# Security Protection over Wireless Fading Channels by Exploiting Frequency Selectivity

Mukhtar Hussain*†, Qinghe Du*‡, Li Sun*‡ and Pinyi Ren*‡
*School of Electronic and Information Engineering, Xi'an Jiaotong University, Xian, P.R. China
†Department of Electrical Engineering, COMSATS Institute of Information Technology, Lahore, Pakistan
‡Shaanxi Smart Networks and Ubiquitous Access Research Center, Shannxi, China
E-mails: {*mukhtarhussain@ciitlahore.edu.pk,* {*duqinghe, lisun, pyren*}*@mail.xjtu.edu.cn*}

***Abstract*—Secure wireless communication has always been a hot research topic due to the vulnerabilities associated with wireless channel. Physical layer aspects to secure wireless communication, based on the information-theoretic security and signal processing methods have gained much recognition over the last decade. Specifically, artificial noise (AN) methods are assumed to be good means for providing security against potential eavesdroppers in multi-input multi-output (MIMO) systems and/or relay systems. However, there are still a large number of nodes which do not have multi-antennas or support sophisticated protocols in wireless networks. In this paper, a novel AN-aided method is proposed to secure wireless communications between the legitimate users (not equipped with multiple antennas) in the presence of an eavesdropper. In this proposed method frequency selective property of wireless channel is exploited. The basic principle is same in which transmitter generate random AN signal utilizing some of the transmission power to confuse eavesdropper. However artificial noise is generated in such a way that it appears to be zero at the sampling time, only for the legitimate receiver while degrading eavesdropper's channel. Artificial noise is specified using the channel state information (CSI) of the legitimate users' link. However, the secrecy of proposed scheme doesn't depend on the secrecy of CSI. Extensive simulation suggests that the proposed scheme can effectively utilized for securing wireless transmissions.**

***Index Terms*—physical-layer security, frequency selectivity, wireless fading channels, wireless networks.**

## I. Introduction

Physical layer security is a significant feature for wireless communication because it employs information theoretic concepts instead of relying on higher layer cryptographic means. Cryptographic methods rely heavily on the computational hardness of mathematical problem. The openness of wireless medium and increase in the computational capabilities made it more vulnerable to eavesdropping. Shannon presented the notion of perfect secrecy in [1], a perfect cipher could achieve perfect secrecy only if secret key is as long as the plain text message. Therefore based on this assumption all presently used ciphers can be theoretically broken.

Wayner [2] presented the concept of wiretap channel to achieve virtually perfect secrecy assuming main channel (legitimate receiver's channel) is discrete memoryless channel while wiretap channel (eavesdroppers channel) is degraded version of main channel. It is considered to be the founding stone of physical layer security for wireless communication. Cheong and Hellman [3] extended Wayner's work [2] for Gaussian channels and presented the secrecy capacity ($SC$) is equal to the difference between the channel capacity of legitimate and eavesdropper. Till now, extensive research in the field of physical layer security has been made to improve the security over wireless channels [4]–[22]. The efforts have been dedicated to the secure communications over Gaussian broadcast channels [5], [6] and single-input single-output (SISO) fading channels [7]–[9], as well as multi-antenna systems [19]–[22]. Applications of error correction codes were presented in [10]–[13]. Li [14] and Soltani [15] presented physical layer approach to secure OFDM based system. Whereas, noise aggregation method have been studied in [16], [17]. However, most of these schemes are based on unrealistic assumptions that either eavesdropper's channel is worse than legitimate receiver's channel or eavesdropper is unknown about the main channel. Negi and Goel [18] presented the idea of AN for MIMO system to secure communication by generating a disturbance signal that degrade the eavesdroppers channel however it has little to none effect on intended receiver s channel.

AN-aided methods [19], [20] have gained a lot of attention for MIMO/MISO system as there is no unrealistic assumption has been made. The information bearing symbols and artificial noise can be transmitted simultaneously, if the transmitter is equipped with multiple antennas. However in practice all mobile nodes are not equipped with powerful hardware and multiple antennas. Motivated by the AN-aided methods, Yang and Jiao [21] proposed a method to generate AN for the transmitter equipped with single antenna based on the CSI of main channel in such a way that it reduce the inter symbol interference (ISI) at legitimate receiver's end, while it appeared to be random noise at eavesdropper's end. However this scheme does not remain effective if eavesdropper knows the CSI of main channel.

To circumvent the aforementioned limitations, we present the AN-aided method to secure wireless communication over multipath fading channel. A signal processing perspective has been considered to ensure secure communication in such a way to weaken the eavesdroppers intercepted signal, however a certain level of signal-to-noise-ratio (SNR) at the intended

The research work reported in this paper is supported by the National Natural Science Foundation of China under the Grant No. 61431011 and Grant No. 61671369, Science and Technology Program of Shaanxi Province under the Grant No. 2016KW-032, and the Fundamental Research Funds for the Central Universities.

978-1-5090-2860-3/16/$31.00 ©2016 IEEE

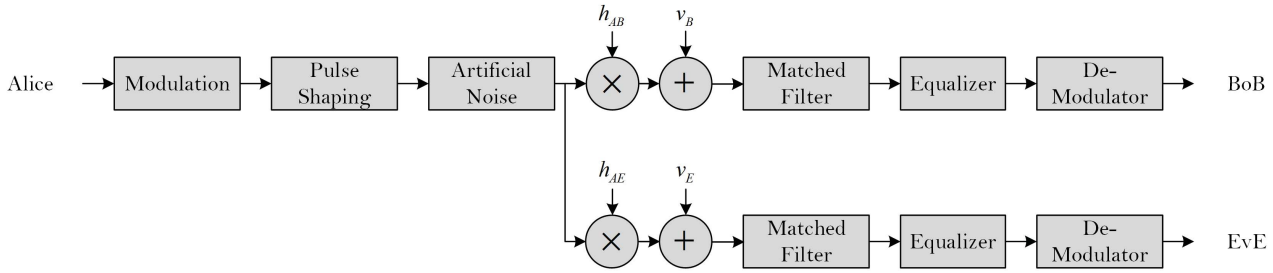


Fig. 1. System model for secure wireless transmission using artificial noise

receiver is guaranteed. The key idea is to generate AN that appeared to be zero at the decision making instance (at the output of matched filter) of intended receiver while degrading the decision making probability at eavesdropper's end. The secrecy of the proposed scheme is independent of the secrecy of CSI.

The rest of the paper is outlined as in Section II, we provide the system model. In Section III, the procedure to generate artificial noise signal is presented in order to protect the wireless transmissions against the potential eavesdropper. In Section IV, system model have been analyzed in terms of secrecy capacity. Section V presents the simulation results and discussion. Finally the paper concludes with Section VI.

## II. System Model

A commonly used three node wireless system that consists of a transmitter (called Alice), a legitimate receiver (called Bob) and an eavesdropper (called Eve) all are equipped with single antenna is presented in Fig. 1. Alice transmits message intended for Bob over the wireless channel, however Eve can also intercept the signal. The channel gains of Alice-Bob and Alice-Eve link are given by $h_{AB}$ and $h_{AE}$. The secrecy is achieved by adding artificial noise in the information signal, at the transmitter side such that it degrade Eve's channel, while it does not effect the Bob's channel.

*1) Multipath Channel:* The wireless channel is assumed to be multipath Rayleigh block fading. In practice it is achieved by designing the frame length, taking into account coherence time of the channel. Coherence time of the channel is the time duration over which the channel state is considered to be not varying also called block fading channel. In mobile radio channels, the Rayleigh distribution is commonly used to describe the time varying nature or individual multipath components [23]. Under the block Rayleigh-fading, the channel entries are zero-mean unit-variance complex Gaussian random variables, drawn at the beginning of each fading block which remain constant for the *N* symbols within that frame. In addition, this process is repeated for every frame in an independent and identically distributed (i.i.d) manner. Therefore the *L*-path channel for the transmission of a single frame could be expressed, $1 \times L$ vector as $\mathbf{h} = [h_1, h_2, \ldots, h_L]$.

*2) Pulse Shaping:* The power spectral density (PSD) of digital signal can be controlled by the choice of pulse shape. The PSD is strongly and directly influenced by the pulse shape. Spreading of pulse beyond its allotted time interval $T_b$ cause interference with neighboring pulses known as ISI [24]. The ideal rectangular pulse shape has infinite bandwidth and the performance is severely effected in multipath channel. Nyquist presented the criterion for design zero-ISI pulse shape. The raised cosine pulse shaping is utilized in the proposed scheme. The impulse response of the digital raised cosine pulse shaping filter is given by:

$$p[n] = \frac{\sin \pi \{(n/k) - m\}}{\pi \{(n/k) - m\}} \frac{\cos (\pi \beta \{(n/k) - m\})}{1 - 4\beta^2 \{(n/k) - m\}^2}$$

*3) Matched Filtering:* The optimal linear filter is utilized at the receivers side to maximize the signal to noise ratio (SNR) in the presence of additive noise called matched filter. The optimum matched filter $q[n]$ at the receiver to match pulse shape $p[n]$ is $q[n] = p[-n]$, because 1) It retains all the spectral components of received signal and, 2) It maximize the SNR at the decision making instance [25]. It is assumed that Eve knows about the communication system completely and employed same matched filter as Bob does.

## III. Artificial Noise Strategy

For the proposed method, frame based communication is assumed between the wireless nodes. Each frame is composed of *M* information-bearing symbols $\bar{\mathbf{s}} = [\bar{s}_1, \bar{s}_2, ..., \bar{s}_M]^T$. To guarantee the secrecy of transmitted messages Alice injects artificial noise $\mathbf{w} = [w_1, w_2, ..., w_N]^T$ into $N$ upsampled (at the rate of $R_s$ i.e. $N = MR_s$) information bearing symbols $\mathbf{s} = [s_1, s_2, ..., s_N]^T$ at the output pulse shaping filter before transmission. Such that

$$\begin{aligned} x_n &= s_n + w_n \qquad n = 1, 2, \cdots, N \\ \mathbf{x} &= \mathbf{s} + \mathbf{w} \end{aligned} \tag{1}$$

For the transmission of the frame given in (1) over *L*-path fading channel, received symbols could be expressed as linear convolution of transmitted symbols and channel coefficients given by expression (2) and (3),

$$\mathbf{y} = \mathbf{h} * \mathbf{x} + \mathbf{v} \tag{2}$$

$$y[i] = \sum_{l=0}^{L} h[l]\, x[i-l] + v[i] \tag{3}$$

where $y[i]$ represents the received $i^{th}$ symbol, and $v[i]$ is the additive white Gaussian noise (AWGN), $i = 1, 2, ..., N$. The matched filter serves to maximize the signal to noise ratio (SNR) of the sampled signal at the output. A discrete time *K*-tap matched filter could be represented as $1 \times K$ vector, $\mathbf{q} = [q_0, q_1, ..., q_k]^T$. The output of matched filter could be

given as the linear convolution of received signal with the filter coefficients.

$$\mathbf{z} = \mathbf{q} * \mathbf{y} \tag{4}$$

$$z\left[i\right] = \sum_{k=0}^{K} q\left[k\right] y\left[i-k\right] \tag{5}$$

Whereas, the downsampled output after matched filtering for decision making could be expressed as,

$$z_s\left[i\right] = \sum_{m=-\infty}^{\infty} z\left[i\right] \delta\left[i - mR_s\right] \tag{6}$$

The vector of *N* output symbols can be represented in the form of matrices [25] as,

$$\begin{aligned} \mathbf{z}_r &= \mathbf{SQ}\left[\mathbf{H}_r \mathbf{x}_r + \mathbf{v}_r\right] \\ \mathbf{z}_r &= \Gamma_r \mathbf{x}_r + \tilde{\mathbf{v}}_r \end{aligned} \tag{7}$$

where $\mathbf{z}_r$ is the $r^{th}$ received frame containing *M* information symbols. $\mathbf{H}_r$ is the $(N+L) \times (N+L)$ channel Toeplitz matrix for the $r^{th}$ received frame, it may vary frame to frame depending upon the characteristics of wireless channel. **Q** is the (*N*+*K*) × (*N*+*K*) Toeplitz matrix also denotes the convolutive relationship of matched filter. While **S** represents the downsampling at the output after matched filter, it could be expressed in the form of diagonal matrix containing ones only in the $m^{th}$ rows, other diagonal entries be zeros. **z**, **H**, **Q** and **S** are represented in matrix form as follows.

$$\mathbf{z} = \begin{bmatrix} z\left[N\right] \\ z\left[N-1\right] \\ \vdots \\ z\left[1\right] \end{bmatrix}$$

$$\mathbf{H} = \begin{bmatrix} h[0] & h[1] & \cdots & h[L] & & & & \\ & h[0] & h[1] & \cdots & h[L] & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & h[0] & h[1] & \cdots & h[L] & \\ & & & & h[0] & h[1] & \cdots & h[L] \end{bmatrix}$$

$$\mathbf{Q} = \begin{bmatrix} q[0] & q[1] & \cdots & q[K] & & & & \\ & q[0] & q[1] & \cdots & q[K] & & & \\ & & \ddots & \ddots & \ddots & \ddots & & \\ & & & q[0] & q[1] & \cdots & q[K] & \\ & & & & q[0] & q[1] & \cdots & q[K] \end{bmatrix}$$

$$\mathbf{S} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \ddots & \cdots & 0 & \ddots & 0 \\ 0 & \ddots & \ddots & \cdots & \ddots & \ddots & 0 \\ \vdots & \ddots & 0 & 1 & 0 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 & \ddots & 0 \\ 0 & \ddots & \ddots & 0 & \ddots & \ddots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$$

$\Gamma_r$ is $(N+K) \times (N+K)$ matrix with $M$ number of nonzero rows. It is not a full rank matrix as the number of nonzero rows are less than the number of columns. Hence there exist a exist a null space. Generation of artificial noise $\mathbf{w}$ is chosen to lie in the null space of $\Gamma_r$ such that $\Gamma_r \mathbf{w}_r = \mathbf{0}$. Let $\mathbf{Z}_r$ is the orthonormal basis for the null space of $\Gamma_r$, then $\mathbf{w} = \mathbf{Z}_r \mathbf{u}_r$. $\mathbf{u}_r$ is chosen to be independent and identically distributed (i.i.d) complex Gaussian random vector with zero mean and variance $\sigma_u^2$. $\Gamma_r$ varies w.r.t $\mathbf{H}_r$, as **Q** and **S** are assumed to be same throughout the transmission. It is assumed that the legitimate receiver is able to estimate its channel perfectly and feed it back to the transmitter noiselessly, while transmitter already knows about the impulse response matched filter and sampling interval. The received signal at Bob and Eve could be expressed as,

$$\mathbf{z}_{r,Bob} = \Gamma_{r,B} \mathbf{s}_r + \tilde{\mathbf{v}}_{r,E} \tag{8}$$

$$\mathbf{z}_{r,Eve} = \Gamma_{r,E} \mathbf{s}_r + \Gamma_{r,E} \mathbf{w}_r + \tilde{\mathbf{v}}_{r,E} \tag{9}$$

where $\mathbf{v}_{r,b}$ and $\mathbf{v}_{r,e}$ are bandlimited gaussian noise components at the output of matched filter, while '$r$' represents the frame number. It could be expressed generally as,

$$\mathbf{z}_{Bob} = \Gamma_B \mathbf{s} + \tilde{\mathbf{v}}_B \tag{10}$$

$$\mathbf{z}_{Eve} = \Gamma_E \mathbf{s} + \Gamma_E \mathbf{w} + \tilde{\mathbf{v}}_E \tag{11}$$

## IV. Analysis of Artificial Noise Approach

The signal received at Bob and Eve's end is given by expression (10) and (11) respectively. It could be observed that $\Gamma_E \mathbf{w}$ is the additional noise component at the Eve's end due to the proposed scheme that degrades the probability of decoding information at Eve's end. Let's find out the secrecy capacity proposed scheme, i.e. the rate at which Alice and Bob can communicate secretly in the presence of Eve. Keeping in mind the limited power is available at the transmitter side given by:

$$\frac{1}{N} \sum_{i=1}^{N} E\left[\left|X(i)\right|^2\right] \leq P,$$

$$\frac{1}{N} \sum_{i=1}^{N} E\left[\left|S(i)\right|^2\right] \leq P_s,$$

$$\frac{1}{N} \sum_{i=1}^{N} E\left[\left|W(i)\right|^2\right] \leq \sigma_u^2,$$

where $P$ represents the average transmitted power for each frame, sum of power allocated for the information signal and artificial noise i.e. $P = P_s + \sigma_u^2$.

Representing the power of noise of Alice-Bob and Alice-Eve channel as $\sigma_B^2$ and $\sigma_E^2$ respectively. The SNR of the received signal at Bob and Eve's end could be given by expression (12) and (13), respectively, as:

$$\gamma_B = \frac{\mathbf{E}\left|\Gamma_B \mathbf{s}\right|^2}{\sigma_B^2} = \frac{\mathbf{E}\left|\Gamma_B\right|^2 P_s}{\sigma_B^2}. \tag{12}$$

$$\gamma_E = \frac{\mathbf{E}\left|\Gamma_E \mathbf{s}\right|^2}{\mathbf{E}\left|\Gamma_E \mathbf{w}\right|^2 + \sigma_E^2} = \frac{\mathbf{E}\left|\Gamma_E\right|^2 P_s}{\mathbf{E}\left|\Gamma_E\right|^2 \sigma_u^2 + \sigma_E^2}. \tag{13}$$

Performance of the proposed scheme can be evaluated in terms of secrecy capacity i.e. the rate at which Alice and Bob can communicate secretly without being eavesdropped. The $SC$ of the proposed system model can be evaluated by using the Barros and Rodrigues [7] formulation for secrecy capacity of wireless channels i.e. difference of the channel capacity of Alice-Bob and Alice-Eve link is given by,

$$SC = C_{AB} - C_{AE} \tag{14}$$

whereas the channel capacity of Alice-Bob and Alice-Eve link is given by,

$$C_{AB} = \log(1 + \gamma_B)$$

and

$$C_{AE} = \log(1 + \gamma_E)$$

The secrecy capacity of the proposed system model can be expressed as,

$$SC = \log(1 + \gamma_B) - \log(1 + \gamma_E) \tag{15}$$

or

$$\begin{aligned} SC = &\log\left(1 + \frac{\mathbf{E}|\Gamma_B|^2 P_s}{\sigma_B^2}\right) \\ &- \log\left(1 + \frac{\mathbf{E}|\Gamma_E|^2 P_s}{\mathbf{E}|\Gamma_E|^2 \sigma_u^2 + \sigma_E^2}\right) \end{aligned} \tag{16}$$

while the $SC$ of wireless fading channel when only information symbols have been transmitted without using artificial noise, has been presented by Barros and Rodrigues in [7] as,

$$SC = \log\left(1 + \frac{\mathbf{E}|\Gamma_B|^2 P_s}{\sigma_B^2}\right) - \log\left(1 + \frac{\mathbf{E}|\Gamma_E|^2 P_s}{\sigma_E^2}\right) \tag{17}$$

The secrecy capacity is a nonnegative term, a positive secrecy capacity can be realized until $\gamma_B > \gamma_E$ and zero if $\gamma_B \leq \gamma_E$. Therefore using expression (14) could be expressed as,

$$SC = \begin{cases} \log(1 + \gamma_B) - \log(1 + \gamma_E) & if \gamma_B > \gamma_E \\ 0 & if \gamma_B \leq \gamma_E \end{cases}$$

It could be noted by comparing expression (16) and (17) that the positive secrecy capacity can be guaranteed, even if $\sigma_E^2 \to 0$, as compared to the scenario where artificial noise is not being utilized (i.e., only the information symbols are transmitted).

## V. Simulation and Results

The performance of the scheme is evaluated against the bit-error-rate (BER) of Eve for different scenarios i.e. 1) target performance level at Bob while varying the AN power, 2) varying no. of multipath and 3) varying no. of samples per symbol. The simulation results have been obtained using Monte Carlo method, over $10^5$ iterations. Quadrature Amplitude Modulation (QAM) scheme is employed for communication system. The channel for both Bob and Eve is assumed to be i.i.d multipath rayleigh fading with $L$ = 3 paths, with additive white Gaussian noise. The multipath coefficients are taken to be independent complex Gaussian random variables. It is assumed that Bob have complete knowledge of his channel gains and he feedback completely to Alice over error free channel, while Eve have complete knowledge of his and Bob's channel gains. The maximum likelihood (ML) equalization technique has been adopted to compensate channel distortion at receiver side.

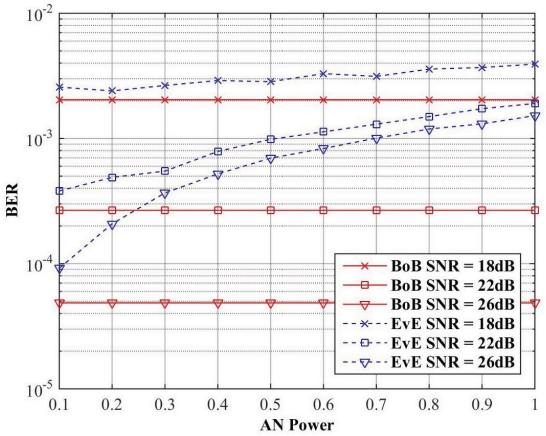


Fig. 2. BER performance comparisons: variation with artificial noise power

Fig. 2 shows the BER gain of Bob and Eve against the power of artificial noise. AN power varied from $0.1 \times E_s$ to $E_s$ considering in mind the power constraints at transmitter side in the real life scenarios. BER of Eve tends to increase with increase in the power of AN. However AN does not effect the Bob's channel as the BER at Bob's end remain same provided the certain level of SNR is maintained. Results have been plotted for the average channel SNR of Bob and Eve i.e. 18dB, 22dB and 26dB.

BER performance comparisons of Bob and Eve have been presented in Fig. 3 for the varying number of multipath channel taps i.e. 2, 3 and 4. It could be observed that the multipath channel scenario which is considered bane for communication systems can be exploited in a way to provide secure wireless communication. Solid lines presents the BER of Bob while dotted line presents the BER curves for Eve. Results have been plotted for the equal average SNR of Bob and Eve i.e. 26dB, while AN power varied from $0.1 \times E_s$ to $E_s$ as for the case-I.

BER performance comparisons of Bob and Eve have been presented in Fig. 4 against the number of samples per symbol for the pulse shaping filter at the transmitter side. It could be observed that the BER for Eve increases with increase in number of samples/symbol while the BER for Bob remains same. However there is a tradeoff between the system performance in terms of secrecy capacity and computational complexity, as both are directly related to the number of samples per symbols therefore an optimal number of samples should have to be selected. Results have been plotted for the equal average SNR of Bob and Eve i.e. 26dB, while AN power is varied.

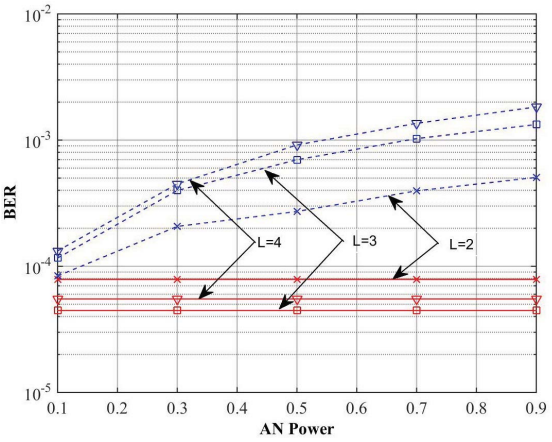


Fig. 3. BER performance comparisons: variation with no. of multipath ($L$)

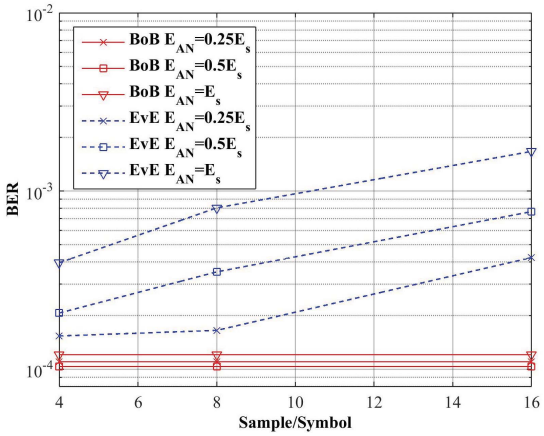


Fig. 4. BER performance comparisons: variation with samples per symbol

## VI. Conclusion

In this paper, secure communication between the legitimate users in the presence of a potential eavesdropper has been studied. It has been demonstrated how wireless transmissions can be protected by generating a disturbance signal (AN) at the transmitter side that degrades eavesdropper's channel by exploiting the frequency selective property of wireless fading channels. Unlike many Physical Layer Security schemes there is no unrealistic assumption is supposed on the eavesdropper's channel quality, computational powers or hardware limitations. The proposed scheme ensure secrecy even when mobile transmitter is not equipped with powerful hardware (i.e. multiple antennas). The secrecy of the proposed scheme is independent of secrecy of channel gains. The results suggest that this method can significantly improve the achievable secrecy rate of the wireless channel. The proposed strategy is believed to be promising physical layer approach for secure communication over wireless fading channels. The proposed scheme can be formulated as an optimization problem to achieve optimum results for allocated artificial noise power. It could also be combined with the existing higher layer cryptography protocols to achieve better secrecy.

## References


[1] C.E. Shanon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, pp. 656-715, 1949.

[2] A.D. Wayner, "The wire-tap channel," *Bell Syst. Tech. J.*, pp. 1355-1387, 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wiretap channel", *IEEE Trans. on Inform. Theory*, vol. 24, no. 4, pp. 451-456, 1978.

[4] L. Zhou, D. Wu, B. Zheng, and M. Guizani, "Joint Physical-Application Layer Security for Wireless Multimedia Delivery," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 66-72, 2014.

[5] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 339-348, 1978.

[6] A. Khisti, A. Tchamkerten and G. W. Wornell, "Secure broadcasting over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2453-2469, 2008.

[7] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," *IEEE Int'l. Symp. Inform. Theory*, Seattle, WA, pp. 356-360, 2006

[8] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2470-2492, June 2008.

[9] P. K. Gopala, L. Lai and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4687-4698, 2008.

[10] M. Bloch, J. Barros and M.R. Rodrigues, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, pp. 2515-2534, 2008.

[11] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros and B.-J. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. Inform. Forens. Security*, vol. 6, pp. 532-540, 2011.

[12] W. K. Harrison and P. Boyce, "Parity modifications and stopping sets in high-rate codes for physical-layer security", *IEEE Conference on Communications and Network Security*, San Francisco, pp. 115-120, 2014.

[13] H. Niu, M. Iwai, K. Sezaki, L. Sun and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," *IEEE Commun. Letters*, vol. 18, no. 5, pp. 777-780, 2014.

[14] H. Li, X. Wang and J. Y. Chouinard, "Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving," *IEEE Trans. on Wireless Commun.*, vol. 14, no. 2, pp. 1155-1165, 2015.

[15] M. Soltani, T. Baykas and H. Arslan, "Achieving secure communication through pilot manipulation," *IEEE PIMRC*, Hong Kong, 2015.

[16] M. Hussain, Q. Du, L. Sun and P. Ren, "Security enhancement for video transmission via noise aggregation in immersive systems," *Multimedia Tools and Applications*, pp. 1-13, 2015.

[17] Q. Xu, P. Ren, Q. Du, L. Sun and Y. Wang, "On achievable secrecy rate by noise aggregation over wireless fading channels", *IEEE Int'l Conference on Communications (ICC)*, Kuala Lumpur, 2016.

[18] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise", *IEEE Trans. Wireless Commun.*, pp. 2515-2534, 2008.

[19] Y. Yang, W. Wang, H. Zhao and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *IEEE Journal of Commun. and Networks*, vol. 14, pp. 374-384, 2012

[20] Y. Zhou, F. Li, P. Guo and Z. Xue, "Robust MIMO beamforming and power allocation for artificial noise generated by both transmitter and receiver", *IEEE CHINACOM*, Maoming, pp. 612-616, 2014

[21] Y. Yang and B. Jiao, "Artificial noise strategy for single antenna system over multi-path fading channels", *IEEE IWCMC*, Croatia, 2015.

[22] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint Information- and Jamming-Beamforming for Physical Layer Security with Full Duplex Base Station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391-6401, Dec. 2014.

[23] T. S. Rappaport, *Wireless communications: principles and practice*. 2nd ed. New Jersey: Prentice Hall PTR; 1996.

[24] W. H. Tranter, K. Sam Shanmugan, T. S. Rappaport, K. L. Kosbar, *Principles of Communication Systems Simulation with Wireless Applications*. New Jersey: Prentice Hall; 2004.

[25] B.P. Lathi and Z. Ding, *Modern digital and analog communication systems*, 4th ed. New York: Oxford Uni. Press, 2009.