Wireless Broadcast Networks: Reliability, Security, and Stability

Yingbin Liang, H. Vincent Poor, Lei Ying

***Abstract*— A secure wireless broadcast network model is investigated, in which a source node broadcasts K confidential message flows to N user nodes, with each message intended to be decoded accurately by one user and to be kept secret from all of other users (who are thus considered to be eavesdroppers with regard to all other messages but their own). The source maintains a queue for each message flow if it is not served immediately. The channel from the source to the K users is modelled as a fading broadcast channel, and the channel state information is assumed to be known to all nodes. Two eavesdropping models are considered. For a collaborative eavesdropping model, in which the eavesdroppers exchange their outputs, the secrecy capacity region is obtained, within which each rate vector is achieved by using a time-division scheme and a source power control policy over channel states. A throughput optimal queue length based scheduling algorithm is further derived that stabilizes all arrival rate vectors contained in the secrecy capacity region. At each packet time slot, the queue length vector determines the power control policy over the channel states at the source, and hence determines the secrecy rate allocation among users. For a non-collaborative model, in which eavesdroppers do not exchange their outputs, the time-division scheme provides an achievable secrecy rate region, and the queue length based scheduling algorithm stabilizes all arrival rate vectors in this region.**

I. Introduction

Wireless broadcast networks constitute one class of basic and important wireless networks, where a source node simultaneously transmits a number of information flows (messages) to different destinations. Three important and challenging issues need to be addressed for wireless broadcast networks: reliability, security and stability. These three issues have been separately studied for wireless broadcast networks in previous work. Reliability requires that each information flow is received correctly at intended corresponding destinations, and the capacity region that includes all achievable rate vectors (rate allocation among users) has been studied in, e.g, [1]–[3]. Following the seminal work of [4], [5], secure communication via the physical layer has been applied to study wireless broadcast networks in [6], [7], where reliability and security are jointly studied. A queue-length based scheduling algorithm that achieves the network throughput region was first proposed in [8]. Subsequently, network stability has also been studied jointly with reliability via the capacity region of wireless networks in, e.g., [9], [10].

Although jointly considering the above three issues has the potential for significant impact in improving network performance and resource efficiency, this perspective has not been examined before. One reason is because the physical layer approach to achieve security, which quantifies the measure of secrecy and greatly facilitates this joint design, has attracted considerable attention only recently. This joint design is the goal of this paper.

In this paper, we study a broadcast network (see Fig.1), in which a source node transmits K confidential message flows to K user nodes, and each message flow is intended to be decoded accurately by one node and is to be kept secret from all other nodes. Nodes are thus considered to be eavesdroppers with regard to all other messages but their own. We consider two eavesdropping models. The first one is referred to as a collaborative eavesdropping model, in which the eavesdroppers can exchange their outputs to interpret the message. The second one is referred to as a non-collaborative eavesdropping model, in which eavesdroppers do not exchange their outputs. We assume that the source maintains a queue for each message flow if it is not served immediately. Each queue needs to remain stochastically stable so that no queue length builds up to infinity.

We assume that the channel from the source to the K users is a fading broadcast channel, in which the channel outputs at each user are corrupted by a multiplicative fading gain process in addition to an additive white Gaussian noise process. We assume that the channel state information (channel gain realization) is known to all nodes. There are two time scales (see Fig.2): one is at symbol time level and the channel state varies across symbol times, the other is at packet time level, which spans a large number of symbol times during which the channel state behaves ergodically.

To achieve reliable and secure communication for users, we adopt the physical layer approach [4], [5] to employ a stochastic encoder at the source node. The source node allocates its power not only among message flows (i.e., among users) but also dynamically according to channel state information to improve secure communication rates. Hence the source power control is over the symbol time scale, and determines the service rate allocation among users at the packet time level. Furthermore, to maintain the stability of all queues, the source needs to adapt its service rate allocation (scheduling) dynamically among users according to the queue lengths. Hence the scheduling is over the packet time level. Our goal is to study how to jointly design

The work of Y. Liang and H. V. Poor was supported by the National Science Foundation under Grants ANI-03-38807, CNS-06-25637 and CCF-07-28208.

Yingbin Liang is with the Department of Electrical Engineering, University of Hawaii at Manoa, Holmes Hall, 2540 Dole Street, Honolulu, HI 96822, USA yingbinl@hawaii.edu

H. Vincent Poor is with the Department of Electrical Engineering, Princeton University, E-Quad, Olden Street, Princeton, NJ 08544, USA poor@princeton.edu

Lei Ying is with the Department of Electrical and Computer Engineering, Iowa State University, 3219 Coover Hall, Ames, IA 50011, USA leiying@iastate.edu

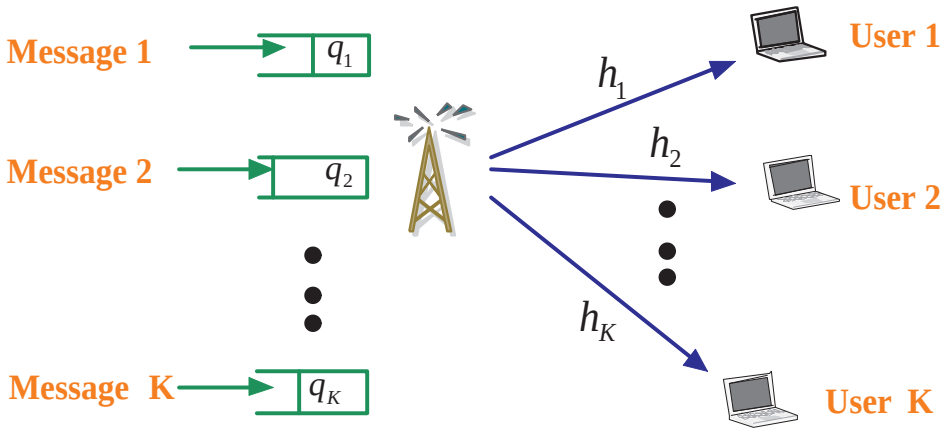

Fig. 1. Fading broadcast network

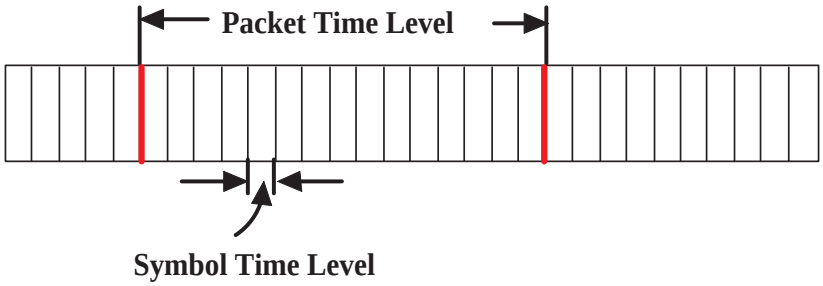

Fig. 2. Two time scales

scheduling at the packet time level and power control at the symbol time level to achieve network reliability, security and stability.

For the collaborative eavesdropping model, we obtain the secrecy capacity region, within which each rate vector can be achieved by a time-division scheme, i.e., at each channel state, the source transmits only to the user whose channel gain is better than the sum of the channel gains of all other users. It is clear that this user must have the best channel gain at this state. The power control among the channel states thus determines the rate allocation among users, i.e., rate allocation among components of a rate vector. We further show that all arrival rate vectors contained in this region can be stabilized by a throughput optimal queue-length based scheduling scheme at the packet time level, where queue length determines the service rate allocation among users, and hence determines the corresponding power control to achieve this service rate vector at the symbol time level. For the non-collaborative eavesdropping model, we study a time-division scheme, where the source transmits to the user with the best channel gain at each channel state. Although this time-division scheme may be suboptimal, it is simple and important from a practical point of view. We obtain an achievable secrecy rate region, and a queue length based scheduling algorithm that stabilizes the arrival rate vectors contained in this region.

The rest of the paper is organized as follows. In Section II, we introduce the channel model of interest. In Section III and IV, we present our results for the collaborative eavesdropping model and the non-collaborative eavesdropping model, respectively. In Section V, we conclude the paper with a few remarks.

II. Channel Model

We consider the K-user fading broadcast network (see Fig. 1), in which a source node transmits K confidential messages to K user nodes. Each message is intended for one user and needs to be kept secret from all other nodes. Hence, with regard to one message, all users other than its intended receiver are considered to be eavesdroppers.

We assume the channel from the source node to the K users is a fading broadcast channel, in which the channel outputs at each user are corrupted by a multiplicative fading gain process in addition to an additive white Gaussian noise process. The channel input-output relationship is given by

$$Y_{in} = h_{in}X_n + w_{in} \quad \text{for} \quad 1 \le i \le K \qquad (1)$$

where i denotes the ith user, n denotes the nth symbol time instant. At the symbol time instant n, X_n is the channel input from the source, Y_{in} is the channel output at user i, h_{in} is the source-to-user i channel gain coefficient, and w_{in} is the noise term at user i. We define $\underline{h}_n := (h_{1n}, \ldots, h_{Kn})$, and assume $\{\underline{h}_n\}_{n=1}^{\infty}$ is a stationary and ergodic vector proper

complex random process. We assume that the channel state information (i.e., the realization of $\underline{h}_n$) is known at both the source node and all user nodes. The noise processes $\{w_{in}\}_{n=1}^{\infty}$ for $i = 1, \ldots, K$ are independent identically distributed (i.i.d.) proper complex Gaussian processes with zero means and unit variances. The input sequence $\{X_n\}$ is subject to the average power constraint P, i.e.,

$$\frac{1}{N}\sum_{n=1}^{N} \mathrm{E}\left[X_n^2\right] \leq P$$

.

A $\left(2^{nR_1}, \ldots, 2^{nR_K}, n\right)$ code consists of the following:

- K message sets: $\mathcal{W}_i = \{1, 2, \ldots, 2^{nR_i}\}$ for $i = 1, \ldots, K$ with each message W_i uniformly distributed over the set $\mathcal{W}_i$, respectively;
- One (stochastic) encoder at the source node that maps each message vector $(w_1, \ldots, w_K) \in (\mathcal{W}_0, \ldots, \mathcal{W}_K)$ to a codeword x^n; and
- K decoders: each at one user node that maps a received sequence y_i^n to a message $\hat{w}_i \in \mathcal{W}_i$ for $i = 1, \ldots, K$.

In this paper, we study two eavesdropping models. The first model is referred to as the *collaborative eavesdropping model*, which assumes that all eavesdroppers collaborate and exchange their outputs to interpret a destination's message. As in [4], the secrecy level of the confidential message W_i is measured by the following *equivocation rate*

$$R_{e,i} \leq \liminf_{n\to\infty} \frac{1}{n} H\left(W_i \middle| Y_1^n, \ldots, Y_{i-1}^n, Y_{i+1}^n, \ldots, Y_K^n\right). \tag{2}$$

In this paper, we focus on the case of perfect secrecy, in which the eavesdroppers do not obtain any information about the messages. This happens if

$$R_{e,i} = R_i \tag{3}$$

for $i = 1, \ldots, K$.

The second model is referred to as the *non-collaborative model*, which assumes that the eavesdroppers do not exchange their outputs. For this model, the secrecy level of the confidential message W_i at user j is measured by the following equivocation rate

$$R_{e,ij} \leq \liminf_{n\to\infty} \frac{1}{n} H\left(W_i \middle| Y_j^n\right). \tag{4}$$

In the case of perfect secrecy, we have

$$R_{e,ij} = R_i \tag{5}$$

for $j \neq i,\ 1 \leq j \leq K$ and $i = 1, \ldots, K$.

A rate vector $(R_1, \ldots, R_K)$ is *achievable* if there exists a sequence of $\left(2^{nR_1}, \ldots, 2^{nR_K}, n\right)$ codes such that the average probability of error goes to zero as n goes to infinity and perfect secrecy is achieved for each message.

The *secrecy capacity region* $\mathcal{C}_s$ is defined to be the set that includes all achievable rate vectors $(R_1, \ldots, R_K)$ such that perfect secrecy can be achieved. Since the source node has access to the channel state information, the source can dynamically change its transmission power to achieve better performance as the channel state varies at the symbol time level. Each rate vector in the secrecy capacity region corresponds to one power control policy at the source. Hence the power control policy determines the service rate allocation among users.

We assume that the source maintains one queue for each message flow if it is not served immediately. The arrivals of the message flows are on the packet time scale, and are assumed to be random and independent of each other. We use $\underline{a}[t]$ to denote an arrival rate vector at packet time slot t, with each component representing the arrive rate of one queue at packet time slot t. The system is *stochastically stable* if no queue builds to infinity (see formal definition in [8, Def. 3.1]). We use the vector $\underline{q}[t] = (q_1[t], \ldots, q_K[t])$ to denote the queue length vector at packet time slot t, with each component $q_i[t]$ denoting the queue length for the ith queue. We note that each packet time slot contains a large number of the symbol time slots, during which the channel state changes in a stationary and ergodic manner. For each packet time slot, the scheduling at the source node is accomplished by choosing an achievable secrecy rate vector as a service rate vector. The stability region is defined to include all arrival rate vectors that can be stabilized by a scheduling algorithm. Our goal in the following is to jointly design a scheduling algorithm at the packet time level and a power control policy at the symbol time level to achieve reliable and perfectly secure communication for all users, and at the same time to maintain the queues of all message flows stochastically stable.

III. Collaborative Eavesdropping Model

In this section, we consider the collaborative eavesdropping model, in which for a given message, all users (eavesdroppers) other than the intended destination can exchange their outputs to try to decode a given message. Thus, for each channel state, only a user whose channel gain is larger than the sum of the channel gains of all other users (eavesdroppers) can receive its message with perfect secrecy. Note that such a user may not exist. It is clear that this user must have the best channel state among all users. This suggests a time-division scheme with the source transmitting to at most one user in each channel state (or at the corresponding symbol time slot).

For a given channel state $\underline{h} = (h_1, \ldots, h_K)$, let $p(\underline{h})$ denote the source power allocation for state $\underline{h}$. We use $\mathcal{P}$ to denote the set that includes all power allocation functions (or power control policies) that satisfy the power constraints, i.e.,

$$\mathcal{P} = \{p(\underline{h}) : \mathrm{E}[p(\underline{h})] \leq P\} \tag{6}$$

Now let $\mathcal{A}_i$ be the set of all channel states for which the channel gain of user i is larger than the sum of the channel gains of all other users, i.e.,

$$\mathcal{A}_i = \left\{ \underline{h} : |h_i|^2 \geq \sum_{j\neq i, 1\leq j\leq K} |h_j|^2 \right\}. \tag{7}$$

The following theorem states that a time-division scheme is optimal to achieve secrecy capacity region.

***Theorem** 1:* For the collaborative eavesdropping model, the secrecy capacity region of the fading broadcast network is given by

$$\mathcal{C}_s = \bigcup_{p(\underline{h})\in\mathcal{P}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i \le \mathrm{E}_{\underline{h}\in A_i}\Big[\log\Big(1+p(\underline{h})|h_i|^2\Big) \\ \qquad\qquad -\log\Big(1+p(\underline{h})\sum\limits_{j\neq i,1\le j\le K}|h_j|^2\Big)\Big] \\ \text{for} \quad 1\le i\le K \end{array} \right\} \tag{8}$$

where the random vector $\underline{h}=(h_1,\ldots,h_K)$ has the same distribution as the marginal distribution of the random process $\{\underline{h}_n\}_{n=1}^{\infty}$ at one symbol time instant.

Proof: See Appendix I. ■

***Remark** 1:* It is clear from (8) that no power is allocated to channel states that are not contained in any of the sets $\mathcal{A}_i$ for $i=1,\ldots,K$, because no user can obtain perfect secrecy over these states.

***Remark** 2:* In Theorem 1, only ergodicity and stationarity are assumed for the fading process $\{\underline{h}_n\}_{n=1}^{\infty}$, which can be correlated across time and across components, and is not necessarily Gaussian.

***Remark** 3:* Each rate vector contained in the secrecy capacity region given in (8) is achieved by a certain power control policy over the symbol time slots. It also represents average service rates for users over a large number of fading states and hence at the packet time level.

The secrecy capacity region given in Theorem 1 includes all achievable secrecy rate vectors with each component representing the service rate for one user. It still remains to determine a scheduling algorithm to choose a service rate vector at each packet time slot to stabilize all queues and to determine a power control policy over the symbol time slots to achieve this service rate vector. The scheduling algorithm and the power allocation policy are given in the following two theorems, respectively.

***Theorem** 2:* For the collaborative eavesdropping model, the network is stable only if the arrival rate vector is in the secrecy capacity region given in (8), i.e., $E[\underline{a}[t]]\in\mathcal{C}_s$. Furthermore, given any arrival rate vector $\underline{a}[t]$ that satisfies $\mathrm{E}[\underline{a}[t]]+\underline{\epsilon}\in\mathcal{C}_s$ ($\underline{\epsilon}$ denotes a K dimensional vector with all components equal to ϵ), the system is stochastically stable under the following queue-based algorithm: for any given queue length vector $\underline{q}[t]$, the secrecy rate vector $\underline{R}[t]$ is chosen to be a solution to the following optimization problem:

$$\max_{(R_1,\ldots,R_K)\in\mathcal{C}_s} q_1[t]R_1+\cdots+q_K[t]R_K \tag{9}$$

Proof: See Appendix II. ■

***Remark** 4:* Since the queue length based algorithm given in Theorem 2 stabilizes any arrival rate vector inside the secrecy capacity region, it is referred to the *secrecy throughput optimal scheduling scheme*.

***Theorem** 3:* For the collaborative eavesdropping model, the power control policy that achieves the secrecy rate vector for the queue length based algorithm given in Theorem 2 is given as follows. For a given queue length vector $\underline{q}[t]$,

$$p(\underline{h}) = \left\{ \begin{array}{ll} \Bigg(\frac{1}{2}\sqrt{\frac{1}{\sum\limits_{j\neq i,1\le j\le K}|h_j|^2}-\frac{1}{|h_i|^2}} \\ \quad\times\sqrt{\frac{1}{\sum\limits_{j\neq i,1\le j\le K}|h_j|^2}+\frac{4q_i[t]}{\lambda\ln 2}-\frac{1}{|h_i|^2}} \\ \quad-\frac{1}{2}\left(\frac{1}{|h_i|^2}+\frac{1}{\sum\limits_{j\neq i,1\le j\le K}|h_j|^2}\right)\Bigg)^+, & \text{if } \underline{h}\in\mathcal{A}_i \\ 0, & \text{otherwise} \end{array} \right. \tag{10}$$

where λ is chosen to satisfy the power constraint given in (6).

Proof: See Appendix III. ■

***Remark** 5:* It can be seen from (10) that more power may be allocated to user i to increase its service rate and stabilize its queue when its queue length increases.

IV. Non-Collaborative Eavesdropping Model

In this section, we consider the non-collaborative eavesdropping model, in which for a given message, all users (eavesdroppers) other than its intended destination do not exchange their outputs. For this given message, the channel can be viewed as the wire-tap channel with multiple eavesdroppers [11] or with one eavesdropper whose channel to the source is a compound channel [12]. For this model, if we consider one message, say message 1, then an achievable secrecy rate is given by [11], [12]

$$R_1 = \min_{2\le j\le K} \mathrm{E}_{\underline{h}\in\mathcal{A}_1}\Big[\log\Big(1+p(\underline{h})|h_1|^2\Big)-\log\Big(1+p(\underline{h})|h_j|^2\Big)\Big] \tag{11}$$

where $\mathcal{A}_1$ is the set that includes all channel states for which the source allocates a positive amount of power.

From (11), the secrecy rate of user 1 is minimal over the secrecy rates achieved with regard to all eavesdroppers. It is clear that for a given channel state in which user 1's channel is not the best among users, if the source assigns a positive amount of power to transmit message 1, then there is a loss in secrecy rates with regard to those eavesdroppers whose channels are better than that of user 1, and there is a gain in secrecy rates with regard to those eavesdroppers whose channels are worse than that of user 1. Hence, there may be a gain in the overall secrecy rate of user 1 if the source allocates power to transmit message 1 when user 1's channel is not the best.

Now when we consider all K messages, a more general scheme is to assign power to send all messages except the one with the worst channel at any channel state. Hence in contrast to the collaborative eavesdropping model, a time-division scheme that transmits only to one user with the best channel at each channel state is suboptimal. However, the more general scheme involves complicated stochastic

superposition coding and may not be useful for practical wireless broadcast networks. Moreover, the optimal control policy may not be easy to find either. Therefore, we focus on a time-division scheme, which may not be optimal, but is simple and easy for practical design.

We define the set $\mathcal{A}_i$ to include all channel states with user i having the best channel state among users, i.e.,

$$\mathcal{A}_i = \left\{\underline{h} : |h_i|^2 \geq |h_j|^2 \ \ \forall j \neq i, 1 \leq j \leq K\right\}. \qquad (12)$$

The following theorem provides an achievable secrecy rate region based on a time-division scheme.

***Theorem** 4:* For the non-collaborative eavesdropping model, an achievable secrecy rate region for the fading broadcast channel is given by

$$\mathcal{R}_s = \bigcup_{p(\underline{h})\in\mathcal{P}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i \leq \min\limits_{j\neq i, 1\leq j\leq K} \mathrm{E}_{\underline{h}\in A_i}\Big[\log\left(1+p(\underline{h})|h_i|^2\right) \\ \qquad\qquad - \log\left(1+p(\underline{h})|h_j|^2\right)\Big] \\ \text{for} \quad 1\leq i\leq K \end{array} \right\} \qquad (13)$$

where the random vector $\underline{h} = (h_1,\ldots,h_K)$ has the same distribution as the marginal distribution of the random process $\{\underline{h}_n\}$ at one symbol time instant.

Proof: For each channel state, the source transmits only to the user with the best channel state, and hence the channel is the wire-tap channel with multiple wire-tappers. The achievable secrecy rate follows directly from the proof in [12]. ■

***Remark** 6:* It is easy to see that the region $\mathcal{R}_s$ given in (13) is larger than the region $\mathcal{C}_s$ given in (8), because the eavesdroppers are less powerful in the non-collaborative eavesdropping model than in the collaborative eavesdropping model.

We also derive an outer bound on the secrecy capacity region, which is given in the following theorem.

***Theorem** 5:* For the non-collaborative eavesdropping model, an outer bound on the secrecy capacity region of the fading broadcast channel is given by

$$\bar{\mathcal{R}}_s = \bigcup_{p(\underline{h})\in\mathcal{P}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i \leq \min\limits_{j\neq i, 1\leq j\leq K} \mathrm{E}_{\underline{h}\in \bar{\mathcal{A}}_{ij}}\Big[\log\left(1+p(\underline{h})|h_i|^2\right) \\ \qquad\qquad - \log\left(1+p(\underline{h})|h_j|^2\right)\Big] \\ \text{for} \quad 1\leq i\leq K \end{array} \right\} \qquad (14)$$

where

$$\bar{\mathcal{A}}_{ij} = \left\{\underline{h} : |h_i|^2 \geq |h_j|^2\right\}. \qquad (15)$$

Proof: The $K-1$ bounds in (14) for $i=1$ follow the steps that are similar to those in Appendix I by replacing $Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L}$ with $Y^n_{21},\ldots,Y^n_{KL}$, respectively. The rest follows by symmetry. ■

It can be seen that the gap between the inner bound given in (13) and the outer bound given in (14) lies in the different sets over which the expectation of the secrecy rate is taken. For the inner bound, the expectation of the secrecy rate for user i is taken over the set $\mathcal{A}_i$ given in (12), in which user i has the best channel among users. However, for the outer bound, the expectation is taken over the set $\bar{\mathcal{A}}_{ij}$ given in (15), in which user i has a better channel than user j (eavesdropper). This suggests there is potential to improve the secrecy rate for user i if the source transmits to user i when its channel is not the best among all users.

***Theorem** 6:* For the non-collaborative eavesdropping model, if the arrival rate vector $\underline{a}[t]$ satisfies $\mathrm{E}[\underline{a}[t]]+\underline{\epsilon}\in\mathcal{R}_s$ given in (13), then the system is stochastically stable under the following queue-based algorithm: for any given queue length vector $\underline{q}[t]$, the secrecy rate vector $\underline{R}[t]$ is chosen to be a solution to the following optimization problem:

$$\max_{(R_1,\ldots,R_K)\in\mathcal{C}_s} q_1[t]R_1 + \cdots + q_K[t]R_K. \qquad (16)$$

The corresponding power control policy that achieves the secrecy rate vector $\underline{R}[t]$ in the preceding algorithm is the solution to the following optimization problem:

$$\max_{p(\underline{h})\in\mathcal{P}} \Big[q_1[t] \min_{j\neq 1, 1\leq j\leq K}\{R_{1j}(\underline{h})\} + \cdots + q_K[t] \min_{j\neq K, 1\leq j\leq K}\{R_{K,j}(\underline{h})\}\Big]. \qquad (17)$$

V. Conclusions

In this paper, we have studied wireless broadcast networks, for which we have obtained the secrecy capacity region for the collaborative eavesdropping model and inner and outer bounds on the secrecy capacity region for the non-collaborative eavesdropping model. We have further obtained a secrecy throughput optimal scheduling scheme and a corresponding jointly optimal power control policy for the collaborative eavesdropping model. To the authors' best knowledge, this is the first work that addresses the reliability, security (via a physical layer approach), and stability jointly for wireless broadcast networks. The approach in this paper can be applied to analyze other wireless networks including multi-access, interference and relay networks. This approach also allows the incorporation of public and common message flows for users in the system as well.

Appendix I
Proof of Theorem 1

Proof of Achievability For a given fading state $\underline{h}\in\mathcal{A}_i$, the ith message is transmitted to user i. Since the eavesdroppers can exchange their outputs, they can be viewed as a super-eavesdropper that has K receive antennas with each antenna receiving the outputs of one eavesdropper. Now the channel is equivalent to the wire-tap channel [4] with the wire-tapper having multiple antennas. Hence the following secrecy rate

is achievable in channel state $\underline{h}$:

$$R_i(\underline{h}) = \log\left(1+p(\underline{h})|h_i|^2\right) - \log\left(1+p(\underline{h})\sum_{j\neq i, 1\leq j\leq K}|h_j|^2\right) \quad (18)$$

Thus, the rate achievable for user i is an average of the rate $R_i(\underline{h})$ over all channel states $\underline{h}\in\mathcal{A}_i$, which provides the rate R_i given in (8).

Proof of Converse To show the converse, we consider the parallel broadcast channel with L subchannels indexed by $l=1,\ldots,L$. Each subchannel is a broadcast channel with one input X_l and K outputs Y_{il} for $i=1,\ldots,K$. In fact, the parallel broadcast channel is equivalent to a fading broadcast channel with the channel state $\underline{h}$ taking finite equiprobable states indexed by $l=1,\ldots,L$. Each subchannel of the parallel broadcast channel corresponds to one channel state of the fading broadcast channel. Extending our proof to the case when $\underline{h}$ has continuous state space is standard.

For the parallel broadcast channel, we consider a code $\left(2^{nR_1},\ldots,2^{nR_K},n\right)$ with average error probability P_e, where P_e approaches zero as n approaches infinity.

We now bound the rate R_1 and obtain:

$$\begin{aligned}
nR_1 &\overset{(a)}{=} nR_{1e} \overset{(b)}{\leq} H\left(W_1|Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L}\right)\\
&\leq I(W_1;Y^n_{[1,K]1},\ldots,Y^n_{[1,K]L})\\
&\quad - I(W_1;Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L})\\
&\quad + H\left(W_1|Y^n_{[1,K]1},\ldots,Y^n_{[1,K]L}\right)\\
&\overset{(c)}{\leq} I(W_1;Y^n_{11},\ldots,Y^n_{1L}|Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L})+n\delta\\
&\leq I(W_1,X^n_1,\ldots,X^n_L;Y^n_{11},\ldots,Y^n_{1L}|Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L})\\
&\quad + n\delta\\
&\overset{(d)}{\leq} I(X^n_1,\ldots,X^n_L;Y^n_{11},\ldots,Y^n_{1L}|Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L})+n\delta\\
&=\\
&\sum_{l=1}^{L} I(X^n_1,\ldots,X^n_L;Y^n_{1l}|Y^n_{11},\ldots,Y^n_{1l-1},Y^n_{[2,K]1},\ldots,Y^n_{[2,K]L})\\
&+n\delta\\
&\leq \sum_{l=1}^{L} H(Y^n_{1l}|Y^n_{[2,K]l}) - H(Y^n_{1l}|X^n_l,Y^n_{[2,K]l})+n\delta\\
&= \sum_{l=1}^{L} I(X^n_l;Y^n_{1l}|Y^n_{[2,K]l})+n\delta
\end{aligned} \quad (19)$$

where $Y^n_{[2,K]L}$ denotes the vector sequence $(Y^n_{2L},\ldots,Y^n_{KL})$. In the preceding equation, (a) follows from the perfect secrecy condition, (b) follows from the definition of the equivocation rate given in (2), (c) follows from Fano's inequality such that

$$H\left(W_1|Y^n_{[1,K]1},\ldots,Y^n_{[1,K]L}\right)\leq nR_1P_e+1:=n\delta \quad (20)$$

where $\delta\to 0$ if $P_e\to 0$, and (d) follows because given $(X^n_1,\ldots,X^n_L)$, $(Y^n_{[1,K]1},\ldots,Y^n_{[1,K]L})$ is independent of W_1.

For each l, we can apply the converse proof in [13] or [14] to obtain

$$\begin{aligned}
&I(X^n_l;Y^n_{1l}|Y^n_{[2,K]l})\\
&\leq \left(n\log\left(1+p(\underline{h})|h_1|^2\right)\right.\\
&\qquad \left. - n\log\left(1+p(\underline{h})\sum_{2\leq j\leq K}|h_j|^2\right)\right)^+
\end{aligned} \quad (21)$$

if subchannel l corresponds to the fading state $\underline{h}$, and the power $p(\underline{h})$ is allocated to this subchannel. It is clear that only those l whose corresponding $\underline{h}\in\mathcal{A}_1$ contribute to the secrecy rate R_1 in (19), and hence the average needs to be taken only over $\underline{h}\in\mathcal{A}_1$ in (8). Following the same steps as above, we can obtain the bounds on the rates $R_2,\ldots,R_K$, which concludes the proof.

Appendix II
Proof of Theorem 2

We first note that since $\mathcal{C}_s$ given in (8) is the secrecy capacity region, it is clear that the network cannot be stabilized if $\mathrm{E}(a[t])\notin\mathcal{C}_s$. We next use the idea proposed in [8] to establish stability. We define the following Lyapunov function

$$V[t]=\sum_{i=1}^{K}\left(q_i[t]\right)^2.$$

We also define

$$\Delta q_i[t]=q_i[t+1]-q_i[t].$$

We further define and derive the drift of $V[t]$ as follows.

$$\begin{aligned}
&\mathrm{E}[\Delta V[t]\mid \underline{q}[t]]\\
&:=\mathrm{E}[V[t+1]-V[t]\mid \underline{q}[t]]\\
&=\mathrm{E}\left[\sum_{i=1}^{K}\left(\left(q_i[t]+\Delta q_i[t]\right)^2-\left(q_i[t]\right)^2\right)\middle|\underline{q}[t]\right]\\
&=\mathrm{E}\left[\sum_{i=1}^{K}\left(\left(\Delta q_i[t]\right)^2+2\Delta q_i[t]q_i[t]\right)\middle|\underline{q}[t]\right]\\
&=\mathrm{E}\left[\sum_{i=1}^{K}\left(\Delta q_i[t]\right)^2+2\sum_{i=1}^{K}q_i[t]\left(a_i[t]-R_i[t]+u_i[t]\right)\middle|\underline{q}[t]\right]\\
&=\mathrm{E}\left[\sum_{i=1}^{K}\left(\Delta q_i[t]\right)^2+2\sum_{i=1}^{K}q_i[t]u_i[t]\right.\\
&\qquad\left.+2\sum_{i=1}^{K}q_i[t]\left(a_i[t]-R_i[t]\right)\middle|\underline{q}[t]\right],
\end{aligned} \quad (22)$$

where $u_i[t]$ denotes the unused service rate due to the lack of packets in queue i.

Let $a_{\max}$ denote the maximum number of arrivals in one time slot, $R_{\max}$ denote the maximum rate achievable in one time slot, and $\eta_{\max}=\max\{a_{\max},R_{\max}\}$. Note that $u_i[t]=0$ if $q_i[t]\geq\eta_{\max}$, and hence

$$q_i[t]u_i[t]\leq\eta^2_{\max},$$

and

$$\mathrm{E}[\Delta V[t]|\underline{q}[t]] \leq 3K\eta_{\max}^2 + 2\sum_{i=1}^{K} q_i[t]\left(\mathrm{E}[a_i[t]] - R_i[t]\right). \tag{23}$$

Now given that $\mathrm{E}[\underline{a}[t]]+\underline{\epsilon} \in \mathcal{C}_s$, there exists $\underline{R}^* \in \mathcal{C}_s$ such that

$$\mathrm{E}[a_i[t]] + \epsilon \leq R_i^*. \tag{24}$$

Thus, we have

$$\begin{aligned}
&\mathrm{E}[\Delta V[t]|\mathbf{q}[t]] \\
&\leq 3K\eta_{\max}^2 + 2\sum_{i=1}^{K} q_i[t]\left(\mathrm{E}[a_i[t]] - R_i^*\right) \\
&\qquad + 2\sum_{i=1}^{K} q_i[t]\left(R_i^* - R_i[t]\right) \\
&\overset{(a)}{\leq} 3K\eta_{\max}^2 - 2\epsilon\sum_{i=1}^{K} q_i[t] + 2\sum_{i=1}^{K} q_i[t]\left(R_i^* - R_i[t]\right) \\
&\overset{(b)}{\leq} 3K\eta_{\max}^2 - 2\epsilon\sum_{i=1}^{K} q_i[t],
\end{aligned} \tag{25}$$

where (a) follows from (24), and (b) follows from the definition of the queue length based algorithm that $R_i[t]$ for $i = 1, \ldots, K$ is a solution to the optimization problem given in (9).

Therefore, we conclude that $\mathrm{E}[\Delta V[t]|\mathbf{q}[t]] < 0$ if $\sum_i q_i[t] > 3K\eta_{\max}^2$. Since $\underline{q}[t]$ is Markovian, the system is stochastically stable according to the Foster-Lyapunov criterion [15].

Appendix III
Proof of Theorem 3

From (9), we obtain

$$\begin{aligned}
&\max_{(R_1,\ldots,R_K)\in\mathcal{C}_s} q_1[t]R_1 + \cdots + q_K[t]R_K \\
&= \max_{p(\underline{h})\in\mathcal{P}} q_1[t]R_1(p(\underline{h})) + \cdots + q_K R_K(p(\underline{h}))
\end{aligned} \tag{26}$$

where R_i for $i = 1, \ldots, K$ are given in (8). The Lagrangian to solve the preceding convex optimization problem is given by

$$\begin{aligned}
\mathcal{L} = \sum_{i=1}^{K} q_i[t]\mathrm{E}_{\underline{h}\in A_i}\Bigg[&\log\left(1 + p(\underline{h})|h_i|^2\right) \\
&- \log\left(1 + p(\underline{h})\sum_{j\neq i, 1\leq j\leq K}|h_j|^2\right)\Bigg] - \lambda(\mathrm{E}_{\underline{h}}p(\underline{h}) - P)
\end{aligned} \tag{27}$$

where λ is a Lagrange multiplier.

For $\underline{h} \in \mathcal{A}_i$, the optimal $p(\underline{h})$ satisfies the following necessary and sufficient condition:

$$\frac{\partial\mathcal{L}}{\partial p(\underline{h})} = \frac{q_i[t]}{\ln 2}\frac{1}{\frac{1}{|h_i|^2} + p(\underline{h})} - \frac{q_i[t]}{\ln 2}\frac{1}{\frac{1}{\sum_{j\neq i, 1\leq j\leq K}|h_j|^2} + p(\underline{h})} \leq \lambda \tag{28}$$

with equality when $p(\underline{h}) = 0$. The power control policy $p(\underline{h})$ in (10) can then be obtained by simple algebra.

References

[1] D. N. Tse, "Optimal power allocation over parallel Gaussian broadcast channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Ulm, Germany, June 1997, p. 27.

[2] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels-Part I: Ergodic capacity," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1083–1102, Mar. 2001.

[3] ——, "Capacity and optimal resource allocation for fading broadcast channels-Part II: Outage capacity," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1103–1127, Mar. 2001.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," to appear in *IEEE Trans. Inform. Theory, Special Issue on Information Theoretic Security*, vol. 54, no. 6, 2008.

[7] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting," *IEEE Trans. Inform. Theory*, submitted Feb. 2007.

[8] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," *IEEE Trans. Automat. Contr.*, vol. 37, no. 12, pp. 1936–1948, 1992.

[9] A. Eryilmaz, R. Srikant, and J. Perkins, "Stable scheduling policies for fading wireless channels," *IEEE/ACM Trans. Network.*, vol. 13, no. 2, pp. 411–424, 2005.

[10] E. M. Yeh and A. S. Cohen, "Throughput optimal power and rate control for multiaccess and broadcast communications," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Chicago, IL, USA, June/July 2004, p. 112.

[11] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, Jun. 2007.

[12] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," in *Proc. 45th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, USA, Sep. 2007.

[13] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," submitted Aug. 2007.

[14] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multi-antenna wire-tap channel," available at http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.4105v1.pdf.

[15] S. Asmussen, *Applied Probability and Queues*. New York: Springer-Verlag, 2003.