Secure Communications in OFDMA networks with active eavesdropper

M. R. Javan[1]

Received :2015\11\25 Accepted:2015\12\25

Abstract

In this paper, we formulate the resource allocation problem for secure communications in a single cell OFDMA network where a base station wants to communicate to the users which are spread over its coverage area while an adversary is present in the network. In our model, we assume that the adversary s an active attacker which is able to either eavesdrop on the information transmitted over the wireless link or jam the connection by sending an interference signal but is not able to both eavesdrop and jam at the same time. The attacker's aim is to choose between eavesdropping and jamming a subcarrier such that the secrecy rate over that subcarrier is minimized. Knowing this strategy, users should consider the minimum of secrecy data rate in both cases as their achievable secrecy rate over each subcarrier. We formulate our proposed resource allocation problem into an optimization problem whose objective is to maximize the total secrecy rate of all users over all subcarriers while it is required that the total transmit power of base station remains below a predefined threshold. To solve the proposed optimization problem, we use the dual Lagrange approach. Using simulations, we study the behavior and the efficiency of the proposed scheme.

Keywords: Power allocation, eavesdropping, jamming, secrecy rate, OFDMA.

1. Introduction

The wireless channel is a broadcast one meaning that the information transmitted such a channel can be accessed by unauthorized users. Therefore, in such a transmission medium, security of information becomes more important. Traditionally, upper layers (the layers above the physical layer) are responsible for providing the security of information transmission. These layers mostly relies on cryptographic methods for securing the information transmission [1]-[3] whose main issue is their excessive computational complexity. Recently, talking the secure communications in physical layer has attracted many attention which provides security of information transmission at the physical layer. The wiretap channel was first introduced in [4] where the security is mainly measured by equivocation rate which the level of ignorance of malicious user. This work was further investigated for Gaussian channel in [5].

Physical layer secure communication over wireless channel has been gained much attention from researchers in recent years [6]-[17]. In [7], the authors consider the problem of secure communications for fading channels where there exists a malicious user which wants to eavesdrop on the information transmission between legitimate parties. In their paper, they consider the scenario in which all the channel state information (CSI), including the legitimate CSs and the CSIs of the eavesdropper channels, is known to the transmitters. In addition, they study the case where only the knowledge of the legitimate CSIs is available. Secure communication for parallel broadcast channels is considered in [8]. The problem of energy efficient communication for wiretap channel is considered in [9]. The authors in [10] consider the problem of energy efficient communications for secure communications in which their objective is to maximize the value of a function measuring the total secure transmitted bits per joule of energy. The authors in [11] consider the problem of secure communications in OFDM networks. In their scheme, they aim at maximizing the secrecy rate of the user under transmit power constraint while an eavesdropper is present and eavesdropping the information transmission. In addition, the eavesdropper is more capable that the legitimate user and its receiver structure is better that that of legitimate receiver. The problem of secure communications in OFDMA networks is considered in [12] where in addition of legitimate receivers, there exists and eavesdropper in the network. In their scheme, the authors divide the total users into two classes: secure and nonsecure users. Secure users are required to maintain their secrecy rate above a predefined threshold. However, the nonsecure users are allowed to use the network resources in an opportunistic manner, i.e., their aim is to maximize their transmission rate under the total

1. Assistant Profrssor, Department of Electrical Engineering, Shahrood University of Technology, Shahrood, Iran, javan@shahrood.ac.ir

transmit power constraint and the individual secrecy rate constraint for each secure user.

The malicious user can be more capable of just eavesdropping the information transmission. In other word, besides the eavesdropping capability, It can also be capable of transmitting the interfering signal toward the legitimate receivers to degrade the channel conditions of legitimate receivers leading to lower channel capacity [13]-[17]. When the malicious user just eavesdrop the information transmission it is a passive attacker while when it also transmits the interfering signals, it is called an active attacker or active eavesdropper [15]. The eavesdropper can be able to both eavesdrop and jam at the same time meaning that it is able to both transmit and receive at the same time has is a full-duplex node [13]. On the other hand, it can be able to eavesdrop and jam but not both at the same time [14]-[17]. In [14], secure communications in the presence of an active eavesdropper is considered. In their model, the attacker has the ability of either eavesdropping or jamming the connections but not both at the same time. Optimal power allocation as well as optimal strategy determining the alternation pattern between jamming and eavesdropping mode is obtained. Game theory can be used to model the problems of secure communications when an active eavesdropper is present in the network [15]. The authors use game theory to formulate the problem of secure communications. Bothe the legitimate user and the attacker are the players of the game. The objective of the legitimate user is to maximize the achievable secrecy rate. On the other hands, the objective of the attacker is to minimize the achievable secrecy rate of legitimate user. After analyzing the proposed game, the authors obtain the Nash equilibrium (NE) of the game in their proposed scheme. In OFDM networks, secure communication in the presence of an active eavesdropper is considered in [16-17]. The attacker can alternates between jamming and eavesdropping such that the achievable secrecy rate of the OFDM use is minimized. While in [16] the objective is to minimize the transmit power under total secrecy rate constraint, in [17], the objective is to maximize the total secrecy rate of the OFDM user under total transmit power constraint, i.e., the dual problem of [16].

In this paper, we extend the works [16-17] to OFDMA networks where in addition to transmit power levels, subcarrier allocation should also be performed. More precisely, we propose a downlink resource allocation scheme for secure transmission in a single cell OFDMA network in which we assume that the base station is located at the center of the cell, network users are spread uniformly over the coverage area, and an active eavesdropper exists in the network. We assume that the malicious user has full knowledge of the network including the channel gains and transmit power of users. Given the transmission power level over a subcarrier, the malicious user chooses between eavesdropping and jamming such that the overall secrecy rate over that subcarrier is minimized, i.e., the attacker sends interfering signal over a subcarrier if the achievable rate over when jamming is less than the achievable secrecy rate over that subcarrier when the attacker eavesdrops it, and the attacker eavesdrops that subcarrier otherwise. Therefore, the base station should consider the worst case, i.e., it considers the secrecy rate over each subcarrier as the minimum of secrecy rates achievable when the malicious user is eavesdropping or jamming. The goal of resource allocation problem is to maximize the total secrecy rate over all subcarriers while it is assumed that the total transmission power stays below a predefined threshold.

Based on these assumptions, we formulate our problem as an optimizations problem whose solution is the transmit power level of each subcarrier and subcarrier assignment. We solve the resource allocation problem using dual Lagrange method. We then propose an iterative algorithm to solve the proposed problem. Finally using simulations, we evaluate the proposed scheme.

This paper is organized a follows. System model and problem formulation is presented in Section II and the proposed problem is analyzed in Section III. Simulations are in Section IV and the paper is concluded in Section V.

2. System Model and Problem Formulation

Consider an OFDMA network consisting of N subcarriers and U users. The central base station wants to communicate to users over these channels in the presence of an active eavesdropper. Assume that the channel gain to noise ratio (CNR) of the channel from the base station to user i over subcarrier n is denoted by g_i^n, the CNR of the channel from the base station to malicious user over subcarrier n is

denoted by g_n^{E}, and the CNR of the channel from the malicious user to user i over subcarrier n is denoted by h_i^n. The transmit power assigned to user i over subcarrier n is denoted by p_i^n, and the transmit power of malicious user over subcarrier n, when it is in jamming mode, is denoted by p_n^{J}. Using the above definitions, when the malicious user eavesdrops the subcarrier n, the secrecy capacity of user i over subcarrier n is given by

$$C_{n,i}^{\mathrm{Se}} = [log(1+g_i^n p_i^n) - log(1+g_n^{\mathrm{E}} p_i^n)]^+ = [log(\frac{1+g_i^n p_i^n}{1+g_n^{\mathrm{E}} p_i^n})]^+. \quad (1)$$

On the other hand, when the malicious user sends the interfering signal over subcarrier n, the secrecy capacity of user i over subcarrier n is given by

$$C_{n,i}^{\mathrm{Sj}} = log(1+\frac{g_i^n p_i^n}{1+h_i^n p_n^{\mathrm{j}}}). \quad (2)$$

We assume that the transmit power of the attacker when it jams the subcarrier n is fixed to p_n^{j}, i.e., we do not consider the problem of power allocation for the attacker in jamming mode.

If the legitimate users know the action of attacker for each subcarrier in advance, i.e., they know whether the attacker is in eavesdropping mode or jamming mode, the secrecy rate of each subcarrier can be obtained by (1) or (2), respectively. Generally, the malicious user can alternate between eavesdropping and jamming according to some probability distribution, i.e., it eavesdrop with probability $p(\text{eavesdropping}) = p_{\mathrm{e}}^n$ and jams with probability $p(\text{jamming}) = p_{\mathrm{j}}^n$ where $p_{\mathrm{e}}^n + p_{\mathrm{j}}^n = 1$. This case is similar to the one considered in [14]. However, different from [14], we adopt the strategy of [16-17], i.e., we assume that, for each subcarrier, between eavesdropping and jamming, the malicious user chooses the action that minimizes the secrecy rate over that subcarrier, i.e., if subcarrier n is assigned to user i, the malicious user chooses the eavesdropping action if $C_{n,i}^{\mathrm{Se}} < C_{n,i}^{\mathrm{Sj}}$ and chooses to jam otherwise. Therefore, the worst case should be considered. The secrecy rate of user i over subcarrier n is

$$C_{n,i}^{\mathrm{S}} = \min(C_{n,i}^{\mathrm{Sj}}, C_{n,i}^{\mathrm{Se}}) \quad (3)$$

and the total secrecy rate achieved by all users is given by

$$C^{\mathrm{S}} = \sum_i \sum_n \min(C_{n,i}^{\mathrm{Sj}}, C_{n,i}^{\mathrm{Se}}). \quad (4)$$

We define assignment variables $\circ_i^n \in \{0,1\}$ where $\circ_i^n = 1$ indicates that the subcarrier n is assigned to user i. Based on these definitions, the aim is to solve the following optimization problem [18]

$$\max_{\mathbf{p}\geq\mathbf{0},\boldsymbol{\rho}} \sum_i \sum_n \circ_i^n \min(C_{n,i}^{\mathrm{Se}}, C_{n,i}^{\mathrm{Sj}}) \quad (5)$$

$$\text{Subject To}: \sum_i \sum_n \circ_i^n p_i^n < P_{\mathrm{BS}}^{\max}, \quad (6)$$

$$\sum_i \circ_i^n = 1, \forall n, \quad (7)$$

$$\circ_i^n \in \{0,1\}, \forall i, n. \quad (8)$$

In the above optimization problem, (5) is the objective function which the total secrecy rate of users, (6) is the transmit power constraint, (7) indicated that each subcarrier can be used by only one user, and (8) states that the assignment factor in an integer taking the values of 0 and 1.

To point out some issues of the behavior of the eavesdropper, suppose that the subcarrier n is allocate to user i, i.e., $\circ_i^n = 1$. For an arbitrary positive transmit power of user i on subcarrier n, i.e., $p_i^n > 0$, the secrecy rate in (1) is positive, i.e., $C_{n,i}^{\mathrm{Se}} > 0$, if the CSI of the channel from legitimate transmitter to its corresponding receiver is better that that of the channel from the transmitter to the malicious user, i.e., $g_i^n > g_n^{\mathrm{E}}$. In this case, depending on the channel gains and the interfering signal power, the eavesdropper may choose to jam the subcarrier, However, when $g_i^n \leq g_n^{\mathrm{E}}$, the transmitter do not send any thing on this subcarrier which means that the transmit power over this subcarrier is zero, i.e., $p_i^n = 0$. Therefore, in this case, the malicious user does not waste its transmit power to jam the connection, i.e., $p_n^{\mathrm{j}} = 0$.

3. Problem Solution

In this section, we provide the solution of the optimization problem (5). To this end, we introduce variables $t_{n,i}$ and reformulate the optimization problem (5) as follows.

$$\max_{\mathbf{p}\geq\mathbf{0},\mathbf{t}\geq\mathbf{0}} \sum_i \sum_n \circ_i^n t_{n,i} \quad (9)$$

$$\text{Subject To:} \sum_i \sum_n \circ_i^n p_i^n < P_{\text{BS}}^{\max}, \quad (10)$$

$$C_{n,i}^{\text{Se}} \geq t_{n,i}, \ \forall n\, i, \quad (11)$$

$$C_{n,i}^{\text{Sj}} \geq t_{n,i}, \ \forall n\, i, \quad (12)$$

$$\sum_i \circ_i^n = 1, \forall n, \quad (13)$$

$$\circ_i^n \in \{0,1\}, \forall i, n. \quad (14)$$

Note that, in the problem (9), the optimization variables are p_i^n, $\circ_i^n$, and $\mathrm{t}_{n,i}$.

Looking at (9), one can see that the function $\sum_i \sum_n \circ_i^n t_{n,i}$ is an increasing function of $\mathrm{t}_{n,i}$. Based on this observation, it is obvious that at the optimal point, for each user i and for each subcarrier n that $\circ_i^n \neq 0$, the values of $\mathrm{t}_{n,i}$ and p_i^n are such that at least one of the constraints (11) or (12) is active, i.e., either $C_{n,i}^{\text{Sj}} = t_{n,i}$ or $C_{n,i}^{\text{Se}} = t_{n,i}$, or in other words, we have either $\min(C_{n,i}^{\text{Sj}}, C_{n,i}^{\text{Se}}) = C_{n,i}^{\text{Sj}}$ or $\min(C_{n,i}^{\text{Sj}}, C_{n,i}^{\text{Se}}) = C_{n,i}^{\text{Se}}$. We call the former subcarrier, i.e., the one for which we have $C_{n,i}^{\text{Sj}} = t_{n,i}$, the jammed subcarrier, and the later, i.e., the one for which we have $C_{n,i}^{\text{Se}} = t_{n,i}$, the eavesdropped subcarrier.

4. Finding values of p and t

To solve the problem (9), we use the dual Lagrange approach. In doing so, we write the Lagrange function [16] of the above optimization problem. We omit the variable $\circ_i^n$ here, and we will consider it in the subcarrier allocation phase. We define the variable « as the Lagrange multiplier corresponding to the constraint (10), $\mathsf{a}_{n,i}^{\text{e}}$ as the Lagrange multiplier corresponding to the constraint (11), and $\mathsf{a}_{n,i}^{\text{j}}$ as the Lagrange multiplier corresponding to the constraint (12). Using this variables the Lagrange function of the optimization problem (9) is given by:

$$\begin{aligned} L(\mathbf{t},\mathbf{p},\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) = & \sum_i \sum_n t_{n,i} + \text{«}(P_{\text{BS}}^{\max} - \sum_i \sum_n p_i^n) \\ & + \sum_i \sum_n \mathsf{a}_{n,i}^{e} (C_{n,i}^{\text{Se}} - t_{n,i}) \\ & + \sum_i \sum_n \mathsf{a}_{n,i}^{\text{j}} (C_{n,i}^{\text{Sj}} - t_{n,i}), \end{aligned} \quad (15)$$

which can be reformulated as

$$\begin{aligned} L(\mathbf{t},\mathbf{p},\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) = & \sum_{i=1}^{U} \sum_{n=1}^{N} t_{n,i}(1-(\mathsf{a}_{n,i}^{\text{j}} + \mathsf{a}_{n,i}^{e})) \\ & + \sum_{i=1}^{U} \sum_{n=1}^{N} \left(\mathsf{a}_{n,i}^{\text{j}} C_{n,i}^{\text{Sj}} + \mathsf{a}_{n,i}^{\text{e}} C_{n,i}^{\text{Se}} - \text{«} p_i^n \right) + \text{«} P_{\text{BS}}^{\max}. \end{aligned} \quad (16)$$

Based on the Lagrange function in (16), the dual function is obtained by maximizing the Lagrange function over variables $\mathbf{p}$ and $\mathbf{t}$, i.e.,

$$\begin{aligned} g(\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) &= \max_{\mathbf{p}\geq\mathbf{0},\mathbf{t}\geq\mathbf{0}} L(\mathbf{t},\mathbf{p},\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) \\ &= \max_{\mathbf{t}\geq\mathbf{0}} \sum_{i=1}^{U} \sum_{n=1}^{N} t_{n,i}(1-(\mathsf{a}_{n,i}^{\text{j}} + \mathsf{a}_{n,i}^{e})) \\ &+ \max_{\mathbf{p}\geq\mathbf{0}} \sum_{i=1}^{U} \sum_{n=1}^{N} \left(\mathsf{a}_{n,i}^{\text{j}} C_{n,i}^{\text{Sj}} + \mathsf{a}_{n,i}^{\text{e}} C_{n,i}^{\text{Se}} - \text{«} p_i^n \right) \\ &+ \text{«} P_{\text{BS}}^{\max} \end{aligned} \quad (17)$$

From (17), the optimal value of the variable $t_{n,i}$ is given by

$$t_{n,i} = \begin{cases} 0, & \text{if} \quad \mathsf{a}_{\text{n,i}}^{\text{j}} + \mathsf{a}_{\text{n,i}}^{\text{e}} > 1, \\ \infty, & \text{if} \quad \mathsf{a}_{\text{n,i}}^{\text{j}} + \mathsf{a}_{\text{n,i}}^{\text{e}} < 1, \\ \text{Any}, & \text{if} \quad \mathsf{a}_{\text{n,i}}^{\text{j}} + \mathsf{a}_{\text{n,i}}^{\text{e}} = 1. \end{cases} \quad (18)$$

To obtain the transmit power variables, i.e., $\mathrm{p}_{n,i}$, if $g_i^n \leq g_n^{\text{E}}$, we have $\mathrm{p}_{n,i} = 0$. Otherwise, if $g_i^n > g_n^{\text{E}}$, to find the optimal value of $\mathrm{p}_{n,i}$, we take the derivatives of the Lagrange function with respect to $\mathrm{p}_{n,i}$, and write

$$\frac{\partial L(\mathbf{t},\mathbf{p},\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«})}{\partial p_{n,i}} = \begin{cases} <0, & \mathrm{p}_{n,i} = 0, \\ =0, & P_{\text{BS}}^{\max} > \mathrm{p}_{n,i} > 0, \\ >0, & p_{n,i} = P_{\text{BS}}^{\max}. \end{cases} \quad (19)$$

In (19) the derivative is given by

$$\begin{aligned} \frac{\partial L(\mathbf{t},\mathbf{p},\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«})}{\partial p_i^n} = & \mathsf{a}_{n,i}^{\text{j}} \frac{g_i^n}{1+h_i^n p_n^{\text{j}} + g_i^n p_i^n} \\ & + \mathsf{a}_{n,i}^{\text{e}} \left(\frac{g_i^n}{1+g_i^n p_i^n} - \frac{g_n^{\text{E}}}{1+g_n^{\text{E}} p_i^n} \right) - \text{«}. \end{aligned} \quad (20)$$

5. Subcarrier Allocation

Let $t_{n,i}^*$ and p_i^{n*} be the optimal values obtained from (18) and (19), respectively. We can rewrite (17) as

$$g(\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) = \sum_{n=1}^{N} g_n(\boldsymbol{\lambda}^{\text{e}},\boldsymbol{\lambda}^{\text{j}},\text{«}) + \text{«} P_{\text{BS}}^{\max}, \quad (21)$$

where

$$g_n(\boldsymbol{\lambda}^{\mathrm{e}},\boldsymbol{\lambda}^{\mathrm{j}},\alpha)=\max_i \left\{t^*_{n,i}\ (1-(a^{\mathrm{j}}_{n,i}+a^{e}_{n,i}))\right. \\ \left.+\left(a^{\mathrm{j}}_{n,i}C^{\mathrm{Sj}}_{n,i}+a^{\mathrm{e}}_{n,i}C^{\mathrm{Se}}_{n,i}-\alpha p_i^{n*}\right)\right\}. \quad (22)$$

From (22), it can be seen that subcarrier n is allocated to user i which maximizes the value of

$$\left\{t^*_{n,i}(1-(a^{\mathrm{j}}_{n,i}+a^{\mathrm{e}}_{n,i}))+\left(a^{\mathrm{j}}_{n,i}C^{\mathrm{Sj}}_{n,i}+a^{\mathrm{e}}_{n,i}C^{\mathrm{Se}}_{n,i}-\alpha p_i^{n*}\right)\right\},$$

i.e., $\rho^{n}_{i}=1$

6. Finding the values of dual variables

Based on the values of $\mathbf{p}$ and $\mathbf{t}$ obtained using (18) and (19) and the subcarrier allocation results, we construct the dual function $g(\boldsymbol{\lambda}^{\mathrm{e}},\boldsymbol{\lambda}^{\mathrm{j}},\alpha)$. To find the optimal values of dual variables, i.e., $\boldsymbol{\lambda}^{\mathrm{e}}$, $\boldsymbol{\lambda}^{\mathrm{j}}$, and α, we should solve the following optimization problem which is called dual problem and is given by

$$\min_{\boldsymbol{\lambda}^{\mathrm{e}}\geq\mathbf{0},\boldsymbol{\lambda}^{\mathrm{j}}\geq\mathbf{0},\alpha\geq 0} g(\boldsymbol{\lambda}^{\mathrm{e}},\boldsymbol{\lambda}^{\mathrm{j}},\alpha) \quad (23)$$

An iterative approach to update the values of $a^{\mathrm{e}}_{n,i}$, $a^{\mathrm{j}}_{n,i}$, and α is adopted which is based on the subgradient approach. At iteration $k+1$, we use the following update formula

$$a^{\mathrm{e}}_{n,i}(k+1)=[a^{\mathrm{e}}_{n,i}(k)-s^{a^{\mathrm{e}}_{n,i}}(k)(C^{\mathrm{Se}}_{n,i}-t_{n,i})]^{+}, \quad (24)$$

$$a^{\mathrm{j}}_{n,i}(k+1)=[a^{\mathrm{j}}_{n,i}(k)-s^{a^{\mathrm{j}}_{n,i}}(k)(C^{\mathrm{Sj}}_{n,i}-t_{n,i})]^{+}, \quad (25)$$

$$\alpha(k+1)=[\alpha(k)-s^{\alpha}(k)(P^{\max}_{\mathrm{BS}}-\sum_i\sum_n p_i^n)]^{+}, \quad (26)$$

where $s^{a^{\mathrm{e}}_{n,i}}(k)$, $s^{a^{\mathrm{j}}_{n,i}}(k)$, and $s^{\alpha}(k)$ are update steps [18] of variables $a^{\mathrm{e}}_{n,i}$, $a^{\mathrm{j}}_{n,i}$, and α, respectively.

7. Simulation Results

In this section, we evaluate our proposed scheme using simulations. We consider the downlink of an OFDMA network with $\mathrm{U}=4$ users and one malicious user. For our simulations, we assume that all CNRs, i.e., those of main channels (g_i^n), channels from base station to users, those from base station to malicious user (g_n^{E}), and those from malicious user to legitimate users (h_i^n), are randomly selected from $(0,1)$. We set the number of subcarriers to $N=40$.

In our simulation, we gradually increase the total power constraint, i.e., $P^{\max}_{\mathrm{BS}}$, from $P^{\max}_{\mathrm{BS}}=5$ watts to $P^{\max}_{\mathrm{BS}}=40$ watts and run our proposed resource allocation scheme. For each step, we compute the total secrecy rate given by (4) and the number of eavesdropped and jammed subcarriers. We show the results in Figs. 1 and 2.It is seen from Fig. 1that the total secrecy rate increases. In addition, form Fig. 2, one can realize that while the number of jammed subcarriers decrease with increasing $P^{\max}_{\mathrm{BS}}$, the number of eavesdropped subcarriers increases. This because, increasing $P^{\max}_{\mathrm{BS}}$ will increase the transmit power level assigned to each subcarrier while the jamming power over each subcarrier, i.e., p_n^{j} is constant. This increase, more likely, will increase the secrecy rate obtainable by (2) above that of (1). This means that, if the attacker eavesdrops on that subcarrier, the secrecy rate will be less than the secrecy rate when it jams that subcarrier. Note that, when the transmit power assigned to a subcarrier is zero, we do not count it as eavesdropped or jammed subcarrier.

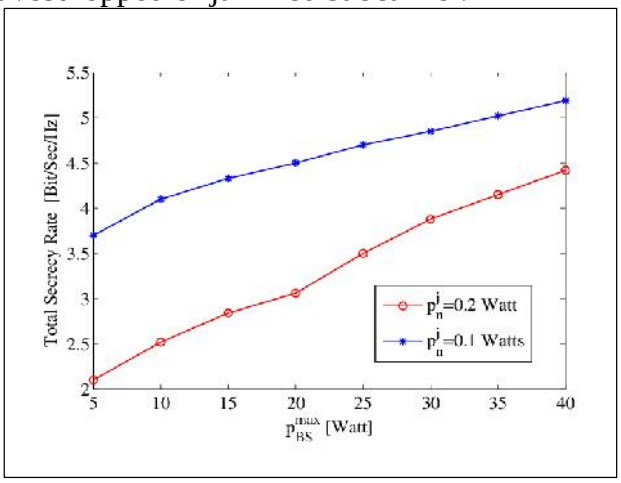

Fig. 1. An instance of proposed scheme and the total secrecy rate as the power upper bound increases.

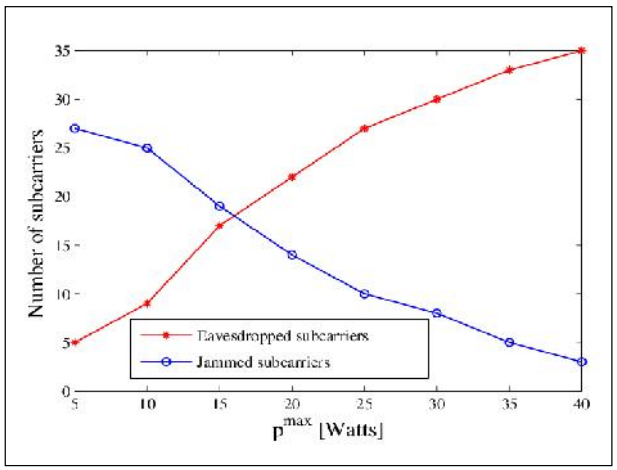

Fig. 2. Number of eavesdropped subcarriers and jammed subcarriers versus total transmit power.

8.Conclusion

In this paper, we considered secure communication for the downlink of an OFDMA network. We assumed that there exists an active attacker which is able to both eavesdrop on and jam the subcarriers but not both at the same time. We formulated the proposed resource allocation problem into an optimization problem and solve it using dual Lagrange approach which gives the subcarriers and transmit power levels assigned to users. By simulations, we evaluated our proposed scheme.

9. References

[1] K. Rajendiran, R. Sankararajan, and R. Palaniappan, “A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography,” ETRI Journal, vol. 33, no. 5, October 2011, pp. 791-801.

[2] S. Tang, L. Xu, N. Liu, X. Huang, J. Ding, and Z. Yang, “Provably Secure Group Key Management Approach Based upon Hyper-Sphere,” To Appear in IEEE Trans. On Par. and Dist. Sys., 2014.

[3] F. Gandino, B. Montrucchio, and M. Rebaudengo, “Key Management for Static Wireless Sensor Networks With Node Adding,” To Appear in IEEE Trans. On Indust. Informatics, 2014.

[4] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. Jour., vol. 54, 1975, pp. 1355-1387.

[5] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Trans. on Inf. Theory, vol. 24, no. 3, October 1978, pp. 339-349.

[6] X. Li, X. Wang, X. Xu, and L. Jin, “A Distributed Implementation Algorithm for Physical Layer Security Based on Untrusted Relay Cooperation and Artificial Noise,” ETRI Journal, vol. 36, no. 1, February 2014, pp. 183-186.

[7] P. K. Gopala, L. Lai, and H. El Gamal, “On the Secrecy Capacity of Fading Channels,” IEEE Trans. on Inf. Theory, vol. 54, no. 10, October 2008, pp. 4687-4698.

[8] Y. Liang, H. Vincent Poor, and S. Shamai, “Secure Communication Over Fading Channels,” IEEE Trans. on Inf. Theory, vol. 54, no. 6, June 2008, pp. 2470-2492.

[9] C. Comaniciu and H. Vincent Poor, “On Energy-Secrecy Trade-Offs for Gaussian Wiretap Channels,” IEEE Trans. on Inform. Foren. and Sec., vol. 8, no. 2, October 2013, pp. 4687-4698.

[10] D. W. Kwan Ng, E. S. Lo, and R. Schober, “Energy-Efficient Resource Allocation for Secure OFDMA Systems,” IEEE on Trans. on Veh. Tech., vol. 61, no. 6, July 2012, pp. 2572-2585.

[11] F. Renna, N. Laurenti, and H. Vincent Poor, “Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels,” IEEE Trans. on Inform. Foren. and Sec., vol. 7, no. 4, August 2012, pp. 1354-1367.

[12] X. Wang, M. Tao, J. Mo, and Y. Xu, “Power and Subcarrier Allocation for Physical-Layer Security in OFDMA-Based Broadband Wireless Networks,” IEEE Trans. on Inform. Foren. and Sec., vol. 6, no. 3, September 2011, pp. 693-702.

[13] A. Mukherjee and A. L. Swindlehurst, “A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures,” Forty Fifth Asilomar Conf. on Sig., Sys. and Comput., Melbourne, Australia, November. 6-9, 2011, pp. 13-18.

[14] G. T. Amariucai and S. Wei, “Half-Duplex Active Eavesdropping in Fast-Fading Channels: A Block-Markov Wyner Secrecy Encoding Scheme,” IEEE Trans. on Inf. Theory, vol. 58, no. 7, July 2012, pp. 4660-4677.

[15] A. Mukherjee and A. L. Swindlehurst, “Jamming Games in the MIMO Wiretap Channel With an Active Eavesdropper,” IEEE Trans. on Sig. Proc., vol. 61, no. 1, January 2013, pp. 82-91.

[16] M. R. Javan, “Guaranteeing secure communication in OFDM network with an active eavesdropper,” in 2014 7th International Symposium on Telecommunications (IST), Tehran, Iran, September 2014, pp. 868-872.

[17] M. R. Javan and N. Mokari, “Resource allocation for maximizing secrecy rate in presence of active eavesdropper,” in 22nd Iranian Conference on Electrical Engineering (ICEE), Tehran, Iran, May 2014, pp. 1565-1568.

[18] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.