A Game Theoretic Approach to Anonymous Networking

Parv Venkitasubramaniam, *Member, IEEE,* Lang Tong, *Fellow, IEEE,*

***Abstract*—Anonymous wireless networking is studied when an adversary monitors the transmission timing of an unknown subset of the network nodes. For a desired quality-of-service (QoS), as measured by network throughput, the problem of maximizing anonymity is investigated from a game-theoretic perspective. Quantifying anonymity using conditional entropy of the routes given the adversary's observation, the problem of optimizing anonymity is posed as a two player zero-sum game between the network designer and the adversary; the task of the adversary is to choose a subset of nodes to monitor so that anonymity of routes is minimum whereas the task of the network designer is to maximize anonymity by choosing a subset of nodes to evade flow detection by generating independent transmission schedules.**

In this two player game, it is shown that a unique saddle point equilibrium exists for a general category of finite networks. At the saddle point, the strategy of the network designer is to ensure that any subset of nodes monitored by the adversary reveals identical amount of information about the routes. For a specific class of parallel relay networks, the theory is applied to study the optimal performance tradeoffs and equilibrium strategies. In particular, when the nodes employ transmitter directed signaling, the tradeoff between throughput and anonymity is characterized analytically as a function of the network parameters and the fraction of nodes monitored. The results are applied to study the relationships between anonymity, fraction of monitored relays and the fraction of hidden relays in large networks.

Keywords– anonymity, wireless networks, saddle point equilibrium, eavesdropper, traffic analysis

I. Introduction

A. Motivation

The packet transmission times[1] of nodes in a network can reveal significant information about the source-destination pairs and routes of traffic flow in the network [1], [2]. Equipped with such information, a malicious adversary can launch more powerful attacks such as wormhole, jamming or denial of service. Anonymous networking is the act of communicating over a network without revealing the identities of source-destinations or the path of flow of packets.

The typical design of anonymous networking protocols models adversaries as omniscient and capable of monitoring every single transmission in the network perfectly. From a practical standpoint, this is far too conservative, and such universal information would be available only to the network owner or a centralized controller. In this work, our goal is to study the problem of anonymity in networks under a more general adversary model, where an *unknown* subset of the nodes are monitored by the adversary. The subset of monitored nodes could depend on the physical location of the adversary, or partial knowledge of network transmission protocols. It is also possible that in some public wireless networks, certain nodes may have weaker physical protection than others, and are hence, more vulnerable to transmission monitoring.

From a network design perspective, the goal is to design transmission and relaying strategies such that the desired level of network performance is guaranteed with maximum *anonymity of network routes*. Providing anonymity to the routes of data flow in a network requires modification of packet transmission schedules and additional transmissions of dummy packets to confuse an external observer. These modifications however reduce the achievable network performance, particularly in ad hoc wireless networks, where the scheduling needs to satisfy medium access constraints on the shared channel. Therefore, depending on the desired quality of service (QoS), it is necessary to pick the optimal set of nodes to modify transmission schedules so that anonymity is maximized without violating QoS requirements.

If the network designer were aware of which nodes of the network were being monitored by the adversary, the optimal set of nodes can be chosen such that minimum information is revealed through the monitored nodes. However, if the adversary is aware of the set of nodes that the network designer has chosen to protect, then he can alter his choice of nodes to monitor so that maximum information about the network routes is retrieved. This "interplay" between the network designer and the adversary is the main subject of this work, and it is studied using a game-theoretic approach.

Since the set of monitored nodes is unknown to the network designer, a conservative approach would be to design the scheduling strategy assuming an omniscient adversary. However, since the power of the adversary, *i.e.* the maximum fraction of monitored nodes, is bounded, we would like to investigate if the strategies of the network designer and the adversary can be analyzed jointly to get a better tradeoff between anonymity and network performance compared to that under the omniscient assumption (see Figure 1). To this end, we propose a two-player zero sum game between the adversary and the network designer, where the payoff is anonymity, the action of the adversary is to choose which nodes to monitor to minimize payoff and the action of the network designer is to choose which nodes of the network to "hide" from the adversary to maximize the payoff subject to the QoS constraint.

Parv Venkitasubramaniam is with the School of Electrical and Computer Engineering, Lehigh University.

Lang Tong is with the School of Electrical and Computer Engineering, Cornell University.

[1] Transmission time in this work refers to the time point of transmission, and not the duration or latency.

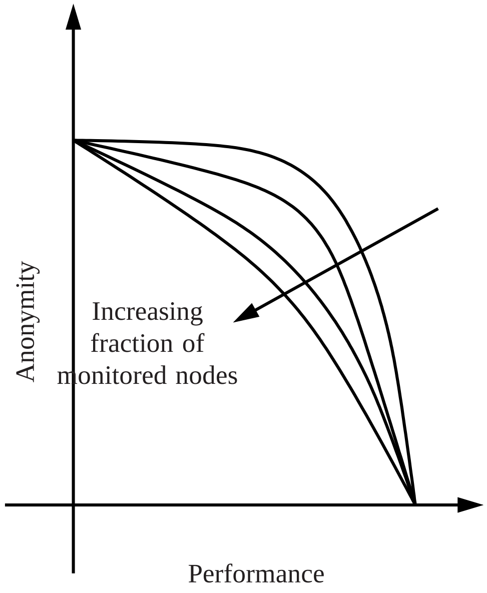


Fig. 1. Anonymity-Performance Tradeoff: as the fraction of monitored nodes gets smaller, we wish to compute the improvement in the performance tradeoffs.

The game-theoretic perspective can be understood using an example of a $2-$relay parallel network as shown in Figure 2. During any period of observation of the adversary, we assume that the network operates in one of two configurations $\mathbf{s}_1$ or $\mathbf{s}_2$ (see Figure 2) wherein,

$$\begin{aligned}\mathbf{s}_1 &= \{(A_1, B_1, C_1), (A_2, B_2, C_2)\},\\ \mathbf{s}_2 &= \{(A_1, B_2, C_2), (A_2, B_1, C_1)\}\end{aligned}$$

are the set of active routes in each configuration (henceforth referred to as a *network session*). The adversary's goal is to identify which of these sessions is currently active in the network by monitoring the transmission timing of the monitored nodes.

Consider a transmitter directed signaling model, where each node transmits on a unique orthogonal channel such that transmissions of multiple nodes are non interfering. Under this signaling scheme, merely detecting the transmission times of packets by a node will not reveal the identity of the intended receiver. Suppose in this setup, the adversary can only afford to monitor the transmissions of two nodes. An adversary would therefore have to detect correlations across transmission schedules of a source and a relay to identify the flow of traffic. For example, if B_1 forwarded packets as and when they arrived from the source, then during network session $\mathbf{s}_1$, the transmission schedules of A_1 and B_1 would be highly correlated, whereas, during $\mathbf{s}_2$, the schedules of A_1 and B_1 would be statistically independent. An adversary who merely monitors nodes A_1 and B_1 would therefore be able to identify the network session perfectly by detecting the dependence between schedules. Suppose, instead, the relays B_1 and B_2 always use transmission schedules that are statistically independent of the arrival schedules from the sources. Then, no information about the session can be obtained by monitoring the transmission schedules of any pair of nodes. Using independent schedules, however, requires dummy transmissions by the relays thus reducing the rate of data packets forwarded by each relay.

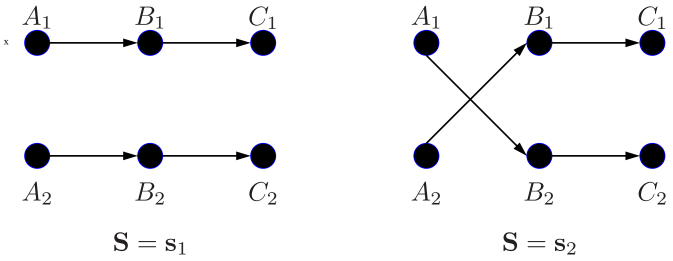


Fig. 2. $2-$relay parallel network: Two possible sessions, each containing two paths. $\mathbf{s}_1 = \{(A_1, B_1, C_1), (A_2, B_2, C_2)\}, \mathbf{s}_2 = \{(A_1, B_2, C_2), (A_2, B_1, C_1)\}$.

Consider a scenario when the throughput requirement mandates that at most one relay can generate independent schedules (using dummy transmissions). If only relay B_1 generates a transmission schedule that is statistically independent of that of A_1 and A_2, then the optimal strategy for the adversary would be to monitor (A_2, B_2) or (A_1, B_2), either of which would help him perfectly determine the session. However, given the knowledge that the adversary would monitor (A_1, B_2) or (A_2, B_2), the optimal strategy of the network designer would be to make the schedule of B_2 always independent thus maximizing anonymity.

A natural question that arises is: is there a pair of strategies for the network designer and the adversary that neither has any incentive to modify? In other words, if formulated as a two-player zero-sum game between the adversary and the network designer with anonymity as the payoff, does a Nash equilibrium exist? As will be shown in Section III, a saddle point equilibrium does exist in the class of mixed strategies. For this example, at the equilibrium point, the optimal strategy for the network designer is to choose one of the relays with probability $\frac{1}{2}$ to generate independent schedules, and the optimal strategy for the adversary is to monitor each source-relay pair with probability $\frac{1}{4}$. By definition, at this operating point, neither the network designer nor the adversary have any incentive to modify their strategies (See Theorem 3).

The example discussed above involves a simple scenario with only two possible network sessions and the adversary has two kinds of observations: a pair of dependent or a pair of independent schedules. In a general multihop network, anonymity based on partial information about the session can be quantified using Shannon's equivocation [3], [4], and our goal in this work is to optimize the tradeoff between the desired network throughput and the achievable anonymity as a function of the adversary's monitoring capability.

B. Main Contributions

In this work, we consider a game-theoretic formulation of anonymous networking in a general class of finite wireless networks when the number of nodes monitored by an adversary model is bounded by a known constant. We pose the design problem as a two player zero sum game with equivocation (conditional entropy) of the network session as the payoff; the adversary's strategy is to pick a random subset of nodes to monitor, and the network designer's strategy is to pick a random subset of nodes to generate independent schedules, thus avoid detection. For the class of finite multihop networks considered, we prove that a saddle point equilibrium always exists in the class of centralized strategies[2]. Note that since anonymity, as defined by conditional entropy, is a non-linear function of the probabilities of mixing multiple strategies, the existence of Nash equilibria in classical two-player zero-sum games [5], where payoff of mixed strategies are weighted sum of pure strategy payoffs, does not directly apply.

To demonstrate the applicability of the game-theoretic model, we consider a general class of parallel relay networks. For a symmetric relay model, we characterize analytically the throughput-anonymity tradeoff as a function of the adversary's power and using the results on player strategies, derive the saddle point strategies which are understandably symmetric. We then introduce asymmetry into the properties of the relay rate and the information model, and using the derived results on saddle point strategies, demonstrate the gain of the game-theoretic approach over naive intuitive strategies. We also show that the game-theoretic approach can be used to study large parallel relay networks, by characterizing the asymptotic relationships among anonymity, the fraction of monitored relays and the fraction of covert relays.

C. Related Work

Anonymous communication over the Internet is fairly well studied, where many applications have been designed based on the concept of traffic mixes proposed by David Chaum [6]. Mixes are routers or proxy servers that collect packets from multiple users and transmit them after reencryption and random delays so that, incoming and outgoing packets cannot be matched by an external observer. While mix-based solutions have been used in applications such as anonymous email or browsing, it has been shown that when long streams of packets with latency or buffer constraints are forwarded through mixes, it is possible to correlate incoming and outgoing streams almost perfectly [7].

In wireless networks, an alternative solution to Mixing is the use of cover traffic [8], [9], which ensures that, irrespective of the active routes, the transmission schedules of all nodes are fixed apriori. If a node does not have any data packets, the transmission schedule is maintained by transmitting dummy packets. While the fixed scheduling strategy provides complete anonymity to the routes at all times, it was found to be inefficient [8] due to high rate of dummy transmissions, and the implementation required synchronization across all nodes which is not practical in ad hoc wireless networks. In this work, the technique used to provide anonymity is similar to that in [10], where a subset of relays (referred to as *covert relays*) generate independent transmission schedules using dummy transmissions.

The general adversary model considered here necessitates a game-theoretic formulation of the problem. Game theory [11] has been used in a wide range of multi-agent problems from economics to networking. In the context of network security, earlier applications were focused on jamming. Basar considered the problem of jamming in Gaussian channels [12] where it was shown that the optimal jamming strategy is either a linear function of jammer's observation or an additive independent Gaussian noise. Borden, Mason and McEliece [13] considered the information theoretic saddlepoints of the jamming game under hard/soft quantization schemes. More recent work along this line include [14]–[16]. Game-theoretic models have also been used to model problems related to distributed intrusion detection [17], [18], where the goal is to design attacking and detection strategies with probability of detection as the payoff. In [19], game-theory was used to study attacker and defense strategies on a graphical model of a network, where the attackers choose nodes to compromise while the defender picks links to "clean up". To the best of our knowledge, ours is the first application of game-theory to hiding traffic flows in the presence of eavesdroppers. The work closest to ours in this regard is that of information concealing games using finite dimensional data [20] where one of the players (the adversary) chooses a subset of available resources to hide, while the opponent (the network user) chooses a subset of resources based on the revealed observation to maximize his utility. The authors identify conditions under which Nash equilibria exist and provide approximation techniques to compute the equilibria. Conceptually, this problem has some similarities to our strategy of choosing covert relays, where the network designer chooses to hide a subset of relays, whereas the adversary chooses a subset of relays to monitor. In our model, the adversary's observation depends on the actions of both the players which are decided apriori, and the payoff is a non-linear function of the probabilities of mixing strategies, thus different from classical mixed strategy models [5].

Our mathematical model for anonymity is based on the framework proposed in [10], where conditional entropy of the network session was proposed as a metric for anonymity. Entropy and measures related to entropy such as K-L divergence have been proposed as payoffs in games of complexity [21]. Entropy in such contexts were used as metrics of complexity, rather than a measure of uncertainty.

II. System Model

Notation: Let the network be represented by a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes in the network and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ is the set of directed links. (A, B) is an element of $\mathcal{E}$ if and only if node B can receive transmissions from node A. A sequence of nodes $P = (V_1, \cdots, V_n)$ is a *valid path* in $\mathcal{G}$ if $(V_i, V_{i+1}) \in \mathcal{E},\ \forall i < n$. The set of all loop-less paths is denoted by $\mathcal{P}(\mathcal{G})$.

A. Adversary Observation and Inference

During any network observation by the adversary, a subset of nodes communicate using a fixed set of paths. This set of paths $\mathbf{S} \in 2^{\mathcal{P}(\mathcal{G})}$ is referred to as a network *session*. The adversary's goal is to use his observation to identify the session. We model $\mathbf{S}$ as an i.i.d. random variable $\mathbf{S} \sim p(\mathbf{s})$.

[2] Centralized strategies are strategies which require co-ordinated action across all nodes of the network. Such strategies can be implemented using a single central controller, the use of shared randomness across nodes, or limited message passing between nodes

The prior $p(\mathbf{s})$ on sessions is assumed to be available to the adversary. The set of possible sessions $\mathcal{S}$ is given by $\mathcal{S} = \{\mathbf{s} \in \mathcal{P}(\mathcal{G}) : p(\mathbf{s}) > 0\}$. (See example sessions in Figure 2).

Transmitter Directed Signaling The adversary's observation would depend on the underlying physical layer signaling model. In this work, we consider orthogonal transmitter directed signaling at the physical layer, where each node utilizes a unique orthogonal signaling scheme such that a transmission schedule detected by the adversary would reveal only the transmitting node and not the intended receiving node.

Observable Session The goal of the network designer is to modify transmission schedules of the nodes in every session such that the monitored nodes reveal as little information about the actual session as possible. For instance, if a subset of relays always generate independent transmission schedules then it is not possible for the adversary to determine which paths pass through them. In effect, the set of (broken) paths observable would be a distorted version of the actual session. Let $\hat{\mathbf{S}}$ (henceforth referred to as *observable session*) denote the set of paths as observed by an omniscient adversary.

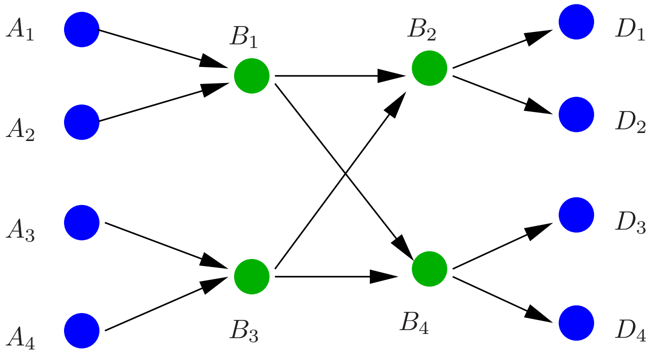


Fig. 3. Switching Network: $\{A_i\}$ transmit to $\{C_i\}$ through relays $\{B_i\}$.

For example, consider the switching network in Figure 3, where every session is defined by a unique pairing of sources and destinations (each A_i sends packets to a unique D_j through intermediate relays). In this network, consider a session $\mathbf{s}_1$ given by the set of paths:

$$\mathbf{s}_1 = \left\{ \begin{array}{c} (A_1, B_1, B_4, D_3), (A_2, B_1, B_2, D_2), \\ (A_3, B_3, B_2, D_1), (A_4, B_3, B_4, D_4) \end{array} \right\}.$$

Suppose node B_1 generated an independent schedule regardless of the arrival times from A_1, A_2. Then, an omniscient adversary would not be able to identify the paths of the packet streams from A_1 and A_2 after they reach B_1. Therefore, the observable session would contain the set of paths:

$$\hat{\mathbf{S}} = \left\{ \begin{array}{c} A_1, A_2, (B_1, B_4, D_3), (B_1, B_2, D_2), \\ (A_3, B_3, B_2, D_1), (A_4, B_3, B_4, D_4) \end{array} \right\}. \quad (1)$$

Adversary Observation Under a general adversary model, packet transmission times of a subset of nodes are observed by the adversary. Specifically, the adversary randomly chooses any subset of nodes, denoted by $\mathbf{N}_a$, to monitor. The maximum number of monitored nodes is denoted by k_a (also referred to as *power of the adversary*). We model $\mathbf{N}_a$ as a random variable where the random distribution of $\mathbf{N}_a$ is chosen by the adversary to maximize his payoff. Depending on the observable session $\hat{\mathbf{S}}$ and the set of monitored nodes $\mathbf{N}_a$, the adversary's observation $\hat{\mathbf{S}}_a$ would be a further distorted version of the underlying session $\mathbf{S}$. The adversary's net observation can be represented by a set of paths $\hat{\mathbf{S}}_a$ and would be given by a deterministic function $f_a(\hat{\mathbf{S}}, \mathbf{N}_a)$. (Note that $f_a(\hat{\mathbf{S}}, \mathcal{V}) = \hat{\mathbf{S}}$).

In the switching network example of Figure 3, let B_1 be covert in session $\mathbf{s}_1$. Then (1) provides the observable session (omniscient adversary). If the adversary monitors nodes A_1, A_3, B_1 and B_3, then

$$\hat{\mathbf{S}}_a = \{A_1, B_1, (A_3, B_3)\}.$$

B. Performance Metrics: Anonymity and Throughput

The task of the network designer is to design the probability distribution of observable sessions, denoted by $q_n(\hat{\mathbf{s}}|\mathbf{s})$, such that a desired QoS is achieved while the adversary obtains minimum information about the session $\mathbf{S}$ by observing $\hat{\mathbf{S}}_a$. The task of the adversary, on the other hand, is to design the probabilities $q_a(\mathbf{N}_a)$ of choosing nodes to monitor s.t. maximum information is obtained by observing $\hat{\mathbf{S}}_a$.

Anonymity We quantify anonymity using Shannon's equivocation [3] which measures the uncertainty of the underlying session given the adversary's observation.

Definition 1: We define the *anonymity* $A(q_n, q_a)$ for a network strategy $q_n(\hat{\mathbf{s}}|\mathbf{s})$ w.r.t adversary strategy $q_a(\mathbf{n}_a)$ as the normalized conditional entropy of the sessions given the adversary observation:

$$A(q_n, q_a) \triangleq \frac{H(\mathbf{S}|\hat{\mathbf{S}}_a)}{H(\mathbf{S})}. \quad (2)$$

The normalization ensures that the anonymity is always between 0 and 1. The motivation behind the above definition comes from Fano's inequality which lower bounds the adversary's probability of error by the conditional entropy [22]. Note that previous entropy-based definitions of anonymity [4], [10] in the context of omniscient adversaries are special cases of Definition 1 (when $\mathbf{N}_a \equiv \mathcal{V}$).

Throughput Since distorting the observable session requires modification of transmission schedules, the latency and bandwidth constraints in the network would require transmission of dummy packets and result in a reduced rate of data packets delivered from the sources to destinations. Let $\Lambda(\mathbf{s}, \hat{\mathbf{s}})$ represent the sum-rate of packets deliverable from sources to destinations when the actual session is $\mathbf{s}$ and the observable session is $\hat{\mathbf{s}}$. Note that $\Lambda(\mathbf{s}, \hat{\mathbf{s}}) \leq \Lambda(\mathbf{s}, \mathbf{s})$.

Definition 2: The *throughput* $\Upsilon(q_n)$ of a scheduling strategy $q_n(\hat{\mathbf{S}}|\mathbf{S})$ is defined as

$$\Upsilon(q_n) = \mathbb{E}\left(\Lambda(\mathbf{S}, \hat{\mathbf{S}})\right) \quad (3)$$

where the expectation is over the joint pdf of $\mathbf{S}$ and $\hat{\mathbf{S}}$.

Anonymity and throughput are essentially two opposing paradigms in the design of the optimal scheduling strategy; transmitting more dummy packets increases anonymity whereas higher throughput necessitates fewer dummy transmissions. Unlike the omniscient adversary setup, since the power of the adversary is bounded, the uncertainty in the identities of the monitored nodes, *i.e.* the randomness in $\mathbf{N}_a$, necessitates the game-theoretic formulation, as was illustrated in the example in Section I. In the following section, we formulate this problem as a two-player zero sum game, and establish the existence of a saddle point equilibrium.

III. Two Player Game using Covert Relaying Strategy

Consider a two-player zero sum game $\mathbb{G}_a$, defined by a $3-$tuple $(\mathcal{A}_n, \mathcal{A}_a, \phi)$ where $\mathcal{A}_n$ and $\mathcal{A}_a$ denote the action spaces of the network designer and the adversary respectively, and $\phi : \mathcal{A}_n \times \mathcal{A}_a \mapsto [0,1]$ is the payoff function for the network designer (the adversary's payoff is $-\phi(\cdot,\cdot)$).

A. Action Spaces

In its most general form, the action space for the network designer would include the set of all probability distributions $q_n(\hat{\mathbf{S}}|\mathbf{S})$ over the space of all loop-less paths $\mathcal{P}$. In this work, we restrict the set of observable sessions to those achievable using the set of *covert relaying strategies* where each relay node belongs to one of two categories: *covert* or *visible*.

Covert relay A covert relay B generates an outgoing transmission schedule that is statistically independent of the schedules of all nodes occurring previously in paths that contain B. Due to statistical independence, no adversary can detect the flow of traffic through a covert relay. Covert relaying is a modification to the transmission scheduling which provides anonymity and yet adheres to the medium access and delay constraints of the system.

Visible relay A visible relay B transmits every received packet immediately upon arrival thereby ensuring all arriving packets are relayed successfully within the latency constraint. However, the traffic flow through the visible relay operating under this highly correlated schedule is easily detected by an eavesdropper. (A statistically consistent detector for this purpose has been designed in [23].)

In a given session $\mathbf{s}$, if the set of covert relays is $\mathbf{b}_n$ then the observable session $\hat{\mathbf{s}}$ can be expressed as a deterministic function $f_o(\mathbf{s}, \mathbf{b}_n)$. For a transmitter directed signaling model, $f_o(\mathbf{s}, \mathbf{b}_n)$ is a set of paths such that: for every path in $\mathbf{s}$ which has k covert relays, $f_o(\mathbf{s}, \mathbf{b}_n)$ contains $k+1$ paths, each beginning at the source or a covert relay and terminating one relay before the subsequent covert relay or the destination. This is because covert relay schedules prevent the adversary from detecting any correlation between the schedule of a prior node in the path with that of the relay.

We model the set of covert relays in a session by a random variable $\mathbf{B}_n$ with conditional distribution $\{q_n(\mathbf{b}_n|\mathbf{s})\}$ and the class of covert relaying strategies is defined by the set of all probability distributions $\{q_n(\mathbf{b}_n|\mathbf{s})\}$. Note that this is a restrictive action space where it may not be possible to realize all observable sessions in $2^{\mathcal{P}(\mathcal{G})}$ for any session $\mathbf{s}$.

As expected, maintaining independent schedules would require covert relays to drop packets or add dummy packets consequently reducing the rate of relayed data packets, whereas visible relays can relay every packet that arrives without any loss in rate. The loss in rate at a covert relay would be a function of the probability distributions of transmission schedules, delay and bandwidth constraints, and the relaying strategy. In a session $\mathbf{s}$, let $\Lambda'(\mathbf{s}, \mathbf{b}_n)$ denote the achievable sum-rate when the relays in the set $\mathbf{b}$ are covert. Note that since $\mathbf{s}, \mathbf{b}$ perfectly determine the observable session $\hat{\mathbf{s}}$,

$$\Lambda'(\mathbf{s}, \mathbf{b}_n) = \Lambda(\mathbf{s}, f_o(\mathbf{s}, \mathbf{b}_n)).$$

The characterization of the exact rate loss is not necessary for this exposition, and we will treat it as an abstract quantity. In the subsequent section, where we study parallel relay networks, we shall use specific scheduling and relaying strategies, and provide an analytical characterization of the rate loss for that class of networks.

For a given strategy $q_n(\mathbf{b}_n|\mathbf{s})$, the throughput Υ can be expressed as a linear function:

$$\Upsilon(q_n) = \sum_{\mathbf{s} \in \mathcal{S}} p(\mathbf{s}) \sum_{\mathbf{b} \in 2^{\mathcal{V}}} q_n(\mathbf{b}|\mathbf{s}) \Lambda'(\mathbf{s}, \mathbf{b}).$$

By restricting ourselves to the class of covert relaying strategies, we define the action spaces for the network designer and the adversary in the game as follows.

The action of the network designer is to select the probability mass function $q_n(\mathbf{b}_n|\mathbf{s})$ that chooses covert relays in each session $\mathbf{s}$. The key constraint in this design is the throughput requirement ($\Upsilon(q_n) \geq \gamma$). Accordingly

$$\mathcal{A}_n = \left\{ \begin{array}{c} \{q_n(\mathbf{b}_n|\mathbf{s}) : \mathbf{s} \in \mathcal{S}, \mathbf{b}_n \subset \mathcal{V}\} : \\ \Upsilon(q_n) \geq \gamma \\ q_n(\mathbf{b}_n|\mathbf{s}) \geq 0, \forall \mathbf{s}, \mathbf{b}_n \\ \sum_{\mathbf{b}_n} q_n(\mathbf{b}_n|\mathbf{s}) = 1, \forall \mathbf{s} \end{array} \right.$$

The action of the adversary is to design the probability distribution $q_a(\mathbf{n}_a)$ of picking nodes to monitor during the session, subject to the constraint on the maximum number of monitored nodes ($\mathbf{n}_a \in \mathcal{V}^{k_a}$). Therefore,

$$\mathcal{A}_a = \left\{ \begin{array}{c} \{q_a(\mathbf{n}_a) : \mathbf{n}_a \in \mathcal{V}^{k_a}\} \\ q_a(\mathbf{n}_a) \geq 0, \forall \mathbf{n}_a \\ \sum_{\mathbf{n}_a} q_a(\mathbf{n}_a) = 1 \end{array} \right.$$

B. Payoff and Saddle Point

For a given observable session $\hat{\mathbf{s}} = f_o(\mathbf{s}, \mathbf{b})$, the adversary observation $\hat{\mathbf{s}}_a$ would be restricted to the paths between monitored nodes in $\mathbf{n}_a$. In other words

$$\hat{\mathbf{s}}_a = f_a(\hat{\mathbf{s}}, \mathbf{n}_a) \stackrel{\triangle}{=} \{\mathbf{p} \bigcap \mathbf{n}_a : \mathbf{p} \in \hat{\mathbf{s}}\}.$$

Define $\mathcal{F}_a : 2^{\mathcal{P}(\mathcal{G})} \times 2^{\mathcal{V}} \mapsto 2^{\mathcal{S}\times 2^{\mathcal{V}}}$ to be the adversary's uncertainty set:

$$\mathcal{F}_a(\hat{\mathbf{s}}_a, \mathbf{n}_a) = \{(\mathbf{s}, \mathbf{b}) : f_a(f_o(\mathbf{s}, \mathbf{b}), \mathbf{n}_a) = \hat{\mathbf{s}}_a\}.$$

In other words, if the adversary monitors $\mathbf{n}_a$, $\mathcal{F}_a(\mathbf{p}, \mathbf{n}_a)$ is the set of possible pairs of session and covert relays that would lead to the observation $\mathbf{p}$ through the nodes $\mathbf{n}_a$.

For a given pair of strategies $(q_n, q_a) \in (\mathcal{A}_n \times \mathcal{A}_a)$, the payoff function $\phi(q_n, q_a)$ is the anonymity which from Definition 1 is given by:

$$\begin{aligned}\phi(q_n, q_a) &= \frac{H(\mathbf{S}|\hat{\mathbf{S}}_a)}{H(\mathbf{S})} \\ &= \frac{1}{H(\mathbf{S})} \sum_{\mathbf{n}_a \in 2^{\mathcal{V}}} \sum_{\mathbf{s}\in\mathcal{S}, \mathbf{b}_n \in 2^{\mathcal{V}}} -q_a(\mathbf{n}_a) p(\mathbf{s}) \times \\ &\quad q_n(\mathbf{b}_n|\mathbf{s}) \log q_{ap}(\mathbf{s}, f_a(f_o(\mathbf{s}, \mathbf{b}_n), \mathbf{n}_a), \mathbf{b}_a)\end{aligned} \tag{4}$$

where $q_{ap}(\mathbf{s}, \hat{\mathbf{s}}_a, \mathbf{n}_a) \triangleq \dfrac{\sum_{\mathbf{b}: f_a(f_o(\mathbf{s},\mathbf{b}),\mathbf{n}_a)=\hat{\mathbf{s}}_a} q_n(\mathbf{b}|\mathbf{s})p(\mathbf{s})}{\sum_{(\mathbf{s}',\mathbf{b}')\in\mathcal{F}_a(\hat{\mathbf{s}}_a,\mathbf{b})} q_n(\mathbf{b}'|\mathbf{s}')p(\mathbf{s}')}$ (5)

is the a posteriori probability that the current session is $\mathbf{s}$ given the adversary observes $\hat{\mathbf{s}}_a$ through the nodes $\mathbf{n}_a$.

In a zero-sum game, we know that the interests of the network designer and the adversary are exactly opposite; while the network designer would prefer to make the monitored nodes covert, the adversary would prefer to monitor the visible nodes. We wish to determine if there is an operating point in the pair of action spaces, where neither the network nor the adversary has any incentive to change their strategy, in other words, if this game has a saddle point equilibrium.

Definition 3: A pair of strategies $(q_n, q_a) \in \mathcal{A}_n \times \mathcal{A}_a$ constitutes a *saddle point equilibrium* if:

$$\phi(q_n, q_a) = \sup_{q\in\mathcal{A}_n} \phi(q, q_a) = \inf_{q\in\mathcal{A}_a} \phi(q_n, q). \tag{6}$$

Note that, although it is well known that two player zero sum standard matrix games as defined in [5], always have a Nash equilibrium in the class of mixed strategies, the result does not extend to the game defined here. In fact, even if modeled as a continuous-kernel game as in [24], the existence of saddle point equilibrium when action spaces are compact does not directly apply here. The reason being, the payoff for a mixed strategy in such two player games is a weighted sum of pure strategy payoffs, in our setup, the payoff is a non-linear function of the pure strategy payoffs and the mixing probabilities (see (4)). The existence of a saddle point in this game is shown in the following theorem.

Theorem 1: 1. For the two player zero-sum game $\mathbb{G}_a$ defined by the action spaces $\mathcal{A}_n, \mathcal{A}_a$ and payoff function ϕ, there exists a unique saddle point equilibrium.

Proof: Refer to Appendix. □

The equilibrium condition guarantees that at the operating point, the adversary can use no other strategy to decrease the anonymity of the session. In addition to proving the existence of a saddle point, characterizing the optimal strategy for the adversary is also important, and particularly helpful in network scenarios where additional protection can be provided to nodes that are more likely to be monitored.

Note that the omniscient adversary setup is a specific instance of this game, when the adversary has exactly one action: monitor all nodes. The existence of an equilibrium is trivial and the operating point is given by the rate distortion optimization [4]:

$$\phi(\gamma) = H(\mathbf{S}) - \inf_{q_n(\hat{\mathbf{S}}|\mathbf{S}):\Upsilon(q_n)\leq\gamma} I(\mathbf{S}; \hat{\mathbf{S}}). \tag{7}$$

The uniqueness of the equilibrium follows from the zero-sum property of the game. Note that while the pair of strategies that achieves the saddle point anonymity is not unique, the saddle point anonymity in the two-player zero-sum game is indeed unique. This game is also an example of an incomplete information game [18] where the adversary does not have complete access to the session or the realization of the network designer's randomness, while the network designer does not have access to the realization of the adversary's randomness.

Although computing saddle point strategies is hard since the action spaces are continuous, properties of player strategies can be derived by studying the conditions.

C. Insights into Player Strategies

In this section, we investigate the properties of the saddle point player strategies using the conditions for equilibrium.

Partial Information For a given subset of nodes $\mathbf{b}$, we define the partial uncertainty from the adversary's perspective as:

$$H_p(\mathbf{b}) = \sum_{\mathbf{s},\hat{\mathbf{s}}} p(\mathbf{s}) q_n(\mathbf{b}_n|\mathbf{s}) \log q_{ap}(\mathbf{s}, f_a(f_o(\mathbf{s}, \mathbf{b}_n), \mathbf{n}_a), \mathbf{b}),$$

where q_{ap} is the a posteriori probability defined in (5). The partial uncertainty represents the uncertainty of the session when the adversary monitors a particular subset of nodes.

Information Leakage Rate For a given action by the network designer– making a set of relays $\mathbf{b}$ covert in a session $\mathbf{s}$— the rate of information leakage is defined as:

$$\mathcal{L}(\mathbf{s}, \mathbf{b}) \triangleq \frac{d\phi(q_n, q_a)}{dq_n(\mathbf{s}, \mathbf{b})} \tag{8}$$

Theorem 2: For the two player zero-sum game $\mathbb{G}_a$, at the saddle point (q_n^*, q_a^*),

1) $\forall \mathbf{b}_a^1, \mathbf{b}_a^2$ s.t. $q_a^*(\mathbf{b}_a^1), q_a^*(\mathbf{b}_a^2) > 0$,
$$H_p(\mathbf{b}_a^1) = H_p(\mathbf{b}_a^2).$$
2) $\forall \mathbf{s}$, if $\exists \mathbf{b}_1, \mathbf{b}_2$, s.t. $q_n^*(\mathbf{s}, \mathbf{b}_1), q_n^*(\mathbf{s}, \mathbf{b}_2) > 0$ and $\Lambda(\mathbf{s}, \mathbf{b}_1) = \Lambda(\mathbf{s}, \mathbf{b}_2)$, then
$$\mathcal{L}(\mathbf{s}, \mathbf{b}_1) = \mathcal{L}(\mathbf{s}, \mathbf{b}_2) \tag{9}$$
3) $\forall \mathbf{s}$, if $\exists \mathbf{b}_1, \mathbf{b}_2$, s.t. $q_n^*(\mathbf{s}, \mathbf{b}_1), q_n^*(\mathbf{s}, \mathbf{b}_2) > 0$ and $\Lambda(\mathbf{s}, \mathbf{b}_1) \neq \Lambda(\mathbf{s}, \mathbf{b}_2)$, then
$$\frac{\mathcal{L}(\mathbf{s}, \mathbf{b}_1) - \mathcal{L}(\mathbf{s}, \mathbf{b}_2)}{\Lambda(\mathbf{s}, \mathbf{b}_1) - \Lambda(\mathbf{s}, \mathbf{b}_2)} \text{ is a constant.} \tag{10}$$

Proof : Refer to Appendix.

The above theorem states that, at the saddle point, for every subset of nodes monitored by the adversary (with non-zero probability), the partial uncertainty of the underlying session is identical. In other words, the set of covert relays are chosen such that any monitored subset reveals equal information about the session. At this operating point, from the perspective of the adversary, any probability distribution over these "degenerate" subsets would give rise to the same anonymity. There, however, exists a unique distribution to choose nodes to monitor, which when employed, gives the network designer no incentive to deviate. At this point, the difference in information leakage rates for any pair of actions is proportional to the difference in throughput. In other words, the throughput cost per unit change in uncertainty is identical for every choice of covert relays (by the network designer).

Although the conditions in (9), (10) appear complicated to analyze owing to aposterior probabilities, in many networks it is possible to utilize network structure and session models to analyze the condition and characterize the optimal throughput-anonymity tradeoffs.

In the following section, we consider one such class of *parallel relay networks* to demonstrate the applicability of the game-theoretic approach. Specifically, we use the derived results on saddle point strategies to study the optimal behaviour of network nodes and the adversary, and in the process, demonstrate the performance improvement due to the game-theoretic approach over naive intuitive player strategies. We also use apply the formulation to characterize fundamental asymptotic relationships between anonymity, throughput and adversary capability in parallel relay networks. The asymptotic relationships are useful in the design of strategies in large networks where numerical computation becomes practically infeasible. In fact , we demonstrate that the maximum loss in using the asymptotic results on a $n-$ node parallel relay network is bounded by $\frac{\log n}{n}$.

IV. Parallel Relay Networks

A. Network Model

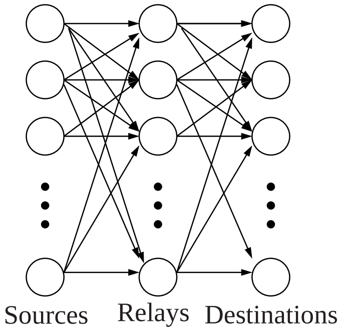


Fig. 4. Parallel Relay Network Model.

Consider a *parallel relay network* as shown in Figure 4, where the set of nodes $\mathcal{V}$ in the network can be divided into 3 subsets $\mathcal{V}^s, \mathcal{V}^r, \mathcal{V}^d$ such that $\mathcal{V}^s = \{A_1, \cdots, A_n\}$ is the set of source nodes, $\mathcal{V}^d = \{D_1, \cdots, D_n\}$ is the set of destination nodes, and $\mathcal{V}^r = \{R_1, \cdots, R_n\}$ is the set of intermediate relay nodes the network. The set of edges $\mathcal{E}$ can similarly be divided into 2 sets $\mathcal{E}_s, \mathcal{E}_r$, where $\mathcal{E}_s$ denotes the set of edges between source nodes and relays, $\mathcal{E}_r$ is the set of edges between relays and the destinations.

We make the following two assumptions in the model:
1. **Full connectivity** Every source is connected to every relay, and every relay is connected to every destination.
2. **Symmetry** The probability of a source-relay-destination connection is identical across sources, relays or destinations.

Note that these assumptions, while not critical to the analytical tractability helps to provide broader insights into optimal strategies for the network designer and the adversary.

Session Model In each session, every source in $\mathcal{V}^s$ picks a distinct destination in $\mathcal{V}^d$ and a distinct intermediate relay in $\mathcal{V}^r$ to forward its packets, such that all sources and relays are transmitting in every session. From a graph-theoretic perspective, each session corresponds to a unique pair of bipartite matchings from the sources to the relays and from the relays to the destinations.

Owing to the symmetry assumption, each session $\mathbf{s}$ has an identical prior probability:

$$p(\mathbf{s}) = \frac{1}{n!n!}.$$

Medium Access Constraints We consider a transmitter directed signaling model, where every node (source or relay) has an independent transmission rate constraint. Let C^s denote the transmission rate constraint for any source and let C^r denote the transmission rate constraint for any relay.

Transmission and Relaying strategy For purposes of analytical characterization, we consider independent Poisson schedules, where all source schedules and covert relay schedules are generated according to independent Poisson processes. The relaying strategy used by any covert relay is the Bounded Greedy Match algorithm [25], which was shown to maximize the sum-rate of relayed data packets.

Throughput Given the transmission rates of the relay and the source nodes, Theorem 1 in [4] characterizes the maximum achievable data rate when the BGM algorithm is used as the relaying strategy. Since all routes in the parallel relay network are $2-$hop routes, the sum-rate $\Lambda(\mathbf{s}, \mathbf{b}_n)$ in a session $\mathbf{s}$ when relays in $\mathbf{b}_n$ are covert is expressible as a sum of achievable rates for each source destination pair:

$$\Lambda(\mathbf{s}, \mathbf{b}) = (n - |\mathbf{b}|)\min(C^s, C^r) + |\mathbf{b}|\lambda^*(C^s, C^r),$$

$$\text{where } \lambda^*(a,b) = a\frac{be^{\Delta(b-a)} - b}{be^{\Delta(b-a)} - a}$$

is the maximum achievable rate for a covert relay using independent Poisson schedules under a strict delay constraint of Δ seconds per packet. [4].

The throughput, as defined in Section II, is given by:

$$\Upsilon(q_n) = \sum_{\mathbf{s}} p(\mathbf{s}) \sum_{\mathbf{b}_n} q_n(\mathbf{b}_n|\mathbf{s})\Lambda(\mathbf{s}, \mathbf{b}_n).$$

The maximum achievable throughput $\Upsilon_{\max}$ when all relays are visible is given by:

$$\Upsilon_{\max} = n\min(C^s, C^r).$$

Note that sum-rate here is used as a specific scalar measure of performance to define the strategy space of the network nodes. In general any function of capacity region can be used to define the strategy space of the network, and the results here can be extended to such models as well.

Adversary Model The adversary monitors a subset of the nodes, which we denote by a pair of random variables $\mathbf{N}_a^s, \mathbf{N}_a^r$, where $\mathbf{N}_a^s$ and $\mathbf{N}_a^r$ denote the sources and relays that are monitored respectively. For every monitored node, the adversary has perfect knowledge of the packet transmission times. We know that $|\mathbf{N}_a^s| + |\mathbf{N}_a^r| \leq k_a$.

Given the bipartite session model, at every monitored relay, the schedule observed by the adversary is either correlated to that of a monitored source node, or independent of every monitored source node. In effect, the adversary observation $f_a(f_o(\mathbf{s}, \mathbf{b}_n), \mathbf{n}_a) = \mathbf{p}_a^{s,r} \cup \mathbf{p}_a^s \cup \mathbf{p}_a^r$ where:
i. $\mathbf{p}_a^{s,r}$ is a set of source-relay pairs with dependent schedules;
ii. $\mathbf{p}_a^s$ is a set of source nodes whose schedules are not correlated with that of any monitored relay;
iii. $\mathbf{p}_a^r$ is a set of relays whose schedules are not correlated with that of any monitored source;

For example, consider a session in a 3 source parallel-relay network, where source A_i communicates with destination D_i through relay R_i. Let the network designer make relay R_1 covert and the adversary monitor the nodes A_1, A_2, R_1, R_2 and R_3. In this example, the adversary observation can be written as $\mathbf{p}_a^{s,r} \cup \mathbf{p}_a^s \cup \mathbf{p}_a^r$ where

$$\mathbf{p}_a^{s,r} = \{(A_2, R_2)\}, \mathbf{p}_a^s = \{A_1\}, \mathbf{p}_a^r = \{R_1, R_3\}.$$

Anonymity By merely monitoring the transmissions of the nodes in the network, an adversary can at most identify every source-relay pair. Since the network utilizes transmitter directed signaling, using transmission timing alone, it is impossible to determine any final destination. We, therefore, measure anonymity using the set of source-relay pairs perfectly identifiable by the adversary. Let $\mathbf{S}'$ denote the set of source-relay pairs in the session. We can write

$$H(\mathbf{S}|\hat{\mathbf{S}}_a) = H(\mathbf{S}'|\hat{\mathbf{S}}_a) + H(\mathbf{S}|\hat{\mathbf{S}}_a, \mathbf{S}').$$

Since $\mathbf{S}'$ contains all the source relay pairings and $\hat{\mathbf{S}}_a$ contains no information about destinations $H(\mathbf{S}|\mathbf{S}', \hat{\mathbf{S}}_a) = H(\mathbf{S}|\mathbf{S}')$, which is a constant irrespective of the set of monitored nodes. We therefore modify the payoff in the two player game as:

$$\phi = \frac{H(\mathbf{S}')|\hat{\mathbf{S}}_a)}{H(\mathbf{S}')}.$$

It is easy to see that the total anonymity as defined in Section II has a monotonic one-one relationship to the above definition.

Our goal is study the saddle point strategies and throughput-anonymity tradeoffs of this network model by jointly optimizing the covert probability function $\{q_n(\mathbf{b}_n|\mathbf{s})\}$ and the adversary strategy $q_a(\mathbf{n}_a)$ subject to the throughput constraint $\Upsilon(q_n) \geq \gamma$ and the adversary power k_a. If q_n^*, q_a^* denote the NE probability distributions of the network designer and adversary respectively, then let

$$A^*(\gamma) = \phi(q_n^*, q_a^*)$$

represent the NE anonymity-throughput tradeoff.

Theorem 3: For an omniscient adversary, the NE throughput anonymity tradeoff is given by:

$$A^*(\gamma) = \frac{(\Upsilon_{\max} - \gamma)}{n\epsilon},$$
$$\text{where } \epsilon = \min(C^s, C^r) - \lambda^*(C^s, C^r).$$

Proof: Refer to Appendix □

The throughput-anonymity tradeoff under an omniscient adversary is linear, which is a consequence of the $2-$hop nature and symmetry in the network model. The constant ϵ represents the per node rate loss. As mentioned earlier, this operating point represents a trivial equilibrium. Against an omniscient adversary, the optimal strategy for the network designer is to make all relays covert together with probability

$$q_n(\mathcal{V}|\mathbf{s}) = \frac{\Upsilon_{\max} - \gamma}{n\epsilon}, \forall \mathbf{s}.$$

The general idea behind this strategy is as follows: If in a session, k relays are covert, then the anonymity from an omniscient adversary's perspective would be restricted to the k relays and cannot exceed $\log k!$. The corresponding loss in throughput for the network designer is $k\epsilon$. The optimal network design strategy would therefore correspond to minimizing the throughput cost per unit gain in anonymity.

B. General Adversary Model

Consider the simplest case of $k_a = 2$. When $k_a = 2$, the only way the adversary can obtain non-zero information is if one of the monitored nodes is a relay and the other is a source. Due to the symmetry assumption, intuition suggests that the optimal strategy for the adversary would be to monitor every source-relay pair with equal probability.

When $k_a > 2$, there is an additional challenge in determining the ratio of relays and sources that should be monitored by the adversary. In general, the optimal ratio need not be fixed and could be a random quantity, as long as the total number of monitored nodes does not exceed k_a. However, optimizing the adversary and network strategies reveals that the optimal strategy would in fact have a fixed ratio. This is shown in the following theorem which characterizes the equilibrium throughput-anonymity tradeoff for the general adversary.

Theorem 4: Let $p_c = \frac{\Upsilon_{\max} - \gamma}{n\epsilon}$, $k = \lfloor \frac{k_a}{2} \rfloor$, $k' = \lceil \frac{k_a}{2} \rceil$ and

$$w(m) = \begin{cases} \frac{((n-k)!)^2}{(n-2k+m)!} & k_a \leq n \\ 0 & \text{o.w} \end{cases}.$$

Then, there exists a unique equilibrium throughput-anonymity tradeoff which is given by:

$$\begin{aligned} A^*(\gamma) &= \left[p_c + \frac{w(0)(1-p_c)}{n!}\right] \log\left(w(0)(1-p_c) + n! p_c\right)\right) \\ &+ \frac{(n! - w(0))}{n!} p_c \log p_c \\ &+ \sum_{(k_a-n-1)^+ + 1}^{k} \binom{k}{m} \binom{k'}{m} \frac{m!}{n!} (1-p_c) w(m) \log(w(m)). \end{aligned}$$

Proof: Refer to Appendix □

The anonymity at the saddle point is composed of two components. The first term represents the uncertainty in determining which of the monitored relays are covert; since only a subset of sources are monitored, independence across schedules does not necessarily imply that the relay is covert. The remaining component of the anonymity is the uncertainty due to the unobserved nodes in the network. The quantity p_c represents the average probability with each a relay is covert, and this probability is influenced by the level of throughput required. The relationship is similar to the omniscient adversary case. As the network size increases, the first component converges to a constant, and the anonymity is dominated by the missing information from unobserved nodes (see Section V).

Saddle Point Strategies The optimal strategy for the adversary at the saddle point, as revealed in the proof, is to monitor equal number of relays and sources such that each $\frac{k_a}{2}$ size subsets of relays and sources are chosen uniformly randomly. When k_a is odd, the adversary monitors one additional relay. The intuitive argument for this strategy is as follows: If the number of sources monitored exceeded the number of monitored relays by 2 or more, then by removing one monitored source and adding a monitored relay, the number of possible routes that can be discovered only stands to increase.

The optimal strategy for the network designer is to make all the relays to be covert with probability:

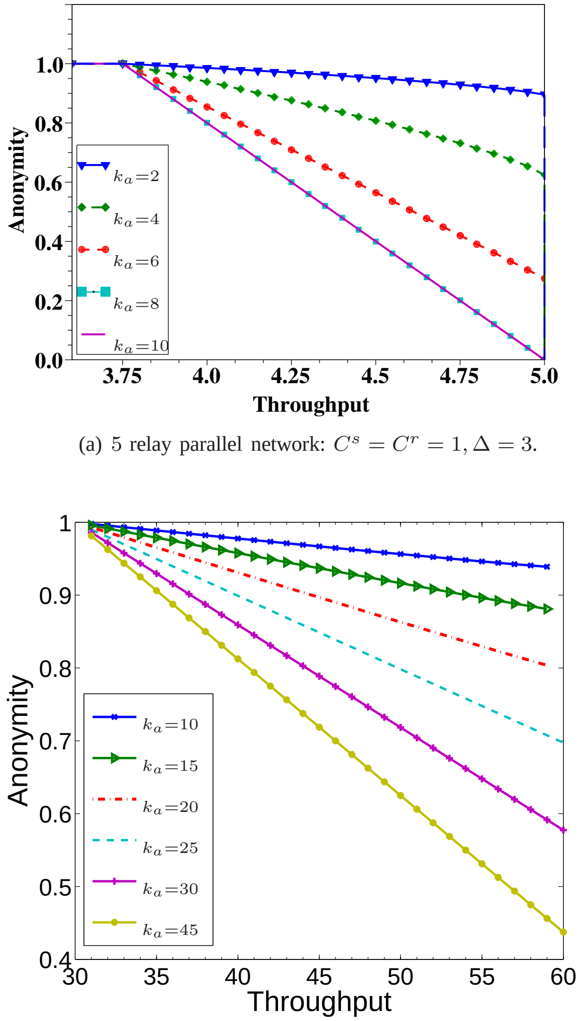
$$q_n(\mathcal{V}|\mathbf{s}) = \frac{\Upsilon_{\max} - \gamma}{n\epsilon}, \forall \mathbf{s}.$$

At first glance, this may be surprising since the adversary only monitors a subset of nodes in any session. However, if all relays were not covert, then the fraction of monitored relays that are visible provide more information per unit cost in throughput than that obtained from sessions when none of the relays are covert. Furthermore, uniform probabilities $q_n(\mathbf{b}_n|\mathbf{s})$ across sessions result in a uniform aposterior probability over all sessions which maximizes entropy.

Figure 5 plots the throughput anonymity tradeoff for two parallel relay networks. The gain in anonymity due to the game-theoretic approach over the omniscient strategy is evident from the plots. Note that in the small network, while the tradeoff is linear for an omniscient adversary (Theorem 2), it is not so in general. For a large network, however, the tradeoffs are mostly linear, except for small values of k_a. This "asymptotic" linearity is shown analytically in Section V.

C. Asymmetric Networks

In the results thus far, the symmetry in the underlying network model resulted in symmetric strategies for the adversary and the network designer. When asymmetry is introduced in the networks, naive intuitions may not provide the saddle point strategies. To understand the effect of asymmetry on the strategies, we consider two kinds of asymmetric networks: networks where the transmission capacities of the relays are unequal, and networks where the number of sources catered by the relays are unequal.



(a) 5 relay parallel network: $C^s = C^r = 1, \Delta = 3$.

(b) 60 relay parallel network: $C^s = C^r = 1, \Delta = 1$.

Fig. 5. Tradeoffs for Parallel Relay Networks

Asymmetry in Covert Relay Rates: Consider first the case of an n parallel-relay network, where the transmission capacities of relays $B_1, \cdots, B_n$ are unequal. Specifically, there exists at least two relays B_i, B_j such that the loss in data rates $\epsilon_i \neq \epsilon_j$.

Theorem 5: For an n relay parallel network, where an adversary monitors $k_a = 2$ nodes, if rate losses due to covert relaying for the relays are given by $\epsilon_1, \cdots, \epsilon_n$ respectively, there exists a unique saddle point where

1. $q_n(B_i|\mathbf{s}) = \frac{\Upsilon_{\max} - \gamma}{\sum_i \epsilon_i} \forall i \leq n$
2. $q_a(A_i, B_j) = \frac{\epsilon_j}{n \sum_i \epsilon_i}$.

Proof: Refer to Appendix □

Interestingly, although the model is asymmetric, the covert relaying strategy is symmetric. This is because each relay, when visible, reveals equal amount of information. Therefore, any asymmetry in the retrievable information from the two relays induced by the network strategy would automatically force the adversary to monitor the less protected (or more informative) relay exclusively. Such a pair of strategies cannot constitute a saddle point.

When the network design strategy is symmetric, the payoff is a constant regardless of the adversary's probability of monitoring each source-relay pair. However, there is only one strategy, at which point the optimal strategy for the network is symmetric, thus resulting in an equilibrium. In particular, the probability of monitoring a relay is proportional to the rate loss at the relay. As intuition would suggest, the more rate loss, the less likely a relay is to be covert and consequently, a greater incentive for it to be monitored. In effect, at the saddle point, the adversary's strategy is to choose the probabilities of monitor each relay so that the network is forced to make all relays covert with equal likelihood.

Under such an asymmetric model, if a network designer were to assume naively that the adversary's strategy were symmetric, then for a required level of throughput, the optimal strategy would be to make relays with lower throughput loss ϵ_i covert with higher probability so that the same level of throughput can be achieved with higher anonymity (w.r.t. the uniform adversary). However, the optimal adversary would then employ unequal probabilities of monitoring the relays which would eventually result in lower than expected anonymity. The difference between the anonymity due to the naive networking strategy and the equilibrium strategy is shown in Figure 6 and clearly demonstrates the benefit of using the game theoretic approach. The figure also plots the tradeoff when the adversary employs the naive strategy of uniform monitoring, and the network designer optimizes the choice of covert relays assuming the uniform adversary.

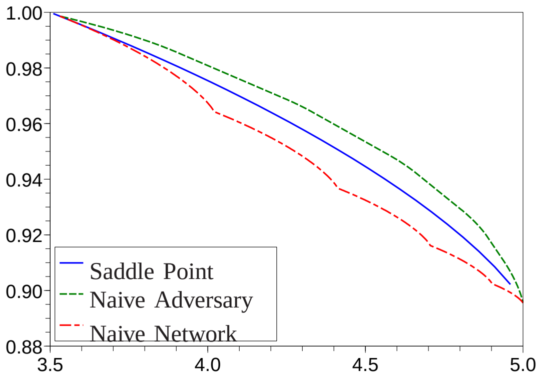


Fig. 6. Asymmetric Rate Loss Model with $n = 5$ relays: Comparison with naive strategies.

Asymmetry in Relay Information In the asymmetric model discussed above, the saddle point strategy for the network designer was symmetric since each relay when monitored provided the same amount of information. We now consider a modification of the parallel network structure and introduce asymmetry in the amount of information provided by a relay. Specifically, let the number of relays be $n-k$, where k relays are multiplexing relays with 2 sources transmitting to each of them every session, and the remaining $n-2k$ relays are non-multiplexing relays with exactly 1 source transmitting to each of them in every session. The capacities of relays are chosen such that each relay, when covert incurs an identical throughput loss ϵ. We consider a $2-$player game where the adversary monitors at most 2 nodes.

Theorem 6: For an $n-1$ relay asymmetric parallel relay network, where an adversary monitors $k_a = 2$ nodes, then there exists a unique saddle point, where

1) The optimal strategy of the network is to make a non-multiplexing relay covert with probability q_r^1 and a multiplexing relay covert with probability q_r^2 where

$$\begin{aligned} & q_r^1 \log(q_r^1) - (q_r^1 + n - 1)\log(q_r^1 + n - 1) \\ = \;& 2q_r^2 \log(2q_r^2) - (2q_r^2 + n - 2)\log(2q_r^1 + n - 2) - 2. \end{aligned}$$

2) The optimal adversary strategy is to monitor a source-multiplexing relay pair with probability p_1 and a source non-multiplexing relay pair with probability p_2 such that:

$$\frac{p_1}{p_2} = \frac{(n-2k)\log\left(\frac{q_r^1}{q_r^1+n-1}\right)}{(k)\log\left(\frac{2q_r^2}{2q_r^2+n-2}\right)}.$$

Proof: Refer to Appendix. □.

In this setup, the theorem states that the optimal strategy for the network designer is asymmetric as well. A naive adversary would choose to monitor non-multiplexing relays with higher probability since they provides more information, whereas a naive network designer would choose to hide all relays with equal probability since all relays provide identical throughput loss. Figure 7 plots the improvement in anonymity over naive strategies due to the game-theoretic approach.

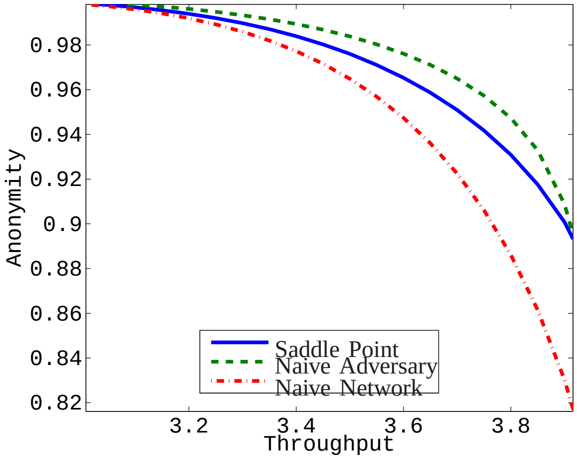


Fig. 7. Asymmetric Relay Information Model with 4 sources and 3 relays: Comparison with naive strategies.

The intuition behind the optimal strategies is similar to the asymmetric rate loss model. The more information provided by a relay, the more likely the adversary is to monitor that relay, and a greater incentive to make it covert. At the saddle point, the network increases the probability of non-multiplexing relays being covert just enough so that the adversary obtains equal information from any relay.

D. Large Networks

In this section, we use the derived results to study equilibria in large networks. When the fraction of monitored nodes $\frac{k_a}{2n}$ is a constant, the anonymity monotonically increases with n but asymptotically converges towards a constant.

Theorem 7: If $\frac{k_a}{2n} = \alpha$ is a constant, then the anonymity for a fixed throughput ratio $\gamma^* = \frac{\gamma}{\Upsilon_{\max}}$ converges as:

$$\lim_{n\to\infty} A(\gamma^*) = 1 - \alpha^2 \frac{(\gamma^* - (1-\epsilon))^+}{\epsilon}.$$

Proof: Refer to Appendix □

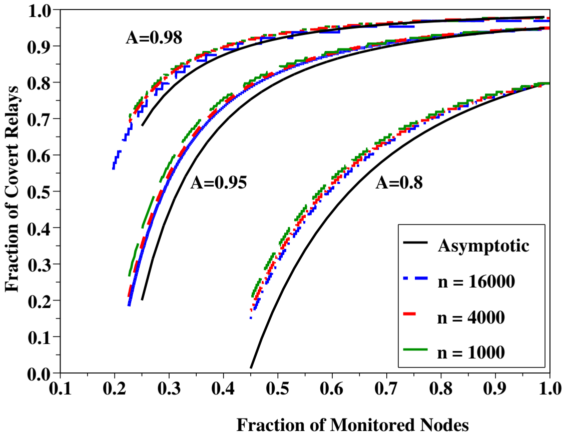


Fig. 8. Covert vs. Monitored Relays: The three sets of curves are plotted for $A = 0.8, 0.95, 0.98$.

According to the theorem, for a fixed throughput, the loss in anonymity is proportional to the square of the fraction of monitored relays. Put in another perspective, for a fixed number of monitored relays, the anonymity asymptotically converges to 1 as :

$$A = 1 - O\left(\frac{1}{n^2}\right).$$

The intuition for this relationship can be understood by looking at the maximum throughput case: $\gamma^* = 1$. At that operating point, $A(\gamma^*) = 1 - \alpha^2$. In the large n regime, the total uncertainty is approximately $n \log n$. Every monitored relay reduces uncertainty by $\log n$ if the corresponding source is also monitored. If the corresponding source is not among the monitored nodes, then the reduction in uncertainty is negligible. For every relay, the corresponding source would be monitored with approximate probability $\frac{k}{n}$. Since k relays are monitored, the net reduction in uncertainty is approximately $\frac{k^2}{n^2}$, thus resulting in the square law of the theorem.

Asymptotic relationships can be used to design approximate strategies for large networks. In particular, it would be useful to characterize the asymptotic relationship between the fraction of covertly relays and the fraction of monitored relays. As the number of monitored relays increases, the fraction of relays that are covert per session would also increase. We can use Theorem 4 to obtain the asymptotic relationship. Specifically, for a fixed anonymity A, the fraction of covert relays per session β is given by

$$\beta = 1 - \frac{1-A}{\alpha^2}.$$

Furthermore, if $\beta(n)$ is the exact fraction of covert relays required for a network of size n, it is easily shown that:

$$\beta(n) - \beta = O\left(\frac{\log n}{n}\right).$$

This is of particular relevance to large wireless sensor networks where the number of covert relays (relays generating dummy transmissions) is directly related to energy overhead. Figure 8 plots this relationship for finite networks in comparison with the asymptotic relationship.

V. Concluding Remarks

In this work, we considered the problem of providing anonymity to network communication when adversaries monitor or compromise an unknown subset of nodes in the network. We presented a game-theoretic formulation and proved the existence of saddle point equilibria. Using the class of parallel relay networks, we demonstrated that this approach can be used to obtain optimal strategies for the network designer and the adversary, as well as provide insights into anonymity-throughput tradeoffs in large networks. The problem of computing the equilibria has not been dealt with in this work, but efficient algorithms for this purpose would fortify the results here, and is part of ongoing research. In this work, we have used specific classes of networks, and assumed knowledge of topology and sessions. A similar approach for random networks with random connections could shed valuable insights into scaling behaviour of anonymous networking.

References

[1] N. Matthewson and R. Dingledine, “Practical traffic analysis: Extending and resisting statistical disclosure,” in *Privacy Enhancing Technologies: 4th International Workshop*, May 2004.

[2] T. He and L. Tong, “Detecting Information Flows: Improving Chaff Tolerance by Joint Detection,” in *Proc. 2007 Conference on Information Sciences and Systems*, (Baltimore, MD), March 2007.

[3] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, 1949.

[4] P. Venkitasubramaniam, T. He, and L. Tong, “Anonymous networking amidst eavesdroppers,” *IEEE Transactions on Information Theory*, vol. 54, pp. 2770–2784, June 2008.

[5] H. S. Kuhn, *Classics in Game Theory*. Princeton, NJ: Princeton University Press, 1944.

[6] D. Chaum, “Untraceable electronic mail, return addresses and digital pseudonyms,” *Communications of the ACM*, vol. 24, pp. 84–88, February 1981.

[7] Y. Zhu, X. Fu, B. Graham, R.Bettati, and W. Zhao, “On flow correlation attacks and countermeasures in mix networks,” in *Proceedings of Privacy Enhancing Technologies workshop*, May 26-28 2004.

[8] B.Radosavljevic and B. Hajek, “Hiding traffic flow in communication networks,” in *Military Communications Conference*, 1992.

[9] R. E. Newman, I. S. Moskowitz, P. Syverson, and A. Serjantov, “Metrics for traffic analysis prevention,” in *Proceedings of Privacy Enhancing Technologies Workshop (PET 2003)*, Springer-Verlag, LNCS 2760, April 2003.

[10] P. Venkitasubramaniam and L. Tong, “ Throughput Anonymity Tradeoff in Wireless Networks under Latency Constraints,” in *Proceedings of 2008 IEEE INFOCOM*, (Phoenix, AZ), pp. 241–245, April 2008.

[11] J. F. Nash, “Equilibrium Points in $n-$Person Games,” *Proceedings of the National Academy of Sciences*, vol. 36, pp. 48–49, January 1950.

[12] T. Basar, “The Gaussian Test Channel with an Intelligent Jammer,” *IEEE Transactions on Information Theory*, vol. 29, Jan. 1983.

[13] J. M. Borden, D. M. Mason, and R. J. McEliece, “Some Information Theoretic Saddle Points,” *SIAM Journal of Control and Optimization*, vol. 23, pp. 129–143, Jan. 1985.

[14] M. M’edard, “Capacity of Correlated Jamming Channels,” in *35th Annual Allerton Conf. on Commun., Control and Comp.*, (Monticello, IL), Sep. 1997.

[15] A. Kashyap, T. Basar, and R. Srikant, “Correlated Jamming on MIMO Wireless Fading Channels,” *IEEE Transactions on Information Theory*, vol. 50, pp. 2119–2123, Sept. 2004.

[16] A. Kashyap, T. Basar, and R. Srikant, “Mutual Information Games in Multiuser Channels With Correlated Jamming,” *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4598–4607, 2009.

[17] T. Alpcan and T. Basar, “A Game-Theoretic Analysis of Intrusion Detection in Access Control Systems,” in *Proc. of 2004 IEEE Conference on Decision and Control.*, (Paradise Island, Bahamas), Dec. 2004.

[18] Y. Liu, C. Comaniciu, and H. Man, “Modeling misbehaviour in adhoc networks: A game-theoretic approach to intrusion detection,” *International Journal of Security and Networks*, vol. 1, no. 3-4, pp. 243–254, 2006.

[19] K. Lye and J. M. Wing, ““Game Strategies in Network Security”,” *International Journal of Information Security*, vol. 4, pp. 71–86, Feb. 2005.

[20] S. Sarkar, E. Altman, R. El-Azouzi, and Y. Hayel, “Information Concealing Games in Comunication Networks,” in *Proc. IEEE INFOCOM*, (Phoenix, AZ), pp. 2119–2127, April 2008.

[21] F. Topsoe, “Entropy and Equilibrium via Games fo Complexity,” *Physica A: Statistical Mechanics and its Applications*, vol. 340, pp. 11–31, September 2004.

[22] T. Cover and J. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[23] T. He and L. Tong, “Detecting Information Flows: Fundamental Limits and Optimal Algorithms.” submitted to IEEE Trans. on Information Theory, 2007.

[24] G. Owen, *Game Theory*. Academic Press Inc., 1995.

[25] A. Blum, D. Song, and S. Venkataraman, “Detection of Interactive Stepping Stones: Algorithms and Confidence Bounds,” in *Conference of Recent Advance in Intrusion Detection (RAID)*, (Sophia Antipolis, French Riviera, France), September 2004.

[26] J. B. Rosen, “Existence and Uniqueness of Equilibrium Points for Concave $N-$Person Games,” *Econometerica*, vol. 33, pp. 520–534, July 1965.

Appendix

A. Proof of Theorem 1

In order to prove the existence of a saddle point in the two player game, it is sufficient to show the following:

1) $\mathcal{A}_n$ and $\mathcal{A}_a$ are closed convex and bounded sets.
2) The payoff is continuous in the domain $\mathcal{A}_n \times \mathcal{A}_a$.
3) For every $q_a \in \mathcal{A}_a$, $\phi(x, q_a)$ is concave in x.
4) For every $q_n \in \mathcal{A}_n$, $-\phi(q_n, y)$ is concave in y.

If the $2-$player game satisfies the above conditions, then it constitutes a general $2-$player concave game, which was shown to have a guaranteed Nash equilibrium in [26].

1) **Convexity of action spaces:** The space $\mathcal{A}_a$ is a finite-dimensional simplex, which is closed, bounded and convex. $\mathcal{A}_n$ is a subset of the simplex with the additional constraint:

$$R(\boldsymbol{q}_a) \geq r.$$

Since the constraint is not a strict inequality, the space is closed. $R(\cdot)$ is a linear function of $\boldsymbol{q}_a$. Therefore, for any pair of probability vectors $\boldsymbol{q}_a^1, \boldsymbol{q}_a^2$

$$\alpha R(\boldsymbol{q}_a^1) + (1-\alpha) R(\boldsymbol{q}_a^2) = R(\alpha \boldsymbol{q}_a^1 + (1-\alpha)\boldsymbol{q}_a^2),$$

which proves the convexity of $\mathcal{A}_n$.

2) Since the payoff is linear in $\boldsymbol{q}_a$ and is an entropy function of $\boldsymbol{q}_n$, the continuity of the payoff can be easily shown (the details are omitted here).

3) In order to show the concavity of ϕ w.r.t. to $\boldsymbol{q}_n$, we need to show that for any $\boldsymbol{q}_n^1, \boldsymbol{q}_n^2 \in \mathcal{A}_n$,$\boldsymbol{q}_a \in \mathcal{A}_a$,

$$\alpha\phi(\boldsymbol{q}_n^1, \boldsymbol{q}_a) + (1-\alpha)\phi(\boldsymbol{q}_n^2, \boldsymbol{q}_a) \leq \phi(\alpha\boldsymbol{q}_n^1 + (1-\alpha)\boldsymbol{q}_n^2, \boldsymbol{q}_a).$$

Consider the following modification to the setup, where apart from the topology and set of network sessions, the network designer and the adversary are given access to a common Bernoulli random variable $Z \sim \mathcal{B}(\alpha)$. Consider any $\boldsymbol{q}_n^1, \boldsymbol{q}_n^2 \in \mathcal{A}_n$. The network designer utilizes the following strategy: If the observed variable $Z = 1$, then the distribution $\boldsymbol{q}_n^1$ is used to make relays covert, and if $Z = 0$, $\boldsymbol{q}_n^2$ is used. Since Z is observed by the adversary as well, this strategy would amount the anonymity being equal to the conditional entropy $H(\mathbf{S}|\hat{\mathbf{S}}, Z)$.

Now, suppose the Bernoulli variable were only available to the network designer, and he utilizes the same strategy. Since the adversary has no knowledge of Z, his entropy would be $H(\mathbf{S}|\hat{\mathbf{S}})$ where the distribution of covert relays would be the effective distribution:

$$\alpha\boldsymbol{q}_n^1 + (1-\alpha)\boldsymbol{q}_n^2$$

. Since conditioning reduces entropy, $H(\mathbf{S}|\hat{\mathbf{S}}, Z) \leq H(\mathbf{S}|\hat{\mathbf{S}}$, and therefore,

$$\alpha\phi(\boldsymbol{q}_n^1, \boldsymbol{q}_a) + (1-\alpha)\phi(\boldsymbol{q}_n^2, \boldsymbol{q}_a) \leq \phi(\alpha\boldsymbol{q}_n^1 + (1-\alpha)\boldsymbol{q}_n^2, \boldsymbol{q}_a).$$

4) For any $\boldsymbol{q}_n$, $\phi(\boldsymbol{q}_n, \boldsymbol{q}_a)$ is a linear function of $\boldsymbol{q}_a$, and therefore,

$$\alpha\phi(\boldsymbol{q}_n, \boldsymbol{q}_a^1) + (1-\alpha)\phi(\boldsymbol{q}_n, \boldsymbol{q}_a^2) = \phi(\boldsymbol{q}_n, \alpha\boldsymbol{q}_a^1 + (1-\alpha)\boldsymbol{q}_a^2),$$

which establishes the required concavity.

For uniqueness, consider two pairs of strategies $(\boldsymbol{q}_n^1, \boldsymbol{q}_a^1)$ and $(\boldsymbol{q}_n^2, \boldsymbol{q}_a^2)$ which achieve saddle point equilibrium. By the definition of saddle point, we know that:

$$\phi(\boldsymbol{q}_n^1, \boldsymbol{q}_a^1) \leq \phi(\boldsymbol{q}_n^1, \boldsymbol{q}_a^2) \leq \phi(\boldsymbol{q}_n^2, \boldsymbol{q}_a^2) \leq \phi(\boldsymbol{q}_n^2, \boldsymbol{q}_a^1) \leq \phi(\boldsymbol{q}_n^1, \boldsymbol{q}_a^1).$$

The above sequence of inequalities establishes the uniqueness of the payoff. □

B. Proof of Theorem 2

According to the definition of payoff:

$$\begin{aligned}\phi(q_n, q_a) &= \frac{H(\mathbf{S}|\hat{\mathbf{S}}_a)}{H(\mathbf{S})} = \frac{1}{H(\mathbf{S})}\sum_{\mathbf{n}_a}\sum_{\mathbf{s},\mathbf{b}_n} -q_a(\mathbf{n}_a)p(\mathbf{s}) \times \\ & q_n(\mathbf{s}, \mathbf{b}_n)\log q_{ap}(\mathbf{s}, f_a(f_o(\mathbf{s}, \mathbf{b}_n), \mathbf{n}_a), \mathbf{b}_a) \end{aligned} \tag{11}$$

From the adversary’s perspective, the goal is to choose q_a such that $\phi(q_n, q_a)$ is minimized. Since q_a is a probability distribution, using Lagrange multipliers, we can write:

$$L_a = \phi(q_n, q_a) + \beta_a \sum_{\mathbf{n}_a} q_a(\mathbf{n}_a).$$

At the minimizing distribution, we know that

$$\frac{dL_a}{dq_a(\mathbf{n}_a)} = 0 \forall \mathbf{n}_a.$$

Therefore, for any subset of nodes $\mathbf{n}_a$ for which $q_a(\mathbf{n}_a) > 0$

$$H_p(\mathbf{n}_a^1) + \beta_a \text{ is a constant,}$$

which proves the first part of the theorem.

From the network designer's perspective, the goal is to design $q_n(\mathbf{b}_n)$ such that $\phi(q_n, q_a)$ is maximized, while maintaining a throughput γ. Again, using Lagrange multipliers, we can define:

$$L_n = \phi(q_n, q_a) + \beta_1 \sum_{\mathbf{s},\mathbf{b}} p(\mathbf{s}) q_n(\mathbf{s},\mathbf{b}) \Lambda(\mathbf{s},\mathbf{b}) + \sum_{\mathbf{s}} p(\mathbf{s}) \sum_{\mathbf{b}} \beta_2(\mathbf{s}) q_n(\mathbf{s},\mathbf{b}).$$

At the maximizing distribution, for every $q(\mathbf{s},\mathbf{b}) > 0$,

$$\begin{aligned} \frac{dL_n}{dq_n(\mathbf{b}_n)} &= 0. \\ \Rightarrow \sum_{\mathbf{n}_a} q_a(\mathbf{n}_a) \Big[p(\mathbf{s}) + p(\mathbf{s}) \log(q_n(\mathbf{s},\mathbf{b}_n)) - p(\mathbf{s}) & \\ -p(\mathbf{s}) \log \left[\sum_{\mathbf{s}',\mathbf{b}'_n} q_n(\mathbf{s}',\mathbf{b}'_n) p(\mathbf{s}') \right] \Big] & \\ +\beta_1(\Lambda(\mathbf{s},\mathbf{b}_n)) + \beta_2(\mathbf{s}) &= 0. \end{aligned}$$

Equating the values of β_1, $\beta_2(\mathbf{b})$, the conditions are obtained. □

C. Proof of Theorem 3

Define $p_k = \sum_{\mathbf{s},\mathbf{b}:|\mathbf{b}|=k} p(\mathbf{s}) q_n(\mathbf{b}|\mathbf{s})$. Due to the symmetric rates, the throughput achievable by a strategy q_n is:

$$\Upsilon(q_n) = \Upsilon_{\max} - \sum_k p_k k \epsilon,$$

where $\epsilon = \min(C^r, C^s) - f(C^r, C^s)$.

For a given strategy q_n, the anonymity for an omniscient adversary can be written as:

$$H(\mathbf{S}|\mathbf{B}) = \sum_{\mathbf{b} \subset calV^r} \left(\sum_{\mathbf{s}} p(\mathbf{s}) q_n(\mathbf{b}|\mathbf{s}) \right) H(\mathbf{S}|\mathbf{B} = \mathbf{b}).$$

For a given realization of $\mathbf{B}$, the omniscient adversary can perfectly correlate the flows through all relays in $\mathcal{V}^r \backslash \mathbf{B}$, therefore, the information lost due to independent schedules can be upper bounded by:

$$H(\mathbf{S}|\mathbf{B} = \mathbf{b}) \leq \log(|\mathbf{b}|!).$$

$$\begin{aligned} \Rightarrow H(\mathbf{S}|\mathbf{B}) &\leq \sum_{\mathbf{b}} \left(\sum_{\mathbf{s}} p(\mathbf{s}) q_n(\mathbf{b}|\mathbf{s}) \right) \log(|\mathbf{b}|!) \\ &= \sum_k p_k \log(k!) \end{aligned}$$

Consider maximizing $\sum_k p_k \log(k!)$ subject to

$$\sum_k p_k k \epsilon \leq \Upsilon_{\max} - \gamma.$$

If $\Upsilon_{\max} - \gamma \geq n\epsilon$, it is easy to see that $q_n = 1$. When $\Upsilon_{\max} - \gamma \geq n\epsilon$, since $\frac{\log(k!)}{k}$ is increasing in k, the maximizing $\{p_k\}$ is given by:

$$p_k = 0, k < n, \; p_n = \frac{\Upsilon_{\max} - \gamma}{n\epsilon}.$$

Therefore, for any throughput t,

$$H(\mathbf{S}|\mathbf{B}) \leq \frac{\Upsilon_{\max} - \gamma}{n\epsilon} \log(n!).$$

The above inequality is achievable by making all relays covert with probability p_n, and hence proves the theorem.

D. Proof of Theorem 4

Consider the following adversary strategy: During every session, the adversary picks $\frac{k_a}{2}$ source-relay pairs with uniform probability. We characterize the optimal network strategy for this adversary, and show that the adversary can do no better by changing his strategy, thus priving equilibrium.

For a given set of monitored nodes $\mathbf{B} \in (\mathcal{V}^s)^k \times (\mathcal{V}^r)^k$, let $X_{\mathbf{B}}$ be a random variable that denotes the set of communicating source relay pairs within the set of monitored nodes. Then, for a given covert relaying strategy $q_n()$, the anonymity for the specified adversary can be expressed as:

$$\begin{aligned} H(\mathbf{S}|\hat{\mathbf{S}}_a) &= \sum_{\mathbf{b}} (H(X_{\mathbf{b}}|\hat{\mathbf{S}}_a) + H(\mathbf{S}|\hat{\mathbf{S}}_a, X_{\mathbf{B_2}}) \\ &= \sum_{\mathbf{b}} (H(X_{\mathbf{b}}|\hat{\mathbf{S}}_a) + H(\mathbf{S}|X_{\mathbf{b}}), \end{aligned}$$

where the second equality is because, given the communications within the monitored nodes, the uncertainty of the rest of the network does not depend on the observation.

Furthermore, given the set of communicating pairs within the set of monitored nodes, the uncertainty in the unobserved portion of the network would be independent of any strategy, and therefore a constant.

Accordingly, consider maximizing $\sum H(X_{\mathbf{B}}|\hat{\mathbf{S}}_a)$ subject to the throughput constraint. This maximization is akin to the omniscient case; the uncertainty refers to the communications within the monitored nodes. The difference comes from the fact that since there are unobserved nodes in the network, some of the monitored sources or relays can communicate with nodes outside the set of monitored nodes. Nevertheless, it can be shown that the optimal network strategy is not affected by this modification. We prove this for $k_a = 2$, the proof for general k_a is a straightforward generalization. Define

$$p^c(\mathbf{b}) = \sum_{\mathbf{S}} p(\mathbf{S})(1 - \sum_{\mathbf{B}:\mathbf{b} \cap \mathbf{B} \neq \phi} q(\mathbf{B}|\mathbf{S}).$$

In other words $p^c(\mathbf{b})$ is the probability that a flow through $\mathbf{b}$ is visible. Therefore,

$$H(X_{\mathbf{b}}|\hat{\mathbf{S}}_a) = h(p^c(\mathbf{b})),$$

where $h(p)$ is the binary entropy function. Due to the throughput requirement, we know that $\sum_{\mathbf{b}} p^c(\mathbf{b})$ is a constant. Since finite entropy is bounded by the size of the alphabet,

$$\sum_{\mathbf{b} \in \mathcal{V}^s \times \mathcal{V}^r} H(X_{\mathbf{b}}|\hat{\mathbf{S}}_a) \leq n^2 h(\frac{1}{n}),$$

where the equality is achieved when $\forall \mathbf{b}, p^c(\mathbf{b})$ is identical.

Furthermore, since $q(\mathbf{B}|\mathbf{S})$ is independent of $\mathbf{S}$,

$$H(\mathbf{S}|X_{\mathbf{B}}) = \log((n-1)!).$$

which is independent of the covert relaying strategy.

The optimal covert relaying strategy is therefore symmetric across all relays and sessions. Using the two derived conditions, the maximizing anonymity is given by:

$$H(\mathbf{S}|\hat{\mathbf{S}}_a) = h(\frac{1}{n}) + \log((n-1)!)$$

For the derived covert relaying strategy, the anonymity w.r.t to a general adversary can be written as:

$$H(\mathbf{S}|\hat{\mathbf{S}}_a) = \sum_{\mathbf{b}\in\mathcal{V}^s\times\mathcal{V}^r} q_a(\mathbf{b})(H(X_{\mathbf{b}}|\hat{\mathbf{S}}_a) + H(\mathbf{S}|X_{\mathbf{b}_2})$$

where $q_a(\mathbf{b}_2)$ is the probability that the adversary monitors the source-relay pair $\mathbf{b}$. Due to the symmetry in covert relaying strategy, $H(X_{\mathbf{b}})$ and $H(\mathbf{S}|X_{\mathbf{b}})$ are identical across pairs $\mathbf{b}$. Therefore, for any probability mass function $\{q_a(\cdot)\}$, the total information gained (or lost) would be no different for the adversary. In other words, there is no incentive for the adversary to deviate from the uniform monitoring strategy, and that pair of strategies is therefore, a saddle point. □.

E. Proof of Theorem 5

Since uniform probability maximizes entropy, we can write

$$q_n(B_1|\mathbf{s}_1) = q_1\forall\mathbf{s}, \quad q_n(B_2|\mathbf{s}) = q_2, \forall\mathbf{s}.$$

Then,$\Upsilon_{\max} - \gamma = q_1\epsilon_1 + q_2\epsilon_2$. If the adversary monitors B_1 with probability p, then

$$\begin{aligned}\phi(p,(q_1,q_2)) &= p\left[\frac{1}{2}\log\left(\frac{1+q_1}{q_1}\right) + \frac{1}{2}\log\left(1+q_1\right)\right] \\ &+(1-p)\left[\frac{1}{2}\log\left(\frac{1+q_1}{q_1}\right) + \frac{1}{2}\log\left(1+q_1\right)\right].\end{aligned}$$

If $q_1 > q_2$, then $p = 0$ is optimal for the adversary. However, if $p = 0$, then the optimal network strategy is to make $q_1 = 0$, which is a contradiction. Hence

$$q_1 = q_2 = \frac{\Upsilon_{\max} - \gamma}{\epsilon_1 + \epsilon_2}.$$

If $p*$ is the saddle point strategy for the adversary, then p^* must necessarily satisfy (from Theorem 2)

$$\frac{d}{dq_1}\phi(p^*, (q_1, \frac{\Upsilon_{\max} - \gamma - q_1\epsilon_1}{\epsilon_2})) = 0,$$

where $q_1 = \frac{\Upsilon_{\max}-\gamma}{\epsilon_1+\epsilon_2}$. It is easily verified that $p^* = \frac{\epsilon_1}{\epsilon_1+\epsilon_2}$ is the unique solution to the above equation.

F. Proof of Theorem 6

The adversary has 2 choices: either monitor a source and a non-multiplexing relay, or a source and a multiplexing relay. Within the set of relays, condition 1 in Theorem 2 requires that the amount of information available through each relay is identical. In other words, within the set of multiplexing relays, the probability of covertness would be identical. Consequently, within the set of multiplexing relays, the probability of an adversary monitoring any particular multiplexing relay would be identical. Likewise, the argument applies to the set of non-multiplexing relays as well. Therefore, if q_r^1, q_r^2 refer to the respective probabilities of monitoring a non-multiplexing and multiplexing relay, and if p_1, p_2 refers the the respective probabilities of an adversary monitoring a non-multiplexing and multiplexing relay, then

$$\begin{aligned}\phi &= 1 - \frac{q_a^1}{\log(S_T)}[q_r^1\log(q_r^1) - (q_r^1+n-1)\log(q_r^1+n-1)] \\ &\quad - \frac{q_a^2}{\log(S_T)}[2q_r^2\log(2q_r^2) + 2 - (2q_r^2+n-2)\log(2q_r^2+n-2)],\end{aligned}$$

where $S_T = \frac{n!}{2^k}$ is the total number of sessions. Applying the conditions in Theorem 2 to the expression above, the theorem is proved. Details are omitted due to paucity of space □.

G. Proof of Theorem 7

We know from Theorem 3 that the anonymity $A(\gamma)$ can be written as:

$$A(\gamma) = \frac{A_1(\gamma) + A_2(\gamma)}{n\log n},$$

where

$$\begin{aligned}A_1(\gamma) &= \left[p_c + \frac{w(0)(1-p_c)}{n!}\right]\log\left(w(0)(1-p_c) + n!p_c)\right) \\ &+ \frac{(n! - w(0))}{n!}\log p_c \\ A_2(\gamma) &= \sum_{\max(1,2k-n)}^{k}\binom{k}{m}\binom{k'}{m}\frac{m!}{n!}(1-p_c)w(m)\log(w(m)).\end{aligned}$$

Using Stirling's approximation for large n, we can write:

$$\begin{aligned}\frac{w(0)}{n!} &= \frac{((n-\alpha n)!)^2}{n!(n-2\alpha n)!} \\ &\approx \frac{(n-\alpha n)^{2n-2\alpha n}\sqrt{(1-\alpha)^2n^24\pi^2}e^{-2n+2\alpha n}}{n^n(n-2\alpha n)^{n-2\alpha n}\sqrt{(1-2\alpha)n^24\pi^2}e^{-2n+2\alpha n}} \\ &= \sqrt{\frac{(1-\alpha)^2}{1-2\alpha}}e^{n[(2-2\alpha)\log(1-\alpha)-(1-2\alpha)\log(1-2\alpha)]} \\ \to 0 &\quad \text{for any } \alpha \in (0,1).\end{aligned}$$

$$\text{Therefore } \lim_{n\to\infty} A_1(\gamma) = p_c. \qquad (12)$$

Using Stirling's approximation on $\log w(m)$, for large n

$$\begin{aligned}\log w(m) &= 2\log((n-k)!) - \log((n-2k+m)!) \\ &= 2(n-k)\log(n-k) - (n-2k+m)\log(n-2k+m) \\ &\quad + \frac{1}{2}\log\left(\frac{(n-k)^2}{n-2k+m}\right) + O(1) \\ &= \left(n - m + \frac{1}{2}\right)\log n + O(1)\end{aligned}$$

Since $m \le \alpha n$, we can write

$$\begin{aligned}A_2(\gamma) &= \sum_{m=\max(1,2k-n)}^{k}\binom{k}{m}\binom{k'}{m}\frac{m!}{n!}(1-p_c)w(m)\log(w(m)) \\ &= \frac{1-p_c}{\binom{n}{k}}\sum_{m=\max(2k-n,1)}^{k}\binom{k}{m}\binom{n-k}{k-m}(n-m)\log n \\ &= \frac{(1-p_c)\log n}{\binom{n}{k}}\left[(n-k)\binom{n}{k} + \frac{k}{n}(n-k)\binom{n}{k}\right] \\ &= \frac{n^2-k^2}{n}(1-p_c)\log n. \qquad (13)\end{aligned}$$

Combining (12) and (13), the result is proven. □.