Achievable Secrecy Sum-Rate in a Fading MAC-WT with Power Control and Without CSI of Eavesdropper

Shahid M Shah, Vireshwar Kumar[1] and Vinod Sharma
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore 560012, India
Email: shahid@ece.iisc.ernet.in, vireshwar.kumar@gmail.com, vinod@ece.iisc.ernet.in

***Abstract*—We consider a two user fading Multiple Access Channel with a wire-tapper (MAC-WT) where the transmitter has the channel state information (CSI) to the intended receiver but not to the eavesdropper (eve). We provide an achievable secrecy sum-rate with optimal power control. We next provide a secrecy sum-rate with optimal power control and cooperative jamming (CJ). We then study an achievable secrecy sum rate by employing an ON/OFF power control scheme which is more easily computable. We also employ CJ over this power control scheme. Results show that CJ boosts the secrecy sum-rate significantly even if we do not know the CSI of the eve's channel. At high SNR, the secrecy sum-rate (with CJ) without CSI of the eve exceeds the secrecy sum-rate (without CJ) with full CSI of the eve.**

***Index Terms*—Channel state information, Cooperative jamming, Fading Channel, Multiple Access Channel, Secrecy sum-rate, Wire-tap channel**

I. Introduction

Security is one of the most important considerations in transmission of information from one user to another. It involves confidentiality, integrity, authentication and non-repudiation [1]. We will be concerned about confidentiality. This guarantees that the legitimate users successfully receive the information intended for them while any eavesdropper is not able to interpret this information. We will be concerned with the eavesdroppers who are passive attackers, e.g., they attempt to interpret the transmitted information without injecting any new information or trying to modify the information transmitted.

Traditional techniques to achieve confidentiality in this setup are based on cryptographic encryption ([2], [3]). However now, Information Theoretical Security is also being actively studied ([1], [4]). This does not require the secret/public keys used in cryptographic techniques. Key management, especially for wireless channels can be very challenging. Also, information theoretical security, unlike for cryptography based techniques can provide provably secure communication. Information theoretic security can also be used in a system in addition to cryptographic techniques to add additional layers of protection to the information transmission or to achieve key agreement and/or distribution.

[1]Vireshwar Kumar is currently a PhD student at Virginia Tech. University, USA

The Information theoretic approach for secrecy systems was first investigated by Shannon [5] in 1949. Wyner [6] considers communicating a message secretly over a wiretap channel in the form of degraded broadcast channels, without using a key. Wyner's work was in turn extended by in [7] to the Additive White Gaussian Noise(AWGN) channel. Csiszàr and Körner [8] considers a general discrete memoryless broadcast channel, and show that the secrecy capacity is positive if the main channel to the intended user is more capable than of the eavesdropper, and zero if the wiretapper's channel is less noisy. The fading channel was studied in [9] where power allocation schemes without CSI of the eavesdropper's channel to the transmitter were also obtained. In [10], a wire-tap channel with slow fading was studied where an outage analysis with full CSI of the eavesdropper and imperfect CSI of the eavesdropper was performed.

Information theoretic security for a Multiple Access Channel (MAC) were obtained in [12] and [13]. In [12], each user treats the other as an eavesdropper while in [13], the eavesdropper is at the receiving end. In [13], Tekin and Yener propose a technique called cooperative jamming in which a user that is not transmitting, can send a jamming signal so that the eavesdropper is more confused. This significantly improves the secrecy rate region. A fading MAC was also studied by Tekin and Yener [14], where they assume that the CSI of the eavesdropper's channel is perfectly known at the transmitting users. The secrecy capacity region of a MAC is still an open problem.

In this paper, we consider a fading MAC-WT assuming no CSI of the eavesdropper at the transmitting users. Since the eavesdropper may not transmit any signal (it is passive), the transmitters often will not know its channel. We obtain a power control scheme that maximizes the sum secrecy rate and then also employ cooperative jamming over this scheme. It will be shown that cooperative jamming can significantly increase the secrecy rate. But these optimal policies are difficult to compute. Thus, next we consider a computationally simpler ON/OFF power control policy. We obtain its thresholds to maximize the secrecy sum-rate. Finally, we also incorporate cooperative jamming over this power control policy. With this, at high SNR, the secrecy sum-rate exceeds the sum-rate when CSI of the eavesdropper is perfectly known at the transmitter

978-1-4673-2014-6/12/$31.00 ©2012 IEEE

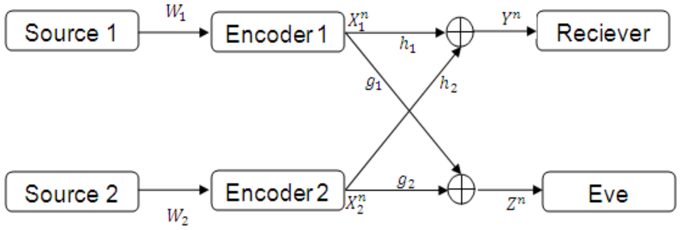

Fig. 1. Two user Fading Multiple Access Channel

but the cooperative jamming is not used.

The rest of the paper is organized as follows: In Section II, we define the channel model and state the problem. In Section III, we obtain the optimal power control policy with and without cooperative jamming. Section IV discusses ON/OFF power control policy with and without cooperative jamming. In Section V, we compare the different policies numerically. Finally in Section VI, we conclude this paper and discuss the future work.

II. Channel Model And Problem Statement

We consider a system with two users who want to communicate over a fading AWGN MAC to a legitimate receiver. There is also an eavesdropper who is trying to get access to the output received by the legitimate receiver. Transmitter k chooses message W_k for transmission from a set $\mathcal{W}_k = \{1, 2, ..., M_k\}$ with uniform distribution. These messages are encoded into $\{X_{k,1}, ..., X_{k,n}\}$ using $(2^{nR_k}, n)$ codes. The legitimate receiver gets Y_i and the eavesdropper gets Z_i at time i. The decoder at the legitimate receiver estimates the transmitted message as $\tilde{W} = (\tilde{W_1}, \tilde{W_2})$ from $\mathbf{Y}^n \equiv \{Y_1, ..., Y_n\}$. The legitimate receiver should receive the message reliably while the eavesdropper should not be able to decode it. It is assumed that the legitimate receiver as well as the eavesdropper know the codebooks.

The channel model can be mathematically represented as:

$$Y_i = \tilde{h}_{1,i}X_{1,i} + \tilde{h}_{2,i}X_{2,i} + N_{R,i} \tag{1}$$

$$Z_i = \tilde{g}_{1,i}X_{1,i} + \tilde{g}_{2,i}X_{2,i} + N_{E,i} \tag{2}$$

where $\tilde{h}_{k,i}$ and $\tilde{g}_{k,i}$ are the complex channel gains from the transmitter k to the legitimate receiver and the eavesdropper respectively. Also $\{N_{R,i}\}$ and $\{N_{E,i}\}$ are Additive White Gaussian Noise (AWGN) with each component distributed as $\mathcal{N}(0, 1)$, where $\mathcal{N}(a, b)$ is Gaussian distribution with mean a and variance b. Also let $|\tilde{h}_{k,i}|^2 = h_{k,i}$ and $|\tilde{g}_{k,i}|^2 = g_{k,i}$, for $k = 1, 2$. We assume that $\{h_{k,i}, i \geq 1\}$ and $\{g_{k,i}, i \geq 1\}$ are independent, identically distributed (iid), and that each sequence is independent of the other.

We use collective secrecy constraint to take the multi-access nature of the channel into account:

$$\Delta_L^n = \frac{H(W_L|Z^n)}{H(W_L)} \tag{3}$$

where $L \subseteq \{1, 2\}$, $Z^n = (Z_1, ..., Z_n)$ and $W_L = \{W_k; k \in L\}$. For each n we need codebooks such that the average probability of error to the legitimate receiver goes to zero and $\Delta_L^n \to 1$ as $n \to \infty$ for each $L \subseteq \{1, 2\}$.

Let $h_i = (h_{1i}, h_2), g_i = (g_{1i}, g_{2i})$. Then from [14], if the CSI h_i, g_i are known at both the transmitters and the receiver at time i, the following rate region for the MAC is achievable which satisfies the secrecy constraints (3) :

$$R_1 \leq \mathsf{E}_{h,g}\left\{\left[\log\frac{(1 + h_1P_1(h, g))(1 + g_2P_2(h, g))}{1 + g_1P_1(h, g) + g_2P_2(h, g)}\right]^+\right\}, \tag{4}$$

$$R_2 \leq \mathsf{E}_{h,g}\left\{\left[\log\frac{(1 + g_1P_1(h, g))(1 + h_2P_2(h, g))}{1 + g_1P_1(h, g) + g_2P_2(h, g)}\right]^+\right\}, \tag{5}$$

$$R_1 + R_2 \leq \mathsf{E}_{h,g}\left\{\left[\log\frac{1 + h_1P_1(h, g) + h_2P_2(h, g)}{1 + g_1P_1(h, g) + g_2P_2(h, g)}\right]^+\right\}, \tag{6}$$

where $P_1(h, g)$ and $P_2(h, g)$ are the transmit powers satisfying

$$\mathsf{E}\left[P_i(h, g)\right] \leq \bar{P}_i, \quad i = 1, 2. \tag{7}$$

Also to achieve these rates Gaussian signalling is used.

In [14], the optimal power allocation policy which maximizes the sum secrecy rate (7) has been found. In this paper, we extend this result to the case when the CSI of the legitimate receiver is known but the CSI of the eavesdropper may not be known at the transmitter; only its distribution is known. Since we are assuming a passive eavesdropper, this will often be a more reasonable assumption, i.e., there is no transmission from the eavesdropper to the transmitters for them to estimate its channel.

III. Optimal Power Control with main CSI only

A. Power control without Cooperative Jamming

In this section we consider power control which maximizes the sum secrecy rate when only the main channel (to the legitimate user) CSI is known at the transmitters. Let $P_k(h)$ be the power used by a policy when the main channel gain is $h = (h_1, h_2)$. We need the following notation

$$\phi^s_{x_1,x_2} = 1 + s_1x_1 + s_2x_2 \tag{8}$$

where s is the channel state (h or g) and x_k is the power used. The following theorem can be proved via standard techniques. The proof is given in the detailed version of this paper[11] and is skipped here due to lack of space.

Theorem 3.1: For a given power control policy $\{P_k(h)\}, \ k = 1, 2$, the following secrecy sum-rate

$$\mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_1,P_2}}{\phi^g_{P_1,P_2}}\right)\right]^+\right\} \tag{9}$$

is achievable. □

The policy that maximizes (9) is not available in closed form, but can be numerically computed (see Appendix). An example will be provided in Section VI. We will also consider a simpler ON/OFF power control policy.

Next we consider power control with cooperative jamming.

B. Optimal Power Control With Cooperative Jamming

The optimal power policy obtained in the last section depends on h. If both the main channels h_1 and h_2 are good, both the transmitters send their coded symbols. If a transmitter's channel is bad, it may not. When a transmitter is not sending its data, it can help the other user by jamming the channel to the eavesdropper.

Let $\{P_k(h)\},\ k=1,2$, be the power control policy when the users are transmitting and $\{Q_k(h)\},\ k=1,2$, be the power control policy when the users are jamming. To satisfy (7) , we need

$$\mathsf{E}_{h,g}[P_k(h)+Q_k(h)] \leq \bar{P}_k,\ k=1,2. \tag{10}$$

Then we can prove the following theorem.

Theorem 3.2: With the above power control policies secrecy sum-rate

$$\mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_1,P_2}+\phi^h_{Q_1,Q_2}-1}{\phi^g_{P_1,P_2}+\phi^g_{Q_1,Q_2}-1}\right)\left(\frac{\phi^g_{Q_1,Q_2}}{\phi^h_{Q_1,Q_2}}\right)\right]^+\right\} \tag{11}$$

is achievable. □

The detailed proof is given in [11].

We will obtain the power control policy that maximizes the sum rate in the Appendix. We will see in Section VI that cooperative jamming can significantly improve the sum-rate.

We also propose a simple ON/OFF power control policy with cooperative jamming.

IV. Fading MAC with ON/OFF Power Control

The optimal policy obtained in Section III can be computed only numerically and its structure is not known. The following ON/OFF policy is easier to compute and is intuitive:
User k transmits with a constant power P_k if $h_k > \tau_k$, where τ_k is an appropriate threshold. Hence the following cases arise:

1) $h_1 > \tau_1,\ h_2 > \tau_2$: Both transmit;
2) $h_1 > \tau_1,\ h_2 < \tau_2$: User-1 transmits;
3) $h_1 < \tau_1,\ h_2 > \tau_2$: User-2 transmits;
4) $h_1 < \tau_1,\ h_2 < \tau_2$: No user transmits.

From average power constraint we get:

$$\bar{P}_1 = P_1 Pr(h_1 > \tau_1) \tag{12}$$

and

$$\bar{P}_2 = P_2 Pr(h_2 > \tau_2). \tag{13}$$

where $Pr(A)$ denotes the probability of event A.

Let

$$A_1 \triangleq \{h_1 > \tau_1,\ h_2 < \tau_2\},\ A_2 \triangleq \{h_1 < \tau_1,\ h_2 > \tau_2\}$$

and

$$A_{12} \triangleq \{h_1 > \tau_1,\ h_2 > \tau_2\}. \tag{14}$$

The secrecy sum-rate by this policy is given by

$$\begin{aligned} R_B = {} & \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_1,P_2}}{\phi^g_{P_1,P_2}}\right)1_{A_{12}}\right]^+\right\} \\ & + \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_1,0}}{\phi^g_{P_1,0}}\right)1_{A_1}\right]^+\right\} \\ & + \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{0,P_2}}{\phi^g_{0,P_2}}\right)1_{A_2}\right]^+\right\} \end{aligned} \tag{15}$$

where $1_{\{\}}$ is the indicator function.

When h_k and g_k have Exponential distribution with densities

$$f_1(h) = \frac{1}{\gamma_1\gamma_2}e^{-\frac{h_1}{\gamma_1}}e^{-\frac{h_2}{\gamma_2}}\ ,\ f_2(g) = \frac{1}{\mu_1\mu_2}e^{-\frac{g_1}{\mu_1}}e^{-\frac{g_2}{\mu_2}} \tag{16}$$

where $\gamma_1 = \mathsf{E}(h_1)$, $\gamma_2 = \mathsf{E}(h_2)$, $\mu_1 = \mathsf{E}(g_1)$ and $\mu_2 = \mathsf{E}(g_2)$, then

$$P_1 = \bar{P}_1 e^{\frac{\tau_1}{\gamma_1}}\ ,\ P_2 = \bar{P}_2 e^{\frac{\tau_2}{\gamma_2}}. \tag{17}$$

We numerically obtain the secrecy sum-rate for thresholds τ_1 and τ_2 which maximize the sum-rate (15).

V. Fading MAC with ON/OFF Power Control and Cooperative Jamming

Cooperative jamming has been found to increase the sum-rate substantially. Therefore, we now use it with the ON/OFF policy studied in Section IV. A user when not transmitting its data jams the channel for the eavesdropper. Also it transmits with different powers taking into account the channel gain of the other user. The following cases arise:

1) $h_1 > \tau_1,\ h_2 > \tau_2$: Both transmit with power $P_{1a},\ P_{2a}$;
2) $h_1 > \tau_1,\ h_2 < \tau_2$: User-1 transmits with power P_{1b}, user-2 jams with power Q_2;
3) $h_1 < \tau_1,\ h_2 > \tau_2$: User-2 transmits with power P_{2b}, user-1 jams with power Q_1;
4) $h_1 < \tau_1,\ h_2 < \tau_2$: None transmits or jams.

The powers and the thresholds in the above scheme are chosen to satisfy the average power constraints.

The secrecy sum-rate for this power control policy is given by:

$$\begin{aligned} R_B^{CJ} = {} & \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_{1a},P_{2a}}}{\phi^g_{P_{1a},P_{2a}}}\right)1_{A_{12}}\right]^+\right\} \\ & + \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{P_{1b},Q_2}}{\phi^g_{P_{1b},Q_2}}\right)1_{A_1}\right]^+\right\} \\ & + \mathsf{E}_{h,g}\left\{\left[\log\left(\frac{\phi^h_{Q_1,P_{2b}}}{\phi^g_{Q_1,P_{2b}}}\right)1_{A_2}\right]^+\right\} \end{aligned} \tag{18}$$

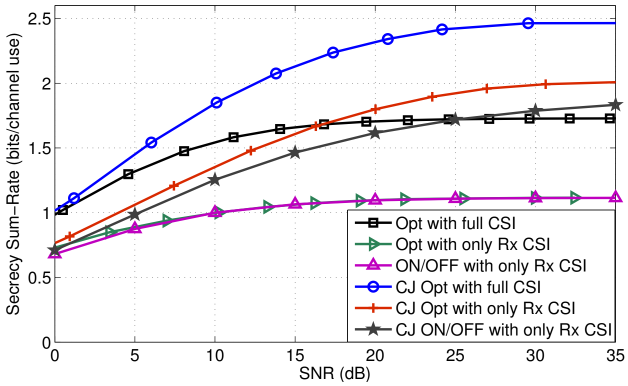

Fig. 2. Comparison of Full CSI, Only Receiver's CSI and ON/OFF Power Control policies: With and without Cooperative Jamming

When h_k and g_k have Exponential distribution

$$\bar{P}_1 = P_{1a}e^{-\frac{\tau_1}{\gamma_1}}e^{-\frac{\tau_2}{\gamma_2}} + P_{1b}e^{-\frac{\tau_1}{\gamma_1}}(1-e^{-\frac{\tau_2}{\gamma_2}}) + Q_1 e^{-\frac{\tau_2}{\gamma_2}}(1-e^{-\frac{\tau_1}{\gamma_1}}), \quad (19)$$

$$\bar{P}_2 = P_{2a}e^{-\frac{\tau_1}{\gamma_1}}e^{-\frac{\tau_2}{\gamma_2}} + P_{2b}e^{-\frac{\tau_2}{\gamma_2}}(1-e^{-\frac{\tau_1}{\gamma_1}}) + Q_2 e^{-\frac{\tau_1}{\gamma_1}}(1-e^{-\frac{\tau_2}{\gamma_2}}). \quad (20)$$

VI. Numerical Results

In this section, we compare the sum rates obtained via the different power control schemes proposed in this paper. The receiver's AWGN noise has variance 1. The fading for each channel is Rayleigh distributed with parameters $\gamma_1 = \gamma_2 = \mu_1 = \mu_2 = 1$. The optimal sum rates are plotted in Fig.1 for different powers $P_1 = P_2$. We observe that cooperative jamming substantially improves the sum-rate (up to 75%). Of course, for each case knowledge of the eavesdropper's CSI at the transmitter improves the sum-rate. At high SNR, the cooperative jamming can provide sum-rate without CSI higher than the full CSI case without cooperative jamming. Also, optimal ON/OFF power control is sufficient to recover most of the sum rate achievable by the optimal policy (for no eavesdropper's CSI and no jamming, ON/OFF provides rate very close to the optimal).

VII. Conclusion and Future Work

In this paper, we provide achievable secrecy sum-rate in a fading MAC with an eavesdropper when the eavesdropper's channel is not known to the transmitter. We obtain the optimal power controls that optimize the secrecy sum-rate. We also obtain the optimal power control when cooperative jamming is also employed. It is shown that cooperative jamming can substantially improve the secrecy sum-rates. We, then, obtain more easily computable ON/OFF power control schemes which provide secrecy sum-rates close to the optimal.

It is shown that via these techniques, one can recover most of the secrecy sum-rate achievable with the perfect knowledge of the CSI of the eavesdropper.

For future work one can consider the schemes when partial CSI of the legitimate receiver's channel is available at the transmitter.

Appendix
Optimal Power Control

A. Without Cooperative Jamming

We provide the details for Rayleigh fading. Similarly one can obtain the optimal powers for other distributions. Let f_1 and f_2 denote the densities of h and g respectively. For Rayleigh fading case, averaging over all fading realizations of eve's channel, i.e., g_1 and g_2, which give positive secrecy sum-rate, we get

$$R = \int_{h_1}\int_{h_2}\left[\log\left(\phi^h_{P_1,P_2}\right) - \frac{1}{\xi_{P_1,P_2}}\left\{P_1\mu_1\theta_{P_1} - P_2\mu_2\theta_{P_2}\right\}\right] f_1(h)dh \quad (21)$$

where
$\phi^h_{P_1,P_2}$ is as defined in (8) and

$$\xi_{a,b} = a\mu_1 - b\mu_2, \quad (22)$$

$$\theta_{P_1} = e^{\frac{1}{P_1\mu_1}}\left[Ei\left(\frac{1}{P_1\mu_1}\right) - Ei\left(\frac{1}{P_1\mu_1} + \frac{h_1P_1 + h_2P_2}{P_1\mu_1}\right)\right], \quad (23)$$

$$\theta_{P_2} = e^{\frac{1}{P_2\mu_2}}\left[\mathrm{Ei}\left(\frac{1}{P_2\mu_2}\right) - \mathrm{Ei}\left(\frac{1}{P_2\mu_2} + \frac{h_1P_1 + h_2P_2}{P_2\mu_2}\right)\right], \quad (24)$$

and

$$\mathrm{Ei}(x) = \int_x^\infty \frac{e^{-t}}{t}dt. \quad (25)$$

After writing the Lagrangian and invoking KKT (Karush-Kuhn-Tucker) conditions (which are only necessary here as the objective function need not be concave [15]), we get

$$\frac{h_1}{\phi^h_{P_1,P_2}} + \frac{1}{\xi_{P_1,P_2}}\left\{\frac{\theta_{P_1}}{P_1} - \mu_1 + \frac{\alpha_1}{h_2\phi^h_{P_1,P_2}} + \frac{P_2(\alpha_1+\alpha_2)}{\phi^h_{P_1,P_2}}\right\} + \frac{P_2\mu_1\mu_2}{\xi^2_{P_1,P_2}}(\theta_{P_1} - \theta_{P_2}) - \lambda_1 = 0 \quad (26)$$

$$\frac{h_2}{\phi^h_{P_1,P_2}} - \frac{1}{\xi_{P_1,P_2}}\left\{\frac{\theta_{P_2}}{P_2} - \mu_2 + \frac{\alpha_2}{h_1\phi^h_{P_1,P_2}} + \frac{P_1(\alpha_1+\alpha_2)}{\phi^h_{P_1,P_2}}\right\} - \frac{P_1\mu_1\mu_2}{\xi^2_{P_1,P_2}}(\theta_{P_1} - \theta_{P_2}) - \lambda_2 = 0 \quad (27)$$

where λ_1 and λ_2 are the Lagrangian multipliers and

$$\alpha_1 = h_2\mu_1 e^{-\left(\frac{h_1P_1+h_2P_2}{P_1\mu_1}\right)}, \quad (28)$$

$$\alpha_2 = h_1\mu_2 e^{-\left(\frac{h_1P_1+h_2P_2}{P_2\mu_2}\right)}. \quad (29)$$

We solve this set of equations numerically for optimum power policy:

1) If we find positive solutions for P_1 and P_2 from (26) and (27), both should be transmitting with their respective powers.
2) If we do not find positive solutions for both and $h_1 > h_2$, we solve (26) for P_1 with $P_2 = 0$.
3) If we do not find positive solutions for both and $h_1 < h_2$, we solve (27) for P_2 with $P_1 = 0$.

B. With Cooperative Jamming

A user can transmit, jam or do nothing. We have different expressions of secrecy sum-rate based on whether the users are transmitting or jamming. Averaging (11) over all the fading realizations (g_1, g_2) and if there is a positive solution P_1 and P_2 from (26) and (27), both users will transmit, and the secrecy sum-rate is given in (21).

When there is no solution of (26) and (27) such that $P_1 > 0$ and $P_2 > 0$, and the channel of user 1 is better than that of user 2, the secrecy sum-rate is

$$\int_{h_1}\int_{h_2}\left[\log\frac{\phi^h_{P_1,Q_2}}{\phi^h_{0,Q_2}} - \frac{1}{\xi_{P_1,Q_2}}\left\{P_1\mu_1\left(\beta_{P_1} - \beta_{Q_2}\right)\right\}\right] f_1(h)dh. \tag{30}$$

Similarly when the channel of user 2 is better than user 1, the secrecy sum-rate is

$$\int_{h_1}\int_{h_2}\left[\log\frac{\phi^h_{Q_1,P_2}}{\phi^h_{Q_1,0}} - \frac{1}{\xi_{Q_1,P_2}}\left\{P_2\mu_2\left(\beta_{Q_1} - \beta_{P_2}\right)\right\}\right] f_1(h)dh. \tag{31}$$

where

$$\begin{aligned}
\beta_{P_1} &= e^{\frac{1}{P_1\mu_1}}\left[\mathrm{Ei}\left(\frac{1}{P_1\mu_1}\right) - \mathrm{Ei}\left(\frac{1}{P_1\mu_1} + \frac{h_1}{\mu_1(1+h_2Q_2)}\right)\right],\\
\beta_{P_2} &= e^{\frac{1}{P_2\mu_2}}\left[\mathrm{Ei}\left(\frac{1}{P_2\mu_2}\right) - \mathrm{Ei}\left(\frac{1}{P_2\mu_2} + \frac{h_2}{\mu_2(1+h_1Q_1)}\right)\right],\\
\beta_{Q_1} &= e^{\frac{1}{Q_1\mu_1}}\left[\mathrm{Ei}\left(\frac{1}{Q_1\mu_1}\right) - \mathrm{Ei}\left(\frac{1}{Q_1\mu_1} + \frac{h_2}{\mu_2(1+h_1Q_1)}\right)\right],\\
\beta_{Q_2} &= e^{\frac{1}{Q_2\mu_2}}\left[\mathrm{Ei}\left(\frac{1}{Q_2\mu_2}\right) - \mathrm{Ei}\left(\frac{1}{Q_2\mu_2} + \frac{h_1}{\mu_2(1+h_2Q_2)}\right)\right].
\end{aligned}$$

Now the problem is to maximize the above objective functions appropriately for each case. This function may not be concave. Hence, KKT conditions are necessary but not sufficient. We solve the equations obtained via KKT numerically to obtain optimal power policy.

References

[1] Y. Liang, H.V. Poor, S. Shamai, "Information theoretic security," *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4-5 (2008), pp. 355–580, 2009.

[2] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," *Boca Raton, FL, USA: CRC Press*, 1996.

[3] W. Stallings, "Cryptography and network security principles and practices," *Upper Saddle River, NJ, USA: Prentice Hall*, 3rd ed., 2003.

[4] R. Liu, W. Trappe, "Securing wireless communications at the physical layer," *Springer Science + Business Media*, LLC 2010.

[5] C.E. Shannon, "Communication of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656-715, October 1949.

[6] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, 1974.

[7] S. K. Leung-Yan-Cheong and M. E. Hellman, "Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 82, no. 24 (4), pp. 451–456, July 1978.

[8] I. Csiszàr and J.Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 82, no. 23, pp. 339–348, May 1978.

[9] P. K. Gopala, L. Lai, H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Info. Theory*, vol. 54, no. 10, pp. 4687–4698, October 2008.

[10] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[11] Shahid M. Shah, Vireshwar Kumar, Vinod Sharma, "Achievable Secrecy Sum-Rate in a Fading MAC-WT with Power Control and without CSI of Eavesdropper," *http://arxiv.org/pdf/1107.5123*, July 2011.

[12] Y. Liang, H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 54, no. 3, pp. 35–45, March 2008.

[13] E. Tekin, A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54 , no. 6, pp. 2735-2751, June 2008.

[14] E. Tekin, A. Yener, "Secrecy sum-rates for the multiple-access wire-tap Channel with ergodic block fading," *45th Annual Allerton Conference, UIUC, Illinois, USA*, Sep 26–28, 2007.

[15] S. Boyd, L. Vandenberghe, "Convex optimization," *Cambridge University Press*, New York, 2004.