On the Target Secrecy Rate for SISOME Wiretap Channels

Shihao Yan, Giovanni Geraci, Nan Yang, Robert Malaney, and Jinhong Yuan
School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia

Abstract—We propose a new framework for optimizing the target secrecy rate for SISOME wiretap channels when the instantaneous capacity of the eavesdropper’s channel is not available at the transmitter. In our framework, we introduce the effective secrecy throughput, a new optimization metric that implicitly captures the two key features of wiretap channels, namely, reliability and secrecy. We derive target secrecy rates which maximize the effective secrecy throughput for two different schemes, an on-off transmission scheme and an adaptive transmission scheme. Our analysis demonstrates that the adaptive transmission scheme outperforms the on-off transmission scheme and that the difference in the effective secrecy throughput between the two schemes increases with the SNR of the main channel. The work reported here solves the important problem of how to optimally set the target secrecy rate of wiretap codes for an important class of channels. Notably, our solution for the target secrecy rate does not require us to set a priori any reliability or secrecy constraint for the channel.

I. INTRODUCTION

Physical layer security in wireless communication networks is of growing importance since it allows network designers to guarantee information secrecy regardless of the eavesdropper’s computational capability and eliminates the requirement of key distribution and management of traditional cryptographic techniques [1]–[3]. In the pioneering studies [4]–[6], the wiretap channel was proposed as the fundamental system model to characterize physical layer security. In the wiretap channel, an eavesdropper (Eve) attempts to intercept the communication between a transmitter (Alice) and an intended receiver (Bob). The prerequisite to achieve physical layer security is $C_B > C_E$, where $C_B$ is the capacity of the channel between Alice and Bob (henceforth referred to as the main channel), and $C_E$ is the capacity of the channel between Alice and Eve (henceforth referred to as the eavesdropper’s channel).

From the perspective of wiretap code design, the instantaneous knowledge of $C_B$ and $C_E$ is required at Alice in order to guarantee perfect secrecy as defined in [7]. In fact, perfect secrecy has two requirements, (i) that the error probability at Bob decreases with increasing code length, and (ii) that the information leakage to Eve decreases with increasing code length. These two requirements are denoted as the reliability constraint and the secrecy constraint, respectively. A wiretap code can be designed by choosing two code rates, namely, the rate of transmitted codewords, $R_B$, and the rate of transmitted confidential information (or equivalently, the target secrecy rate), $R$. The rate difference $R_E = R_B - R$ is the rate of redundancy, which is used to confuse Eve. In order to guarantee the reliability constraint of wiretap channels, the rate of transmitted codewords has to be chosen as $R_B \leq C_B$. In order to guarantee the secrecy constraint of wiretap channels, the rate of redundancy has to be chosen as $R_E > C_E$. If both $C_B$ and $C_E$ are available at Alice, the maximum target secrecy rate $R$ is achievable, which is referred to as the secrecy capacity of a wiretap channel given by $C = C_B - C_E$ [8], [9]. However, it is unrealistic to assume that Alice possesses the instantaneous knowledge of $C_E$ if Eve does not feed back the channel state information (CSI) of the eavesdropper’s channel to Alice.

We note that it is impossible for Alice to guarantee $R_E > C_E$ in the case where only the statistical knowledge of the eavesdropper’s channel is available at Alice (but where $C_B$ is available at Alice). In this case, the performance of wiretap channels has been characterized in terms of the ergodic secrecy capacity [10], [11], and in terms of the secrecy outage probability [12]–[17]. However, the ergodic secrecy capacity is an average performance metric, and it cannot be utilized to set the target secrecy rate $R$. The use of the secrecy outage probability in setting $R$ has the serious drawback that it is conditioned on an a priori (and subjective) determination of this probability. A new approach to setting the target secrecy rate would therefore be valuable.

In this paper, we propose a framework to optimize $R$ when only the statistical knowledge of the eavesdropper’s channel is available at Alice. We focus on the scenario where Alice and Bob are equipped with a single antenna and Eve is equipped with multiple antennas. This scenario is denoted as the single-input single-output multi-antenna eavesdropper (SISOME) wiretap channel. Our framework is based on a new metric, referred to as the effective secrecy throughput. We determine the target secrecy rates for an on-off transmission scheme and an adaptive transmission scheme through maximizing the effective secrecy throughput. In both schemes, the rate of transmitted codewords, $R_B$, is set equal to the capacity of the main channel. In the on-off transmission scheme, $R$ is optimized based on the average signal-to-noise ratio (SNR) of the main channel, and Alice only transmits confidential messages when $C_B > R$. In the adaptive transmission scheme, $R$ is optimized based on the instantaneous SNR of the main channel. Through detailed analysis we demonstrate how the adaptive transmission scheme outperforms the on-off transmission scheme. We also demonstrate how the difference in the effective secrecy throughput between the adaptive transmission scheme and the on-off transmission scheme increases as the SNR of the main channel increases. Importantly, we
exploit the combining (MRC) to combine the received signals in order to eavesdropper’s channel. As such, Eve applies maximum ratio of successful eavesdropping. 

C the average SNR of the eavesdropper’s channel. This indicates of the instantaneous CSI of the main channel, but only knows length. We also assume that Alice possesses the full knowledge main channel and the eavesdropper’s channel are subject to

where $h$ is the complex gain of the main channel, $x$ is the transmit signal, and $n_B$ is the Gaussian noise of the main channel with zero mean and variance $\sigma_B^2$. The transmit power constraint is given by $E[|x|^2] = P_A$, where $E[\cdot]$ denotes expectation and $P_A$ is the total transmit power. Based on (1), the instantaneous SNR at Bob is obtained as

$$\gamma_B = \frac{|h|^2 P_A}{2\sigma_B^2},$$

which indicates that $\gamma_B$ follows an exponential distribution with $1/\gamma_B$ as the rate parameter, where $\gamma_B = E[|h|^2]$. The cumulative distribution function (cdf) of $\gamma_B$ is given by

$$F_{\gamma_B}(\gamma_B) = 1 - e^{-\frac{\gamma_B}{\gamma_B}}. \quad (3)$$

The $N_E \times 1$ received signal vector at Eve is given by

$$y_E = g^\dagger x + n_E,$$ \quad (4)

where $g$ is the $1 \times N_E$ eavesdropper’s channel vector with independent and identically distributed (i.i.d.) Rayleigh fading entries, and $n_E$ is circularly symmetric complex Gaussian noise vector of the eavesdropper’s channel with zero mean and covariance matrix $I_{N_E} \sigma_E^2$. Applying MRC to exploit the $N_E$-antenna diversity at Eve, the instantaneous SNR at Eve after MRC is obtained as

$$\gamma_E = \frac{\|g\|^2 P_A}{\sigma_E^2},$$ \quad (5)

which indicates that $\gamma_E$ follows a Gamma distribution with $N_E$ and $\tau_E = E[|g|^2]/N_E$ as the shape and scale parameters, respectively. Then, the probability density function (pdf) of $\gamma_E$ is given by [18]

$$f_{\gamma_E}(\gamma_E) = \frac{\gamma_E^{N_E-1} e^{-\gamma_E/\tau_E}}{(N_E-1)! \tau_E^{N_E}}, \quad (6)$$

and the cdf of $\gamma_E$ is given by

$$F_{\gamma_E}(\gamma_E) = 1 - e^{-\frac{\gamma_E}{\tau_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left(\frac{\gamma_E}{\tau_E}\right)^j. \quad (7)$$

### II. System Model

The wiretap channel of interest is illustrated in Fig. 1, where the transmitter (Alice) and the intended receiver (Bob) are equipped with a single antenna, and the eavesdropper (Eve) is equipped with $N_E$ antennas at Eve. We assume that the main channel and the eavesdropper’s channel are subject to independent quasi-static Rayleigh fading with equal block length. We also assume that Alice possesses the full knowledge of the instantaneous CSI of the main channel, but only knows the average SNR of the eavesdropper’s channel. This indicates that Alice only knows $C_B$ but does not know $C_E$. We further assume that Eve knows the instantaneous CSI of the eavesdropper’s channel. As such, Eve applies maximum ratio combining (MRC) to combine the received signals in order to exploit the $N_E$-antenna diversity and maximize the probability of successful eavesdropping.

The received signal at Bob is given by

$$y_B = h^\dagger x + n_B, \quad (1)$$

Fig. 1. Illustration of the wiretap channel with a single antenna at Alice and Bob but $N_E$ antennas at Eve.

demonstrate that the derived target secrecy rates for both schemes are independent of any channel constraints related to quality-of-service or secrecy outage probability, thus making our solutions pragmatic and widely applicable.

**Notation:** Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Given a complex number $p$, $|p|$ denotes the modulus. Given a complex vector $q$, $\|q\|$ denotes the Euclidean norm and $(q)^\dagger$ denotes the conjugate transpose. The $m \times m$ identity matrix is referred to as $I_m$.

### III. Optimization of Target Secrecy Rates

In this section, we optimize the target secrecy rates for the on-off transmission scheme and the adaptive transmission scheme. Since the capacity of the main channel is available at Alice, the rate of transmitted codewords, $R_B$, is set equal to $C_B$ in the two schemes. We determine $R$ for the two schemes through maximizing the effective secrecy throughput, which is given in the following definition.

**Definition 1:** The effective secrecy throughput is defined as the target secrecy rate multiplied by the probability of guaranteeing both the reliability constraint and the secrecy constraint.

**A. On-Off Transmission Scheme**

In the on-off transmission scheme, Alice chooses a constant value for $R$ according to $\gamma_B$ and transmits confidential messages only when $C_B > R$. Thus, in case of transmission the reliability constraint can be guaranteed. We now determine the optimal value of $R$ that maximizes the effective secrecy throughput.

Authorized licensed use limited to: UNSW Library. Downloaded on August 28, 2021 at 07:37:14 UTC from IEEE Xplore. Restrictions apply.
We first express the probability that Alice transmits messages within the on-off transmission scheme as
\[ P_{tx}(R) = \text{Pr}(C_B > R) = \text{Pr}(\gamma_B > 2R - 1). \] (8)
We then express the secrecy outage probability which is defined as the probability that the rate of redundancy is less than the capacity of the eavesdropper’s channel in case of transmission. Specifically, it is written as
\[ O_o(R) = \text{Pr}(C_E > R_E|C_B > R) = \frac{\text{Pr}(2R - 1 < \gamma_B < 2R(1 + \gamma_E) - 1)}{\text{Pr}(\gamma_B > 2R - 1)}. \] (9)

As such, the probability of guaranteeing both the reliability constraint and the secrecy constraint is \( P_{tx}(R) [1 - O_o(R)] \). This leads to the effective secrecy throughput of the on-off transmission scheme given in the following lemma.

**Lemma 1:** The effective secrecy throughput of the on-off transmission scheme is
\[ \Psi_o(R) = R e^{-R (2R - 1) \left( \frac{\gamma_B}{\gamma_B + 2R \gamma_E} \right)^{N_E}}. \] (10)

*Proof:* As per Definition 1, the effective secrecy throughput of the on-off transmission scheme is given by
\[ \Psi_o(R) = R P_{tx}(R) [1 - O_o(R)]. \] (11)

Substituting (8) and (9) into (11), we have
\[ \Psi_o(R) = R \left[ 1 - \text{Pr}(\gamma_B < 2R(1 + \gamma_E) - 1) \right] = R - R \int_0^{\infty} F_{\gamma_B} (2R(1 + \gamma_E) - 1) \] (12)
\[ \times f_{\gamma_E} (\gamma_E) d\gamma_E. \]

Substituting (3) and (6) into (12), we obtain
\[ \Psi_o(R) = R \int_0^{\infty} e^{-\frac{R}{\gamma_E}} \frac{e^{-2R(1+\gamma_E) - 1} - 2R e^{-\gamma_E}}{(N_E - 1)!} N_E d\gamma_E. \] (13)

We then solve the integral in (13) by using \( \int_0^{\infty} x^n e^{-\mu x} dx = n! \mu^{-n-1} \), which gives the result in (10) after performing some manipulations.

The optimal value of \( R \) for the wiretap code design in the on-off transmission scheme is provided in the following theorem.

**Theorem 1:** The optimal value of \( R \) that maximizes \( \Psi_o(R) \) of the on-off transmission scheme, \( R^*_o \), can be obtained by solving the fixed-point equation given by
\[ R^*_o = \frac{\gamma_B \left( \gamma_B + 2R^*_o \gamma_E \right)}{2R^*_o \log 2 \left( \gamma_B + 2R^*_o \gamma_E + N_E \gamma_B \gamma_E \right)}. \] (14)

*Proof:* We note that \( \frac{\gamma_B}{\gamma_B + 2R \gamma_E} > 0 \) and \( e^{-2R \gamma_E} > 0 \). As such, by setting the first derivative of (10) with respect to \( R \) equal to zero, we obtain
\[ 1 - R 2^R \log 2 \left( \frac{1}{\gamma_B} + \frac{N_E \gamma_E}{\gamma_B + 2R \gamma_E} \right) = 0. \] (15)

After performing some manipulations, we obtain the fixed-point equation in (14).

Substituting \( R^*_o \) into (10), we obtain the maximum value of \( \Psi_o(R) \), which is denoted as \( \Psi^*_o \). We now provide some valuable insights into \( R^*_o \) by conducting asymptotic analysis.

**Corollary 1:** As \( \gamma_E \to 0 \), the secrecy outage probability, \( O_o(R) \), converges to zero. As such, the optimal value of \( R \) is the one that maximizes \( R P_{tx} \). By setting the first derivative of \( R P_{tx} \) with respect to \( R \) equal to zero, we obtain the fixed-point equation in (16) after performing some manipulations.

From Corollary 1, we point out that \( O_o(R) \to 0 \) as \( \gamma_E \to 0 \) indicates that Eve can be ignored if she is located far away from Alice.

**Corollary 2:** When \( \gamma_B > \gamma_E \to \infty \) with a fixed ratio \( \gamma_B/\gamma_E = \alpha \), \( R^*_o \) can be obtained by solving the fixed-point equation given by
\[ R^*_o = \frac{\gamma_B}{2R^*_o \log 2 \gamma_E}. \] (17)

*Proof:* When \( \gamma_B \to \infty \) with a fixed ratio \( \gamma_B/\gamma_E = \alpha \), we note \( R \) is still finite and therefore \( e^{-2R \gamma_E} \) approaches one. By substituting \( \gamma_B/\gamma_E = \alpha \) into (10) and setting the first derivative of the resultant equation with respect to \( R \) equal to zero, we obtain the fixed-point equation in (17) after performing some manipulations.

From Corollary 2, we highlight that \( R^*_o \) only depends on \( \alpha \) and \( N_E \) when \( \gamma_B > \gamma_E \to \infty \) with a fixed ratio \( \gamma_B/\gamma_E = \alpha \). We note that an attempt to optimize \( R \), subject to a predetermined secrecy outage probability (when only \( \gamma_E \) is available at Alice) was made in [19]. The legitimate approach of [19] explores the tradeoff between the quality of service and secrecy requirements. This is different from the approach pursued here where we optimize \( R \) by maximizing the effective secrecy throughput, a metric which implicitly captures both the quality of service (reliability) and secrecy constraints. Our framework allows us to avoid a determination of the secrecy outage probability a priori or subjectively, and therefore makes our proposed framework more pragmatic.

### B. Adaptive Transmission Scheme

In the adaptive transmission scheme, Alice adjusts \( R \) using the constraint \( 0 < R < C_B \) according to \( \gamma_B \). This indicates that Alice transmits confidential messages for each \( \gamma_B \) with a different \( R \) (transmission probability is one), and the reliability constraint is guaranteed. We now determine the optimal value of \( R \) that maximizes the effective secrecy throughput.

The secrecy outage probability in the adaptive transmission scheme is defined as the probability that the rate of redundancy is less than the capacity of the eavesdropper’s channel.
Specifically, it is written as
\[
O_a(R) = \Pr(C_E > R_E) = \Pr(\gamma_E > 2^{CB - R} - 1) = 1 - F_{\gamma_E}(2^{CB - R} - 1).
\]  
(18)

As such, the effective secrecy throughput of the adaptive transmission scheme is given in the following lemma.

**Lemma 2:** The effective secrecy throughput of the adaptive transmission is
\[
\Psi_a(R) = R \left[ 1 - e^{-\frac{2^{CB-R_a}}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2^{CB-R} - 1}{\gamma_E} \right)^j \right].
\]  
(19)

**Proof:** As per Definition 1, the effective secrecy throughput of the adaptive transmission scheme is given by
\[
\Psi_a(R) = R [1 - O_a(R)] = RF_{\gamma_E}(2^{CB-R} - 1).
\]  
(20)

Substituting (7) into (20), we obtain the result in (19).

The optimal value of \( R \) for the wiretap code design in the adaptive transmission scheme is provided in the following theorem.

**Theorem 2:** The optimal value of \( R \) that maximizes \( \Psi_a(R) \) of the adaptive transmission scheme, \( R^*_a \), can be obtained by solving the fixed-point equation given by
\[
R^*_a = \frac{\pi E (N_E - 1)!}{2^C B \log 2} \left( \frac{\pi E}{2^{CB-R^*_a} - 1} \right)^{N_E-1} 
\times \left[ 1 - e^{-\frac{2^{CB-R^*_a}}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2^{CB-R^*_a} - 1}{\gamma_E} \right)^j \right].
\]  
(21)

**Proof:** The first derivative of (19) with respect to \( R \) is obtained as
\[
\frac{\partial \Psi_a(R)}{\partial R} = \left[ 1 - e^{-\frac{2^{CB-R_a}}{\gamma_E}} \sum_{j=0}^{N_E-1} \frac{1}{j!} \left( \frac{2^{CB-R} - 1}{\gamma_E} \right)^j \right]
- R \left( \frac{2^{CB-R} \log 2}{\gamma_E} \right) e^{-\frac{2^{CB-R_a}}{\gamma_E}} \left( \frac{2^{CB-R} - 1}{\gamma_E} \right)^{N_E-1}.
\]

By setting \( \partial \Psi_a(R) / \partial R = 0 \), we obtain the fixed-point equation in (21) after performing some algebra.

Substituting \( R^*_a \) into (19), we obtain the maximum value of \( \Psi_a(R) \), which is denoted as \( \Psi^*_a \). We now provide some valuable insights into \( R^*_a \) for \( N_E = 1 \) by conducting the following asymptotic analysis.

**Corollary 3:** As \( \pi E \to 0 \), \( R^*_a \to C_B \).

**Proof:** When \( N_E = 1 \), (19) reduces to
\[
\Psi_a(R) = R \left[ 1 - e^{-\frac{2^{CB-R_a}}{\gamma_E}} \right].
\]  
(22)

As such, \( \Psi_a(R) \) converges to \( R \) as \( \pi E \to 0 \). Moreover, \( \Psi_a(R) \) is a monotonic increase function of \( R \). Due to the constraint \( 0 < R < C_B \), we have \( R^*_a \to C_B \).

It is indicated from Corollary 3 that Eve can be ignored if she is far from Alice.

**Corollary 4:** As \( \pi E \to \infty \), \( R^*_a \) can be obtained by solving the fixed-point equation given by
\[
R^*_a = 1 - \frac{2^{R^*_a - CB}}{\log 2}.
\]  
(23)

**Proof:** Applying \( \lim_{x \to 0} e^{-x} \approx 1 - x \) into (22), we obtain
\[
\lim_{\pi E \to \infty} R \left[ 1 - e^{-\frac{2^{CB-R^*_a}}{\gamma_E}} \right] \approx \frac{2^{CB-R^*_a} - 1}{\beta^2 - 1}.
\]  
(24)

By setting the first derivative of (24) with respect to \( R \) equal to zero, we obtain the fixed-point equation in (24) after performing some algebra.

From Corollary 4, we see that \( R^*_a \) does not approach 0 as \( \pi E \to \infty \). Notably, \( R^*_a \) approaches a constant value that is a function of \( C_B \).

**Corollary 5:** When \( \gamma_B, \pi E \to \infty \) with a fixed ratio \( \gamma_B / \pi E = \beta \), \( R^*_a \) can be obtained through solving the fixed-point equation given by
\[
R^*_a = \frac{e^{\frac{2^{R^*_a - CB} - 1}{\beta^2 - 1}}}{\log 2}.
\]  
(25)

**Proof:** When \( \gamma_B, \pi E \to \infty \) with a fixed ratio \( \gamma_B / \pi E = \beta \), we note that \( R \) is finite and therefore \( 2^{R^*_a - CB} - 1 \) approaches zero. We also note that \( C_B \approx \log_2 \gamma_B \). By applying \( \lim_{x \to 0} e^{-x} \approx 1 - x \) and setting the first derivative of the resultant equation with respect to \( R \) equal to zero, we obtain the fixed-point equation in (25) after performing some algebra.

It is highlighted from Corollary 5 that \( R^*_a \) is a function of \( \beta \) when \( \gamma_B, \pi E \to \infty \) with a fixed ratio \( \gamma_B / \pi E = \beta \).

**IV. Numerical Results**

In this section we present numerical results to examine the impact of the number of antennas at Eve and the SNRs of the main channel and eavesdropper’s channel on the optimal target secrecy rates. We also conduct a thorough performance comparison between the on-off transmission scheme and the adaptive transmission scheme.

In Fig. 2, we plot the effective secrecy throughput of the on-off transmission scheme, \( \Psi_o(R) \), versus \( R \) for different values of \( \pi E \). The theoretic curve is generated from (10). In this figure, we first observe that the Monte Carlo simulations, marked by blue circles, precisely match the theoretic curves, which confirms our analysis in Lemma 1. We also observe that \( \Psi_o(R) \) increases as \( \pi E \) decreases, which demonstrates that the further Eve is away from Alice the larger effective secrecy throughput the on-off transmission scheme achieves. Moreover, we observe that there is indeed an unique value of \( R \) that maximizes \( \Psi_o(R) \). Focusing on the peaks of the three curves, we observe that \( R^*_o \) increases as \( \pi E \) decreases, which indicates that the further Eve is away from Alice the larger target secrecy rate we set in order to maximize the effective secrecy throughput.

In Fig. 3, we plot the optimal \( R \) of the on-off transmission scheme, \( R^*_o \), versus \( \pi E \) for different values of \( \pi E \). The curves represent the theoretic results for \( R^*_o \) obtained from (14), and
Fig. 2. Effective secrecy throughput of the on-off transmission scheme for \( N_E = 1 \), \( \gamma_B = 10 \text{ dB} \), and different values of \( \gamma_E \).

Fig. 3. Optimal target secrecy rate of the on-off transmission scheme for different values of \( \tau_E \).

Fig. 4. Effective secrecy throughput of the adaptive transmission scheme for \( N_E = 1 \), \( \gamma_B = 10 \text{ dB} \), and different values of \( \gamma_E \).

Fig. 5. Optimal target secrecy rate of the adaptive transmission scheme for different values of \( \tau_E \).

the symbols represent the simulated results for \( R^*_a \) obtained from Monte Carlo simulations. The figure demonstrates that the theoretic result is accurate, which confirms the validity of our analysis in Theorem 1. In this figure, we first observe that \( R^*_a \) increases as \( \tau_B \) increases, which indicates that the better the main channel is the larger target secrecy rate we set in order to maximize the effective secrecy throughput. We also observe that \( R^*_a \) decreases as \( \tau_E \) increases. Furthermore, we observe that \( R^*_a \) decreases as \( N_E \) increases. This can be explained by the fact that Eve applies MRC to combine the received signals. The more antennas she possesses the better the eavesdropper’s channel is.

In Fig. 4, we plot the effective secrecy throughput of the adaptive transmission scheme, \( \Psi_a(R) \), versus \( R \) for different values of \( \tau_E \). The theoretic curve is obtained from (19). In this figure, we first observe that the Monte Carlo simulations precisely match the theoretic curves, which confirms our analysis in Lemma 2. We also observe that \( \Psi_a(R) \) increases as \( \tau_E \) decreases, which demonstrates that the worse the eavesdropper’s channel is the larger effective secrecy throughput the adaptive transmission scheme achieves. Moreover, we observe that an unique value of \( R \) exists which maximizes \( \Psi_a(R) \) for a given \( \gamma_B \). Focusing on the peaks of the three curves, we also observe that \( R^*_a \) increase as \( \tau_E \) decreases, which demonstrates that the further Eve is away from Alice the larger target secrecy rate we set in order to maximize the effective secrecy throughput.

In Fig. 5, we plot the optimal target secrecy rate \( R \) of the adaptive transmission scheme, \( R^*_a \), versus \( \gamma_B \) for different values of \( \tau_E \). The curves represent the theoretic results for \( R^*_a \).
Moreover, we observe that $R_\star^a$ decreases as $\gamma_B$ increases. We also observe that $R_\star^o$ increases as $\gamma_B$ increases, which indicates that keeping a constant $R$ for all the realizations of $\gamma_B$ with the same $\gamma_E$ is not optimal in terms of maximizing the effective secrecy throughput. Furthermore, we observe that $R_\star^o$ decreases as $N_E$ increases.

Finally, we conduct a comparison between the on-off transmission scheme and the adaptive transmission scheme. Fig. 6 compares the maximum effective secrecy throughput of the on-off transmission scheme, obtained by substituting $R_\star^o$ into (10), with the average maximum effective secrecy throughput of the adaptive transmission scheme, obtained by $\Psi_*=E_{\gamma_D}[\Psi^*]$.

We observe that $\Psi_*$ and $\Psi^*_o$ increase as $\gamma_B$ increases. We also observe that $\Psi^*_a$ and $\Psi^*_o$ decrease as $N_E$ increases. Moreover, we observe that $\Psi^*_a$ is larger than $\Psi^*_o$, which indicates that the adaptive transmission scheme outperforms the on-off transmission scheme. This can be explained by the fact that Alice achieves some positive effective secrecy throughput in the adaptive transmission scheme when she stops transmission in the on-off transmission scheme. In addition, we observe that the effective secrecy throughput gain of the adaptive transmission scheme over the on-off transmission scheme is negligible in the regime of low $\gamma_B$, but significant in the regime of high $\gamma_B$.

V. CONCLUSION

In this paper, we proposed a new framework in order to optimize the target secrecy rate for the SISOME wiretap channel when only the statistical knowledge of the eavesdropper’s channel is available at Alice. The framework is based on a new metric, the effective secrecy throughput, which captures implicitly the reliability constraint and secrecy constraint of wiretap channels. The framework does not require to determine a value for the secrecy outage probability $a$ priori or subjectively, and therefore is more suitable in practice. By applying this framework, we optimized the target secrecy rates of the on-off transmission scheme and the adaptive transmission scheme. We demonstrated that the effective secrecy throughput gain is achieved by adapting the target secrecy rate according to the instantaneous SNR of the main channel relative to the target secrecy rate based on the average SNR of the main channel.

ACKNOWLEDGEMENT

This work was funded by The University of New South Wales and Australian Research Council Grant DP120102607.

REFERENCES


