Control of Wireless Networks with Secrecy

C. Emre Koksal
Department of Electrical and Computer Engineering,
The Ohio State University Columbus, OH
Email: koksal@ece.osu.edu

Ozgur Ercetin and Yunus Sarikaya
Faculty of Engineering and Natural Sciences,
Sabanci University,Istanbul, TR.
Email: {oercetin,ysarikaya}@sabanciuniv.edu

***Abstract*—We consider the problem of cross-layer resource allocation in time-varying cellular wireless networks, and incorporate information theoretic secrecy as a Quality of Service constraint. Specifically, each node in the network injects two types of traffic, private and open, at rates chosen in order to maximize a global utility function, subject to network stability and secrecy constraints. The secrecy constraint enforces an arbitrarily low mutual information leakage from the source to every node in the network, except for the sink node. We first obtain the achievable rate region for the problem for single and multi-user systems assuming that the nodes have full CSI of their neighbors. Then, we provide a joint flow control, scheduling and private encoding scheme, which does not rely on the knowledge of the prior distribution of the gain of any channel. We prove that our scheme achieves a utility, arbitrarily close to the maximum achievable utility.**

I. Introduction

In the recent years, there have been a number of investigations on wireless information theoretic secrecy. These studies have been largely confined within the boundaries of the *physical layer* in the wireless scenario and they have significantly enhanced our understanding of the fundamental limits and principles governing the design and analysis of secure wireless communication systems. For example, [5], [2], [11] have unveiled the **opportunistic secrecy** principle which allows for transforming the multi-path fading variations into a secrecy advantage for the legitimate receiver, even when the eavesdropper is enjoying a higher average signal-to-noise ratio (SNR). The fundamental role of **feedback** in enhancing the secrecy capacity of point-to-point wireless communication links was established in [10], [1], [6]. More recent works have explored the use of **multiple antennas** to induce ambiguity at the eavesdropper under a variety of assumptions on the available transmitter channel state information (CSI) [7], [12]. The multi-user aspect of the wireless environment was studied in [9], [13], [11] revealing the potential gains that can be reaped from appropriately constructed user cooperation policies.

Despite the significant progress in information theoretic secrecy, most of the work has focused on physical layer techniques and on a single link. The area of wireless information theoretic secrecy remains in its infancy, especially as it relates to the design of wireless networks and its impact on network control and protocol development. Therefore, our understanding of the interplay between the secrecy requirements and the critical functionalities of wireless networks, such as *scheduling, routing, and congestion control* remains very limited.

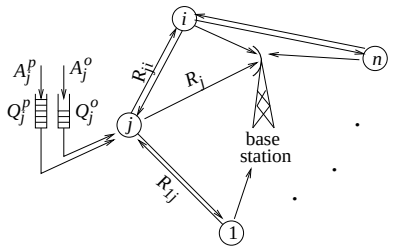


Fig. 1. Uplink communication with private and open information.

To that end, in this paper[1] we address the basic wireless network control problem in order to develop a cross-layer resource allocation solution that will incorporate information privacy, *measured by equivocation*, as a QoS metric. In particular, we consider the single hop uplink setting, in which nodes collect private and open information, store them in separate queues and transmit them to the base station. At a given point in time, only one node is scheduled to to transmit and it may choose to transmit some combination of open and private information. We assume the knowledge of the instantaneous channel gains at all nodes. First, we evaluate the region of achievable open and private data rate pairs for a single node scenario, with and without joint encoding of open and private information. Then, we consider the multi-node uplink scenario and introduce **private opportunistic scheduling**. We find the achievable **private rate region** of private opportunistic scheduling and show that it achieves the maximum sum privacy rate over all joint scheduling and encoding strategies. Next, we model the problem as that of network utility maximization. Then, we provide a joint flow control, scheduling and private encoding scheme, which does not rely on the knowledge of the prior distribution of the gain of any channel. We prove that our scheme achieves a utility, arbitrarily close to the maximum achievable utility. Also, we show via simulations that the privacy rates achievable by the joint scheme is fairly close to the information theoretic limit (achievable with known channel priors).

II. Problem Model

We consider the single hop uplink scenario illustrated in Fig. 1. The network is consists of n nodes, each of which has

[1]This material is based upon work supported by the National Science Foundation under Grants CNS-0831919, CCF-0916664.

both open and private information to be transmitted to a single base station over the associated uplink channel. When a node is transmitting, every other node overhears the transmission over the associated cross channel. Every channel is assumed to be iid block fading, with a block size of N_1 channel uses. Let the entire session last for N_2 blocks, which correspond to a total of $N = N_1 N_2$ channel uses. We denote the instantaneous achievable rate for the uplink channel of node j by $R_j(k)$, which is the the maximum mutual information between output symbols of node j and received symbols at the base station over block k. Likewise, we denote the rate of the cross channel between nodes j and i with $R_{ji}(k)$, which is the maximum mutual information between output symbols of node j and input symbols of node i over block k. Note that there is no actual data transmission between any pair of nodes, but $R_{ji}(k)$ will be necessary, when we evaluate the private rates between node j and the base station.

Even though our results are general for all channel models, in numerical evaluations, we assume all channels to be *Gaussian* and a constant transmit power, identical to P over all blocks k, $1 \leqslant k \leqslant N_2$. We represent the uplink channel for node j and the cross channel between nodes j and i with a power gain (magnitude square of the channel gains) $h_j(k)$ and $h_{ji}(k)$ respectively over block k. We normalize the power gains such that the (additive Gaussian) noise has unit variance. Then, as $N_1 \to \infty$,

$$R_j(k) = \log(1 + P h_j(k)) \tag{1}$$

$$R_{ji}(k) = \log(1 + P h_{ji}(k)). \tag{2}$$

Each node j have a private message $W_j \in \{1, \ldots, 2^{N R_j^{\text{priv}}}\}$ to be transmitted to the base station over N channel uses. Let the vector of symbols received by node i be $\mathbf{Y}_i$. To achieve *perfect privacy*, following constraint must satisfied by node j: for all $i \neq j$, $\frac{1}{N} I(W_j, \mathbf{Y}_i) \leqslant \varepsilon$ as $N \to \infty$. We define the instantaneous privacy rate over block k as:

$$R_j^p(k) = [R_j(k) - R_{ji}(k)]^+. \tag{3}$$

It is shown in [5] that a long term rate of $R_j^{\text{priv}} = \mathbb{E}\left[R_j^p(k)\right]$ is achievable by node j, subject to perfect privacy from node i.

The amount of open traffic, $A_j^o(k)$, and private traffic, $A_j^p(k)$, injected in the queues at node j in block k are both selected by node j at the beginning of each block. Open and private information are stored in separate queues with sizes $Q_j^o(k)$ and $Q_j^p(k)$ respectively. At any given block, a scheduler chooses which node will transmit and the amount of open and private information to be encoded over the block. We use the indicator variable $\mathscr{I}_j(k)$ to represent the scheduler decision:

$$\mathscr{I}_j(k) = \begin{cases} 1, & \text{private information from node } j \\ 0, & \text{otherwise} \end{cases}. \tag{4}$$

We assume throughout the paper that every user has full CSI of its uplink channel and all of its cross channels, i.e., $h_j(k)$ and $h_{ji}(k)$ is available to node j at every block k.

III. Achievable Rates

A. Single User Achievable Rates

Consider the single user scenario in which the primary user (node 1) is transmitting information over the primary channel and a single secondary user (node 2) is overhearing the transmission over the secondary channel. Over each block k, the primary user chooses the rate of private and open information to be transmitted to the intended receiver. As discussed in [3] it is possible to encode open information at a rate $R_1(k) - R_1^p(k)$ over each block k, jointly with the private information. One can simply replace the randomization message of the binning strategy of the achievability scheme with the open message, which is allowed to be decoded by the secondary user. In the rest of the section, we analyze both the case in which open information can and cannot be encoded along with the private information. We find the region of achievable private and open information rates, $(R^{\text{priv}}, R^{\text{open}})$, over the primary channel.

1) Separate encoding of private and open messages: First we assume that each block contains either private or open information, but joint encoding over the same block is not allowed. Let us define $\mathscr{I}(k)$ as the indicator variable, which takes on a value 1, if information is encoded privately over block k and 0 otherwise. Then, one can find R^{priv}, associated with the point $R^{\text{open}} = \alpha$ by solving the following integer program:

$$\max_{\mathscr{I}(k) \in \{0,1\}} \quad \mathbb{E}\left[\mathscr{I}(k) R_1^p(k)\right] \tag{5}$$

$$\text{subject to} \quad \mathbb{E}[(1 - \mathscr{I}(k)) R_1(k)] \geqslant \alpha, \tag{6}$$

where the expectations are over the joint distribution of the instantaneous rates $R_1(k)$ and $R_{12}(k)$. Note that, since the channel rates are iid, the solution, $\mathscr{I}^*(k) = \mathscr{I}^*(R_1(k), R_{12}(k))$ will be a stationary policy. Also, a necessary condition for the existence of a feasible solution is $\mathbb{E}[R_1(k) \geqslant \alpha]$. Dropping the block index k for simplicity, the problem leads to the following Lagrangian relaxation:

$$\begin{aligned} \min_{\lambda > 0} \max_{\mathscr{I} \in \{0,1\}} & \mathbb{E}\left[\mathscr{I} R_1^p\right] + \lambda \left(\mathbb{E}[(1 - \mathscr{I}) R_1] - \alpha\right) \\ &= \min_{\lambda > 0} \max_{\mathscr{I} \in \{0,1\}} \int_0^\infty \int_0^\infty \left[\mathscr{I} R_1^p - \lambda (1 - \mathscr{I}) R_1\right] \\ &\qquad p(R_1, R_{12})\, dR_1 dR_{12}, \end{aligned} \tag{7}$$

where we got rid of α in the expectation as it is merely a constant and does not affect the solution. For any given values of the Lagrange multiplier λ and (R_1, R_{12}) pair, the optimal policy will choose $\mathscr{I}^*(R_1, R_{12}) = 0$ if the integrant is maximized for $\mathscr{I} = 0$, or it will choose $\mathscr{I}^*(R_1, R_{12}) = 1$ otherwise. If both $\mathscr{I} = 0$ and $\mathscr{I} = 1$ lead to an identical value, the policy will choose one of them randomly. The solution can be summarized as follows:

$$\frac{R_1^p}{R_1} \underset{I^*=0}{\overset{I^*=1}{\gtrless}} \lambda^*, \tag{8}$$

where λ^* is the value of λ for which $\mathbb{E}[(1 - \mathscr{I}^*) R_1] = \alpha$, since $\lambda^*(\mathbb{E}[(1 - \mathscr{I}) R_1] - \alpha) \leqslant 0$.

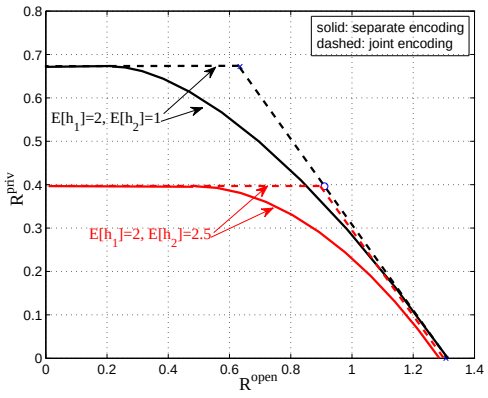


Fig. 2. Achievable rate regions for the single user scenario with iid Rayleigh block fading channels.

For Gaussian uplink and cross channels described in Section II, plugging in (1)-(3) in the solution, we obtain:

$$(1+h_1)^{1-\lambda^*} \underset{I^*=0}{\overset{I^*=1}{\gtrless}} 1+h_{12}. \tag{9}$$

In Fig. 2, the achievable pair of private and open rates, $(R^{\text{priv}}, R^{\text{open}})$, is illustrated for iid Rayleigh fading Gaussian channels, i.e., the power gains h_1 and h_{12} have an exponential distribution. The regions for both the separate (solid boundaries) and joint encoding (dashed boundaries) are illustrated on the same plot two different scenarios in which the mean power gains, $(\mathbb{E}[h_1], \mathbb{E}[h_{12}])$, are $(2,1)$ and $(2,2.5)$, and $P=1$. To plot the regions for separate encoding, we varied λ from 0 to 1 and calculated the achievable rate pair for each point. Note that the flat portion on the top part of the rate regions for separate encoding correspond to the case in which Constraint (6) is inactive.

2) Joint encoding of private and open messages: With the possibility of joint encoding of the open and private messages over the same block, the indicator variable $\mathscr{I}(k)=1$ implies that the private and open messages are encoded at rate $R_1^p(k)$ and $R_1(k)-R_1^p(k)$ respectively over block k simultaneously. Otherwise, i.e., if $\mathscr{I}(k)=0$, open encoding is used solely over the block. To find achievable R^{priv}, associated with the point $R^{\text{open}}=\alpha$, one needs to consider a slightly different optimization problem this time:

$$\max_{\mathscr{I}(k)\in\{0,1\}} \quad \mathbb{E}\left[\mathscr{I}(k)R_1^p(k)\right] \tag{10}$$

$$\text{subject to } \mathbb{E}\left[(1-\mathscr{I}(k))R_1(k)+\mathscr{I}(k)(R_1(k)-R_1^p(k))\right] \geqslant \alpha, \tag{11}$$

Defining the Lagrangian $L(\mathscr{I},\lambda) = \mathbb{E}\left[\mathscr{I}R_1^p\right] + \lambda\left(\mathbb{E}\left[(1-\mathscr{I})R_1+\mathscr{I}(R_1-R_1^p)\right]-\alpha\right)$, leads to a similar problem to (7): $\min_{\lambda>0} \max_{\mathscr{I}\in\{0,1\}} L(\mathscr{I},\lambda)$. Thus, the optimal policy $\mathscr{I}^*$ satisfies the following for any given λ:

$$(1-\lambda)R_1^p \underset{I^*=0}{\overset{I^*=1}{\gtrless}} 0. \tag{12}$$

Now let us study how the optimal solution varies for different values of λ in order to evaluate the value, λ^*, of the Lagrange multiplier that solves the relaxed problem:

(1) If $\lambda \leqslant 1$, then $\mathscr{I}^*=1$ from (12) and $L(\mathscr{I}=1,\lambda) = \mathbb{E}\left[R_1^p+\lambda(R_1-R_1^p-\alpha)\right]$. Consequently,

$$\min_{0\leqslant\lambda\leqslant 1} L(\mathscr{I}=1,\lambda) = \begin{cases} \mathbb{E}\left[R_1^p\right], & \mathbb{E}\left[R_1-R_1^p\right]>\alpha \quad \Rightarrow \lambda^*=0 \\ \mathbb{E}[R_1]-\alpha, & \mathbb{E}\left[R_1-R_1^p\right]\leqslant\alpha \quad \Rightarrow \lambda^*=1 \end{cases}. \tag{13}$$

(2) If $\lambda \geqslant 1$, then $\mathscr{I}^*=0$ from (12) and $L(\mathscr{I}=,\lambda) = \lambda\mathbb{E}[(R_1-\alpha)]$. Consequently,

$$\min_{\lambda\geqslant 1} L(\mathscr{I}=0,\lambda) = \begin{cases} \mathbb{E}[R_1]-\alpha, & \mathbb{E}[R_1]\geqslant\alpha \quad \Rightarrow \lambda^*=1 \\ -\infty, & \mathbb{E}[R_1]<\alpha \quad \Rightarrow \lambda^*=\infty \end{cases}. \tag{14}$$

From Case (2), we can deduce that if $\mathbb{E}[R_1]<\alpha$, there is no feasible solution, which is expected, since even when $\mathscr{I}=0$ at all times, the constraint will not be met. Likewise, from Case (1), if $\mathbb{E}[R_1]-\mathbb{E}\left[R_1^p\right]>\alpha$, then $\lambda^*=0$ and $\mathscr{I}^*=1$ for all blocks. Thus, at all times secure encoding will be applied and the remaining capacity, $\mathbb{E}[R_1]-\mathbb{E}\left[R_1^p\right]>\alpha$, is sufficient to meet Constraint (11), i.e., the constraint will not be active. Finally, if $\mathbb{E}[R_1]-\mathbb{E}\left[R_1^p\right]\leqslant\alpha$, $\lambda^*=1$ and from (12), any choice of $\mathscr{I}$ is acceptable as long as Constraint (11) is met. In this case, one can choose $\mathscr{I}$ probabilistically as follows:

$$\mathscr{I}^* = \begin{cases} 1, & \text{w.p. } p^p \\ 0, & \text{w.p. } 1-p^p \end{cases} \tag{15}$$

independently of R_1 and R_{12}, where $p^p = \frac{\mathbb{E}[R_1]-\alpha}{\mathbb{E}\left[R_1^p\right]}$, i.e., the constraint is met with equality.

In Fig. 2, to plot the achievable rate region (for iid Rayleigh fading Gaussian channels) with joint encoding (dashed boundaries), we varied p^p from 0 to 1 and found $(\mathbb{E}\left[R_1-R_1^p\right], \mathbb{E}\left[R_1^p\right])$ pair for each value. Similar to the separate encoding scenario, the flat portion on the top part of the regions correspond to the cases in which Constraint (11) is inactive. Note that the achievable rate region with joint encoding can be summarized by the intersection of two regions specified by: (i) $R^{\text{priv}}+R^{\text{open}}) \leqslant \mathbb{E}[R_1]$ and (ii) $R^{\text{priv}} \leqslant \mathbb{E}\left[R_1^p\right]$. The entire region specified by (i) and (ii) can be achieved by the simple probabilistic scheme described above.

B. Multiuser Achievable Rates

Now, we consider the multiuser uplink scenario in which each node j has a private message $W_j \in \{1,\ldots,2^{NR_j^{\text{priv}}}\}$ to be transmitted to a base station over its uplink channel and all other nodes $i, i\neq j$ overhear the transmission over the cross channel (j,i). The perfect privacy constraint is required for each message W_j and all nodes $i\neq j$.

Let $i^*(j) \triangleq \text{argmax}_{i\neq j}\mathbb{E}[R_{ji}(k)]$. In private opportunistic scheduling (POS), only one of the nodes is scheduled for data transmission in any given block. In particular, in block k, we opportunistically schedule node

$$j^M(k) = \underset{j\in\{1,\ldots,n\}}{\text{argmax}} \left[R_j(k)-R_{ji^*(j)}(k)\right].$$

Hence, only one node can be scheduled to receive data at a given block and the indicator variable $\mathscr{I}_j^{\text{POS}}(k)$ takes on a value 1, if node j is scheduled over block k and 0 otherwise. Let $p_j \triangleq \mathbb{P}\left(j^M(k)=j\right)$, $R_j^m \triangleq \mathbb{E}\left[R_{ji^*(j)}(k)\right]$, and $R_j^M \triangleq \mathbb{E}\left[R_j(k)|j=j^M(k)\right]$, where the expectation is over the joint distribution of the instantaneous rates of all channels.

As will be shown shortly, private opportunistic scheduling achieves a privacy rate $R_j^{\text{priv}} = p_j(R_j^M - R_j^m)$ for all $j \in \{1,\ldots,n\}$. To achieve this set of rates, we follow the following steps: To begin, node j generates $2^{Np_j(R_j^M-\delta)}$ random binary sequences. Then, it assigns each random binary sequence to one of $2^{NR_j^{\text{priv}}}$ bins, so that each bin contains exactly $2^{Np_j(R_j^m-\delta)}$ binary sequences. We call the sequences associated with a bin, the *randomization sequences* of that bin. Each bin of node j is one-to-one matched with a private message $w \in \{1,\ldots,2^{NR_j^{\text{priv}}}\}$ randomly and this selection is revealed to the base station and all nodes before the communication starts. Then, the stochastic encoder of node j selects one of the randomization sequences associated with each bin at random, independently and uniformly over all randomization sequences associated with that bin. Whenever a message is selected by node j, this particular randomization message is used. This selection is not revealed to any of the nodes nor to the base station.

Private opportunistic scheduler schedules node $j^M(k)$ in each block k and the transmitter transmits $N_1 R_{j^M(k)}(k)$ bits of the binary sequence associated with the message of node $j^M(k)$ for all $k \in \{1,\ldots N_2\}$.

Theorem 1: Among the set of all schedulers, $\{\mathscr{I}_j(\mathbf{h})\}$, $j \in \{1,\ldots,n\}$, private opportunistic scheduler $\{\mathscr{I}_j^{\text{POS}}(\mathbf{h})\}$ maximizes the sum privacy rate, $R_{\text{sum}}^{\text{priv}} = \sum_{j=1}^n R_j^{\text{priv}}$. Furthermore, the maximum achievable sum privacy rate is

$$R_{\text{sum}}^{\text{priv}} = \sum_{j=1}^{n} \left[p_j\left(R_j^M - R_j^m\right)\right].$$

The proof of Theorem 1 can be found in [8]. Next we combine Theorem 1 and the results of Section III-A2 to find the boundary of the region of achievable sum open and sum private rate pair with *joint encoding of private and open information*. Let the achievable rate with opportunistic scheduling without any privacy constraint be $R_{\text{sum}}^{\text{opp}} = \mathbb{E}\left[\max_{j\in\{1,\ldots,n\}} R_j(k)\right]$. An outer bound for the achievable rate region for the sum rate can be characterized by: (i) $R_{\text{sum}}^{\text{priv}} + R_{\text{sum}}^{\text{open}} \leqslant R^M$; (ii) $R_{\text{sum}}^{\text{priv}} \leqslant \sum_{j=1}^n \left[p_j\left(R_j^M - R_j^m\right)\right]$.

IV. Network Control of Private Communications

In this section, we are going to present a dynamic control algorithm to opportunistically schedule the user nodes with the objective of maximizing total expected utility of the system while maintaining the stability of queues. In previous sections, achievable rate, and hence, the rate region is calculated based on the assumption that complete channel statistics are available. In reality, users usually only observe the instantaneous channel conditions. Hence, the scheduling decision should be based only on the instantaneous channel rates. In this section, we develop a dynamic algorithm that takes as an input the queue lengths and current channel rates between all users and their eavesdroppers, and selects a user and its mode of transmission, i.e., open or private.

Let $g_j^p(k)$ and $g_j^o(k)$ be the utilities obtained by user j from private and open transmission during block k respectively. The utility during each block k depends on the channel conditions and more specifically on the instantaneous private and open transmission rates $R_j^p(k)$, and $R_j^o(k)$. In general, this dependence can be described as $g_j^p(k) = U_j^p(R_j^p(k))$ and $g_j^o(k) = U_j^o(R_j^o(k))$. Assume that $U_j^p(0) = 0$ and $U_j^o(0) = 0$, and $U_j^p(\cdot)$ and $U_j^0(\cdot)$ are non-decreasing functions. We assume that the utility of a private transmission is higher than the utility of open transmission at the same rate.

The amount of open traffic $A_j^o(k)$, and private traffic $A_j^p(k)$ injected in the queues at node j have arrival rates λ_j^o and λ_j^p respectively. Our objective is to support a fraction of the traffic demand to achieve a long term secure and unsecure throughput that maximizes the sum of user utilities. We consider the solution of the following optimization problem:

$$\max \sum_{j=1}^{n} \left[\mathbb{E}\{g_j^p(k)\} + \mathbb{E}\{g_j^o(k)\}\right] \tag{16}$$

$$\text{subject to } (\lambda_j^o, \lambda_j^p) \in \Lambda \tag{17}$$

The cross-layer dynamic control algorithm discussed next is motivated by the work of [4]. We assume an infinite backlog of data at the transport layer of each node. The dynamic control algorithm determines the amount of open and private traffic injected into the queues at the network layer. The dynamics of private and open traffic queues is given as follows:

$$Q_j^p(k+1) = \left[Q_j^p(k) - \mathscr{I}_j^p(k)R_j^p(k)\right]^+ + A_j^p(k), \tag{18}$$

$$Q_j^o(k+1) = \left[Q_j^o(k) - \mathscr{I}_j^o(k)R_j^o(k)\right]^+ + A_j^o(k), \tag{19}$$

where $[x]^+ = \max\{0,x\}$, and $\mathscr{I}_j^p(k)$ and $\mathscr{I}_j^o(k)$ are indicator functions taking value $\mathscr{I}_j^p = 1$ when transmitting private or $\mathscr{I}_j^o = 1$ when transmitting open information respectively. Also note that at any block k, $\mathscr{I}_j^p(k) + \mathscr{I}_j^o(k) \leq 1$.

(1) Flow control: For some $V > 0$, at block k, each node j injects $A_j^p(k)$ private and $A_j^o(k)$ open bits, where

$$\left(A_j^p(k), A_j^o(k)\right) = \underset{A^p,A^o}{\text{argmax}} \left\{V\left[U_j^p(A^p) + U_j^o(A^o)\right] - \left(Q_j^p(k)A^p + Q_j^o(k)A^o\right)\right\}$$

(2) Scheduling: At block k, schedule node j and transmit private ($\mathscr{I}_j^p = 1$) or open ($\mathscr{I}_j^o = 1$) information, where

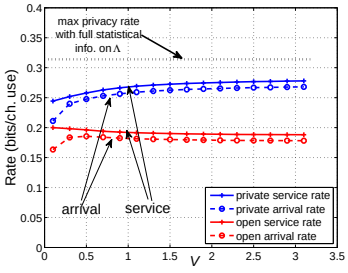
$$(\mathscr{I}_j^p(k), \mathscr{I}_j^o(k)) = \underset{\mathscr{I}^p,\mathscr{I}^o}{\text{argmax}} \left\{Q_j^p(k)R_j^p(k) + Q_j^o(k)R_j^o(k)\right\},$$

and for each node j, encode private data over each block k at rate

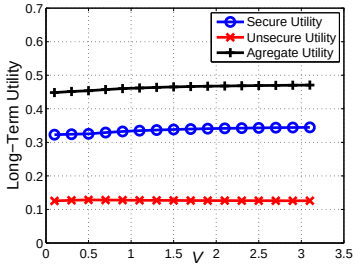
$$R_j^p(k) = \mathscr{I}_j^p(k)\left[R_j(k) - \max_{i\neq j} R_{ji}(k)\right],$$

and transmit open data at rate

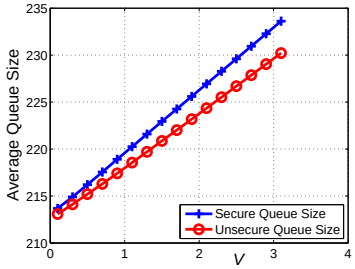
$$R_j^o(k) = \mathscr{I}_j^o(k)R_j(k) + \mathscr{I}_j^p(k)(R_j(k) - R_j^p(k))$$



(a) Arrival and service rates



(b) Long-term Utility



(c) Average queue length

Fig. 3. Simulation results

The optimality proof of the algorithm is similar in nature to that in [4] and is relegated to [8].

Theorem 2: If $R_j(k) < \infty$ for all j,k, then dynamic control algorithm satisfies:

$$\liminf_{N\to\infty} \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=1}^{n}\mathbb{E}\left[U_j^p(k)+U_j^o(k)\right] \geqslant U^* - \frac{B}{V}$$

$$\limsup_{N\to\infty} \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=1}^{n}\mathbb{E}\left[Q_j^p(k)\right] \leqslant \frac{B+V(\bar{U}-U^*)}{\varepsilon_1}$$

$$\limsup_{N\to\infty} \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=1}^{n}\mathbb{E}\left[Q_j^o(k)\right] \leqslant \frac{B+V(\bar{U}-U^*)}{\varepsilon_2},$$

where $B,\varepsilon_1,\varepsilon_2 > 0$ are constants, U^* is the optimal utility and $\bar{U}$ is the maximum possible utility.

V. Numerical Results

The performance of the proposed dynamic network control algorithm for private communications is evaluated in a 5-node system with Rayleigh block fading. The expected gain of the channel between the users and the base station is taken as $\bar{h}_j = 2$, and the expected gain between the transmitting user and the eavesdropper is taken as $\bar{h}_{ij} = 1$ for all (i,j). We assume that all channels are Gaussian as described in Section II and $P = 1$. The simulation is run for $N = 10^6$ blocks. In the simulations, we assume a linear utility function where the utility of private communication is twice the utility of open communication at the same rate, i.e., $U_j^p(\lambda_j^p) = 2\lambda_j^p$ and $U_j^o(\lambda_j^o) = \lambda_j^o$.

In Figure 3a, we depict the arrival and service rates of the private and open traffic for varying values of the system parameter V. For low values of V, the difference between the service rates and arrival rates are high, but this difference reduces as V increases. More importantly, we see that for increasing values of V private traffic service rate increases while the service rate of open traffic decreases. This is because the utility of private traffic is higher than the open traffic. Recall that the achievable rates are calculated when full statistical information was available, whereas in dynamic control algorithm all scheduling decisions are made according to instantaneous channel conditions. The penalty of not having the complete statistical information is also depicted in Figure 3a. In this example, the maximum achievable privacy rate is 0.31 while the maximum privacy rate of the dynamic control algorithm is 0.28.

Figure 3b depicts the change in the long-term private, open and total utility with respect to increasing values of V. As expected, higher total utility is attained for increasing values of V; however, as shown in Figure 3c, this comes at a price of longer queue lengths at the nodes.

VI. Conclusions and Future Work

In this paper, we obtained the achievable privacy rate region of single- and multi-user wireless systems using opportunistic scheduling when full CSI information of the neighbors was available. Then, we described a cross-layer dynamic algorithm that works without prior distribution of channel gains, and state a theorem showing that the algorithm achieves utility arbitrarily close to achievable optimal utility. The simulation results also verify the efficacy of the algorithm.

As a future direction, we will consider the case when partial CSI is available at each node, and we will also consider scheduling in the downlink.

References

[1] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y. Kim. The secrecy capacity of the wiretap channel with rate-limited feedback. *IEEE Trans. Inform. Theory*, 2009. To appear.

[2] J. Barros and M. R. D. Rodrigues. Secrecy capacity of wireless channels. In *Proc. IEEE Int. Symposium Inform. Theory*, pages 356–360, Seattle, WA, July 2006.

[3] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inform. Theory*, 24(3):339–348, May 1978.

[4] L. Georgiadis, M. J. Neely, and L. Tassiulas. Resource allocation and cross-layer control in wireless networks. *Found. Trends Netw.*, 1:1–144.

[5] P. K. Gopala, L. Lai, and H. El Gamal. On the secrecy capacity of fading channels. *IEEE Trans. Inform. Theory*, 54(10):4687–4698, 2008.

[6] D. Gunduz, R. Brown, and H. V. Poor. Secret communication with feedback. In *Proc. IEEE Intl. Symposium on Information Theory and its Applications*, Auckland, New Zealand, Dec. 2008.

[7] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas: The MISOME wiretap channel. *IEEE Trans. Inform. Theory*, 2009. To appear.

[8] C. E. Koksal and O. Ercetin. Control of wireless networks with secrecy. Technical report, The Ohio State University, 2010.

[9] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inform. Theory*, 54(9):4005–4019, Sept. 2008.

[10] L. Lai, H. El Gamal, and H. V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. Inform. Theory*, 54(11):5059 – 5067, Nov. 2008.

[11] Y. Liang, H. V. Poor, and S. Shamai (Shitz). Secure communication over fading channels. *IEEE Trans. Inform. Theory*, 54(6):2470–2492, June 2008.

[12] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inform. Theory*, Oct. 2007. Submitted.

[13] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inform. Theory*, 54(12):5747 – 5755, Dec. 2008.