GUIDEX: A Game-Theoretic Incentive-Based Mechanism for Intrusion Detection Networks

Quanyan Zhu, *Student Member, IEEE,* Carol Fung, *Student Member, IEEE,*
Raouf Boutaba, *Fellow, IEEE,* and Tamer Başar, *Fellow, IEEE*

***Abstract*—Traditional intrusion detection systems (IDSs) work in isolation and can be easily compromised by unknown threats. An intrusion detection network (IDN) is a collaborative IDS network intended to overcome this weakness by allowing IDS peers to share detection knowledge and experience, and hence improve the overall accuracy of intrusion assessment. In this work, we design an IDN system, called GUIDEX, using game-theoretic modeling and trust management for peers to collaborate truthfully and actively. We first describe the system architecture and its individual components, and then establish a game-theoretic framework for the resource management component of GUIDEX. We establish the existence and uniqueness of a Nash equilibrium under which peers can communicate in a reciprocal incentive compatible manner. Based on the 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 security features of GUIDEX against free riders, dishonest insiders and DoS attacks.**

***Index Terms*—Intrusion detection systems, collaborative networks, game theory, network optimization, incentive compatibility, network security and economics.**

I. INTRODUCTION

IN RECENT years, Internet intrusions have become more sophisticated and harder to detect. Attackers not only invade and harvest private data from victim nodes, but also compromise a large number of nodes to form a botnet [1], and use those compromised nodes to launch distributed attacks such as Distributed Denial of Service (DDoS) attacks [2]. To protect computer users from malicious intrusions, Intrusion Detection Systems (IDSs) have been designed to identify intrusions by comparing observable behaviors against suspicious patterns. In a broad sense, IDSs can be agents with intrusion detection capabilities, such as antivirus software, NIDS, HIDS, firewalls, and honeynets.

Manuscript received 15 December 2011; revised 1 June 2012. Research of the first and fourth authors was supported in part by Boeing Company and NSA through the Information Trust Institute of the University of Illinois. The work of the second and third authors was supported in part by the Natural Science and Engineering Council of Canada (NSERC) under its Discovery Program and by the World Class University (WCU) Program under the Korea Science and Engineering Foundation funded by the Ministry of Education, Science and Technology (Project No. R31-2008-000-10100-0).

Q. Zhu and T. Başar are with the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana Champaign (e-mail:{zhu31, basar1}@illinois.edu).

C. Fung is with the Cheriton School of Computer Science at University of Waterloo, Ontario, Canada (e-mail: j22fung@uwaterloo.ca).

R. Boutaba is with the Cheriton School of Computer Science at University of Waterloo, Ontario, Canada (e-mail: rboutaba@cs.uwaterloo.ca). He is also with the ITCE Division at POSTECH, Pohang, Korea).

Digital Object Identifier 10.1109/JSAC.2012.121214.

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.

As shown in Fig. 1, an IDN is composed of a group of independent IDSs in a peer-to-peer manner. Each IDS maintains a list of other IDSs which it currently collaborates with. IDSs can have different ways to detect intrusions. For example, antivirus software and Host-based IDSs (HIDSs) scan suspicious files or logs and look for pattern matching with known malware or attacks. Network-based IDSs (NIDSs) inspect network data flows and packets for suspicious activities. IDSs can freely choose their collaborators for maximizing individual benefits. For example, an antivirus software can choose to work with another one from a different security vendor, and an NIDS can choose to collaborate with a honeynet to obtain a fresh attacker list. In this paper, we consider distributed self-interested IDSs in the Internet that can cross administration domains.

Malicious insiders in an IDN can compromise the system by providing false information or overloading the system with spam. Also, "free riders" [3] can exploit the system by benefiting from others without contributing themselves. This can discourage IDN participants and eventually degrade the overall performance of the collaboration system. Therefore, trust management and a resource allocation mechanism are critical for designing an incentive-compatible and attack-proof IDN system.

A. Main Contributions

In this work, we propose an IDN system, called GUIDEX,[1] based on reciprocal incentive-based resource allocation and trust management, where the amount of resources that each IDS allocates to assist its neighbors is proportional to the trustworthiness and the amount of resources allocated by its neighbors to help this IDS. The motivation for reciprocal incentive design is to encourage participants to contribute more in collaboration so as to keep their IDS knowledge up-to-date. This exchange of knowledge is particularly important for IDSs to protect the system from new or zero-day attacks. We formulate an $N-$person (or peer) non-cooperative continuous-kernel game model to investigate incentive compatibility of the

[1]"GUIDEX" stands for "Game-theoretic Utility-based Intrusion Detection nEtwork SystemS."

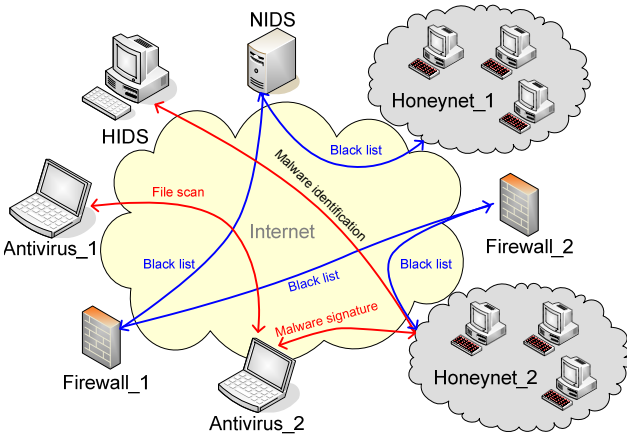


Fig. 1. An example of an IDN network. An IDS can collaborate with other IDSs by sending suspicious files or IP addresses for diagnosis. For example, a NIDS can send the IP of a suspicious attacking source to honeynets and firewalls to see whether it has been blacklisted anywhere. An antivirus software sends a suspicious file to another one for scanning.

IDS collaboration system. In our framework, each IDS finds an optimal resource allocation to maximize the aggregated satisfaction levels of its neighbors. 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 helping resource an IDS receives is proportional to its helpfulness to others. We also demonstrate security features of GUIDEX against free riders, dishonest insiders, and DoS attacks.

Main contributions of this paper are: 1) Architecture design of the GUIDEX collaborative intrusion detection network and its essential components; 2) A mechanism for optimal resource allocation for each peer to maximize its social welfare with a convex utility function; 3) An N-person non-cooperative game model and an iterative primal/dual algorithm to reach the Nash equilibrium; and 4) Incentive compatibility and robustness that is derived from the resource allocation scheme to tackle the "free riders", dishonest insiders, and DoS attacks.

B. Related Work

Many IDS collaboration systems have been proposed in literature, such as [4], [5], and [6]. They all assume IDSs cooperate honestly and unselfishly. The lack of trust infrastructure leaves the systems vulnerable to malicious peers.

A few trust-based collaboration systems (e.g. [7] and [8]) and distributed trust management models (e.g. [8], [9], and [10]) have been proposed for effective IDS collaboration. However, none of these proposed models have led to a study of incentives for IDS collaboration. Our previous work proposed a trust management system where IDSs exchange test messages to build trust among themselves. The feedback from the collaboration peers is evaluated and a numerical trust value is accessed to predict the level of truthfulness of collaborators. [8] uses a simple weighted average model to predict the trust value while [10] uses a Bayesian statistics model to estimate the trust value as well as the confidence level of the trust estimation.

A variety of game-theoretic approaches have been applied to network resource allocation in traditional routing networks and peer-to-peer (P2P) networks. In traditional routing networks, non-cooperative game models such as in [11] and [12] have been used in a dynamic resource allocation context; authors of these references have considered a network with a general topology where each source has a window-based end-to-end flow control. The available information for a user is the number of packets within the network not yet acknowledged. Each user aims to maximize his own throughput, with bounded delay, and hence faces a constrained optimization problem. The equilibrium obtained is decentralized since each user has only local information on his own unacknowledged packets. Their focus has been on the maximal network performance with given resource instead of incentive mechanisms. In peer-to-peer networks, Ma et al. [13] have used a game-theoretical approach to achieve differentiated services allocation based on the peer's contribution to the community. Yan et al. [14] have proposed an optimal resource allocation scheme for file providers. A max-min optimization problem has been constructed to find the optimal solution which achieves fairness in the resource allocation. Both works rely on an independent central reputation system. Reciprocity has not been incorporated. Also the resilience and robustness of the system has not been their focus. Grothoff [15] has proposed a resource allocation economic model to deal with malicious nodes in peer-to-peer networks. It depends solely on the trust values of the peer nodes, and the resource allocation is priority-based on the trust value of the request sender. Grothoff's model can effectively prevent malicious nodes from overusing the network resource since their requests will be dropped due to their low trust. It is also reciprocal altruistic. However, this model may result in unfairness since nodes with the highest trust may take the entire resource. Our model differs from the above ones in that we have made use of the pair-wise nature of the network for designing scalable network algorithms, ensuring secure and resilient properties of the solution, and provide fairness and reciprocal incentive compatibility in resource allocation.

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. In [16], and [17], 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. Our previous work [19] provides a game-theoretical model for IDSs to allocate collaboration resource to achieve the goal of fairness and incentive compatibility. This paper extends our previous work by integrating a complete IDN framework and a robustness evaluation.

C. Paper organization

The rest of the paper is organized as follows: Section II discusses desirable features of IDN and presents the system architecture of GUIDEX and its building blocks. In section III, we describe our incentive-based resource allocation scheme

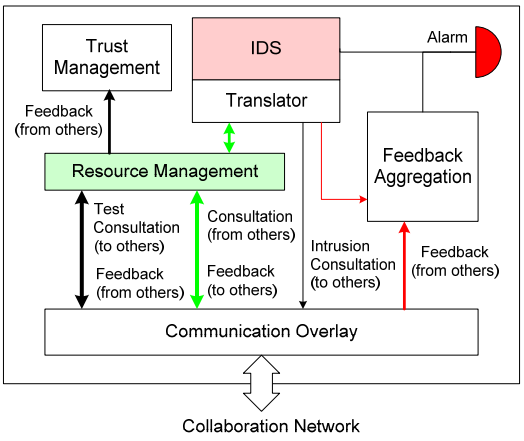


Fig. 2. Architecture of an IDS Collaboration System

for resource management in GUIDEX. 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 the paper.

II. Collaboration Framework

The purpose of an IDN is to connect IDSs to achieve a higher detection capability network-wide. In this context, we identify the following requirements for an efficient IDN:

1) An effective trust management model to reduce the negative impact of dishonest IDSs and discover compromised ones;
2) An efficient feedback aggregation method to minimize the cost of false intrusion detection;
3) Robustness design against malicious insiders;
4) Scalability in terms of IDN size, trust evaluation, and intrusion assessment.

To achieve the preceding goals, we propose an IDN architecture design as shown in Fig. 2. It is composed of several components, namely, intrusion detection system, communication overlay, trust management, resource management, feedback aggregation, and IDS mediator.

A. Consultation and Feedback

When an IDS detects suspicious traffic or activities but does not have enough experience to make a decision whether it should raise an alarm or not, it may send the suspicious trace or file to its collaborating IDSs for diagnosis. We call this a *consultation message*. *Feedbacks* from the collaborators are aggregated and a final alarm decision is made based on the aggregated results. A consultation message can be the binary of a suspicious file, the data packets of a suspicious data flow, or intrusion alerts. The feedback from the collaborators can be one value from the set {'positive', 'negative', 'unknown'}. The 'unknown' feedback is given when the requested IDS does not have enough information to make a judgment. *Test consultations* are "bogus" consultation requests, sent out in a way that makes them difficult to be distinguished from real consultation requests. The testing node needs to know beforehand the true diagnosis result of the test consultations and uses the received feedback to derive a trust value for the collaborators.

B. Mediator and Communication Overlay

The mediator is the component which helps different IDSs to communicate with each other. It translates consultation requests and consultation feedbacks into a common protocol and data format understood by different IDSs. Communication overlay is the component which handles all the communications between the host node and other peers in the collaboration network. The messages passing through the communication overlay include: test messages from host node to its acquaintances; intrusion consultations from host node to its acquaintances; feedback from acquaintances; consultation requests from acquaintances; feedback to acquaintances.

C. Trust Management

The trust management component allows IDSs in the IDN to evaluate the trustworthiness of others based on their personal experiences with them. The host node can use *test consultations* to gain experience quickly. Indeed, the verified consultation results can also be used as experience. In GUIDEX, we have adopted a Bayesian learning-based trust management model [20] to evaluate the trustworthiness of IDSs.

D. Feedback Aggregation

Feedback aggregation is an important component and it has a direct impact on the accuracy of the collaborative intrusion detection. After the host IDS sends out a consultation request to its acquaintances, the collected feedbacks are used to decide whether the host IDS should raise an alarm to the administrator or not. If an alarm is raised, the suspicious intrusion flow will be suspended and the system administrator investigates the intrusion immediately. On one hand, false alarms create disruptions and waste human resources. On the other hand, undetected intrusions may cause damages.

E. Resource Management

To help the nodes in the IDN use their resource effectively in collaboration, a resource management system is required to decide whether the host should allocate resources to respond to consultation requests. An incentive-compatible resource management can assist IDSs to allocate resources to their acquaintances so that other IDSs are fairly treated based on their past assistance to the host IDS. Therefore, an IDS which abusively uses the collaboration framework will be penalized by receiving fewer responses from others. In our IDN, we use an incentive-compatible resource allocation scheme as described in section III for IDSs in the IDN.

III. Resource Management and Incentive Design

In this section, we first mathematically model resource allocation in an IDN environment as individual optimization problems for its member peers. A game problem (GP) can then be introduced for each peer. We employ a Lagrangian approach to find the Nash equilibrium of the constrained game. Finally, we show that there exists a unique Nash equilibrium in the game and characterize the equilibrium solution in closed form.

A. Modeling of Resource Allocation

We consider a collaborative intrusion detection network (CIDN) with N peers or nodes where all the nodes adopt the GUIDEX scheme. Each IDS user can distribute information to other IDS users in form of messages (in bytes). We denote the set of nodes by $\mathcal{N} = \{1, 2, \cdots, N\}$. The set of neighbor nodes of peer u is denoted by $\mathcal{N}_u$. The communications between IDSs become constrained when the network size is large and the number of collaborators $|\mathcal{N}_u|$ grows. Note that information in the network is symmetric. If u is a neighbor of v, then v is also a neighbor of u. We can represent the topology of an IDN by a graph $\mathcal{G} := (\mathcal{N}, \mathcal{E})$, where $\mathcal{E}$ is the set of (u, v) pairs in the network. 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}. Note that r_{vu}, m_{vu} are chosen by node v and informed to node u during negotiation. 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 each node has its own mechanism to evaluate the trust of its neighbors, and the trust values have already been determined. This assumption is practical if a distributed trust management exists in the system and this is one of the building blocks in our GUIDEX system designed in Section II. 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. Interested reader can refer to the trust models employed in [21] and [20] and they are applicable to the GUIDEX system.

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:

$$\sum_{v \in \mathcal{N}_u} p_{uv} \leqslant C_u, \text{ for all } u \in \mathcal{N}. \tag{1}$$

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

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

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 under the condition $\alpha > 1$. The choice of logarithmic functions is motivated by the proportional fairness properties as in [22], [23] and has been used in the literature on power control, congestion control and rate control in communication networks [23]–[25].

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

$$U_u = \sum_{v \in \mathcal{N}_u} w_{uv} S_{uv}, \; w_{uv} = T_v^u p_{vu}, \tag{3}$$

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:

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

where S_{uv} and w_{uv} are given by (2) and (3), respectively. The upper and lower bounds on resources are imposed by the collaborators. The design of the utility function in OP is built upon the intuition behind how people form collaborations in social networks. With the freedom to choose and design collaborative schemes, we assume that all legitimate agents in the network start with an intent to form collaborations with each other.

Every peer in the network is faced with an optimization problem (OP) to solve. (OP) is a concave problem in which the objective function is a concave function in p_{uv} and the constraint set is an $L(u)$-dimensional simplex, where $L(u) = \text{card}(\mathcal{N}_u)$, the cardinality of the set $\mathcal{N}_u$. Under the assumptions that the size of the network is large and peers can only communicate locally within a distance d, we have N individual 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 $A_u = A_u^1 \bigcap A_u^2$, where $A_u^1 = \{\mathbf{p}_u \in \mathbb{R}_+^{L(u)} \mid \sum_{v \in \mathcal{N}_u} p_{uv} \leqslant C_u\}$ and $A_u^2 = \{\mathbf{p}_u \in \mathbb{R}_+^{L(u)} \mid m_{vu} \leqslant p_{uv} \leqslant r_{vu}, v \in \mathcal{N}_u\}$. It is not difficult to prove that under the condition $C_u \geqslant \sum_{v \in \mathcal{N}_u} m_{vu}$, 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 $\mathscr{L}_u(\mathbf{p}_u, \sigma_u, \mu_u, \lambda_u)$ as follows denote the Lagrangian of peer u's optimization problem:

$$\begin{aligned} \mathscr{L}_u = & \sum_{v \in \mathcal{N}_u} T_v^u p_{vu} S_{uv} - \sum_{v \in \mathcal{N}_u} \mu_{uv}(p_{uv} - r_{vu}) \\ & + \sum_{v \in \mathcal{N}_u} \sigma_{uv}(p_{uv} - m_{vu}) - \lambda_u \left(\sum_{v \in \mathcal{N}_u} p_{uv} - C_u \right), \end{aligned} \tag{5}$$

where $\mu_{uv}, \sigma_{uv}, \lambda_u \in \mathbb{R}_+$ are the Lagrange multipliers. Using Lagrangian relaxation, we can transform the game problem to its relaxed counterpart (RGP), where the abbreviation "R" is short for "Relaxed". The triplet of RGP is given by $\langle \mathcal{N}, \bar{A}_u, \mathscr{L}_u \rangle$, where $\bar{A}_u$ is the action set described by the base constraint $p_{uv} \geqslant 0$, i.e., $\bar{A}_u = \{\mathbf{p}_u \mid p_{uv} \geqslant 0, v \in \mathcal{N}_u\}$; and the payoff function is replaced by the relaxed Lagrangian function $\mathscr{L}_u$. [2].

[2]In the definition of the relaxed game (RGP), we have chosen 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., $\bar{A}_u = \{\mathbf{p}_u \mid m_{vu} \leqslant p_{uv} \leqslant r_{vu}, v \in \mathcal{N}_u\}$.

By formulating the collaborative 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.

The framework described in this subsection can be potentially applied to a wide range of collaborative networks where reciprocal altruism is desirable. However, many distinct features of IDS networks have been incorporated into the design. Firstly, an attacker can compromise nodes in the network and then start to spread malware to degrade the level of protection provided by the collaborative network. The special structure of the utility function together with the trust values have been used in the model to mitigate malicious and dishonest behaviors of compromised nodes. Secondly, insider threats in IDS networks have been considered by imposing upper and lower bounds on p_{uv}, which can be used to prevent denial-of-service attacks from the insiders.

Remark 3.1: The choice of using the word *collaborative* networks is to distinguish this approach from its *cooperative* counterpart. Cooperative networks often refer to a network of nodes that are able to act as a team and then split the team utility among the members. This will require global communications, coordination and bargaining. This appears to be unrealistic for CIDN systems. In collaborative networks, nodes behave strategically not because they are selfish agents but because they are unable to coordinate or act as a team. Our work is essentially different from non-cooperative network formation problems, where all agents act selfishly to achieve their individual goals, which can be misaligned with each other. In GUIDEX, the players have their goals aligned in a certain way to achieve efficient exchange of knowledge with each other. This is similar to classical strategic games such as Battle of the Sexes and Bach and Stravinsky game [26]. However, the goals become less aligned when agents have low trust values. This flexibility in the model essentially attributes to the reciprocal altruism.

B. Characterization of Nash Equilibrium

In this subsection, we solve the GP for its Nash equilibrium. Each peer u has a concave optimization problem as in (4). Applying the first-order KKT condition as in [27] and [28] to each peer's concave problem in OP, $\frac{\partial \mathscr{L}_u}{\partial p_{uv}} = 0, \forall v \in \mathscr{N}_u, u \in \mathscr{N}$, we find

$$\frac{\delta_{uv} T_v^u p_{vu}}{1 + \alpha'_{uv} p_{uv} - \alpha'_{uv} m_{vu}} = \xi_{uv}, \forall v \in \mathscr{N}_u, u \in \mathscr{N}, \tag{6}$$

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 $u \in \mathscr{N}$:

$$\lambda_u \left(\sum_{v \in \mathscr{N}_u} p_{uv} - C_u \right) = 0. \tag{7}$$

$$\sigma_{uv}(p_{uv} - m_{vu}) = 0, \forall v \in \mathscr{N}_u, \tag{8}$$

$$\mu_{uv}(p_{uv} - r_{vu}) = 0, \forall v \in \mathscr{N}_u. \tag{9}$$

The variable ξ_{uv} is composed of three Lagrange multipliers. If $\xi_{uv} \neq 0$, we can further simplify the first-order condition into

$$p_{uv} - \frac{T_v^u p_{vu}}{\xi_{uv} \ln(1+\alpha)} = \left(1 + \frac{1}{\alpha}\right) m_{vu} - \frac{1}{\alpha} r_{vu}. \tag{10}$$

Definition 3.1: (Başar & Olsder, [29]) A Nash equilibrium $p^*_{uv}, u, v \in \mathscr{N}$ for the game (GP) is a point that satisfies $\mathscr{L}_u(\mathbf{p}^*_u, \mathbf{p}^*_{-u}) \geqslant \mathscr{L}_u(\mathbf{p}_u, \mathbf{p}^*_{-u}),\ \forall \mathbf{p}_u \in A_u, u \in \mathscr{N}$, and $p_{uv} = p_{vu} = 0$, for $v \in \mathscr{N}_u \backslash \mathscr{N}_u$ and $u \in \mathscr{N}$, where the vector $\mathbf{p}_{-u} = \{\mathbf{p}_i : i \neq u, i \in \mathscr{N}\}$ is comprised of decision vectors of other peers.

Proposition 3.1: 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 $u \in \mathscr{N}, v \in \mathscr{N}_u$ and concave in $\mathbf{p}_u$. By Theorem 4.4 in [29], 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 (10) and similarly, node v has its decision vector $\mathbf{p}_v$ satisfying (10) by interchanging indices u and v. Hence, we obtain a pair of equations involving p_{uv} and p_{vu} and they are described by

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

or in the matrix form, $\mathbf{M}_{uv}\mathbf{q}_{uv} = \mathbf{b}_{uv}$, 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, [30]) 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:

(F1) the sign patterns $a_{ii} > 0,\ i = 1, ..., N$, and $a_{ij} \leqslant 0,\ i \neq j$,
(F2) the eigenvalues of $\mathbf{A}$ have all positive real parts.

Theorem 3.2: (Berman and Plemmons, [30]) If $\mathbf{A}$ is an M-matrix, then $\mathbf{A}^{-1} > 0$, i.e. all of its entries are positive.

Using Theorem 3.2, we next state a result on uniqueness of Nash equilibrium for a sufficiently large system parameter α.

Theorem 3.3: Suppose that only capacity constraints are active and $\alpha > \max_{u,v} \{e^{\frac{T_v^u}{\xi_{uv}}}, \frac{r_{vu}}{m_{vu}}\} - 1$. Then, the game admits a unique Nash equilibrium. For each pair of peers u and v, the equilibrium is given by $\mathbf{q}^*_{uv} = \mathbf{M}^{-1}_{uv} \mathbf{b}_{uv}, \forall u, v \in \mathscr{N}$.

Proof: Under the condition that the capacity constraints are 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 (10); hence, $\mathbf{M}_{uv}$ are strictly diagonally dominant and thus non-singular; and by Theorem 3.2, the entries of the inverse matrix $\mathbf{M}_{uv}^{-1}$ is strictly positive.

Secondly, provided that $\alpha > \frac{r_{uv}}{m_{vu}} - 1$, the vector $\mathbf{b}_{uv}$ is positive, i.e., $\left(1+\frac{1}{\alpha}\right) m_{vu} > \frac{1}{\alpha} r_{uv}$. Thus, we arrive at a unique solution $\mathbf{q}_{uv}^*$, whose entries are all positive, residing in the base constraint action set $\bar{A}_u$ for all u. Since (10) holds for any interactive pair, the game admits a unique Nash equilibrium under conditions in Theorem 3.3. ∎

Note that Theorem 3.3 provides a condition to choose system parameter α. Since the system designed in Section II can determine the value of α, the condition can be met easily.

Remark 3.2: 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 3.3 that only capacity constraint is active, it simply leads to $\xi_{uv} > 0$ itself.

C. Incentive Properties

We call a network design reciprocal 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 Theorem 3.3.

Proposition 3.4: Under the conditions of Theorem 3.3, the Nash equilibrium solution of the game (GP) is *reciprocal 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 (6), we take the derivative with respect to p_{vu} and let $\partial p_{uv}/\partial p_{vu}$ denote the marginal helping rate from u to v. Since $T_v^u > 0$, $\xi_{uv} > 0$, under the conditions in Theorem 3.3, we have $\partial p_{uv}/\partial p_{vu} > 0$, and thus p_{uv} is increasing with p_{vu} at Nash equilibrium. The incentive compatibility results follow. ∎

In the following, we study the incentives of nodes that decide on the lower and upper bounds on desired reply rates. We assume that the lower bound on reply rates are uniformly determined by the system once they join the network, i.e., $m_{vu} = \bar{m}$ for all $v \in \mathcal{N}, u \in \mathcal{N}_v$.

Lemma 3.5: Nodes do not have incentives to overstate their upper bound on the reply rate $r_{vu}, v \in \mathcal{N}, u \in \mathcal{N}_v$.

Proof: From (6), we can observe that $\frac{\partial p_{uv}}{\partial r_{vu}} = -1/\alpha < 0$. Hence, a higher level of request results in a lower value of p_{uv}. ∎

Lemma 3.5 admits an intuitive interpretation. When a request level is high, it becomes harder for a node to satisfy it and the node will allocate resources to satisfy other ones with lower request levels first. Hence, a higher level of request will result in a lower reply rates.

In the following, we study the effect of understating the upper bound. We first introduce the notion of ε-resilience and then derive a condition for achieving it.

Definition 3.3: The Nash equilibrium p_{uv}^* under truthful r_{vu}^* is *ε-resilient* if a deviation r_{vu} from r_{vu}^* results in an equilibrium p_{uv} such that $\|p_{uv}^* - p_{uv}\| \leqslant \varepsilon \|r_{vu}^* - r_{vu}\|$ for all pairs of $(u,v) \in \mathcal{E}$.

Proposition 3.6: Suppose $\bar{m}$ is sufficiently small and only capacity constraints are active. The Nash equilibrium, if it exists, is ε-resilient if $\alpha \geqslant \frac{1}{\varepsilon} \max_{(u,v)\in\mathcal{E}} \left| \frac{T_v^u p_{vu}}{\sum_{v\in\mathcal{N}_u} p_{vu} T_v^u} - 1 \right|$.

Proof: Let r_{vu}^* be the true upper bound, under which the reply rates are $\hat{p}_{uv}^* = \min\{\max\{\bar{m}, p_{uv}^*\}, r_{vu}^*\} \leqslant r_{vu}^*$, where

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

For any other $r_{vu} < r_{vu}^*$, the allocated resource is $\hat{p}_{uv} = \min\{\max\{\bar{m}, p_{uv}\}, r_{vu}\} \leqslant r_{uv} < r_{vu}^*$, where

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

Suppose that $\bar{m}$ is sufficiently small. Due to the assumption that only capacity constraints are active, we only need to study the case where $p_{uv} \leqslant r_{vu}$. Then, from Lemma 3.5, we obtain $p_{uv} > p_{uv}^*$ since $r_{vu} < r_{vu}^*$, and hence $p_{uv}^* < p_{uv} \leqslant r_{vu} < r_{vu}^*$. Therefore, $\|\hat{p}_{uv} - \hat{p}_{uv}^*\| = \|p_{uv} - p_{uv}^*\|$ and we have

$$\|p_{uv} - p_{uv}^*\| \leqslant \left\| -\frac{1}{\alpha}(r_{vu} - r_{vu}^*) + \frac{T_v^u p_{vu}}{\ln(1+\alpha)} \left[\frac{1}{\xi_{uv}} - \frac{1}{\xi_{uv}^*} \right] \right\|.$$

Under the relaxed conditions, we can use the closed form expression of Lagrangian multiplier (16), which is derived later in Section IV, to obtain $\frac{1}{\xi_{uv}} - \frac{1}{\xi_{uv}^*} = \frac{1}{\lambda_u} - \frac{1}{\lambda_u^*} = \frac{\ln(1+\alpha)}{\alpha P_T}(r_{vu} - r_{vu}^*)$. Hence combining with the result above, we arrive at

$$\|p_{uv} - p_{uv}^*\| \leqslant \frac{1}{\alpha} \left\| \frac{T_v^u p_{vu}}{P_T} - 1 \right\| \|r_{vu} - r_{vu}^*\|.$$

Therefore, to ensure ε-resiliency, we need $\frac{\|p_{uv} - p_{uv}^*\|}{\|r_{vu} - r_{vu}^*\|} \leqslant \frac{1}{\alpha} \left\| \frac{T_v^u p_{vu}}{P_T} - 1 \right\| \leqslant \varepsilon$, which leads to the result. ∎

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:

$$\begin{cases} p_{uv}(t+1) = s_{uv} + t_{uv} p_{vu}(t) \\ p_{vu}(t+1) = s_{vu} + t_{vu} p_{uv}(t) \end{cases}, \tag{11}$$

where $s_{uv} = \left(1+\frac{1}{\alpha}\right) m_{vu} - \frac{1}{\alpha} r_{vu}$, $t_{uv} = \frac{T_v^u}{\xi_{uv}(\ln(1+\alpha))}$, and s_{vu}, t_{vu} are defined similarly by interchanging indices u and v, with initial conditions $p_{uv}(0) = \min\left\{\frac{C_u}{\mathcal{N}_u}, r_{uv}.\right\}, \forall u, v \in \mathcal{N}$.

Proposition 4.1: Suppose that capacity constraints are active, and r_{vu} and m_{uv} are chosen such that the associated constraints become inactive constraints, i.e., $\sigma_{uv} = 0, \mu_{uv} = 0$ in (8) and (9). Given a Lagrange multiplier $\lambda_u^* \neq 0$ and provided

that $\alpha > e^{\frac{T_v^u}{\lambda_u}} - 1$, algorithm (11) converges to the unique Nash equilibrium in Theorem 3.3 at dual optimal λ_u^*.

The algorithm described in (11) 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 $D_u(\lambda_u) = \max_{\mathbf{p}_u} \mathscr{L}_u(\mathbf{p}_u, \lambda_u)$. The dual function $D_u(\lambda_u)$ is a convex function and a dual optimal λ_u^* solves the dual optimization problem (DOP)[3]

$$\min_{\lambda_u > 0} D_u(\lambda_u). \tag{12}$$

Using the solution from Theorem 3.3, we can obtain $D_u(\lambda_u)$ as follows.

$$D_u = \lambda_u \left(C_u + \frac{K_R}{\alpha} + \left(1 + \frac{1}{\alpha}\right) K_M \right) + \frac{\overline{P_T} - P_T}{\ln(\alpha + 1)},$$

and its first-order derivative as follows:

$$D_u' = C_u - \frac{\sum_{v \in \mathscr{N}_u} p_{vu} T_v^u}{\lambda_u \ln(1+\alpha)} + \frac{1}{\alpha} \sum_{v \in \mathscr{N}_u} r_{vu} - \frac{\alpha + 1}{\alpha} \sum_{v \in \mathscr{N}_u} m_{vu},$$

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

$$\overline{P_T} = \sum_{v \in \mathscr{N}_u} p_{vu} T_v^u \ln \left(\frac{\alpha}{\ln(\alpha+1)} \frac{p_{vu} T_v^u}{\lambda_u (r_{vu} - m_{vu})} \right). \tag{13}$$

The gradient of the dual function 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

$$D_u''(\lambda_u) = \frac{\sum_{v \in \mathscr{N}_u} p_{vu} T_v^u}{\lambda_u^2 \ln(1+\alpha)}. \tag{14}$$

The dual function in (12) is not only a convex function but also a strong convex function, whose Hessian is bounded uniformly as in $L_1 \leqslant \nabla^2 D_u(\lambda_u)$, for some L_1 [28]. In addition, provided that the sum of weights w_{uv} is bounded from above, i.e.,

$$\sum_{v \in \mathscr{N}_u} p_{vu} T_v^u \leqslant M, \tag{15}$$

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

Proposition 4.2: Suppose that the sum of weights is bounded as in (15). 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, $\varepsilon_1 \leqslant \lambda_u \leqslant \bar{\lambda}_u, \varepsilon_1 > 0$. In addition, $\sum_{v \in \mathscr{N}_u} w_{uv} \neq 0$; otherwise, the primal problem is trivial because $w_{uv} = 0$, for all v. Therefore, $\varepsilon_2 \leqslant \sum_{v \in \mathscr{N}_u} w_{uv} \leqslant M, \varepsilon_2 > 0$. Hence, the statement is true. ■

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

$$\lambda_u^* = \frac{P_T}{\left(C_u - K_M + \frac{1}{\alpha}(K_R - K_M)\right) \ln(1+\alpha)}. \tag{16}$$

To find the dual optimal, we can also devise a dynamic algorithm that can be used in conjunction with Algorithm (11). An iterative algorithm based on gradient methods to find λ_u is given by

$$\lambda_u(t+1) = \lambda_u(t) - \beta_u D_u'(\lambda_u(t)), \forall u \in \mathscr{N}, \tag{17}$$

where $\beta_u \in (0,1)$ is the step size. The gradient algorithm in (17) is distributed over the network. Each peer needs to collect openly accessible information from its neighboring peers to evaluate K_M, K_R and P_T. With the property of strong convexity, we can show in the following the fast convergence of the algorithm to (16).

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 $D_u''(\lambda_u) \geqslant L_1$. The dual algorithm (17) converges geometrically to dual optimal λ_u^* in (16) with step size $\beta_u < \frac{\min(2, L_1)}{L_3}$.

Proof: We can use the technique in [28] to prove the proposition. Using the property of strong convexity and Lipschitz property, we obtain

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

Hence, when $\beta_u < \frac{\min(2, L_1)}{L_3}$, we have a contraction. In addition, $\|\lambda_u(t+1) - \lambda_u^*\|^2 \leqslant (1 - \beta_u L_1 + \beta_u^2 L_3)^{t+1} \|\lambda_u(0) - \lambda_u^*\|^2$. Hence, the convergence rate is geometric. ■

Note that the condition of strong convexity can be easily satisfied from (14) if we eliminate trivial cases that all trust values of neighbors or p_{vu} are zeros.

V. Experiments and Evaluation

In this section, we perform numerical experiments and evaluate the trust and resource management capabilities of the GUIDEX system as described in Sections II, III and IV.

A. Nash Equilibrium Computation

In this section, we implement the dynamic algorithm described in Section IV to calculate the Nash equilibrium centrally. We simulate a three-node network with initial trust values $0.2, 0.6, 1.0$, respectively. For the ease of demonstration, we assume that the trust between pair nodes is homogeneous. i.e., the trust value of node i is the same to all other nodes. We set the minimum demand of resource to 1 unit and the maximum to 20 units for all nodes. Every node has an equal capacity of 20 units and the system parameter $\alpha = 100$. We

[3]Peer 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 and turn a constrained game into an unconstrained one.

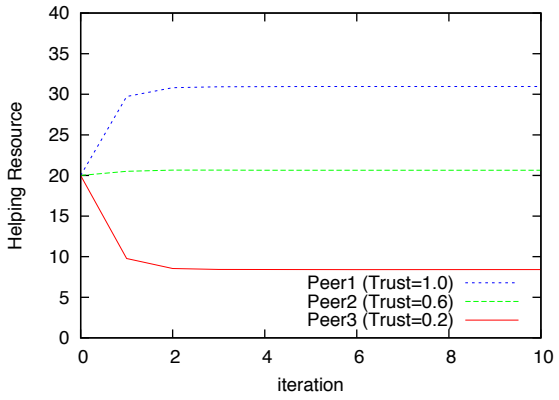


Fig. 3. Helping Resources v.s. Time - First Approach

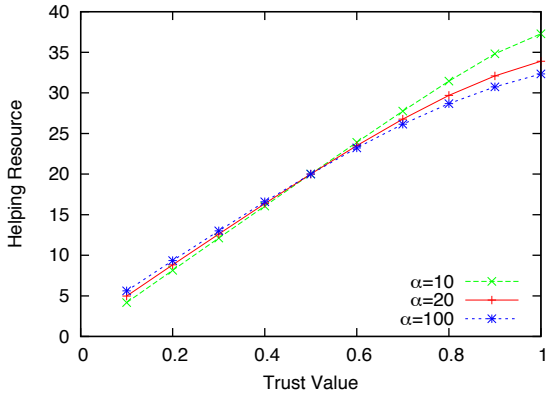


Fig. 4. Helping Resource Received Varies with Trust Value - First Approach

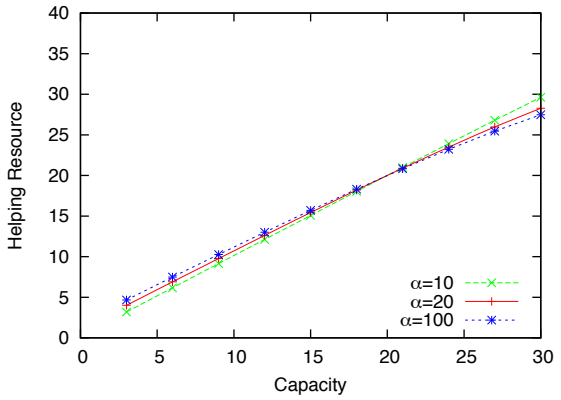


Fig. 5. Helping Resource Received Varies with Resource Contribution - First Approach

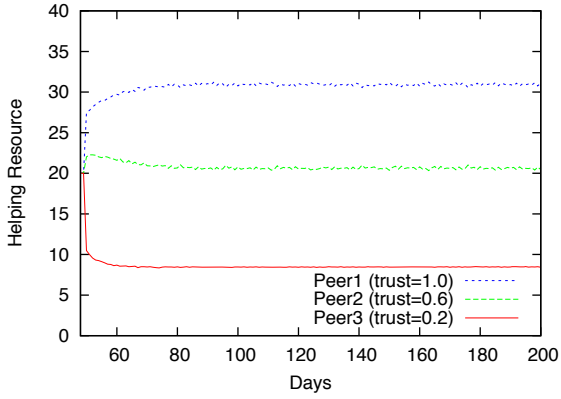


Fig. 6. Helping Resources v.s. Time - Second Approach

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. Fig. 3 shows that the resources received by three peers with different trust values converge fast within two or three iterations. A peer with higher trust value receives more help than a peer with lower trust value.

Fixing the resource capacity of all peers to 20 units and the trust values of two of the nodes to 0.5, we vary the trust value of the third peer from 0.1 to 1.0. In Fig. 4, we observe that the resource received by the third peer increases with its trust value under different α values. We also see that all curves cross at trust value 0.5 and resource 20 units. This is because all peers should receive equal amount of resources when they are identically 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 Fig. 5 that the amount of resources a peer receives is roughly linearly proportional to the resources it provides to the others. Similarly, all curves intersect at capacity 20 and resource 20. These results further confirm our theoretical analysis in Section III. Figs. 4 and 5 also reveal that a larger α value leads to a lower marginal helping resource. A smaller α value provides stronger incentive to the participants.

B. Nash Equilibrium using Distributed Computation

In this experiment, we use a stochastic discrete-event based simulation to model the IDN. In this simulation, each node collaborates with others by sending out requests and waits for their responses. At the beginning of each day, nodes send resource upper-bound/lower-bound to all their neighbors and wait for the resource quota from them. The resource quota allocation is determined through optimizing (4). The consultation requests are generated randomly following a Poisson process with an average arrival rate equal to the resource quota they receive. Upon the arrival of a request at its destination queue, it will be replied by the corresponding peer on a first-come-first-serve basis. Each peer estimates the resource it receives from other peers by calculating the average number of consultation requests answered by each peer. In this experiment, all peers initialize with an unbiased allocation, and then apply the resource allocation scheme.

For the purpose of comparing with the numerical experiment, 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 request/day and the maximum to 20 requests/day for all peers; each peer has a capacity of 20 requests; we set $\alpha = 100$ and the trust values of nodes to be 0.2, 0.6, and 1.0, respectively.

Fig. 6 illustrates the received resources for all three nodes with respect to time. We note that the helping resource

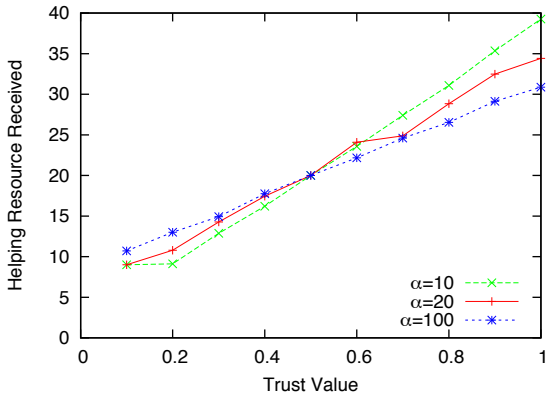


Fig. 7. Helping Resource Received Varies with Trust Value - Second Approach

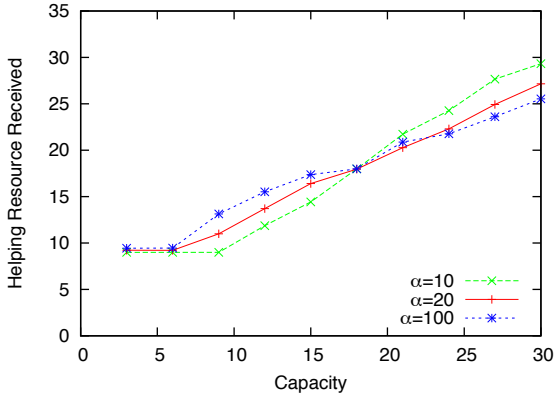


Fig. 8. Helping Resource Received Varies with Resource Contribution - Second Approach

converges to the Nash equilibrium at steady state, and nodes with higher trust values obtain more resource. This confirms that our resource allocation scheme provides incentives in 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 Fig. 7 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 requests/day and trust values to 1.0 for all peers, we vary the capacity of the third peer from 3 requests/day to 30 requests/day and observe that the resource received by the third node also increases with its resource capacity under different α values, as shown in Fig. 8. The simulation results are consistent with the theoretical results obtained in Section III and the ones in Section V-A.

C. Robustness Evaluation

Robustness is a required and important feature for the design of an IDN. In this subsection, we discuss a few common insider threats against the incentive-based resource allocation mechanism, and we show how GUIDEX is robust to these attacks. Note that all participants in GUIDEX have to abide by the protocols with a given flexibility in parameters tuning. However, due to the reciprocity of the mechanism, IDSs with selfish or dishonest behaviors will be punished and

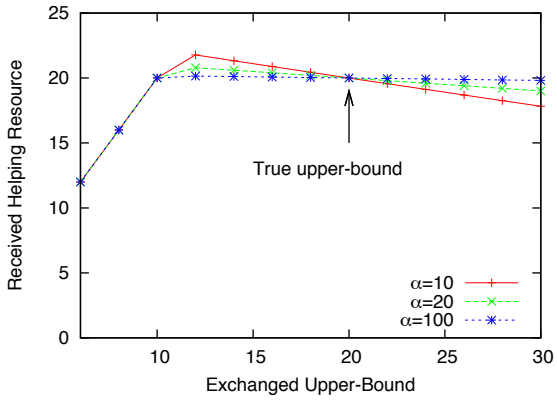


Fig. 9. Resource received vs. exchanged upper-bound. We simulate a network of 3 identically configured nodes with true desired upper-bound $r_{ij} = 20$ requests/day, lower-bound $m_{ij} = 1$ request/day and resource capacity $C_i = 20$ requests/day, for all $i, j \in \{1,2,3\}$. We observe the received resources from nodes 2 and 3 when node 1 changes its claimed upper-bound from 6 requests/day to 30 requests/day.

eventually removed from the network. This execution process is an integrated part of the GUIDEX system.

1) Free Riding: Free riders are nodes that enjoy resources from others while not contributing themselves [31], [32]. A free rider in GUIDEX may collaborate with a large number of IDSs, aiming at receiving a good amount of accumulated resources $\bar{m}$ from the large number of collaborators. However, GUIDEX is not beneficial to free riders. First, the amount of help that a node receives is proportional to the resources it allocates to others. Second, the larger the number of collaborators a node has, the more demanding it is for the node to maintain the collaboration since each collaborator needs minimum resource $\bar{m}$ to be satisfied. Therefore, a node that does not contribute to the collaboration will end up receiving bare minimum helping resources from others. We simulate a scenario where a free rider with initial trust value 1.0 switches to a free riding mode at day 200 (Fig. 10). We notice that the amount of helping resources received by the free rider drops quickly and converges to a low level. This is because the collaborators of the free rider can notice the drop of contributed resources from the free rider and adjust their resource allocation according to (4). The result coorroborates that free riding is not practical in GUIDEX.

2) Denial-of-Service (DoS) Attacks: DoS attacks happen when malicious nodes send a large amount of information to overload the victim [33]. In GUIDEX, the amount of information exchanged between participant nodes is negotiated beforehand. A quota is calculated and sent to all nodes. If a node sends more data than the given quota, then it is considered malicious, and hence will be removed from the collaboration network.

3) Dishonest Insiders: In GUIDEX, dishonest nodes can report false information to gain advantages. For example, a dishonest node can misinform about its upper-bound and lower-bound requests for gaining more resources from its collaborators. GUIDEX imposes a maximum lower-bound $\bar{m}$ for all nodes. In addition, experimental results in Fig. 9 show that claiming a higher upper-bound than the true value lowers received resource, while claiming a lower upper-bound may

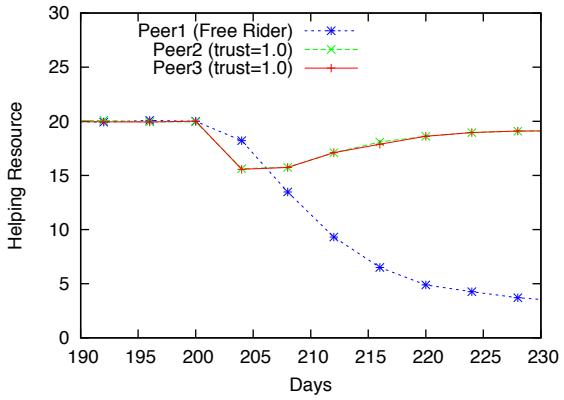


Fig. 10. Resource received after free riding attack

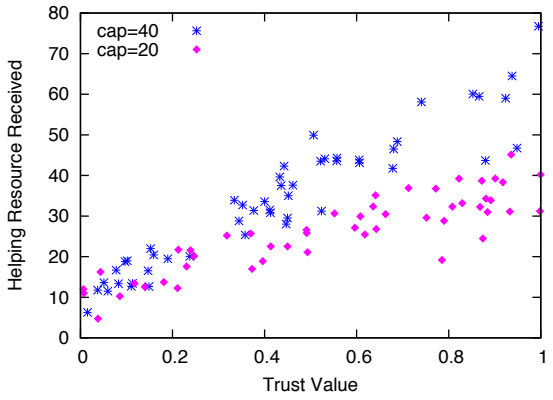


Fig. 11. Resource received for peers with different trust values

lead to a bounded gain that is controllable by system parameter α. A lower upper-bound will not lead to full satisfaction of the node when resource constraints are inactive.

D. Large-Scale Simulation

Previous experiments are 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 resources with the other nodes in the vicinity at a distance of 5. The trust values are generated according to a uniform distribution from 0 to 1.0. The lower bound and the upper bound on the requests are 1 and 20, respectively, for each node. We separate nodes into two groups: one group with a capacity of 20 units and the other with 40. In Fig. 11, we can see that, in both groups, 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 40 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 between 0 and 30. Fig. 12 shows the resource received by nodes with different resource capacities. We note that, on the average, nodes with higher resource capacities receive more resources. This confirms the incentives under a large collaboration group.

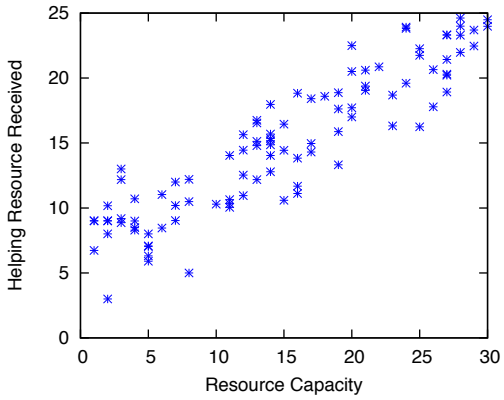


Fig. 12. Resource received for peers with different resource capacities

VI. Conclusion

In this paper, we have proposed GUIDEX, a collaborative intrusion detection architecture, and have discussed its two major building blocks, namely, trust and resource management. In particular, we have analyzed an incentive-based resource allocation problem based on trust management in the context of a collaborative intrusion detection network. By formulating an associated continuous-kernel noncooperative game, we have shown that a Nash equilibrium exists and is unique under certain system conditions. We have also shown that the unique Nash equilibrium possesses features that allow peers to communicate in a conducive environment in which peers endeavor to contribute knowledge 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 showed that the algorithm converges to the Nash equilibrium at a geometric rate, further corroborating the theoretical results. We have also discussed the resistance of GUIDEX to common insider attacks, such as free-riding, dishonest insiders, and DoS attacks. As a future work, we plan to develop an admission control system for IDSs to construct their neighbor lists based on dynamic evaluations of trust and expertise levels. In addition, we can study other potential attacks to the GUIDEX system, for example, the application of reverse engineering for modifying objectives from binary codes.

References

[1] R. Vogt, J. Aycock, and M. Jacobson, "Army of botnets," in *ISOC Symp. on Network and Distributed Systems Security*, 2007.

[2] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, 2004.

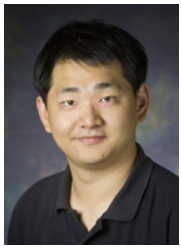
[3] J. Keppler and H. Mountford, *Handbook of Incentive Measures for Biodiversity: Design and Implementation*. OECD, 1999.

[4] V. Yegneswaran, P. Barford, and S. Jha, "Global Intrusion Detection in the DOMINO Overlay System," in *Proc. Network and Distributed System Security Symposium (NDSS'04)*, 2004.

[5] Y. Wu, B. Foo, Y. Mei, and S. Bagchi, "Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS," in *Proc. 19th Annual Computer Security Applications Conference*, 2003.

[6] C. Zhou, S. Karunasekera, and C. Leckie, "A Peer-to-Peer collaborative intrusion detection system," in *International Conference on Networks*, 2005.

[7] 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. CISIM'08.*, pp. 121–126, 2008.
[8] 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.
[9] C. Duma, M. Karresand, N. Shahmehri, and G. Caronni, "A trust-aware, P2P-based overlay for intrusion detection," in *DEXA Workshops*, 2006.
[10] 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)*, 2009.
[11] M. Hsiao and A. Lazar, "Optimal decentralized flow control of Markovian queueing networks with multiple controllers," *Performance Evaluation*, vol. 13, no. 3, pp. 181–204, 1991.
[12] Y. Korilis and A. Lazar, "On the existence of equilibria in noncooperative optimal flow control," *J. ACM (JACM)*, vol. 42, no. 3, pp. 584–613, 1995.
[13] 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.
[14] Y. Yan, A. El-Atawy, and E. Al-Shaer, "Ranking-based optimal resource allocation in peer-to-peer networks," in *Proc. 26th annual IEEE conference on computer communications (INFOCOM 2007), May*, 2007.
[15] C. Grothoff, "An excess-based economic model for resource allocation in peer-to-peer networks," *Wirtschaftsinformatik*, vol. 45, no. 3, pp. 285–292, 2003.
[16] Q. Zhu and T. Başar, "Dynamic Policy-Based IDS Configuration," in *Proc. 47th IEEE Conference on Decision and Control (CDC)*, 2009.
[17] ——, "Indices of power in optimal ids default configuration: theory and examples," in *Proc. 2nd Conference on Decision and Game Theory for Security (GameSec 2011), College Park, MD, USA.*, November 2011.
[18] H. M. Y. Liu, C. Comaniciu, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *Valuetools*, October 2006.
[19] Q. Zhu, C. Fung, R. Boutaba, and T. Başar, "A game-theoretical approach to incentive design in collaborative intrusion detection networks," in *International Conference on Game Theory for Networks (GameNets 09)*, 2009.
[20] C. Fung, J. Zhang, I. Aib, and R. Boutaba, "Dirichlet-based trust management for effective collaborative intrusion detection networks," *IEEE Trans. Network Service Management (TNSM)*, vol. 8, no. 2, pp. 79–91, 2011.
[21] ——, "Robust and scalable trust management for collaborative intrusion detection," in *11th IFIP/IEEE International Symposium on Integrated Network Management*, 2009.
[22] J. Mo and J. Walrand, "Fair end-to-end window-based congestion control," *IEEE/ACM Trans. Netw. (ToN)*, vol. 8, no. 5, pp. 556–567, 2000.
[23] R. Srikant, *The Mathematics of Internet Congestion Control*. Birkhäuser, 2004.
[24] Q. Zhu and L. Pavel, "End-to-end DWDM optical link power-control via a Stackelberg revenue-maximizing model," *Int. J. Netw. Manag.*, vol. 18, no. 6, pp. 505–520, Nov. 2008. [Online]. Available: http://dx.doi.org/10.1002/nem.705
[25] ——, "Enabling osnr service differentiation using generalized model in optical networks," *IEEE Transactions on Communications*, vol. 57, no. 9, pp. 2570–2575, September 2009.
[26] T. Shelling, *The Strategy of Conflict*. Harvard University Press, 1980.
[27] D. Bertsekas, *Network Optimization: Continuous and Discrete Models*. Athena Scientific, 1998.
[28] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.
[29] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. SIAM, Philadelphia, 1999.
[30] A. Berman and R. Plemmons, *Nonnegative Matrices in Mathematical Sciences*. SIAM, 1994.
[31] M. Feldman, C. Papadimitriou, J. Chuang, and I. Stoica, "Free-riding and whitewashing in peer-to-peer systems," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 5, pp. 1010–1019, 2006.
[32] S. Grossman and O. Hart, "Takeover bids, the free-rider problem, and the theory of the corporation," *The Bell Journal of Economics*, pp. 42–64, 1980.
[33] D. Moore, C. Shannon, D. Brown, G. Voelker, and S. Savage, "Inferring internet denial-of-service activity," *ACM Trans. Computer Systems (TOCS)*, vol. 24, no. 2, pp. 115–139, 2006.



Quanyan Zhu (S'04) received his Bachelors degree in Honors Electrical Engineering with distinction from McGill University in 2006. He received his Masters degree in Electrical Engineering from University of Toronto in 2008. He is currently a PhD candidate at the ECE Department and the Coordinated Science Laboratory at University of Illinois at Urbana-Champaign (UIUC), working with Prof. Tamer Başar at the Information Trust Institute (ITI). He is a recipient of NSERC Canada Graduate Scholarship, University of Toronto Fellowship, Ernest A. Reid Fellowship and Mavis Future Faculty Fellowships. He is a recipient of the best track paper award at the 4th international symposium on resilient control systems (ISRCS). He is the organizer of the resilient control system tutorial at CPSWEEK 2012, the TPC Chair (Smart Grid Track) of the 2012 1st INFOCOM workshop on communications and control on sustainable energy systems (CCSES), and the organizer of the 1st midwest workshop on control and game theory (WCGT).

Carol Fung is a PhD student in University of Waterloo, Canada. She received her BSc and Msc from University of Manitoba, Canada. Her research topic is collaborative Intrusion Detection networks, which includes trust management, collaborative decision, resource management, and incentive design of a collaboration framework for intrusion detection networks. She is also interested in the security problems in wireless networks and social networks. She is the recepient of NSERC postgraduate scholarship, NSERC postdoc fellowship, and David Cheriton scholarship. Her papers received the best paper award in IM 2009 and the best student paper award in CNSM 2010.

Raouf Boutaba received the M.Sc. and Ph.D. degrees in computer science from the University Pierre & Marie Curie, Paris, in 1990 and 1994, respectively. He is currently a professor of computer science at the University of Waterloo and a distinguished visiting professor at the division of IT convergence engineering at POSTECH. His research interests include network, resource and service management in wired and wireless networks. He is the founding editor in chief of the IEEE Transactions on Network and Service Management (2007-2010) and on the editorial boards of other journals. He has received several best paper awards and other recognitions such as the Premiers Research Excellence Award, the IEEE Hal Sobol Award in 2007, the Fred W. Ellersick Prize in 2008, and the Joe LociCero and the Dan Stokesbury awards in 2009. He is a fellow of the IEEE.

Tamer Başar (S'71–M'73–SM'79–F'83) is with the University of Illinois at Urbana-Champaign (UIUC), where he holds the positions of Swanlund Endowed Chair; Center for Advanced Study Professor of Electrical and Computer Engineering; Professor, Coordinated Science Laboratory; and Professor, Information Trust Institute. He received B.S.E.E. from Robert College, Istanbul, and M.S., M.Phil, and Ph.D. from Yale University. He is a member of the US National Academy of Engineering, is Fellow of IEEE, IFAC and SIAM, and has served as president of IEEE CSS, ISDG, and AACC. He has received several awards and recognitions over the years, including the highest awards of IEEE CSS, IFAC, AACC, and ISDG, and a number of international honorary doctorates and professorships. He has around 600 publications in systems, control, communications, and dynamic games, including books on non-cooperative dynamic game theory, robust control, network security, and wireless and communication networks. He is the Editor-in-Chief of Automatica and editor of several book series. His current research interests include stochastic teams, games, and networks; security; and cyber-physical systems.