level analysis of the 9/11 and simulated network structures based on these five hidden groups was conducted, the details of which are reported next.

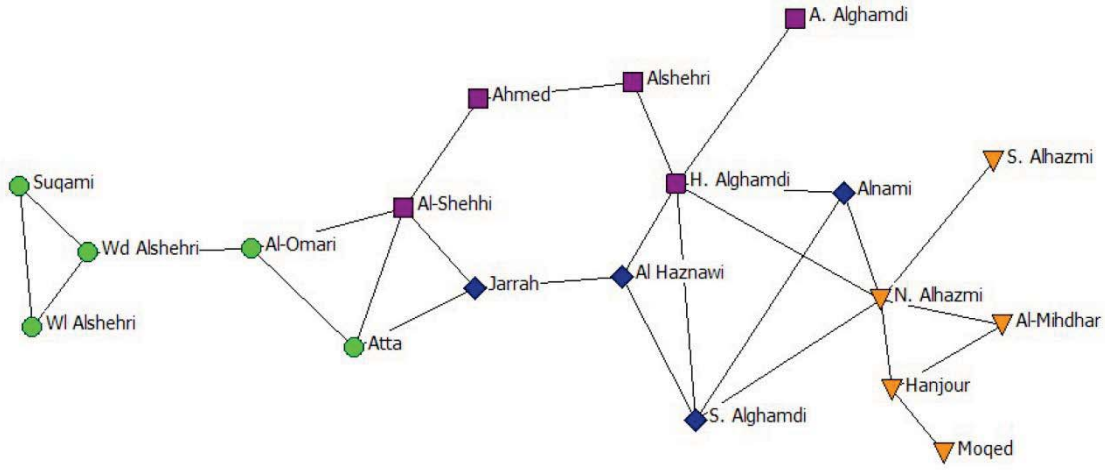



*Figure 1: A Reproduction Of The September 11 Terrorist Network From (Krebs, 2002).*

## Micro-Level Analysis

The micro level group-based social network metrics were computed using UCINET (Borgatti et al., 2002) and custom-written scripts in Perl and R (R, 2010). Group degree centralities were calculated for all 1,000 networks of each type, from which averages were calculated and normalised. A selection of group degree centrality distributions for the Kreb975 network along with their mean and standard deviation statistics are presented in Figure (1). It can be seen the centralities are Normally distributed, thereby supporting the use of an average statistic. For reasons of space consideration, not all distributions are presented here, however it should be noted the degree and betweenness distributions for the remaining simulated networks were similar to those of Figure (2).

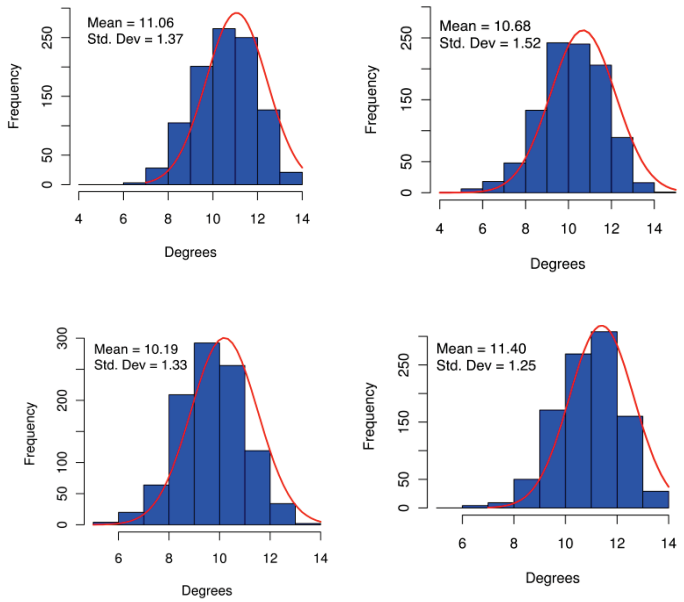



*Figure 2: Histograms Of The Raw Group Degree Centralities For The Krebs975 Network.*

The normalised group degree centralities are presented in Table (1), from which it is interesting to note that the centralities of Flights AA #77, UA #93 and UA #11 are considerably lower than those generated by the random

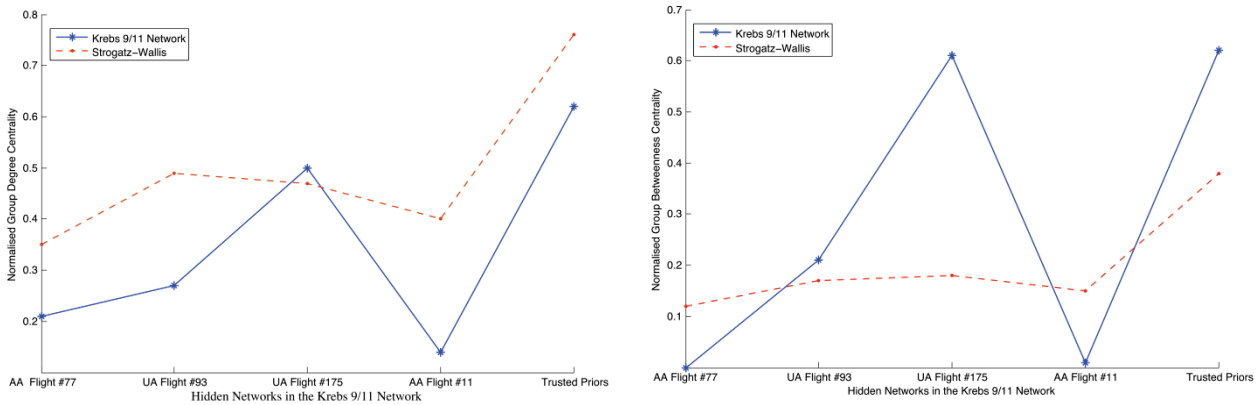
graph structures. Low centralites indicate the hidden networks are not prominent, whereas their simulated counterparts display higher prominence, meaning they would render themselves more easily detectable.

*Table 1: Normalised Group Degree Centralities*

| Network Type | Normalised Degree | | | | |
|---|---|---|---|---|---|
| | AA Flight #77 | UA Flight #93 | UA Flight #175 | AA Flight #11 | Trusted Priors |
| **Krebs 9/11 Network** | **0.21** | **0.27** | **0.50** | **0.14** | **0.62** |
| Krebs975 | 0.79 | 0.71 | 0.81 | 0.73 | 0.86 |
| Krebs500 | 0.79 | 0.72 | 0.82 | 0.74 | 0.87 |
| Krebs275 | 0.79 | 0.72 | 0.82 | 0.76 | 0.87 |
| Erdös Rényi | 0.57 | 0.72 | 0.59 | 0.58 | 0.66 |
| Barabási | 0.70 | 0.29 | 0.29 | 0.25 | 0.48 |
| Strogatz-Wallis | 0.35 | 0.49 | 0.47 | 0.40 | 0.76 |

More prominent however, are the hidden networks of UA Flight #75 and the Trusted Priors group. Intriguingly, it appears that while the latter network is highly prominent (due to the wealth of internal and external connectivity of its members), once these members are allocated to other hidden network structures, they essentially camoflauge their connectivity by hiding within less prominent networks.

Of the simulated networks only the Erdös Rényi network is able to replicate the prominence of one 9/11 hidden network (Trusted Priors), with a normalised degree centrality in the vicinity of 0.62. While the Strogatz-Wallis model did not capture the values of the group degree centralities, it almost perfectly captured their trend (Figure (3) (a)), suggesting a structural similarity between the 9/11 and the Strogatz-Wallis simulated network.




(a) (b)

*Figure 3: The Normalised Group Degree (a) and Betweenness (b) Centralities Of The Krebs 9/11 Network And The Strogtaz-Wallis Network.*

The normalised group betweenness centralities are presented in Table (2) where a large value indicates that the hidden network appears on a large proportion of shortest paths through the network, which we would expect to control how or if information is passed through the network. Once again there is a marked difference between the actual and simulated structures, with the exception of the Flight UA #93 network. Interesting to note is that Flight AA #77 has no group betweenness centrality and is effectively invisible as a group, even though the individual members may not be. This suggests very little interaction between this group and the remainder of the network, making them less easily detectable. Indeed, the only group member easily distinguishable in this case would be Jarrah, which is by virtue of his membership to the more prominent Trusted Priors group. The Strogatz-Wallis model has again captured the overall trend of the 9/11 network group betweenness centralities (Figure 3 (b)) indicating that at the micro-level, the Strogatz-Wallis model reflects the structural properties of the 9/11 network.

Finally, it was of interest to determine how a terrorist network "should" look. Using a standard clique-based search to detect hidden network structures, we used UCINET (Borgatti et al., 2002) to form cliques from the 9/11 network. The results in Table (3) show that for a minimum clique size of 4 (the minimum hidden network size in the 9/11 network), only one clique is formed, comprising N.Alhazmi, S.Alhazmi, Alnami and H. Alghamdi. Notably these members do not belong to the same hidden network in Figure (1).

The normalised group degree and betweenness centralities indicate a prominent clique, which contradicts the low prominence of the 9/11 subgroups. Reducing the minimum clique size to 3, results in the formation of 6 cliques, most of which are also highly prominent.

*Table 2: Normalised group betweenness centralities*

| | Normalised Betweenness | | | | |
|---|---|---|---|---|---|
| Network Type | AA Flight #77 | UA Flight #93 | UA Flight #175 | AA Flight #11 | Trusted Priors |
| **Krebs 9/11 Network** | **0.00** | **0.21** | **0.61** | **0.01** | **0.62** |
| Krebs975 | 0.18 | 0.16 | 0.22 | 0.16 | 0.32 |
| Krebs500 | 0.18 | 0.16 | 0.22 | 0.17 | 0.32 |
| Krebs275 | 0.18 | 0.16 | 0.22 | 0.17 | 0.32 |
| Erdös Rényi | 0.26 | 0.19 | 0.26 | 0.26 | 0.34 |
| Barabási | 0.50 | 0.15 | 0.13 | 0.07 | 0.42 |
| Strogatz-Wallis | 0.12 | 0.17 | 0.18 | 0.15 | 0.38 |

*Table 3: Summary Of Group Centrality Measures For UCINET (Borgatti Et Al., 2002) Generated Cliques*

| Clique | Clique Sizes | Degree | Betweennness |
|---|---|---|---|
| Size 3 | (4,3,3,3,3,3) | (0.38, 0.31, 0.31, 0.19, 0.19, 0.06) | (1.17 , 1.34 , 3.26 , 2.29 , 1.90) |
| Size 4 | 6 | 0.4 | 4.68 |

In contrast, the theorised networks of (Lindelauf et al., 2009) that trade off between group secrecy and information efficiency, shows a greater similarity of structure when compared to the actual hidden networks (Figures (6) and (7)). The theorised four-node network indicates a structural similarity to the 9/11 network, however the actual hidden network contains one less communication path. The five-node theorised structure replicates the 9/11 hidden network containing Atta, Omari and others, and is almost identical to that containing Moqed, Hanjour and others. It appears that in place of clique-based searching of hidden network structures, it may be of higher value to use the methods, or variations of, those outlined in (Lindelauf et al., 2009).

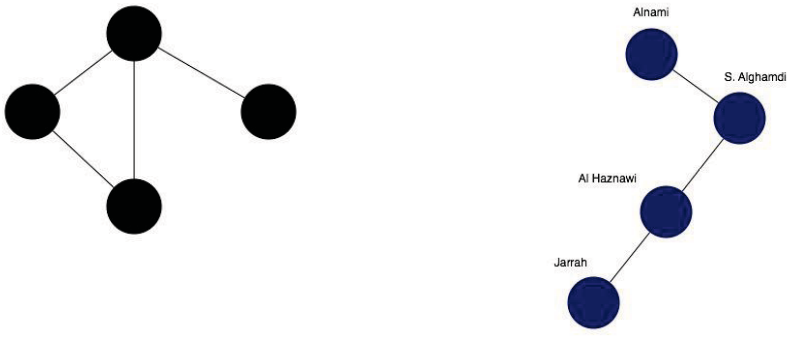



*Figure 6: The Idealised 4-Node Group Structure Of (Lindelauf Et Al., 2009) (Black, Unlabelled Graph) Versus The 9/11 4-Node Subgroup Structure.*

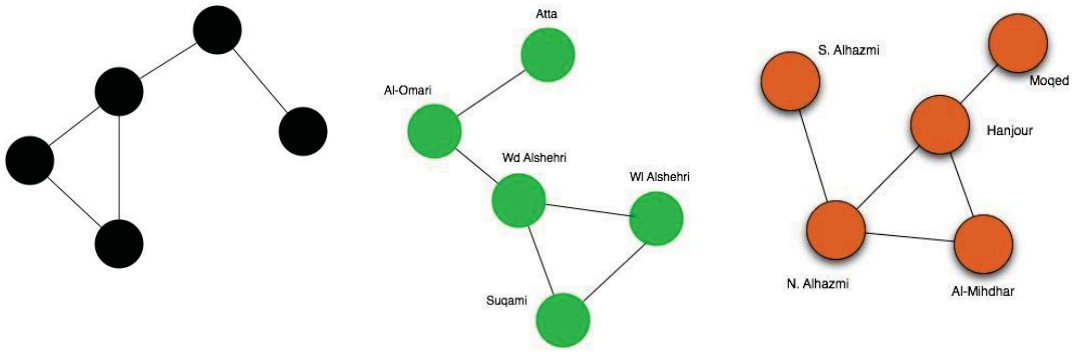



*Figure 7: The Idealised 5-Node Group Structure Of (Lindelauf Et Al., 2009) (Black, Unlabelled Graph) Versus Two Of The 9/11 5-Node Subgroup Structures.*

## Meso-Level Analysis

At the meso-level the total and dyadic centralities of group degree and betweenness centrality were computed to determine the effect each hidden network has on the whole network structure and on the remainder of the network. The results are given in Tables (4) and (5), where entries labelled by the network structure contain the total centralities.

*Table 4: Total Centrality And Dyadic Decomposition Of The Group Degree Of The Hidden Networks*

| | Total Centrality Decomposition: Degree | | | | |
|---|---|---|---|---|---|
| Network Type | AA Flight #77 | UA Flight #93 | UA Flight #175 | AA Flight #11 | Trusted Priors |
| **Krebs 9/11 Network** | **0.50** | **0.60** | **1.07** | **0.36** | **1.31** |
| **Dyadic** | **0.21** | **0.27** | **0.50** | **0.14** | **0.62** |
| KrebsFixed975 | 1.21 | 1.09 | 1.28 | 1.14 | 1.43 |
| *Dyadic* | 0.56 | 0.51 | 0.60 | 0.53 | 0.67 |
| KrebsFixed500 | 1.20 | 1.09 | 1.28 | 1.13 | 1.43 |
| *Dyadic* | 0.57 | 0.51 | 0.60 | 0.54 | 0.68 |
| KrebsFixed275 | 1.19 | 1.08 | 1.29 | 1.19 | 1.44 |
| *Dyadic* | 0.56 | 0.50 | 0.61 | 0.57 | 0.68 |
| Erdös Rényi | 1.22 | 1.04 | 1.24 | 1.22 | 1.39 |
| *Dyadic* | 0.58 | 0.50 | 0.59 | 0.58 | 0.66 |
| Barabási | 1.46 | 0.59 | 0.61 | 0.52 | 1.01 |
| *Dyadic* | 0.47 | 0.29 | 0.29 | 0.25 | 0.47 |
| Strogatz-Wallis | 0.76 | 1.05 | 1.01 | 0.88 | 1.59 |
| *Dyadic* | 0.35 | 0.49 | 0.47 | 0.40 | 0.76 |

The total group degree centrality decompositions indicates that besides the Strogatz-Wallis simulated networks, all other simulated network structures both over- and underestimated the prominence of the 9/11 network at the meso-level. The centralities for the Strogatz-Wallis networks followed the same trend as the 9/11 network, however surprisingly, the simulated Krebs-based networks produced centralities closer to those of the Erdös Rényi networks, rather than the actual 9/11 network upon which they were based. The exception was the Trusted Priors group, for which the results were comparable. The results for the dyadic entries showed that the simulated networks produced similar centralities to all groups barring AA Flight #11, for which the original centrality was quite low, indicating this particular group was of low prominence and could be considered well hidden.

Both the overall effect on the network structure as well as the dyadic effects of each hidden network are far more prominent than reported thus far, when considering group betweenness centrality (Table (5)). The

increased prominence may stem from the need to pass information both between hidden network members and across hidden networks, to allow the 9/11 network to function. The positive values in Table (5) indicates hidden networks which aid to *reveal* the presence of other nodes in the 9/11 network. In particular, the UA Flight #175 and the Trusted Priors networks both raise the prominence of the overall network structure, rendering it more easily detectable. In contrast, the negative values in Table (5) indicates a particular network that will *conceal* the presence of other nodes in the 9/11 network, by reducing their betweenness. This is a powerful feature as it can be used to decrease the detectability of the network as a whole.

*Table 5: Total Centrality And Dyadic Decomposition Of The Group Betweenness Of The Hidden Networks*

| | Total Centrality Decomposition: Betweenness | | | | |
|---|---|---|---|---|---|
| Network Type | AA Flight #77 | UA Flight #93 | UA Flight #175 | AA Flight #11 | Trusted Priors |
| **Krebs 9/11 Network** | **0.19** | **-0.30** | **-0.51** | **0.19** | **0.72** |
| **Dyadic** | **0.19** | **-0.51** | **-0.79** | **0.19** | **0.36** |
| KrebsFixed975 | 0.14 | -0.22 | -0.35 | -0.19 | -0.27 |
| *Dyadic* | -0.34 | -0.22 | -0.35 | -0.19 | -0.27 |
| KrebsFixed500 | 0.14 | -0.22 | -0.35 | -0.19 | -0.25 |
| *Dyadic* | -0.34 | -0.22 | -0.35 | -0.19 | -0.25 |
| KrebsFixed275 | 0.15 | -0.22 | -0.35 | -0.20 | -0.26 |
| *Dyadic* | -0.34 | -0.22 | -0.35 | -0.20 | -0.26 |
| Erdös Rényi | 0.03 | -0.19 | -0.22 | -0.24 | -0.19 |
| *Dyadic* | -0.21 | -0.19 | -0.22 | -0.24 | -0.19 |
| Barabási | 0.77 | 0.22 | 0.09 | -0.03 | 0.34 |
| *Dyadic* | 0.31 | 0.22 | 0.09 | -0.03 | 0.34 |
| Strogatz-Wallis | -0.08 | -0.38 | -0.33 | -0.25 | -0.32 |
| *Dyadic* | -0.19 | -0.38 | -0.33 | -0.25 | -0.32 |

Finally, both the Erdös Rényi and Strogatz-Wallis networks underestimate the meso-level impact the subgroups have on the 9/11 network, whereas the Krebs 275, 500 and 975 networks capture the value, but not necessarily the sign, of these meso-level contributions. However these networks require knowledge of the actual 9/11 network structure, which is not as useful when locating a hidden network unless there is a factual understanding of its structure.

## Macro-Level Analysis

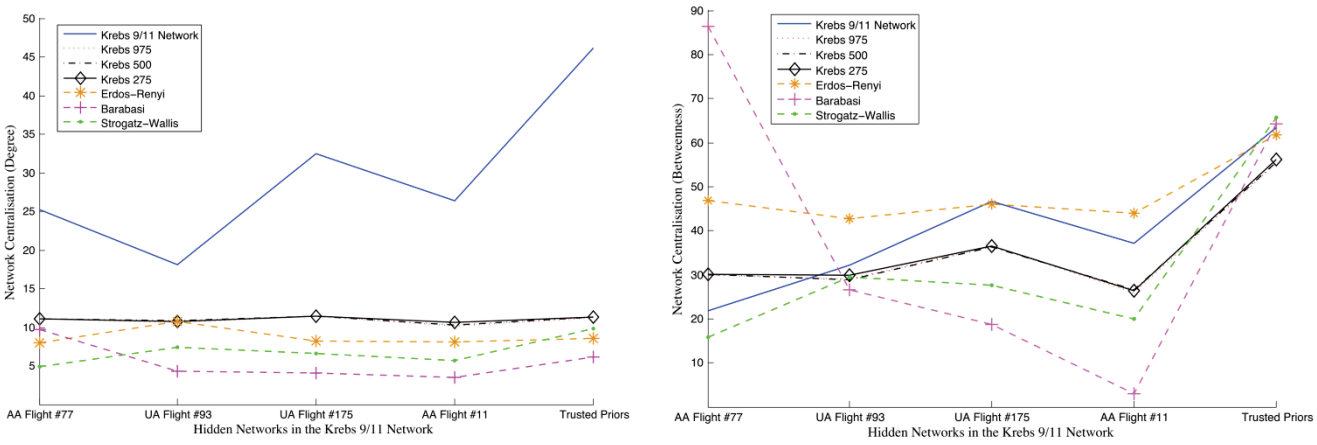
At the macro-level, centralisation percentages of group centrality metrics (degree, betweenness) were calculated for each network type, with results as shown in Figures (6) (a) and (b). From group degree centralisation it can be seen that the 9/11 terrorist network is now more visible, as opposed to when viewed at the micro- and meso-levels.

Most prominent are the UA Flight #175 and the Trusted Priors hidden networks and thus compromising either group would have made the overall 9/11 network more vulnerable to detection. At the macro level, it is interesting to see that the Erdös Rényi and Strogatz-Wallis networks are considerably less prominent and do not capture the trend of the 9/11 network.

A different result emerges from the centralisation of group betweenness centrality; Figure (6) (b) indicates an important distinction — all but Flight AA #77 are now highly prominent. This suggests that the need for information flow between group members cannot be successfully camouflaged at the macro-level, even though it was successfully concealed at the micro- and meso-levels.

Finally it should be noted that as with all analyses, there are naturally limitations that come with the research presented here; in particular the understanding of the 9/11 network relies upon the social network metrics chosen, as differing metrics will provide different viewpoints of the same network structure. Specifically, group degree centrality is designed to capture the most richly connected group in a network, however the metric is very much dependent upon the definition used; here we counted multiple ties to the same individual within a group of interest once only, however this definition does not take into account the strength of the relationships between individuals inside the hidden group to those outside the hidden group. It may be that it would be more useful to capture the combined weights of these relationships, rather than the existence of a relationship itself. It is further conceivable that there would be individuals considered to be more valuable to the organisation than

others (in a non-social networks sense), and thus capturing this worth could provide greater insight into the




(a) (b)

analysis of hidden groups. Group degree centrality also does not take into

*Figure 6: Centralisation Of (a) Group Degree And (b) Group Betweenness Centrality For All Network Types. Note That The The Krebs 275, 500 And 975 Networks Are Barely Distinguishable From One Another.*

account the indirect ties of a hidden group, which could also provide useful information about the detectability of such groups. Similarly, the definition of group betweenness centrality used here relies on detecting the presence of hidden groups on many shortest paths in the network, however it may be that a terrorist network of the size of the 9/11 network would not rely upon shortest paths for information flow, and may prefer circuitous information paths to help coneal communications patterns. Irrespective of these limitations however, the results presented here have provided a crucial first step in understanding the usefulness and applicability of group-based social network metrics for the detection of hidden groups, and combined with the limitations addressed here, will form the focus of future research.

## CONCLUSION AND FUTURE DIRECTIONS

The detection of small hidden networks in high-dimensional network structures is a difficult problem. In this paper we investigated the novel approach of characterising these hidden networks using group-based social network degree and betweenness centrality metrics applied at micro-, meso- and macro-network levels. We characterised the September 11 network as well as a collection of simulated network structures. It was shown that the hidden networks contained within the September 11 network predominantly displayed low prominence, when compared with their simulated counterparts. Erdös Rényi and Strogatz-Wallis network structures were able to capture the group-based social network trends at the micro- and meso-levels, but not at the macro-level. Also, when viewing hidden networks at the macro-level, it was demonstrated that they become more easily detectable through the centralisation of group betweenness centrality. Future work will involve utilising the results presented here to construct a methodology to locate small network neighbourhoods of interest that hide within high-dimensional networks.

## REFERENCES

Baumes, J., Goldberg, M., Hayvanovych, M., Magdon-Ismail, M., Wallace, W. and Zaki, M. (2006) "Finding Hidden Group Structure in a Stream of Communications". In *IEEE Intnl Conf. on Intelligence and Security Informatics,* 3975, San Diego, CA.

Baumes, J., Goldberg, M., Hayvanovych, M., Magdon-Ismail, M., Wallace, W. and Zaki, M. (2004) "Discovering Hidden Groups in Communication Networks". In *Proc. 2nd NSF/NIJ Symposium on Intelligence and Security Informatics*.

Borgatti, S.P., Everett, M.G. and Freeman, L.C. (2002) "Ucinet for Windows: Software for Social Network Analysis". Harvard, MA: Analytic Technologies.

Chawathe, S.S. (2010) “Tracking Hidden Groups Using Communucations”. *Lecture Notes in Computer Science,* 2665:195-208.

Everett, M.G. and Borgatti, S.P. (2010) “Induced, endogenous and exogenous centrality”. *Social Networks,* doi:10.1016/j.socnet.2010.06.004.

Everett, M.G. and Borgatti, S.P. (2005) “Extending centrality”. In P. Carrington, J Scott, S. Wasserman (eds) *Models and Methods in Social Network Analysis.* Cambridge University Press: Cambridge:57-76.

Krebs, V. (2002) “Mapping networks of terrorist cells”. *Connections***,** 24(3): 43-52.

Lindelauf, R., Borm, P. and Hamers, H. (2009) “On Heterogeneous Covert Networks”. In N. Memon *et al*. (eds) *Mathematical Methods in Counterterrorism,* Springer-Verlag, Wien: 215-228.

Maeno, Y. and Yukio, O. (2006) “Hidden structure visualization adaptive to human's prior understanding”. *Joint Conf. Information Sciences 2006*, Taiwan.

R Development Core Team (2010) “R: A Language and Environment for Statistical Computing”. R Foundation for Statistical Computing, Vienna, Austria, http://www.R-project.org.

Skillicorn, D. (2004) “Finding unusual correlation using matrix decompositions”. *Lecture Notes in Computer Science*, 3073/2004:83-99.

Wasserman, S. and Faust, K. (1994) “Social Network Analysis: Methods and Applications”, Cambridge University Press, 857 pages.