

A Game-Theoretical Approach to Incentive Design in Collaborative Intrusion Detection Networks

Quanyan Zhu, Carol Fung, Raouf Boutaba, and Tamer Başar

Abstract—Traditional intrusion detection systems (IDSs) work in isolation and may be easily compromised by new threats. An intrusion detection network (IDN) is a collaborative IDS network intended to overcome this weakness by allowing IDS peers to share collective knowledge and experience, hence improve the overall accuracy of intrusion assessment. In this work, we design an incentive model based on trust management by using game theory for peers to collaborate truthfully without free-riding in an IDN environment. We show the existence and uniqueness of a Nash equilibrium under which peers can communicate in an incentive compatible manner. Using duality of the problem, we develop an iterative algorithm that converges geometrically to the equilibrium. Our numerical experiments and discrete event simulation demonstrate the convergence to the Nash equilibrium and the incentives of the resource allocation design.

I. INTRODUCTION

Intrusion Detection Systems (IDSs) identify intrusions by comparing observable behavior against suspicious patterns. They can be network-based (NIDS) or host-based (HIDS). Traditional IDSs work in isolation and may be easily compromised by unknown or new threats. An Intrusion Detection Network (IDN) is a collaborative IDS network intended to overcome this weakness by having each peer IDS benefit from the collective knowledge and experience shared by other peers. This enhances the overall accuracy of intrusion assessment as well as the ability of detecting new intrusion types. However, many proposed IDS collaboration systems, such as [1], [2], and [3], assume all IDSs cooperate honestly. The lack of trust management leaves the system vulnerable to malicious peers.

A few trust-based collaboration systems (e.g. [4] and [5]) and distributed trust management models (e.g. [5], [6], and [7]) have been proposed for IDSs to cooperate with each other effectively. However, none of these proposed models have studied incentives for IDS collaboration. Without incentives, a collaboration system may suffer from a “free-rider” problem [8], where some IDSs may take advantage of others by always asking for assistance from others but not contributing. This will eventually degrade the expected performance of the collaboration system. Therefore, an effective incentive design is important to encourage peers in the IDN to cooperate truthfully and actively.

Quanyan Zhu and Tamer Başar are with the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana Champaign (1308 West Main, Urbana, IL 61801, USA); E-mail: {zhu31,tbasar}@decision.csl.uiuc.edu. Carol Fung and Raouf Boutaba are with the Cheriton School of Computer Science at University of Waterloo, Ontario, Canada; E-mail: {j22fung,rboutaba}@cs.uwaterloo.ca

More specifically, as shown in Figure 1, an IDN is composed of a group of independent IDSs and the communication among the peers is through a peer-to-peer communication layer. An IDS may send requests to selected neighbors to seek assistance when suspicious activities are detected. These requests can be related to alert ranking, problem diagnosis, or blacklist identification. The responses from its neighbors can help the IDS to identify new types of intrusions. An IDS may receive requests from different peers. Responding to those requests requires a certain amount of computing resources, such as CPU, memory, or network bandwidth. An IDS may have a limited resource budget to assist other IDSs in the network and cannot satisfy all the requests. An IDS may also free-ride the system or send out false intrusion assessments. Therefore, an effective resource allocation scheme is needed for an IDS to manage responses to requests from neighboring IDSs.

In this work, we propose an incentive compatible resource allocation scheme for trust-based IDS collaboration networks, where the amount of resources that each IDS allocates to help its neighbors is proportional to the trustworthiness and the amount of resources allocated by its neighbors to help this IDS. We construct an optimization problem where an IDS can find an optimal resource allocation to maximize the aggregated satisfaction levels of its neighbors. We introduce an N -person (or peer) non-cooperative game to investigate incentive compatibility of the IDS collaboration system. We show that under certain controllable system conditions, there exists a unique Nash equilibrium. Our experimental results demonstrate that an iterative algorithm which we introduce converges geometrically fast to the Nash equilibrium, and the amount of help an IDS receives from others is proportional to its helpfulness to others.

The contributions of this paper are: 1) a mechanism for optimal resource allocation for each peer to maximize its social welfare with a convex utility function, 2) an N -person non-cooperative game model and an iterative primal/dual algorithm to reach the Nash equilibrium, and 3) incentive compatibility that is derived from the resource allocation scheme to avoid the “free-rider” problem.

The rest of this paper is organized as follows: Section II presents a brief overview of related work from other areas. In section III, we describe our incentive compatible resource allocation scheme. In Section IV, we devise a primal/dual algorithm to compute the Nash equilibrium, and in Section V we evaluate the convergence and incentives of the resource allocation design. Finally, Section VI concludes this paper.

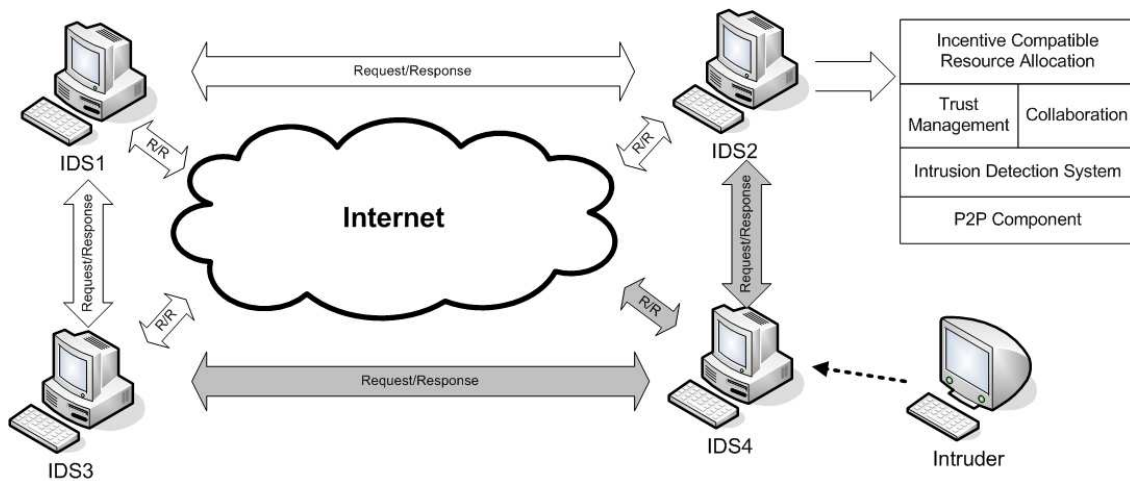


Fig. 1. Architecture of an IDS Collaboration System

A list of symbols and notations, as well as their information patterns, is summarized in Table I for readers' convenience.

II. RELATED WORK

Much work has been done for the collaborative framework and trust management among intrusion detection systems, such as [5], [6], [7]. In our previous work for trust management in IDS collaboration, we have proposed a trust management system where IDSs exchange test messages to build trust among themselves. Each IDS selects a trace of possible attacks from its knowledge database where the risk level of the attack is known by the IDS. Then, it sends the trace to its acquaintances for the purpose of testing their trustworthiness. Each acquaintance evaluates the risk of the possible attacks based on the trace it receives and sends back the feedback to the sender. The sender IDS compares the feedbacks from others with its own knowledge and generates a satisfaction level for each feedback using a satisfaction mapping function. A trust value is a numerical value used to predict the level of truthfulness for the next feedback from a certain peer. [5] uses a simple weighted average model to predict the trust value while [7] uses a Bayesian statistics model to estimate the trust value as well as the confidence level of the trust estimation.

Incentive design has been well studied in peer-to-peer (P2P) networks. Ma et al. [9] have used a game-theoretical approach to achieve differentiated services allocation based on the history of a peer's contribution to the community. However, this system relies on a centralized contribution ranking system which constitutes a single-point-of-failure. Yan et al. [10] have proposed an optimal resource allocation scheme for file providers. The resource allocation is based on the ranking of consumers of files shared by file providers. A max-min optimization problem has been constructed to find the optimal solution which achieves fairness in the resource allocation. However, their approach relies on an independent ranking system, and the relation between ranking and the contributions of consumers has not been studied. The authors also have not studied the convergence of the resource

allocation of the entire system. Theodorakopoulos and Baras [11] have used a game-theoretical approach to study the impact of malicious users in P2P networks. The modeling of malicious behavior there is based on users' choice of either "cooperate" or "defect" at each time slot. A game learning algorithm is used for each peer to make a decision at each stage by aggregating the play history in a certain way. However, there is no theoretical result yet to show the convergence of fictitious play to a unique Nash equilibrium in the general topology for the proposed model.

Incentive compatibility has also been an important topic in auction design whose analysis heavily relies on game-theoretical approach, [12], [13]. For example, in [12], incentive compatibility relates to a mechanism in which bidders can only benefit the most by bidding at their true valuations. It is also shown in [12] that under certain conditions, the bidding profiles converge to a Nash equilibrium which provides an efficient allocation of the resource under this mechanism.

Recently, game-theoretical methods have been used for intrusion detection where in a two-player context, the attacker (intruder) is one player and the intrusion detection system (IDS) is the other player. Most of the existing work appears in the context of matrix games in either normal form or extensive form, but there are also a few exceptions to that. In [14], cooperative game theory, namely, Shapley value, has been used to analyze the relative importance of each sensor in an intrusion detection system, and a two-person, non-zero-sum, single-act, finite game with dynamic information is used to model the interaction between the attacker and the IDS. In [15], [16] and [17] also non-cooperative game frameworks have been used to address different aspects of intrusion detection. In [18], Liu et al. use a Bayesian game approach for intrusion detection in ad-hoc networks; a two-person non-zero-sum incomplete information game is formulated to provide a framework for an IDS to minimize its loss based on its own belief. It appears, however, that game theory has not yet been used to study incentive compatibility problems in networked IDS systems.

TABLE I
NOTATIONS

Symbol	Meaning	Information Private to
T_v^u	Trust value of v perceived by u	u
p_{uv}	Frequency of help response from u to v	u, v
r_{vu}	Desired reply rate request of v to u	u, v
m_{vu}	Minimum reply rate request of v to u	u, v
C_u	Resource capacity of u	u
$S_{u,v}$	Satisfaction level of node u in response to v	u, v

III. RESOURCE ALLOCATION AND INCENTIVE DESIGN

In this section, we first mathematically model resource allocation in an IDN environment as independent optimization problems for its member peers. A game problem (GP) can then be defined for each peer. We use Lagrangian relaxation to solve this problem for Nash equilibrium. Finally, we prove that there exists a unique Nash equilibrium in the game.

A. Modeling of Resource Allocation

We consider an IDN with N peers or nodes. We denote the set of nodes by $\mathcal{N} = \{1, 2, \dots, N\}$. The set of neighbor nodes of peer u is denoted by \mathcal{N}_u^d , which is parameterized by a given distance $d \in \mathbb{R}_+$, i.e., $\mathcal{N}_u^d = \{i \in \mathcal{N} : \text{dist}(i, u) \leq d, i \neq u\}$, where $\text{dist} : \mathcal{N} \times \mathcal{N} \rightarrow \mathbb{R}_+$ is a distance function measuring the distance between two nodes. For convenience, we let $\mathcal{N}_u^\infty = \mathcal{N} - \{u\}$, a set of all nodes in a network except the peer itself. Note that information in the network is symmetric. If u is a neighbor of v , then v is also a neighbor of u . We use r_{vu} to denote the units of resource that node u should allocate in order to serve v with full satisfaction. The minimum acceptable resource from u to v is m_{vu} . Let $p_{uv} \in \mathbb{R}_+$ be the resource that u allocates to v , for every $u, v \in \mathcal{N}$. The parameter p_{uv} is a decision variable of peer u and is private information between peer u and peer v . To satisfy neighbor v , node u should allocate resource to v over the interval $[m_{vu}, r_{vu}]$.

In this model, we assume that for each node, the trust values of its neighbors are given. This assumption is practical if a distributed trust management exists in the system, as shown in Figure 1. Let $T_v^u \in [0, 1]$ be the trust value of peer v assessed by peer u , representing how much peer u trusts peer v . The allocated resource p_{uv} from peer u to v is closely related to the trust value T_v^u perceived by u .

Each peer maximizes its effort to help its neighbor nodes under its capacity constraint C_u , which is dependent on its own resource capacity such as bandwidth, CPU, memory, etc. Then, resource allocation should satisfy the following capacity constraint:

$$\sum_{v \in \mathcal{N}_u^d} p_{uv} \leq C_u, \text{ for all } u \in \mathcal{N}. \quad (1)$$

Our system introduces a utility function for each peer to model the satisfaction level of its neighbors. The utility function S_{uv} is given by

$$S_{uv} = \frac{\ln\left(\alpha \frac{p_{uv} - m_{vu}}{r_{vu} - m_{vu}} + 1\right)}{\ln(\alpha + 1)}, \quad (2)$$

where $\alpha \in (0, \infty)$ is a system parameter which controls the satisfaction curve and the term $\ln(\alpha + 1)$ in the denominator is the normalization factor. The function S_{uv} is a concave function on its domain. The choice of \ln function is also motivated by its property of proportional fairness.

Let $U_u : \mathbb{R}_+^{L(u,d)} \rightarrow \mathbb{R}_+$ be the peer u 's aggregated altruistic utility, where $L(u, d) = \text{card}(\mathcal{N}_u^d)$, the cardinality of the set \mathcal{N}_u^d . Let the payoff function, U_u , for u be given by:

$$U_u = \sum_{v \in \mathcal{N}_u^d} w_{uv} S_{uv}, \quad w_{uv} = T_v^u p_{vu}, \quad (3)$$

where w_{uv} is the weight on peer v 's satisfaction level S_{uv} , which is the product of peer v 's trust value and amount of helping resource allocated to u . A higher weight is applied on peer v 's satisfaction level S_{uv} if peer v is better trusted and more generous to provide help to u . In this system, each peer $u \in \mathcal{N}$ in the IDN intends to maximize U_u within its resource capacity. A general optimization problem (OP) can then be formulated as follows:

$$\begin{aligned} \max_{\{p_{uv}, v \in \mathcal{N}_u^d\}} & \sum_{v \in \mathcal{N}_u^d} w_{uv} S_{uv} \\ \text{s.t.} & \sum_{v \in \mathcal{N}_u^d} p_{uv} \leq C_u \\ & m_{vu} \leq p_{uv} \leq r_{vu}, \forall v \in \mathcal{N}_u^d, \end{aligned} \quad (4)$$

where S_{uv} and w_{uv} are given by (2) and (3), respectively.

Every peer in the network is faced with an optimization problem (OP) to solve. The problem (OP) is a concave problem in which its objective function is a concave function in p_{uv} and the constraint set is an $L(u, d)$ -dimensional simplex, where $L(u, d) = \text{card}(\mathcal{N}_u^d)$, the cardinality of the set \mathcal{N}_u^d . Under the assumptions that the size of the network is large and peers can only communicate locally within a distance d , we have N independent optimization problems in the form of (OP) for each node. Hence, we can introduce a corresponding game (GP) by the triplet $\langle \mathcal{N}, A_u, U_u \rangle$, where \mathcal{N} is the set of players or peers, $A_u, u \in \mathcal{N}$, is the action set of each peer, and U_u is the payoff function of peer u , defined in (3). An action of a peer here is a decision on the resource allocated to a neighbor peer. The action set of each peer A_u is given by $A_u = A_u^1 \cap A_u^2$, where $A_u^1 = \{\mathbf{p}_u \in \mathbb{R}_+^{L(u,d)} \mid \sum_{v \in \mathcal{N}_u^d} p_{uv} \leq C_u\}$ and $A_u^2 = \{\mathbf{p}_u \in \mathbb{R}_+^{L(u,d)} \mid m_{vu} \leq p_{uv} \leq r_{vu}, v \in \mathcal{N}_u^d\}$. It is not difficult to prove that under the condition

$$C_u \geq \sum_{v \in \mathcal{N}_u^d} m_{vu}, \quad (5)$$

the action set is nonempty.

We note that the decision variable of each peer is a vector \mathbf{p}_u and the action sets of players are not coupled. We thus can use Lagrangian relaxation to penalize the constraints to solve for the Nash equilibrium. Let $\mathcal{L}_u(\mathbf{p}_u, \sigma_u, \mu_u, \lambda_u)$ as follows denote the Lagrangian of peer u 's optimization problem:

$$\begin{aligned} \mathcal{L}_u(\mathbf{p}_u, \sigma_u, \mu_u, \lambda_u) &= \sum_{v \in \mathcal{N}_u^d} \frac{T_v^u p_{vu}}{\ln(1+\alpha)} \\ &\cdot \ln \left(1 + \alpha \frac{p_{uv} - m_{vu}}{r_{vu} - m_{vu}} \right) - \sum_{v \in \mathcal{N}_u^d} \mu_{uv} (p_{uv} - r_{vu}) \\ &+ \sum_{v \in \mathcal{N}_u^d} \sigma_{uv} (p_{uv} - m_{vu}) - \lambda_u \left(\sum_{v \in \mathcal{N}_u^d} p_{uv} - C_u \right), \end{aligned}$$

where $\mu_{uv}, \sigma_{uv}, \lambda_u \in \mathbb{R}_+$ are the Lagrange multipliers. Using Lagrangian relaxation, we can transform the game (GP) to its relaxed counterpart (RGP), where the abbreviation ‘‘R’’ is short for ‘‘Relaxed’’. The triplet of the relaxed game (RGP) is given by $\langle \mathcal{N}, \bar{A}_u, \mathcal{L}_u \rangle$, where \bar{A}_u is the action set described by the base constraint $p_{uv} \geq 0$, i.e., $\bar{A}_u = \{\mathbf{p}_u \mid p_{uv} \geq 0, v \in \mathcal{N}_u^d\}$; and the payoff function is replaced by the relaxed Lagrangian function \mathcal{L}_u .

Remark 3.1: In the definition of the relaxed game (RGP), we chose to relax simultaneously the two sets of constraints, capacity constraint and range constraints. Instead, we could have relaxed only the capacity constraint. In that case, the action set \bar{A}_u in the relaxed game would include a range constraint, i.e.,

$$\bar{A}_u = \{\mathbf{p}_u \mid m_{vu} \leq p_{uv} \leq r_{vu}, v \in \mathcal{N}_u^d\}.$$

Remark 3.2: By formulating the problem as a game, we use a non-cooperative approach to model altruistic behavior among peers. The non-cooperativeness is appropriate here because there is no centralized control agent in the network, and communications between peers are local and symmetric. The aggregated utility comes from peers’ general intention to help other peers. We assume that peers intend to be altruistic when they are introduced into the network. Free-riding peers are penalized via the weighting of the aggregation function. When one peer appears to refuse to help other peers, the other peers will correspondingly decline to assist in return, and as a result free-riding is avoided.

B. Characterization of Nash Equilibrium

In this section, we solve the game (GP) for its Nash equilibrium. Each peer u has a concave optimization problem as in (4). Applying the first-order KKT condition as in [19] and [20] to each peer’s concave problem in (OP),

$$\frac{\partial \mathcal{L}_u}{\partial p_{uv}} = 0, \forall v \in \mathcal{N}_u^d, u \in \mathcal{N}, \quad (6)$$

we find

$$\frac{\delta_{uv} T_v^u p_{vu}}{1 + \alpha'_{uv} p_{uv} - \alpha'_{uv} m_{vu}} = \xi_{uv}, \forall v \in \mathcal{N}_u^d, u \in \mathcal{N}, \quad (7)$$

where

$$\delta_{uv} = \frac{\alpha'_{uv}}{\ln(1+\alpha)} ; \xi_{uv} = -\sigma_{uv} + \mu_{uv} + \lambda_u$$

and

$$\alpha'_{uv} = \frac{\alpha}{r_{vu} - m_{vu}}.$$

In addition, from the feasibility condition, it is required that an optimal solution satisfies the base constraints in \bar{A}_u and the complimentary slackness conditions for every $u \in \mathcal{N}$:

$$\lambda_u \left(\sum_{v \in \mathcal{N}_u^d} p_{uv} - C_u \right) = 0. \quad (8)$$

$$\sigma_{uv} (p_{uv} - m_{vu}) = 0, \forall v \in \mathcal{N}_u^d, \quad (9)$$

$$\mu_{uv} (p_{uv} - r_{vu}) = 0, \forall v \in \mathcal{N}_u^d. \quad (10)$$

The variable ξ_{uv} is composed of three Lagrange multipliers. If $\xi_{uv} \neq 0$, we can further simplify (7) into

$$p_{uv} - \frac{T_v^u p_{vu}}{\xi_{uv} \ln(1+\alpha)} = \left(1 + \frac{1}{\alpha} \right) m_{vu} - \frac{1}{\alpha} r_{vu}. \quad (11)$$

Definition 3.1: (Başar & Olsder, [21]) A Nash equilibrium $\mathbf{p}_{uv}^*, u, v \in \mathcal{N}$ for the game (GP) is a point that satisfies

$$\mathcal{L}_u(\mathbf{p}_u^*, \mathbf{p}_{-u}^*) \geq \mathcal{L}_u(\mathbf{p}_u, \mathbf{p}_{-u}^*), \forall \mathbf{p}_u \in A_u, u \in \mathcal{N}, \quad (12)$$

and $p_{uv} = p_{vu} = 0$, for $v \in \mathcal{N}_u \setminus \mathcal{N}_u^d$ and $u \in \mathcal{N}$, where the vector $\mathbf{p}_{-u} = \{\mathbf{p}_i : i \neq u, i \in \mathcal{N}\}$ is comprised of decision vectors of other peers.

Theorem 3.1: (Başar & Olsder, [21]) For each $u \in \mathcal{N}$, let A_u be a closed, bounded and convex subset of a finite-dimensional Euclidean space, and the payoff functional $U_u : A_1 \times A_2 \cdots \times A_N \rightarrow \mathbb{R}$ be jointly continuous in all its arguments and strictly concave in $\mathbf{p}_u \in A_u$ for every $u \in \mathcal{N}$. Then, the associated N -person non-zero-sum game admits a Nash equilibrium in pure strategies.

Relying on Theorem 3.1, we can show that the game (GP) admits a Nash equilibrium.

Proposition 3.2: The game (GP) admits a Nash equilibrium in pure strategies.

Proof: The action set A_u is a closed and bounded simplex and U_u is continuous in p_{uv} for all $u \in \mathcal{N}, v \in \mathcal{N}_u^d$ and concave in \mathbf{p}_u . By Theorem 3.1, there exists a Nash equilibrium to (GP). ■

With the existence of Nash equilibrium at hand, we can further investigate the solutions to the relaxed game by looking at a pair of nodes u and v . Node u has its decision vector \mathbf{p}_u satisfying (11) and similarly, node v has its decision vector \mathbf{p}_v satisfying (11) by interchanging indices u and v . Hence, we obtain a pair of equations involving p_{uv} and p_{vu} and they are described by

$$\begin{aligned} &\begin{bmatrix} 1 & -\frac{T_v^u}{\xi_{uv}(\ln(1+\alpha))} \\ -\frac{T_u^v}{\xi_{vu}(\ln(1+\alpha))} & 1 \end{bmatrix} \begin{bmatrix} p_{uv} \\ p_{vu} \end{bmatrix} \\ &= \begin{bmatrix} \left(1 + \frac{1}{\alpha} \right) m_{vu} - \frac{1}{\alpha} r_{vu} \\ \left(1 + \frac{1}{\alpha} \right) m_{uv} - \frac{1}{\alpha} r_{uv} \end{bmatrix}, \quad (13) \end{aligned}$$

or in the matrix form,

$$\mathbf{M}_{uv}\mathbf{q}_{uv} = \mathbf{b}_{uv}, \quad (14)$$

where $\mathbf{q}_{uv} = [p_{uv}, p_{vu}]^T$, and \mathbf{b}_{uv} is the right-hand side vector and \mathbf{M}_{uv} is the incident matrix.

Definition 3.2: (*M*-matrix, [22]) An N by N real matrix $\mathbf{A} = [A_{ij}]$ is called an *M*-matrix if it is of the form $\mathbf{A} = \theta\mathbf{I} - \mathbf{P}$, where \mathbf{P} is entrywise nonnegative and θ is larger than the spectral radius of \mathbf{P} , i.e., $\theta > \rho(\mathbf{P})$. An *M*-matrix A has two key features:

- 1) the sign patterns $a_{ii} > 0$, $i = 1, \dots, N$ and $a_{ij} \leq 0$ $i \neq j$
- 2) the eigenvalues of A have all positive real parts.

Theorem 3.3: [22] If \mathbf{A} is an *M*-matrix, then $\mathbf{A}^{-1} > 0$, i.e. all of its entries are positive.

Using Theorem 3.3, we next state a result on uniqueness of Nash equilibrium for a sufficiently large system parameter α .

Theorem 3.4: Suppose only capacity constraints are active and

$$\alpha > \max_{u,v} \left\{ e^{\frac{T_v^u}{\xi_{uv}}}, \frac{r_{vu}}{m_{vu}} \right\} - 1. \quad (15)$$

Then, the game admits a unique Nash equilibrium. For each pair of peers u and v , the equilibrium is given by

$$\mathbf{q}_{uv}^* = \mathbf{M}_{uv}^{-1}\mathbf{b}_{uv}, \forall u, v \in \mathcal{N}. \quad (16)$$

Proof: Under the condition that the capacity constraint is active, $\xi_{uv} = k_v\lambda_u > 0$, since the objective function is an increasing function. Firstly, we show that provided that $\alpha > e^{\frac{T_v^u}{\xi_{uv}}} - 1$, we have the inequality $1 > \frac{T_v^u}{\xi_{uv} \ln(1+\alpha)}$. For each pair of nodes u and v , matrix \mathbf{M}_{uv} is an *M*-matrix in (11); hence, \mathbf{M}_{uv} is strictly diagonally dominant and thus non-singular; and by Theorem 3.3, the entries of the inverse matrix \mathbf{M}_{uv}^{-1} is strictly positive.

Secondly, provided that $\alpha > \frac{r_{vu}}{m_{vu}} - 1$, the vector \mathbf{b}_{uv} is positive, i.e., $(1 + \frac{1}{\alpha})m_{vu} > \frac{1}{\alpha}r_{vu}$. Using (14) together with the conclusion above, we arrive at a unique solution given by (16), whose entries are all positive, residing in the base constraint action set \bar{A}_u for all u . Since (11) holds for any interactive pair, the game admits a unique Nash equilibrium under conditions in Theorem 3.4. ■

Remark 3.3: Under general conditions, to have $\xi_{uv} > 0$ requires multipliers μ_{uv} , λ_u , σ_{uv} to satisfy $\mu_{uv} + \lambda_u k_v > \sigma_{uv}$. Since payoff function U_u is increasing in p_{uv} , $\lambda_u > 0$ and only μ_{uv} and σ_{uv} can be zero. To ensure $\xi_{uv} > 0$, we can separate into three cases for general discussion: (1) when $\sigma_{uv} = 0$, $\mu_{uv} \neq 0$, we require $\mu_{uv} + \lambda_u k_v > 0$; (2) when $\sigma_{uv} = 0$, $\mu_{uv} = 0$, we require $\lambda_u k_v > 0$; (3) when $\sigma_{uv} \neq 0$, $\mu_{uv} = 0$, we require $\lambda_u k_v > \sigma_{uv}$. With an assumption as in Theorem 3.4 that only capacity constraint is active, it simply leads to $\xi_{uv} > 0$ itself.

C. Incentive Compatibility

We call a network design incentive compatible when at the steady state, the helping resource p_{uv} from peer u to v increases as the helping resource p_{vu} from peer v to u also increases. In addition, it is also desirable to have p_{uv} to be

proportional to the trust value of v , i.e., the more peer u trusts peer v , the more help u is willing to give. We can further study these properties of the solution obtained in (7) and (16).

Proposition 3.5: Under the conditions of Theorem 3.4, the Nash equilibrium solution of the game (GP) is incentive compatible, i.e.,

- 1) the helping resource p_{uv} from u to v increases with helping resource p_{vu} from v to u ;
- 2) when the system parameter α increases, the marginal helping resource from u to v decreases for all u and v ;
- 3) when peer u trusts v more, i.e., T_v^u increases, the marginal helping resource from u to v increases.

Proof: Using (7), we take the derivative with respect to p_{vu} and denote $\partial p_{uv} / \partial p_{vu}$ as marginal helping rate from u to v .

$$\begin{aligned} \frac{\partial p_{uv}}{\partial p_{vu}} &= \frac{\partial}{\partial p_{vu}} \left\{ \left(1 + \frac{1}{\alpha}\right) m_{vu} - \frac{1}{\alpha} r_{vu} + \frac{T_v^u p_{vu}}{\xi_{uv} \ln(1+\alpha)} \right\} \\ &= \frac{T_v^u}{\xi_{uv} \ln(1+\alpha)} \end{aligned}$$

Since $T_v^u > 0$, $\xi_{uv} > 0$, under the conditions in Theorem 3.4, we have $\frac{\partial p_{uv}}{\partial p_{vu}} > 0$, and thus p_{uv} is increasing with p_{vu} at Nash equilibrium. The incentive compatibility results follow. ■

IV. PRIMAL / DUAL ITERATIVE ALGORITHM

In this section, we introduce a dynamic algorithm to compute the unique Nash equilibrium. Let $p_{uv}(t)$ be the resource from peer u to v at step t . Consider the algorithm:

$$\begin{cases} p_{uv}(t+1) = s_{uv} + t_{uv} p_{vu}(t) \\ p_{vu}(t+1) = s_{vu} + t_{vu} p_{uv}(t) \end{cases}, \quad (17)$$

where

$$s_{uv} = \left(1 + \frac{1}{\alpha}\right) m_{vu} - \frac{1}{\alpha} r_{vu}, \quad t_{uv} = \frac{T_v^u}{\xi_{uv} \ln(1+\alpha)},$$

and s_{vu} , t_{vu} are defined similarly by interchanging indices u and v .

Proposition 4.1: Suppose that capacity constraints are active, and r_{vu} and m_{uv} are chosen such that they are large and small enough to be inactive constraints, i.e., $\sigma_{uv} = 0$, $\mu_{uv} = 0$ in (9) and (10). Given a Lagrange multiplier $\lambda_u^* \neq 0$ and provided that $\alpha > e^{\frac{T_v^u}{\lambda_u^*}} - 1$, algorithm (17) converges to the unique Nash equilibrium in (16) at dual optimal λ_u^* .

The algorithm described in (17) depends on the Lagrange multiplier λ_u . We can exploit duality to devise an iterative algorithm for the Lagrange multiplier. Let $D_u(\lambda_u)$ be the dual functional given by

$$D_u(\lambda_u) = \max_{\mathbf{p}_u} \mathcal{L}_u(\mathbf{p}_u, \lambda_u). \quad (18)$$

The dual function $D_u(\lambda_u)$ is a convex function and a dual optimal λ_u^* solves the dual optimization problem (DP)¹

$$\min_{\lambda_u > 0} D_u(\lambda_u). \quad (19)$$

Using the solution from (16), we can obtain $D_u(\lambda_u)$ as

$$D_u = \lambda_u \left(C_u + \frac{KR}{\alpha} + \left(1 + \frac{1}{\alpha}\right) KM \right) + \frac{\overline{PT} - PT}{\ln(\alpha + 1)},$$

and its first-order derivative in (20) as below

$$\begin{aligned} D'_u(\lambda_u) &= C_u - \frac{\sum_{v \in \mathcal{N}_u^d} p_{vu} T_v^u}{\lambda_u \ln(1 + \alpha)} + \frac{1}{\alpha} \sum_{v \in \mathcal{N}_u^d} r_{vu} \\ &\quad - \left(1 + \frac{1}{\alpha}\right) \sum_{v \in \mathcal{N}_u^d} m_{vu}, \end{aligned} \quad (20)$$

where $PT = \sum_{v \in \mathcal{N}_u^d} p_{vu} T_v^u$ is the sum of the weights; $KM = \sum_{v \in \mathcal{N}_u^d} m_{vu}$; $KR = \sum_{v \in \mathcal{N}_u^d} r_{vu}$. KM and KR can be interpreted as the total request weighted by marginal costs; and

$$\overline{PT} = \sum_{v \in \mathcal{N}_u^d} p_{vu} T_v^u \ln \left(\frac{\alpha}{\ln(\alpha + 1)} \frac{p_{vu} T_v^u}{\lambda_u (r_{vu} - m_{vu})} \right) \quad (21)$$

The gradient of the dual function in (20) is dependent on the local capacity of node u and the information sent by the neighbor node v of peer u such as the helping resource p_{vu} , and the maximum (minimum) requested resources r_{vu} (m_{vu}) from v . All the information is available to peer u to calculate the gradient locally at each λ_u .

By taking the second-order derivative of the dual function, we obtain

$$D''_u(\lambda_u) = \frac{\sum_{v \in \mathcal{N}_u^d} p_{vu} T_v^u}{\lambda_u^2 \ln(1 + \alpha)}. \quad (22)$$

The dual function in (19) is not only a convex function but also a strong convex function, whose Hessian is bounded uniformly as in $L_1 \leq \nabla^2 D_u(\lambda_u)$, for some L_1 [20]. In addition, provided that the sum of weights w_{uv} are bounded from above, i.e.,

$$\sum_{v \in \mathcal{N}_u^d} p_{vu} T_v^u \leq M, \quad (23)$$

for some $M \in \mathbb{R}_{++}$, then $\nabla^2 D_u(\lambda_u) \leq L_2$, for some constant L_2 .

Proposition 4.2: Suppose that the sum of weights are bounded as in (23). The dual function D_u is strongly convex and its Hessian is bounded from above and below uniformly.

Proof: Firstly, λ_u is bounded from above by some constant $\bar{\lambda}_u$ since the dual problem is feasible. Thus, $\epsilon_1 \leq \lambda_u \leq \bar{\lambda}_u, \epsilon_1 > 0$. In addition, $\sum_{v \in \mathcal{N}_u^d} w_{uv} \neq 0$; otherwise, the primal problem is trivial because $w_{uv} = 0$, for all v . Therefore, $\epsilon_2 \leq \sum_{v \in \mathcal{N}_u^d} w_{uv} \leq M, \epsilon_2 > 0$. Hence, the statement is true. ■

¹Peer u 's dual function is expressed in terms of λ_u and \mathbf{p}_{-u} , and the decision variable for peer u changes from a multi-dimensional vector \mathbf{p}_u to a scalar variable λ_u . Using the dual function, we can reduce the dimension of the game (GP) as well as turn a constrained game into an unconstrained one.

Strong duality ensures a unique optimal solution. The unique dual optimal λ_u^* can be found explicitly by applying the unconstrained optimality condition, i.e., $D'_u(\lambda_u) = 0$. As a result, we obtain

$$\lambda_u^* = \frac{PT}{\left(C_u - KM + \frac{1}{\alpha}(KR - KM)\right) \ln(1 + \alpha)}. \quad (24)$$

To find the dual optimal, we can also devise a dynamic algorithm that can be used in conjunction with Algorithm (17). An iterative algorithm based on gradient methods to find λ_u is given by

$$\lambda_u(t+1) = \lambda_u(t) - \beta_u D'_u(\lambda_u(t)), \forall u \in \mathcal{N}, \quad (25)$$

where $\beta_u \in (0, 1)$ is the step size. The gradient algorithm in (25) is distributed over the network. Each peer needs to collect accessible open information from its neighboring peers to evaluate KM , KR and PT . With the property of strong convexity, we can show in the following the fast convergence of the algorithm to (24).

Proposition 4.3: Suppose that $D'_u(\lambda_u)$ is Lipschitz with Lipschitz constant L_3 and $D_u(\lambda_u)$ is strongly convex with $D''_u(\lambda_u) \geq L_1$. The dual algorithm (25) converges geometrically to dual optimal λ_u^* in (24) with step size $\beta_u < \frac{\min(2, L_1)}{L_3}$.

Proof: We can use the technique in [20] to prove the proposition. Using the property of strong convexity and Lipschitz property, we obtain

$$\begin{aligned} &\|\lambda_u(t+1) - \lambda_u^*\|^2 \\ &= \|\lambda_u(t) - \lambda_u^*\|^2 - 2\beta_u D'_u(\lambda_u(t))(\lambda_u(t) - \lambda_u^*) \\ &\quad + \beta_u^2 \|D'_u(\lambda_u(t))\|^2 \\ &\leq \|\lambda_u(t) - \lambda_u^*\|^2 - 2\beta_u (D_u(\lambda_u(t)) - D_u(\lambda_u^*)) \\ &\quad + \beta_u^2 L_3 \|\lambda_u(t) - \lambda_u^*\|^2 \\ &\leq \|\lambda_u(t) - \lambda_u^*\|^2 - \beta_u L_1 \|\lambda_u(t) - \lambda_u^*\|^2 \\ &\quad + \beta_u^2 L_3 \|\lambda_u(t) - \lambda_u^*\|^2 \\ &= (1 - \beta_u L_1 + \beta_u^2 L_3) \|\lambda_u(t) - \lambda_u^*\|^2 \end{aligned}$$

Hence, when $\beta_u < \frac{\min(2, L_1)}{L_3}$, we have a contraction. In addition,

$$\|\lambda_u(t+1) - \lambda_u^*\|^2 \leq (1 - \beta_u L_1 + \beta_u^2 L_3)^{t+1} \|\lambda_u(0) - \lambda_u^*\|^2.$$

Hence, the convergence rate is geometric. ■

V. EXPERIMENTS AND EVALUATION

In this section, we adopt two different approaches to evaluate the Nash equilibrium of the collaborative system. In the first experiment, we implement the dynamic algorithm in Section IV to find the Nash equilibrium. We show that the algorithm yields the Nash equilibrium of the game at the steady state and the system is incentive compatible under the equilibrium. In the second experiment, we use a stochastic discrete-event based simulation to model an IDS network. In the simulation, peers estimate their resources received from the other peers and adjust their allocations of resources to the others accordingly. We are interested in finding the Nash equilibrium and verifying the incentives in the collaborative system at the equilibrium.

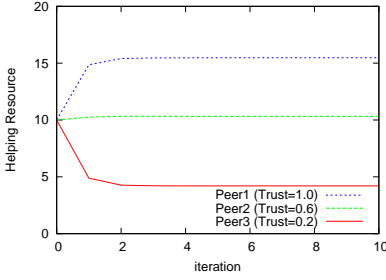


Fig. 2. Helping resources v.s. time - first approach

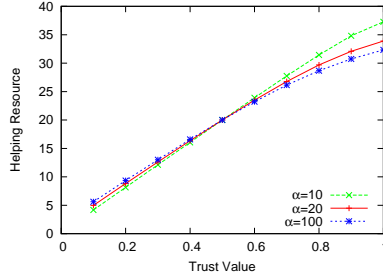


Fig. 3. Resource received varies with trust value -first approach

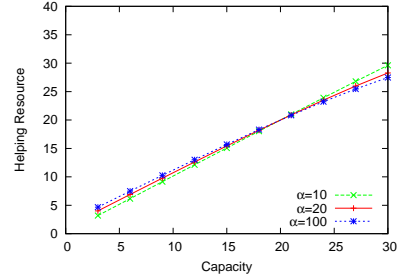


Fig. 4. Resource received varies with resource contribution - first approach

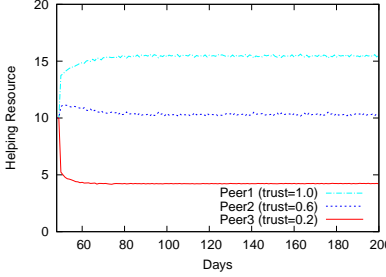


Fig. 5. Helping resources v.s. time - second approach

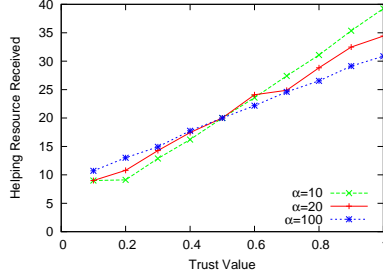


Fig. 6. Resource received varies with trust value - second approach

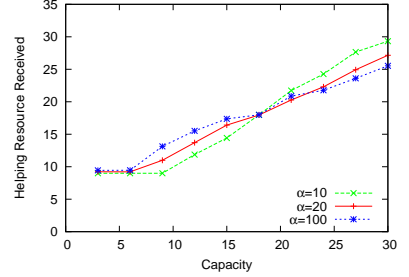


Fig. 7. Resource received varies with resource contribution - second approach

A. Implementation of the Dynamic Algorithm

In this section, we implement the dynamic algorithm in Section IV and design numerical experiments to evaluate the incentives of the resource allocation scheme. We set up a three-node network and observe that the algorithm yields a Nash equilibrium within several updates. In this experiment, we set the minimum demand of resource to 1 unit and the maximum to 10 units for all peers. Every peer has an equal capacity of 20 units and the system parameter $\alpha = 100$. We assume that trust values of all peers are publicly and truthfully known. We find that, if all peers have the same trust values, then the resource is fairly and evenly distributed among all peers. When the trust values are different, peers with higher trust values receive more resources. Figure 2 shows that the resources given to three peers with different trust values converge fast within two or three iterations.

Fixing the resource capacity of all peers to 20 units and the trust values of two of the peers to 0.5, we vary the trust value of the third peer from 0.1 to 1.0. In Figure 3, we observe that the resource that the third peer receives increases with its trust value under different α values. We also see that all curves cross at trust value 0.5 and resource 20. This is because all peers should receive equal amount of resources when they are equally configured, regardless of the α value we choose. By fixing the trust values of all nodes to 1.0 and varying the resource capacity of the third peer from 3 to 30, we observe in Figure 4 that the amount of resource a peer receives is almost linearly proportional to the resource it contributes to the others. Similarly, all curves intersect at capacity 20 and resource 20. The reason for that is resources are evenly distributed when all peers are the same. These results further confirm our theoretical analysis in Section III.

Figure 3 and 4 also reveal that a larger α value leads to a lower marginal helping resource. This is because a larger α value means that peers are easier to be satisfied, and therefore peers have less incentives to contribute.

B. Stochastic Discrete-Event Based Simulation

In this experiment, we use a stochastic discrete-event based simulation [23] to model the collaboration mechanism in an IDS network. It is commonly used to aid strategic decision making since it has the capability of emulating complex real world problems. Discrete-event simulation concerns the modeling of a system as it evolves over time by representing the changes as separate events. It bridges over our model and a real-life IDS network.

In this simulation, each node collaborates with others by sending out requests and waits for their responses. The requests from each node are generated randomly following a Poisson process with an average arrival rate of 10 requests per day. Upon the arrival of a request at its destination queue, it will be replied by the corresponding peer on first-come-first-serve basis. The processing rate of requests depends on the amount of resource that the node allocates to the sender. Each peer estimates the resource they have received from other peers by observing traffic and updates its allocation to other peers accordingly. In the experiment, all peers initialize with an unbiased allocation and then apply the optimized resource allocation scheme.

For the purpose of comparing with numerical experiments, we use the same experiment configuration as in Section V-A, i.e., we simulate a network of 3 nodes; we set the minimum resource requirement to 1 unit and the maximum to 10 units for all peers; every peer has a capacity of 20 units; we set

$\alpha = 100$ and the trust values of nodes to be 0.2, 0.6, and 1.0, respectively.

Figure 5 illustrates the received resources for all three nodes with respect to time. We note that the helping resource converges to the Nash equilibrium at the steady state and nodes with higher trust values obtain more share of the resources. It confirms that our resource allocation scheme provides incentives to the collaborative network.

By fixing the resource capacity of all peers to 20, the trust values of two of the peers to 0.5, and varying the trust values of the third peer from 0.1 to 1.0, we obtain in Figure 6 that the received resource of the third peer increases with its trust value under different α values. Fixing the resource capacity of the first two peers to 20 and trust values to 1.0 for all peers, we vary the capacity of the third peer from 3 to 30 and observe that the resource received by the third node also increases with its resource capacity under different α values, as shown in Figure 7. These results also reveal that a higher α value brings less incentive to the resource allocation. The simulation results are consistent with the theoretical results obtained in Section III and the ones in Section V-A.

C. Large-Scale Simulation

Previous experiments were based on a small-scale network. In this subsection, we design numerical experiments to study the resource allocation in a large-scale intrusion detection network. We set up a network of 100 nodes, which are randomly scattered in a 100×100 square. Each node shares its resource with the other nodes in the proximity distance of 5. The trust values are generated according to a uniform distribution from 0 to 1.0. The lower bounds and the upper bounds on the requests are 1 and 10, respectively, for each node. We separate nodes into two groups: one group with capacity of 10 units and the other with 20. In Figure 8, we can see that, for either group of nodes, nodes with higher trust values tend to receive more assistance. The response to trust value appears to be more prominent for the group with capacity of 20 units. It can be explained by the fact that when the resource capacity is low, most of the resource is used to satisfy the lower bound of all the neighbors and little is left to allocate based on incentives. In the second experiment, we fix trust values of all nodes to 1.0 and randomly choose the resource capacity of each node from 0 to 30. Figure 9 shows the resource received by nodes with different resource capacities. We note that, on average, nodes with higher resource capacities receive more resources. This confirms the incentives under a large collaboration group.

VI. CONCLUSION

In this paper, we have studied an incentive compatible resource allocation problem in the context of a collaborative intrusion detection network. By formulating an associated continuous kernel game, we have shown that a Nash equilibrium exists and is unique under certain system conditions. We have also shown that the Nash equilibrium possesses features that allow peers to communicate in a conducive environment in which peers endeavor to contribute knowledge

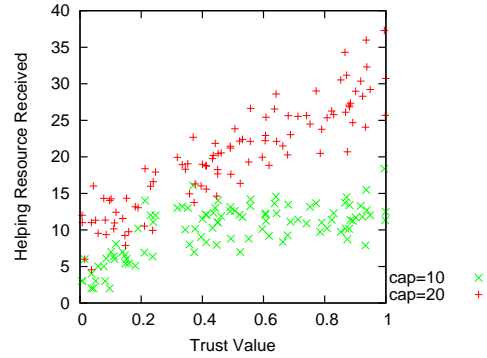


Fig. 8. Resource received for peers with different trust values

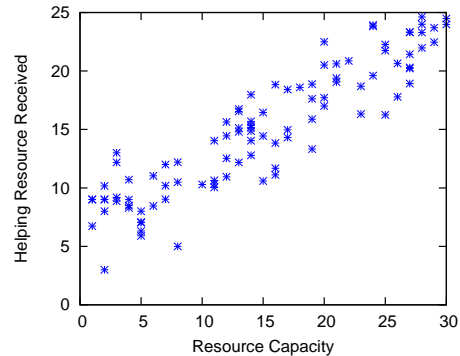


Fig. 9. Resource received for peers with different resource capacities

and resource to assist neighbor nodes. Any selfish or free-riding behavior will receive a tit-for-tat response from the neighbors as a consequence. The dynamic algorithm proposed in the paper is used to compute the Nash equilibrium. Experimental results show that the algorithm converges to the Nash equilibrium at a geometric rate, further confirming the theoretical results. In follow-up work, we plan to develop an admission control system for IDSs to build up their dynamic neighbor lists based on dynamic evaluations of trust and expertise levels.

VII. ACKNOWLEDGMENTS

The authors gratefully acknowledge helpful discussions with Jie Zhang. The work of the authors from Illinois was supported in part by a grant from Boeing through the Information Trust Institute.

REFERENCES

- [1] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System," in *Proceedings of Network and Distributed System Security Symposium (NDSS04)*, 2004.
- [2] Y. Wu, B. Foo, Y. Mei, and S. Bagchi, "Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS," in *Computer Security Applications Conference, 2003. Proceedings. 19th Annual*, 2003, pp. 234–244.
- [3] C. Zhou, S. Karunasekera, and C. Leckie, "A Peer-to-Peer Collaborative Intrusion Detection System," in *International Conference on Networks*, 2005.
- [4] P. Sen, N. Chaki, and R. Chaki, "HIDS: Honesty-Rate Based Collaborative Intrusion Detection System for Mobile Ad-Hoc Networks," *Computer Information Systems and Industrial Management Applications, 2008. CISIM'08. 7th*, pp. 121–126, 2008.

- [5] C. Fung, O. Baysal, J. Zhang, I. Aib, and R. Boutaba, "Trust management for host-based collaborative intrusion detection," in *19th IFIP/IEEE International Workshop on Distributed Systems*, 2008.
- [6] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, "A trust-aware, p2p-based overlay for intrusion detection," in *DEXA Workshops*, 2006.
- [7] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Robust and scalable trust management for collaborative intrusion detection," in *11th IFIP/IEEE International Symposium on Integrated Network Management (IM09)*, to appear, 2009.
- [8] J. Keppler and H. Mountford, *Handbook of Incentive Measures for Biodiversity: Design and Implementation*. OECD, 1999.
- [9] R. Ma, S. Lee, J. Lui, and D. Yau, "A game theoretic approach to provide incentive and service differentiation in P2P networks," in *Sigmetrics/Performance*, 2004.
- [10] Y. Yan, A. El-Atawy, and E. Al-Shaer, "Ranking-based optimal resource allocation in peer-to-peer networks," in *Proceedings of the 26th annual IEEE conference on computer communications (IEEE INFOCOM 2007)*, May, 2007.
- [11] G. Theodorakopoulos and J. Baras, "Malicious Users in Unstructured Networks," in *Proceedings of the 26th annual IEEE conference on computer communications (IEEE INFOCOM 2007)*, May, 2007.
- [12] N. Semret, R. Liao, A. Campbell, and A. Lazar, "Peering and provisioning of differentiated internet services," *IEEE Infocom 2000*, March 2000.
- [13] V. Krishna, *Auction Theory*, 1st ed. Academic Press, 2002.
- [14] T. Alpcan and T. Başar, "A game theoretic approach to decision and analysis in network intrusion detection," *Proc. of the 42nd IEEE Conference on Decision and Control*, December 2003.
- [15] —, "A game theoretic analysis of intrusion detection in access control systems," in *Proc. IEEE Conference on Decision and Control (CDC 04)*, Nassau, The Bahamas, 2004, pp. 1568–1573.
- [16] —, "An intrusion detection game with limited observations," in *Preprints of the 12th Intl. Symp. Dynamic Games and Applications (ISDGA 2006)*, Sophia Antipolis, France, 2006.
- [17] K. C. Nguyen, T. Alpcan, and T. Başar, "Fictitious play with imperfect observations for network intrusion detection," in *Preprints of the 13th Intl. Symp. Dynamic Games and Applications (ISDGA 2008)*, Wroclaw, Poland, 2008.
- [18] H. M. Y. Liu, C. Comaniciu, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *Valuetools*, October 2006.
- [19] D. Bertsekas, *Network Optimization: Continuous and Discrete Models*. Athena Scientific, 1998.
- [20] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
- [21] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. SIAM, Philadelphia, 1998.
- [22] A. Berman and R. Plemmons, *Nonnegative Matrices in Mathematical Sciences*. SIAM, 1994.
- [23] G. Fishman, *Discrete-event simulation: modeling, programming, and analysis*. Springer, 2001.