Enhancing the Security of Wireless Communication with the Aid of Guard Nodes

Lukman A. Olawoyin, Hongwen Yang, and Yue Wu
Wireless Communication Center, Beijing University of Posts and Telecommunication, Beijing, 100876, China
Email: {lolawoyin, yanghong, wuyue}@bupt.edu.cn

Abstract —The wireless system secrecy capacity over the fading channel can be improved with the use of intentionally generated noise signal broadcasted from the transmitter or external jammers. In this paper, the impact of deployment of multiple multi-antenna guard/independent noise generator nodes with each node broadcasting artificial noise to disrupt the signal received by passive eavesdropper is examined on the secrecy performance of wireless networks. Compared with the existing methods, the proposed scheme is very simple for the implementation because it requires no Channel State Information (CSI) about eavesdropper, no cooperation among the guard nodes, no complicated algorithms for scheduling, joint beamforming or other resource managements. Simulation results show that the system performance metric, secrecy capacity and the interception probability, can be improved by 9%.

Index Terms—Wireless security, artificial noise, guard node, uplink and downlink communications, secrecy capacity, intercept probability.

I. Introduction

Wireless systems have become the most widely and easiest means of transferring information between two parties or locations because of its flexibility, adaptability, mobility and it availability. Consequently, wireless systems is very useful in all the human day-to-day activities such as in health management systems, stock and banking operations, sensor and signaling control systems and so on. Although wireless transmission have contributed immensely in revolutionizing the modern day communication systems, however, the security challenges have been the major issues associated with the systems due to its broadcast nature. Traditionally, security issues had been largely addressed with the use of cryptography methods [1]. Several shortcomings and other requirements that associated with the cryptography approaches make the technique unsuitable for wireless system as presented by Mandal *et al* in [2]. These include inappropriate prediction of the computational power of an eavesdropper, complex key exchange management and complex distribution algorithm. Recently, there has been a growing interest to ensure system secrecy and information reliability in wireless system without the use of secret key exchange. Thus, the use of physical layer in information security has become a hot research area and topical issues [3].

The concept of wire-tap channel was first introduced by Wyner [4] and it is shown that a positive secrecy data rate can be achieved when the channel between the source and eavesdropper is a degraded version of the source to legitimate receiver channel. This concept was further generalized by Csiszár *et al* in [5], and also, the notion of secrecy capacity was introduced. Barros *et al* in [6] defined secrecy capacity as the maximum transmission rate of reliable information in wireless system from the source to legitimate receiver in the presence of eavesdropper. The use of intermediate relay node transmitting information between the source and the receiver which is referred to as Cooperative Communication (CC) was presented in [7]. The authors, in their work, showed that secrecy capacity could be enhanced in broadcast wireless network with the use of external relay nodes. Several CC techniques have been proposed such as beamforming (BF), Artificial Noise (AN) and they have been seen effective in improving secrecy capacity of wireless system [8], [9]. The author in [10] presented the use of three types of relay selections: minimum, conventional and optimal relay selection in secrecy enhancement. Al-Qahtani in [11] discussed the concept of opportunistic relay selection where the solution to outdated CSI, the notion of best and worst relay selection and their antecedent effects on information security in wireless system are discussed.

Employing multiple antennas at a node is usually costly and limited by the size of the node and the power consumption. Alternatively, improved secrecy can be obtained by employing Multiple-Input Multiple-Output (MIMO) antenna system or cooperating relays which can either forward the signal to the destination, or jam the eavesdropper. Recently, multiple decode-and-forward (DF) relays were employed in [12], [13] to cooperatively beam form the signal to the destination. In such cooperative system, transmission takes two-hop slots; in the first slot, the source transmits, and in the second slots, the relay cooperatively beam form the decoded source signal to the destination. The secrecy capacities of many wireless systems were investigated such as in [14] where the authors proposed the method to enhance the transmitter-receiver channel and leave the eavesdropper

Manuscript received February 10, 2016; revised June 22, 2016.
Corresponding author email: lolawoyin@bupt.edu.cn.
doi:10.12720/jcm.11.6.586-591

channel unaffected. The application of Full-Duplex (FD) technique for secrecy enhancement in wireless system was presented in [15], [16] where the legitimate receiver assist the transmitter in degrading the channel capacity of eavesdropper by transmitting additional AN from its own transmit antenna due to its FD mode. Ciao *et al* in [17] proposed the use of BF method where the perspective of quality of service was discussed. In their work, the BF technique is applied in such that the quality of main channel is enhanced while the eavesdropper channel is degraded with the assumption that both the main Channel State Information (CSI) and eavesdropper CSI are known to the transmitter. The authors in [18] investigated the MIMO wiretap channels with imperfect CSI. The use of transmit antenna selection was presented in [19], in their work, the authors proposed the use of best antenna at the transmitter to transmit the information signal while the other antennas are used for transmitting AN. The system realization can be greatly simplified since there is minimum requirements for nodes cooperation. Although, in cooperation communication, such as joint BF or joint jamming will definitely enhance the secrecy performance, however it requires heavy overhead in backhaul signaling for exchanging precoding information, sharing user data for joint BF or AN for joint BF. In addition, the joint BF or jamming also requires strict synchronization among cooperative nodes.

To the best of our knowledge, no literature has ever discussed the application of guard nodes to protect the information transmission in broadcast wireless system. In this work, a simple secure transmission scheme for cellular wireless system which employs the use of guard nodes to degrade the eavesdropper's channel. The guard nodes in the proposed scheme are simply interferers which transmit AN all the time but the noise is aligned to the null-space of the legitimate receiver. The proposed scheme requires no CSI about the passive eavesdropper, and neither the backhaul links between guard nodes and base station. Simulation results show that, by deploying multiple guard nodes, the secrecy performance of wireless network can be improved significantly.

The rest of this paper is organized as follows. In Section II, we describe the system model. In Section III, we present the proposed secrecy technique while the system performance evaluation is discussed in Section IV. The numerical simulations to verify our proposed scheme is presented in Section V. The paper is concluded in Section VI.

Notation: throughout this paper, the following notations are used: italics and non-boldface denote scalar variables. boldface, lower and upper case denote vectors and matrices, respectively. $\|.\|$ and $|\cdot|$ represent Euclidean norm and absolute value, respectively. $.^{\mathrm{T}}$, $(\cdot)^{\mathrm{H}}$ and $(\cdot)^{*}$ denote transpose, Hermitian and complex conjugates, respectively while $\mathrm{E}[\cdot]$ is used for expectation value.

II. System Model

Consider the system model shown in Fig. 1. Alice is communicating a secret message with Bob in the presence of passive eavesdropper (Eve). There are M guard nodes which help to degrade the Eve channel by transmitting AN from their respective nodes.

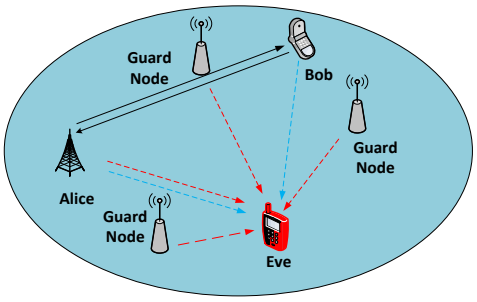


Fig. 1. The system model

In this work, Alice is denoted by cellular base station or Access Point (AP) in a wireless fidelity (Wi-Fi) network, guard nodes are fixed stations intentionally deployed by the operator of the cellular system or the owner of the AP. Bob, Eve are mobile terminals or users, respectively. We assume that Alice, Eve and each guard node have multiple antennas while Bob has a single antenna. Alice and guard nodes have perfect CSI about the links to Bob, guard nodes have perfect CSI about the links between the guard node and Alice. Eve is a passive node which is unaware to the network devices and hence its CSI is not available to Alice and guard nodes. We also assume that there are no backhaul link or special interface between Alice and guard nodes. In other words, Alice has no control over guard nodes i.e. each guard node operates independently. Both uplink and downlink are taken into considerations and we assume that Alice operates in half-duplex mode. For downlink, Alice transmits both data and AN all with power P but with different precoder: Alice transmits the information signal to Bob while AN is projected towards the Bob's null space. For uplink communication, Bob, which is equipped with single antenna, sends only the data with power P . All guard nodes are simple interferers transmitting AN all the time with power P. In the downlink communication, the AN transmitted by Alice lies in the null space of Bob while in the uplink communication, the AN from Bob lies in the null space of Alice.

We also assume that the uplink/downlink channels are reciprocal and symmetrical. The path link between node x to node y is denoted by β_{xy} and we use the simplified path loss model [20]

$$\beta_{\mathrm{xy}} = K\left(\frac{d_{\mathrm{xy}}}{d_0}\right)^{-\lambda} \tag{1}$$

where d_{xy} is the distance between node x and node y, d_0 is the reference distance, λ is the path-loss exponent, K is a constant.

The fast fading channel from Alice and Bob is denoted by a row vector $\boldsymbol{h}_{\mathrm{ab}}^{\mathrm{T}}$ of length N since Alice has N antennas while Bob has only one antenna. The channel from Bob to Alice is the column vector $\mathbf{h}_{\mathrm{ab}}$ due to the reciprocity. Similarly, the fast fading channel from Alice to Eve is denoted by an $N\times N$ matrix $\mathbf{H}_{\mathrm{ae}}$. The channel form i-th guard node to Eve is denoted by an $N\times N$ matrix $\mathbf{H}_i$. For the purpose of simplifying the notations, we take Alice as the guard node indexed by $i=1$. Thus we will interchangeably use both $\boldsymbol{H}_1$ and $\mathbf{H}_{\mathrm{ae}}$ to denote the channel from Alice to Eve. The channel from Bob to Eve is denoted by a column vector $\mathbf{h}_{\mathrm{be}}$. The channel from guard node to Alice and Bob are denoted by $\boldsymbol{H}_{\mathrm{a},i}$ and $\boldsymbol{h}_{\mathrm{b},i}^{\mathrm{T}}$, respectively. Note that $\boldsymbol{h}_{\mathrm{b},1}^{\mathrm{T}}=\boldsymbol{h}_{\mathrm{ab}}$.

III. Proposed Secrecy Technique

During the downlink transmission, Alice transmits the information signal x_a which a unit power $\mathrm{E}\left[\left|x_a\right|^2\right]=1$.The received signal at the Bob node during the downlink is given by

$$\begin{aligned} y_{\mathrm{b}} &= \sqrt{\beta_{\mathrm{ab}}P}\boldsymbol{h}_{\mathrm{ab}}^{\mathrm{T}}\boldsymbol{u}x_{\mathrm{a}}+n_{\mathrm{b}} \\ &= \sqrt{\beta_{\mathrm{ab}}P}\left\|\boldsymbol{h}_{\mathrm{ab}}\right\|x_{\mathrm{a}}+n_{\mathrm{b}} \end{aligned} \tag{2}$$

where $\boldsymbol{u}=\dfrac{\boldsymbol{h}_{\mathrm{ab}}^{*}}{\left\|\boldsymbol{h}_{\mathrm{ab}}\right\|}$ is the precoding vector, n_{b} is the noise which is defined as a Gaussian variable with zero mean and variance σ^2.

Ignoring the AN from Bob which is in null space of Alice, the received signal at the Alice node during the uplink is a vector given by

$$\boldsymbol{y}_{\mathrm{a}}=\sqrt{\beta_{\mathrm{ab}}P}\boldsymbol{h}_{\mathrm{ab}}x_{\mathrm{b}}+\boldsymbol{n}_{\mathrm{a}} \tag{3}$$

where x_{b} is the information carrying signal transmitted by Bob which has unit power $\mathrm{E}\left[\left|x_{\mathrm{b}}\right|^2\right]=1$, $\boldsymbol{n}_{\mathrm{a}}$ is the noise vector at the receiver and its elements are independently and identically distributed (i.i.d.) Gaussian random variables with zero mean and variance σ^2.

Since Alice has multiple antennas, in order to obtained the maximum signal, we assume it employed maximum ratio combining (MRC), then the Signal-to-Noise Ratio (SNR) for both uplink and downlink communication is given by

$$\begin{aligned} \gamma_{\mathrm{b}} &= \frac{\beta_{\mathrm{ab}}\left\|\boldsymbol{h}_{\mathrm{ab}}\right\|^2P}{\sigma^2} \\ &= \bar{\gamma}.\beta_{\mathrm{ab}}\left\|\boldsymbol{h}_{\mathrm{ab}}\right\|^2 \end{aligned} \tag{4}$$

where $\bar{\gamma}=\dfrac{P}{\sigma^2}$.

During the downlink transmission, the received signal at Eve is given by vector

$$\boldsymbol{y}_{\mathrm{e}}^{\mathrm{DL}}=\sqrt{\beta_{\mathrm{ae}}P}\boldsymbol{H}_{\mathrm{ae}}\boldsymbol{u}x_{\mathrm{a}}+\sum_{i=1}^{M}\sqrt{\beta_iP}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{DL}}w_i^{\mathrm{DL}}+\boldsymbol{n}_{\mathrm{e}}^{\mathrm{DL}} \tag{5}$$

where x_a is as defined above, w_i^{DL} is the artificial noise transmitted by i-th guard node, $\mathrm{E}\left[\left|w_i^{\mathrm{DL}}\right|^2\right]=1$, $\boldsymbol{v}_i^{\mathrm{DL}}$ is the unit norm precoding vectors used at i-th guard node which is orthogonal to the channel between Bob and guard node, i.e. $\boldsymbol{h}_{\mathrm{b},i}^{\mathrm{T}}\boldsymbol{v}_i^{\mathrm{DL}}=0$. M is the number of guard nodes (include Alice); $\beta_1=\beta_{\mathrm{ae}}$; $\boldsymbol{n}_{\mathrm{e}}^{\mathrm{DL}}$ is the noise vector at Eve during downlink transmission, the elements of $\boldsymbol{n}_{\mathrm{e}}^{\mathrm{DL}}$ are i.i.d. Gaussian variables with zero mean and variance σ^2

It is worth-noting that, for fixed $\boldsymbol{h}_{\mathrm{b},i}$,the equation $\boldsymbol{h}_{\mathrm{b},i}^{\mathrm{T}}\boldsymbol{v}_i^{\mathrm{DL}}=0$ has many solutions. Assuming that the guard node randomly select one solution for $\boldsymbol{v}_i^{\mathrm{DL}}$, then $\boldsymbol{v}_i^{\mathrm{DL}}$ is unknown to Eve. Under this condition, the best strategy for Eve to obtain the maximum signal reception is by using MRC. The SNR at Eve is then given by

$$\begin{aligned} \gamma_{\mathrm{e}}^{\mathrm{DL}} &= \frac{\beta_{\mathrm{ae}}P\left\|\boldsymbol{H}_{\mathrm{ae}}\boldsymbol{u}\right\|^2}{\dfrac{1}{\left\|\boldsymbol{H}_{\mathrm{ae}}\boldsymbol{u}\right\|}\sum_{i=1}^{M}\beta_iP\left\|\boldsymbol{u}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ae}}^{\mathrm{H}}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{DL}}\right\|^2+\sigma^2} \\ &= \frac{\beta_{\mathrm{ae}}\left\|\boldsymbol{H}_{\mathrm{ae}}\boldsymbol{u}\right\|^2}{\dfrac{1}{\left\|\boldsymbol{H}_{\mathrm{ae}}\boldsymbol{u}\right\|}\sum_{i=1}^{M}\beta_i\left\|\boldsymbol{u}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{ae}}^{\mathrm{H}}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{DL}}\right\|^2+1/\bar{\gamma}}. \end{aligned} \tag{6}$$

Similarly, during uplink transmission, the received signal at Eve is given by vector

$$\boldsymbol{y}_{\mathrm{e}}^{\mathrm{UL}}=\sqrt{\beta_{\mathrm{be}}P}\boldsymbol{h}_{\mathrm{be}}x_{\mathrm{b}}+\sum_{i=2}^{M}\sqrt{\beta_iP}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{UL}}w_i^{\mathrm{UL}}+\boldsymbol{n}_{\mathrm{e}}^{\mathrm{UL}} \tag{7}$$

where w_i^{UL} is the artificial noise transmitted by i-th guard node and $\mathrm{E}\left[\left|w_i^{\mathrm{UL}}\right|^2\right]=1$, $\boldsymbol{v}_i^{\mathrm{UL}}$ is the unit norm precoding vectors used at i-th guard node satisfying $\boldsymbol{h}_{\mathrm{ab}}^{\mathrm{H}}\boldsymbol{H}_{\mathrm{a},i}\boldsymbol{v}_i^{\mathrm{UL}}=0$ while $\boldsymbol{n}_{\mathrm{e}}^{\mathrm{UL}}$ is the noise vector which has identical distribution as $\boldsymbol{n}_{\mathrm{e}}^{\mathrm{DL}}$. The SNR at the Eve is given by

$$\begin{aligned} \gamma_{\mathrm{e}}^{\mathrm{UL}} &= \frac{\beta_{\mathrm{be}}P\left\|\boldsymbol{h}_{\mathrm{be}}\right\|^2}{\dfrac{1}{\left\|\boldsymbol{h}_{\mathrm{be}}\right\|}\sum_{i=2}^{M}\beta_iP\left\|\boldsymbol{h}_{\mathrm{be}}^{\mathrm{H}}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{UL}}\right\|^2+\sigma^2} \\ &= \frac{\beta_{\mathrm{be}}\left\|\boldsymbol{h}_{\mathrm{be}}\right\|^2}{\dfrac{1}{\left\|\boldsymbol{h}_{\mathrm{be}}\right\|}\sum_{i=2}^{M}\beta_i\left\|\boldsymbol{h}_{\mathrm{be}}^{\mathrm{H}}\boldsymbol{H}_i\boldsymbol{v}_i^{\mathrm{UL}}\right\|^2+1/\bar{\gamma}} \end{aligned} \tag{8}$$

It should be noted in (8) that the summation in the denominator starts from $i=2$, which means that no AN is transmitted by Alice during uplink transmission.

IV. Performance Estimation

The average secrecy capacity is defined as the difference in capacity of the main channel and eavesdropper's channel and thus is given as

$$C_{\mathrm{S}}^{\mathrm{DL}} = \mathrm{E}\left[\left(\log\frac{1+\gamma_{\mathrm{b}}}{1+\gamma_{\mathrm{e}}^{\mathrm{DL}}}\right)^{+}\right] \tag{9}$$

$$C_{\mathrm{S}}^{\mathrm{UL}} = \mathrm{E}\left[\left(\log\frac{1+\gamma_{\mathrm{b}}}{1+\gamma_{\mathrm{e}}^{\mathrm{UL}}}\right)^{+}\right] \tag{10}$$

For both downlink and uplink transmission, respectively, where $(x)^{+} = \max(x, 0)$ .Note that the expectation in (9) and (10)is over all random variables (including path loss β_{xy}, channel vector $\boldsymbol{h}_{\mathrm{xy}}$ or $\boldsymbol{H}_{\mathrm{xy}}$).

Assuming capacity achieving channel codes are used for both uplink and downlink transmission and the code rate ρ is set to channel capacity of the main channel, i.e. $\rho = \log(1+\gamma_{\mathrm{b}})$. According to Shannon's coding theorem, this codeword is decodable by Eve if and only if the channel capacity seen by Eve is larger than or equal to ρ. In other words, Eve can decode the codewords sent by Alice or Bob when $\log(1+\gamma_{\mathrm{e}}) \geq \rho = \log(1+\gamma_{\mathrm{b}})$ or $\gamma_{\mathrm{e}} > \gamma_{\mathrm{b}}$ .In this work, we define "secrecy outage" as the event that Eve can decode the codewords in main channel. Thus the outage probability is given by

$$P_{\mathrm{out}}^{\mathrm{DL}} = \Pr\left\{\gamma_{\mathrm{b}} \leq \gamma_{\mathrm{e}}^{\mathrm{DL}}\right\} \tag{11}$$

$$P_{\mathrm{out}}^{\mathrm{UL}} = \Pr\left\{\gamma_{\mathrm{b}} \leq \gamma_{\mathrm{e}}^{\mathrm{UL}}\right\} \tag{12}$$

V. Numerical Simulation

The random variables γ_{b}, $\gamma_{\mathrm{e}}^{\mathrm{DL}}$ and $\gamma_{\mathrm{e}}^{\mathrm{UL}}$ as defined in (4), (6) and (8) are functions of many other random variables including the path loss (β_{XY}) which depends on the random locations of Eve and Bob, the fast fading (elements of $\boldsymbol{h}_{\mathrm{xy}}$ or $\boldsymbol{H}_{\mathrm{xy}}$). It is almost impossible to find a closed form expression for secrecy capacity defined in (9) and (10). Also it will be mathematically intractable to obtain the outage probability as defined in (11) and (12). So we use simulation to obtain the results.

In this section, we consider a square plane with dimension 4km by 4km as shown in Fig. 2, where we have $M = 5$ guard nodes, including Alice as the guard node with index $i = 1$. Alice, the base station or AP, is located at the center of the plane $(0,0)$. The rest four guard nodes are located at $(1,1i)$, $(1,-1i)$, $(-1,1i)$ and $(-1,-1i)$. All the simulation results are based on Fig. 2. In case, if $M = 3$, then the guard nodes at $(-1,1i)$ and $(1,-1i)$ are turned off, i.e. they did not contribute any AN to the network. More so, if $M = 1$, all the 4 guard nodes surrounding Alice are turned off. Eve and Bob are randomly located within the two-dimensional plane.

For the path loss model (1), we assume that the path-loss exponent is $\lambda = 3.5$, $d_0 = 1\mathrm{km}$, $K = 1$. For the fast fading, we assume that all the channel undergo Rayleigh fading, i.e. the elements of $\boldsymbol{h}_{\mathrm{xy}}$ and $\boldsymbol{H}_{\mathrm{xy}}$ are i.i.d. complex Gaussian variables with zero mean and unit variance.

Furthermore, in the simulation setup, each guard nodes (include Alice) and the Eve are equipped with $N = 4$ antennas while Bob has only one antenna. The Fig. 3 is the average secrecy capacity in bits per symbol for both the downlink and uplink communication.

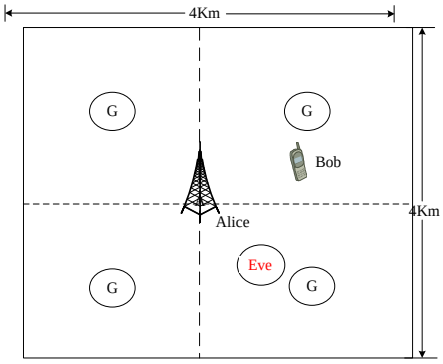


Fig. 2. The geometrical representation of the simulation

The Fig. 3, shows that when $M > 1$, the performance of downlink is slightly higher than uplink performance which is as a result of one additional noise signal that is transmitted from Alice. In case $M = 1$, the uplink secrecy capacity is much smaller than that of downlink since Alice works in half-duplex mode and thus no AN is present during the uplink transmission. Moreover, it can be observed in the figure that the secrecy capacity performance when $M = 3$ during the downlink is somewhat similar to $M = 5$ for uplink transmission, this is so because the guard nodes located at (1,1i) and (1,-1i) have significant influence on the secrecy performance of the design since they have close proximity to both the Bob and Eve, respectively.

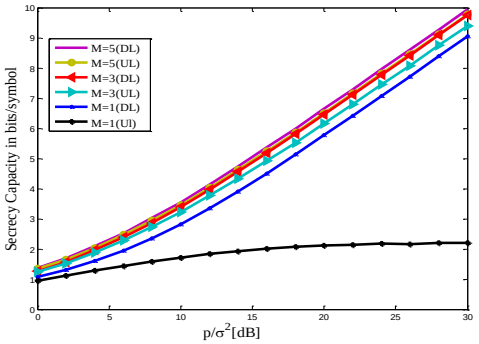


Fig. 3. The secrecy capacity in bits per symbol

Fig. 4, is the outage probability curve which shows that as the transmit power increases, the outage probability decreases accordingly. This is expected as from (4) and

(6) we can observe that, when $\bar{\gamma} \to \infty$, γ_b increases linearly with $\bar{\gamma}$ while γ_e^{DL} is approximately upper bounded by β_{ae}/β_{xe} where x denotes the guard node closest to Eve. If Alice is the closest guard node to Eve, then $\beta_{ae}/\beta_{xe}=1$, otherwise $\beta_{ae}/\beta_{xe}<1$ since $d_{ae}>d_{xe}$. This implies that γ_e^{DL} is approximately upper bounded by 1 or 0dB. This can explain the fast dropping of outage rate curves of downlink. For the uplink, γ_e^{UL} is approximately upper bounded by β_{be}/β_{xe} where x denotes the guard node closest to Eve. Due to the randomness of the location of Eve, the distance between Eve and guard node can be much smaller than the distance between Eve and Bob, i.e. it is possible that $d_{be} << d_{xe}$, $\beta_{be}/\beta_{xe} >> 1$, hence γ_e^{UL} can be arbitrarily large depending on the relative location of Eve, guard node and Bob. Therefore, the outage performance for uplink is obviously poor than downlink. In particular, in case $M=1$, the secrecy outage probability is approximately equals to the probability of Bob being closer to Eve than to Alice.

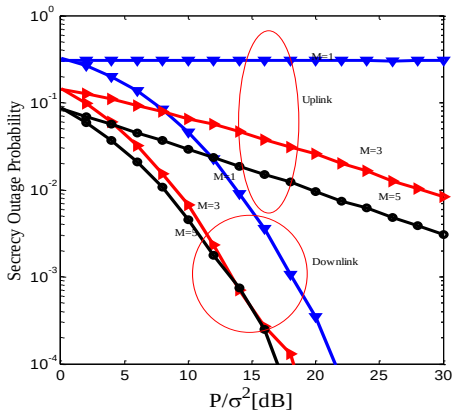
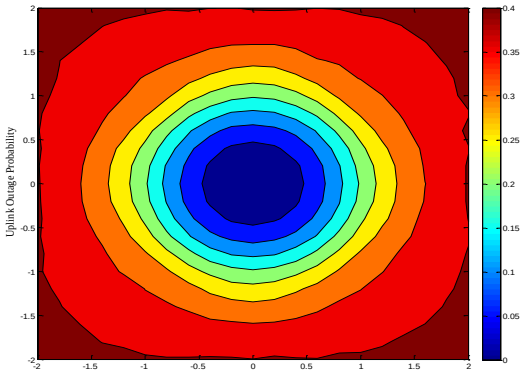
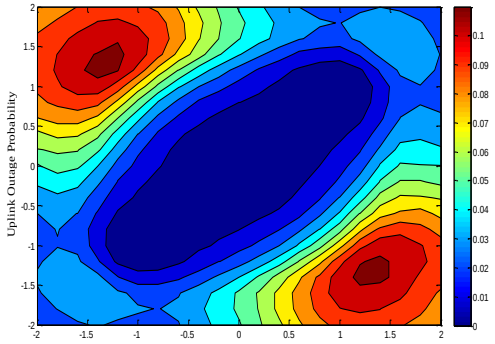


Fig. 4. The secrecy outage probability

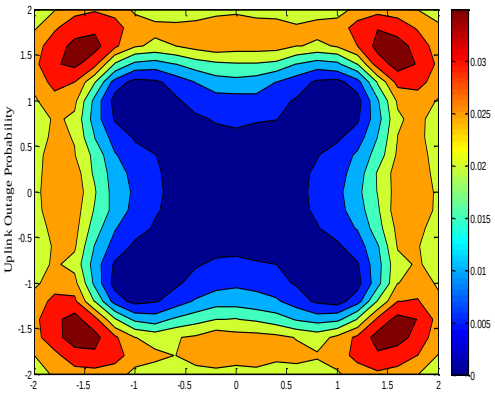
For the fixed deployment of guard nodes, the secrecy performance depends on the relative geometrical locations of Bob, Eve and guard nodes. From the perspective of Bob, some area may be safer than others. Fig. 5 (a) - (c) are the contour plot of the uplink secrecy outage probability in view of Bob.



(a) M=1



(b) M = 3



(c) M = 5

Fig. 5. The uplink secrecy outage probability contour for M = 1, 3, 5, $\bar{\gamma}$ = 15dB.

These figures are obtained by fixing Bob in each pixels of the 4kmx4km square plane, and drop Eve randomly within the square. The blue portion denotes the secure region while the red area indicates high secrecy risk if Bob stays there. It is obvious that deployment of more guard nodes can significantly reduce the risk area. It can be seen in Fig. 5(a) that when M=1 which denotes the AN is from Alice only, the probability for Eve to eaves drop the message is very high, only the area close to Alice is relatively safe. More so, when M=3, the secrecy performance improves. Generally, as the number of guard nodes increases, the secrecy level of the system increases which confirms the effectiveness of our proposal, hence the information secrecy is enhanced. For a practical network, where some places are of important high security concern, the deployment of more guard nodes in such an area will be of great value so as to ensure information secrecy.

VI. Conclusion

In this work, we propose to deploy simple guard nodes to enhance the secrecy performance of a wireless network. These guard nodes are *simple* in sense that they require no CSI about the passive eavesdropper, no cooperation for joint beamforming or jamming, and no complicated algorithms are required for optimizing system performance. The guard nodes work as a simple interferer transmitting AN all the time in the null space of the legitimate receiver. Although the proposed scheme is very simple in implementation, this scheme shows that

the deployment of guard node can improve the secrecy performance of wireless system by order of approximate of 9%.

REFERENCES

[1] D. T. Rajanbabu and C. Raj, "Implementing a reliable cryptography based security tool for communication networks," in *Proc. Inter. Conf. ScienceEngr. and Manag. Research*, Nov. 2014, pp. 1-4.

[2] B. Mandal, S. Chandra, S. S. Alam, and S. S. Patra, "A comparative and analytical study on symmetric key cryptography," in *Proc. Intern. Conf. Electr., Commun. and Comput. Engr.*, Honsur, Nov. 2014, pp. 131-136.

[3] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Proceed. (INFOCOM)*, Shanghai, China, April, 2011.

[4] A. D. Wyner, "The wire-tap channel," *The Bell Syst. Techn. Journal*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[5] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theo*., vol. 24, no. 3 pp. 339-348, May 1978.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Symposium. Inform. Theo*., Jul. 2006, pp. 356-360.

[7] H. Jing and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process*., vol. 59, no. 10, pp. 4871-4884, Oct. 2011.

[8] W. Hui-Ming, L. Feng, and Y. Mengchen, "Joint cooperative beamforming, jamming, and power allocation to secure AF relay systems," *IEEE Trans. Veh. Tech.* vol. 64, no. 10, pp. 4893-4898, Oct. 2015.

[9] M. Jianhua, T. Meixia, and L. Yuan, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett*., vol. 16, no. 6, pp. 878-881, June 2012.

[10] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Commun.*, vol. 8, no. 10 pp. 5003-5011, Oct. 2009.

[11] F. S. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1768, 2015.

[12] R. Ou, X. Wenjun, L. Shengyu, and L. Jiaru, "Energy-Efficient multicast resource allocation based on beamforming technique," in *Proc. IEEE Intern. Symposium. Personal Indoor and Mob. Radio Prop.*, pp. 3208-3212, Sept. 2013.

[13] M. Ghaderi, *et al*., "Efficient wireless security through jamming, coding and routing," in *Proc. IEEE Conf. Sensor, Mesh and Ad Hoc Commun. and Networks*, June 2013, pp. 505-513.

[14] L. Tie and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2547-2553, June 2009.

[15] L. A. Olawoyin, Y. Wu, H. Yang, *et al*., "Secrecy enhancing in wireless communication with a full-duplexing at the receiver," in *Proc. IEEE Global Commun. Conf., (GLOBECOM)*, San Diego, California, 2015.

[16] M. Abedi, *et al*., "Secure robust resource allocation using full-duplex receivers," in *Proc. IEEE Intern. Conf. Commun. Workshop*, 2015.

[17] W. C. Liao, T. H. Chang, W. K. Ma, and C. Y. Chi, "QoS-Based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Sig. Proc*., vol. 39, no. 3, March 2011.

[18] M. Pei, J. Wei, K. K. Wong, and X. Wang, "Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI," *IEEE Trans. Wireless Commun.*, vol. 11, no. 2, pp. 544-549, Feb. 2012.

[19] Z. Yajun and L. Tao, "Secrecy wireless information and power transfer with transmit antenna selection in MISO systems," in *Proc. IEEE Intern. Conf. Comp. and Commun.*, Oct. 2015, pp. 362-367.

[20] A. Goldsmith, *Wireless Communications*, Cambridge University Press, 2005.

Lukman A Olawoyin received the B.Eng. degree in Electrical and Electronic Engineering from Federal University of Technology, Akure (FUTA), Nigeria in 2003 and M.Sc. degree in Modern Digital Communication Systems (MDCS) from the University of Sussex, United Kingdom in2010. He is currently pursuing the Ph.D. degree with the Wireless Communication Center, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include Physical Layer security, signal processing, MIMO and information theory

Yang Hongwen was born in 1964. Prof. Yang is currently the director of the wireless communication center, school of Information and Communication Engineering at the Beijing University of Posts and Telecommunications (BUPT). His research interest is on wireless aspect of physical layer such as modulation, channel coding, security, signal processing, CDMA, MIMO, OFDM, etc. and information theory

Yue Wu is currently a Ph.D. candidate at Beijing University of Posts and Telecommunications. He obtained MSc degree in wireless communication from Chongqing University of Posts and Telecommunication in 2010. His research interest is HARQ technology and signal processing in wireless communication system