Random Time Slot Assignment for enhancing wireless security in Multi-User SISO Systems

Jin Guang *
School of Vehicle Engineering
Zhengzhou Railway Vocational and Technical College
Zhengzhou 450052 China,13603998031
Jguang80@sina.com

Zhang Tiantong
School of Vehicle Engineering
Zhengzhou Railway Vocational and Technical College
Zhengzhou. 450052 China

***Abstract*—Considering a multi-user SISO system, a random time slot assignment scheme is proposed for enhancing wireless security. For each time slot, single antenna transmitter selects a user randomly. Signals of the intended user are pre-processed before transmitting using known wireless channel state information, which not only offsets the impact of multipath channels but also produces characteristic mark for intended user. Eavesdropper cannot demodulate the signal and couldn't know the intended receiver. Formal derivation shows that the intended user can get the signals based on the characteristic mark, but eavesdropper cannot obtain any information because that the equivalent channel between him and transmitter is changed randomly. Simulation results show that BER performance of intended user can achieve the SNR gain dramatically. But that of the eavesdropper is very poor, just as guessing aimlessly.**

Keywords-PHY-Layer Security, Wireless Communication, SISO

I. INTRODUCTION

Wireless security has become a critical concern when wireless devices become increasingly pervasive and essential [1]. Traditional high-level security techniques encounte many challenges due to the broadcasting nature of wireless transmissions. Although conventional cryptographic security mechanisms are essential to secure wireless system, the techniques do not leverage the sole characteristics of wireless domain to address security threats directly. So physical-layer security are useful, since they can be effective in resolving the link reliability issues.

Recent researches [2-4] have proposed exploitation of physical layer approaches to enhance wireless security by using the unique wireless channel state information (CSI). In [4], a special deliberate randomization method for designing the transmit antenna weights, with more detailed explanation, security analysis and the proof of LPI (Low Probability of Interception). In fact, the method depends on two special properties of wireless transmissions for security: channel diversity that makes signals received by the eavesdroppers and the authorized receiver different, and array redundancy that provides degrees of freedom for randomizing the transmitted signals deliberately. But there is not array redundancy in SISO system. How to guarantee wireless security is very important in many existing SISO system. Multi-user system can provide users redundancy in SISO system. In multi-user system, TDMA is the most intuitive way of multiple access. It divides time into periodic frame, and some time slots are divided in each frame. Then a certain criteria is used to ensure proper communication between multiple users and base station. Every user receives signals in specified time slots, who can distinguish his signals from received combined signal easily.

There are two important issues related to physical-layer security of SISO system that should be addressed. First is that in a richly scattered multipath environment, it is difficult for an adversary to create or precisely model a waveform that is transmitted and received by entities that are more than a wavelength away from the adversary. The second issue is the idea that any adversary and users in a wireless setting have different channels with little correlation is the basic for considering physical-layer security.

In this paper, we propose a random time slot assignment scheme for enhancing wireless security. By pre-processing the transmitted data with the intended user channel state information and applying the randomization of the user selection, the eavesdropper would suffer from high received interference level and the interception probability is therefore decreased. Our analytical and numerical results have shown that the proposed scheme can guarantee excellent performance for the intended user, while the worst performance for eavesdropper Eve. The paper is organized as follows: In Section II we introduce the system model of wireless security studied in the paper. In Section III we present the formal derivation of the proposed security scheme. Then, in Section IV, we analyze the impacts of randomization for fairness and throughput of the system. Simulation results are presented in Section V followed by conclusions in Section VI.

II. SYSTEM MODEL

We also draw on conventional terminology of the security community by using three different parties: Alice, Bobs and Eve. Where Bobs stand for multi-users. The three entities may be thought as wireless transmitters/receivers that are potentially located in separated positions. Our two legitimate protagonists are the usual Alice and Bobs, and their nefarious adversary, Eve, will serve as a silent

This work was supported by the National Natural Science Foundation of China.

adversary for the sake of discussion throughout this paper. In our system model we assume that the eavesdropper Eve can hear all the communications between legitimate nodes Alice and Bobs. She can also achieve the channels between herself and Bob when Bob is sending the pilot signal to measure the channel between him and Alice. The only thing, Eve cannot know, is the wireless channel characteristics between Alice and Bob because that she cannot be very close to either Alice or Bob. Literature [5] [6] addressed that the distance of more than a few multiples of the wavelength of radio waves being used will ensure that Eve achieve a different, uncorrelated radio channel.

We consider the scenario where two legitimate entities Alice and Bobs wish to establish a secure communication link in the presence of an unknown eavesdropper Eve. Alice transmits a symbol sequence S_i, which is assumed as i.i.d uniformly distributed with zero-mean and unit variance using one antenna to user i. In establishing step, we consider that Bobs send probe signals to make Alice know the SISO channels, $[h_0(t), h_1(t), \mathrm{L}, h_{M-1}(t)]$. In a multipath rich environment, the channel appears to be time dispersive, which represented as an FIR filter. So $h_i(t)$ is the CSI of the i th user, which can be written as

$$h_i(t) = \sum_{j=0}^{L-1} \alpha_{i,j} \delta(t - \tau_{i,j}) \tag{1}$$

where $\alpha_{i,j}$ is the j th multipath attenuation of user i, $0 \le i \le M-1$ and $0 \le j \le L-1$. L is the number of multipath. And $\tau_{i,j}$ is the j th multipath delay of user i. Our objective, broadly speaking, is to provide security between Alice and Bobs using these scattering channels, despite the presence of Eve.

III. THE PROPOSED SECURITY SCHEME

This paper proposes a security scheme for time division duplex (TDD) multi-user SISO systems. In the proposed scheme, the single antenna transmitter not only selects a user randomly and sends corresponding signals for each time slot, but also pre-processes the signals using known channel statement information getting from pilot signals of uplink. Fig.1 shows the procedure for the proposed security scheme. When uplink pilot signal is obtained, Alice can get the channels information of all of users, which determine the parameters of pre-processing. This operation not only offsets the impact of multipath channels but also produces characteristic mark for intended user. The former allows the intended user can receive signal directly without considering the impact of wireless multipath channel. The later can inform the intended user to receive. The formal derivation is as follows. Without loss of generality, suppose there are M users and a data frame is divided into NM time slots. In each time slot only one user can be chosen to communicate.

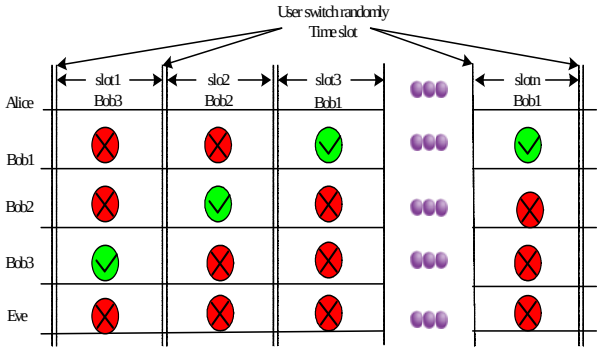

Fig. 1. Illustration of proposed scheme

The pre-processing parameters of the k th time slot depend on CSI of current selected user totally, which must be best matched with the target channel response. Assuming user i is selected in the k th time slot, the pre-processing parameters $\omega(T_k)$ can be expressed as

$$\omega(T_k) * h_i(T_k) = R_i^{auto}(T_k) \tag{2}$$

where, " * " denotes convolution operation, $0 \le i \le M-1$ and $0 \le k \le NM-1$, $R_i^{auto}(t)$ is the autocorrelation function of $h_i(T_k)$. $h_i(T_k)$ denotes CSI between user i and Alice in the k th time slot. Without loss of generality, suppose fading is sufficiently slow, so $h_i(T_k) = h_i(t), 0 \le t \le \sum_{k=0}^{MN-1} \mathrm{T_k}$. Then signals sent by Alice can be written as $S(T_k) = s_i(T_k) * \omega(T_k)$ in k th time slot. The received signals of user i can be stated as

$$y_i(T_k) = s_i(T_k) * \omega(T_k) * h_i(T_k) + n_i(T_k) = s_i(T_k) * R_i^{auto}(T_k) + n_i(T_k) \tag{3}$$

where $n_i(T_k)$ is the additive white Gaussian noise that corrupt the received signal of user i with zero-mean and positive definite covariance $\sigma^2 I$. So $y_i(T_k)$ can be written as

$$y_i(T_k) = s_i(T_k) * \sum_{m=0}^{L-1} \alpha_{i,m}^2 \delta(T_k) + \underbrace{s_i(T_k) * \sum_{n=0}^{L-1} \sum_{m=0, m \ne n}^{L-1} \alpha_{i,m} \alpha_{i,n} \delta(T_k - \tau_{i,m} + \tau_{i,n}) + n_i(T_k)}_{I_i \text{interference+niose}} \tag{4}$$

The first term is the desired signal corresponding to symbols of user k and the remaining terms represent the

interference and noise corruption at the receiver, I_i. According to the above equation, the received signal is temporal focused, which can shorten the channel response. As a result, the complexity of receiver is reduced for Bobs.

In the paper, we define characteristic mark as CM, which stands for a ratio expressed as

$$CM_i = \frac{\left(\sum_{m=0}^{L-1} \alpha_{i,m}^2\right)^2}{\left(\sum_{m=0}^{L-2} \alpha_{i,m}\alpha_{i,m+1}\right)^2 + \sigma^2} \tag{5}$$

The received signals of user $j(j \neq i)$ and Eve can be stated as

$$y_{j(Eve)}(T_k) = s_i(T_k) * \omega(T_k) * h_{j(Eve)}(T_k) + n_{j(Eve)}(T_k) = s_i(T_k) * R_{i,j(Eve)}^{cross}(T_k) + n_{j(Eve)}(T_k) \tag{6}$$

where $R_{i,j(Eve)}^{cross}(T_k)$ is the cross-correlation function of $h_i(T_k)$ and $h_{j(Eve)}(T_k)$. So $y_{j(Eve)}(T_k)$ can be written as

$$y_{j(Eve)}(T_k) = s_i(T_k) * \left(\sum_{n=0}^{L-1}\sum_{m=0}^{L-1} \alpha_{i,m}\alpha_{j(Eve),n}\delta(T_k - \tau_{i,m} + \tau_{j(Eve),n})\right) + n_{j(Eve)}(T_k) \tag{7}$$

The CM of user j and Eve is given by theorem 1:

Theorem 1: Assume i is current intended user and the CSI of any user is not related to others. For user $j(j \neq i)$ and eavesdropper Eve, the characteristic mark is $CM_{j(Eve)}$. We can draw the inequality as follows

$$0 \le CM_{j(Eve)} < \frac{\left(\sum_{m=0}^{L-1} \alpha_{i,m}^2\right)^2}{\left(\sum_{m=0}^{L-2} \alpha_{i,m}\alpha_{i,m+1}\right)^2 + \sigma^2} \tag{8}$$

Proof: Because the CSI of any user is not related to others, in the case that multipath delays are not equal to each other, the characteristic mark has minimum value without multipath overlapping after pre-processing. According to (7), the characteristic mark equals to zero, namely

$$\mathrm{CM}_{\mathrm{j(Eve)}} = 0 \tag{9}$$

Another case is the phenomenon of overlapping multipath delays. The most extreme case is that all the corresponding multipath delays are equal, which is also the largest characteristic mark case. We have

$$CM_{j(Eve)} \le \frac{\left(\sum_{m=0}^{L-1} \alpha_{i,m}\alpha_{j,m}\right)^2}{\left(\sum_{m=0}^{L-2} \alpha_{i,m}\alpha_{j,m+1}\right)^2 + \sigma^2} \tag{10}$$

Because the CSI of any user is not correlated to others. we can get $\sum_{m=0}^{L-1} \alpha_{i,m}\alpha_{j,m} < \sum_{m=0}^{L-1} \alpha_{i,m}^2$. So

$$\frac{\left(\sum_{m=0}^{L-1} \alpha_{i,m}\alpha_{j,m}\right)^2}{\left(\sum_{m=0}^{L-2} \alpha_{i,m}\alpha_{j,m+1}\right)^2 + \sigma^2} < \frac{\left(\sum_{m=0}^{L-1} \alpha_{i,m}^2\right)^2}{\left(\sum_{m=0}^{L-2} \alpha_{i,m}\alpha_{i,m+1}\right)^2 + \sigma^2} \tag{11}$$

The theory can be proved clearly by the above inequalities. The result of theory 1 show that the characteristic mark for intended user is only detected by intended user itself. So Bobs can determine their own time slots to communicate by the characteristic mark, neglecting other time slots. Now there is a discussion of what happens over time. The received signals of Eve during the time of a data frame can be stated as

$$y_{Eve}(t) = s_{T_{[0,L\ NM-1]}}(t) * \omega_{T_{[0,L\ NM-1]}}(t) * h_{Eve}(t) + n_{Eve}(t) \tag{12}$$

where $s_{T_{[0,L\ NM-1]}}(t)$ is the sent signals of NM time slots, and $\omega_{T_{[0,L\ NM-1]}}(t)$ is the pre-processing parameters of NM time slots. So the equivalent channel between Alice and Eve is $\omega_{T_{[0,L\ NM-1]}}(t) * h_{Eve}(t)$, which is $R_{q(T_k),Eve}^{cross}(t), T_k \in T_{[0,L\ NM-1]}$. $q(T_k)$ is selected user in time slot k, which is varied randomly from one time slot to another. That is to say, Eve cannot achieve any characteristic mark and she cannot know who is the intended user in the current time slot. The result indicates that unauthorized Eve cannot demodulate the original signals by blind deconvolution method, as proved in [4], which is the most typical iterative method.

IV. THE IMPACT OF RANDOMIZATION FOR FAIRNESS AND THROUGHPUT OF THE SYSTEM

According to the analysis above, we can get that the fairness of users of the system is affected by the distribution of random user selection. Without loss of generality, we assume that the distribution of random user selection is

uniform. In a certain time slot, the probability of any user being selected is equal. Statistically, any user is fair in the physical-layer security system. However, obviously, the proposed scheme cannot meet any other different rate demand for some users. It is easily observed that the proposed scheme has a reduction in throughput because that the station select randomly a user in a certain time slot instead of an optimize one, which can guarantee to obtain the biggest throughput of the system.

V. SIMULATION RESULTS

In order to verify the analysis presented above, the uncoded BER of users and Eve are studied through computer simulations. Eve is assumed to estimate symbols by blind equalization (specifically, via the constant modulus algorithm [7,8]). The frequency-selective channel consists of six independent Rayleigh multipath components is used. And we use QPSK transmission. Each BER was evaluated as the average of 10000 runs, and 12800 QPSK symbols were transmitted in one data frame for all users.

Results for systems employing $M = 2,4,8$ users are plotted in Fig.2 (only one user is pictured). We used the frame length is $20ms$ and 200 time slots are achieved in one frame, $T = 64$. We can get that the security does not depend on the number of user in the network. Because that the time slot is small, in which Eve cannot estimate symbols by blind equalization. And the equivalent channel between him and Alice is changed randomly over time even $M = 2$. Fig.3 shows the comparison of BER vs SNR among three cased, including time slot equates to 64 times symbol interval, 128 times symbol interval and 256 times symbol interval respectively. As illustrated in Fig.3, the security depends on the length of time slot, which does not affect the performance of intended user markedly.

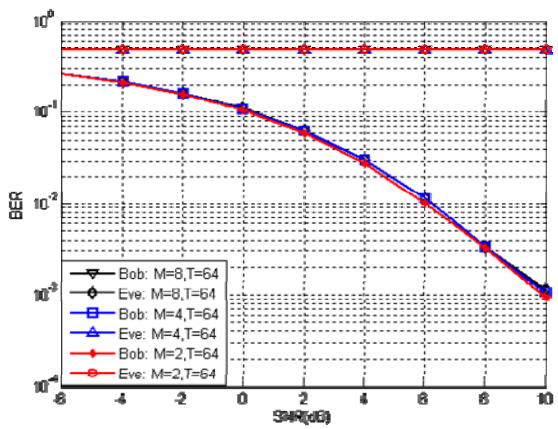

Fig. 2. BER of Bobs and Eve vs. SNR with the different number of users

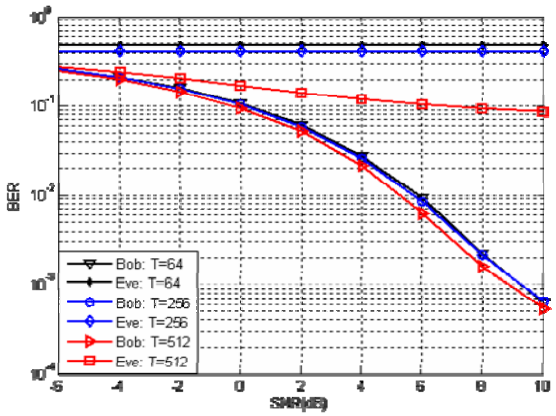

Fig. 3. BER of Bobs and Eve vs. SNR with the different length of time slot

VI. CONCLUSION

We have proposed and analyzed a random time slot assignment scheme for enhancing wireless security in multi-user SISO TDD system where CSI can be used. In this scheme, time is divided to time slots, a station randomly picks one user to communicate. The estimated multipath components are used to hide the communication from an eavesdropper that experiences independent multipath characteristics. Our analytical and numerical results have shown that the proposed scheme can guarantee excellent performance for the intended user, while the worst performance for eavesdropper Eve. Before closing this paper, we should highlight that the impact of imperfect CSI is not considered for page limit, but which would be another interesting future direction.

REFERENCES

[1] X. Q. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor Network Security: A Survey," IEEE Commun. Surveys Tutorials, vol. 11. pp.52-72, 2009.

[2] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," IEEE Commun. Surveys Tutorials, vol. 7, pp. 2-28, 2005.

[3] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in WSNs," IEEE Commun. Surveys Tutorials, vol. 8, pp. 2-23, 2006.

[4] X. Li, J. Hwu, and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," J. Commun, vol. 2, pp. 24-32, 2007.

[5] S. Mathur, W. Trappe, N. B. Mandayam, C. Ye, and A. Reznik. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," In ACM MOBICOM Conference, Sept. 2008. pp. 698-721

[6] G. D. Durgin. Space-Time Wireless Channels. Prentice Hall PTR, 2002.

[7] S. V. Kim, C. H. Choi, "An Enhanced Godard Blind Equalizer Based on the Analysis of Transient Phase," IEEE Trans. On Signal Processing, pp. 919-926, 2001.

[8] D. N. Godard, "Self-recovering equalization and carrier tracking in two-dimensional data communication systems," IEEE Trans. Commun. vol. COM-28, pp. 1867-1875, 1980.