Anonymous Networking amidst Active Adversaries

Parv Venkitasubramaniam
Electrical Engineering
Lehigh University
Bethlehem, PA 18016
Email: parv@lehigh.edu

Lang Tong
Electrical and Computer Engineering
Cornell University
Ithaca, NY 14853
Email: ltong@ece.cornell.edu

***Abstract*—The problem of anonymous wireless networking is considered when adversaries who monitor the transmissions in the network are also capable of compromising a fraction of nodes to extract network information. For a given level of network performance, as measured by network throughput, the problem of maximizing anonymity is studied from a game-theoretic perspective. The metric of anonymity considered is the conditional entropy of network routes given the monitored packet transmission times. In order to provide anonymity, a random subset of nodes (referred to as covert relays) are chosen to generate independent transmission schedules. These covert relays, unless compromised, can effectively hide the flow of traffic through them. Depending on the routes and the throughput requirement, the network designer needs to optimize the choice of covert relays such that anonymity is maximized. Whereas, the eavesdropper needs to optimize the choice of nodes to compromise subject to a constraint on maximum number of monitored nodes, such that the anonymity of the network routes is minimized. This problem is posed as a two player zero-sum game, and it is shown that a unique Nash equilibrium exists for a general category of finite networks. Using numerical examples, the tradeoff between the achievable anonymity and the power of the adversary is demonstrated as a function of the throughput for passive and active adversaries.**

Keywords– anonymity, wireless networks, Nash 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]. Equipped with such information, a malicious adversary can launch more powerful attacks such as wormhole, jamming and denial of service. The problem of anonymous communication in traditional IP based networks has been well studied, beginning with the seminal work by David Chaum on Mix networks [2]. In ad hoc wireless networks, however, the problem has attracted significant attention only recently [3]. The primary challenge in the design of anonymous protocols for wireless networks is to hide the routing information from eavesdroppers without violating the constraints imposed by the shared medium. In particular, the shared medium is band limited, transmissions are susceptible to fading and interference, and in many networks, nodes/routers are deployed with limited physical protection.

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

The typical design of anonymous networking protocols models adversaries as passive and capable of monitoring the transmissions in the network perfectly. However, in networks with limited physical protection, for example sensor networks, adversaries would be capable of compromising a few nodes and extract additional flow related information. In this work, our goal is to study the problem of anonymity in such networks, where an *unknown* subset of the nodes are compromised by the adversary. The subset of compromised nodes could depend on the physical location of the adversary, or partial knowledge of cryptographic keys. It is also possible that in public wireless networks, certain nodes may have lesser physical protection than others, and are hence, more vulnerable.

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 the adversary. These modifications however reduce the achievable network performance, particularly in ad hoc wireless networks, where the scheduling needs to satisfy constraints due to limited bandwidth and interference on the shared channel. Therefore, depending on the level of network performance desired, it is necessary to pick the optimal set of nodes to modify transmission schedules so that the quality of service (QoS) criterion is met while providing maximum anonymity. If the network designer were aware of which nodes were compromised by the adversary, the optimal set of nodes can be chosen such that minimum information is available through the compromised nodes. However, if the adversary is aware of the set of nodes chosen to modify schedules, then he can choose to compromise only those nodes that provide him maximum information about the network routes. Since neither the adversary nor the network designer may have perfect knowledge, this "interplay" between the two parties is studied using game theory.

When the set of compromised nodes is unknown to the network designer, intuition may suggest that the network designer would have to design the scheduling strategy assuming a passive adversary. However, when the power of the adversary, *i.e.* the maximum fraction of monitored nodes, is bounded, 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 achievable under the omniscient assumption. 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 should be compromise 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.

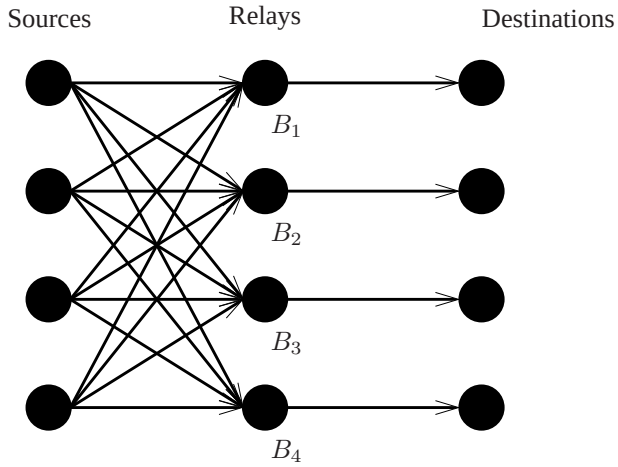

Fig. 1. Example Network.

The game theoretic formulation can be motivated using the following example. Consider the network $\mathcal{G}_1$ as shown in Figure 1. We assume that during any period of observation of the adversary, the network operates in one of six configurations, one for each source-relay pairing (each source picks a distinct relay). The adversary's goal is to identify which of these configurations is currently active in the network. Consider an adversary who can compromise atmost one relay in the network.

If a relay generates a transmission schedule that is statistically independent from other schedules, then passive monitoring would reveal no information about the flow of traffic through the relay. However, if the relay were to be compromised then the node would reveal this information. If all relays generated independent schedules, then it is easy to see that the network has maximum anonymity regardless of which node is compromised. Let us suppose that, for a given level of network performance, the network is allowed to modify the transmission schedule of at most two of the relays. If the relays generating independent schedules are B_1 and B_2, then an adversary who compromises B_1 or B_2 (aside from passively monitoring all other transmissions in the network) would perfectly identify the set of source-destination pairs. However, given the knowledge that the adversary would compromise B_1 or B_2, the optimal strategy of the network designer would be to make the schedules of B_3, B_4 independent. This "interplay" between the optimal design of adversary and the network designer forms the motivation for the game-theoretic model. In particular, this example can be formulated by an equivalent two-player zero-sum game between the adversary and the network designer, and it is easily shown that a Nash equilibrium exists in the class of randomized strategies. At the equilibrium point, the optimal strategy for the network designer is to choose two of the relays with probability $\frac{1}{6}$ to generate independent schedules, and the optimal strategy for the adversary is to compromise any relay with probability $\frac{1}{4}$. By definition, at this operating point, neither the network designer nor the adversary have any incentive to modify their strategy.

The example considered a simple scenario of a two hop network. In a general multihop network, anonymity based on partial information about the routes can be quantified using Shannon's equivocation [4], [5], and the goal is to optimize the tradeoff between the desired network throughput and the achievable anonymity given the adversary's monitoring capability.

B. Main Contributions

In this work, we consider a general class of finite networks with a *localized adversary* who monitors the transmissions of an unknown subset of the nodes. When the maximum number of monitored nodes is bounded by a known quantity, we present a game-theoretic formulation of the design problem with anonymity as payoff, where the adversary chooses a random subset of nodes to compromise and the network designer chooses a random subset of nodes to modify transmission schedules. For the class of finite multihop networks considered, we prove that a unique Nash equilibrium exists in the class of randomized strategies. We provide numerical examples to demonstrate the tradeoff between the anonymity and throughput under different adversarial restrictions.

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 [2]. 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 [6] or browsing [7], the strategies have not been designed for long streams of packets under physical layer constraints on latency or bandwidth. In fact, 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 [8].

In wireless networks, an alternative solution to Mixing is the use of cover traffic [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 [9] due to high rate of dummy transmissions and

the implementation requires synchronization across all nodes which is not practical in ad hoc wireless networks.

In this work, we adopt the mathematical framework developed in [5], [10] for omniscient adversaries, where equivocation was used to quantify anonymity of routes, and it was shown that anonymity in network communication requires a reduction in network throughput. In particular, for long streams of packets transmitted across the network, it was proven that any desired level of anonymity is achievable by making a subset of relays (referred to as *covert relays*) generate independent transmission schedules.

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, game-theoretic models have primarily been used to model problems related to distributed intrusion detection [12], [13], where the goal is to design attacking and detection strategies with probability of detection as the payoff. In [14], 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 [15] 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 covert relaying, 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. Furthermore, the payoff is given by conditional entropy— a non linear function of probabilities of mixing strategies— and is thus different from classical mixed strategy models [16].

Entropy and measures related to entropy such as K-L divergence have been proposed as payoffs in games of complexity between two players, *Nature* and *the Physicist*, where the goal of nature is to design the distribution of the observable information, and the goal of the physicist is to guess the chosen distribution with maximum accuracy. The equilibrium strategies in such games of complexity have been shown to belong to a category of maximum entropy distributions [17].

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 $P = (V_1, \cdots, V_n) \in \mathcal{V}^*$ 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 $\mathbf{S} \sim p(\mathbf{s})$. 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 $\mathcal{S} = \{\mathbf{s} \in \mathcal{P}(\mathcal{G}) : p(\mathbf{s}) > 0\}$.

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 observed schedules reveal as little information about the actual session as possible. For instance, if a subset of relays always generated independent transmission schedules then it is not possible for the adversary to determine which paths pass through them unless all of them are compromised. In effect, the set of (broken) paths observeable would be a distorted version of the actual session. Let $\hat{\mathbf{S}}$ (henceforth referred to as *observeable session*) denote the set of paths observed by an omniscient adversary.

Adversary Observation. We consider a general adversary model, where all packet transmission times are observed by the adversary, and a fraction of relays are compromised. Specifically, the adversary randomly picks any subset of relays, denoted by $\mathbf{N}_a$, to monitor subject to a constraint on the maximum number of monitored nodes, 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 observeable session $\hat{\mathbf{S}}$ and the set of monitored nodes, the adversary would observe a less distorted version of the underlying session $\mathbf{S}$. In effect 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 $f_a(\mathbf{S}, \hat{\mathbf{S}}, \mathbf{N}_a)$. Note that $f_a(\mathbf{S}, \hat{\mathbf{S}}, \mathcal{V}) = \mathbf{S}$ and $f_a(\mathbf{S}, \hat{\mathbf{S}}, \phi) = \hat{\mathbf{S}}$.

B. Performance Metrics: Anonymity and Throughput

The task of the network designer is to design a probabilistic strategy, denoted by $q_n(\hat{\mathbf{s}}|\mathbf{s})$, such that a desired quality of service is achieved while the adversary obtains minimum information about the session $\mathbf{S}$ by observing $\hat{\mathbf{S}}_a$. The task of the adversary is to design the probabilistic strategy $q_a(\mathbf{N}_a)$

of monitored nodes such that maximum information can be obtained by observing $\hat{\mathbf{S}}_a$.

Anonymity We quantify anonymity using Shannon's equivocation which measures the uncertainty of the underlying session given the adversary's observation (of the broken paths).

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:

$$A(q_n, q_a) \triangleq \frac{H(\mathbf{S}|\hat{\mathbf{S}}_a)}{H(\mathbf{S})}. \tag{1}$$

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 [18]. Note that previous entropy-based definitions of anonymity [5], [10] in the context of omniscient adversaries are special cases of Definition 1 (when $\mathbf{N}_a \equiv \mathcal{V}$).

Throughput Since distorting the observeable 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 rates of data packes 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 $\mathbf{S}$ and the observeable session is $\hat{\mathbf{S}}$. Note that $\Lambda(\hat{\mathbf{S}}, \mathbf{S}) \leq \Lambda(\mathbf{S}, \mathbf{S})$.

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

$$\Upsilon(q_n) = \mathbb{E}\left(\Lambda(\mathbf{S}, \hat{\mathbf{S}})\right) \tag{2}$$

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 while higher throughput necessitates fewer dummy transmissions. Unlike the passive adversary setup, the uncertainty in the identities of the compromised nodes, *i.e.* the randomness in $\mathbf{N}_a$, complicates the design of the optimal scheduling strategy, as was illustrated in the example in Section I. In the following section, we therefore formulate this problem as a two-player zero sum game, and establish the existence of Nash equilibria.

III. Two Player Game using Covert Relaying Strategy

Consider a two-player zero sum game, 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 $q_n(\hat{\mathbf{S}}|\mathbf{S})$ which is a distribution over the space of loop-less paths $\mathcal{P}$. In this work, we design the observeable session $\hat{\mathbf{S}}$ 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.

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.

In a given session $\mathbf{s}$, if the set of covert relays is $\mathbf{b}_n$ then the observeable 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 the independent schedule of a covert relay would prevent the adversary from detecting any correlation between the schedule of any prior node in the path and that of the covert 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 set of strategies where it may not be possible to realize all observeable sessions in $2^{\mathcal{P}(\mathcal{G})}$ for any given session $\mathbf{s}$.

As expected, maintaining independent schedules would require covert relays to drop packets or add dummy packets thereby resulting in rate loss, whereas visible relays can relay every packet that arrives without any rate loss. The loss in rate at a covert relay would be the function of the number of arrival processes, distribution of transmission schedules and the relaying strategy to forward packets. In a session $\mathbf{s}$, let $\Lambda^c(\mathbf{s}, \mathbf{b})$ denote the achievable sum-rate when the relays in the set $\mathbf{b}$ are covert. The characterization of the exact rate loss is not necessary for the remainder of this exposition, and we will treat it as an abstract quantity. In the subsequent section, where we apply the theory to 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:

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

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:

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

$$\mathcal{A}_a = \begin{cases} \{q_a(\mathbf{n}_a) : \mathbf{n}_a \in \mathcal{V}^{k_a}\} \\ q_a(\mathbf{n}_a) \geq 0, \forall \mathbf{N}_a \\ \sum_{\mathbf{n}_a} q_a(\mathbf{n}_a) = 1 \end{cases}$$

The task of the two participants is to design the probability mass functions q_n, q_a to maximize their respective payoffs. The key constraint in the action of the network designer is the throughput requirement ($\Upsilon(q_n) \geq \gamma$). The key constraint for the adversary's action is the maximum number of monitored nodes k_a.

B. Payoff and Nash Equilibrium

Since the adversary obtains complete information from the compromised nodes, the adversary observation would be equivalent to the observeable session when the set of covert relays exclude the compromised nodes. In other words, for a given session $\mathbf{s}$, with covert relays $\mathbf{b}$, the adversary observation $\hat{\mathbf{s}}_a$ would be given by

$$f_a(\mathbf{s},\mathbf{b},\mathbf{n}_a) = f_o(\mathbf{s},\mathbf{b}/\mathbf{n}_a).$$

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:

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

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

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

$$\begin{aligned}\phi(q_n,q_a) &= \frac{H(\mathbf{S}|\hat{\mathbf{S}}_a)}{H(\mathbf{S})} = \frac{1}{H(\mathbf{S})} \sum_{\mathbf{n}_a\in 2^{\mathcal{V}}} \sum_{\mathbf{s}\in\mathcal{S},\mathbf{b}_n\in 2^{\mathcal{V}}} q_a(\mathbf{n}_a)p(\mathbf{s}) \times \\ &\quad -q_n(\mathbf{s},\mathbf{b}_n)\log q_{ap}(\mathbf{s}, f_a(f_o(\mathbf{s},\mathbf{b}_n),\mathbf{n}_a),\mathbf{b}_a) \quad (3)\end{aligned}$$

where

$$q_{ap}(\mathbf{s},\mathbf{p},\mathbf{n}) = \frac{q_n(\mathbf{n},\mathbf{s})p(\mathbf{s})}{\sum_{(\mathbf{s}',\mathbf{b}')\in\mathcal{F}_a(\mathbf{p},\mathbf{n})} q_n(\mathbf{s}',\mathbf{b}')p(\mathbf{s}')}$$

is the aposteriori probability that the current session is $\mathbf{s}$ given the adversary observes $\mathbf{p}$ obtained through nodes $\mathbf{n}$.

In a zero-sum game, we know that the interests of the network designer and the adversary are exactly the opposite; while the network designer would prefer to make the monitored nodes covert, the adversary would prefer to monitor the nodes that are not covert. We wish to determine if there is an operating point in the pair of action spaces, where neither the network designer nor the adversary has any incentive to change their strategy, in other words, if this game has a Nash equilibrium.

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

$$\phi(q_n,q_a) = \sup_{q\in\mathcal{A}_n} \phi(q,q_a) = \inf_{q\in\mathcal{A}_a} \phi(q_n,q). \quad (4)$$

Note that, although it has been shown that two player zero sum games, as defined classically [16], always have a Nash equilibrium in the class of mixed strategies, the result does not extend to the game defined here. While the payoff for a mixed strategy in classical two player games is a weighted sum of the mixing probabilities, in our setup, the payoff is a non-linear function of the mixing probabilities, as given in (3). The existence of a Nash equilibrium in this game is shown in the following theorem.

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

Proof: Refer to Appendix. □

The Nash equilibrium condition guarantees that at the operating point, the adversary can use no other strategy to decrease the anonymity of the session. Characterizing the optimal strategy for the adversary is particularly helpful in network scenarios where additional protection can be provided to nodes that are more likely to be monitored. Note that since the action spaces are defined on the probability simplex, any pair of pure strategies in $\mathcal{A}_a \times \mathcal{A}_n$ corresponds to a random choice of deterministic strategies, and the Nash equilibrium would therefore be a "pure" (albeit random) strategy equilibrium on the defined action spaces.

Note that the omnisicient adversary setup is a specific instance of this game, when the adversary compromises 0 nodes. The existence and uniqueness of the Nash equilibrium is trivial in that instance and the operating point is given by the rate distortion optimization:

$$\phi(\gamma) = H(\mathbf{S}) - \inf_{q_n(\hat{\mathbf{S}}|\mathbf{S}):\Upsilon(q_n)\leq\gamma} I(\mathbf{S};\hat{\mathbf{S}}), \quad (5)$$

which was proven in [5].

The uniqueness of the equilibrium in the general adversary model follows from the zero-sum property of the game. Note that this game is also an example of an incomplete information game [13] 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.

Consider the example of a switching network as shown in Figure 2. In any session of the network, each source node A_i picks a unique destination C_j to transmit packets

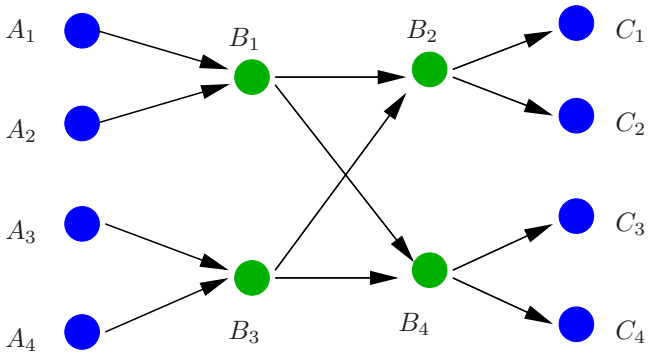

Fig. 2. Switching Network: $\{A_i\}$ transmit to $\{C_i\}$ through relays $\{B_i\}$.

to. Given a set of source-destination pairs, it is easy to see that the set of routes are fixed. Figure 3 plots the tradeoff between anonymity and throughput for the example network for an active adversary for different values of L_e (number of compromised nodes). Note that the adversary passively monitors all other nodes in the network.

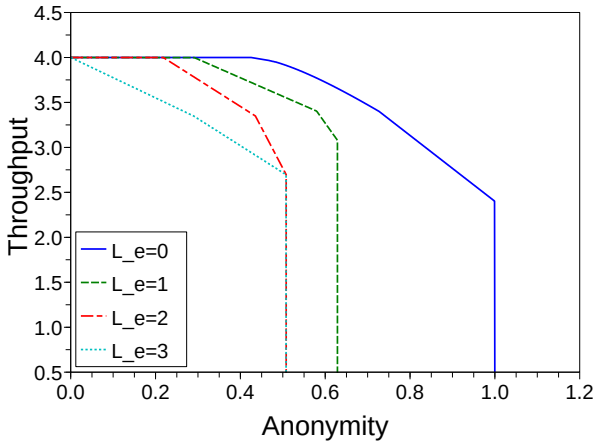

Fig. 3. Throughput-Anonymity Trade-offs for switching network with an active adversary.

In Figure 3, the curve corresponding to $L_e = 0$ represents the omniscient passive eavesdropper. As is evident from the plots, active compromising of nodes significantly reduces anonymity of the network routes. In this example, it is sufficient for the adversary to compromise the 4 relays $B_1, \cdots, B_4$ in order to perfectly determine the session. For every value of L_e, there is a maximum level of anonymity (less than 1) that is achievable. This would correspond to the minimum side information that can be obtained by the adversary by compromising L_e relays.

Comparison with Localized Passive Adversary In [19], we adopted a game-theoretic approach to study networks under partial eavesdropping, where a passive adversary monitors only a fraction of nodes. In that setup, the uncertainty in the choice of nodes to monitor gives rise to a game-theoretic formulation. The key difference between the partial eavesdropping and active adversary problems lies the choice of nodes by the adversary. This is illustrated in Tables I and II, where we summarize the optimal strategies of the adversaries with different power levels. In the case of active adversaries, there is a high correlation between compromised nodes and covert relays, whereas, for passive adversaries, a higher percentage of non-covert nodes are likely to be monitored.

K_e	Eavesdropper support	Designer Support
2	$\{ \begin{matrix}(B_1,B_3),(B_1,B_4)\\(B_2,B_3),(B_2,B_4)\end{matrix} \}$	$\{ (B_3),(B_4) \}$
3	$\{(B_1,B_3,B_4),(B_2,B_3,B_4)$ $(A_1,A_3,B_3),(A_2,A_3,B_4)\}$ or $\{(B_1,B_3,B_4),(B_2,B_3,B_4)$ $(A_1,A_4,B_4),(A_2,A_4,B_3)\}$	$\{(B_3,B_4),(B_1,B_2)$ $(B_1),(B_2)\}$
4	$\{(A_1,A_2,A_3,B_3),(A_1,A_2,A_3,B_4)$ $(A_1,A_3,B_1,B_3),(A_2,A_3,B_2,B_4)$ $(A_1,A_3,A_4,B_4),(A_1,A_3,A_4,B_3)$ $(A_2,A_4,B_1,B_4),(A_1,A_4,B_2,B_3)\}$	$\{(B_3,B_4),(B_1,B_2)$ $(B_1),(B_2)\}$

TABLE I
OPTIMAL SUPPORT SET OF STRATEGIES FOR NETWORK DESIGNER AND THE LOCALIZED ADVERSARY.

L_e	Eavesdropper support	Designer Support
1	$\{ (B_2),(B_4) \}$	$\{ (B_2,B_4),(B_4),(B_2) \}$
2	$\{(B_1,B_2),(B_1,B_4)$ $(B_3,B_2),(B_3,B_4)\}$	$\{(B_2,B_4),(B_2)$ $(B_4),(B_1,B_2)\}$
3	$\{(B_1,B_2,B_4),(B_3,B_2,B_4)\}$	$\{(B_3,B_4),(B_1,B_2)$ $(B_1,B_2,B_3,B_4)\}$

TABLE II
OPTIMAL SUPPORT SET OF STRATEGIES FOR NETWORK DESIGNER AND THE ACTIVE ADVERSARY.

IV. Concluding Remarks

In this work, we considered the problem of providing anonymity to network communication when adversaries compromise an unknown subset of nodes in the network. We formulated a game-theoretic equivalent, and proved the existence of Nash equilibrium. Although the numerical simulation was based on a simple switching network, the solutions indicate that this approach can provide significant insight into optimal design of anonymizing strategies as well as the optimal adversarial behaviour. The problem of computing the Nash 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 a speficic network model, and assumed knowledge of topology and sessions. A similar approach for random networks with random connections could shed valuable insights on scaling behaviour of anonymous communication.

V. Acknowledgements

This work is supported in part by the National Science Foundation under awards CCF-0635070, CCF-0728872, the U. S. Army Research Laboratory under the Collaborative

Technology Alliance Program DAAD19-01-2-0011 and Army Research Office MURI program under award W911NF-08-1-0238.

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

[3] X. Hong, P. Wang, J. Kong, Q. Zheng, and J. Liu, "Effective Probabilistic Approach Protecting Sensor Traffic," in *Military Communications Conference, 2005*, (Atlantic City, NJ), pp. 1–7, Oct. 2005.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, 1949.

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

[6] C. Gulcu and G. Tsudik, "Mixing e-mail with babel," in *Proceedings of the Symposium on Network and Distributed System Security*, pp. 2–19, February 1996.

[7] O. Berthold, H. Federrath, and S. Kopsell, "Web MIXes: A system for anonymous and unobservable Internet access," in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science*, vol. 2009, (Berkeley, CA), pp. 115–129, July 2000.

[8] 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.

[9] B.Radosavljevic and B. Hajek, "Hiding traffic flow in communication networks," in *Military Communications Conference*, 1992.

[10] P. Venkitasubramaniam and L. Tong, "Anonymous networking amidst eavesdroppers," *IEEE Transactions on Information Theory*, vol. 54, pp. 2770–2784, June 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. 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.

[13] 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.

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

[15] 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.

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

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

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

[19] P. Venkitasubramaniam and L. Tong, "Anonymous Network with Localized Adversaries: A Game Theoretic Formulation." Submitted to *Conference on Information Systems and Sciences.*, Jan. 2009.

[20] 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 Nash equilibrium in the two player game, it is sufficient to show the following:

1) The action spaces $\mathcal{A}_n$ 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 $q_a \in \mathcal{A}_a$, the function $\phi(x, q_a)$ is concave in x.
4) For every $q_n \in \mathcal{A}_n$, the function $-\phi(q_n, y)$ 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 [20].

1) **Convexity of action spaces:** The space $\mathcal{A}_a$ is a finite-dimensional simplex, which, by definition 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.