3-26-2015

A Dynamic Game on Network Topology for Counterinsurgency Applications

Jared K. Nystrom

A Dynamic Game on Network Topology for Counterinsurgency Applications

THESIS

MARCH 2015

Jared K. Nystrom, Major, USA

AFIT-ENS-MS-15-M-144

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENS-MS-15-M-144

A DYNAMIC GAME ON NETWORK TOPOLOGY FOR COUNTERINSURGENCY APPLICATIONS

THESIS

Presented to the Faculty

Department of Operational Sciences

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Operations Research

Jared K. Nystrom, BS, BA, MA

Major, USA

MARCH 2015

AFIT-ENS-MS-15-M-144

A DYNAMIC GAME ON NETWORK TOPOLOGY FOR COUNTERINSURGENCY APPLICATIONS

THESIS

Jared K. Nystrom, BS, BA, MA
Major, USA

Committee Membership:

Lt Col Matthew J. Robbins, PhD
Chair

Richard F. Deckro, DBA
Member

James Morris, PhD
Member

Abstract

Successful military operations are increasingly reliant upon an advanced understanding of relevant networks and their topologies. The methodologies of network science are uniquely suited to inform senior military commanders; however, there is a lack of research in the application of these methods in a realistic military scenario. This study creates a dynamic game on network topology to provide insight into the effectiveness of offensive targeting strategies determined by various centrality measures given limited states of information and varying network topologies. Improved modeling of complex social behaviors is accomplished through incorporation of a distance-based utility function. Moreover, insights into effective defensive strategies are gained through incorporation of a hybrid model of network regeneration. Model functions and parameters are thoroughly presented, followed by a detailed sensitivity analysis of factors. Two designed experiments fully investigate the significance of factor main effects and two-factor interactions. Results show select targeting criteria utilizing uncorrelated network measures are found to outperform others given varying network topologies and defensive regeneration methods. Furthermore, the attacker state of information is only significant given certain defending network topologies. The costs of direct relationships significantly impact optimal methods of regeneration, whereas restructuring methods are insignificant. Model applications are presented and discussed.

I would like to thank my family for their limitless support. I owe my wife immeasurably as none of my accomplishments would have been possible without her patience, compassion, and encouragement. Words can not express my love and appreciation for my two lovely children who, without fail, remind me to smile every day.

I would like to dedicate this work to my father and late grandfather, for giving me a lifetime love for the pursuit of scholarship.

Acknowledgements

I would like to express my deep gratitude to Dr. Robbins for his mentorship and counsel. Without his supervision and guidance this thesis would not have been possible. In addition, I would like to thank my committee members, Dr. Deckro and Dr. Morris. Their expertise and professional dedication greatly assisted in the development of this study.

Jared K. Nystrom

Table of Contents

Page

List of Figures

List of Tables

A DYNAMIC GAME ON NETWORK TOPOLOGY
FOR COUNTERINSURGENCY APPLICATIONS

I. Introduction

The combinatorial effect of rising populations and rapidly expanding technologies points to globalization as a significant driving force for continued modernization. Despite the fantastic promises of such capabilities, pragmatists point out the obvious shortfalls. Failed states and non-state actors have exploited these advances through acts of terror facilitated by relatively small and efficient groups of individuals. These groups have proven to be both effective and resilient, mostly due to their unique social structure that enables military actions facilitated by fragmented leadership and powerful international financing. The United States Army doctrine concerning counterinsurgency suggests that the same fantastic process bringing the people of the world closer is also enhancing the operational capabilities of insurgents and terrorists (U.S. Army Field Manual 3-24 Insurgencies and Countering Insurgencies). Technology enables proliferation and unity of disparate radical ideologies, as well as offers sharing of resources despite distance or political boundaries. The same technology that promises a utopian future is being exploited to provide insurgent or terrorist groups greater strategic effects.

President Bush first defined the national strategy for the United States in combatting these forces in response to the attacks of September 2001 (Bush, 2002). President Obama (2011) affirmed these policies following the death of Usama bin Laden, redefining national priorities for future security operations. A key area of focus for the President is developing counterterrorism tools. These are to be employed in both for-

eign theaters in support of counterinsurgency operations, as well as locally in defense of the American homeland. This is echoed throughout the Department of Defense's Joint Publication 3-26 Counterterrorism and the U.S. Army Field Manual 3-24 Insurgencies and Countering Insurgencies. Both levels of military command doctrine dictate that a cornerstone effort against terrorist organizations is the development of actionable intelligence. This is especially difficult considering the complexities inherit in large social networks, as well as the massive amount of data available from the technologies that now unite them. Understanding and exploiting the social networks driving these groups enables an attacker to more precisely strike in order to disrupt, disable, and ultimately dismantle these groups.

The Committee on Network Science for Future Army Applications (2005) defines network science as "the organized knowledge of networks based on their study using the scientific method". Despite being a relatively new discipline, network science is uniquely positioned to combat both traditional enemies as well as modern evolving threats. Recent research shows two promising trends for the field; that engineered networks are effective in modeling organic social and biological networks, and advances in computing technology now enable researchers to exploit massive amounts of data with relative ease (Committee on Network Science for Future Army Applications, 2005). Researchers can now model a terrorist network paradigm under varying constraints to inform senior military decision makers on the effectiveness of particular policies and operational strategies.

1.1 Motivation

> For an insurgency, a network is not just a description of who is in the insurgent organization; it is a picture of the population, how it is put together and how members interact with one another (U.S. Army Field Manual 3-24 Insurgencies and Countering Insurgencies).

Insurgent or terrorist organizations are subject to the same social phenomena common to all other social networks. These universal tenants of human interaction offer military analysts the chance to observe important insights into how an enemy network is structured and operates. These groups normally seek to operate covertly to blend with the local population and confound the effects of counterinsurgency operations. Military commanders employ their resources through a targeting cycle to effectively select and prioritize targets and match them to appropriate responses considering operational requirements and capabilities (Joint Publication 3-0 Joint Operations). A military commander thus relies exclusively on their ability to correctly identify the members of these covert networks for targeting. Intelligence analysts provide commanders this insight of available information through collection, processing, integration, evaluation, analysis, and interpretation (Joint Publication 2-0 Joint Intelligence). A critical task for any intelligence analyst is to define the enemy threat for their commander, something that proves exceptionally difficult against a cunning and covert insurgent group.

The Committee on Network Science for Future Army Applications (2005) explains the incredible potential of network science for U.S. Army and Department of Defense (DoD) applications. Network-centric Operations (NCO) is now a burgeoning field within the DoD and is being integrated at almost every level. Studying networks yields dividends in more reliable communication systems, streamline command and headquarters processes, and provides valuable insight into enemy operations. Committee on Network Science for Future Army Applications (2005) states that although network science is still a discipline within relative infancy, the DoD is uniquely positioned to develop this field for great effect within defense applications. Developing network science models to inform military commanders not only aids in defining the operational environment, but also builds these capabilities into the targeting and

intelligence processes.

1.2 Focus of Research

Computer simulation already effectively models attack and defense scenarios to evaluate the effectiveness of competing strategies. This study extends the earlier work of Nagaraja & Anderson (2008) by restricting the attacker's state of information, enriching the action spaces of both players, and performing a rigorous analysis utilizing designed experiments. The desired end state is a model that gives insight to effective tactical targeting strategies given limited states of information and varying network topology characteristics.

Much of the current literature assumes that the attacker possesses a perfect state of information concerning the defending network, a fact that would be nearly impossible to replicate in a real-world case study. Furthermore, what studies do account for limited information states fail to incorporate a dynamic process of expanding information states as part of the attacker's targeting process. This study incorporates a process to expand the attacker state of information, either through consuming resources as part of an attack round or a probabilistic mechanism associated with a network attack. Accounting for an attacker's state of information with respect to the defender's network will better model real-world scenarios of interest to the DoD. Consider, for example, the 2003 coalition invasion of Iraq lead by the United States. The initial state of information was very limited, however, expanded over time due to passive intelligence gathering or information gained through the kill or capture of targeted individuals. The purpose of this research is to provide a set of offensive and defensive strategies that perform best given a current state of information, as well as identify thresholds at which those strategies should change. For example, an attacker may employ a simple strategy whereby vertex order attacks are used when its state of

information is poor and a centrality-based attack when its state of information is of higher quality. Such a strategy could prove highly economical and effective against a sophisticated defense network. Moreover, optimized strategies given a force strength and resourcing is measured by adjusting the economic resources available to each player.

An almost universal assumption in attack and defense scenarios is the use of defending average path length as the measure of success. This draws heavily upon computer science applications where average path length dramatically affects network stability, and has been shown to cause system-wide breakdowns if correctly targeted (Zhao *et al.*, 2004). However, average path length does not adequately describe attributes of social network interactions. It can be easily assumed a cunning defensive network could reattach disconnected edges, especially true in the case of an ideologically motivated defender. A better measure of overall network health and individual motivation could be achieved by forming the network on a modified version of a distance-based utility model. This method captures more intricate phenomena within the network. For example, removing one high-value node may dramatically decrease the marginal utility versus cost in a localized region and force lower-ranking nodes to drop out of the network. Applying a limited state of information on the attacking force against a utility-based defense network would better describe why certain strategies outperform others. Furthermore, the results would be more valid by applying a more accurate metric for both targeting and defense.

Montgomery (2008) states that a factorial experiment is the most effective approach to experimenting with multiple factors. Simpler experimental designs only vary one factor at a time resulting in a range of results but failing to capture any effects due to interaction. A factorial design varies the factors together and provides much greater insight into the underlying forces driving a particular observed result.

This design structure provides the capability of a fractional factorial design. These specialized designs allow powerful analysis of experimental factors while only requiring a subset of the originally required experimental runs. This drastically decreases overall required resources without significant impact to the quality of the results. These methods are employed in this study to ensure effective experimentation across the factor spaces given the computationally demanding requirements from such a complex simulation.

1.3 Summary

This chapter introduced the national strategic priorities for combatting terrorism and how network science can effectively aid military researchers. The remainder of this paper is organized as follows. Chapter II presents network science literature to provide both background context and current works pertaining to dynamic games on network topology. Studies presenting useful measures for modeling social networks are also explored. In Chapter III we set forth the process for a hybridized network growth model that is subsequently partitioned for use within both the offensive and defensive paradigms. Chapter IV gives the results of this attack and defense evolutionary game in regard to differing levels of the attacker's knowledge of the defending network. Chapter V presents conclusions as well as focus points for future studies.

II. Literature Review

This chapter examines current literature concerning the fundamentals of network science, simulations of dynamic network games, and important explanations of measures and phenomena. The intent is to provide a justification to the reader of the efficacy of these studies as well as the chosen factors described in Chapter III. The first section provides a brief overview of the varied history of network science. Section 2 introduces the static network, a classic concept in network science that will be later enriched. Section 3 presents some related studies that demonstrate some similar application of network science, as well as justify certain measures later used in the course of the simulation. A series of dynamic network topology games is given in Section 4, giving insight into related works. Section 5 presents several studies providing technical bases for later work.

2.1 Background

Network science spans several academic disciplines. Researchers in the social, information, and natural sciences apply network scientific methods within their respective fields, creating several unique sub-disciplines adhering to the same basic concepts. Jackson (2010) and Lewis (2011) provide exhaustive histories of network science, both of which are reviewed here to provide background and context.

Social Networks.

The application of network science to the study of social interactions is the oldest application with original applications in sociology and social psychology. Early researchers such as Davis *et al.* (1969), who mapped the social circles of women in the 1930's American South, sought to describe the relationships and group dynam-

ics of their target populations. Early economic and marketing researchers focused upon the diffusion of thoughts and innovations throughout complex social networks. Coleman *et al.* (1966) and Ryan & Gross (1950) investigated the diffusion of medical innovation and hybrid corn technologies, respectively. Milgram (1967) famously measured and defined the small world problem during this period. Researchers distributed packages throughout the American Midwest containing a chain of custody roster and instructions to return the packets to researchers in Massachusetts. The results showed a median value of five intermediaries for each package, however only 25% were successfully returned (Milgram, 1967) (Travers & Milgram, 1969). Guare (1990) would later famously coin the phrase "6 degrees of separation", a reference to Milgram's discovery of the surprisingly short diameters of complex social networks. Contemporary researchers still apply these concepts, however technology facilitates application at a much grander scale. Backstrom *et al.* (2012) sampled 721.1 million Facebook accounts and found the average path length between users to be only 4.74 links.

Labor markets have long been known to exhibit networked characteristics, even so far as to spawn the adage to "network" for a job. Early studies confirm the importance of informal channels and networks in attaining a job. Rees (1966) distinguishes the importance of informal networks, such as direct and indirect referrals, while searching for employment. The more contemporary work by Ioannides & Loury (2004) models this behavior and found considerable evidence to support claims of heterogeneity within the labor market. Research is not limited to legitimate labor markets; there is considerable analysis of criminal networks. Reiss Jr (1988) finds that two-thirds of criminals do not act alone, and Glaeser *et al.* (1995) find significant evidence for a wide range in the degree of social interactions in crimes.

Based upon earlier diffusion studies, analysis of information networks demon-

strates how ideas and information spreads. One example is through the study of academic citation networks. Citations represent a directional relationship; one author cites another's to build a case for their own original idea. De Solla Price (1965) is one of the first to study scientific citations using a relatively simple matrix analysis. Newman (2001) reexamines these networks from the perspective of scientific collaboration in the 1990's, finding that they displayed various small-world phenomena such as small diameter and high clustering. Clustering is the formation of relationships based upon current relationships; scientists are more likely to collaborate together if they are tied through a mutual friend or colleague. Goyal *et al.* (2006) provide an exhaustive analysis of coauthorship within the economics community from the 1970's through 2000. Their analysis shows that the professional network expanded significantly over this period, with significant drops in both the average path length and an increase in average degree of all researchers. Such a result provides one of the most unique and intriguing cases for the effects of modern telecommunications and globalization upon network formation.

Information networks are also defined by the spread of ideas through developing technologies such as the world-wide web. Albert *et al.* (1999) provides one of the first studies into the small-world phenomena as the technology first emerged. The study employs a web crawler to sample a significant portion of the world-wide web and cataloged documents and links (URLs) that pointed from one website to another. They find a complex topology displaying a small diameter. This result suggests that an intelligent agent could effectively navigate significant portions of the web with only a few link selections. Further research demonstrates the clustered nature of the web with few unusually long paths between nodes (Barabási *et al.*, 2000) (Adamic, 1999). Jackson (2010) shows that these networks, although previously thought to be uniquely random or scale-free, are in fact hybrid combinations drawing upon both

methodologies of formation.

2.2 Military Applications

Network science offers many potential applications within military operations. Miller (2013) presents a novel application of network analysis in the Islamic Maghreb, Mali. Using the concept of social balance, Miller (2013) examines the interrationships of subgroups during the 2012-2013 conflict. The results indicate possible tensions between two specific groups, despite no overt indication of such conflict. In the course of completing the study, current events validate these results as one of the groups unexpectedly alters allegiances as the network model predicted.

Network science is a highly technical and specialized skillset, and thus is challenging to integrate into military operations. Geffre *et al.* (2009) bridge this gap by establishing a process to target a terrorist organization based upon network topology. The study presents a quantitative method using three measures for individuals in a terrorist organization; social connectedness, operational involvement, and known attendance to operationally significant events or locations. The measures can be weighted to then establish critical individuals for military targeting in order to most efficiently disrupt the network.

Carley *et al.* (2003) identify a critical shortfall in the application of network analysis in counterterrorism. Classic network analysis fails to account for the dynamic nature of covert networks and tends to only examine trivial-sized networks. Carley *et al.* (2003) state is more important to understand how a network evolves versus a detailed analysis of its structure. Moreover, military commanders and intelligence analysts conduct biased analysis of terrorist network structures. Terrorist networks have a structure far different than the hierarchical military networks these individuals may understand more intuitively.

Carley *et al.* (2003) present a dynamic network analysis process that incorporates multiple measures within a single network. The toolset then examines the effectiveness of the network over time given the removal of a specified key node. The process captures the destabilizing effects over time as the network adapts to its now constrained topology. Carley (2004) extends this process to estimate vulnerabilities of covert networks. The study examines network topologies for both al-Qa'ida and Hamas using dynamic network topology. Both organizations are comprised of intricate and unique topologies, but differ significantly from standard military hierarchical structures. The results from analysis show the destabilization and effects caused by the removal of certain key individuals.

2.3 The Static Network

The seminal work of Erdös & Rényi (1959) define the parameters for a set of randomly formed graphs. Erdös-Rényi graphs establish a set of nodes with a designated probability of forming links with neighboring nodes. Although these prove immensely helpful to generate measures and study baseline cases, they fail to adequately capture the complex nature of real-world networks. Albert *et al.* (1999) best encapsulate this while studying the complexity of the world-wide web. By mapping the URL links from the Notre Dame website, they show the observed network displayed far more higher-order vertex nodes then expected by pure random formation. They effectively model the observed set using a scale-free model based upon preferential attachment. In such models newer nodes are more likely to form links with older and better connected nodes (Jackson, 2010). Their resulting scale-free model produce networks with small average path lengths and a high degree of clustering, providing a far better fit to the observed data.

Barabási & Albert (1999) produce one of the innovative cases demonstrating the attributes of a static network. Erdös-Rényi graphs fail to capture much of the complexity due to clustering seen throughout the natural world. This study builds scale-free networks that more closely resemble those found throughout the real world using the concept of preferential attachment. The distribution of the scale-free networks allows for new vertices to constantly be formed and in a non-random fashion. Furthermore, the formation of vertices is preferential towards attaching to nodes that are already well-connected. Therefore as certain nodes fail or are destroyed, the network shows preferential edge formation with highly connected nodes. This closely mimics the authors' observations of naturally occurring scale-free networks such as the world-wide web or the structure of popular culture networks. As certain key nodes are removed, edge reconnection is deliberate and directed primarily towards the largest and most well-connected ones. Perhaps most interestingly, these ideas would later help form the basis for dynamic network topology.

2.4 Parallel Research

Cohen *et al.* (2000) continue the application of modeling the world-wide web using a scale-free design, this time to analyze the network's robust nature against random breakdown. Their results show that this particular network structure proves highly resilient towards simple error and mechanical breakdown. The dense nature and high clustering results in data traffic simply being routed around the affected node. The overall effect of the network slows, but almost 99% of all nodes could be destroyed while still maintaining connectivity. Their results show that large scale-free networks can dilute to amazingly low levels, but will rarely disintegrate due to random breakdowns.

The vulnerability of scale-free networks to attacks is further explored by Zhao

et al. (2004). They study the effects of pointed attacks against a scale-free network, concentrating upon the vulnerability of these networks toward a cascading failure in these instances. Networks such as the world-wide web function with separate nodes operating at a certain capacity with a load somewhere below the maximum capacity. Random failures or errors would be distributed throughout the large network as surrounding nodes bore the brunt of the extra load, however would still not fail as the overall capacity would not be disrupted. A series of pointed attacks against key nodes could effectively disrupt the load and capacity of the network in order to cause a cascading series of failures throughout the network. The higher load would systematically move throughout the nodes and quickly overpower their capacities. Zhao *et al.* (2004) model a scale-free network under a specified load and then conduct a series of attacks to try and instigate a cascading failure by surpassing a critical value of load. The results show that removing very well connected nodes within a network indeed force a cascading failure, especially under networks of lower tolerance. Less-connected, periphery nodes cause little impact on the overall system, even when tolerance is exceedingly high. The networks studied showed a phased phenomenon, where depending upon the network tolerance it either remains integrated or completely disintegrates due to the attacking force.

Holme *et al.* (2002) study the resiliency of various complex networks, both real-world and simulated, to attacks directed upon edges. This study attempted to test not only the effectiveness of certain types of attacks and defense, but also measured the validity of certain models against real-world network data. The real-world networks include one formed of authors in an e-print archive and resulting works cited. The other real-world network included one formed by 24-hours of traffic on a large computer network server. Theoretical networks include a model of random networks, a scale-free network, and a clustered scale-free network. The clustered scale-free net-

work included an additional formation step that included the probability of a triad formation following a preferential edge formation. The result is a scale-free network with small cliques tied to each high-vertex order node, resulting in a theoretically more resilient network. The study incorporated numerous attack strategies to include removals by descending order of the degree and betweeness centrality based upon earlier work by Freeman (1977). Both strategies are either based on the initial network conditions, or updated dynamically at the end of each iteration. They found that none of the modeled networks behaved in a fashion similar to the real-world examples. Furthermore, the attack strategies that updated targeting information dynamically at every iteration performed far better then those conditioned simply on initial network conditions. This is unsurprising as edge formation following repeated iterations of attack would drastically alter the shape and resiliency of any network. The randomly generated networks fared far better against an attack compared against the scale-free networks in both the modeled and real-world examples. This demonstrates that although scale-free networks are very resilient against random failures, their unique structure leaves them extremely vulnerable to an aggressive attacker.

Lin *et al.* (2012a) present a network survivability study incorporating non-deterministic properties to model limited network information for both sides. This is the first study to incorporate real-world constraints and considerations into the study of network topology. They incorporate the probabilistic nature of network information for both sides, as well as develop a more realistic method to game the results of network contests. Previous research assumed the side that expended the most resources would control a node. This is not entirely applicable to the real-world where a cunning adversary can easily overcome a highly resourced one through a higher degree of intensity in conflict. Their measures of network effectiveness focused on quality of service measures, allowing analysis from both a system and service perspective. This

enables a more detailed analysis of the effects of attacks on a defending network's overall capabilities and not just the network's ability to maintain basic connectivity.

The approach employed by Lin *et al.* (2012a) model real-world scenarios, as the defending network would be primarily reactive in nature and is constrained in maintaining a specified quality of service to all its nodes. However, defenders can adopt several effective strategies to include defense in depth and resource concentration. Their approach captures these nuances in a balanced objective function for the defender: maintaining network quality of service while shifting defense resources in response to on-going attacks. The overarching defense constraint concerns budgetary restrictions. The attacker carries a limited budget as well, but can balance capability and aggressiveness in an attempt to overcome the dynamic defender. The simulation is then conducted while adjusting several parameters for sensitivity. The results include verification of the logical assumption that a conflict with a higher intensity prefers the attacker. More interesting results are seen when the aggressiveness of the attacker is jointly considered with the intensity of the conflict. Lower intensity conflicts force more aggressive attackers to expend additional resources to compromise a node. Likewise, a higher intensity conflict requires a more passive attacker to expend greater amounts of resources. The results show an aggressive attacker will prefer to develop high-intensity conflicts to reduce overall expended resources. Moreover, a high-intensity conflict results in a highly aggressive adversary compromising the network within an affordable range of resources. The results further show that defense in depth is more effective against a less aggressive attacker. This is because the less aggressive attackers are less likely to expend large amounts of resources. Likewise, a defense in depth strategy is relatively weak against a highly aggressive foe expending large amounts of resources. In agreement with these findings is that a resource concentration strategy for defense is best against a more aggressive attacker expending

large amounts of resources. This result is shown in a later study where the authors operationalize the concepts in an analysis of specific threats against a local computer network (Lin *et al.*, 2012b). The concepts again show a defense in depth is best against a less aggressive attacker, while a strategy of maximizing defense resources is best against extremely aggressive attackers.

2.5 Dynamic Network Paradigms

Albert *et al.* (2000) show that the unique structures of scale-free networks make them extremely resilient against errors but very vulnerable to attack. Most interestingly, a determined attacker can remove well-connected nodes to a certain threshold after which the communication of the network is reduced exponentially. Communications networks such as the internet are extremely stable, despite frequent hardware failures and network outages. This is because of the robust formation of nodes throughout the network, most especially the likelihood of large nodes becoming hubs with many nodes. Biological networks such as bacteria growth are also extremely resilient to random error, however modern medicine has proven their structure very easy to exploit. The same tendency of a network to naturally build clusters for resiliency makes them especially susceptible to hostile attack. They found that a scale-free network expands quickly in response to targeted attacks on the most well-connected nodes. The result of this growth is a decreased ability for the nodes to maintain communication throughout the network. They show that the world-wide web is especially susceptible to attack as even moderate attacker scenarios are able to fully disrupt communications. The same structure that made the network so resilient to error makes it completely defenseless to an attack concentrating upon the most well-connected nodes.

Nagaraja & Anderson (2008) model an iterative dynamic game to capture the

interactions between attack and defense strategies of scale-free networks. They try to identify how these network attributes may contribute towards the structure of modern terrorist organizations, most especially towards their unique defensive structures. They start with an analysis of the effectiveness of naive defenses, specifically how they are ineffective against a decapitation attack. As shown through earlier works, an attack focused upon well-connected nodes in a scale-free network holds a high probability of causing a cascading network failure. Edge replenishment can take place after an attack, but the overall effect towards reestablishing the network is minimal. The aggressive attack will always defeat the naive defense. Nagaraja & Anderson (2008) utilize game theory to model a multiple-round attack and defense game to develop more robust defense strategies. Their model consists of three phases for every round: attack, replenishment and adaptation. This allows a more robust and adaptive defense, as seen in the three overall defense strategies used. First is the naive defense of random replacement. New nodes form random edges and the defender does not use the adaptive phase. The second defense is based off the dining stenographers problem developed by Chaum (1988); high-vertex order nodes split into subsections in an attempt to thwart vertex-order attacks. The splitting of key nodes to form rings not only provides additional network resiliency, but also aids in further concealing the network's communications to outside entities. In effect, this structure hides high-vertex order nodes from any attacking force. The third and final defense strategy again splits high-vertex order nodes into smaller subsections, however now forms these sub-nodes into an organization of cliques. The edges of the previously high-vertex order nodes are then distributed evenly throughout the cliques.

Nagaraja & Anderson (2008) conduct a simulation of these three defense strategies against a vertex-order attack strategy. Unsurprisingly, the naive defense performed poorly against the attack. The ring-based defense fared somewhat better but still

failed to adequately protect the network for a significant time. Only the clique defense protects the network for a significant period, but in the end still fails to provide adequate defense. Each of the unique defensive structures is compared against several unique attack strategies; both centrality and vertex-order attacks outperform the others. They found that the centrality algorithm developed by Brandes (2001) was superior to other attack strategies against cliques, however required an extensive knowledge of the defending network's structure. With the understanding that centrality attacks worked best against clique defenses, the researchers then developed a hybrid clique defense designed to protect against centrality attacks. Using a variation of Chaum's ring-based defense (Chaum, 1988) coupled with clique formation, they found significant protection against a focused centrality attack.

Domingo-Ferrer & González-Nicolás (2011) enrich the model from Nagaraja & Anderson (2008) to further consider weighted and directed networks, economic limitations on the attack and defense strategies, as well as limiting the information state of the attacking force. One of their most significant contributions is the requirement of the defender to obfuscate their topology from an attacking force. They perform simulations to evaluate the robustness of both weighted and directed scale-free networks to attack. The simulations failed to show a significant difference between weighted and unweighted networks. Directed networks did show significant resilience compared to undirected networks, a fact attributed to the robust nature of bilateral communications between most nodes. Domingo-Ferrer & González-Nicolás (2011) also limit the state of information of the attacking force by creating a sub-network of limited size and restricting all attacks to this reduced space. The most ill-informed attackers fared far more poorly compared to those with greater or even perfect knowledge of the defending network structure. While this made a very compelling point, it failed to account for the dynamics of information states as would be found in real-world

attack and defense scenarios.

Kim & Anderson (2013) further expand the influential work of Nagaraja & Anderson (2008) by incorporating a sophisticated economic system to limit the action rounds of both the defender and the attacker. They report a set of maximized strategies for given scenarios primarily using network models based upon computer and peer-to-peer networks. The study provides valuable insights into the performance of certain targeting and defense resilience measures.

2.6 Quantifying a Network

Several works develop a comprehensive evaluation of network measurements and attributes (Newman, 2001) (Albert & Barabási, 2002). The complexity inherit in statistical models used to describe social networks is well captured by Albert & Barabási (2002) in an overall summary of commonly used processes. Their seminal work evaluates the topology of both real world and modeled networks; they consider traditional random graph networks, small-world networks, and scale-free networks. Their work serves to show the complexity inherit in each real-world network, and the adequacy of various models to correctly capture those nuances. The study summarizes statistic mechanics available to analyze these complex networks.

Guzman *et al.* (2014) build upon earlier studies by conducting an analysis into the relationships of the various measures used to examine networks. Twenty-four network measures are analyzed for overall success and ease of implementation with interesting results. Their results indicate significant correlation between 14 of 24 considered network measures, with several measures being highly correlated. Four distinct groups of correlated measures are identified, but several measures remained separate from these groups. The implication is that these individual measures effectively capture specific and unique network phenomena. The computational difficulty

of each process is also considered, giving an overall view of some of the trade-offs for each strategy. The results prove highly useful to researchers seeking to apply a network measure when computation time is an important consideration. A computationally demanding measure may have a highly correlated partner with far fewer computational requirements. Guzman *et al.* (2014) conduct their analysis using a random graph generation algorithm created by Morris *et al.* (2013). (Morris *et al.*, 2013) introduce a model for random network generation enabling the construction of networks exhibiting desirable qualities. The Prescribed Node Degree, Connected Graph (PNDCG) algorithm builds networks effective for testing measures in network analysis.

III. Methodology

This chapter presents the simulation of the dynamic game on network topology. Experimental factors, player action spaces, and state of information functions are introduced and defined. A discussion of the simulation provides an overview to the processes being implemented in Chapter IV.

3.1 Defining the Network

This study represents networks using a network science approach to classical graph theory and adopts the notation found in Jackson (2010). The set $N = \{1, \ldots, n\}$ represents the set of nodes in a network of relationships. In a social network, each node corresponds to an individual person. A graph (N, g) consists the node set N and a $n \times n$ matrix g, where g_{ij} represents the relation between nodes i and j. A graph can consist of directed relationships if it is possible that $g_{ij} \neq g_{ji}$, or strictly undirected relationships if $g_{ij} = g_{ji}$ for all nodes i and j. This study only considers undirected graphs as they better model social and economic relationships (Jackson, 2010). The relationships in g can also be weighted to provide greater context and meaning to a relationship, however this study only utilizes unweighted graphs, where g_{ij} can equal either 0 or 1, as Domingo-Ferrer & González-Nicolás (2011) show weighting effects to be insignificant within the framework of this manner of dynamic game. Nodal self-relations are not considered.

Attributes of a network g can be defined to describe social characteristics. A network g is connected if any node i can reach any other node j. Many networks are not connected, however, analysis can be conducted on the components of the overall network. A network component is a connected subset of the overall network. A geodesic, $P(ij)$, is the shortest path between nodes i and j. This notation can be

refined to $P_k(ij)$ to designate all geodesics between nodes i and j upon which node k resides. The number of links in a geodesic is designated as $\ell(ij)$. A node's localized position within a network is defined as its neighborhood. The direct neighbors of a node i in network g can then be defined as $N_i(g) = \{j : g_{ij} = 1\}$. An extended network represents all nodes within k steps of node i, or the "friends of friends" for a particular node, and can be thought of all the union of all local neighborhoods. It is designated as $N_i^k(g) = N_i(g) \cup \left(\bigcup_{j \in N_i(g)} N_j^{k-1}(g)\right)$. Table 1 provides an overview of all pertinent graph notation.

Table 1. Table of Graph Notation

Parameter	Description
N	Set of all nodes in g, $N = \{1, \ldots, n\}$
g	$n \times n$ network matrix where g_{ij} represents a relationship
(N, g)	Graph of network g with node set N
g_{ij}	Edge between nodes i and j
$d_i(g)$	Degree of node i in g, or $\lvert N_i(g) \rvert$
$N_i(g)$	Direct neighborhood of node i in g, or the set $\{j : g_{ij} = 1\}$
$N_i^k(g)$	k-step neighborhood of node i, or $N_i(g) \cup \left(\bigcup_{j \in N_i(g)} N_j^{k-1}(g)\right)$
$P(ij)$	Geodesic connecting i and j
$P_k(ij)$	Geodesic connecting i and j, but also including node k
$\ell(ij)$	Number of links in geodesic $P(ij)$

Building the Game.

It is self-evident that human social interaction is a dynamic process. Nagaraja & Anderson (2008) effectively captured this artifact of social dynamics through a simulated dynamic game and this study seeks to expand upon that work. Traditional game theory does not adequately capture evolving factors found in social networks such as dynamic covert networks. Player actions update and define the parameters of the game over time, resulting in a constant adaptation of costs and payouts. A dynamic game captures this co-evolution of players' behavior through time phases

and models the characteristics of a dynamic covert network, or one that is constantly evolving to respond to external social influences (Carley *et al.*, 2003). The dynamic games of earlier works are enriched by expanding the two players' state of information and action space. This is done to more effectively model the interactions between an attacking counterinsurgency force and a defending terrorist or insurgent force.

The defending player's objective is to maintain network cohesion while maximizing nodal utility values. This is accomplished by effectively recruiting new nodes with strategic placement within the network as well as restructuring as required to minimize individual costs to maximize benefit. The attacking player's objective is to effect the formation of a network topology such that the defender's total utility is minimized. This is accomplished through removing defending nodes based on certain targeting criteria. An important issue is determining the effectiveness of the different targeting criteria. A significant challenge for the attacking player is building on a restricted state of information through investment in intelligence collection. An effective attack strategy will incorporate precise targeting, fueled by expenditures into intelligence, to expand the state of information.

Figure 1 shows the overall structure of the simulation. The simulation is comprised of three primary phases: initialization, attack, and defense. The initialization phase consists of building the initial defending network and establishing the attacker's state of information. The attack phase consists of an evaluation of the current information state and then determining an action, either attack or intelligence collection. The defense phase consists of an evaluation of utility scores and then determining an action, either restructure or recruit additional members. A termination phase determines if any simulation stopping criteria have been met, otherwise the simulation continues back to the attack phase.

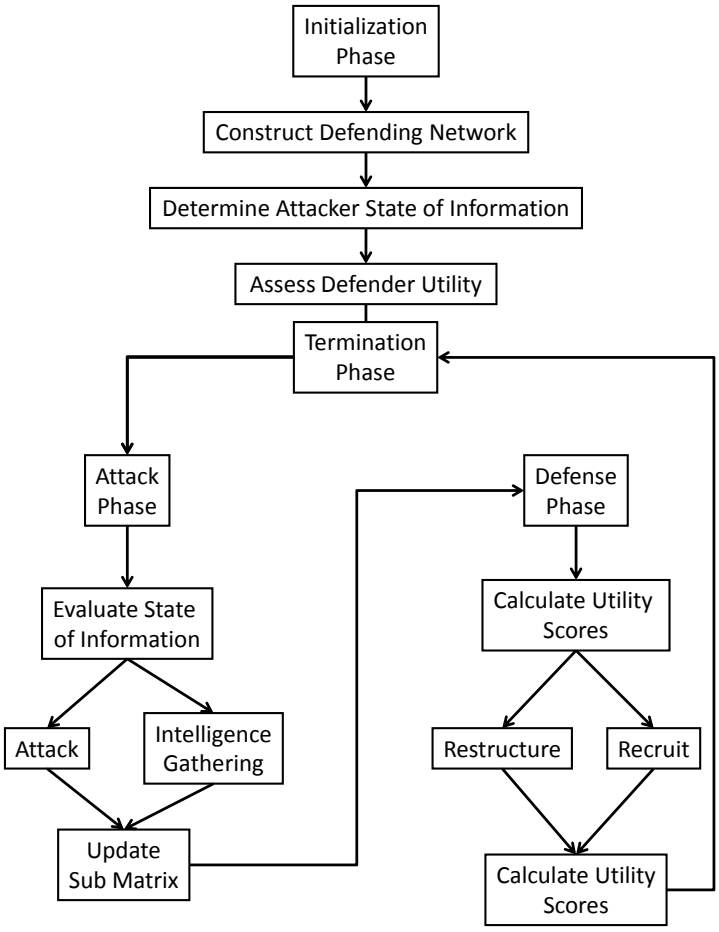

Figure 1. Structure of the Simulation

3.2 Initialization Phase

Initial starting conditions are set by forming the defending network and the attacker's state of information. The initial node set N remains fixed throughout the entire simulation. The PNDCG algorithm is utilitzed to generate an individual network g that best mimics a specific covert network. Graph (N, g) represents the defending player for the game.

The initial starting topology for the defending network is designed to closely represent known covert networks. The PNDCG algorithm offers flexibility in creating engineered networks with desired characteristics (Morris *et al.*, 2013). This flexibility allows modeling of highly cellular networks such as al-Qa'eda, more stratified networks such as Hamas, or highly hierarchical networks such as the early Iraqi insurgency. Each topology drives a unique strategy for both the attacking and defending players.

The attacker's state of information is captured by the set $\bar{N} \subseteq N$, where inclusion of nodes in $\bar{N}$ indicates information known to the attacker. The attacker is also aware of any edges between known nodes. As such, the attacker's state of information can then be represented by the sub-matrix $\bar{g}$, a $|\bar{N}| \times |\bar{N}|$ matrix.

The attacker's initial state of information is determined by stipulating the size of $\bar{N}$. A random permutation of nodes in N is used to initially populate $\bar{N}$, where $|\bar{N}| = \lfloor \phi n \rfloor$ and where ϕ is the proportion of the defending network initially known to the attacker.

The defender's state of information is established by use of a distance-based utility function using the connections model of distance-based utility, discussed in the following sub-section. This function returns a vector of node utilities incorporating both the value of network inclusion and the costs of maintaining direct relationships.

Connections Model of Distance-Based Utility.

Jackson & Wolinsky (1996) present a connections model on network topology that produces a utility measure for both individual nodes as well as the overall network. Individuals derive benefits, or utility, from those with whom they directly communicate. They also gain benefit from indirect relationships, or having "friends of friends" within their social network. The value of an indirect relationship is proportional to the distance between nodes. Finally, maintaining a direct relationship between nodes is costly, so that individuals are required to weigh the benefit against the cost of a direct relationship.

Jackson & Wolinsky (1996) define the model as follows. Let

$$\kappa_{ij} \geq 0, \ \forall (i,j) \in g \tag{1}$$

denote the cost of a direct relationship between nodes i and j. The costs, κ_{ij}, represent the time and economic costs associated with maintaining a direct relationship.

Let $\ell(i,j)$ denote the number of links in the shortest path between nodes i and j where $\ell(i,j) = \infty$ if there is no geodesic connecting nodes i and j. Let $\delta \in [0,1]$ denote the decay parameter which modifies the benefit node i derives from its relationship with any other node. The benefits of "friends of friends" provides diminishing returns as $\ell(i,j)$ increases. The utility of node i in network g is

$$u_i(g) = \sum_{i \neq j} \delta^{\ell(i,j)} - \sum_{i \neq j} \kappa_{ij}. \tag{2}$$

This model includes the decay parameter δ as a measure of the overall benefit of inclusion in the network. The value of δ impacts the observed utility for individual nodes and the overall network, and indirectly represents the organizational social trajectory of the defending network. For example, if a covert network exhibits regional

dominance and possesses tactical momentum, defined as a series of small-scale successes enabling a perception of imminent strategic victory, the δ parameter would be relatively higher as membership increases perceived individual payouts. Likewise, if a covert network sustained considerable damage due to actions taken by counterinsurgent forces, the δ parameter would be relatively lower as the perceived benefit of group membership decreases due to increased risk and possibly decreased social benefit.

The summation of all node utilities is used to represent the overall utility of the network $\nu(g)$, where

$$\nu(g) = \frac{\sum_{i \in N} u_i(g)}{|N|}. \tag{3}$$

Figure 2 shows the utility curve given varying values for the decay parameter (δ) and cost (κ). The δ parameter affects the vertical offset of the curve, while κ determines the slope. Cost (κ) shows a more significant impact on higher degree nodes as utility decreases more dramatically as κ increases. Moreover, κ greatly impacts the marginal utility of adding another direct relationship. This is due to the costs associated with maintaining a direct relationship. The two parameters can be used in conjunction to define payouts for insurgency members, given dynamic values of both the benefit and cost of membership.

3.3 Attack Phase

The attacking player begins by measuring the size of $\bar{x}$, the largest component within the limited state of information sub-matrix $\bar{g}$. The measure $\bar{x}$ is used to model a commander's state of information and determine the player's logical course of action. The attacking player can choose to proactively attack or passively collect intelligence. If the size of the largest component exceeds a predetermined proportion

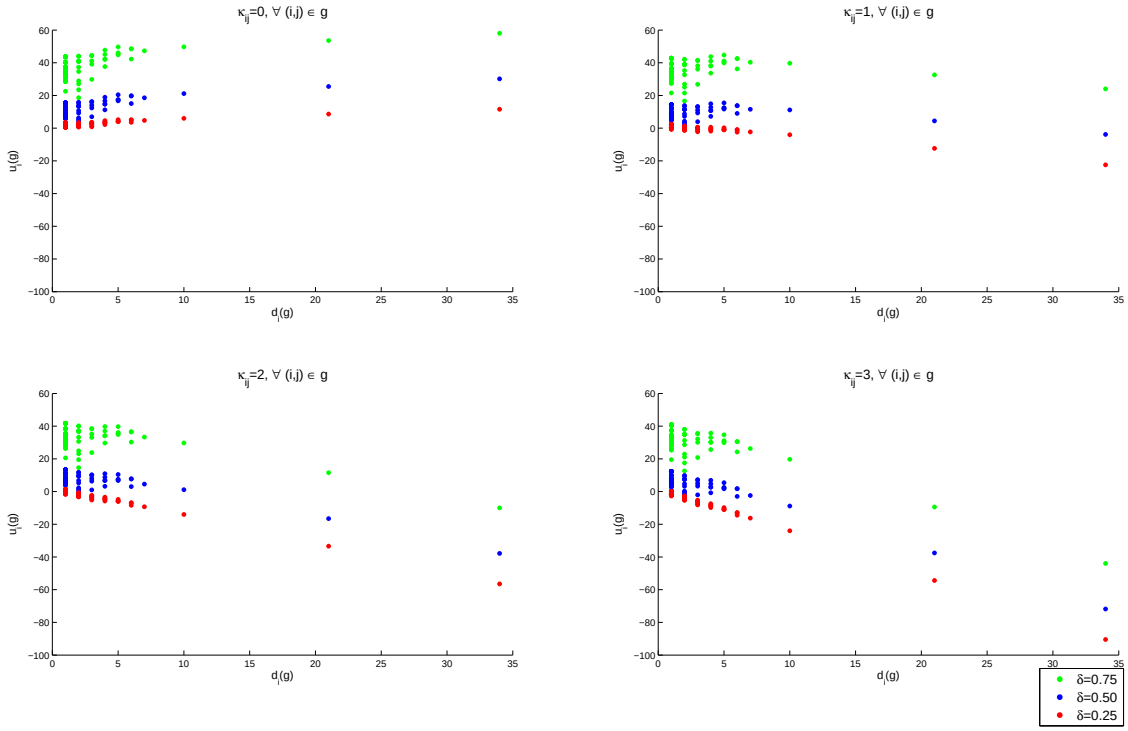

Figure 2. Utility vs Node Degree: Cost($\kappa_{ij} = 0, 1, 2, 3$), Decay($\delta = 0.25, 0.50, 0.75$)

of the network, $\bar{x} \geq n\tau$ where $\tau \in [0, 1]$, then the attacker is satisfied with the current state of information and attacks. The parameter τ is fixed throughout the game and represents the level of tactical patience demonstrated by the attacker, or the amount of time an attacking commander allows to pass prior to committing forces to action. The attacker may begin a campaign with intelligence collection, however once a commitment to action is made the player is not limited to a strictly offensive strategy. The attacker's state of information may allow an attack in one turn; effective targeting may split a component and force the attacker back into an intelligence collection cycle.

Node Removal.

To initiate an attack, the player selects, or targets, a single node within $\bar{N}$ and removes it. The attacker targets nodes based on certain network centrality measures.

Measures of centrality attempt to capture the position of a node, and perhaps its relative importance within the overall graph (Jackson, 2010). The selected centrality measure remains fixed throughout the game.

As introduced in Chapter II, Guzman *et al.* (2014) identify four distinct groups of highly correlated network centrality measures. Uncorrelated measures are categorized into a fifth group. Groups of network measures are found to capture the same network phenomena while requiring vastly differing computational times. This study utilizes the least computationally difficult centrality measure from each of the four groups: clustering coefficient, betweenness centrality, proximal target betweenness, and degree centrality. These selections facilitate evaluation of fourteen network measures in a highly efficient design. Two additional network measures, eigenvector centrality and closeness centrality, are included from the fifth group due to common use in literature (Jackson, 2010).

Clustering Coefficient.

Let $C^L(i)$ denote the cluster coefficient of node i, as first defined by Watts & Strogatz (1998). The clustering coefficient represents the amount of clustering, or triangular relationships, found within a network. Consider node i and two immediate neighbors, $N_i(g) = \{j, k\}$. Given g_{ij} and g_{ik}, the clustering coefficient represents, on average, how often the edge g_{jk} exists. Jackson (2010) defines the clustering coefficient for node i as

$$C_i^L(g) = \frac{\sum_{j \neq i; k \neq j; k \neq i} g_{ij} g_{ik} g_{jk}}{\sum_{j \neq i; k \neq j; k \neq i} g_{ij} g_{ik}}. \tag{4}$$

The measure is thus the quotient of the number of triangles and the total number of paired edges.

Betweenness Centrality.

Let $C_i^B(g)$ denote the betweenness centrality of node i. Betweenness centrality is a centrality measure for a node in terms of "the degree to which a point falls on the shortest path between others and therefore has a potential for control of communication" (Freeman, 1979). This measure captures the relative importance of a node given a particular network. Consider a network with three nodes: i, j, and k. If the ratio $\frac{P_k(ij)}{P(ij)}$ approaches 1, then k lies on all or nearly all geodesics between i and j. Node k is less critical to i and j if the ratio approaches 0. This ratio describes the overall importance of k within the context of the relationship between i and j. Averaging this ratio across all pairs of nodes gives the betweenness centrality, defined by Jackson (2010), as

$$C_i^B(g) = \frac{2}{(n-1)(n-2)} \sum_{k \neq j : i \notin \{k,j\}} \frac{P_k(ij)}{P(ij)} \tag{5}$$

Proximal Target Betweenness.

Let $C_i^P(g)$ denote the proximal target betweenness of node i as first proposed by Brandes (2008). This measure is an extension of betweenness centrality by using proxies that gives weights to the nodes one step away from the source node s to target node t. This proxy node is highly influential on the geodesic $P(ij)$.

$$C_i^P(g) = \sum_{s \in N_i(g), t:(i,t)=1 \in g} \frac{P_i(jk)}{P(jk)} \tag{6}$$

Degree Centrality.

Let $C_i^D(g)$ denote the degree centrality of node i. Degree centrality indicates how well a node is connected in terms of direct connections (Freeman, 1977). This is simply represented as $d_i(g)$ proportional to the number of remaining nodes within

the network $(n-1)$. This measure requires little computational rigor.

$$C_i^D(g) = \frac{d_i(g)}{n-1} \tag{7}$$

Eigenvector Centrality.

Let $C_i^E(g)$ denote the eigenvector centrality of node i, first proposed by Bonacich (1972). This measure is an extension of degree centrality, defining the centrality of a node as being proportional to the sum of the centrality of all its direct neighbors' neighbors, $N_i^2(g)$. $C_j^E(g)$ represents the centrality of each node $j \in g$. The value g_{ij} identifies all direct neighbors of node i. The structure of this problem facilitates computation through solving an eigenvector formulation. The measure in matrix notation

$$C^E(g) = \frac{1}{\lambda} \sum_{j=1}^{n} g C^E(a_j), \tag{8}$$

where λ is the eigenvalue corresponding to $C_i^E(g)$.

Closeness Centrality.

Let $C_i^C(g)$ denote the closeness centrality of node i as defined by Freeman (1979) and Beauchamp (1965). This measure captures centrality through the inverse of the average distance between i and any other node j (Jackson, 2010). The closeness centrality is thus

$$C_i^C(g) = \frac{n-1}{\sum_{i \neq j} \ell(i,j)}. \tag{9}$$

Sensitive Site Exploitation.

An attacker's ability to effectively conduct intelligence operations is critical to effectively target key nodes within an insurgent network (U.S. Army, 2014). Intelligence production takes many forms, however it is restricted to two activities for the purposes of simplicity in simulation. The attacker can obtain intelligence on the defending network immediately following the removal of a node, thereby incentivizing node removal and mimicking real-world operations. Military operations conducted to kill or capture an individual include processes that exploit available resources for possible intelligence. In the simulation, intelligence collection is tied to the degree of the removed node. The amount of intelligence gathered is dictated by a probability, $\beta \in [0, 1]$, evaluated against a uniform random number $r \in [0, 1]$. The direct neighbors, $N_i(g)$ of removed node i^* are evaluated individually with a new random number draw r for each node $j \in N_{i^*}(g)$. If $j \in N_i(g))$ and $\beta < r$, j is added to $\bar{N}$. The submatrix $\bar{g}$ is updated to include node j, and the attacker expands its current state of information on the defending network. This process models sensitive site exploitation (SSE), a procedure by which a military unit gathers intelligence following a detention mission.

Intelligence Gathering.

If the size of the largest component $\bar{x}$ is less than the threshold $n\tau$, the attacker conducts intelligence gathering to enhance its state of information. The intelligence gathering mission is a stochastic process similar to that in the SSE cycle following node removal. The attacking player first generates the set of highest priority targets, $T = \{C^{\theta}_{(1)}(g), \ldots, C^{\theta}_{(10)}(g)\}$ where $|T| = 10$, based upon the sorted targeting scores of centrality measures θ. The arbitrary selection of 10 nodes in the target set models a common practice by military commanders in maintaining a "top ten" list of highest

priority targets. A random permutation of this set, $\bar{T}$, is used to generate the final targeting list. This permutation restricts the attacking player's ability to simply target the top nodes for collection. This models real-world intelligence collection which is highly dependent upon target accessibility and detectability.

The attacking player selects the first ζ nodes from the set $\bar{T}$ for intelligence gathering. Each node is evaluated individually, as in the SSE process. The probability of a successful intelligence mission is controlled by the parameter $\gamma \in [0, 1]$, which remains fixed throughout the game. The parameter γ is evaluated against a uniform random number $r \in [0, 1]$. The set of direct neighbors of a target node i^*, $N_{i^*}(g)$, are evaluated individually with a new random number draw r for each node $j \in N_{i^*}(g)$. If $j \in N_{i^*}(g)$ and $\gamma < r$, j is added to $\bar{N}$. The process continues until the first ζ nodes in $\bar{T}$ are completely evaluated.

3.4 Defense Phase

The defending player begins by recalculating the network utility following the attack phase. The defender decides to recruit new nodes or restructure based upon the current set of utility scores $u_i(g), i \in N$. A predetermined threshold for minimum utility score, ρ, determines the defender's actions.

Network Restructure.

If $\min_{i \in N} u_i(g) < \rho$, the defending player will choose to restructure the network topology in the vicinity of the node with the lowest utility, $i^* = \arg\min_{i \in N} u_i(g)$. If more than one node shares the lowest utility value, the node with the lowest index will be selected. Low utility results from a node being over connected, meaning there are too many costly direct connections that outweigh the benefits of network participation. This models a situation in which an individual becomes overburdened

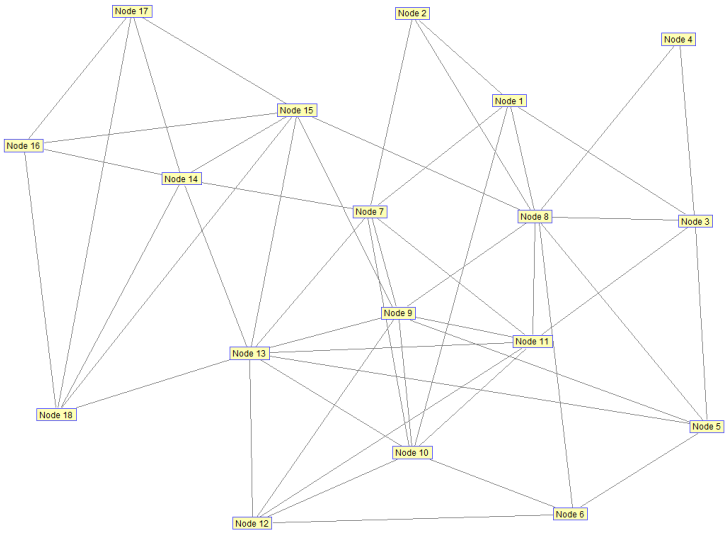

Figure 3. Terrorist Network Responsible for the 1998 U.S. Embassy bombings in Kenya and Tanzania (Geffre, 2007)

with organizational responsibility from excessive connections, as well as excessive risk associated with being a prominent member of a covert network. Restructuring spreads the burden and risk throughout the neighboring nodes and increases the targeted node's utility. This study adopts the restructuring methods defined in Nagaraja & Anderson (2008): ring and clique formation. Restructuring strategy is determined by the categorical variable λ and remains fixed throughout the game.

The following sections introduce and discuss the two methods of network restructure. A visual representation of restructured networks is provided. The terrorist network attributed to the 1998 U.S. Embassy bombings in Kenya and Tanzania (Geffre, 2007) is used to illustrate these methods on a real-world organization. Figure 3 illustrates the initial network structure, which is more formally discussed in Chapter IV.

Ring Formation.

Ring formation redistributes direct connections from the vulnerable node to high utility neighbors, forming a small ring in place of one high vertex order individual.

External links from ring members are shared within the group, however, the overall effect is to increase the benefit of utility against the costly direct connections. The ring formation can be compared to the division of one executive position to a small council of individuals.

Ring restructuring in the simulation is accomplished by first identifying the node $i^* = u_i^{(1)}(g)$ in the ordered set of utility scores $U = \{u_i^{(1)}(g), \ldots, u_j^{(n)}(g)\}$, where $u_i^{(1)}(g) = \arg\min_{i \in N} u_i(g)$. A set R of nodes is assembled where

$$R = \{u_i^{(1)}(g), u_k^{(n-\epsilon+1)}(g), \ldots, u_m^{(n-1)}, u_j^{(n)}(g)\} \tag{10}$$

and $|R| = \epsilon$. Node indices are used in the event of a tie in utility scores. Each node in R is subsequently connected to one another sequentially in g until $u_i^{(1)}(g)$ is connected to $u_j^{(n)}(g)$. Only sequential linking is allowed. The nodes are then formed into a ring structure within the network. The original external links belonging to $u_i^{(1)}(g)$ are redistributed by index in the set R until no more remain.

Figure 4 illustrates a ring restructure on node 13 in the embassy bombing network where $\epsilon = 5$. Table 2 gives the initial and resulting utility values for all nodes involved in the ring restructure. The ring structure redistributes costly direct relationships from the low utility node throughout the ring. The result is a redistribution of utility throughout the group. This structure proves somewhat problematic as communication within the network is now channeled through the ring members.

Table 2. Utility Values of Select Nodes for Ring Restructure

Node	Starting Utility	Ending Utility
13	-0.727	3.233
4	5.174	2.096
2	4.772	1.4
5	3.086	2.939
6	3.783	1.4

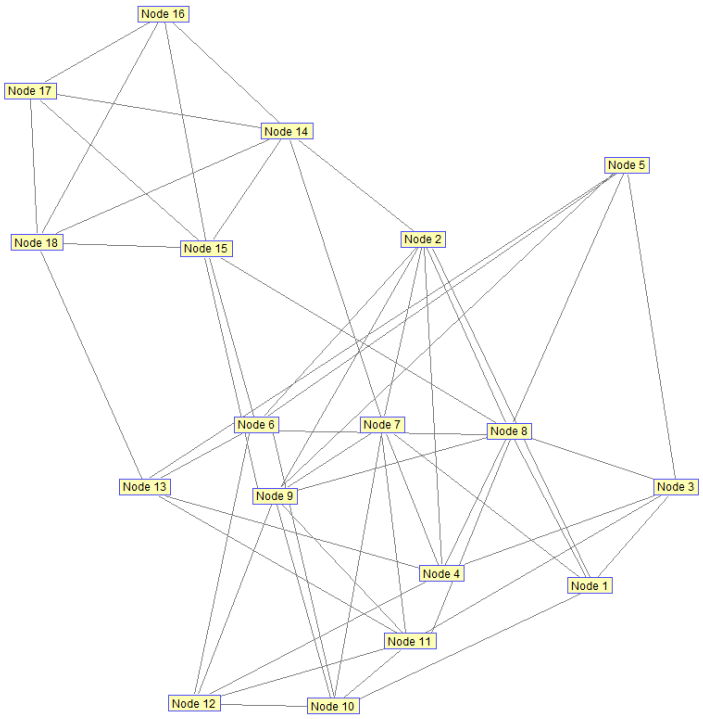

Figure 4. Network following ring restructure on node 13

Clique Formation.

Clique formation breaks a high vertex-order node into a small clique of individual nodes utilizing low vertex order neighbors. It acts much like the ring formation, however, it allows for more inter-connectivity within the group. This restructuring strategy is comparable to a senior commander appointing an executive officer to shoulder the burden of some direct responsibilities.

Clique restructuring in the simulation is accomplished by first identifying the node $i^* = u_i^{(1)}(g)$ in the ordered set of utility scores $U = \{u_i^{(1)}(g), \ldots, u_j^{(n)}(g)\}$, where $u_i^{(1)}(g) = \arg\min_{i \in N} u_i(g)$. A set, C, of nodes is assembled where

$$C = \{u_i^{(1)}(g), u_k^{(n-\epsilon+1)}(g), \ldots, u_m^{(n-1)}, u_j^{(n)}(g)\} \tag{11}$$

and $|C| = \epsilon$. Node indices are used in the event of a tie in utility scores. Each node

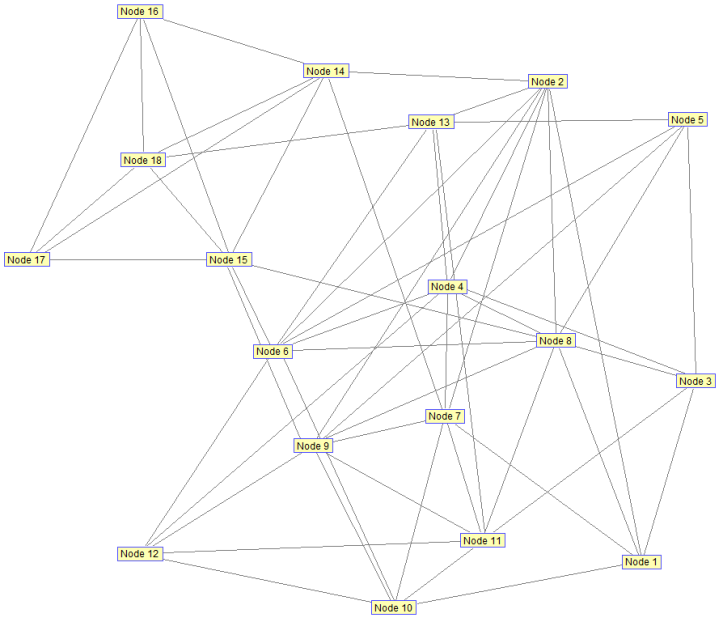

Figure 5. Network following clique restructure on node 13

in C is then connected to every other node in C. The nodes form a dense clique structure within the original network. The original external links belonging to $u_i^{(1)}(g)$ are redistributed by index in the set C until no more remain.

Figure 5 illustrates a ring restructure on node 13 in the embassy bombing network where $\epsilon = 5$. Table 3 gives the initial and resulting utility values for all nodes involved in the ring restructure. The clique structure redistributes the costly direct connections throughout all clique members, while also ensuring any node within the clique is connected. This incurs a higher cost in utility compared to ring restructure due to the addition of more costly direct connections. This method does benefit by creating a more robust network structure.

Restructuring Effects on Network.

Restructuring increases the utility of a target node to the detriment of ϵ other nodes. However there is also an associated cost to the entire network. Table 4 gives the values for $\nu(G)$, average utility, for the initial network, as well as the networks

Table 3. Utility Values of Select Nodes for Clique Restructure

Node	Starting Utility	Ending Utility
13	-0.727	2.39
4	5.174	1.106
2	4.772	0.41
5	3.086	2.939
6	3.783	0.41

following ring and clique restructure. The network experiences an overall drop in $\nu(G)$ due to the redistribution of edges to high utility nodes, as well as the inclusion of two additional costly links. Although this restructuring mechanism fails to include a direct cost, the drop in average network utility incurs an indirect cost. Repetitive network restructuring could prove detrimental to any network.

Table 4. $\nu(g)$ Following Network Restructure

Initial $\nu(g)$	Ring Restructure $\nu(g)$	Clique Restructure $\nu(g)$
2.2137	2.0307	1.827

It should be noted that if $1 \leq \epsilon \leq 3$, both ring and clique restructuring methods result in identical network structures.

Network Recruitment.

If $\min_{i \in N} u_i(g) \geq \rho$, the defending player will instead choose to recruit new nodes to expand the operational capabilities of the overall organization. These new nodes will connect to existing nodes and expand the organization. This condition is indicative of a network where all members are satisfied with group participation and seek to expand their operational capabilities. The simulation models recruitment using a hybrid regeneration model that uses growth through either exponential random or preferential attachment methods.

Hybrid Regeneration Model.

Networks can grow or regenerate through various methods, however, two of the most widely researched are the Erdös-Rényi random exponential method and preferential attachment method (Jackson, 2010). Randomly generated graphs form uniformly and independently within the existing network. The probability of forming a link with an existing node a_i is simply the proportion of that node relative to all other nodes in the network

$$p_i^R = \frac{1}{|N|}. \tag{12}$$

Nodes formed through preferential attachment are assigned edges probabilistically based upon existing nodes' edges proportional to the number of edges within the network. The probability of forming a link with node i is the quotient of the degree of node i and the sum of degrees of all existing nodes

$$p_i^P = \frac{d_i(g)}{\sum_{j \in N} d_j(g)}. \tag{13}$$

Bloch & Jackson (2007) present a hybrid model utilizing both the exponential random method and preferential attachment method concurrently to better model observed data. For every node added to an existing network, j^*, a total of $\lceil \alpha\psi \rceil$ edges are first added randomly to g where $\alpha \in [0, 1]$. These edges form a new neighborhood of direct connections, $N_{j^*}(g)$ giving the newly created node $\lceil \alpha\psi \rceil$ direct relationships. These direct relationships provide node j^* access to an expanded neighborhood, or "friends of friends", defined by the set $N^2_{j^*}(g)$. Once all random edges are created, $\psi - \lceil \alpha\psi \rceil$ edges are added to g through preferential attachment connecting j^* to nodes within $N^2_{j^*}(g)$ probabilistically based upon their degrees, as seen in Equation 13. This method allows a new node to show preference towards higher degree nodes during

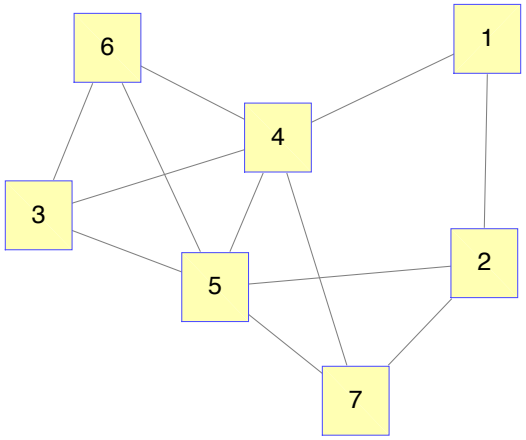

Figure 6. Network on 7 nodes and 12 edges

the formation phase.

To visually represent the hybrid regeneration model, consider the network displayed in Figure 6. The network is a randomly generated network of 7 nodes on 12 edges. The hybrid regeneration method is employed to add one additional node, where $\psi = 3$ and $\alpha = \frac{2}{3}$. These values result in two edges first being added randomly and the third edge being added through preferential attachment.

For the first phase of the hybrid regeneration method, nodes a_3 and a_6 are randomly selected for connection to node a_8. The probability of selection, as determined by Equation 12, is $p_3^R = p_6^R = \frac{1}{7}$ for every node in N. Figure 7 displays the resulting network once $g_{3,8}, g_{6,8} = 1 \in g$.

The second phase of the hybrid regeneration begins with identification of the 2-step neighbors of node 8, or all the new node's "friends of friends". The set $N_8(g) = \{4, 5\}$ is identified and the probability of selection, in accordance with Equation 13, is $p_4^P = p_5^P = \frac{1}{2}$. The method chooses node 4 for connection through preferential attachment, shown in Figure 8, and the process now terminates.

As Bloch & Jackson (2007) conclude, this formulation creates more robust network

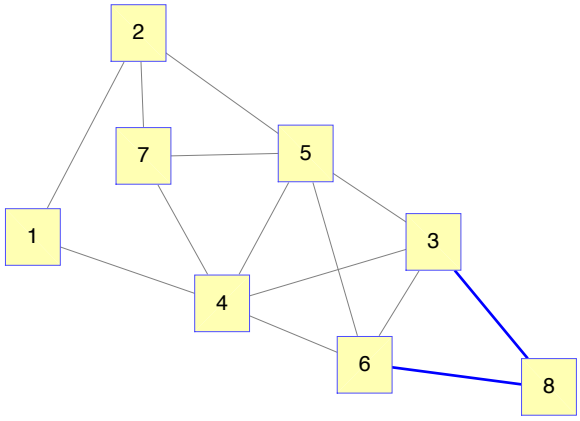

Figure 7. Random network regeneration through node $8 : \psi = 3, \alpha = \frac{2}{3}$

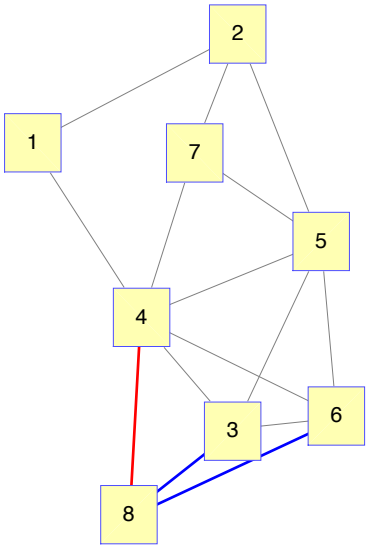

Figure 8. Preferential attachment network regeneration through node $8 : \psi = 3, \alpha = \frac{2}{3}$

designs and greater flexibility in matching a network growth model to observable data. By varying α, the growth model fluctuates from purely random to purely preferential attachment regeneration.

3.5 Termination Phase

The defense phase concludes with a recalculation of the defending player's utility values. The simulation continues advancing through game phases until at least one of three criteria are met: the defending player's network size is successfully reduced to prespecified level, the overall defending utility drops below a prespecified level, or the simulation exceeds a prespecified number of rounds.

Reducing the Defending Player.

The simulation terminates if the number of members in the defending network drops to ϵ, or $|N_t| \leq \epsilon$ where N_t is the set N at time t. Continuing the simulation when $|N_t| \leq \epsilon$ results in a full restructuring of the network during either ring or clique restructuring. A defending network reduced so dramatically would also represent an enemy force that is significantly reduced but still gathering utility from network participation. Such a small group of network members represents an entirely different form of opponent, forcing a reevaluation of the dynamic game.

Overall Drop in Utility.

The simulation terminates given the conditions in Equation 14, or if the defending player's average utility drops, $\nu(g_t)$ where g_t is the network at time t, below 25% of its initial value $\nu(g_0)$.

$$\nu(g_t) < 0.25\nu(g_0) \tag{14}$$

This condition represents effective targeting by the attacking player. Intuitively a defending player experiencing such a loss in utility will perceive a continuation of this devaluation. Low utility values would force dissolution or a significant restructure of network topology. The proportion of lost utility is chosen arbitrarily based upon the author's experience in the intelligence community.

Simulation Reaches Maximum Rounds.

The simulation terminates once 500 rounds are completed. Given 500 rounds, the simulation either results in a winning player or a steady equilibrium.

3.6 Summary

This chapter provides a basic introduction to graph theory concepts and terminology. Five measures of centrality are presented. Furthermore, this chapter outlines the sequence of play modeled by the simulation and the methodology used in its definition. Chapter IV presents the results of the simulation, an enriched simulation within a designed experiment, and follow-on experimentation dictated by the experimental design.

IV. Implementation, Results, and Analysis

This chapter discusses the implementation and results of the simulation presented in Chapter III. The purpose of this application of the simulation model is to investigate the impact of attacker and defender interactions on the size of the largest network component and average network utility. Of particular interest is the effects of limited information states on an attacker given uncorrelated attack strategies. Also explored is the effectiveness of the defender's regeneration and restructuring strategies. Finally, the efficacy of the chosen utility function is examined. Test networks are carefully constructed so as to emulate observed convert networks, and sensitivity analysis is presented on all experimental factors. Two designed experiments are presented to study the significance of factors and their interactions.

4.1 Network Construction

The PNDCG algorithm constructs representative networks using N_0 to closely emulate the characteristics of a known covert network. The PNDCG algorithm employs specified network measures to generate a structure that meets desired specifications. The node set N_0, the initial starting set where $|N_0| = 100$, is selected to provide a network of adequate size for analysis while maintaining reasonable computational requirements. The size of the network remains fixed throughout the simulation. The PNDCG network output is stochastic, requiring additional analysis to select networks that best represent desired characteristics. The following subsections introduce two constructed network analogs, selected network measures, and resulting networks used for the designed experiments.

9/11 Hijacker Network Dataset.

The 11 September, 2001 hijacker network compiled by Krebs (2002) is chosen for its relevance and relative simplicity. The nineteen node network is a relatively sparse organization that limits highly connected nodes to provide greater operational security. The structure of this network is seen in Figure 9.

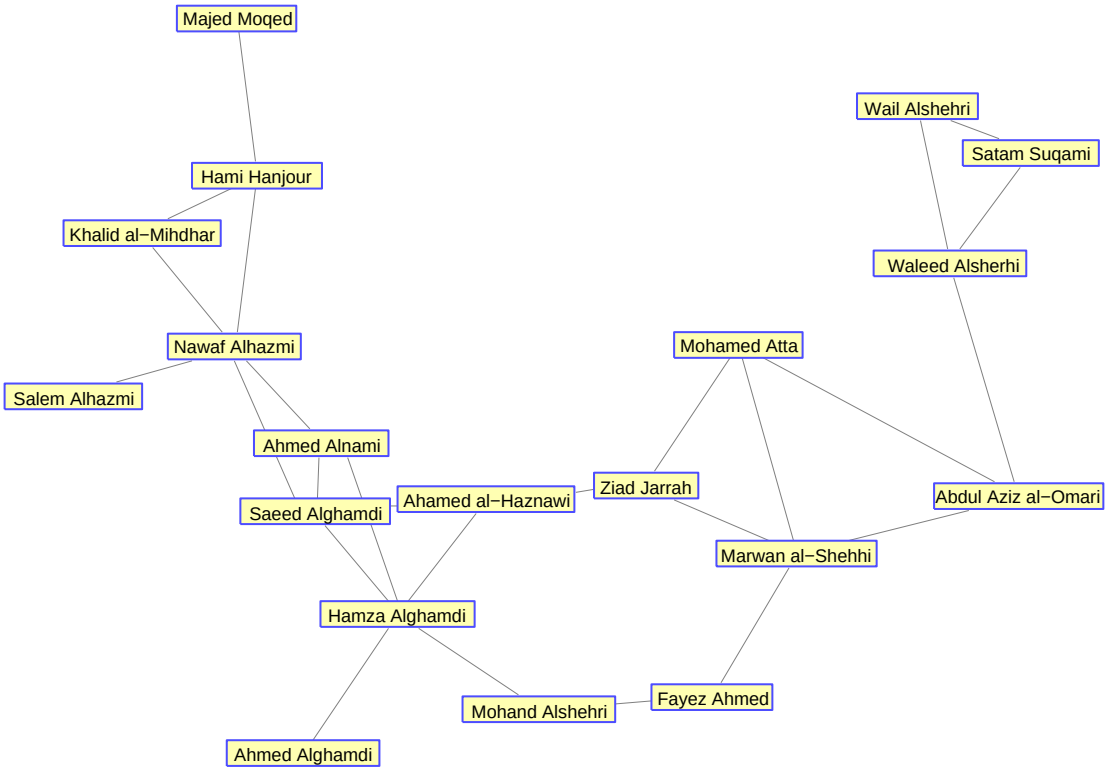

Figure 9. Trusted connections within the 11 September, 2001 Hijacker Network (Krebs, 2002)

Degree distribution within N provides the primary network measure used to specify the structure of g. Specifying degree distribution results in a network that most closely resembles the sparse structure of the hijacker network. Preferential attachment methods are undesirable as they result in several highly connected nodes. Methods utilizing strictly random network generation can be used, however the resulting network properties vary significantly relative to the specified probability.

The PNDCG algorithm produces a user-defined number of constructed networks, each of which is compared to find the network that best fits the observed network. Ten constructed networks are generated and compared for adequacy. The discrete degree distributions of both observed and constructed hijacker networks are analyzed using the Kullback-Leibler divergence. The divergence, denoted $D_{KL}(P \parallel Q)$, represents the information lost when Q is used to approximate P, where Q is a theoretical model and P is the true distribution (Kullback & Leibler, 1951). All PNDCG output are compared and the constructed network where $D_{KL}(P \parallel Q) = 0.0278$ is selected as the best fit.

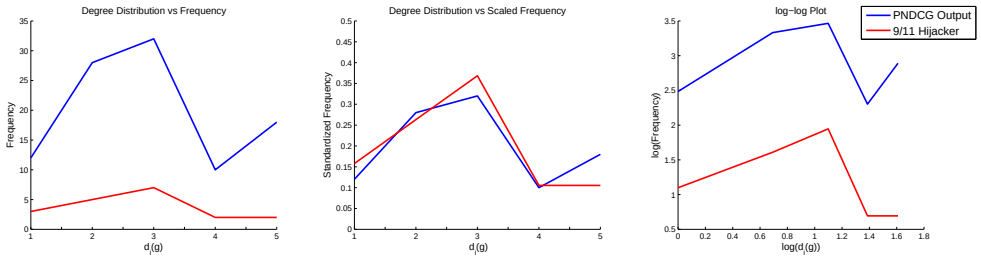

Figure 10. Comparison of the 11 September, 2001 Hijacker Network (Krebs, 2002) and PNDCG Hijacker Networks

Figure 10 visually compares the degree distribution of the hijacker organization with the PNDCG output. The left plot displays the frequency of degree distributions in both networks. The center plot displays a scaled frequency for each network, giving a better picture of the true organizational composition. The right plot indicates the rate of change between degree distribution levels. The figure shows the close similarity in degree distribution between the observed hijacker network and the engineered network using the PNDCG algorithm.

Table 5. Comparison of Major Network Measures in 11 September, 2001 Hijacker Network and Constructed Network

Measure	Hijacker Network (Krebs, 2002)	PNDCG Output
Cluster Coefficient	0.3807	0.1533
Betweenness Centrality	0.3096	0.0834
Proximal Target Betweenness	0.8421	0.9600
Closeness Centrality	0.2877	0.2006

Table 5 presents select network measures for the observed hijacker network and the PNDCG constructed network. Degree and eigenvector centrality are omitted as the measures do not scale to network size, failing to provide adequate comparison between differing networks. Expanding the network to 100 nodes while maintaining the same degree distributions results in minor changes in network measure scores. The cluster coefficient and betweenness centrality measures differ significantly. The constraint on degree distribution limits the PNDCG algorithm's ability to create triad relationships. Closeness centrality remains quite similar though, showing that the average distance between nodes is relatively the same.

The PNDCG output provides an adequate representation of a 100 node analog network for the 9/11 hijacker network. Some network measures are significantly altered due to restrictions on degree distribution, however limiting the number of high degree nodes is of greater importance.

1998 U.S. Embassy bombings in Kenya and Tanzania Dataset.

Geffre *et al.* (2009) presents a terrorist network responsible for the bombing of the U.S. embassies in Kenya and Tanzania. The degree distribution of this group has a greater magnitude compared to the hijacker network, most likely due to the decreased

operational security concerns in 1998.

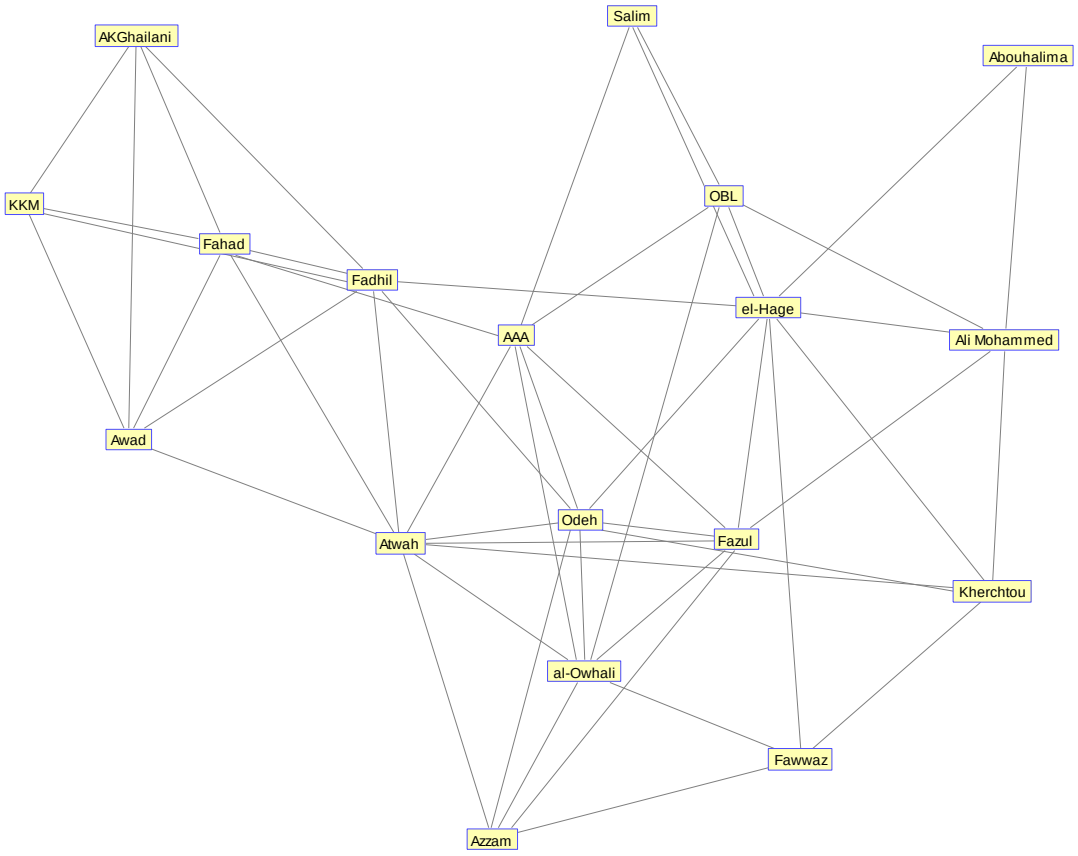

Figure 11. 1998 U.S. Embassy Bombing Network (Geffre *et al.*, 2009)

Figure 11 displays the network structure of the nineteen node real-world organization. Ten representative networks are again compared, and the network $D_{KL}(P \parallel Q) = 0.1121$ is selected as the representative network analog. Degree distribution is once again analyzed and employed as the primary desired network structure characteristic for the PNDCG algorithm. Figure 12 provides a visual comparison of the degree distributions of both the observed embassy bombing network and the PNDCG constructed network. The degree distributions are a close match for both networks.

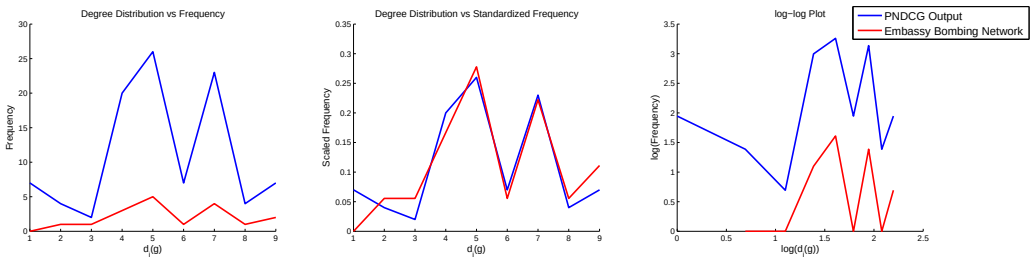

Figure 12. Comparison Between Real-Life and Constructed Embassy Bombing Networks

Table 6 provides basic network measures for both the embassy network and the PNDCG output. Significant differences between network structures exist, however there is improvement over the hijacker network. Despite these differences, the PNDCG output provides an adequate representation of the embassy bombing group.

Table 6. Comparison of Major Network Measures in Embassy Bombing Network and Constructed Network

Measure	Embassy Bomber Network	PNDCG Output
Cluster Coefficient	0.5788	0.4111
Betweenness Centrality	0.0543	0.0277
Proximal Target Betweenness	0.6667	0.9200
Closeness Centrality	0.5455	0.2734

4.2 Factors

This section presents the experimental response, magnitude of factors, and an investigation of each factor in single experiments.

Response.

The experiment response is determined to be the size of the largest network component, $|x|$, once the simulation satisfies at least one of its two termination criteria.

Component sizes are low when the attacker effectively reduces the defending network. Conversely, a larger final component is indicative of a successful defense. Although average network utility at time t, $\nu_t(g)$, is a more intuitive response for player success, the values for $|x|$ accurately represent success while being subject to far fewer perturbations within the simulation. This phenomenon is more thoroughly discussed in the following sections.

An initial assessment conducts 1,750 simulation replications to analyze the variance inherit within the response. Assuming normality of the response means over greater sampling, the number of runs is decreased to obtain a tighter confidence interval around the true mean while conserving computational requirements. The results of these initial repetitions are shown in Figure 13. The observed variance within the response is a result of the stochastic nature of the simulation. The attacker's success many times depends exclusively upon the nodes selected in the initial permutation of the state of information vector. Some draws result in an attacker submatrix that facilitates almost immediate destruction of the defending network, whereas other draws enable the defender to sustain prolonged attack. The stochastic processes tied to the attacker expanding its state of information introduces further variance into the results. A sample size of 200 is determined to be adequate using the sample size and power calculator in JMP. This sample size minimizes runs while maintaining 80% power and the ability to detect a 5% change in the response.

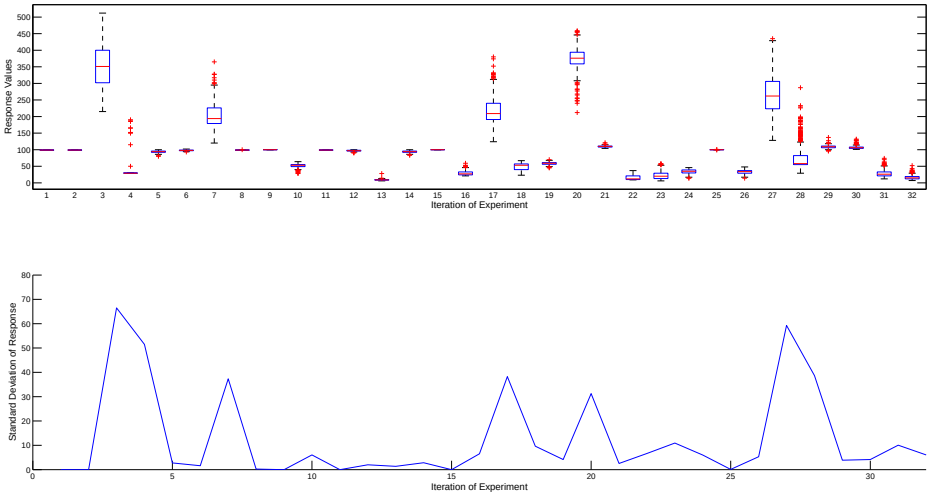

Figure 13. Boxplot and Standard Deviation of Response

Magnitude of Factor Levels.

Manual repetitions of the simulation are used to determine the magnitude of factor levels for continuous variables. These magnitudes should be large enough to adequately detect significance while remaining within a reasonably feasible space. Table 7 summarizes continuous factor levels to be used in the designed experiment.

Table 7. Factor Levels for Continuous Variables

	Factor	Low	Medium	High
α	Hybrid Regeneration Method	0.1	0.5	0.9
β	Probability of Successful SSE	0.1	0.5	0.9
γ	Probability of Successful Intelligence	0.1	0.5	0.9
δ	Utility Decay Parameter	0.1	0.5	0.9
ϵ	Size of Rings or Cliques	3	6	8
ζ	Number of Nodes Investigated for Intelligence	4	7	10
κ	Cost of a Direct Relationship	0.1	0.8	1.5
ρ	Defender Decision Criteria	-1	0	1
τ	Attacker Decision Criteria	0.1	0.5	0.9
ϕ	State of Attacker Information	0.1	0.5	0.9
ψ	Number of Edges Assigned to New Nodes	3	6	8

The following subsections present analysis of the effects of an individual factor at varying levels using the embassy bombing network. Unless under consideration, all continuous factor levels are set to the medial level of magnitude. Categorical variables include betweenness centrality for attacker targeting strategy and ring method for defender defensive strategy, and remain consistent throughout unless otherwise noted. Random number seeds are maintained between experimental runs in order to restrict variance to the effects of the factor under consideration.

Base Network Measures.

Figure 14 presents the value of the overall network size and largest component given a complete game round. Despite some minor perturbations, the network is sustained as a single connected component for the duration of the round. This demon-

strates the resiliency of the network against a series of attacks. The redundancy in relationships allows for the removal of important nodes while still maintaining the general organizational structure.

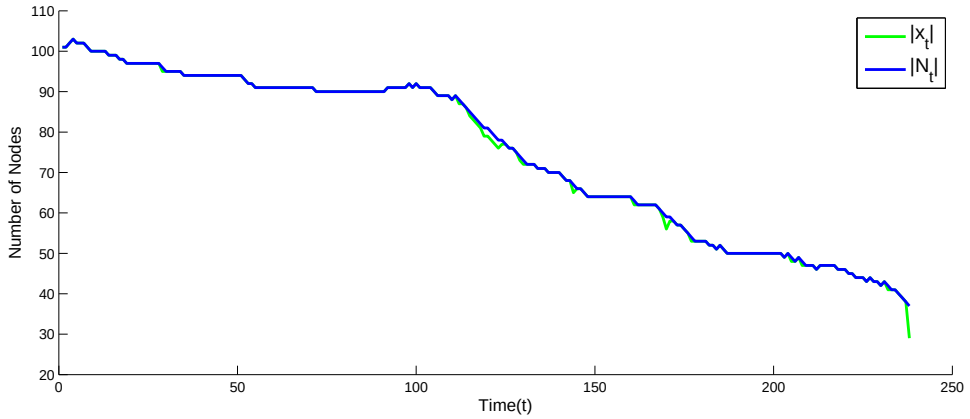

Figure 14. Network Size $|N_t|$ and Size of the Largest Component $|x_t|$ over Time

Figure 15 shows the defender utility values for the same simulation depicted in Figure 14. Perturbations in utility can be seen throughout as attacker and defender strategies interact dynamically.

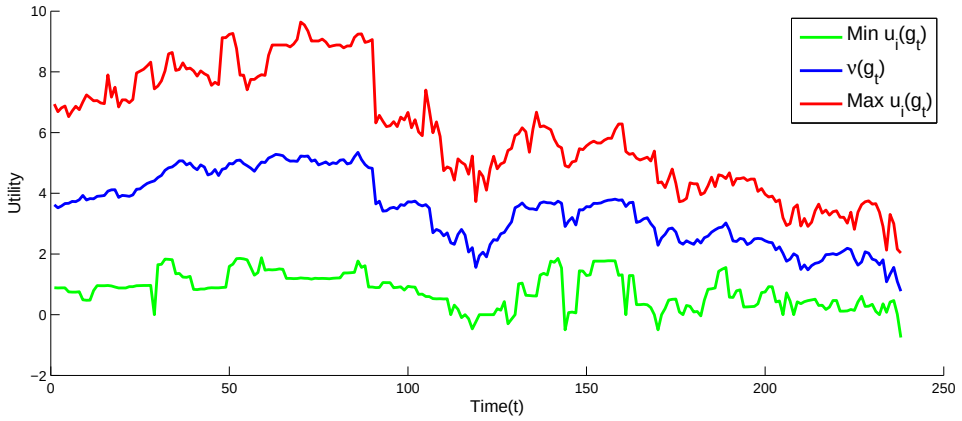

Figure 15. Utility Scores over Time

It is interesting to note the variance in utility scores throughout the round as it relates to network size. The defense is initially successful in expanding the network,

and the utility values show an initial increase in maximum and mean values. However, both utility values and variance decrease as the attacker proves successful in degrading the defending network.

Hybrid Regeneration (α).

Figure 16 demonstrates the effect on $\nu_t(g)$, the average network utility at time t, by varying the level of α. At $\alpha = 0.9$, the defending network is regenerating almost exclusively by random connections. This results in a robust network capable of withstanding repeated attacks. At $\alpha = 0.5$, the defending network is regenerating half randomly and half by preferential attachment. The resulting network is more robust, capable of maintaining a higher utility against sustained attacks. Decreasing to $\alpha = 0.1$ significantly impacts the ability of the network to withstand attack. The algorithm determines preferential attachment connections based upon the initial random draw of connections. Decreasing α to its lowest level greatly diminishes the size of the second-step neighborhood of node i, $|N_i^2(g)|$, limiting the quantity and quality of nodes available for preferential attachment. With $\psi = 6$ and $\lceil \psi \times \alpha \rceil = \lceil 6 \times 0.1 \rceil = 1$, one node j being chosen randomly and $\psi - 1$ edges assigned to the nodes in $N_j(g)$. This results in a highly localized connection for newly created nodes.

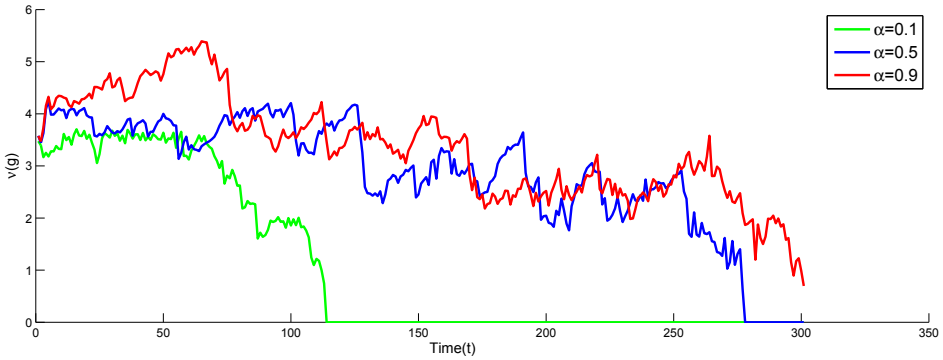

Figure 16. α Effect on Average Utility $\nu_t(g)$

Figure 17 further demonstrates the effects of α on the defending network. The effect of $\alpha = 0.1$ is a rapid reduction in $|x|$ until the game round completes relatively quickly. The results for $\alpha = 0.5$ and $\alpha = 0.9$ offer more compelling and interesting results. The effect of $\alpha = 0.5$ shows the strongest initial performance as a balanced regeneration increases or maintains the structure of the largest component. This is because the balanced regeneration method is allowed superior choices for preferential connections. However, as the round continues, $\alpha = 0.9$ dominates by sustaining the network slightly longer.

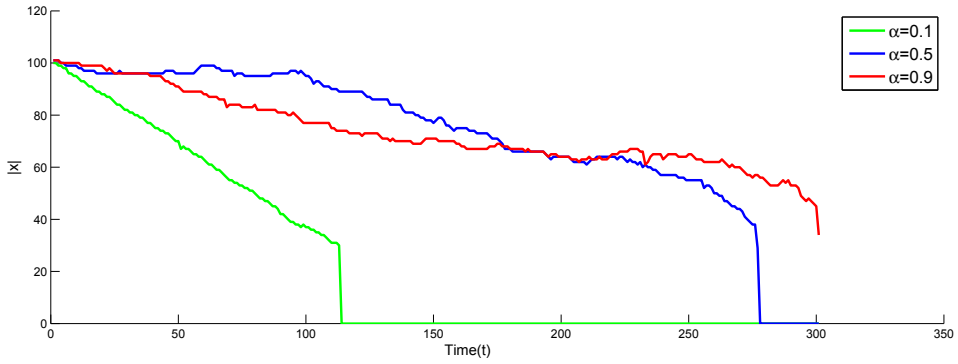

Figure 17. α and Size of the Largest Component $|x_t|$

Varying α results in dramatically different behavior during defensive regeneration. Defender network defense performance, as measured by the size of the largest network component $|x|$, is generally better when $\alpha = 0.5$ or $\alpha = 0.9$. While $\alpha = 0.9$ proved the most robust in performance across the entire round, $\alpha = 0.5$ showed significantly better initial performance. Greater investigation during the designed experiment will describe these behaviors.

Probability of Successful Sensitive Site Exploitation (SSE) (β).

The magnitude of β greatly impacts the results of the game despite only occurring during node removal in the attack phase.

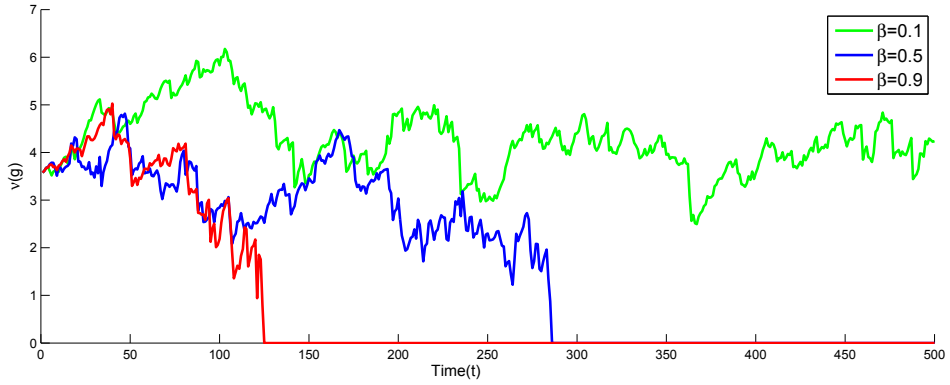

Figure 18. β **Effect on Average Utility** $\nu_t(g)$

Figure 18 presents the significance of β on the attacker's effectiveness at reducing $\nu_t(g)$. Figure 19 complements this result as lower levels of β weaken the attacker's ability to effectively target key members of the network.

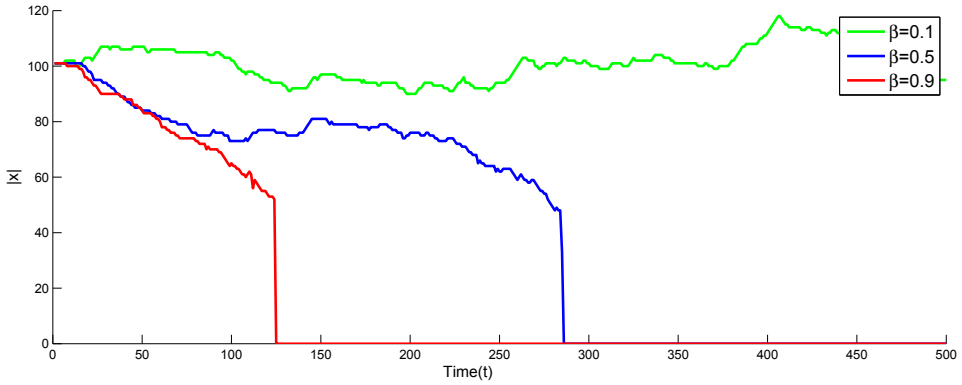

Figure 19. β **and Size of the Largest Component** $|x_t|$

The attacker's ability to discover additional information given a node removal significantly impacts attacker effectiveness. By lowering β, the attacker's ability to expand its state of information is restricted to intelligence gathering. This significantly slows the attacker's ability to effectively target key nodes and reduce the defender. This process also accurately represents real-world operations where SSE is critical to the intelligence cycle.

Probability of Successful Intelligence (γ).

As already discussed, the attacker's ability to expand its state of information is a critical component of its attack strategy. Figure 20 shows the defender is able to withstand repeated attack rounds given a lower γ, however the attacker proves more successful as γ increases.

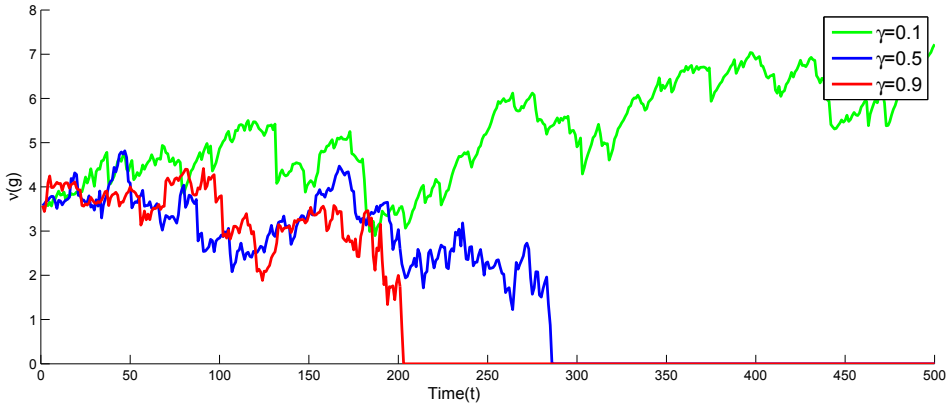

Figure 20. γ Effect on Average Utility $\nu_t(g)$

Figure 21 presents an interesting phenomenon as γ increases. Both $\gamma = 0.5$ and $\gamma = 0.9$ result in similar impacts on $|x|$, however $\gamma = 0.9$ ends significantly sooner. This result indicates the attacker's ability to decisively target critical nodes given a higher state of information. The higher rate of successful intelligence gathering facilitates better targeting, allowing the attacker to complete the round more quickly.

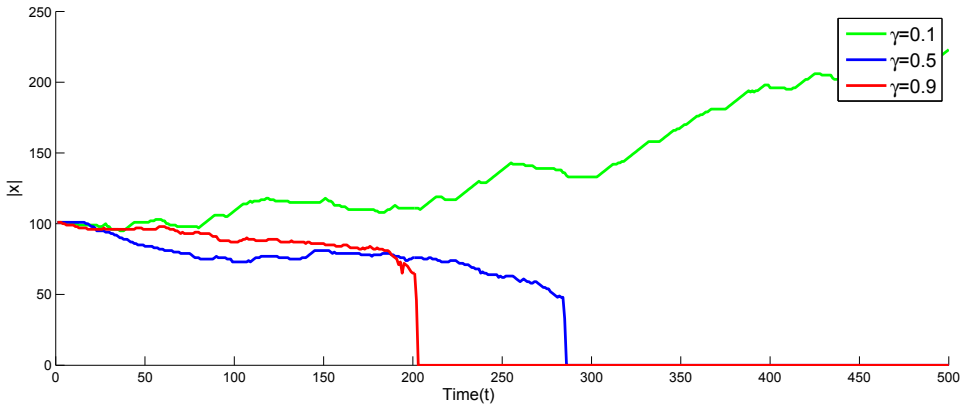

Figure 21. γ and Size of the Largest Component $|x_t|$

Utility Decay Parameter (δ).

Figure 22 shows the effects of varying δ on $\nu_t(g)$, with drastic differences between the responses. This is due to the cost of directed relationships, κ, being set at its medial level. There are suspected two-factor relationships between δ and related factors ρ and κ. These three factors comprise the defender's decision criteria and greatly impact its resilience against attack.

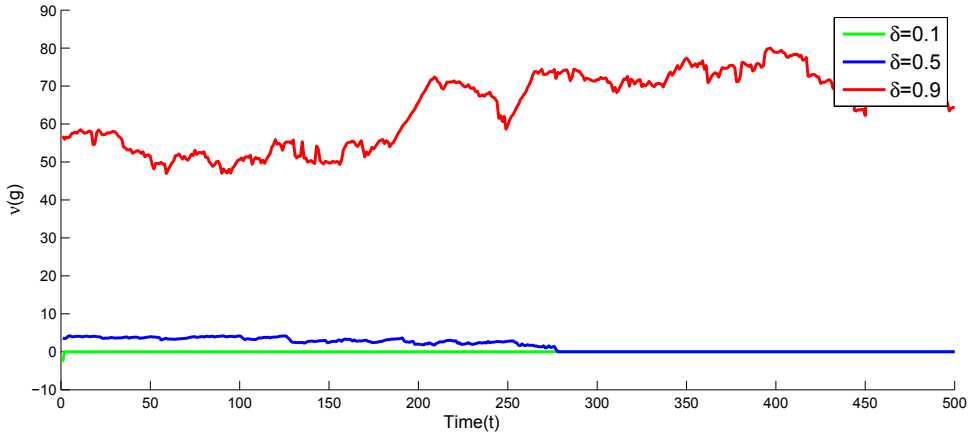

Figure 22. δ Effect on Average Utility $\nu_t(g)$

Figures 22 and 23 show the significant impact δ has on the defending network. High levels of benefits due to relationships result in a network that outpaces the

attacker. Low levels result in a network that is immediately defeated.

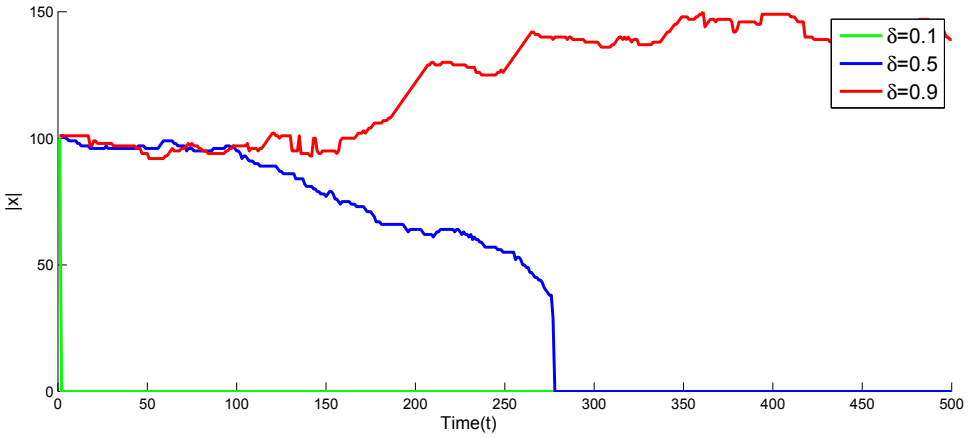

Figure 23. δ and Size of the Largest Component $|x_t|$

Size of Rings or Cliques (ϵ).

Figure 24 presents the effects of larger restructuring rings or cliques on $\nu_t(g)$. The defending network proves more robust as ϵ increases. This result is attributed to the method of restructuring. As connections are redistributed amongst restructured nodes, the network becomes denser and thus more difficult for the attacking player to effectively target.

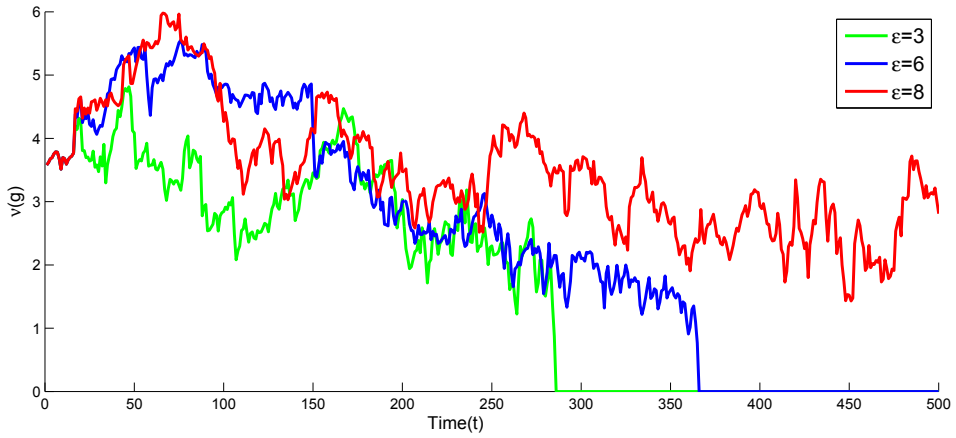

Figure 24. ϵ Effect on Average Utility $\nu_t(g)$

Figure 25 shows how large restructuring groups allow the defending player to maintain cohesion within the largest component throughout the round.

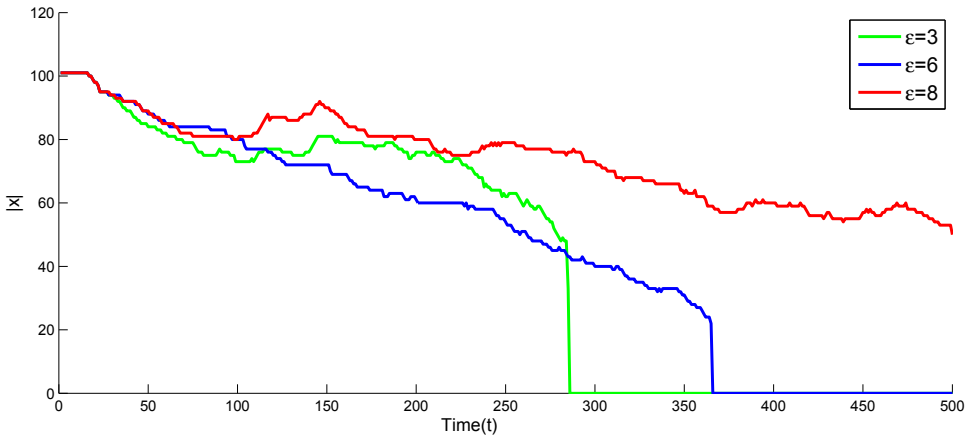

Figure 25. ϵ and Size of the Largest Component $|x_t|$

Number of Nodes Investigated for Intelligence (ζ).

Figure 26 shows a minimal impact from varying ζ on the attacker's success.

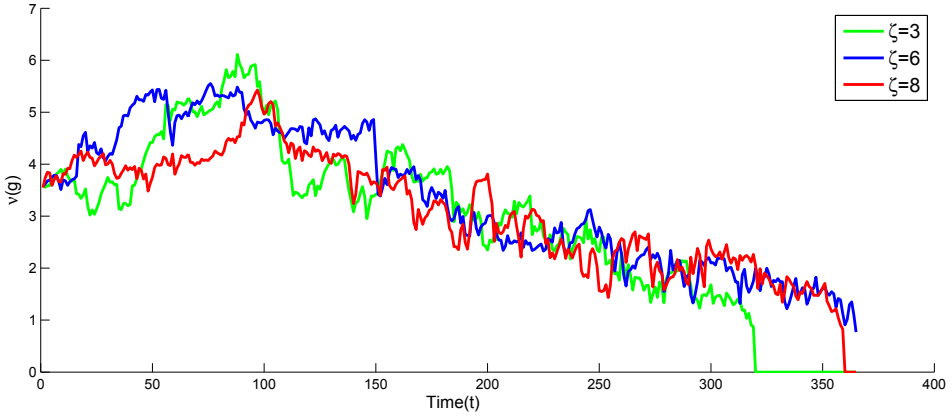

Figure 26. ζ Effect on Average Utility $\nu_t(g)$

This impact is reiterated in Figure 27, where only $\zeta = 3$ shows a slightly reduced impact on the round. These results indicate the success of intelligence gathering is more a function of γ and target selection rather than thoroughly searching ad-

ditional available targets. This emphasizes the importance of intelligence targeting procedures.

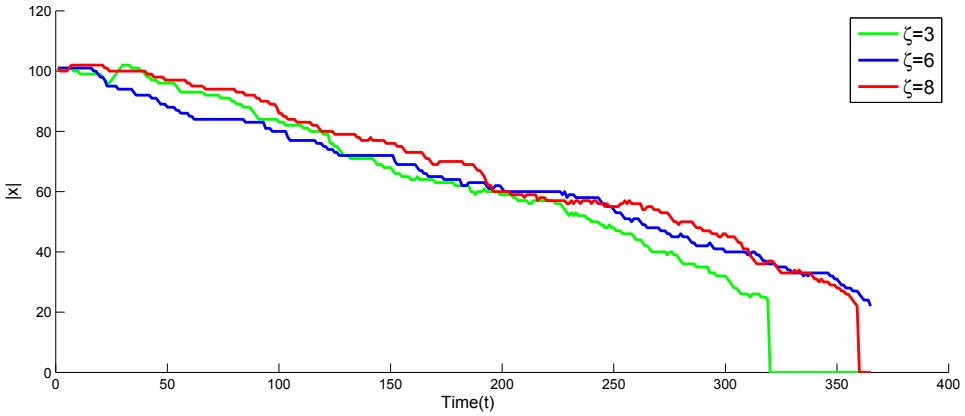

Figure 27. ζ and Size of the Largest Component $|x_t|$

Cost of a Direct Relationship (κ).

Figures 28 and 29 present the impact of the cost of relationships on network utility and structure. The defender is unable to withstand the attacker when $\kappa = 1.5$, however both other levels prove resilient throughout the round.

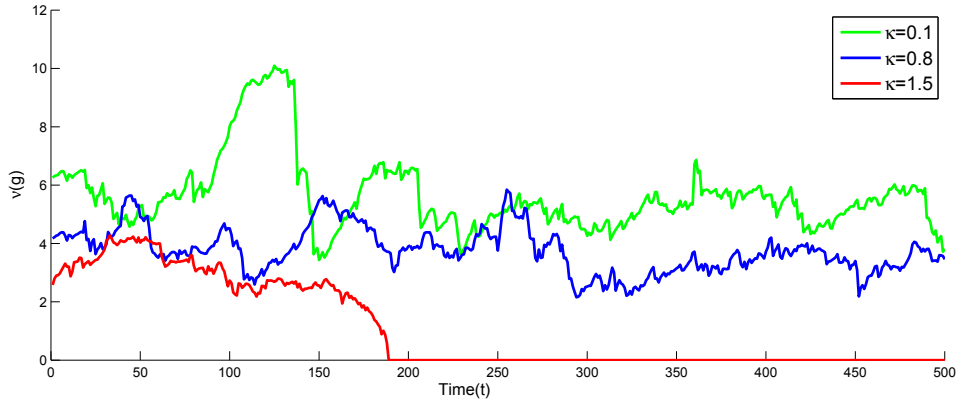

Figure 28. κ Effect on Average Utility $\nu_t(g)$

The impact of κ on $|x|$ when $\kappa = 0.1$ is of particular interest. The decreased costs of direct relationships allow the defender to continue connecting without negative

consequence. The higher utility values allow the network to continue recruiting and expanding.

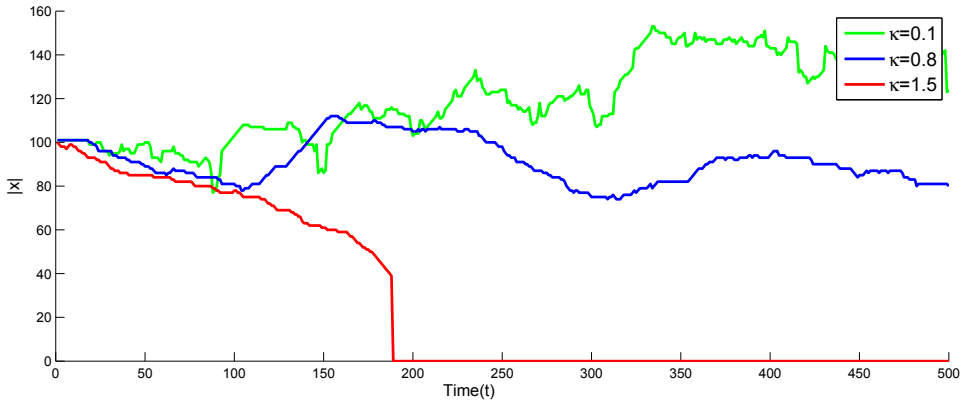

Figure 29. κ and Size of the Largest Component $|x_t|$

Defender Decision Criteria (ρ).

Figures 30 and 31 present a significant impact on the game by varying ρ. A lower value of ρ results in the defender electing to recruit rather than restructure low utility relationships. Defenders with a higher ρ would then rely upon a restructure strategy rather than recruitment.

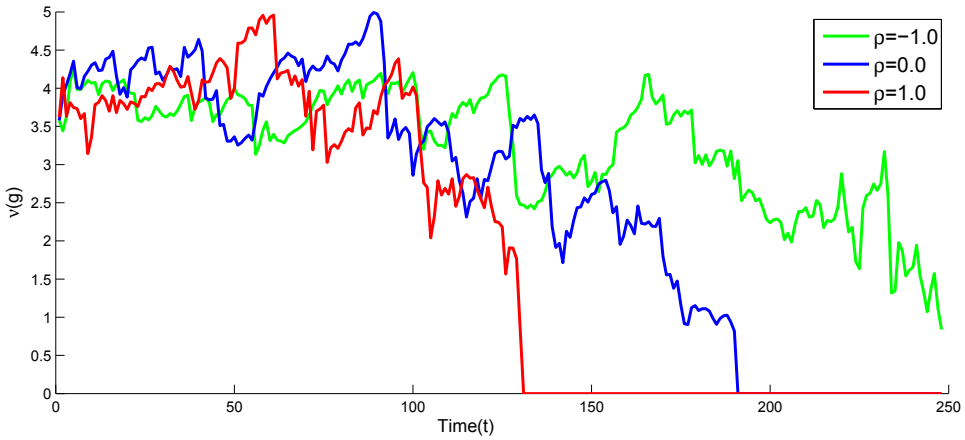

Figure 30. ρ Effect on Average Utility $\nu_t(g)$

A defender who relies upon restructuring proves less resilient to a determined

attacker. This is due to the implicit utility costs associated with restructuring. Although utility is increased for a node targeted for restructure, there is a negative impact on $\nu_t(g)$ over time as the low utility is distributed throughout the network.

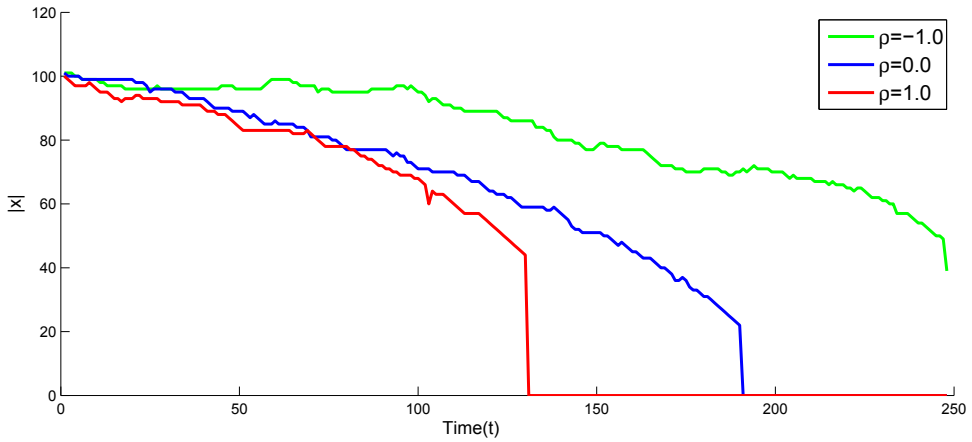

Figure 31. ρ and Size of the Largest Component $|x_t|$

Attacker Decision Criteria (τ).

The value of τ determines whether an attacker chooses to conduct node removal or intelligence gathering. Attackers with a higher value of τ will more often elect to conduct intelligence gathering. Figure 32 shows the benefits of an aggressive attack strategy during the round; the more aggressive attackers prove more successful reducing the defender's utility. An attacker with $\tau = 0.9$ is one who relies heavily upon intelligence gathering to gain a near perfect state of information, presumably then followed by precise removal of key targeted nodes. This strategy shows promise towards the end of the round, but the overall effect is to allow the defender freedom to recruit and restructure with decreased attacks.

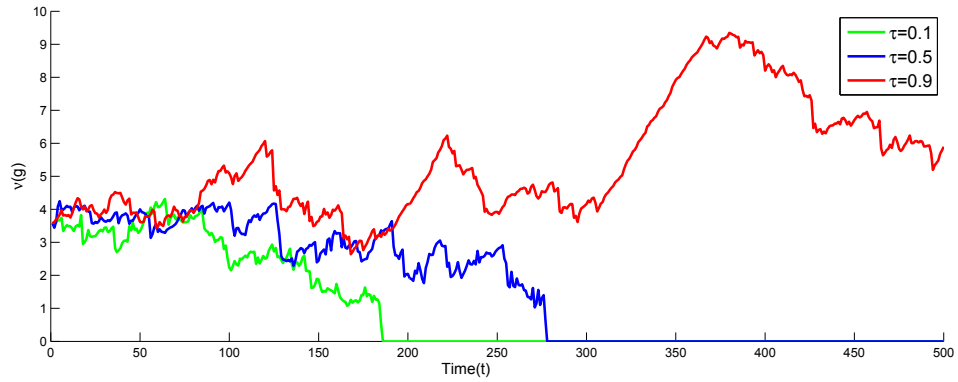

Figure 32. τ Effect on Average Utility $\nu_t(g)$

Figure 33 shows the advantage gained by an aggressive attacker. The lower values of τ prove far more successful at reducing the largest component, while $\tau = 0.9$ is unsuccessful in this regards.

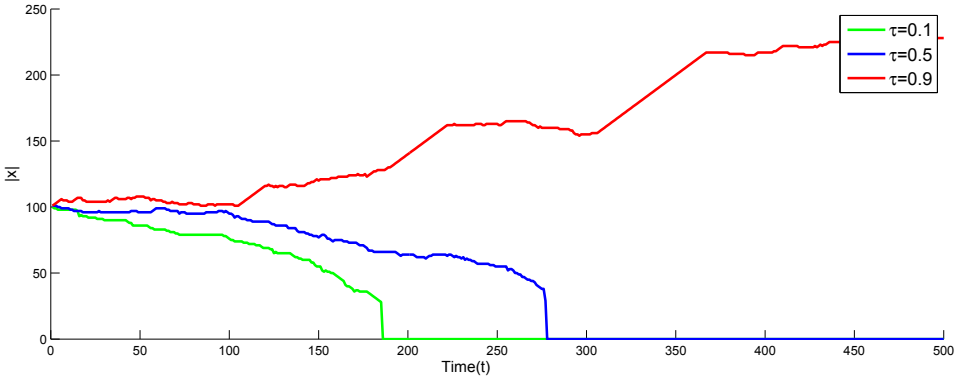

Figure 33. τ and Size of the Largest Component $|x_t|$

A tactically patient attack strategy, where τ is high, effectively targets nodes by developing a near perfect state of information. However this type of attacker personality fails over the course of the round. The more aggressive attacker is more successful in reducing the defending network. In real-life operations, this manner of strategy selection would be tempered by rules of engagement and strategic goals. A more aggressive attacker is more likely to cause collateral damage to the civilian population, possibly resulting in an overall failure in the conflict despite effectively

reducing a single enemy network.

State of Attacker Information (ϕ).

Figure 34 demonstrates the effects of varying ϕ on mean network utility $\nu_t(g)$. There is a pronounced effect on $\nu_t(g)$ as higher states of information allow the attacker improved targeting capabilities. Figure 35 shows the effect of varying ϕ on the size of the largest component.

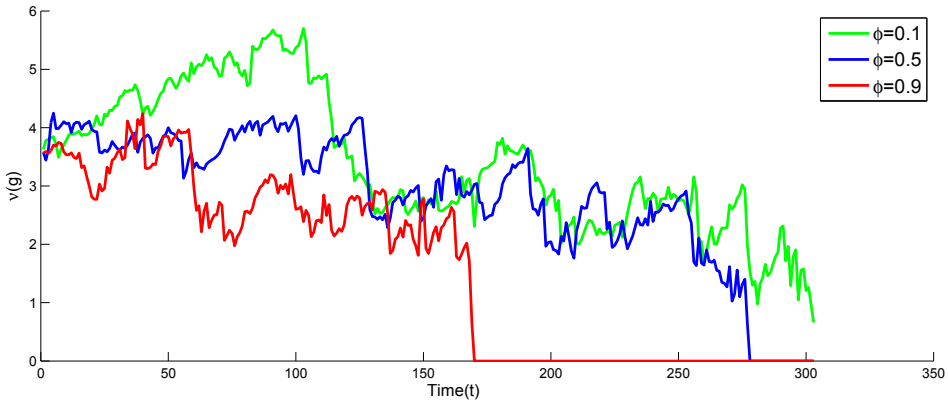

Figure 34. ϕ Effect on Average Utility $\nu_t(g)$

When $\phi = 0.9$, there is an initial increase in utility due to regeneration that is quickly overcome by effective attacker targeting. Figure 35 shows the increased success and efficiency of the attacker by a rapid decrease in the size of the largest component. The defending network is defeated in a relatively short amount of time.

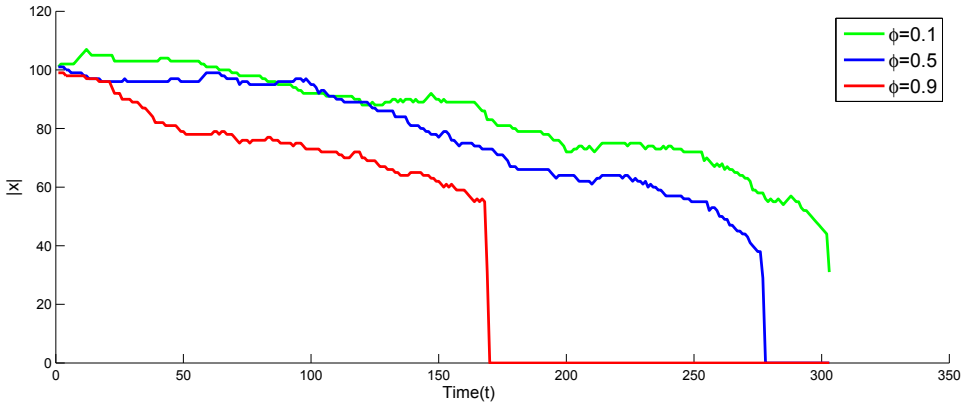

Figure 35. ϕ **and Size of the Largest Component** $|x_t|$

When $\phi = 0.1$, utility shows an initial increase despite degradation by the attacking force. Although the attacker is removing nodes, the limited state of information results in poor targeting selection and a reducing impact on the defender's utility.

Edges Assigned to Formed Nodes (ψ).

The value of ψ shows no impact on the overall results of average utility, as seen in Figure 36, however it does significantly impact the defending player. A defender with a high ψ invests heavily into connecting newly recruited nodes with the existing network. This investment pays dividends in overall utility, despite being counterintuitive due to the increased costs associated with additional links.

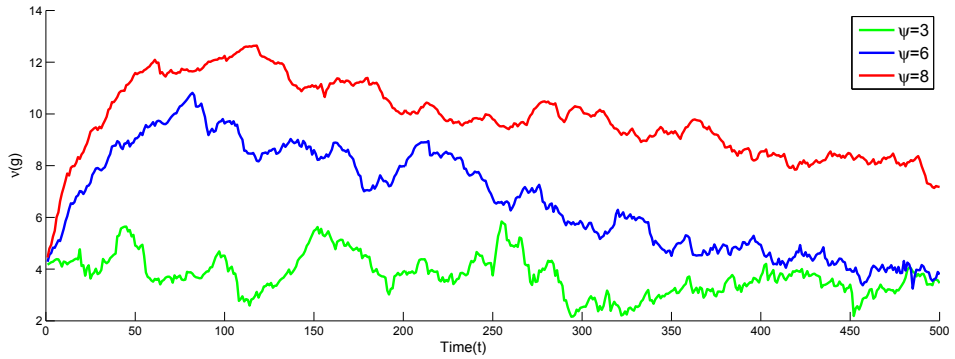

Figure 36. ψ **Effect on Average Utility** $\nu_t(g)$

Using the hybrid regeneration method, the increased investment into random connections for node i ensures an increase in $|N_i^2(g)|$. This results in a larger population of nodes available for preferential attachment.

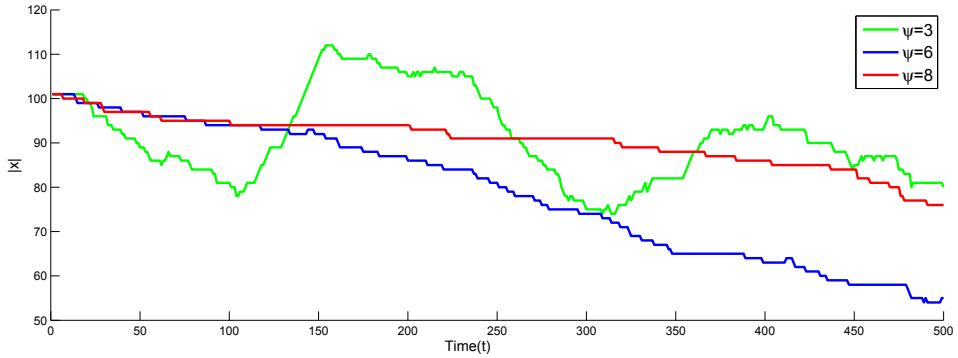

Figure 37. ψ **and Size of the Largest Component** $|x_t|$

Defense Regeneration Method (λ).

Figure 38 shows the effect of defense regeneration strategy on the size of the largest component. Clique restructure appears to result in a more robust network defense. This is due to the connection of all clique members with each other following clique formation. These results are consistent with the findings of Nagaraja & Anderson (2008).

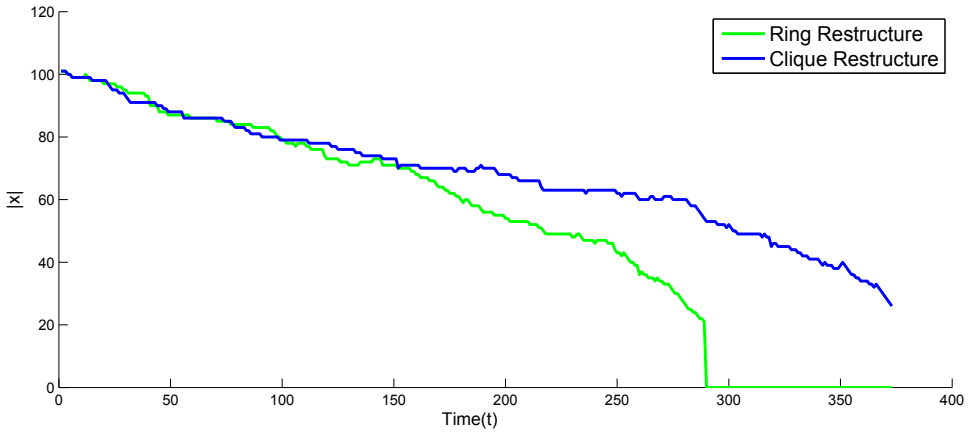

Figure 38. λ **Effect on Average Utility** $\nu_t(g)$

Figure 39 shows the effects of regeneration method on $|x|$, with the clique method demonstrating better performance.

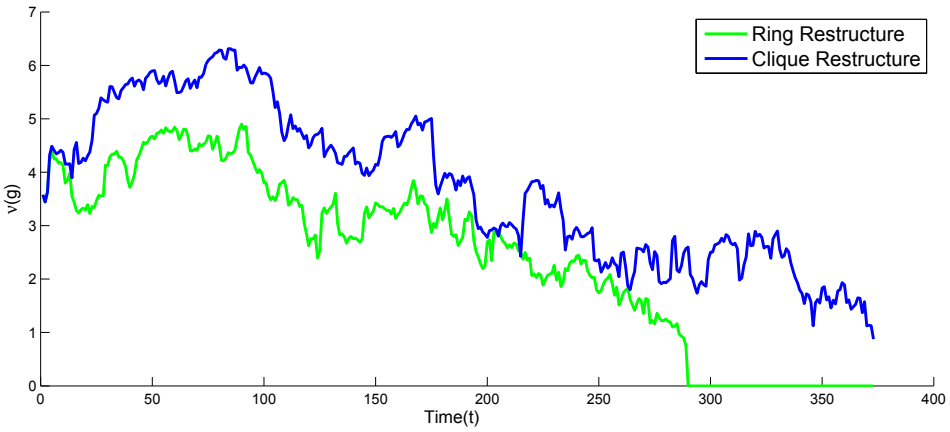

Figure 39. λ and Size of the Largest Component $|x_t|$

Although these initial results show clique regeneration as superior to ring regeneration, there are suspected interactions with several other factors to consider.

Attack Strategy (θ).

Figure 40 shows the effect on average utility given differing attack strategies through one game round. There appears to be a significant impact due to the performance of each measure. Degree centrality C^D appears to dominate all other strategies for the attacker. Although there is significant overlap within the round, it appears that closeness centrality C^C is the poorest performing strategy. Recall that defender strategy is fixed at ring restructuring, and so these initial findings fail to adequately assess performance based upon all factors. The designed experiment in the following section addresses this shortcoming.

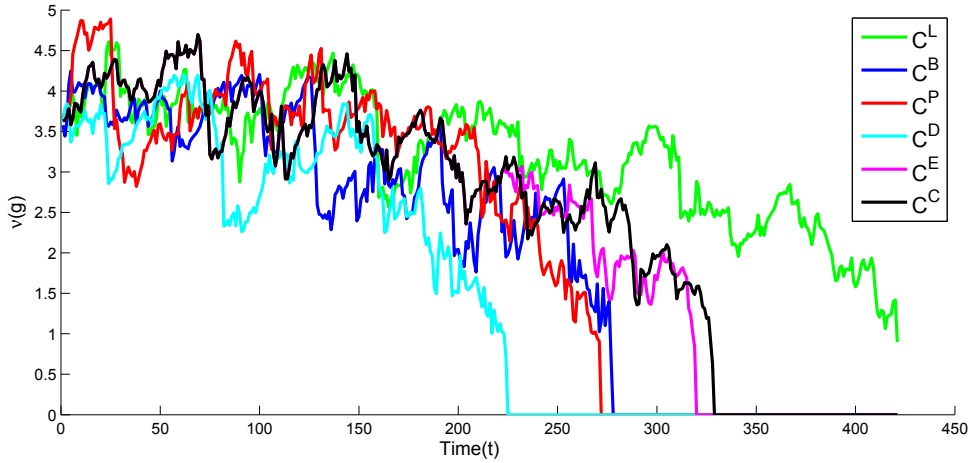

Figure 40. θ **and Average Utility** $\nu_t(g)$

Figure 41 shows much the same impacts of attack strategy on size of the largest component. This is only a single round of the game, so more experimentation is required to adequately measure the magnitude of impact by each strategy.

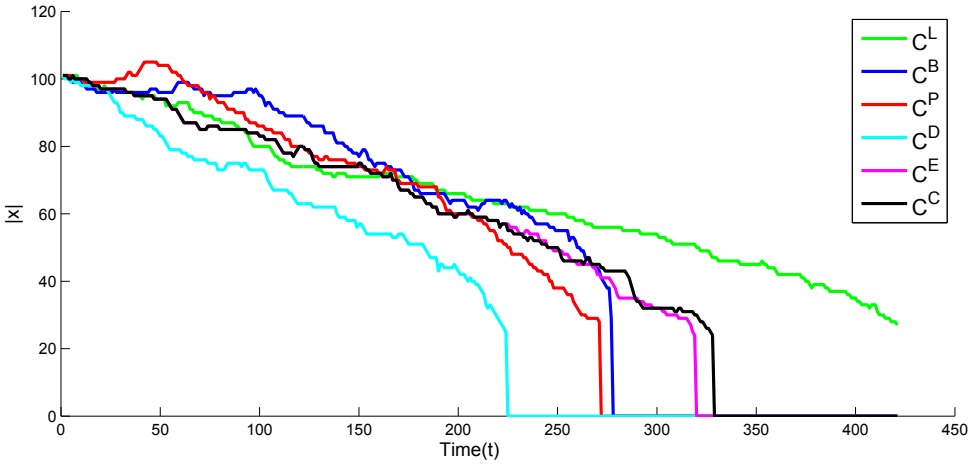

Figure 41. θ **and Size of the Largest Component** $|x_t|$

4.3 Designed Experiment

A designed experiment is employed to investigate the significance of important game factors and their interactions. Although all factors show significance in single

Table 8. Factors in the Designed Experiment

Term	Description	Player	Type
α	Regeneration method	Defender	Continuous
δ	Decay value of networks connection utility	Defender	Continuous
θ	Attack Strategy	Attacker	6-level Categorical
κ	Utility cost of maintaining direct links	Defender	Continuous
λ	Network restructuring strategy	Defender	2-level Categorical
ϕ	Initial probability of attacker state of information	Attacker	Continuous

run analysis, the designed experiment only investigates the factors indicated in Table 8. The categories of θ correspond to the six network centrality measures employed as targeting by the attacker and the two categories of λ correspond to the two defensive restructuring strategies.

Factors β, γ,ϵ, ζ and ψ are omitted from the final analysis as they are deemed to be trivial. Although each significantly impacts the results of a single game, none are tied to a cost or benefit function and thus would fail to present significant findings. Both ρ and τ are highly significant within the model, however serve only as artifacts of the simulation rather than describing real-world phenomena. All omitted factors are set to their medial level for the duration of the designed experiment.

Experimental Design.

The experimental design is a $2^5 \times 6^1$ resolution V design. This design implies all main effects being confounded with four factor and higher order interactions, and all two-factor interactions are confounded with three factor or higher order interactions. This results in the independence of all main effects and two-factor interactions. The design is augmented with six center run treatments to test for curvature, one for each of the six levels of θ. We chose this design to avoid confounding effects and fully investigate curvature and two-factor relationships. Effects of three factor or higher order interactions are assumed to be trivial due to the variance inherit in the system.

The simulation requires considerable computational requirements, even under small-scale network implementation. The parallel processing toolkit in MATLAB allows multiple instances of the simulation to run simultaneously on a multiple core computer. The simulation is structured to allow parallel processing and thus greatly reduces the requisite time for multiple run experiments. The simulation is implemented on a dual Intel Xeon E5-2650v2 workstation with 192 GB of RAM.

Results.

This section presents the results of the designed experiment followed by a discussion of each significant factor individually.

Experimental responses appear normally distributed, and residuals are evenly distributed against the predicted response. One data point proved to be a significant outlier and exhibit unusually high variance within the response. The unusually high level of variance is assumed to be a result of simulation and the data point is removed from analysis.

Table 9 provides the summary of analysis for the 9/11 hijacker network. As expected, the model's fit is not exceptionally high due to significant noise in a social network model. The lack of fit analysis determines that the model adequately fits the data. The table includes variance inflation factors (VIF) to investigate any multicollinearity within the factors. All VIF values are adequately low, indicating the variance for each factor estimated in the model is not significantly impacted by multicollinearity with other factors.

Table 9. 9/11 Hijacker Network Results

Summary of Fit					
	R^2	0.5061			
	Adjusted R^2	0.4536			
	Root Mean Square Error	27.0568			
	Mean of Response	99.1097			
	Observations (or Sum Wgts)	53			
Analysis of Variance					
Source	DF	Sum of Squares	Mean Square	F Ratio	Prob>F
Model	5	35256.9920	7051.4000	9.6321	<.0001
Error	47	34407.2650	732.0700		
C. Total	52	69664.2570			
Lack of Fit					
Source	DF	Sum of Squares	Mean Square	F Ratio	Prob>F
Lack Of Fit	4	1708.1260	427.0320	0.5616	0.6918
Pure Error	43	32699.1380	760.4450		Max R^2
Total Error	47	34407.2650			0.5306
Parameter Estimates					
Term	Estimate	Std Error	r Ratio	Prob> $\|t\|$	VIF
Intercept	98.1836	3.7251	26.3600	<.0001	
α	-7.6708	3.9938	-1.9200	0.0608	1.0626
κ	-11.2668	3.9508	-2.8500	0.0064	1.0096
$\theta\{C^D\&C^P\&C^C - C^B\&C^L\&C^E\}$	-12.8223	3.7251	-3.4400	0.0012	1.0202
$\alpha * \kappa$	16.1008	3.9508	4.0800	0.0002	1.0160
$\alpha * \theta\{C^D\&C^P\&C^C - C^B\&C^L\&C^E\}$	9.0764	3.9938	2.2700	0.0277	1.0099

Table 10 provides the summary of analysis for the embassy bombing network. As expected, the model's fit is not exceptionally high due to significant noise in a social network model. The lack of fit analysis determines that the model adequately fits the data. An analysis of main effects follows, with 1st order interactions subsequently addressed.

Table 10. Embassy Bombing Network Results

Summary of Fit	
R^2	0.4845
Adjusted R^2	0.4043
Root Mean Square Error	22.7328
Mean of Response	91.5722
Observations (or Sum Wgts)	53

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio	Prob>F
Model	7	21852.3410	3121.7600	6.0408	<.0001
Error	45	23255.0080	516.7800		
C. Total	52	45107.3490			

Lack of Fit

Source	DF	Sum of Squares	Mean Square	F Ratio	Prob>F
Lack Of Fit	10	3637.9570	363.7960	0.6491	0.7619
Pure Error	35	19617.0510	560.4870		Max R^2
Total Error	45	23255.0080			0.5651

Parameter Estimates

Term	Estimate	Std Error	r Ratio	Prob> $\|t\|$	VIF
Intercept	94.4195	3.2628	28.9400	<.0001	
α	-3.3119	3.4188	-0.9700	0.3379	1.0626
κ	-5.3753	3.3325	-1.6100	0.1137	1.0096
ϕ	6.7289	3.3498	2.0100	0.0506	1.0202
$\theta\{C^C\&C^E\&C^P\&C^D - C^L\&C^B\}$	-9.9107	3.2816	-3.0200	0.0042	1.0160
$\alpha * \kappa$	10.8969	3.3329	3.2700	0.0021	1.0099
$\alpha * \phi$	-10.0571	3.3502	-3.0000	0.0044	1.0171
$\alpha * \theta\{C^C\&C^E\&C^P\&C^D - C^L\&C^B\}$	8.2353	3.4411	2.3900	0.0209	1.0765

Hybrid Regeneration α.

Both experiments find α significant within interactions however the main effect is insignificant at the 0.05 significance level. These interactions are introduced following a discussion of related main effects.

Utility Costs κ.

Both experiments identify κ as a significant main effect. This is an intuitive result as higher costs of relationships will result in a less stable network topology due to high degree nodes with low utility.

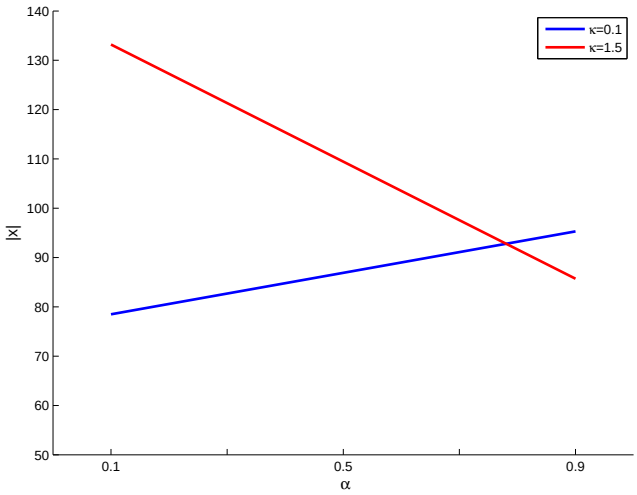

Figure 42. Interaction of α and κ in the Hijacker Network

The interaction of α and κ is significant in both experiments. Given a low level of κ, a regeneration strategy utilizing random attachment is preferable for the defending player. Given a high level of κ, a regeneration strategy utilizing preferential attachment is preferred. This highlights the importance of selecting relationships versus the associated costs. When costs are low, randomly forming nodes creates a more robust network more difficult for the attacker to degrade. Higher costs require more selective structure to relationships or risk adversely impacting the network utility.

Attacker State of Information ϕ.

Only the embassy bombing network identified ϕ as a significant factor. This is a result of the different and unique network topologies. The embassy network has high degree nodes and a more robust structure. This increased structure would

allow a well-informed attacker to quickly degrade the network by careful selection of critical nodes. Conversely, the hijacker network is relatively disperse with a structure that lacks critical nodes. This structure results in a network that remains equally robust against attackers of differing states of information. The hijacker network lacks critical nodes that can be exploited for quick degradation and thus requires prolonged attrition.

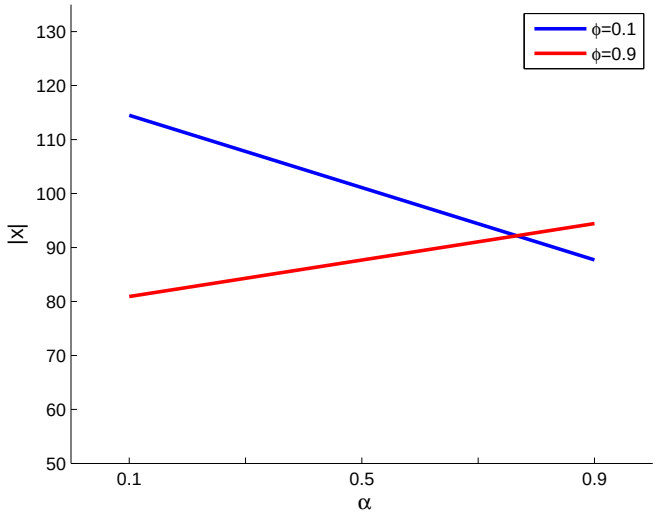

Figure 43. Interaction of θ and ϕ in the Embassy Bombing Network

The embassy network also identifies the interaction of ϕ and α as a significant factor. Given α at a low level, lower levels of ϕ result in a more successful attacker. Moreover, higher levels of α and ϕ result in a more successful attacker. Therefore, a defender facing a poorly informed attacker would do best to recruit using preferential attachment. Building new relationships with existing highly connected nodes would build a more robust network. However, random recruitment is preferable against a well-informed attacker. Randomly forming relationships within the existing network would spread the degree distribution evenly and not draw additional scrutiny upon highly connected nodes.

Attacker Strategy θ.

The interaction of α and θ is significant in both models, however each model specifies different groups of preferable attack strategies. These measures are grouped by significance, however each measure was evaluated individually within the simulation. The model differentiates the grouping $\{C^D\&C^P\&C^C - C^B\&C^L\&C^E\}$ in the hijacker network, with $\{C^D\&C^P\&C^C\}$ being the more effective measures. Likewise, $\{C^C\&C^E\&C^P\&C^D - C^L\&C^B\}$ are identified in the embassy bombing with $\{C^C\&C^E\&C^P\&C^D\}$ being the more effective measures. The primary difference between the groups is the inclusion of eigenvector centrality. This result demonstrates that the effectiveness of network measures as attack criteria depends upon network topology.

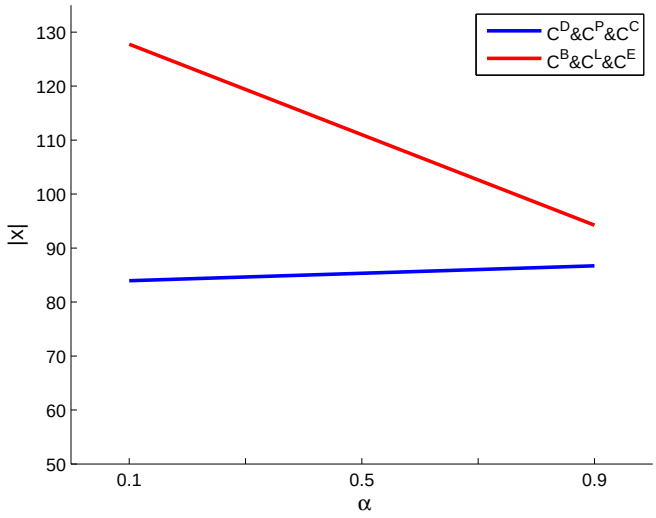

Figure 44. Interaction of θ and α in the Hijacker Network

As presented in Figure 44, given low levels of α, attack strategies using $\{C^B\&C^L\&C^E\}$ result in a higher ending component size in the hijacker network. Likewise, high levels of α and attack strategies $\{C^B\&C^L\&C^E\}$ result in a lower final component size. Attack strategies dependent upon $\{C^D\&C^P\&C^C\}$ do not significantly interact with

α, however they do dominate the other group of strategies by always resulting in a smaller ending component size. Figure 45 shows strategies $\{C^C \& C^E \& C^P \& C^D\}$ dominate across all levels of α in the embassy bombing network, however the measures do almost converge as $\alpha \to 1$.

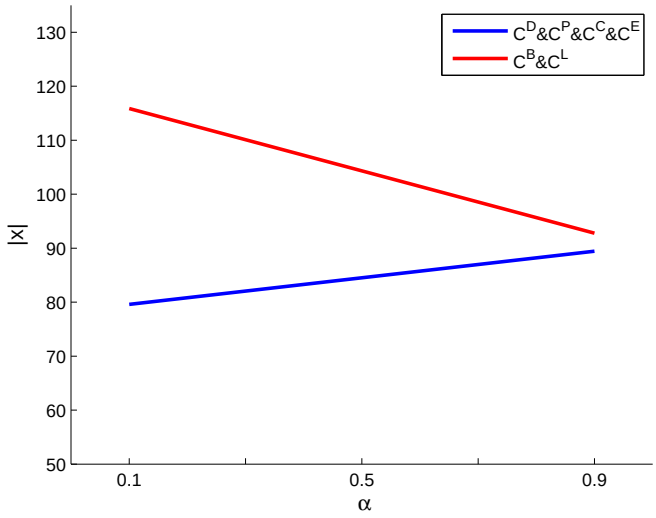

Figure 45. Interaction of θ and α in the Embassy Bombing Network

4.4 Conclusions

The effectiveness of select targeting criteria depends upon the defending network topology and regeneration method. Guzman *et al.* (2014) found that each uncorrelated measure captures a slightly different network phenomenon, and select measures appear to perform best as targeting criteria: degree centrality, proximal target centrality, and closeness centrality. Degree centrality describes the individuals with the most relationships, but fails to describe its relative importance or position within the network topology. Proximal target betweenness captures nodes by relative importance in terms of geodesics, giving insight into the importance of a node based upon position within network hierarchy. Closeness centrality captures the node's position relative to the entire network. Operational application of network targeting measures

should include a weighted multi-faceted approach to develop a clearer picture of the relationships within a defending network.

Betweenness centrality and the clustering coefficient prove to be poor targeting criteria. Both measures are heavily reliant upon knowledge of relationships throughout the entire defending network making them ill-suited for operational applications. Eigenvector centrality is effective only in the more robust embassy bombing network. Eigenvector centrality determines centrality based upon the relative importance of a node's neighbors. In sparse networks, such as the hijacker network, network topology and degree distribution fail to capture the relative importance of nodes. Eigenvector centrality should be applied with greater care given a defending network topology.

The simulation uses measures individually to test for significance and reduce computational requirements. However, the timeline of real-world operations allow for more detailed and thorough analysis. Analysts applying multiple network measures, given knowledge of their applicability within a network topology, can best describe complex network attributes and relationships.

The method of network regeneration significantly impacts the effectiveness of targeting criteria, however optimal measures always dominate. In operational application, any indication of regeneration method should be incorporated into the overall assessment of targeting effectiveness. Betweenness centrality and clustering coefficient perform significantly worse when a defender is regenerating through localized clusters. The measures appear to almost converge as regeneration becomes more random.

State of attacker information is significant within the more robust embassy bombing network, where relative importance can be determined by network topology. This network is indicative of most social networks where relative node importance is determined by relationships. Manufactured networks, such as the hijacker network, enforce a specific network organization to obscure relative importance. The unique structure

of the sparse hijacker network results in an organization difficult for the attacker to degrade despite information state. The sparse structure and relatively low degree distribution allows utility and operational capabilities to remain high despite continuous node removal.

The significant interaction of state of information and network regeneration demonstrates the importance of relationship structures to the defender. The defender prefers localized node connections against a poorly informed attacker. The localized connections greatly benefit network utility and grow a more robust structure. However, a defender facing a well-informed enemy benefits from randomly connecting new nodes. The erratic nature of random growth obscures network topology and decreases the effectiveness of targeting.

In application, an attacker should understand the importance of network regeneration on their information state. Truly random connections would be costly and difficult to coordinate for a defender, however simple social phenomenon may mimic this behavior. A new individual to a network may be assigned certain operational relationships, however dynamic social relationships create artificially random connections within the network. The new individual may have attended school with other members, or be distantly related to others. These complex social relationships, occurring outside the information state of almost any attacker, result in seemingly random defender behavior and negatively impact targeting effectiveness.

Improved modeling of complex social behaviors is accomplished through incorporation of the distance-based utility function. Although cost is identified as the most significant factor, the function allows a modeler significant flexibility in recreating certain player behavior. Balancing costs and risks versus the benefits of network participation better simulate an intuitive defender. Additionally, utility values can be weighted to model benefits inherit to network participation. For instance, members

of a highly idealistic or religiously fanatic network derive great benefit from organizational participation. Likewise, membership in certain elite military units bestows personal benefits far greater than those of simple network inclusion.

Although clique restructuring appears to be more effective, both methods of network restructuring are insignificant in the overall network. A defender who continuously recruits is best postured to withstand repeated attacks.

4.5 Limitations

Model defender networks are only analyzed under basic interpretations. In this application, the distance-based utility function is restricted to realizing benefit only from participation in a given network topology. This created a more parsimonious model, but failed to adequately model the cost and benefits realized by observed network members. Defender restructuring strategies are nested in current literature, but fail to incorporate more realistic and observed restructuring strategies. The simulation allows greater flexibility in capturing observed social phenomenon. Subject matter expert (SME) input should be incorporated to analyze and validate parameter levels given an observed network.

The attacker is limited in targeting criteria to analyze potentially optimal measures. However, the targeting process is best modeled as the value of multiple weighted measures. Weights can be analyzed through assessment of network topology and SME input. This results in a more valid representation of an attacking player's targeting criteria.

Resources constraints are not included as a model parameter. Intelligence processes are included in the model to allow the attacker to expand state of information, however these intelligence rates are not tied to a cost function. Any conclusions are trivial, as better intelligence logically leads to more effective targeting. Likewise, deci-

sion criteria do not include a weighted measure against resource constraints. Despite being a dynamic model, the lack of resource constraints limit the simulation's ability to infer significance of certain parameters.

V. Conclusions and Recommendations

The dynamic game on network topology presented in this study provides insight into optimal strategies for counterinsurgency forces. The model includes novel applications of utility functions and hybrid regeneration to better model an insurgency within complex social networks. The effective modeling of an insurgent force is paramount towards gaining insight into effective attacker strategies. Incorporation of uncorrelated network measures as targeting criteria enable analysis into their individual effectiveness for an attacking force. Attacker state of information is constrained to better model observed case studies, as well as provide insight into optimal strategies in differing phases of conflict. Furthermore, intelligence gathering processes are included to allow a dynamic expansion of the attacker's state of information.

This model can be incorporated into planning and operational cycles of a counterinsurgency operations. Model parameters can be fixed according to SME input, creating a defending network that is an approximate representation of specified insurgency forces. The players' action spaces can be adjusted according to the rules of engagement and operational tactics, techniques, and procedures. The model can then determine the optimal attack strategy and targeting network measures given the stated parameters. Tactical and operational decisions are frequently based upon a commander's state of information. Sensitivity analysis conducted on the model results indicate the significance of state of information on counterinsurgency operations.

The flexible structure of this model allows numerous enhancements to develop further insight into counterinsurgency operations or applications in different operational environments.

Understanding the optimal state of information for an action poses a significant challenge to any counterinsurgency commander. The addition of a cost or utility function to intelligence gathering activities would allow insights into the benefits of

these operations. Constantly gathering intelligence to expand states of information is a trivial conclusion. Likewise is the unrealistic expectation of a perfect state of information given a dynamic operational environment. Modeling the cost benefit of intelligence gathering would provide insight into understanding adequate information states given constraints and a specified insurgent force.

This study analyzes the effectiveness of individual network measures as attack criteria. However, weighting multiple measures to determine targeting priorities would more effectively model counterinsurgency forces. Each of the uncorrelated measures captures a unique facet of social networks. Additionally, the effectiveness of each measure is dependent upon attributes of the defender. Modeling these effects would provide insight into optimal strategies given a specified defending network. The weights from optimal model strategies could then be applied to operational counterinsurgency targeting.

The model presented in this study provides valuable insights into counterinsurgency operations, however arguably more important is the model's inherit flexibility. Minor enhancements can make the model relevant in evaluating almost any network-centric warfare application. Most compelling are the possible applications in the burgeoning field of cyber communications. Infectious diseases and computer virus outbreaks can be simulated given several enhancements to the basic model. These enhancements are structured loosely from the Susceptible-Infected-Susceptible (SIS) model in Jackson (2010). The defending player becomes the entire population with weighted relationships between nodes representing probability of infection between nodes. A certain proportion of nodes can be designated as immune to infection. The model includes a rate of recovery following infection, which can be a set parameter or random variate. An infection is introduced to the network, whereby attacker detection and strategy are analyzed. The model would provide insight into the cost and

benefits of detection and control of infections, as well as optimal strategies to target an infection within a given network.

Successful military operations will continue to rely upon an advanced understanding of relevant networks and their topologies. Flexible models, such as the one presented in this study, enable commanders to assess optimal strategies and operational effectiveness prior to commitment of military resources.

Appendix A. Storyboard

Bibliography

Adamic, Lada A. 1999. The small world web. *In: Research and Advanced Technology for Digital Libraries*. Springer.

Albert, Réka, & Barabási, Albert-László. 2002. Statistical mechanics of complex networks. *Reviews of modern physics*, **74**(1), 47.

Albert, Réka, Jeong, Hawoong, & Barabási, Albert-László. 1999. Internet: Diameter of the world-wide web. *Nature*, **401**(6749), 130–131.

Albert, Réka, Jeong, Hawoong, & Barabási, Albert-László. 2000. Error and attack tolerance of complex networks. *nature*, **406**(6794), 378–382.

Backstrom, Lars, Boldi, Paolo, Rosa, Marco, Ugander, Johan, & Vigna, Sebastiano. 2012. Four degrees of separation. *In: Proceedings of the 3rd Annual ACM Web Science Conference*.

Barabási, Albert-László, & Albert, Réka. 1999. Emergence of scaling in random networks. *science*, **286**(5439), 509–512.

Barabási, Albert-László, Albert, Réka, & Jeong, Hawoong. 2000. Scale-free characteristics of random networks: the topology of the world-wide web. *Physica A: Statistical Mechanics and its Applications*, **281**(1), 69–77.

Beauchamp, Murray A. 1965. An improved index of centrality. *Behavioral Science*, **10**(2), 161–163.

Bloch, Francis, & Jackson, Matthew O. 2007. The formation of networks with transfers among players. *Journal of Economic Theory*, **133**(1), 83–110.

Bonacich, Phillip. 1972. Factoring and weighting approaches to status scores and clique identification. *Journal of Mathematical Sociology*, **2**(1), 113–120.

Brandes, Ulrik. 2001. A faster algorithm for betweenness centrality. *Journal of Mathematical Sociology*, **25**(2), 163–177.

Brandes, Ulrik. 2008. On variants of shortest-path betweenness centrality and their generic computation. *Social Networks*, **30**(2), 136–145.

Bush, George W. 2002. *The national security strategy of the United States of America*. Tech. rept. DTIC Document.

Carley, Kathleen M. 2004. *Estimating vulnerabilities in large covert networks*. Tech. rept. DTIC Document.

Carley, Kathleen M, Dombroski, Matthew, Tsvetovat, Maksim, Reminga, Jeffrey, Kamneva, Natasha, *et al.* 2003. Destabilizing dynamic covert networks. *In: Proceedings of the 8th international Command and Control Research and Technology Symposium*.

Chaum, David. 1988. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, **1**(1), 65–75.

Cohen, Reuven, Erez, Keren, Ben-Avraham, Daniel, & Havlin, Shlomo. 2000. Resilience of the Internet to random breakdowns. *Physical Review Letters*, **85**(21), 4626.

Coleman, James Samuel, Katz, Elihu, Menzel, Herbert, *et al.* 1966. *Medical innovation: A diffusion study*. Bobbs-Merrill Company Indianapolis.

Committee on Network Science for Future Army Applications, National Research Council. 2005. *Network Science*. National Academies Press.

Davis, Allison, Gardner, Burleigh Bradford, & Gardner, Mary R. 1969. *Deep south*. University of Chicago Press.

de Solla Price, Derek J. 1965. Networks of Scientific Papers. *Science*, **149**(3683), 510–515.

Domingo-Ferrer, Josep, & González-Nicolás, Úrsula. 2011. Decapitation of networks with and without weights and direction: The economics of iterated attack and defense. *Computer Networks*, **55**(1), 119–130.

Erdös, Paul, & Rényi, Alfred. 1959. On Random Graphs, I. *Publicationes Mathematicae*, **6**, 290–297.

Freeman, Linton C. 1977. A set of measures of centrality based on betweenness. *Sociometry*, 35–41.

Freeman, Linton C. 1979. Centrality in social networks conceptual clarification. *Social Networks*, **1**(3), 215–239.

Geffre, Jennifer L. 2007. *A layered social and operational network analysis*. Tech. rept. DTIC Document.

Geffre, Jennifer L, Deckro, Richard F, & Knighton, Shane A. 2009. Determining critical members of layered operational terrorist networks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*.

Glaeser, Edward L, Sacerdote, Bruce, & Scheinkman, Jose A. 1995. *Crime and social interactions*. Tech. rept. National Bureau of Economic Research.

Goyal, Sanjeev, Van Der Leij, Marco J, & Moraga-González, José Luis. 2006. Economics: An emerging small world. *Journal of Political Economy*, **114**(2), 403–412.

Guare, John. 1990. *Six degrees of separation: A play*. Random House LLC.

Guzman, Joshua D., Deckro, Richard F., Robbins, Matthew J., Morris, James F., & Ballester, Nicholas A. 2014. An Analytical Comparison of Social Network Measures. *Computational Social Systems, IEEE Transactions on*, **1**(1), 35–45.

Holme, Petter, Kim, Beom Jun, Yoon, Chang No, & Han, Seung Kee. 2002. Attack vulnerability of complex networks. *Physical Review E*, **65**(5), 056109.

Ioannides, Yannis M, & Loury, Linda Datcher. 2004. Job information networks, neighborhood effects, and inequality. *Journal of Economic Literature*, 1056–1093.

Jackson, Matthew O. 2010. *Social and economic networks*. Princeton University Press.

Jackson, Matthew O, & Wolinsky, Asher. 1996. A strategic model of social and economic networks. *Journal of Economic Theory*, **71**(1), 44–74.

Kim, Hyoungshick, & Anderson, Ross. 2013. An experimental evaluation of robustness of networks. *IEEE Systems Journal*, **7**(2), 179–188.

Krebs, Valdis E. 2002. Mapping networks of terrorist cells. *Connections*, **24**(3), 43–52.

Kullback, Solomon, & Leibler, Richard A. 1951. On information and sufficiency. *The Annals of Mathematical Statistics*, 79–86.

Lewis, Ted G. 2011. *Network science: Theory and applications*. John Wiley & Sons.

Lin, Frank Yeong-Sung, Wang, Yu-Shun, Wu, Yu-Pu, & Hsu, Chia-Yang. 2012a. Effective Network Defense Strategies against Malicious Attacks with Various Defense Mechanisms under Quality of Service Constraints. *Pages 165–170 of: Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. IEEE.

Lin, Frank Yeong-Sung, Wang, Yu-Shun, Chung, Hui-Yu, & Pan, Jia-Ling. 2012b. Maximization of Network Survivability under Malicious and Epidemic Attacks. *Pages 412–417 of: Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. IEEE.

Milgram, Stanley. 1967. The small world problem. *Psychology Today*, **2**(1), 60–67.

Miller, Eric A. 2013. *A Network Analysis of Social Balance in Conflict in the Maghreb*. Tech. rept. DTIC Document.

Montgomery, Douglas C. 2008. *Design and analysis of experiments*. John Wiley & Sons.

Morris, James F, O'Neal, Jerome W, & Deckro, Richard F. 2013. A random graph generation algorithm for the analysis of social networks. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 1548512912450370.

Nagaraja, Shishir, & Anderson, Ross. 2008. Dynamic topologies for robust scale-free networks. *In: Bio-Inspired Computing and Communication*. Springer.

Newman, Mark EJ. 2001. Scientific collaboration networks. I. Network construction and fundamental results. *Physical review E*, **64**(1), 016131.

Obama, Barack. 2011. *National Strategy for Counterterrorism*. Tech. rept. DTIC Document.

Rees, Albert. 1966. Information networks in labor markets. *The American Economic Review*, 559–566.

Reiss Jr, Albert J. 1988. Co-offending and criminal careers. *Crime and justice*, 117–170.

Ryan, Bryce, & Gross, Neal Crasilneck. 1950. *Acceptance and diffusion of hybrid corn seed in two Iowa communities*. Vol. 372. Agricultural Experiment Station, Iowa State College of Agriculture and Mechanic Arts.

Travers, Jeffrey, & Milgram, Stanley. 1969. An experimental study of the small world problem. *Sociometry*, 425–443.

U.S. Army. 2014. FM 3-24 Insurgencies and Countering Insurgencies. *Washington, DC: Headquarters of the Army*.

U.S. Joint Chiefs of Staff. 2009. JP 3-26 Counterterrorism. *Washington DC: Joint Chiefs of Staff*.

U.S. Joint Chiefs of Staff. 2011. JP 3-0 Joint Operations. *Washington DC: Joint Chiefs of Staff*.

U.S. Joint Chiefs of Staff. 2013. JP 2-0 Joint Intelligence. *Washington DC: Joint Chiefs of Staff*.

Watts, Duncan J, & Strogatz, Steven H. 1998. Collective dynamics of 'small-world' networks. *Nature*, **393**(6684), 440–442.

Zhao, Liang, Park, Kwangho, & Lai, Ying-Cheng. 2004. Attack vulnerability of scale-free networks due to cascading breakdown. *Physical Review E*, **70**(3), 035101.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
26–03–2015	Master's Thesis	Oct 2013 — Mar 2015

4. TITLE AND SUBTITLE

A Dynamic Game on Network Topology
for Counterinsurgency Applications

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Nystrom, Jared K., Major, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/ENS)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENS-MS-15-M-144

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

August G. "Greg" Jannarone
Deputy Chief, Strategic Plans Division/SOCOM-J51 Leader, HQ USSOCOM
RED TEAM United States Special Operations Command
7701 Tampa Point Blvd
MacDill AFB, FL 33621-5323
Email: august.jannarone@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

HQ USSOCOM

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A.
Approved for Public Release; distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Successful military operations are increasingly reliant upon an advanced understanding of relevant networks and their topologies. The methodologies of network science are uniquely suited to inform senior military commanders; however, there is a lack of research in the application of these methods in a realistic military scenario. This study creates a dynamic game on network topology to provide insight into the effectiveness of offensive targeting strategies determined by various centrality measures given limited states of information and varying network topologies. Improved modeling of complex social behaviors is accomplished through incorporation of a distance-based utility function. Moreover, insights into effective defensive strategies are gained through incorporation of a hybrid model of network regeneration. Model functions and parameters are thoroughly presented, followed by a detailed sensitivity analysis of factors. Two designed experiments fully investigate the significance of factor main effects and two-factor interactions. Results show select targeting criteria utilizing uncorrelated network measures are found to outperform others given varying network topologies and defensive regeneration methods. Furthermore, the attacker state of information is only significant given certain defending network topologies. The costs of direct relationships significantly impact optimal methods of regeneration, whereas restructuring methods are insignificant. Model applications are presented and discussed.

15. SUBJECT TERMS

Dynamic Game; Network Topology; Counterinsurgency; Targeting

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Lt Col Matthew J. Robbins, PhD (ENS)
U	U	U	UU	103	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636 x4539 matthew.robbins@afit.edu