Secrecy Capacity Achievable Time Reversal Pre-filter in MISO Communication System and the Unequal Secrecy Protection Application

Article *in* Wireless Personal Communications · August 2017

DOI: 10.1007/s11277-017-4787-x

CITATION
1

READS
23

4 authors, including:

Wei Cao
National University of Defense Technology
12 PUBLICATIONS **13** CITATIONS

SEE PROFILE

Wei li
National University of Defense Technology
29 PUBLICATIONS **217** CITATIONS

SEE PROFILE

Wireless Pers Commun (2017) 97:5427–5437
https://doi.org/10.1007/s11277-017-4787-x

Secrecy Capacity Achievable Time Reversal Pre-filter in MISO Communication System and the Unequal Secrecy Protection Application

Wei Cao[1] · Jing Lei[1] · Weidong Hu[1] · Wei Li[1]

Published online: 5 August 2017

Abstract Classical time reversal (TR) pre-filtering has been considered as one of the key physical layer security techniques for wireless communication applications in the last decade. This paper proposes a secrecy capacity achievable time reversal pre-filter to further enhance the confidentiality of a multi-input single-output (MISO) wireless communication system. In addition, an unequal secrecy protection (UESP) MISO broadcast configuration is constructed in frequency selective channels by exploiting classical and secrecy capacity achievable TR pre-filters, so that UESP wireless communication services can be offered. Theoretical proofs and simulation results show that the proposed TR pre-filter achieves the secrecy capacity in frequency selective channels (HIPERLAN/2 BranA), and the MISO broadcast configuration can provide mobile users with three levels of UESP hierarchical services in terms of public, private and confidential messages.

Keywords Time reversal · Physical layer security · Secrecy capacity · Unequal secrecy protection · Multi-input single-output

1 Introduction

Eavesdropping is a well known security vulnerability introduced by wireless networks due to their broadcast nature. Traditionally, the regular ways to cope with this worrisome concern are primarily based on computationally demanding cryptographic algorithms in upper layers of communication model [1]. A plethora of remarkable cryptographic algorithms, whatever private or public key schemes, all contribute to defend wireless communications against unapproved eavesdroppers. However, the existing cryptographic communication systems are vulnerable to quantum attacks if large-scale quantum computers are successfully produced in the near future. Under the circumstances, some

✉ Wei Cao
cassanocao@hotmail.com

[1] ATR Key Lab, College of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan Province, People's Republic of China

classical cryptographic schemes are likely to be solved easily, such as integer factorization based RSA algorithm.

Besides that, an alternative solution to guarantee the confidential transmission in wireless environment is to exploit spatio-temporal characteristics of wireless channels, i.e. physical layer security [2, 3]. The essential feature of physical layer security is aimed to guarantee the secrecy from the perspective of information theory rather than computational hardness. The past decade has witnessed a plentiful prosperity in physical layer security ever since its original birth from Shannon's perfect secrecy idea [4]. Eavesdropping concerns can be eliminated by Multi-input Multi-output (MIMO) beam-forming [5] and artificial noise [6] in flat fading channels. However, those physical layer security techniques cannot directly be adopted into some practical scenarios because of the severe multi-path propogation effects, such as ultra wideband (UWB) communications [7] in urban areas. Thus researchers are motivated to make the physical layer security methods in flat fading channels compatible to frequency selective channels. Two potential strategies are orthogonal frequency division multiplexing (OFDM) and time reversal (TR).

OFDM is able to convert broadband frequency selective channels into a series of parallel flat fading sub-channels, thus beam-forming and artificial noise that are originally proposed for flat fading channels can be employed in frequency selective channels [8]. Aside from that, TR is a very promising pre-filtering technique in frequency selective channels. Chen. etc in [9] claimed that compared with OFDM system, the computational complexity of a time-reversal system at the transmitter side is lower since it requires similar amount of addition but no multiplication operations.

TR has been widely used in acoustics [10], ultrasonics [11], underwater communications [12] and UWB communications [13]. Moreover, TR is currently considered as an ideal candidate platform for 5G indoor systems [14] owing to its temporal compression and spatial focusing characteristics. TR equivalently reduces the delay spread of multi-path channels and mitigates negative effects of inter-symbol interference (ISI), which is called "temporal compression" [15]. While on the other hand, TR fully exploits multi-path propagation, recollects broadcast signals from the wireless environment and adds them coherently in the cooperative receivers, thus enabling legitimate users superior to illegitimate users in terms of signal-to-noise ratio (SNR), which is called "spatial focusing" [16]. Therefore, TR is a novel physical layer security technique in frequency selective channels [17]. To further improve the confidentiality, TR can be combined with Gram-Schmidt orthogonalization method to produce null fields at eavesdroppers, namely "Shielding Eve TR" [18]. Nevertheless, contrary to the first intuition, secrecy capacity cannot be simply achieved by shielding eavesdroppers.

Motivated by this consideration, in this paper we will propose a novel secrecy achievable TR pre-filters by imitating the optimal secrecy achievable beam-forming in [19], and then attempt to construct an unequal secrecy protection (UESP) MISO broadcast configuration by exploiting classical and secrecy capacity achievable TR pre-filters. The idea of UESP stems from the unequal protection (UEP) coding [20]. In contrast with the equal error protection (EEP) performance for all information symbols in the common channel coding, UEP assigns different levels of protection to different information symbols according to their importance. Herein, we extend the application of UEP into the wireless broadcast configuration, so that offering multifarious wireless communication services with different levels of secrecy to mobile users. Note that the UEP coding focuses on the reliability while our proposed UESP configuration attach more importance to the secrecy performance.

The remainder of this paper is organized as follows. We introduce the mathematical preliminaries involving convenient notations, frequency selective channel model and

secrecy capacity in Sect. 2. In Sect. 3, we first introduce classical and shielding Eve TR pre-filters, and then propose the optimal TR pre-filter to achieve the secrecy capacity. Section 4 presents the simulation results. The TR based UESP MISO broadcast configuration is constructed in Sect. 5 and the concluding remarks are finally made in Sect. 6.

2 Preliminaries

2.1 Notations

Bold upper and lower case characters are used for matrices and vectors. M_T, M_R and M_E represent Alice, Bob and Eves' antenna number, respectively. γ and ρ stand for transmit SNR and artificial noise power allocation factor. Time and frequency domain forms of signal are distinguished by the use of lower and upper case characters. $\mathrm{E}(X)$ represents the expectation of random variable X. $\langle \mathbf{x}, \mathbf{y} \rangle$ denotes the inner product of vector $\mathbf{x}$ and $\mathbf{y}$. $\{\bullet\}^+ \triangleq \max\{0, \bullet\}$.

2.2 Channel Model

The channel model used in this paper is the BranA that was employed for HIPERLAN/2 tests in indoor scenario. This channel has been set for a bandwidth of 100MHz, and is constituted of 40 taps. The power delay profile is given in Table 1 and an example realization is shown in Fig. 1.

2.3 Secrecy Capacity

The achievable secrecy rate is a theoretical metric for the practical physical layer security scheme. In the wiretap channel, the achievable secrecy rate is a transmission rate that can be reliably supported on the primary channel, but which is un-decodable on the eavesdroppers' channels. In particular, it is calculated as the difference of the mutual information between the primary and eavesdroppers for Gaussian wiretap channels

$$\begin{aligned} R_S &= \{R_{S\_Bob} - R_{S\_Eve}\}^+ \\ &= \{I(X; Y_{Bob}) - I(X; Y_{Eve})\}^+ \end{aligned} \tag{1}$$

And the supremum of secrecy rate is named secrecy capacity C_S when the difference of Bob and Eve's transmission rates R_S are maximized [21].

Table 1 HIPERLAN/2 BranA channel model

Delay (ns)	Power	Delay (ns)	Power	Delay (ns)	Power
0	0.181019	60	0.0546668	170	0.0185235
10	0.147138	70	0.0369593	200	0.0101794
20	0.122384	80	0.0369593	240	0.00772189
30	0.0994772	90	0.0300416	290	0.00286896
40	0.0808581	110	0.0613372	340	0.00104165
50	0.0672549	140	0.0337073	390	0.000387011

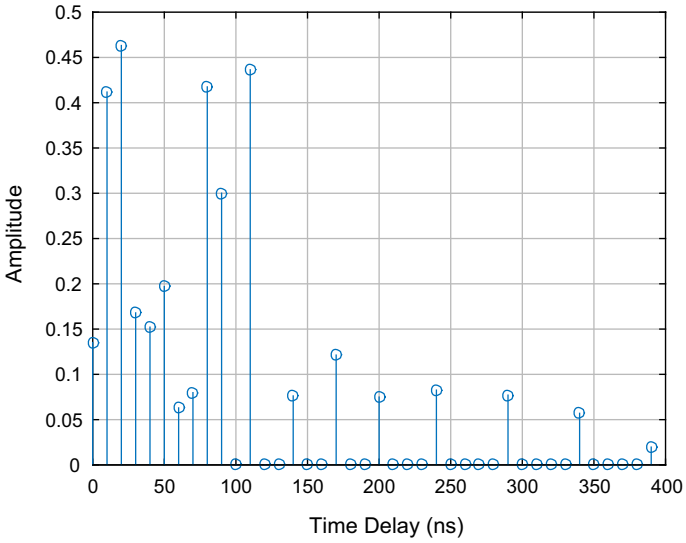

Fig. 1 HIPERLAN/2 BranA channel model

3 Time Reversal Pre-filters

In this section, we will introduce the classical and shielding Eve TR pre-filters in subsection 3.1 and 3.2, respectively, and then give out the secrecy capacity achievable TR pre-filter and its asymptotic analysis in subsection 3.3.

3.1 Classical Time Reversal Pre-filter

We describe a downlink TR communication system with M_T transmit antennas and M_R receive antennas as a two-stage process. In particular, we assume that $M_T > 1$ and $M_R = 1$ for a MISO communication scenario. Additionally, M_E stands for the number of eavesdroppers, but each eavesdropper only has one receive antenna for interception purpose.

Channel Estimation In the first stage, Alice manages to estimate the frequency Channel State Information (CSI) $\mathbf{H_B}(\mathbf{f}) = \left[H_{B,1}(f), H_{B,2}(f), \ldots, H_{B,M_T}(f)\right]$ through the pilot-aided symbols transmitted from Bob. Herein, we assume the channel estimation of $\mathbf{H_B}(\mathbf{f})$ is perfect.

Data Transmission In the second stage, Alice transmits the actual data to Bob and uses the conjugate of $\mathbf{H_B}(\mathbf{f})$ as a pre-filter,

$$\mathbf{H_{TR}}(\mathbf{f}) = \mathbf{H_B^*}(\mathbf{f}) \tag{2}$$

And the achievable secrecy rate is expressed as

$$\begin{aligned} R_S &= \{I(X;Y_{Bob}) - I(X;Y_{Eve})\}^+ \\ &= \left\{\log_2\left(\frac{1+\left|\left\langle \mathbf{H_{TR}}(\mathbf{f}), \mathbf{H_B^*}(\mathbf{f})\right\rangle\right|^2\gamma}{1+\left|\left\langle \mathbf{H_{TR}}(\mathbf{f}), \mathbf{H_E^*}(\mathbf{f})\right\rangle\right|^2\gamma}\right)\right\}^+ \end{aligned} \tag{3}$$

3.2 Shielding Eve Time Reversal Pre-filter

If all eavesdroppers' CSI are perfectly known to Alice, TR can be combined with Gram-Schmidt orthogonalization method to produce null fields at all the eavesdroppers' locations [18]. From the perspective of information leakage, this scheme seems to be the optimal secure design since no information would leak to Eavesdroppers.

Assume there are M_E eavesdroppers in the wireless environment, then the shielding Eve TR pre-filter is designed as

$$\mathbf{H}_{\mathbf{TR}}^{\mathbf{Null}}(\mathbf{f}) = \mathbf{H}_{\mathbf{TR}}(\mathbf{f}) - \sum_{i=1}^{M_E} \frac{\left\langle \mathbf{H}_{\mathbf{TR}}(\mathbf{f}), \mathbf{H}_{\mathbf{Ei}}^{*}(\mathbf{f}) \right\rangle}{\left\langle \mathbf{H}_{\mathbf{Ei}}^{*}(\mathbf{f}), \mathbf{H}_{\mathbf{Ei}}^{*}(\mathbf{f}) \right\rangle} \mathbf{H}_{\mathbf{Ei}}^{*}(\mathbf{f}) \tag{4}$$

where $\langle \mathbf{a}, \mathbf{b} \rangle = \mathbf{b}^H \mathbf{a}$ stands for the inner conduct of vector $\mathbf{a}$ and $\mathbf{b}$, $\mathbf{b}^H$ is the conjugate transpose of $\mathbf{b}$. $\mathbf{H}_{\mathbf{Ei}}(\mathbf{f}) = \left[H_{Ei,1}(f), H_{Ei,2}(f), \ldots, H_{Ei,M_T}(f)\right], i = 1, 2, \ldots, M_E$ is CSI of the i^{th} eavesdropper. So that TR pre-filter $\mathbf{H}_{\mathbf{TR}}^{\mathbf{Null}}(\mathbf{f})$ is orthogonal to all Eves' CSI, i.e.

$$\left\langle \mathbf{H}_{\mathbf{TR}}^{\mathbf{Null}}(\mathbf{f}), \mathbf{H}_{\mathbf{Ei}}^{*}(\mathbf{f}) \right\rangle = 0 \tag{5}$$

Compared with classical TR pre-filter, shielding Eve TR pre-filter has a better secure performance at the cost of transmission efficiency. Since all eavesdroppers are nulled, the mutual information between Alice and Eves is $I(X; Y_{Eve}) = 0$. Therefore the achievable secrecy rate is

$$\begin{aligned} R_S &= \{I(X; Y_{Bob}) - I(X; Y_{Eve})\}^+ \\ &= \left\{ \log_2 \left(1 + \left| \left\langle \mathbf{H}_{\mathbf{TR}}^{\mathbf{Null}}(\mathbf{f}), \mathbf{H}_{\mathbf{B}}^{*}(\mathbf{f}) \right\rangle \right|^2 \gamma \right) \right\}^+ \end{aligned} \tag{6}$$

3.3 Secrecy Capacity Achievable Time Reversal Pre-filter

Although shielding Eve TR pre-filter enables Eve to intercept nothing, it is never the optimal pre-filter since Bob's transmission efficacy is degraded to some extent. Therefore secrecy capacity cannot be achieved by exploiting shielding Eve TR pre-filter. In this subsection, we attempt to derive the optimal TR pre-filter $\mathbf{H}_{\mathbf{opt}}(\mathbf{f})$ in frequency selective channels by imitating the optimal beam-forming case in flat fading channels in [19].

$$\begin{aligned} C_S &= \arg\max_{\mathbf{H}_{\mathbf{opt}}(\mathbf{f})} \left\{ \log_2 \left(1 + \left| \mathbf{H}_{\mathbf{B}}(\mathbf{f}) \mathbf{H}_{\mathbf{opt}}(\mathbf{f}) \right|^2 \gamma \right) - \log_2 \left(1 + \left| \mathbf{H}_{\mathbf{E}}(\mathbf{f}) \mathbf{H}_{\mathbf{opt}}(\mathbf{f}) \right|^2 \gamma \right) \right\}^+ \\ &= \arg\max_{\mathbf{H}_{\mathbf{opt}}(\mathbf{f})} \left\{ \log_2 \left(\frac{1 + \left| \mathbf{H}_{\mathbf{B}}(\mathbf{f}) \mathbf{H}_{\mathbf{opt}}(\mathbf{f}) \right|^2 \gamma}{1 + \left| \mathbf{H}_{\mathbf{E}}(\mathbf{f}) \mathbf{H}_{\mathbf{opt}}(\mathbf{f}) \right|^2 \gamma} \right) \right\}^+ \\ &= \arg\max_{\mathbf{H}_{\mathbf{opt}}(\mathbf{f})} \left\{ \log_2 \left(\frac{\mathbf{H}_{\mathbf{opt}}^{\mathbf{H}}(\mathbf{f}) \left(\mathbf{I} + \mathbf{H}_{\mathbf{B}}(\mathbf{f}) \mathbf{H}_{\mathbf{B}}^{\mathbf{H}}(\mathbf{f}) \gamma \right) \mathbf{H}_{\mathbf{opt}}(\mathbf{f})}{\mathbf{H}_{\mathbf{opt}}^{\mathbf{H}}(\mathbf{f}) \left(\mathbf{I} + \mathbf{H}_{\mathbf{E}}(\mathbf{f}) \mathbf{H}_{\mathbf{E}}^{\mathbf{H}}(\mathbf{f}) \gamma \right) \mathbf{H}_{\mathbf{opt}}(\mathbf{f})} \right) \right\}^+ \\ &= \left\{ \log_2 \lambda_{\max} \left(\mathbf{I} + \mathbf{H}_{\mathbf{B}}(\mathbf{f}) \mathbf{H}_{\mathbf{B}}^{\mathbf{H}}(\mathbf{f}) \gamma, \mathbf{I} + \mathbf{H}_{\mathbf{E}}(\mathbf{f}) \mathbf{H}_{\mathbf{E}}^{\mathbf{H}}(\mathbf{f}) \gamma \right) \right\}^+ \end{aligned} \tag{7}$$

Therefore $\mathbf{H}_{\mathbf{opt}}(\mathbf{f})$ is the generalized eigenvector corresponding to the largest generalized eigenvalue of the matrix pair $\left(\mathbf{I} + \mathbf{H}_{\mathbf{B}}(\mathbf{f}) \mathbf{H}_{\mathbf{B}}^{\mathbf{H}}(\mathbf{f}) \gamma, \mathbf{I} + \mathbf{H}_{\mathbf{E}}(\mathbf{f}) \mathbf{H}_{\mathbf{E}}^{\mathbf{H}}(\mathbf{f}) \gamma \right)$. $\mathbf{H}_{\mathbf{opt}}(\mathbf{f})$ involves Bob and Eves CSI ($\mathbf{H}_{\mathbf{B}}(\mathbf{f})$ and $\mathbf{H}_{\mathbf{E}}(\mathbf{f})$) and SNR ($\gamma$), thus making the entire communication system secrecy capacity achievable.

$$C_S = \left\{\log_2 \lambda_{\max}\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})\gamma, \mathbf{I} + \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\gamma\right)\right\}^+ \tag{8}$$

In the following, we imitate the asymptotic results in [18] and present the corresponding asymptotic analysis of secrecy capacity.

Corollary 1 *In high SNR regime, the asymptote of secrecy capacity is*

$$\lim_{\gamma\to\infty} C_S = \left\{\log \lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f}), \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)\right\}^+ \tag{9}$$

Proof

$$\begin{aligned}
\lim_{\gamma\to\infty} C_S &= \lim_{\gamma\to\infty}\left\{\log_2 \lambda_{\max}\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})\gamma, \mathbf{I} + \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\gamma\right)\right\}^+ \\
&= \lim_{\gamma\to\infty}\left\{\log_2\left(\frac{1 + \left|\mathbf{H_B}(\mathbf{f})\mathbf{H_{opt}}(\mathbf{f})\right|^2\gamma}{1 + \left|\mathbf{H_E}(\mathbf{f})\mathbf{H_{opt}}(\mathbf{f})\right|^2\gamma}\right)\right\}^+ \\
&= \left\{\log_2\left(\frac{\left|\mathbf{H_B}(\mathbf{f})\mathbf{H_{opt}}(\mathbf{f})\right|^2}{\left|\mathbf{H_E}(\mathbf{f})\mathbf{H_{opt}}(\mathbf{f})\right|^2}\right)\right\}^+ \\
&= \left\{\log_2 \lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f}), \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)\right\}^+
\end{aligned} \tag{10}$$

Now the proof is complete. □

Corollary 2 *In low SNR regime, the asymptote of secrecy capacity is*

$$\lim_{\gamma\to-\infty} \frac{C_S}{\gamma} = \frac{1}{\ln 2}\left\{\lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f}) - \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)\right\}^+ \tag{11}$$

Proof We assume the power of transmit signal and noise are P and 1, respectively. So when SNR goes to infinitely small quantity, P will approach 0, i.e.

$$\lim_{\gamma\to-\infty} \overset{\Delta}{=} \lim_{P\to 0}. \tag{12}$$

Then,

$$\begin{aligned}
\lim_{\gamma\to-\infty} C_S &= \lim_{\gamma\to-\infty}\left\{\log_2 \lambda_{\max}\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})\gamma, \mathbf{I} + \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\gamma\right)\right\}^+ \\
&\overset{\Delta}{=} \lim_{P\to 0}\left\{\log_2 \lambda_{\max}\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})P, \mathbf{I} + \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})P\right)\right\}^+ \\
&= \lim_{P\to 0}\left\{\log_2 \lambda_{\max}\left(\left(\mathbf{I} + \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})P\right)^{-1}\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})P\right)\right)\right\}^+ \\
&= \lim_{P\to 0}\left\{\log_2 \lambda_{\max}\left(\left(\mathbf{I} - \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})P + O(P)\right)\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})P\right)\right)\right\}^+ \\
&= \lim_{P\to 0}\left\{\log_2 \lambda_{\max}\left(\left(\mathbf{I} - \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})P\right)\left(\mathbf{I} + \mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})P\right) + O(P)\right)\right\}^+ \\
&= \lim_{P\to 0}\left\{\log_2 \lambda_{\max}\left(\mathbf{I} + \left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f}) - \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)P + O(P)\right)\right\}^+ \\
&= \lim_{P\to 0}\left\{\log_2\left(1 + \lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f}) - \mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)P + O(P)\right)\right\}^+
\end{aligned} \tag{13}$$

where $O(P)$ represents one order of infinitesimals of P, i.e.

$$\lim_{P\to 0}\frac{O(P)}{P}=0 \tag{14}$$

Then,

$$\begin{aligned}\lim_{\gamma\to-\infty}\frac{C_S}{\gamma}&=\lim_{P\to 0}\frac{C_S}{P}\\&=\lim_{P\to 0}\left\{\frac{\log_2\left(1+\lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})-\mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)P+O(P)\right)}{P}\right\}^+\\&=\lim_{P\to 0}\left\{\frac{\lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})-\mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)}{\ln 2}+\frac{O(P)}{LP}\right\}^+\\&=\frac{1}{\ln 2}\left\{\lambda_{\max}\left(\mathbf{H_B}(\mathbf{f})\mathbf{H_B^H}(\mathbf{f})-\mathbf{H_E}(\mathbf{f})\mathbf{H_E^H}(\mathbf{f})\right)\right\}^+\end{aligned} \tag{15}$$

Now the proof is complete. □

4 Simulation Results

In this section, Monte Carlo simulations are carried out to evaluate the secure performance of the proposed TR pre-filter in HIPERLAN/2 BranA channel.

Figure 2 gives out the achievable transmission rate for Bob and Eve using the proposed and shielding Eve TR pre-filters, respectively. We discover that the shielding Eve TR pre-fiter totally isolates Eve at the cost of Bob's transmission rate. In contrast, although the proposed TR pre-filter cannot guarantee the complete elimination of Eve, it improves Bob's transmission rate performance, which will contribute to a higher secrecy rate.

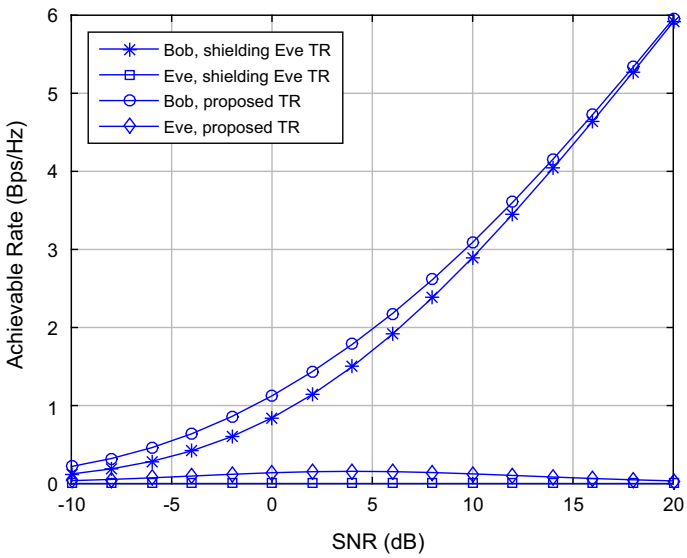

Fig. 2 Transmission performance comparisons between the proposed and shielding Eve TR pre-filter

In Fig. 3, the secure performance comparisons (the transmission rate difference of Bob and Eve) involving the classical, shielding Eve and the proposed TR pre-filters are presented when $M_T = 2$, $M_R = 1$, $M_E = 1$. In this scenario, the proposed TR pre-filter outperforms the classical and shielding Eve TR pre-filters in the achievable secrecy rate. And more importantly, although the proposed TR pre-filter cannot isolate Eve from interception complectly as shielding Eve TR pre-filter does, it is superior to shielding Eve TR pre-filter in terms of secure performance by nearly achieving secrecy capacity.

We conclude that, all the TR pre-filters (classical, shielding Eve and the proposed TR) can provide efficient and secure transmission in different levels. More specifically,

1. in terms of Bob's transmission efficiency, the classical TR pre-filter is the best of the three pre-filters since it matches with the frequency selective channel;
2. while from the perspective of the secure performance, the proposed TR pre-filter is the optimal as it achieves the secrecy capacity.

5 Unequal Secrecy Protection MISO Broadcast Configuration

In this section, we will propose a UESP MISO broadcast configuration to meet the unequal secrecy protection requirement for wireless mobile users (Table 2).

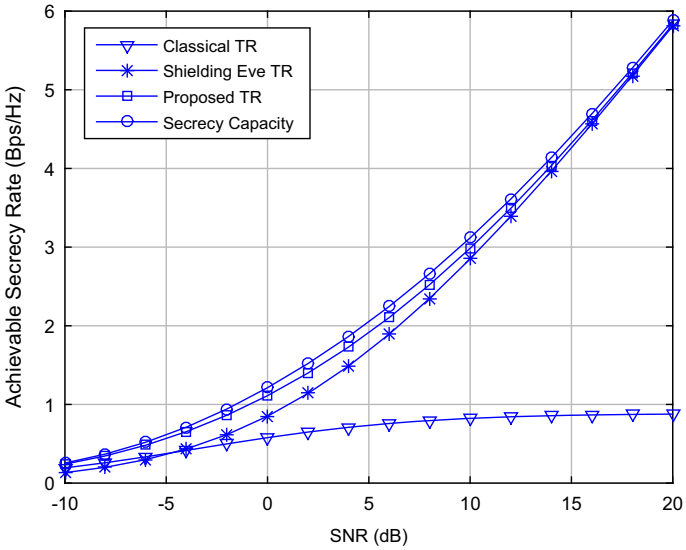

Fig. 3 Secure performance comparisons of the TR pre-filters

Table 2 Time Reversal Based Unequal Protection MISO Broadcast Configuration

Message category	Pre-filter Type
Public message	No TR pre-filter
Private message	Classical TR Pre-filter
Confidential message	Secrecy capacity achievable TR Pre-filter

1. To start with, public messages are meant to be received by all the legal mobile users in the wireless communication configuration, i.e. radio programmes about the traffic conditions. Thus no TR pre-filters are needed to make sure the full coverage of public messages.
2. Furthermore, private messages are often subscribed by specific mobile users for personal conversation and business contracts. We claim that privacy should always be guaranteed. But for private messages, the transmission efficiency issue should also be involved in consideration. So we select the classical TR pre-filter to meet the dual requirements of both efficiency and secrecy.
3. Ultimately, secrecy performance is the most primary factor for the wireless transmission of confidential messages. So we select the secrecy capacity achievable TR pre-filter for confidential messages transmission to offer the optimal physical layer security protection.

6 Conclusions

In this paper, an optimal TR pre-filter is proposed to achieve secrecy capacity in frequency selective channels for MISO wireless communication applications. Simulation results show that the proposed TR is superior to classical and shielding Eve TR pre-filters in terms of secrecy performance. Furthermore, we construct a UESP MISO broadcast configuration by exploiting the aforementioned classical and secrecy capacity achievable TR pre-filters, so that three levels of hierarchical services in terms of public, private and confidential messages can be offered for the 5G wireless communication systems in the near future.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant Nos. 61502518, 61501479 and 61372098).

References

1. Stallings, W. (2006). *Cryptography and network security principles and practices*. Englewood Cliffs: Prentice Hall PTR.
2. Bloch, M., & Barros, J. (2011). *Physical-layer security: From information theory to security engineering*. Cambridge: Cambridge University Press.
3. Shiu, Y.-S., Chang, S. Y., Hsiao-Chun, W., Huang, S. C.-H., & Chen, H.-H. (2011). Physical layer security in wireless networks: A tutorial. *IEEE Wireless Communications*, *18*(2), 66–74.
4. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal*, *28*(4), 656715.
5. Mukherjee, A., & Swindlehurst, A. L. (2011). Robust beamforming for security in MIMO wiretap channels with imperfect CSI. *IEEE Transactions on Signal Processing*, *59*(1), 351–361.
6. Goel, S., & Negi, R. (2008). Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, *7*(6), 21802189.
7. Kaiser, T., & Zheng, F. (2010). *Ultra wideband systems with MIMO*. New York: Wiley.
8. Romero-Zurita, N., Ghogho, M., & McLernon, D. (2011). Physical layer security of MIMO OFDM systems by beamforming and artificial noise generation. *Physical Communication*, *4*(4), 313–321.
9. Yan, C., Yu-Han, Y., Feng, H., & Ray, L. (2013). Time-reversal wideband communications. *IEEE Signal Processing Letters*, *20*(12), 1219–1222.
10. Fink, M. (1999). Time-reversed acoustic. *Scientific American*, *281*(5), 91–97.
11. Fink, M. (1992). Time reversal of ultrasonic fields. Part I: Basic principles. *IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control*, *39*(5), 555–566.

12. Rouseff, D., Jackson, D. R., Fox, W. L. J., Jones, C. D., Ritcey, J. A., & Dowling, D. R. (2001). Underwater acoustic communication by passive-phase conjugation: Theory and experimental results. *IEEE Journal of Oceanic Engineering*, *26*(4), 821–831.
13. Nguyen, H. T., Kovacs, I. Z., & Eggers, P. C. F. (2006). A time reversal transmission approach for multiuser UWB communications. *IEEE Transactions on Antennas and Propagation*, *54*(11), 3216–3224.
14. Yan, C., Beibei, W., Yi, H., Hung-Quoc, L., Zoltan, S., & Ray, L. (2016). Why time reversal for future 5G wireless? *IEEE Signal Processing Magazine*, *33*(2), 17–26.
15. Kyritsi, P., Papanicolaou, G., Eggers, P., & Oprea, A. (2004). MISO time reversal and delay-spread compression for FWA channels at 5 GHz. *IEEE Antennas and Wireless Propagation Letters*, *3*(1), 96–99.
16. Henty, B. E., & Stancil, D. D. (2004). Multipath enabled super-resolution for RF and microwave communication using phase-conjugate arrays. *Physical Review Letters*, *93*(24), 11945–11945.
17. Beibei, W., Yongle, W., Feng, H., Yu-Han, Y., & Ray, L. (2011). Green wireless communications: A time-reversal paradigm. *IEEE Journal on Selected Areas in Communications*, *29*(8), 1698–1710.
18. Fouda, A. E., Teixeira, F. L., & Yavuz, M. E. (2012). Time-reversal techniques for MISO and MIMO wireless communication systems. *Radio Science*, *47*, RS0P02.
19. Khisti, A., & Wornell, G. W. (2010). Secure transmission with multiple antennas I: The MISOME wiretap channel. *IEEE Transactions on Information Theory*, *56*(7), 3088–3104.
20. Ahmad, S., Hamzaoui, R., & Al-Akaidi, M. (2011). Unequal error protection using fountain codes with applications to video communication. *IEEE Transactions on Multimedia*, *13*(1), 92–101.
21. Wyner, A. D. (1975). The wiretap channel. *Bell Labs Technical Journal*, *54*(8), 1355–1387.

Wei Cao received his B.S. and M.S. from National University of Defense Technology (NUDT) in Changsha, China, in 2012 and 2014, respectively. He is currently a Ph.D student in Information and Communication Engineering in the Automatic Target Recognition (ATR) Key Lab, College of Electronic Science and Engineering, NUDT. His research interests include passive bistatic radar, multi-carrier modulation techniques and physical layer security.

Jing Lei received her B.S., M.S. and Ph.D. degree in Communication Engineering in the National University of Defense Technology (NUDT) in Changsha, China, in 1990, 1994 and 2009, respectively. She is a professor in the Department of Communications Engineering, College of Electronic Science and Engineering as well as a group head in Communication Experiment Center in NUDT. She was a visiting scholar in the School of Electronics and Computer Science, University of Southampton, U.K in 2014. Her researching interests include information theory, correction coding, wireless communication system and physical layer security.

Weidong Hu was born in September 1967. He received the B.S. degree in microwave technology and the M.S. and Ph.D. degrees in communication and electronic system from the National University of Defense Technology, Changsha, China, in 1990, 1994, and 1997, respectively. He is currently a Full Professor with the ATR Laboratory, National University of Defense Technology, Changsha. His research interests include radar signal and data processing.

Wei Li received the B.Sc. (first class) degree, M.Sc. degree and Ph.D. degree in Communication Engineering from the National University of Defense Technology (NUDT), Changsha, P.R. China, in 2002, 2006, and 2012, respectively. He is currently a lecturer in the Department of Communication Engineering of NUDT. He was awarded the exemplary reviewer of IEEE communications letters in 2014. His research interests include wireless communications, wireless network resource allocation, and physical layer security.