



Channel Equalization Secret Communication Method Based on Time Reversal

Zhu Jiang^{1,2} and Ding Qiang^{1,2}(✉)

¹ School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
1325242@qq.com, 676068591@qq.com

² Chongqing Key Lab of Mobile Communications Technology, Chongqing 400065, China

Abstract. For the eavesdropping channel problem in physical layer security research. A wireless channel equalization and secretive transmission method based on time reversal is proposed, which is called equalized time reversal (ETR) technology. The method is applicable to rayleigh fading channel, and reduces the inter-symbol interference (ISI) component of the traditional time reversal (TR) by equalizing the indoor wireless channel to improve the secrecy performance.

Keywords: Channel equalization · Time reversal · Secrecy performance

1 Introduction

In communication system, the upper network layer of protocol stack uses private key and public key cryptosystem to manage the problems related to authentication privacy. With the enhancement of modern computer functions, the encryption and decryption algorithms have been broken, and the upper-level specific security protocols ignore the most basic layer in wireless communication [1, 2]. The communication of the wireless device is transmitted by the message through the wireless channel through encoding and information data modulation. Wireless channels lack physical boundaries, and any nearby receivers may listen for transmission signals or may block transmissions. It is important to design a wireless transmission system that guarantees low probability of interception and does not rely on the upper layer encryption and key.

The wireless communication has the characteristic of openness, the information transmission of terminals is easy to be overheard by the illegal users, and the security of wireless communication system has become the hotspot of research. The wireless channel has the characteristics of frequency domain, spatial domain and time-domain diversity, and provides the space for the wireless communication security to be studied. Wyner first put forward the interception channel model, which consists of three nodes of sender (Alice), legal receiver (Bob) and illegal receiver (Eve) [3]. The study of physical layer security has obtained good results in the fields of secure coding, key extraction [4], coordinated jamming [5], random weighting of antenna array [6], artificial noise [7], and so on [8].

Time reversal (TR) is a signal processing technology, which not only has the function of focusing signal, but also simplifies the complexity of receiver, and is used for multiple input multiple output (MIMO) ultra-wideband (UWB) Communication and beyond the diffraction limit of the super resolution and other characteristics. TR can play its greatest role in a rich scattering environment. The enclosed or semi-closed interior has a rich scattering scene, the environment is relatively complex, the channel is usually slow to change, and the channel state information does not need to be updated quickly. Therefore, the use of TR in indoor communication is a good choice. TR is also widely used in indoor position [9], cancer detection [10], underwater communications [11] and many other fields. In a TR process, the time reversal mirror (TRM) which is located near the target point, receives the detection signal from the target point, TRM each unit will receive the signal after the reversal of the timeline to launch again, at the target point will receive a higher main peak amplitude signal, And the signal in the time domain has the compression phenomenon, which is called the time reversal spatial focusing characteristic and the time focusing characteristic. Because time reversal has the characteristics of space-time focusing, it gets a lot of attention in the physical layer secure transmission.

In [12], Tan presents a MIMO-UWB TR model combining MIMO-UWB systems with TR technology. The physical layer confidentiality of the MIMO-UWB system with TR was studied and compared with the system without the TR technique. It is verified that the TR technology can improve the confidentiality of the system, and also analyzes the influence of the number of the legitimate receiver antenna and the number of the interception antenna, and the multipath number on the system secrecy capacity in the TR-MIMO system. In [13], El-Sallabi presents the characterization of the secrecy capability of the time reversal technique based on physical layer security, and studies the secrecy ability of the time inversion technique of the dense diffuse scattering radio channel. For diffuse wireless channels, the signal-to-noise ratio (SNR) saturation threshold varies with the number of multipath components in the mirror channel. In [14, 15], Han proposed a time-reversed multiple access scheme for multi-path multi-user downlink networks. This scheme takes advantage of the nature of the multipath channel. Due to the spatial focusing effect of the TR structure, energy can be collected at a predetermined receiving location, reducing interference between users. Under the Rayleigh fading channel model, the proposed scheme can increase the signal to interference and noise ratio (SINR) and the reachable confidentiality rate. In [16], the concept of an average effective secret SINR is proposed by Tran, which is used to show the security of the time inversion transmission system. The authors consider two correlations, namely the correlation of channel between transmission antennas and the channel correlation between legitimate users and eavesdroppers. Based on this, the analytic formula of the average effective SINR is deduced. The numerical simulation shows that the analytic expression can measure the security of physical layer transport in the correlated multipath channel environment well. The spatial focus of TR is that all the multipath components are added in the position of the receiver, and they are incoherent in other positions in the space. This is allowed by the spatial signature contained in the channel impulse response (CIR). The in-phase increase of the multipath component occurs at a specific sampling time. This effect is due to the matching filter behavior of the TR-Filter and the partial equalization characteristic, which reduces

the Inter symbol Interference (ISI) [17]. The main advantage of TR technology relative to the traditional multicarrier system is that it decreases the complexity of receiving computation significantly in the receiver [18, 19].

From the above analysis, some researchers have analyzed the theory of TR technology in physical layer and the confidentiality of interception channel model in the context of low complexity communication, less on how to further improve the traditional TR confidentiality can further research. Based on the above background, this paper puts forward a new equalization time reversal (ETR) technique to improve the secrecy performance. This technique is used to configure the equalizer and TRM at the sending end, and to balance the wireless channel to improve the system confidentiality.

2 System Model

In this paper, the Wyner eavesdropping model is improved. The transmitter uses the equalizer and TRM cascade configuration. The specific system model is shown in Fig. 1.

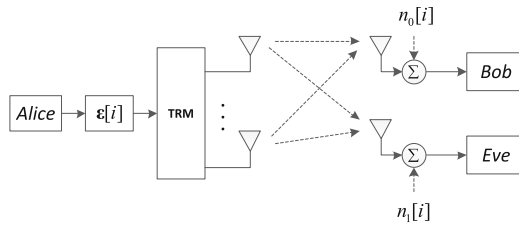


Fig. 1. System model

The system is mainly composed of the sender (Alice), the legal receiver (Bob), and the eavesdropping user. (Eve) constitutes. The eavesdropping user is passive eavesdropping, and no active attack is issued. The number of transmitting antennas is M , and both the legal receiver and the eavesdropping user are received by a single antenna. For convenience, 0 indicates the legal receiver Bob, and 1 indicates the eavesdropping user Eve. The CIR of the sender Alice and the receiver n (0, 1) can be expressed as

$$h_{mn}(i) = \sum_{l=0}^{L-1} \sigma_{mn,l} \delta(i - \tau_{mn,l}) \tag{1}$$

Where L is the number of resolvable multi-paths of the wireless channel. $\sigma_{mn,l}$ and $\tau_{mn,l}$ respectively represent the amplitude and delay of the l path. And satisfied with $E[h_{mn}(i)] = 0$, $E[|h_{mn}(i)|^2] = \sigma_{mn,i}^2$. In the TRM module, record $g_{m0}(i) \in C^{L \times 1}$ as the information transmission pre-filtering vector and satisfy

$$\begin{aligned}
 g_{m0}[i] &= \frac{\sqrt{\rho}h_{m0}^*[L-1-i]}{\sqrt{\sum_{m=1}^M E[||h_{m0}||^2]}} \\
 &= \frac{\sqrt{\rho}h_{m0}^*[L-1-i]}{\sqrt{P_0}}
 \end{aligned} \tag{2}$$

ρ is the total average transmission power, h_{m0}^* represents the conjugate of h_{m0} , $||\cdot||$ represents the Frobenius norm, defined as $||x(t)||^2 = \int_{-\infty}^{+\infty} |x(t)|^2 dt$. P_0 is the power normalization factor denoted as $P_0 = \sum_{m=1}^M E[||h_{m0}||^2]$, and the equivalent channel after time inversion is

$$\begin{aligned}
 h_{mn}^{eq}[i] &= g_{m0}[i] \otimes h_{mn}[i] \\
 &= \frac{1}{\sqrt{P_0}} \sum_{l=0}^{L-1} h_{mn}[l] h_{m0}^*[L-1-i+l]
 \end{aligned} \tag{3}$$

where $i \in (0 \dots 2L - 2)$.

2.1 Equalizer Design

Traditional TR technology has a large number of ISI components at the receiving end. Depending on the specific channel implementation, ISI can represent a significant percentage of the overall received power, affecting detection. The usual solution is to use RAKE receiver or equalization technology at the receiver. However, this will increase the computational complexity. To reduce the reception complexity, this paper considers adding a single equalizer to all the transmitting antennas at the sender. The equalizer and TRM are cascaded to minimize the ISI component of the receiver through wireless channel equalization. Therefore, an equalization vector $\varepsilon[i]$ of length $L_E = 2L_e + 1$ is designed. The equivalent power normalization factor is P_ε after the equalizer and the time reversal mirror are cascaded.

$$P_\varepsilon = \sum_{m=1}^M \sum_{i=0}^{L+2L_e-1} |h_{m0}^*[L-1-i] \otimes \varepsilon[i]|^2 \tag{4}$$

Then, the sender transmitting antenna m sends a signal $s[i]$ after being processed.

$$x_m[i] = \sqrt{\rho} s[i] \otimes \frac{h_{m0}^*[L-1-i] \otimes \varepsilon[i]}{\sqrt{P_\varepsilon}} \tag{5}$$

After adopting the equalization combined with the TR scheme, the receiver receives the signal as

$$y_0[i] = \frac{\sqrt{\rho}}{\sqrt{P_\varepsilon}} x[i] \otimes \varepsilon[i] \otimes \sum_{m=1}^M h_{m0}^{eq}[i] + n_0[i] \tag{6}$$

The equalizer is designed to reduce the ISI power, and its specific design satisfies the following formula.

$$\varepsilon[i] \otimes \sum_{m=1}^M h_{m0}^{eq}[i] = \delta[i - i_0] \tag{7}$$

where $i_0 \in (0 \dots 2L + L_E - 3)$, Eq. (8) with L_E unknowns and $2L + L_E - 2$ over-determined linear equations can be expressed as a matrix

$$\begin{pmatrix} \sum_{m=1}^M h_{m0}^{eq}[0] & & & & \\ \vdots & & & & \\ \sum_{m=1}^M h_{m0}^{eq}[2L - 2] & \ddots & & & \\ 0 & & \ddots & & \\ \vdots & & & \ddots & \end{pmatrix} \begin{pmatrix} \varepsilon[0] \\ \vdots \\ \varepsilon[L_E - 1] \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \tag{8}$$

The first matrix $\mathbf{H} \in C^{(2L+L_E-2) \times L_E}$ in the formula is the Toeplitz matrix, so the vector ε has a unique solution $\varepsilon = (\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H \delta_{n0}$ [20]. When $L_E \rightarrow \infty$, the ISI is completely eliminated. φ and H_{m0}^{eq} are the DFT of $\varepsilon[i]$ and $h_{m0}^{eq}[i]$, respectively, so it can be expressed in the frequency domain

$$\varphi[k] = \frac{\exp(-j\frac{2\pi(n_0-L+1)k}{2L+2L_E-1})}{\sum_{i=1}^M |H_{m0}^{eq}[k]|^2} \tag{9}$$

After the traditional TR channel is subjected to the above equalization processing, the equivalent channel is re-recorded as

$$h_{eq} \approx \frac{\sqrt{P}}{\sqrt{P_c}} \varepsilon[i] \otimes \sum_{m=1}^M h_{m0}^{eq}[i] \tag{10}$$

It can be seen from Eqs. (3) and (4) that the equivalent channel is related to the equalizer length and the number of channel resolvable multi-paths. As L_E increases, the normalization factor increases. Then according to Eq. (6), normalization is known. The increase of the factor causes the peak amplitude of the channel to decrease.

Figure 2 is an equivalent channel simulation diagram with 4 antennas at the sender and single antennas at the receiver. It can be seen from the figure that the main peak amplitude of the TR equivalent channel is high, and the sub-peaks of the main peak are also prominent. The main peak amplitude of the equivalent channel after ETR is slightly lower than TR, and the sub-peaks on both sides of the main peak have been greatly reduced, so that the ISI is alleviated. The equalized power peak amplitude of the channel after equalization decreases. The above analysis inferred consistency, thus verifying the correctness of the inference.

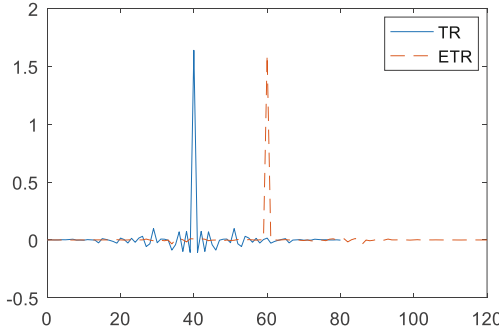


Fig. 2. Equivalent channel contrast diagram

2.2 Received Signal Component

After the equalization is used, it can be seen from the above analysis that the legal receiver can theoretically completely eliminate the ISI. In fact, it can only be greatly reduced and cannot be completely eliminated. This is because the receiver’s performance limit, the receiver can determine the number of multipath. The design of the equalizer, the length of the equalization vector will also be affected.

Due to the focusing characteristics of TR, the desired signal takes a sample at the center tap of the receiver, while the other tap signal samples are the main factor of inter-symbol interference. Therefore, the Eq. (6) in Sect. 2.1 is split, and the signal received by the legal receiver is re-recorded as

$$\begin{aligned}
 y_0[i] = & \sqrt{\frac{\rho}{P_g}} \left(\boldsymbol{\varepsilon} \otimes \sum_{m=1}^M \mathbf{h}_{m0}^{eq} \right) x[i - L - 1 + L_E] + \\
 & \sqrt{\frac{\rho}{P_g}} \sum_{l=0, l \neq L-1+L_E}^{2L+2L_E-2} \left(\boldsymbol{\varepsilon} \otimes \sum_{m=1}^M \mathbf{h}_{m0}^{eq} \right) x[i - l] + n_0[i]
 \end{aligned} \tag{11}$$

The received signal consists of three parts: expected signal, ISI and additive white Gaussian noise.

3 Secrecy Performance Analysis

In this section, the secrecy performance of the system will be analyzed, starting from the secrecy SINR, the secrecy capacity and the bit error rate (BER). The theoretical analysis and derivation will be used to obtain the analytical formula, and finally the conclusion will be drawn.

3.1 Signal-to-Interference-Plus Noise Ratio

Consider a digital multiple input single output (MISO) baseband wireless communication system with M transmit antennas and single antennas for receiving legitimate

users and eavesdropping users. According to Eq. (10), the expected signal power and symbol interference power of the legitimate users in the ETR scheme are respectively

$$P_{Sig}^0 = \frac{\rho}{P_g} |(\boldsymbol{\varepsilon} \otimes \sum_{m=1}^M \mathbf{h}_{m0}^{eq})[L-1+L_E]| \quad (12)$$

$$P_{ISI}^0 = \frac{\rho}{P_g} \sum_{l=0, l \neq L-1+L_E}^{2L+2L_E-2} |(\boldsymbol{\varepsilon} \otimes \sum_{m=1}^M \mathbf{h}_{m0}^{eq})[l]|^2 \quad (13)$$

It is known from Eqs. (7) and (8) that the design of the equalizer greatly reduces the ISI component of the legal receiver, so the ISI will be very small. The SNR of the legitimate user under the ETR scheme for

$$\gamma_0 = \frac{P_{Sig}^0}{P_{ISI}^0 + \sigma_0^2} \quad (14)$$

The reduction of P_{ISI}^0 will theoretically increase the SINR of the legal receiver. Similarly, the SINR of the eavesdropping end can be expressed as

$$\gamma_1 = \frac{P_{Sig}^1}{P_{ISI}^1 + \sigma_1^2} \quad (15)$$

The system's secret SINR is defined as

$$\gamma = \frac{\gamma_0 - \gamma_1}{1 + \gamma_1} \quad (16)$$

From the above analysis, the expectation of confidential SINR can be expressed as

$$\bar{\gamma} = E[\gamma] = E\left[\frac{\gamma_0 - \gamma_1}{1 + \gamma_1}\right] \quad (17)$$

known by the literature [10]

$$E\left[\frac{\gamma_0 - \gamma_1}{1 + \gamma_1}\right] = \frac{E[\gamma_0 - \gamma_1]}{E[1 + \gamma_1]} + \eta \quad (18)$$

where η is a very small number, which can be ignored, and re-record the Eq. (18) as

$$E[\gamma] = E\left[\frac{\gamma_0 - \gamma_1}{1 + \gamma_1}\right] = \frac{E[\gamma_0 - \gamma_1]}{E[1 + \gamma_1]} \quad (19)$$

This will give you the expectation of secrecy SINR.

In the traditional TR scheme, the secrecy SINR of the legal receiver has a large amount of ISI, which makes the secrecy SINR greatly affected by ISI. Using the ETR scheme greatly reduces the ISI, so that the secrecy SINR is improved and the secret SINR is also improved.

3.2 Capacity of System

Generally, the secret capacity is inferred from the secret SINR in the eavesdropping channel. The secret capacity is defined as the difference between the legal user channel capacity and the eavesdropping user channel capacity. According to the Shannon formula, the formula for the secret capacity is defined as

$$\begin{aligned} C &= \log_2(1 + \gamma_0) - \log_2(1 + \gamma_1) \\ &= \log\left(1 + \frac{\gamma_0 - \gamma_1}{1 + \gamma_1}\right) \end{aligned} \quad (20)$$

From Sect. 3.1, $\frac{\gamma_0 - \gamma_1}{1 + \gamma_1}$ is the confidential SINR of the whole system, which is expressed by γ .

$$\gamma = \max\left(\frac{\gamma_0 - \gamma_1}{1 + \gamma_1}, 0\right) \quad (21)$$

For any eavesdropping to achieve absolute secure communication, it is necessary to satisfy $0 < C_1 \leq C$ and C_1 as the information transmission rate of secure communication. By analyzing the secret signal to noise ratio of Sect. 3.1 to ETR, the Eqs. (14) and (15) are brought into Eq. (20). After the equalization, the system's confidential capacity C is

$$\begin{aligned} C &= \log\left[1 + \frac{E[\gamma_0 - \gamma_1]}{E[1 + \gamma_1]}\right] \\ &= \log\left[1 + \frac{\left[E\left[\frac{p^0_{Sig}}{p^0_{ISI} + \sigma_0^2}\right] - E\left[\frac{p^1_{Sig}}{p^1_{ISI} + \sigma_1^2}\right]\right]}{1 + E\left[\frac{p^1_{Sig}}{p^1_{ISI} + \sigma_1^2}\right]}\right] \end{aligned} \quad (22)$$

The secrecy capacity of the system is proportional to the expected signal power of the legitimate user, and inversely proportional to the power of the ISI signal.

3.3 Bit Error Rate Analysis

The transmitting end adopts QPSK modulation, and the expression of expected signal power, ISI signal power and noise signal power of the ETR legal receiving end has been given in the equation of Sect. 3.1. The BER can be expressed according to the literature [21].

$$P \approx Q\left(\sqrt{\frac{p^0_{Sig}}{p^1_{ISI} + \sigma_0^2}}\right) \quad (23)$$

Where $Q(\cdot)$ is the complementary cumulative distribution function of the standard Gaussian random variable.

3.4 Complexity Analysis

In this paper, the number of transmit antennas is not considered, and the complexity of TR and ETR is analyzed and compared. The following figure compares the detection time of TR and ETR in time domain. The effect of TRM pre-filtering in traditional TR leads to the focus of the received signal at the legal receiver. The peak energy is collected at the center tap L . In ETR, the channel equalization of the TRM and the equalizer causes the focus peak energy to shift backward in the time domain. The specific time delay is extended by the length of the equalization vector and the delay of the actual detection environment determined (Fig. 3).

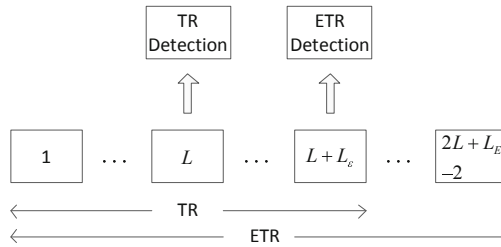


Fig. 3. Comparison of TR and ETR detection maps

It can be known from Eq. (3) that the computational complexity of TR is $O(L^2)$. After adding the equalizer, it is equivalent to the TR equivalent channel convolutional equalization vector $\varepsilon[i]$. Equalizing the TR equivalent channel will perform a matrix multiplication operation on the original channel matrix. According to Eq. (8), the computational complexity of ETR is $O(L^2 \times L_E)$.

From the above analysis, the ETR calculation complexity is greater than TR. The advantage of ETR security performance is that it is exchanged for the computational complexity.

4 Numerical Results

From the previous theoretical analysis, the secrecy SINR of the legal receiver, the system’s secrecy capacity, and the BER are closely related to the expected signal power, ISI power, and noise power at the receiver. The computer simulation experiment will be used to further analyze the secrecy performance of the indoor secure communication system. The parameter settings involved in the simulation are shown in Table 1:

The paper uses the single cluster frequency selective fading statistical channel model in [22] to carry out simulation experiments. According to the simulations of Eqs. (12), (13) and (14), the following Fig. 4 is obtained, which shows the relationship between the transmitted SNR and the system-secured SINR, and also compares the secrecy SINR of ETR and TR. It can be seen from the figure that the increase in the

Table 1. Simulation parameter settings

Parameters	Values
T_S	2 ns
B	500 MHz
L_E	41
L	41
θ_T	80 ns
K	10000

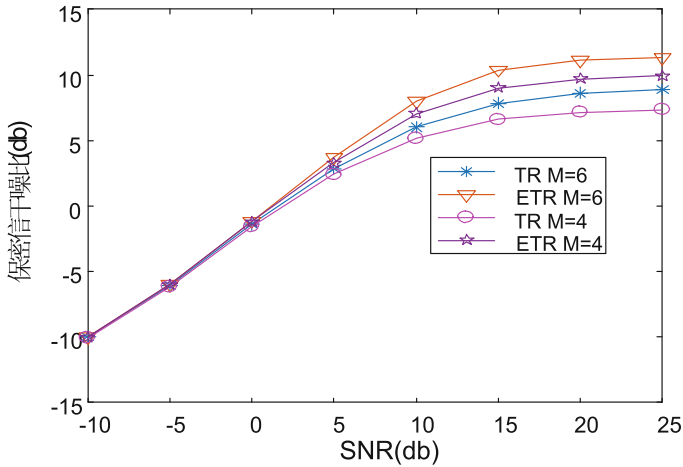


Fig. 4. Relationship between transmitted SNR and secrecy SINR

number of antennas also leads to an increase in the secrecy SINR. When the transmitted SNR is greater than 4 db, the secrecy SINR is significantly better than TR, which is consistent with the analysis in Sect. 3.1.

Figure 5 shows the confidential capacity map of ETR and TR. It can be seen from the figure that the transmission rate of ETR to achieve absolute secure communication is greater than TR. When the transmit SNR is greater than 25 db, the confidential capacity of TR is close to convergence, and the secrecy capacity of ETR is still improving, which also proves the advantage of ETR. The increase in transmit SNR and the increase in the number of transmit antennas increase the system’s secrecy capacity.

Figure 6 is a simulation of the BER of the legal receiver. The simulation is performed when the number of antennas is 2, 4, and 6 at the sender. The BER of ETR and TR is compared. It can be seen from the curve that the BER of the two schemes is related to the number of antennas at the sender. We can see from the picture that the more antennas, the lower the BER. The simulation results are completely consistent with the analysis in Sect. 3.3, which verifies the correctness of the analysis.

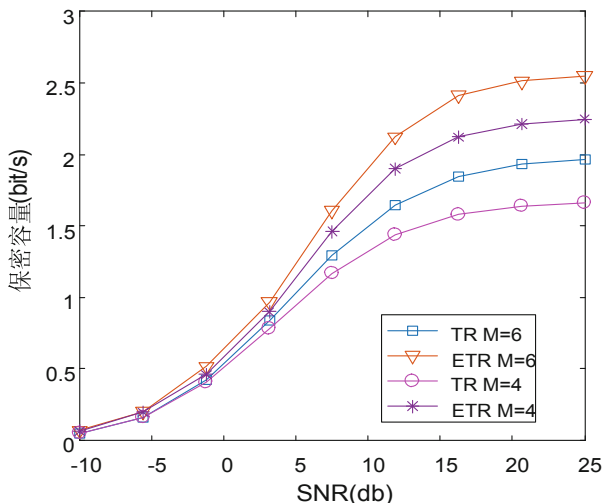


Fig. 5. The relationship between sending SNR and secrecy capacity

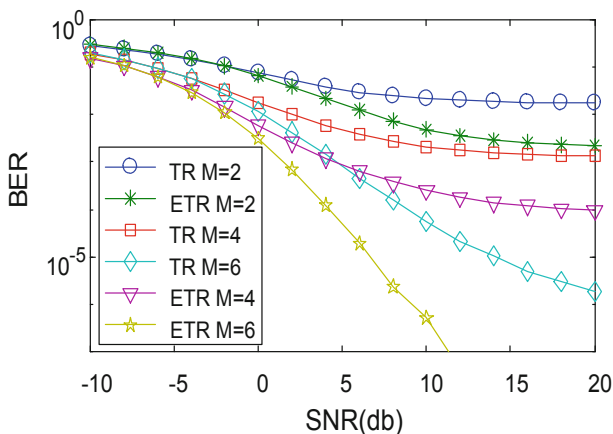


Fig. 6. Relation graph of sending SNR and BER

5 Conclusion

In order to improve the secrecy performance of TR under the eavesdropping model, this paper proposes an ETR solution. In this scheme, a forced zero equalizer is added between the source and the TRM, and the channel equalization is processed to enhance the system confidentiality. In this paper, The equalizer is designed, and the secrecy SINR, the system secrecy capacity, and the BER expression of the legal receiver are deduced. The simulation results show that the ETR technology can greatly reduce the equivalent channel sub-peak energy, but has little effect on the main peak energy.

The secrecy SINR and system secrecy capacity of the legal receiver are significantly improved, and the error performance is also improved. The main channel peak amplitude of the equivalent channel has a slight decrease compared with the traditional TR, and the effect on the focusing ability of TR is weak. The improvement of secretive performance is at the expense of the peak energy and computational complexity of the equivalent channel, and it is worth considering from the perspective of security. In the future work, the secretive performance of the richer channel model will be further studied.

References

1. Jiang, D., Wang, Y., Han, Y., et al.: Maximum connectivity-based channel allocation algorithm in cognitive wireless networks for medical applications. *Neurocomputing* **220**, 41–51 (2017). (SCI, EI)
2. Jiang, D., Xu, Z., Li, W., et al.: An energy-efficient multicast algorithm with maximum network throughput in multi-hop wireless networks. *J. Commun. Netw.* **18**(5), 713–724 (2016). (SCI, EI)
3. Shannon, E.: Communication theory of secrecy systems. *Bell Syst. Tech. J.* **29**, 656–715 (1949)
4. Maurer, U.M.: Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **39**(3), 733–742 (1993)
5. Dong, L., Han, Z., Petropulu, A.P., et al.: Improving wireless physical layer security via cooperating relays. *IEEE Trans. Sig. Process.* **58**(3), 1875–1888 (2010)
6. Li, X.-H., Hwu, J.: Using antenna array redundancy and channel diversity for secure wireless transmissions. *J. Commun.* **2**(3), 24–32 (2007)
7. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **7**(6), 2180–2189 (2008)
8. Wu, D., Si, S., Wu, S., Wang, R.: Dynamic trust relationships aware data privacy protection in mobile crowd-sensing. *IEEE Internet Things J.* <https://doi.org/10.1109/jiot.2017.2768073>
9. Gao, X., Li, J., Ma, J., Shi, F.F., Wang, W., Wang, C.H.: Weighting technique for detection and location of targets by time reversal-reverse time migration mixed method. In: 2017 Symposium on Piezoelectricity, Acoustic Waves, and Device Applications (SPAWDA), Chengdu, China, pp. 393–396 (2017)
10. Tao, Y., Mu, T., Song, Y.: Time reversal microwave imaging method based on SF-ESPRIT for breast cancer detection. In: 2017 3rd IEEE International Conference on Computer and Communications (ICCC), Chengdu, pp. 2094–2098 (2017)
11. Li, C., Shen, X., Jiang, Z., Wang, X.: Mobile underwater acoustic communication based on passive time reversal. In: 2017 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), Xiamen, pp. 1–5 (2017)
12. Tan, V.T., Ha, D.B., Tran, D.D.: Evaluation of physical layer secrecy in MIMO ultra-wideband system using time-reversal techniques. In: 2014 International Conference on Computing, Management and Telecommunications (ComManTel), Da Nang, pp. 70–74 (2014)
13. El-Sallabi, H., Aldosari, A.: Characterization of secrecy capacity of time reversal technique for wireless physical layer security. In: 2016 19th International Symposium on Wireless Personal Multimedia Communications (WPMC), Shenzhen, pp. 194–198 (2016)

14. Han, F., Yang, Y.H., Wang, B., Wu, Y., Liu, K.J.R.: Time-reversal division multiple access in multi-path channels. In: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, Houston, TX, USA, pp. 1–5 (2011)
15. Han, F., Yang, Y.H., Wang, B., Wu, Y., Liu, K.J.R.: Time-reversal division multiple access over multi-path channels. *IEEE Trans. Commun.* **60**(7), 1953–1965 (2012)
16. Tran, H.V., Tran, H., Kaddoum, G., Tran, D.D., Ha, D.B.: Effective secrecy-SINR analysis of time reversal-employed systems over correlated multi-path channel. In: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, pp. 527–532 (2015)
17. Kyritsi, P., Papanicolaou, G., Eggers, P., Oprea, A.: MISO time reversal and delay-spread compression for FWA channels at 5 GHz. *IEEE Antennas Wirel. Propag. Lett.* **3**, 96–99 (2004)
18. Chen, Y., Yang, Y.H., Han, F., Liu, K.J.R.: Time-reversal wideband communications. *IEEE Sig. Process. Lett.* **20**(12), 1219–1222 (2013)
19. Cardoso, F.D., Correia, L.M., Petersson, S., Boldi, M.: Beamforming strategies for energy efficient transmission in LTE. In: 2013 IEEE 77th Vehicular Technology Conference (VTC Spring), Dresden, pp. 1–5 (2013)
20. Viteri-Mera, C.A., Teixeira, F.L.: Equalized time reversal beamforming for frequency-selective indoor miso channels. *IEEE Access* **5**, 3944–3957 (2017)
21. Proakis, J., Salehi, M.: *Digital Communications*. McGraw-Hill, New York (2008)
22. Saleh, A.A.M., Valenzuela, R.A.: A statistical model for indoor multi-path propagation. *IEEEJ. Sel. Areas Commun.* **5**(2), 128–137 (1987)