entropy

MDPI

Article

Some New Results on the Gaussian Wiretap Feedback Channel

Chenxu Wei [1], Linman Yu [2] and Bin Dai [1,*]

[1] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, China
[2] School of Economics and Management, Chengdu Textile College, Chengdu 611731, China
* Correspondence: daibin@home.swjtu.edu.cn

Received: 11 July 2019; Accepted: 20 August 2019; Published: 21 August 2019

Abstract: In this paper, the Gaussian wiretap feedback channel is revisited, and some new results on its secrecy capacity are obtained. To be specific, first, we show that the Schalkwijk–Kailath (SK) feedback scheme, which achieves the secrecy capacity of the degraded Gaussian wiretap feedback channel, also achieves the secrecy capacity of the non-degraded Gaussian wiretap feedback channel. Second, applying the existing secret key-based feedback schemes to Gaussian wiretap feedback channels, we derive some new lower bounds on the secrecy capacities of these models. Finally, we compare the performances of the above feedback schemes in the degraded and non-degraded Gaussian wiretap feedback channels and show which feedback scheme performs better for these channel models.

Keywords: Gaussian wiretap channel; noiseless feedback; Schalkwijk–Kailath scheme; secrecy capacity

1. Introduction

In recent years, mobile wireless communication has been widely used and has become an essential part in people's daily life. Due to the broadcast nature of wireless communications, the private information in people's wireless mobile devices (such as bank card information, energy pricing messages, e-health data, and password messages) is more vulnerable to eavesdropping. Physical layer security (PLS), realizing secure communication over wireless channels by information-theoretic approaches, is shown to be an effective way to prevent information eavesdropping. The research on PLS in communication systems started from Wyner's outstanding work on the degraded wiretap channel (DWTC) [1], where a transmitter broadcasts its message M over N channel uses to a legitimate receiver and an eavesdropper via a degraded broadcast channel, and the perfect secrecy is guaranteed if the information leakage rate $\frac{1}{N}I(M;Z^N)$, where Z^N denotes the received output at the eavesdropper, vanishes as the transmitted codeword length N tends to infinity (Here note that the perfect secrecy defined in [1] is in fact weak secrecy. Another definition of the perfect secrecy is strong secrecy, which is defined as the information leakage $I(M;Z^N)$ at the wiretapper vanishes as N tends to infinity.).The secrecy capacity, defined as the channel capacity under the weak secrecy constraint, was established in [1]. Subsequently, the work in [2] generalized the DWTC [1] by considering a general broadcast channel and the transmission of a common message, which is allowed to be decoded by both the legitimate receiver and the eavesdropper. The capacity results of [1] and [2] indicated that for the wiretap channel (WTC) and its extended model, the positive secrecy rates are guaranteed only if the legitimate receiver's channel is less noisy than the wiretapper's channel. Thus, it is natural to ask the following two questions:

- (1) How can a positive secrecy rate be achieved if the eavesdropper's channel is less noisy than the legitimate receiver's channel?

- (2) If the eavesdropper's channel is noisier than the legitimate receiver's channel, can the secrecy rate be further enhanced beyond the secrecy capacity?

The schemes that exploit artificial noise-aided cooperative jamming [3–5] and channel feedback address the above two questions. However, in some circumstances, such as Internet of Things (IoT) systems, artificial noise-aided cooperative jamming may not be suitable since the IoT devices have significant energy constraints [6,7], and hence, channel feedback is of particular interest in such circumstances.

The role of channel feedback in PLS of communication systems was first studied in [8], where the pioneering work [1] was re-visited by considering the case that the legitimate receiver can send its received channel outputs back to the transmitter via a noiseless feedback channel, which is not known by the eavesdropper. Since the transmitter also knows the legitimate receiver's channel output via the noiseless feedback channel, the work in [8] showed that generating the secret key from the legitimate receiver's channel output and using it to encrypt the transmitted message help to increase the secrecy capacity of the WTC. Furthermore, the work in [8] showed that such a secret key-based feedback scheme achieves the secrecy capacity of the DWTC with noiseless feedback, which implies that it is an optimal feedback scheme for the DWTC. Here, note that in [8], the feedback channel only transmits the legitimate receiver's channel output, and what happens if the channel can transmit anything as the legitimate receiver wishes? The work in [9] investigated this case and pointed out that directly transmitting pure random bits instead of the legitimate receiver's channel output over the noiseless feedback channel may perform even better. [9] further showed that transmitting pure random bits performs better than transmitting the legitimate receiver's channel output if the rate of the pure random bits is larger than that of the secret key generated from the legitimate receiver's channel output, and vice versa. Later, the work in [10] extended the WTC with rate-limited feedback [9] to a broadcast case, where one secret message is sent to two legitimate receivers via a general broadcast wiretap channel, and two legitimate receivers independently send their secret keys to the transmitter via two noiseless feedback channels. Encrypting the transmitted message for its intended legitimate receiver by the corresponding secret key and using time-sharing between these two encrypted messages, the work in [10] derived an achievable secrecy rate for this extended model and showed that these secret keys help to increase the achievable secrecy rate (lower bound on the secrecy capacity) of the same model without feedback [11]. Other related works on the feedback channels with secrecy constraints include [12–16], where the channel state was introduced into various feedback channel models in the presence of an eavesdropper.

Here, note that the feedback schemes mentioned above mainly focus on generating secret keys from the feedback. Recently, exploiting other usages of feedback has attracted considerable attention. To be specific, the work in [17] showed that for feedback communication systems, a better use of the channel output feedback is to produce not only a secret key, but also a helping message from it, and such a helping message improves the legitimate receiver's decoding performance. Later, the works in [18] and [19] further applied the scheme of [17] to the state-dependent WTC with and without the action encoder, respectively. Moreover, the work in [20] found that the classical Schalkwijk–Kailath (SK) scheme [21] achieving the capacity of the Gaussian channel with feedback also achieved the secrecy capacity of the Gaussian wiretap channel with feedback. Furthermore, the work in [22] investigated the finite-order autoregressive moving average (ARMA) Gaussian wiretap channel with noiseless feedback. A variation of the SK scheme was proposed to achieve the secrecy capacity, which equals the capacity of the same model without the secrecy constraint.

In this paper, we revisit the Gaussian wiretap feedback channel [20] (see Figure 1), and would like to answer the following questions:

- (1) In [20], the secrecy capacity of the degraded Gaussian wiretap feedback channel was derived, and it equaled the capacity of the same model without the secrecy constraint. Does this still hold for the non-degraded Gaussian wiretap feedback channel (see Figure 2), i.e., does the secrecy

capacity of the non-degraded Gaussian wiretap feedback channel equal the capacity of the same model without the secrecy constraint?

- (2) For the already existing feedback schemes such as the secret key based feedback scheme [8], the improved secret key-based feedback scheme [17], and the SK feedback scheme [20,21], which one performs the best for the Gaussian wiretap feedback channel?

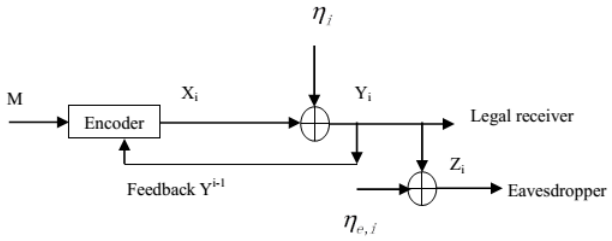

Figure 1. The degraded Gaussian wiretap feedback channel.

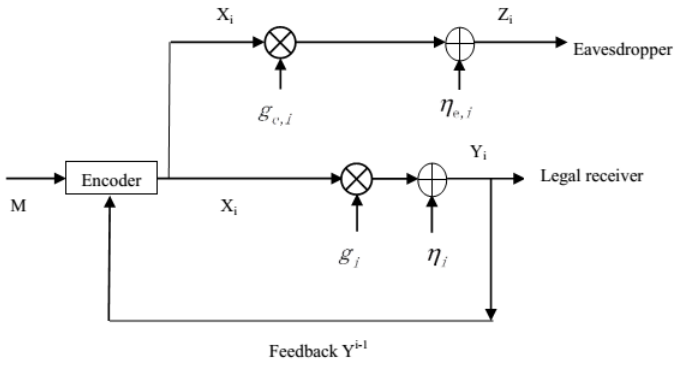

Figure 2. The non-degraded Gaussian wiretap feedback channel.

The main contribution of this paper is as follows:

- (1) We derive the secrecy capacity of the non-degraded Gaussian wiretap feedback channel and show that it also equals the capacity of the same model without the secrecy constraint.
- (2) In [8], it was shown that the secret key-based feedback scheme was optimal for the discrete memoryless DWTC. However, this is not true for the degraded Gaussian wiretap feedback channel, i.e., in this paper, we show that the secret key-based feedback scheme only achieves a lower bound on the secrecy capacity of the degraded Gaussian wiretap feedback channel. Hence, for the degraded Gaussian wiretap feedback channel, the SK feedback scheme performs the best. In addition, in this paper, we show that for the non-degraded Gaussian wiretap feedback channel, the improved secret key-based feedback scheme performs as well as the SK scheme, and both of them perform better than the secret key-based feedback scheme.

This paper is organized as follows. Section 2 shows the capacity result on the non-degraded Gaussian wiretap feedback channel and its proof. Section 3 shows the performances of the secret key-based feedback scheme, the improved secret key-based feedback scheme, and the SK feedback scheme in the Gaussian wiretap feedback channel. Final conclusions are presented in Section 4.

2. The Non-Degraded Gaussian Wiretap Feedback Channel

In the remainder of this paper, random variables (RVs), their realizations, and alphabets are denoted by uppercase letters, lowercase letters, and calligraphic letters, respectively. Random vectors and their realizations are written in a similar way. For example, Y denotes an RV, and y denotes

the value of a realization in the alphabet $\mathcal{Y}$. Similarly, Y^N denotes a random vector $(Y_1, ..., Y_N)$, and $y^N = (y_1, ..., y_N)$ denotes the value of a realization in $\mathcal{Y}^N$ (the N^{th} Cartesian power of $\mathcal{Y}$). Moreover, for simplicity, the probability $Pr\{X = x\}$ is denoted by $P(x)$, and in the remainder of this paper, the base of the log function is taken to be two.

For the non-degraded Gaussian wiretap feedback channel (see Figure 2), the transmitted message M is uniformly drawn from the set $\mathcal{M} = \{1, 2, ..., |\mathcal{M}|\}$. The channel input and outputs at time $i \in \{1, 2, ..., N\}$ satisfy:

$$Y_i = g_i X_i + \eta_i, \quad Z_i = g_{e,i} X_i + \eta_{e,i}, \tag{1}$$

where X_i is the channel input subject to an average power constraint P, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, $g_i = g$ and $g_{e,i} = g_e$ are the gains of the legitimate receiver's channel and the eavesdropper's channel, respectively, and η_i and $\eta_{e,i}$ are independent Gaussian noises and are i.i.d. across the time index i. Moreover, $\eta_i \sim \mathcal{N}(0, \sigma^2)$, $\eta_{e,i} \sim \mathcal{N}(0, \sigma_e^2)$ and the noises η_i, $\eta_{e,i}$ are independent of the transmitted message M, and the i^{th} channel input X_i is a stochastic function of the message M and the channel output feedback Y^{i-1}.

The legitimate receiver produces $\hat{M} = \psi(Y^N)$, where ψ is the legitimate receiver's decoding function, and the decoding error probability is denoted by:

$$P_e = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} Pr\{\psi(y^N) \neq m | m \text{ sent}\}. \tag{2}$$

Let:

$$\Delta = \frac{1}{N} H(M|Z^N) \tag{3}$$

be the eavesdropper's equivocation rate of the message M. Given a non-negative number R, if for any $\epsilon > 0$, there exists a pair of encoder and decoder such that:

$$\frac{\log |\mathcal{M}|}{N} \geq R - \epsilon, \ \Delta \geq R - \epsilon, \ P_e \leq \epsilon, \tag{4}$$

R is achievable under the weak secrecy constraint. The secrecy capacity $\mathcal{C}_{s-f}$ is the supremum over all achievable weak secrecy rates, and it will be given in the following Theorem 1.

Theorem 1. *The secrecy capacity $\mathcal{C}_{s-f}$ of the non-degraded Gaussian wiretap feedback channel is given by:*

$$\mathcal{C}_{s-f} = \frac{1}{2} \log \left(1 + \frac{g^2 P}{\sigma^2} \right). \tag{5}$$

Remark 1. *Here, note that in the model of Figure 2, the eavesdropper's channel may be less noisy than the legitimate receiver's. Theorem 1 indicates that even if the eavesdropper's channel is less noisy than the legitimate receiver's, the perfect secrecy can still be achieved without loss of the transmission rate, i.e., the secrecy capacity equals the legitimate receiver's channel capacity.*

Proof. First, remember that the capacity of the legitimate receiver's channel is $\frac{1}{2} \log(1 + \frac{g^2 P}{\sigma^2})$, and it is obtained by substituting (1) into $\max I(X; Y)$ and using the fact that the maximum is achieved if X is Gaussian distributed with zero mean and variance P. Then, the converse of Theorem 1 follows from the fact that feedback does not increase the capacity of the legitimate receiver's channel and $\mathcal{C}_{s-f}$ cannot exceed the capacity of the legitimate receiver's channel with feedback, i.e., $\mathcal{C}_{s-f} \leq \frac{1}{2} \log(1 + \frac{g^2 P}{\sigma^2})$. Now, it remains to show the achievability of $\mathcal{C}_{s-f}$; see the following.

From (1), we know that the input and output of the legitimate receiver's channel satisfy:

$$Y_i = g X_i + \eta_i. \tag{6}$$

Notice that (6) can be re-written as:

$$Y_i^{'} = X_i + \eta_i^{'}, \tag{7}$$

where $Y_i^{'} = \frac{Y_i}{g}$ and $\eta_i^{'} = \frac{\eta_i}{g}$. Now, the legitimate receiver's channel is equivalent to a new Gaussian channel with input X_i, output $Y_i^{'}$, and channel noise $\eta_i^{'} \sim \mathcal{N}(0, \sigma^{'2} = \frac{\sigma^2}{g^2})$. Then, we describe the SK scheme for this equivalent channel as follows.

The message M takes values in the set $\mathcal{M} = \{1, 2, ..., 2^{NR}\}$. Divide the overall interval $[-0.5, 0.5]$ into 2^{NR} equally-spaced sub-intervals, and the center of each sub-interval is mapped to a message value in $\mathcal{M}$. Let θ be the center of the sub-interval with respect to (w.r.t.) the choosing message M. At Time 1, the transmitter sends:

$$X_1 = \theta\alpha, \tag{8}$$

where $\alpha = \sqrt{\frac{P+\sigma'^2}{\sigma'^2}} = \sqrt{\frac{g^2P+\sigma^2}{\sigma^2}}$. Upon receiving the output $Y_1 = hX_1 + \eta_1$, the legitimate receiver obtains $Y_1^{'} = \frac{Y_1}{g} = X_1 + \frac{\eta_1}{g} = X_1 + \eta_1^{'}$ and computes:

$$\hat{\theta}_1 = \frac{Y_1^{'}}{\alpha} = \theta + \frac{\eta_1^{'}}{\alpha} \tag{9}$$

as an estimation of θ at Time 1. At time i ($i \in \{2, 3, ..., N\}$), the transmitter sends:

$$X_i = \alpha_i(\theta - \hat{\theta}_{i-1}) = -\alpha_i \frac{\sum_{j=1}^{i-1} \alpha_j \eta_j^{'}}{\sum_{j=1}^{i-1} \alpha_j^2}, \tag{10}$$

where $\alpha_i = \sqrt{\frac{P}{\sigma'^2}}\alpha^{i-1} = \sqrt{\frac{g^2P}{\sigma^2}}\alpha^{i-1}$ for $i \in \{2, 3, ..., N\}$. Upon receiving the output $Y_i = gX_i + \eta_i$, the legitimate receiver obtains $Y_i^{'} = \frac{Y_i}{g} = X_i + \frac{\eta_i}{g} = X_i + \eta_i^{'}$ and computes:

$$\hat{\theta}_i = \theta + \frac{\sum_{j=1}^{i} \alpha_j \eta_j^{'}}{\sum_{j=1}^{i} \alpha_j^2} \tag{11}$$

as an estimation of θ at time i. In [21], it was shown that the decoding error probability P_e (the probability of $\hat{\theta}_N$ not belonging to the sub-interval of the choosing message M) of this proposed scheme doubly-exponentially decays to zero for sufficiently large N and $R \leq \frac{1}{2}\log(1 + \frac{P}{\sigma'^2}) = \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2})$. Hence, letting $R = \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2})$, for a given ϵ, $\frac{\log|\mathcal{M}|}{N} \geq \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2}) - \epsilon$ and $P_e \leq \epsilon$ are satisfied by using the above proposed SK scheme. Then, it remains to show $\Delta \geq \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2}) - \epsilon$, and the proof is given as follows.

$$\begin{aligned}
\Delta &= \frac{1}{N}H(M|Z^N) \overset{(1)}{=} \frac{1}{N}H(M|g_eX_1 + \eta_{e,1}, ..., g_eX_N + \eta_{e,N}) \\
&\overset{(2)}{=} \frac{1}{N}H(M|g_e\theta\alpha + \eta_{e,1}, g_e(\frac{-\alpha_2\eta_1^{'}}{\alpha_1}) + \eta_{e,2}, ..., g_e(-\alpha_N\frac{\sum_{j=1}^{N-1}\alpha_j\eta_j^{'}}{\sum_{j=1}^{N-1}\alpha_j^2}) + \eta_{e,N}) \\
&\geq \frac{1}{N}H(M|g_e\theta\alpha + \eta_{e,1}, g_e\frac{-\alpha_2\eta_1^{'}}{\alpha_1} + \eta_{e,2}, ..., g_e(-\alpha_N\frac{\sum_{j=1}^{N-1}\alpha_j\eta_j^{'}}{\sum_{j=1}^{N-1}\alpha_j^2}) + \eta_{e,N}, \eta_1^{'}, ..., \eta_N^{'}, \eta_{e,2}, ..., \eta_{e,N}) \\
&= \frac{1}{N}H(\theta|g_e\theta\alpha + \eta_{e,1}, \eta_1^{'}, ..., \eta_N^{'}, \eta_{e,2}, ..., \eta_{e,N}) \\
&\overset{(3)}{=} \frac{1}{N}H(\theta|g_e\theta\alpha + \eta_{e,1})
\end{aligned}$$

$$\begin{aligned}
&\overset{(4)}{=} \frac{1}{N}(H(\theta) + h(\eta_{e,1}) - h(g_e\theta\alpha + \eta_{e,1}))\\
&\overset{(5)}{=} \frac{1}{N}(NR + h(\eta_{e,1}) - h(g_e\theta\alpha + \eta_{e,1}))\\
&\overset{(6)}{=} \frac{1}{N}(NR + \frac{1}{2}\log(2\pi e\sigma_e^2) - h(g_e\theta\alpha + \eta_{e,1}))\\
&\overset{(7)}{\geq} \frac{1}{N}(NR + \frac{1}{2}\log(2\pi e\sigma_e^2) - \frac{1}{2}\log(2\pi e(\alpha^2 g_e^2 Var(\theta) + \sigma_e^2)))\\
&\overset{(8)}{=} \frac{1}{N}(NR + \frac{1}{2}\log(2\pi e\sigma_e^2) - \frac{1}{2}\log(2\pi e(\alpha^2 g_e^2 \frac{1}{12} + \sigma_e^2)))\\
&= R - \frac{1}{2N}\log(1 + \frac{\alpha^2 g_e^2}{12\sigma_e^2})\\
&\overset{(9)}{=} \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2}) - \frac{1}{2N}\log(1 + \frac{(g^2P + \sigma^2)g_e^2}{12\sigma_e^2\sigma^2}),
\end{aligned} \tag{12}$$

where (1) follows from (1), (2) follows from (8) and (10), (3) follows from the fact that $(\eta_1, ..., \eta_N, \eta_{e,2}, ..., \eta_{e,N})$ are independent of θ, $g_e\theta\alpha + \eta_{e,1}$, and $\eta_i^{'} = \frac{\eta_i}{g}$, (4) follows from θ being independent of $\eta_{e,1}$, (5) follows from the fact that M is uniformly distributed over $\mathcal{M} = \{1, 2, ..., 2^{NR}\}$, (6) follows from $h(\eta_{e,1}) = \frac{1}{2}\log(2\pi e\sigma_e^2)$, (7) follows from the fact that $h(X) \leq \frac{1}{2}\log(2\pi eVar(X))$, where the equality holds if X is Gaussian distributed, (8) follows from the fact that the variance of θ is $\frac{1}{12}$ while N tends to infinity (see a similar argument in [20]), and (9) is from the definitions $R = \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2})$ and $\alpha = \sqrt{\frac{g^2P+\sigma^2}{\sigma^2}}$. Finally, choosing sufficiently large N, $\Delta \geq \frac{1}{2}\log(1 + \frac{g^2P}{\sigma^2}) - \epsilon$ is proven. The proof of Theorem 1 is complete. □

Remark 2. *From the above proof of Theorem 1 (especially the inequality below Step (2) of (12)), we see that even if the eavesdropper obtains his/her own channel noises of all time indexes except Time* 1 *and knows the legitimate receiver's channel noises of all time indexes, the weak secrecy can still be guaranteed with the transmission rate* $R = \frac{1}{2}\log\left(1 + \frac{g^2P}{\sigma^2}\right)$*, and the intuition behind this fact is given as follows. The transmitter transmits the original message* M *only at the first transmission (see (8) and (10)), and then, the transmissions after the first one combine only channel noises in the previous transmissions. Since the information leakage occurs only in the first transmission, the information leakage rate* $\frac{1}{N}I(M; Z^N)$ *vanishes as the codeword length* N *tends to infinity.*

The equivocation analysis (see (12)) of the proof of Theorem 1 also indicates that if the eavesdropper knows the legitimate receiver's channel noises of all time indexes, i.e., $\eta_1^{'}$*,...,*$\eta_N^{'}$*, he/she also obtains the channel feedback from Time* 2*–*N *(i.e.,* Y_2*,...,*Y_N*) due to the reason that for* $i \in \{2, 3, ..., N\}$*,* X_i *is only a combination of the channel noises in the previous transmissions (see (10)) and* $Y_i = gX_i + g\eta_i^{'}$*. Then, we can conclude that even if the channel output feedback* Y_2*,...,*Y_N *is obtained by the eavesdropper, the weak secrecy can still be guaranteed. However, we should note that if the eavesdropper knows* Y_1 *and* $\eta_1^{'}$*, he/she also obtains the transmitted message since* $Y_1 = gX_1 + g\eta_1^{'}$ *and* $X_1 = \theta\alpha$*, which implies that the weak secrecy cannot be guaranteed for this case.*

3. Comparison of the Already Existing Feedback Schemes for the Gaussian Wiretap Feedback Channel

In this section, we compare the performances of the secret key-based feedback scheme [8], the improved secret key-based feedback scheme [17], and the SK feedback scheme [21] in the Gaussian wiretap feedback channel.

3.1. Comparison of the Feedback Schemes for the Degraded Gaussian Wiretap Feedback Channel

For the degraded Gaussian wiretap feedback channel (see Figure 1), at time i ($i \in \{1, 2, ..., N\}$), the channel input and outputs are given by:

$$Y_i = X_i + \eta_i, \ Z_i = X_i + \eta_i + \eta_{e,i}, \tag{13}$$

where X_i is the channel input with power constraint P, Y_i and Z_i are channel outputs respectively at the legitimate receiver and the eavesdropper, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$ and $\eta_{e,i} \sim \mathcal{N}(0, \sigma_e^2)$ are independent channel noises and are i.i.d. across the time index i. The channel encoder, decoder, and the achievable secrecy rate are defined the same as in Section 2. The following Theorem 2 [20] determines the secrecy capacity $\mathcal{C}_{s-f}^d$ of the degraded Gaussian wiretap feedback channel; see the following.

Theorem 2. *The secrecy capacity $\mathcal{C}_{s-f}^d$ of the degraded Gaussian wiretap feedback channel is given by:*

$$\mathcal{C}_{s-f}^d = \frac{1}{2}\log(1 + \frac{P}{\sigma^2}). \tag{14}$$

Remark 3. *Here, note that $\mathcal{C}_{s-f}^d$ is achieved by using the SK feedback scheme. Theorem 2 indicates that for the degraded Gaussian wiretap feedback channel, the perfect secrecy can be achieved without loss of the transmission rate, i.e., the secrecy capacity equals the capacity of the legitimate receiver's channel.*

Proof. See [20]. □

In [8], it has been shown that the secrecy capacity $\mathcal{C}_s^*$ of the discrete memoryless degraded wiretap feedback channel can be achieved by using the secret key-based feedback scheme (here, note that for the degraded wiretap feedback channel, the work in [17] showed that the improved secret key-based feedback scheme reduces to the original secret key-based feedback scheme [8]), and it is given by:

$$\mathcal{C}_s^* = \max_{P(x)} \min\{I(X;Y), H(Y|Z)\}, \tag{15}$$

where $X \to Y \to Z$. However, we should note that the capacity formula in (15) is only an achievable secrecy rate for the degraded Gaussian wiretap feedback channel, and this is because the converse of $H(Y|Z)$ in (15) does not hold for the Gaussian case. To be specific, first, note that the term $H(Y|Z)$ in (15) follows from:

$$\begin{aligned}
R - \epsilon &\leq \frac{1}{N} H(M|Z^N) \\
&= \frac{1}{N}(H(M|Z^N) - H(M|Y^N, Z^N) + H(M|Y^N, Z^N)) \\
&\leq \frac{1}{N}(I(M; Y^N|Z^N) + \delta(\epsilon)) \\
&\overset{(a)}{\leq} \frac{1}{N}(H(Y^N|Z^N) + \delta(\epsilon)) \\
&\leq \frac{1}{N}(\sum_{i=1}^{N} H(Y_i|Z_i) + \delta(\epsilon)) \\
&\overset{(b)}{=} H(Y_J|Z_J, J) + \frac{1}{N}\delta(\epsilon) \\
&\overset{(c)}{\leq} H(Y|Z) + \frac{1}{N}\delta(\epsilon),
\end{aligned} \tag{16}$$

and letting $\epsilon \to 0$, where (a) follows from $I(M; Y^N|Z^N) \leq H(Y^N|Z^N)$, (b) follows from J being uniformly distributed over $\{1, 2, ..., N\}$ and it being independent of Y^N and Z^N, and (c) follows from the definitions $Y \triangleq Y_J$ and $Z \triangleq Z_J$. Next, from (16), we can check that for the Gaussian case, Step (a) of (16) does not hold due to the fact that the differential conditional entropy $h(Y^N|Z^N, M)$ may be a negative number. Finally, substituting $X \sim \mathcal{N}(0, P)$ and (13) into (15), a lower bound R_{s-f}^* on the secrecy capacity $\mathcal{C}_{s-f}^d$ is obtained, and it is given by the following Corollary 1.

Corollary 1. *A lower bound R^*_{s-f} on the secrecy capacity C^d_{s-f} of the degraded Gaussian wiretap feedback channel is given by:*

$$R^*_{s-f} = \min\left\{\frac{1}{2}\log\left(1+\frac{P}{\sigma^2}\right), \frac{1}{2}\log\left(\frac{2\pi e\sigma_e^2(P+\sigma^2)}{P+\sigma^2+\sigma_e^2}\right)\right\}. \tag{17}$$

Comparing R^*_{s-f} in Corollary 1 with C^d_{s-f} in Theorem 2, we can conclude that for the degraded Gaussian wiretap feedback channel, the secret key-based feedback scheme performs no better than the SK scheme. The following Figure 3 shows the gap between the lower bound R^*_{s-f} and the secrecy capacity C^d_{s-f} for $\sigma^2 = 3$, $\sigma_e^2 = 10$, and P taking values in $[0, 1800]$. It is easy to see that the gap is increasing while the power P is increasing.

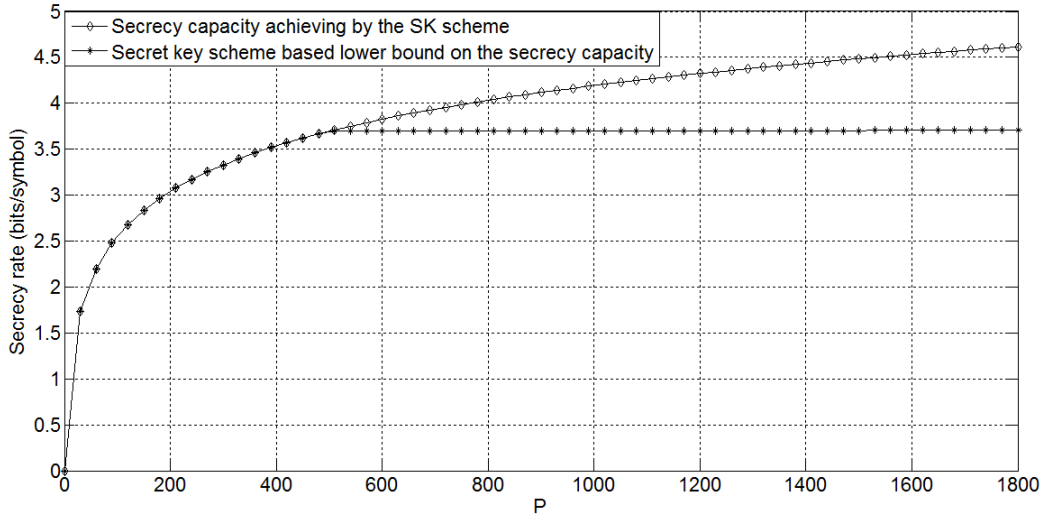

Figure 3. The capacity results on the degraded Gaussian wiretap feedback channel for $\sigma^2 = 3$, $\sigma_e^2 = 10$, and P taking values in $[0, 1800]$. SK, Schalkwijk–Kailath.

3.2. Comparison of the Feedback Schemes for the Non-Degraded Gaussian Wiretap Feedback Channel

In Section 2, we showed that the secrecy capacity of the non-degraded Gaussian wiretap feedback channel equals the legitimate receiver's channel capacity. For comparison, in this subsection, we calculate the lower bounds constructed by the secret key-based feedback scheme [8] and the improved secret key-based feedback scheme [17]; see the following.

First, note that in [8], it has been shown that for the discrete memoryless non-degraded wiretap feedback channel, a lower bound R^{**}_{s-f} on the secrecy capacity, which is constructed by the secret key-based feedback scheme, is given by:

$$R^{**}_{s-f} = \max_{P(x)} \min\{[I(X;Y) - I(X;Z)]^+ + H(Y|X,Z), I(X;Y)\}, \tag{18}$$

where $Y \to X \to Z$ and $[x]^+ = \max\{0, x\}$. The intuition behind (18) is given as follows. The feedback channel output is used to generate a secret key shared between the legitimate parties, and this key is completely unknown by the wiretapper. Moreover, the transmitted message M is divided into two parts M_1 and M_2, where M_1 is encoded the same as the message in [1], and M_2 is encrypted by the secret key generated from the feedback. Then, the total secrecy rate also consists of two parts: one equals $I(X;Y) - I(X;Z)$, which is the same as the secrecy capacity of the wiretap channel [1], and the other equals $H(Y|X,Z)$, which is the rate of the secret key. In addition, note that the total secrecy rate cannot exceed the channel capacity $I(X;Y)$ of the legitimate parties, and hence, the lower bound

in (18) is obtained. Then, substituting $X \sim \mathcal{N}(0, P)$ and (1) into (18), a lower bound R_{s-f}^{non*} on the secrecy capacity $\mathcal{C}_{s-f}$ is obtained, and it is given by the following Corollary 2.

Corollary 2. *A lower bound R_{s-f}^{non*} on the secrecy capacity $\mathcal{C}_{s-f}$ of the non-degraded Gaussian wiretap feedback channel is given by:*

$$R_{s-f}^{non*} = \min\left\{\frac{1}{2}\log(1+\frac{g^2P}{\sigma^2}), [\frac{1}{2}\log(1+\frac{g^2P}{\sigma^2}) - \frac{1}{2}\log(1+\frac{g_e^2P}{\sigma_e^2})]^+ + \frac{1}{2}\log(2\pi e\sigma^2)\right\}. \quad (19)$$

Second, in [17], it has been shown that for the discrete memoryless non-degraded wiretap feedback channel, a lower bound R_{s-f}^{***} on the secrecy capacity, which is constructed by the improved secret key-based feedback scheme, is given by:

$$R_{s-f}^{***} = \max_{P(x)} \min\{[I(X;V,Y) - I(X;Z)]^+ + H(Y|X,Z), I(X;Y)\}, \quad (20)$$

where the joint distribution is denoted by:

$$P(v,x,y,z) = P(v|x,y)P(y|x)P(z|x)P(x). \quad (21)$$

Then, substituting $X \sim \mathcal{N}(0, P)$, $V = X + Y$, and (1) into (20), a lower bound R_{s-f}^{non**} on the secrecy capacity $\mathcal{C}_{s-f}$ is obtained, and it is given by the following Corollary 3.

Corollary 3. *A lower bound R_{s-f}^{non**} on the secrecy capacity $\mathcal{C}_{s-f}$ of the non-degraded Gaussian wiretap feedback channel is given by:*

$$R_{s-f}^{non**} = \frac{1}{2}\log(1+\frac{g^2P}{\sigma^2}). \quad (22)$$

Proof. First, substituting $X \sim \mathcal{N}(0, P)$, $V = X + Y$, and (1) into (20), we have:

$$R_{s-f}^{non**} = \min\{\frac{1}{2}\log(1+\frac{g^2P}{\sigma^2}), [\frac{1}{2}\log(2\pi eP) - h(X|X,Y) - \frac{1}{2}\log(1+\frac{g_e^2P}{\sigma_e^2})]^+ + \frac{1}{2}\log(2\pi e\sigma^2)\}. \quad (23)$$

Next, note that the conditional differential entropy term $h(X|X,Y)$ in (23) equals $-\infty$. Now, substituting $h(X|X,Y) = -\infty$ into (23), we can conclude that:

$$[\frac{1}{2}\log(2\pi eP) - h(X|X,Y) - \frac{1}{2}\log(1+\frac{g_e^2P}{\sigma_e^2})]^+ + \frac{1}{2}\log(2\pi e\sigma^2) = \infty, \quad (24)$$

and this leads to the fact that $R_{s-f}^{non**} = \frac{1}{2}\log(1+\frac{g^2P}{\sigma^2})$. The proof is complete. □

From Corollary 3, we see that R_{s-f}^{non**} is exactly the same as the secrecy capacity given in Theorem 1, which indicates that for the non-degraded Gaussian wiretap feedback channel, the improved secret key-based feedback scheme performs as well as the SK feedback scheme, and both of them achieve the secrecy capacity of this non-degraded model.

The following Figure 4 shows the comparison of the SK scheme, secret key-based scheme, and the improved secret key-based scheme for $g = 0.9$, $g_e = 0.7$, $\sigma^2 = 3$, $\sigma_e^2 = 10$, and P taking values in $[0, 1800]$. It is easy to see that the performance gap between the secret key-based scheme and other two schemes is increasing while the transmitting power P is increasing.

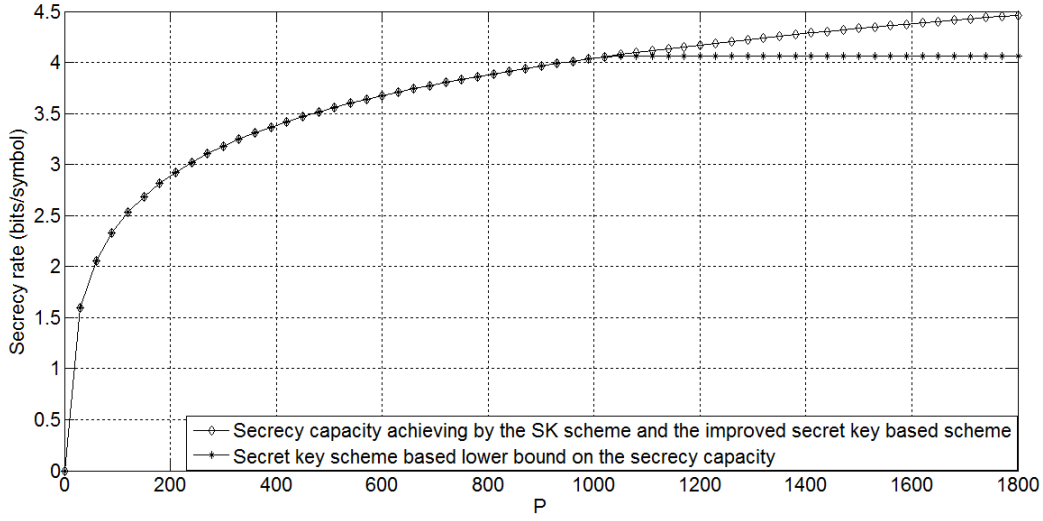

Figure 4. The capacity results on the non-degraded Gaussian wiretap feedback channel for $g = 0.9$, $g_e = 0.7$, $\sigma^2 = 3$, $\sigma_e^2 = 10$, and P taking values in $[0, 1800]$.

In addition, the following Figure 5 shows the comparison of the SK scheme, the secret key-based scheme, and the improved secret key-based scheme for $g = 0.9$, $g_e = 0.7$, $\sigma^2 = 3$, $\sigma_e^2 = 0.1$, and P taking values in $[0, 1800]$. Comparing Figure 5 with Figure 4, we can conclude that when the eavesdropper's channel noise variance is decreasing and the transmitting power P is increasing, the performance gap between the secret key-based scheme and other two schemes is increasing.

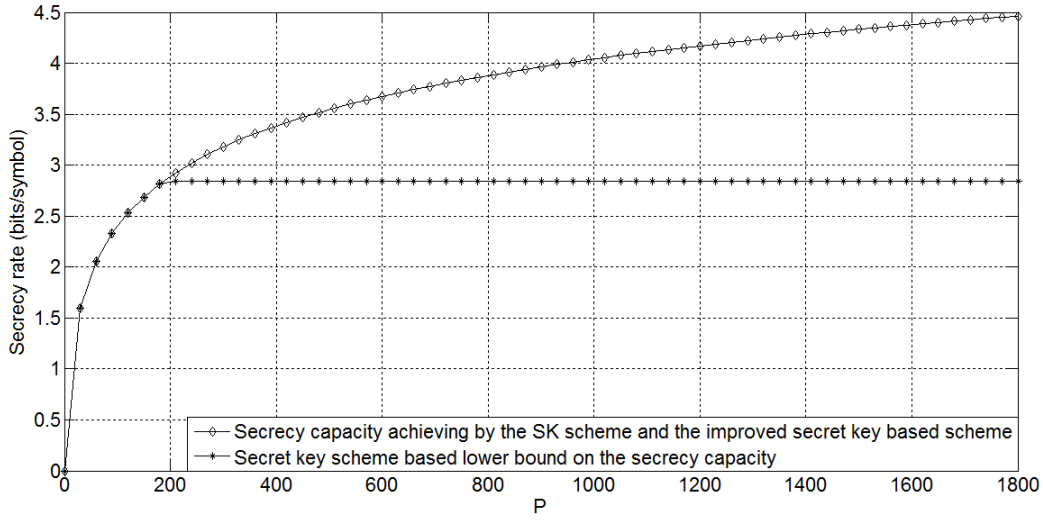

Figure 5. The capacity results on the non-degraded Gaussian wiretap feedback channel for $g = 0.9$, $g_e = 0.7$, $\sigma^2 = 3$, $\sigma_e^2 = 0.1$, and P taking values in $[0, 1800]$.

4. Conclusions

In this paper, we determined the secrecy capacity of the non-degraded Gaussian wiretap feedback channel and showed that it equals the channel capacity of the same model without the secrecy constraint. Moreover, we compared the performances of the SK scheme, the secret key-based scheme, and the improved secret key-based scheme in the Gaussian wiretap feedback channel and showed that for the non-degraded case, the improved secret key-based scheme performs as well as the SK scheme,

and both of them are better than the secret key-based scheme. Numerical results indicated that the performance gap between the secret key-based scheme and other two schemes was increasing while the eavesdropper's channel noise variance was decreasing and the transmitting power P was increasing.

Author Contributions: C.W. did the theoretical work, performed the experiments, analyzed the data, and drafted the work; B.D. designed the work, did the theoretical work, analyzed the data, performed the interpretation of the data, and revised the work; L.Y. did the theoretical work, performed the interpretation of the data, and revised the work; all of the authors approved of the version to be published and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work were appropriately investigated and resolved.

Funding: This work was supported by the National Natural Science Foundation of China under Grants 61671391, U1734209, 61571373, and 6161101297, the China Scholarship Council (File No. 201807005013), the EU Marie Sklodowska-Curie individual Fellowship under Grant 796426, and the 111 Project No. 111-2-14.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theor.* **1978**, *24*, 339–348.
3. Jameel, F.; Wyne, S.; Kaddoum, G.; Duong, T.Q. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. *IEEE Commun. Surv. Tuts.* **2018**, 1. [CrossRef]
4. Atallah, M.; Kaddoum, G. Secrecy analysis in wireless network with passive eavesdroppers by using partial cooperation. *IEEE Trans. Veh. Technol.* **2019**, *68*, 7225–7230. [CrossRef]
5. Atallah, M.; Kaddoum, G. Design and performance analysis of secure multicasting cooperative protocol for wireless sensor network applications. *arXiv* **2019**, arXiv: 1902.07345.
6. Liang, J.M.; Chen, J.J.; Cheng, H.H.; Tseng, Y.C. An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-Advanced networks for Internet of Things. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2013**, *3*, 13–22. [CrossRef]
7. Mukherjee, A. Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
8. Ahlswede, R.; Cai, N. Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder. In *General Theory of Information Transfer and Combinatorics*; Springer: Berlin, Germany, 2006; pp. 258–275.
9. Ardestanizadeh, E.; Franceschetti, M.; Javidi, T.; Kim, Y. Wiretap channel with secure rate-limited feedback. *IEEE Trans. Inf. Theor.* **2009**, *55*, 5353–5361. [CrossRef]
10. Schaefer, R.F.; Khisti, A.; Poor, H.V. Secure broadcasting using independent secret keys. *IEEE Trans. Commun.* **2018**, *66*, 644–661. [CrossRef]
11. Ekrem, E.; Ulukus, S. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP J. Wirel. Commun. Netw.* **2009**, *2009*, 824235. [CrossRef]
12. Cohen, A.; Cohen, A. Wiretap channel with causal state information and secure rate-limited feedback. *IEEE Trans. Commun.* **2016**, *64*, 1192–1203. [CrossRef]
13. Dai, B.; Han Vinck, A.J.; Luo, Y. Wiretap channel in the presence of action-dependent states and noiseless feedback. *J. Appl. Math.* **2013**, *2013*. [CrossRef]
14. Dai, B.; Ma, Z.; Fang, X. Feedback enhances the security of state-dependent degraded broadcast channels with confidential messages. *IEEE Trans. Inf. Forensic. Secur.* **2015**, *10*, 1529–1542. [CrossRef]
15. Dai, B.; Ma, Z.; Luo, Y. Finite state Markov wiretap channel with delayed feedback. *IEEE Trans. Inf. Forensic. Secur.* **2017**, *12*, 746–760. [CrossRef]
16. Dai, B.; Ma, Z.; Xiao, M.; Tang, X.; Fan, P. Secure communication over finite state multiple-access wiretap channel with delayed feedback. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 723–736. [CrossRef]
17. Dai, B.; Luo, Y. An improved feedback coding scheme for the wiretap channel. *IEEE Trans. Inf. Forensic. Secur.* **2019**, *14*, 262–271. [CrossRef]
18. Zhang, H.; Yu, L.; Dai, B. Feedback schemes for the action-dependent wiretap channel with noncausal state at the transmitter. *Entropy* **2019**, *21*, 278–292. [CrossRef]

19. Zhang, H.; Yu, L.; Wei, C.; Dai, B. A new feedback scheme for the state-dependent wiretap channel with noncausal state at the transmitter. *IEEE Access* **2019**, *7*, 45594–45604. [CrossRef]
20. Gunduz, D.; Brown, D.R.; Poor, H.V. Secret communication with feedback. In Proceedings of the 2008 International Symposium on Information Theory and Its Applications, Auckland, New Zealand, 7–10 December 2008.
21. Schalkwijk, J.P.M.; Kailath, T. A coding scheme for additive noise channels with feedback. part I: No bandwidth constraint. *IEEE Trans. Inf. Theor.* **1966**, *12*, 172–182. [CrossRef]
22. Li, C.; Liang, Y.; Poor, H.V.; Shamai, S. Secrecy capacity of colored Gaussian noise channels with feedback. *IEEE Trans. Inf. Theor.* **2019**, *65*, 5771–5782. [CrossRef]