Dai *et al. EURASIP Journal on Wireless Communications and Networking* (2020) 2020:58
https://doi.org/10.1186/s13638-020-01673-w

EURASIP Journal on Wireless Communications and Networking

REVIEW Open Access

Enhancing physical layer security via channel feedback: a survey

Bin Dai[1]*, Chong Li[2], Yingbin Liang[3], H. Vincent Poor[4] and Shlomo Shamai (Shitz)[5]

Abstract

Physical layer security (PLS), which is based on information-theoretic principles of message confidentiality, has attracted considerable attention in recent years. This paper provides a comprehensive survey of using channel feedback (CF) to enhance the quality of PLS of various communication models. To be specific, the survey starts from the secret key-based CF scheme and its variations for the wiretap channel (WTC) and other communication models. Then, for the WTC and its generalized models, an improved feedback scheme and its variations are respectively introduced, where the improved scheme combines the secret key-based CF scheme with the Wyner-Ziv scheme for source coding with side information. It has been shown that these improved schemes perform better than the original secret key-based schemes for several cases. Next, the Schalkwijk-Kailath (SK) feedback scheme and its variations are introduced, which are optimal for the Gaussian WTC and its variations. Finally, the already existing CF schemes are summarized and the future challenges of using CF to enhance PLS are discussed.

Keywords: Channel feedback, Physical layer security, Wiretap channel

1 Introduction

Due to the broadcast nature of wireless communications, mobile devices are vulnerable to eavesdropping. Physical layer security (PLS), which uses information-theoretic approaches to achieve secure transmission over wireless channels, has been proven to be an effective way to prevent information eavesdropping [1–10]. The study of PLS starts from Wyner's ground-breaking work on the wiretap channel (WTC) [11], where a transmitter broadcasts its message W over N channel uses to a legitimate receiver and a wiretapper via a degraded broadcast channel, and the perfect secrecy is guaranteed if the information leakage rate $\frac{1}{N}I(W;Z^N)$, where Z^N denotes the received output at the wiretapper, vanishes as the transmitted codeword length N tends to infinity[1]. The secrecy capacity, defined as the channel capacity under the perfect secrecy constraint, was established in [11]. Later, [12] generalized the WTC [11] 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 wiretapper. Here note that the secrecy capacities characterized in [11] and [12] indicate that positive secrecy rate is achieved 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 positive secrecy rate be achieved if the wiretapper's channel is less noisy than the legitimate receiver's channel?
- 2) If the wiretapper'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 and channel feedback (CF) 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 [13, 14], and hence CF is of particular interest in such circumstances.

*Correspondence: daibin@home.swjtu.edu.cn
[1] School of Information Science and Technology, Southwest JiaoTong University, 610031 Chengdu, China
Full list of author information is available at the end of the article

[1] Here note that the perfect secrecy defined in [11] is in fact perfect weak secrecy. Another definition of the perfect secrecy is perfect strong secrecy, which is defined as the information leakage $I(W;Z^N)$ at the wiretapper vanishes as N tends to infinity.

© The Author(s). 2020 **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

This paper provides a comprehensive review of CF techniques that help to enhance PLS in communication systems. The remainder of this paper is organized as follows. In Section 2, the model of the degraded WTC with CF [15] and its capacity-achieving feedback scheme (the secret key-based feedback scheme) are presented, and applications of the secret key-based feedback coding scheme to other communication channel models with CF are introduced. Section 3 introduces an improved secret key-based feedback coding scheme for the general WTC with CF and its applications to other channel models. In Section 4, first, we introduce the classical Schalkwijk-Kailath (SK) feedback scheme [58] for the Gaussian channel and show that this classical feedback scheme achieves the secrecy capacity of the Gaussian WTC with CF. Next, we introduce applications of the SK scheme to other channel models. Finally, in Section 5, we summarize this paper and discuss future research challenges.

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_1 denotes a RV, and y_1 denotes the value of a realization in the alphabet $\mathcal{Y}_1$. Similarly, $Y_{1,1}^N$ denotes a random vector $(Y_{1,1}, ..., Y_{1,N})$, and $y_{1,1}^N = (y_{1,1}, ..., y_{1,N})$ denotes the value of a realization in $\mathcal{Y}_1^N$ (the Nth Cartesian power of $\mathcal{Y}_1$). 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 2.

2 The secret key-based feedback scheme and its applications

2.1 The wiretap channel with noiseless feedback

The effect of CF on the PLS in communication systems was first investigated in [15], where the WTC [11] 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 wiretapper (see the following Fig. 1). In Fig. 1, the channel is a discrete memoryless broadcast channel with input X^N and outputs $Y_{1,1}^N$, $Y_{2,1}^N$, where $Y_{1,1}^N$ is for the legitimate receiver, and $Y_{2,1}^N$ is for the wiretapper. The channel transition probability is given by

$$P\left(y_{1,1}^N, y_{2,1}^N | x^N\right) = \prod_{i=1}^{N} P(y_{1,i}, y_{2,i} | x_i), \tag{1}$$

where $x_i \in \mathcal{X}$, $y_{1,i} \in \mathcal{Y}_1$, and $y_{2,i} \in \mathcal{Y}_2$. Let W be the transmission message, and it is uniformly drawn from the alphabet $\mathcal{W}$. At time $i \in \{1, 2, ..., N\}$, the transmitter produces the time-i channel input X_i as a function of the message W and the previous channel outputs $Y_{1,1}, ..., Y_{1,i-1}$, i.e.,

$$X_i = f_i\left(W, Y_{1,1}^{i-1}\right) \tag{2}$$

for some stochastic encoding function f_i.

First, note that without CF, the model of Fig. 1 reduces to the general WTC [12], and its secrecy capacity is given by

$$C_s = \max_{P(x|v),P(v)} \left[I(V;Y_1) - I(V;Y_2)\right]^+, \tag{3}$$

where the function $[x]^+ = \max\{x, 0\}$ and $V \rightarrow X \rightarrow (Y_1, Y_2)$ forms a Markov chain. The intuition behind the secrecy capacity C_s is that for the legitimate parties, in order to achieve perfect secrecy, the channel capacity $I(V;Y_1)$ suffers a loss of $I(V;Y_2)$, where the sacrificed rate $I(V;Y_2)$ is used to completely confuse the wiretapper.

Then, for the model of Fig. 1, [15] showed that its secrecy capacity C_s^f is lower bounded by

$$C_s^f \geq \max_{P(x|v),P(v)} \min\{[I(V;Y_1) - I(V;Y_2)]^+ + H(Y_1|Y_2,V), I(V;Y_1)\}, \tag{4}$$

where $V \rightarrow X \rightarrow (Y_1, Y_2)$. Comparing (4) with (3), we can conclude that the CF enhances the secrecy capacity of the general WTC. The intuition behind the lower bound (4) on the secrecy capacity C_s^f is given as follows. In [15], the feedback channel output is used to generate a secret key shared between the legitimate parties, and this key is completely unknown for the wiretapper. Moreover, the

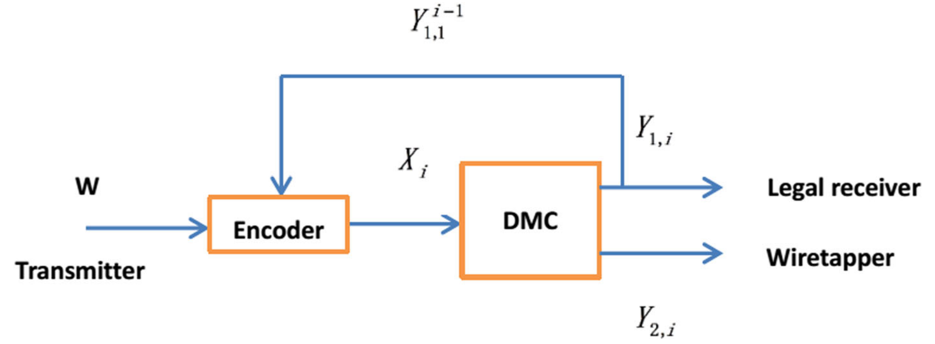

Fig. 1 The general WTC with noiseless feedback

transmitted message W is divided into two parts W_1 and W_2, where W_1 is encoded the same as the message in [11], and W_2 is encrypted by the secret key generated from the feedback. Then, the total secrecy rate also consists of two parts: one equals $I(V;Y_1) - I(V;Y_2)$ which is the same as C_s, and the other equals $H(Y_1|Y_2,V)$ which is the rate of the secret key. In addition, note that the total secrecy rate cannot exceed the channel capacity $I(V;Y_1)$ of the legitimate parties, and hence the lower bound in (4) on C_s^f is obtained.

Ahlswede and Cai [15] further pointed out that if the wiretapper's received signal Y_2 is a "degraded" version of the legitimate receiver's received signal Y_1, i.e., Markov chain $X \rightarrow Y_1 \rightarrow Y_2$ holds, the secrecy capacity C_s^f of the model of Fig. 1 is established, which is given by

$$C_s^f = \max_{P(x)} \min\{I(X;Y_1) - I(X;Y_2) + H(Y_1|X,Y_2), I(X;Y_1)\}. \tag{5}$$

Here note that for the degraded WTC ($X \rightarrow Y_1 \rightarrow Y_2$), [11] showed that its secrecy capacity is given by

$$C_s = \max_{P(x)} [I(X;Y_1) - I(X;Y_2)]\,. \tag{6}$$

Comparing (5) with (6), we can also conclude that the CF enhances the secrecy capacity of the degraded WTC.

The secrecy capacity C_s^f for the reversely degraded case (i.e., Markov chain $X \rightarrow Y_2 \rightarrow Y_1$ holds) is also determined in [15], and it is given by

$$C_s^f = \max_{P(x)} \min\{H(Y_1|Y_2), I(X;Y_1)\}. \tag{7}$$

However, note that for this reversely degraded case, the secrecy capacity C_s of the WTC equals 0, which also implies that CF enhances the secrecy capacity of the reversely degraded WTC. Moreover, recently, the secrecy capacity C_s^f for the case of parallel channels ($Y_1 \rightarrow X \rightarrow Y_2$) is studied in [16], and it has been shown that C_s^f is determined when one of the channels is more capable than the other.

In recent years, the secret key-based feedback scheme introduced in this section has been widely used in various channel models, and we introduce the applications of the secret key-based feedback scheme in the next subsection.

2.2 Applications of the secret key-based feedback scheme to other channel models

In the preceding subsection, we review the WTC with noiseless feedback, where 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? [17] investigated this case and pointed out that the best way is to transmit random bits over the noiseless feedback channel, and these random bits are used to encrypt the transmitted message as the secret key in [15] does. In addition, the feedback channel in [17] is assumed to be rate limited, i.e., the rate of the secret key is upper bounded by R_f. Using a similar coding scheme of [15], [17] determined the secrecy capacity C_s^{f-l} of the degraded WTC with rate limited feedback, and it is given by

$$C_s^{f-l} = \max_{P(x)} \min\{I(X;Y_1) - I(X;Y_2) + R_f, I(X;Y_1)\}. \tag{8}$$

Comparing (8) with (5), we can conclude that if $R_f \geq H(Y_1|X,Y_2)$, sending pure random bits is better than sending legitimate receiver's channel output Y_1, and vice versa. The follow-up study of [17] includes

- 1) Extension of the degraded WTC with rate limited feedback [17] to a situation that an additional common message together with the secret message are sent by the transmitter, and the common message can be decoded by both the legitimate receiver and the wiretapper [18].
- 2) Extension of the WTC with rate limited feedback [17] to a broadcast situation [19], 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, [19–21] 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 [22, 23].
- 3) Extension of the WTC with rate limited feedback [17] to the case that the channel depends on channel state information (CSI), and the CSI is causally known[2] by the transmitter and the legitimate receiver [24]. Since the CSI is shared between the legitimate parties, it can be used to generate secret key as the channel output feedback in [15] does. Hence, the transmitted message is encrypted by two keys, where one is the random bits generated from the rate limited feedback channel, and the other is generated from the CSI. Cohen and Cohen [24] proved that this

[2] Here, note that causal CSI indicates that the transmitter has the knowledge of current and previous CSI, while non-causal CSI indicates that the transmitter has the knowledge of current, previous, and future CSI.

new scheme performs better than that in [17] due to the additional secret key generated from the CSI.

Besides the work of [24], recently, the use of CSI-feedback as a means to generate secret keys receives a lot of attention. In [25], the general WTC with CSI causally known at both the legitimate receiver and the transmitter was investigated. A lower bound on the secrecy capacity, which is constructed according to the secret key-based feedback scheme (the secret key is generated from the CSI which is causally known by both the legitimate receiver and the transmitter), is provided in [25], and this lower bound is shown to be tight for several special cases. In [26], a broadcast erasure channel with one transmitter and multiple receivers was studied, where the transmitter sends messages to multiple receivers, the message to each receiver remains secret from all the other receivers, and the receivers causally feed back their CSI to the transmitter. The capacity is characterized according to a linear complexity two-phase scheme: in the first phase, secret keys are produced which are exploited during the second phase to encrypt each message. In [27], a secret key-based feedback scheme was proposed for the WTC with the feedback of the legitimate receiver's CSI and without the feedback of the wiretapper's CSI.

Other applications of the secret key-based feedback scheme include

- *a*) Extension of the WTC with noiseless channel output feedback [15] to the case that the channel depends on independent identically distributed (i.i.d.) CSI and the CSI is non-causally known by the transmitter [28–30]. This extended model is also called the state-dependent WTC with noiseless feedback and noncausal CSI at the transmitter. Similarly to the WTC with noiseless feedback [15], the secrecy capacity of this state-dependent model is determined for the degraded case $X \to Y_1 \to Y_2$ (the wiretapper's received signal is a degraded version of the legitimate receiver's), where the capacity-achieving coding scheme combines the already existing coding scheme for the same model without channel output feedback [31, 32] and the secret key-based feedback scheme [15]. Here, note that the CSI in [28–30] is independent of the transmitted message. Recently, [33, 34] further extended the model of [28–30] to the situation that the transmitter can take action on the CSI (i.e., the CSI is dependent on the transmitted message). Similarly, it is shown that the secrecy capacity of the model in [33, 34] is determined for the degraded case, and the corresponding capacity-achieving coding scheme combines the already existing coding scheme for the same model without feedback [35] and the secret key-based feedback scheme [15].
- *b*) Extension of the WTC with noiseless channel output feedback [15] to the case that the channel depends on CSI which is not i.i.d. generated, and the CSI is known by both the transmitter and the legitimate receiver [36]. To be specific, in [36], the CSI is assumed to be generated from a state process which is a stationary irreducible aperiodic ergodic Markov chain. The CSI is perfectly known by the legitimate receiver, and the CSI together with the legitimate receiver's received channel output are sent back to the transmitter via a noiseless feedback channel after some delay. The secrecy capacity of this model is determined for the degraded case, and the corresponding capacity-achieving coding scheme combines the already existing coding scheme for the same model without secrecy constraint [37] and the secret key-based feedback scheme [15].
- *c*) Extension of the WTC with noiseless feedback [15] to the WTC with noisy feedback. To be specific, in [38], the modulo-additive WTC with a full-duplex legitimate receiver was studied. The noisy feedback is used to generate pure noise (random bits) protecting the transmitted message and confusing the wiretapper. This feedback scheme is similar to the secret key-based scheme and it achieves the legitimate receiver's channel capacity, i.e., the perfect secrecy is guaranteed at no rate cost. Later, [39, 40] considered a more general case, i.e., the WTC with generalized feedback, where the generalized feedback includes many already existing feedback scenarios in the literature such as CSI feedback, noiseless channel output feedback, and noisy channel output feedback. A lower bound on the secrecy capacity of this generalized model is constructed according to the secret key-based feedback scheme. Yang et al. [41] considered a variation of the wiretap channel with noisy feedback and proposed a feedback scheme similar to that of [38]. It is shown in [41] that if the transmission power is large enough, a positive secrecy rate can be achieved even when the wiretapper's channel is less noisy. Kim and Poor [42] studied the multiple-input multiple-output (MIMO) WTC with noisy and insecure feedback, and proposed a secret key-based feedback scheme for this model. Recently, the role of noisy feedback in Gaussian full-duplex two-way wiretap channel and Gaussian half-duplex two-way relay channel was investigated [43], and a feedback scheme similar to that of [38] was proposed to protect the transmitted message.
- *d*) Extension of the WTC with noiseless feedback [15] to other multi-user communication scenarios with feedback. To be specific, in [44, 45], the multiple-access wiretap channel (MAC-WT) with generalized

feedback was investigated, where the feedback is only used to allow the transmitters to cooperate with each other. Combining the feedback scheme of [44] with the secret key-based feedback scheme [15], [46] proposed a new feedback scheme for the MAC-WT, where the feedback channel output is not only used to generate secret keys encrypting the messages sent by the transmitters, but also used to allow the transmitters to cooperate with each other. Dai and Ma [46] proved that this secret key-based new feedback scheme is better than the previous one in [44, 45]. Based on the work of [46], a similar feedback scheme is proposed for the state-dependent MAC-WT [47], where the MAC-WT depends on CSI which is generated the same as that in [36], and the CSI together with the legitimate receiver's channel output are sent to the transmitters via noiseless feedback channels after some delay. In addition, [48] studied the two way wiretap channel with noiseless feedback and designed a practical code for this model which combines the low density parity check (LDPC) code and the secret key-based feedback scheme.

- *e*) Investigation of how to realize the secret key sharing between the legitimate parties via feedback channels. To be specific, [49] investigated key agreement over a multiple-access scenario with noisy or noiseless public feedback channel, [50] investigated key agreement over an interference channel with noiseless feedback channel, [51, 52] studied key agreement over the wiretap channel model with noiseless public feedback channel, and [53, 54] studied the noisy feedback case. Other related works in the key agreement over channels are in [55–57].

In the next section, we introduce an improved secret key-based feedback scheme, which uses the channel output feedback to generate not only secret keys, but also help information improving the legitimate receiver's decoding performance.

3 An improved secret key-based feedback scheme and its applications

3.1 New result on the general WTC with noiseless feedback

In the previous section, we have introduced the widely used secret key-based feedback scheme. However, we should note that this scheme is not optimal for the general WTC, and it is natural to ask: can any other feedback schemes do better than the secret key-based scheme? The answer is yes, and currently there are two kinds of feedback schemes that perform better than the secret key-based scheme. One is the improved secret key-based scheme introduced in this section, and the other is the Schalkwijk-Kailath (SK) feedback scheme [58] that will be introduced in the next section. In the remainder of this section, first, we introduce the improved secret key-based feedback scheme for the general WTC. Next, we introduce the applications of this new scheme to other channel models.

A vital part of the improved secret key-based feedback scheme is the classical Wyner-Ziv (WZ) coding scheme [59], and it is used in the lossless source coding with side information (see the following Fig. 2). In Fig. 2, the source sequence X^N together with the correlated side information Y^N are i.i.d. generated according to the probability $P(x,y)$. Using an encoding function $\phi : \mathcal{X}^N \rightarrow \{1, 2, ..., 2^{\mathrm{NR}}\}$, the transmitter compresses X^N into an index W taking values in $\{1, 2, ..., 2^{\mathrm{NR}}\}$, and W together with Y^N are perfectly obtained by the receiver. The receiver produces a reconstruction sequence $\hat{U}^N = \varphi(W, Y^N)$ by applying a reconstruction function $\varphi : \{1, 2, ..., 2^{\mathrm{NR}}\} \times \mathcal{Y}^N \rightarrow \mathcal{U}^N$ to the index W and the side information Y^N. The object of the communication is that the reconstruction sequence $\hat{U}^N$ is jointly typical with the source X^N according to the probability $P(u,x)$, i.e., $(X^N, \hat{U}^N) \in T_{\epsilon}^N(P(x,u))$.

A rate R is achievable if for any $\epsilon > 0$, there exists a sequence of encoding and reconstruction functions (ϕ, φ) such that

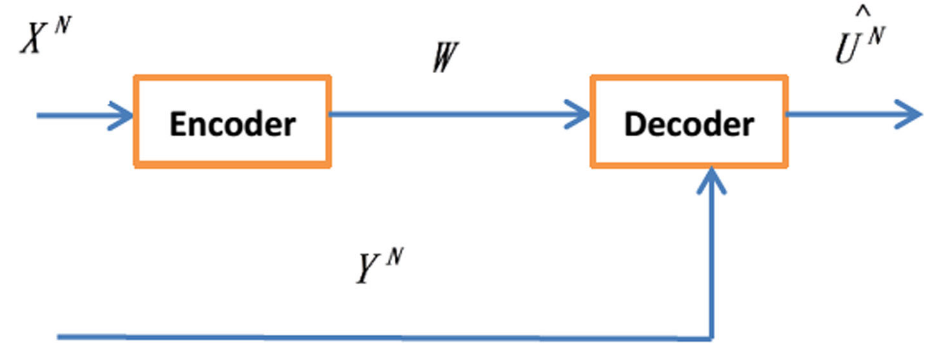

Fig. 2 The lossless source coding with side information

$$Pr\{(X^N, \hat{U}^N) \notin T_\epsilon^N(P(x,u))\} \to 0 \tag{9}$$

as $N \to \infty$. The minimum achievable rate R of this lossless source coding with side information problem is achieved by using the classical WZ scheme [59], and the key idea of the WZ scheme is described as follows:

- First, generate an auxiliary random sequence U^N i.i.d. with respect to the probability $P(u)$, and U^N is chosen according to a bin index and a sub-index in a given bin.
- Next, the source encoder tries to find a U^N that is jointly typical with the source X^N. If there exists such U^N, the source encoder extracts the corresponding bin index W from U^N and sends W as the output of the source encoder.
- Finally, once the receiver obtains W and the side information Y^N, it tries to find a unique $\hat{U}^N$ that belongs to the bin W and is jointly typical with Y^N. If such $\hat{U}^N$ exists, choose it as the output of the source decoder.

Inspired by the above WZ scheme, [60] proposed a new feedback scheme for the general WTC, which combines the secret key-based feedback scheme [15] and the WZ scheme [59]. This scheme is described below.

- First, note that for the general WTC with noiseless feedback shown in Fig. 1, the legitimate receiver's received signal $Y_{1,1}^N$ is similar to the side information Y^N in the lossless source coding with side information as shown in Fig. 2.
- Next, differently from the feedback scheme of [15], the feedback channel output is not only used to generate secret key, but also used as the side information Y^N in the WZ scheme. Hence, in each transmitted block, besides generating the transmitted codeword X^N, an auxiliary sequence U^N which is similar to that in WZ scheme is also generated. Similarly to the WZ scheme, the indexes of U^N are chosen by finding a U^N that is jointly typical with X^N and the feedback (side information) $Y_{1,1}^N$. If there exists such U^N, extract the corresponding bin index W^* from U^N, and let W^* together with the encrypted transmitted message be the indexes of X^N for the next transmission.
- The legitimate receiver does backward decoding. First, viewing $Y_{1,1}^N$ as the side information, the legitimate receiver applies the WZ decoding scheme to decode U^N. Next, viewing $Y_{1,1}^N$ together with the decoded U^N as the received signal, the legitimate receiver applies the secret key-based feedback scheme of [15] to decode the codeword X^N and extract the encrypted message. Finally, since the secret key is known by the legitimate receiver, the transmitted message is decrypted.

Using the above new feedback scheme, a new lower bound R_s^* on the secrecy capacity C_s^f of the general WTC with feedback is given by

$$\begin{aligned} C_s^f \geq R_s^* = \max_{P(u|y_1,v),P(x|v),P(v)} & \min\{[I(V;Y_1,U) - I(V;Y_2)]^+ \\ & + H(Y_1|Y_2,V), \\ I(V;Y_1)\}, \end{aligned} \tag{10}$$

where the joint distribution is denoted by

$$P(u,v,x,y_1,y_2) = P(u|v,y_1)P(y_1,y_2|x)P(x|v)P(v). \tag{11}$$

Comparing (10) with (4), we can conclude that for the general WTC with feedback, the new feedback scheme is better than the secret key-based feedback scheme because $I(V;Y_1,U) \geq I(V;Y_1)$, and the new feedback scheme generalizes the secret key-based feedback scheme because (10) reduces to (4) when U becomes a constant.

3.2 Applications of the improved secret key-based feedback scheme to other channel models

In this subsection, we introduce some applications of the new feedback scheme introduced in the preceding subsection to other channel models.

- Extension of the WTC with noiseless feedback to other multi-user channel models with feedback. To be specific, in [61], the broadcast channel with two confidential messages and noiseless feedback [61] was investigated, where a transmitter wishes to send two independent messages to two receivers via a general broadcast channel, each receiver can successfully decode its intended message and attempts to overhear the other one's intended message, and the receivers send their received signals back to the transmitter via two independent noiseless feedback channels. For this extended model, a new feedback scheme which is an extension of the improved secret key-based feedback scheme for the WTC with noiseless feedback [60] is proposed, and it combines a generalized WZ scheme [62] (see Fig. 3) for the distributed source coding with side information problem[3], the secret key-based feedback scheme [15] and the coding scheme for the broadcast channel with two confidential messages

[3] The generalized WZ scheme shown in Fig. 3 can be viewed as an extension of the source coding with side information problem in Fig. 2, where the source X^N is compressed into three indexes W_0^*, W_1^*, and W_2^*. The indexes W_0^*, W_j^* ($j \in \{1,2\}$) together with the side information $Y_{j,1}^N$ are decoded into a reconstruction sequence $\hat{U}_{j,1}^N$. The object of the communication is that for $j \in \{1,2\}$, the reconstruction sequence $\hat{U}_{j,1}^N$ is jointly typical with the source X^N according to the probability $P(u_j, x)$.

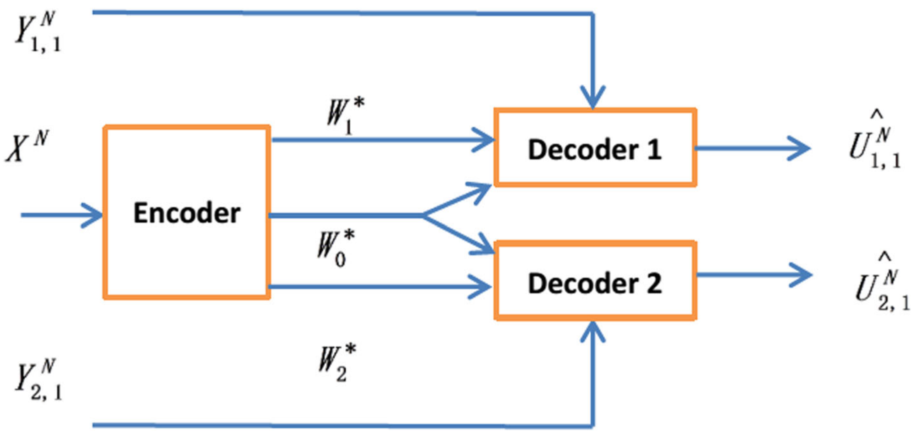

Fig. 3 The distributed source coding with side information

[63, 64]. From a Dueck-type example of this extended model, [61] showed that the proposed feedback scheme may perform better than the secret key-based feedback scheme for several special cases. In addition, for the broadcast channel with one common message, one confidential message and noiseless feedback, [65] proposed a feedback scheme combining the WZ scheme [59], the secret key-based feedback scheme [15] and the coding scheme of [12], and showed that this new scheme performs better than the secret key-based feedback scheme for some cases.

- Extension of the WTC with noiseless feedback to the case that the channel depends on i.i.d. CSI which is non-causally known by the transmitter. To be specific, for the wiretap channel with i.i.d. CSI non-causally known by the transmitter, [66] proposed a variation of the improved secret key-based feedback scheme [60] which combines the WZ scheme [59] and the already existing secret key-based feedback scheme of the same model [28, 30], and proved that the proposed feedback scheme is better than the already existing one. Based on the work of [66, 67] further extended the model of [66] to the situation that the transmitter can take action on the i.i.d. CSI and proposed a feedback scheme similarly to that of [66] for this extended model.

Here, note that though the improved secret key-based feedback scheme introduced in this section is better than the original one for some general channel models (without degradedness assumption), it is still not the optimal feedback scheme. In the next section, we introduce the Schalkwijk-Kailath (SK) feedback scheme for the Gaussian channel with feedback and show that it achieves the secrecy capacity of the Gaussian wiretap channel with noiseless feedback, i.e., for the Gaussian wiretap channel, the SK scheme is the optimal feedback scheme.

4 The Schalkwijk-Kailath feedback scheme and its applications

4.1 The capacity-achieving scheme for the Gaussian wiretap channel with noiseless feedback

In this subsection, we first introduce the classical SK scheme for the Gaussian channel with feedback, and then we show that this scheme also achieves the secrecy capacity of the Gaussian wiretap channel with feedback. For the Gaussian channel with noiseless feedback, the channel input and output at time $i \in \{1, 2, ..., N\}$ satisfy

$$Y_i = X_i + \eta_i, \tag{12}$$

where X_i is the channel input subject to an average power constraint P, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$ is the channel noise and is i.i.d. across the time index i. The ith channel input X_i is a function of the message W and the channel feedback Y^{i-1}. It is well known that the capacity C_{gf} of the Gaussian channel with feedback equals

$$C_{gf} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma^2}\right). \tag{13}$$

In [58], it has been shown that the classical SK scheme achieves C_{gf}, and this scheme is described below.

Suppose that the transmitted message W takes values in $\mathcal{W} = \{1, 2, ..., 2^{\mathrm{NR}}\}$. 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 $\mathcal{W}$. Let θ be the center of the sub-interval with respect to the choosing message W. At time 1,

$$X_1 = \theta\alpha \tag{14}$$

is sent by the transmitter, where $\alpha = \sqrt{\frac{P+\sigma^2}{\sigma^2}}$. Upon receiving the output $Y_1 = X_1 + \eta_1$, the receiver computes

$$\hat{\theta}_1 = \frac{Y_1}{\alpha} = \theta + \frac{\eta_1}{\alpha} \tag{15}$$

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

$$X_i = \alpha_i(\theta - \hat{\theta}_{i-1}) = -\alpha_i \frac{\sum_{j=1}^{i-1} \alpha_j \eta_j}{\sum_{j=1}^{i-1} \alpha_j^2} \tag{16}$$

is sent by the transmitter, where $\alpha_i = \sqrt{\frac{P}{\sigma^2}} \alpha^{i-1}$ for $i \in \{2, 3, ..., N\}$. Upon receiving the output $Y_i = X_i + \eta_i$, the receiver computes

$$\hat{X}_i = \hat{\theta}_{i-1} + \frac{Y_i}{\alpha_i}, \tag{17}$$

$$\hat{\theta}_i = \frac{\sum_{j=1}^{i} \alpha_j^2 \hat{X}_j}{\sum_{j=1}^{i} \alpha_j^2} = \theta + \frac{\sum_{j=1}^{i} \alpha_j \eta_j}{\sum_{j=1}^{i} \alpha_j^2} \tag{18}$$

as an estimation of θ at time i. In [58], it has been shown that the decoding error probability P_e (the probability that $\hat{\theta}_N$ does not belong to the sub-interval of the choosing message W) of this proposed scheme doubly exponentially decays to 0 for sufficiently large N if $R \leq \frac{1}{2} \log\left(1 + \frac{P}{\sigma^2}\right)$.

Now, we turn to the Gaussian WTC with noiseless feedback (see Fig. 4). In Fig. 4, the channel input and outputs at time i satisfy

$$Y_i = X_i + \eta_{1,i}, \quad Z_i = X_i + \eta_{1,i} + \eta_{2,i}, \tag{19}$$

where X_i is the channel input with the power constraint P, Y_i, and Z_i are the channel outputs respectively at the legitimate receiver and the wiretapper, and $\eta_{1,i} \sim \mathcal{N}\left(0, \sigma_1^2\right)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are independent channel noises and are i.i.d. across the time index i. The ith channel input X_i is a function of the message W and the channel feedback Y^{i-1}.

Recently, [68] showed that the SK scheme also achieves the secrecy capacity $\mathcal{C}_{s-gf}$ of the Gaussian wiretap channel with noiseless feedback, and $\mathcal{C}_{s-gf} = \mathcal{C}_{gf}$, which indicates that the perfect secrecy can be achieved without loss of transmission rate. The intuition behind this result is that the transmitter transmits the original message only at the first transmission (see (14) and (16)), 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 leakage rate $\frac{1}{N} I(W; Z^N)$ vanishes as the codeword length N tends to infinity. Hence, the perfect secrecy can be achieved even when the transmission rate is up to the channel capacity $\mathcal{C}_{gf}$.

4.2 Applications of the SK scheme to other channel models

In this subsection, we introduce some applications of the SK scheme introduced in the preceding subsection to other channel models.

- Extension of the Gaussian WTC with noiseless feedback to other Gaussian-type channels with feedback. To be specific, [69–71] investigated the finite-order autoregressive moving average (ARMA) Gaussian wiretap channel with noiseless feedback. Variations of the SK scheme are proposed to achieve the secrecy capacity, which equals the capacity of the same model without secrecy constraint. Similar to the SK scheme, the intuition of the proposed variations is that the transmitter transmits a (scaled) message only in the first d transmissions, in which d is determined by the order of the ARMA Gaussian channel. In the sequential transmissions, the transmitter only transmits the projected values of the past noise to refine legitimate receiver's estimate. By doing so, the wiretapper only receives some leakage of the message in the first few transmissions and 0 leakage in the

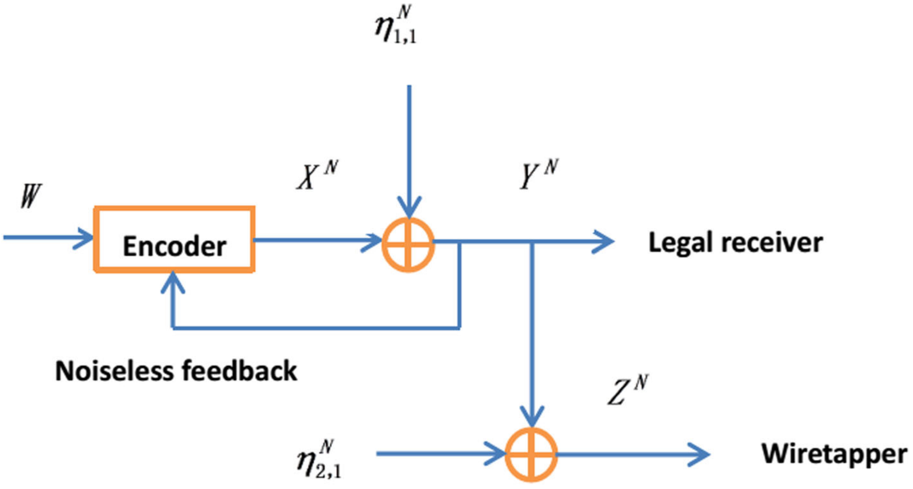

Fig. 4 The Gaussian WTC with noiseless feedback

sequential transmissions. As a result, the averaged leakage tends to be 0. Furthermore, [71] extended the results to AWGN channels with quantized feedback, which is an initial step towards understanding the secrecy capacity of noisy feedback Gaussian channels. Li et al. [71] showed that the proposed variation of the SK scheme can achieve a positive secrecy rate, which converges to the AWGN capacity as the feedback noise decreases (in terms of the noise's variance).

- Extension of the Gaussian WTC with noiseless feedback to the case that the channel is equipped with i.i.d. interference which is non-causally known by the transmitter. To be specific, for the Gaussian channel with i.i.d. interference non-causally known by the transmitter (also known as the dirty paper channel [72]), a modified SK feedback scheme [73] is shown to achieve its feedback capacity, where the main difference between the modified SK scheme and the SK scheme is the transmission of the original message. Namely, in the modified SK scheme, the original message is transmitted through all transmissions, while in the SK scheme, it is transmitted only at the first transmission. Based on the work of [73], [74] further showed that the modified SK scheme in [73] also achieves the secrecy capacity of the dirty paper channel with noiseless feedback and a wiretapper (also called the dirty paper wiretap feedback channel), and the secrecy capacity equals the capacity of the dirty paper channel with noiseless feedback, i.e., the secrecy constraint does not reduce the capacity. The intuition behind this result is that for the modified SK scheme, though the original message is transmitted through all transmissions, the amount of leakage information to the wiretapper is shrinking exponentially, and hence the information leakage rate still vanishes as the codeword length tends to infinity. In addition, [74] further extended the dirty paper wiretap feedback channel to the situation that the transmitter can take action on the i.i.d. interference and found that since the interference and the action are known by the transmitter, the channel input can be designed to be linear combination of the interference and the action, and this leads to the equivalence of the extended model and the Gaussian wiretap channel with feedback (see Fig. 4). Then, applying the original SK scheme as used in [68], a lower bound on the secrecy capacity of the extended model is obtained, and this lower bound is shown to be tight for a special case.

5 Conclusions and future work

Secure communication over wireless channels is one of the most pressing problems in the development of 5G networks. Physical layer security (PLS) is a promising approach to addressing this problem, and in this paper, we have addressed the role of channel feedback in enhancing the PLS. In particular, we have summarized existing feedback schemes, including the secret key-based feedback scheme, the improved secret key-based feedback scheme and the SK scheme. Moreover, applications of the three feedback techniques mentioned above to various communication channel models have been presented in this survey.

For the current channel feedback techniques, there are still open questions to be resolved, and they are summarized as follows:

- For the general WTC, the optimal feedback scheme is still not known, i.e., what is the secrecy capacity of the general WTC with noiseless feedback, and how to achieve it?
- What are the optimal feedback schemes for multi-user channel models (such as the broadcast channel, multiple-access channel, two way channel [75], relay channel, etc.) with secrecy constraints?
- It has been shown that the SK scheme and its variations are optimal for some Gaussian wiretap feedback channel models, and the secrecy capacities of these feedback models equal the capacities of the same models without secrecy constraints. Are these feedback schemes still optimal for Gaussian multi-user channel models (such as the Gaussian broadcast channel, Gaussian multiple-access channel, and Gaussian relay channel) with secrecy constraints, and the secrecy capacity regions of these feedback multi-user models also equal the capacity regions of the same models without secrecy constraints?
- In [76], it has been shown that for the broadcast channel with two legitimate receivers and one wiretapper (also called the broadcast wiretap channel), the perfect secrecy can be guaranteed by using Marton's coding scheme [77] for the general broadcast channel. Can we combine Marton's coding scheme [77] and channel feedback to further enhance the achievable secrecy rate region of the broadcast wiretap channel?
- In practical wireless communication scenarios, the feedback CSI from the legitimate receiver to the transmitter is often imperfect [78–80]. How can we use the imperfect CSI feedback to enhance secrecy capacities of various wireless wiretap channel models?

These questions are important topics for future research in this field.

Abbreviations

ARMA: Autoregressive moving average; CF: Channel feedback; CSI: Channel state information; IoT: Internet of Things; LDPC: Low-density parity check; MAC-WT: Multiple-access wiretap channel; PLS: Physical layer security; PLS: Wiretap channel; RV: Random variable; SK: Schalkwijk-Kailath

Authors' contributions

BD, CL, and YL drafted the manuscript. HVP and SS helped to draft the manuscript. All authors read and approved the final manuscript.

Funding

The work of Bin Dai was supported by the National Natural Science Foundation of China under Grants 61671391, U1734209 and U1709219, Key Project of Sichuan Province (No. 2017SZYZF0002), the China Scholarship Council (file No. 201807005013), and the 111 Project No.111-2-14. The work of Yingbin Liang was supported by the U.S. National Science Foundation under Grant CCF-1801846. The work of H. Vincent Poor was supported by the U.S. National Science Foundation under grants CCF-0939370 and CCF-1513915. The work of Shlomo Shamai was supported by the European Union's Horizon 2020 Research And Innovation Programme under grant 694630.

Availability of data and materials

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests

The authors declare that they have no competing interests.

Author details

[1]School of Information Science and Technology, Southwest JiaoTong University, 610031 Chengdu, China. [2]Nakamoto & Turing Labs, New York,10018 USA. [3]Department of Electrical and Computer Engineering, The Ohio State University, 43220 Columbus, USA. [4]Department of Electrical Engineering, Princeton University, 08544 Princeton, NJ, USA. [5]Department of Electrical Engineering, Technion-Israel Institute of Technology, 32000 Technion City, Israel.

Received: 2 August 2019 Accepted: 18 February 2020
Published online: 05 March 2020

References

1. Y. Liang, H. Vincent Poor, S. Shamai (Shitz), *Information Theoretic Security*. (Foundations and Trends in Communications and NOW Publishers, Hanover, 2009)
2. R. F. Schaefer, H. V. Poor, Wireless physical layer security. Proc. Nat. Acad. Sci. U.S.A. **114**(1), 19–26 (2017)
3. Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends. Proc. IEEE. **104**(9), 1727–1765 (2016)
4. Y. Liu, H. Chen, L. Wang, Physical layer security for next generation wireless networks: Theories, technologies, and challenges. IEEE Commun. Surv. Tutor. **19**(1), 347–376 (2017)
5. X. Zhou, L. Song, Y. Zhang, Physical Layer Security in Wireless Communications (2016)
6. Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, X. Gao, A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Sel. Areas Commun. **36**(4), 679–695 (2018)
7. A. Mukherjee, S. A. Fakoorian, J. Huang, A. L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
8. F. Jameel, S. Wyne, G. Kaddoum, T. Q. Duong, A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Commun. Surv. Tutor. **21**(3), 2734–2771 (2019)
9. M. Bloch, J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. (Cambridge University Press, Cambridge, 2011)
10. T. Q. Duong, X. Zhou, H. V. Poor, *Trusted communications with physical layer security for 5G and beyond*. (IET Publisher, UK, 2016)
11. A. D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
12. I. Csiszár, J. Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **24**(3), 339–348 (1978)
13. J. M. Liang, J. J. Chen, H. H. Cheng, Y. C. Tseng, An energy-efficient sleep scheduling with QoS consideration in 3GPP LTE-Advanced networks for Internet of Things. IEEE J. Emerg. Sel. Top. Circuits Syst. **3**(1), 13–22 (2013)
14. A. Mukherjee, Physical-layer security in the Internet of Things: sensing and communication confidentiality under resource constraints. Proc. IEEE. **103**(10), 1747–1761 (2015)
15. R. Ahlswede, N. Cai, *General Theory of Information Transfer and Combinatorics*. (Springer-Verlag, Berlin, 2006)
16. B. Dai, A. J. Han Vinck, Y. Luo, Z. Zhuang, in *2012 IEEE International Symposium on Information Theory Proceedings*. Capacity region of non-degraded wiretap channel with noiseless feedback (IEEE, Boston, 2012), pp. 244–248
17. E. Ardestanizadeh, M. Franceschetti, T. Javidi, Y. Kim, Wiretap channel with secure rate-limited feedback. IEEE Trans. Inf. Theory. **55**(12), 5353–5361 (2009)
18. X. Yin, L. Pang, Z. Xue, Y. Zhou, in *2013 8th International Conference on Communications and Networking in China (CHINACOM)*. Degraded broadcast channels with rate-limited feedback (IEEE, 2013). https://doi.org/10.1109/chinacom.2013.6694724
19. R. F. Schaefer, A. Khisti, H. V. Poor, Secure broadcasting using independent secret keys. IEEE Trans. Commun. **66**(2), 644–661 (2018)
20. R. F. Schaefer, A. Khisti, H. V. Poor, in *2015 IEEE International Symposium on Information Theory (ISIT)*. How to use independent secret keys for secure broadcasting of common messages (IEEE, 2015). https://doi.org/10.1109/isit.2015.7282800
21. R. F. Schaefer, A. Khisti, in *2014 48th Annual Conference on Information Sciences and Systems (CISS)*. Secure broadcasting of a common message with independent secret keys (IEEE, 2014). https://doi.org/10.1109/ciss.2014.6814137
22. E. Ekrem, S. Ulukus, Secrecy capacity of a class of broadcast channels with an eavesdropper. EURASIP J. Wirel. Commun. Netw. **2009**(1) (2009). https://doi.org/10.1155/2009/824235
23. G. Bagherikaram, A. S. Motahari, A. K. Khandani, in *Proceedings of the Allerton Conference on Communications, Control and Computing*. Secure broadcasting: The secrecy rate region (IEEE, 2008), pp. 834–841
24. A. Cohen, A. Cohen, Wiretap channel with causal state information and secure rate-limited feedback. IEEE Trans. Commun. **64**(3), 1192–1203 (2016)
25. Y.-K. Chia, A. El Gamal, Wiretap channel with causal state information. IEEE Trans. Inf. Theory. **58**(5), 2838–2849 (2012)
26. L. Czap, V. M. Prabhakaran, C. Fragouli, S. N. Diggavi, Secret communication over broadcast erasure channels with state-feedback. IEEE Trans. Inf. Theory. **61**(9), 4788–4808 (2015)
27. H. He, P. Ren, L. Sun, Q. Du, Y. Wang, in *2016 IEEE Global Communications Conference (GLOBECOM)*. Secure communication using noisy feedback (IEEE, Washington, 2016). https://doi.org/10.1109/glocom.2016.7842249
28. B. Dai, Z. Ma, X. Fang, Feedback enhances the security of state-dependent degraded broadcast channels with confidential messages. IEEE Trans. Inf. Forensics Secur. **10**(7), 1529–1542 (2015)
29. B. Dai, Z. Ma, L. Yu, Feeding back the output or sharing state, which is better for the state-dependent degraded wiretap channel with noncausal csi at the transmitter? Entropy. **17**(12), 7900–7925 (2015)
30. B. Dai, A. H. Vinck, Y. Wang, Feedback enhances the security of wiretap channels with states. AEU Int. J. Electr. Commun. **69**(7), 1047–1057 (2015)
31. C. Mitrpant, A. J. Han Vinck, Y. Luo, An achievable region for the Gaussian wiretap channel with side information. IEEE Trans. Inf. Theory. **52**(5), 2181–2190 (2006)
32. Y. Chen, A. J. Han Vinck, Wiretap channel with side information. IEEE Trans. Inf. Theory. **54**(1), 395–402 (2008)
33. X. Yin, X. Chen, P. Guo, Z. Xue, in *2014 IEEE/CIC International Conference on Communications in China (ICCC)*. The role of feedback in channels with information embedding on actions (IEEE, Shanghai, 2014). https://doi.org/10.1109/iccchina.2014.7008240
34. B. Dai, A. J. Han Vinck, Y. Luo, Wiretap channel in the presence of action-dependent states and noiseless feedback. J. Appl. Math. **2013**, 1–17 (2013)
35. B. Dai, A. J. Han Vinck, Y. Luo, X. Tang, Wiretap channel with action-dependent channel state information. Entropy. **15**(2), 445–473 (2013)
36. B. Dai, Z. Ma, Y. Luo, Finite state Markov wiretap channel with delayed feedback. IEEE Trans. Inf. Forensics Secur. **12**(3), 746–760 (2017)
37. H. Viswanathan, Capacity of Markov channels with receiver CSI and delayed feedback. IEEE Trans. Inf. Theory. **45**(2), 761–771 (1999)
38. L. Lai, H. El Gamal, H. V. Poor, The wiretap channel with feedback: encryption over the channel. **54**(11), 5059–5067 (2008)
39. G. Bassi, P. Piantanida, S. Shamai (Shitz), The wiretap channel with generalized feedback: secure communication and key generation. IEEE Trans. Inf. Theory. **65**(4), 2213–2233 (2019)

40. G. Bassi, P. Piantanida, S. Shamai (Shitz), in *On the capacity of the wiretap channel with generalized feedback*. 2015 IEEE International Symposium on Information Theory (ISIT) (IEEE, 2015). https://doi.org/10.1109/isit.2015.7282636
41. B. Yang, W. Wang, Q. Yin, J. Fan, Secret wireless communication with public feedback by common randomness. IEEE Wirel. Commun. Lett. **3**(3), 269–272 (2014)
42. T. Kim, H. V. Poor, in *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*. The Gaussian wiretap channel with noisy public feedback: Breaking the high-SNR ceiling (IEEE, 2009). https://doi.org/10.1109/acssc.2009.5469976
43. X. He, A. Yener, The role of feedback in two-way secure communications. IEEE Trans. Inf. Theory. **59**(12), 8115–8130 (2013)
44. X. Tang, R. Liu, P. Spasojevic, H. V. Poor, in *2007 IEEE Information Theory Workshop*. Multiple access channels with generalized feedback and confidential messages (IEEE, 2007). https://doi.org/10.1109/itw.2007.4313144
45. E. Ekrem, S. Ulukus, in *2008 42nd Annual Conference on Information Sciences and Systems*. Effects of cooperation on the secrecy of multiple access channels with generalized feedback (IEEE, 2008). https://doi.org/10.1109/ciss.2008.4558628
46. B. Dai, Z. Ma, Multiple access wiretap channel with noiseless feedback. IET Commun. **11**(14), 2190–2198 (2017)
47. B. Dai, Z. Ma, M. Xiao, X. Tang, P. Fan, Secure communication over finite state multiple-access wiretap channel with delayed feedback. IEEE J. Sel. Areas Commun. **36**(4), 723–736 (2018)
48. H. Wen, G. Gong, P. Ho, Build-in wiretap channel I with feedback and LDPC codes. J. Commun. Netw. **11**(6), 538–543 (2009)
49. S. Salimi, M. Skoglund, J. D. Golic, M. Salmasizadeh, M. R. Aref, Key agreement over a generalized multiple access channel using noiseless and noisy Feedback. IEEE J. Sel. Areas Commun. **31**(9), 1765–1778 (2013)
50. S. Salimi, E. A. Jorswieck, M. Skoglund, P. Papadimitratos, in *2015 IEEE Conference on Communications and Network Security (CNS)*. Key agreement over an interference channel with noiseless feedback: Achievable region & distributed allocation (IEEE, 2015). https://doi.org/10.1109/cns.2015.7346811
51. U. E. Maurer, Secret key agreement by public discussion from common information. IEEE Trans. Inform. Theory. **39**(5), 733–742 (1993)
52. R. Ahlswede, I. Csiszar, Common randomness in information theory and cryptography-part i: Secret sharing. IEEE Trans. Inform. Theory. **39**(7), 1121–1132 (1993)
53. G. T. Amariucai, S. Wei, in *Proc. 42nd Annu. Conf. Inf. Sci. Syst.* Strictly positive secrecy rates of binary wiretapper channels using feedback schemes (IEEE, Princeton, 2008), pp. 624–629
54. G. T. Amariucai, S. Wei, Feedback-based collaborative secrecy encoding over binary symmetric channels. IEEE Trans. Inform. Theory. **58**(8), 5248–5266 (2012)
55. A. A. Gohari, V. Anantharam, Information-Theoretic Key Agreement of Multiple Terminals–Part I. IEEE Trans. Inform. Theory. **56**(8), 3973–3996 (2010)
56. A. A. Gohari, V. Anantharam, Information-Theoretic Key Agreement of Multiple Terminals–Part II: Channel Model. IEEE Trans. Inform. Theory. **56**(8), 3997–4010 (2010)
57. A. Khisti, S. N. Diggavi, G. W. Wornell, Secret-key agreement with channel state information at the transmitter. IEEE Trans. Inf. Forensics Secur. **6**(3), 672–681 (2011)
58. J. P. M. Schalkwijk, T. Kailath, A coding scheme for additive noise channels with feedback. part I: No bandwidth constraint. IEEE Trans. Inf. Theory. **12**(1), 172–182 (1966)
59. A. Wyner, J. Ziv, The rate-distortion function for source coding with side information at the decoder. IEEE Trans. Inf. Theory. **22**(1), 1–10 (1976)
60. B. Dai, Y. Luo, An improved feedback coding scheme for the wiretap channel. IEEE Trans. Inf. Forensics Secur. **14**(1), 262–271 (2019)
61. B. Dai, L. Yu, X. Liu, Z. Ma, Feedback coding schemes for the broadcast channel with mutual secrecy requirement at the receivers. IEEE Trans. Commun. **67**(9), 6039–6052 (2019). https://doi.org/10.1109/tcomm.2019.2924206
62. R. Timo, A. Grant, T. Chan, G. Kramer, in *2008 IEEE International Symposium on Information Theory*. Source coding for a simple network with receiver side information (IEEE, 2008). https://doi.org/10.1109/isit.2008.4595402
63. R. Liu, I. Maric, P. Spasojević, R. D. Yates, Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions. IEEE Trans. Inf. Theory. **54**(6), 2493–2507 (2008)
64. J. Xu, Y. Cao, B. Chen, Capacity bounds for broadcast channels with confidential messages. IEEE Trans. Inf. Theory. **55**(6), 4529–4542 (2009)
65. X. Li, B. Dai, Z. Ma, How can we fully use noiseless feedback to enhance the security of the broadcast channel with confidential messages. Entropy. **19**(10), 1–15 (2017)
66. H. Zhang, L. Yu, C. Wei, B. Dai, A new feedback scheme for the state-dependent wiretap channel with noncausal state at the transmitter. IEEE Access. **7**, 45594–45604 (2019)
67. H. Zhang, L. Yu, B. Dai, Feedback schemes for the action-dependent wiretap channel with noncausal state at the transmitter. Entropy. **21**(3), 278–292 (2019)
68. D. Gunduz, D. R. Brown, H. V. Poor, in *2008 International Symposium on Information Theory and Its Applications*. Secret communication with feedback (IEEE, 2008). https://doi.org/10.1109/isita.2008.4895417
69. C. Li, Y. Liang, H. V. Poor, S. Shamai, in *2018 IEEE International Symposium on Information Theory (ISIT)*. A coding scheme for colored Gaussian wiretap channels with feedback (IEEE, 2018). https://doi.org/10.1109/isit.2018.8437720
70. C. Li, Y. Liang, in *2017 IEEE International Symposium on Information Theory (ISIT)*. Secrecy capacity of the first-order autoregressive moving average Gaussian channel with feedback (IEEE, 2017). https://doi.org/10.1109/isit.2017.8006872
71. C. Li, Y. Liang, H. V. Poor, S. Shamai, Secrecy capacity of colored Gaussian noise channels with feedback. IEEE Trans. Inf. Theory. **65**(9), 5771–5782 (2019). https://doi.org/10.1109/tit.2019.2904684
72. M. H. M. Costa, Writing on dirty paper. IEEE Trans. Inf. Theory. **29**(3), 439–441 (1983)
73. J. Liu, N. Elia, Writing on dirty paper with feedback. Commun. Inf. Syst. **5**(4), 401–422 (2005)
74. B. Dai, C. Li, Y. Liang, Z. Ma, S. Shamai, in *2019 IEEE International Symposium on Information Theory (ISIT)*. The dirty paper wiretap feedback channel with or without action on the state (IEEE, 2019). https://doi.org/10.1109/isit.2019.8849443
75. C. Qi, Y. Chen, A. J. Han Vinck, X. Tang, Effects of feedback on the one-sided secrecy of two-way wiretap through multiple transmissions. arXiv:1707.05932, 1–17 (2017)
76. J. Y. Tan, L. Ong, B. Asadi, Can Marton coding alone ensure individual secrecy? arXiv:1906.12326, 1–5 (2019)
77. K. Marton, A coding theorem for the discrete memoryless broadcast channel. IEEE Trans. Inf. Theory. **25**(3), 306–311 (1979)
78. B. He, X. Zhou, T. D. Abhayapala, Wireless physical layer security with imperfect channel state information: A survey. arXiv:1307.4146, 1–9 (2013)
79. A. Hyadi, Z. Rezki, M.-S. Alouini, An overview of physical layer security in wireless communication systems with CSIT uncertainty. IEEE Access. **4**, 6121–6132 (2016)
80. A. Hyadi, Z. Rezki, M.-S. Alouini, Secure multiple-antenna block-fading wiretap channels with limited CSI feedback. IEEE Trans. Wirel. Commun. **16**(10), 6618–6634 (2017)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.