SCIENCE CHINA
Information Sciences

• LETTER •

January 2016, Vol. 59 019301:1–019301:3
doi: 10.1007/s11432-015-5463-y

Transmission frequency-band hidden technology in physical layer security

Xiangyu LI, Liang JIN*, Kaizhi HUANG & Lu LIU

National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002*, China*

Received September 14, 2015; accepted October 19, 2015; published online December 21, 2015

Citation Li X Y, Jin L, Huang K Z, et al. Transmission frequency-band hidden technology in physical layer security. Sci China Inf Sci, 2016, 59(1): 019301, doi: 10.1007/s11432-015-5463-y

Dear editor,

In recent years, privacy concerns grow rapidly since an eavesdropper can probably overhear the wireless communication. However, it becomes much more challenging for the traditional key-based encryption to distribute and manage the secret key in large-scale wireless networks.

In 1975, Wyner [1] introduced the model of physical layer security, which provides a feasible idea to improve security of wireless systems. Goel et al. [2] proposed the artificial noise (AN) strategy to confuse the eavesdropper, which initiated a new research direction for physical layer security. Based on this scheme, Khisti et al. [3, 4] analyzed the system's ergodic secrecy rate under different scenarios. However, references [2] and [5] have pointed out that, if the eavesdropper has more antennas than the transmitter, the secrecy rate will be greatly reduced. Especially in the finite alphabet input system, Liu et al. [6, 7] found that when the channel is slow fading, the eavesdropper with more antennas could intercept confidential messages by canceling the spatial scrambling. It reveals that, with the slow fading channel characteristics, the eavesdropper can estimate the channel state information (CSI) much easier and coherently detect the intercepted signals. Moreover, most existing researches just focus on hiding the transmitted information, but ignore protecting other peripheral information like frequency spectrum and so on, which facilitates the eavesdropper's interception and demodulation.

In this paper, we propose a transmission fre quency-band hidden (TFBH) method to enhance the physical layer security, combining the AN and the adaptive frequency hopping (FH) [8]. Contrast to the traditional AN method, this approach can hide the true signal-bands and increase the difficulty of eavesdroppers' demodulation. Moreover, as channel characteristics of the legitimate receiver become time-varying, the eavesdropper cannot extract useful information even with more antennas.

Model and methodology. We consider a system of three nodes as illustrated in Figure 1(a). The source node Alice, with N_A ($N_A \geqslant 2$) antennas, expects to send some confidential information to the destination node, Bob, in the presence of a passive eavesdropper Eve with N_E antennas. The system uses J frequency bands for transmission and each two adjacent ones have half overlap. In each symbol interval, Alice randomly selects k bands, i.e., signal-bands, to send signals, and the remaining bands, i.e., interference-bands, to send signal-like interferences. The k signal-bands, $1 \leqslant k \leqslant J/2$, should be non-overlapped in order to avoid mutual interferences.

The channel vector of the jth frequency band f_j ($j = 1, \ldots, J$) between Alice and Bob can be described as $\boldsymbol{h}_{f_j}$. The channel matrix between Alice

* Corresponding author (email: liangjin@263.net)

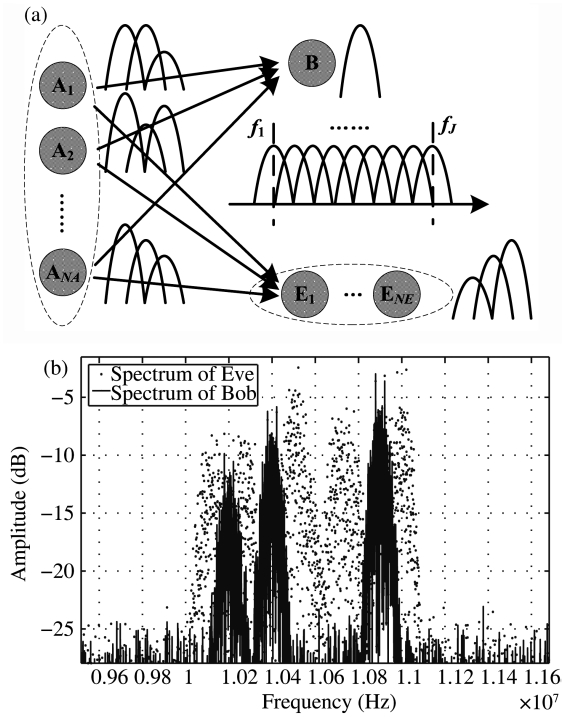

Figure 1 (a) The system model; (b) the received signal spectrums of Bob and Eve.

and Eve of f_j can be denoted as $\boldsymbol{G}_{f_j}$. We assume that all their elements are complex Gaussian random variables with zero means and unit variances. All channels are assumed to be flat fading and block-invariant.

Bob sends training sequences periodically for channel estimation before the information transmission. Training symbols in non-overlapped bands can be sent simultaneously. Hence, we can use two orthogonal training sequences to estimate the channel of all bands at the same time. Since Eve is a passive eavesdropper, we assume that Alice only know the instantaneous CSI $\boldsymbol{h}_{f_j}$ and the distribution of $\boldsymbol{G}_{f_j}$, while Eve knows both $\boldsymbol{h}_{f_j}$ and $\boldsymbol{G}_{f_j}$ perfectly.

For simplicity, the time index will be omitted. We assume that Alice sends signal s_j in the jth frequency band constrained with $\boldsymbol{E}\{|s_j|^2\} = 1$. The total transmission power is constrained to P_A and assumed to be averagely distributed in J bands. The weight projection vector for each antenna of Alice in sub-band f_j is $\boldsymbol{\omega}_{f_j}$. Here, each element ω_{n,f_j} is the projection weight of the nth antenna of Alice using the jth carrier frequency. Each projection vector will be normalized to unity.

We know that each sub-band will be interfered by two adjacent ones. Then, the signal received by Bob and Eve in frequency band f_j can be expressed, respectively, as

$$y_{B,j} = \sqrt{\frac{P_A}{J}}\boldsymbol{h}_{f_j}\boldsymbol{\omega}_{f_j}^{\mathrm{H}} s_j + \frac{1}{2}\sqrt{\frac{P_A}{J}}(\boldsymbol{h}_{f_{j-1}}\boldsymbol{\omega}_{f_{j-1}}^{\mathrm{H}} s_{j-1} + \boldsymbol{h}_{f_{j+1}}\boldsymbol{\omega}_{f_{j+1}}^{\mathrm{H}} s_{j+1}) + n_{B,j}, \quad (1)$$

$$\boldsymbol{y}_{E,j} = \sqrt{\frac{P_A}{J}}\boldsymbol{G}_{f_j}\boldsymbol{\omega}_{f_j}^{\mathrm{H}} s_j + \frac{1}{2}\sqrt{\frac{P_A}{J}}(\boldsymbol{G}_{f_{j-1}}\boldsymbol{\omega}_{f_{j-1}}^{\mathrm{H}} s_{j-1} + \boldsymbol{G}_{f_{j+1}}\boldsymbol{\omega}_{f_{j+1}}^{\mathrm{H}} s_{j+1}) + \boldsymbol{n}_{E,j}, \quad (2)$$

where $n_{B,j}$ and the elements of $\boldsymbol{n}_{E,j}$ are independent identically distributed (i.i.d) additive white Gaussian complex noise (AWGN), with zero-mean and variance σ_n^2. Here, we also assume $s_j = 0$ ($j < 1$ or $j > J$).

During each symbol interval, Alice can select k non-overlapped sub-bands randomly as the signal-bands and the remaining bands as interference-bands. We use a function to mark the selected frequency band

$$f_{\mathrm{sig}}(j) = 1,\ f_j \in \text{signalbands},\ \sum_{j=1}^{J} f_{\mathrm{sig}}(j) = k. \quad (3)$$
$$f_{\mathrm{sig}}(j) = 0,\ f_j \notin \text{signalbands},$$

The projection vectors $\boldsymbol{\omega}_{f_j}$ can be designed to make all the interference signals lay in the null space of Bob's channel, while the useful information transmitted by beam-forming. Then, $\boldsymbol{\omega}_{f_j}$ can be denoted as

$$\begin{aligned} &\boldsymbol{h}_{f_j}\boldsymbol{\omega}_{f_j}^{\mathrm{H}} = 0,\ \text{when } f_{\mathrm{sig}}(j) = 0, \\ &\boldsymbol{\omega}_{f_j} = \boldsymbol{h}_{f_j} / \left\|\boldsymbol{h}_{f_j}\right\|,\ \text{when } f_{\mathrm{sig}}(j) = 1. \end{aligned} \quad (4)$$

Bob will demodulate the information of all the frequency bands simultaneously. As signals received from interference-bands are just white noises, Bob can distinguish the signal-bands accurately. For this case, signals received by Eve are broadband-like as they contain plenty of frequency bands. We note that the signals and the interferences are independent and identically Gaussian distributed with zero-mean and unit variance. The antenna weights are both normalized to unity and the transmit powers are also the same. As a result, it is impossible for Eve, at least from the statistical characteristics of the receiving amplitudes and phases, to separate these bands effectively or judge the signal-band during a block of transmission. Since k may vary during each transmission cycle, Eve cannot know how many and which bands are chosen by Alice, leading to greater uncertainty and higher system security level. Moreover, these bands can also be used by other users in order to improve the system's power efficiency.

Simulations and results. In this section, we give the signal spectrums of the proposed TFBH

scheme through some simulations. All channels of the system are generated to be zero-mean standardized complex Gaussian variables. The received additive noise is assumed to be zero-mean complex Gaussian distributed with variance 0 dB. Alice transmits with the power $P_A = 20$ dB. Bob divides the frequency bands to 10 sub-bands with carriers of $(1 + 0.01n) \times 10^7$ Hz, $n = 1, 2, \ldots, 10$. At the current time, the second, the fourth and the ninth frequency bands are randomly selected as the signal-bands, while others for the interference. The symbol rate is 10^5 bits/s and the sampling frequency is 4×10^7 Hz. The received signal spectrums of Bob and Eve are shown in Figure 1(b).

As illustrated in Figure 1(b), Bob can find the signal-band, and then demodulate the information correctly. Eve receives a wideband signal and cannot separate it accurately. Considering the worst case that Eve is able to separate the various transmission bands by some means, he still cannot determine which band is for the information and which for interference. The confusion of the spectrums will greatly reduce the leakage rate to Eve. Thus, the security level of the system will be improved.

Conclusion and future work. In this paper, we propose a new physical layer security scheme based on the TFBH technology. This scheme can be effectively used to improve the security of the system and has been validated by simulations under various typical backgrounds. Moreover, if Alice is equipped with massive array antennas, it is easy to make the signal to Bob lie in the null spaces of other nodes' channels. As signals to other nodes can be used as interferences, there is no need to transmit interferences intentionally and the power efficiency of the system will be improved. A comprehensive secrecy rate analysis for this scheme will be our major research direction in future.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61171108, 61379006, 61401510, 61471396, 61521-003), National High-Tech Research & Development Program of China (863) (Grant Nos. 2014AA01A707, 2015AA01A708).

Conflict of interest The authors declare that they have no conflict of interest.

Supporting information Secrecy Rate Analysis and Simulations. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Wyner A D. The wire-tap channel. Bell Syst Tech J, 1975, 54: 1355–1387
2 Goel S, Negi R. Guaranteeing secrecy using artificial noise. IEEE Trans Wirel Commun, 2008, 7: 2180–2189
3 Khisti A, Zhang D. Artificial-noise alignment for secure multicast using multiple antennas. IEEE Commun Lett, 2013, 17: 1568–1571
4 Lin P H, Lai S H, Lin S C, et al. On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels. IEEE J Sel Area Commun, 2013, 31: 1728–1740
5 Khisti A, Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel. IEEE Trans Inf Theory, 2010, 56: 3088–3104
6 Liu L, Jin L, Huang K Z. Eavesdropping against artificial noise: hyperplane clustering. In: Proceedings of IEEE International Conference on Information Science and Technology, Tangier, 2013. 1571–1575
7 Wu F L, Wang W J, Yao B L, et al. Effective eavesdropping in the artificial noise aided security scheme. In: Proceedings of IEEE/CIC International Conference on Communications in China, Wuhan, 2013. 214–218
8 Popovski P, Yomo H, Prasad R. Strategies for adaptive frequency hopping in the unlicensed bands. IEEE Wirel Commun, 2006, 13: 60–67