Secure Spectrum Sharing via Rate Adaptation

Secure Spectrum Sharing via Rate Adaptation

Behrooz Makki and Thomas Eriksson
Department of Signals and Systems, Chalmers University of Technology, Gothenburg, Sweden
Email: {behrooz.makki and thomase}@chalmers.se

***Abstract*—This paper addresses the problem of secure communication in spectrum sharing networks. The achievable rates are determined such that the unlicensed user security is guaranteed, i.e., the unlicensed user massages are not decodable by the license holders. Considering slowly-fading channels, the results are obtained under the licensed user interference- and signal-to-interference-and-noise ratio (SINR)-limited conditions. The results indicate that there is considerable potential for the unlicensed user secure data transmission under different license holder's quality-of-service requirements. Moreover, depending on the channel condition and the license holder's SINR constraint, the unlicensed user's achievable rates may increase with the license holder transmission power.**

I. Introduction

Spectrum is a scarce valuable resource in today's wireless communication networks; with ever-increasing number of wireless devices such as smart phones, there is growing demand for spectrum resources. This point has led to complaints about spectrum shortage which is expected to grow even more in the future. On the other hand, recent studies show that the spectrum shortage comes mainly from outdated resource allocation policies where, at any given instant and location, large portions of the spectrum are under- or un-utilized by the license holders that allow little sharing [1], [2]. This is the motivation for the spectrum sharing concept that has received considerable attention during the last decade.

Generally, the goal of a spectrum sharing scheme is to alleviate the spectrum scarcity problem by allowing unlicensed secondary users (SUs) to access the spectrum that is allocated to licensed primary users (PUs) under the condition of preserving the PUs quality-of-service requirements. There are two, namely, interference-avoiding and simultaneous transmission, approaches to exploit the idea of spectrum sharing. The interference-avoiding technique [3]–[5] refers to the scheme where, provided that the SU can sense the spatial, temporal or spectral gaps of the PU resources, it can adjust its transmission parameters to fill these white spaces. Theoretically, this approach leads to significant spectral efficiency improvement. However, it suffers from some practical shortcomings mainly related to imperfect gap detection. Also, it is not appropriate for online applications, because the SU activity is decided based on the PU data transmission status. In the simultaneous transmission technique, on which we concentrate, a SU can simultaneously coexist with a PU as long as it operates below a certain interference level [6], [7].

Assuming different levels of channel state information (CSI) at the SU transmitter and receiver, there are many papers that have investigated the spectrum sharing networks from different aspects. For example, [8]–[12] have studied the SU achievable rates under perfect CSI assumption. These works were later extended by e.g., [13]–[19] where the SU data transmission efficiency was analyzed under different SU transmitter knowledge imperfection conditions. In these works, the PU peak/average received interference power, the PU received signal-to-interference-and-noise ratio (SINR) or the SU peak/average transmission power have been considered as the constraint.

According to, e.g., [5]–[19], the spectrum sharing is accomplished with low transmission rate for the SU. This is particularly because of the PU quality-of-service requirements where the presence of the SU should not affect the performance of the PU considerably. However, with low transmission rate, the network is not secure for the SU, as the SU massages may be decoded by the PU receiver. This is not desirable for many practical applications requiring privacy for the users.

With this background, this paper studies the secure ergodic achievable rates of the spectrum sharing networks. Here, in contrast to [5]–[19], the secondary user achievable rates are maximized such that the PU receiver can not decode the SU massages. Considering slowly-fading channels, the achievable rates are obtained under the PU peak and average interference power and SINR constraints. The results show that there is considerable potential for the SU secure data transmission under the PU interference- and SINR-limited conditions. Moreover, depending on the channel condition, the SU achievable rates may increase with the PU transmission power under a PU received SINR constraint. Finally, the sensitivity to the SU security constraint increases when the PU received SINR decreases.

II. System model

As demonstrated in Fig.1, we consider a spectrum sharing network where a SU attempts to reuse the spectrum resources of a PU. Let H_{pp}, H_{ps}, H_{sp} and H_{ss} be the instantaneous channel fading variables of the PU-PU, PU-SU, SU-PU and SU-SU links, respectively. Correspondingly, we define the *channel gains* as $G_{\text{pp}} \doteq |H_{\text{pp}}|^2$, $G_{\text{ps}} \doteq |H_{\text{ps}}|^2$, $G_{\text{sp}} \doteq |H_{\text{sp}}|^2$ and $G_{\text{ss}} \doteq |H_{\text{ss}}|^2$. The gains probability density functions (pdf:s) are denoted by $f_{G_{\text{pp}}}$, $f_{G_{\text{ps}}}$, $f_{G_{\text{sp}}}$ and $f_{G_{\text{ss}}}$, respectively. The results are obtained for Rayleigh-fading channels, e.g., $f_{G_{\text{pp}}}(g) = \lambda_{\text{pp}} e^{-\lambda_{\text{pp}} g}, g \geq 0$. However, the arguments are valid for any combination of independent random variables. The complex AWGNs Z_{p} and Z_{s} added at the PU and SU receivers, are supposed to have distributions $\mathcal{CN}(0,1)$. In this way, the channel can be modeled as

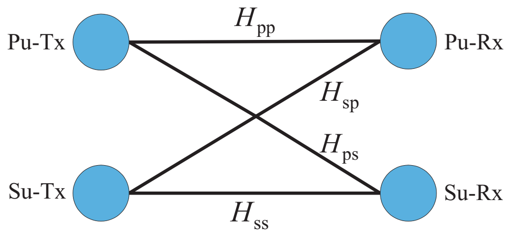

Figure 1. Channel model.

$$\begin{cases} Y_{\rm p} = X_{\rm p}H_{\rm pp} + X_{\rm s}H_{\rm sp} + Z_{\rm p} \\ Y_{\rm s} = X_{\rm s}H_{\rm ss} + X_{\rm p}H_{\rm ps} + Z_{\rm s} \end{cases} \tag{1}$$

where $X_{\rm p}$ and $X_{\rm s}$ are the PU and SU input signals, respectively, and $Y_{\rm p}$ and $Y_{\rm s}$ represent their corresponding outputs. Finally, the PU and the SU transmission powers are denoted by $\mathbf{E}\{|X_{\rm p}|^2\} = T_{\rm p}$ and $\mathbf{E}\{|X_{\rm s}|^2\} = T_{\rm s}$, respectively, where $\mathbf{E}\{.\}$ is the expectation operator.

We consider the slowly-fading channels where the channel gains remain constant for a long time, generally determined by the channel coherence time, and then change independently according to their corresponding distributions. In each block, the channel gains are supposed to be known by the SU transmitter and receiver which is an acceptable assumption in slowly-fading channels [8]–[12].

In the following, we study the secure ergodic achievable rate of the secondary user under different primary user quality-of-service requirements.

III. Theoretical results

In each block, the SU received SINR can be modeled as

$$\text{SINR}_{\rm s} = T_{\rm s}U_{\rm s},\ U_{\rm s} \doteq \frac{G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}, \tag{2}$$

where $U_{\rm s}$ is an auxiliary random variable. For Rayleigh-fading channels, the cumulative distribution function (cdf) of the auxiliary variable $U_{\rm s}$ is found as

$$\begin{aligned} F_{U_{\rm s}}(u) &= \Pr\{\frac{G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}} \le u\} \\ &= \int_0^\infty \lambda_{\rm ps} e^{-\lambda_{\rm ps}x}(1-e^{-\lambda_{\rm ss}u(1+T_{\rm p}x)}){\rm d}x \\ &= 1 - \frac{e^{-\lambda_{\rm ss}u}}{1+\frac{\lambda_{\rm ss}}{\lambda_{\rm ps}}T_{\rm p}u}. \end{aligned} \tag{3}$$

Here, $\lambda_{\rm ss}$ and $\lambda_{\rm ps}$ are the fading parameters of the SU-SU and PU-SU channels, respectively, which are determined by the path loss and shadowing between the terminals. From (2), the maximum achievable rate at the SU receiver is

$$R_{\rm s} \le \log(1+\frac{T_{\rm s}G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}). \tag{4}$$

On the other hand, using a sequential decoder, the PU receiver can decode the SU massages if

$$R_{\rm s} < \log(1+T_{\rm s}U_{\rm p}), U_{\rm p} \doteq \frac{G_{\rm sp}}{1+T_{\rm p}G_{\rm pp}} \tag{5}$$

where, with the same procedure as in (3), we have

$$F_{U_{\rm p}}(u) = 1 - \frac{e^{-\lambda_{\rm sp}u}}{1+\frac{\lambda_{\rm sp}}{\lambda_{\rm pp}}T_{\rm p}u}. \tag{6}$$

In this way, the secure data transmission is possible iff

$$\log(1+\frac{T_{\rm s}G_{\rm sp}}{1+T_{\rm p}G_{\rm pp}}) < R_{\rm s} \le \log(1+\frac{T_{\rm s}G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}) \tag{7}$$

and the SU secure ergodic achievable rate is obtained by

$$\begin{aligned} \eta = \mathbf{E}\Big\{ \log(1+\tfrac{T_{\rm s}G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}) \Big| \log(1+\tfrac{T_{\rm s}G_{\rm sp}}{1+T_{\rm p}G_{\rm pp}}) \\ < \log(1+\tfrac{T_{\rm s}G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}) \Big\}. \end{aligned} \tag{8}$$

Remark 1: Equation (7) implies that, to provide the SU security, the data is transmitted only if, considering the SU massage as the desired signal, the SU receiver experiences better SINR conditions, compared to the PU receiver. In this case, the data is transmitted with the maximum rate decodable by the SU receiver, while the PU can not decode the codeword. Moreover, the SU turns off when $\log(1+\frac{T_{\rm s}G_{\rm ss}}{1+T_{\rm p}G_{\rm ps}}) \le \log(1+\frac{T_{\rm s}G_{\rm sp}}{1+T_{\rm p}G_{\rm pp}})$, since the PU can decode any codeword decodable by the SU receiver. This is a new constraint, compared to the constraints in, e.g., [5]–[19], which as discussed in following affects the system performance substantially.

Remark 2: According to (8), the SU secure data transmission is achieved by rate adaptation. This is in contrast to the many proposed schemes [8]–[19], where the spectrum sharing is based on power allocation at the SU transmitter which, due to power amplifiers nonlinearity, is not practically feasible. Finally, among practical coding schemes providing the rate adaptation requirements, e.g., [20]–[23] can be mentioned.

Considering (3), (6) and (8), the secure achievable rate can be rewritten as

$$\begin{aligned} \eta &= \int_{v=0}^{\infty}\int_{u=v}^{\infty} f_{U_{\rm p}}(v) f_{U_{\rm s}}(u)\log(1+T_{\rm s}u){\rm d}u{\rm d}v \\ &\overset{(a)}{=} \int_{v=0}^{\infty} f_{U_{\rm p}}(v)\left((F_{U_{\rm s}}(u)-1)\log(1+T_{\rm s}u)\Big|_{u=v}^{\infty}\right){\rm d}v \\ &+ \int_{v=0}^{\infty} f_{U_{\rm p}}(v)\int_{u=v}^{\infty} T_{\rm s}\frac{1-F_{U_{\rm s}}(u)}{1+uT_{\rm s}}{\rm d}u{\rm d}v = \Omega+\Theta, \\ \Omega &= \int_{v=0}^{\infty} f_{U_{\rm p}}(v)\big(1-F_{U_{\rm s}}(v)\big)\log(1+T_{\rm s}v){\rm d}v, \\ \Theta &= T_{\rm s}\int_{v=0}^{\infty}\int_{u=v}^{\infty} f_{U_{\rm p}}(v)\frac{1-F_{U_{\rm s}}(u)}{1+uT_{\rm s}}{\rm d}v{\rm d}u. \end{aligned} \tag{9}$$

Here, $f_{U_{\rm p}}$ and $f_{U_{\rm s}}$ are the pdf:s of the auxiliary variables $U_{\rm p}$ and $U_{\rm s}$, respectively. Also, (a) is obtained by partial integration. Then, using (3) and the pdf

$$\begin{aligned} & f_{U_{\rm p}}(v) = \frac{{\rm d}F_{U_{\rm p}}(v)}{{\rm d}v} \\ & \Rightarrow f_{U_{\rm p}}(v) = \frac{\lambda_{\rm sp}e^{-\lambda_{\rm sp}v}}{1+\frac{\lambda_{\rm sp}}{\lambda_{\rm pp}}T_{\rm p}v} + \frac{\lambda_{\rm sp}T_{\rm p}e^{-\lambda_{\rm sp}v}}{\lambda_{\rm pp}(1+\frac{\lambda_{\rm sp}}{\lambda_{\rm pp}}T_{\rm p}v)^2}, \end{aligned} \tag{10}$$

we have

$$\Omega = \Gamma_1 + \Gamma_2,$$
$$\Gamma_1 = \lambda_{\text{sp}} \int_{v=0}^{\infty} \frac{\log(1+T_{\text{s}}v)e^{-(\lambda_{\text{ss}}+\lambda_{\text{sp}})v}}{(1+\frac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}}T_{\text{p}}v)(1+\frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}}v)}\text{d}v,$$
$$\Gamma_2 = \frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}} \int_{v=0}^{\infty} \frac{\log(1+T_{\text{s}}v)e^{-(\lambda_{\text{ss}}+\lambda_{\text{sp}})v}}{(1+\frac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}}T_{\text{p}}v)(1+\frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}}v)^2}\text{d}v, \quad (11)$$

where Γ_1 is simplified to

$$\begin{aligned}
\Gamma_1 &= r(\tfrac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}} \int_{v=0}^{\infty} \tfrac{\log(1+T_{\text{s}}v)e^{-qv}}{(1+\frac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}}T_{\text{p}}v)}\text{d}v - \tfrac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}} \int_{v=0}^{\infty} \tfrac{\log(1+T_{\text{s}}v)e^{-qv}}{(1+\frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}}v)}\text{d}v)\\
&\overset{(b)}{=} r\sum_{n=1}^{\infty} T_{\text{s}}^n \tfrac{(-1)^{n+1}}{n} \int_{v=0}^{\infty} (\tfrac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}} \tfrac{v^n e^{-qv}}{1+\frac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}}T_{\text{p}}v} - \tfrac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}} \tfrac{v^n e^{-qv}}{1+\frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}}v})\text{d}v\\
&\overset{(c)}{=} re^{\frac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{ps}}^n \phi(n,k)}{(\lambda_{\text{ss}}T_{\text{p}})^n} \int_{x=1}^{\infty} x^{k-1} e^{-\frac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}}x}\text{d}x\\
&- re^{\frac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{pp}}^n \phi(n,k)}{(\lambda_{\text{sp}}T_{\text{p}})^n} \int_{u=0}^{\infty} x^{k-1} e^{-\frac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}x}\text{d}x\\
&\overset{(d)}{=} re^{\frac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{ps}}^{n+1} \phi(n,k)}{(\lambda_{\text{ss}}T_{\text{p}})^{n+1}} E_{1-k}(\tfrac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}})\\
&- re^{\frac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{pp}}^n \phi(n,k)}{(\lambda_{\text{sp}}T_{\text{p}})^n} E_{1-k}(\tfrac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}).
\end{aligned} \quad (12)$$

Here, it is defined $r = \frac{\lambda_{\text{sp}}}{\frac{\lambda_{\text{ss}}}{\lambda_{\text{ps}}} - \frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}}$, $q = \lambda_{\text{ss}} + \lambda_{\text{sp}}$ and $\phi(n,k) = \frac{(-1)^{2n+1-k}}{n}\binom{n}{k}$ where $\binom{n}{k}$ is the "*n choose k*" operator. Then, (b) is obtained by Taylor expansion of the function $h(u) = \log(1+T_{\text{s}}u)$, (c) follows from variable transformation and some calculations and (d) is based on the definition of the exponential integral function $E_k(x) \doteq \int_1^{\infty} \frac{e^{-xt}\text{d}t}{t^k}$.

With the same procedure as in (12), Γ_2 in (11) is determined as

$$\begin{aligned}
\Gamma_2 &= \tfrac{\lambda_{\text{sp}} e^{\frac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}}} A}{\lambda_{\text{pp}}T_{\text{p}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{ps}}^{n+1}\phi(n,k)}{(\lambda_{\text{ss}}T_{\text{p}})^{n+1}} E_{1-k}(\tfrac{q\lambda_{\text{ps}}}{\lambda_{\text{ss}}T_{\text{p}}})\\
&+ \tfrac{\lambda_{\text{sp}} e^{\frac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}} C}{\lambda_{\text{pp}}T_{\text{p}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{pp}}^{n+1}\phi(n,k)}{(\lambda_{\text{sp}}T_{\text{p}})^{n+1}} E_{1-k}(\tfrac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}})\\
&+ \tfrac{\lambda_{\text{sp}} e^{\frac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}} B}{\lambda_{\text{pp}}T_{\text{p}}} \sum_{n=1}^{\infty}\sum_{k=0}^{n} T_{\text{s}}^n \tfrac{\lambda_{\text{pp}}^{n+2}(-1)^{2n+2-k}}{(\lambda_{\text{sp}}T_{\text{p}})^{n+2}} \tbinom{n+1}{k} E_{1-k}(\tfrac{q\lambda_{\text{pp}}}{\lambda_{\text{sp}}T_{\text{p}}}),
\end{aligned} \quad (13)$$

where $A = \frac{1}{(1-\frac{\lambda_{\text{sp}}\lambda_{\text{ps}}}{\lambda_{\text{ss}}\lambda_{\text{pp}}})^2}$, $B = -\frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}(\frac{\lambda_{\text{ss}}\lambda_{\text{pp}}}{\lambda_{\text{sp}}\lambda_{\text{ps}}}-1)^2}$ and $C = 1 - A$. Note that although there are infinite terms in the summations of (12) and (13), the results converge very fast when truncating the summations.

In order to find Θ in (9), it can be written

$$\begin{aligned}
\Theta &= T_{\text{s}} \int_{v=0}^{\infty}\int_{u=v}^{\infty} f_{U_{\text{p}}}(v) \tfrac{1-F_{U_{\text{s}}}(u)}{1+T_{\text{s}}u}\text{d}u\text{d}v\\
&\overset{(e)}{=} T_{\text{s}}\left((F_{U_{\text{p}}}(v)-1) \int_{u=v}^{\infty} \tfrac{1-F_{U_{\text{s}}}(u)}{1+T_{\text{s}}u}\text{d}u \right)\Bigg|_0^{\infty}\\
&+ T_{\text{s}} \int_0^{\infty} \tfrac{(1-F_{U_{\text{p}}}(v))(1-F_{U_{\text{s}}}(v))}{1+T_{\text{s}}v}\text{d}v\\
&= T_{\text{s}} \int_{u=0}^{\infty} \tfrac{1-F_{U_{\text{s}}}(u)}{1+T_{\text{s}}u}\text{d}u + T_{\text{s}} \int_0^{\infty} \tfrac{e^{-(\lambda_{\text{ss}}+\lambda_{\text{sp}})v}}{(1+T_{\text{s}}v)(1+\frac{\lambda_{\text{ss}}}{\lambda_{\text{sp}}}T_{\text{p}}v)(1+\frac{\lambda_{\text{sp}}}{\lambda_{\text{pp}}}T_{\text{p}}v)}\text{d}v\\
\Theta &= \frac{e^{\frac{\lambda_{\text{ps}}}{T_{\text{p}}}} E_1(-\frac{\lambda_{\text{ps}}}{T_{\text{p}}}) - e^{\frac{\lambda_{\text{ss}}}{T_{\text{s}}}} E_1(-\frac{\lambda_{\text{ss}}}{T_{\text{s}}})}{\frac{T_{\text{p}}\lambda_{\text{ss}}}{T_{\text{s}}\lambda_{\text{ps}}}-1}\\
&+ \frac{T_{\text{s}}}{(\frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}} - \frac{\lambda_{\text{sp}}T_{\text{p}}}{\lambda_{\text{pp}}})(\frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}} - T_{\text{s}})(\frac{\lambda_{\text{sp}}T_{\text{p}}}{\lambda_{\text{pp}}} - T_{\text{s}})} \times\\
&\Bigg\{ \frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}} e^{\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{\lambda_{\text{ss}}T_{\text{p}}}\lambda_{\text{ps}}} (\frac{\lambda_{\text{sp}}T_{\text{p}}}{\lambda_{\text{pp}}} - T_{\text{s}}) E_1(-\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{\lambda_{\text{ss}}T_{\text{p}}}\lambda_{\text{ps}})\\
&- \frac{\lambda_{\text{sp}}T_{\text{p}}}{\lambda_{\text{pp}}} e^{\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{\lambda_{\text{sp}}T_{\text{p}}}\lambda_{\text{pp}}} (\frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}} - T_{\text{s}}) E_1(-\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{\lambda_{\text{sp}}T_{\text{p}}}\lambda_{\text{pp}})\\
&+ T_{\text{s}} e^{\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{T_{\text{s}}}} (\frac{\lambda_{\text{ss}}T_{\text{p}}}{\lambda_{\text{ps}}} - \frac{\lambda_{\text{sp}}T_{\text{p}}}{\lambda_{\text{pp}}}) E_1(-\frac{\lambda_{\text{sp}}+\lambda_{\text{ss}}}{T_{\text{s}}}) \Bigg\}
\end{aligned} \quad (14)$$

where (e) is obtained by partial integration and the last equality follows from some manipulations and the definition of the exponential integral function. Finally, from (9), (11)-(14), the secondary user secure ergodic achievable rate is found as $\eta = \Gamma_1 + \Gamma_2 + \Theta$.

A. Primary user quality-of-service requirements

Given that the SU is transmitting at power T_{s}, the PU instantaneous received interference power is $\varphi_{\text{p}} = G_{\text{sp}}T_{\text{s}}$. Hence, constraining the PU average received interference power to be less than β leads to

$$\mathbf{E}\{\varphi_{\text{p}}\} = \mathbf{E}\{G_{\text{sp}}T_{\text{s}}\} \leq \beta \Rightarrow T_{\text{s}} \leq \beta\lambda_{\text{sp}}. \quad (15)$$

Under a more realistic constraint, we can consider the case where the PU instantaneous received interference power is with probability π less than a threshold β. Here, according to

$$\text{Prob}\{\varphi_{\text{p}} \leq \beta\} = \text{Prob}\{G_{\text{sp}} \leq \frac{\beta}{T_{\text{s}}}\} = 1 - e^{-\lambda_{\text{sp}}\frac{\beta}{T_{\text{s}}}}, \quad (16)$$

the SU transmission power is found as $T_{\text{s}} \leq \frac{-\lambda_{\text{sp}}\beta}{\log(1-\pi)}$.

The primary user received SINR is a random variable given by $\text{SINR}_{\text{p}} = T_{\text{p}}\Delta, \Delta \doteq \frac{G_{\text{pp}}}{1+T_{\text{s}}G_{\text{sp}}}$. Therefore, using partial integration and the same procedure as in (3), the PU average received SINR is found as

$$\begin{aligned}
\mathbf{E}\{\text{SINR}_{\text{p}}\} &= T_{\text{p}} \int_{x=0}^{\infty} x f_{\Delta}(x)\text{d}x\\
&= T_{\text{p}} \int_{x=0}^{\infty} \Big(1 - F_{\Delta}(x)\Big)\text{d}x = \tfrac{T_{\text{p}}\lambda_{\text{sp}}}{\lambda_{\text{pp}}T_{\text{s}}} e^{\frac{\lambda_{\text{sp}}}{T_{\text{s}}}} E_1(\tfrac{-\lambda_{\text{sp}}}{T_{\text{s}}}),
\end{aligned} \quad (17)$$

where $f_{\Delta}(.)$ and $F_{\Delta}(.)$ are the pdf and the cdf of the random variable Δ, respectively. Hence, the SU transmission power under a PU average received SINR constraint $\mathbf{E}\{\mathrm{SINR}_\mathrm{p}\} \geq \alpha$ is obtained by

$$T_\mathrm{s} = \arg_{T_\mathrm{s}}\{\frac{\lambda_\mathrm{sp}}{\lambda_\mathrm{pp}T_\mathrm{s}} e^{\frac{\lambda_\mathrm{sp}}{T_\mathrm{s}}} E_1(\frac{-\lambda_\mathrm{sp}}{T_\mathrm{s}}) = \frac{\alpha}{T_\mathrm{p}}\}. \tag{18}$$

Finally, for the case where the PU instantaneous received SINR is with probability π higher than a given value α the SU transmission power is determined as

$$\Pr\{\mathrm{SINR}_\mathrm{p} > \alpha\} \geq \pi \ \Rightarrow T_\mathrm{s} \leq \max\left\{\frac{T_\mathrm{p}\lambda_\mathrm{sp}}{\lambda_\mathrm{pp}\alpha}(\frac{e^{\frac{-\lambda_\mathrm{pp}\alpha}{T_\mathrm{p}}}}{\pi} - 1), 0\right\}. \tag{19}$$

Here, (19) is based on the fact that $F_\Delta(x) = 1 - \frac{e^{-\lambda_\mathrm{pp}x}}{1+\frac{\lambda_\mathrm{pp}}{\lambda_\mathrm{sp}}T_\mathrm{s}x}$.

In the following, the simulation results are presented for different PU quality-of-service requirements.

IV. Simulation Results and Discussions

Considering different PU transmission powers and received interference power constaints, Fig. 2 shows the SU secure ergodic achievable rate under the PU average interference-limited condition. In all figures, we set $\lambda_\mathrm{ss} = \lambda_\mathrm{pp} = 0.1$ and $\lambda_\mathrm{ps} = \lambda_\mathrm{sp} = 1$, unless otherwise stated. Figures 3a and 3b demonstrate the SU achievable rates versus the probability constraint π in the instantaneous interference- and SINR-limited conditions, respectively. Moreover, Fig. 4 studies the SU achievable rates as a function of the PU instantaneous SINR constraint α. Finally, setting $\lambda_\mathrm{ss} = \lambda_\mathrm{sp} = \lambda_\mathrm{ps} = \lambda_\mathrm{pp} = 1$, Fig. 5 investigates the effect of the SU security constraint on its achievable rates. Here, the security gain $I = \frac{\eta}{\eta^\mathrm{unsecured}}$ is depicted for different PU transmission powers where the SU unsecured ergodic achievable rate is found by

$$\eta^\mathrm{unsecured} = \mathbf{E}\{\log(1+T_\mathrm{s}U_\mathrm{s})\} = \frac{e^{\frac{\lambda_\mathrm{ss}}{T_\mathrm{s}}}E_1(-\frac{\lambda_\mathrm{ss}}{T_\mathrm{s}}) - e^{\frac{\lambda_\mathrm{ps}}{T_\mathrm{p}}}E_1(-\frac{\lambda_\mathrm{ps}}{T_\mathrm{p}})}{1-\frac{\lambda_\mathrm{ss}T_\mathrm{p}}{\lambda_\mathrm{ps}T_\mathrm{s}}}. \tag{20}$$

The following points are deduced from the figures:

- Although there is considerable potential for the SU secure data transmission under the PU interference-limited condition (Figs. 2a and 3a), the achievable rates decrease as the PU transmission power increases (Figs. 2b and 3a).
- With a PU received SINR constraint, the PU transmission power is not necessarily something *bad* for the SU; with high PU transmission power the SU received interference increases which deteriorates the SU performance. On the other hand, the PU received SINR constraint becomes more relaxed when the PU transmission power increases. Hence, the SU transmission power can be increased, which is desirable for the SU. Therefore, depending on the fading parameters, the SU achievable rate may increase or decrease with the PU transmission power in the SINR-limited conditions (Figs. 3b and 4).

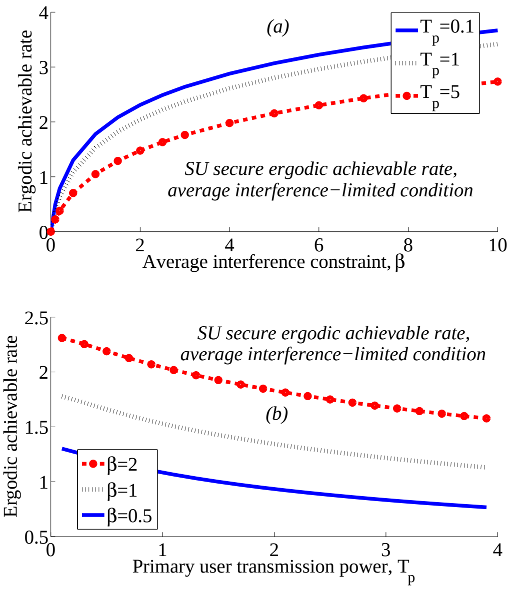

Figure 2. Secondary user secure ergodic achievable rate vs (a): the PU average received interference power constraint β and (b): the PU transmission power T_p. Average interference-limited condition, $\lambda_\mathrm{ss} = \lambda_\mathrm{pp} = 0.1$ and $\lambda_\mathrm{ps} = \lambda_\mathrm{sp} = 1$.

- Under both limited PU received interference and SINR conditions, the PU intolerability, modeled by the probability parameter π, plays a great role in the SU achievable rates; the more conservatively the PU instantaneous quality-of-service requirements should be satisfied (high values of π), the less rate is achieved at the secondary channel, converging to zero. On the other hand, the achievable rates increase as the probability constraint decreases (Figs. 3 and 4). Particularly, with a PU instantaneous received SINR constraint no data transmission is permitted in the SINRs less than the PU received signal-to-noise ratio (SNR) (Figs. 3b and 4).
- Compared to the case of unsecured data transmission, the *relative* drop of the SU achievable rate, due to the security constraint, is more when the PU transmission power decreases or the PU received interference constraint gets more relaxed (Fig. 5). That is, the SU security constraint becomes more important when the PU received SINR decreases.

V. Conclusion

This paper studies the secure ergodic achievable rate of the spectrum sharing networks under different PU interference- and SINR-limited conditions. The achievable rates are obtained under the constraint that the SU massages should not be decodable by the PU receiver. The results show that under different PU quality-of-service constraints there is considerable potential for the SU secure data transmission. Moreover, depending on the channel condition, the SU achievable rates may increase with the PU transmission power under a PU received SINR constraint. Finally, for both interference- and SINR-limited conditions, the PU tolerability to the received interference plays a great role in the SU achievable rates.

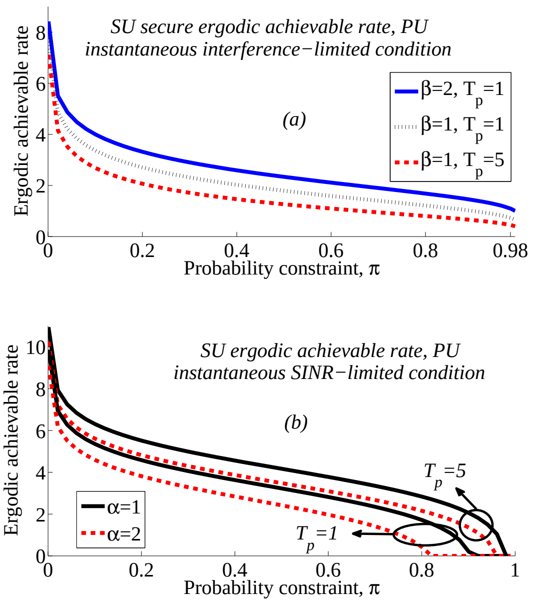

Figure 3. Secondary user secure ergodic achievable rate vs the probability constraint π. (a): Instantaneous interference-limited and (b): instantaneous SINR-limited condition, $\lambda_{ss} = \lambda_{pp} = 0.1$ and $\lambda_{ps} = \lambda_{sp} = 1$.

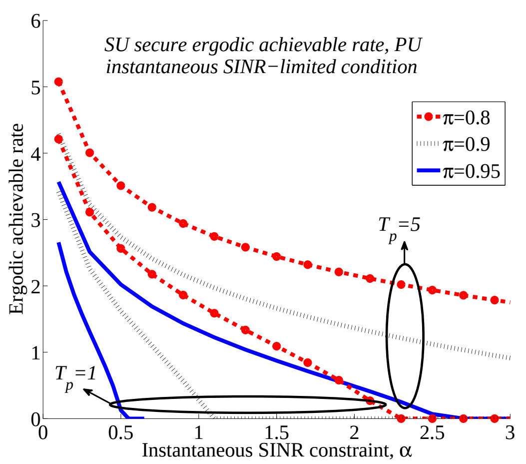

Figure 4. Secondary user secure ergodic achievable rate vs the PU instantaneous received SINR constraint, $\lambda_{ss} = \lambda_{pp} = 0.1$ and $\lambda_{ps} = \lambda_{sp} = 1$.

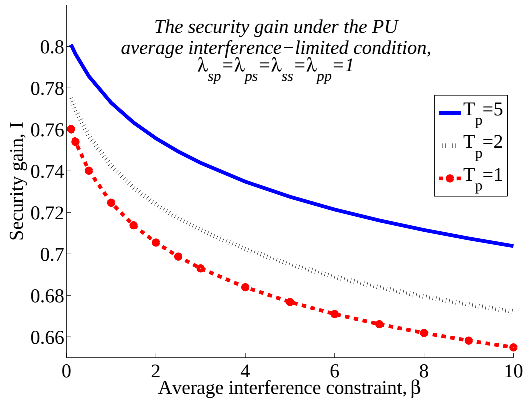

Figure 5. The security gain vs the PU average received interference constraint, $\lambda_{ss} = \lambda_{pp} = \lambda_{ps} = \lambda_{sp} = 1$.

References

[1] F. Berggren, et. al, "Dynamic spectrum access, phase 1: scenarios and research challenges," Sept. 2004, available: http://www.queseth.se/olav/pubs/DSAReportPhase1.pdf.

[2] W. D. Horne, "Adaptive spectrum access: using the full spectrum space," 2003, available: http://intel.si.umich.edu/tprc/papers/2003/225/Adaptive_Spectrum_Horne.pdf.

[3] S. M. Mishra, et. al, "Cooperative sensing among cognitive radios," in *ICC*, vol. 4, June 2006, pp. 1658–1663.

[4] S. A. Jafar and S. Srinivasa, "Capacity limits of cognitive radio with distributed and dynamic spectral activity," *IEEE Journal on Selected Areas in Commun.*, vol. 25, no. 3, pp. 529–537, April 2007.

[5] N. Devroye, et. al, "Cognitive radio networks," *IEEE Signal Processing Magazine*, vol. 25, no. 6, pp. 12–23, Nov. 2008.

[6] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. on Info. Theory*, vol. 53, no. 2, pp. 471–487, Feb. 2007.

[7] Y. Xing, et. al, "Dynamic spectrum access with QoS and interference temperature constraints," *IEEE Trans. on Mobile Computing*, vol. 6, no. 4, pp. 423–433, April 2007.

[8] B. Makki and T. Eriksson, "On the ergodic achievable rates of spectrum sharing networks with finite backlogged primary users and an interference indicator signal," *IEEE Trans. on Wireless Commun.*, vol. 11, no. 9, pp. 3079–3089, Sept. 2012.

[9] X. Kang, et. al, "Optimal power allocation for fading channels in cognitive radio networks: Ergodic capacity and outage capacity," *IEEE Trans. on Wireless Commun.*, vol. 8, no. 2, pp. 940–950, Feb. 2009.

[10] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Trans. on Wireless Commun.*, vol. 6, no. 2, pp. 649–658, Feb. 2007.

[11] C.-X. Wang, et. al, "On capacity of cognitive radio networks with average interference power constraints," *IEEE Trans. on Wireless Commun.*, vol. 8, no. 4, pp. 1620–1625, April 2009.

[12] L. Musavian and S. Aissa, "Capacity and power allocation for spectrum-sharing communications in fading channels," *IEEE Trans. on Wireless Commun.*, vol. 8, no. 1, pp. 148–156, Jan. 2009.

[13] B. Makki and T. Eriksson, "On the average rate of HARQ-based quasi-static spectrum sharing networks," *IEEE Trans. on Wireless Commun.*, vol. 11, no. 1, pp. 65–77, Jan. 2012.

[14] N. Mokari, K. Navaie, and M. G. Khoshkholgh, "Downlink radio resource allocation in OFDMA spectrum sharing environment with partial channel state information," *IEEE Trans. on Wireless Commun.*, vol. 10, no. 10, pp. 3482–3495, Oct. 2011.

[15] B. Makki, et. al, "HARQ feedback in spectrum sharing networks," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1337–1340, Sept. 2012.

[16] B. Makki and T. Eriksson, "Capacity bounds of spectrum sharing networks with no channel state information," in *European Wireless*, April 2011, pp. 1–5.

[17] L. Musavian and S. Aissa, "Fundamental capacity limits of cognitive radio in fading environments with imperfect channel information," *IEEE Trans. on Commun.*, vol. 57, no. 11, pp. 3472–3480, Nov. 2009.

[18] H. A. Suraweera, et. al, "Capacity limits and performance analysis of cognitive radio with imperfect channel knowledge," *IEEE Trans. on Veh. Tech.*, vol. 59, no. 4, pp. 1811–1822, May 2010.

[19] B. Makki and T. Eriksson, "On the capacity of rayleigh-fading correlated spectrum sharing networks," *Eura. J. on Wireless Commun. and Net.*, vol. 2011, Aug. 2011, doi:10.1186/1687-1499-2011-83.

[20] S. Sesia, et. al, "Incremental redundancy hybrid ARQ schemes based on low-density parity-check codes," *IEEE Trans. on Commun.*, vol. 52, no. 8, pp. 1311–1321, Aug. 2004.

[21] J. Kim, et. al, "Design of rate-compatible irregular LDPC codes for incremental redundancy hybrid ARQ systems," in *ISIT*, July 2006, pp. 1139–1143.

[22] N. Varnica, et. al, "LDPC code ensembles for incremental redundancy hybrid ARQ," in *ISIT*, Sept. 2005, pp. 995–999.

[23] "Trellisware technologies, white papers on flexicodes and F-LDPC," available: www.trellisware.com.