2018 IEEE Wireless Communications and Networking Conference (WCNC)

Artificial Noise Inserted Secure Communication in Time-Reversal Systems

Si Li*†, Na Li*†, Xiaofeng Tao*, Zunning Liu*, Haowei Wang*, and Jin Xu*
*National Engineering Lab for Mobile Network Technologies,
Beijing University of Posts and Telecommunications, Beijing, 100876, China
†Beijing University of Posts and Telecommunications Research Institute, Shenzhen, China
Email: lis@bupt.edu.cn

***Abstract*—Artificial noise (AN) assisted secure communication is a promising technique in the area of physical layer security. In this paper, we propose a new AN method to enhance the secrecy performance of a time reverse (TR) transmission system. Based on the proposed AN model, we first derive the closed-form secrecy rate, whose accuracy is verified through simulations. Then using it as an objective function, we further study the power allocation issue between useful information signals and the AN with the aid of maximizing the secrecy rate. The optimal power allocation is first derived in closed form and then analyzed in some special cases such as Rayleigh channel. Analytical and simulation results show that the secrecy performance can be considerably improved by over 10% even with a small amount of AN. And when there are less multi-paths in the channel or when the transmit power is small, more power for AN is required.**

***Index Terms*—Physical layer security, Time-reversal, artificial noise, power allocation.**

I. Introduction

Time reversal (TR) technique, which is from underwater sound and ultrasound communications [1]–[3], has been extended to the wireless communication in recent years since this technique can make full use of multi-path propagation while requires no complicated channel measurements and estimation [4]. It can realize a focus of wireless signals in both space and time domain. [5] showed that the TR technique can improve the energy efficiency of the wireless transmission and prolong the battery life of terminal devices in green Internet of Things (IoT). [6] demonstrated TR is an approach which can address communication problems in heterogeneous bandwidths. [7] investigated the power transfer gain of power transfer system over regular TR system. Similar channel estimation error distribution between the TR and massive multiple input multiple output (MIMO) system was revealed in [8].

On the other hand, as information security has become an important concern, substantial attention has been devoted to physical layer security [9]–[11]. It prevents eavesdropping by exploiting the imperfection of communication channels to realize secure transmission between the transmitter and the legitimate receiver. One important approach in physical layer security is the artificial noise (AN) assisted transmission which masks the communication between legitimate nodes with an artificially generated noise. It was first introduced by Negi and Goel [12], and has been extensively studied in beamforming [13], training schemes for channel estimation [14], massive MIMO system [15] and small cell networks [16]. And when AN is used, power allocation (PA) between information signals and the AN is an important design parameter [17]. Sub-optimal PA algorithms were proposed in [18]. Further researches were carried out in [19]–[21], where the optimal PA was obtained based on the closed-form expression of the ergodic secrecy rate. In these works, the AN is usually generated using multiple antennas or cooperative helpers, with the assumption that the eavesdropper has limited amount of spatial degrees to eliminate the AN. At the same time, several works proposed the time-domain AN method which utilizes the time diversity instead of the conventional spatial diversity to insert AN into the transmit signals. In [22], a time domain AN method was proposed for orthogonal frequency division multiplexing (OFDM) systems. And time domain AN was designed in [23] to achieve the optimal resource allocation for orthogonal frequency division multiple access (OFDMA) systems with simultaneous wireless information and power transfer (SWIPT).

The secure communication issue in TR systems has also been studied by a handful of works [24]–[26]. The signal-to-interference-plus-noise ratio (SINR) was studied to evaluate the secrecy performance of correlated multi-path channel [25]. And [26] analyzed the signal-to-noise ratio (SNR) at the intended and unintended receivers of distributed time reversal (DTR) transmission, demonstrating that the TR transmission can improve the secrecy performance. The time and space focusing characteristic of TR technique makes TR technique an ideal candidate paradigm for time domain AN. At the same time, the TR system is of less complexity compared to the OFDM system as a technique against multi-path channel fading. However, to our best knowledge, no study has been done on introducing AN to TR transmissions.

Motivated by aforementioned reasons, we propose an AN-inserted TR transmission method where AN is designed to jam the eavesdroppers while impacting on legitimate receivers as little as possible.

The contributions of the paper are as follows.

- First, for the TR transmission system, we propose an AN inserted method where the AN can confuse eavesdroppers while has little interference to legitimate receivers. This is the first time that an artificial noise approach is introduced into the TR transmission.

978-1-5386-1734-2/18/$31.00 ©2018 IEEE

- Second, we derive the closed-form expression of secrecy rate for the proposed method. In fact, it is a no complicated math problem which indicates a low complexity for realization. Furthermore, simulations demonstrate the accuracy of the expression.
- Third, based on the derived secrecy rate, we study the optimal power allocation to optimize the secrecy performance. Several special cases are also discussed to show the relationship between the optimal power allocation factor and parameters such as the number of multi-path and the transmitted power. We find that when there are less multi-paths in the channel or when the transmitted power is small, more power for AN is required.

The rest of the paper is organized as follows. Section II describes the system model where we derive the closed-form secrecy rate for the proposed method. Section III investigates the power allocation issue. Section IV presents simulations to verify our analysis. Section V concludes the paper.

II. System Model

We consider a broadcast channel which consists of a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve). All three nodes are equipped with single antenna as depicted in Fig. 1. The channels between the transmitter, Alice, and the receivers are slow fading multi-path channels. At the same time, a root raised cosine (RRC) filter is assumed to exist at both Bob and Eve, which is independent with the channel. Taking the receiver RRC filter response $p(t)$ as a part of the channel impulse response (CIR), the CIR is modeled in continuous time domain as

$$h_j(t) = \sum_{i=0}^{L} h_{j,i} p(t - \tau_{j,i}), \tag{1}$$

where $j \in \{b, e\}$, b and e denote Bob and Eve respectively. $h_{j,i}$ denotes the complex amplitude of the $i-th$ tap which is modeled as i.i.d. complex Gaussian variables, i.e., $h_{b,i} \sim CN(0, \sigma_B^2)$, $h_{e,i} \sim CN(0, \sigma_E^2)$. Similarly, $\tau_{j,i}$ is the time delay of the $i-th$ tap, which follows i.i.d. truncated exponential distributions within $(0, T_p)$, where T_p is the maximum multi-path delay. $p(t)$ is the impulse response of the root raised-cosine receiver filter with $\int_{-\infty}^{\infty} |p(t)|^2 dt = 1$, and $L+1$ is the number of channel taps. All channel taps are assumed to be constant during a coherence time T and change independently from one duration to another. For analytical convenience, the CIRs of different receivers are assumed to be independent with each other.

Prior to the transmission, Bob sends out a delta-like pilot pulse, which propagates through the multi-path channel to Alice which records the received waveforms and uses its normalized time-reversed conjugated version as the base waveform for information transmission, i.e.,

$$g(t) = E^{-1/2} \sum_{i=0}^{L} h_{b,i}^* p(T_p - t), \tag{2}$$

where $h_{b,i}^*$ denotes the conjugation of $h_{b,i}$,

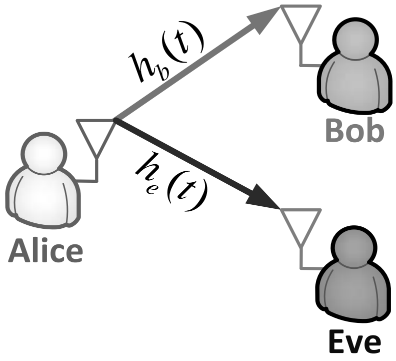

Fig. 1. System model

$$\begin{aligned} E &= \mathbf{E}\left\{\int_{-\infty}^{\infty} |h_b(t)|^2 dt\right\} \\ &= (L+1)\sigma_B^2, \end{aligned} \tag{3}$$

which is the energy of $h_b(t)$ and $\mathbf{E}$ denotes expectation.

To enhance the secrecy performance, we introduce a precode method for AN. Based on the CIR of Bob's channel, the normalized base waveform is given by

$$g_a(t) = {E_a}^{-1/2} \sum_{i=0}^{L} u_i p(T_p - t), \tag{4}$$

where

$$\begin{aligned} E_a &= \mathbf{E}\left\{\int_{-\infty}^{\infty} \left|\sum_{i=0}^{L} n_i p(t - \tau_i)\right|^2 dt\right\} \\ &= (L+1)\sigma_{an}^2, \end{aligned} \tag{5}$$

where u_i is the equivalent tap gain for AN which is distributed with Rayleigh fading whose mean is zero as well, i.e., $u_i \sim CN(0, \sigma_{an}^2)$, each u_i is a random variable which is independent with $h_{b,i}$. Without of generality, we set $\sigma_{an}^2 = \sigma_B^2$, i.e., $E_a = E$. To offset the effect of artificial noise at Bob farthest, u_i is designed as

$$\sum_{i=0}^{L} (h_{b,i} u_i) = 0. \tag{6}$$

For a given transmitted power P, we assume that a_m is the Quadrature Amplitude Modulation (QAM) data symbol, b_m is the AN symbol drawing from the complex Gaussian distribution and $P_s \triangleq \mathbf{E}\left\{|a_m|^2\right\}$, $P_b \triangleq \mathbf{E}\left\{|b_m|^2\right\}$. Therefore P=P_s+P_b. The transmitted signal from Alice can be described as

$$s(t) = \sum_{-\infty}^{\infty} [a_m g(t - mT) + b_m g_a(t - mT)]. \tag{7}$$

The received signals at Bob and Eve are denoted as $d(t)$ and $e(t)$, respectively,

$$\begin{aligned} d(t) &= s(t) * h_b(t) + n(t), \\ e(t) &= s(t) * h_e(t) + n_e(t), \end{aligned} \tag{8}$$

where $*$ denotes discrete convolution, $n(t)$ and $n_e(t)$ are additive Gaussian random processes, and at any time the noise follows $CN(0, \sigma_n^2)$. Let $q(t)$ denote the received pulse of the information symbol at Bob, $q_a(t)$ denote the received pulse of the AN symbol at Bob, the expressions of $q(t)$ and $q_a(t)$ are shown next as

$$q(t) \triangleq g(t) * h_b(t), \tag{9}$$

$$q_a(t) \triangleq g_a(t) * h_b(t). \tag{10}$$

Similarly we can get the received pulse for the information symbol and the AN symbol, respectively at Eve, i.e., the expressions of $q_e(t)$ and $q_{e,a}(t)$ are shown next as

$$q_e(t) \triangleq g(t) * h_e(t), \tag{11}$$

$$q_{e,a}(t) \triangleq g_a(t) * h_e(t). \tag{12}$$

Then $d(t)$ and $e(t)$ can also be expressed as

$$d(t) = \sum_{-\infty}^{\infty} [a_m q(t-mT) + b_m q_a(t-mT)] + n(t),$$
$$e(t) = \sum_{-\infty}^{\infty} [a_m q_e(t-mT) + b_m q_{e,a}(t-mT)] + n_e(t).$$

It should be stressed that at the time $t = T_p$, the pulse at Bob reaches the peak of the power. For the $m-th$ QAM symbol, the ensemble received signal at Bob is denoted as

$$y_b(T_p) = a_m q(T_p) + b_m q_a(T_p). \tag{13}$$

While the pulse at Eve doesn't have this characteristic, so Eve samples at time T_e which is arbitrary. The sampling instants at Bob and Eve are t_l and $t_l{}^{(e)}$, respectively

$$t_l = T_p + lT,$$
$$t_l{}^{(e)} = T_e + lT.$$

We analyze the received signal at one sampling slot, after the sampling process, the received signal except for channel noise for the $m-th$ QAM symbol can be expressed as

$$y_e(T_e) = a_m q_e(T_e) + b_m q_{e,a}(T_e). \tag{14}$$

The general expression of SNR at Bob is

$$SNR_d = \frac{\mathbf{E}\left\{|a_m q(T_p)|^2\right\}}{\sigma_n^2 + \mathbf{E}\left\{|b_m q_a(T_p)|^2\right\}}, \tag{15}$$

where $\mathbf{E}\left\{|a_m q(T_p)|^2\right\}$ and $\mathbf{E}\left\{|b_m q_a(T_p)|^2\right\}$ are the average powers of information symbols and AN symbols, respectively.

The SNR at Eve is accordingly expressed as

$$SNR_e = \frac{\mathbf{E}\left\{|a_m q_e(T_e)|^2\right\}}{\sigma_n^2 + \mathbf{E}\left\{|b_m q_{e,a}(T_e)|^2\right\}}. \tag{16}$$

Similar as the foregoing SNR_d, $\mathbf{E}\left\{|a_m q_e(T_e)|^2\right\}$ and $\mathbf{E}\left\{|b_m q_{e,a}(T_e)|^2\right\}$ denote the average powers of information symbols and AN symbols, respectively.

***Theorem** 1: The closed-form expression of SNR_d is*

$$SNR_d = \frac{P_s \beta^2 \sigma_B^4 [(L+1)(L+L\rho+2)]}{\sigma_n{}^2 + P_b \beta^2 \sigma_B^2 \sigma_{an}^2 L(L+1)\rho}, \tag{17}$$

where ρ can be explained in the proof section, $\beta \triangleq \frac{1}{\sqrt{E}}$.

Proof: According to (9), we have

$$\begin{aligned} q(T_p) &= \sum_{i=0}^{L}\sum_{l=0}^{L} \frac{h_{b,i}h_{b,l}{}^*}{\sqrt{E}} \int_{-\infty}^{\infty} p(v-\tau_i)p^*(v-\tau_l)dv \\ &= \frac{1}{\sqrt{E}} \int_{-\infty}^{\infty} \left| \sum_{i=0}^{L} h_{b,i} p(v-\tau_i) \right|^2 dv. \end{aligned} \tag{18}$$

Then we can derive

$$\mathbf{E}\left\{|a_m q(T_p)|^2\right\} = P_s \beta^2 \sigma_B^4 \Big[(L{+}1)(L{+}2){+}\sum_{i1\neq i2}^{L} \rho\Big] \tag{19}$$

following the method introduced in [26], where $\rho{=}\mathbf{E}_\tau\left\{|R_p(\tau_{i1}-\tau_{i2})|^2\right\}$, which is the average value by τ.

According to (6),

$$\sum_{i=l} h_{b,i} u_l \int_{-\infty}^{\infty} |p(\lambda_i)|^2 dv = \sum_{i=l} h_{b,i} u_l = 0, \tag{20}$$

where $\lambda_i \triangleq v - \tau_i$, $\omega_j \triangleq v - \tau_j$. Then according to (10), we have

$$\begin{aligned} q_a(T_p) &= \frac{1}{\sqrt{E_a}} \left(\sum_{i\neq l} h_i u_l \int_{-\infty}^{\infty} p(\lambda_i)p^*(\omega_j)dv \right. \\ &\qquad \left. + \sum_{i=l} h_i u_l \int_{-\infty}^{\infty} |p(\lambda_i)|^2 dv \right) \\ &= \frac{1}{\sqrt{E_a}} \sum_{i\neq l} h_i u_l \int_{-\infty}^{\infty} p(\lambda_i)p^*(\omega_j)dv, \end{aligned} \tag{21}$$

where due to the power peak when $i = l$, most part of AN has been offset at Bob while AN can interfere Eve severely. Then we have

$$\mathbf{E}\left\{|b_m q_a(T_p)|^2\right\} = P_b \beta^2 \sigma_B^2 \sigma_{an}^2 \sum_{i1\neq i2}^{L} \rho. \tag{22}$$

For $\tau_{i1} \neq \tau_{i2}$, ρ can be calculated as

$$\rho{=}\int_0^{T_p} 2 f_\delta(x) |R_p(x)|^2 dx, \tag{23}$$

where

$$R_p(\tau_1{-}\tau_2) = \int_v p(v-\tau_1)p^*(v-\tau_2)dv,$$

and the probability density function of $\delta{=}\tau_{i1} - \tau_{i2}$ is symmetric,

$$\begin{aligned} f_\delta(x) &= \int_0^{T_p} p_{\tau_i}(x+\tau)\, p_{\tau_i}(\tau) d\tau, \quad |x| < T_p \\ &= \frac{e^{-T_p/T_0}}{T_0\left(1-e^{-T_p/T_0}\right)^2} \cdot \sinh\left(\frac{T_p - |x|}{T_0}\right),\ |x| < T_p \end{aligned} \tag{24}$$

where $T_0 \to \infty$.

After substituting parameters in (19), (22) and (15), the closed-form SNR_d can be expressed as (17). ■

***Theorem** 2: The close form expression of SNR_e is*

$$SNR_e = \frac{P_s \beta^2 \sigma_B^2 \sigma_E^2 (L+1)^2 \rho_e}{\sigma_n^2 + P_b \beta^2 \sigma_{an}^2 \sigma_E^2 (L+1)^2 \rho_e}, \tag{25}$$

where ρ_e can be explained in the proof section.

Proof: According to (11), (12),

$$q_e(T_e) = \sum_{i=0}^{L} \sum_{l=0}^{L} \frac{h_{e,i} h_{b,l}^*}{\sqrt{E}} \int_{-\infty}^{\infty} p(v - \tau_{e,i}) p^*(T_p - T_e + v - \tau_l) dv, \tag{26}$$

where the power peak doesn't exist compared to (18).

$$q_{e,a}(T_e) = \sum_{i=0}^{L} \sum_{l=0}^{L} \frac{h_{e,i} u_l}{\sqrt{E_a}} \int_{-\infty}^{\infty} p(v - \tau_{e,i}) p^*(T_p - T_e + v - \tau_l) dv, \tag{27}$$

where the peak value of AN can not be offset compared to (21) as aforementioned.

Then we can get

$$\mathbf{E}\left\{ |a_m q_e(T_e)|^2 \right\} = P_s \beta^2 \sigma_B^2 \sigma_E^2 (L+1)^2 \rho_e, \tag{28}$$

$$\mathbf{E}\left\{ |b_m q_{e,a}(T_e)|^2 \right\} = P_b \beta^2 \sigma_{an}^2 \sigma_E^2 (L+1)^2 \rho_e, \tag{29}$$

following the method in [26].

$$\begin{aligned} \rho_e &= \mathbf{E}_\tau \left\{ |R_p(T_p - T_e - \tau_j + \tau_{e,i})|^2 \right\} \\ &= \int_{-T_p}^{T_p} f_\delta(x) |R_p(T_p - T_e + x)|^2 dx. \end{aligned} \tag{30}$$

After substituting parameters to (28), (29) and (16), the closed-form SNR_e can be expressed as (25). ■

Now we can use the secrecy rate R_s to evaluate the performance of the AN-inserted method after substituting parameters to the equation next as

$$R_s = [\log_2(1 + SNR_d) - \log_2(1 + SNR_e)]^+, \tag{31}$$

where $[x]^+$ denotes the max value between x and 0, SNR_d and SNR_e are the SNR at the legislate receiver and the eavesdropper, respectively.

III. Power Allocation

In section II, AN symbols are inserted to the TR-transmission system. To further investigate the relation between the AN's share and the secure performance. We consider about the power allocation between the information symbols and AN symbols

Without loss of generality, we let $\sigma_B^2 = \sigma_E^2$. Set $P_s = \varphi P$, $P_b = (1-\varphi)P$, where φ is the power allocation factor for P_s. We can rewrite the SNR expressions of Rs as

$$SNR_d = \frac{\varphi A}{\sigma_n^2 + \varphi B}, \tag{32}$$

$$SNR_e = \frac{\varphi C}{\sigma_n^2 + (1-\varphi) C}, \tag{33}$$

where $A \triangleq P\beta^2\sigma_B^4[(L+1)(L+L\rho+2)]$, $B \triangleq P\beta^2\sigma_B^2\sigma_{an}^2 L(L+1)\rho$, $C \triangleq P\beta^2\sigma_B^2\sigma_E^2(L+1)^2\rho_e$.

The optimal power allocation factor maximizing the secrecy rate can be calculated numerically from our derived closed-form expression of Rs in Section II within the range that $0 < \varphi \leq 1$.

To gain more insights into the characteristic of φ, we consider the following two special situations:

CASE I : $T_p = T_e$, then $\rho = \rho_e$, therefore $C > B$. Let R denote $\frac{1+SNR_d}{1+SNR_e}$. We can get

$$\frac{\partial^2 R}{\partial^2 \varphi} = -\frac{2A(\sigma_n^2 + B)(C - B)}{[\sigma_n^2 + B(1-\varphi)]^3} < 0.$$

It can be confirmed that R is a concave function which has its optimal solution, which can be derived from $\frac{\partial R}{\partial \varphi} = 0$, i.e.

$$\begin{gathered} BC(A-B)\varphi^2 + 2C(\sigma_n^2 + B)(B - A)\varphi + \\ \left[(A - C)\sigma_n^2 + C(A - B)\right] \times (\sigma_n^2 + B) = 0. \end{gathered}$$

Then the optimal power allocation scalar is attained as

$$\varphi^* = \frac{-b - \sqrt{b^2 - 4ac}}{2a}, \tag{34}$$

where $a \triangleq BC(A-B)$, $b \triangleq 2C(\sigma_n^2 + B)(B - A)$, $c \triangleq \left[(A-C)\sigma_n^2 + C(A-B)\right] \times (\sigma_n^2 + B)$, whose optimality will be justified in the next section.

CASE II : When $L = 0$, which means multi-path is 1, i.e., there is merely one channel in Alice-Bob channel and Alice-Eve channel which is a Rayleigh fading channel. After substituting corresponding parameters to (34), we can give the φ^* as

$$\varphi^* = \frac{1}{2} + \frac{\sigma_n^2}{4P\sigma_B^2} k, \tag{35}$$

from which we can get the conclusion that

$$\lim_{P \to \infty} \varphi^* = 0.5, \tag{36}$$

which agrees with [20] which studied AN power allocation in Rayleigh channel.

IV. Simulation Results

The simulation results are presented to evaluate the performance of proposed AN inserted transmission system. Also, we justify the accuracy of the theoretical results shown in Section II and Section III.

It is assumed that the channel between Alice and Bob and that between Alice and Eve are independent with each other. The channel variances are σ_B^2 and σ_E^2 respectively with the

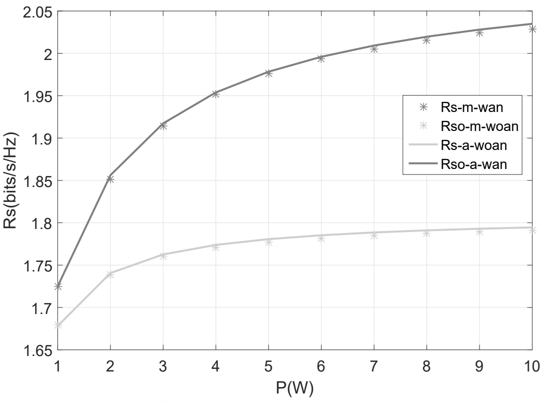

Fig. 2. Secrecy rate with regular TR system and AN-inserted system where T_e=T_p, $L = 3$. The legend "a" stands for analytical simulation results while the legend "m" stands for numerical results. The legend "woan" means without artificial noise while "wan" means with artificial noise.

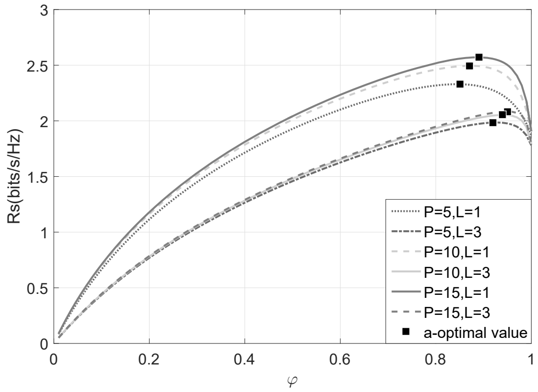

Fig. 3. Secrecy rate with different P where T_e=T_p, two bunches of lines shown in the figure are R_s curves when $L = 1$ and $L = 3$, respectively. The black rectangles denote the peak values of analytical results at φ^*.

same value $0.4mW$. And σ_n^2 is set as $0.1mW$. As discussed in Section II, T_e is an arbitrary value. We here set T_e=T_p.

In Fig. 2, we compare the secrecy rate of the proposed AN inserted TR transmission and the regular TR transmission [26]. The Monte Carlo simulations are obtained as the average values over 100000 channels and delay realizations. The system parameters are $P_s = 0.94P$, $L = 3$. The simulation curves match well with the analytical secrecy rates, which proves the accuracy of our derivations in (31). The slight mismatch mainly comes from the truncated RRC function. Moreover, the secrecy rate is significantly improved when AN is used. When P reaches $10W$, R_s approaches 2.05 bits/s/Hz, which is over 10% than the regular TR system. What's more, a stable increase of the gap shows up as the P grows. Therefore, we can verify that the proposed method with AN can improve the secrecy performance of TR-system considerably. What's more, the improvement is promoted with the increase of the transmitted power.

In Fig. 3, we compare the secrecy rate of the proposed AN inserted TR transmission with different multi-paths and transmitted powers. The Monte Carlo simulations are obtained as the average values over 100000 channels and delay realizations. The system parameters are $L = 1$ and $L = 3$ when $P = 5, 10, 15W$, respectively. The simulation peaks match well with the analytical φ^*, which proves the accuracy of our derivations in (31). Moreover, we find that with the growth of P, the corresponding R_s increases, which agrees with the trend in Fig. 2. Alice allocates less than 7% power to AN to achieve the optimal secure performance, which illustrates the efficiency of the proposed method.

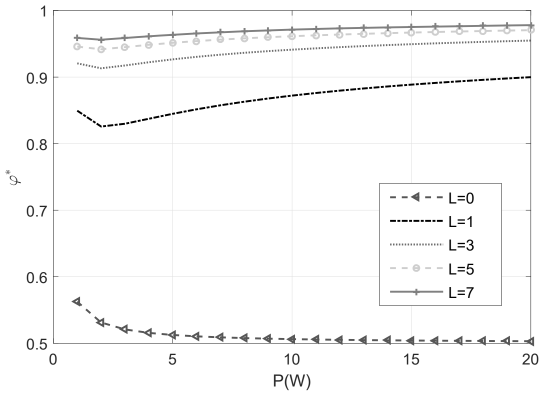

Fig. 4. Optimal φ with different P where T_e=T_p, $L = 0, 1, 3, 5, 7$.

In Fig. 4, we compare the optimal power allocation factors of the proposed AN inserted TR transmission with different transmitted powers. The Monte Carlo simulations are obtained as the average values over 100000 channels and delay realizations. The system parameters are T_e=T_p, $L = 0, 1, 3, 5, 7$. The optimal power allocation factor approaches 1 with the increase of transmitted power, which means when the number of multipath is comparatively small, the secrecy performance is better due to the serious interference of large amount of multi-path. Moreover, we find that when the transmitted power increases to a considerably high value, φ^* approaches 0.5, which agrees with the conclusion in (36) .

V. Conclusion

In this paper, we considered the performance of artificial noise inserted communication over TR transmission. We derived the the closed-form expressions of secrecy rate and the optimal power allocation factor. Moreover, the relationships between optimal power allocation and system parameters were investigated, which demonstrated that inserting AN method can improve the secrecy performance considerably. When there are less multi-paths in the channel or when the transmitted power is small, more power for AN is required. Furthermore, we verified the accuracy of analytical results with the aid of simulations.

Acknowledgement

This research was supported by the National Key Research and Development Program of China (2016YFB0800102), the National Natural Science Foundation of China under Grant No.61325006, 61601051), Shenzhen Science and Technology Innovation Commission Free Exploring Basic Research Project(JCYJ20170307172830043), and the 111 Project of China(B16006).

REFERENCES

[1] M. Fink, “Time reversed acoustics,” *Phys. Today*, pp. 34-40, 1997.

[2] D. R. Dowling and D. R. Jackson, “Phase conjugation in underwater acoustics,” *J. Acoust. Soc. Amer*, vol. 89, pp. 171-181, 1990.

[3] W. A. Kuperman, W. S. Hodgkiss, H. C. Song, T. Akal, C. Ferla, and D. R. Jackson, “Phase conjugation in the ocean: Experimental demonstration of an acoustic time-reversal mirror,” *J. Acoust. Soc. Amer*, vol. 103, pp. 25-40, 1998.

[4] B. Wang, Y. Wu, F. Han, Y. H. Yang, and K. J. R. Liu, “Green wireless communications: a time-reversal paradigm,” *IEEE J. Sel. Areas Commun.*, vol. 29, no. 8, pp. 1698-1710, Sept. 2011.

[5] Y. Chen, F Han and Y. H. Yang, “Time-Reversal wireless paradigm for green Internet of Things: an overview,” *IEEE Internet of Things Journal*, vol. 1, no. 1, pp.81-98, Feb. 2014.

[6] Y. Han, Y. Chen, B. Wang and K. J. Ray Liu, “Enabling heterogeneous connectivity in Internet of Things: a Time-Reversal approach,” *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1036-1047, 2016.

[7] M. L. Ku, Y. Han, H. Q. Lai, Y. Chen and K. J. R. Liu, “Power Waveforming: wireless power transfer beyond time reversal,” *IEEE Trans. Signal Process.*, vol. 64, no. 22, pp. 5819-5834, Nov. 2016.

[8] Z. H. Wu, B. Wang, C. Jiang and K. J. R. Liu, “Downlink MAC scheduler for 5G communications with spatial focusing effects,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 6, pp. 3968-3980, Jun. 2017.

[9] Y. Liang, H. V. Poor and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[10] Q. Yang, H. M. Wang, Y. Zhang and Z. Han, “Physical layer security in MIMO backscatter wireless systems,” *IEEE Trans. Wireless Commun.*, vol. 15, no. 11, pp. 7547-7560, Nov. 2016.

[11] J. H. Lee, “Optimal power allocation for physical layer security in multi-hop DF relay networks, ” *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 28-38, Jun. 2016.

[12] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, Jun. 2008.

[13] A. Mukherjee and A. L. Swindlehurst,“Robust beamforming for security in MIMO wiretap channels with imperfect CSI,” *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[14] T. H. Chang, W. C. Chiang, Y. W. P. Hong, and C. Y. Chi, “Training sequence design for discriminatory channel estimation in wireless MIMO systems,” *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223-6237, Dec. 2010.

[15] J. Zhu and R. Schober and V. K. Bhargava. “Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems.” *IEEE Trans. Wireless Commun.*, vol.15, no. 3, pp. 2245-2261, Mar. 2016.

[16] Wang, Wei, Kah Chan Teh, and Kwok Hung Li. “Artificial Noise Aided Physical Layer Security in Multi-Antenna Small-Cell Networks.” *IEEE Trans. Inf. Forensics Security,* vol. 12, no. 6, pp. 1470-1482, Jun. 2017.

[17] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831-3842, Oct. 2010.

[18] L. Dong and H. Yousefi’zadeh and H. Jafarkhani, “Cooperative jamming and power allocation for wireless relay networks in Presence of Eavesdropper,” *IEEE International Conference on Communications (ICC).*, pp. 1-5, Jun. 2011.

[19] T. X. Zheng and H. M. Wang, “Optimal Power Allocation for Artificial Noise Under Imperfect CSI Against Spatially Random Eavesdroppers,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 8812-8817, Oct. 2016.

[20] N. Li, X. F. Tao, and H. C. Wu, “Large-System analysis of Artificial-Noise-Assisted Communication in the multiuser downlink: ergodic secrecy sum rate and optimal power allocation,” *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7036-7050, Sept. 2016.

[21] S. H. Tsai and H. V .Poor, “Power allocation for Artificial-Noise secure MIMO precoding systems,” *IEEE Trans. Signal Process*, vol. 62, no. 13, pp. 3479-3493, July. 2014.

[22] H. Qin, Y. Sun, T. H. Chang, X. Chen, C. Y. Chi, M. Zhao, and J. Wang, “Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs,” *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717-2729, Jun. 2013.

[23] M. Zhang, Y. Liu, and R. Zhang, “Artificial noise aided secrecy information and power transfer in OFDMA systems,” *IEEE Trans. Wireless Commun*, vol. 15, no. 4, pp. 3085-3096, Apr. 2016.

[24] V. T. Tan and D. B. Ha and D. D. Tran, “Evaluation of physical layer secrecy in MIMO Ultra-WideBand system using Time-Reversal techniques,” *International Conference on Computing, Management and Telecommunications (ComManTel).*, pp. 70-74, April. 2014.

[25] H. V. Tran, H. Tran, G. Kaddoum, D. D. Tran and D. B. Ha, “Effective secrecy-SINR analysis of time reversal-employed systems over correlated multi-path channel Sign In or Purchase,” *IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob).*, pp. 527-532, 2015.

[26] L. Wang, R. Li, C. Cao, and G. Stuber, “SNR analysis of time reversal signaling on target and unintended receivers in distributed transmission,” *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2176-2191, May. 2016.