Dynamic Control for Cooperative Jamming with a Non-altruistic Node

Yunus Sarikaya, Ozgur Ercetin, Ozgur Gurbuz
Faculty of Engineering and Natural Sciences, Sabanci University, Istanbul, Turkey.
{sarikaya,oercetin,ogurbuz} @sabanciuniv.edu

***Abstract*—Cooperative jamming approach in secure communication typically assumes dedicated and/or altruistic jamming nodes, investing their resources for the good of the whole system. In this paper, we consider a cognitive radio network with non-altruistic jamming nodes, from which a source node utilizes jamming service, compensating them with a fraction of its bandwidth for transmission of its data. The nodes only know the distribution of the gains of channels to the eavesdropper. Particularly, the primary node injects confidential data and secondary nodes inject open data at rates in order to maximize global utility function, while keeping data queues stable and meeting a constraint on the secrecy outage probability. The constraint on the secrecy outage probability is met with the help of jamming service obtained from the secondary nodes. Our scheme achieves a utility, arbitrarily close to the maximum achievable utility.**

***Index Terms*—Physical layer security, cooperative jamming, cognitive radio**

I. Introduction

Recently, information theoretic security has gained significant attention, provisioning an ultimate goal of guaranteed security against adversaries with unlimited computational resources. Particularly, deploying cooperative jammers that transmit Gaussian noise [1] or jamming codewords [2] can help improving secure communication rates between legitimate nodes by impairing the reception of the eavesdropper.

The jamming signal power should be high enough to disturb the received signal at the eavesdropper; however, allocating too much power on the jamming signal can also degrade the signal quality at the destination. Thus, recent studies about the secrecy gains acquired with the cooperative jamming involves the optimization of jamming powers with the objective of maximizing the secrecy rate [3], [4]. However, they generally assume dedicated jamming nodes to the benefit of the system performance. This assumption is not valid, especially for the nodes with limited power. To that end, [5] has investigated a class of secrecy problem in cognitive radio networks with non-altruistic nodes. They propose a distributed solution using a game-theoretic framework where a source node, towards the maximization of its secrecy rate, utilizes the jamming services from non-altruistic nodes, and in return these nodes obtain utilization of some fraction of bandwidth of the source node for their own data. Differently, here, we analyze a more realistic scenario where only distribution of the channel gains to the eavesdropper is available. Due to the lack of the knowledge of instantaneous channel gains, perfect secrecy cannot be ensured with probability 1 for confidential information. Thus, to meet a constraint on the secrecy outage probability, secondary nodes transmit jamming signal to disturb the signal received by the eavesdropper, and in return gain access to the channel to send their own data which is proportional to the power of their jamming signals. Secondly, with the goal of maximizing the aggregate utility, i.e., sum utilities of a source (primary) node and separate non-altruistic jamming (secondary) nodes, we model the problem as that of network utility maximization. We provide a dynamic solution, in which a joint flow control, power and bandwidth allocation scheme is obtained by using the stochastic optimization framework [6]. We prove that our scheme achieves a utility, arbitrarily close to the maximum achievable utility.

This work was supported in part by Marie Curie Fellowship PIRSES-GA-2010-269132 AGILENet.

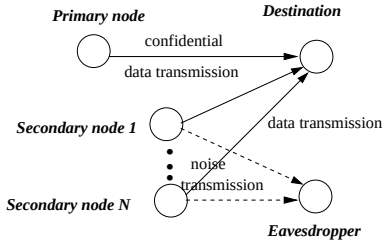

Fig. 1. Network Model

II. System Model and Preliminaries

A. System Model

We consider a cognitive radio network of one primary user and n secondary users, all wishing to communicate with a common destination as shown in Figure 1, and there is an eavesdropper whose goal is to interpret the information transmitted by the primary user without trying to modify it. Since secondary users do not own the spectrum band, the transmission has to be approved by the primary node.

Traffic is assumed to be a mixture of confidential data stored by the primary node and open data stored by the secondary nodes. Let $A_p(t)$ and $A_i(t)$ represent input rates in bits per channel use with which data is injected in the primary node and the secondary node i in slot t, respectively. The rates $A_p(t)$ and $A_i(t)$ have long-term averages λ_p and λ_i, respectively. $U_p(\lambda)$ represents the utility obtained by the primary node from the transmission of confidential data, and $U_i(\lambda)$is the utility obtained by the secondary node i from the transmission of open data, both at a rate of λ bits per channel use. We assume that $U_p(0) = 0$, $U_i(0) = 0$, and $U_p(.)$ and $U_i(.)$ are continuously differentiable, monotonically increasing and concave functions.

Time is slotted where the time-slot is the resource to be shared among the primary and secondary users, and each slot has a length of N channel uses (physical layer symbols), where N is sufficiently large to allow for invoking random coding

arguments. All channels undergo quasi-static flat Rayleigh fading, i.e., all channel gains have exponential distribution, in which the channel gain remains constant within a time slot and varies independently from slot to slot. For a time slot t, $h_{SD}(t)$ denotes the gain of the channel between the source and the destination nodes; $h_{SE}(t)$ is the gain of the source-eavesdropper channel; $h_{J_iE}(t)$ and $h_{J_iD}(t)$ denote the gains of the channels from the the secondary node i to the eavesdropper and destination node respectively. We normalize the power gains such that the (additive Gaussian) noise has unit variance.

We denote the instantaneous achievable rate for the main channel by $R_p(t)$, which is the mutual information between the channel between the primary node and destination in time slot t. Likewise, $R_e(t)$ corresponds to the mutual information between the channel input at the primary node and the channel output at the eavesdropper.

In our work, we consider cooperative jamming where the secondary user creates interference at the eavesdropper by transmitting a jamming signal [3]. We assume that each secondary node independently transmits noise signal, which lies in the null space of the secondary node-destination channel, thus creating zero interference to the destination. Defining P_s and $P_i^J(t)$ as the transmission powers of the primary node and secondary node i respectively in a cooperative jamming setting in time slot t, the transmission rates, $R_p(t)$ and $R_e(t)$, can be obtained as:

$$\begin{aligned} R_p(t) &= \log\left(1+P_s h_{SD}(t)\right) \\ R_e(t) &= \log\left(1+\frac{P_s h_{SE}(t)}{1+\sum_i h_{J_iE}(t)P_i^J(t)}\right) \end{aligned} \tag{1}$$

Let $\beta(t)$ be the fraction of time slot granted to the secondary user in slot t for cooperating with the primary user to enhance its secrecy rate. Defining $P_i^T(t)$ as the transmission power of the secondary node i reserved for its own transmission, the instantaneous achievable rate of the secondary node is:

$$R_i^T(t) = \beta_i(t)\log\left(1+P_i^T(t)h_{J_iD}(t)\right)$$

B. Confidential Transmission Scheme and Secrecy

We assume the availability of perfect channel-state information (CSI) of the channels to the destination, $h_{SD}(t)$ and $h_{J_iD}(t)$, at the transmitters. We assume that transmitters do not have the knowledge of the instantaneous values of the gains of eavesdropper channels, $h_{SE}(t)$ and $h_{J_iE}(t)$, but their distributions are available [1]. One should realize that, since instantaneous CSI is not available, one cannot choose the code rates based on a particular fading channel state. Instead, a particular coding rate is chosen for the confidential message and the same code is used for the primary node at all times. Specifically, the primary node uses Wyner coding to provide confidentiality, which basically inserts a randomization message to the actual message to increase the level of secrecy [7]. Let $C(\hat{R}_p;\hat{R}_p^{priv};N)$ be a Wyner code of size $2N\hat{R}_p$ codewords, generated to convey a confidential message set $W_p \in 1,\ldots 2N\hat{R}_p^{priv}$. Thus, every codeword has a length of $N\hat{R}_p$ bits to convey $N\hat{R}_p^{priv}$ bits of confidential information.

Let the vector of symbols received by the eavesdropper be Y_e. To achieve perfect secrecy, the following constraint must be satisfied by the primary node, for all t,

$$\lim_{N\to\infty}\frac{1}{N}I(W_p;Y_e) \le \varepsilon. \tag{2}$$

Next, we define the notion of *secrecy outage* employed in our analysis. We say that the secrecy outage event occurs, when the confidential message is intercepted by an eveasdropper node. This is when the perfect secrecy constraint in (2) is violated, such that $\hat{R}_p - \hat{R}_p^{priv} < R_e(t)$. Specifically, when $\hat{R}_p - \hat{R}_p^{priv}$, the rate of the randomization message the source uses in the random binning scheme for secrecy in time slot t, is lower than the actual rate of the eavesdropper, $R_e(t)$, in time slot t, a secrecy outage has occurred. The probability of secrecy outage in time slot t is given by,

$$P_s^{out}(t) = P(\hat{R}_p - \hat{R}_p^{priv} < R_e(t)). \tag{3}$$

As a qualify of service (QoS) requirement, the expected probability of secrecy outage of the primary node can be required to be below a given threshold γ. Note that the primary node may not have channel quality to satisfy this QoS requirement. With the help of secondary users, the primary user may have a higher secrecy rate and meet this constraint, which provides the incentive to share the spectrum with the secondary user. The secondary users, on the other hand, are willing to join the cooperation because they need such a spectrum opportunity to transmit their own data streams. This lays the incentive foundation of cooperation.

The potential cooperation can be established in the following procedure. The primary user first announces the jamming power levels of the secondary users such that the secrecy outage requirement is satisfied. Then, the maximum spectrum shared with the secondary users is constrained with these jamming power levels, i.e., the expected value of $\beta_i(t)$ is below a prescribed level, which is assumed to be proportional to the jamming power level of node i. Thus, the primary user first aims to minimize total jamming power purchased from the secondary nodes while satisfying secrecy outage requirement. Secondly, based on the predetermined jamming power, we seek a solution to the spectrum sharing problem, where we want to maximize the sum utilities of the primary node and secondary nodes.

III. Cross-layer Algorithm

In this section, our objective is to design a cross-layer algorithm considering joint flow control, time and power optimization while satisfying a secrecy outage constraint of the primary node. We investigate two problems for this objective. In the first problem, we aim to minimize total jamming power subject to the secrecy outage constraint of the primary node. In the second problem, we aim to maximize the aggregate utility of the primary and secondary nodes by the optimized jamming powers obtained in the first problem.

In time-varying wireless channels, a channel outage occurs when the received signal to interference/noise ratio drops

[1]The distribution of channel gains can be inferred by the node from the received signals over the reverse channels, exploiting channel reciprocity.

below a threshold necessary for decoding the transmitted signal. Likewise, a secrecy outage event occurs, when the randomized information rate drops below the information rate obtained by the eavesdropper. In this case, the amount of randomized bits is not sufficient to confuse the eavesdropper, and the eavesdropper obtains sufficient amount of information to decode the secret packet. In the following, we analyze the secrecy outage probability, P_s^{out}.

Lemma 1: Given the statistics of the channels to the eavesdropper and the chosen secret encoding rates $\hat{R}_p$ and $\hat{R}_p^{priv}$, the secrecy outage probability, is calculated as:

$$P_s^{out} = \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) e^{-\lambda_{SE} D} \left[1 - \frac{\lambda_{SE}}{\lambda_{SE} + \frac{\lambda_i}{D}} \right] \tag{4}$$

where $D = 2^{\hat{R}_p - \hat{R}_p^{priv}} - 1$, and $\lambda_i = \frac{1}{P_i^J \mathbb{E}[h_{J_i E}]}$ for the secondary node i and $\lambda_{SE} = \frac{1}{P_s \mathbb{E}[h_{SE}]}$ for the source node. The proof of Lemma 1 is provided in Appendix A.

A. Jamming Power Allocation

Here, we focus on designing the transmission scheme such that the secrecy outage P_s^{out} can satisfy certain secure level γ while minimizing total jamming power of the secondary nodes. Specifically, we analyze the following problem:

$$\min_{P_i^J} \sum_{i=1}^{n} P_i^J \tag{5}$$

$$\text{subject to } P_s^{out} \leq \gamma \tag{6}$$

Note that the above problem is a static optimization problem, since only the statistics of the channels to the eavesdropper are known, and the secrecy outage probability calculated in Lemma 1 is a function of these statics. Here, we solve the problem using dual decomposition method that is particularly appealing to our problem structure, since the objective function is linear, and the constraint is affine function.

Let $\mathbf{P}^J$ represent the vector of the jamming powers of the secondary nodes. Let us first introduce dual variable μ to relax constraint in (6). Then we have the dual function as:

$$D(\mu) = \min_{\mathbf{P}^J} L(\mathbf{P}^J; \mu) \tag{7}$$

where

$$L(\mathbf{P}^J; \mu) = \sum_{i=1}^{n} P_i^J + \mu \left(P_s^{out} - \gamma \right) \tag{8}$$

and accordingly, the dual problem is given by

$$\max_{\mu} D(\mu) \tag{9}$$

Let $\mathbf{P}^{J*} = [P_1^{J*}, P_2^{J*}, \ldots, P_n^{J*}]$ be optimal values of jamming power levels obtained based on the optimization in (5) and (6), which are obtained by the primary node in a offline fashion before the start of spectrum sharing session. Note that to obtain $\mathbf{P}^{J*}$, we need to solve (7) and (9). Since the function in (7) is highly non-linear with respect to P_i^J, obtaining optimal P_i^{J*} is rather involved. Therefore, we use one of the search methods like gradient or bisection methods. Furthermore, the dual problem in (9) can be solved using the subgradient projection method [8].

B. Cross-layer Algorithm

Our objective is to design a joint flow control, time and power allocation algorithm that maximizes the aggregate network utility given the optimal jamming power allocation of the secondary nodes, $\mathbf{P}^{J*}$. We aim to find the solution of the following problem:

$$\max_{P_i^T(t), \beta_i(t)} \mathbb{E}\left[U_p(x_p)\right] + \sum_{i=1}^{n} \mathbb{E}\left[U_i(x_i)\right] \tag{10}$$

$$\text{subject to } x_p \leq \mathbb{E}\left[(1 - \sum_{i=1}^{n} \beta_i(t)) \hat{R}_p^{priv} \right] \tag{11}$$

$$x_i \leq \mathbb{E}\left[R_i^T(t)\right] \tag{12}$$

$$\mathbb{E}\left[P_i^T(t)\right] \leq \alpha_i \tag{13}$$

$$\mathbb{E}\left[\beta_i(t)\right] \leq \theta_i P_i^{J*} \tag{14}$$

The objective function in (10) calculates the total expected utility of the primary and secondary nodes over random stationary channel conditions, and the time and power allocation decisions. Condition (13) requires that the average power used for its own transmission by the secondary node should be smaller than a given constant power budget α. Condition (14) is the spectrum allocation constraint of the secondary nodes, where we assume that the maximum allocated spectrum to the secondary node is proportional to its jamming power, i.e, $\theta_i P_i^*$, used to help the confidential transmission of the primary node.

Next, we propose a dynamic control solution based on the stochastic network optimization framework developed in [6]. The dynamics of the primary and secondary node i queues $Q_p(t)$ and $Q_i(t)$ are given as follows:

$$Q_p(t+1) = \left[Q_p(t) - (1 - \sum_{i=1}^{n} \beta_i(t)) \hat{R}_p^{\text{priv}} \right]^+ + A_p(t), \tag{15}$$

$$Q_i(t) = \left[Q_i(t) - R_i^T(t) \right]^+ + A_i(t), \tag{16}$$

where $[\cdot]^+ = \max\{0, \cdot\}$, and we can relate the constraints in (13) and (14) with a virtual queue as:

$$Z_i(t+1) = \left[Z_i(t) + P_i^T(t) - \alpha \right]^+, \tag{17}$$

$$K_i(t+1) = \left[K_i(t) + \beta_i(t) - \theta_i P_i^{J*} \right]^+, \tag{18}$$

Strong stability of (17) and (18) ensure that the constraints are also satisfied [6].

Control Algorithm: The algorithm executes the following steps in each slot t:

Flow Control: For some $V > 0$, the primary node and secondary node i injects $A_p(t)$ and $A_i(t)$ bits, respectively, where

$$(A_p(t), A_i(t)) = \underset{A_p, A_i}{\text{argmax}} V \left[U_p(A_p) + \sum_{i=1}^{n} U_i(A_i) \right] - Q_p(t) A_p - \sum_{i=1}^{n} Q_i(t) A_i$$

Time and Power Allocation: For some $P_i^{J*} > 0$ and $P_s > 0$, the primary node shares $\beta_i(t)$ portion of the slot with the

secondary node i, and the secondary node allocates the power $P_i^T(t)$ for its own transmissions. We choose these parameters as the solution of:

$$\{\beta_i(t), P_i^T(t)\} = \underset{\beta_i, P_i^T}{\operatorname{argmax}} Q_p(t)(1-\sum_{i=1}^{n}\beta_i(t))\hat{R}_p^{\text{priv}} + \sum_{i=1}^{n}\left(Q_i(t)R_i^T(t) - Z_i(t)P_i^T(t) - K_i(t)\beta_i(t)\right),$$

Let us define $F_i(t) = Q_i(t)\log(1+P_i^T(t)h_{J_iD}(t)) - K_i(t) - P_i^T(t)Z_i(t)$, then

$$\beta_i(t) = \begin{cases} 1, & \text{if } F_i(t) > F_l(t),\ \forall l \\ & \text{and } F_i(t) > Q_p(t)\hat{R}_p^{\text{priv}} \\ 0, & \text{otherwise.} \end{cases}$$

and

$$P_i^T(t) = \begin{cases} 1, & \text{if } \left[\frac{Q_i(t)h_{J_iD}(t) - Z_i(t)}{h_{J_iD}(t) - Z_i(t)}\right]^+ \text{ and } \beta_i(t) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

Theorem 1: If $R_T(t) < \infty$ for all t, then dynamic control algorithm satisfies:

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} U_p(x_p) + \sum_{i=1}^{n} U_i(x_i) \geqslant U^* - \frac{B}{V},$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1} \mathbb{E}[Q_p(t)] \leq \frac{B + V(\bar{U} - U^*)}{\varepsilon_1}$$

$$\liminf_{T\to\infty} \frac{1}{T}\sum_{t=0}^{T-1}\sum_{i=1}^{n} \mathbb{E}[Q_i(t)] \leq \frac{B + V(\bar{U} - U^*)}{\varepsilon_2}$$

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

Theorem 1 can be proven following the same approach in Theorem 4.5 in [6], and the proof of Theorem 1 is given in Appendix B.

IV. Simulation Results

In our simulation results, we consider logarithmic utility functions of the primary and secondary nodes, where the utility obtained by the primary node is $\kappa > 1$ times more than the utility obtained by the secondary node at the same rate. More specifically, we take $U_p(x) = \kappa\log(1+x)$ and $U_i(x) = \log(1+x)$. The utility function $U(x) = \log(1+x)$ captures resource allocation according to the criterion of proportional fairness, which is based on maximizing total throughput while allowing users at least a minimal level of service. We assume that the gains of the primary node to destination and the secondary nodes to eavesdropper channels are chosen uniformly randomly in the interval [5,15], and the gains of the primary node to eavesdropper and the secondary node to destination channels are chosen in the interval [1,5]. The simulation is repeated for 3 realizations of the channel gains, and the result presented is the average of these realizations. In addition, the ratio of the utility obtained by the primary node and the utility obtained by the secondary node, κ, is taken as 5. The power of the primary node $P_s = 1$ and θ_i is taken as 0.5 for all i.

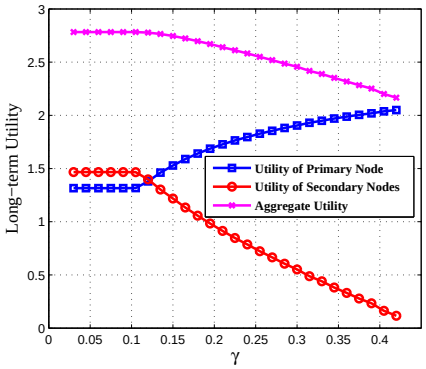

Fig. 2. Long-term utilities with respect to γ

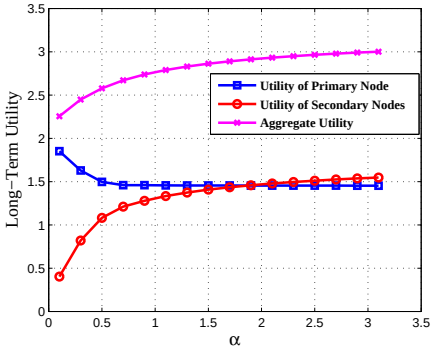

Fig. 3. Long-term utilities with respect to α

Fig. 2 illustrates the effect of the secrecy outage probability constraint, γ, where α is taken as 1. As seen from Fig. 2, the utility obtained by the secondary nodes decreases with increasing γ except when γ is between 0 and 0.1. This is because for low γ values, in order to satisfy a tight secrecy outage constraint, the primary node purchases a larger cooperative jamming power, i.e., the maximum fraction of time can be used by the secondary nodes is high. Thus, when γ is between 0 and 0.1, the spectrum allocation constraint in (14) is active. After $\gamma = 0.1$, the time allocation constraint becomes inactive, since the constraint is realized with strict inequality. Meanwhile, the utility obtained by the secondary nodes decreases, since there is a smaller number of transmission opportunities left for the secondary nodes with more confidential information being transmitted by the primary node.

In Fig. 3, we analyze the effect of the average power constraint, α, on the utilities of the primary and secondary nodes when $\gamma = 0.15$. As seen in Fig. 3, the utilities of the secondary nodes and the aggregate utility, are increased with the average power constraint, as expected. Starting around $\alpha = 1.5$, the power constraint becomes inactive. In other words, giving a larger power budget to the secondary nodes does not help improve the system performance beyond a certain level.

V. Conclusion

In this paper, we have proposed a dynamic solution for enhancing secret communications in wireless channel with a non-altruistic jammer where secondary users help a primary user to enhance secrecy against an intelligent and passive

eavesdropper. Assuming that the transmitters only know their channel to the legitimate receiver and has statistical CSI on their channel to eavesdropper, we have formulated and solved a network utility maximization problem. Simulation results are presented to verify the performance. In our future work, we will investigate distributed version of our dynamic control algorithms, where the optimal jamming powers and time allocation decision are given according to local information.

REFERENCES

[1] E. Tekin and A. Yener, "The general gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, pp. 2735–2751, June 2008.

[2] E. Tekin and A. Yener, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, pp. 4005–4019, Sep. 2008.

[3] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. on Signal Processing*, vol. 58, pp. 4033–4039, March 2010.

[4] G. Zheng, L. Choo, and K. Wong, "Optimal Cooperative Jamming to Enhance Physical Layer Security Using Relay," *IEEE Trans. on Signal Processing*, vol. 59, March 2011.

[5] I. Stanojev and A. Yener, "Cooperative jamming via spectrum leasing," in *Proc. Intl. Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks*, (Princeton, NJ), pp. 265–272, May 2011.

[6] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resouce Allocation and Cross-layer Control in Wireless Networks," *Foundations and Trends in Networking*, vol. 1, no. 1, pp. 1–144, 2006.

[7] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1380, Oct. 1975.

[8] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Upper Saddle Rive, NJ: Prentice-Hall, 1989.

[9] K. Smaili, T. Kadri, and S. Kadry, "Hypoexponential Distribution with Different Parameters," *Applied Mathematics*, vol. 4, pp. 624–631, Apr. 2013.

APPENDIX A
PROOF OF LEMMA 1

In order to derive the secrecy outage probability, we first need to statistically characterize $R_e(t)$ in (1), since transmitters do not have the knowledge of the instantaneous values of the gains of eavesdropper channels, $h_{SE}(t)$ and $h_{J_iE}(t)$, but their distributions are available. Note that the channel gains are exponentially distributed with parameters $\lambda_{SE} = \frac{1}{P_s\mathbb{E}[h_{SE}]}$ and $\lambda_i = \frac{1}{P_i^J\mathbb{E}[h_{J_iE}]}$. We define Z and $(X_i)_{i=1,\ldots,n}$ as independent exponential random variables with distinct respective parameters λ_{SE} and λ_i, $i = 1,\ldots,n$. We start with the distribution of the sum of independent exponential random variables for the summation in the denominator of the rational term in the log function, i.e., interference terms created by the secondary nodes, in (1). The sum of independent exponential distributions is hypoexponentially distributed [9]. Defining $Y = X_1 + \ldots + X_n$, the probability density function (PDF) of Y is :

$$f_Y(y) = \sum_{i=1}^{n} \lambda_i e^{-y\lambda_i} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) \tag{19}$$

We know that Z is also exponential with pdf $f_Z(z) = \lambda_{SE} e^{-\lambda_{SE} z}$. Now, re-writing the definition in (3), we are ready to extrect the secrecy outage probability,

$$\begin{aligned} P_s^{\text{out}} &= \mathbb{P}\left(\hat{R}_p - \hat{R}_p^{\text{priv}} < \log\left(1 + \frac{Z}{1+Y}\right)\right) \\ &= \mathbb{P}\left(D < \frac{Z}{1+Y}\right) = \mathbb{P}\left(D(1+Y) < Z\right) \end{aligned} \tag{20}$$

where $D = 2^{\hat{R}_p - \hat{R}_p^{\text{priv}}} - 1$. Since the random variables Z and Y are independent, we can calculate the secrecy outage probability as:

$$\begin{aligned} P_s^{\text{out}} &= \int_{z=D}^{\infty} \int_{y=0}^{z/D-1} f_Z(z) f_Y(y) dy dz \\ &= \sum_{i=1}^{n} \int_{z=D}^{\infty} \int_{y=0}^{z/D-1} \lambda_{SE} e^{-\lambda_{SE} z} \lambda_i e^{-y\lambda_i} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) dy dz \\ &= \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) \int_{z=D}^{\infty} \lambda_{SE} e^{-\lambda_{SE} z} \left[1 - e^{-(z/D-1)\lambda_i} \right] \\ &= \sum_{i=1}^{n} \left(\prod_{j=1, j\neq i}^{n} \frac{\lambda_j}{\lambda_j - \lambda_i} \right) e^{-\lambda_{SE} D} \left[1 - \frac{\lambda_{SE}}{\lambda_{SE} + \frac{\lambda_i}{D}} \right] \end{aligned} \tag{21}$$

Now, we obtain the result in Lemma 1. This has concluded the proof.

APPENDIX B
PROOF OF THEOREM 1

The optimality of the algorithm can be shown by applying the Lyapunov optimization theorem [6]. We consider queue backlog vectors as $\mathbf{Q}(t) = (Q_p(t), Q_1(t), \ldots, Q_n(t))$, $\mathbf{K}(t) = (K_1(t), \ldots, K_n(t))$, and $\mathbf{Z}(t) = (Z_1(t), \ldots, Z_n(t))$, where n is the number of secondary nodes in the network. Let $L(\mathbf{Q}, \mathbf{K}, \mathbf{Z})$ be a quadratic Lyapunov function of real and virtual queue backlogs defined as:

$$L(\mathbf{Q}(\mathbf{t}), \mathbf{K}(\mathbf{t}), \mathbf{Z}(\mathbf{t})) = \frac{1}{2} \left(Q_p(t)^2 + \sum_{i=1}^{n} \left[(Q_i(t))^2 + (Z_i(t))^2 + (K_i(t))^2 \right] \right). \tag{22}$$

Also consider the one-step expected Lyapunov drift, $\Delta(t)$ for the Lyapunov function as:

$$\begin{aligned} \Delta(t) = \mathbb{E}\big[& L(\mathbf{Q}(\mathbf{t}+\mathbf{1}), \mathbf{K}(\mathbf{t}+\mathbf{1}), \mathbf{Z}(\mathbf{t}+\mathbf{1})) \\ & - L(\mathbf{Q}(\mathbf{t}), \mathbf{K}(\mathbf{t}), \mathbf{Z}(\mathbf{t})) | \mathbf{Q}(\mathbf{t}), \mathbf{K}(\mathbf{t}), \mathbf{Z}(\mathbf{t}) \big]. \end{aligned} \tag{23}$$

The following lemma provides an upper bound on $\Delta(t)$.

Lemma 2:

$$\begin{aligned} \Delta(t) \leq B &- \mathbb{E}\left[Q_p(t) \left(A_p(t) - (1 - \sum_{i=1}^{n} \beta_i(t)) \hat{R}_p^{\text{priv}} \right) \;\middle|\; Q_p(t) \right] \\ &- \sum_{i=1}^{n} \mathbb{E}\left[Q_i(t) \left(A_i(t) - R_i^T(t) \right) \;\middle|\; Q_i(t) \right] \\ &- \sum_{i=1}^{n} \mathbb{E}\left[Z_i(t) \left(P_i^T(t) - \alpha \right) \;\middle|\; Z_i(t) \right] \\ &- \sum_{i=1}^{n} \mathbb{E}\left[K_i(t) \left(\beta_i(t) - \theta_i P_i^{J*} \right) \;\middle|\; K_i(t) \right] \end{aligned} \tag{24}$$

where $B > 0$ is a constant.

Proof Since the maximum transmission power is finite, in any interference-limited system transmission rates are bounded. Also assume that the arrival rates are bounded, i.e., $A_p^{\max}$ and

$A_i^{\max}$ are the maximum number of bits that may arrive in a slot for the primary node and secondary node i, respectively. By simple algebraic manipulation one can obtain a bound for the difference $(Q_i(t+1))^2-(Q_i(t))^2$ and also for other queues to obtain the result in (24)

■

Applying the above lemma, we can complete our proof. In particular, Lyapunov Optimization Theorem [6] suggests that a good control strategy is the one that minimizes the following:

$$\Delta^U(t)=\Delta(t)-V\mathbb{E}\left[U_p(t)+\sum_{i=1}^{n}(U_i(t))\,|\,(\mathbf{Q}(\mathbf{t}),\mathbf{K}(\mathbf{t}),\mathbf{Z}(\mathbf{t}))\right]. \tag{25}$$

By using (24) in the lemma, we obtain an upper bound for (25), as follows:

$$\begin{aligned}\Delta^U(k)\leq B&-\mathbb{E}\left[Q_p(t)\left(A_p(t)-(1-\sum_{i=1}^{n}\beta_i(t))\hat{R}_p^{\text{priv}}\right)\;\middle|\;Q_p(t)\right]\\&-\sum_{i=1}^{n}\mathbb{E}\left[Q_i(t)\left(A_i(t)-R_i^T(t)\right)\;\middle|\;Q_i(t)\right]\\&-\sum_{i=1}^{n}\mathbb{E}\left[Z_i(t)\left(P_i^T(t)-\alpha\right)\;\middle|\;Z_i(t)\right]\\&-\sum_{i=1}^{n}\mathbb{E}\left[K_i(t)\left(\beta_i(t)-\theta_iP_i^{J*}\right)\;\middle|\;K_i(t)\right]\\&-V\mathbb{E}\left[U_p(A_p(t))+\sum_{i=1}^{n}U_i(A_i(t))\right]\end{aligned} \tag{26}$$

Our proposed dynamic network control algorithm is designed such that it minimizes the right hand side of (26). If the arrival rates, and the time allocation parameter, θ_i, are in the feasible region, it has been shown in [6] that there must exist a stationary time and power allocations and rate control policy that chooses the allocations and their arrival rates independent of queue backlogs and only with respect to the channel statistics. In particular, the optimal stationary policy can be found as the solution of a deterministic policy if the channel statistics are known a priori.

Let U^* be the optimal value of the objective function of the problem (10-14) obtained by the aforementioned stationary policy. Also let ${\lambda_p}^*$ and ${\lambda_i}^*$ be optimal traffic arrival rates of the primary node and secondary node i, respectively, found as the solution of the same problem. Note that the expectations on the right hand side of (26) can be written separately due to independence of backlogs with allocation and rate control policy. In particular, the optimal input rate ${\lambda_p}^*$ and ${\lambda_i}^*$ could in principle be achieved by the simple backlog-independent admission control algorithm of new arrival $A_i(p)$ and $A_i(t)$ for the primary node and the secondary node i in block t independently with probability $\zeta_p={\lambda_p}^*/\lambda_p$ and $\zeta_i={\lambda_i}^*/\lambda_i$, respectively.

Also, since ${\lambda_p}^*$ and ${\lambda_i}^*$ are in the achievable rate region, i.e., arrival rates are strictly interior of the rate region, there must exist a stationary scheduling and rate allocation policy that is independent of queue backlogs and satisfies the followings:

$$\mathbb{E}\left[\sum_{\{i|(s,i)\in L\}}\mu_{si}(t)|\mathbf{Q}\right]\geq{\lambda_p}^*+\varepsilon_1 \tag{27}$$

$$\mathbb{E}\left[\sum_{i=1}^{n}R_i^T(t)|\mathbf{Q}\right]\geq\lambda_i^*+\varepsilon_2 \tag{28}$$

$$\mathbb{E}\left[P_i^T(t)|\mathbf{Z}\right]+\varepsilon_3\leq\alpha_i \tag{29}$$

$$\mathbb{E}\left[\beta_i(t)|\mathbf{K}\right]+\varepsilon_4\leq\theta_iP_i^{J*} \tag{30}$$

Clearly, any stationary policy should satisfy (26). Recall that our proposed policy minimizes the right hand side (RHS) of (26), and hence, any other stationary policy (including the optimal policy) has a higher RHS value than the one attained by our policy. In particular, the stationary policy that satisfies (27)-(30), and implements aforementioned probabilistic admission control can be used to obtain an upper bound for the RHS of our proposed policy. Inserting (27)-(30) into (26), we obtain the following upper bound for our policy:

$$\begin{aligned}RHS<B&-\varepsilon_1\mathbb{E}[Q_p(t)]-\varepsilon_2\sum_{i=1}^{n}\mathbb{E}[Q_i(t)]\\&-\varepsilon_3\sum_{i=1}^{n}\mathbb{E}[Z_i(t)]-\varepsilon_4\sum_{i=1}^{n}\mathbb{E}[K_i(t)]-VU^*.\end{aligned}$$

where (55) follows from Jensen's inequality together with concavity of $U_p(.)$ and $U_i(.)$. This is exactly in the form of Lyapunov Optimization Theorem given in [6], and hence, we can obtain bounds on the performance of the proposed policy and the sizes of queue backlogs as given in Theorem 1.