NET Institute*

www.NETinst.org

Working Paper #12-25

September 2012

Defending a Star: Coordinating the Defense of a Network

Kory M. Garner
Purdue University
Department of Economics

* The Networks, Electronic Commerce, and Telecommunications ("NET") Institute, http://www.NETinst.org, is a non-profit institution devoted to research on network industries, electronic commerce, telecommunications, the Internet, "virtual networks" comprised of computers that share the same technical standard or operating system, and on network issues in general.

Defending a Star: Coordinating the Defense of a Network*†

Kory M. Garner‡

October 19, 2012

Abstract

This experiment focuses on a contest played over a star network of 6 nodes. By placing targets in a network, the value of a target is dependent on its connectivity to other targets. The experiment compares the cases where the defense is centrally planned by a defense planner with a case where the defense is coordinated by six individuals each placed at one node in the network. By additionally varying how many targets the attacker may target, the experimental design consists of a 2×2 design. Attackers tend to over exert effort on the Center Node whereas defenders tend to place too little effort on the Center Node (with one exception). These attack and defense allocations lead to defenders earning smaller than equilibrium profits (again with one exception). It appears that Defense Planners manage to plan a defense better than the Coordinated Defenders when facing an attacker who may only target one node. However, Defense Planners are not certain to perform better than Coordinated Defenders as the Planner earns a smaller profit on average (but is less volatile in his earnings).

1 Introduction

With the recent advent of cyber terrorism, corporations are struggling to maintain secure systems which allow for continued e-commerce. Forming in 2003, the group of "hacktivists" called Anonymous gained notoriety in 2010 due to "Operation Payback." The initial purpose of this operation was to target corporations that were in favor of anti-piracy law enforcement, however it was transformed into a payback venture against the companies which pulled support from WikiLeaks and its founder Julian Assange. This group managed to completely take

*I thank the NET Institute www.NETinst.org for financial support

†This is a working paper. Please do not cite. Data work is preliminary and further experimental sessions may be run.

‡Department of Economics, Purdue University, West Lafayette, IN 47907, USA

down websites for Visa and MasterCard while slowing service for PayPal. Some have even blamed Anonymous for the PlayStation Network outage in 2011 which lasted 24 days and cost Sony Corporation $171 million. Properly defending a network is not something which should be taken lightly. Cyber terrorists exist and a successful attack against a corporation can result in significant losses, both monetary and in the corporation's reputation.

Defending a network against a potential terrorist attack can be modeled as an economic contest. Colonel Blotto games have separate battlefields which players attempt to win by expending their limited resources for attack and defense. Roberson (2006)[9] solves the general form of the Colonel Blotto game, but does follow with Friedman (1958)[6] which shows that, under a lottery contest success function, equivalently valued battlefields are to be treated equivalently in equilibrium allocation of attack/defense resources.

The battlefields in Colonel Blotto games are assumed to have an exogenously determined value and are not connected to one another in any way. As Goyal and Vigier (2012) discuss, however, a clear example of Cyber Terrorism shows that often battlefields are interconnected in a network framework. They go on to develop a model for a network contest with contagion. The model proceeds in two stages. In the first stage, a central planner decides upon a formation for a network of targets. In the second stage, the planner is endowed with a non-valuable defense budget. The defender chooses a strategy, then an outside attacker is endowed with his own attack budget perfectly observes the network and defense strategy chose by the planner. The attacker wins a node following a modified Lottery Contest Success Function. If a node is won by the attacker it is removed from the network and the attack spreads along the links with contagion. The final profit of the planner is the value of the resultant subnetwork whereas the attacker is rewarded with whatever value was lost by the planner. The goal of the attacker is to create as much disruption as possible in the network, whereas the planner wishes to maintain communication pathways. They find that, under a certain parameter space, a star network is the most robust. Here robust is a concept introduced by Albert, Jeong and Barabasi (2000)[1] who ran simulation experiments to show

that exponential networks are vulnerable to an outside attack. An exponential network is one where there are few centrally located nodes and many peripherally located nodes.

This paper will follows a similar game as described in Goyal and Vigier (2012) with changes in a few of the assumptions. In particular, there are four changes, most of which are minor. The first alteration is the skipping of the first stage. Instead of having subjects play a Network Formation game followed by a Network Contest game (and potentially arriving at utter confusion on the part of the subjects), no Network Formation stage occurs and an exogenously determined network is given to the subjects. In particular, we will assume a Star Network with six total nodes (five periphery nodes and a Center Node). The second alteration from the model is the use of a standard Lottery Contest Success Function as opposed to the modified version used in Goyal and Vigier. The third change is the largest. No possibility of contagion is present in this game, so an attacker may only win a node if he directly attacks that node. The final change is in the assumption of sequential moves. In the previous model, the attacker moved after the defender. In this paper, both entities will make their decisions simultaneously. This may seem like a significant assumption however the equilibrium in this model does not change if we assumed sequential move.

This paper will use the Goyal and Vigier (2012) model with the alterations described above as a baseline treatment. From this point a 2×2 experimental design will unfold. One potential way to analyze robust networks is through Cyber Terrorism, however there is also significant literature on Transnational Terrorism.

A common assumption to Transnational Terrorism (such as in Powell, 2007a and 2007b) is that an attacker may only target one battlefield at a time (perhaps due to a high fixed cost for each battlefield targeted). While the assumption of single target attack is realistic for Transnational Terrorism, Cyber Terrorists, however, are able to target many sites simultaneously. Using a strategy called Distributed Denial of Service (DDoS), Cyber Terrorists can rapidly target websites shutting them down for long periods of time. Not only will the company which owns the website suffer, but anyone who uses the website to conduct business

will also suffer due to the lost communication pathway. So this paper will vary the quality of the attacker in whether he is able to attack as many nodes in the network as he wishes (Cyber Terrorism) or is limited to being able to only attack one (Transnational Terrorism).

We also vary the quality of how the defense is organized. In the baseline treatment, there is a Defense Planner who coordinates the defense for every node in the network. She is endowed with the total sum of the defense budget and splits it among the nodes. A possibly more realistic scenario is, instead of having a defense planner, having Coordinated Defense. In treatments with Coordinated Defense, a subject will take charge of a single node in the network and she will win only the earnings at her node. There are six nodes and six individuals who must coordinate the defensive strategy of the network. To the best of the author's knowledge, this is the first paper to approach a contest as a coordination game for the defense.

While this paper does introduce various new concepts, they are strikingly similar to recently discussed versions of contests. Having a Coordinated Defense is similar to the idea that "The enemy of my enemy is my friend" as discussed in Rietzke and Roberson (2012)[8]. Additionally, while little work has been done on network contests, Kovenock and Roberson (2012)[7] discuss weakest link networks. A weak link in a network is one where, if the attacker wins that node, the attacker wins the entire value of the network. In a Star Network, the Center Node is a weakest link. If the Center Node is removed from the network, then no node is able to communicate with any other node.

Given the experimental environment, our results will be compared with other experiments on contests. Bull, Schotter and Weigelt (1987)[2], Ehrenberg and Bognanna (1990)[5], and many others show that there is a small correlation between effort exerted to win a contest and the size of the prize. Specifically, too much effort is placed on larger prizes whereas not enough effort is placed on smaller prizes. If prizes are equivalent in size, however, Chowdhury, Kovenock and Sheremeta (2012)[3] show that under a Lottery Contest Success Function subjects recognize that the values are the same and equal effort should be placed on

all prizes. We find little support for the over exertion of effort on the larger prize (the Center Node), but significant evidence that subjects recognize the equivalence of the periphery nodes.

The main results in the paper suggest that, in all treatments, there is a movement toward equilibrium. This movement is more noticeable in Cyber Terrorism treatments than in Transnational Terrorism treatments. Not surprisingly, Defense Planners perform significantly better than Coordinated Defenders when facing a Transnational Terrorist. Yet, when facing a Cyber Terrorist, Coordinated Defenders outperform Defense Planners.

2 Model and Theoretical Predictions

2.1 Network Theory Background

Let $\mathcal{N} = \{1, 2, \ \dots \ , n\}$ be a set of nodes. Let g be a graph which consists of the set of nodes and a set of links. Two nodes $i, j \in \mathcal{N}$ are linked if $ij \in g$. If $ij \notin g$ then no link exists between nodes i and j. We will assume a simply-connected network with non-directed information transfer. Additionally, $g{-}ij$ is the graph g removing link ij and $g{+}ij$ is the graph g adding link ij. Let the value of a graph, g, be defined by the function $v : \{g \mid g \subset g^N\} \rightarrow \mathbb{R}$ where g^N denotes the complete graph.

In the vein of Jackson and Wolinsky (1996) and Bala and Goyal (2000), the value of the network is assumed separable by node following a Balanced Allocation Rule: $\forall i = 1, \dots, n \ \exists \mathcal{U}_i : \{g \mid g \subset g^N\} \rightarrow \mathbb{R}$ such that $v(g) = \sum_{i=1}^{n} \mathcal{U}_i(g)$ where $\mathcal{U}_i(g)$ is the value of node i given network g. In addition, we assume that the utility functions $\mathcal{U}_i(g)$ are separable between benefits, $u_i(g)$, and costs, $c_i(g)$. Thus $\forall i = 1, \dots, n \ \exists \, u_i : \{g \mid g \subset g^N\} \rightarrow \mathbb{R}_+$ and $\exists \, c_i : \{g \mid g \subset g^N\} \rightarrow \mathbb{R}_+$ such that $\mathcal{U}_i = u_i(g) - c_i(g)$.

2.2 The Network Contest

Disregarding a stage for Network Formation we assume a network, g, is exogenously given. Since the network is exogenously given we will make a final assumption that the standard

costs of the network formation are not paid, i.e. $c_i(g) = 0 \ \forall i, g$. Therefore the value of the network is $v(g) = \sum_{i=1}^{n} \mathcal{U}_i(g) = \sum_{i=1}^{n} u_i(g)$.

Attackers of the network are endowed with total budget A and defenders of the network are endowed with total budget D. Both attackers and defenders have complete information regarding the network g and the size of the budgets A and D. At this point, attackers and defenders split their resources across the nodes in $\mathcal{N}$. The attack and defense budgets are assumed to have no value if left unused.

Both attacker and defender choose effort levels at each node subject to their budget constraints. Let a_i be the total level of attack at node i and let d_i be the total level of defense at node i. Let $p(a_i, d_i)$ denote the probability that the attacker wins node i given a_i and d_i.

If the attacker wins node i, then i and any link containing i as an endpoint are removed from the network. If $ij \in g$ and the defender wins both i and j, then i, j and ij all remain in the network. Let $\mathcal{R} = \{i_1, \ \dots \ , i_{n_1}\}$ be the nodes removed from the network, the resultant subnetwork is denoted by $g'_{\mathcal{R}}$. The final profit for the attacker is denoted by $\Pi_{\mathcal{A}}$. The final profit for node i is denoted by $\Pi_{\mathcal{D}_i}$ and the final profit for the network is $\Pi_{\mathcal{D}} = \sum_{i=1}^{n} \Pi_{\mathcal{D}_i}$.

In the final subnetwork, the defender's profit at each node is equal to the value of the node in the subnetwork. The attacker's profit is equal to the profit that was lost by the defender. Thus we have,

$$\begin{aligned} \Pi_{\mathcal{D}_i}(g) &= u_i(g'_{\mathcal{R}}) \\ \Pi_{\mathcal{A}}(g) &= \sum_{i=1}^{n} u_i(g) - u_i(g'_{\mathcal{R}}). \end{aligned}$$

The game is a constant-sum contest where the total value of the contest is the initial value of the network $v(g) = \sum_{i=1}^{n} u_i(g)$.

2.3 Defender and Attacker Profits in Four Cases

In this paper, we consider four treatments in the experiment. The four treatments result by varying a quality in both the attacker and defender. This results in a 2×2 experimental design.

For the attacker, the varied quality is the number of nodes he is allowed to target at one time. A common assumption in political science and economic models on Transnational Terrorism is to assume that the attacker may only target one node at a time, such as in Powell (2007). One can logically validate this assumption by recognizing that transnational terrorists face difficulties targeting multiple sites due to large fixed costs associated with launching such an attack. However, as mentioned in Goyal and Vigier (2012), Cyber Terrorism faces no such limitation and cyber terrorists frequently target multiple sites during one attack. This paper will refer to these treatments as Transnational Terrorism (TT) and Cyber Terrorism (CT).

Defenders face no limitation on how many of the nodes may be defended at one time (outside of the restriction of the budget constraint). Instead, the defense varies depending on how it is allocated. In most multi-battle tullock contests there is but a single Defense Planner who plans the defense for every site. However this game's design lends itself to multiple entities that plan a Coordinated Defense. In this case, each node represents its own entity which earns only the profit at its own node leading to choices made based on self-interest rather than the group-interest as a whole. These treatments are refered to as Defense Planner (DP) and Coordinated Defense (CD).

We will now define the problem faced by the attacker and defender(s) under each of the four treatments. Before we move on, however, we must mathematically clarify what has changed from the base model. In the TT treatments, attackers may only target one node at a time. Since the budgets are assumed to have no value, neither the attacker nor the defender has any incentive to not allocate the entire budget. Thus $\forall i = 1, \dots, n$ $a_i \in \{0, A\}$ and if $a_i = A$ then $\forall j \neq i$ $a_j = 0$ and the attacker is no longer deciding the

level of attack. Instead, he attacks node i with full force with probability α_i. In the CD treatments, defenders now only receive part of the total defense. Defender k is endowed with budget D_k where $\sum_{k=1}^{n} D_k = D$ and allocates d_{k_i} of his budget to node i. Thus the total level of defense at node i is $\sum_{k=1}^{n} d_{k_i} = d_i$.

2.3.1 Defense Planner with Cyber Terrorism (DP - CT)

The Defense Planner solves

$$\max_{\{d_i\}_{i=1}^{n}} \left[\mathrm{E}\left[\Pi_{\mathcal{D}}\right] = \sum_{i=1}^{n} \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \;\middle|\; \forall i = 1, \ \ldots \ , n \ d_i \geq 0, \sum_{i=1}^{n} d_i \leq D \right]$$

and the Cyber Terrorist attacker solves

$$\max_{\{a_i\}_{i=1}^{n}} \left[\mathrm{E}\left[\Pi_{\mathcal{A}}\right] = \sum_{i=1}^{n} u_i(g) - \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \;\middle|\; \forall i = 1, \ \ldots \ , n \ a_i \geq 0, \sum_{i=1}^{n} a_i \leq A \right]$$

where

$$\mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] = \sum_{\mathcal{R} \in 2^{\mathcal{N}}} \left[\prod_{j \in \mathcal{R}} p(a_j, d_j) \right] \left[\prod_{j \notin \mathcal{R}} \left[1 - p(a_j, d_j)\right] \right] u_i(g'_{\mathcal{R}}).$$

2.3.2 Defense Planner with Transnational Terrorism (DP - TT)

The Defense Planner solves

$$\max_{\{d_i\}_{i=1}^{n}} \left[\mathrm{E}\left[\Pi_{\mathcal{D}}\right] = \sum_{i=1}^{n} \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \;\middle|\; \forall i = 1, \ \ldots \ , n \ d_i \geq 0, \sum_{i=1}^{n} d_i \leq D \right]$$

and the Transnational Terrorist attacker solves

$$\max_{\{\alpha_i\}_{i=1}^{n}} \left[\mathrm{E}\left[\Pi_{\mathcal{A}}\right] = \sum_{i=1}^{n} u_i(g) - \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \;\middle|\; \forall i = 1, \ \ldots \ , n \ \alpha_i \geq 0, \sum_{i=1}^{n} \alpha_i = 1 \right]$$

where

$$\Pi_{\mathcal{D}_i} = \sum_{j=1}^{n} \alpha_j \left[\left(1 - p_j(d_j)\right) u_i(g) + p_j(d_j) u_i(g'_j) \right].$$

2.3.3 Coordinated Defense with Cyber Terrorism (CD - CT)

When there is Coordinated Defense, defender k solves

$$\max_{\{d_{k_i}\}_{i=1}^n} \left[\mathrm{E}\left[\Pi_{\mathcal{D}_k}\right] \,\middle|\, \forall i = 1,\ \ldots\ , n\ d_{k_i} \geq 0, \sum_{i=1}^n d_{k_i} \leq D_k \right]$$

and the Cyber Terrorist attacker solves

$$\max_{\{a_i\}_{i=1}^n} \left[\mathrm{E}\left[\Pi_{\mathcal{A}}\right] = \sum_{i=1}^n u_i(g) - \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \,\middle|\, \forall i = 1,\ \ldots\ , n\ a_i \geq 0, \sum_{i=1}^n a_i \leq A \right]$$

where

$$\mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] = \sum_{\mathcal{R} \in 2^{\mathcal{N}}} \left[\prod_{j \in \mathcal{R}} p(a_j, d_j) \right] \left[\prod_{j \notin \mathcal{R}} \left[1 - p(a_j, d_j)\right] \right] u_i(g'_{\mathcal{R}}).$$

2.3.4 Coordinated Defense with Transnational Terrorism (CD - TT)

When there is Coordinated Defense, defender k solves

$$\max_{\{d_{k_i}\}_{i=1}^n} \left[\mathrm{E}\left[\Pi_{\mathcal{D}_k}\right] \,\middle|\, \forall i = 1,\ \ldots\ , n\ d_{k_i} \geq 0, \sum_{i=1}^n d_{k_i} \leq D_k \right]$$

and the Transnational Terrorist attacker solves

$$\max_{\{\alpha_i\}_{i=1}^n} \left[\mathrm{E}\left[\Pi_{\mathcal{A}}\right] = \sum_{i=1}^n u_i(g) - \mathrm{E}\left[\Pi_{\mathcal{D}_i}\right] \,\middle|\, \forall i = 1,\ \ldots\ , n\ \alpha_i \geq 0, \sum_{i=1}^n \alpha_i = 1 \right]$$

where

$$\Pi_{\mathcal{D}_i} = \sum_{j=1}^n \alpha_j \left[\left(1 - p_j(d_j)\right) u_i(g) + p_j(d_j) u_i(g'_j) \right].$$

2.4 Parameters used in Experiment

In order to test the model in the lab we will choose simple parameters in order to develop simple theoretical predictions. To begin, the network g chosen for this experiment is, as the title suggests, a Star Network with six nodes. The center node is labeled C and the periphery

nodes are labeled $1, 2, 3, 4, 5$. Star Networks have been the focus of recent literature in social networks as Star Network structures are commonly seen in various networks. We will be looking at the robustness of Star Networks to an outside attack. Note that in a Star network periphery nodes are symmetric to one another, but the Center Node is far more valuable. In particular, if the attacker successfully destroys the Center Node then he wins all profits from the Network (or, put another the way, the defender must successfully defend the center node in order to maintain any of the profit).

The value of a node in the network is 100∗(the number of other nodes it is connected to). Note that this does not require a direct connection to another node, a node will receive value from a node it is indirectly connected to. Additionally note that at the start of a round the value of each node in the network is $100 * 5 = 500$. This formation for the value of a node is fundamentally that discussed in Jackson and Wolinsky (1996) defined by the parameters w, δ and c. In this experiment, $w = 100$, $\delta = 1 - \epsilon$ and $c = 0$.

The attacker's budget is $A = 40$ and the total defense budget is $D = 120$. In the Coordinated Defense treatments, each defender receives an equal split of the inital endowment, $\forall k = 1, \ldots, n \; D_k = 20$. The assumption that $A < D$ is common to multi-battle tullock contests with an attacker. Finally, the probability that the attacker wins a node follows a Lottery Contest Success Function $p(a_i, d_i) = \frac{a_i}{a_i + d_i}$.

2.5 Theoretical Predictions

Table 1 above lists all of the variables we will need for equilibrium analysis. One thing to note about the above variables is that d_i, a_i, α_i and $\Pi_{\mathcal{D}_i}$ are associated with all of the periphery nodes. In star networks, the periphery nodes are symmetric, thus, in the contest equilibrium, the periphery nodes are symmetric with respect to the attack and defense efforts placed on the nodes.

Table 2 lists the equilibrium allocations and profits for all players in all treatments.[1] Again note that, in all treatments, both attackers and defenders treat the periphery nodes

[1]See the Appendix for proofs associated with the numbers in Table 2.

Table 1: List of Variables used

Variable		Description
d_C	=	Total Defense on Node C
d_i	=	Total Defense on Node i, $i = 1, \ldots, 5$
a_C	=	In CT Treatments, Total Attack on Node C
a_i	=	In CT Treatments, Total Attack on Node i, $i = 1, \ldots, 5$
α_C	=	In TT Treatments, Probability of an Attack on Node C
α_i	=	In TT Treatments, Probability of an Attack on Node i, $i = 1, \ldots, 5$
$\Pi_{\mathcal{D}}$	=	Total Profit for the Defender
$\Pi_{\mathcal{D}_C}$	=	Profit for the Defender at Node C
$\Pi_{\mathcal{D}_i}$	=	Profit for the Defender at Node i, $i = 1, \ldots, 5$
$\Pi_{\mathcal{A}}$	=	Total Profit for the Attacker

Table 2: Equilibrium Allocations and Profits in each Treatment

Treatment	$d_C^\star$	$d_i^\star$	$a_C^\star$	$a_i^\star$	$\alpha_C^\star$	$\alpha_i^\star$	$\Pi_{\mathcal{D}}^\star$	$\Pi_{\mathcal{D}_C}^\star$	$\Pi_{\mathcal{D}_i}^\star$	$\Pi_{\mathcal{A}}^\star$
DP – CT	46.15	14.77	15.40	4.92	–	–	1406.25	281.22	225.01	1593.75
CD – CT	45.50	14.90	16.00	4.80	–	–	1406.00	279.75	225.25	1594.00
DP – TT	95.00	5.00	–	–	$\frac{1}{6}$	$\frac{1}{6}$	2111.11	401.23	341.96	888.89
CD – TT	95.00	5.00	–	–	$\frac{1}{6}$	$\frac{1}{6}$	2111.11	401.23	341.96	888.89

as symmetric in equilibrium. The determining factor in differences in the equilibrium across treatments is whether the attacker is a transnational terrorist or cyber terrorist. There is little to no change between the DP and CD treatments, however $\Pi_{\mathcal{D}}^\star$ in TT treatments is significantly larger than $\Pi_{\mathcal{D}}^\star$ in CT treatments. In TT treatments, we restrict the play of the attacker, so the attacker must do at least as well in the CT treatments. Since the restriction placed on attackers in the TT treatments is stifling, the defenders are able to maintain a much larger chunk of the network profits.

Regardless of whether the defense is allocated by a Defense Planner of Coordinated, equilibrium allocations under the case of Transnational Terrorism are equivalent. This means that in the Coordinated Defense, self-interest does not get in the way of the group's interest. Coordination errors, however, may still exist. The most obvious method of reaching equilibrium is for each periphery node to keep 5 units at their own node and give 15 units to the Center node (and the Center node keeps all of her units of defense), but this is not the only way to reach the equilibrium allocation.

There are difference in the equilibrium between the DP - CT and CD - CT treatments, however the differences are exceptionally small. In equilibrium, the Defense Planner places more effort on the center node than what is placed on the center node in Coordinated Defense. When defense is coordinated, the periphery nodes try to maximize their own profit leading them to hold more of the defensive units for themselves. The periphery nodes' profit does increase (i.e. $(\Pi_{\mathcal{D}_i}^{\text{CD - CT}})^\star > (\Pi_{\mathcal{D}_i}^{\text{DP - CT}})^\star$), but this is at the cost of the center node's profit and the profit of the network as a whole (i.e. $(\Pi_{\mathcal{D}_C}^{\text{CD - CT}})^\star < (\Pi_{\mathcal{D}_C}^{\text{DP - CT}})^\star$ and $(\Pi_{\mathcal{D}}^{\text{CD - CT}})^\star < (\Pi_{\mathcal{D}}^{\text{DP - CT}})^\star$). The differences in profit are small but still exist. Thus, while TT treatments experience only coordination errors, the CT treatments face coordination errors and self-interest conflicting with the group's interest.

3 Experimental Design

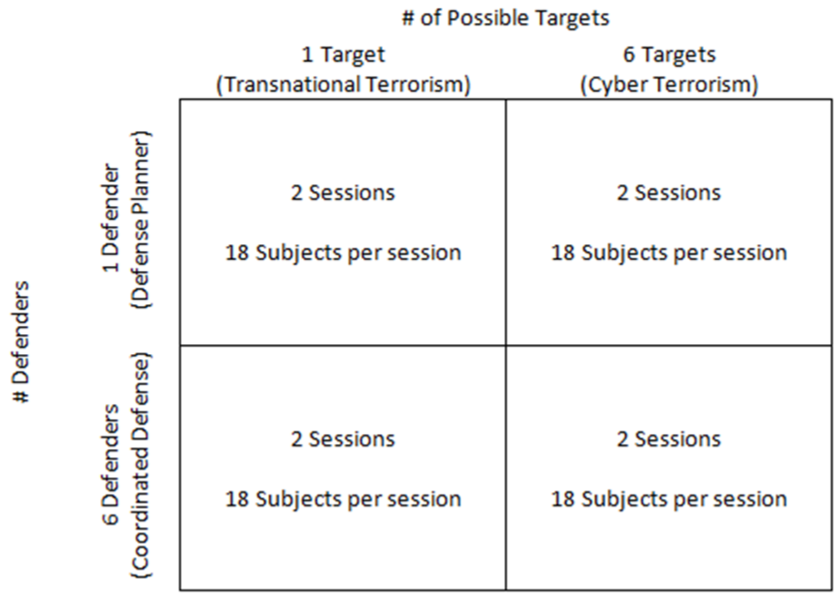
3.1 Procedures

The experiment was conducted at the Vernon Smith Experimental Economics Laboratory at Purdue University. A total of 144 subjects participated in 8 sessions with 18 subjects per session (see Figure 1). Sessions were conducted during the Fall semester 2012.

The experiment consisted of four treatments. As outlined previously, the defense quality was varied between Defense Planner and Coordinated Defense and the attack quality was varied between Transnational Terrorism and Cyber Terrorism. This leads to 2×2 design (as indicated in Figure 1). The experiment was conducted using a between-subject design. Some subjects had participated in other experiments, but none had participated in similar experiments.

The computerized experimental sessions used zTree (Fischbacher, 2007). Each session proceeded in four parts. At the beginning of each part, instructions were given to the subjects and read aloud. After the instructions were read, subjects took a paid quiz over the instructions. Upon completion of the quiz, subjects participated in 30 rounds of the network contest in one of the four treatments. Of the 30 rounds, only 6 were paid and these rounds

Figure 1: Experimental Design



were randomly selected at the end of the session. After the network contest we elicited the subject's attitudes on risk (Holt and Laury, 2002) and envy (Bolton and Ockenfels, 2009). Subjects spent 90 - 120 minutes in the lab and earned an average of $26.30. Subjects also completed a demographic questionnaire at the end of each session.

In Defense Planner treatments, there were nine (9) networks defended by nine Defense Planners paired one-to-one with nine attackers every period for thirty (30) periods. Thus, a total of 270 networks are observed with 270 defense allocations and 270 attack allocations in each session. In Coordinated Defense treatments, twelve (12) subjects were split between two (2) networks which were paired one-to-three with six (6) attackers each period for thirty periods. In Coordinated Defense treatments, three of the attackers were paired with one network while the other three were paired with the other, the defenders only saw the outcome of one of the attackers, but each attacker saw their own outcome. Thus, a total of 60 networks are observed with 60 total defense allocations and 180 attack allocations in each session.

Subjects in all sessions acted as both a defender and attacker over the course of the session. Subjects in DP treatments acted as a defender for exactly 15 periods and an attacker for exactly 15 periods. Subjects in CD treatments acted as a defender for exactly 20 periods

and an attacker for exactly 10 periods.

Instead of referring to the subjects as "attackers" "defenders," neutral framing was used by instead calling them circle types and square types.[2] All subjects played both roles; defender (circle type) and attacker (square type). On the screen, subjects saw a depiction of the network of which there is a screenshot in the instructions.

3.2 Conjectures

This section discusses a few of the conjectures about anticipated behavior in the Network Contest.

3.2.1 All Defense and Attack Units are Used

Conjecture 1. *Nearly* 100% *of the time, we will have*

- $\sum d_i^{DP\text{ - }CT} = \sum d_i^{DP\text{ - }TT} = D = 120$
- $\sum d_{k_i}^{CD\text{ - }CT} = \sum d_{k_i}^{CD\text{ - }TT} = D_k = 20$
- $\sum a_i^{DP\text{ - }CT} = \sum a_i^{DP\text{ - }TT} = \sum a_i^{CD\text{ - }CT} = \sum a_i^{CD\text{ - }TT} = A = 40$

In general, we should expect to see subjects using all of their resources. Since the resources are not valuable and cannot be saved for future periods, there is no reason to not use all of the resources. Subjects should recognize this fact and expend their entire budget.

3.2.2 Small Variance on the Periphery

Conjecture 2.

- $\sum_{i=1}^{5} \left(d_i^{DP} - \sum_{i=1}^{5} \frac{d_i^{DP}}{5} \right) \approx 0$
- $\sum_{i=1}^{5} \left(a_i^{CT} - \sum_{i=1}^{5} \frac{a_i^{CT}}{5} \right) \approx 0$
- $\alpha_1 \approx \alpha_2 \approx \alpha_3 \approx \alpha_4 \approx \alpha_5$
- $\sum_{i=1}^{5} \left(d_i^{CD} - \sum_{i=1}^{5} \frac{d_i^{CD}}{5} \right) > \sum_{i=1}^{5} \left(d_i^{DP} - \sum_{i=1}^{5} \frac{d_i^{DP}}{5} \right)$

[2]See the appendix for a copy of the instructions

As mentioned in Chowdhury, Kovenock and Sheremeta (2012), equivalent battlefields are recognized to be so by subjects. In a Star Network, periphery nodes are equivalent. If subjects recognize this fact, then they should place equivalent amounts of their budget on the periphery nodes. We will use variance to determine if subjects recognize the equivalence.

In DP treatments, defenders should easily recognize and act on the equivalence causing the variance to be zero or small. The same holds true for attackers in CT treatments. The defense variance in CD treatments is expected to be larger than that in DP treatments for obvious reasons of the difficulty for 6 subjects to reach the same or similar decisions without any form of communication. For attackers in TT treatments it is impossible to have zero variance on the periphery unless the periphery is not attacked. Instead we will simply use relative frequency of an attack at each periphery node.

3.2.3 Over Exerted Effort on Center Node for Attacker and Defense Planner

Conjecture 3.

- $d_C^{DP\text{ - }CT} > (d_C^{DP\text{ - }CT})^\star$
- $d_C^{DP\text{ - }TT} > (d_C^{DP\text{ - }TT})^\star$
- $a_C^{DP\text{ - }CT} > (a_C^{DP\text{ - }CT})^\star$
- $a_C^{CD\text{ - }CT} > (a_C^{CD\text{ - }CT})^\star$
- $\alpha_C^{DP\text{ - }TT} > (\alpha_C^{DP\text{ - }TT})^\star$
- $\alpha_C^{CD\text{ - }TT} > (\alpha_C^{CD\text{ - }TT})^\star$

Experimental evidence suggests that subjects tend to exert too much effort on "large" prizes. In a Star Network, the "large" prize is the Center Node since if the attacker wins the Center Node he wins the entire value of the network. For this reason, we anticipate both attackers and defense planners to overexert effort on the Center Node compared to the equilibrium.

3.2.4 Coordinated Defense Exerts Less Effort on Center Node than Defense Planner

Conjecture 4.

- $d_C^{CD\text{ - }CT} < (d_C^{DP\text{ - }CT})^\star$
- $d_C^{CD\text{ - }TT} < (d_C^{DP\text{ - }TT})^\star$

In contrast to the Defense Planner, defenders in Coordinated Defense treatments are anticipated to have significantly less focus on the Center Node. Subjects on the periphery are expected to hold extra units for themselves in an attempt to ensure their continue survival. This strategy will likely lead to under exerted total effort on the Center Node and may be caused by a myriad of behavioral responses such as attitudes toward risk and envy.

3.2.5 Defense Planner does Better than Equilibrium

Conjecture 5.

- $\Pi_{\mathcal{D}}^{DP\text{ - }CT} > (\Pi_{\mathcal{D}}^{DP\text{ - }CT})^\star$
- $\Pi_{\mathcal{D}}^{DP\text{ - }TT} > (\Pi_{\mathcal{D}}^{DP\text{ - }TT})^\star$

The over exertion of effort on the Center Node as disscussed in Conjecture 3 above is to the defender's advantage. The Defense Planner will be near best responding to the Attacker's strategy since if the attacker places more units on the Center Node then so should the Defender. The attacker should, instead, be placing fewer units on the Center Node if the Defender places more units there. Thus, the Defense Planner should earn higher than expected profits.

3.2.6 Defense Planner does Better than Coordinated Defense

Conjecture 6.

- $\Pi_{\mathcal{D}}^{DP\text{ - }CT} > \Pi_{\mathcal{D}}^{CD\text{ - }CT}$

- $\Pi_{\mathcal{D}}^{DP\text{ - }TT} > \Pi_{\mathcal{D}}^{CD\text{ - }TT}$

In Coordinated Defense treatments, the under exerted effort on the Center Node has the opposite effect of the over exerted effort in the Defense Planner treatments. For similar reasons as given in Conjecture 5 above, the Network in Coordinated Defense is anticipated to earn less than equilibrium profits.

4 Results

4.1 Defense and attack units are usually all used

Table 3: Percentage of time all units were used

	DP - CT	**DP - TT**	**CD - CT**	**CD - TT**	**Total**
Defender	93.33%	94.81%	93.19%	94.31%	93.89%
Attacker	85.74%	95.74%	84.07%	72.96%	88.00%
Total	89.54%	95.28%	91.48%	89.44%	91.44%

Table 3 displays the probability that subjects use all of their resources in every treatment. It appears that most subjects, particularly when a defender, expend all of their resources.

Attackers appear, at first glance, to be less successful in allocating all units. This difference is likely due to a simple factor: equally splitting resources in CT treatments causes unused resources.

In treatments where attackers are Cyber Terrorists, the attackers may split their tokens across any or all 6 nodes. If a subject wishes to place an equal allocation at all nodes, then she must place $\frac{40}{6} \approx 6.66$ units at each node. In early periods subjects would frequently place 6.66 units at each node using almost all units, but leaving a total of 0.04 units unused. This accounts for the difference between attackers and defenders in CT treatments. Note that in Defense Planner treatments if defenders wish to equally split resources, an allocation of 20 units at each node results with no unused resources.

As far as why attackers are so less likely to use all of their resources in the CD-TT treatment, no clear explanation is apparent. It seems that subjects in these sessions merely

took longer to realize they should leave no unit unallocated.

4.2 Variance on the periphery is small

Figure 2:

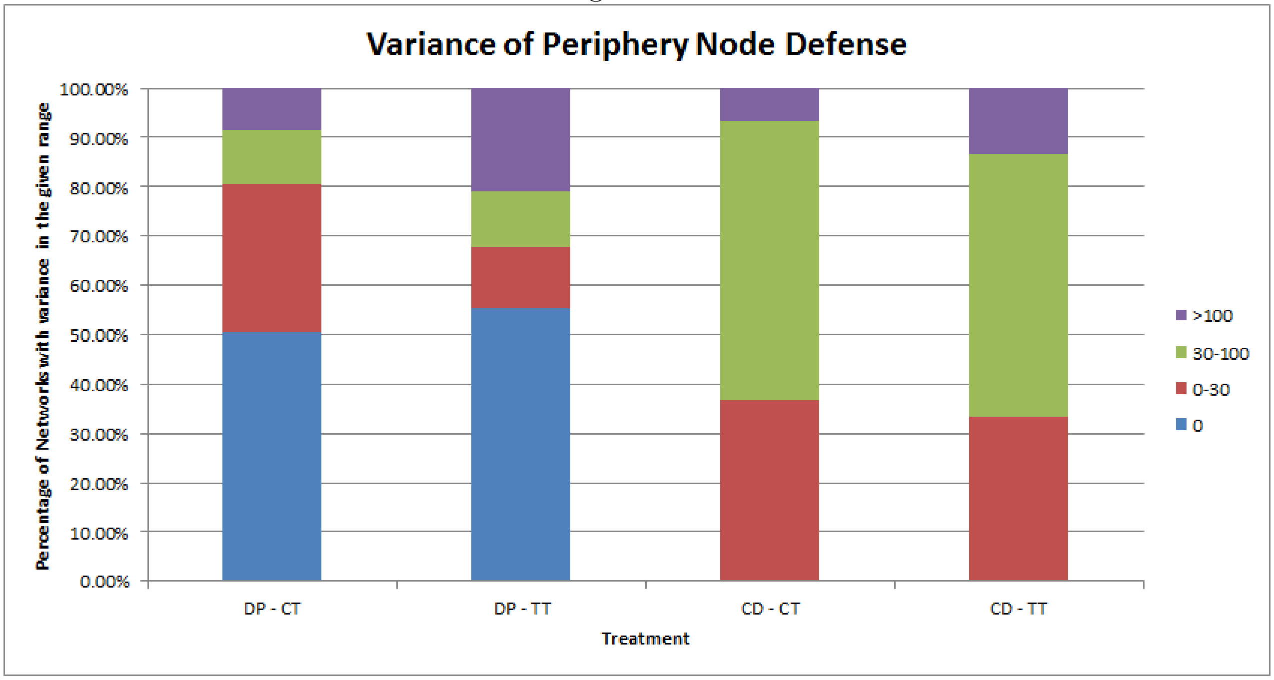


Figure 2 shows the variance of the defensive allocation on the periphery nodes in each treatment. In equilibrium, the periphery nodes are equivalent and by looking at the variance we are able to see if subjects recognize this fact. Based on Figure 2 we see that Defense Planners allocate equivalent units to all periphery nodes (resulting in zero variance) more than 50% of the time, and allocate relatively equivalent units a large portion of the time. This supports previous research which suggests that subjects recognize equivalent battlefields (Chowdhury et al., 2012).

When defense is coordinated by multiple individuals who are not able to communicate, the variance of periphery nodes is expected to be significantly larger than that for a Defense Planner. However, it does appear that subjects are moderately able to coordinate defense on the periphery nodes.

Figure 3 shows similar results for Cyber Terrorists as Figure 2 did for defenders: Attackers

Figure 3:

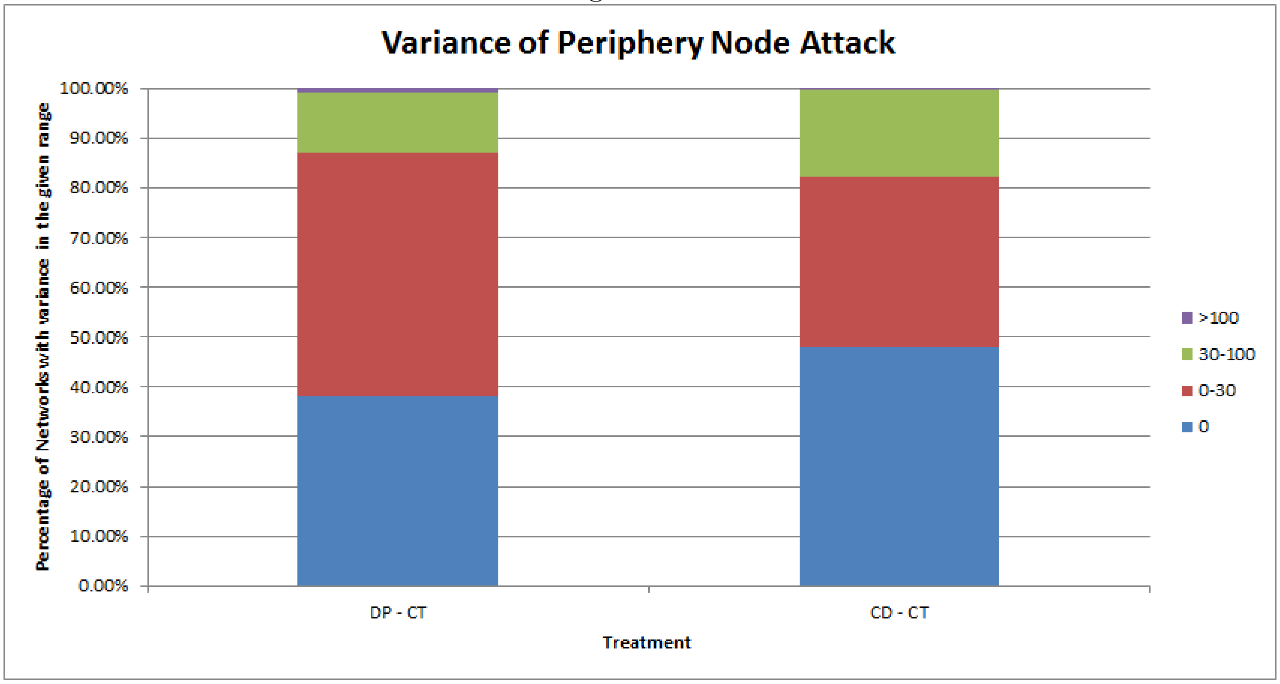


Table 4: Attack on Periphery Nodes in TT Treatments

	DP - TT	**CD - TT**
α_1	19.07%	10.28%
α_2	9.81%	12.22%
α_3	8.52%	8.61%
α_4	11.30%	10.00%
α_5	15.37%	13.33%

recognize the equivalence of periphery nodes and choose an allocation that has zero periphery variance about 40% of the time. Table 4 shows the percentage of the time a periphery node is chosen for attack in Transnational Terrorist treatments. There is some evidence for equivalent focus on the periphery nodes with a bit of emphasis on the first and last nodes. This extra focus is likely due to the presentation of the problem to the subjects. The emphasis on the first node is likely due to it being labeled as "Node 1" and the emphasis on the last node is likely due to it being listed last in the table of choices.

4.3 Attackers over exert effort on the Center Node compared to equilibrium

Figure 4:

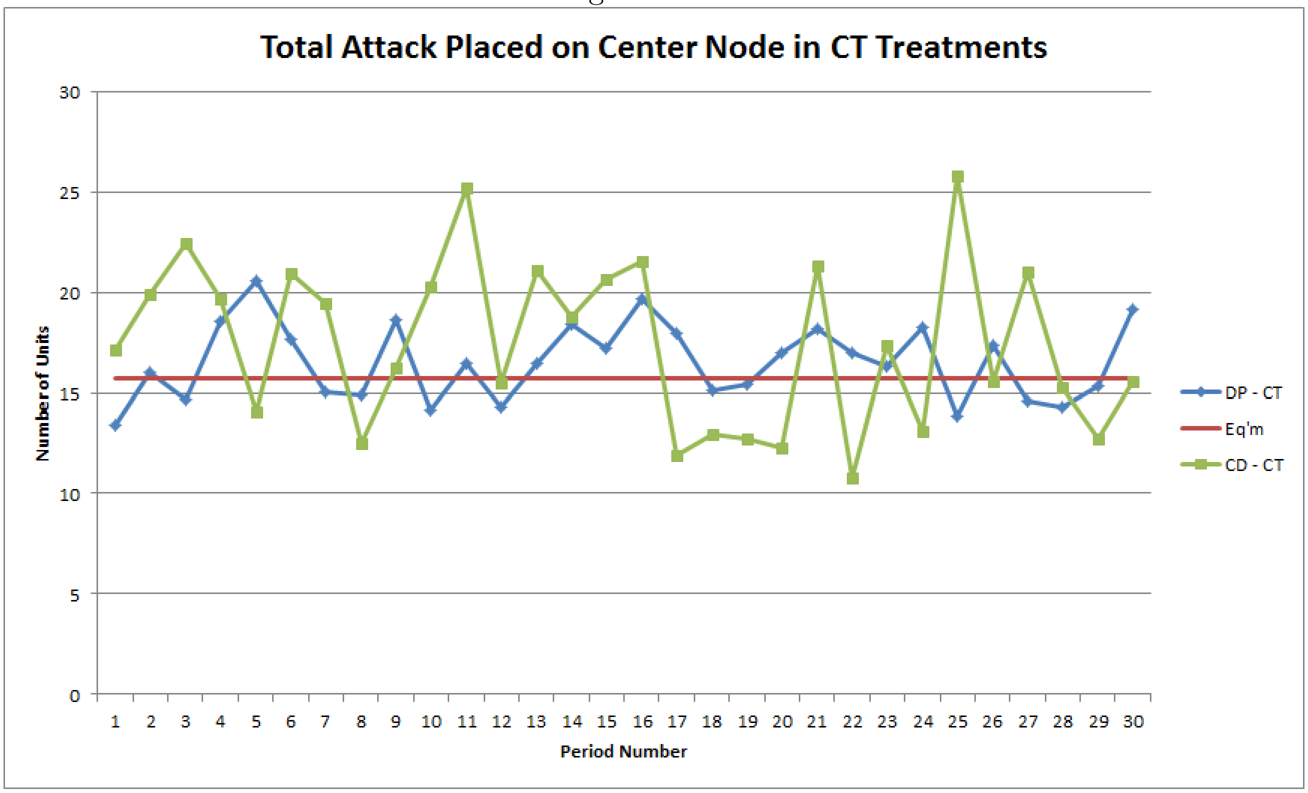


Figure 4 displays the effort exerted on the Center Node by Cyber Terrorists. In the DP-CT treatment the equilibrium effort on the Center Node is 15.40 and the in the CD-CT treatment the equilibrium is 16.00. Since the equilibria are close, only one line is plotted on the graph. Cyber Terrorists bounce around the equilibrium, but, on average, over exert effort on the Center Node. Average effort exerted in the DP-CT treatment is 16.53 (1.13 units above equilibrium) and average effort exerted in the CD-CT treatment is 17.45 (1.45 above equilibrium).

Transnational Terrorists attack the Center Node 52.5% of the time when facing a Defense Planner and 45.58% of the time when facing Coordinated Defense. In equilibrium, a Transnational Terrorist is to attack a node 16.67% of the time.

4.4 Defenders under exert effort on the Center Node compared to equilibrium (except in the CD - CT Treatment)

Figure 5:

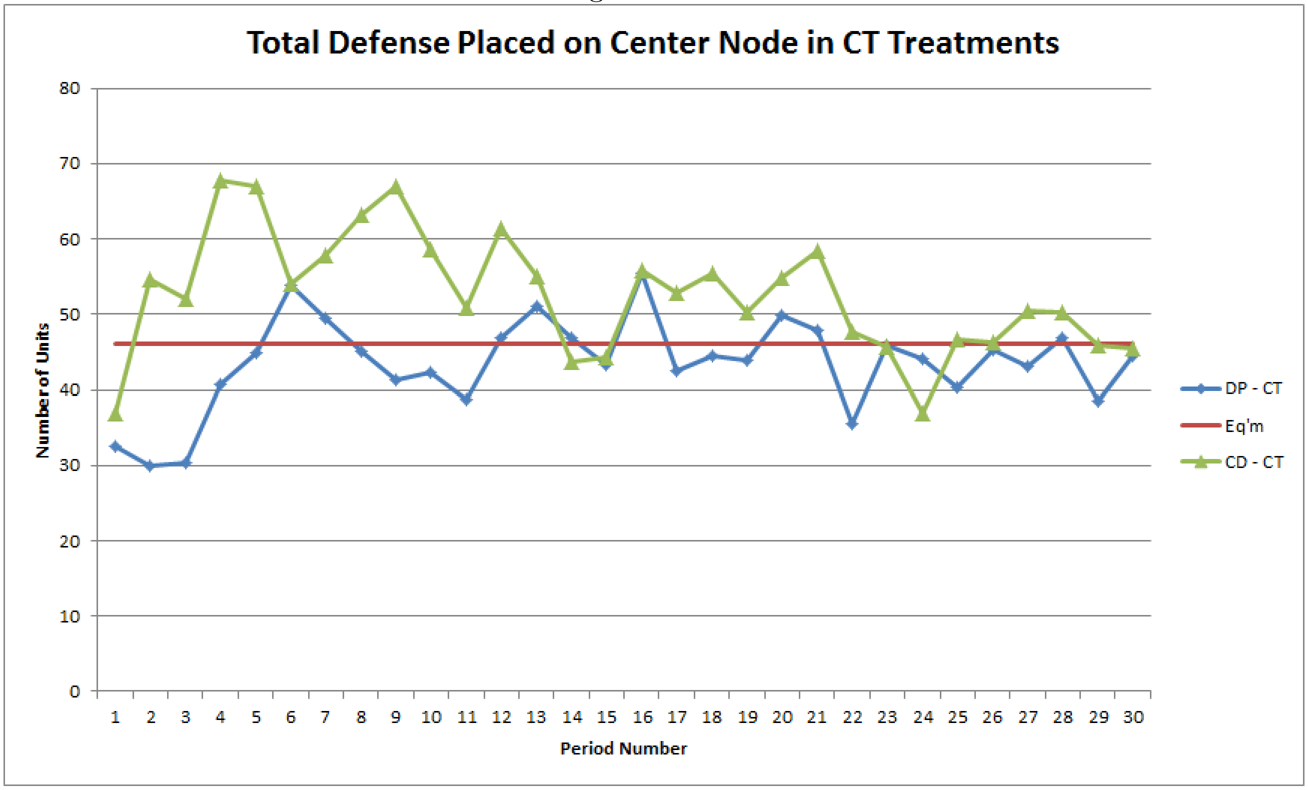
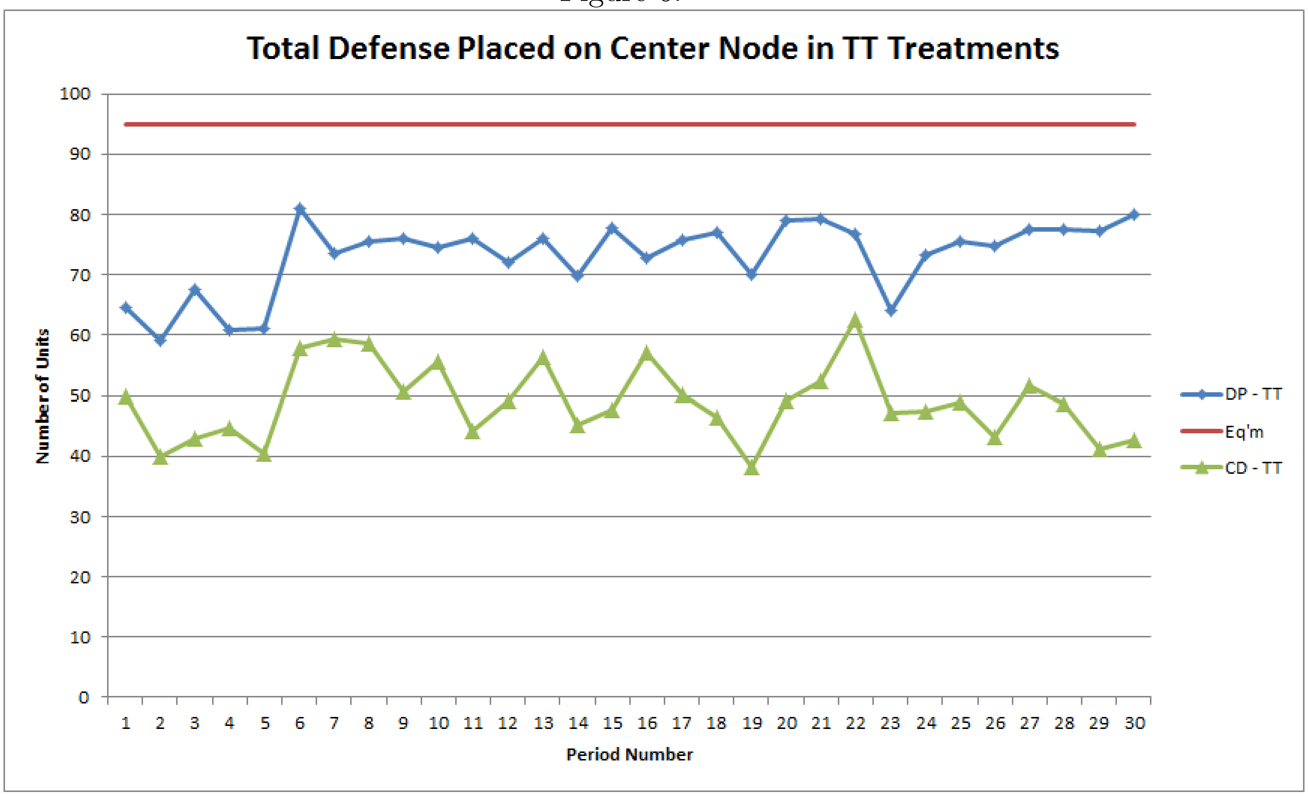


Figure 5 displays the total effort exerted by the defender(s) in the CT treatments and Figure 6 for the TT treatments. Again the equilibria allocations are close (or, in the case of the TT treatments equivalent), so only one line for equilibrium is drawn for simplicity of the graph. Defense Planner tend to be close to equilibrium but tend to place less than the equilibrium allocation on the Center Node (an average allocation of 43.15 units versus an equilibrium allocation of 46.15 units). When defense is coordinated, however, the average allocation to the Center Node begins well above equilibrium and gradually falls to be around the equilibrium in the late periods. On average, Coordinated Defenders far exceed equilibrium by placing 52.59 units on the Center Node whereas the equilibrium is just 45.15 units.

This result is quite counter-intuitive as one might expect cautious Defense Planners to over exert effort on the Center Node whereas greedy Coordinated Defenders on periphery nodes will keep more than the equilibrium allocation of defense units for their own node. A possible explanation for this might be due to the low level of Attack budget relative to Defense budget. In equilibrium, those in charge of the periphery nodes need only give 5.03 defense units to the Center Node to reach equilibrium. Defenders seem to think that this amount is too small and give to the Center Node with a mode of 8 units being given to the Center Node by periphery nodes.

Figure 6:

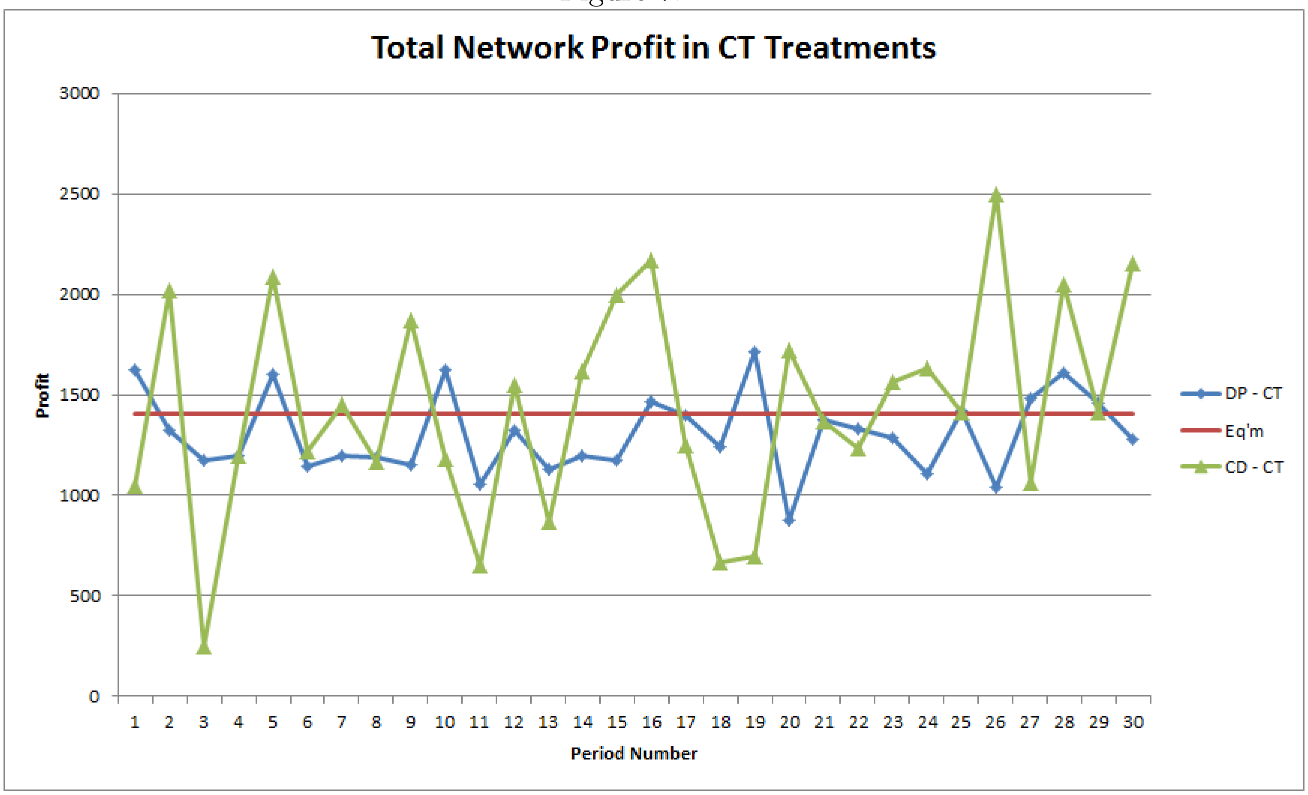


In TT treatments, both Defense Planners and Coordinated Defenders exert far too little effort on the Center Node as shown in Figure 6. The equilibrium for both treatments is to place 95 units of defense on the Center Node. Defense Planners manage to place an average of 73.19 units of defense on the Center Node, but the Coordinated Defenders only manage 48.99 units of defense.

Note that Defenders and Attackers all move closer to the equilibrium allocations in later periods.

4.5 Total Network Profit is below equilibrium (except in the CD - CT Treatment)

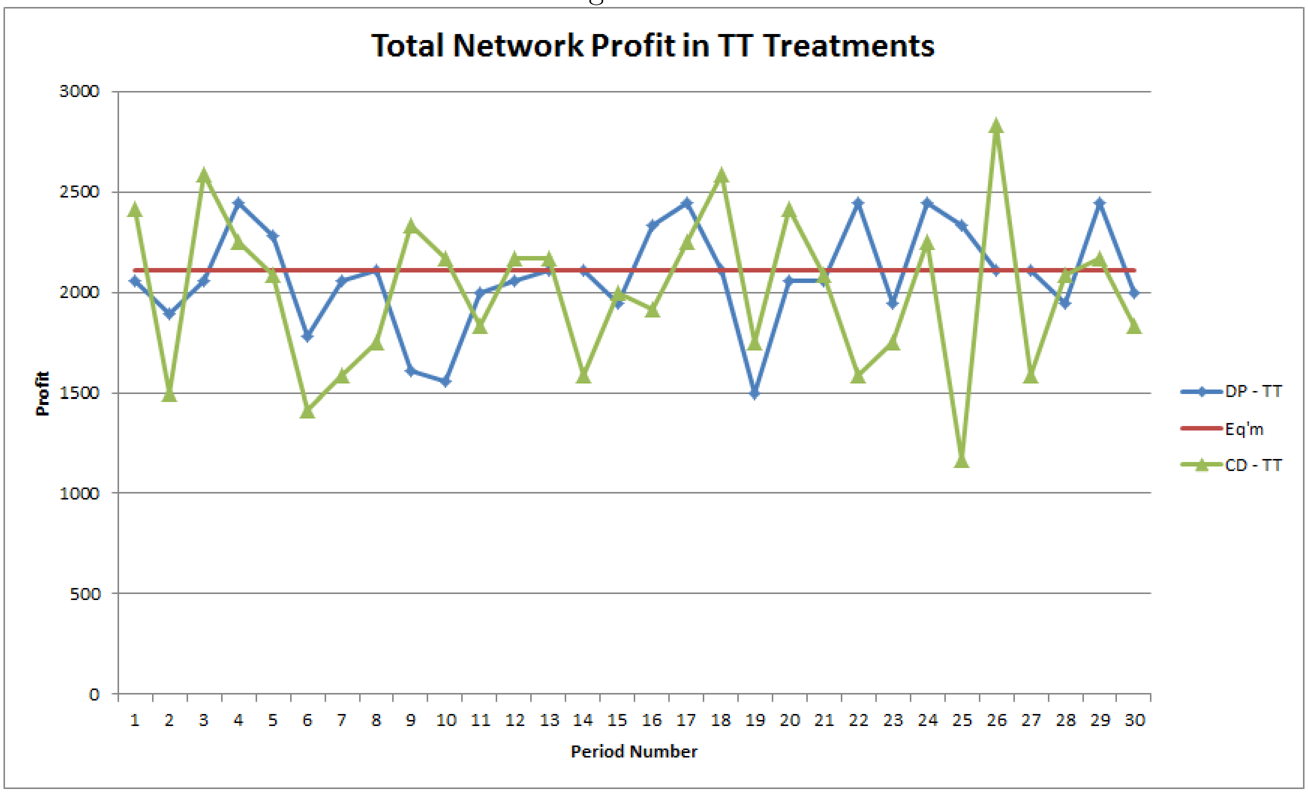
Figure 7:



When facing a Cyber Terrorist, Coordinated Defenders have total network earnings that are much higher than for the Defense Planners on average despite the fact they are predicted to earn less, though the difference is quite small. Defense Planners earn an average of 1307.41 points significantly below the equilibrium of 1406.25 points. Coordinated Defenders earn an average of 1435.53 points which is actually above equilibrium at 1406 points. This difference is primarily due to the difference in Center Node allocations and the fact that attackers place too much effort on the Center Node. When the attack on the Center Node is above equilibrium, the best response for the defender is to also over exert effort on the Center Node:

Coordinated Defenders manage to accomplish this allocation whereas Defense Planners do not. Even though Coordinated Defenders manage to earn a higher average of earnings, Figure 7 shows that earnings are much more volatile for Coordinated Defenders.

Figure 8:



Defense Planners manage to perform better than Coordinated Defenders when facing a Transnational Terrorist. Both have equilibrium expected earnings of 2111.11 points, yet neither manages to earn an equilibrium payoff on average. Defense Planners earn an average of 2077.78 points and Coordinated Defenders earn an average of 2002.78 points. It seems that Defense Planners perform better than Coordinated Defenders when facing a Transnational Terrorist, but, when facing a Cyber Terrorist, Coordinated Defense earns higher average payoffs whereas Defense Planners have less volatile earnings.

5 Conclusion

In this paper, I have laid the framework for a Network Contest in an experimental setting. The only previously studied network in a contest setting was a weakest link network where the only goal of the network is complete transmission from a single starting point to a single ending point. When you have multiple starting and ending nodes, the complexity of the contest skyrockets though can still be related to common themes seen in many contests; The Center Node is a weakest link and the periphery nodes are equivalent Blotto-type battlefields. The experiment has a baseline treatment that studies this game under common assumptions made in contests. In addition, I consider three other possibilities by varying attacker and defender qualitiies. In particular, I make an assumption common to literature on Transnational Terrorism that an attacker may target only a single node. In addition, I am the first to consider the case of having multiple entities responsible for the defense of the network as a whole but earning the payoff of only their single node leading to potential coordination errors.

Subjects tend toward equilibrium in later periods, but attackers over exert effort on the Center Node and defenders under exert effort on the Center Node compared to equilibrium. The only exception to this rule is Coordinated Defense when faced with a Cyber Terrorist who over exert effort on the Center Node.

References

[1] Reka Albert, Hawoong Jeong, and Albert-Laszlo Barabasi. Error and attack tolerance of complex networks. *Nature*, 406:378–382, 2000.

[2] Clive Bull, Andrew Schotter, and Keith Weigelt. Tournaments and piece rates: An experimental study. *The Journal of Political Economy*, 9(1):1–33, 1987.

[3] Subhasish Modak Chowdhury, Dan Kovenock, and Roman M. Sheremeta. An experimental investigation of colonel blotto games. *Economic Theory*, forthcoming, 2012.

[4] Nicholas Economides and Lawrence J. White. Networks and compatibility: Implications for antitrust. *European Economic Review*, 38:651–662, 1994.

[5] Ronald G. Ehrenberg and Michael L. Bognanno. Do tournaments have incentive effects? *The Journal of Political Economy*, 98(6):1307–1324, 1990.

[6] Lawrence Friedman. Game-theory models in the allocation of advertising expenditure. *Operations Research*, 6:699–709, 1958.

[7] Dan Kovenock and Brian Roberson. The optimal defense of networks of targets. 2012.

[8] David Rietzke and Brian Roberson. The robustness of 'enemy-of-my-enemy-is-my-friend' alliances. *Social Choice and Welfare*, forthcoming, 2012.

[9] Brian Roberson. The colonel blotto game. *Economic Theory*, 29:1–24, 2006.

Instructions

Welcome to the Vernon Smith Experimental Economics Laboratory. Thank you for participating in this experiment on economic decision making. Please follow along with me as I read the instructions out loud. If you have a question at any point, raise your hand and wait for an experimenter to come to you. Do not ask your question out loud. **Do not exclaim, laugh or talk out loud**. Any talking during the experiment will eliminate the validity of the results, and you will be asked to leave without being paid. In addition please turn off your cell phones, etc. and put them away during the experiment.

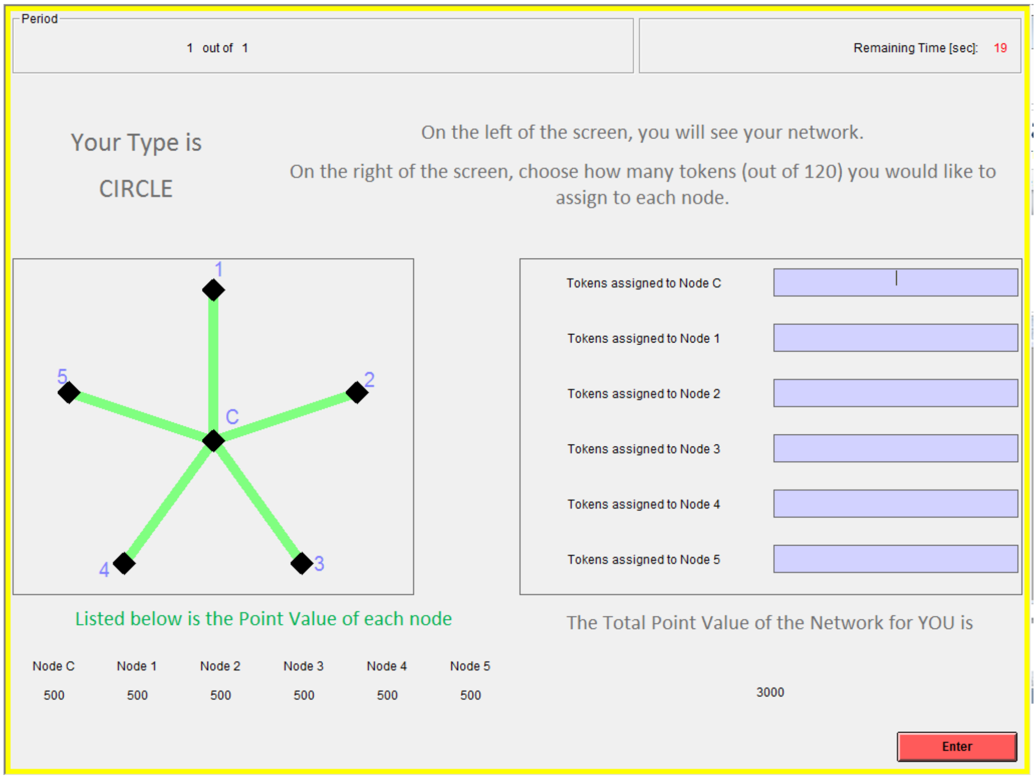
In this experiment you have the opportunity to earn money. The amount of money you earn depends on the decisions you and other participants make. The experiment will consist of three (3) parts. In the first part you will earn points, and in the final two parts you will earn US Dollars directly. At the end of the experiment we will convert the points you have earned into US dollars according to the rate: **500 points equal $1.00**. Additionally, at the end of these instructions, you will take a 10 question quiz over these instructions. You will receive $0.50 for every correct answer. You will be paid your earnings privately and confidentially at the end of the experiment.

Instructions for Part 1

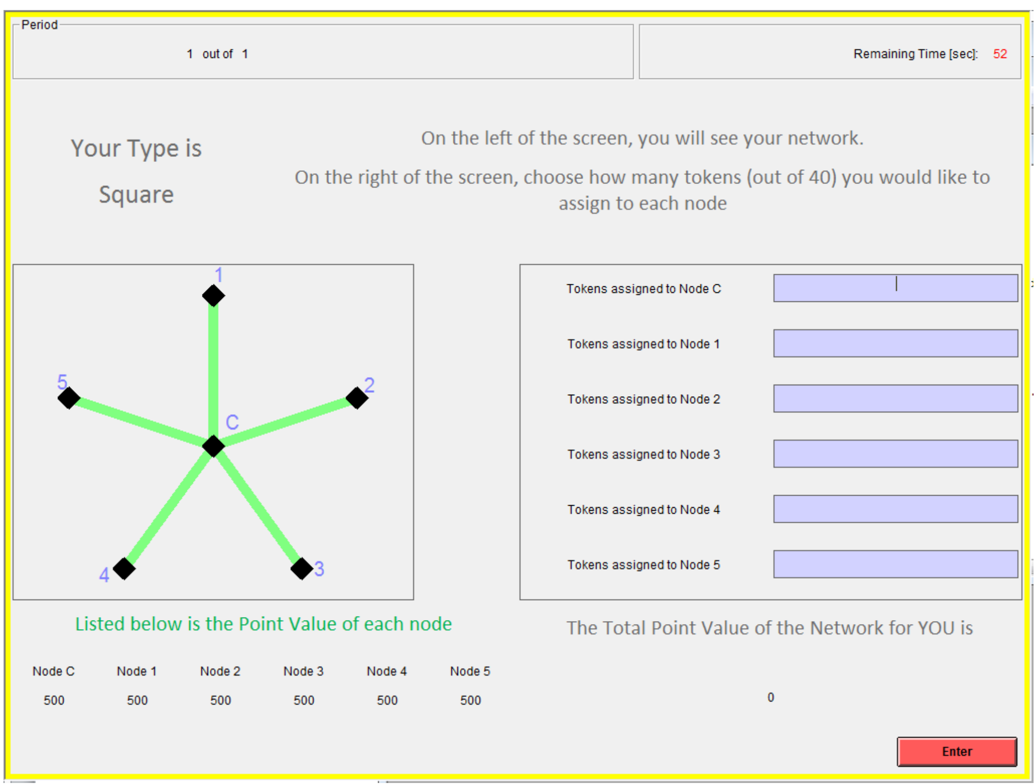
The first part of the experiment will consist of **30 decision making periods.** You will be paid for **6 periods which will be randomly selected at the conclusion of the experiment.** Since you do not know which periods will be paid, **you should pay careful attention to your decisions in all periods.** At the beginning of the first period, you will be randomly assigned as either a circle type or a square type. **You will switch roles every five periods for the duration of the experiment.** Make sure you pay attention to your role during EVERY period. Each period, you will be randomly re-paired with another participant of the opposite type as yourself. That is: if you are a circle type, you will be paired with a randomly-chosen square type in that period. If you are a square type, you will be paired with a randomly-chosen circle type in that period.

At the beginning of each period you will see one of the following two screens depending on if you are a circle or square type. (See figures 1 and 2 below).

(Figure 1)



(Figure 2)



At the top of the screen, you will see the period number you are on, the time remaining in seconds, which type you are (circle or square) and a short description of the screen below. Below you will see a picture of a network, a section to fill out token assignments, the point value of each node in the network and the total point value for you. Notice that the screens are nearly identical. The only differences are which type you are, the number of tokens you are able to assign and the Total Point Value of the Network for YOU.

THE NETWORK

As you can see from the picture in Figure 1 (and Figure 2) above, a network consists of dots (nodes) and lines (links) which connect the nodes. In this experiment, there are six (6) nodes labeled: **C, 1, 2, 3, 4, and 5.** Additionally, each node labeled 1, 2, 3, 4, 5 is linked to node C and there are no additional links. Note that, while nodes 4 and 5 are not directly linked, they are **indirectly linked through node C.**

At the start of each period, all nodes and links are active. **Active nodes are represented by black dots and active links are represented by green lines.** The point value of a node is determined by the number of other nodes it is linked to. If you can draw a path between two active (black) nodes using active (green) links, then the nodes are linked.

PointValueofNode = 100 * (# of other nodes it is connected to)

For example

- Node C is directly linked to nodes 1, 2, 3, 4, 5. Thus
  - PointValueofC = 100 * 5 = 500
- Node 1 is directly linked to C and indirectly linked to 2, 3, 4, 5 through C. Thus
  - PointValueof1 = 100 * 5 = 500

At the start of each period, all nodes are connected to the other five (5) nodes, so the point value for each node is 500.

The payoff for you in a given period depends on which type you are. If your type is circle, then your point value is the sum of the point values for each node. If you are a square type, then your point value is the difference between 3000 and the sum of the point values for each node.

PayoffCircle = PointValueC + PointValue1 + PointValue2 + PointValue3 + PointValue4 + PointValue5

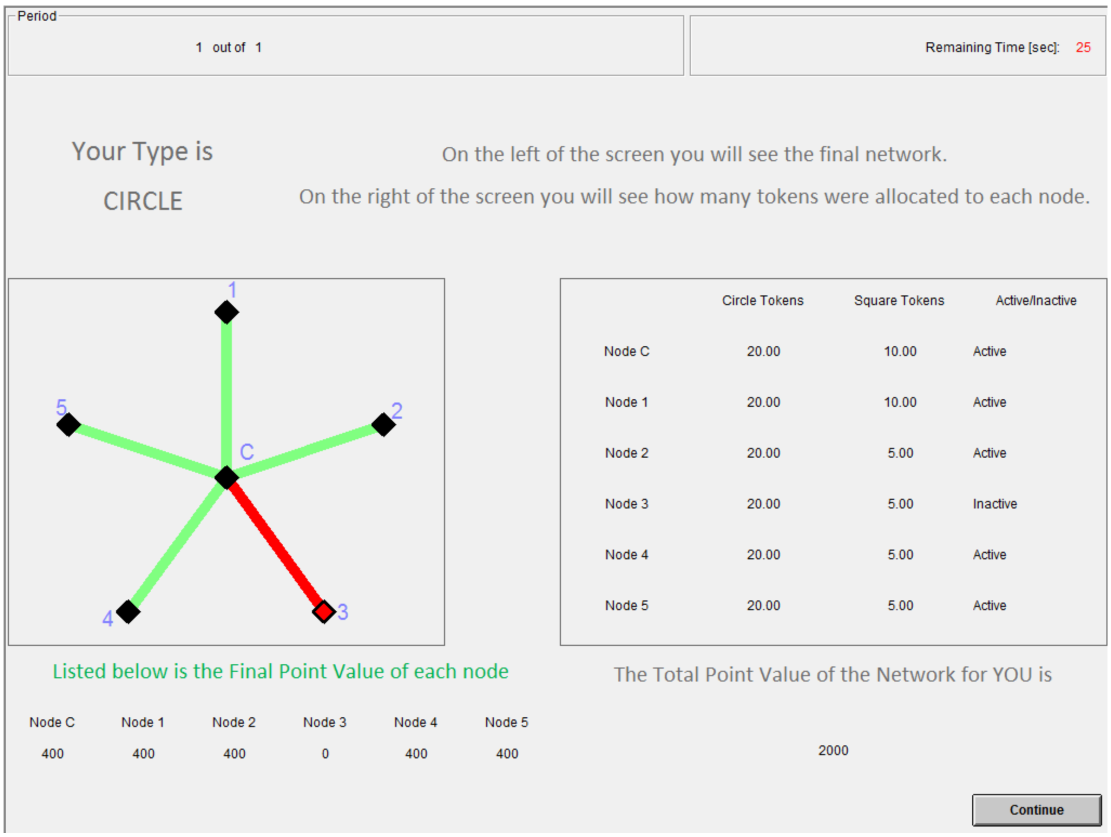
PayoffSquare = 3000 – PointValueC – PointValue1 – PointValue2 – PointValue3 – PointValue4 – PointValue5

Notice at the start of each period that the point value of circle types is 3000 and the point value of square types is 0.

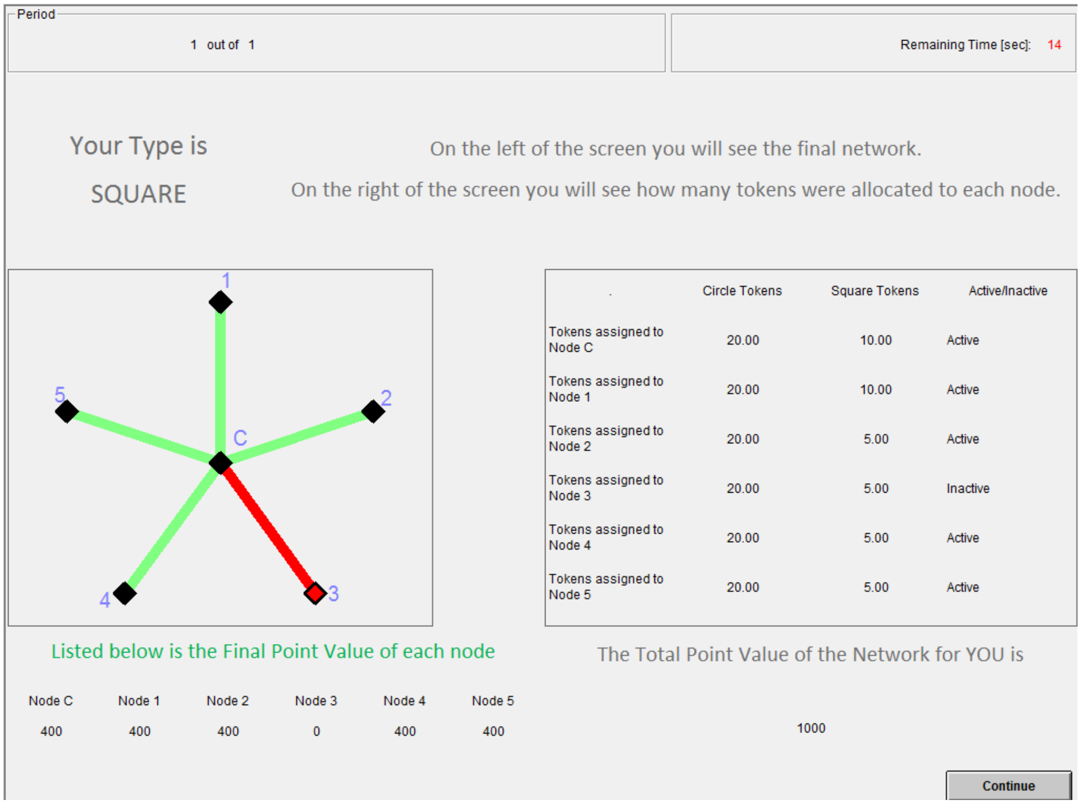
INACTIVE NODES AND LINKS

When a node becomes inactive, all links that pass through the node also become inactive. An inactive node is represented by a red dot with a black outline and an inactive link is represented by a red line. Look to Figures 3 and 4 to see an example. Also the outcome table displays whether or not the node is Active or Inactive

(Figure 3)



(Figure 4)



Notice that in this example only Node 3 is inactive (the link connecting Node 3 to Node C is also inactive). Under this scenario Nodes C, 1, 2, 4 and 5 are now only connected to four (4) other nodes. Thus **the point value for these nodes is 100 * 4 = 400.** Also, Node 3 is now inactive, and so is linked to no other nodes. Thus **the point value for Node 3 is 100 * 0 = 0.** We now obtain the Total Point Values for both the circle and square types.

PayoffCircle = 400 + 400 + 400 + 0 + 400 + 400 = 2000

PayoffSquare = 3000 – 400 – 400 – 400 – 0 – 400 – 400 = 1000.

THE USE OF TOKENS

Each period all circle types are given 120 tokens and all square types are given 40 tokens. **The tokens have no value in either US Dollars or points, and you may not save the tokens for future periods (If you do not use them, then you lose them).** You may allocate your tokens across any or all six (6) nodes in the network. Both the Circle and Square types allocate their tokens as they desire. You may allocate the tokens in increments of one hundredth of a token (So, for example, you may allocate 4.21 tokens to a node). You may use the calculators help with your decisions (for instance assuring that you do not assign more than 120 tokens if you are a Circle type).

The probability that a node remains Active is equal to the number of Circle Tokens allocated to the node divided by the total number of tokens allocated to the node. The probability that a node goes Inactive is equal to the number of Square Tokens allocated to the node divided by the total number of tokens allocated to the node.

ProbabilityNodeisActive = CircleTokens / (CircleTokens + SquareTokens)

ProbabilityNodeisInactive = SquareTokens / (CircleTokens + SquareTokens)

You may think about this as both players putting their tokens into bags labeled with the names of the nodes. For each bag I will randomly draw one of the tokens out of the bag. If I draw a Circle Token out of a bag then that node will remain Active. If I draw a Square Token out of the bag then that node will go Inactive. **If no tokens of either type are placed on any node, then the node remains active.**

After both types have allocated their tokens the final network and token allocations are revealed along with your earnings in that period.

SUMMARY

1. The starting screen displays the initial network, the point values of each node (which start at 500) and your total point value.
2. Your total point value depends on which type of player you are (Circle or Square) and your type will change throughout the course of the experiment.
3. Circle types allocate no more than 120 tokens to any or all of the six (6) nodes which are labeled C, 1, 2, 3, 4 and 5.
4. Square types allocate no more than 40 tokens to any or all of the six (6) nodes which are labeled C, 1, 2, 3, 4 and 5.
5. After both types have allocated their tokens, nodes remain active or go inactive depending on who allocated more tokens to that node.
6. At the start of each new round, each person will be randomly paired with someone else of a different type.
7. At the conclusion of the experiment six (6) periods will be randomly selected for payment and we will convert point earnings into US Dollars at the rate of **500 points equal $1.00**.
8. You will now take a 10 question quiz. For each correct answer, you will receive $0.50.

NOTE – RECORDING RULES

You should have received a Record Sheet along with the Instructions. Please be sure to fill out the Record Sheet after EACH Round

ARE THERE ANY QUESTIONS???