Physical Layer Secure Data Transmission for Mobile Edge Computing: Beamforming and Artificial Noise

Aidong Xu¹,a, Jie Tang²,b, Yonggang Zeng¹, Li Cheng Li¹, Yixin Jiang¹,c, Yunan Zhang¹,d and Hong Wen¹,e

¹ Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
² School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China

Email: ¹ xuad@csg.cn; ²cs.tan@uestc.edu.cn; ³jiangyx@csg.cn; ⁴zhangyn@csg.cn; ⁵sunlike@uestc.edu.cn;

Abstract. As increasing threat to wireless data communication for mobile edge computing and high cost of conventional encryption implement in wireless environments, the physical layer security has aroused widespread concern to increase the security of data transmission in mobile edge computing. However, too much idealistic and unrealistic assuming in this area’s research result in security can hardly guarantee in the reality. This paper proposed a secure communications for mobile edging computing, which is using the sequenece combining with physical layer beamforming and artificial noise. By contrast to conventional schemes, the proposed scheme could enhance the security with probability 1 in two adverse situation. An advantage of the proposed scheme is that the upper layer can help the physical layer to defend each other, while up-layer system break by opponent, natural randomness of physical channel will play role to ensure system safety. We conduct simulations to verity the effectiveness of the proposed scheme for mobile edging computing.

1. Introduction

Data secure transmission in mobile edge computing [1, 2] has become increasingly pervasive and essential. Because of the nature of broadcasting, wireless networks lack of physical wireless boundary of wireless transmissions, which is easy to be overheard by the passive eavesdroppers. Therefore the wireless data secure transmission of mobile edge computing has become a very critical concern for the massive services of the future 6G network. Cryptographic techniques [3] are employed in the wireless networks. In the same time, they are also used to provide security in mobile edge computing. However, Cryptographic techniques do not consider to use the unique property of the wireless domain to address security threats.

Physical layer security is a new technique for mobile edging computing. In the physical layer secure communication, the system exploit physical characteristics of wireless channel together with the signal processing methods to achieve the unconditional security and reliable communication [1]. Work [2] proposed the so called wiretap channel. The wiretap channel is a physical layer secure model for the physical layer security. The security coding was proved existed under degraded channel to achieve unconditionally secrecy. Numerous research have discussed the achievable secrecy rate and the lower or upper secrecy capacity bounds in various communication scenario [4-6]. However, these
study all have unrealistic assumptions such as the transmitter known both main and eavesdropping channel state information (CSI) or at least statistics information. Furthermore, none of them proposed a practical secure transmission method. Goel [4] use artificial noise (call AN method in this paper where the transmitter utilized it to degrade the eavesdropper’s channel without jamming the legitimate user. Works [5] (call AR method in the rest of this following paper) proposed a physical layer secure transmission skill by using random antenna redundancy. However, the security conditions are assuming too idealistic and unrealistic which lead it hardly to put into application.

However, large numbers of physical layer security techniques are unable to guarantee the absolute security [6] in real communication. If eavesdropper can utilize more antennas than the transmitter, she or he can separate the useful signal from interference [7,8]. As it analysis [7], if the ratio of if the antenna number ratio between eavesdropper and transmitter is greater than 2, the secrecy capacity is zero. In fact the attacker may locate very close to a legitimate receiver in wireless network, or he may adopt unexpected attack to make channel correlated or similar to the legitimate channel in a certain degree. The current physical layer methods did not analyze secure performance in this situation.

What mentioned above seems to be the deficiency of secure system based on physical channel characteristics, hence the physical layer security cannot guarantee security with probability one for each bit of the transmission. Therefore, we should use the cross-layer security designs with both physical-layer security techniques for the mobile edging wireless networks. H.Wen [9-13] combined MIMO artificial noise with cryptographic technique in delay diversity system, however the security performance was far away from demand.

In this paper, a cross-layer approach is proposed to enhance the security of wireless mobile edging networks. Extensive theoretical proving and simulations is presented that the perfect secrecy is always achieving in the limit of adverse situations. Unlike the method in [14-18], in our this new proposed approach, the physical-layer signal processing method can be helped by the upper-layer sequences and the physical-layer security techniques can also help to increase the security robust of the mobile edging system.

2. Secure transmission for mobile edge computing

In typical MIMO wiretap channel of mobile edge computing networks. where three parts are involved, Alice is the edge nodes who needs to securely transmit messages with NT transmitting antennas to the target edge terminal user (Bob) with NR receiving antennas, while an eavesdropper (Eve) with NE receiving antennas attempts to eavesdrop the message transmitting between Alice and Bob. In the mobile edging communication scenario, it is reasonable to assume that neither Alice nor Bob knows the location and the channels of Eve. We consider the time-duplex division (TDD) where the channel reciprocity is guaranteed. The system model for mobile edge computing is shown in figure 1 below.

Figure 1. The wiretap channel for mobile edge computing
At the beginning, Bob first transmits training symbols to Alice, and Alice estimates the channel between Alice and Bob. After that, the symbols where Alice wants to transmit to Bob are multiplied by the special designed weighted on each antennas, according to the wireless propagation channel of Alice-to-Bob as the antenna weights base-band signal processing. The antenna weights base-band signal processing is shown in figure 2 below. Two typical MIMO physical layer secure transmission methods utilizing randomness properties of wireless channel are introduced following.

\[ y(n) = H_s w(n)s(n) + V_A \]

\[ y_{\text{Eve}}(n) = H_{\text{E}} w(n)s(n) + V_E \]

\[ V_A, V_E \] denotes the NR x 1 dimension AWGN vector with zero-mean and variance 0.5. The dimension of channel matrix \( H_A, H_E \) is NR x NT, NE x NT, whose coefficients are the independent complex circular symmetric Gaussian distributions zero-mean and variance unit. The antenna number of the three terminals must meet NT > NR ≥ NE. Furthermore, each element of \( H_E \) is independent from \( H_A \) either. Then Alice to design the matrix \( w(n) \) where \( H_A w(n) = A \), and \( A \) is a NR dimension of diagonal matrix with the positive and same diagonal elements \( A \). Therefore, Bob can detect

\[ y_{\text{Bob}}(n) = A s(n) + V_A \]

\[ \hat{s}(n) = A^{-1} y_{\text{Bob}}(n) \]

\[ 2.2. \text{Artificial Noise} \]

when NT > NR, the artificial noise is denoted as \( z_n \), where \( z_n \) lies in the null space of Alice-to-Bob channel. Therefore, the transmitted signals \( w_n s(n) \) are \( x_n = w_n \hat{s}(n) + z_n \), where.

\[ y_{\text{Bob}}(n) = H_s w_n \hat{s}(n) + V_A \]

\[ y_{\text{Eve}}(n) = H_E w_n \hat{s}(n) + H_E z_n + V_E \]

\[ 3. \text{Channel similarity analysis} \]

In the real wireless network the eavesdroppers with unknown position and cannot controlled by any legitimate users. Attackers can also adopt some advanced estimate algorithm or other unexpected means to gain the similar channel. So a channel similarity based methods is utilizing in our scheme to aid for secure performance analysis when unknown eavesdroppers channel. Assuming the track down normalized channel \( H_A \) and unknown Eve’s channel \( H_E \). The following conditions are expressed using the \( H_A \) estimated \( H_E \). First SVD decomposition \( H_A \):

\[ H_A = U \Sigma \Phi \]

\[ 5 \]
Where $U$ represents a unitary transformation matrix, $\Sigma$ represents the diagonal elements represent zero Nonzero eigenvalue. $V^1$ and $V^0$ respectively shows Nonzero eigenvalues and zero eigenvalues corresponding eigenvectors, then $V^0$ As Zero-based space of $H_A$.

$$V^0 = [V_1^0, V_2^0, ..., V_k^0] = H^\text{null}_A$$

(6)

When the number of antennas $N_E \leq NR$, $H_E \subset \{ C | NR\times NT \text{ dimension space} \}$ can be expressed as linear ratio of synthetic and orthogonal decomposition of $H_A$

$$H_E = \begin{pmatrix}
\alpha_{i,1} & L & \alpha_{i,\text{NR}} \\
M & O & M \\
\alpha_{\text{NR,}1} & L & \alpha_{\text{NR,}\text{NR}}
\end{pmatrix}
+ \begin{pmatrix}
\beta_{i,1} & L & \beta_{i,k} \\
M & O & M \\
\beta_{\text{NR,}1} & L & \beta_{\text{NR,}k}
\end{pmatrix}
\begin{pmatrix}
V_1^0 \\
V_k^0
\end{pmatrix}$$

(7)

Where $\alpha_i, \beta_m$ ($1 \leq i, j \leq \text{NR}, 1 \leq m \leq k$) are random variables obey certain distribution. For MISO system, above analysis could be intuitively simplified as $h_E = \alpha h_A + \beta_1 v_1^0 + \beta_2 v_2^0 + ... + \beta_k v_k^0$, where

$$\alpha = \cos \theta = \frac{h_A h_A^H}{\|h_A^H\|^2}, \beta_0, ..., \beta_k = \sin \theta$$

To AR system, Eve received signal can represent:

$$y_{\text{Eve}}(n) = \alpha h_A x(n) + (\beta_1 V_1^0 + \beta_2 V_2^0 + ... + \beta_k V_k^0) x(n) + V_E$$

$$= h_A \cos \theta x(n) + h_A^\text{null} \sin \theta x(n) + V_E$$

(8)

SINR of Eve (Signal to interference noise ratio) at receiving end can represent as

$$\text{SINR}_{\text{Eve}} = \frac{\|h_A \cos \theta\|^2}{\|h_A^\text{null} \sin \theta\|^2 + \delta_E^2}$$

(9)

$h_A^\text{null}$ is null space of $h_A$ and $\delta_E^2$ is the noise power. To AN system, Eve received signal:

$$y_{\text{Eve}}(n) = (h_A \cos \theta + h_A^\text{null} \sin \theta) \cdot (w(n) s(n) + z) + V_E$$

$$= h_A \cos \theta w(n) s(n) + h_A^\text{null} \sin \theta w(n) s(n) + h_A^\text{null} \sin \theta \cdot z + V_E$$

$$= h_A \cos \theta x(n) + h_A^\text{null} \sin \theta x(n) + h_A^\text{null} \sin \theta \cdot z + V_E$$

(10)

Eve’s SINR (Signal to interference noise ratio) at receiving end can represent as

$$\text{SINR}_{\text{Eve}} = \frac{\|h_A \cos \theta\|^2}{\|h_A^\text{null} \sin \theta\|^2 + \|h_A^\text{null} \sin \theta \cdot z\|^2 + \delta_E^2}$$

(11)

As can be seen above, AN and AR method respectively add the interference $h_A^\text{null} \sin \theta x(n)$ and $h_A^\text{null} \sin \theta x(n) + h_A^\text{null} \sin \theta \cdot z$ at the Eve receiving end. Since the Eve channel state is unknown to Alice, consider the worst case, Eve near from the transmitting and $\theta$ will approaching zero, thus case security performance decreased significantly. Related simulation results will give in follow figure in section 4.

4. Simulation results

In this section, we simulated the proposed mobile edge computing physical layer secure transmission scheme. The channel is block Rayleigh fading, where the channel matrix keeps constant during the transmission of one mobile edge computing packet, but randomly changes between the different transmitted mobile edging packets. Each of the channel between the transmit and receive antennas are independent. The BPSK modulation are employed for the wireless mobile edge computing. We randomly generate the control sequences. According to the characteristics of the scheme in this article referred to CB(cross-layer based on beamforming). Reference methods were AR(random array) and AN(artificial noise). The situation that the attackers can get channel that are very similar to the
This paper investigated the secure communications for the wireless mobile edge computing. The method is based on secure beamforming and artificial noise on the physical layer of wireless mobile edge computing. In this scheme, a random beam forming which is controlled by sequence is used to confuse the eavesdroppers in the wireless mobile edge computing scenarios. Through analysis and simulations, we found that the proposed scheme can achieve desired secure performance for the intended receiver is considered. The transmit antennas is 2 and antenna employed at both Eve and Bob is 1. Firstly in figure 3 (a), the BER performances are evaluated as a function of Signal-to-noise ratio(SNR) when the channel fading coefficients similarity degree intersection angle between the attackers and intended receiver are 10°, 20°and 45°respectively. Then in figure 3 (b) the Eve’s BER performances are evaluated by SNR fixed respectively in 4db,14db with similar degree intersection angle between the attackers and intended receiver are ranging from 10°to 90°.

![Figure 3](image1.png)(a)BER performance when similar angle $\theta=10°, 20°$and 45°respectively. (b) BER performance of Eve. Fixed SNR=4db ,14db and $\theta$ scope is 0°– 90°

Figure 4 indicates clearly that attacker can obtain lower and constant BER with more similar channel for both AN and AR methods. Attackers can achieving BER of 10−2 approximately in high SNR. Comparing to AR method the AN methods hardly to take any effect in this circumstance. However, the CB method steadily keeping Eves’ BER to be 0.5 in all situations, figures 3 and 4 clearly display secure performance of CB scheme maintain Eve’s BER close to 0.5 and don’t affect by channel similar degree between the attackers and intended receiver. In contrast, BER of attackers in AR and AN schemes linear decline with similar angle decreasing, and only when $\theta = 90°$ can achieves 0.5. Therefore, the CB methods can resist the similar CSI attacks.

![Figure 4](image2.png)Figure 4. Security capacity of CB, AR and AN methods when similar angle $\theta=10°, 20°$and 45°respectively.

5. Conclusion
This paper investigated the secure communications for the wireless mobile edge computing. The method is based on secure beamforming and artificial noise on the physical layer of wireless mobile edge computing. In this scheme, a random beam forming which is controlled by sequence is used to confuse the eavesdroppers in the wireless mobile edge computing scenarios. Through analysis and simulations, we found that the proposed scheme can achieve desired secure performance for the
wireless mobile edge computing scenarios. We think it is very good method for the secure communication of the wireless mobile edge computing scenarios.

Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

References
[1] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.
[2] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.
[3] Ding L, Jin C, Guan J, et al. Cryptanalysis of Lightweight WG-8 Stream Cipher[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(4): 645-652.
[4] Goel S, Negi R. Guaranteeing Secrecy using Artificial Noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.
[5] Li X, Hwu J, Ratazzi E P, et al. Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions[J]. Journal of Communications, 2007, 2(3): 24-32.
[6] Maurer U. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.
[7] Shah A, Haimovich A M. Performance analysis of optimum combining in wireless communications with Rayleigh fading and cochannel interference[J]. IEEE Transactions on Communications, 1998, 46(4): 473-479.
[8] Hu L, Wen H, Wu B, et al. Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(1): 219-228.
[9] Wen H, Gong G, Lv S, et al. Framework for MIMO cross-layer secure communication based on STBC[J]. Telecommunication Systems, 2013, 52(4): 2177-2185.
[10] Liao R, Wen H, Wu J, et al. The rayleigh fading channel prediction via deep learning[J]. Wireless Communications and Mobile Computing, 2018: 1-11.
[11] Wen H, Ho P, Qi C, et al. Physical layer assisted authentication for distributed ad hoc wireless sensor networks[J]. Iet Information Security, 2010, 4(4): 390-396.
[12] Wen H, Ho P, Wu B, et al. Achieving Secure Communications over Wiretap Channels via Security Codes from Resilient Functions[J]. IEEE Wireless Communications Letters, 2014, 3(3): 273-276.
[13] Chen S, Wen H, Wu J, et al. Internet of Things Based Smart Grids Supported by Intelligent Edge Computing[J]. IEEE Access, 2019: 74089-74102.
[14] Xie F, Wen H, Li Y, et al. Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(5): 3967-3977.
[15] Wen H, Tang J, Wu J, et al. A Cross-Layer Secure Communication Model Based on Discrete Fractional Fourier Transform (DFRFT)[J]. IEEE Transactions on Emerging Topics in Computing, 2015, 3(1): 119-126.
[16] Wen H, Wang Y F, Zhu X, et al. Physical layer assist authentication technique for smart meter system[J]. Iet Communications, 2013, 7(3): 189-197.
[17] Wen H, Ho P, Gong G, et al. A Novel Framework for Message Authentication in Vehicular Communication Networks[C]. global communications conference, 2009: 3067-3072.
[18] Wen H, Li S, Zhu X, et al. A framework of the PHY-layer approach to defense against security threats in cognitive radio networks[J]. IEEE Network, 2013, 27(3): 34-39.