Towards a Cooperative Defense Model Against Network Security Attacks

Harikrishna Narasimhan[1], Venkatanathan Varadarajan[1], C. Pandu Rangan[2]

[1]Department of Computer Science and Engineering,
College of Engineering Guindy,
Anna University, Chennai, India.
{nhari88,venk1989}@gmail.com

[2]Theoretical Computer Science Laboratory,
Department of Computer Science and Engineering,
Indian Institute of Technology Madras, Chennai, India.
prangan@iitm.ac.in

Abstract. It is widely acknowledged that internet security issues can be handled better through cooperation rather than competition. We introduce a game theoretic cooperative model against network security attacks, where users form coalitions and invest in joint protection. We analyze coalition formation in three canonical security games described in a previous work by Grossklags et al. Our findings reveal that the success of cooperative security efforts depends on the nature of the attack and the attitude of the defenders.

Keywords: Economics of Security, Cooperative Game Theory, Coalition, Partition Function Game (PFG), Core

1 Introduction

Spam is a perennial problem in today's internet and has caught the attention of corporate giants like Google and Yahoo. It is widely acknowledged that the best way to fight spam is "through cooperation and not competition". In fact, the Organization for Economic Co-operation and Development recommends international cooperation in the battle against spam [1]. A recent study shows that such cross-border cooperation can deter cyber crimes to a substantial extent [34].

In [26], Moore finds evidence of non-cooperation among defenders in the fight against phishing and highlights the need for cooperative information sharing. Cooperation is also warranted in the detection [7, 5] and mitigation [27, 22] of DDoS attacks. Cooperative intrusion detection systems aim at achieving high detection rates through exchange of attack information among various sites. Cooperative security has also been employed against attacks in peer-to-peer services [25, 11] and adhoc networks [18].

Economics of information security is a fast growing area of research today [2]. Study of cooperation in this field has primarily focused on the economic aspects of information sharing and regulatory policies for disclosure of vulnerabilities [12, 10, 4, 6]. A lot of work on the economics of coalition formation and alliances can be seen in the public goods literature [28, 31]. However, in the network security domain, the notion of cooperation warrants greater attention than it has received. The motivation behind our work is to analyze the economic incentives that network users have in cooperating and engaging in joint security measures.

People invest in security only if the perceived loss due to lack of security is sufficiently high. Due to interdependencies in a network, individuals who do not secure themselves could become vulnerabilities for everyone else in the network [9]. Clearly, when every entity in a network is secured, all its users are benefited. We believe that users who are desperately in need of security will not only invest in self-protection, but will also agree to contribute to the cost of protection of other users in the network.

A lot of work has been done on non-cooperative models that capture the economic aspects of security attacks [33, 14, 15, 9, 13, 24]. In this paper, we introduce a cooperative game theoretic model against security attacks, where a set of network users come together and invest in joint protection. We analyze coalition formation in three canonical security games described by Grossklags et al. [14]. Due to externalities between coalitions, we model the games in partition function form [32, 19, 21]. Using the solution concept of the core, we find that the success of joint protection efforts depends on the nature of the attack and the attitude of the network users.

The rest of the paper is organized as follows. Three canonical security games are described in Section 2. We present our cooperative model in Section 3 and investigate the conditions for non-emptiness of the core in Section 4. In Section 5, we conclude the paper along with future research directions.

2 Security Games

A security game can be defined as a game-theoretic model that captures the essentials of decision making to protect and self-insure resources within a network [14]. We now describe the basic game model used by Grossklags et al. [14].

2.1 Basic Model

Consider a network with n defending entities, each receiving an endowment W. Let L be the loss that a defender incurs when subjected to a successful attack. Each defender chooses a level of protection $0 \leq e_i \leq 1$ and a level of self-insurance $0 \leq s_i \leq 1$. Protection efforts include firewall, patches and intrusion detection systems, while self-insurance refers to backup technologies [9]. Let b and c be the unit cost of self-protection and self-insurance respectively. (Note that attackers are not players in this game [14].)

The preference of an attacker to target a defender depends on several economic, political and reputational factors. Hence, it is assumed that a defender i is attacked with a probability $0 \leq p_i \leq 1$. The utility for defender i is given by

$$U_i = W - p_i L(1 - H(e_i, e_{-i}))(1 - s_i) - b e_i - c s_i, \tag{1}$$

where H is the security contribution function, which characterizes the effect of e_i, subject to the set of protection levels chosen by other defenders e_{-i}.

The contribution function H represents the *interdependencies* that exist within a network. Based on H, three canonical security games have been studied for tightly coupled network [14, 15, 9, 13]. They include:

Weakest-link security game: Here, the overall protection level of the network depends on the minimum contribution among the defenders. Hence,

$$H(e_i, e_{-i}) = min(e_i, e_{-i}).$$

This game is relevant when an attacker wants to breach the perimeter of an organization's virtual private network through a hidden vulnerability like a weak password.

Total effort security game: In this game, the global protection depends on the average protection level of a defender*.

$$H(e_i, e_{-i}) = \frac{1}{n}\sum_{k=1}^{n} e_k.$$

This is applicable to distributed file transfer services as in peer-to-peer networks, where an attacker's motive is to slow down the rate of file transfer.

Best shot security game: If the overall protection level depends on the maximum protection level of the defenders,

$$H(e_i, e_{-i}) = max(e_i, e_{-i}).$$

For example, when an attacker wants to censor a piece of information, he has to ensure that no single copy of the information is available in the network. This scenario can be modeled as a best shot game.

2.2 Nash Equilibrium

A lot of analysis has been done on the non-cooperative behavior of defenders in security games [14, 15, 9]. In [14], Grossklags et al. analyze the Nash equilibrium strategies of a set of homogeneous defenders (defenders with identical utilities). They identify three possible Nash equilibria in the game:

- Full-protection: $(e_i, s_i) = (1, 0)$
- Full-insurance: $(e_i, s_i) = (0, 1)$
- Passivity: $(e_i, s_i) = (0, 0)$.

* This game can also called an average effort security game.

Full protection is a social optimum in security games. In [15], the authors analyze the full protection equilibria in security games with heterogeneous defenders. In the heterogeneous version of a weakest-link game, full-protection is not possible even when a single player chooses passivity or self-insurance over self-protection. This is because no other defender will have an incentive to protect himself and would instead choose self-insurance or remain passive. On the other hand, full protection is an equilibrium in best-shot games only when one player protects, while all others free-ride on him. In the case of total effort games, full-protection cannot be achieved if one or more players are passive or self-insured.

While in both the models, protection and self-insurance levels are continuous, in a recent work [13], Grossklags et al. state that it is reasonable to approximate the security decisions of the defenders to binary choices, i.e. $e_i, s_i \in \{0, 1\}$. They justify this by observing that efficient Nash equilibria in security games are binary in nature even when the players have a continuous range of values to choose from. We retain this assumption in the cooperative game model proposed in the next section.

Motivation. It is clear now that full protection is very difficult in a network when it contains a set of non-cooperative players, some of whom are passive or self-insured. An extreme case is in the weakest-link game, where a single unprotected player is enough to compromise the security of the entire network. The question that arises is whether in such situations, players are better off cooperating rather than competing. In this paper, we investigate whether full protection can be achieved in a network if players cooperate with each other.

3 Cooperative Model

We define cooperation as *the willingness of players to form a coalition and contribute to the cost of protection of the entire coalition.* This kind of cooperation, where one or more players subsidize the protection efforts of other players, is called joint protection. This can be contrasted against self-protection, where a player invests for his protection alone. Unlike the previous works, where players are individually rational, we assume that a player would choose to be part of a coalition that minimizes his expenditure towards security. Clearly, a player would not cooperate if forming a coalition is more expensive than remaining alone.

We now outline some of the key assumptions that we make in our model. As in [14], we assume that the unit cost of protection and self-insurance is the same for all players. Given the cost of protection b and cost of self-insurance c, consider the case where $c < b$. This would mean that every player would prefer self-insurance over self-protection. In such a scenario, each player is content in individually insuring himself and has no incentive to engage in cooperative protection measures. Clearly, full-protection is not possible when insurance costs are lower than protection costs. Hence, in our work, we focus on the case where protection is cheaper than self-insurance, i.e $b < c$.

Types of Defenders. The defenders differ in the probability with which they are targeted by an attacker and the loss incurred due to the attack. In the game being modeled, we consider two classes of players, one consisting of defenders who may have an incentive to protect themselves (active players) and the other consisting of defenders who never have an incentive to protect themselves and remain passive (passive players). The players in each class have identical utilities. In the future, we intend to extend our model to analyze the cooperative behavior among completely heterogenous players.

Let p_1 be the probability with which an active player is attacked and let L_1 be the loss incurred by him due to the attack. Similarly, let p_2 be the probability with which a passive defender is attacked and L_2 be the corresponding loss due to the attack.

Active Player: A player is active if protection is cheaper for him when compared to the expected loss due to an attack and the insurance cost, i.e.

$$b = min(p_1 L_1, b, c).$$

Note that an active player need not always engage in self-protection. His decision on protection depends on the decision taken by all other players in the network.

Passive Player: A player is passive when he finds it cheaper to remain passive than to engage in self-protection or self-insurance, i.e.

$$p_2 L_2 = min(p_2 L_2, b, c).$$

As seen earlier, in our game setting, self-insurance is never preferred as it is more expensive than self-protection.

Let the expected loss due to attack for an active player be L_a and that for a passive player be L_p. In general, $L_a = p_1 L_1 \geq b$ (this condition is varied later for total effort games) and $L_p = p_2 L_2 < b$. The utility for an active player i who engages in self-protection is given by

$$U_i = W - b$$

and that for a passive player j is given by

$$U_j = W - L_p.$$

Another assumption that we make initially is that a player is aware of the utilities of other players. Later, we discuss how our model can be extended to cases where players have incomplete information about other players.

3.1 Game Model

Unlike non-cooperative games, cooperative or coalitional games focus on what groups of players can achieve together rather than what individual players can achieve alone [29]. In this paper, the three canonical security games described by Grossklags et al. [14] have been modeled as coalitional games. In a coalition, the active players contribute to the cost of protection of the passive players and thus engage in joint protection.

A value is associated with each coalition, which is shared among the members of the coalition. As against a non-cooperative game, where individual players are assigned a payoff, in a coalitional game, each player is *allocated a part of the value associated with his coalition.* The payoffs are hence said to be transferable.

Coalitional games can be modeled either in characteristic function form or partition function form. Characteristic function form games (CFGs) assume that there is no externality in coalition formation, i.e. the formation of a coalition of players has no impact on the coalitions of other players. Hence, the value assigned to a coalition depends only on the coalitional members and not on other coalitions. On the other hand, partition function form games (PFGs) assign values to coalitions based on the overall partitioning of players.

Due to the interdependencies in a network, the protection efforts of one player creates positive externalities for every other player [23]. Since externalities exist among coalitions in a security game, we model the games in partition function form.

Partition Function Form Game (PFG): Partition function form games were introduced by Thrall and Lucas in 1963 [32] to model coalition formation with externalities. We now give a brief description of partition function form games (PFGs) [19, 21].

Let $N = \{1, 2, ..., n\}$ be a finite set of players. Any non-empty subset of N is a coalition. The players in N are partitioned into a number of disjoint coalitions. A coalition structure or partition $\mathcal{P} = \{P_1, P_2, ..., P_k\}$ is a set of disjoint coalitions P_i such that their union is N.

A coalitional game in partition function form consists of a finite set of players N and a partition function V. The partition function assigns a value to each coalition in a given partition. The value assigned to a coalition is then shared among the coalitional members. We use the notation $V(P, \mathcal{P})$ to denote the value assigned to a coalition P in partition $\mathcal{P}$. Consider a partition containing the grand coalition of all players. The notation $V(N)$ is used to denote the value of the grand coalition in such a partition.

In a security game, the value assigned to a coalition depends on the cost of joint protection. We now model each security game as a coalitional game in partition function form. The partition function for each security game is described next.

Weakest-link Security Game: Let *surplus* denote the maximum contribution of an active player towards the protection of passive players in the coalition. If E_{an} is the expenditure incurred by an active player in the absence of cooperation and E_{ac} is the expenditure incurred by him when he cooperates, then

$$surplus = E_{an} - E_{ac}. \tag{2}$$

When there is no cooperation, an active player has no incentive to protect himself as unprotected players are present in the network. Hence, his expenditure is L_a. On the other hand, when there is full cooperation, an active player invests in self-protection and also, incurs no loss. Therefore,

$$surplus = L_a - b.$$

If an active player is required to contribute more than $L_a - b$ in a coalition, he would prefer to stay out.

Let $deficit$ denote the additional amount of money that a passive player requires if he needs to engage in full protection. Clearly, if E_{pc} is the expenditure incurred by a passive player when he cooperates and if E_{pn} is the expenditure incurred by him when there is no cooperation,

$$deficit = E_{pc} - E_{pn} = b - L_p. \tag{3}$$

Consider a coalition P with l active players and k passive players. If every player outside P is protected, the value of the coalition in a partition $\mathcal{P}$ is given by

$$V(P, \mathcal{P}) = l \times surplus - k \times deficit = l\alpha - k\beta, \tag{4}$$

where $\alpha = L_a - b$ and $\beta = b - L_p$. However, if there is at least one player outside P who is not protected, every player would incur a loss due to attack and

$$V(P, \mathcal{P}) = l\alpha - k\beta - lL_a - kL_p = -(l + k)b.$$

Note that any non-singleton coalition will contain at least one active player (as joint protection would not be possible otherwise). The partition function for a weakest-link game is thus given by $V(\{i\}, \mathcal{P}) = 0$ for a passive player i and

$$V(P, \mathcal{P}) = \begin{cases} l\alpha - k\beta & \text{if every player } j \in Q \text{ for all } Q \in \mathcal{P} \text{ is protected} \\ -(l + k)b & \text{otherwise,} \end{cases} \tag{5}$$

where P contains $l > 0$ active players and $k \geq 0$ passive player.

Total Effort Security Game: Let $n_a > 0$ and $n_p > 0$ be the number of active and passive players respectively in the network. In a total effort game, a player is assured of only $\frac{1}{n}^{th}$ of his protection efforts. Unlike the other two games, here, a player self-protects only when his loss due to an attack is at least as high as n times the cost of protection. Hence, it is assumed that $L_a \geq nb > b$ for an active player [14]. On the other hand, we assume the extreme case $L_p < b < nb$ for a passive player. (We reserve the case where $b \leq L_p < nb$ for future analysis.)

Consider the formation of a coalition P with l active players and k passive players. All active players are self-protected irrespective of coalition formations. Hence, in the absence of cooperation, only n_a players are protected in the network. When P is formed, k passive players are protected. Let $0 \leq r \leq n_p - k$ be the number of passive players protected outside P. Clearly, $E_{an} = L_a\big(1 - \frac{n_a}{n}\big) + b$ and $E_{ac} = L_a\big(1 - \frac{n_a+r+k}{n}\big) + b$. From (2),

$$surplus = \frac{(k + r)L_a}{n}.$$

Similarly, $E_{pc} = L_p\big(1 - \frac{n_a+r+k}{n}\big) + b$ and $E_{pn} = L_p\big(1 - \frac{n_a}{n}\big)$. From (3),

$$deficit = b - \frac{(k + r)L_p}{n}.$$

As in (4), the value of the coalition P in a partition $\mathcal{P}$ is given by

$$V(P,\mathcal{P}) = \frac{l(k+r)L_a}{n} - k\Big(b - \frac{(k+r)L_p}{n}\Big) = (k+r)(l\alpha' + k\beta') - kb, \qquad (6)$$

where $l > 0$, $\alpha' = \frac{L_a}{n}$ and $\beta' = \frac{L_p}{n}$. Passive players do not form a non-singleton coalition without an active player, i.e. a group of passive players have no incentive to invest in joint protection. When a passive player i is alone, he does not self-protect and when r remaining passive players are protected, $V(\{i\},\mathcal{P}) = r\beta'$.

Best Shot Security Game: In best shot security games, we define cooperation in a slightly different manner. The players in a coalition either take turns and protect themselves [8] or a single elected player is self-protected throughout, while every one shares the cost of protection. As long as a single active player is protected, passive players have no effect on the overall protection level. Therefore, in a best shot game, passive players are not considered in coalition formation. Note that the grand coalition contains all active players and no passive players.

In the absence of cooperation, the behavior of active players is not predictable as full protection is not an equilibrium in the game [14]. Hence, we cannot model the partition function in the same way we did in the other two games. Here, the value of a coalition P in partition $\mathcal{P}$ is given by

$$V(P,\mathcal{P}) = lW - b, \qquad (7)$$

where $l > 1$ is the number of (active) players in P. If a lone active player chooses to protect himself, he receives a value $W - b$. On the other hand, if he chooses to remain passive, his value is dependent on the other players in the game. Hence,

$$V(\{i\},\mathcal{P}) = \begin{cases} W - b & \text{if } i \text{ is a protected active player} \\ W - L_a(1 - H_e) & \text{if } i \text{ is an unprotected active player,} \end{cases} \qquad (8)$$

where

$$H_e = \begin{cases} 1 & \text{if } \exists i \in P \text{ for some } P \in \mathcal{P} \text{ s.t. player } i \text{ is protected} \\ 0 & \text{otherwise.} \end{cases}$$

Equations (7) and (8) give the partition function for a best shot security game.

4 Core

The core is a solution concept for coalitional games [29]. It is analogous to the concept of Nash equilibrium in non-cooperative games. The core of a partition function form game is a set of partitioning of players along with the allocated payoff for each player, where no player has an incentive to deviate from the setup. In a security game, the success of cooperation among the players depends on the non-emptiness of the core. If the core is empty, stable coalitions will not be formed and hence, joint protection measures will not be possible.

In this section, we state a number of propositions that allows us to characterize the core of a security game and thus, gain useful insights about the cooperative behavior of network users.

Outcome. An outcome in a coalitional game is a partitioning of the players along with their allocated payoffs. A subset of players may deviate from an outcome leading to a new partitioning of players. The deviation is profitable only when the deviating players are allocated higher payoffs in the new partition. An outcome is present in the core if there exists no subset of players who can profitably deviate from it. An outcome of interest is the one containing the ***grand coalition*** of all players.

Proposition 1. *If the core of a security game in partition function form is non-empty, it would contain an outcome with the grand coalition.*

Proof. Refer Appendix B.1.

When players in a security game have an incentive to cooperate and stay in a coalition, the grand coalition is possible. However, in reality, the formation of the grand coalition may be difficult if the network size is large and the players are geographically distributed.

Allocation. The allocation (or allocated payoff) to a player is an indication of the benefit he receives in a coalition. It also determines his share of payment towards joint protection. The greater the allocation to a player, the lesser is his contribution to joint protection. The allocation to the players in a partition can be represented as a vector x, where x_i is the allocated payoff to player i.

An outcome of a partition function form game can be represented by the pair $(x, \mathcal{P})$, where x is the vector of allocated payoffs and $\mathcal{P}$ is a partitioning of the players into disjoint coalitions. In an outcome, the allocations to the players must satisfy two conditions:

- **Feasibility and Efficiency:** The sum of the allocated payoffs to the players in a coalition must be equal to the value of the coalition, i.e. $\forall C \in \mathcal{P}, \sum_{i \in C} x_i = V(C, \mathcal{P})$,
- **Participation Rationality:** Every player must be allocated a non-negative payoff, i.e. $\forall i \in N, x_i \geq 0$.

An outcome is said to be dominated if there exists another outcome, where a subset of the players are allocated higher payoffs.

Ideal Allocation. Consider an allocation vector x, where all active players are assigned equal payoff, while all passive players are assigned zero payoff, i.e.

$$x_i = \begin{cases} \frac{V(N)}{n_a} & \text{if player } i \text{ is active} \\ 0 & \text{if player } i \text{ is passive.} \end{cases} \tag{9}$$

We call x as the **ideal allocation** (vector). If $V(N) \geq 0$, the ideal allocation would satisfy both the conditions mentioned previously. Hence, the grand coalition with the ideal allocation is a possible outcome. (Note that in a best shot game, passive defenders are not considered in coalition formation.)

The following two propositions help us in determining the conditions under which the core of a security game is non-empty.

Proposition 2. *In a security game in partition function form containing $n_a > 0$ active players and $n_p > 0$ passive players, an outcome corresponding to the ideal allocation is dominated via $S \subset N$ containing $0 < l \leq n_a$ active players and $0 \leq k \leq n_p$ passive players only if $\frac{l}{n_a} > \frac{k}{n_p}$.*

Proof. Refer Appendix B.2.

Note that proposition 2 holds only when the deviating set of players contains at least one active player.

Proposition 3. *The core of a security game in partition function form is empty if a set of players containing at least one active player can profitable deviate from an outcome corresponding to the ideal allocation.*

Proof. Refer Appendix B.3.

Player Attitude. Whether a deviation is profitable for a set of players depends on the resultant partition after deviation. If the deviating players are ***optimistic***, they would expect the best case scenario, where the residual players form coalitions in such a way that the deviating players are benefited to the maximum. If the deviating players are ***pessimistic***, they would expect the worst case scenario, where the residual players would partition themselves in such a way that the deviating players attain the least benefit. These are two extreme cases that need to be analyzed in a partition function form game. The core of a security game corresponding to optimistic players is called an **optimistic core** and that corresponding to pessimistic players is called a **pessimistic core**.

It has to be noted that optimism and pessimism are a property of the game and not of individual players, i.e. all players in a game are either optimistic or pessimistic. (However, we could extend our analysis further by introducing heterogeneity in the attitude of players.)

We now investigate the conditions under which the pessimistic and optimistic cores of security games are non-empty.

4.1 Weakest-Link Security Game

In a weakest-link game, a single unprotected passive player is enough to compromise the security of the entire network. Even if every other player engages in self-protection, the network remains vulnerable to attacks. Hence, we expect that the players are better off investing in joint protection rather than self-protection.

We first analyze the core of a weakest-link game with pessimistic players. The question to be answered here is whether there exists a partitioning of players with corresponding payoff allocations such that no subset of players can profitably deviate together. If a single active player deviates or breaks away from the partition, he would possibly engage in self-protection independent of the rest of the players. If a group of active and passive players deviate together, they would possible engage in joint-protection among themselves, leaving out the rest of the players.

There are two cases that we need to consider regarding a deviation:

– *The deviating set of players does not contain all the passive players.* This would mean that there is at least one passive player in the residual set, who could remain unprotected in the worst case and be a threat to all other players. Since the players are pessimistic, they would not take the risk to deviate.
– *The deviating set of players contains all the passive players.* Since there is no passive player in the residual set, full protection is assured even in the worst case after deviation. However, such a deviation would be profitable to the deviating players only if each of them is allocated higher payoff after deviation.

From proposition 1, it is clear that a non-empty core would contain an outcome with the grand coalition. For such an outcome to exist, players must have an incentive to form the grand coalition and invest in joint protection. This is possible only if the total expected loss due to an attack for the active players is sufficiently high that they are better off contributing to the cost of protection of passive players ($n_a\alpha - n_p\beta \geq 0$). We formally state and prove this in the following proposition.

Proposition 4. *The pessimistic core of a weakest-link security game in partition function form with $n_a > 0$ active players and $n_p > 0$ passive players is non-empty if and only if $n_a\alpha - n_p\beta \geq 0$.*

Proof. Refer Appendix B.4.

Interpretation. From proposition 4, we can conclude that full protection is possible through cooperation in a weakest-link game if the following hold.

– All players are pessimistic.
– The expected loss due to an attack for active players is sufficiently high that they profit more by investing in joint protection than otherwise.

When players are pessimistic in a weakest-link game, more than one coalition structure (partition) may exist in the core and hence, the formation of the grand coalition would be less likely in large networks.

Allocations. Let S_a be the set of all active players in N. A set of pessimistic players will deviate only if all the passive players are present in the deviating set. Then, the solutions to the following set of linear inequalities is the set of allocations for which an outcome containing the grand coalition is present in the pessimistic core.

$$\forall S \in 2^{S_a}, \sum_{i \in S} x_i \geq |S|\alpha - n_p\beta.$$

These inequalities are satisfied by the ideal allocation vector.

Optimistic players stay in a coalition structure only if the best case scenario after every deviation is not as beneficial as the grand coalition. We now check whether an outcome with the grand coalition is present in the optimistic core. If the number of active players n_a and the number of passive players n_p have a common factor other than 1, there would exist at least one outcome with an alternate coalition structure, where every player receives the same payoff as in the grand coalition. What we need to check is whether there exists an outcome where a subset of players receive higher payoff than what they receive in the grand coalition.

Proposition 5. *The optimistic core of a weakest-link security game in partition function form with $n_a > 0$ active players and $n_p > 0$ passive players is non-empty if and only if (i) $n_a\alpha - n_p\beta \geq 0$ and (ii) there exists no values of $0 \leq l \leq n_a$ and $0 \leq k \leq n_p$ such that $\frac{k}{l} \neq \frac{n_p}{n_a}$ and $0 \leq l\alpha - k\beta \leq n_a\alpha - n_p\beta$.*

Proof. Refer Appendix B.5.

Interpretation. When all players are optimistic and their expected losses due to attack are sufficiently high, full protection is possible in a weakest-link game if *one* of the following holds true.

- The grand coalition is the only formation, where all passive players can be protected.
- There exists multiple coalition structures where all passive players are protected, but the ratio between the number of active and passive players is the same in all the coalitions and equal to that of the grand coalition.

In large networks, when the second condition holds, coalition structures with small coalitions are more likely to occur than the grand coalition.

Allocations. We now look at the set of allocations for which the grand coalition is part of the optimistic core when the conditions stated in proposition 5 hold. Let l_0 and k_0 be the smallest values of $0 \leq l \leq n_a$ and $0 \leq k \leq n_p$ respectively for which $\frac{k}{l} = \frac{n_p}{n_a}$. Let D be the set of all subsets of N, each containing l_0 active players and k_0 passive players. Then, it can be shown that the solutions to the following linear inequalities gives the desired set of allocations.

$$\forall S \in D, \sum_{i \in S} x_i \geq l_0\alpha - k_0\beta.$$

Note that these inequalities are satisfied by the ideal allocation vector. Also, if the grand coalition is the only partition in the optimistic core, any non-negative allocation to the players is permissible.

4.2 Total effort game

Unlike the weakest-link game, in a total effort game, the presence of an unprotected passive player has a marginal effect on the protection level of other players. In fact, an active player here can benefit even when he pays for the protection of every passive player in the network (as $L_a \geq nb$).

Let us analyze the case where the players are pessimistic. We show in the following proposition that a total effort game containing non-zero active and passive players will always have a non-empty pessimistic core.

Proposition 6. *The pessimistic core of a total effort security game in partition function form with $n_a > 0$ active players and $n_p > 0$ passive players is non-empty.*

Proof. Refer Appendix B.6.

Now, let us consider a total effort game with optimistic players. Assume that the game has more than one active player. Each active player would invest only in self-protection hoping for the best case, where the other active player(s) would contribute to the protection of passive players. This observation leads to the following proposition.

Proposition 7. *The optimistic core of a total effort security game in partition function form is non-empty if and only if there is exactly one active player in the game.*

Proof. Refer Appendix B.7.

Interpretation. Full protection is possible in a total effort game when *one* of the following hold.

- The players are optimistic, but there is *exactly one* active player in the network.
- The players are pessimistic, but there is *at least one* active player in the network.

When the network size is large, we can definitely expect more than one active player in the network. Only if they are pessimistic, will cooperation be successful.

Allocations. Let l_i and k_i be the number of active and passive players respectively in a subset of players $S_i \subset N$. Then, the solutions to the following linear inequations give the set of possible allocations for the grand coalition in the pessimistic core.

$$\forall S_i \in 2^N, \sum_{j \in S_i} x_j \geq k_i(l_i\alpha' + k_i\beta' - b).$$

Clearly, these inequations are satisfied by the ideal allocation.

4.3 Best shot game

Unlike the other two games, in a best shot game, active players may prefer to remain passive and free-ride on other protected players. If the game contains only one active player, free-riding is not possible and hence, full protection is achieved. However, when the game contains more than one active player, cooperation is necessary and the non-emptiness of the core depends on whether the players are optimistic or pessimistic.

Let us consider a best shot game with more than one active player. It is clear that when the players are pessimistic, no active player attempts to free ride on the others anticipating the worst case, where every player chooses to remain passive. On the other hand, if the players are optimistic, an active player would choose to remain passive in anticipation of the best case, where every other active player chooses to self-protect himself. This is summarized in the following two propositions.

Proposition 8. *The pessimistic core of a best shot security game in partition function form with more than one active player is non-empty.*

Proof. Refer Appendix B.8.

Proposition 9. *The optimistic core of a best shot security game in partition function form with more than one active player is empty.*

Proof. Refer Appendix B.9.

Interpretation. In a best shot game, full protection is possible when *one* of the following holds true.

- There is *only one* active player in the network.
- There is *more than one* active player in the network, but all players are pessimistic.

As in the total effort game, when the network size is large, full protection is possible only if players are pessimistic (as the chances of there being more than one active player is high).

Allocations. The set of allocations for which the grand coalition is part of the pessimistic core is given by the solutions to the following set of linear inequalities.

$$\forall S \in 2^N, \sum_{i \in S} x_i \geq |S|W - b.$$

It is easily seen that the ideal allocation vector satisfies the given inequalities.

4.4 Other Issues

Incomplete Information. The results obtained till now have been based on the assumption that every user in the network has complete information about every other user, i.e., every player is aware of whether the other players are active or passive. This assumption may not hold when the network is large and the users are geographically apart. Incomplete information in non-cooperative security games has been dealt with in detail by Grossklags et al. [16, 17, 13]. In the case of cooperative security games in partition function form, we can take advantage of the attitude of network users. A pessimistic player may assume that all players whose utilities are unknown to him are passive, and an optimistic player may assume that all players unknown to him are active. However, a fundamental question that needs to be answered is *whether the formation of the grand coalition is possible when a player does not have complete information about other players in the coalition.* We reserve this analysis for our future work.

Cost of Stability. Cooperative security measures will not be successful when the core of a security game is empty. In a recent work, Bachrach et al. focus on stabilizing coalition games through external payments [3]. They show that any coalition structure can be made stable through additional payments from a third party. It is important to investigate how external payments can be used to stabilize cooperative security games. The cost of stability or the minimal cost required to stabilize the games would have to be determined.

5 Conclusions and Future Work

Based on the existing models of security attacks [14, 15], we have constructed a cooperative game model that captures the economic incentives of network users in joint security measures. We summarize our findings on the cooperative behavior of players in three canonical security games.

- **Weakest-link game.** Full protection is possible if all players are pessimistic and their losses due to attack are sufficiently high. When players are optimistic, full protection is less likely to be observed.
- **Total effort game.** Full protection can be achieved if either (i) there is exactly one active player in the network or (ii) there is more than one active player, but all players are pessimistic.
- **Best shot game.** The network is fully protected if (i) there is exactly one active player or (ii) there is more than one active player, all of whom are pessimistic.

In all three games, as the network size increases, full protection becomes less probable when the players are optimistic. Clearly, the success of joint protection efforts is entirely dependent on the nature of the attack and the attitude of the defending users.

One limitation of our model is the assumption that the network consists of two sets of homogeneous players. This is reasonable in places like universities, where students (passive players) have little incentive to secure their systems, while the faculty members (active players) appreciate the need for security. Since in general, network users are heterogeneous, the model has to be suitably extended. Another assumption that we make is that every user is aware of the security decision of other users in the network. Though this assumption has been borrowed from some of the previous models of security [14, 15, 9], it may not hold always and hence, it is important to analyze cooperation in security games with incomplete information.

We conclude the paper by acknowledging that cooperation in security, though essential, is difficult when the network size is large. However, the existence of incentive-based schemes in large peer-to-peer networks [30] shows that large-scale cooperative investments are possible if suitable incentives are provided to the users. In the future, we plan to investigate the overheads that could arise in coalition formation when network users attempt to cooperatively invest in security. In order to get a better understanding of the cooperative behavior of network users, we also intend to apply the solution concept of recursive core [21] to security games.

Acknowledgement. We would like to thank the three anonymous reviewers for their valuable comments and suggestions, which helped us improve our paper.

References

1. Report of the oecd task force on spam: Anti-spam toolkit of recommended policies and measures. Directorate for Science, Technology and Industry, Committee on Consumer Policy Committee for Information, Computer and Communications Policy, April 2006.
2. R. Anderson. Why information security is hard-an economic perspective. In *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, pages 358–365, Washington, DC, USA, 2001. IEEE Computer Society.
3. Yoram Bachrach, Edith Elkind, Reshef Meir, Dmitrii Pasechnik, Michael Zuckerman, Jörg Rothe, and Jeffrey S. Rosenschein. The cost of stability in coalitional games. In *SAGT '09: Proceedings of the 2nd International Symposium on Algorithmic Game Theory*, pages 122–134, Berlin, Heidelberg, 2009. Springer-Verlag.
4. Jay Pil Choi, Chaim Fershtman, and Neil Gandal. Network security: Vulnerabilities and disclosure policy. In *Proceeding of the 2007 Workshop on the Economics of Information Security (WEIS 2007)*, Carnegie Mellon University, Pittsburgh, PA (USA), June 2007.
5. Frédéric Cuppens and Alexandre Miège. Alert correlation in a cooperative intrusion detection framework. In *SP '02: Proceedings of the 2002 IEEE Symposium on Security and Privacy*, pages 202–215, Washington, DC, USA, 2002. IEEE Computer Society.
6. Stefan Frei, Dominik Schatzmann, Bernhard Plattner, and Brian Tramme. Modelling the security ecosystem-the dynamics of (in)security. In *Proceeding of the Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 2009.
7. Deborah Frincke, Don Tobin, Jesse McConnell, Jamie Marconi, and Dean Polla. A framework for cooperative intrusion detection. In *Proc. 21st NIST-NCSC National Information Systems Security Conference*, pages 361–373, 1998.
8. Neal Fultz. Distributed attacks as security games. Technical report, US Berkeley School of Information, 2008.
9. Neal Fultz and Jens Grossklags. Blue versus red: Towards a model of distributed security attacks. In *Proceedings of the Thirteenth International Conference Financial Cryptography and Data Security*, pages 167–183, February 2009.
10. Esther Gal-Or and Anindya Ghose. The economic incentives for sharing security information. *Info. Sys. Research*, 16(2):186–208, 2005.
11. Christos Gkantsidis and Pablo Rodriguez. Cooperative security for network coding file distribution. In *Proceeding of IEEE INFOCOM'06*, pages 1–13, April 2006.
12. Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6):461–485, 2003.
13. J. Grossklags, B. Johnson, and N. Christin. When information improves information security. Technical report, CMU-CyLab-09-004, UC Berkeley & Carnegie Mellon University, CyLab, February 2009.
14. Jens Grossklags, Nicolas Christin, and John Chuang. Secure or insure? a game-theoretic analysis of information security games. In *Proceedings of the 17th International World Wide Web Conference*, pages 209–218, April 2008.
15. Jens Grossklags, Nicolas Christin, and John Chuang. Security and insurance management in networks with heterogeneous agents. In *EC '08: Proceedings of the 9th ACM conference on Electronic commerce*, pages 160–169, New York, NY, USA, 2008. ACM.
16. Jens Grossklags and Benjamin Johnson. Uncertainty in the weakest-link security game. In *GameNets'09: Proceedings of the First ICST international conference on Game Theory for Networks*, pages 673–682, Piscataway, NJ, USA, 2009. IEEE Press.

17. Jens Grossklags, Benjamin Johnson, and Nicolas Christin. The price of uncertainty in security games. In *Proceeding of the Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 2009.
18. Yi-an Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, New York, NY, USA, 2003. ACM.
19. László A. Kóczy. The core of a partition function game. Technical report, KUL Centre for Economic Studies, Working Paper No. 25, November 2000.
20. László A. Kóczy. *Solution Concepts and Outsider Behaviour in Coalition Formation Games*. PhD thesis, Centre for Economic Studies, Catholic University Leuven, 2003.
21. László A. Kóczy. A recursive core for partition function form games. *Theory and Decision*, 63(1):41–51, August 2007.
22. G. Koutepas, F. Stamatelopoulos, and B. Maglaris. Distributed management architecture for cooperative detection and reaction to ddos attacks. *J. Netw. Syst. Manage.*, 12(1):73–94, 2004.
23. Howard Kunreuther and Geoffrey Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3):231–249, March-May 2003.
24. Marc Lelarge. Economics of malware: Epidemic risks model, network externalities and incentives. In *Proceeding of the Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 2009.
25. M.E. Locasto, J.J. Parekh, A.D. Keromytis, and S.J. Stolfo. Towards collaborative security and P2P intrusion detection. In *Proceedings of 6th Annual IEEE SMC Information Assurance Workshop (IAW)*, pages 333–339, June 2005.
26. Tyler Moore. *Cooperative attack and defense in distributed networks*. PhD thesis, University of Cambridge, 2008.
27. D. Nojiri, Jeff Rowe, and Karl N. Levitt. Cooperative response strategies for large scale attack mitigation. In *3rd DARPA Information Survivability Conference and Exposition (DISCEX-III 2003)*, pages 293–302, Washington, DC, USA, April 2003.
28. Mancur Olson and Richard Zeckhauser. An economic theory of alliances. *Review of Economics and Stastistics*, 48(3):266–279, 1966.
29. M.J. Osborne and A. Rubinstein. *An Course in Game Theory*. MIT Press, USA, 1998.
30. Muntasir Raihan Rahman. A survey of incentive mechanisms in peer-to-peer systems. Technical Report CS-2009-22, Cheriton School of Computer Science, University of Waterloo, 2009.
31. Todd Sandler and Keith Hartley. Economics of alliances: The lessons for collective action. *Journal of Economic Literature*, 39(3):869–896, September 2001.
32. Robert M. Thrall and William F. Lucas. n-person games in partition function form. *Research Logistics Quarterly*, 10(1):281–298, 1963.
33. Hal R. Varian. System reliability and free riding. In *the First Workshop on Economics of Information Security*, University of California, Berkeley, May 2002.
34. Qiu-Hong Wang and Seung-Hyun Kim. Cyber attacks: Cross-country interdependence and enforcement. In *Proceeding of the Eighth Workshop on the Economics of Information Security (WEIS 2009)*, University College London, England, June 2009.

A Definitions and Notations

We now give the basic definitions required to understand partition function form games (PFGs) [19, 21].

Let $N = \{1, 2, ..., n\}$ be a finite set of players. Any non-empty subset of N is a coalition. A coalition structure or partition $\mathcal{P} = \{P_1, P_2, ..., P_k\}$ is a set of disjoint coalitions such that their union is N. Let Π be the set of all such partitions.

Definition 1. *A coalitional game in partition form consists of a finite set of players N and a partition function V that assigns a value to a coalition in a given partition, i.e. $V : 2^N \times \Pi \rightarrow \mathbb{R}$.*

Partition function games have transferable utility, i.e. a value is assigned to an entire coalition, which is shared among the coalitional members.

Definition 2. *An outcome of a partition function form game (N, V) is a pair $(x, \mathcal{P})$, where $x \in \mathbb{R}^N$ is a vector of payment allocations x_i to player $i \in N$ and $\mathcal{P} \in \Pi$ such that the following conditions are satisfied: $\forall C \in \mathcal{P}, \sum_{i \in C} x_i = V(C, \mathcal{P})$ (feasibility and efficiency) and $\forall i \in N, x_i \geq 0$ (participation rationality).*

We shall use the notation $x(S)$ to denote $\sum_{i \in S} x_i$, where $S \subseteq N$.

Definition 3. *An outcome $(x, \mathcal{P})$ dominates another outcome $(y, \mathcal{Q})$ via $S \subset N$ if $\forall i \in S$, $x_i \geq y_i$ and $\exists i \in S$ such that $x_i > y_i$.*

Note that $(x, \mathcal{P})$ dominates $(y, \mathcal{Q})$ via $S \subset N$ only if $x(S) > y(S)$. We say that an outcome $(y, \mathcal{Q})$ is dominated if there exists an outcome $(x, \mathcal{P})$ such that $x(S) > y(S)$ for some $S \subset N$. We call the players in S as deviators and those in $\bar{S} \equiv N \backslash S$ as residuals. The deviators are said to be pessimistic if they expect the worst possible outcome after deviation and are optimistic if they expect the best possible outcome after deviation.

Definition 4. *The core of a partition function game is the set of all undominated outcomes. It is of two types:*

Pessimistic Core. *An outcome $(x, \mathcal{P})$ is in the pessimistic core if there exists no outcome $(x', \mathcal{P}')$ such that for* **all** *partitions $\mathcal{P}' \supset P_S$, where P_S is a partition of some $S \subset N$, $(x', \mathcal{P}')$ dominates $(x, \mathcal{P})$ via S.*

Optimistic Core. *An outcome $(x, \mathcal{P})$ is in the optimistic core if there exists no outcome $(x', \mathcal{P}')$ such that for* ***some*** *partition $\mathcal{P}' \supset \mathcal{P}_S$, where $\mathcal{P}_S$ is a partition of some $S \subset N$, $(x', \mathcal{P}')$ dominates $(x, \mathcal{P})$ via S.*

A coalition consisting of all players in N is called the **grand coalition**. We shall denote the value of the grand coalition as $V(N)$. Note that $V(N) = V(N, \mathcal{P})$, where $\mathcal{P} = \{N\}$.

Definition 5. *A coalitional game with transferable utility is said to be cohesive if for every partition $\mathcal{P} = \{P_1, P_2, ..., P_t\}$, $t > 1$, $V(N) \geq \sum_{i=1}^{t} V(P_i, \mathcal{P})$ [29].*

Clearly, when a PFG is cohesive, the grand coalition can perform at least as well as any other coalition structure in the game [20].

B Proof of Propositions

B.1 Proposition 1

Proof. It is sufficient to prove that the three security games are cohesive.

Weakest-link Security Game. Consider a weakest-link security game in partition function form (N, V). Let $0 \leq l_i \leq n_a$ and $0 \leq k_i \leq n_p$ be the number of active and passive players respectively in a coalition P_i in partition $\mathcal{P} = \{P_1, P_2, ..., P_t\}$, $t > 1$. Considering the case where all players are protected, we get

$$\sum_{i=1}^{t} V(P_i, \mathcal{P}) = \sum_{i=1}^{t} l_i\alpha - k_i\beta = \sum_{i=1}^{t} l_i\alpha - \sum_{i=1}^{t} k_i\beta = n_a\alpha - n_p\beta = V(N).$$

When $1 \leq r_u \leq n_p$ passive players are in singleton coalitions and unprotected, we get

$$\sum_{i=1}^{t} V(P_i, \mathcal{P}) = -(n_a + n_p - r_u)b \leq V(N)$$

provided $V(N)$ is positive. In games where $V(N)$ is negative, the participation rationality condition will not hold for any partitioning of players and hence, the core would be empty. Clearly, a weakest-link security game with a non-empty core is cohesive.

Total Effort Security Game. Consider a total effort security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players. Let $0 \leq l_i \leq n_a$ and $0 \leq k_i \leq n_p$ be the number of active and passive players respectively in a coalition P_i in partition $\mathcal{P} = \{P_1, P_2, ..., P_t\}$, $t > 1$. Let $0 \leq r_p \leq n_p$ be the total number of protected passive players, i.e. the total number of passive players in non-singleton coalitions. Let $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$, where $\mathcal{P}_1$ contains the set of singleton passive players, while $\mathcal{P}_2$ contains the rest. Note that $|\mathcal{P}_1| = n_p - r_p$. Then,

$$\begin{aligned}
\sum_{i=1}^{t} V(P_i, \mathcal{P}) &= \sum_{P_i \in \mathcal{P}_1} r_p\beta' + \sum_{P_i \in \mathcal{P}_2} (r_p(l_i\alpha' + k_i\beta') - k_i b) \\
&= \sum_{P_i \in \mathcal{P}_1} r_p\beta' + r_p(\sum_{P_i \in \mathcal{P}_2} l_i\alpha' + \sum_{P_i \in \mathcal{P}_2} k_i\beta') - \sum_{P_i \in \mathcal{P}_2} k_i b \\
&= (n_p - r_p)r_p\beta' + r_p(n_a\alpha' + r_p\beta') - r_p b = r_p(n_a\alpha' + n_p\beta' - b) \\
&\leq n_p(n_a\alpha' + n_p\beta' - b) = V(N).
\end{aligned}$$

Hence, the game is cohesive.

Best Shot Security Game. Consider a best shot security game in partition function form (N, V) with $n_a > 0$ active players. Let $\mathcal{P} = \{P_1, P_2, ..., P_t\}$, $t > 1$, be a partitioning of the active players. Let $\mathcal{P} = \mathcal{Q} \cup \mathcal{R}$, where $\mathcal{Q}$ is the set of singleton coalitions, while $\mathcal{R}$ contains the rest. When $|\mathcal{R}| > 0$, players in singleton coalitions free ride on others and hence,

$$\sum_{i=1}^{t} V(P_i, \mathcal{P}) = |\mathcal{Q}|W + \sum_{R \in \mathcal{R}} (|R|W - b) = |\mathcal{Q}|W + (n_a - |\mathcal{Q}|)W - |\mathcal{R}|b$$

$$= n_a W - |\mathcal{R}| b \leq n_a W - b = V(N).$$

When $|\mathcal{R}| = 0$, either one or more players choose protection, while others free-ride on them or no one is protected. In both cases, it can be shown that the condition for cohesiveness holds. The game is thus cohesive.

B.2 Proposition 2

Proof. Consider a security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players. Let $(x, \mathcal{P})$ be an outcome with the ideal allocation vector x. An outcome $(y, \mathcal{Q})$ dominates $(x, \mathcal{P})$ via $S \subset N$ containing $0 < l \leq n_a$ active players and $0 \leq k \leq n_p$ passive players only if $y(S) > x(S)$. We need to prove that in each security game, $y(S) > x(S)$ only if $\frac{l}{n_a} > \frac{k}{n_p}$.

Weakest-link Security Game. $x(S) = \frac{l}{n_a}(n_a\alpha - n_p\beta)$ and $y(S) \leq l\alpha - k\beta$. Clearly, $y(S) > x(S)$ only if $l\frac{n_p}{n_a} > k$ or $\frac{l}{n_a} > \frac{k}{n_p}$.

Total Effort Security Game. $x(S) = \frac{l}{n_a}(n_p(n_a\alpha' + n_p\beta') - n_p b) = l n_p \alpha' - \frac{l}{n_a} n_p (b - n_p\beta')$ and $y(S) \leq n_p(l\alpha' + k\beta') - kb = l n_p \alpha' - k(b - n_p\beta')$. Since $L_p < b$, $n_p\beta' < b$ and hence, $y(S) > x(S)$ only if $k < \frac{l}{n_a} n_p$ or $\frac{l}{n_a} > \frac{k}{n_p}$.

Best Shot Security Game. The proof is trivial as $k = 0$.

B.3 Proposition 3

Proof. Consider a security game in partition function form (N, V) with n_a active players and n_p passive players and an outcome $(x, \mathcal{P})$, where x is given by (9). Assume the outcome is dominated by another outcome $(y, \mathcal{Q})$ via some subset $S_0 \subset N$ containing $0 < l \leq n_a$ active players and $0 \leq k \leq n_p$ passive players, where the partitioning $\mathcal{Q}$ corresponds to the worst case for the deviating players in S_0 if the core is pessimistic and corresponds to the best case for the players in S_0 if the core is optimistic. (Note that for a best shot security game, $k = 0$.) We now need to prove that the core is empty.

Let $f = y(S_0)$ and $T = x(N) = V(N)$. Since $(x, \mathcal{P})$ is dominated by $(y, \mathcal{Q})$ via S_0, $x(S_0) < y(S_0)$ or

$$\frac{l}{n_a} T < f. \tag{10}$$

We need to show that there exists no allocation vector x' such that for every $S_1 \subset N$ containing l active players and k passive players, $x'(S_1) \geq f$. On the contrary, assume that such an allocation exists.

Let N_p be the set of n_p passive players and let T_p be the sum of the allocations for the passive players in x'. Let t_p be the minimum value of $x'(S_p)$ for all $S_p \subset N_p$ containing k passive players. It can be easily shown that $t_p \leq \frac{k}{n_p} T_p$.

Claim. We claim that "for a set of players N and for given values of $\omega \geq 0$ and $0 < m \leq |N|$, if there exists an allocation vector z such that $z(S) \geq \omega$ for every subset $S \subset N$ of cardinality m, then $z(N) \geq \frac{|N|}{m}\omega$." (The proof is given at the end of the section.)

If x' exists, then for every $S_a \subseteq N_a$ containing l active players, $x'(S_a) \geq f - t_p$. From our claim, this is possible only if

$$T - T_p \geq \frac{n_a}{l}(f - t_p) \geq \frac{n_a}{l}(f - \frac{k}{n_p}T_p). \tag{11}$$

From proposition 2, $\frac{l}{n_a} > \frac{k}{n_p}$. Thus, (11) reduces to $T \geq \frac{n_a}{l}f$, which contradicts (10). Therefore, for every possible allocation vector, there exists a subset of l active players and k passive players in N such that they can profitably deviate. Hence, the core is empty.

Proof of Claim. The proof is by induction on m. For $m = 1$, the statement is trivial. Assume the statement is true for $m = m_1 - 1$, $m_1 > 0$. Consider an allocation vector z for a set of players N such that $z(S) \geq \omega$ for every $S \subset N$ of cardinality m_1. Let $\tilde{z} = min_{i \in N} z_i$. Clearly, when $\tilde{z} \geq \frac{\omega}{m_1}$, $z(N) \geq \frac{|N|}{m_1}\omega$. Consider the case where $\tilde{z} < \frac{\omega}{m_1}$. Let $j \in N$ be a player with allocation $z_j = \tilde{z}$ and let $N' = N - \{j\}$. Note that $z(S) \geq \omega$ for every $S \subset N$ of cardinality m_1 only if $z(S') \geq \omega - \tilde{z}$ for every $S' \subset N'$ of cardinality $m_1 - 1$. By our assumption, this is true only if $z(N') \geq \frac{|N'|}{m_1 - 1}(\omega - \tilde{z}) = \frac{|N|-1}{m_1-1}(\omega - \tilde{z})$. Then,

$$z(N) = \tilde{z} + z(N') \geq \tilde{z} + \frac{|N|-1}{m_1-1}(\omega - \tilde{z}) = \frac{|N|-1}{m_1-1}\omega - \frac{|N|-m_1}{m_1-1}\tilde{z}.$$

Since $\tilde{z} < \frac{\omega}{m_1}$,

$$z(N) \geq \frac{|N|-1}{m_1-1}\omega - \frac{|N|-m_1}{m_1-1}\frac{\omega}{m_1} = \frac{|N|}{m_1}\omega.$$

Hence, the statement is true for $m = m_1$.

B.4 Proposition 4

Proof. Consider a weakest-link security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players. From proposition 1, we state that it is enough to prove that an outcome with the grand coalition exists in the pessimistic core if and only if $n_a\alpha - n_p\beta \geq 0$.

For the grand coalition to be part of an outcome, the participation rationality condition must be satisfied. This is possible only if it has a non-zero value, i.e.

$$n_a\alpha - n_p\beta \geq 0.$$

This proves the necessity part of the proposition.

We now prove the sufficiency part, i.e. we prove that there exists an allocation vector for which an outcome containing the grand coalition exists in the pessimistic core. Consider the grand coalition with the ideal allocation x^w given by

$$x_i^w = \begin{cases} \alpha - \frac{n_p}{n_a}\beta & \text{if player } i \text{ is active} \\ 0 & \text{if player } i \text{ is passive.} \end{cases} \tag{12}$$

Consider the deviation of a set of players $S \subset N$, where S contains $0 \le l \le n_a$ active players and $0 \le k \le n_p$ passive players. Then, $x^w(S) = l\alpha - \frac{l}{n_a} n_p \beta$. Let y be the new allocation vector after the deviation. If $0 \le l \le n_a$ and $0 \le k < n_p$, in the worst case, one or more of the remaining $n_p - k$ passive players are unprotected and $y(S) \le 0 \le x^w(S)$. On the other hand, if $0 \le l < n_a$ and $k = n_p$, $y(S) \le l\alpha - n_p\beta < x^w(S)$. In both cases, the deviation is not profitable and hence, the grand coalition is present in the pessimistic core.

B.5 Proposition 5

Proof. Consider a weakest-link security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players.

The necessity of condition (i) can be proved in the same way as in proposition 4. We now prove the necessity of the second condition. Consider an outcome $(x^w, \mathcal{P})$, where $\mathcal{P} = \{N\}$ and x^w is the ideal allocation vector given by (12). By our assumption, there exists a subset of players $S \subset N$ with $0 \le l \le n_a$ active players and $0 \le k \le n_p$ passive players such that $\frac{k}{l} \ne \frac{n_p}{n_a}$ and $0 \le l\alpha - k\beta \le n_a\alpha - n_p\beta$. Note that this is possible only if $l \ne 0$ and $l \ne n_a$. When the players in S deviate, in the best case, every player in $\bar{S}$ is protected. Let $(y, \mathcal{Q})$ be the corresponding outcome. Since $\frac{k}{l} \ne \frac{n_p}{n_a}$, it can be shown that $x^w(S) \ne y(S)$. Also, $y(N) = y(S) + y(\bar{S}) = x^w(S) + x^w(\bar{S}) = x^w(N)$. It is clear that either $y(S) > x^w(S)$ or $y(\bar{S}) > x^w(\bar{S})$ must hold. Thus, $(x^w, \mathcal{P})$ is dominated by $(y, \mathcal{Q})$ via S_1, where S_1 is either S or $\bar{S}$. By proposition 3, the optimistic core is empty.

We now prove the sufficiency part. Under the conditions stated, for all values of $0 \le l \le n_a$ and $0 \le k \le n_p$, if $\frac{k}{l} \ne \frac{n_p}{n_a}$, either $l\alpha - k\beta < 0$ or $l\alpha - k\beta > n_a\alpha - n_p\beta$. In the first case, the participation rationality condition will not be satisfied for at least one deviating player. In the second case, $(n_a - l)\alpha - (n_p - k)\beta < 0$ and hence, the participation rationality condition will not be satisfied for at least one residual player. In both cases, there exists no outcome which dominates an outcome with the grand coalition. On the other hand, if there exists values of $0 \le l \le n_a$ and $0 \le k \le n_p$ such that $\frac{k}{l} = \frac{n_p}{n_a}$,

$$l\alpha - k\beta = \frac{l}{n_a}(n_a\alpha - n_p\beta) \ge 0 \text{ and}$$

$$(n_a - l)\alpha - (n_p - k)\beta = \frac{n_a - l}{n_a}(n_a\alpha - n_p\beta) \ge 0 \text{ (from condition (i))}.$$

Clearly, there exists a set of outcomes of the form $(y, \mathcal{Q})$, where $\mathcal{Q}$ does not contain the grand coalition and for every $Q \in \mathcal{Q}$ with $0 \le l \le n_a$ active players and $0 \le k \le n_p$ passive players, $\frac{k}{l} = \frac{n_p}{n_a}$. Let A be the set of all such outcomes. We show that there exists an outcome $(x^w, \mathcal{P})$, where $\mathcal{P} = \{N\}$ and x^w is given by (12), which is not dominated by any outcome in A. For all $(y, \mathcal{Q}) \in A$ and $S_i \subset N$ such that $\mathcal{Q}$ contains a partition of S_i, $y(S_i) = l_i\alpha - k_i\beta = \frac{l_i}{n_a}(n_a\alpha - n_p\beta) = x^w(S_i)$, where l_i and k_i are the number of active and passive players in S_i respectively. Hence, $(x^w, \mathcal{P})$ is not dominated and thus present in the optimistic core.

B.6 Proposition 6

Proof. Consider a total effort security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players. Consider an outcome with the grand coalition and the ideal allocation vector x^t given by

$$x_i^t = \begin{cases} \frac{n_p}{n_a}(n_a\alpha' + n_p\beta' - b) & \text{if player } i \text{ is active} \\ 0 & \text{if player } i \text{ is passive.} \end{cases} \tag{13}$$

Clearly, x^t is feasible and efficient. Since in a total effort game $\alpha' = \frac{L_a}{n} > b$, the allocation for an active player in x^t is non-negative. Hence, x^t satisfies the partition rationality condition.

Consider the deviation of a set of players $S \subset N$ from the given outcome, where S contains $0 \leq l \leq n_a$ active players and $0 \leq k \leq n_p$ passive players. Note that $x^t(S) = \frac{l}{n_a}n_p(n_a\alpha' + n_p\beta' - b)$. In the worst case, the remaining $n_p - k$ passive players are unprotected. If y is the corresponding allocation vector after the deviation, $y(S) \leq k(l\alpha' + k\beta' - b)$. Assume the deviation is profitable for the players in S. Then, $y(S) > x^t(S)$, which implies

$$k(l\alpha' + k\beta' - b) > \frac{l}{n_a}n_p(n_a\alpha' + n_p\beta' - b).$$

From proposition 2, $k < \frac{l}{n_a}n_p$ and hence,

$$l\alpha' + k\beta' > n_a\alpha' + n_p\beta'.$$

Since $l \leq n_a$ and $k \leq n_p$, this is not possible and hence, a contradiction. Hence, no deviation from the grand coalition with the ideal allocation is profitable. As the pessimistic core contains an outcome with the grand coalition, it is non-empty.

B.7 Proposition 7

Proof. Consider a total effort security game in partition function form (N, V) with $n_a > 0$ active players and $n_p > 0$ passive players.

Assume $n_a > 1$. To prove the necessity part, it is enough to show that the outcome with the grand coalition and the ideal allocation vector x^t given by (13) is dominated via a set of players containing at least one active player. (Refer propositions 1 and 3.) Consider the deviation of a single active player i. As $\alpha' \geq b$, $n_p((n_a - 1)\alpha' + n_p\beta' - b) \geq 0$ and thus, all residual players are protected in the best case. In the corresponding outcome, the allocation to the active player i is $n_p\alpha' > \frac{n_p}{n_a}(n_a\alpha' - (b - n_p\beta')) = x(\{i\})$ as $b > n_p\beta'$. The deviation is therefore profitable for player i and hence, the grand coalition with the ideal allocation vector x^t does not exist in the optimistic core.

We now prove the sufficiency part. Assume $n_a = 1$. Consider an outcome $(x, \mathcal{P})$, where $\mathcal{P} = \{N\}$, $x_i \geq 0$ for every active player i, $x_j \geq (n_p - 1)\beta'$ for every passive player j and $x(N) = n_p(n_a\alpha' + n_p\beta' - b)$. We prove that this outcome exists in the optimistic core. Consider the deviation of a set of players $S \subset N$ containing $0 \leq l \leq 1$ active players and $0 \leq k \leq n_p$ passive players. If $l = 0$, none of the deviating players are protected. Since $\alpha' > b$, $(n_p - k)(\alpha' + (n_p - k)\beta' - b) \geq 0$ and thus all residual players are protected in the best case. Let y be the corresponding allocation vector after deviation. Since $y(S) = k(n_p - 1)\beta' \leq x(S)$, the deviation is not profitable. On the other hand, if $l = 1$, none of the residual players are protected. As shown in proposition 6, the deviation will not be profitable. Thus, the core is non-empty when $n_a = 1$.

B.8 Proposition 8

Proof. Consider a best shot security game in partition function form (N, V) with $n_a > 1$ active players. Consider the outcome $(x^b, \mathcal{P})$, where $\mathcal{P} = \{N\}$ and x^b is the ideal allocation vector given by $x_i^b = W - \frac{b}{n_a}$. Consider the deviation of a set of players $S \subset N$, where $1 \leq |S| < n_a$. In the worst case, at least one of the $n_a - |S| > 0$ residual players may remain unprotected. Let $(y, \mathcal{Q})$ be the corresponding outcome. Then,

$$y(S) = \begin{cases} W - \frac{b}{|S|} & \text{if } |S| > 1 \\ W - b & \text{if } |S| = 1 \text{ and the single player is protected} \\ W - L_a & \text{if } |S| = 1 \text{ and the single player is unprotected.} \end{cases}$$

Since $y(S) < W - \frac{b}{n_a} = x^b(S)$ for every $S \subset N$, no deviation from the grand coalition with the ideal allocation is profitable and hence, the pessimistic core is non-empty.

B.9 Proposition 9

Proof. Consider a best shot security game in partition function form (N, V) with $n_a > 1$ active players. Consider the outcome $(x, \mathcal{P})$, where $\mathcal{P} = \{N\}$ and x^b is the ideal allocation vector given by $x_i^b = W - \frac{b}{n_a}$. From propositions 1 and 3, we state that it is sufficient to prove that this outcome is dominated via a set containing at least one active player. Any player i in the grand coalition can deviate by remaining single and unprotected hoping that in the best case, at least one residual player is protected. Let $(y, \mathcal{Q})$ be the resultant outcome after deviation. Since $y(\{i\}) = W > W - \frac{b}{n_a} = x^b(\{i\})$, the deviation is profitable and hence, the optimistic core is empty.