Modelling Terrorist Networks
CD Dissertation (Whole Unit)

Candidate Number: 564456

March 17, 2011

Abstract

Network theory is a powerful tool that allows scientists to mathematically model complex organisational structures as a collection of distinct components interacting in some manner. I examined four analytical network metrics; degree, eigenvector centrality, betweenness centrality and local clustering coefficient, as a method of revealing specific network features and structural elements. Modelling terrorist organisations using simple, unweighted, undirected networks, I have examined real terrorist cell data for; September 11^{th} 2001 World Trade Centre attack, March 11^{th} 2004 Madrid train bombing, Francs-Tireurs Partisans WWII résistance group and 7^{th} July 2005 London Underground bombing. Using normalised metric distributions, I identified the graphically important terrorist members and compared my findings to the known cell leaders. Using simple mathematical rules for the recruitment, removal and desertion of terrorists, I developed four generative models. The dynamics of each generative mechanism were examined using two different initial networks, and simulation metric distributions were calculated and compared to those obtained from the real terrorist networks. My examination of real terrorist cells suggests degree centrality as a good indicator of the leaders, and other valuable cell members. The use of a network percolation mechanism to model a systematic head-hunting tactic for disbanding terrorist cells, is examined and found to have varying success depending on the terrorist cell construction. Finally, I evaluated each generative mechanism, evaluated the systematic percolation attack and outlined aspects for further investigation.

Acknowledgements

I am grateful to my supervisor [name omitted in accordance with dissertation submission rules] for his enthusiasm in my unusual dissertation topic, his invaluable guidance and advice, and for developing my understanding of, and inspiring my interest in, network theory.

I thank Alexander Gutfraind for providing access to the terrorist network data sets used in my investigation, his helpful discussions and for his suggestions on further research material.

I acknowledge Aaron Clauset, José A. Rodríguez and Alexander Gutfraind as the respective owners of the data sets; S11, M11 and FTP.

I am grateful to Amanda Traud, Christina Frost, Peter Mucha and Mason Porter for allowing me use of their online network visualisation MATLAB procedures.

Finally, I thank my mother, father and sister for their unwavering support, patience, and encouragement throughout my four years reading Mathematics at Oxford University.

Contents

Chapter 1

Network Theory

1.1 Introduction to Networks

The world consists of thousands of highly complex organisational networks and processes, which are best described and understood as a collection of distinct components interacting with each other in some manner. *Network theory* allows us to investigate such networks by mathematically representing a system of interest as a collection of points (called *vertices* or *nodes*) connected together by a set of lines (called *edges* or *links*). We call this collection of vertices and edges a *network*, or *graph* [34].

For any finite network G of n vertices, we denote the sets of vertices and edges by $V(G)$ and $E(G)$ respectively [12]:

$$\begin{aligned} V(G) &= \{v_i \mid i = 1 \dots n\}, & |V(G)| &= \textit{Size} \text{ of network } G = n, \\ E(G) &= \{e_{ij} \mid i, j = 1 \dots n\}, & e(G) &= |E(G)| = \text{Number of network edges.} \end{aligned}$$

The *Adjacency matrix*, $A \in \mathcal{M}_{n\times n}(\mathbb{R})$, of network G is defined such that each matrix element, a_{ij}, indicates if G contains an edge e_{ij} connecting vertex v_j to v_i [34]:

$$a_{ij} = \begin{cases} 1 & \text{if there is an edge connecting } v_j \text{ to } v_i, \\ 0 & \text{otherwise.} \end{cases}$$

Network G is said to be a *simple network* if the adjacency matrix elements satisfy:

$$a_{ij} \in \{0, 1\} \text{ for all } 1 \le i, j \le n, \qquad a_{ii} = 0 \text{ for all } 1 \le i \le n.$$

Thus, G is a simple network if there are at most one edge connecting each pair of vertices $v_i, v_j \in G$, and no vertex is connected to itself by a single edge e_{ii}.

We define the *neighbourhood* of a vertex v_i, denoted $\Gamma(v_i)$, to be the set of vertices v_k connected to v_i:

$$\Gamma(v_i) = \{v_k \in G \mid a_{ik} = 1\}.$$

Network theory allows scientists to model a range of different network structures by adjusting the properties of vertices and edges contained within the network [34], as shown in Appendix A.1.

Drawing and visually examining a network is a simplistic, yet robust, tool for comprehending network patterns and structural elements. However, while this technique is useful for networks of small size, the sheer volume and variety of information means a different approach is required to easily gain insight into the structure of larger networks.

1.2 Network Centrality Measures and Metrics

There are many commonly used analytical techniques, called *network metrics*, which reveal specific network features by considering vertex and edges properties. My investigation will focus on a class of network metrics called *centrality measures.* A centrality measure of a vertex or edge gives a numerical qualification of that element's relative network importance [34].

By comparing a selection of network metrics, it is possible to gain an insight into the key network vertices. If vertex $v_i \in G$ has comparatively large network metrics, I will say that v_i is a *graphically important* vertex, reflecting the fact that the quantified metric importance obtained is a result of the network topology, and may not indicate the true importance of a vertex within a real network application.

I defined a network metric measure as *dynamically stable* if the graphical importance of each vertex $v_i \in G$ remain constant, or experiences a small variation, when a network vertex, or edge, is removed from G.

1.2.1 Degree Centrality

Degree centrality (or *degree*) is the most commonly used network centrality. Degree centrality measures the number of edges incident (i.e. connected) to a vertex [34].

> **Degree Centrality:** The degree of vertex v_i, denoted k_i, is equal to the number of network edges incident to v_i.

If a vertex v_α is removed from network G, the degree of each previously connected neighbourhood vertex, $v_\beta \in \Gamma(v_\alpha)$, decreases by one. If G has large mean degree, removing v_α affects a large number of degree centralities k_β, however decreasing k_β by one has little effect on the relative importance of each vertex v_β. If instead G has small mean degree, removing v_α produces a more significant change in vertex importance, but affects fewer vertices. Hence, the dynamic stability depends on mean degree of G.

1.2.2 Eigenvector Centrality

Eigenvector centrality is a recursive vertex centrality measure that calculates the relative importance of network vertices by considering any connections the vertex has to other recursively important network vertices.

> **Eigenvector Centrality:** Consider a network G with size n and adjacency matrix $A \in \mathcal{M}_{n\times n}(\mathbb{R})$.
>
> Let x_i denote the eigenvector centrality value of vertex v_i, and define x_i to be proportional to the sum of eigenvector centrality values of all neighbouring vertices $v_j \in \Gamma(v_i)$. Thus:
>
> $$\begin{aligned} x_i &= \frac{1}{\lambda} \sum_{v_j \in \Gamma(v_i)} x_j \\ &= \frac{1}{\lambda} \sum_{j=1}^{n} A_{ij} x_j \end{aligned}$$
>
> where $\Gamma(v_i)$ is the neighbourhood of vertex v_i and λ is the constant of proportionally.
>
> Using vector notation, $\underline{\mathbf{x}} = \left(x_i\right)_{1\leq i\leq n}$, we obtain the characteristic equation for eigenvector $\underline{\mathbf{x}}$ with eigenvalue λ:
>
> $$\begin{aligned} \underline{\mathbf{x}} &= \frac{1}{\lambda} A\underline{\mathbf{x}}, \\ \Rightarrow A\underline{\mathbf{x}} &= \lambda\underline{\mathbf{x}}. \end{aligned}$$

In general, the solution eigenvector is non-unique, but using the Perron-Frobenius theorem [Appendix A.2], we have that the eigenvector $\underline{\mathbf{x}}$ corresponding to the largest eigenvalue λ, has non-negative entries. Because we require each eigenvector centrality to be non-negative, the eigenvector with largest eigenvalue defines the network eigenvector centrality values [34].

As with degree centrality, removing a vertex v_α alters the eigenvector centralities for each vertex $v_\beta \in \Gamma(v_\alpha)$, however the recursive construction means that removing v_α causes a small variation in x_β values, making eigenvector centrality dynamically stable.

1.2.3 Betweenness Centrality

A *path* is a set of vertices and edges connecting two network vertices together, and the *path length* is equal to the number of edges traversed by the path. We define a *geodesic path*, between vertices v_r and v_s, as a path of shortest length between these vertices. *Geodesic length* is denoted d_{rs} [34].

Betweenness centrality measures vertex importance by examining which vertices lie on the geodesic paths between each pair of network vertices v_r, v_s [34].

Betweenness Centrality: To calculate the betweenness centrality, we first require:

1. The number of geodesic paths, σ_{rs}, between each pair of vertices v_r and v_s $(r \neq s)$.
2. The number of geodesic paths between v_r and v_s $(r \neq s)$, that contain vertex v_i, $\sigma_{rs}(v_i)$.

The betweenness centrality, $C_B(v_i)$, of vertex v_i is then:

$$C_B(v_i) = \sum_{\substack{r,s\in\{1\ldots n\}\setminus\{i\}\\ r\neq s}} \left(\frac{\sigma_{rs}(v_i)}{\sigma_{rs}}\right).$$

Given that removing a single network vertex can drastically alter the length and existence of geodesic paths, we find that betweenness is an unstable centrality measure.

1.2.4 Clustering Coefficient

The *(local) clustering coefficient* C_i of vertex v_i, measures the proportion of connections within the neighbourhood $\Gamma(v_i)$ [34].

Clustering Coefficient Metric: Considering a simple undirected network G, containing v_i, the total number of possible connected pairs of vertices $v_r, v_s \in \Gamma(v_i)$ $(r \neq s)$ is equal to $\frac{1}{2}k_i(k_i - 1)$.

The local clustering coefficient C_i, is calculated as:

$$C_i = \left(\frac{\text{number of connected pairs of vertices } v_r, v_s \in \Gamma(v_i)\ (r \neq s)}{\frac{1}{2}k_i(k_i-1)}\right).$$

Since clustering coefficient C_i is undefined for $k_i \in \{0, 1\}$, I will define $C_i = 0$ for any vertex v_i with degree $k_i = 0$ or 1.

Removing a network vertex v_α decreases the degree of each neighbour $v_\beta \in \Gamma(v_\alpha)$ by one, and may decrease the number of connected pairs in each neighbourhood $\Gamma(v_\beta)$. Since C_i is a fractional function of these decreasing values, and that typically more than one vertex v_β is affected by the removal, the clustering coefficient values C_β vary proportionally to each other and the network vertices experience a small change in graphical importance. Thus clustering coefficient is a dynamically stable metric measure.

1.3 Metric Distributions

Let G be a network of size n. Considering a network metric θ (where θ_i represents $k_i, x_i, C_B(v_i)$ or C_i), the probability distribution function is calculated for θ_i so that the structure and properties of G can be compared to those of other networks.

The *metric distribution* of the metric θ is defined as:

$$\rho_\theta(x) = \left(\frac{\text{number of vertices, } v_i \in G\text{, with centrality measure } \theta_i = x}{n}\right),$$

and plotting $\rho_\theta(x)$ against x, gives the probability distribution curve of metric values θ_i attained in G.

A network metric θ is said to have a *power law distribution* if $\rho_\theta(x)$ can be written in the form:

$$\rho_\theta(x) = \alpha x^{-\beta}$$

for positive constants $\alpha, \beta \in \mathbb{R}_{>0}$ [34].

1.4 Hubs and Cliques

Finally, by considering a scatter plot of degree distribution versus clustering coefficient distribution, structural network characteristics can be revealed [42].

Reference [34] describes a highly connected vertex $v_i \in G$, where v_i is a common vertex of disconnected network components, as a *hub*. Thus, vertices with large degree k_i, relative to clustering coefficient C_i, are described as hubs, and a network containing hubs is characterised by a negative correlation between degree and clustering coefficient distributions.

A *clique* is a maximal subset of vertices $v_i \in G$, that produces a network consisting only of vertices connected to every other vertex. Network G contains a clique of size n provided the complete graph K_n is a subgraph of G. Vertices with clustering coefficient $C_i = 1$ are members of some network clique.

Chapter 2

Investigating Organised Terrorism

2.1 Epidemic Model Application

My initial investigation into terrorist dynamics examined the construction of terrorist cells using an epidemic model. Postulating that terrorist ideologies and influences are spread between individuals in a similar manner to how infections spread through biological populations, it is possible to investigate terrorist dynamics using a modified *susceptible-infectious-recovered* (*SIR*) model [22].

Modelling terrorism using dynamical systems has previously been studied in [14, 18]. Reference [18] splits an experiment population into three distinct categories; Terrorists $x(\tau)$, Susceptibles $y(\tau)$, and Non-susceptibles $z(\tau)$, and examined a 3-dimensional system of non-linear ordinary differential equations (ODEs) modelling the interactions and movement of individuals between categories:

Terrorist Population, $x(\tau)$:

Using $x(\tau) =$ *Number of terrorist members in population (at time τ)*, ODE (2.1) is created using the terms described in Table 2.1.

$$\frac{\mathrm{d}x(\tau)}{\mathrm{d}\tau} = \alpha xy - \beta x^2 + (\gamma_1 - \gamma_2)x. \tag{2.1}$$

Variable	Description
αxy	Direct recruitment of new terrorist members from the susceptible population.
$-\beta x^2$	Counter-terrorists rapidly decrease terrorist population by capturing or killing individuals.
$\gamma_1 x$	Population increases as a result of appeals for support to terrorist organisations in other geographical locations.
$-\gamma_2 x$	Terrorists are removed due to death by natural causes, violent action or suicide attacks.

Table 2.1: Motivation of terrorist population ODE, (2.1)

Susceptible Population $y(\tau)$:

Using $y(\tau) =$*Number of individuals susceptible to both terrorist propaganda and counter-terrorist influences (at time τ)*, equation (2.2) is created using Table 2.2.

$$\frac{\mathrm{d}y(\tau)}{\mathrm{d}\tau} = -\alpha xy - \epsilon x^2 y + (\delta_1 + \delta_2)x + \lambda y. \tag{2.2}$$

Variable	Description
$-\alpha xy$	Direct recruitment from susceptible population into terrorist population.
$-\epsilon x^2 y$	Depletion of susceptible population by counter-terrorist influences convincing individuals to join the non-susceptible population.
$\delta_1 x$	Notorious terrorist attacks increases susceptible population by convincing non-susceptible individuals to adopt susceptible values.
$\delta_2 x$	Susceptible population increases when individuals, keen to join the terrorist population, relocate from other geographical regions.
λy	Population increases proportionally to its size as offspring are brought up to share same personal beliefs as parents.

Table 2.2: Motivation of susceptible population ODE, (2.2)

Non-susceptible Population, $z(\tau)$:

Using $z(\tau)$ =*Number of individuals not susceptible to terrorist propaganda (at time τ)*, equation (2.3) is created using Table 2.3.

$$\frac{\mathrm{d}z(\tau)}{\mathrm{d}\tau} = \epsilon x^2 y - \delta_1 x + \mu z. \tag{2.3}$$

Variable	Description
$\epsilon x^2 y$	Counter-terrorist influences persuade susceptible individuals to join the non-susceptible population.
$-\delta_1 x$	Non-susceptible individuals are swayed to join the susceptible population by the notoriety of successful high profile terrorist attacks.
μz	Population increases proportionally to its size as offspring are brought up to share same personal beliefs as parents.

Table 2.3: Motivation of non-susceptible population ODE, (2.3)

Reference [18] assumed that $z \gg x, y$, which represents terrorists and susceptible individuals as a minority within the experiment population.

Using the substitution $t = \gamma_2 \tau$,we non-dimensionalise the 3-dimensional system (2.1), (2.2), and (2.3) to obtain:

$$\frac{\mathrm{d}x(t)}{\mathrm{d}t} = axy - bx^2 + (c-1)x \tag{2.4a}$$

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = -axy - ex^2 y + fx + gy \tag{2.4b}$$

$$\frac{\mathrm{d}y(t)}{\mathrm{d}t} = ex^2 y - hx + lz \tag{2.4c}$$

Noticing that equation (2.4c) uncouples from the remaining 2-dimensional system (2.4a) and (2.4b), we can obtain $z(t)$ by direct integration once expressions for $x(t)$, and $y(t)$ have been found. Furthermore, as $x(t)$ and $y(t)$ represent population numbers, the 2-dimensional phase-plane analysis of (2.4a) and (2.4b) is performed in the upper right quadrant only.

Using the derived ODEs, (2.4a) and (2.4b), Reference [18] investigated the stability of this system's steady states and, by adjusting the values of constants $\{a, b, c, e, f, g, h, l\}$, examined the effects of non-violent and military/police interventions on the terrorist population [18].

While this differential equation model highlights many general properties which suggest practical strategies for disrupting terrorist populations through different types of interventions, the usefulness of any results obtained heavily depend on the extent that an epidemic model simulates terrorist cell construction. Investigating the spread of ideas and information between individuals requires both an understanding of how a population is inter-connected, and of the mechanisms used to decide how information is shared [32].

Using a SIR model requires adopting several assumptions which do not realistically translate to individuals wishing to spread terrorist ideologies. Noticeably, the ODE terms x^2, xy, x^2y, etc. are chosen using arbitrary modelling assumptions, and the system (2.4a), (2.4b) assumes each population member is able to contact all other individuals. In reality, even taking into account that on average most individuals are connected together by "6 Degrees of Separation" [24, 45], this is an over simplification.

2.2 Modelling Terrorist Cells using Network Theory

Since the invasion of Iraq, 20th March 2003, British and United States forces in the theatre of war have sustained heavy losses from improvised explosive devices (IEDs) detonated against coalition patrols and supply convoys. Planning and preparation of a roadside IED attack is rarely completed by a single individual, and is typically the result of the combined efforts of an organised group; each member responsible for, and skilled in, completing one aspect of the ambush.

As of December 2010, nearly 90% of all U.S. military deaths in Iraq have been attributed to IED attacks, prompting investigation into network theory as a means to accurately and efficiently identify individuals responsible for planning such attacks [50].

Although there is no universally agreed criminal law definition of terrorism [47], organised terrorism typically uses threats and violence as a means of coercion. Organisational structures have been found in terrorist cells where members work together, each specialising and overseeing different aspects of operations, to achieve a shared goal. It is this organisational structure that makes network theory a useful tool with which to model and analyse complex terrorist cells.

Using network theory, I represent terrorists as vertices and any direct communication between cell members by network edges. To date, network theory has been used to investigate a range of terrorist cell features [1, 2, 4, 19, 36]. References [27, 28] considered terrorist cells as simple networks, and investigated the mean number of vertices that need to be removed before a terrorist cell is split into disbanded partitions.

Reference [30] examines changes in terrorist cell leadership following removal of terrorist members. Considering "cognitive demand" (i.e. the demand on an individual's time; communicating or participating in specialised tasks), and degree of each cell member, Reference [30] models shifts in organisational hierarchy after removing the leaders of the terrorist organisations al-Qaeda and Hamas. Reference [30] speculates that removing al-Qaeda figurehead, Osama bin Laden, would produce relatively little change in network structure, whilst noting the removal of Hamas leader, Sheik Ahmed Yassin, resulted in a number of competing faction leaders emerging.

While motivations for, and methodologies of constructing terrorist cells vary greatly [40], the most successful organisational structures will include contingency measures so that if a terrorist member is compromised, the cell can remain operational and largely undetected by counter-terrorists. Reference [3] examines the construction of terrorist cells that protect against catastrophic cascades (i.e. a systematic counter-terrorist attack removing cell members), while still supporting efficient communications.

2.3 Terrorist Cell Data Sets

The violent, covert nature of terrorist organisations makes collecting social and operational information incredibly difficult. Additionally, counter-information and misdirection tactics used to protect the identities of terrorists mean, that any collected data must be closely scrutinised before being acted upon. Table 2.4 shows three possible sources of terrorist information.

Data Source	**Description**
Media Coverage	Newspaper articles, news websites and television broadcasts provide sources of data. However, media coverage can be politically skewed, reporting the official details complied and released by law enforcement agencies.
Terrorist Interviews	Firsthand information obtained from captured terrorists and co-conspirators will be typically strictly classified and censored by counter-terrorist organisations. Interviews are only released, if at all, once active investigations have been completed. Furthermore, any intelligence obtained may be incomplete, inaccurate, intentionally misleading or irrelevant.
Intelligence Agencies	Counter-terrorist agencies will likely possess the most comprehensive data on active and disbanded terrorist cells. However, the tactical value of such data means that information is closely guarded and not publically available.

Table 2.4: Sources of terrorist information

For my investigation I had access to three network data sets:

1. September 11th 2001 Attack on the World Trade Centre (denoted S11)
2. March 11th 2004 Madrid Train Bombing (M11)
3. Francs-Tireurs Partisans WWII Résistance Group (FTP).

In addition, I researched website and newspaper articles collecting information on members of the 7th July 2005 London Underground Bombing terrorist cell (LUn) and their interactions. However, limited available information and small LUn network size, meant I did not fully examine the structure.

Each data set was received as a raw database of names and connections from which I generated and validated each network's adjacency matrix, ready for analysis in MATLAB. Using network visualisation MATLAB procedures, described in [5], I visualised the network for each data set.

Degree, betweenness centrality, eigenvector centrality and local clustering coefficient were calculated for each network vertex, and the corresponding metric distributions plotted. Using these network distributions, I identified individuals who seemed the most important and compared my findings to the corresponding cell leaders.

2.3.1 September 11th 2001 World Trade Centre Attack

On the morning of September 11th 2001, the militant Islamist extremist organisation al-Qaeda, executed co-ordinated terrorist attacks against the U.S. Described as "American's Worst Terrorist Attack" [37], nearly 3,000 victims were killed in attacks that destroyed the World Trade Centre in New York, and severely damaged The Pentagon in Virginia.

Utilising an extensive support network, nineteen suicide terrorists hijacked four commercial airliners, three of which were purposely crashed into the WTC North (flight number AA11) and South (UA175) towers, and the Pentagon building (AA77). The fourth flight (UA93), on route to the U.S. Capitol Building, crashed in Pennsylvania after a passenger-led revolt attempted to regain control.

I was given access to a comprehensive S11 data set based on Reference [52], with inputs from a wide selection of sources. I generated a simple, undirected, unweighted S11 network:

$$\text{Size: } |\text{S11}| = 62, \qquad \text{Number of edges: } e(\text{S11}) = 152.$$

Figure 2.1 visualises the S11 network.

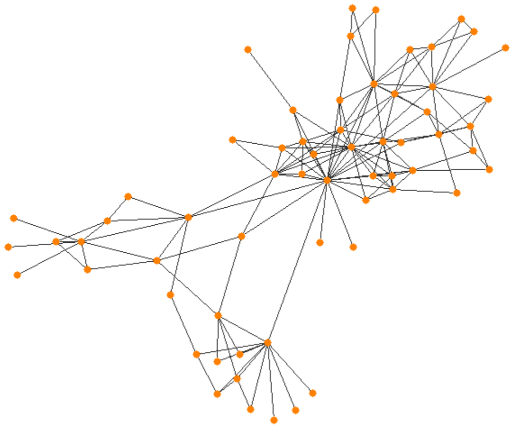


Figure 2.1: S11 terrorist network visualisation

2.3.1.1 S11 Centrality Measures and Metrics

Figure 2.2 shows the metric distributions for each vertex $v_i \in$ S11.

Figure 2.3 shows a scatter plot of degree distribution versus clustering coefficient distribution. Plotting a linear line of best fit:

$$y = -0.17x + 0.52,$$

we find S11 has a slight negative correlation between degree and clustering coefficient distributions, suggesting the existence of network hubs described in Section 1.4.

Figure 2.4 compares the S11 degree distribution with the two power-law curves:

$$y_1 = (\frac{1}{x}), \qquad \text{(shown in black)},$$
$$y_2 = 0.42x^{-1.07}, \qquad \text{(shown in orange)}.$$

However, there are insufficient degree distribution data points to conclude concretely that S11 has a degree power-law distribution.

2.3.1.2 Identifying Key Cell Members

Calculating the mean metric distribution $\bar{\rho}_i$, [Appendix B.1], Figure 2.5 shows that v_{32}, v_{38} and v_{51} are the most graphically important vertices.

The S11 data set records vertices v_{32}, v_{38} and v_{51} as al-Qaeda terrorists:

> v_{32}**: Mohamed Atta** Considered one of the masterminds behind the September 11th attacks, he led the team of four terrorists hijacking flight AA11, and was the suicide pilot crashing into the WTC North tower [61].
>
> v_{38}**: Marwan Al-Shehhi** Hijacker-pilot of flight UA175. Travelled with Mohamed Atta to Afghani terrorist training camps in 1999, where they discussed the recruitment for the September 11th attacks with Osama bin Laden [60].
>
> v_{51}**; Hani Hanjour** Hijacker-pilot of flight AA77. Rented a one-bedroom apartment in Paterson, New Jersey, where he was visited by Mohamed Atta in May 2001 [59].

Thus, I found that the mean metric distribution gives a good indication of the actual real world S11 cell leaders.

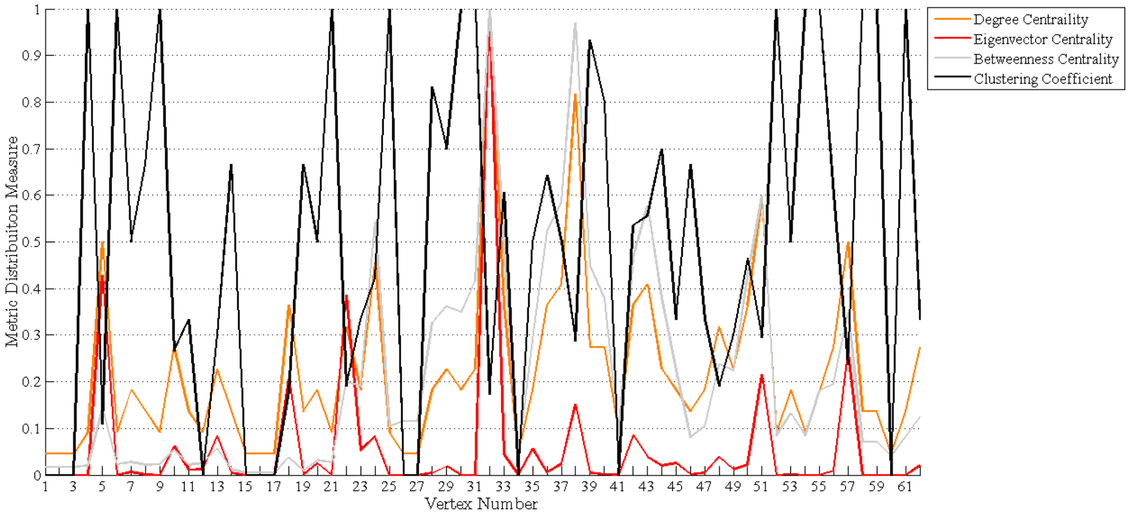


Figure 2.2: Summary of the S11 metric distributions

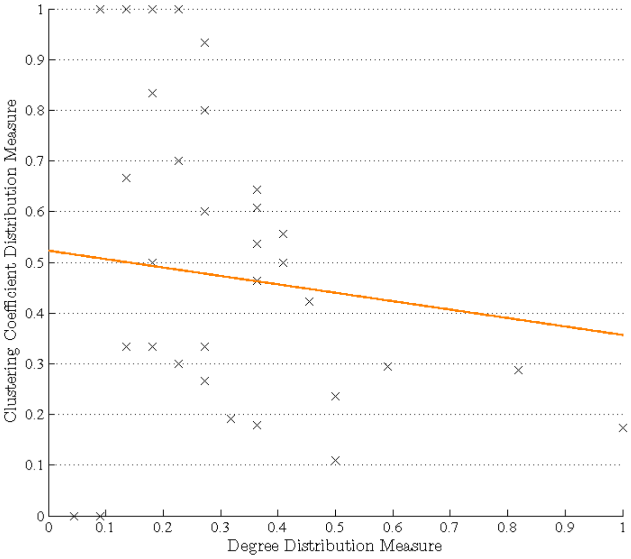


Figure 2.3: S11 degree distribution versus clustering coefficient distribution

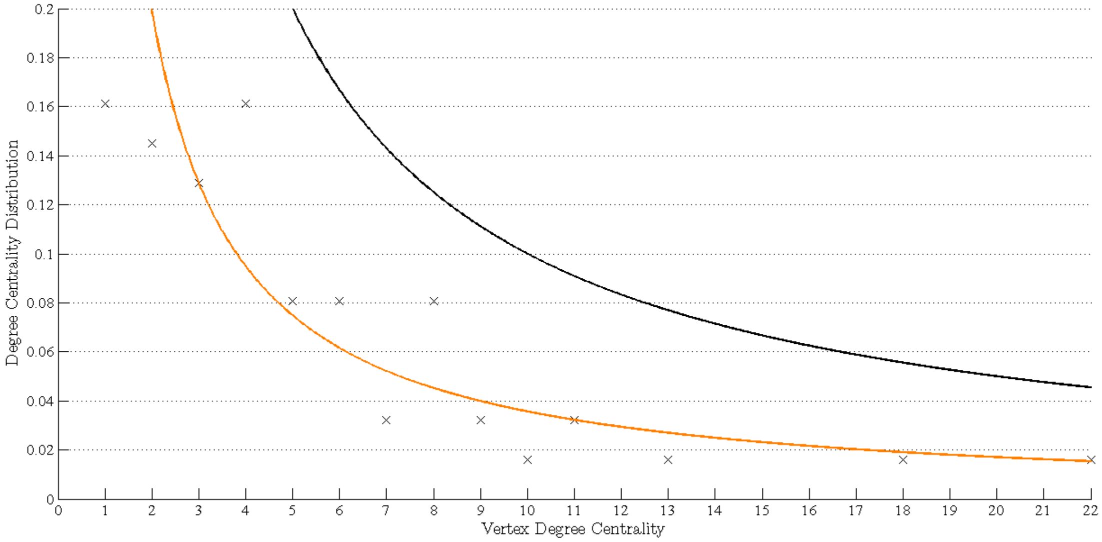


Figure 2.4: S11 degree centrality distribution

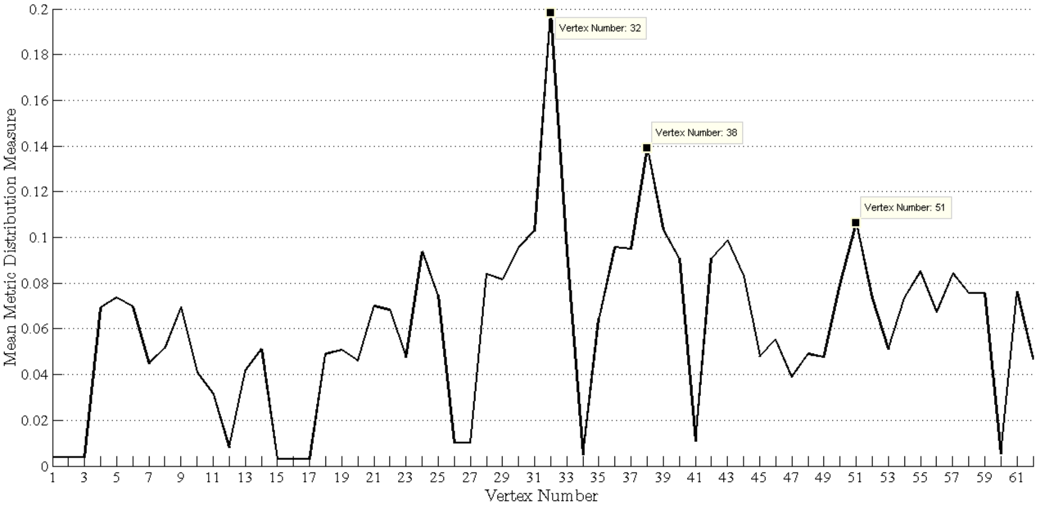


Figure 2.5: S11 mean metric distribution

2.3.2 March 11th 2004 Madrid Train Bombing

Between 07:37 am and 07:40 am March 11th 2004, ten IEDs detonated on four trains departing Alcalá de Henares station, Madrid. This al-Qaeda inspired coordinated terrorist attack [38], killed 191 and wounded at least 600 people travelling on the Spanish Cercanías train network. [10].

Following a lengthy investigation, four men were convicted of orchestrating the attacks. However, the suspected mastermind, Rabei Osman Sayed Ahmed, was acquitted of any involvement after translations of recorded Arabic conversations were contested in court [17].

Reference [29] divides the terrorists responsible into four component networks, each representing a different cell aspect:

1. **Friendship:** Long-held friendships in existence before joining the terrorist cell.
2. **Kinship:** Family relationships between cell members.
3. **Reliability:** Links to, and involvements with, other terrorist organisations enhanced the reputation and reliability of cell members.
4. **Shop:** Cell members cohabitated in Jamal Zougam's mobile phone shop.

Because each component assigns edge weightings using different methods, and since no component contains all terrorist members, I disregarded the network weightings and combined the four component networks to obtain a single, simple, undirected and unweighted M11 terrorist network:

$$\text{Size: } |\text{M11}| = 70, \qquad \text{Number of edges: } e(\text{M11}) = 240.$$

Figure 2.6 visualises the M11 network (6 isolated vertices not shown).

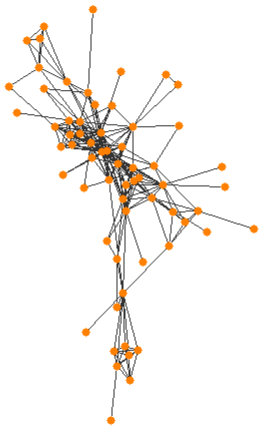


Figure 2.6: M11 terrorist network visualisation

2.3.2.1 M11 Centrality Measures and Metrics

Figure 2.7 summaries the metric distributions for each vertex $v_i \in$ M11.

Figure 2.8 shows that degree versus clustering distribution has a line of best fit:

$$y = 0.49x + 0.42,$$

with positive gradient, suggesting the vertices $v_i \in M11$ with large degree will tend to have a highly inter-connected neighbourhood $\Gamma(v_i)$.

Figure 2.9 shows the M11 degree distribution, however the limited number of data points means we cannot conclude if the degree distribution is linear, or follows a power-law curve:

$$y_1 = -0.003x + 0.084, \qquad \text{(linear distribution, shown in black)},$$
$$y_2 = 0.19x^{-0.69}, \qquad \text{(power-law distribution, shown in orange)}.$$

2.3.2.2 Identifying Key Cell Members

The mean metric distribution $\bar{\rho_i}$, Figure 2.10, shows v_1, v_3 and v_7 to be the most graphically important vertices.

Reference [29] records v_1, v_3 and v_7 as:

> v_1**: Jamal Zougam** Owner of the mobile phone shop where some cell members lived. Suspected of having links to September 11th 2001 and Casablanca 2003 terror attacks [49].
>
> v_3**: Mohamed Chaoui** Associated with Jamal Zougam through family connections [48]. Purchased the thirteen mobile phone SIM cards [9] used to detonate the planted IEDs.
>
> v_7**: Imad Eddin Barakat (Abu Dahdah)** Imprisoned for twenty-seven years for his involvement in the September 11th terror attacks. Spanish intelligence officer Rafael Gomez Menor speculated that Abu Dahdah oversaw the planning of the train bombings [54].

Thus, the mean metric distribution seems to have correctly identified the cell members most influential in the planning and, with the exception of Abu Dahdah, in the execution of the attack.

2.3.3 Francs-Tireurs Partisans WWII Résistance Group

Francs-Tireurs, literally *"Free Shooters"*, was the name adopted by two World War II (WWII) résistance groups in German occupied France. The Francs-Tireurs Partisans, *"Partisan irregular riflemen"*, was established by members of the French Communist Party after Germany invaded the Soviet Union in 1941 [57].

The Francs-Tireurs Partisans (FTP) network's operation was primarily sabotage and ambush, and it was the first French resistance group to deliberately kill a German soldier [57]. It eventually merged with the Forces Françaises de l'Intórieur, " French Forces of the Interior", led by Charles de Gaulle [58,62].

Using the received FTP data set, researched from reference [15], I generated a simple, undirected, unweighted FTP network:

$$\text{Size: } |\text{FTP}| = 174, \qquad \text{Number of edges: } e(\text{FTP}) = 264.$$

Figure 2.11 shows a visualisation of the FTP network.

2.3.3.1 FTP Centrality Measures and Metrics

The FTP network metric distributions are summarised in Figure 2.12.

Examining the scatter plot of degree distribution versus clustering distribution, the FTP network produces five distinct data points, summarised in Table 2.5. This small number of observed data points, relative to network size, indicates that the FTP network vertices are arranged in a strongly repeating structure, as seen in the network visualisation in Figure 2.11.

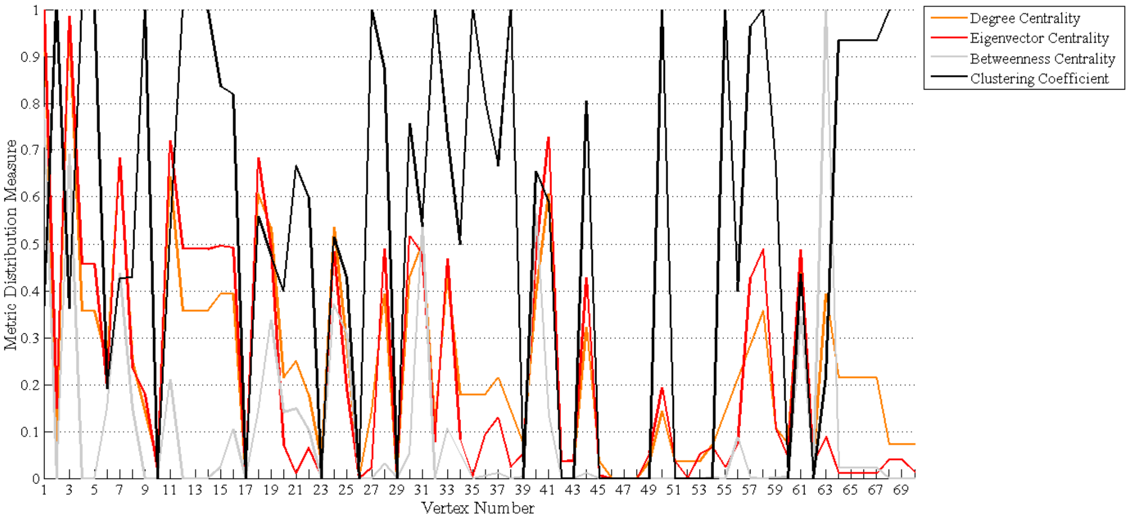


Figure 2.7: Summary of the M11 metric distributions

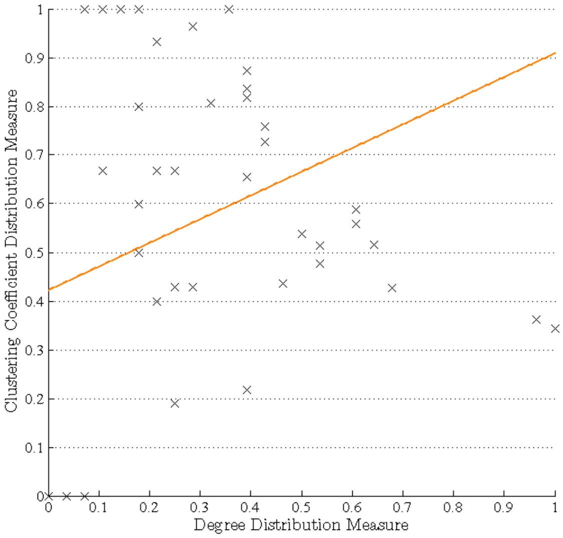


Figure 2.8: M11 degree distribution versus clustering coefficient distribution

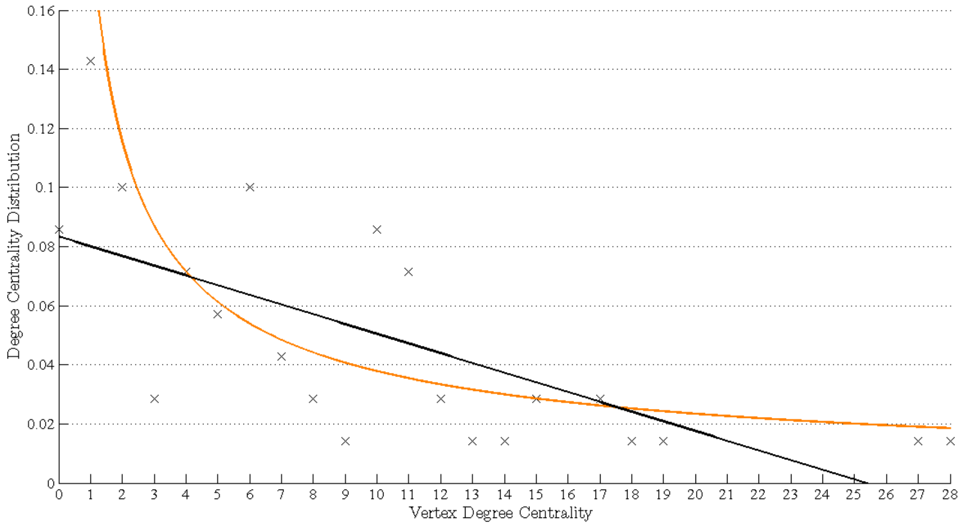


Figure 2.9: M11 degree distribution

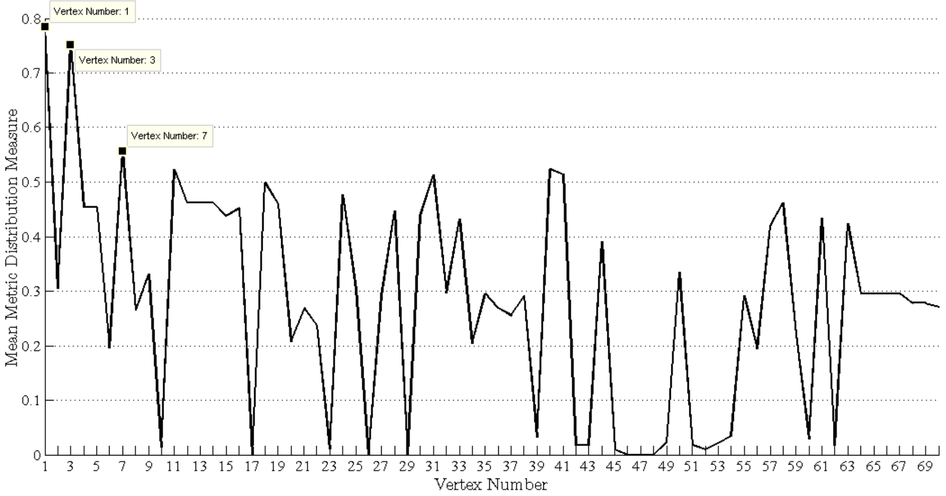


Figure 2.10: M11 mean metric distribution

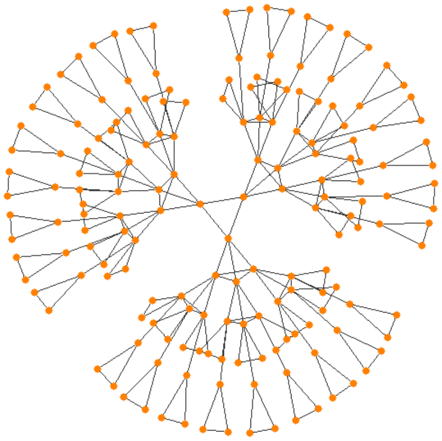


Figure 2.11: FTP terrorist network visualisation

Degree versus clustering coefficient					
k_i	0.3333	0.5	0.8333	1	1
C_i	1	0.3333	0.4	0.2667	0.4

Table 2.5: FTP degree distribution versus clustering coefficient distribution data points

2.3.3.2 Identifying Key Cell Members

The mean metric distribution $\bar{\rho}_i$, Figure 2.13, shows that the central FTP vertices v_1, v_2 and v_3, are the most graphically important vertices and can be speculated to represent the cell commanders.

Few historical sources detailing the organisational structure and leaders of the FTP cell exist, and descriptions in [15] are ambiguous as to the numbers of individuals in different saboteur teams. Hence, despite the obvious organisational characteristics of the FTP network, without further historical information I am unable to confirm if the central vertices, v_1, v_2 and v_3, are the FTP cell leaders.

2.3.4 7th July 2005 London Underground Bombing

On the morning of July 7th 2005, four suicide bombers detonated homemade IEDs on three London Underground trains and a double-decker bus. These blasts killed 56 people, including the bombers, and injured over 700 others [8].

The term “Home-Grown” terrorist cell [31], refers to a group of terrorist individuals who have not received any combat training, have few contacts with organised terrorism, or have not received any illegal financial funding. These typically small terrorist cells are formed with a single planned objective; the intention of attacking targets and individuals, within the terrorists’ home nation. It is suggested that the cell’s small size and “home-grown” nature was one reason why it remained undetected by counter-terrorist organisations [31].

Using newspaper reports of the terror attack and following investigation [41, 53], I found profiles for the close-knit group of friends who executed the attack. Little information is available on any known interactions between them and other terrorists, so I constructed a LUn network consisting of only the four suicide bombers. Figure 2.14 shows a complete four-vertex network, K_4, representing the LUn cell.

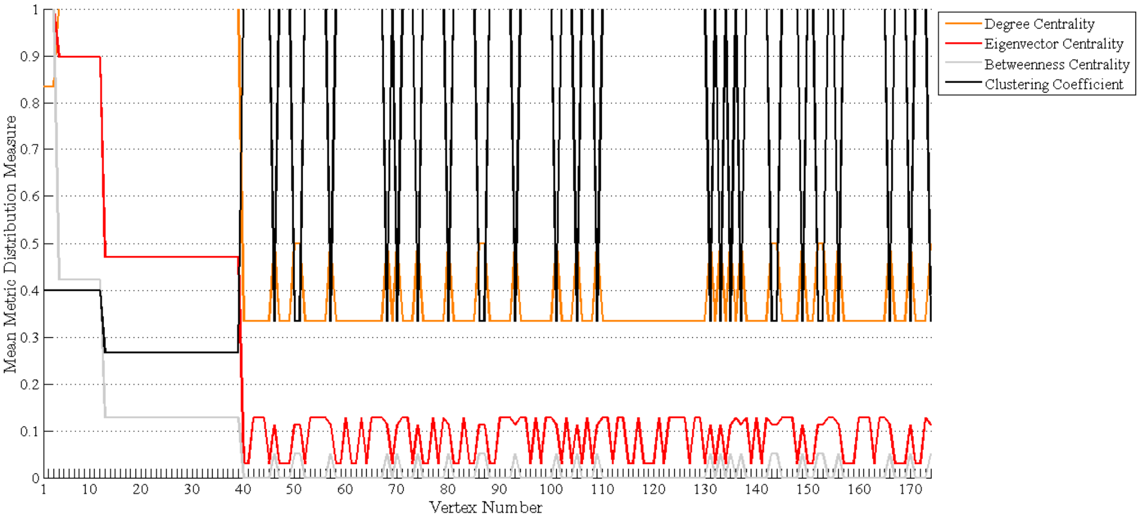


Figure 2.12: Summary of the FTP metric distributions

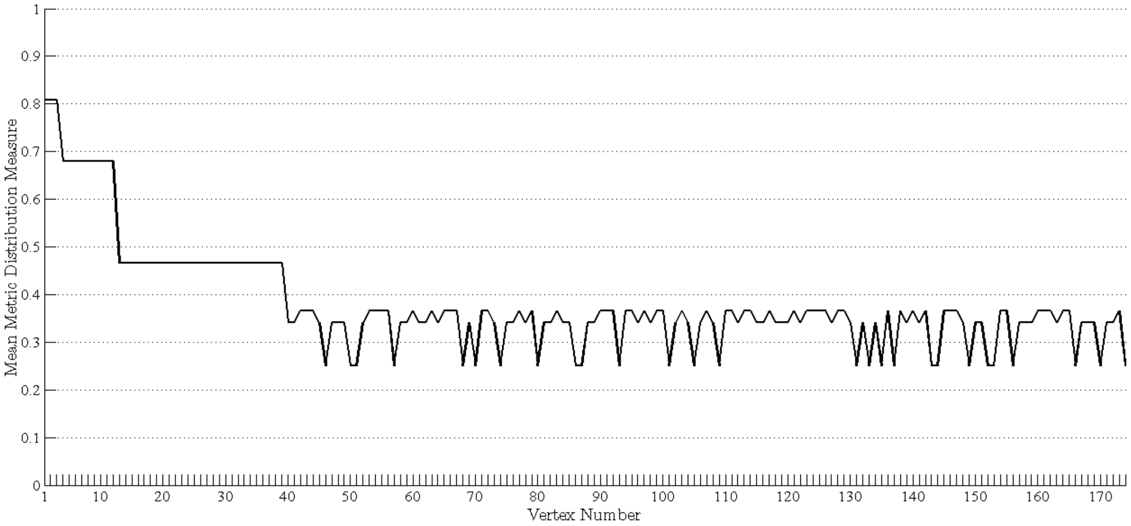


Figure 2.13: FTP mean metric distribution values

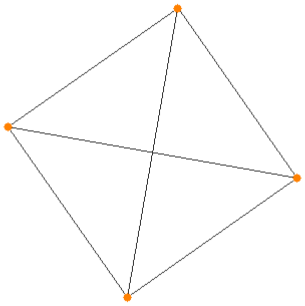


Figure 2.14: LUn terrorist network visualisation

2.3.4.1 LUn Centrality Measures and Metrics

Since the LUn network is a complete four-vertex graph, K_4, each vertex has identical network properties and metric values. Table 2.6 shows the identical metric distributions.

Degree, ρ_k	**Eigenvector, ρ_x**	**Betweenness, ρ_{C_B}**	**Clustering Coefficient, ρ_C**
1	1	0	1

Table 2.6: Summary of identical LUn metric distributions

2.3.4.2 Identifying Key Cell Members

From Section 2.3.4.1, each LUn vertex has identical metric distributions, and are thus equally graphically important. Since the cell members were close friends, identical metric distributions suggests that the cell operated under a communal command structure.

Profiles for the four LUn suicide bombers are obtained from References [41, 53]:

v_1**: Mohammad Sidique Khan** Detonated his suicide bomb on the London Underground, just after leaving Edware Road at 8:50am, killing 6 victims.

v_2**: Shehzad Tanweer** At 8:50 a.m, on a Tube train travelling between Liverpool Street and Aldgate, his suicide bomb killed 8 people (including himself). Of Pakistani descent, Shehzad had been in contact with al-Qaeda trainers and propagandists after travelling to Pakistan and Afghanistan in the months prior to the attack.

v_3**: Germaine Lindsay** Known as Jamal following his conversion to Islam, he detonated a rucksack bomb on the Tube travelling between Kings Cross-St. Pancras and Russell Square, killing 26 victims.

v_4**: Hasib Hussain** The youngest cell member, aged 18, Hasib completed a pilgrimage to Mecca where it is believed he adopted his radical Islamic views. Detonated his bomb on the No. 30 bus travelling through Tavistock Square, killing 14 victims (including himself).

2.4 Degree Centrality as a Strong Indicator of Importance

Examination of S11 and M11 terrorist cell data shows that the identified terrorist leaders are also the individuals with largest network degree values. Additionally, the leaders of the FTP network attain the second largest degree centralities, and the equally important LUn vertices share identical degree values.

The similarity between degree centrality and the importance of network vertices has been observed in the spread of infections within social networks. Reference [39] investigated the usefulness of degree centrality as an indication of individuals at high-risk of infection, concluding that degree centrality is at least as good an indication as other network centrality measures.

While I have adopted degree as an indication of valuable terrorist members and cell leaders, it should be noted that the number of connections with other terrorist cell members is unlikely to be the only factor considered when forming the command structure of real terrorist organisations.

Chapter 3

Modelling Terrorist Cell Dynamics

3.1 Key Elements of Terrorist Cell Construction

To investigate possible terrorist cell construction mechanisms, I developed several sets of simplified mathematical rules to simulate the recruitment of individuals into, and the removal of existing members from, terrorist cells. The generative mechanisms examined incorporate three basic elements shown in Table 3.1.

Element	**Comment**
Recruitment	The hierarchical structure of a terrorist cell determines which cell members are involved, and to what extent, in the recruitment of new terrorist members.
Removal	The effects of removing terrorist cell members are determined by the cell's topological and social structures.
Desertion	Terrorists who become isolated from all other cell members can either choose to desert terrorist activities or recruit new terrorists to form a splinter cell.

Table 3.1: Key elements of terrorist cell construction

3.2 Outline of Derived Terrorist Cell Models and Analysis

I developed and programmed generative mechanisms to model four possible terrorist cell constructions, outlined in Table 3.2. Each model aimed to describe and investigate different characteristic of real terrorist networks.

I considered two initial terrorist cells for each generative mechanism, and investigated if the starting network affects the structural properties of the generated simulations. Since it is difficult to obtain information on real terrorist cells, each initial network is chosen to mimic key characteristics of the generative mechanism, and to consist of vertices with similar metric values.

Each generative mechanism was observed for a set number of discrete time steps, chosen to alleviate data processing limitations and to construct simulations of mean sizes comparable to the motivating real terrorist cells [Appendix C.1].

I generated 1,000 distinct simulations for each generative mechanism (500 for each initial terrorist cell), and examined the dynamics of each model using the network metrics, and corresponding distributions, discussed in Section 1.2.

Model	**Comment**	**Motivation**
“Guerrilla Terrorists”	Simple two-level “Captain” and “Foot soldier” hierarchical model, typically observed in guerrilla warfare. Each “Foot soldier” participates in the recruitment of new cell members, earning a promotion to “Captain” once a specified number of new recruitments are made.	This generative mechanism is motivated by Reference [29], which investigates the recruitment of terrorists into the Movimiento 19 de Abril guerrilla army, and by the FTP network examined in Section 2.3.3.
“Friends and Family”	Models recruitment by assuming new recruits have existing connections to terrorists and terrorism sympathisers. Considers two different terrorist types, “Active” and “Passive”, who vary in risk of discovery, and in operational involvement within the cell.	Discussed in Section 2.3.2, M11 contained sub-networks of long-held friendships and family relationships, which [29] investigated as separate cell components. Additionally, the graphically important cell members Jamal Zougam and Mohamed Chaoui were related [Section 2.3.2.2].
“Multiple References”	Recruitment of a new cell members is modelled as a communal decision; where two or more existing terrorists select and invite potential new members to join the cell.	Since its formation in late 1989, the Islamic terrorist organisation al-Qaeda has carried out numerous attacks. This established organisation uses many recruitment methods [43] and is assumed to have a rigorous recruitment process that utilises the opinions of more than one recruiter, to prevent infiltration by counter-terrorists.
“Group of Friends”	Small, closely connected and highly trusted group of friends are modelled with each member playing an equal role in the command of the cell.	The communal command structure modelled has been observed in “home-grown” terrorist cells [31], such as the 7th July 2005 London Underground bombings examined in Section 2.3.4.

Table 3.2: Outline of derived terrorist cell models

3.3 “Guerrilla Terrorists” Construction Model

Guerrilla organisations aim to achieve political change and are often formed in response to; government or social changes, instability caused by war or environmental disaster, uncertainty due to inconclusive or corrupt elections, or with the aim of overthrowing occupying forces. Guerrilla groups traditionally attack defined military targets with ambush, sabotage and raiding tactics [33] in pursuit of their objectives.

The “Guerrilla Terrorists” generative mechanism mimics the formation and operation of a guerrilla military wing.

3.3.1 Terrorist Recruitment

The “Guerrilla Terrorists” generative mechanism investigates the construction of terrorist cells within a population controlled by a well-developed government, which opposes terrorist activities and wishes to disband terrorist networks by capturing or killing cell members. In developed countries, the population majority willingly accepts and upholds this stance. Conversely, populations in some developing countries will likely be sympathetic to the guerrilla organisation’s objectives, however threat of harsh punishments often deters potential recruits.

Reference [35] investigated the different influences for joining the Movimiento 19 de Abril (19th

April Movement, M-19) guerrilla army. Interviewing captured cell members, Reference [35] found family influences were one motivation, however, a majority admitted fabricating “University study trips” and “work placements” to keep family and friends unaware of their involvment. While [35] does not investigate mechanisms for constructing terrorist cells, I have used this research to develop my “Guerrilla Terrorists” model.

A guerrilla military wing typically adopts an organisational structure similar to traditional armies, with a strict command structure, of higher ranked individuals passing tactical orders down a command chain to foot soldiers.

To encourage recruitment, promotion is offered to individuals who successfully recruit a specified number of new guerrilla soldiers.

3.3.1.1 Recruitment Mechanism

Using a two-level “Captain” and “Foot soldier” command structure, the “Guerrilla Terrorist” mechanism assumes “Captain” cell members are no longer involved in recruitment, since there is no further promotion incentive. The model promotes “Foot soldier” terrorists once they recruit ten or more new members.

Each “Foot soldier” participates in the recruitment process by randomly recruiting $Y_{\text{GT}} \in \{0, 1, \dots, 5\}$ new terrorist members. Modelling that a recruiter is most likely to recruit zero new terrorists, and has smaller (decreasing) probabilities of recruiting $Y_{\text{GT}} \in \{1, \dots, 5\}$, the generative mechanism distributes Y_{GT} using a discrete approximation to the exponential distribution [Appendix C.2]. My preliminary analysis suggested that $\hat{Y} \sim \text{Exp}(\lambda = 2)$ produces a suitable approximate discrete probability distribution, Table 3.3, shows the PDF values for Y_{GT}.

y	0	1	2	3	4	5	≥6
$\mathbb{P}(Y_{\text{GT}} = y)$	0.6321	0.3181	0.0430	0.0058	0.0007	0.0001	0

Table 3.3: “Guerrilla Terrorists” recruitment PDF values

The generative mechanism assumes recruited individuals will not reveal their terrorist involvement to family and friends, for fear of betrayal, or exposing them to the risk of detention by known association. Thus, cell members are recruited singly, with no connections except with their original recruiter.

Appendix C.6 shows the pseudocode for this recruitment mechanism.

3.3.2 Terrorist Removal

Guerrilla organisations are typically far smaller than the target military organisations, so it is assumed that all terrorist members participate in the cell's tactical operations. Hence “Foot soldiers” and “Captains” are exposed to the same combat risks and are equally likely to be removed from the cell.

Tactical information available to “Foot Soldiers” is limited to orders obtained from “Captains”. Terrorists promoted to “Captain” will be highly loyal to the cell's objectives and existence.

3.3.2.1 Removal Mechanism

My preliminary analysis suggests the following time independent probability to model the removal of existing terrorist members:

$$\mathbb{P}(\text{Vertex } v_i \text{ is removed at time step } t) = 0.05.$$

“Captain” loyalty, and the limited information possessed by “Foot Soldiers”, allows me to model that any detained terrorist will either not possess actionable information, or will be resistive to interrogation. Thus removed terrorist members will not jeopardise the identities or locations of the remaining network. Appendix C.7 shows the removal pseudocode.

3.3.3 Terrorist Desertion

A terrorist, isolated due to the removal of other cell members, can either desert terrorist activities or form a new splinter cell.

While terrorists sometimes surrender to counter-terrorist organisations while still part of active cell [13,16], the threat of retaliation from the remaining members will deter voluntary removal. Only isolated cell members have the option to safely and secretly integrate back into the general population.

3.3.3.1 Desertion Mechanism

At each time step, isolated terrorists (vertices with degree $k_i = 0$) are eligible to desert the cell. Considering the population environment and attitudes in Reference [35], the generative mechanism adopts the probability:

$$\mathbb{P}(\text{Vertex } v_i \text{ deserts the terrorist cause at time step } t \mid k_i = 0) = 0.60.$$

Appendix C.8 shows the desertion pseudocode.

3.3.4 Initial Terrorist Cells

I considered two initial terrorist cells to investigate if the starting network affects the structural properties of the generated simulations. Table 3.4 shows the initial cells, GT_1 and GT_2, used.

Initial Cell	**Comment**
GT_1	The initial network, Figure 3.1(a), was chosen so a single "Foot soldier", central vertex v_1, has almost fulfilled the criterion for promotion and requires at least two new recruits for exemption from further terrorist recruitment. Table 3.1(c) shows the GT_1 metric values.
GT_2	The initial network, Figure 3.1(b), is more evenly spread with no obvious potential "Captain". Table 3.1(d) shows the GT_2 metric values.

Table 3.4: Initial terrorist cells used in the "Guerrilla Terrorist" model

3.3.5 "Guerrilla Terrorists" Simulation Properties

I generated 1,000 simulations, considering the "Guerrilla Terrorists" mechanism for ten discrete time steps. The investigation generated eleven "dead" simulations, of zero size and trivially zero metric distributions, which I disregarded and replaced.

The resultant simulation properties are summarised in Table 3.5.

3.3.6 Comparison to Real Terrorist Data

From Section 2.3.3, the Francs-Tireurs Partisans (FTP) were a French résistance group who fought the occupying German army during WWII, and therefore their objectives would have mimicked those of a guerrilla army, making the FTP network a sensible data set with which to evaluate the "Guerrilla Terrorists" model.

Considering the strong similarities between the metric distributions of simulations generated by GT_1 and GT_2 , it is safe to conclude that the differences between the chosen initial cells do not significantly affect the structure of the generated simulations. However, as I have only investigated two initial cells, and not investigated the asymptotic simulation properties, as simulation size $n \to +\infty$, I cannot draw any conclusions on the relationship between generated "Guerrilla Terrorists" simulations and the

Metric Distribution	**Comment**
Simulation Size	Figures 3.2(a) and 3.2(b) show the observed simulation sizes, and the number of times each network size was generated. Table 3.2(c) summaries the mean size and standard deviation for each initial cell.
Degree Centrality	Figures 3.3(a) and 3.3(b) show the degree distributions for GT_1 and GT_2. The mean degree distribution curves are calculated and plotted, including standard deviation error bars. They show that on average the “Guerrilla Terrorists” model produces a simulation with a degree distribution split into two tiers, and is more likely to have vertices of degree $k_i \in \{8, 9, 10, 11\}$, than smaller degree $k_i \in \{0, 1, 2, 3, 4, 5\}$.
Eigenvector Centrality	Figures 3.4(a) and 3.4(b), show that the model produces simulations containing vertices with evenly spread eigenvalue distributions, slightly favouring zero eigenvector values $x_i = 0$.
Betweenness Centrality	Calculating the betweenness distribution values for the 1,000 generated simulations, I obtained betweenness distribution plots consisting of data points densely clustered near the origin. Considering a restricted range of vertex betweenness centralities, Figures 3.5(a) and 3.5(b) show the mean betweenness distribution curve represents a large standard deviation of data points, before rapidly decreasing to an approximately constant value for the remaining range of betweenness values.
Clustering Coefficient	Examining the generative mechanism, we find that all simulations generated are tree networks which do not contain closed loops between network vertices v_i. Thus there are no connected pairs of neighbourhood vertices $v_r, v_s \in \Gamma(v_i)$ and the clustering coefficients C_i are trivially zero.

Table 3.5: “Guerrilla Terrorists” simulation properties

mechanism’s initial cell.

While the size of the real world FTP network ($|\text{FTP}| = 174$) is comparable to the mean “Guerrilla Terrorists” simulation size, and lies within the standard deviation error bars, the FTP metric distributions vary greatly to those seen in Section 3.3.5.

The significant differences between FTP and “Guerrilla Terrorists” simulation properties stems from the relatively small range of centrality values observed within the FTP network. For example, the FTP betweenness centrality distribution (omitted from Section 3.3.5) shows that every vertex $v_i \in \text{FTP}$ has a betweenness distribution value $\rho_{C_B}(v_i) \in \{0, 0.0517, 0.1279, 0.4220, 1\}$, whereas the generated simulations attain 2,840 different betweenness values.

Given that the “Guerrilla Terrorists” generative mechanism produces tree networks (Table 3.5), the existence of connected groups and loops within the FTP network (Figure 2.11) further suggests that the construction model does not share many structural features with the FTP network.

3.4 “Friends and Family” Construction Model

Threat of capture and punishment deter terrorist involvement in many countries. Individuals joining a terrorist organisation risk losing their liberty, and often their lives, so they must possess a strong belief in the group’s objectives. Motivations for joining terrorist cells include religious (the Islamic group al-Qaeda), political (the IRA sort reunification of North and South Ireland) or specific personal beliefs (the Oxford Arson Squad is a violent Animal Liberation Front group).

The “Guerrilla Terrorist” model, Section 3.3, assumes threat of detention and persecution deters members from disclosing their involvement to others. However, strongly held beliefs are rarely kept secret, and are often shared by family and close friends.

3.4.1 Terrorist Recruitment

The "Friends and Family" generative mechanism models a newly recruited terrorist member as likely having existing connections with individuals (friends and family) either sympathetic to, or actively keen to join the cell. Whilst families may share the same attitudes towards terrorism the roles they perform within the cell will likely differ, and so "Friends and Family" terrorists are modelled as "Active" or "Passive" members.

Level of involvement in cell objectives, will depend on terrorist type and thus "Active" and "Passive" terrorists will have different credibility when recruiting new cell members. The generative mechanism assumes only "Active" cell members participate in recruitment.

3.4.1.1 Recruitment Mechanism

Modelling that at each time step, the number of new terrorists each "Active" cell member recruits, Y_{FF}, is selected using the PDF values in Table 3.6. "Active" terrorists are not likely to recruit new cell members because the population majority is against terrorism, and when they do, the PDF values chosen during preliminary analysis favour the recruitment of small family groups (e.g. two "Active" parents with one "Passive" child):

y	0	1	2	3	4	5	6	7	8	9	$\geq$10
$\mathbb{P}(Y_{\mathrm{FF}} = y)$	0.60	0.04	0.05	0.10	0.06	0.05	0.04	0.03	0.02	0.01	0

Table 3.6: "Friends and Family" recruitment PDF values

Each recruitment group consists of one "Active" terrorist (connected directly to the recruiter) and $(Y_{\mathrm{FF}} - 1)$ terrorist members of unassigned type (connected to the "Active" terrorist and each other). The unassigned cell members are then defined as "Active" or "Passive" using equal probabilities:

$$\mathbb{P}(\text{"Friends and Family" vertex } v_i \text{ is an "Active" member}) = 0.50,$$
$$\mathbb{P}(\text{"Friends and Family" vertex } v_i \text{ is a "Passive" member}) = 0.50.$$

Thus, the "Friends and Family" generative mechanism constructs terrorist cells by adding complete graphs, $K_{Y_{\mathrm{FF}}}$, to the existing network. Appendix C.9 shows the recruitment pseudocode.

3.4.2 Terrorist Removal

Counter-terrorism organisations have a variety of resources, information and techniques that can identify terrorists within a population. The "Friends and Family" generative model adopts a simplified mechanism to represent how terrorists are revealed and removed.

At each time step, counter-terrorists perform a terrorist search inspecting all cell members. Each member is either discovered and detained, or evades detection and remains in the network. Because "Passive" terrorists play significantly smaller roles, primarily supporting their "Active" neighbours, the model assumes they are more difficult to detect than "Active" members.

If a cell member is detected, counter-terrorist information on family relationships, and known associates, immediately puts their friends and family at risk of discovery. The generative mechanism assumes "Active" terrorists are the best trained and able to adopt steps to remain hidden whilst "Passive" terrorists are easily detained if a neighbouring vertex is removed.

3.4.2.1 Removal Mechanism

At each time step, the “Friends and Family” model decides if a selected cell member is removed using probabilities that reflect the relative difficulties of detecting “Active” and “Passive” terrorists. I have set the probabilities of discovering each terrorist type as:

$$\mathbb{P}(\text{“Passive” vertex } v_i \text{ is removed at time step } t) = 0.025$$
$$\mathbb{P}(\text{“Active” vertex } v_i \text{ is removed at time step } t) = 0.05$$

Because “Passive” members do not possess the same training as “Active” terrorists, when a network terrorist is successfully removed, any neighbouring “Passive” members are also removed, however neighbouring “Active” terrorists have skills to evade capture and remain in the cell.

Appendix C.10 shows the removal mechanism pseudocode.

3.4.3 Desertion Mechanism

Using the same desertion mechanism as the “Guerrilla Terrorists” model, if a terrorist becomes disconnected from all other cell members, this isolated vertex can either desert organised terrorism or form a splinter cell.

Appendix C.11 shows the desertion pseudocode.

3.4.4 Initial Terrorist Cells

My two initial cells, FF_1 and FF_2, for the “Friends and Family” generated simulations are shown in Table 3.7.

Initial Cell	**Comment**
FF_1	Initial network, Figure 3.6(a), is generated by combining four small terrorist groups. A central group of three “Active” members, considered the cell’s architects, and three family groups (e.g. two “Active” parents and two “Passive” children) are connected. Table 3.6(c) summaries the FF_1 metric values.
FF_2	Initial network, Figure 3.6(b), is constructed using a complete graph, K_6, of “Active” terrorists with three smaller, passive terrorist groups branching from it. Table 3.6(d) summaries the FF_2 metrics values.

Table 3.7: Initial terrorist cells used in the “Friends and Family” model

3.4.5 “Friends and Family” Simulation Properties

As for “Guerrilla Terrorists”, I have run 500 distinct simulations for each initial cell. Because of computing limitations [Appendix C.1] and the rate at which simulation size increases, I programmed the generative mechanism to run for 5 discrete time steps.

The resultant simulation properties are summarised in Table 3.8.

3.4.6 Comparison to Real Terrorist Data

Comparing the metric distribution curves for FF_1 and FF_2, the strong similarities observed show that the chosen initial networks both generate simulations with similar structures.

I compared my generated simulations to the September 11^{th}2001 terrorist cell (S11 discussed in Section 2.3.1), and the March 11^{th} 2004 Madrid bombing cell (M11, Section 2.3.2). The eigenvector and

Metric Distribution	**Comment**
Simulation Size	Figures 3.7(a) and 3.7(b) show the frequency at which each generated simulation size occurs, producing curves that mimic the shape of a positively skewed normal distribution. Table 3.7(c) summaries the simulation size statistics.
Degree Centrality	The degree centrality distributions, Figures 3.8(a) and 3.8(b), show an approximately linearly dependent mean degree distribution for both initial cells.
Eigenvector Centrality	As for "Guerrilla Terrorists" model the eigenvector distribution plots, Figures 3.9(a) and 3.9(b), show an evenly distributed set of eigenvector distribution values.
Betweenness Centrality	The betweenness distributions are generated for FF_1 and FF_2. Examining a restricted range of betweenness values close to the origin, Figures 3.10(a) and 3.10(b) show a similarly decreasing mean betweenness distribution curve, also seen in the "Guerrilla Terrorists" betweenness distributions (Figures 3.5(a) and 3.5(b)).
Clustering Coefficient	Figures 3.11(a) and 3.11(b), show the clustering coefficient distributions for FF_1 and FF_2. In contrast to the wide range of distinct network eigenvector and betweenness centrality values, the generated simulations contain far fewer different clustering coefficient values. Figures 3.11(a) and 3.11(b) show the most likely clustering coefficient is $C_i = 0$ followed by $C_i = 1$, $C_i = 0.3333$ and $C_i = 0.5$.

Table 3.8: "Friends and Family" simulation properties

betweenness centrality distributions of the "Friends and Family" mechanism consist of tightly clustered data points near the origin, as do the distributions for S11 and M11 (omitted from Sections 2.3.1 and 2.3.2). Furthermore, the S11 and M11 clustering coefficient distributions have peaks that match the simulation peaks observed at $C_i = 0$, $C_i = 1$ and $C_i = 0.3333$, in Figures 3.11(a) and 3.11(b).

The "Friends and Family" generative mechanism produces simulations, with mean size 68.80, which is of comparable size to the S11 (size 62) and M11 (size 70) networks.

However, the model's distinctive linear degree distributions, Figures 3.8(a) and 3.8(b), differ to the S11 and M11 degree distributions (Figures 2.4 and 2.9). Given degree value is a good indicator of network importance, Section 2.4, this discrepancy leads me to doubt if S11 and M11 terrorist cells can be generated from the "Friends and Family" construction model.

3.5 "Multiple References" Construction Model

Membership of certain exclusive social clubs and societies is subject to a vote of approval by existing members [55]. During a probationary period, potential new members are often required to meet existing members, before the entire club, or elected committee, decides if full society membership should be granted. This system of prior majority approval results in the preservation of the club's ethos as approved candidates will share similar outlooks and values with existing members.

3.5.1 Terrorist Recruitment

Unlike the "Guerrilla Terrorists" (Section 3.3) and "Friends and Family" (Section 3.4) generative models, which allow existing cell members to recruit new terrorists without the approval of other cell members, the "Multiple References" model mimics a social club membership system.

This mechanism may increase the time needed to completely integrate new terrorists into a cell, but provides increased protection against counter-terrorist infiltration. By pooling different opinions, existing

"Multiple References" cell members can judge the operational value, commitment and trustworthiness of new recruits.

Because of the secretive nature of terrorism, it can be assumed not all cell members participate in each recruitment, and those that do, experience the recruitment challenges modelled in the "Guerrilla Terrorists" mechanism, see Section 3.3.1.1.

3.5.1.1 Recruitment Mechanism

As with the "Guerrilla Terrorists" mechanism, a cell is most likely to recruit zero new terrorists, and has smaller (decreasing) probabilities of recruiting $\{1, 2 \ldots, 5\}$ individuals.

At each time step, the "Multiple References" construction model randomly selects the number Y_{MR} of new recruits, using the same discrete exponential distribution approximation used for the "Guerrilla Terrorists" model. Table 3.9 repeats the recruitment PDF values motivated in Section 3.3.1.1.

y	0	1	2	3	4	5	≥ 6
$\mathbb{P}(Y_{\text{MR}} = y)$	0.6321	0.3181	0.0430	0.0058	0.0007	0.0001	0

Table 3.9: "Multiple References" recruitment PDF values

Each new recruit is assigned a number of existing cell references required to join the network, Z_{MR}. Modelling $Z_{\text{MR}} \in \{2, 3, 4, 5\}$ to favour admitting new recruits with two or three references, preliminary analysis suggests Z_{MR} is randomly distributed using the PDF values shown in Table 3.10.

z	0	1	2	3	4	5	≥ 6
$\mathbb{P}(Z_{\text{MR}} = z)$	0	0	0.50	0.25	0.15	0.10	0

Table 3.10: Number of existing cell references required by new recruits PDF

Finally, the generative mechanism connects the new recruit to Z_{MR} randomly selected vertices, using the *degree preferential probability distribution*, [Appendix C.4]. The model also ensures that distinct members are chosen, so that a new cell recruit is not accidentally recruited by a single terrorist member multiple times. Appendix C.12 shows the "Multiple References" recruitment pseudocode.

3.5.2 Terrorist Removal

As for the "Guerrilla Terrorists" and "Friends and Family" construction models, the "Multiple References" generative mechanism is modelled in a population that condemns terrorist ideologies and activities.

The self-perpetuating nature of the recruitment method ensures new recruits are firm believers in the terrorist cause, and if captured, will not willingly reveal actionable information to counter-terrorists.

3.5.2.1 Removal Mechanism

Using the same removal mechanism adopted by the "Guerrilla Terrorists" generative mechanism, Section 3.3.2.1, each terrorist member is modelled as having the same chance of removal by counter-terrorist organisations:

$$\mathbb{P}(\text{Vertex } v_i \text{ is removed at time step } t) = 0.05.$$

Appendix C.13 shows the removal pseudocode.

3.5.3 Desertion Mechanism

The "Multiple References" construction model simulates the actions of isolated terrorist members using the same terrorist desertion mechanism discussed in the "Guerrilla Terrorists" generative mechanism, Section 3.3.3.

Appendix C.14 shows the "Multiple References" desertion pseudocode.

3.5.4 Initial Terrorist Cells

My two initial cells, MR_1 and MR_2, are shown in Table 3.11.

Initial Cell	**Comment**
MR_1	Initial cell, Figure 3.12(a), consists of vertices of degree $k_i = 2$ or 3 only, reflecting that the generative mechanism favours new recruits requiring two or three recruitment references. Table 3.12(c) shows the MR_1 metric values.
MR_2	In contrast to MR_1, the initial cell MR_2 was chosen to contain an obvious leader, vertex v_{10}, see Figure 3.12(b). Table 3.12(d) shows the MR_2 metric values.

Table 3.11: Initial terrorist cells used in the "Multiple References" model

3.5.5 "Multiple References" Simulation Properties

The "Multiple References" generative mechanism generates 1,000 simulation networks, considering 100 discrete times steps for MR_1 and MR_2.

The resultant simulation properties are summarised in Table 3.12.

3.5.6 Comparison to Real Terrorist Data

As for "Guerrilla Terrorists" and "Friends and Family", comparison of metric distributions, for each initial cell MR_1 and MR_2, show the generative method does not appear to be affected by the choice of initial network.

Similarly to the "Friends and Family" model, the generated "Multiple References" betweenness and eignvector centrality distributions show clustered data points similar to those observed in the S11 and M11 distributions. Additionally Figures 3.15(a) and 3.15(b) show clustering coefficient peaks at $C_i = 0, C_i = 0.333$ and $C_i = 1$ matching those seen in the S11 and M11 clustering coefficient distributions.

Figures 3.14(a) and 3.14(b) show that the generative mechanism produces simulations with degree distributions vastly different to the M11 and S11 distributions, suggesting that these real terrorist networks were formed using different construction mechanisms.

Reference [43] suggests al-Qaeda uses many different recruitment mechanisms. The range of recruitment techniques discussed indicates that the differences between "Multiple References" and S11 degree distributions, may be because more than one construction process was employed during the formation of the S11 network.

3.6 "Group of Friends" Construction Model

Finally, I investigated the formation of "home-grown" [31] terrorist cells, similar to that responsible for the July 7th 2005 London Underground bombings. The term "home-grown" can describe individuals

Metric Distribution	**Comment**
Simulation Size	Figures 3.13(a) and 3.13(b) show the frequency at which each generated simulation size occurs. Each curve resembles a slightly positively skewed normal curve. Table 3.13(c) summaries the simulation size statistics.
Degree Centrality	Similarly to "Friends and Family", the degree centrality distributions, shown in Figures 3.14(a) and 3.14(b), initially show an approximately linearly dependent mean degree distribution for both initial starting cells. However, as degree increases, the degree distribution moves above and below the linear trajectory.
Eigenvector and Betweenness Centrality	The eigenvector distribution plots show an evenly spread set of data points with an approximately constant mean eigenvector curve. Additionally, the "Multiple References" model betweenness distribution plot, depicts a densely clustered collection of data points near to the origin. Since the betweenness and eigenvector distributions are very similar to those generated by the "Guerrilla Terrorists" and "Friends and Family" mechanisms, they provide no insight into any unique "Multiple References" structural features and I have omitted these plots.
Clustering Coefficient	Figures 3.15(a) and 3.15(b), show the clustering coefficient distributions for initial cells MR_1 and MR_2. As in "Friends and Family" generative mechanisms, the clustering coefficient distributions show network vertices attain a small range of clustering coefficients, opposed to the wide range of observed network eigenvector and betweenness centrality values. The "Friends and Family" clustering coefficient distributions, Figures 3.11(a) and 3.11(b), show that $C_i = 0, C_i = 1$ or $C_i = 0.333$ are the most likely clustering coefficient values. However Figures 3.15(a) and 3.15(b)do not show a peak in distribution values for $C_i = 0.5$.

Table 3.12: "Multiple References" simulation properties

participating in terror activities against their home nation, using skills and knowledge primarily self-researched and without tactical help or funding from established terrorist organisations. Because such individuals have no strong links to known terrorist cells, they are difficult to detect.

Home-grown terrorists are likely to operate as a network of highly trusted individuals, formed from long-term friendships or from contacts made while attending training camps [31]. This construction produces a terrorist cell that adopts an informal communal command structure, with each "Group of Friends" cell member having equal say in plans and decisions.

3.6.1 Terrorist Recruitment

One disadvantage of a small terrorist cell is that individuals need to possess a wide range of skills to complete the cell's objectives. While terrorist instructional manuals exist [51,63], these publications are closely monitored by security forces. Therefore, if a cell has a task for which current members are not qualified, new cell members with the required specialised skills must be recruited.

As when the cell initially formed, the new recruit must be trusted and known by existing members before admittance. If an existing cell member is unable to approve a new member before recruitment, the level of trust, and shared command structure within the group, means that any missing "friendships" will quickly form following acceptance.

3.6.1.1 Recruitment Mechanism

At each time step, the construction model randomly selects the number of new recruits, Y_{GF}. My preliminary analysis suggests the PDF values, shown in Table 3.13, can be used to mimic the rarity of recruiting new cell members:

y	0	1	2	3	4	5	≥6
$\mathbb{P}(Y_{\mathrm{GF}} = y)$	0.85	0.05	0.04	0.03	0.02	0.01	0

Table 3.13: "Group of Friends" recruitment PDF values

Consider a network of size n. Each existing cell member v_i, for $i = 1 \dots n$, is connected to the new recruits $\hat{v}_j$, for $j = 1 \dots Y_{\mathrm{GF}}$, using the probability:

$$\mathbb{P}(\text{New vertex } \hat{v}_j \text{ is connected to existing vertex } v_i) = 0.90.$$

The large probability for adding "missing" edges was chosen to reflect the speed at which friendships are made within the cell.

Furthermore, because the cell members work closely together, if the cell has any missing edge connections at time t, the construction model adds them with probability:

$$\mathbb{P}(\text{Add missing edge } e_{ij} \text{ at time step } t) = 0.90.$$

Appendix C.15 shows the recruitment pseudocode.

3.6.2 Terrorist Removal

As in the previous three generative mechanisms, the surrounding population is modelled to actively oppose terrorist activities. Furthermore, the trust between cell members means if a terrorist is captured by counter-terrorist forces, the detained individual will not endanger the cell's operations.

3.6.2.1 Removal Mechanism

Using the same removal mechanism as "Guerrilla Terrorists" and "Multiple References", the "Group of Friends" model considers the removal of members detected by concentrated efforts of counter-terrorist organisations. My preliminary analysis suggests the time independent probability

$$\mathbb{P}(\text{Vertex } v_i \text{ is removed at time step } t) = 0.05,$$

sensibly models the difficulties in detecting cell members.

Appendix C.16 shows the removal pseudocode.

3.6.3 Desertion Mechanism

The "Group of Friends" generative mechanism models the desertion of isolated terrorist members as discussed in the "Guerrilla Terrorists" generative mechanism, Section 3.3.3.

Appendix C.17 shows the desertion pseudocode.

3.6.4 Initial Terrorist Cells

My two initial cells, GF_1 and GF_2, are shown in Table 3.14.

3.6.5 "Group of Friends" Simulation Properties

Using GF_1 and GF_2, I generated 1,000 simulations by running the generative mechanism for 100 discrete time steps. Examining the generated networks G, I found that they are either complete networks, $G = K_{|G|}$, or highly connected, $G \approx K_{|G|}$.

Initial Cell	Comment
GF_1	The five-vertex complete network, K_5 was chosen as the initial cell GF_1, see Figure 3.16(a), because of its similarities to K_4, the network structure of the 7th July 2005 London Underground bombings and K_6, the network structure of the failed 21st July 2005 London terror cell [11]. Table 3.16(c) shows the GF_1 metric measures which all vertices share.
GF_2	Initial cell, Figure 3.16(b), was chosen so each vertex initially has one "missing" edge. Table 3.16(d) shows the GF_2 metric measures which all vertices share.

Table 3.14: Initial terrorist cells used in the "Group of Friends" model

Since complete networks have identical metric distributions, and given that a very large proportion of the generated simulations are complete, I have omitted my metric distributions analysis.

The resultant simulation size properties are summarised in Table 3.15.

Metric Distribution	Comment
Simulation Size	During my investigation, the generative mechanism produced 39 "dead" simulations, which were disregarded and replaced. Figures 3.17(a) and 3.17(b) show the frequencies of each generated simulation size. They show that simulation sizes have a roughly positively-skewed normal distribution, or follow an approximate Wiebull distribution curve [Appendix C.5]. Finally, Table 3.17(c) summaries the size statistics for each initial cell.

Table 3.15: "Group of Friends" simulation size properties

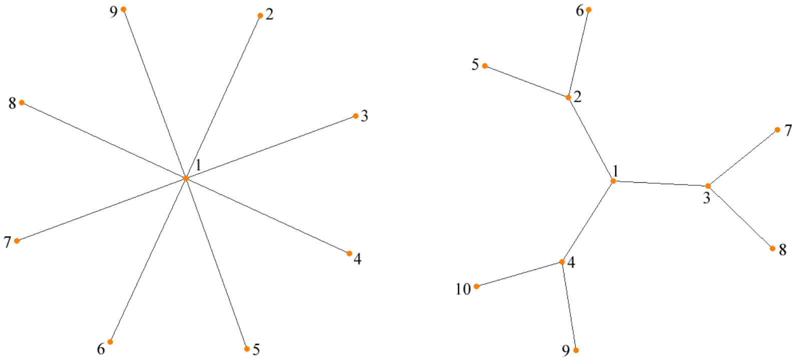
3.6.6 Comparison to Real Data

Having developed the "Group of Friends" generative mechanism to construct "home-grown" terrorist cells, the 7th July 2005 London Underground bombing and failed 21st July 2005 London attack networks are used to evaluate the model.

Considering the similarities between the metric distributions generated using GF_1 and GF_2, I find that these choices of initial cell have little effect on the generated simulations.

Discussed in Section 3.6.5, the generative mechanism favours generating completely connected networks. The resulting approximately identical network metrics suggest that the simulations produced consist of equally graphically important vertices, as observed in the LUn terrorist cell 2.3.4.

The calculated mean size, 7.22, of generated simulations is approximately twice the size of the LUn cell. However, despite generating terrorist cells of larger size, the "Group of Friends" generative mechanism accurately and consistently produces terrorist cells which show the characteristics of "home-grown, clean skin" terrorist organisations.



(a) Initial cell GT_1 (b) Initial cell GT_2

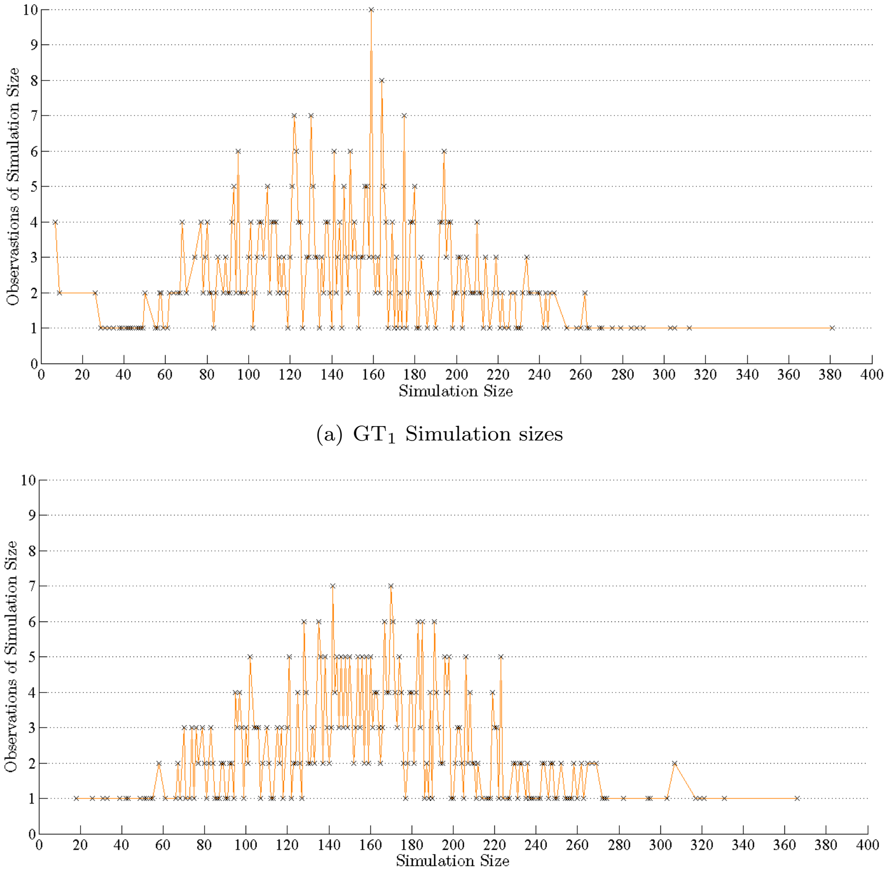
Vertex Number, i	**Degree, k_i**	**Eigenvector, x_i**	**Betweenness, $C_B(v_i)$**	**Clustering, C_i**
1	8	1	1	0
2, 3, 4, 5, 6, 7, 8, 9	1	0.3536	0	0

(c) GT_1 Cell metric values

Vertex Number, i	**Degree, k_i**	**Eigenvector, x_i**	**Betweenness, $C_B(v_i)$**	**Clustering, C_i**
1	3	1	1	0
2, 3, 4	3	0.7453	0.5556	0
5, 6, 7, 8, 9, 10	1	0.3334	0	0

(d) GT_2 Cell metric values

Figure 3.1: Network visualisation and metric values for initial cells GT_1 and GT_2



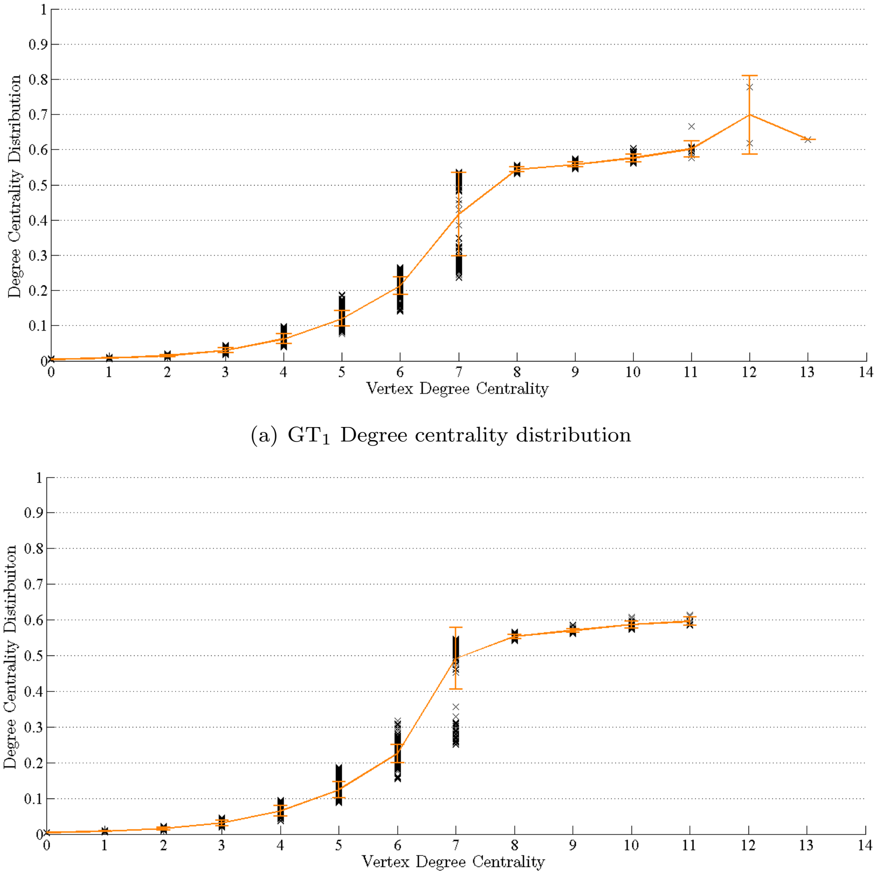
(a) GT$_1$ Simulation sizes

(b) GT$_2$ Simulation sizes

Initial Cell	**Mode Size**	**Mean Size**	**Standard Deviation**	**Minimum**	**Maximum**
GT$_1$	159	146.86	57.99	7	381
GT$_2$	142	161.22	56.56	18	366

(c) “Guerrilla Terrorists” Simulation size statistics

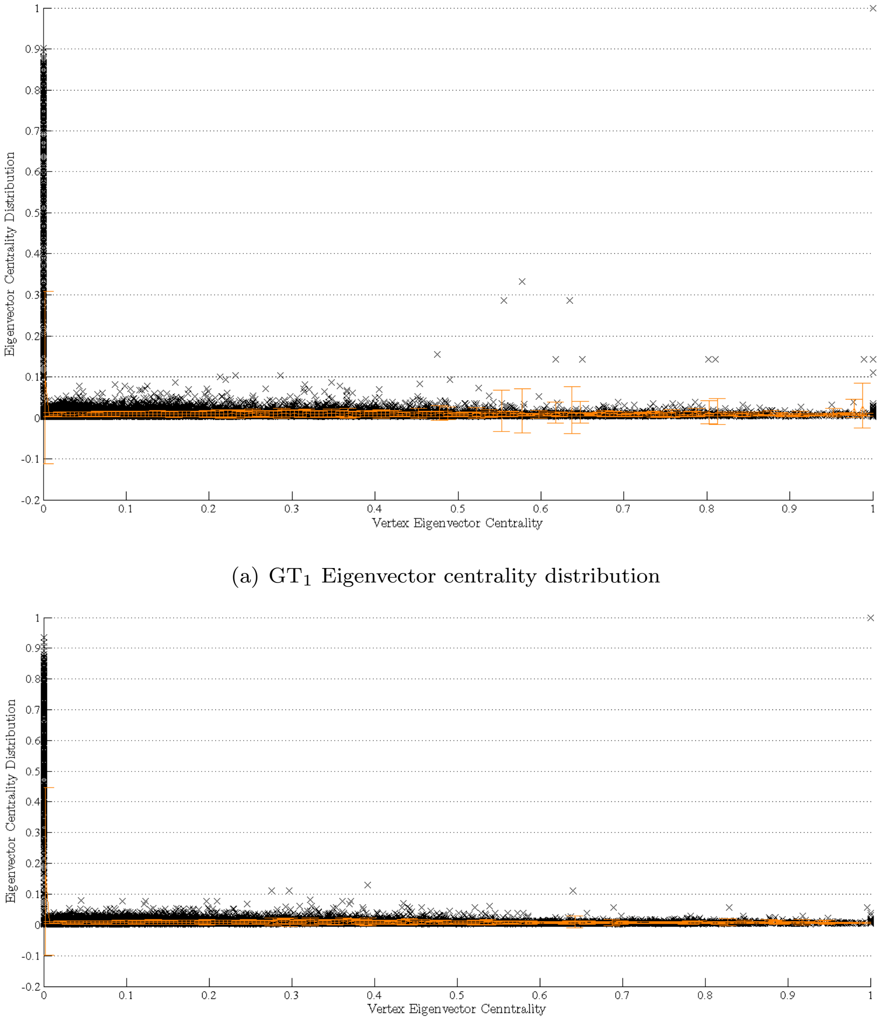
Figure 3.2: “Guerrilla Terrorists” model size properties



(a) GT_1 Degree centrality distribution

(b) GT_2 Degree centrality distribution

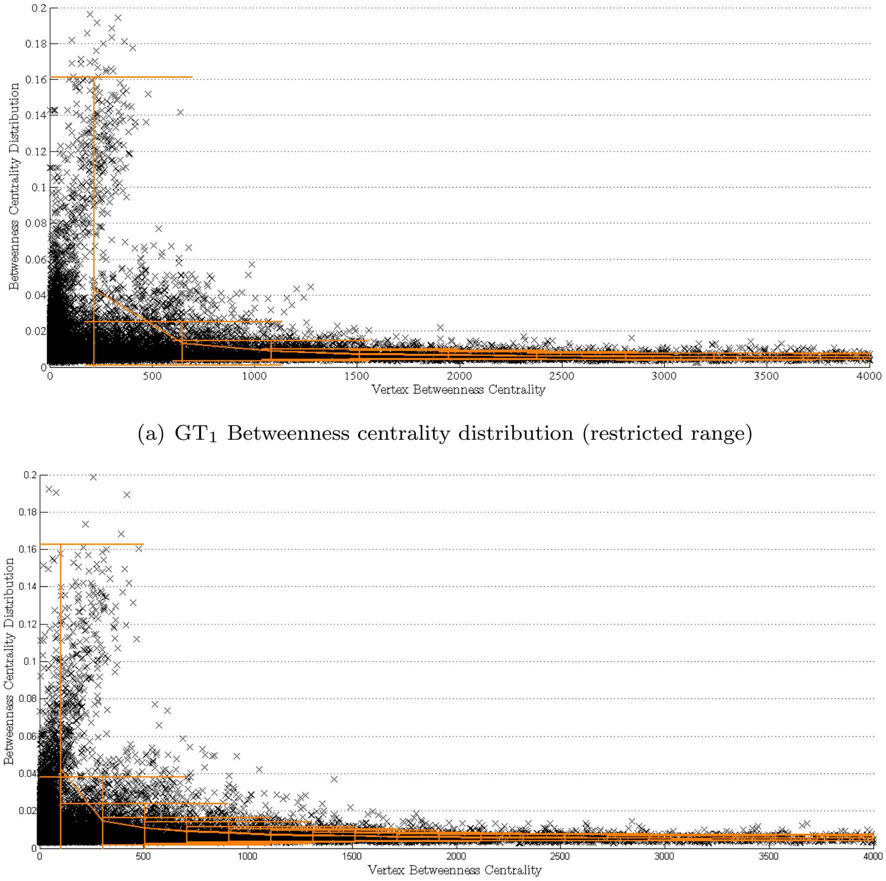
Figure 3.3: “Guerrilla Terrorists” degree centrality distributions



(a) GT_1 Eigenvector centrality distribution

(b) GT_2 Eigenvector centrality distribution

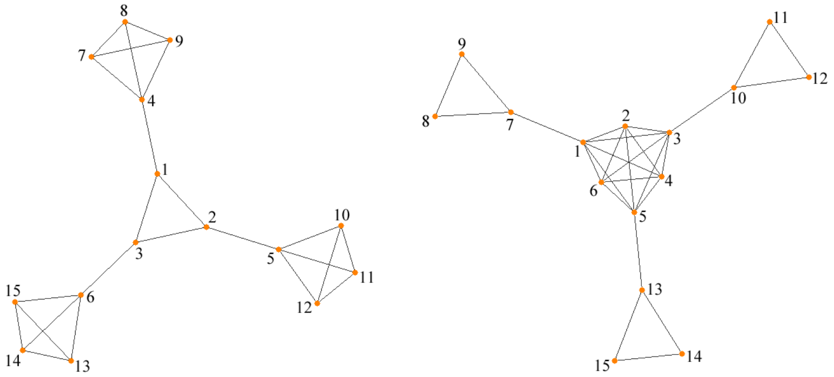
Figure 3.4: “Guerrilla Terrorists” eigenvector centrality distributions



(a) GT_1 Betweenness centrality distribution (restricted range)

(b) GT_2 Betweenness centrality distribution (restricted range)

Figure 3.5: “Guerrilla Terrorists” betweenness centrality distributions



(a) Initial cell FF_1

(b) Initial cell FF_2

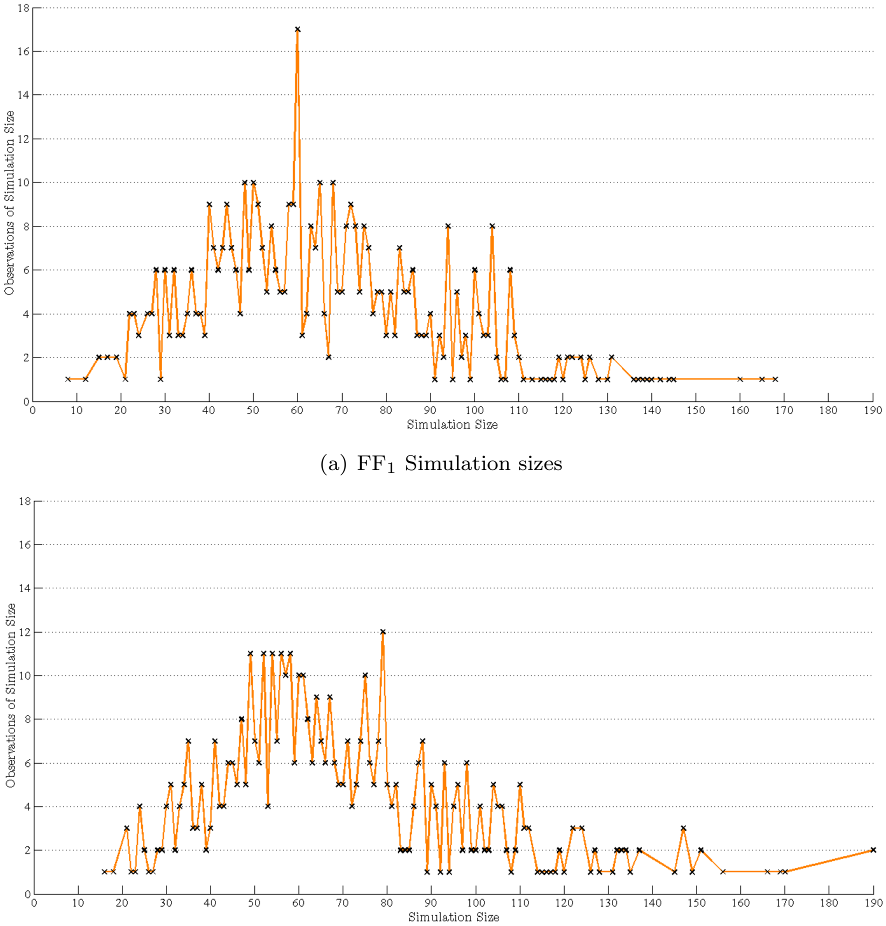
Vertex Number, i	**Degree,** k_i	**Eigenvector,** x_i	**Betweenness,** $C_B(v_i)$	**Clustering,** C_i
1, 2, 3	3	0.8092	1	0.3333
4, 5, 6	4	1	0.825	0.5
(7, 8, 9, 10, 11, 12 and 13, 14, 15)	3	0.8092	0	1

(c) FF_1 Cell metric values

Vertex Number, i	**Degree,** k_i	**Eigenvector,** x_i	**Betweenness,** $C_B(v_i)$	**Clustering,** C_i
1, 3, 5	6	1	1	0.6667
2, 4, 6	5	0.9646	0	1
7, 10, 13	3	0.2163	0.7273	0.3333
8, 9, 11, 12, 14, 15	2	0.0527	0	1

(d) FF_2 Cell metric values

Figure 3.6: Network visualisation and metric values for initial networks FF_1 and FF_2



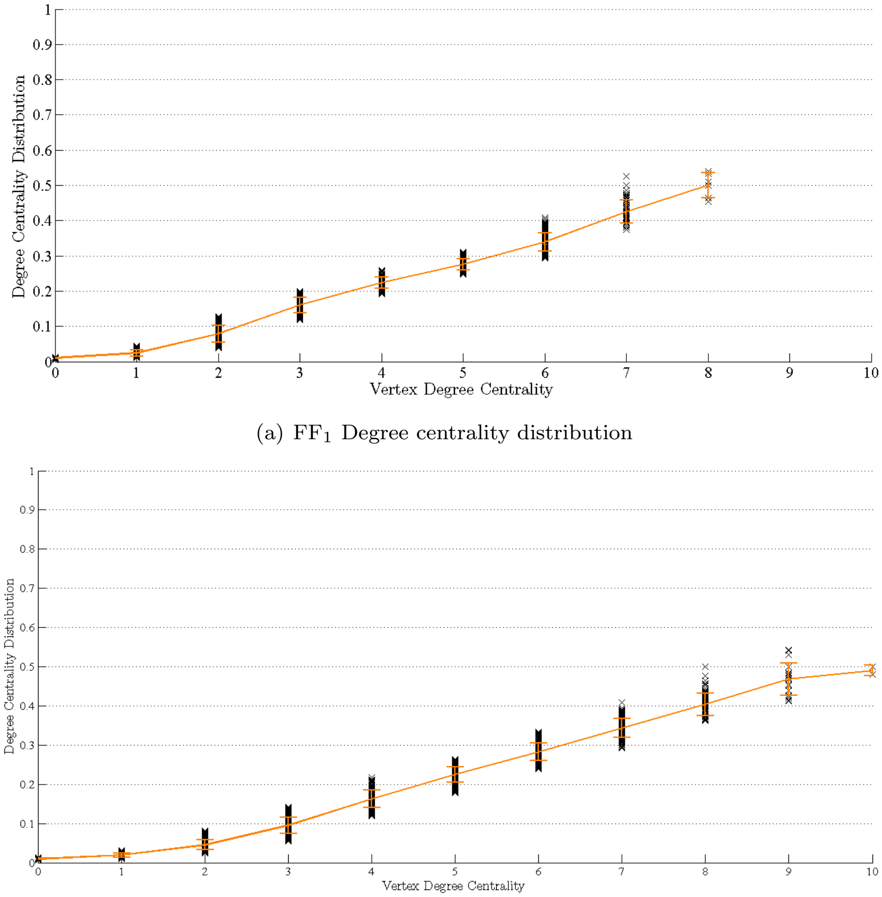
(a) FF$_1$ Simulation sizes

(b) FF$_2$ Simulation sizes

Initial Cell	Mode Size	Mean Size	Standard Deviation	Minimum	Maximum
FF$_1$	60	66.79	28.20	8	168
FF$_2$	79	70.81	29.42	16	190

(c) "Friends and Family" Simulation size statistics

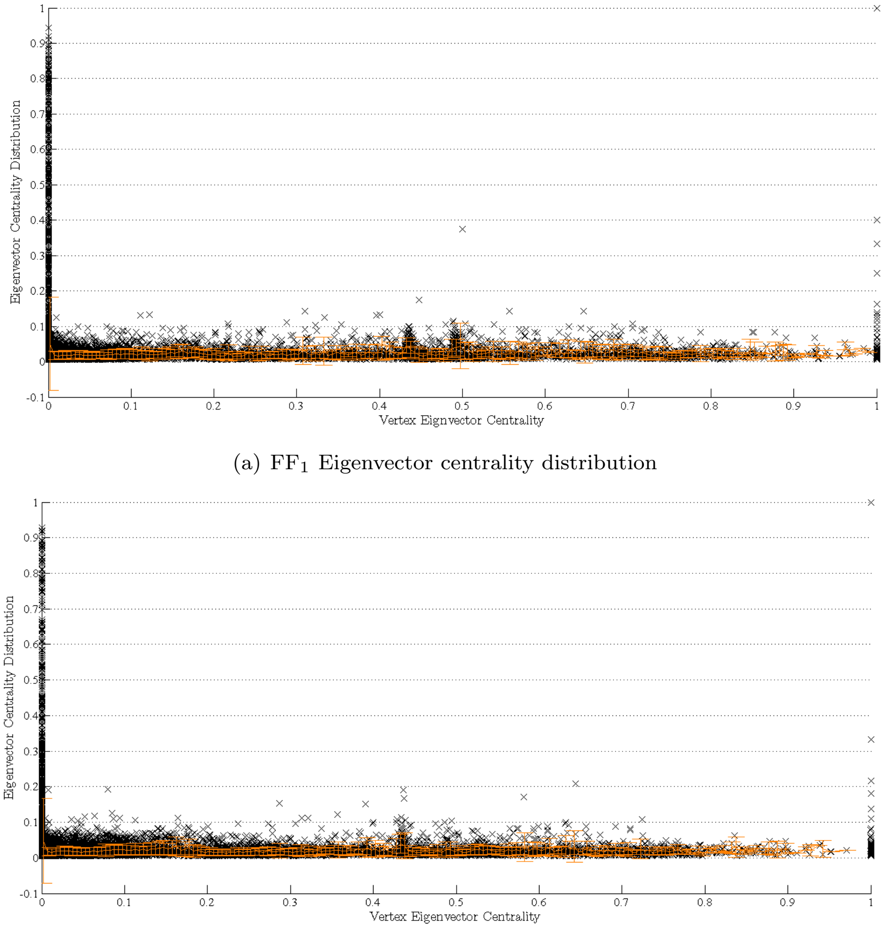
Figure 3.7: "Friends and Family" model size properties



(a) FF_1 Degree centrality distribution

(b) FF_2 Degree centrality distribution

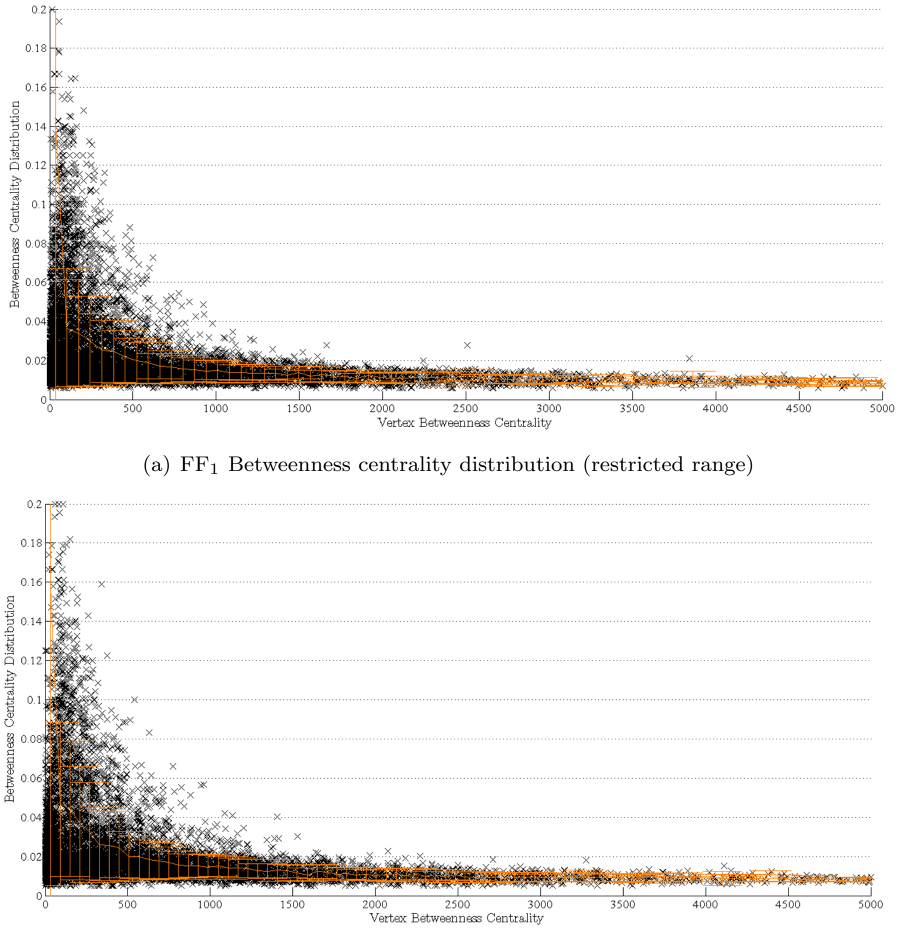
Figure 3.8: “Friends and Family” degree centrality distributions



(a) FF_1 Eigenvector centrality distribution

(b) FF_2 Eigenvector centrality distribution

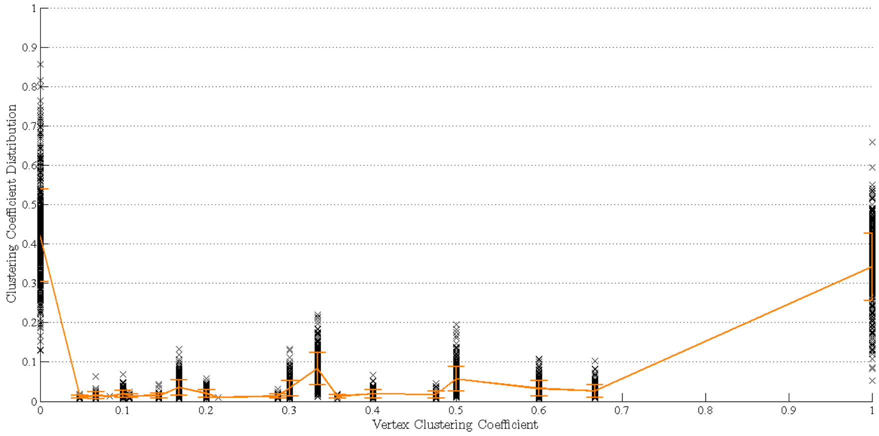
Figure 3.9: "Friends and Family" eigenvector centrality distributions



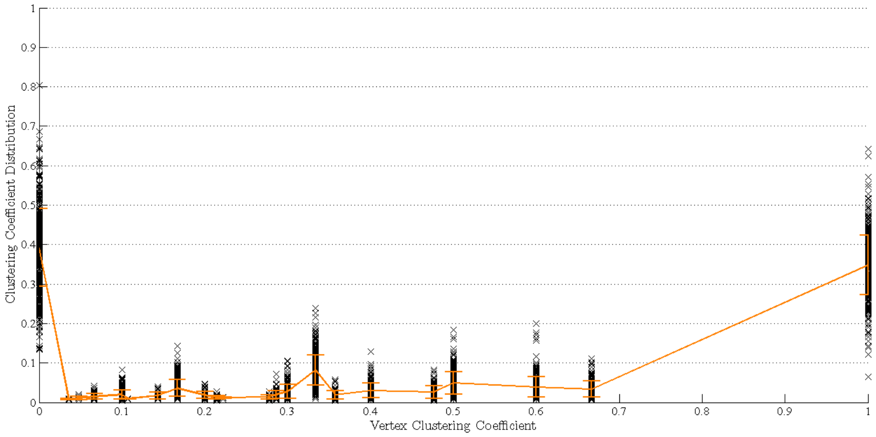
(a) FF_1 Betweenness centrality distribution (restricted range)

(b) FF_2 Betweenness centrality distribution (restricted range)

Figure 3.10: Betweenness distributions (restricted range) of "Friends and Family" model

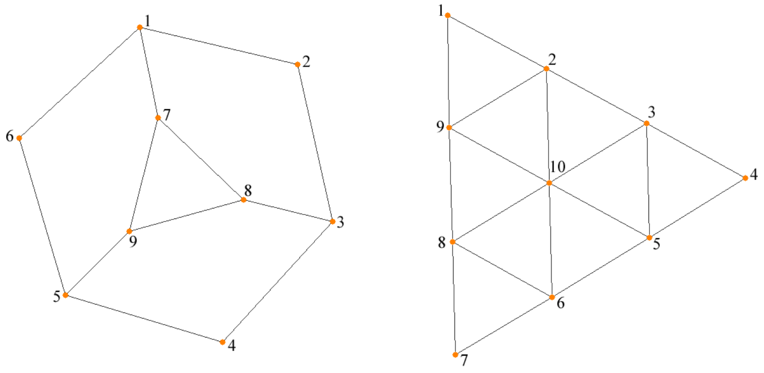


(a) FF_1 Clustering coefficient distribution



(b) FF_2 Clustering coefficient distribution

Figure 3.11: “Friends and Family” clustering coefficient distribution



(a) Initial cell MR_1

(b) Initial cell MR_2

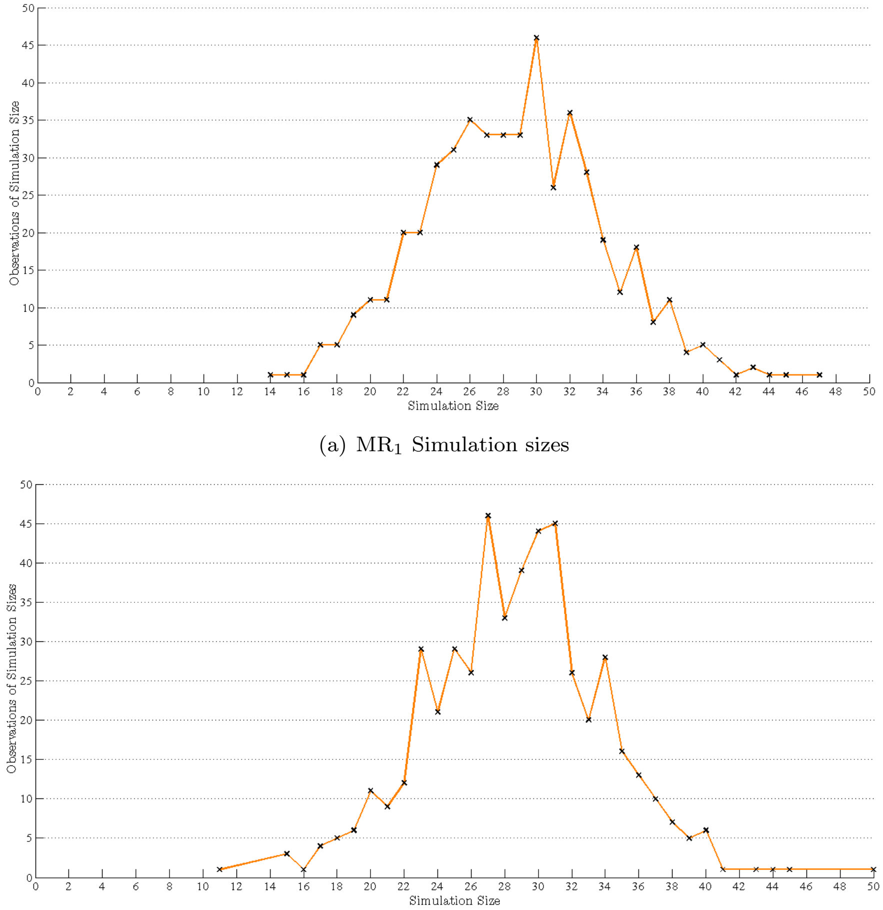
Vertex Number, i	**Degree,** k_i	**Eigenvector,** x_i	**Betweenness,** $C_B(v_i)$	**Clustering,** C_i
1, 3, 5	3	0.7616	1	0
2, 4, 6	2	0.5515	0.4	0
7, 8, 9	3	1	0.6	0.3333

(c) MR_1 Cell metric values

Vertex Number, i	**Degree,** k_i	**Eigenvector,** x_i	**Betweenness,** $C_B(v_i)$	**Clustering,** C_i
1, 4, 7	2	0.3333	0	1
2, 3, 5, 6, 8, 9	4	0.6667	0.4333	0.5
10	6	1	1	0.4

(d) MR_2 Cell metric values

Figure 3.12: Network visualisation and metric values for initial networks MR_1 and MR_2



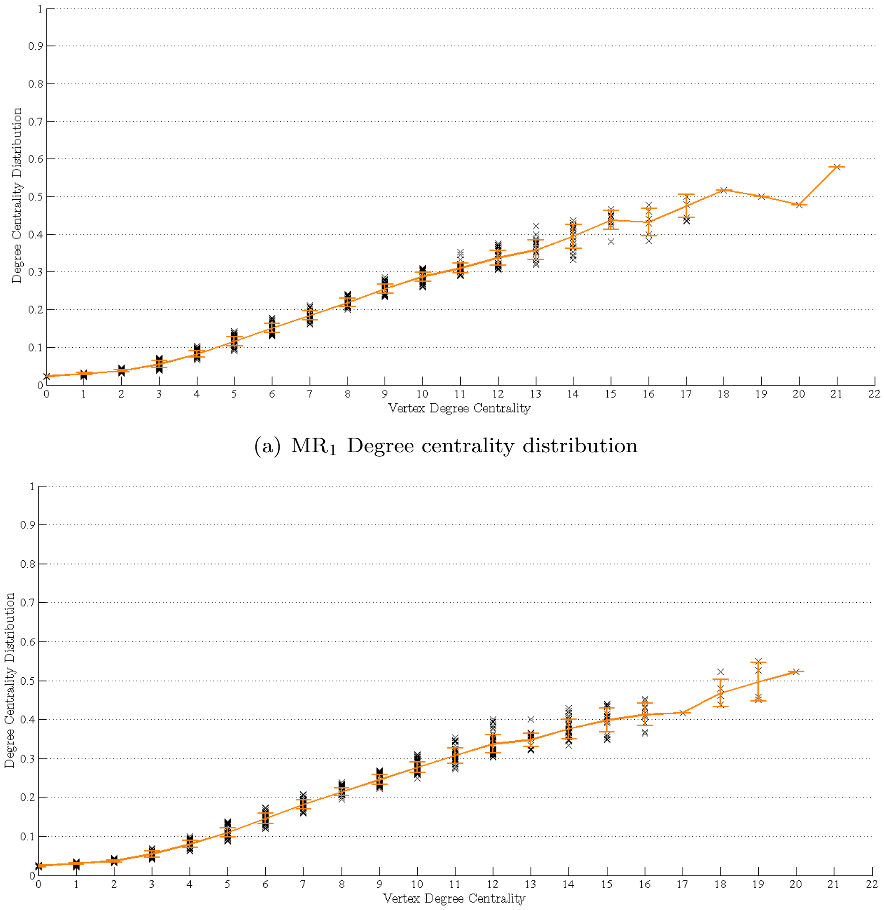
(a) MR_1 Simulation sizes

(b) MR_2 Simulation sizes

Initial Cell	Mode Size	Mean Size	Standard Deviation	Minimum	Maximum
MR_2	27	28.73	5.25	11	50
MR_2	30	28.66	5.42	14	47

(c) “Multiple References” Simulation size statistics

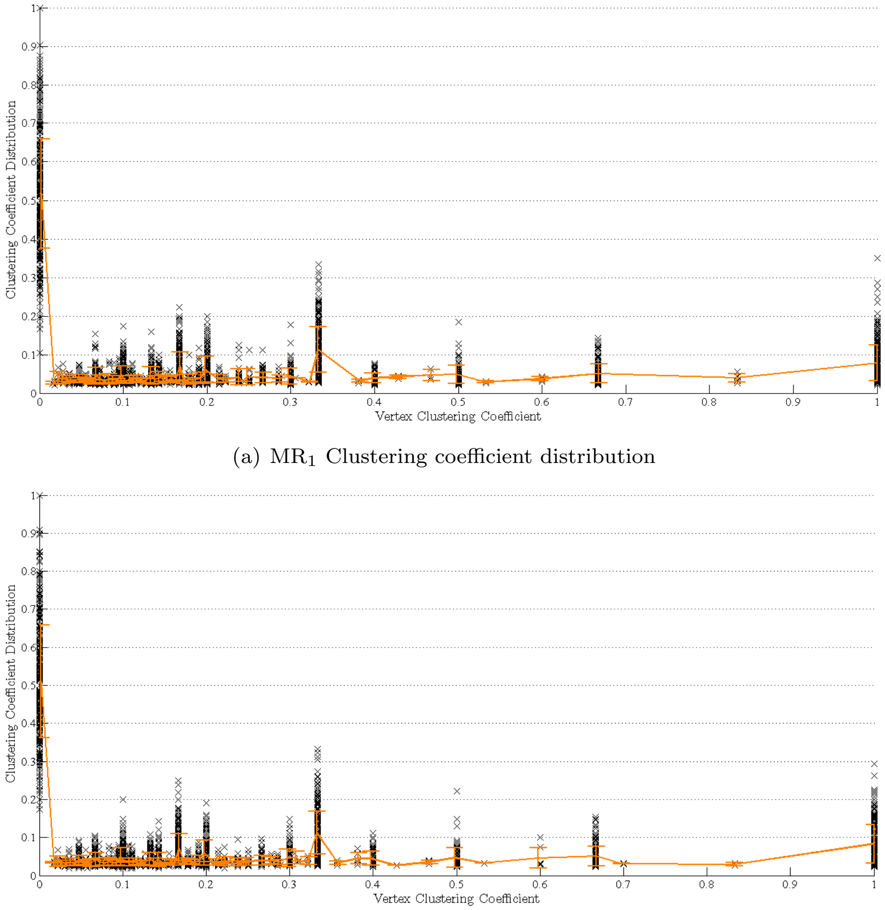
Figure 3.13: “Multiple References” model size properties



(a) MR_1 Degree centrality distribution

(b) MR_2 Degree centrality distribution

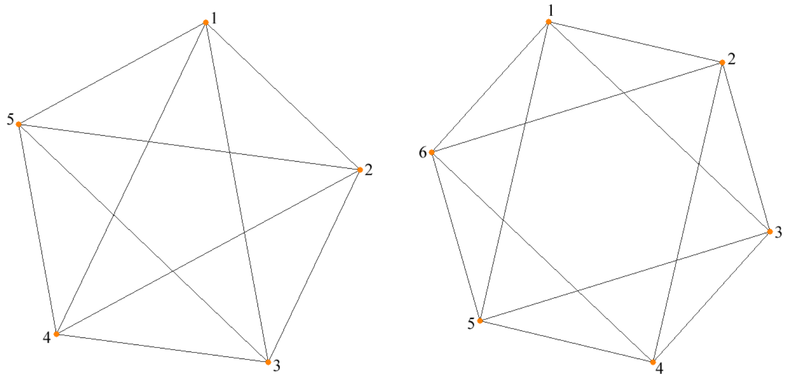
Figure 3.14: "Multiple References" degree centrality distributions



(a) MR_1 Clustering coefficient distribution

(b) MR_2 Clustering coefficient distribution

Figure 3.15: “Multiple References” clustering coefficient distribution



(a) Initial cell GF_1 (b) Initial cell GF_2

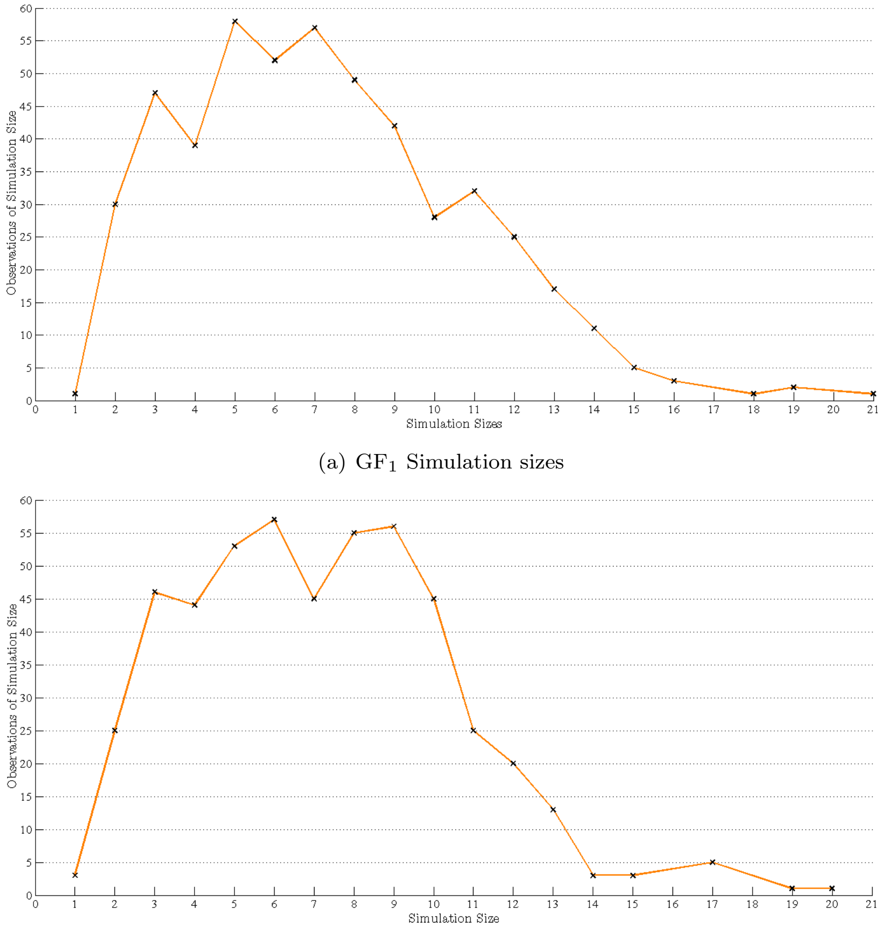
Vertex Number, i	**Degree,** k_i	**Betweenness,** $C_B(v_i)$	**Eigenvector,** x_i	**Clustering,** C_i
1,2,3,4,5	4	0	1	1

(c) GF_1 Cell metric values

Vertex Number, i	**Degree,** k_i	**Betweenness,** $C_B(v_i)$	**Eigenvector,** x_i	**Clustering,** C_i
1,2,3,4,5,6	4	1	1	0.6667

(d) GT_2 Cell metric values

Figure 3.16: Network visualisation and metric values for initial cells GF_1 and GF_2



(a) GF_1 Simulation sizes

(b) GF_2 Simulation sizes

Initial Cell	**Mode Size**	**Mean Size**	**Standard Deviation**	**Minimum**	**Maximum**
GF_1	5	7.27	3.49	1	21
GF_2	6	7.61	3.27	1	20

(c) "Group of Friends" Simulation size statistics

Figure 3.17: "Group of Friends" model size properties

Chapter 4

Dynamics of Attacking Terrorist Cells

4.1 Introduction to "Dark Networks"

The term *"dark network"* has been used to describe any group of individuals acting together to pursue an illegal goal; such as drug trafficking, gun running or organised terrorism [26]. Regardless of objectives, the group will wish to adopt a network topology that minimises members' risk of exposure to law enforcement agencies, whilst allowing efficient and reliable communication between individuals [3]. Networks specifically constructed to prevent infiltration by an opposing organisation are described as *clandestine cells* [56].

Many connections can exist between a "dark network" and its opposing law enforcement agency (e.g. infiltration by double agents, collected counter-intelligence), however it is unlikely either organisation knows the complete structure of the other. While counter-terrorists may hold information on prominent terrorist cell leaders, intelligence gathered on the remaining cell members' identities and interactions may be limited. Thus, when working towards disrupting "dark networks", strategies seek to reveal as many unknown members as possible.

4.1.1 High-Value Targets

Despite typically large national defence budgets, counter-terrorist organisations inevitably face funding and manpower limitations, mainly because the logistics required to combat terrorist cells differ from traditional military intelligence gathering. Therefore, efficient tactics to neutralise terrorist cells are sort.

Since September 11th 2001, the U.S. government has focused on the capture of *high-value targets (HVTs)* to combat terrorisms [26]. A terrorist is described as a HVT for reasons including:

1. Rank within terrorist organisation (e.g. captain, foot soldier),
2. Operational role (e.g. recruiter, bomb maker, hacker),
3. Specialised skills and connections (e.g. multilingual, knowledge of intended target),
4. Links to other HVTs (e.g. shared geographical locations, frequent communication).

4.1.2 HVT Evasion Strategies

HVTs can employ many evasion techniques [26], however collected evidence indicates three basic strategies shown in Table 4.1.

Strategy	**Description**
Masking	Individuals deny participation in terrorism, hiding their involvement to conceal their true identity, location or support network.
Disengagement	HVTs relocate to, and operate in environments where counter-terrorists are unable to search due to political, economic, military or geographical conditions.
Mobility	HVTs continually change location in an erratic and unpredictable manner, forcing counter-terrorist organisations to continually revise their search locations.

Table 4.1: HVT Evasion strategies

HVTs can also utilise a support network within their terrorist cell, which provides assistance and plays an important role in ensuring they evade capture and remain active within the cell.

4.1.3 Head-Hunting and Interrogation

Controversially, the U.S. *Central Intelligence Agency (CIA)* has used waterboarding to extract tactical information from captured terrorists [7,44]. While extreme interrogation methods are rarely employed, bargaining techniques are used to obtain actionable information by testing the loyalty and resolve of detained terrorists.

The ability of HVTs to evade capture, means gathering information directly on a suspect is difficult and time consuming. With interrogation methods in mind, one stratagem is to question known cell members and extract viable information on the intended HVT [21]. This method of *head-hunting* provides a systematic approach to locating and detaining HVTs, and provides valuable information on the overall terrorist cell structure.

4.1.4 Percolation Analysis

Percolation is a mathematical tool that can be used to analyse the dynamic structure of networks by removing some fraction of vertices (*site percolation*) and edges (*bond percolation*) [34]. The criterion for removing network elements can either use a specified set of rules, or be a random attack [34]. A network's resilience to targeted and random percolation attacks, is an important consideration when developing organisational infrastructure.

For example, the World Wide Web (WWW) network structure remains largely operational when subjected to a random percolation attack removing web pages. However, a targeted attack (e.g. removal of Google.com, Bing.com) quickly splits the WWW into disconnected partitions. Reference [25] investigates this phenomena, describing the WWW as "robust yet fragile".

Combining site and bond percolation, I modelled a HVT head-hunting attack on a terrorist cell, and investigated the success of this strategy by comparing generated percolation networks to their original terrorist cell.

4.1.4.1 Modelling Head-Hunting of HVTs

Counter-terrorist organisations typically maintain "watch lists" of individuals; suspected of having terrorist connections, participated in illegal activities, or been exposed to radical extremist views. Individuals are closely monitored until there is sufficient evidence to detain them and/or other suspects.

Discussed in Section 2.4, degree centrality can be a good indicator of the relative importance of terrorist cell members. Thus, my percolation mechanism defines any network vertex with maximal degree to be a terrorist cell HVT:

Terrorist Cell HVTs: Consider a network, G, with size n. Vertex $v_i \in G$ is defined as a HVT of G if it has degree k_i such that:

$$k_i = \max_{j=1\ldots n}\{k_j\}.$$

Because HVTs are actively pursued, and likely to be prominent cell members, it is modelled that HVTs are more likely than non-HVTs to be captured during the initial stage of a systematic percolation attack. The percolation mechanism uses a *degree preferential probability distribution* [Appendix C.4] when capturing initial terrorists.

Terrorist head-hunting is likely to be performed under a range of restrictive factors and timescales, however, my percolation mechanism is modelled under conditions conducive to full interrogation of detained terrorists.

Assuming that actionable information obtained from interrogations is used in subsequent terrorist interrogations, the compounded effects of omitted and incorrect terrorist information decreases the reliability of information obtained as cell members are systematically captured.

4.1.4.2 Head-Hunting Percolation Mechanism

Consider a network G, size n. My percolation mechanism first selects the number of initial captured cell members, $m \in \{1, 2, 3, 4, 5\}$ (uniformly distributed) and uses a degree preferential probabilistic distribution [Appendix C.4] to randomly select m vertices $\{\hat{v}_1 \ldots \hat{v}_m\} \in G$, called "Round 1" terrorist members.

Given satisfactory conditions and time to conduct thorough interrogations, the percolation mechanism models that the quality of any information obtained from captured vertex $\hat{v}_i$, gives an 80% chance of detaining each of neighbouring cell member $\hat{w}_i \in \Gamma(\hat{v}_i)$. Then, examining the neighbourhood $\Gamma(\hat{v}_i)$ of each "Round 1"terrorist, we add a neighbouring vertex $\hat{w}_j \in \Gamma(\hat{v}_i)$, and corresponding edge $e(\hat{v}_i, \hat{w}_j)$, to the percolation network $\hat{G}$ with probability:

$$\mathbb{P}(\text{Vertex } \hat{w}_j \in \Gamma(\hat{v}_i) \text{ is added to the percolation network } \hat{G}) = 0.80.$$

If vertex $\hat{v}_i$ has a neighbour $\hat{w}_k \in \hat{G}$, already contained within the percolation network, the above probability is simply used only to decide if the edge $e(\hat{v}_i, \hat{w}_k)$ is added to $E(\hat{G})$. Any newly added vertices $\hat{w}_j \in \hat{G}$ are called "Round 2" terrorists.

My percolation mechanism also models how interrogation information becomes less reliable as the systematic percolation attack progresses. Thus, for a "Round 2" terrorist $\hat{w}_i \in \hat{G}$, it is modelled that the "Round 3" terrorist $\hat{u}_j \in \Gamma(\hat{w}_i)$ is added to $\hat{G}$ with probability:

$$\mathbb{P}(\text{Vertex } \hat{u}_j \in \Gamma(\hat{w}_i) \text{ is added to the percolation network } \hat{G}) = (0.80)^2.$$

This percolation mechanism continues by adding "Round $(k+1)$" terrorists, selected from the neighbourhoods of each "Round k" terrorist, to the percolation network $\hat{G}$ with probability:

$$\mathbb{P}(\text{``Round } (k+1)\text{'' vertex } \hat{v}_i \in \Gamma(\text{``Round } k\text{'' vertex}) \text{ is added to } \hat{G}) = (0.80)^{k-1},$$

and iterates until no new percolation vertices are added, or until all members of the original network G are added to the percolation network $\hat{G}$.

4.1.5 Comparing Percolation Networks with Original Terrorist Cells

Using the above percolation mechanism, I generated a single percolation network for each simulation constructed by the three generative models; "Guerrilla Terrorists" (Section 3.3), "Friends and Family"

(Section 3.4) and "Multiple References" (Sections 3.5).

I calculated the network size, degree centrality distribution and the number of HVTs contained within each generative mechanism simulation, and found the network size and degree distribution for each percolation network. Additionally, to quantify the success of the percolation attacks, I calculated the number of HVTs present within each percolation network as a fraction of possible simulation HVTs.

1. **"Guerrilla Terrorists"**
   Identifying the HVTs in each simulation G, and noting the number of HVTs contained within the corresponding percolation network $\hat{G}$, I found the mean fraction of HVTs successfully captured by the percolation mechanism is 0.1561.

   Sorting data values by increasing "Guerrilla Terrorists" simulation size, Figure 4.1 compares the size of each simulation G with the size the corresponding percolation network $\hat{G}$. Figure 4.1 shows that generated percolation networks appear to have sizes limited to less than 70.

   Figures 4.2(a) and 4.2(b) compare the degree distributions of the simulations with the corresponding percolation networks distributions, for the two initial networks GT_1 and GT_2.

   This analysis shows that the percolation mechanism generates networks with very different characteristics to their original simulations, which on average contain 15% of the simulation HVTs. Hence, the "Guerrilla Terrorists" model generates simulations that are particularly effective at protecting HVTs, and the overall cell structure, from the modelled percolation attack.

2. **"Friends and Family"**
   The mean fraction of "Friends and Family" HVTs successfully captured by the percolation mechanism, is approximately 63.6% of all HVT terrorists.

   Sorting data values by increasing simulation size, Figure 4.3 , shows a similar limited range of percolation size values as in Figure 4.1.

   Figures 4.4(a) and 4.4(b) show the simulation degree distributions for initial cells FF_1 and FF_2, and the corresponding generated percolation networks.

   Hence we see the percolation method is more successful at locating "Friends and Family" simulation HVTs, but produces percolation networks of limited size. This suggests that the percolation mechanism is effective at locating HVTs, but leaves a significant number of unknown cell members undetected. Depending on the changes in hierarchical structure once a HVT is removed, the percolation mechanism may successfully disband the cell, or simply shift the leadership to another terrorist member.

3. **"Multiple References"**
   Percolation networks generated on "Multiple References" simulations successfully capture a mean fraction 0.9741 of HVTs. Hence, HVTs in "Multiple References" simulations appear particularly vulnerable to capture by this systematic percolation attack.

   Figure 4.5 compares the sizes of "Multiple References" simulations with the corresponding percolation networks. In contrast to Figures 4.1 and 4.3, the percolation size does not take a limited range of values, and we see that there are several simulations completely captured by the percolation method.

   Figures 4.6(a) and 4.6(b) compare degree distributions of the simulations with percolation networks, for initial networks MR_1 and MR_2. Differences in degree distribution curves suggest a significant difference in the network structures.

   We find that the systematic percolation mechanism is highly effective at capturing HVTs within "Multiple References" simulations, and is observed to occasionally reveal every simulation terrorist. Differences in simulation and percolation degree distributions suggest the percolation networks contain few original simulation edges, meaning that the terrorist interactions are not fully uncovered.

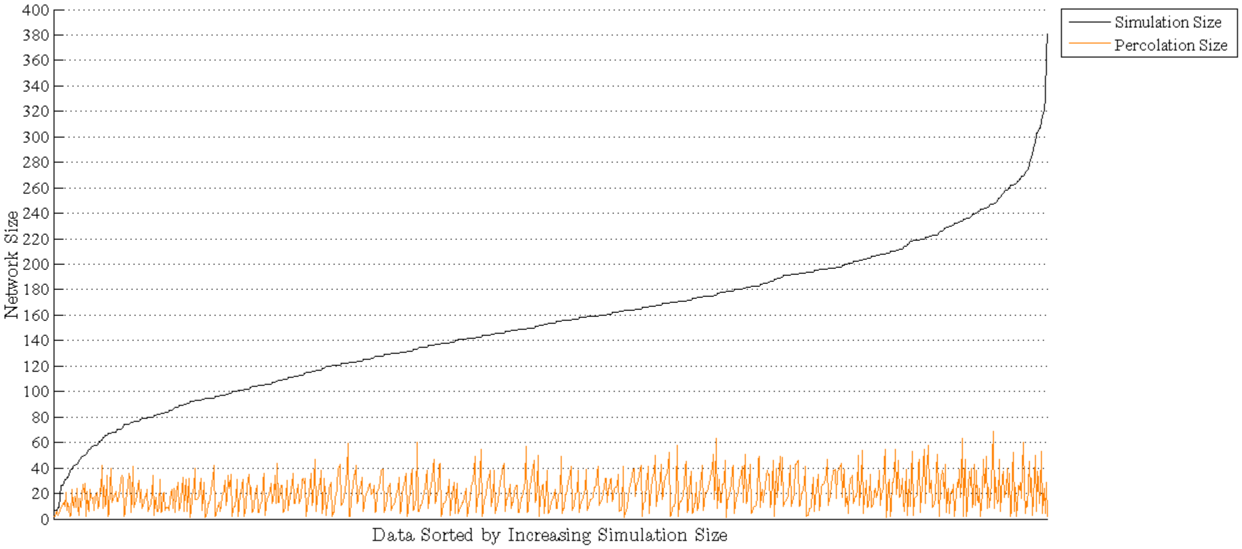
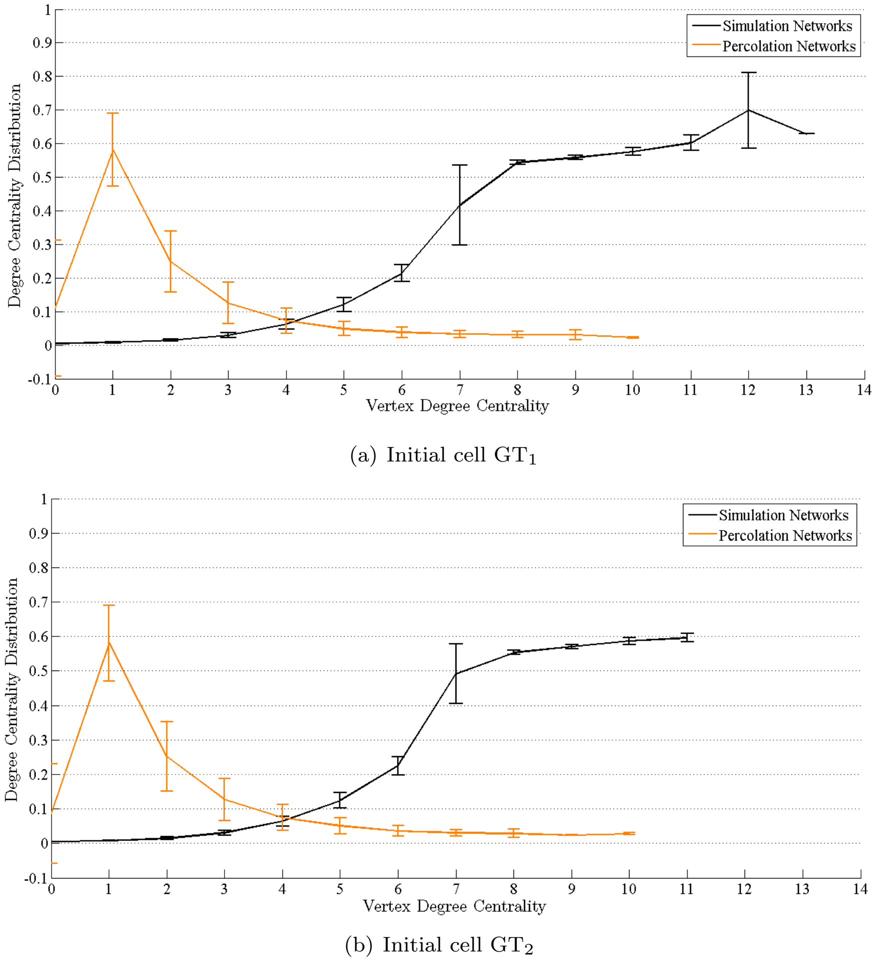


Figure 4.1: Comparison of “Guerrilla Terrorists” simulation and percolation sizes



(a) Initial cell GT_1

(b) Initial cell GT_2

Figure 4.2: “Guerrilla Terrorists” simulation and percolation network degree distributions

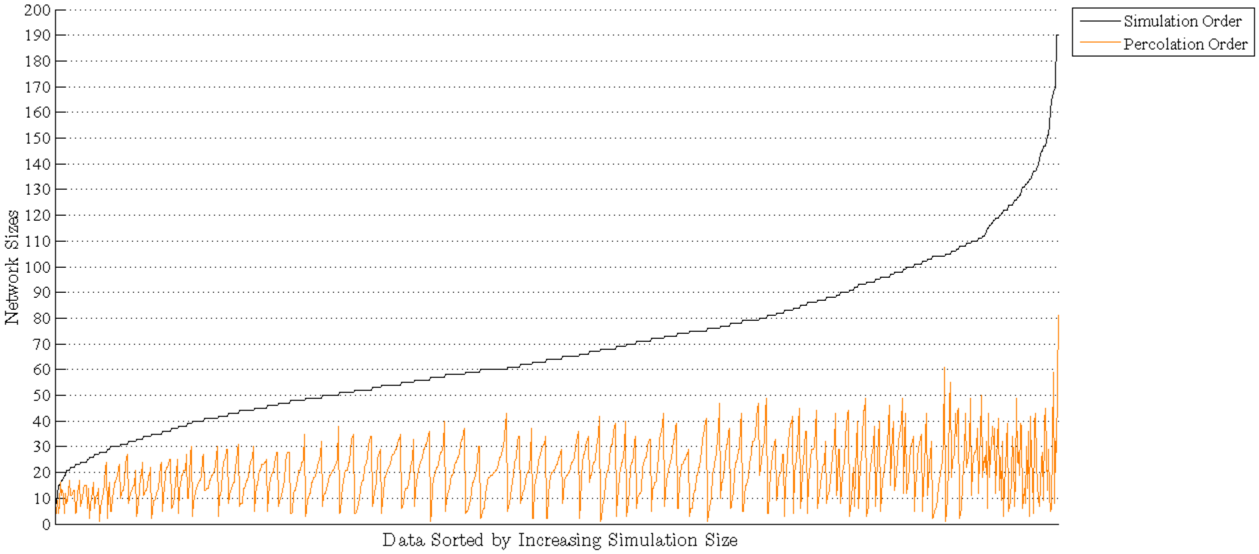
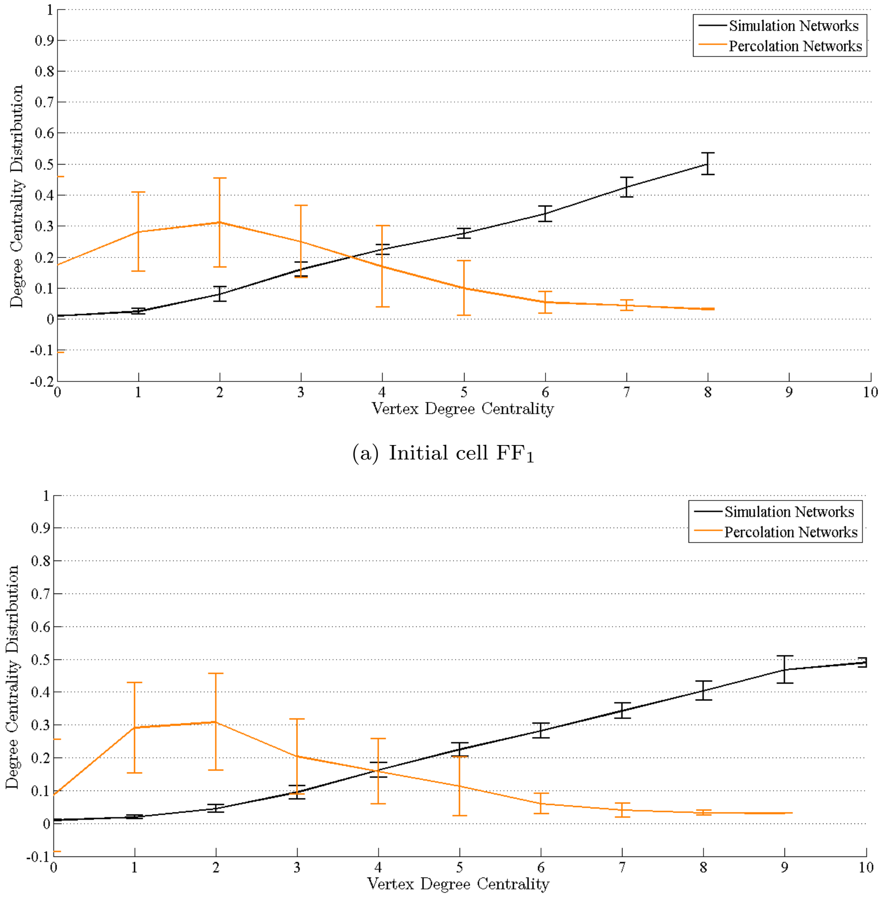


Figure 4.3: Comparison of “Friends and Family” simulation and percolation sizes



(a) Initial cell FF_1

(b) Initial cell FF_2

Figure 4.4: “Friends and Family” simulation and percolation network degree distributions

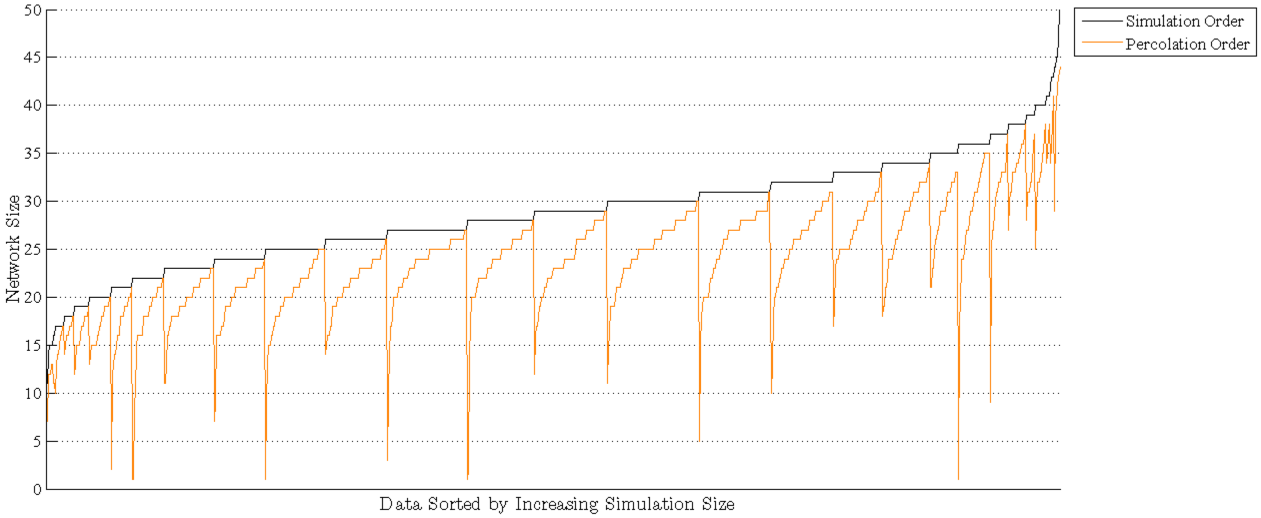
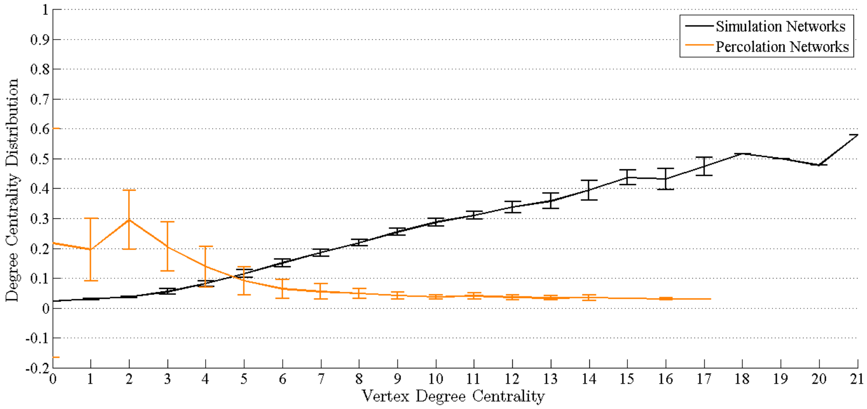
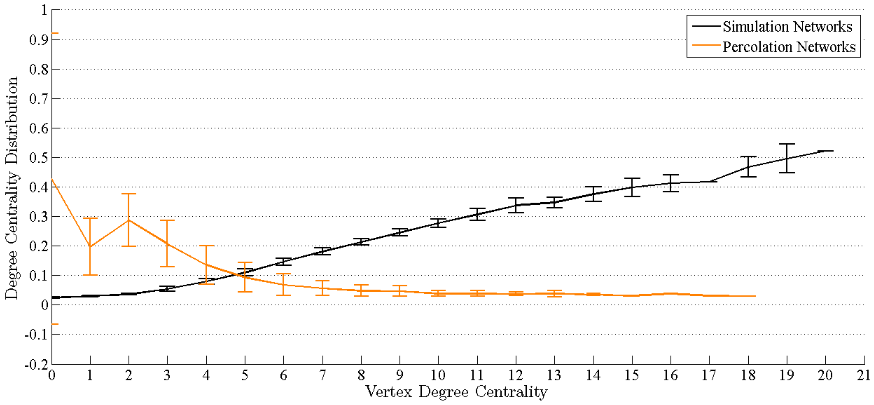


Figure 4.5: Comparison of “Multiple References” simulation and percolation sizes



(a) Initial cell MR_1



(b) Initial cell MR_2

Figure 4.6: “Multiple References” simulation and percolation network degree distributions

Chapter 5

Conclusions

5.1 Evaluation of Generative Mechanisms

My investigation into terrorist networks primarily aimed to examine and develop generative mechanisms that simulate the formation of different terrorist cells. Considering a range of possible recruitment motivations and methodologies, I programmed and evaluated four different terrorist cell construction methods. These models were motivated by using real terrorist network data, whose network properties I had previously investigated.

Considering two different initial networks, I generated 1,000 distinct simulations for each of the four generative mechanisms, and calculated the mean network metric distributions. Comparing the simulation's mean metric distribution curves with those calculated from the real terrorist networks, I have found that certain terrorist cell characteristics were simulated better than others.

This suggests that select aspects of terrorist recruitment can be successfully modelled using network theory. The "Friends and Family" and "Multiple References" mechanisms generate networks that display similar eigenvector centrality, betweenness centrality and clustering coefficient distributions to those produced by the S11 and M11 terrorist networks. However, differences in degree distributions suggest the generated simulations have network structures that vary to those of the real terrorist cell.

The extent to which I am able to evaluate my generative models is limited by the amount and quality of real terrorist data available to me, and I have only been able to make comparisons with terrorist data used to motive each model.

5.2 Percolation Analysis Evaluation

Examining descriptions of real counter-terrorist head hunting tactics [21, 26], I developed a percolation mechanism to simulate a selective systematic attack on terrorist networks.

I generated percolation networks for each simulation constructed using my "Guerrilla Terrorists", "Friends and Family" and "Multiple References" generative mechanisms, however due to time constraints, I could only perform one percolation analysis on each simulation and therefore was unable to calculate mean percolation properties for each network.

My investigation showed that the percolation mechanism was more successful at uncovering the simulation networks of some generative mechanisms than others. Given the huge range of possibilities for terrorist network structures, this is not a surprising result. If similar percolation attacks are employed to disband real terrorist networks, information on the structure of the target terrorist cell will need to be gathered so that percolation parameters can be chosen to optimise the attack results. Additionally, a specific criterion used to define HVTs should be chosen to ensure the percolation removes terrorists whose removal is most likely to result in the cell being disbanded.

5.3 Improvements and Alterations

Generative Mechanism Development
During the preliminary analysis and development of each generative mechanism, I selected modelling constants and event probabilities without quantitative input from previous construction model research. For example, the number of terrorists recruited by each "Guerrilla Terrorists" active recruiter follows a discrete approximation of the exponential distribution, chosen to favour the recruitment of zero new terrorist members, with a decreasing probability of recruiting $\{1, 2 \dots 5\}$ new members.

Given chance to investigate my generative mechanism using different probability density functions and modelling constants, I would investigate the effects these constants have on the final simulation network structures.

Using an optimisation method, for example *HillClimbing* or *Simulated Annealing* techniques [6], it may be possible to adjust my generative mechanisms to produce simulation networks that better mimic the organisational structures of the real terrorist networks.

Initial Cell Choice
Each generative mechanism is considered for two different initial networks. As with the development of the generative mechanisms, there was little information available suggesting initial suitable networks to consider, and the cells I chose were motivated by my preliminary analysis.

Considering a sample of two initial cells provided little variation in generated simulation structure, and I could not conclude if the generated simulations depended on their initial conditions. By investigating a greater number of different initial cells, it may highlight any varying effects an initial network has on the resultant generated simulations.

Furthermore, my choices of initial cell displayed symmetrical features, so investigating asymmetrical and random initial cells should be considered.

5.4 Further Investigations

M11 Weighted Network Analysis
My investigation examined the structural properties of the simple, unweighted, undirected M11 terrorist network. Using the weightings assigned in Reference [29], and a selection of network metric measures redefined to evaluate weighted networks, an enhanced investigation could be undertaken.

Interactions Between Fragmented Terrorist Cells
My generative models each incorporate mechanisms that allow terrorists to become isolated from all members of a terrorist cell, and allow terrorist networks to be split into disconnected subgraphs. In order to simplify computation of simulations networks, I assumed that once individuals become isolated they lost faith in the security of their original terrorist cell and do not try to rejoin it.

Whilst this is a reasonable assumption to make under certain circumstances, including a mechanism which allows disconnected cell members to reconnect with terrorist cells would enhance my generative mechanisms.

The following example mechanism would allow isolated vertices to reattach to a terrorist cell using a degree preferential probability distribution. Considering an isolated vertex v and terrorist network G of size n:

1. At each time step, an isolated vertex v decides to reattach to the terrorist cell G with probability:
$$\mathbb{P}(\text{Vertex } v \text{ reattaches to network } G) = \alpha$$
for some positive constant $0 < \alpha \leq 1$.
2. Using a preferential degree probability distribution, a single cell vertex $w_i \in G$ with degree $= k_i$, is chosen by v to reconnect to:
$$\mathbb{P}(v \text{ reattaches to vertex } w_i \in G\ ) = \frac{k_i}{\left(\sum_{j=1}^{n} k_j\right)}.$$

Combinations of Generative Mechanisms

Extending the ideas above, the a reattachment mechanism could also allow the interactions between multiple initial terrorist cells, each cell consisting of vertices controlled by a different generative mechanism, to be modelled.

By examining the resultant network of interconnected initial terrorist cells, the structural features could give an insight into the relative dominance of each generative mechanism.

HVT Definitions

As discussed is Section 5.2, the effectiveness of systematic percolation attacks are likely to depend on the criterion used to define terrorist cell members as a HVT. My investigation uses network degree to define HVT cell members, Section 4.1.4.1.

Further investigation into systematic percolation attacks could examine the effects of using different network metrics to define HVTs.

Appendix A

A.1 Additional Network Types

As discussed in Section 1.1, network theory is a powerful analytical tool that allows a range of different network structures to be mathematically modelled. Adjusting the properties of vertices and edges contained within a network, the following structural types can be examined [34]:

Complex Network
If two vertices are connected by $\alpha \in \mathbb{N}_{>0}$ distinct edges, we say that there is a *multi-edge* of order α between these two points. If an edge connects a vertex to itself, we say the vertex has a *self-edge*. Any network that contains either a multi-edge or self-edge is said to be a *complex network*.

Weighted Network
If we can numerically evaluate the strength of interactions between network vertices, we can assign *weights* to the corresponding edges to highlight the more important network interactions. This is achieved using a modified adjacency matrix:

$$A = (a_{ij})_{1 \leq i,j \leq n} \qquad\qquad \text{where } a_{ij} \in \mathbb{R}_{\geq 0}.$$

Directed Network
Interactions between vertices can be restricted to occur in one direction only. By assigning a direction of travel to each network edge, we can simulate directional interactions within a network using an asymmetrical adjacency matrix.

Multiple Vertices/Edges
Organisational structures containing two or more types of components (e.g. customers, products, and employees within a business) can be modelled by a network containing more than one set of vertices. Similarly if a network contains multiple types of vertex connections, more than one type of edge is used.

A.2 Perron-Frobenius Theorem

The matrix $A \in \mathcal{M}_{n\times n}(\mathbb{R})$ is said to be *regular* if there exists an integer $k \in \mathbb{N}_{>0}$ such that:

$$\left(A^k\right)_{ij} > 0, \qquad\qquad \text{for all } 1 \leq i, j \leq n.$$

Equivalently, A is a regular matrix if A has a corresponding digraph G, such that there exists a directed path between every pair of graph vertices $v_i, v_j \in G$.

Let $A \in \mathcal{M}_{n\times n}(\mathbb{R})$, be a regular, non-negative matrix with entries $a_{ij} \geq 0$, for all $1 \leq i, j \leq n$. There then exists an eigenvalue λ_{PF} of A, called the Perron-Frobenius eigenvalue [46], such that:

1. $\lambda_{\mathrm{PF}} \in \mathbb{R}$ and $\lambda_{\mathrm{PF}} > 0$.

2. The corresponding right, $\underline{\mathbf{x}}_{\mathrm{PF}}$, and left, $\underline{\mathbf{y}}_{\mathrm{PF}}$, eigenvectors of λ_{PF} are strictly positive:

$$\begin{aligned}\underline{\mathbf{x}}_{\mathrm{PF}} &= (x_i)_{1\leq i\leq n}, &\qquad \text{with } x_i > 0 \text{ for all } 1 \leq i \leq n,\\ \underline{\mathbf{y}}_{\mathrm{PF}} &= (y_j)_{1\leq j\leq n}, &\qquad \text{with } y_j > 0 \text{ for all } 1 \leq j \leq n.\end{aligned}$$

3. All other eigenvalues λ, of matrix A, satisfy the inequality:

$$|\lambda| < \lambda_{\mathrm{PF}}.$$

The Perron-Frobenius can be extended to the non-negative case for *irreducible* matrices. The matrix $B \in \mathcal{M}_{n\times n}(\mathbb{R})$ is said to be irreducible if there is no permutation that transforms B into block upper-triangular form [23]:

$$\begin{pmatrix}\beta_{11} & \beta_{12}\\ 0 & \beta_{22}\end{pmatrix}.$$

Equivalently, B is irreducible if B forms a corresponding digraph which is non-strongly connected.

Let $B \in \mathcal{M}_{n\times n}(\mathbb{R})$, be a irreducible, non-negative matrix with entries $b_{ij} \geq 0$, for all $1 \leq i, j \leq n$. The Perron-Frobenius eigenvalue, λ_{PF}, satisfies:

1. $\lambda_{\mathrm{PF}} \in \mathbb{R}$ and $\lambda_{\mathrm{PF}} \geq 0$.
2. The corresponding right, $\underline{\mathbf{x}}_{\mathrm{PF}}$, and left, $\underline{\mathbf{y}}_{\mathrm{PF}}$, eigenvectors of λ_{PF} are strictly positive:

$$\begin{aligned}\underline{\mathbf{x}}_{\mathrm{PF}} &= (x_i)_{1\leq i\leq n}, &\qquad \text{with } x_i \geq 0 \text{ for all } 1 \leq i \leq n,\\ \underline{\mathbf{y}}_{\mathrm{PF}} &= (y_j)_{1\leq j\leq n}, &\qquad \text{with } y_j \geq 0 \text{ for all } 1 \leq j \leq n.\end{aligned}$$

3. All other eigenvalues λ, of matrix B, satisfy the inequality:

$$|\lambda| \leq \lambda_{\mathrm{PF}}.$$

Appendix B

B.1 Mean Metric Distribution Calculation

Consider a network G of size n. Suppose we have the degree centrality, k_i, eigenvector centrality, x_i, betweenness centrality, $C_B(v_i)$, and clustering coefficient, C_i, values for each vertex $v_i \in G$. Calculating the corresponding non-dimensionalised metric distributions, I obtain $\rho_k(v_i), \rho_x(v_i), \rho_{C_B}(v_i)$ and $\rho_C(v_i)$, for each vertex v_i.

I have defined the *mean metric distribution*, $\bar{\rho}(v_i)$, to be the mean value of the above four metric distributions:

$$\bar{\rho}(v_i) = \left(\frac{\rho_k(v_i) + \rho_x(v_i) + \rho_{C_B}(v_i) + \rho_C(v_i)}{4} \right).$$

Appendix C

C.1 Programming Limitations

During my investigation I have made extensive use of MATLAB, to calculate network metric measures, plot metric distribution graphs and create network visualisations using procedures written for Reference [5]. I also programmed my generative models with Microsoft Visual Basic for Applications (VBA), in conjunction with Microsoft Excel.

Using Excel and VBA code to produce generative simulations, allowed me to record the step-by-step simulation construction, as I was able to store the generative adjacency matrix, for each distinct time step, using separate Excel worksheet.

While my adopted programming method produced data rich simulation files, the time required to run each simulation limited the number of time steps I could feasibly study, and the complexity of my programming. Hence, I have run my generative mechanisms for different numbers of time steps to alleviate data processing limitations.

C.2 Exponential Probability Distribution

The *Exponential probability distribution* describes a family of continuous random probability distributions, denoted $X \sim \mathrm{Exp}(\lambda)$, for a positive parameter $\lambda > 0$.

The exponential probability density function (PDF) of a random variable $X \sim \mathrm{Exp}(\lambda)$ is defined as [20, 64]:

$$f(x;\lambda) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Figure C.1 shows the exponential PDF for three values of λ.

C.3 Number of Edges–Degree Relationship

Consider a network G with size n and vertices $V(G) = \{v_i \mid i = 1 \dots n\}$. The number of edges in G, $e(G)$, satisfies the relationship [12]:

$$\sum_{j=1}^{n} k_j = 2e(G)$$

where k_i is the degree of vertex $v_i \in G$.

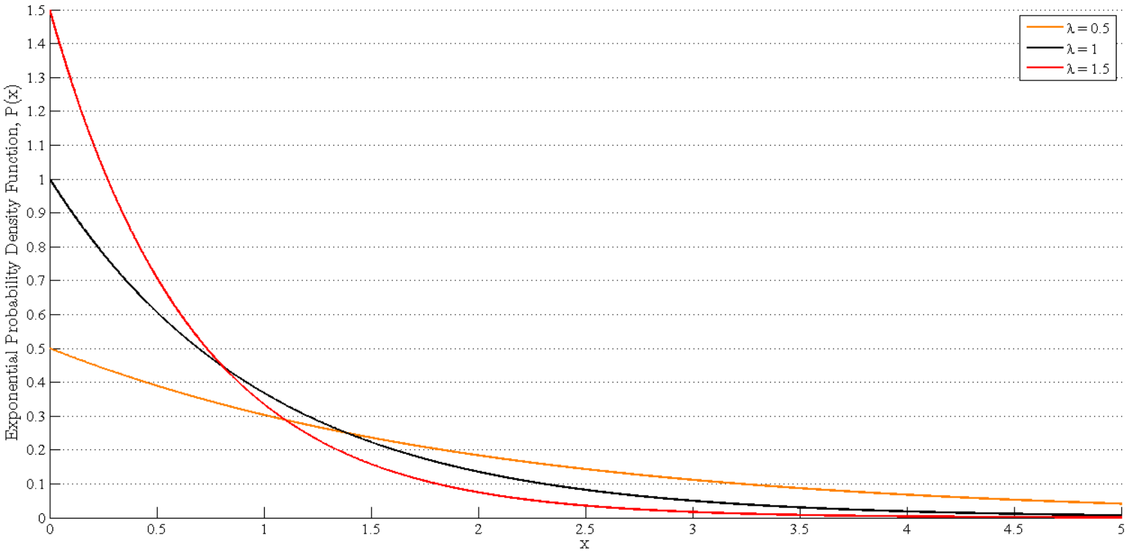


Figure C.1: Exponential probability density function

C.4 Degree Preferential Probability Distribution

As discussed in Reference [34], there are many common generative mechanisms used to construct random networks. One such generative method is called *degree preferential attachment* that constructs a network by randomly attaching a new vertex $\hat{v}$ to an existing network vertex $v_i \in G$, using a probability distribution that favours selecting v_i with large degree k_i.

Consider a network G, size n, and vertices $V(G) = \{v_i \mid i = 1 \dots n\}$ with degrees k_i. The *degree preferential probability distribution* selects a vertex $v_i \in G$, to attach $\hat{v}$ to, with probability:

$$\begin{aligned} \mathbb{P}(\text{Vertex } \hat{v} \text{ is attached to } v_i \in G) &= \frac{k_i}{\left(\sum_{j=1}^{n} k_j\right)} \\ &= \left(\frac{k_i}{2e(G)}\right) \end{aligned}$$

where the final equation form is obtained using Appendix C.3.

C.5 Weibull Probability Distribution

The *Weibull distribution* is a continuous probability distribution characterised by tow positive parameters; *shape* parameter $k > 0$ and *scale* parameter $\lambda > 0$.

The Weibull PDF for a random variable $X \sim \text{Weibull}(k, \lambda)$ is defined as [65]:

$$f(x; k, \lambda) = \begin{cases} \frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} e^{-(x/\lambda)^k} & x \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Figure C.2 shows the Weibull PDF for four different combinations of $k > 0, \lambda > 0$ values.

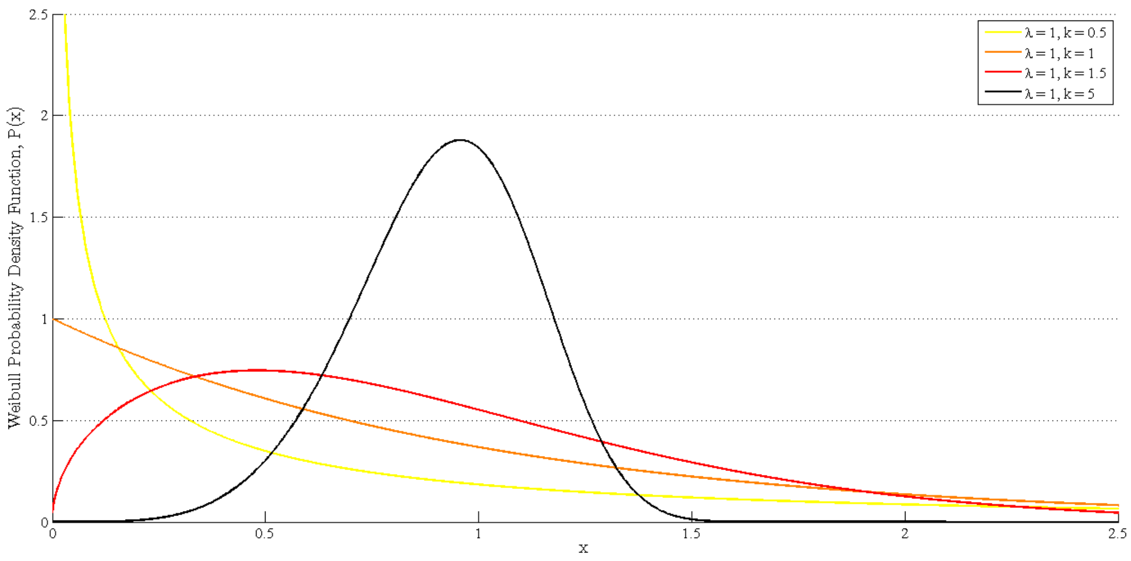


Figure C.2: Weibull probability density function

C.6 "Guerrilla Terrorists" Recruitment Pseudocode

The following pseudocode is performed on a network G, of size n, using the probability distribution X_{GT} from Section 3.3.1.1.

```
{Iterate through all "Foot Solider" network vertices}
for $i = 1$ to $i = n$ and $v_i$ = "Foot Solider" do
  {Select number of new recruits to be added to selected vertex $v_i$}
  NumberOfNewRecruits = RandomNumber(Distributed by $X_{\mathrm{GT}}$)
  for $j = 1$ to $j$ = NumberOfNewRecruits do
    {Attach new recruit $v_j$ to selected vertex $v_i$}
    $v_i \leftarrow v_j$
  end for
end for
```

C.7 "Guerrilla Terrorists" Removal Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
  {Check the probability that selected vertex $v_i$ is removed}
  if vertex $v_i$ is removed from $G$ (Probability = 0.05) then
    Remove vertex $v_i$
  end if
end for
```

C.8 "Guerrilla Terrorists" Desertion Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
```

```
  {Check the degree value of vertex $v_i$}
  if $k_i = 0$ then
    {Check the probability that selected vertex $v_i$ deserts}
    if vertex $v_i$ deserts $G$ (Probability = 0.60) then
      Remove vertex $v_i$
    end if
  end if
end for
```

C.9 "Friends and Family" Recruitment Pseudocode

The following pseudocode is performed on a network G, of size n, using the probability distribution X_{FF} from Section 3.4.1.1.

```
{Iterate through all "Active" network vertices}
for $i = 1$ to $i = n$ and $v_i$ = "Active" do
  {Select number of new recruits to be added to selected vertex $v_i$}
  NumberOfNewRecruits = RandomNumber(Distributed by $X_{\mathrm{FF}}$)
  {Add complete graph $K_{\mathrm{NumberOfNewRecruits}}$ (with $\hat{v}_1 \in K_{\mathrm{NumberOfNewRecruits}}$) to $G$}
  $G \leftarrow K_{\mathrm{NumberOfNewRecruits}}$
  {Connect new "Active" vertex $\hat{v}_1 \in K_{\mathrm{NumberOfNewRecruits}}$ to selected vertex $v_i$}
  $v_i \leftarrow \hat{v}_1$
  {Assign each member $\{\hat{v}_2 \ldots \hat{v}_{\mathrm{NumberOfNewRecruits}}\}$ to be "Active" or "Passive"}
  for $j = 2$ to $j$ = NumberOfNewRecruits do
    $\hat{v}_j$ = "Active" with probability 0.5 or $v_j$ = "Passive" with probability 0.5
  end for
end for
```

C.10 "Friends and Family" Removal Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
  {Check the probability that selected vertex $v_i$ is removed}
  if vertex $v_i$ is removed from $G$ (Probability = 0.05 for "Active", Probability = 0.025 for "Passive")
  then
    {Remove "Passive" vertices $w_j$, connected to $v_i$}
    for $j = 1$ to $j = n$ do
      if $w_i \leftarrow v_i$ and vertex $w_j$ = "Passive" then
        Remove vertex $w_i$
      end if
    end for
    Remove vertex $v_i$
  end if
end for
```

C.11 "Friends and Family" Desertion Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
  {Check the degree value of vertex $v_i$}
  if $k_i = 0$ then
```

```
        {Check the probability that selected vertex $v_i$ deserts}
        if vertex $v_i$ deserts $G$ (Probability = 0.60) then
            Remove vertex $v_i$
        end if
    end if
end for
```

C.12 "Multiple References" Recruitment Pseudocode

The following pseudocode is performed on a network G, of size n, using the probability distribution X_{MR} from Section 3.5.1.1.

```
{Select number of new recruits to be added to $G$}
NumberOfNewRecruits = RandomNumber(Distributed by $X_{\mathrm{MR}}$)
{Iterate through each of the $v_{\mathrm{New}}$ new recruits}
for $i = 1$ to $i =$ NumberOfNewRecruits do
    {Assign number of references required by the selected $v_{\mathrm{New}}$}
    NumberOfReferencesNeeded(i) = RandomNumber(Distributed by Z)
    {Select NumberOfReferencesNeeded(i) distinct vertices to connect to the vertex $v_{\mathrm{New}}$}
    for $j = 1$ to $j =$ NumberOfReferencesNeeded(i) do
        Select $w_j$ (Preferential Degree Attachment Distribution), such that we
        obtain a set $W = \{w_k \mid k = 1 \ldots$ NumberOfReferencesNeeded(i), $w_k$ vertices are distinct}
    end for
end for
```

C.13 "Multiple References" Removal Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
    {Check the probability that selected vertex $v_i$ is removed}
    if vertex $v_i$ is removed from $G$ (Probability = 0.05) then
        Remove vertex $v_i$
    end if
end for
```

C.14 "Multiple References" Desertion Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
    {Check the degree value of vertex $v_i$}
    if $k_i = 0$ then
        {Check the probability that selected vertex $v_i$ deserts}
        if vertex $v_i$ deserts $G$ (Probability = 0.60) then
            Remove vertex $v_i$
        end if
    end if
end for
```

C.15 “Group of Friends” Recruitment Pseudocode

The following pseudocode is performed on a network G, of size n, using the probability distribution X_{GF} from Section 3.6.1.1.

```
{Select number of new recruits to be added to $G$}
NumberOfNewRecruits = RandomNumber(Distributed by $X_{\text{GF}}$)
{Iterate through each $v_i$ new terrorist cell recruit}
for $i = 1$ to $i =$ NumberOfNewRecruits do
  {Iterate through each $v_j$ existing terrorist cell member}
  for $j = 1$ to $j = n$ do
    {Check the probability that $v_i$ is connected to the existing cell member $v_j$}
    if New vertex $v_i$ is connected to existing vertex $v_j$ (Probability = 0.90) then
      $v_j \leftarrow v_i$
    end if
  end for
end for
```

C.16 “Group of Friends” Removal Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
  {Check the probability that selected vertex $v_i$ is removed}
  if vertex $v_i$ is removed from $G$ (Probability = 0.05) then
    Remove vertex $v_i$
  end if
end for
```

C.17 “Group of Friends” Desertion Pseudocode

The following pseudocode is performed on a network G, of size n.

```
{Iterate through all network vertices}
for $i = 1$ to $i = n$ do
  {Check the degree value of vertex $v_i$}
  if $k_i = 0$ then
    {Check the probability that selected vertex $v_i$ deserts}
    if vertex $v_i$ deserts $G$ (Probability = 0.60) then
      Remove vertex $v_i$
    end if
  end if
end for
```

Bibliography

[1] Aaron Clauset and Maxwell Young, *Scale Invariance in Global Terrorism*, Physics and Society, Cornell University Library, `http://arxiv.org/abs/physics?0502014` (cited 15 March 2001), **2005**.

[2] Alexander Gutfraind, *Mathematical Terrorism*, Doctor of Philosophy Dissertation, Cornell University, New York **2010**.

[3] Alexander Gutfraind, *Optimizing Topological Cascade Resilience Based on the Structure of Terrorist Networks* , PLoS ONE, Vol. 5, No. 11, Public Library of Science, **2010**.

[4] Alexander Gutfraind, *Terrorism as a Mathematical Problem*, SIAM News, Vol. 42, No. 8, Society for Industrial and Applied Mathematics, **2009**.

[5] Amanda L. Traud, Christina Frost, Peter J. Mucha and Mason A. Porter, *Visualization of Communities in Networks*, Netwiki, `http://netwiki.amath.unc.edu/VisComms/VisComms` (cited 15 March 2001).

[6] Andrew Moore, *Iterative Improvement Search: Hill Climbing, Simulated Annealing, WALKSAT and Genetic Algorithms*, Carnegie Mellon University, `http://www.autonlab.org/tutorials/hillclimb02.pdf` (cited 15 March 2001).

[7] BBC News Correspondent , *CIA Admits Waterboarding Inmates*, BBC News, `http://news.bbc.co.uk/1/hi/world/americas/7229169.stm` (cited 15 March 2001), **2008**.

[8] BBC News Correspondent, *London Blasts: What Happened*, BBC News, `http://news.bbc.co.uk/1/shared/spl/hi/uk/05/london_blasts/what_happened/html/default.stm` (cited 15 March 2001).

[9] BBC News Correspondent, *Madrid Bombings: The Investigation*, BBC News, `http://news.bbc.co.uk/1/shared/spl/hi/europe/05/madrid_bombings/html/2.stm` (cited 15 March 2001), **2004**.

[10] BBC News Correspondent, *Scores Die in Madrid Bomb Carnage*, BBC News, `http://news.bbc.co.uk/1/hi/3500452.stm` (cited 15 March 2001), **2004**.

[11] BBC News Correspondent, *Six accused of London bomb plot*, BBC News, `http://news.bbc.co.uk/1/hi/6261899.stm` (cited 15 March 2001), **2007**.

[12] Béla Bollobás, *Modern Graph Theory*, Graduate Texts in Mathematics, Vol. 184, Springer Science+Business Media, New York, **1998**.

[13] Boualam Ghimrassa, *Al-Qaeda Members Surrender in Algeria*, Asharq Alawsat (English Edition), `http://www.aawsat.com/english/news.asp?section=1&id=17907` (cited 15 March 2001), **2009**.

[14] Erika A. Schaub and Christian J. Darken, *Utilizing Biological Models to Determine the Recruitment of the Irish Republican Army*, International Journal of Human and Social Sciences Vol. 2, No. 7 World Academy of Science, Engineering and Technology, `http://www.waset.org/journals/ijhss/v2/v2-7-66.pdf` (cited 15 March 2001), **2007**.

[15] F.O. Miksche, *Special Forces: The Technique of Underground Movements*, Faber and Faber, London, **1950**.

[16] Farzad Lameh, *Taliban militants surrender in northern Afghanistan*, Al-Shorfa.com, `http://www.al-shorfa.com/cocoon/meii/xhtml/en_GB/features/meii/features/main/2011/02/02/feature-03` (cited 15 March 2001), **2011**.

[17] Fiona Govan, *Profiles: Madrid Train Bombers*, The Telegraph, `http://www.telegraph.co.uk/news/worldnews/1567965/Profiles-Madrid-train-bombers.html` (cited 15 March 2001), **2007**.

[18] Firdaus Udwadia, George Leitmann and Luca Lambertini, *A Dynamical Model of Terrorism*, Discrete Dynamics in Nature and Society, Vol. 2006, Hindawi Publishing Corporation, New York, **2006**.

[19] Friedrich August, Philippe Blanchard, Sascha Delitzscher, Gerald Hiller and Tyll Krueger, *Passive Supporters of Terrorism and Phase Transitions*, Physics and Society, Cornell University Library, `http://arxiv.org/PS_cache/arxiv/pdf/1010/1010.1953v2.pdf` (cited 15 March 2001), **2010**.

[20] Geoffrey Grimmett and Dominic Welsh, *Probability: An Introduction*, Oxford Science Publications, Oxford, **1986**.

[21] George A. Crawford, *Manhunting: Counter-Network Organization for Irregular Warfare*, JSOU Report, Vol. 7, The Joint Special Operations University Press, Florida, **2009**.

[22] J.D. Murray, *Mathematical Biology: I. An Introduction*, Interdisciplinary Applied Mathematics, Springer Science+Business Media, New York, **2005**.

[23] James P. Keener, *The Perron—Forbenius Theorem and the Ranking of Football Teams*, SIAM Review, Vol. 35, No. 1, Society for Industrial and Applied Mathematics, `http://www.jstor.org/stable/2132526` (cited 15 March 2001), **1993**.

[24] Jeffrey Travers and Stanley Milgram, *An Experimental Study of the Small World Problem*, Sociometry, Vol. 32, No. 4, American Sociological Association, `http://www.jstor.org/stable/2786545` (cited 15 March 2001), **1969**.

[25] John C. Doyle, David L. Alderson, Lun Li, Steven Low, Matthew Roughan, Stanislav Shalunov, Reiko Tanaka, Walter Willinger, *The "robust yet fragile" Nature of the Internet*, National Academy of Sciences of the United States of America, Vol. 102, No. 41, **2005**.

[26] John R. Dodson, *Man-hunting, Nexus Topography, Dark Networks and Small Worlds*, IO Sphere, Vol. Winter, Air University, **2006**.

[27] Jonathan David Farley, *Breaking Al-Qaeda Cells: A Mathematical Analysis of Counterterrorism Operations (A Guide for Risk Assessment and Decision Making)*, Studies in Conflict and Terrorism, Vol. 26, No. 6, Taylor & Francis Group, **2003**.

[28] Jonathan David Farley, *Towards a Mathematical Theory of Counterterrorism*, The Proteus Monograph Series, Vol. 1, No. 2, **2007**.

[29] José A. Rodríguez, *The March 11th Terrorist Network: In its Weakness lies its Strenght [sic]*, Doctor of Philosophy Dissertation, Universitat de Barcelona, WP EPP-LEA: 03, **2005**.

[30] Kathleen M. Carley, *Estimating Vulnerabilities in Large Covert Networks*, Office of Naval Research and Carnegie Mellon University, **2004**.

[31] Kim Sengupta, *The Police's Nightmare: Home-Grown Terrorists*, The Independent, `http://www.independent.co.uk/news/uk/crime/the-polices-nightmare-homegrown-terrorists-498611.html`, **2005**.

[32] M. Nekovee, Y. Moreno, G. Bianconi and M. Marsili, *Theory of Rumour Spreading in Complex Social Networks*, Physica A: Statistical Mechanics and its Applications, Vol. 374, No. 1, Elsevier, **2006**.

[33] Mao Tse-tung (translated by Samuel B Griffith), *On Guerrilla Warfare*, University of Illinois Press, Illinois, **1961**.

[34] Mark E. J. Newman, *Networks: An Introduction*, Oxford University Press, Oxford, **2010**.

[35] Mauricio Florez-Morris, *Joining Guerrilla Groups in Colombia: Individual Motivations and Processes for Entering a Violent Organization*, Studies in Conflict & Terrorism, Routledge: Taylor & Francis Group, **2007**.

[36] Michael Genkin and Alexander Gutfraind, *How Do Terrorist Cells Self-Assemble? Insights from an Agent-Based Model*, Working Paper, http://ssrn.com/abstract=1031521 (cited 15 March 2001), **2008**.

[37] Mike Rupert, *9/11... The Worst Terrorist Attack Ever on U.S. Soil... Nearly 3,000 Dead in New York, Washington and Pennsylvania... Countless American Lives Change*, The Washington Examiner, http://washingtonexaminer.com/local/911-worst-terrorist-attack-ever-us-soilnearly-3000-dead-new-york-washington-and-pennsylvania-c (cited 15 March 2001), **2006**.

[38] MSNBC News Correspondent *Madrid Bombing Probe Finds No Al-Qaida [sic] Link*, msnbc, http://www.msnbc.msn.com/id/11753547/ns/world_news-terrorism/ (cited 15 March 2001), **2006**.

[39] R. M. Christley, G. L. Pinchbeck, R. G. Bowers, D. Clancy, N. P. French, R. Bennett and J. Turner, *Infection in Social Networks: Using Network Analysis to Identify High-Risk Individuals*, American Journal of Epidemiology, Vol. 162, No. 10, Oxford Journals, Oxford, **2005**.

[40] Rex A. Hudson *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and Why?*, Federal Research Devision, Library of Congress, http://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf **1999**.

[41] Russell Jenkins, Dominic Kennedy, David Lister and Carol Midgley, *The London Bombers*, The Times Online, http://www.timesonline.co.uk/tol/news/uk/article543829.ece (cited 15 March 2001), **2005**.

[42] S. N. Dorogovtsev and J. F. F. Mendes, *Evolution of Networks*, Advances in Physics, Vol. 51, No. 4, **2002**.

[43] Scott Gerwehr and Sara Daly, *Al-Qaida [sic]: Terrorist Selection and Recruitment*, RAND Corporation, Vol. Reprint, Chapter 5, McGraw-Hill Companies, **2003**.

[44] Scott Shane, David Johnston and James Risen, *Secret U.S. Endorsement of Severe Interrogations*, The New York Times, http://www.nytimes.com/2007/10/04/washington/04interrogate.html (cited 15 March 2001), **2007**.

[45] Stanley Milgram, *The Small World Problem*, Psychology Today, Vol. 1, **1967**.

[46] Stephen P. Boyd, *Lecture 17: Perron-Frobenius Theory*, Winter Term, Stanford University, California, http://www.stanford.edu/class/ee363/lectures/pf.pdf (cited 15 March 2001), **2008–09**.

[47] Thalif Deen, *U.N. Member States Struggle to Define Terrorism*, Inter Press Service New Agency, http://ipsnews.net/news.asp?idnews=29633 (cited 15 March 2001), **2005**.

[48] Tim Gaynor, *Madrid Bomb Suspects are Linked to Attacks on Twin Towers*, The Independent, http://www.independent.co.uk/news/world/europe/madrid-bomb-suspects-are-linked-to-attacks-on-twin-towers-566359.html (cited 15 March 2001), **2004**.

[49] Tim Golden, *Moroccan Suspect Has Ties To 9/11 Figure, Files Show*, The New York Times, http://www.nytimes.com/2004/03/15/world/bombings-madrid-investigation-moroccan-suspect-has-ties-9-11-figure-files-show.html (cited 15 March 2001), **2004**.

[50] Tom Gjelten, *U.S. 'Connects The Dots' To Catch Roadside Bombers*, National Public Radio, http://www.npr.org/2010/12/03/131755378/u-s-connects-the-dots-to-catch-roadside-bombers (cited 15 March 2001), **2010**.

[51] Unknown, *The Terrorist's Handbook*, http://www.capricorn.org/~akira/home/terror.html (cited 15 March 2001), **Approx. 1988**.

[52] Valdis Krebs, *Connecting the Dots: Tracking Two Identified Terrorists*, Orgnet.com, http://www.orgnet.com/prevent.html (cited 15 March 2001), **2008**.

[53] Wikipedia Collaboration, *7 July 2005 London Bombings: Profiles* http://en.wikipedia.org/wiki/7_July_2005_London_bombings#Profiles (cited 15 March 2001).

[54] Wikipedia Collaboration, *Abu Dahdah*, http://en.wikipedia.org/wiki/Abu_Dahdah (cited 15 March 2001).

[55] Wikipedia Collaboration, *Blackballing*, http://en.wikipedia.org/wiki/Blackballing (cited 15 March 2001).

[56] Wikipedia Collaboration, *Clandestine Cell System*, http://en.wikipedia.org/wiki/Clandestine_cell_system (cited 15 March 2001).

[57] Wikipedia Collaboration, *Francs-tireurs [sic]: World War II*, http://en.wikipedia.org/wiki/Francs-tireurs#World_War_II (cited 15 March 2001).

[58] Wikipedia Collaboration, *French Forces of the Interior* http://en.wikipedia.org/wiki/French_Forces_of_the_Interior (cited 15 March 2001).

[59] Wikipedia Collaboration, *Hani Hanjour*, http://en.wikipedia.org/wiki/Hani_Hanjour (cited 15 March 2001).

[60] Wikipedia Collaboration, *Marwan al-Shehhi*, http://en.wikipedia.org/wiki/Marwan_Al-Shehhi.

[61] Wikipedia Collaboration, *Mohamed Atta*, http://en.wikipedia.org/wiki/Mohamed_Atta (cited 15 March 2001).

[62] Wikipedia Collaboration, *National Front (French Resistance)*, http://en.wikipedia.org/wiki/National_Front_(French_Resistance) (cited 15 March 2001).

[63] William Powell, *The Anarchists Cookbook*, http://lccn.loc.gov/71127797 (cited 15 March 2001), **1971**.

[64] Wolfram Collaboration, *Exponential Distribution*, Wolfram MathWorld http://mathworld.wolfram.com/ExponentialDistribution.html (cited 15 March 2001).

[65] Wolfram Collaboration, *Weibull Distribution*, http://mathworld.wolfram.com/WeibullDistribution.html (cited 15 March 2001).