The Secrecy Capacity of Gaussian Wiretap Channels with Rate-Limited Help at the Encoder

Sergey Loyka, Neri Merhav

2023 IEEE Information Theory Workshop (ITW) | 979-8-3503-0149-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ITW55543.2023.10161609

***Abstract*—The Gaussian wiretap channel (WTC) with rate-limited help, available at the transmitter/encoder (Tx), in addition to or instead of the same help at the legitimate receiver, is studied under various channel configurations. For the degraded or reversely-degraded WTC, rate-limited non-secure Tx help results in a secrecy capacity boost equal to the help rate irrespective of whether the help is causal or not. For the non-degraded WTC, the secrecy capacity boost is lower bounded by the help rate. A capacity-achieving signaling is two-phase time sharing, where wiretap coding without help is used in Phase 1 and help without wiretap coding is used in Phase 2. The secrecy capacity with Tx help is positive for the reversely-degraded channel (where the no-help secrecy capacity is zero) and no Phase 1 is needed to achieve it. Unlike the no-help case, more noise at the legitimate receiver can sometimes result in higher secrecy capacity with Tx help. In the case of the joint Tx/Rx non-secure help, one help link can be omitted without affecting the capacity.**

I. Introduction

Physical-layer security has emerged as a valuable addition to cryptography-based techniques [1], [2], especially over wireless channels and networks, and it also plays an important role in modern industrial standards [3], [4]. While the original work on information-theoretic secrecy dates back to Shannon himself [5], Wyner's wiretap channel (WTC) model [6] established itself as a very useful tool for many different settings and configurations. It includes one legitimate transmitter-receiver pair and one wiretapper (or eavesdropper) to be kept ignorant of the transmitted message. Its key performance metric is the secrecy capacity, i.e. the largest achievable rate subject to (weak or strong) secrecy in addition to a reliability constraint, possibly under a power constraint. The original degraded WTC model has been extended and developed in many respects, see e.g. [1]-[3] and references therein. More refined performance metrics (beyond secrecy capacity), including secrecy exponents, finite blocklength and second-order coding rates, have also been studied [7], [8].

While feedback does not increase the ordinary (no secrecy) capacity of memoryless channels, it is often able to boost the secrecy capacity, even in the memoryless settings, see e.g. [9] and references therein. The memoryless Gaussian WTC with noiseless (and hence rate-unlimited) feedback was considered in [10], whereby the transmitter (Tx) has access to the signal of the legitimate receiver (Rx) in a causal manner while the eavesdropper (Ev) has access to its noisy version. Its secrecy capacity C_{snf} was shown to be equal to the ordinary (no Ev, no feedback) AWGN channel capacity C_0,

$$C_{snf} = C_0 \tag{1}$$

i.e. secrecy comes for free with the noiseless feedback and the secrecy capacity with feedback exceeds the no-feedback one, even though the channel is memoryless and, possibly, not degraded. The capacity-achieving strategy is the Schalkwijk-Kailath scheme and no wiretap coding is needed. This result was further extended to a colored (ARMA) Gaussian noise channel with noiseless (rate-unlimited) feedback in [9]. Note, however, that, in this setting, the Tx has access to the causal but noiseless feedback while the Ev observes only its noisy version, i.e. the Ev is at a significant disadvantage and the feedback is at least partially secure (hidden by the noise in the Ev feedback link). The situation changes dramatically and the above result does not apply if the Ev has access to the same noiseless (and, hence, non-secure) feedback as well or if the Rx-to-Tx feedback link is also noisy or rate-limited. The degraded memoryless Gaussian WTC with a secure *rate-limited* feedback of rate $R_f < \infty$ was considered in [11] and its secrecy capacity C_{sf} was established:

$$C_{sf} = \min\{C_0, C_{s0} + R_f\} \tag{2}$$

where C_{s0} is the secrecy capacity without feedback. An optimal Tx strategy is fundamentally different from [9], [10] in this setting: it is a combination of the standard wiretap coding as in [6] with a secure key generated by the Rx and sent to the Tx via the secure rate-limited feedback link. Note, however, that this strategy requires a secure feedback link, so that the feedback is (completely) unknown to the Ev, and it does not apply otherwise.

Various forms of side information, beyond feedback, are often available in modern systems/networks (e.g. in a cloud radio access network) and can boost the capacity [12]. One particular configuration was recently studied in [13], [14] in the no-Ev/no-secrecy setting, where a rate-limited (and error-free) help is available to the decoder or/and encoder. In particular, a helper observes the noise sequence (which can be a signal intended for other users in a multi-user environment) and communicates his observation to the receiver (decoder) or transmitter (encoder) via an error-free but rate-limited data pipe. This model is appealing from a practical perspective since it considers a rate-limited help link, unlike some noiseless feedback models that essentially require rate-unlimited and error-free feedback links that are hardly possible in practice. This rate-limited help was shown in [13], [14] to provide a boost in the no-secrecy channel capacity equal to the help rate R_h so that the with-help channel capacity is $C_0 + R_h$; flash signalling (i.e. using high-resolution help infrequently) was shown to be an optimal help strategy, in combination with two-phase time sharing. Error exponents of Gaussian and modulo-additive channels with rate-limited Tx help were established in [15], where it was also shown that the channel with Tx help is equivalent to the regular (no-help)

S. Loyka is with the School of Electrical Engineering and Computer Science, University of Ottawa, Ontario, Canada, e-mail: sergey.loyka@uottawa.ca.

N. Merhav is with the Andrew and Erna Viterbi Faculty of Electrical and Computer Engineering, Technion - Israel Institute of Technology, Haifa, Israel, e-mail: merhav@ee.technion.ac.il.

979-8-3503-0149-6/23/$31.00 ©2023 Crown

channel and an additional parallel error-free bit-pipe of rate R_h.

The Rx help setting in [13] was extended to the memoryless Gaussian wiretap channel in [19] and its secrecy capacity with Rx help was established for various channel configurations (degraded, reversely degraded and non-degraded)[1]. However, the respective WTC with Tx/encoder help was not studied (the capacity result was briefly stated, without proof, for the degraded case only).

A. Our contribution

Here, we present a study of various configurations of Gaussian WTC with Tx or joint Tx/Rx help and a complete proof of its secrecy capacity. The techniques needed to establish the secrecy capacity with Tx help are substantially different from those in the Rx help case in [19] since, unlike the latter case, the codebooks as well as capacity-achieving input distributions do depend on help in the former case. This has significant impact on the converse and achievability schemes. Unlike the Rx help case, where causality of help is immaterial (since the Rx waits until the whole codeword is received to start its decoding), it can potentially make a difference in the case of Tx help. Therefore, we distinguish between causal and non-causal Tx help. For the degraded, non-degraded and reversely-degraded channels (see footnote 1), the secrecy capacity C_s with Tx help of rate R_h, in addition to or instead of the same Rx help, secure or non-secure, causal or non-causal, is shown to satisfy (see Theorems 1,2)

$$C_s \geq C_{s0} + R_h, \tag{3}$$

where C_{s0} is the regular (no-help) secrecy capacity ($C_{s0} = 0$ for the reversely-degraded case). (3) holds with equality for the degraded and reversely-degraded channels if the help is not secure (the capacity with secure Tx help as well as for the non-degraded channel remain open problems, for which (3) gives only a lower bound). Some unusual properties of C_s are pointed out. In particular, it is strictly positive in the reversely-degraded case (where the no-help secrecy capacity is zero), even if the help is not secure, and no wiretap coding is needed at all to achieve it. More noise at the legitimate receiver can sometimes result in higher secrecy capacity. Non-causal help does not bring in any advantage over the causal one. If the Tx and Rx help links are identical (carry the same information) and non-secure, then any one can be omitted without affecting the secrecy capacity (this is not the case anymore if the help links are independent).

An optimal Tx strategy to achieve C_s in (3) is fundamentally different from those in [9]-[11]: it is a two-phase time sharing whereby no help is used in Phase 1 but just regular (no help) wiretap coding; on the contrary, much shorter Phase 2 makes use of high-resolution help in combination with regular (no Ev) channel coding but no wiretap coding at all. In the case of the reversely-degraded WTC, Phase 1 and hence wiretap coding are not needed so that burst signaling alone (with regular channel coding) is sufficient.

Comparing (3) to (2) with $R_h = R_f$, note that $C_s > C_{sf}$ if the help/feedback rate is sufficiently high, $R_h = R_f > C_0 - C_{s0} = C_2$, where C_2 is the no-help capacity of the Tx-Ev link, i.e. the helper setting provides larger secrecy capacity compared to the rate-limited but secure feedback setting, even though the help is not required to be secure. The same applies to (1), where the feedback is rate-unlimited and at least partially-secure. Note also that, unlike C_{sf} in (2), the increase in C_s in (3) with R_h does not saturate.

Unlike the studies of Gaussian WTCs with noiseless (and hence rate-unlimited) feedback in [9], [10], our help links are rate-limited, as in [13], [14], and we also allow here the Ev to have access to the same help as the legitimate Rx and Tx. In our rate-limited setting, causality of help has no impact on the secrecy capacity. Unlike the study in [11], our help link is not required to be secure or causal and the channel is not required to be degraded.

Secure communication with a helper acting as a cooperating jammer was studied in [16], [17]. However, no secrecy capacity was established but only the generalized degrees of freedom. Unlike [16], [17], the present paper considers no jamming at all; rather, the (passive) help comes in a form of rate-limited information about the Rx noise sequence, which is available to the Tx and/or Rx.

Notations: random variables and their realizations are denoted by capital and lower case letters, respectively, and their alphabets follow from the respective channel models; X^n denotes the sequence $(X_1, ..., X_n)$; $H(\cdot)$, $h(\cdot)$ and $h(\cdot|\cdot)$ are the entropy, differential and conditional differential entropies, respectively, and $I(\cdot;\cdot)$ is the mutual information; $\mathbb{E}\{\cdot\}$ and $\Pr\{\cdot\}$ are statistical expectation and probability with respect to relevant random variables; $X - Y - Z$ denotes a Markov chain of random variables X, Y, and Z.

II. Degraded Gaussian WTC With Tx Help

We begin with the real-valued degraded (discrete-time) Gaussian wiretap channel:

$$Y_i = X_i + W_i,\ Z_i = Y_i + V_i,\ i = 1, ..., n \tag{4}$$

where X_i is the real-valued transmitted symbol at time i, W_i, V_i are Rx and Ev noise, which are zero-mean Gaussian, independent of each other with variances σ_W^2 and σ_V^2, respectively, see Fig. 1. The channel is stationary and memoryless, so that W^n and V^n are i.i.d. sequences. We further assume that $\sigma_V^2 > 0$ (unless stated otherwise).

The helper model is as in [14] but extended to the WTC setting, whereby discrete help $T = T(W^n)$ of rate $n^{-1}H(T) \leq R_h < \infty$ is available to the Tx, Ev and, possibly, Rx (no further constraints on the helper function $T(W^n)$ are assumed, beyond its rate, unless stated otherwise), which we term ”non-secure Tx help”, so that the Ev can estimate transmitted message M using T and its received signals Z^n while the Rx uses Y^n (no Rx help) or Y^n and T (Rx help). This falls into the framework of cooperative communications or communications with side information [12] and models practical links, which are always rate-limited. If no help is available to the Ev, we call it ”secure help”.

We use the standard definition of the secrecy capacity as the supremum of all achievable secrecy rates, subject to the

[1] While the standard (no help) SISO non-degraded Gaussian WTC is equivalent to either degraded or reversely-degraded one, this is not the case anymore when Rx/Tx help is also available to the Ev.

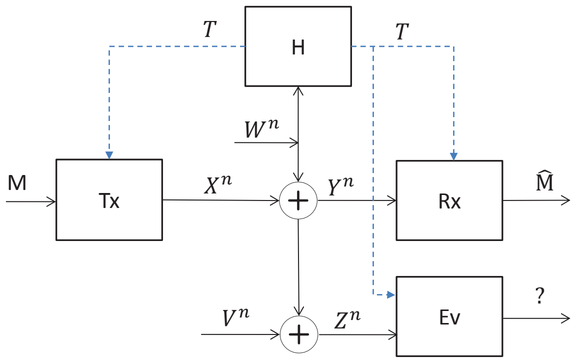

Fig. 1. Degraded wiretap channel with a rate-limited help T at the Tx, Rx and Ev (T is not available to the Ev if the help is secure). W^n and V^n are i.i.d. noise sequences, $\sigma_V^2 > 0$; V^n is independent of W^n, X^n, M; $X^n = X^n(M,T)$, $T = T(W^n)$, $H(T) \le nR_h$.

reliability, secrecy and power constraints, see e.g. [1]-[3], [6]. In particular, the (secret) message M is selected randomly and uniformly from $\{1, ..., 2^{nR_s}\}$, where R_s is a secrecy rate and n is the blocklength. The Tx encoder maps it into X^n using the available help T and the Rx decoder maps Y^n and, possibly, T into a message estimate $\hat{M}$. The constraints are as follows:

Reliability constraint: the error probability $P_e \triangleq \Pr\{M \neq \hat{M}\} \le \varepsilon$ for any $\varepsilon > 0$ and sufficiently large n.

Weak secrecy constraint: information leakage rate (to the Ev) R_l satisfies

$$R_l \triangleq n^{-1} I(M; Z^n T) \le \delta \tag{5}$$

for any $\delta > 0$ and sufficiently large n; T is omitted in the case of secure help.

Average power constraint:

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\{X_i^2\} \le P \tag{6}$$

Unlike the Rx help case where the causality of help is immaterial (since the Rx starts decoding after the whole block of length n is received), it becomes important for the Tx help setting. Thus, we distinguish between causal Tx help, whereby at time i the Tx help is based on the Rx noise sequence up to time i, and non-causal Tx help, whereby the Tx help at time $i = 1$ (the very beginning of the transmission) is based on the whole noise sequence W^n. The secrecy capacity of this channel with Tx help is established below.

Theorem 1. *Consider the degraded Gaussian WTC in Fig. 1 with causal or non-causal Tx help of rate R_h, secure or non-secure, in addition to or instead of the same Rx help, and let $\sigma_V^2, P > 0$. Its secrecy capacity C_s satisfies*

$$C_s \ge C_{s0} + R_h \tag{7}$$

where C_{s0} is the secrecy capacity without help. This holds with equality if the help is not secure.

Proof. First, we establish that (7) holds with equality in the case of non-secure help, from which the inequality will follow in the case of secure help (since the availability of help to the Ev cannot increase the secrecy rate).

Converse: To establish the converse, consider the case when the same non-causal non-secure help T is available to all ends, i.e. the Tx, Rx and Ev as in Fig. 1. Clearly, the same converse will hold if no Rx help is available or if the help is causal. Using the appropriate Markov chain and functional relationships between the random variables, in addition to the secrecy and reliability constraints, note the following:

$$\begin{aligned}
nR_s &= H(M) \qquad (8)\\
&\le H(M|Z^nT) + n\epsilon \qquad (9)\\
&= I(M;Y^n|Z^nT) + H(M|Y^nZ^nT) + n\epsilon \qquad (10)\\
&\le I(M;Y^n|Z^nT) + 2n\epsilon \qquad (11)\\
&\le I(X^n;Y^n|Z^nT) + 2n\epsilon \qquad (12)\\
&= I(X^n;Y^n|T) - I(X^n;Z^n|T) + 2n\epsilon \qquad (13)\\
&= h(Y^n|T) - h(Y^n|X^nT)\\
&\qquad - [h(Z^n|T) - h(Z^n|X^nT)] + 2n\epsilon \qquad (14)\\
&= h(W^n + V^n|T) - h(W^n|T)\\
&\qquad + h(Y^n|T) - h(Z^n|T) + 2n\epsilon \qquad (15)\\
&\le \frac{n}{2}\log(2\pi e(\sigma_V^2 + \sigma_W^2)) + I(W^n;T) - h(W^n)\\
&\qquad + h(Y^n|T) - h(Z^n|T) + 2n\epsilon \qquad (16)\\
&= \frac{n}{2}\log\frac{\sigma_V^2 + \sigma_W^2}{\sigma_W^2} + H(T) + h(Y^n|T)\\
&\qquad - h(Z^n|T) + 2n\epsilon \qquad (17)\\
&\le nR_h + \frac{n}{2}\log\frac{\sigma_V^2 + \sigma_W^2}{\sigma_W^2}\frac{\sigma_W^2 + P}{\sigma_W^2 + \sigma_V^2 + P} + 2n\epsilon \qquad (18)\\
&= n(R_h + C_{s0} + 2\epsilon) \qquad (19)
\end{aligned}$$

where (9) follows from the secrecy constraint $I(M;Z^nT) \le n\epsilon$; (11) follows from Fano inequality (due to the reliability constraint) $H(M|Y^nZ^nT) = H(M|Y^nT) \le n\epsilon$; (12) and (13) follow from Markov chain $M - X^n - Y^n - Z^n$ conditional on T; (15) is due to the independence of X^n and (W^n, V^n) conditional on T; (16) follows since conditioning cannot increase entropy; (17) is due to $I(W;T) = H(T)$; (18) follows from Lemma 1 below. Since (19) holds for any $\epsilon > 0$, it follows that $C_s \le C_{s0} + R_h$, as desired. Clearly, the same inequality holds if T is not available to the Rx.

Lemma 1. *The following inequality holds in the considered setting:*

$$\Delta h = h(Y^n|T) - h(Z^n|T) \le \frac{n}{2}\log\frac{\sigma_W^2 + P}{\sigma_W^2 + \sigma_V^2 + P} \tag{20}$$

Proof. It has been proved in [14, eq. (46)] that

$$h(Y^n|T) \le \frac{n}{2}\log(2\pi e(\sigma_W^2 + P)) \tag{21}$$

(the proof is not trivial since X^n and W^n are *not* independent, due to help $T = T(W^n)$). To bound $h(Z^n|T)$ likewise, note that

$$h(Z^n|T) = \sum_t p_T(t) h(Y^n + V^n|T = t) \tag{22}$$

where $p_T(t)$ is the distribution of T. Using the entropy power inequality

$$2^{\frac{2}{n}h(Y^n+V^n|T=t)} \ge 2^{\frac{2}{n}h(Y^n|T=t)} + 2^{\frac{2}{n}h(V^n|T=t)} \tag{23}$$

it follows that

$$h(Y^n + V^n|T = t) \ge \frac{n}{2}\log(2^{\frac{2}{n}h(Y^n|T=t)} + 2\pi e\sigma_V^2) \tag{24}$$

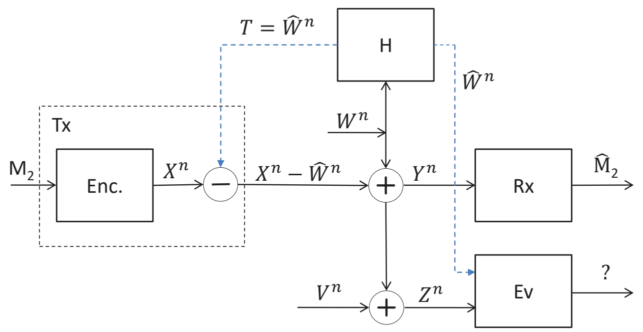

Fig. 2. Phase 2 signalling for the degraded WTC: the causal help T is a scalar-quantized noise $\hat{W}^n$, $\hat{W}_i = Q(W_i)$, pre-subtracted at the Tx; $X^n = X^n(M_2)$ is a codeword from i.i.d.-generated codebook, as in [14].

and hence

$$h(Z^n|T) \geq \frac{n}{2}\log\left(2^{\frac{2}{n}\sum_t p_T(t)h(Y^n|T=t)} + 2\pi e\sigma_V^2\right) \quad (25)$$
$$= \frac{n}{2}\log\left(2^{\frac{2}{n}h(Y^n|T)} + 2\pi e\sigma_V^2\right)$$

where the inequality is due to the convexity of the log-sum-exp function [18, p. 72]. Finally,

$$\Delta h \leq h(Y^n|T) - \frac{n}{2}\log\left(2^{\frac{2}{n}h(Y^n|T)} + 2\pi e\sigma_V^2\right) \quad (26)$$
$$\leq \frac{n}{2}\log\frac{2\pi e(\sigma_W^2 + P)}{2^{\log(2\pi e(\sigma_W^2+P))} + 2\pi e\sigma_V^2} \quad (27)$$
$$= \frac{n}{2}\log\frac{\sigma_W^2 + P}{\sigma_W^2 + \sigma_V^2 + P} \quad (28)$$

as required, where the inequality is due to (21) and $f(x) = x - \log(2^x + c)$ being an increasing function of x for any $c > 0$. □

Achievability: We consider the case of causal help being available to the Tx and Ev but not to the Rx. This will also establish achievability when the same help is also available to the Rx or/and when Tx help is non-causal (since adding Rx help or removing causality constraint cannot decrease achievable rates). Following [14], we use a two-phase flash signalling properly extended to the wiretap setting to ensure secrecy as follows. Phase 1 of duration $(1-\tau)$ makes use of no-help regular wiretap coding and thus achieves the secrecy rate $C_{s0} - \epsilon$ for any $\epsilon > 0$. Phase 2 of much-shorter duration τ is the same as in [14][2], which makes use of regular (no-wiretap) coding and pre-substraction of the scalar-quantized noise (available via the rate-limited help link) at the Tx, as shown in Fig. 2:

$$Y_i = X_i - \hat{W}_i + W_i$$
$$Z_i = Y_i + V_i \quad (29)$$

where $X^n = X^n(M_2)$ using i.i.d.-generated codebook $\mathcal{C}$, $T = \hat{W}^n$ is a scalar-quantized noise, $\hat{W}_i = Q(W_i)$, where the quantizer uses $L = \lfloor 2^{R_h/\tau} \rfloor$ levels for each sample, which require the average rate $\tau\log(L) \leq R_h$ to be transmitted over the help link. For further use, note that $V^n \perp (W^n, \hat{W}^n, X^n, M_2)$ and $(W^n, \hat{W}^n) \perp (V^n, X^n, M_2)$, where $\perp$ means statistical independence, so that the following Markov chains hold:

$$(M_2, \mathcal{C}) - X^n - Y^n - Z^n;\ (M_2, \mathcal{C}) - X^n - (Z^n, W^n, \hat{W}^n)$$

Following [14, eq. (24)], this Phase 2 signalling achieves the rate arbitrary close to

$$\frac{R_h}{\tau} + \frac{1}{2}\log\left(2^{-2R_h/\tau} + \alpha_W P(1 - 2^{-R_h/\tau})^2[1 + o(1)]\right)$$
$$= R_h/\tau[1 + o(1)] \quad (30)$$

where $\alpha_W = 2(\pi\sqrt{3}\sigma_W^2)^{-1}$ and $o(1) \to 0$ as as $\tau \to 0$. Thus, the overall two-phase signalling rate (after time sharing) is

$$(1-\tau)(C_{s0} - \epsilon) + R_h(1 + o(1)) \to C_{s0} + R_h - \epsilon \quad (31)$$

for any $\epsilon > 0$, as $\tau \to 0$.

It remains to show that this rate is indeed secure, i.e. the information leakage rate to the Ev is arbitrary small. This is clearly the case in Phase 1 since regular wiretap coding is used in this phase so that its leakage rate is $R_{l1} = n^{-1}I(M_1; Z^n) \leq \delta$ for any $\delta > 0$ and sufficiently-large n. To see that secrecy is guaranteed after two-phase time sharing (even though no wiretap coding is used in Phase 2), we show that Phase 2 leakage rate is uniformly bounded for any τ:

$$R_{l2} = n^{-1}I(M_2; Z^n\hat{W}^n|\mathcal{C}) \quad (32)$$
$$\leq n^{-1}I(X^n; Z^n\hat{W}^n|\mathcal{C}) \quad (33)$$
$$\leq n^{-1}I(X^n; Z^n\hat{W}^n) \quad (34)$$
$$\leq n^{-1}I(X^n; Z^n W^n) \quad (35)$$
$$\leq I_0(X; ZW) \quad (36)$$
$$= I_0(X; X + V) \quad (37)$$
$$\leq \frac{1}{2}\log\left(1 + \frac{P}{\sigma_V^2}\right) = C_2 < \infty \quad (38)$$

where (33) is due to Markov chain $M_2 - X^n - Z^n\hat{W}^n$; (34) is due to Markov chain $\mathcal{C} - X^n - Z^n\hat{W}^n$; (35) is due to $\hat{W}^n = Q(W^n)$; (36) holds since the channel is memoryless; I_0 is the mutual information induced by input X with the distribution $p_0(x) = n^{-1}\sum_i p_{x_i}(x)$.

Thus, the overall leakage rate after two-phase time sharing is

$$R_l = (1-\tau)R_{l1} + \tau R_{l2} \leq (1-\tau)\delta + \tau C_2 \to \delta \quad (39)$$

as $\tau \to 0$, for any $\delta > 0$, as required. This completes the proof. □

Note that the availability of the Rx help, in addition to the Tx help, does not increase the secrecy capacity (provided the non-secure help T is the same at all ends) so that one help link can be omitted without affecting the capacity. The non-causal non-secure Tx help does not increase the secrecy capacity over the causal one either (this mimics the respective property of the no-Ev/no-secrecy channel capacity with Tx help in [14]).

If $\sigma_V^2 = 0$ and the Tx (or joint Tx/Rx) help is not secure, then the secrecy capacity is zero, since the Ev has access to exactly the same information as the Rx so that no secrecy is possible, i.e. $C_s(\sigma_V^2)$ is a discontinuous function at $\sigma_V^2 = 0$:

$$\lim_{\sigma_V^2 \to 0^+} C_s(\sigma_V^2) = R_h > 0 \quad (40)$$

[2] An alternative Phase 2 strategy using a simple lattice code with a uniform scalar quantizer is proposed in [15] and can be used here as well.

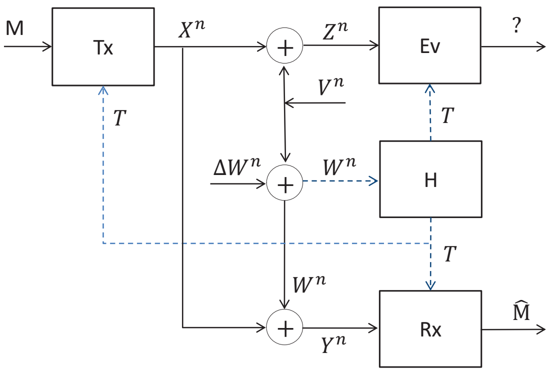

Fig. 3. Reversely-degraded wiretap channel with a rate-limited help T at the Tx, Rx and Ev. ΔW^n and V^n are i.i.d. noise sequences, $\sigma_V^2, \sigma_{\Delta W}^2 > 0$; V^n, ΔW^n and M are independent of each other; $X^n = X^n(M, T)$, $T = T(W^n)$, $H(T) \leq nR_h$.

while $C_s(0) = 0$ - a remarkable difference to the no-help case. This also implies that help is especially important when the no-help secrecy capacity is zero or close to it.

Using a similar approach, Theorem 1 can be shown to hold for the non-degraded channel as well (without the equality part), even if the Rx and Ev noise sequences are correlated with each other (provided the correlation is not singular), see [20] for details.

III. The Reversely-Degraded WTC with Tx Help

Let us consider the reversely-degraded Gaussian WTC, as in Fig. 3, with Tx help, in addition to or instead of the Rx help (T is not available to the Ev if help is secure). While its secrecy capacity is zero without help, this is not the case when help is present, even if it is not secure, as the following Theorem shows.

Theorem 2. *Consider the reversely-degraded Gaussian WTC with causal or non-causal Tx help of rate R_h, secure or not, in addition to or instead of the same Rx help, as in Fig. 3, and let $\sigma_V^2, \sigma_{\Delta W}^2, P > 0$. Its secrecy capacity C_s satisfies*

$$C_s \geq R_h \tag{41}$$

and this holds with equality if the help is not secure.

Proof. See the full version [20]. □

We remark that, as in the reversely-degraded WTC with Rx help, no wiretap coding is needed here to achieve its secrecy capacity if the help is not secure. Burst signalling alone (with regular coding) is sufficient and arbitrarily low leakage rate can be achieved by reducing signaling interval τ. The presence of help T at the Rx, in addition to the Tx, does not increase the capacity. Even though the help is not secure, it still boosts significantly the secrecy capacity, which is zero without help. This is so since the help T serves here as a public key: even though this key is available to the Ev, it cannot make use of it since it does not have the right ”lock”.

Note that $C_s = 0$ if $\sigma_{\Delta W}^2 = 0$ and help is not secure (since the Ev receives the same information as the Rx so that no secrecy is possible) and therefore $C_s(\sigma_{\Delta W}^2)$ is discontinuous at $\sigma_{\Delta W}^2 = 0$:

$$C_s(\sigma_{\Delta W}^2) = R_h > 0 \; \forall \; \sigma_{\Delta W}^2 > 0 \tag{42}$$

while $C_s(0) = 0$, for any $R_h > 0$, i.e. more noise at the Rx ($\sigma_{\Delta W}^2 > 0$) is actually better for the secrecy capacity of this channel.

* * *

Note that the presence of the same Rx help, in addition to the Tx help, does not result in extra secrecy capacity boost (one link can be omitted without loss in the capacity). One can also consider various other configuration of Tx and Rx help links of rates R_{h1} and R_{h2}, respectively. If these links are fully correlated, then the secrecy capacity boost is $\max\{R_{h1}, R_{h2}\}$ and, if the links are independent, the boost is $R_{h1} + R_{h2}$, see [20] for details.

References

[1] M. Bloch, J. Barros, Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press, 2011.

[2] P. A. Regalia et al (Eds.), Secure Communications via Physical-Layer and Information-Theoretic Techniques, Proceedings of the IEEE, vol.103, no.10, Oct. 2015.

[3] Y. Wu et al., A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead, IEEE JSAC, vol. 36, no. 4, pp. 679-695, Apr. 2018.

[4] A. Chorti et al., Context-Aware Security for 6G Wireless: The Role of Physical Layer Security, IEEE Comm. Standards Magazine, vol. 6, no. 1, pp. 102-108, Mar. 2022.

[5] C. E. Shannon, Communication Theory of Secrecy Systems, Bell Syst. Tech. J., vol. 28, pp. 656–715, Oct. 1949.

[6] A.D. Wyner, The Wire-Tap Channel, Bell System Technical Journal, v. 54, no. 8, pp. 1355–1387, Oct. 1975.

[7] M. Bastani Parizi, E. Telatar and N. Merhav, Exact Random Coding Secrecy Exponents for the Wiretap Channel, IEEE Trans. Info. Theory, vol. 63, no. 1, pp. 509–531, Jan. 2017.

[8] W. Yang, R. F. Schaefer and H. V. Poor, Wiretap Channels: Nonasymptotic Fundamental Limits, IEEE Trans. Info. Theory, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[9] C. Li at al, Secrecy Capacity of Colored Gaussian Noise Channels With Feedback, IEEE Trans. Info. Theory, v. 65, no. 9, pp. 5771–5782, Sep. 2019.

[10] D. Gunduz et al, Secret Communication With Feedback, Int. Symp. Info. Theory Appl., Auckland, New Zealand, Dec. 2008.

[11] E. Ardestanizadeh et al, Wiretap Channel With Secure Rate-Limited Feedback, IEEE Trans. Info. Theory, vol. 55, no. 12, pp. 5353–5361, Dec. 2009.

[12] G. Keshet, Y. Steinberg, N. Merhav, Channel Coding in the Presence of Side Information, Foundations and Trends in Comm. Info. Theory, vol. 4, no. 6, pp. 445–586, June 2008.

[13] S. I. Bross, A. Lapidoth, and G. Marti, Decoder-assisted communications over additive noise channels, IEEE Trans. Commun., vol. 68, no. 7, pp. 4150–4161, Jul. 2020.

[14] A. Lapidoth, G. Marti, Encoder-Assisted Communications Over Additive Noise Channels, IEEE Trans. Info. Theory, vol. 66, no. 11, pp. 6607–6616, Nov. 2020.

[15] N. Merhav, On Error Exponents of Encoder-Assisted Communication Systems, IEEE Trans. Info. Theory, vol. 67, no. 11, pp. 7019–7029, Nov. 2021.

[16] R. Fritschek and G. Wunder, Towards A Constant-Gap Sum-Capacity Result For The Gaussian Wiretap Channel With a Helper, Int. Symp. Info. Theory (ISIT), Jul. 2016, pp. 2978–2982.

[17] J. Chen, C. Geng, Optimal Secure GDoF of Symmetric Gaussian Wiretap Channel With a Helper, IEEE Trans. Info. Theory, v. 67, no. 4, pp. 2334–2352, Apr. 2021.

[18] S. Boyd and L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004.

[19] S. Loyka, N. Merhav, The Secrecy Capacity of The Gaussian Wiretap Channel with Rate-Limited Help at the Decoder, IEEE Int. Symp. Info. Theory (ISIT), Helsinki, Finland, 26 June - 1 July 2022.

[20] S. Loyka, N. Merhav, The Secrecy Capacity of The Gaussian Wiretap Channel with Rate-Limited Help (full version), arXiv preprint arXiv:2209.09356. Sep. 2022.