Secure Broadcasting over Fading Channels with Statistical QoS Constraints

Deli Qiao, Mustafa Cenk Gursoy, and Senem Velipasalar
Department of Electrical Engineering
University of Nebraska-Lincoln, Lincoln, NE 68588
Email: dqiao726@huskers.unl.edu, gursoy@engr.unl.edu, velipasa@engr.unl.edu

Abstract—In this paper, the fading broadcast channel with confidential messages is studied in the presence of statistical quality of service (QoS) constraints in the form of limitations on the buffer length. We employ the effective capacity formulation to measure the throughput of the confidential and common messages. We assume that the channel side information (CSI) is available at both the transmitter and the receivers. Assuming average power constraints at the transmitter side, we first define the effective secure throughput region, and prove that the throughput region is convex. Then, we obtain the optimal power control policies that achieve the boundary points of the effective secure throughput region.

I. INTRODUCTION

Security is an important issue in wireless systems due to the broadcast nature of wireless transmissions. In a pioneering work, Wyner in [1] addressed the security problem from an information-theoretic point of view and considered a wire-tap channel model. He proved that secure transmission of confidential messages to a destination in the presence of a degraded wire-tapper can be achieved, and he established the secrecy capacity which is defined as the highest rate of reliable communication from the transmitter to the legitimate receiver while keeping the wire-tapper completely ignorant of the transmitted messages. Recently, there has been numerous studies addressing information theoretic security. For instance, the impact of fading has been investigated in [2], where it has been shown that a non-zero secrecy capacity can be achieved even when the eavesdropper channel is better than the main channel on average. The secrecy capacity region of the fading broadcast channel with confidential messages and associated optimal power control policies have been identified in [4], where it is shown that the transmitter allocates more power as the strength of the main channel increases with respect to that of the eavesdropper channel.

In addition to security issues, providing acceptable performance and quality is vital to many applications. For instance, voice over IP (VoIP) and interactive-video (e.g., videoconferencing) systems are required to satisfy certain buffer or delay constraints. In this paper, we consider statistical QoS constraints in the form of limitations on the buffer length, and incorporate the concept of effective capacity [5], which can be seen as the maximum constant arrival rate pairs that can be supported while satisfying statistical QoS guarantees. The analysis and application of effective capacity in various settings have attracted much interest recently (see e.g., [6]–[8] and references therein). We define the effective secrecy throughput region as the maximum constant arrival rate pairs that can be supported while the service rate is confined by the secrecy capacity region. We assume that the channel side information is known at both the transmitter and receivers. Then, following a similar analysis as shown in [4], we obtain the optimal power allocation policies that achieve points on the boundary of the effective secrecy throughput region.

The rest of the paper is organized as follows. Section II briefly describes the system model and the necessary preliminaries on statistical QoS constraints and effective capacity. In Section III, we present our main results on the optimal power control policies. Finally, Section IV concludes the paper.

II. SYSTEM MODEL AND PRELIMINARIES

A. System Model

We consider a scenario in which a single transmitter broadcasts messages to two receivers. The transmitter wishes to send receiver 1 confidential messages that need to kept secret from receiver 2, and also at the same time send common messages to both receivers. A depiction of the system model is given in Figure 1. It is assumed that the transmitter generates data sequences which are divided into frames of duration \(T\). These data frames are initially stored in the buffer before they are transmitted over the wireless channel. The channel input-
output relationships are given by

$$Y_i[i] = h_1[i]X[i] + Z_1[i] \text{ and } Y_2[i] = h_2[i]X[i] + Z_2[i] \quad (1)$$

where $i$ is the frame index, $X[i]$ is the channel input in the $i$th frame, and $Y_1[i]$ and $Y_2[i]$ represent the channel outputs at the receivers 1 and 2 at frame $i$, respectively. We assume that $\{h_j[i], j = 1, 2\}$’s are jointly stationary and ergodic discrete-time processes, and we denote the magnitude-square of the fading coefficients by $z_j[i] = |h_j[i]|^2$. Considering that receiver 1 is the main user to which we send both the common and confidential messages, while receiver 2, to which we send only the common messages, can be regarded as an eavesdropper for the confidential messages, we replace $z_1$ with $z_M$ and $z_2$ with $z_E$ to increase the clarity in the subsequent formulations. The channel input is subject to an average power constraint $\mathbb{E}\{|X[i]|^2\} \leq P$, and we assume that the bandwidth available for the system is $B$. Above, $Z_j[i]$ is a zero-mean, circularly symmetric, complex Gaussian random variable with variance $\mathbb{E}\{|Z_j[i]|^2\} = N_j$. The additive Gaussian noise samples $\{Z_j[i]\}$ are assumed to form an independent and identically distributed (i.i.d.) sequence.

Note that we denote the average transmitted signal-to-noise ratio with respect to receiver 1 as $\text{SNR} = \frac{P}{P + 1}$. We also denote $P[i]$ as the instantaneous transmit power in the $i$th frame. Now, the instantaneous transmitted SNR level for receiver 1 becomes $\mu_1[i] = \frac{P[i]}{\text{SNR} + 1}$. Then, the average power constraint at the base station is equivalent to the average SNR constraint $\mathbb{E}\{\mu_1[i]\} \leq \text{SNR}$ for receiver 1. If we denote the ratio between the noise powers of the two channels as $\gamma = \frac{N_M}{N_E}$, the instantaneous transmitted SNR level for receiver 2 becomes $\mu_2[i] = \gamma \mu_1[i]$.

We denote $z = (z_E, z_M)$ as the vector composed of the channel states for receivers 2 and 1. Under the block fading assumption, the maximal instantaneous service rate is decided by the secrecy capacity region of the Gaussian broadcast channel with confidential messages (BCC) for each channel with a pair of specific channel states realization $(z_E, z_M)$. We define $\mu = (\mu_0(z), \mu_1(z))$ as the power allocation policies for the common and confidential messages, respectively. We denote the region $Z = \{z: z_M > \gamma z_E\}$ as the region in which both confidential and common messages are transmitted. $Z^c$ represents the region where $z_M \leq \gamma z_E$. If $z$ lies in $Z^c$, only the common messages are transmitted. Note that $\mu_1(z) = 0$ for $z \in Z^c$. We then define the set $U$ as the power allocation policies satisfying the power constraints

$$U = \{\mu: \mathbb{E}_{z \in Z}\{\mu_0(z) + \mu_1(z)\} + \mathbb{E}_{z \in Z^c}\{\mu_0(z)\} \leq \text{SNR}\}. \quad (2)$$

With the above notations, the secrecy capacity region of the fading BCC is given by [4]

$$\mathcal{R}_s = \bigcup_{\mu \in U} \left\{ (R_0, R_1): \begin{array}{l}
R_0 \leq \min \left\{ \begin{array}{l}
\mathbb{E}_{z \in Z}\{\log_2 \left( 1 + \frac{\mu_0(z)z_M}{1 + \gamma \mu_1(z)z_E} \right) \}
+ \mathbb{E}_{z \in Z^c}\{\log_2 \left( 1 + \frac{\mu_0(z)z_M}{1 + \gamma \mu_1(z)z_E} \right) \}
\end{array} \right\}
\right\}$$

$$R_1 \leq \mathbb{E}_{z \in Z}\{\log_2 \left( 1 + \mu_1(z)z_M \right) - \log_2 \left( 1 + \gamma \mu_1(z)z_E \right) \} \quad (3)$$

B. Statistical QoS Constraints and Effective Secure Throughput

In [5], Wu and Negi defined the effective capacity as the maximum constant arrival rate that a given service process can support in order to guarantee a statistical QoS requirement specified by the QoS exponent $\theta$. If we define $Q$ as the stationary queue length, then $\theta$ is the decay rate of the tail distribution of the queue length $Q$:

$$\lim_{q \to \infty} \frac{\log P(Q \geq q)}{q} = -\theta. \quad (4)$$

Therefore, for large $q_{\text{max}}$, we have the following approximation for the buffer violation probability: $P(Q \geq q_{\text{max}}) \approx e^{-\theta q_{\text{max}}}$. Hence, while larger $\theta$ corresponds to more strict QoS constraints, smaller $\theta$ implies looser QoS guarantees. Similarly, if $D$ denotes the steady-state delay experienced in the buffer, then $P(D \geq d_{\text{max}}) \approx e^{-\theta d_{\text{max}}}$ for large $d_{\text{max}}$, where $\delta$ is determined by the arrival and service processes [7].

The effective capacity is given by

$$C(\theta) = -\frac{\Lambda(-\theta)}{\theta} = -\lim_{t \to \infty} \frac{1}{\theta t} \log_e \mathbb{E}\{e^{-\theta S[t]}\} \text{ bits/s,} \quad (5)$$

where the expectation is with respect to $S[t] = \sum_{i=1}^t s[i]$, which is the time-accumulated service process. $S[i], i = 1, 2, \ldots$ denote the discrete-time stationary and ergodic stochastic service process. We define the effective capacity region obtained when the service rate is confined by the secrecy capacity region as the effective secrecy throughput region.

In this paper, in order to simplify the analysis while considering general fading distributions, we assume that the fading coefficients stay constant over the frame duration $T$ and vary independently for each frame and each user. In this scenario, $s[i] = TR[i]$, where $R[i]$ is the instantaneous service rate for common or confidential messages in the $i$th frame duration $[iT; (i+1)T)$. Then, [5] can be written as

$$C(\theta) = -\frac{1}{\theta T} \log_e \mathbb{E}\{e^{-\theta TR[i]}\} \text{ bits/s,} \quad (6)$$

where $R[i]$ denotes the instantaneous rate sequence with respect to $z$. [6] is obtained using the fact that instantaneous rates $\{R[i]\}$ vary independently. The effective secrecy throughput normalized by bandwidth $B$ is

$$C(\theta) = \frac{C(\theta)}{B} \text{ bits/s/Hz.} \quad (7)$$

III. Effective Secrecy Throughput Region

In this section, we investigate the fading broadcast channel with confidential message (BCC) by incorporating the statistical QoS constraints. Liang et al. in [4] have shown that the fading channel can be viewed as a set of parallel subchannels with each corresponding to one fading state. In [4], it has been assumed that no delay constraints are imposed on the

2For time-varying arrival rates, effective capacity specifies the effective bandwidth of the arrival process that can be supported by the channel.
transmitted messages. Under such an assumption, the ergodic secrecy capacity region is determined and the optimal power allocation policies achieving the boundary of the capacity region are identified.

In this paper, we analyze the performance under statistical buffer constraints by considering the effective capacity formulation. According to the formula for effective capacity (6), we first have the following result.

**Proposition 1:** The effective secure throughput region of the fading BCC is

\[
C_{es} = \bigcup_{\mu \in \mathcal{U}} \left\{ (C_0, C_1) : C_j \leq -\frac{1}{\theta T} \log_e \mathbb{E}\{e^{-\theta T R[i]}\}, \quad \right.
\]

subject to \( \forall \mathbb{E}\{R\} \in C_s \) \hspace{1cm} (8)

where \( R = (R_0, R_1) \) is the vector composed of the instantaneous rates for the common and confidential messages, respectively.

We assume that \( \mathbb{E}\{R\} \) can take any possible value defined in the ergodic secrecy capacity region \( C_s \). Since the secrecy capacity region is convex [4], we can easily prove the following.

**Theorem 1:** The effective secure throughput region is convex.

**Proof:** Let the two effective capacity pairs \( C_1 = (C_{10}, C_{11}) \) and \( C_2 = (C_{20}, C_{21}) \) belong to \( C_s \). Therefore, there exists some \( R[i] \) and \( R'[i] \) for \( C_1(\Theta) \) and \( C_2(\Theta) \), respectively. By a time sharing strategy, for any \( \alpha \in (0, 1) \), we know that \( \mathbb{E}\{\alpha R[i] + (1-\alpha)R'[i]\} \in \mathcal{R}_s \).

\[
\alpha C_1 + (1-\alpha)C_2
\]

Next, we derive the optimal power allocation \( \mu_* \) that solves (10) for the different cases detailed above. Note that the maximal confidential message rate is defined as

\[
\text{Lemma 1:} \quad \text{The optimal } \mu^* \text{ that solves (10) falls into the one of the following three cases:}
\]

Case I: \( R_{01}(\mu^*) < R_{02}(\mu^*) \) and \( \mu^* \) maximizes \( \lambda_0 C_0(\mu) + \lambda_1 C_1(\mu) \);

Case II: \( R_{01}(\mu^*) > R_{02}(\mu^*) \) and \( \mu^* \) maximizes \( \lambda_0 C_0(\mu) + \lambda_1 C_1(\mu) \);

Case III: \( R_{01}(\mu^*) = R_{02}(\mu^*) \) then

A) \( \mu^* \) maximizes \( \lambda_0 C_0(\mu) + \lambda_1 C_1(\mu) \), if \( C(\mu) > C_2(\mu) \);

B) \( \mu^* \) maximizes \( \lambda_0 C_0(\mu) + \lambda_1 C_1(\mu) \), if \( C(\mu) < C_2(\mu) \);

C) \( \mu^* \) maximizes \( \lambda_0 (\delta C_0(\mu) + (1-\delta)C_2(\mu)) + \lambda_1 C_1(\mu) \), if there exists \( 0 \leq \delta \leq 1 \) such that \( C_0(\mu) = C_2(\mu) \).

(11)

Above, \( R_{01}(\mu) \) and \( R_{02}(\mu) \) are the two terms that \( R_0(\mu) \) can take in the minimization in (3), and \( C_{01}(\mu) \) and \( C_{02}(\mu) \) are the associated effective throughput values.

Next, we derive the optimal power allocation \( \mu^* \) that solves (10) for the different cases detailed above. Note that the maximal confidential message rate is defined as

\[
R_{01}(\mu) = \left\{ \begin{array}{ll}
\log_2 \left( \frac{1}{\lambda_0 z M + \lambda_1 z} \right), & z \in \mathcal{Z} \\
0, & z \in \mathcal{Z}^c
\end{array} \right.
\]

(12)

**Case I:** The maximal instantaneous common message rate is given by the rate of receiver 1

\[
R_{01}(\mu) = \left\{ \log_2 \left( \frac{1 + \mu_0(z) z M}{1 + \mu_1(z) z M} \right), \quad z \in \mathcal{Z} \\
\log_2 \left( \frac{1 + \mu_0(z) z M}{1 + \mu_1(z) z M} \right), \quad z \in \mathcal{Z}^c
\}
\]

(13)

as long as the obtained power control policy satisfies

\[
R_{01}(\mu) < R_{02}(\mu).
\]

(14)

Then, the Lagrangian is given by

\[
J = \frac{1}{\beta \log_2 e} \log_2 \left( \frac{1 + \mu_0(z) z M - \beta \rho(z, z M, z, p_x) + \int_{z \in \mathcal{Z}} \rho(z, z M, z, p_x) dz}{1 + \mu_1(z) z M - \beta \rho(z, z M, z, p_x) + \int_{z \in \mathcal{Z}} \rho(z, z M, z, p_x) dz} \right)
\]

(15)

With specific power control policies, the values of \( (C_0, C_1) \) are determined. Hence, we can define the following

\[
\phi_0 = \int_{z \in \mathcal{Z}} \left( 1 + \frac{\mu_0(z) z M}{1 + \mu_1(z) z M} \right) - \beta \rho(z, z M, z, p_x) dz
\]

(16)

\[
\phi_1 = \int_{z \in \mathcal{Z}} \left( 1 + \frac{\mu_1(z) z M}{1 + \mu_1(z) z M} \right) - \beta \rho(z, z M, z, p_x) dz
\]

(17)

Although implicitly, \( \phi_0 \) and \( \phi_1 \) in the other cases in the following analysis can be defined similarly. These two equa-
sions can be viewed as additional constraints that the power control policies need to satisfy, i.e., the right hand side (RHS) of the two equations are also functions of \((\phi_0, \phi_1)\), denoted as \(\phi(\phi_0, \phi_1)\). Since the power control policies \(\mu\) depend on \((\phi_0, \phi_1)\). Now that \(\phi_0\) and \(\phi_1\) take values from \([0, 1]\) and the RHS function takes values from \([0, 1]\), we can find the solution through an iterative algorithm according to the fixed-point theorem.\(^3\)

It is clear that \((\mu_0, \mu_1)\) are the solutions to the following

\[
\frac{\lambda_0}{\phi_0 \log_e 2} \left(1 + \mu_0 z M\right)^{-\beta - 1} z M - \kappa = 0 \tag{18}
\]

\[
\frac{\lambda_0}{\phi_0 \log_e 2} \left(1 + \frac{\mu_0 z M}{1 + \mu_1 z M}\right)^{-\beta - 1} z M - \frac{1 + \mu_0 z M}{1 + \mu_1 z M} \kappa = 0 \tag{19}
\]

\[
- \frac{\lambda_0}{\phi_0 \log_e 2} \left(1 + \frac{\mu_0 z M}{1 + \mu_1 z M}\right)^{-\beta - 1} \frac{\mu_0 z M^2}{(1 + \mu_1 z M)^2} - \frac{1 + \mu_0 z M}{1 + \mu_1 z M} \kappa = 0 \tag{20}
\]

where \((18)-(20)\) are obtained by taking the derivative of \(J\) with respect to \(\mu_0\) for \(z \in Z^c\), \(\mu_0\) for \(z \in Z\), and \(\mu_1\) for \(z \in Z\), respectively. Whenever \(\mu_0\) and \(\mu_1\) turn out to have negative values through these equations, they are set to 0 according to the convexity of the optimization problem. Although the closed form expressions for \((\mu_0, \mu_1)\) are hard to find, we can get some insight by examining \((18)-(20)\). Define \(\alpha_1 = \frac{\lambda_0 \phi_0 \log_e 2}{\lambda_0}\) and \(\alpha_2 = \frac{\lambda_0 \phi_1 \log_e 2}{\lambda_0}\), which are chosen to satisfy the average power constraint \((3)\) with equality. Not surprisingly, \(\mu_0\) in \(Z^c\) behaves similarly as in point-to-point transmission \((6)\). Now, consider \((20)\). In order for \(\mu_1\) to have a nonnegative value, the following should be satisfied

\[
\frac{z M - \gamma z E}{\alpha_2} - 1 \geq 0. \tag{21}
\]

If \(\mu_0 = 0\), we have from \((20)\) that

\[
\frac{1}{\alpha_2} \left(1 + \frac{\mu_0 z M}{1 + \mu_1 z M}\right)^{-\beta - 1} \frac{z M - \gamma z E}{(1 + \mu_1 z M)^2} = 1 \tag{22}
\]

After a simple computation using \((19)\), we get

\[
\frac{\mu_0 z M}{1 + \mu_1 z M} = \left(\frac{z M}{\alpha_1 (1 + \mu_1 z M)}\right)^\alpha_1 - 1 \tag{23}
\]

which gives us that \(\mu_0 < 0\) if

\[
\frac{z M}{\alpha_1 (1 + \mu_1 z M)} < 1. \tag{24}
\]

This tells us that when the power allocated to confidential message is large enough, there should be no common message transmission. Furthermore, substituting \((19)\) and \((22)\) into \((20)\), we have

\[
\frac{1}{\alpha_2} \left(1 + \frac{\mu_0 z M}{1 + \mu_1 z M}\right)^{-\beta - 1} \frac{z M - \gamma z E}{(1 + \mu_1 z M)^2} \left(\frac{z M}{\alpha_1 (1 + \mu_1 z M)}\right)^\alpha_1 = 0 \tag{25}
\]

This is for the case when both \(\mu_0\) and \(\mu_1\) turn out to

\(^3\)Although trivially, either \(\phi_0\) or \(\phi_1\) taking value 0 or 1 will at the same time turn out to be some value in \((0,1)\) for the function \(\phi(\phi_0, \phi_1)\), which tells us that the solution of \(\phi_0\) or \(\phi_1\) is in \((0,1)\).
(µ₀, µ₁) are the solutions to the following
\[ \frac{\lambda_0}{\phi_0 \log_e 2} (1 + γµ₀z_E)^{−β−1}γz_E − κ = 0 \]
\[ \frac{\lambda_0}{\phi_0 \log_e 2} (1 + γµ₀z_E)^{−β−1}γz_E − \frac{1 + µ₁z_M}{1 + µ₁z_E} z_M = 0 \]
\[ \frac{\lambda_0}{\phi_1 \log_e 2} (1 + γµ₁z_E)^{−β−1}γz_E − \frac{1 + µ₁z_M}{1 + µ₁z_E} z_M = 0 \]
where (29)-(31) are obtained by taking the derivative of \( J \) with respect to \( µ₀ \) for \( z \in \mathbb{Z}^c \), \( µ₀ \) for \( z \in \mathbb{Z} \), and \( µ₁ \) for \( z \in \mathbb{Z} \), respectively. Whenever \( µ₀ \) or \( µ₁ \) turns out to have negative values through these equations, they are again set to 0.

Following a similar analysis as shown for Case I, we obtain the following algorithm to determine the optimal power control policies.

**Algorithm PC-II (Power Control II)**

1. Given \( λ₀, λ₁, \) obtain \( κ^*, φ₀^*, φ₁^*; \)
2. Denote \( α₁ = \frac{κ^* φ₀^* \log_e 2}{λ₀}, \) \( α₂ = \frac{κ^* φ₁^* \log_e 2}{λ₁}; \)
3. if \( z_M − γz_E > α₂ \) then Compute \( µ₁ \) from (22);
   4. if \( µ₁ > \frac{1}{α₁} − \frac{1}{α₂} \) or \( γz_E < α₁ \) then \( µ₀ = 0; \)
5. else if \( \frac{z_M − γz_E}{α₁} > \left( \frac{γz_E}{α₁} \right)_{γz_E} \) then \( µ₀ = \left[ \frac{1}{α₁} (γz_E)^{−γz_E} − 1 \right]^{−1}_{γz_E}; \)
6. else \( µ₁ = 0, µ₀ = \left[ \frac{1}{α₁} (γz_E)^{−γz_E} − 1 \right]^{−1}_{γz_E}; \)
7. else \( µ₁ = 0, µ₀ = \left[ \frac{1}{α₁} (γz_E)^{−γz_E} − 1 \right]^{−1}_{γz_E}; \)
8. \( \frac{λ₀}{\phi_0 \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M = 0 \)
9. \( \frac{λ₀}{\phi_0 \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M + (1 − δ) \left( 1 + \gamma µ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} = 0 \)
10. \( \frac{λ₀}{\phi_1 \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M + (1 − δ) \left( 1 + \gamma µ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} = 0 \)

where \( κ^*, φ₀^*, φ₁^* \) can be numerically computed to satisfy the average power constraint.

According the above optimal power allocation policy of \((µ₀, µ₁)\), in contrast to Case I, the condition (27) indicates that the power allocated to \( µ₁ \) is small such that the interference from sending confidential messages can be ignored in \( R₀₁(µ) \), i.e., smaller effective secrecy throughput.

**Case III:** The first two sub-cases A) and B) are trivial because, other than the condition \( R₀₁(µ) = R₀₂(µ) \), there is no difference in the power allocation policies from what we have derived in Case I and Case II. We are more interested in the case in which there is 0 < \( δ^* < 1 \) decided by the following condition
\[ R₀₁(µ^{δ^*}) = R₀₂(µ^{δ^*}) \text{ and } C₀₁(µ^{δ^*}) = C₀₂(µ^{δ^*}). \] (32)
We will first derive the optimal power control policies for any given \( δ^* \), and then determine \( δ^* \).

The Lagrangian is given by
\[ \mathcal{J} = -\frac{\lambda₀}{β \phi_0 \log_e 2} \left( \frac{δ \log_e \left( \int_{x \in \mathbb{Z}} \left( 1 + \gamma µ₀ z_E \right)^{−β} p_a(z_M, z_E) \right)}{\int_{x \in \mathbb{Z}} \left( 1 + \gamma µ₀ z_E \right)^{−β} p_a(z_M, z_E) \right)} \]
\[ + (1 - δ) \left( 1 + \gamma µ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} \]
\[ + \left( \frac{λ₀}{φ₁ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M + (1 - δ) \left( 1 + γµ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} \right) \]
\[ - \frac{λ₁}{α₁ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M - \frac{λ₀}{α₂ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M = 0 \]
(33)
where (29)-(31) are obtained by taking the derivative of \( J \) with respect to \( µ₀ \) for \( z \in \mathbb{Z}^c \), \( µ₀ \) for \( z \in \mathbb{Z} \), and \( µ₁ \) for \( z \in \mathbb{Z} \), respectively. Similarly as before, whenever \( µ₀ \) or \( µ₁ \) have negative values through these equations, they are set to 0. Considering (33), we see that when \( µ₀ = 0, µ₁ \) needs to satisfy
\[ \frac{λ₀}{φ₀ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M + (1 - δ) \gamma z_E - κ ≤ 0 \]
and \( µ₁ \) is given by (36)
\[ \frac{λ₁}{φ₁ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M - κ = 0 \]
(37)

When \( µ₁ = 0, µ₀ \) is given by
\[ \frac{λ₀}{φ₀ \log_e 2} \left( \frac{δ \log_e \left( \int_{x \in \mathbb{Z}} \left( 1 + \gamma µ₀ z_E \right)^{−β} p_a(z_M, z_E) \right)}{\int_{x \in \mathbb{Z}} \left( 1 + \gamma µ₀ z_E \right)^{−β} p_a(z_M, z_E) \right)} \]
\[ + (1 - δ) \left( 1 + γµ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} \frac{µ₀ z_M}{1 + µ₁ z_E} \]
\[ + \left( \frac{λ₀}{φ₁ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M + (1 - δ) \left( 1 + γµ₀ z_E \right)^{−β} \frac{µ₀ z_M}{1 + µ₁ z_E} \right) \]
\[ - \frac{λ₁}{α₁ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M - \frac{λ₀}{α₂ \log_e 2} \left( \frac{δz_M}{1 + µ₀z_M} \right)^{−β−1} z_M = 0 \]
(38)
Now, for $\mu_1 \geq 0$, we need to have the following

$$-\frac{\lambda_0}{\phi_0 \log_e 2} \left( \delta(1 + \mu_0 z_M) - \beta - 1 \middle( \mu_0 z_M \right)^{2} + (1 - \delta)(1 + \gamma \mu_0 z_E) - \beta - 1 \mu_0 z_E)^{2} \right) + \frac{\lambda_1 (z_M - \gamma z_E)}{\phi_1 \log_e 2} - \kappa \geq 0$$

(40)

where $\mu_0$ is computed from (39).

For any $\delta$, we need to find the associated power control policy $(\mu_0, \mu_1)$ satisfying (38), (39). Then, we need to further search over $0 < \delta < 1$ for $\delta^*$ that satisfies

$$C_{01}(\mu^*) = C_{02}(\mu).$$

(41)

We obtain the following algorithm to determine the optimal power control policies.

**ALGORITHM PC-III-C (Power Control III - C)**

1. Given $\lambda_0, \lambda_1$, obtain $\kappa^*, \phi_0*, \phi_1*$;
2. Denote $\alpha_1 = \frac{\kappa^* \phi_0^* \log_e 2}{\lambda_0}, \alpha_2 = \frac{\kappa^* \phi_1^* \log_e 2}{\lambda_1}$;
3. if $z_M - \gamma z_E > \alpha_2$
   4. then Compute $\mu_1$ from (38);
   5. if (37) holds or $\delta z_M + (1 - \delta) \gamma z_E < \alpha_1$;
   6. then $\mu_1 = 0$;
   7. else if (40) holds
   8. then Compute $\mu_0$ and $\mu_1$ from (35) and (36);
   9. else $\mu_1 = 0, \mu_0$ is given by (39);
10. else $\mu_1 = 0, \mu_0$ is given by (39);

where $\kappa^*, \phi_0^*, \phi_1^*$ can be numerically computed to satisfy the average power constraint.

Based on the previous results, we have the following algorithm to find the optimal power control policies.

**ALGORITHM PC (Power Control)**

1. Find $\mu_1^{(1)}$ given in Case I;
2. if $R_{01}(\mu_1^{(1)}) < R_{02}(\mu_1^{(1)})$
3. then $\mu^* = \mu_1^{(1)}$;
4. else if $R_{01}(\mu_1^{(1)}) = R_{02}(\mu_1^{(1)})$ and $C_{01}(\mu) > C_{02}(\mu)$
5. then $\mu^* = \mu_1^{(1)}$;
6. else Find $\mu_2^{(2)}$ given in Case II;
7. if $R_{01}(\mu_2^{(2)}) > R_{02}(\mu_2^{(2)})$
8. then $\mu^* = \mu_2^{(2)}$;
9. else if $R_{01}(\mu_2^{(2)}) = R_{02}(\mu_2^{(2)})$ and $C_{01}(\mu) < C_{02}(\mu)$
10. then $\mu^* = \mu_2^{(2)}$;
11. else For a given $\delta$, find $\mu_3^{(3)}$ given in Case III-C;
12. Search over $0 \leq \delta \leq 1$ to find $\delta$ that satisfies
13. $R_{01}(\mu_3^{(3)}) = R_{02}(\mu_3^{(3)})$ and $C_{01}(\mu_3^{(3)}) = C_{02}(\mu_3^{(3)})$
14. $\mu^* = \mu_3^{(3)}$.

In Fig. 2 we plot the achievable effective secrecy throughput region in Rayleigh fading channel. We assume that $\gamma = 1$, i.e., the noise variances at both receivers are equal. In the figure, the circles fall into Case I or Case III-A, and the pluses fall into Case II or Case III-B, and Case III-C is shown as line only.

IV. CONCLUSION

In this paper, we have investigated the fading broadcast channels with confidential message under statistical QoS constraints. We have first defined the effective secrecy throughput region, which was later proved to be convex. Then, the problem of finding points on the boundary of the throughput region is shown to be equivalent to solving a series of optimization problem. We have extended the approach used in previous studies to the scenario considered in this paper. Following similar steps, we have determined the conditions satisfied by the optimal power control policies. In particular, we have identified the algorithms for computing the power allocated to each fading state from the optimality conditions. Numerical results are provided as well.

REFERENCES

[1] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol. 54, pp. 1355-1387, Oct. 1975.
[2] P. Gopala, L. Lai, and H. El Gamal, “On the secrecy capacity of fading channels,” IEEE Trans. Inform. Theory, vol. 54, no. 10, pp. 4678-4698, Oct. 2008.
[3] Y. Liang, V. V. Veeravalli, and H. V. Poor, “Resource allocation for wireless fading relay channels: Max-min solution,”IEEE Trans. Infom. Theory, vol. 53, no. 10, pp. 3432-3453, Oct. 2007.
[4] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,”IEEE Trans. Inform. Theory, vol. 54, pp. 2470-2492, June 2008.
[5] D. Wu and R. Negi “Effective capacity: a wireless link model for support of quality of service,”IEEE Trans. Wireless Commun., vol.2.no. 4, pp.630-643, July 2003
[6] J. Tang and X. Zhang, “Quality-of-service driven power and rate adaptation over wireless links,” IEEE Trans. Wireless Commun., vol. 6, no. 8, pp. 3058-3068, Aug. 2007.
[7] J. Tang and X. Zhang, “Cross-layer-model based adaptive resource allocation for statistical QoS guarantees in mobile wireless networks,”IEEE Trans. Wireless Commun., vol. 7, no. 6, pp.2318-2328, June 2008.
[8] L. Liu, P. Parag, and J.-F. Chamberland, “Quality of service analysis for wireless user-cooperation networks,”IEEE Trans. Inform. Theory, vol. 53, no. 10, pp. 3833-3842, Oct. 2007
[9] A. Goldsmith, Wireless Communications, 1st ed. Cambridge University Press, 2005.
[10] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.