International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Applying Opportunistic Scheduling On Miso Wiretap Broadcast Channel

**Arlin Thomas**

M.Tech student, Department of Communication Engineering,
Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

**Abstract:** ***The problem of broadcasting secret information over wireless links under an secrecy constraint has recently been considered in this paper. The work was among the first to consider the impact of multiuser diversity on secrecy systems and proposed an opportunistic scheme that selects the user with the strongest channel at each time slot. In this work, we study the secrecy implications of opportunistic beam forming for the multiple-input single-output broadcast channel. Two opportunistic scheduling schemes exploiting multiuser diversity are investigated. It requires limited feedback of the effective signal-to-noise ratio (SNR) from the legitimate users. We derive new closed-form expressions for the ergodic secrecy rate with beam forming over which Rayleigh fading is considered for two scheduling schemes. The ergodic secrecy rate for two opportunistic scheduling polices: 1) the user with maximal instantaneous channel quality is scheduled for communication, and 2) the proportional fair scheduling (PFS) approach are investigated. illustrate the impact of multiuser diversity on the secrecy performance in under information theoretic perspective.***

**Keywords:** secrecy, wiretap, opportunistic beamf orming, Rayleigh fading

## 1. Introduction

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. Broadcasting is an important technology in wireless communication. Broadcasting is the distribution of audio and/or video content to a dispersed audience via any electronic mass communications medium, but typically one using the electromagnetic spectrum (radio waves), in a one-to-many model. Broadcasting is usually associated with radio and television, though in practice radio and television transmissions take place using both wires and radio waves. The receiving parties may include the general public or a relatively small subset; the point is that anyone with the appropriate receiving technology can receive the signal. Transmission of radio and television programs from a radio or television station to home receivers over the spectrum is referred to as OTA (over the air) or terrestrial broadcasting and in most countries requires a broadcasting license. Transmissions using a combination of satellite and wired transmission, like cable television (which also retransmits OTA stations with their consent), are also considered broadcasts, and do not require a license.

Multi antenna arrays are finding great use in wireless communication systems. Researches to date has focused on the role of such arrays in enhancing the throughput and flexibility for wireless communication systems. Here considering the problem of broadcasting secret information over wireless links in information theoretic perspective. Different antenna techniques simplifies our work load. They are MISO, MIMO, SIMO, SISO. These antenna's made broadcasting simpler. We know that network security is a complicated subject, we need to provide secrecy for each broadcasting information. Eavesdropper places a crucial role in network communication. Eavesdropping which is done in telephone communication is called wiretapping. Here considering the problem of broadcasting secret information over wireless links. And applying opportunistic scheduling schemes to improve the performance of broadcasting. In this paper the secrecy rate of two opportunistic scheduling policies are considered.1) the maximum instantaneous SNR 2) PFS approach [6]

## 2. Literature Survey

Wyner's wiretap channel investigated the role of multiple antennas for secure communication [1]. A natural framework for protecting information at the physical layer is the so-called wiretap channel and associated notion of secrecy capacity is introduced.. In the basic wiretap channel, there are three terminals, one sender, one receiver, and one eavesdropper. Wyner's original treatment established the secrecy capacity for the case where the underlying broadcast channel between the sender and the receiver and eavesdropper is a degraded one.In this work we study the MISO broadcast channel and its secrecy implications when opportunistic beamforming is applied. This model is an extension of [1].

For the eavesdropping channel we are assuming the BS has only statistical CSI (Channel State Information)[7].The channel strength due to constructive and destructive interference between muitipath is important characteristics of wireless channels[6].Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices. Rayleigh fading models assume that the magnitude of a signal that has passed through such a transmission medium (also called a communications channel) will vary randomly, or fade, according to a Rayleigh distribution the radial component of the sum of two uncorrelated Gaussian random variables.

In [2] investigate the problem of broadcasting secret information to one or more receivers over wireless links in the presence of potential eavesdroppers. A fast fading channel model is assumed, with perfect channel state information(of intended receivers) at the transmitter. Both the case of independent messages and common message are considered. For the case of independent messages we

propose a schemethat achieves the sum capacity as the number of receivers goesto infinity. We note that in the limit of large number of intendedusers, capacity scales with the number of intended receivers,but not with power.For the case where a common message is broadcasted, wepresent a coding scheme that achieves a certain positive rateindependently of the number of intended receivers.

## 3. System Model and Assumptions

We consider a MISO wiretap broadcast channel with Mantennas at the BS, K mobile users each with one antenna, and an eavesdropper equipped with N antennas. We assume that the BS communicates with only a single user at a given time, and that the BS has knowledge of only the instantaneousSNR (but not the channels) of all legitimate users, and only statistical information about the eavesdropper channel. Next assumption is that slow block fading for channel to the legitimate users and stationary eavesdropper channel and ergodic within one fading block.

Since we assume uncorrelated Rayleigh fading, limited feedback with only SNR available from legitimate users, we cant provide structured transmit beamformingdesign .. Instead, weassume the BS employs an opportunistic beamforming technique, in which during the nth block, the BS randomly chooses an M × 1 vector of zero-mean unit-variance complex Gaussian random variables, which will be used to form the unit-norm transmit beamformer .The individual users only measure their SNR, and are unaware of the actual value of w(n). During block n ,at time t the received signal at the kth user and eavesdropper can be written as

$$Yk(n,t) = hk(n,t)w(n)s(t) + nk(t) \quad (1)$$

$$Ye(n,t) = he(n,t)w(n)s(t) + ne(t) \quad (2)$$

where s(t) is the transmitted signal with nk(t) and ne(t) represent circularly symmetric zero-mean and unit-variance Gaussian noise at the kth user and eavesdropper, respectively. The channel vector between the BS and the kth user is denoted by whose elements are assumed to be independent and identically distributed (i.i.d.) complex Gaussian random variables with variance $\sigma^2$b , i.e., hk(n) ~ CN(0, $\sigma^2$ b I). The channels for different users are assumed to be mutually independent. He(n, t) ∈ CN×M is the eavesdropper's channel which is stationary and ergodic during block n with i.i.d. entries distributed as CN(0, $\sigma^2$ e ). Since ne(t) is spatially white, the optimal beamformer for the eavesdropper in terms of both SNR and MMSE is maximal ratio combining (MRC) and the corresponding instantaneous SNR at the eavesdropper is given by

$$\bar{\gamma}_e(n,t) = \gamma_e(n,t)P \quad (3)$$

The beginning of each block n ,the BS schedules one of the users,after the BS chosen the transmit beamformer w(n).we are going discuss about the two scheduling policies.

### 3.1 Maximum Instantaneous SNR scheduling

The user with highest instantaneous SNR is scheduled by the BS in this approach.According to (1) the instantaneous SNR of the kth user's channel is given by We will refer to the maximum instantaneous SNR user scheduling criterion as M-SNR, as defined by

$$k1^* = \arg \max_{k=1,\ldots,K} \bar{\gamma}_k(n) = \arg \max_{k=1,\ldots K} \gamma_k(n) \quad (4)$$

### 3.2 Approximate proportional fair scheduling

The PFS approach investigated in[6].It schedules a user when its ratio of instantaneous to average data rate is largest among all users. The user whose ratio of instantaneous to peak received snr is largest then the approach can be simplified. Define the random variable mk (n) as the ratio of instantaneous- to-peak received SNR for user k during the nth block:

$$mk(n) = \frac{\gamma_k(n)}{\tilde{\gamma}(n)} \quad (5)$$

this quantity can be referred as the normalized SNR for user k. Each user to be aware of its own channel hk (n),can be estimating using some training symbols at the beginning of the block. However, the users still feedback only the scalar quantity mk (n) to the BS and they do not need to know w(n). Under this approach, which we refer to as the A-PFS criterion, the user k∗ 2 with the largest normalized SNR is scheduled:

$$m_{k2^*}(n) = \max_{k\in\{1,\ldots K\}} m_k(n) \quad (6)$$

## 4. Secrecy Performance Analysis

In this section, we derive analytical expressions for the ergodic secrecy rate of both of the above multiuser scheduling schemes over Rayleigh fading channels. Preliminaries are given in [10].

### 4.1 Ergodic Secrecy Rate Analysis

The achievable secrecy rate is given by

$$R_s^{(m)} = \max_{0\le\lambda_m\le 1}\{\log_2(1+\lambda_m p\gamma_m) - E_{\gamma_e}[\log_2(1+\lambda_m p\gamma_e)]\}$$

$$R_s^{(m)} = R_s(\lambda_m) \quad (7)$$

This is applicable when the main channel after user scheduling is constant while eavesdropper's channel is fading.

The optimal optimalλm results in an on-off power allocation given in [11]with the threshold

$$\zeta = \frac{1}{P}[\exp\{e^{\frac{1}{p\sigma_e^2}} \sum_{n=1}^{N} E_n(\frac{1}{P\sigma_e^2})\} - 1] \quad (8)$$

Since the users only need to transmit their channel gain to the transmitter when it is greater than the threshold ζ,the on-off approach can reduce the amount of required feedback. The threshold ζ is deliberately devised so that the scheduled

user can achieve a positive secrecy rate, and has the following asymptotic expression in the limit P →∞:

$$\varsigma_{\inf} = \lim_{P\to\infty} \varsigma = \sigma_e^2 \exp(-\gamma + \sum_{n=1}^{N-1} \frac{1}{n}) \quad (9)$$

where γ ≈ 0.577216 is Euler's constant. The asymptotic on-off threshold increases with and N, independent on the number of transmit antennas M.

Theorem 1: The ergodic secrecy rate of the MISO Rayleigh-fading wiretap broadcast channel achieved by opportunistic beamforming under the M-SNR scheduling policywith the on-off power allocation is given by

$$\langle R_s^1 \rangle \zeta = \log_2(e) \sum_{k=1}^{K} KC_k (-1)^{k-1} e^{\frac{k}{P\sigma_b^2}} E_1(\frac{(1+P\zeta)k}{P\sigma_b^2}) \quad (10)$$

Let $\sigma_e^2 = \alpha\sigma_b^2$ The ergodic secrecy rate under the M-SNR scheduling policy is independent of M ≥ 1, it decreases with increasing N and α, and converges to a constant in the limit as P →∞:

$$\langle R_s^1 \rangle \zeta = \log_2(e) \sum_{k=1}^{K} KC_k (-1)^{k-1} E_1(k.\alpha \exp(-\gamma + \sum_{n=1}^{N-1} \frac{1}{n})) \quad (11)$$

Theorem 2: The ergodic secrecy rate of the MISO Rayleigh-fading wiretap broadcast channel achieved by opportunistic beamforming under the A-PFS policy with the on-off power allocation is given in[10]. It is worth noting that as M increases, A-PFS will approach the performance of the M-SNR scheduling policy. Unlike the M-SNR scheduling policy, the ergodic secrecy rate for A-PFS increases with the number of transmit antennas M, and decreases with N and α = σ2 e/σ2b. This is due to the fact that for large M, there is little difference in the value of $\tilde{\gamma}_k$ for different users, and the two scheduling policies will both typically select the same user.

## 5. Simulation Results

In this section, numerical results are presented to examine the impact of the number of antennas, the number of users and the average SNR on the secrecy performance. The solid and dashed lines represent the derived analytical expressions Each result is obtained by averaging over 10000 independent blocksamples. In Fig. 1, we plot the achieved average secrecy rate under both user scheduling polices versus the number of users with M = 4, N = 1 and σ2e = σ2b = 1. We can understand from result as the ergodic secrecy rate increases with the number of users K and the transmit power P.The M-SNR scheme achieves a higher average secrecy rate than A-PFS, since A-PFS ensures scheduling fairness at the cost of throughput loss. Fig. 2 shows the achieved average secrecy rate Rs as a function of transmit power P under the M-SNR scheduling policy with M = 4, K = 40 and σ2e = ασ2b for α = 0 (no intruder), 0.4 and N = 1, 2, 3, 4. The case without wiretapping is used as a reference. We see that the ergodic secrecy rate decreases with increasing N and α, and that the secrecy rate converges at high transmit power P to the constant value.

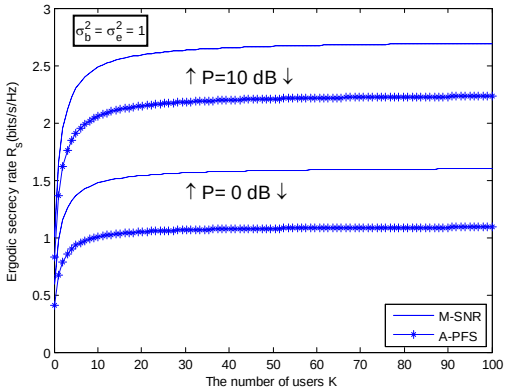


**Figure 5.1:** Average achievable secrecy rate versus the number of users with M = 4, N = 1, for different values of transmit power.

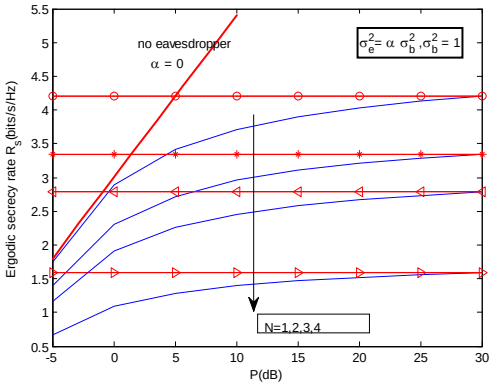


**Figure 5.2:** Average achievable secrecy rate as a function of transmit power P for the M-SNR scheduler with M = 4, K = 40.

## 6. Conclusion

For the secrecy performance of MISO downlink wiretap channels in the presence of a passive multi-antenna eavesdropperwe investigated the use of multiuser scheduling. The MSNR scheme maximizes the instantaneous SNR without considering fairness, while the A-PFS scheme ensures fairness and schedules the user with the largest normalized SNRare the two opportunistic scheduling schemes which were investigated.The ergodic secrecy rateperformance of both methods assuming an on-off power allocation policy and Rayleigh fading channelswere analysed. Through the thorough study we found out that the ergodic secrecy rate of the M-SNR scheme is independent of the number of BS antennas M, while the performance of A-PFS improves with M and ultimately aproaches that of M-SNR. While M-SNR provides a better secrecy rate than A-PFS, it does so at the price of user fairness. Our opportunistic scheduling is effective in providing substantial security at the physical layer.

## References

[1] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," IEEE Signal Process. Lett., vol. 20, no. 2, pp. 141–144, Feb. 2013.

[2] D. Bliss and S. Govindasamy, Adaptive Wireless Communications: MIMO Channels and Networks. Cambridge University Press, 2013.
[3] T. V. Nguyen and H. Shin, "Power allocation and achievable secrecy rate in MISOME wiretap channels," IEEE Commun. Lett., vol. 15, no.11, pp. 1196–1198, Nov. 2011.
[4] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fastRayleigh fading channels," IEEE Trans. Wireless Commun., vol. 9, no.9, pp. 2792–2799, Sept. 2010.
[5] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in Proc. 2009 Military Commun. Conf.
[6] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting over fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453–2469, Jun. 2008
[7] A. Khisti, A. Tchamkerten, and G. W. Wornell, "Secure broadcasting with multiuser diversity," in Proc. 2006 Allerton Conf. Commun. Contr.Computing.
[8] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," IEEE Trans. Inf. Theory, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.
[9] N. Sharma and L. Ozarow, "A study of opportunism for multiple-antenna systems," IEEE Trans. Inf. Theory, vol. 51, no. 5, pp. 1804 1814, May 2005.
[10] Minyan Pei, A. Lee Swindlehurst, Fellow, IEEE, Dongtang Ma, and Jibo Wei ,"On Ergodic Secrecy Rate for miso wiretap broadcast channels
[11] T. V. Nguyen and H. Shin, "Power allocation and achievable secrecy rate in MISOME wiretap channels," IEEE Commun. Lett., vol. 15, no. 11, pp. 1196–1198, Nov. 2011.

## Author Profile

**Arlin Thomas** received the B.Tech degreein Electronics And Communication Engineering from M.G University, Kerala at Mar Baselios Christian College Of Engineering And Technology 2013. And now she is pursuing her M.Tech degree in Communication Engineering under the same university in Mount Zion College of Engineering.