2011 50th IEEE Conference on Decision and Control and
European Control Conference (CDC-ECC)
Orlando, FL, USA, December 12-15, 2011

Secret Information in Communications Networks

Khoa Tran Phan, Mihaela van der Schaar, and William R. Zame

***Abstract*— Some users of a communications network may have more information about traffic on the network than do others – and this fact may be secret. Such information would allow the possessor to tailor its own traffic to the traffic of others, sending a larger amount of traffic when congestion is low and a smaller amount of traffic when congestion is high; this would help the possessor of secret information and (might) harm others.**

To study the impact of secret information we formulate a flow control game with incomplete information where users choose their flows in order to maximize their (expected) utilities given the actions of others. In this environment, the natural baseline notion is Bayesian Nash equilibrium (BNE); we establish the existence of BNE in pure strategies. To capture the effect of secret information, we assume that there is a user who knows the congestion created by other users, but that the presence of this user is *not* known by other users; thus this user has *secret information*. For this environment, we define a new equilibrium concept: the Bayesian Nash Equilibrium with Secret Information (BNE-SI) and establish its existence. We establish rigorous estimates for the benefit and harm that result from secret information; both the benefit and the harm are *smaller* for large networks than for small networks. Simulations confirm the estimates of benefit and harm for networks of different sizes and demonstrate that secret information may in fact benefit *all* users. Secret information may also harm other users in other scenarios. This analysis can be used as a starting point for securing communications networks, both from the network manager and the user's perspectives.

I. Introduction

In this paper we study the interaction of self-interested users in communication networks. Much of the previous analysis of such networks has assumed that users are identically informed about the parameters of the network such as capacity, links, etc. and the characteristics of other users, for instance costs, benefits, etc.; some of the literature allows for the possibility that users have private information (for example, they may know their own characteristics but not the characteristics of others). In many circumstances, however, some users may know much more than other users – and more interestingly, this fact may be secret. The purpose of this paper is to explore the implications of such secret knowledge in communications networks. In particular, we ask how helpful such secret knowledge may be for a user who possesses it and how harmful it may be to users who do not possess it. We show that the answers to these questions depend on the characteristics of the network and especially on the size of the network.

We set our study in the context of flow control. We consider a network of $N+1$ users, drawn at random from a pool of potential users. Users are distinguished by their utility functions, which we think of as their *type*. Each of the users chooses a flow to send to the network and derives a utility that depends on its own flow and on network congestion (which we proxy by average flow). In our baseline scenario, users know the distribution over the pool of potential users but not the realized draw from the distribution. For this scenario, an appropriate solution notion is (symmetric) Bayesian Nash Equilibrium (BNE). Under appropriate assumptions, we show that BNE exist. To explore the impact of secret information, we depart from the baseline scenario by assuming that some user knows, not only its own type (utility function) and the distribution of types of potential users, but also the *realized average flow* of the users in the particular network – but that no other users know this user has this information. Thus, this user has *secret information*. Because in the considered games, only the average flow of others is relevant, the user with secret information is (effectively) *omniscient*: it knows everything. For this scenario, an appropriate solution notion is what we call Bayesian Nash Equilibrium with Secret Information (BNE-SI); under the same assumptions as before, we show that BNE-SI exist.

Information matters because a user who knows the average flow of the other users in the network can choose to send a low flow when the network is congested and a high flow when it is not. Secret information matters because it prevents others from countering the effects of this information. Secret information *always* confers a benefit to a user who possesses it.[1] The actions of a user with secret information are beneficial to other users when those actions reduce congestion and detrimental to others when they increase congestion. However, both of these effects are attenuated when there are many users in the network – most obviously because the impact of *any* one user is attenuated when the network is large, more subtly because the Law of Large Numbers reduces the usefulness of secret information, and more subtly still because the latter effect feeds back into the behavior of a user who possesses secret information. Paradoxically, the overall implication is that secret information may be less important in larger networks than in smaller networks. Our findings have implications for

This work is supported in part by National Science Foundation under Grant No. 0830556 (Phan, van der Schaar) and SES-0518936 (Zame)

K. Phan and M. van der Schaar are with the Department of Electrical Engineering, University of California, Los Angeles (UCLA), USA kphan, mihaela@ee.ucla.edu

W. R. Zame is with the Department of Economics, University of California, Los Angeles (UCLA), USA zame@econ.ucla.edu

[1] By contrast, information that a user is known to possess need *not* confer a benefit on the possessor, and may be harmful.

the necessity for a network manager to provide security, and suggest – again, paradoxically – that security may be less of a concern in larger networks than in smaller networks.

To analyze the mentioned scenarios, we use game-theoretic tools which have been applied to analyze the behavior of users and their performance in communications networks, for example see [1] and references therein. Particularly, there is by now a substantial literature that uses Bayesian games [2] to model the interactions among selfish users with incomplete information who compete for access to network resources (e.g., power and bandwidth). [3], [4] use Bayesian games to capture the effects of information availability and asymmetry on the problem faced by a profit-maximizing manager. Moreover, a literature that might seem parallel to ours but is actually quite distinct considers the problem of malicious users: users whose objective is to damage the network and/or increase the cost incurred by other users; see for instance [5], [6]. Our omniscient users seek only to maximize their own utility from flow; their behavior may harm others, but this is a side consequence of their own selfish maximizing behavior; it is *not* malicious.[2]

II. Bayesian Communication Networks

We consider a network formed by the set $\mathcal{N}$ of $N+1$ users, denoted users $0, 1, \ldots, N$. Potential users in this network are distinguished by their *types*, which we identify with their utility functions; for tractability we assume the space of types is a compact subset of the nonnegative real line: $\Theta \subset \mathbb{R}_+$. Each user in the network sends a flow to the network, and derives an utility/payoff $U(x_i, \overline{x}, \theta_i)$ that depends on its own flow $x_i \in \mathcal{A}$, on the average $\overline{x} = \frac{1}{N+1}\sum_{j\in\mathcal{N}} x_j$ of the flows of all users, and on the type $\theta_i \in \Theta$ of the user. Throughout we assume:

(A1) Flow choices lie in some compact interval $\mathcal{A} \subset \mathbb{R}_+$

(A2) User types are drawn independently from some distribution f with full support in Θ

(A3) Utility U is bounded, measurable, continuously twice differentiable in each of the there variables

(A4) Utility U is differentiably strictly concave in own flow x_i.[3]

Most of the utility functions commonly used in the literature have these properties; examples include:

(i) $U(x_i, \overline{x}, \theta_i) = \theta_i b(x_i) - C(\overline{x})$, where b is strictly increasing, strictly concave, and continuously differentiable; C is strictly increasing, strictly convex, and continuously differentiable

(ii) $U(x_i, \overline{x}, \theta_i) = \theta_i b(x_i) - x_i c(\overline{x})$, where b is assumed as in (i), and c has similar assumptions as C in (i).

The above utility model has been deployed in numerous research works, including [3], [4], [7]– [11] and references therein. We interpret $\theta_i b(x_i)$ as the *benefit* derived by a user with type θ_i who sends flow x_i and $C(\overline{x})$ or $x_i c(\overline{x})$ as the corresponding *cost* incurred on the user when the average flow through the network is $\overline{x}$. The literature typically assumes that cost depends on the total flow through the network [7] rather than on the average flow. We prefer using average flow because it facilitates comparisons across networks of different sizes, especially when we study many users regime. Thus, using the average flow in the cost function makes more sense when considering many users regime. It is worth stressing that the forms (i), (ii) differ only in the cost term. In both cases, cost depends on average flow, which we interpret as a proxy for congestion. In case (i), it is the *total cost* that depends on congestion while in case (ii) it is the *per-unit cost* that depends on congestion. We should note that the utility forms exhibit negative externalities which is typical scenario in flow control games in communications networks [**?**]. Typical benefit and cost functions used in the literature are

- $b(x_i) = \log(x_i)$ (logarithmic benefit) [3], [7], [10]; $b(x_i) = x_i - \alpha x_i^2$ (quadratic benefit) [9], [11]
- $C(\overline{x}) = \gamma \overline{x}^2$ (quadratic total cost) [4], [8]; $c(\overline{x}) = \kappa \overline{x}$ (linear per-unit cost).

We assume for the moment that all of the above is *common knowledge*; that is, each user knows the description of the environment and his own type; each user knows that all other users have the same knowledge; each user knows that all other users know that all other users have the same knowledge, etc. (We deviate from the common knowledge assumption in the following Section when we introduce secret information.) In this context a *strategy* is a (measurable) function $X : \Theta \to \mathcal{A}$ that specifies, for each potential user, the flow choice (as a function of type). To define payoffs conditional on this strategy, write $\theta = (\theta_0, \ldots, \theta_N) \in \Theta^{N+1}$ for a profile of types and $(x_0, \ldots, x_N)$ for a profile of flows; write θ_{-i} for the profile of types of users other than user i. Write

$$\overline{x}_{-i} = \frac{1}{N}\sum_{j\neq i} x_j$$

for the average of flows of users other than user i. Note that the average of flows of all users is $\overline{x} = (x_i + N\overline{x}_{-i})/(N+1)$. To economize on notation, define

$$V(x_i, y, \theta_i) = U(x_i, (x_i + Ny)/(N+1), \theta_i)$$

If user i chooses the flow x_i and others follow the strategy X then the profile of flows of other users is $X(\theta_{-i}) = (X(\theta_0), \ldots, X(\theta_{i-1}), X(\theta_{i+1}), \ldots, X(\theta_N))$ and the average flow of other users is

$$\overline{X}(\theta_{-i}) = \frac{1}{N}\sum_{j\neq i} X(\theta_j)$$

Hence the average flow of all users is $(x_i + N\overline{X}(\theta_{-i}))/(N+1)$. Thus, if user i chooses the flow x_i and others follow the

[2]Due to space limitations, all the proofs are not presented in this version and are included in the technical report available online on the second author's website.

[3]Keep in mind that own flow x_i enters into average flow; hence differentiable strict concavity with respect to own flow x_i means

$$\frac{\partial^2 U}{\partial x_i^2} = U_{11} + \left(\frac{2}{N+1}\right) U_{12} + \left(\frac{1}{N+1}\right)^2 U_{22} < 0$$

strategy X and have realized types θ_{-i}, then user i's user's utility will be $V(x_i, \overline{X}(\theta_{-i}), \theta_i)$. Given the distribution of types, user i's expected utility if he chooses flow x_i and others follow the strategy X will therefore be

$$EU(x_i, \theta_i|X) = \int V(x_i, \overline{X}(\theta_{-i}), \theta_i) f(\theta_{-i}) d(\theta_{-i}) \quad (1)$$

where $f(\theta_{-i}) = f(\theta_0) \dots f(\theta_{i-1}) f(\theta_{i+1}) f(\theta_N)$ and $d(\theta_{-i}) = d\theta_0 \dots d\theta_{i-1} d\theta_{i+1} d\theta_N$. By definition, the strategy X is a *(symmetric) Bayesian Nash Equilibrium* (BNE) where users with the same type choose the same flow if for each type θ_i the flow choice $X(\theta_i)$ is optimal given that others follow the strategy X:

$$X(\theta_i) = \arg\max_{x_i \in \mathcal{A}} \ EU(x_i, \theta_i|X) \quad (2)$$

Notice that given the strategy X of other users, the optimal flow choice $X(\theta_i)$ is unique due to the strict concavity of the utility functions.

Theorem 1: Under assumptions (A1)-(A4), a (symmetric) Bayesian Nash Equilibrium exists.

A monotone increasing strategy is a strategy such that a user of higher type chooses a weakly higher action than a user of lower type. We show that when the utilities are of particular forms, the BNE is monotone.

Proposition 1: Under assumptions (A1)-(A4) and if U is of forms (i) or (ii), then a monotone Bayesian Nash Equilibrium exists.

We caution the reader that Theorem 1 (Proposition 1, respectively) guarantees that a BNE (monotone BNE, respectively) exists but not that it is unique. If BNE is not unique, the assumption that users behave according to a particular BNE requires a form of coordination; such coordination could be obtained, for instance, by a recommendation of the network manager. By definition, no user would have an incentive to deviate (unilaterally) from such a recommendation.

A. Calculating BNE

To illustrate the nature of BNE and in particular the influence of the number of users and the distribution of user types, we offer two examples. Before presenting them, it is useful to make a simple observation. Fix a (symmetric) BNE X and a type θ_i. By definition, $X(\theta_i)$ solves the following optimization problem:

$$X(\theta_i) = \arg\max_{x_i \in \mathcal{A}} \int V(x_i, \overline{X}(\theta_{-i}), \theta_i) f(\theta_{-i}) d(\theta_{-i}). \quad (3)$$

Assuming that the solution to (3) is interior, due to the strict concavity of the utility functions, the solution is determined by the first order condition

$$\int V_1(X(\theta_i), \overline{X}(\theta_{-i}), \theta_i) f(\theta_{-i}) d(\theta_{-i}) = 0. \quad (4)$$

Equation (4) provides a functional equation for the BNE. In general, this functional equation will be intractable and impossible to solve in closed form – even if the utility function V is relatively simple. However, this functional equation is solvable in several representative cases.

Example 1 There are $N+1$ users. Utility has the form

$$U(x_i, \overline{x}, \theta_i) = \theta_i \log(x_i) - \gamma x_i \overline{x}$$

where the cost coefficient $\gamma > 0$ is a constant. The type space and action space are $\Theta = [0, 1]$, and $\mathcal{A} = [0, 1]$, respectively; types are independently and identically distributed according to the distribution $f(\theta_i)$.

Assuming that optimal flow is interior, the first order condition that determines $X(\theta_i)$ reduces to

$$\frac{\theta_i}{X(\theta_i)} - \frac{2\gamma X(\theta_i)}{N+1} - \frac{\gamma N}{N+1} \int_0^1 X(\theta_i) f(\theta_i) d\theta_i = 0. \quad (5)$$

Write $A = \int_0^1 X(\theta_i) f(\theta_i) d\theta_i \in (0, 1)$ and rewrite (5) as a quadratic equation in $X(\theta_i)$

$$2\gamma X(\theta_i)^2 + \gamma N A X(\theta_i) - (N+1)\theta_i = 0. \quad (6)$$

The unique positive solution to this equation is

$$X(\theta_i) = -\frac{NA}{4} + \frac{1}{4\gamma}\sqrt{(\gamma N A)^2 + 8(N+1)\gamma\theta_i}. \quad (7)$$

By definition A must satisfy the identity:

$$A = -\frac{NA}{4} + \frac{1}{4\gamma} \int_0^1 \sqrt{(\gamma N A)^2 + 8(N+1)\gamma\theta_i} f(\theta_i) d\theta_i. \quad (8)$$

It is easy to see that (8) has a unique solution since the left hand side is strictly increasing in A and the right hand side is strictly decreasing in A. Moreover, it can be shown that $A \in (0, 1)$. Hence (continuing to assume that optimal flows are interior) we can solve for the unique BNE by finding the solution to (8) and substituting in (7). Equilibrium expected utility for each type and *ex ante* expected utility are:

$$v(\theta_i) = \theta_i \log X(\theta_i) - \frac{\gamma}{N+1} X(\theta_i)^2 - \frac{\gamma N A}{N+1} X(\theta_i)$$
$$v = \int_0^1 v(\theta_i) f(\theta_i) d\theta_i.$$

An issue of particular interest to us is the way in which BNE depends on the size of the network. It is important to understand that we are not concerned with the exercise of holding the physical network fixed and increasing the number of users. Instead, we imagine that the physical network (capacity, etc.) grows at the same rate as the number of users. In particular, we might imagine that a network doubles in size because two identical networks merge, creating a network with twice the capacity and twice the usage. It is for this reason that we write utility as a function of *average flow* rather than total flow. As noted previously, such capacity expansion rule when the number of users in the system grows has been mentioned and/or considered in [3]

To give some insight into this issue, we calculate and display in Figures 1 and 2 the BNE flow $X(\theta_i)$ and equilibrium expected utility $v(\theta_i)$, respectively for particular parameter choices and various numbers of users. Types are uniformly distributed in $[0, 1]$. We have fixed $\gamma = 8$. The optimal flows are interior in $[0, 1]$ and are monotone with type θ_i as in Proposition 1. When there are large number of users, i.e., more than 100 users, the optimal flows are less dependent on the network size. As in the case of flows, the utility is less dependent on the network size when the network is large.

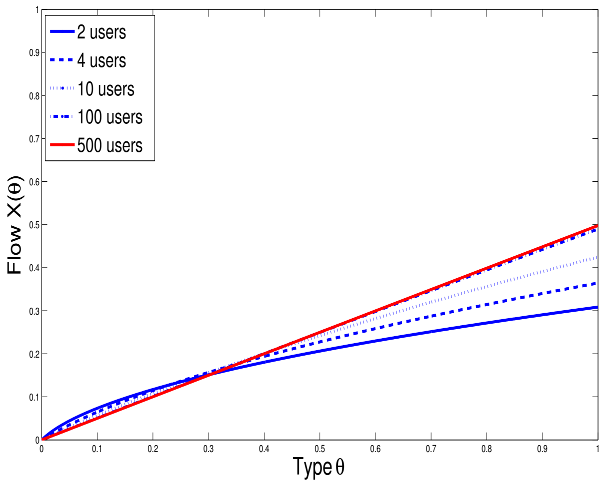

Fig. 1. BNE flow $X(\theta_i)$; $U(x_i, \overline{x}, \theta_i) = \theta_i \log(x_i) - 8x_i\overline{x}$; pdf $f(\theta) = 1$ (uniform distribution)

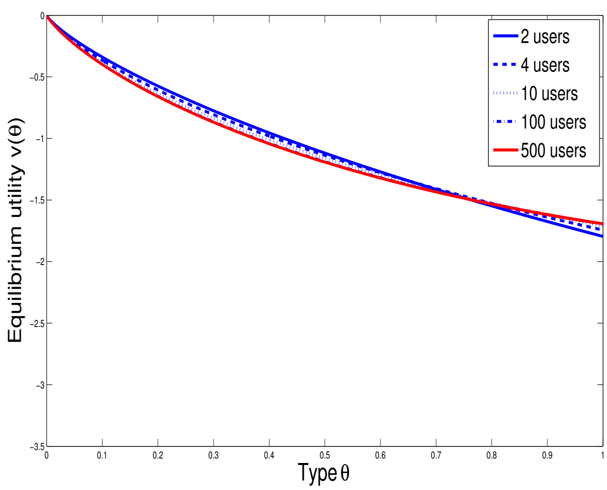

Fig. 2. BNE utility $v(\theta_i)$; $U(x_i, \overline{x}, \theta_i) = \theta_i \log(x_i) - 8x_i\overline{x}$; pdf $f(\theta) = 1$ (uniform distribution)

III. Secret Information: Equilibrium

We now depart from the formulation given above by assuming that one user – say user 0 – has additional information about other users.[4] We focus on the starkest scenario in which user 0 is *omniscient* and hence knows everything relevant about other users; in our scenario that means that user 0 is able to observe the average flow of other users, and hence knows the network congestion.[5] However, the fact that user 0 possesses this information is not common knowledge; rather users $1, \dots, N$ have the same beliefs as in the previous Section, and hence use the same strategies – and user 0 knows this. Thus, user 0 has *secret information*.[6] In this environment, *Bayesian Nash Equilibrium with Secret Information* BNE-SI consists of a strategy $X : \Theta \to \mathcal{A}$ for users $1, \dots, N$ and a strategy $F : \mathcal{A} \times \Theta \to \mathcal{A}$ for the omniscient user 0 such that:

- for each $\theta_i \in \Theta$: $x_i = X(\theta_i)$ maximizes $EU(x_i, \theta_i | X)$
- for each $\theta_0 \in \Theta$, $y \in \mathcal{A}$: $x_0 = F(y, \theta_0)$ maximizes $V(x_0, y, \theta_0)$

Note that at BNE-SI, it is optimal for the omniscient user to exploit its secret knowledge. The interpretation is that users other than 0 behave according to the BNE X (as in the Section 2) but the omniscient user 0 optimizes given the *realized congestion* in the network. We emphasize that at BNE-SI equilibrium, the omniscient user conditions her behavior on her own type and on the realized congestion, but other users believe (wrongly) that 0 conditions only on her own type (and follows the strategy X). We can also interpret that at BNE, users take their actions simultaneously and the action of a user is not revealed to others when they take actions. However, at BNE-SI, users $0, \dots, N$ move first, then, omniscient user 0 moves next after observing the congestion caused by other users.

Our approach to secret information departs from the usual approach in the economics literature, which (almost) always assumes that all details of the environment are common knowledge; see [2], [13], [14] for instance. The usual approach in the economics literature would be to posit that there are two components to the type of user 0, the first component being user 0's utility function (as above) and the second component being user 0's knowledge (ordinary or omniscient); that this is common knowledge; and that all users assign a common prior probability $\varepsilon > 0$ to user 0 being omniscient. Our approach seems more appropriate to the problem at hand.

Our assumptions guarantee that user 0's optimization problem always has a unique solution, so the assumptions of the previous Section guarantee the existence of a BNE-SI.

Theorem 2: Bayesian Nash Equilibrium with Secret Information exists. Moreover, if the Bayesian Nash Equilibrium is unique, so is the Bayesian Nash Equilibrium with Secret Information.

We continue the example in Section 2 and study the strategy of the omniscient user.

Example 2 Consider $N+1$ users with log benefit and linear

[4]The advantage of information in wireless systems has been somewhat considered in [12] where the authors showed that a user would improve its performance if it has more information about the strategy of the competing user.

[5]It would be more than enough for user 0 to observe the types of other users, and hence, given a particular BNE, to infer their flow choices. However it seems much more natural to assume, as we do here, that user 0 observes congestion (average flow) directly, perhaps because it is able to observe network information that is improperly secured.

[6]If that user 0 knows the realized congestion caused by other users is *common* knowledge, then we would have conventional Bayesian game with asymmetric information. However, such games, tho interesting, are out of the scope of this paper.

per-unit cost functions. The strategy of the omniscient user 0 can be shown as

$$F(y,\theta_0) = \min\left\{1, -\frac{Ny}{4} + \frac{1}{4\gamma}\sqrt{(\gamma Ny)^2 + 8(N+1)\gamma\theta_0}\right\} \tag{9}$$

where y is the realized average flow of other users.

IV. Secret Information: Benefit and Harm

The benefit that secret information confers on an omniscient user is the difference between the utility the omniscient user obtains when all others follow a BNE but the omniscient user conditions on its own type *and* on the realized congestion, and the utility the omniscient user obtains when it and all others follow a (given) BNE. We fix a particular type of the omniscient user and focus on the expected benefit of this type (where we take expectations over the types of other users). This seems appropriate because the decision to acquire secret information – which might require the expenditure of resources – might be dependent on type. Hence, given a type $\theta_0 \in \Theta$ of the omniscient user we define:

$$\begin{aligned} G_N(\theta_0) = & \int V\Big(F(\overline{X}(\theta_{-0}),\theta_0), \overline{X}(\theta_{-0}), \theta_0\Big) f(\theta_{-0}) d(\theta_{-0}) \\ & - \int V\Big(X(\theta_0), \overline{X}(\theta_{-0}), \theta_0\Big) f(\theta_{-0}) d(\theta_{-0}) \end{aligned}$$

We retain the subscript N to emphasize that the size of the network matters.

The harm inflicted on any user – say user N – when user 0 has secret information is the difference between the (expected) utility of user N when *all* users follow a BNE and the (expected) utility of user N when user 0 has secret information and conditions on the realization of types. To define the latter utility, fix a type profile $(\theta_0, \ldots, \theta_N)$ and write

$$\overline{Y}(\theta_{-N}) = \left(\frac{1}{N}\right)\Big[N\overline{X}(\theta_{-N}) - X(\theta_0) + F(\overline{X}(\theta_{-0}),\theta_0)\Big]$$

This is the average flow of users other than N provided that user 0 has secret information and chooses the flow $F(\overline{X}(\theta_{-0}),\theta_0)$ but users $i = 1, \ldots, N$ follow X. Hence the expected harm to user N when when user 0 has secret information is

$$\begin{aligned} H_N = & \int V(X(\theta_N), \overline{X}(\theta_{-N}), \theta_N) f(\theta) d(\theta) \\ & - \int V(X(\theta_N), \overline{Y}(\theta_{-N}), \theta_N) f(\theta) d(\theta) \end{aligned} \tag{10}$$

Because user 0 could always disregard his secret information and others do not know he has it, user 0 must (for each of his types $\theta_0 \in \theta_0$) do at least as well in a BNE-SI as in the corresponding BNE, and he will do strictly better except in degenerate scenarios. That is, secret information always has positive value to the user who possesses it: $G_N(\theta_0) > 0$. The magnitude of this value will of course depend on the particular environment; we return to this point below.

However, the impact of user 0's secret information on *other* users is not obvious. To see why, suppose that the BNE X is *monotone*. When users $1, \ldots, N$ have high types, they will send high flows; user 0, observing a highly congested network, will choose to send a lower flow than he would if he followed the BNE strategy X. However, a lower flow from user 0 means that users $1, \ldots N$ in turn experience less congestion than they would if user 0 followed X – and hence users $1, \ldots N$ obtain higher utility than they would if user 0 followed X. The presence of a user with secret information will *benefit* other users for at least *some* type realizations which can be shown to be in the following set

$$\Theta_B^{N+1} = \Big\{\theta \in \Theta^{N+1} \mid F(\overline{X}(\theta_{-0}),\theta_0) < X(\theta_0)\Big\}. \tag{11}$$

Moreover, whether the presence of a user with secret information will benefit other users on average depends on the parameters of the environment and in particular on the distribution of types. Although one might guess that situations in which the presence of a user with secret information will benefit the other users would be unusual, our simulations (discussed below) suggest that they may be quite robust. As an example, let us examine the case of linear per-unit cost function with BNE X. The harm inflicted on user N is

$$\begin{aligned} H_N &= \frac{1}{N+1}\int X(\theta_N)\Big(F(\overline{X}(\theta_{-0}),\theta_0) - X(\theta_0)\Big) f(\theta) d\theta \\ &= \frac{1}{N+1}\Big[\int X(\theta_N) F(\overline{X}(\theta_{-0}),\theta_0) f(\theta) d\theta - A^2\Big] \end{aligned} \tag{12}$$

Since $X(\theta_N)$ and $F(\overline{X}(\theta_{-0}),\theta_0)$ are increasing and decreasing, respectively with θ_N, we have

$$H_N \le \frac{1}{N+1}\Big[A \int F(\overline{X}(\theta_{-0}),\theta_0) f(\theta) d\theta - A^2\Big] \tag{13}$$

An immediate result is that H_N is negative if $\int F(\overline{X}(\theta_{-0}),\theta_0) f(\theta) d\theta < A$. In other words, secret information benefits user N if the expected flow of omniscient user 0 at BNE-SI is less than its expected flow at BNE. On the other hands, the effect of secret information to user N remains unclear even when user 0 sends larger flow at BNE-SI than at BNE on average.

A. Secret Information in Large Networks

We first establish rigorous (although probably coarse) estimates of the benefit that secret information confers on a user who possesses it and the harm inflicted on others by the actions of that user. Intuition suggests that, in a large network, secret information will be of little benefit because (by the Law of Large Numbers) the realized distribution of types 'usually' mimics the known underlying distribution of types, so knowledge of the realized flow of others will not tell a user much it cannot already infer from knowledge of the distribution and the BNE. Intuition also suggests that, in a large network, the actions of a user with secret information will inflict little harm on other users because the flow choice of *any* single user has little impact on average congestion. We show that both of these intuitions are correct and quantify them, and also that there is an additional effec (stemming from the optimization behavior of the user wit secret information) that further dampens the harm caused t other users.

To simply demonstrate the above intuition, we look a the above example of log benefit and linear per-unit co functions where the BNE and BNE-SI strategies are give by (7) and (9), respectively. Due to Law of Large Numbers since users $1, \ldots, N$ follow the BNE strategy, their realize average flow y approaches, i.e., becomes close to, the averag flow of each of them A with high probability. Hence, the flo $F(y, \theta_0)$ in (9) approaches the flow $X(\theta_0)$ in (7). Since th interim expected utility is continuous in own flow, the utilit which user 0 playing BNE-SI obtains approaches the utilit which user 0 playing BNE obtains, i.e., the gain become small. Similarly, the effect of secret information on othe users becomes small.

We are now trying to quantify the gain and harm with respect to the size of the network. As noted earlier, it is appropriate to focus on the benefit to a user of a particular type but on the expected harm to others (taking expectations over types). Because the benefit is always non-negative but the harm to other users may be either positive or negative, we bound the benefit and the absolute value of the harm.

Theorem 3: There is a constant C_1 that depends only on derivatives of U such that

$$G_N(\theta_0) \leq C_1 N^{-1/3} \quad \text{for all} \quad \theta_0 \in \Theta \tag{14}$$

Theorem 4: There is a constant C_2 that depends only on derivatives of U such that

$$|H_N| \leq C_2 N^{-4/3} \tag{15}$$

Notice that the expected *total* harm to other users is NH_N and that $|NH_N| \leq C_2 N^{-1/3}$; in particular, the expected *total* harm to other users tends to 0 as the network becomes large. We should emphasize that the results in Theorem 4 and 5 hold in general for both cases of multiple and unique equilibria.

B. Simulations

To illustrate Theorems 3 and 4, we present simulations in Figure 3 that show the maximum gain available to a user with secret information and the average harm inflicted on others. In Figure 3 utility is $U(x_i, \overline{x}, \theta_i) = \theta_i \log(x_i) - 8x_i\overline{x}$; we consider three distributions. In all cases, we present the average of 10,000 draws from the given distribution. These simulations suggest that the bounds presented in Theorems 3, 4 are crude: at least, convergence of gain and harm appear to be much faster than $N^{-1/3}$ and $N^{-4/3}$. The gain is smallest and largest when types are distributed with increasing, and decreasing distributions f, respectively. Importantly, Figure 3 illustrates the possibility that a user with secret information may benefit others.

We have considered here a scenario in which a single user, otherwise no different from other users, has secret information, which is complete. We have studied the gain and harm to user who possesses secret information and to users who do not, respectively.

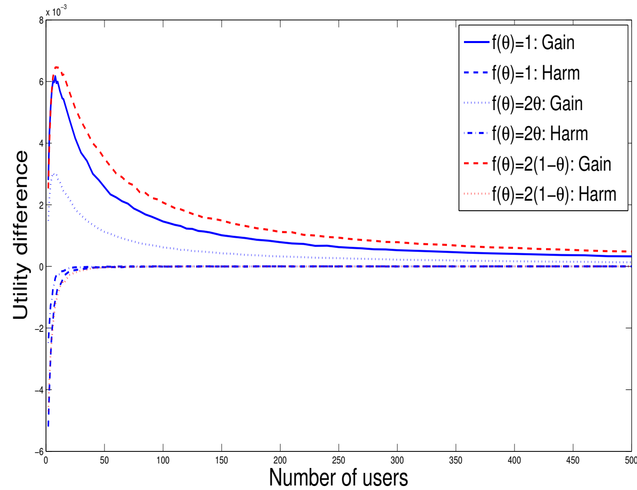

Fig. 3. $U(x_i, \overline{x}, \theta_i) = \theta_i \log(x_i) - 8x_i\overline{x}$; Gain and Harm

REFERENCES

[1] S. Lasaulce, M. Debbah, and E. Altman, “Methodologies for analyzing equilibria in wireless games,” *IEEE Signal Proc. Magazine*, vol. 26, no. 5, pp. 41–52, Sept. 2009.

[2] J. Harsanyi, “Games with incomplete information played by Bayesian players,” *Management Science*, no. 14, pp. 159–182, 320–334, 486–502, 1967-68.

[3] H.-X. Shen, and T. Basar, “Optimal nonlinear pricing for a monopolistic network service provider with complete and incomplete information,” *IEEE Jour. on Sel. Areas in Comms.*, vol. 25, no. 6, pp. 1216–1223, Aug. 2007.

[4] H.-X. Shen, and T. Basar, “Network game with a probabilistic description of user types,” in *Proc. IEEE Conference on Decision and Control* (CDC), 2004.

[5] G. Theodorakopoulos, and J. S. Baras, “Game theoretic modeling of malicious users in collaborative networks,” *IEEE Journal on Sel. Areas in Comms.*, vol. 26, no. 7, pp. 1317–1327, Sept. 2008.

[6] M. Gairing, “Malicious Bayesian congestion games,” *Proc. of the Workshop on Approximation and Online Algorithms* (WAOA), LNCS, pp. 119–132, 2009.

[7] A. Orda, R. Rom, and N. Shimkin, “Competitive routing in multiuser communication networks,” *IEEE/ACM Trans. Networking*, vol. 1, pp. 510–521, Oct. 1993.

[8] O. Candogan, K. Bimpikis, and A. Ozdaglar, “Optimal pricing in the presence of local network effects,” in *Proc. of WINE*, 2010.

[9] S. Stidham Jr., “Pricing and congestion management in a network with heterogeneous users,” *IEEE Trans. Auto. Control*, no. 6, vol. 49, pp. 976–981, June 2004.

[10] J. Mo, and J. Walrand, “Fair end-to-end window-based congestion control,” *IEEE/ACM Trans. Networking*, vol. 8, no. 5, pp. 556–567, Oct. 2000.

[11] M. Mehyar, D. Spanos, and S. H. Low, “Optimization flow control with estimation error,” in *Proc. INFOCOM*, 2004.

[12] Y. Su, and M. van der Schaar, “A simple characterization of strategic behaviors in broadcast channels,” *IEEE Signal Process. Lett.*, vol. 15, pp. 37–40, 2008.

[13] A. Mas-Colell, M. Whinston and J. Green, *Microeconomic Theory*, Oxford University Press, 1995.

[14] J. Ely, D. Fudenberg, and D. Levine, “When is reputation bad?” *Games and Economic Behavior*, vol. 63, pp. 498-526, 2008.