The Secrecy Capacity of The Gaussian Wiretap Channel with Rate-Limited Help at the Decoder

Sergey Loyka, Neri Merhav

***Abstract*—The Gaussian wiretap channel with rate-limited help available at the legitimate receiver (decoder) is studied under various channel configurations (degraded, reversely degraded and non-degraded). In all considered cases but one, the rate-limited help results in a secrecy capacity boost equal to the help rate. This holds irrespective of whether the help is secure or not, so that secure help does not provide any advantage over non-secure one. The secrecy capacity is positive for the reversely-degraded channel (where the no-help secrecy capacity is zero) and no wiretap coding is needed to achieve it. More noise at the legitimate receiver can sometimes result in higher secrecy capacity. The same secrecy capacity boost also holds if non-secure help is available to the transmitter (encoder), in addition to or instead of the receiver help.**

I. Introduction

Physical-layer security has attracted significant attention as a valuable alternative to cryptography-based techniques, especially over wireless channels [1]-[3]. While the original work of information-theoretic secrecy originates back to Shannon himself [4], Wyner's wiretap channel model [5] established itself as a very useful tool for many different settings and configurations. Its key performance metric is the secrecy capacity, i.e. the largest achievable rate subject to reliability, secrecy and possibly power constraints. The original discrete memoryless model was extended to single-antenna (SISO) Gaussian settings in [6] and to multi-antenna (MIMO) settings in [8]-[10] and the respective secrecy capacities were established. The Gaussian WTC with noiseless feedback was considered in [11], 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 a noisy version of the feedback. Its secrecy capacity was shown to be equal to the regular AWGN channel capacity (no Ev), i.e. secrecy comes for free with noiseless feedback, even if the main Tx-Rx channel is not degraded. This result was extended to a colored (ARMA) Gaussian noise channel with feedback in [12]. Note, however, that while the Tx has access to noiseless feedback, the Ev observes only its noisy version, i.e. it is at a significant disadvantage, and the situation changes dramatically if the Ev has access to the same noiseless feedback as well.

In modern communication systems/networks, various forms of side information are often available to encoder or/and decoder (e.g. in a cloud radio access network). This can be used to facilitate reliable communications and often results in a boost to the capacity [13]. One particular configuration was recently studied in [14]-[16], 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 another user) and communicates his observation to the receiver (decoder) or transmitter (encoder) via an error-free rate-limited data pipe. This was shown to provide a capacity boost equal to the help rate. In our opinion, this model is useful from a practical perspective since it considers rate-limited help, unlike noiseless feedback models which essentially require rate-unlimited and error-free feedback links, which are impossible in practice.

In the present paper, we extend the receiver help setting in [14] to the Gaussian wiretap channel and show that the same capacity boost as in [14] also holds for the wiretap channel in terms of its secrecy capacity: a receiver help of rate R_h results in the secrecy capacity boost of R_h (if noises are not Gaussian, then the rate boost is upper bounded by R_h). This holds for all possible configurations of the SISO Gaussian WTC, i.e. degraded, reversely degraded and non-degraded[1], with only one exception. Some surprising properties are observed. In particular, the secrecy capacity is the same irrespective of whether the help is secure (i.e. unknown to the eavesdropper) or not, so that secure help does not provide any advantage in secrecy rates over non-secure one, and this also applies to the case of partially-secure help. For the reversely-degraded channel (where the secrecy capacity is zero without help), we show that the secrecy capacity with Rx help is positive, that no wiretap coding is needed to achieve it, and that burst signaling is optimal. Sometimes, more noise at the legitimate receiver can result in higher secrecy capacity. We further show that, in the case of the degraded Gaussian WTC, the same secrecy rate boost also holds when non-secure help is available to the transmitter, in addition to or instead of the Rx help. Unlike the studies in [11][12], we allow here the Ev to have access to exactly the same help as the legitimate Rx or Tx (in the case of non-secure help).

In a related line of work, secure communication with a helper acting as a cooperating jammer was studied in [17][18] (this setting is partialy equivalent to an interference channel). However, no secrecy capacity was established but only the generalized degrees of freedom (GDoF), which characterize the high-SNR scaling of the secrecy capacity and are essentially the multiplexing gain in terms of secrecy rates. Unlike [17][18], the present paper considers no jamming at all; rather, the help comes in a form of rate-limited error-free information about the noise sequence affecting the legitimate Rx.

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.

[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 help is also available to the Ev.

978-1-6654-2159-1/22/$31.00 ©2022 Crown

II. Degraded Gaussian Wiretap Channel

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

$$Y_i = X_i + W_i,\ Z_i = Y_i + V_i \tag{1}$$

where X_i is the transmitted symbol at time i, $W_i,\ V_i$ are Rx and Ev noise, which are zero-mean Gaussian, independent of each other, of variance 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 $\sigma_v > 0$ and that the input power constraint is strictly positive, $P > 0$. A slightly more general case, where noises are not Gaussian, will also be considered.

Help T of rate R_h is available to the Rx and Ev, which we term "non-secure Rx help", so that the Rx and the Ev can estimate transmitted message M using T and their respective received signals Y^n and Z^n. If no help is available to the Ev, we call it "secure Rx help". For Rx help, the difference between causal and non-causal help is immaterial, since the Rx waits until the whole block of length n is transmitted before decoding it.

We use the standard definition of the secrecy capacity as the supremum of all achievable secrecy rates, subject to the reliability, secrecy and power constraints, see e.g. [1]-[7]. In particular, (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 and the Rx decoder maps Y^n and the available help T into message estimate $\hat{M}$. The constraints are as follows:

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

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

$$R_l \triangleq n^{-1} I(M; Z^n T) \leq \epsilon \tag{2}$$

for any $\epsilon > 0$ and sufficiently large n, where I is the mutual information; T is omitted in the case of secure help.

Average power constraint:

$$\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}|X_i|^2 \leq P \tag{3}$$

The secrecy capacity of this channel is established below.

Theorem 1. *The secrecy capacity C_s of the degraded memoryless WTC (not necessarily Gaussian) with Rx help of rate R_h, secure or not, is bounded as follows*

$$C_s \leq C_{s0} + R_h \tag{4}$$

where C_{s0} is the secrecy capacity without help. The upper bound is attained in the Gaussian case if $\sigma_V > 0$, for which $C_{s0} = C_1 - C_2$, where C_1, C_2 are the capacities of the Tx-Rx and Tx-Ev links (without help).

Proof. Converse: For the converse, we do not assume that the noises are Gaussian and consider the case of secure Rx help (not available to the Ev); the case of non-secure help will follow since the availability of help to the Ev cannot increase secrecy rate. The converse is based on the following chain argument, incorporating the secrecy and reliability constraints as well as functional relationship between random variables in the channel model:

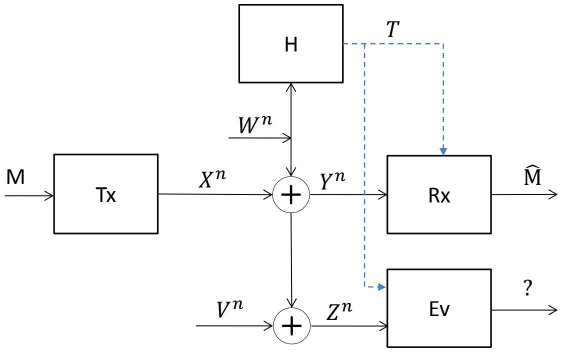

Fig. 1. Degraded wiretap channel with a rate-limited help T at the Rx and Ev. W^n and V^n are i.i.d. noise sequences independent of each other.

$$\begin{aligned}
nR_s &= H(M) \\
&\leq H(M|Z^n) + n\epsilon && (5)\\
&\leq H(M|Z^n) - H(M|Y^nT) + 2n\epsilon && (6)\\
&\leq H(M|Z^n) - H(M|Y^nZ^nT) + 2n\epsilon && (7)\\
&= I(M; Y^nT|Z^n) + 2n\epsilon && (8)\\
&\leq I(X^n; Y^nT|Z^n) + 2n\epsilon && (9)\\
&= I(X^n; Y^n|Z^n) + I(X^n; T|Y^nZ^n) + 2n\epsilon && (10)\\
&\leq I(X^n; Y^n|Z^n) + H(T) + 2n\epsilon && (11)\\
&\leq nI_0(X; Y|Z) + nR_h + 2n\epsilon && (12)\\
&= n(I_0(X; Y) - I_0(X; Z) + R_h + 2\epsilon) && (13)\\
&\leq n(C_{s0} + R_h + 2\epsilon) && (14)
\end{aligned}$$

where (5) follows from the secrecy constraint $I(M; Z^n) \leq n\epsilon$; (6) follows from Fano inequality (due to the reliability constraint) $H(M|Y^nT) \leq n\epsilon$; (9) follows from Markov chain $M - X^n - Y^nT - Z^n$; (11) follows from $I(X^n; T|Y^nZ^n) \leq H(T)$; (12) follows from

$$I(X^n; Y^n|Z^n) \leq \sum_{i=1}^{n} I(X_i; Y_i|Z_i) \leq nI_0(X; Y|Z) \tag{15}$$

where the first inequality is due to the assumed memorylessness of the channels and the second one is due to the concavity of the MI in the input distribution [5][7]; I_0 is the MI induced by input X with the distribution $p_0(x) = n^{-1}\sum_i p_{xi}(x)$, where $p_{xi}(x)$ is the distribution of X_i; (13) follows from Markov chain $X - Y - Z$. Thus,

$$R_s \leq C_{s0} + R_h + 2\epsilon \tag{16}$$

Since this holds for any $\epsilon > 0$, it follows that $R_s \leq C_{s0} + R_h$. This establishes the converse with secure Rx help. Since the presence of help at Ev cannot increase secrecy rate, the same upper bound applies with non-secure Rx help.

Achievability. To prove achievability, we assume that noises are Gaussian and combine the regular wiretap coding with the flash signaling as in [14]. We consider first the case of non-secure Rx help (when the same help is available at the Rx and

Ev), from which achievality with secure Rx help follows. To this end, recall that the regular flash signaling (no Ev) with Rx help consists of 2 phases of time-sharing:

- Phase 1: no help is used at all for $(1-\tau)$ fraction of time, which achieves a rate arbitrary close to the regular channel capacity C.
- Phase 2: help is used at rate R_h/τ for τ fraction of time. In this phase, high-resolution (scalar) quantization (with $2^{R_h/\tau}$ levels) of each noise sample is provided to the Rx, so that the help $T = \hat{W}^n$, where $\hat{W}_i = Q(W_i)$ and $Q(\cdot)$ is a scalar quantizer. The Rx subtracts $\hat{W}^n$ from its received signal Y^n and decodes it using nearest-neighbour decoding, which achieves the rate arbitrary close to

  $$R_h/\tau(1+o(1)) \tag{17}$$

  where $o(1) \to 0$ at $\tau \to 0$, see [14] for details.

Overall, as $\tau \to 0$, the rate achieved after time-sharing is arbitrary close to

$$(1-\tau)C + \tau R_h/\tau(1+o(1)) \to C + R_h \tag{18}$$

To accommodate the Ev and the secrecy constraint, we modify this strategy as follows:

- Phase 1: use the regular WTC coding with no help [1]-[7] for $(1-\tau)$ fraction of time; this achieves a secrecy rate R_s arbitrary close to the regular WTC secrecy capacity C_{s0}: $R_s = C_{s0} - \epsilon$ for any $\epsilon > 0$.
- Phase 2: use no WTC coding at all, just the regular flash signaling as above.

While it is clear that secrecy is guaranteed during Phase 1 (via wiretap coding), it is also clear that secrecy is not guaranteed during Phase 2 (since no wiretap coding is used at all) so it is not clear whether secrecy is guaranteed overall (after time sharing). To demonstrate that this is indeed the case, we show that, during Phase 2, the information leakage rate to the Ev is finite, $R_{l2} < \infty$ so that the overall leakage rate R_l (after time sharing) is

$$R_l = (1-\tau)R_{l1} + \tau R_{l2} \le (1-\tau)\delta + \tau R_{l2} \to \delta \tag{19}$$

as $\tau \to 0$, for any $\delta > 0$, where $R_{l1} \le \delta$ is the information leakage rate during Phase 1.

To see that indeed $R_{l2} < \infty$, observe the following:

$$\begin{aligned}
R_{l2} &= n^{-1} I(M_2; Z^n \hat{W}^n | \mathcal{C}) && (20)\\
&\le n^{-1} I(M_2; Z^n \hat{W}^n W^n | \mathcal{C}) && (21)\\
&= n^{-1} I(M_2; Z^n | W^n \mathcal{C}) && (22)\\
&\le n^{-1} I(X^n; Z^n | W^n \mathcal{C}) && (23)\\
&= n^{-1} I(X^n; X^n + W^n + V^n | W^n \mathcal{C}) && (24)\\
&= n^{-1} I(X^n; X^n + V^n | \mathcal{C}) && (25)\\
&\le \frac{1}{2} \log\left(1 + \frac{P}{\sigma_V^2}\right) = C_2' < \infty && (26)
\end{aligned}$$

where M_2 is a message sent in Phase 2, X^n is a codeword (which depends on M_2, see Fig. 1), and the conditioning is on an i.i.d. randomly-generated codebook $\mathcal{C}$ (the codebook generation, encoding and decoding are as in [14]); (22) follows from independence of M_2 and $W^n, \hat{W}^n$ and from $\hat{W}_i = Q(W_i)$; (23) follows from the Markov chain $M_2 - X^n - Z^n W^n$; (25) follows from independence of W^n and X^n, V^n.

Hence, arbitrary low information leakage rate is guaranteed after time sharing with $\tau \to 0$, which satisfies the secrecy constraint. At the same time the overall secrecy rate (after time sharing) is

$$\begin{aligned}
(1-\tau)(C_{s0} - \epsilon) + \tau R_h/\tau(1+o(1)) &\\
\to C_{s0} + R_h - \epsilon & \qquad (27)
\end{aligned}$$

for any $\epsilon > 0$, as $\tau \to 0$, so that the secrecy capacity is $C_{s0} + R_h$, as required.

In the above secrecy analysis, we assume that the help is not secure, i.e. it is available to the Ev. Clearly, the secrecy constraint is also satisfied if the help is secure, i.e. not available to the Ev (since the lack of Ev help cannot increase leakage rate), and an achievable secrecy rate remains the same. Since the converse also holds for the secure Rx help, the secrecy capacity also remains the same, regardless whether help is secure or not, i.e. the secrecy of help does not increase the secrecy capacity. □

It is worthwhile to note that flash signaling provides here the same boost in secrecy capacity as in the regular channel capacity (no Ev) in [14], i.e. the $+R_h$ boost comes with secrecy for free in the degraded Gaussian WTC. If noises are not Gaussian, then the rate boost is upper bounded by R_h.

Since C_s in Theorem 1 is the same for secure and non-secure help, it also applies to the case of partially-secure help, i.e. when the Ev has access to a part of T.

III. Reversely-Degraded Channel

Now, we consider the reversely-degraded case of the wiretap channel as in Fig. 2:

$$Z_i = X_i + V_i,\ Y_i = Z_i + \Delta W_i \tag{28}$$

where ΔW_i is an extra Rx noise, independent of Ev noise V_i, so that the sequences V^n and ΔW^n are i.i.d and independent of each other. Note that the total Rx noise is $W_i = V_i + \Delta W_i$ and its variance

$$\sigma_W^2 = \sigma_V^2 + \sigma_{\Delta W}^2 \ge \sigma_V^2 > 0 \tag{29}$$

so it is indeed a reversely-degraded case (we exclude the trivial case $\sigma_V = 0$, for which the secrecy capacity is zero). It is well-known that, without help, the secrecy capacity of this channel is zero, $C_{s0} = 0$. However, the availability of Rx help, either secure or not, changes the situation dramatically.

Theorem 2. *The secrecy capacity C_s of the reversely-degraded WTC (not necessarily Gaussian) with Rx help of rate R_h, secure or not, is bounded as follows*

$$C_s \le R_h \tag{30}$$

and the upper bound is attained in the Gaussian case if $\sigma_{\Delta W} > 0$; if $\sigma_{\Delta W} = 0$, then $C_s = R_h$ if help is secure and $C_s = 0$ otherwise.

Proof. Converse: to prove the converse, we do not assume that the noises are Gaussian and consider the case of secure Rx help (i.e. no Ev help). The case of non-secure help will

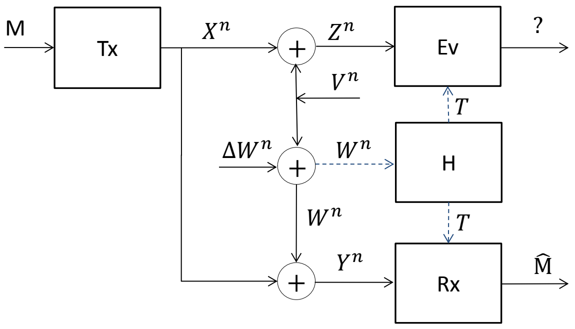

Fig. 2. Reversely-degraded wiretap channel with a rate-limited Rx help T. ΔW^n and V^n are i.i.d. noise sequences independent of each other.

follow, since the availability of help to the Ev cannot increase the secrecy rate. The proof follows the steps similar to those in Theorem 1. In particular, we observe that (5)-(11) still hold for the reversely-degraded channel (since channel degradedness plays no role there), so that

$$
\begin{aligned}
nR_s &\leq I(X^n;Y^n|Z^n) + H(T) + 2n\epsilon && (31)\\
&\leq n(R_h + 2\epsilon) && (32)
\end{aligned}
$$

where the last inequality is due to $I(X^n;Y^n|Z^n) = 0$, which in turn follows from Markov chain $X^n - Z^n - Y^n$. Thus, $R_s \leq R_h + \epsilon$ for any $\epsilon > 0$ and therefore $R_s \leq R_h$, as required.

Achievability: to prove achievability, we assume that the noises are Gaussian and consider the case of non-secure Rx help (when the same help is also available to the Ev); the case of secure help will follow since the absence of help to the Ev cannot increase leakage rate and hence cannot decrease secrecy rate.

To this end, we use the same two-phase flash signaling as in Theorem 1 except that nothing is transmitted in phase 1 and the whole message is transmitted in phase 2 (without any wiretap coding at all). To show that this provides arbitrary-low leakage rate after time-sharing (which is equivalent to burst signaling of duration τ in this case), we show that Phase 2 leakage rate R_{l2} is finite. To this end, we observe that

$$
\begin{aligned}
R_{l2} &= n^{-1}I(M_2;Z^n\hat{W}^n|\mathcal{C}) && (33)\\
&\leq n^{-1}I(M_2;Z^n\hat{W}^nW^n|\mathcal{C}) && (34)\\
&= n^{-1}I(M_2;Z^n|W^n\mathcal{C}) && (35)\\
&\leq n^{-1}I(X^n;Z^n|W^n\mathcal{C}) && (36)\\
&= n^{-1}I(X^n;X^n+V^n|V^n+\Delta W^n,\mathcal{C}) && (37)\\
&= n^{-1}(H(X^n+V^n|V^n+\Delta W^n,\mathcal{C}) && (38)\\
&\quad - H(V^n|X^n,V^n+\Delta W^n,\mathcal{C}))\\
&\leq n^{-1}(H(X^n+V^n) - H(V^n|V^n+\Delta W^n) && (39)\\
&\leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_V^2}\right) + \frac{1}{2}\log\left(1+\frac{\sigma_V^2}{\sigma_{\Delta W}^2}\right) < \infty && (40)
\end{aligned}
$$

where we assumed that $\sigma_{\Delta W} > 0$; (33)-(36) hold due to the same reasons as in the proof of Theorem 1; (39) holds since (i) conditioning cannot increase the entropy and (ii) $V^n, \Delta W^n$ are independent of $X^n, \mathcal{C}$; (40) holds since (i) the entropy is maximized by Gaussian distribution and

$$
\begin{aligned}
&H(V^n|V^n+\Delta W^n)\\
&\quad = H(V^n, V^n+\Delta W^n) - H(V^n+\Delta W^n) && (41)\\
&\quad = H(V^n) + H(\Delta W^n) - H(V^n+\Delta W^n) && (42)\\
&\quad = \frac{n}{2}\log\frac{\sigma_V^2}{\sigma_V^2+\sigma_{\Delta W}^2} + \frac{n}{2}\log(2\pi e\sigma_{\Delta W}^2) && (43)
\end{aligned}
$$

where (42) is due to the independence of ΔW^n and V^n. Thus, the total leakage rate (after time-sharing) is

$$
\begin{aligned}
R_l &= (1-\tau)0 + \tau R_{l2} && (44)\\
&\leq \frac{\tau}{2}\log\left(1+\frac{P}{\sigma_V^2}\right) + \frac{\tau}{2}\log\left(1+\frac{\sigma_V^2}{\sigma_{\Delta W}^2}\right) \to 0 && (45)
\end{aligned}
$$

when $\tau \to 0$, as required (notice that the condition $\sigma_{\Delta W} > 0$ is essential here, as $\sigma_{\Delta W} = 0$ results in zero secrecy capacity for non-secure help). The overall secrecy rate (after time-sharing) is

$$
R_s = (1-\tau)0 + \tau R_h/\tau(1+o(1)) \to R_h \qquad (46)
$$

when $\tau \to 0$.

Let us now consider the case of $\sigma_{\Delta W} = 0$, which implies $Y^n = Z^n$. If help is not secure, the same information is available to the Ev and Rx and hence no positive secrecy rate is achievable, $C_s = 0$. However, if the help is secure, then the Rx has an extra information not available to the Ev. It is not difficult to see that the above converse still holds if $\sigma_{\Delta W} = 0$. To prove achievability, we use the same signaling as above and show that the leakage rate R_{l2} of Phase 2 is finite:

$$
\begin{aligned}
R_{l2} &= n^{-1}I(M_2;Z^n|\mathcal{C}) && (47)\\
&\leq n^{-1}I(X^n;Z^n|\mathcal{C}) && (48)\\
&\leq n^{-1}(H(Z^n) - H(V^n)) && (49)\\
&\leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_V^2}\right) < \infty && (50)
\end{aligned}
$$

Thus, secrecy is guaranteed after time-sharing with $\tau \to 0$ and the achieved secrecy rate is as in (46). □

A surprising observation follows from this result: in the case of non-secure help, $C_s = 0$ if $\sigma_W = \sigma_V$ (i.e. $\sigma_{\Delta W} = 0$) but $C_s = R_h > 0$ if $\sigma_W > \sigma_V$, so that more noise at the legitimate Rx is actually better for secrecy in this case. This is due to the fact that the extra Rx noise $\Delta W_i \neq 0$ makes it impossible for the Ev to cancel its own noise using non-secure help $\hat{W}^n$ in the same way the Rx does (since $V_i \neq W_i$ in this case). However, if $\Delta W_i = 0$, then the Ev can do noise cancellation in the same way the Rx does, which results in $C_s = 0$.

To summarize, the secrecy capacity C_s of the degraded or reversely degraded Gaussian wiretap channel with Rx help of rate R_h (secure or not) is given by

$$
C_s = C_{s0} + R_h \qquad (51)
$$

if either $\sigma_W \neq \sigma_V$ or else the help is secure, where, of course, $C_{s0} = 0$ for the reversely-degraded case. Thus, not only the secrecy capacity is boosted by R_h for the degraded case, but also the secrecy capacity is positive for the reversely-degraded case, where it is zero without help, and this positive capacity is achievable by burst signalling without wiretap coding at all.

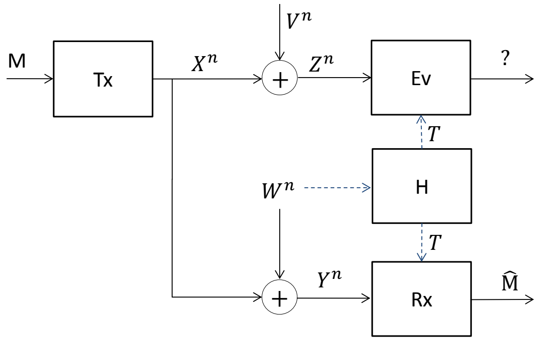

Fig. 3. Non-degraded Gaussian wiretap channel with a rate-limited Rx help T; noise sequences W^n and V^n are i.i.d. Gaussian and independent of each other.

IV. Non-Degraded Channel

Now, we consider the case where the channel is neither degraded nor reversely-degraded since its Rx and Ev branches have independent noises, as in Fig. 3:

$$Z_i = X_i + V_i,\ Y_i = X_i + W_i \tag{52}$$

where the sequences V^n and W^n are i.i.d Gaussian and independent of each other. It is well-known that, without help, this case can be equivalently reduced to either degraded or reversely-degraded case, since the Rx and Ev performance depends on the marginal distributions of W^n and V^n, respectively, not on their join distribution [1]. While this is still true for the secure Rx help (no Ev help), it is no longer true for the non-secure help (since Ev performance now depends on both V^n and W^n). Thus, the secrecy capacity of this channel does not follow from that of the degraded or reversely-degraded one. Yet, we show below that it is still $C_{s0} + R_h$.

Theorem 3. *The secrecy capacity C_s of the non-degraded Gaussian WTC with Rx help of rate R_h, secure or not, is*

$$C_s = C_{s0} + R_h \tag{53}$$

Proof. Converse: we follow the steps of the proof of Theorem 2 and consider first the case of secure Rx help (i.e. no Ev help). Note that, in this case, Ev's performance depends on V^n only, not on W^n; likewise, Rx's performance depends on W^n only, not on V^n. Hence, this channel can now be equivalently reduced to degraded or reversely-degraded case, for which the converse have been established in Theorem 1 or 2, respectively, so that $R \le C_{s0} + R_h$. This argument does not apply for non-secure Rx help. However, since the availability of help to Ev cannot increase the secrecy rate, the same upper bound still holds. This establishes the converse for non-secure Rx help as well.

Achievability: Likewise, we can argue that, in the case of secure Rx help, the achievability result of Theorem 1 or 2 apply. However, it is no longer the case for non-secure help. Furthermore, the achievability under secure help does not imply the achievability under non-secure help. To establish the latter, we use the signaling strategy of Theorem 1 if $\sigma_W < \sigma_V$ and of Theorem 2 if $\sigma_W \ge \sigma_V$, and show that the leakage rate R_{l2} of Phase 2 is finite in both cases:

$$\begin{aligned} R_{l2} &= n^{-1} I(M_2; Z^n \hat{W}^n | \mathcal{C}) && (54)\\ &= n^{-1} I(M_2; Z^n | \hat{W}^n \mathcal{C}) && (55)\\ &= n^{-1} I(M_2; Z^n | \mathcal{C}) && (56)\\ &\le n^{-1} I(X^n; Z^n | \mathcal{C}) && (57)\\ &\le \frac{1}{2} \log\left(1 + \frac{P}{\sigma_V^2}\right) = C_2 < \infty && (58) \end{aligned}$$

where (55) and (56) follow from independence of M_2, Z^n and $\hat{W}^n$. This ensures secrecy after time sharing with $\tau \to 0$, as in (19). □

Note that, if $\sigma_W \ge \sigma_V$, then $C_{s0} = 0$ and $C_s = R_h$, i.e. if the Tx-Rx channel is weaker than the Tx-Ev channel, the secrecy capacity with Rx help is still positive (if $R_h > 0$), even if the help is not secure. This also holds for the non-degraded channel if $\sigma_W = \sigma_V$, unlike the case of the reversely-degraded channel, where $C_s = 0$ if $\sigma_W = \sigma_V$ and the help is not secure. This is due to the independence of W^n and V^n in the non-degraded channel. It can be further shown that Theorem 3 also holds if V_i and W_i are correlated provided that their joint covariance matrix is not singular.

V. The Degraded WTC with Tx Help

Finally, we consider the setting of Fig. 1 and extend Theorem 1 to the scenario where non-secure rate-limited help is available to the Tx, in addition to or instead of the Rx help.

Theorem 4. *The secrecy capacity C_s of the degraded Gaussian WTC with non-secure Tx help of rate R_h, in addition to or instead of the same Rx help, is*

$$C_s = C_{s0} + R_h \tag{59}$$

where C_{s0} is the secrecy capacity without help.

Proof. The achievability is based on the 2 phases of flash signaling as in Theorem 1, with noise pre-cancellation at the Tx (a.k.a. dirty-paper coding, as in [15]) in Phase 2. The converse is based on a judicious incorporation of the secrecy constraint into the converse of Theorem 2 in [15]. The details are omitted due to the page limit. □

Note that the availability of the Rx help, in addition to the Tx help, does not increase the secrecy capacity (provided the help T is the same in both cases).

VI. Conclusion

The SISO Gaussian wiretap channel with rate-limited help at the receiver (decoder) was studied and its secrecy capacity has been established under various channel configurations (degraded, reversely degraded and non-degraded) for secure and non-secure help. In all considered cases but one, the rate-limited help results in the secrecy capacity boost (compared to the standard ”no help” case) equal to the help rate, so that positive secrecy rate is achievable even for reversely-degraded channel, where the secrecy capacity is zero without help. Surprisingly, secure help does not result in higher capacity compared to non-secure one and more noise at the legitimate receiver can sometimes be beneficial for secrecy.

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

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

[6] S. K. Leung-Yan-Cheong and M. Hellman, The Gaussian Wire-Tap Channel, IEEE Trans. Info. Theory, v. 24, no. 4, pp. 451–456, July 1978.

[7] J.L. Massey, A Simplified Treatment of Wyner's Wiretap Channel, 21st Allerton Conf. on Comm., Control and Computing, pp. 268-276, Monticello, IL, Oct. 5-7, 1983.

[8] A. Khisti, G. W. Wornell, Secure transmission with multiple antennas - Part I: The MISOME wiretap channel, IEEE Trans. Inf. Theory, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[9] A. Khisti, G. W. Wornell, Secure transmission with multiple antennas - Part II: The MIMOME wiretap channel, IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[10] F. Oggier, B. Hassibi, The secrecy capacity of the MIMO wiretap channel, IEEE Trans. Inf. Theory, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

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

[12] 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.

[13] 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.

[14] 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.

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

[16] G. Marti, Channels With a Helper, M.S. Thesis, Signal Info. Process. Lab., ETH Zrich, Zurich, Switzerland, Sep. 2019.

[17] 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.

[18] 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.

[19] T.M. Cover, J.A. Thomas, Elements of Information Theory, Wiley, 2006.