Feedback Capacity of Gaussian Multiple-Access Wiretap Channel with Degraded Message Sets

Bin Dai*¶, Chong Li†, Yingbin Liang‡, Zheng Ma*, Shlomo Shamai (Shitz)§
* School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 610031, China.
¶ The State Key Laboratory of Integrated Services Networks, Xidian University, Xi′an, Shaanxi 710071, China.
† Nakamoto & Turing Labs, New York, 10018, USA.
‡ Department of Electrical and Computer Engineering, The Ohio State University, Columbus, 43220, USA.
§ Department of Electrical Engineering, Technion-Israel Institute of Technology, Technion City, 32000, Israel.
daibin@home.swjtu.edu.cn, chongl@ntlabs.io, liang.889@osu.edu, zma@home.swjtu.edu.cn, sshlomo@ee.technion.ac.il.

***Abstract*—The Schalkwijk-Kailath (SK) feedback scheme is a capacity-achieving coding scheme for the point-to-point white Gaussian channel with feedback. Recently, it has been shown that the SK scheme, which is not designed with consideration of secrecy, already achieves perfect weak secrecy by itself, i.e., the secrecy capacity of the Gaussian wiretap channel with feedback equals the capacity of the same model without secrecy constraint. In this paper, we propose a capacity-achieving SK type feedback scheme for the two-user Gaussian multiple-access channel with degraded message sets (GMAC-DMS). Similarly to the inherent secrecy nature of the classical SK scheme, we show that the proposed scheme is also secure by itself, which indicates that the feedback secrecy capacity of the two-user Gaussian multiple-access wiretap channel with degraded message sets (GMAC-WT-DMS) equals the capacity of the same model without secrecy constraint.**

***Index Terms*—Gaussian multiple-access wiretap channel, feedback, secrecy capacity region.**

I. Introduction

[1] Schalkwijk and Kailath [1] showed that although feedback does not increase the capacity of the white Gaussian channel, it helps to improve the channel encoding-decoding performance. Recently, [2] found the inherent secrecy nature of the Schalkwijk-Kailath (SK) feedback scheme [1], i.e., the SK scheme, which is not designed with consideration of secrecy, achieves perfect weak secrecy by itself. The inherent secrecy nature found in [2] indicates that the secrecy capacity of the white Gaussian wiretap channel with feedback equals the capacity of the same model without secrecy constraint, and it can be achieved by the SK feedback scheme. The follow-up work of [2] includes:

- For the dirty paper channel with feedback, [4] found the inherent secrecy nature of a capacity-achieving SK type feedback scheme proposed in [3].
- [5] proposed a capacity-achieving SK type feedback scheme for the colored Gaussian channel, and showed that the inherent secrecy nature of this scheme holds.

Although the inherent secrecy nature of SK type feedback schemes has been found for the point-to-point Gaussian channels, such a topic is mostly open for multi-user Gaussian channel models. In this paper, we focus on the two-user Gaussian multiple-access channel with degraded message sets (GMAC-DMS), and would like to answer the following two open questions:

- Does there exist a capacity-achieving SK type feedback scheme for the two-user GMAC-DMS?
- Does the inherent secrecy nature still hold for this capacity-achieving scheme, namely, the capacity-achieving scheme of the two-user GMAC-DMS also achieves the feedback secrecy capacity region of the two-user Gaussian multiple-access wiretap channel with degraded message sets [2](GMAC-WT-DMS)?

We summarize our contributions as follows.

- A capacity-achieving SK type feedback scheme is proposed for the two-user GMAC-DMS.
- This capacity-achieving scheme is shown to be secure by itself, i.e., the proposed capacity-achieving feedback scheme for the two-user GMAC-DMS also achieves the feedback secrecy capacity region of the two-user GMAC-WT-DMS, which indicates that the feedback secrecy capacity region equals the capacity region of the same model without secrecy constraint.

II. Preliminaries: The SK Scheme for the White Gaussian channel with feedback

For the white Gaussian channel with feedback (see Figure 1), at each time i ($i \in \{1, 2, ..., N\}$), the channel input-output relationship is given by

$$Y_i = X_i + \eta_{1,i}, \tag{2.1}$$

where X_i is the channel input subject to average power constraint P, Y_i is the channel output, and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$

[1]Acknowledgment: The work of B. Dai was supported by the National Natural Science Foundation of China under Grants 62071392, 61671391, the 111 Project No.111-2-14, and the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University (No. ISN21-12). The work of Y. Liang was supported by U.S. NSF CCF-1801846. The work of Z. Ma was supported by U1734209 and Marie Curie Fellowship (no. 796426). The work of S. Shamai was supported by the European Union's Horizon 2020 Research And Innovation Programme under Grant 694630.

[2]In [6], a sub-optimal feedback scheme has been shown to achieve an inner bound on the feedback secrecy capacity region of the two-user GMAC-WT-DMS.

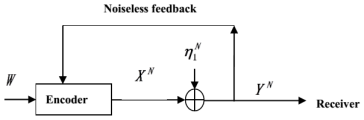

Fig. 1: The white Gaussian channel with feedback.

is the white Gaussian noise and it is independent identically distributed (i.i.d.) across the time index i. The message W is uniformly distributed in $\mathcal{W} = \{1, 2, ..., |\mathcal{W}|\}$. The channel input X_i is a function of the message W and the feedback $Y^{i-1} = (Y_1, ..., Y_{i-1})$. The receiver generates an estimation $\hat{W} = \psi(Y^N)$, where ψ is the receiver's decoding function, and the average decoding error probability equals

$$P_e = \frac{1}{|\mathcal{W}|} \sum_{w \in \mathcal{W}} Pr\{\psi(y^N) \neq w | w \text{ sent}\}. \tag{2.2}$$

The capacity of the white Gaussian channel with feedback is denoted by $\mathcal{C}_g^f$, and it equals the capacity $\mathcal{C}_g$ of the white Gaussian channel, which is given by

$$\mathcal{C}_g^f = \mathcal{C}_g = \frac{1}{2} \log(1 + \frac{P}{\sigma_1^2}). \tag{2.3}$$

In [1], it has been shown that SK scheme achieves $\mathcal{C}_g^f$, and this classical scheme is briefly described below.

Since W takes values in $\mathcal{W} = \{1, 2, ..., 2^{NR}\}$, divide the 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 (w.r.t.) the message W (the variance of θ approximately equals $\frac{1}{12}$). At time 1, the transmitter sends

$$X_1 = \sqrt{12P}\theta. \tag{2.4}$$

The receiver obtains $Y_1 = X_1 + \eta_{1,1}$, and gets an estimation of θ by computing

$$\hat{\theta}_1 = \frac{Y_1}{\sqrt{12P}} = \theta + \frac{\eta_{1,1}}{\sqrt{12P}} = \theta + \epsilon_1, \tag{2.5}$$

where $\epsilon_1 = \hat{\theta}_1 - \theta = \frac{\eta_1}{\sqrt{12P}}$. Let $\alpha_1 \triangleq Var(\epsilon_1) = \frac{\sigma_1^2}{12P}$.

At time $2 \leq k \leq N$, the receiver obtains $Y_k = X_k + \eta_{1,k}$, and gets an estimation of θ_k by computing

$$\hat{\theta}_k = \hat{\theta}_{k-1} - \frac{E[Y_k \epsilon_{k-1}]}{E[Y_k^2]} Y_k, \tag{2.6}$$

where $\epsilon_k = \hat{\theta}_k - \theta$. (2.6) yields that

$$\epsilon_k = \epsilon_{k-1} - \frac{E[Y_k \epsilon_{k-1}]}{E[Y_k^2]} Y_k. \tag{2.7}$$

Meanwhile, for time $2 \leq k \leq N$, the transmitter sends

$$X_k = \sqrt{\frac{P}{\alpha_{k-1}}} \epsilon_{k-1}, \tag{2.8}$$

where $\alpha_{k-1} \triangleq Var(\epsilon_{k-1})$.

In [1], it has been shown that if $R < \frac{1}{2} \log(1 + \frac{P}{\sigma_1^2})$, the decoding error P_e of the above coding scheme *doubly exponentially decays to zero* as $N \to \infty$.

III. Capacity-Achieving Feedback Scheme for the Two-User GMAC-DMS

A. Problem formulation

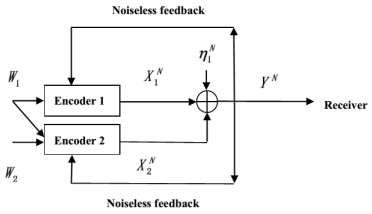

Fig. 2: The two-user GMAC-DMS with noiseless feedback.

For the GMAC-DMS with feedback (see Figure 2), at each time i ($i \in \{1, 2, ..., N\}$), the channel input-output relationship is given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_{1,i}, \tag{3.1}$$

where $X_{1,i}$ and $X_{2,i}$ are the channel inputs subject to average power constraints P_1 and P_2, respectively, Y_i is the channel output, and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$ is the i.i.d. channel noise across the time index i. The message W_j ($j = 1, 2$) is uniformly distributed in $\mathcal{W}_j = \{1, 2, ..., |\mathcal{W}_j|\}$. The channel input $X_{1,i}$ is a function of the message W_1 and the feedback Y^{i-1}, and the channel input $X_{2,i}$ is a function of the messages W_1, W_2 and the feedback Y^{i-1}. The receiver generates an estimation $(\hat{W}_1, \hat{W}_2) = \psi(Y^N)$, where ψ is the receiver's decoding function, and the average decoding error probability equals

$$P_e = \frac{1}{|\mathcal{W}_1| \cdot |\mathcal{W}_2|} \sum_{w_1, w_2} Pr\{\psi(y^N) \neq (w_1, w_2) | (w_1, w_2) \text{ sent}\}. \tag{3.2}$$

A rate pair (R_1, R_2) is said to be achievable if for any ϵ and sufficiently large N, there exist channel encoders and decoder such that

$$\frac{\log |\mathcal{W}_1|}{N} = R_1, \ \frac{\log |\mathcal{W}_2|}{N} = R_2, \ P_e \leq \epsilon. \tag{3.3}$$

The capacity region $\mathcal{C}_{gmac-dms}^f$ of the GMAC-DMS with feedback is composed of all such achievable rate pairs. In addition, note that the model of GMAC-DMS is defined almost in the same fashion as GMAC-DMS with feedback, except that the channel input $X_{1,i}$ is a function of the message W_1 and $X_{2,i}$ is a function of the messages W_1 and W_2. The capacity region of GMAC-DMS is denoted with $\mathcal{C}_{gmac-dms}$.

B. A SK-type feedback scheme for the two-user GMAC-DMS with noiseless feedback

In this subsection, we propose a two-step SK type feedback scheme for the two-user GMAC-DMS with noiseless feedback, and in the next subsection, we will show that this two-step SK type scheme achieves the feedback capacity $\mathcal{C}_{gmac-dms}^f$. The two-step SK type feedback scheme is described below.

The main idea of the two-step SK type feedback scheme is briefly illustrated by Figure 3. In Figure 3, the common message W_1 is encoded by both transmitters, and the private

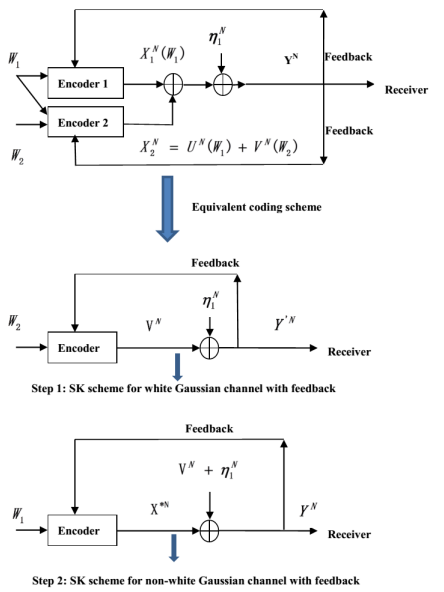

Fig. 3: Feedback coding scheme for GMAC-DMS with feedback.

message W_2 is only available at Transmitter 2. Specifically, Transmitter 1 uses power P_1 to encode W_1 and the feedback Y^N as X_1^N. Transmitter 2 uses power $(1-\rho^2)P_2$ to encode W_2 and Y^N as V^N, and power $\rho^2 P_2$ to encode W_1 and Y^N as U^N, where $0 \le \rho \le 1$ and

$$X_2^N = U^N + V^N. \tag{3.4}$$

Here note that the power of X_2^N equals P_2, and it can be checked by [10, eq. (5.38), p.33] and the properties in [10, Appendix B]. Since W_1 is known by Transmitter 2, the codeword X_1^N and U^N can be subtracted when applying SK scheme to W_2, i.e., for the SK scheme of W_2, the equivalent channel model has input V^N, output $Y^{'N} = Y^N - X_1^N - U^N$, and channel noise η_1^N.

In addition, since W_1 is known by both transmitters and W_2 is only available at Transmitter 2, for the SK scheme of W_1, the equivalent channel model has inputs X_1^N and U^N, output Y^N, and channel noise $\eta_1^N + V^N$, which is non-white Gaussian noise since V^N is not i.i.d. generated. Furthermore, observing that

$$Y_i = X_{1,i} + U_i + V_i + \eta_{1,i} = X_i^* + V_i + \eta_{1,i}, \tag{3.5}$$

where $X_i^* = X_{1,i} + U_i$, X_i^* is Gaussian distributed with zero mean and variance P_i^*,

$$\begin{aligned} P_i^* &= P_1 + \rho^2 P_2 + 2\sqrt{P_1 P_2}\rho\rho_i^{'} \\ &\le P_1 + \rho^2 P_2 + 2\sqrt{P_1 P_2}\rho = P^*, \end{aligned} \tag{3.6}$$

$\rho_i^{'} = \frac{E[X_{1,i}U_i]}{\rho\sqrt{P_1 P_2}}$ and $0 \le \rho_i^{'} \le 1$. Hence for the SK scheme of W_1, the input of the equivalent channel model can be viewed as X_i^*. Since $X_{1,i}$ is known by Transmitter 2, let

$$U_i = \rho\sqrt{\frac{P_2}{P_1}} X_{1,i}. \tag{3.7}$$

Then we have $\rho_i^{'} = 1$, which leads to $P_i^* = P^*$ and $X_i^* \sim \mathcal{N}(0, P^*)$. The encoding and decoding procedure of Figure 3 is described below.

Since W_j $(j = 1, 2)$ takes values in $\mathcal{W}_j = \{1, 2, ..., 2^{NR_j}\}$, divide the interval $[-0.5, 0.5]$ into 2^{NR_j} equally spaced sub-intervals, and the center of each sub-interval is mapped to a message value in $\mathcal{W}_j$. Let θ_j be the center of the sub-interval w.r.t. the message W_j (the variance of θ_j approximately equals $\frac{1}{12}$).

Encoding: At time 1, Transmitter 1 sends

$$X_{1,1} = 0. \tag{3.8}$$

Transmitter 2 sends

$$V_1 = \sqrt{12(1-\rho^2)P_2}\theta_2, \tag{3.9}$$

and

$$U_1 = \rho\sqrt{\frac{P_2}{P_1}} X_{1,1} = 0. \tag{3.10}$$

The receiver obtains $Y_1 = X_{1,1} + X_{2,1} + \eta_{1,1} = X_{1,1} + V_1 + U_1 + \eta_{1,1} = V_1 + \eta_{1,1}$, and sends Y_1 back to Transmitter 2. Let $Y_1^{'} = Y_1 = V_1 + \eta_{1,1}$, Transmitter 2 computes

$$\frac{Y_1^{'}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \epsilon_1. \tag{3.11}$$

Let $\alpha_1 \triangleq Var(\epsilon_1) = \frac{\sigma_1^2}{12(1-\rho^2)P_2}$.

At time 2, Transmitter 2 sends

$$V_2 = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_1}}\epsilon_1. \tag{3.12}$$

On the other hand, at time 2, Transmitters 1 and 2 respectively send $X_{1,2}$ and $U_2 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,2}$ such that

$$X_2^* = U_2 + X_{1,2} = \sqrt{12P^*}\theta_1. \tag{3.13}$$

Once receiving the feedback $Y_2 = X_2^* + V_2 + \eta_{1,2}$, both transmitters compute

$$\frac{Y_2}{\sqrt{12P^*}} = \theta_1 + \frac{V_2 + \eta_{1,2}}{\sqrt{12P^*}} = \theta_1 + \epsilon_2^{'}. \tag{3.14}$$

and send $X_{1,3}$ and $U_3 = \rho\sqrt{\frac{P_2}{P_1}}X_{1,3}$ such that

$$X_3^* = U_3 + X_{1,3} = \sqrt{\frac{P^*}{\alpha_2^{'}}}\epsilon_2^{'}, \tag{3.15}$$

where $\alpha_2^{'} \triangleq Var(\epsilon_2^{'})$. In addition, subtracting $X_{1,2}$ and U_2 from Y_2 and let $Y_2^{'} = Y_2 - X_{1,2} - U_2 = V_2 + \eta_{1,2}$, Transmitter 2 computes

$$\epsilon_2 = \epsilon_1 - \frac{E[Y_2^{'}\epsilon_1]}{E[(Y_2^{'})^2]}Y_2^{'}. \tag{3.16}$$

and sends

$$V_3 = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_2}}\epsilon_2, \tag{3.17}$$

where $\alpha_2 \triangleq Var(\epsilon_2)$.

At time $4 \leq k \leq N$, once receiving $Y_{k-1} = X_{1,k-1} + U_{k-1} + V_{k-1} + \eta_{1,k-1}$, Transmitter 2 computes

$$\epsilon_{k-1} = \epsilon_{k-2} - \frac{E[Y_{k-1}^{'}\epsilon_{k-2}]}{E[(Y_{k-1}^{'})^2]}Y_{k-1}^{'}, \quad (3.18)$$

where

$$Y_{k-1}^{'} = Y_{k-1} - X_{1,k-1} - U_{k-1}, \quad (3.19)$$

and sends

$$V_k = \sqrt{\frac{(1-\rho^2)P_2}{\alpha_{k-1}}}\epsilon_{k-1}, \quad (3.20)$$

where $\alpha_{k-1} \triangleq Var(\epsilon_{k-1})$. In the meanwhile, Transmitters 1 and 2 respectively send $X_{1,k}$ and $U_k = \rho\sqrt{\frac{P_2}{P_1}}X_{1,k}$ such that

$$X_k^* = U_k + X_{1,k} = \sqrt{\frac{P^*}{\alpha_{k-1}^{'}}}\epsilon_{k-1}^{'}, \quad (3.21)$$

where

$$\epsilon_{k-1}^{'} = \epsilon_{k-2}^{'} - \frac{E[Y_{k-1}\epsilon_{k-2}^{'}]}{E[(Y_{k-1})^2]}Y_{k-1}, \quad (3.22)$$

and $\alpha_{k-1}^{'} \triangleq Var(\epsilon_{k-1}^{'})$.

Decoding:

The receiver uses a two-step decoding scheme. First, from (2.6), we observe that at time k ($3 \leq k \leq N$), the receiver's estimation $\hat{\theta}_{1,k}$ of θ_1 is given by

$$\hat{\theta}_{1,k} = \hat{\theta}_{1,k-1} - \frac{E[Y_k\epsilon_{k-1}^{'}]}{E[(Y_k)^2]}Y_k, \quad (3.23)$$

where $\epsilon_{k-1}^{'} = \hat{\theta}_{1,k-1} - \theta_1$ and it is computed by (3.22), and

$$\hat{\theta}_{1,2} = \frac{Y_2}{\sqrt{12P^*}} = \theta_1 + \frac{V_2 + \eta_{1,2}}{\sqrt{12P^*}} = \theta_1 + \epsilon_2^{'}. \quad (3.24)$$

The following lemma 1 shows that the decoding error probability of θ_1 can be arbitrarily small if $R_1 < \frac{1}{2}\log(1 + \frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2})$ is satisfied.

Lemma 1: For the two-step SK type feedback scheme described above, let P_{e1} be the decoding error probability of W_1 (θ_1). If $R_1 < \frac{1}{2}\log(1 + \frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2})$, P_{e1} tends to 0 as $N \to \infty$.

Proof: See our full paper [10, Appendix B]. ∎

Second, after decoding W_1 and the corresponding codewords $X_{1,k}$ and U_k for all $1 \leq k \leq N$, the receiver subtracts $X_{1,k}$ and U_k from Y_k, and obtains $Y_k^{'} = V_k + \eta_{1,k}$. At time k ($1 \leq k \leq N$), the receiver's estimation $\hat{\theta}_{2,k}$ of θ_2 is given by

$$\hat{\theta}_{2,k} = \hat{\theta}_{2,k-1} - \frac{E[Y_k^{'}\epsilon_{k-1}]}{E[(Y_k^{'})^2]}Y_k^{'}, \quad (3.25)$$

where $\epsilon_{k-1} = \hat{\theta}_{2,k-1} - \theta_2$ and it is computed by (3.18), and

$$\hat{\theta}_{2,1} = \theta_2 + \frac{\eta_{1,1}}{\sqrt{12(1-\rho^2)P_2}} = \theta_2 + \epsilon_1. \quad (3.26)$$

The decoding error probability P_e of the receiver is upper bounded by $P_e \leq P_{e1} + P_{e2}$, where P_{ej} ($j = 1, 2$) is the receiver's decoding error probability of W_j. From the classical SK scheme [1] (also introduced in Section II), we know that the decoding error probability P_{e2} of W_2 tends to 0 as $N \to \infty$ if $R_2 < \frac{1}{2}\log(1+\frac{(1-\rho^2)P_2}{\sigma_1^2})$, and hence we omit the derivation here.

Now we have shown that if $R_1 < \frac{1}{2}\log(1 + \frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2})$ and $R_2 < \frac{1}{2}\log(1+\frac{(1-\rho^2)P_2}{\sigma_1^2})$, the decoding error probability P_e of the receiver tends to 0 as $N \to \infty$, i.e., the following region

$$\begin{aligned}&\mathcal{C}_{gmac-dms}^{f-in}\\ &= \bigcup_{0\leq\rho\leq1}\left\{(R_1,R_2): R_2 \leq \frac{1}{2}\log\left(1+\frac{P_2(1-\rho^2)}{\sigma_1^2}\right),\right.\\ &\left. R_1 \leq \frac{1}{2}\log\left(1+\frac{P_1+\rho^2P_2+2\sqrt{P_1P_2}\rho}{(1-\rho^2)P_2+\sigma_1^2}\right)\right\} \quad (3.27)\end{aligned}$$

is achievable.

C. Capacity of the two-user GMAC-DMS with noiseless feedback

The following Theorem 1 determines the capacity region $\mathcal{C}_{gmac-dms}^{f}$ of the two-user GMAC-DMS with feedback.

Theorem 1: $\mathcal{C}_{gmac-dms}^{f} = \mathcal{C}_{gmac-dms}^{f-in}$, where $\mathcal{C}_{gmac-dms}^{f-in}$ is given in (3.27).

Proof: The achievability of $\mathcal{C}_{gmac-dms}^{f}$ directly follows from the two-step SK type feedback scheme proposed in the preceding subsection. The converse proof of $\mathcal{C}_{gmac-dms}^{f}$ consists of two parts. First, from the converse proof of the bounds on R_2 and $R_1 + R_2$ in GMAC with feedback [9, pp. 627-628], we conclude that $\mathcal{C}_{gmac-dms}^{f}$ is outer bounded by

$$\begin{aligned}&\mathcal{C}_{gmac-dms}^{f-out}\\ &= \bigcup_{0\leq\rho\leq1}\left\{(R_1,R_2): R_2 \leq \frac{1}{2}\log\left(1+\frac{P_2(1-\rho^2)}{\sigma_1^2}\right),\right.\\ &\left. R_1+R_2 \leq \frac{1}{2}\log\left(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma_1^2}\right)\right\} \quad (3.28)\end{aligned}$$

Next, it is easy to check that the outer bound $\mathcal{C}_{gmac-dms}^{f-out}$ in (3.28) is exactly the same as the inner bound $\mathcal{C}_{gmac-dms}^{f-in}$ in (3.27), which completes the proof. ∎

Remark 1:

- The capacity region $\mathcal{C}_{gmac-dms}$ of the GMAC-DMS equals $\mathcal{C}_{gmac-dms}^{f-out}$ in (3.28), and the proof is briefly explained as follows. First, note that in [7], it has been shown that the capacity $\mathcal{C}_{mac-dms}$ of the discrete memoryless multiple-access channel with degraded message sets is given by

$$\begin{aligned}\mathcal{C}_{mac-dms} = \quad &\{(R_1,R_2): R_2 \leq I(X_2;Y|X_1),\\ &R_1+R_2 \leq I(X_1,X_2;Y)\} \quad (3.29)\end{aligned}$$

for some joint distribution $P_{X_1X_2}(x_1,x_2)$. Substituting $X_1 \sim \mathcal{N}(0,P_1)$, $X_2 \sim \mathcal{N}(0,P_2)$ and (3.1) into (3.29), defining $\rho = \frac{E[X_1X_2]}{\sqrt{P_1P_2}}$, and applying the encoding-decoding scheme of [7], an achievable region which

equals $\mathcal{C}_{gmac-dms}^{f-out}$ is obtained. Next, applying the converse proof of the bounds on R_2 and $R_1 + R_2$ in GMAC with feedback [9, pp. 627-628], we can conclude that $\mathcal{C}_{gmac-dms}$ is outer bounded by $\mathcal{C}_{gmac-dms}^{f-out}$, which completes the proof.

- In [8], it has been shown that feedback does not increase the capacity $\mathcal{C}_{mac-dms}$ of the discrete memoryless multiple-access channel with degraded message sets. Since $\mathcal{C}_{gmac-dms} = \mathcal{C}_{gmac-dms}^{f-out}$ and $\mathcal{C}_{gmac-dms}^{f} = \mathcal{C}_{gmac-dms}^{f-out}$, we can conclude that feedback also does not increase the capacity of the GMAC-DMS.

IV. Inherent Secrecy Nature of the Capacity-Achieving Feedback Scheme for the Two-User GMAC-DMS

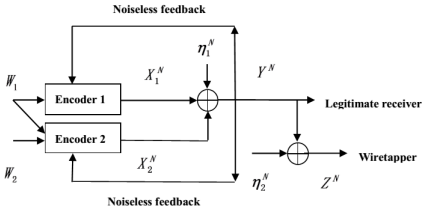

Fig. 4: The Gaussian multiple-access wiretap channel with degraded message sets and noiseless feedback.

For the Gaussian multiple-access wiretap channel with degraded message sets (GMAC-WT-DMS) and noiseless feedback (see Figure 4), at each time i ($i \in \{1, 2, ..., N\}$), the channel input-output relationships are given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_{1,i},\ Z_i = Y_i + \eta_{2,i}, \quad (4.1)$$

where $X_{1,i}$ and $X_{2,i}$ are the channel inputs subject to average power constraints P_1 and P_2, respectively, Y_i and Z_i are the channel outputs of the legitimate receiver and the wiretapper, respectively, and $\eta_{1,i} \sim \mathcal{N}(0, \sigma_1^2)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are i.i.d. channel noises across the time index i. The channel encoders and decoder are defined in the same fashion as those in Section III. The wiretapper's equivocation rate of the messages W_1 and W_2 is defined as

$$\Delta = \frac{1}{N} H(W_1, W_2 | Z^N). \quad (4.2)$$

A rate pair (R_1, R_2) is said to be achievable with perfect weak secrecy if for any ϵ and sufficiently large N, there exist channel encoders and decoder such that

$$\frac{\log |\mathcal{W}_1|}{N} = R_1,\ \frac{\log |\mathcal{W}_2|}{N} = R_2,$$
$$\Delta \geq R_1 + R_2 - \epsilon,\ P_e \leq \epsilon. \quad (4.3)$$

The *secrecy* capacity region $\mathcal{C}_{s,gmac-dms}^{f}$ of the GMAC-WT-DMS with feedback is composed of all achievable secrecy rate pairs (R_1, R_2) defined in (4.3). The following Theorem 2 establishes that the secrecy constraint does not reduce the capacity of GMAC-DMS with feedback.

Theorem 2: $\mathcal{C}_{s,gmac-dms}^{f} = \mathcal{C}_{gmac-dms}^{f}$, where $\mathcal{C}_{s,gmac-dms}^{f}$ is the secrecy capacity region of the GMAC-WT-DMS with feedback, and $\mathcal{C}_{gmac-dms}^{f}$ is given in Theorem 1.

Proof: Since $\mathcal{C}_{s,gmac-dms}^{f} \subseteq \mathcal{C}_{gmac-dms}^{f}$, we only need to show that any achievable rate pair (R_1, R_2) in $\mathcal{C}_{gmac-dms}^{f}$ satisfies the secrecy constraint in (4.3). In the preceding section, we introduce a two-step SK type scheme for the GMAC-DMS with feedback, and show that this scheme achieves $\mathcal{C}_{gmac-dms}^{f}$. In this new scheme, the transmitted codewords $X_{1,i}$, U_i and V_i at time i ($1 \leq i \leq N$) can be expressed as those in [10, eq. (5.38), p.33]. From these expressions, we can conclude that for $3 \leq i \leq N$, θ_1 and θ_2 are not contained in the transmitted $X_{1,i}$, U_i and V_i. Hence following similar steps in [10, eq. (3.18), p.17] and choosing sufficiently large N, we can prove that $\frac{1}{N} H(W_1, W_2 | Z^N) \geq R_1 + R_2 - \epsilon$, which completes the proof. ■

V. Conclusion and Future Work

In this paper, a capacity-achieving SK type feedback scheme is proposed for the GMAC-DMS with feedback, and it is also shown to achieve the secrecy capacity region of the GMAC-WT-DMS with feedback. One possible future work of this paper is that whether one can identify dualities of some kind between the GMAC and the Gaussian broadcast models when feedback and secrecy constraint are considered.

References

[1] J. P. M. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback. part I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, pp. 172-182, 1966.

[2] D. Gunduz, D. R. Brown and H. V. Poor, "Secret communication with feedback," *International Symposium on Information Theory and Its Applications, (ISITA)*, 2008.

[3] J. Liu and N. Elia, "Writing on dirty paper with feedback," *Communications in Information and Systems*, vol. 5, no. 4, pp. 401-422, 2005.

[4] B. Dai, C. Li, Y. Liang, Z. Ma and S. Shamai, "Impact of action-dependent state and channel feedback on Gaussian wiretap channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3435-3455, 2020.

[5] C. Li, Y. Liang, H. V. Poor and S. Shamai, "Secrecy capacity of colored Gaussian noise channels with feedback," *IEEE Trans. Inf. Theory*, vol. 65, no. 9, pp. 5771-5782, 2019.

[6] B. Dai, C. Li, Y. Liang, Z. Ma and S. Shamai, "On the capacity of Gaussian multiple-access wiretap channels with feedback," *2020 International Symposium on Information Theory and Its Applications, (ISITA 2020)*, accepted, 2020.

[7] D. Slepian, J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell Syst. Tech. J.*, vol. 51, no. 7, pp. 1037-1076, 1973.

[8] O. Sabag, H. H. Permuter and S. Shamai, "Capacity-achieving coding scheme for the MAC with degraded message sets and feedback," *Proceedings of 2019 International Symposium on Information Theory (ISIT 2019)*, pp. 2259-2263, 2019.

[9] L. H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 292-298, 1981.

[10] B. Dai, C. Li, Y. Liang, Z. Ma and S. Shamai, "Feedback capacities of Gaussian multiple-access wiretap channels," https://arxiv.org/abs/2007.14555, 2020.