Secure Data Communication for Wireless Mobile Edge Computing Based on Artificial Noise and Security Code

Zhining Lv¹, Jie Tang²,a, Wei Deng¹, Zhongwei Qiao¹, Hong Wen²,b and Yu Du¹

¹ Shenzhen Power Supply Bureau Co, Ltd., Shenzhen 510820, China
² School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China

Email: acs.tan@uestc.edu.cn; sunlike@uestc.edu.cn;

Abstract. As increasing threat to wireless mobile edge computing communication and high cost of conventional encryption implement in wireless mobile edge computing environments. The physical layer security has aroused widespread interests to increase the secure transmission and communications of mobile edge computing data communication in wireless networks. This work investigates the mobile edge computing secure communication by MIMO beamforming and artificial noise (AN) system with secure code. From practical consideration, in this work, we consider a coded system and investigate its achievable secrecy rate under the realistic wiretap code with limited code length and modulation. We proposed the mobile edge computing secure transmission scheme which could make almost zero information obtained by the unknown eavesdroppers with keeping certain quality of BER performance for the main channel simultaneously. The simulation results verify this proposed mobile edge computing secure transmission scheme performance. It shows great implement ability.

1. Introduction

Secure communication has become increasingly pervasive and essential [1,2, 3]. Mobile edge computing wireless communication has the broadcasting nature of, a passive eavesdropper, e.g., the attacker or the earwig man as the mobile edge terminals, where they can overhear the communication between the legitimate terminals and mobile edge service agent. Recently, this unique weakness of mobile edge computing wireless communication which is really called for innovative physical-layer security designs in future 6G mobile communication system,. Work [1] firstly proposed the physical layer wiretap channel model where the transmitter can encode the messages and send messages to the destination to achieve both unconditional security and reliable communication. The artificial noise (AN) [4] was recognized as a practical signal processing method to enhance security in mobile edge computing wireless communication. There has been a great interesting on the secrecy of mobile edge computing wireless communication [5, 6]. The investigations on MIMO secrecy capacity of mobile edge computing wireless communication have also been extended to various communication scene like some relay and cooperate mobile edge computing wireless communication scenarios [7,8]. Many works have applied the AN in various multi-antenna communication scene and characterize its secrecy capacity.

However, most works are based on the ideal secrecy code with infinite code length [8-10]. According to work [1,2], the final secrecy must guarantee the eavesdropper’s BER is keeping to 0.5 by a theory perfect wiretap code with infinite code length. The wiretap code in [10] is based on the
theoretical bin structure and cannot be directly employ in realistic. However, in a practical system, the binary source signals could only be processed by a practical wiretap code in limited code length. Thus the ideal assumptions may hard to meet and the final secrecy performance remains unknown under practical wiretap code. Even so, as far as we know, construct such a practical wiretap code [10] in low complexity and short length to approach the secrecy is still very difficult.

Unlike previous works focus on the theory secrecy capacity [11-14]. In this work, we consider such a practical coded system and investigate its achievable secrecy rate under the realistic wiretap code and modulation for wireless mobile edge computing data communication. Firstly, the secrecy capacity for power limited system under finite alphabet modulation (e.g. M-PSK, QAM) is analysis [15,16]. Then, different from the previous work on the theoretical secrecy capacity, we deduce the coded secrecy capacity could be achieved by ensure eavesdropper’s final achievable minimum BER larger than demanded threshold. The coded secrecy capacity could be easily to calculate and the transmitter could make unknown eavesdropper’s minimum achievable BER approach to 0.5 by a practical wiretap code. Based on it, a BER-Qos (Quality of Service) method is proposed. It can make sure that almost no information was obtained by the eavesdroppers with keeping certain quality of BER performance for the main channel.

The rest of the paper is shown as follows. The system model and description are proposed in section 2. In section 3, we provide theory secrecy capacity analysis for system under finite alphabet modulation. Section 4 shows the simulation results. In the end, Section 5 concludes the paper.

2. System model for the mobile edge computing communication

The system model of mobile edge computing data communication is shown in figure 1 below. First, the legitimate transmitter Alice is acted as the mobile edge server. She encodes binary bits message \( b = (b_1, b_2, \ldots, b_n) \) ( \( b_i \in \{0,1\} \) ) by a secret coding as \( s = (s_1, s_2, \ldots, s_n) \), where the code rate could be intuitive descript as \( R_s = m / n \) [17, 18]. After that, since Alice is the edge server, and she transmits the coded and modulated signal symbols by the special beamforming and AN processing. The legitimate receiver Bob is the mobile edge terminal. Bob received the signals and perform MIMO receiving combining and demodulation operations, and then he can get the sequence \( \hat{s} \), which is the noisy version of the transmitted sequence from the edge sever Alice [18]. Meanwhile, the eavesdropper Eve, who may be the attacker or the ear man, and she can also observe the noisy sequence \( \hat{s} \) from the edge sever Alice. Finally, both Bob and Eve perform decoding of the security code to obtain the transmitted sequence from the edge sever Alice, respectively. The Bob and Eve can decode \( \hat{s} = (\hat{s}_1, \hat{s}_2, \ldots, \hat{s}_n) \) and \( \hat{b} = (\hat{b}_1, \hat{b}_2, \ldots, \hat{b}_n) \) from their respective receive signals from the edge sever Alice.

![Figure 1. System model](image)

By assuming a flat-fading scenario, the signals received of the front MIMO processing at the edge terminal Bob and eavesdropper Eve that can be represented as
\[
\begin{align*}
    y_{\text{Bob}}(n) &= H_A x + n_A \\
    y_{\text{Eve}}(n) &= H_E x + n_E,
\end{align*}
\]

(1)

Where \( n_A \) and \( n_E \) are the white noise of Bob and Eve with power levels \( \epsilon( n, n_A^H ) = \sigma^2 I \), \( \epsilon( n, n_E^H ) = \sigma_E^2 I \), respectively. The operator \( (\cdot)^H \) denotes the Hermitian matrix operator, and \( \epsilon(\cdot) \) denotes expectation. The channel \( H_A \) and \( H_E \) are \( N_r \times N_r \), \( N_r \times N_r \) dimension of channel matrix, respectively, whose coefficients \( h_{ij} \) are all independent complex Gaussian distribution with zero-mean variance and unit one [17]. The transmit power available for Alice is \( \epsilon( xx^H ) = Q_A \) and \( \epsilon( zz^H ) = Q_E \).

\[
\text{Tr}(Q_A) \leq P_{\text{max}}. \quad I \text{ is an identity matrix. Alice is full of power because she is the edge server, and she can take part of the power to generate artificial noise (AN) to degrade the received quality of Eve, where the transmitted signal is } x = f s + G \cdot z. \text{ Where } s \text{ is the secret information symbol, and } z \text{ is the artificial noise vector with size } N_r - 1. \text{ The } z \text{ are assumed to be complex Gaussian vectors. Alice transmits modulated symbol with multipling by the vector } f = (f_1, f_2, ..., f_{N_r}), \text{ where } \| f \| = 1 \text{ and } \| f \| \text{ denotes the norm operation. And } G \text{ is the precoding matrix with size for } N_r \times (N_r - 1) \text{, and } G^H G = I. \text{ We let the transmitted power that allocate to the confidential modulated symbol is } P_S. \text{ Then, all of the other remained power is averagely distributed to each AN symbols, where}
\]

\[
\epsilon( zz^H ) = \frac{P_{\text{max}} - P_S}{N_r - 1} I
\]

(2)

The total power for AN is denoted by \( P_{AN} = P_{\text{max}} - P_S \). We let \( w_A \) and \( w_E \) denote \( N_r \times 1, N_r \times 1 \) receive combiner at Bob and Eve, respectively. After received the signals with the combiner, we have:

\[
\begin{align*}
    \mathcal{g}_{\text{Bob}}(n) &= w_A^H y_{\text{Bob}}(n) = w_A^H (H_A x + n_A) \\
    \mathcal{g}_{\text{Eve}}(n) &= w_E^H y_{\text{Eve}}(n) = w_E^H (H_E x + n_E).
\end{align*}
\]

(3)

If we let \( H_A = U \Sigma V^H \) denote the singular value decomposition [17], the mobile edge server Alice should make \( f \) as the singular vector corresponding to the largest singular value, [17] which is the right singular vectors of \( H_A \). We can denote by \( f = V(:,1) \). And we will constrain the interference signal \( G \cdot z \) in formula (5) so that it does not cause any interference to the secret symbols for Bob. To guarantee this, we require

\[
H_A G \cdot z \perp H_A f
\]

(4)

This goal can be easily achieved by choosing \( G \) to be the remaining \( N_r - 1 \) right singular vectors \( G = V(:,2:N_r - 1) \). The optimal combiner \( w_A^H \) then is equivalent to be

\[
w_A = H_A^H f.
\]

(5)

As for the eavesdropper Eve, the maximum SINR combiner is given by:

\[
w_E = (H_E^H Q_s H_E^H + \sigma_E^2 I)^{-1} H_E^H f
\]

(6)

Where

\[
Q_s = \frac{P_{AN}}{N_r - 1} G \cdot G^H
\]

(7)

In the mobile edging communication scenarios, Eve is very hard to peep the information about \( H_A, Q_s \) and \( f \). Therefore, for research of security, here we assume the worst case for Alice and Bob, the eavesdropper Eve can get the all of the information of \( Q_s \) and \( H_N f \). Therefore, at the worst case for secrecy, the eavesdropper Eve will obtain the largest SINR by linear MMSE processing [17]. The Bob and Eve can receive the signals.
\( y_{\text{Bob}}(n) = w_{\text{Bob}}^H y_{\text{Bob}}(n) = w_{\text{Bob}}^H (H_{\text{Bob}} s + H_{\text{Bob}} \cdot z + n_{\text{Bob}}) \)
\( y_{\text{Eve}}(n) = w_{\text{Eve}}^H y_{\text{Eve}}(n) = w_{\text{Eve}}^H (H_{\text{Eve}} s + H_{\text{Eve}} \cdot z + n_{\text{Eve}}) \).  

(8)

For the worst case consider for secrecy, the transmitter could assume background noise power of Eve trend to zero
\( y_{\text{Eve}}^H(n)_{\text{UP}} = w_{\text{Eve}}^H y_{\text{Eve}}(n) = w_{\text{Eve}}^H (H_{\text{Eve}} s + H_{\text{Eve}} \cdot z) \),
\( y_{\text{Eve}}^H(n)_{\text{UP}} \) could be viewed as the best receive signal for Eve. The detail of the security codes and the method associating with the MIMO system will be discussed in the next section.

3. The Framework of AN with Secure Code

The secure code with threshold \( \rho \) is employed in the system. The received SINR for Eve could denoted as:

\[
\text{SINR}_E = \frac{P_S \left| w_E^H H_{\text{Eve}} f \right|^2}{w_E^H (H_{\text{Eve}} Q_{\text{Eve}} H_{\text{Eve}}^H + \sigma_E^2 I) w_E}.
\]

(10)

And the maximum that Eve can achieve when combiner is given by formula (10):

\[
\text{SINR}_{E, \text{max}} = P_S f^H H_{\text{Eve}}^H (H_{\text{Eve}} Q_{\text{Eve}} H_{\text{Eve}}^H + \sigma_E^2 I)^{-1} H_{\text{Eve}} f
\]

(11)

The legitimate partners could assume the background noise of Eve is zero. It is obviously that the upper bound of maximum SINR that Eve could achieve is:

\[
\text{SINR}_{E, \text{LU}} = P_S f^H H_{\text{Eve}}^H (H_{\text{Eve}} Q_{\text{Eve}} H_{\text{Eve}}^H + \sigma_E^2 I)^{-1} H_{\text{Eve}} f > \text{SINR}_{E, \text{max}}
\]

(12)

By combining the formula (11), the SINR_{E, \text{LU}} could represent as

\[
\text{SINR}_{E, \text{LU}} = \left( \frac{(N_f - 1)}{1/\phi - 1} \right) f^H H_{\text{Eve}}^H (H_{\text{Eve}} G G^H H_{\text{Eve}}^H)^{-1} H_{\text{Eve}} f
\]

(13)

It could be seen obviously from formula (24), if fixed the antenna numbers, the upper bound of the maximum SINR the passive Eve can obtain related to the ratio \( \phi \) and random variable \( f^H H_{\text{Eve}}^H (H_{\text{Eve}} G G^H H_{\text{Eve}}^H)^{-1} H_{\text{Eve}} f \). It is distinctly that we hope \( \text{SINR}_{E, \text{LU}} \) as low as possible. We define the random variable

\[
X = f^H H_{\text{Eve}}^H (H_{\text{Eve}} G G^H H_{\text{Eve}}^H)^{-1} H_{\text{Eve}} f
\]

(14)

If we define the SINR outage probability for Eve is

\[
P(\text{SINR}_{E, \text{LU}} \geq \eta') \leq \varepsilon
\]

(15)

If \( \varepsilon \) is very close to zero, then

\[
P(\text{SINR}_{E, \text{LU}} < \eta') > 1 - \varepsilon
\]

(16)

Therefore, the maximum SINR of Eve could always be constrain to a threshold \( \eta' \)

\[
P(\text{SINR}_{E, \text{max}} < \text{SINR}_{E, \text{LU}} < \eta') > 1 - \varepsilon
\]

(17)

4. Simulation results

In this section, the performances of proposed secure communication system for wireless mobile edge computing secure communication scenarios is numerically simulated. We employ the BPSK modulation, and the channel is assumed to be block Rayleigh fading and. The antenna number of Bob and Eve are both set as 2, respectively. The transmit antenna number of Alice has is set as 4. The background noise power of Bob and Eve are set as \( s_{\text{Bob}}^2 = 1 \) and \( s_{\text{Eve}}^2 = 0 \). We assuming Eve fully known
precise information about $H, f$ and $Q, \sigma$ covariance information and he can always achieve his upper-value of the maximum SINR.

Figure 2. (a) BER performance with $N_r = 4, N_e = 2$ and $N_f = 2$ (b) SINR outage probability of Eve

In figure 2 (a), the total transmit power $P_{\text{max}}$ are assume to limited with 10dB and 20dB, respectively. The SNR required for Bob are ranged from -10db to 10db. The BER of Bob and Eve after secure codes (SC) decoding is denoted by label Bob, BobSC, EveSC10 and EveSC20, the solid line in figure 2 (a). The two dash line represent the BER of Eve after MIMO receiving before the secure decoding, with label Eve10 and Eve20, respective corresponding to $P_{\text{max}} = 10\text{db}, 20\text{db}$. In figure 2(a), it could be clearly seen that after the MIMO receive, without the secure code, the BER performance curve of Eve almost remain a high-level error rate and could achieve little drops before the 10 db range. From figure 2, we could see that by joint the secure code, the Eve’s BER curve improve and very close to about 0.5. Meanwhile, the BER curve of Bob after secure decoding is still exponential decline with the SNR increasing. When the SNR for secret signal is more than 4 db, the BER of Bob is trend to decline lower than $10^{-4}$, while the BER of Eve is still close to 0.5. The figure 2(b) illustrate the SINR outage probability of Eve with $P_{\text{max}} = 10\text{db}, 20\text{db}$, and $\phi = 0.5$ and 0.25 respectively. From figure 2(b), we could see that the outage probability is decline with the SINR increasing, which mean the Eve is more unlikely to achieve the high SINR. And the larger $P_{\text{max}}$ will make the SINR outage probability performance better.

5. Conclusion

In this paper, we investigated the secure communication scheme on the wireless mobile edge computing communication system form the practical consider. In our practical system. By ensuring eavesdropper’s final achievable minimum BER larger than demand threshold, the coded secrecy capacity is deduced from signal process view. A further study about the secrecy effect of non-linear MIMO receiving processing and soft decision is left for the future.

Acknowledgments

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

References

[1] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.
[2] Xie Y, Wen H, Wu B, et al. A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing[C]. ieee international conference on cloud computing technology and science, 2019, 7(2): 383-391.
[3] Li X, Ratazzi E P. MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks[C]. military communications conference, 2005: 1353-1359

[4] Goel S, Negi R. Guaranteeing Secrecy using Artificial Noise[J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] Tang J, Wen H, Zeng K, et al. Achieving Unconditional Security for MIMO-BAN under Short Blocklength Wiretap Code[C]. vehicular technology conference, 2017: 1-5.

[18] Tang J, Wen H, Hu L, et al. Associating MIMO beamforming with security codes to achieve unconditional communication security[J]. IET Communications, 2016, 10(12): 1522-1531.