On the Capacity of Gaussian Multiple-Access Wiretap Channels with Feedback

Bin Dai*¶, Chong Li†, Yingbin Liang‡, Zheng Ma*, Shlomo Shamai (Shitz)§
* School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 610031, 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.
¶ The State Key Laboratory of Integrated Services Networks, Xidian University, Xi′an, Shaanxi 710071, China.
daibin@home.swjtu.edu.cn, chongl@ntlabs.io, liang.889@osu.edu, zma@home.swjtu.edu.cn, sshlomo@ee.technion.ac.il.

***Abstract*—Two-user Gaussian multiple-access wiretap channel models with feedback are investigated. First, we show that the secrecy capacity regions of both the Gaussian multiple-access wiretap channel (GMAC-WT) with feedback and the GMAC-WT with noncausal channel state information at the transmitters (GMAC-WT-NCSIT) and feedback equal the capacity region of the Gaussian multiple-access channel (GMAC) with feedback and without the secrecy constraint and the state corruption. Next, we derive inner and outer bounds on the secrecy capacity region of the GMAC-WT with degraded message set and feedback. Our numerical results show that the perfect secrecy of the private message can be achieved without loss of any reliable transmission rate.**

The role of channel feedback in physical layer security was initially investigated in [1], where the secrecy capacity of the discrete memoryless wiretap channel (WTC) [2] was shown to be enhanced by a secret key shared between the legitimate parties, and such a key is generated from channel feedback. [1] showed that this secret key based feedback coding scheme is optimal for some degraded discrete memoryless wiretap channels, but it is not optimal for the general WTC. Very recently [3] combined the secret key based feedback scheme [1] with the Wyner-Ziv coding [4], and showed that this hybrid feedback scheme achieves a higher secrecy rate than [1] does. Recently, the Gaussian WTC with feedback also attracts a lot attention. To be specific, [5] showed that even for the degraded Gaussian WTC, the secret key based feedback scheme [1] is not optimal. The optimal feedback scheme for the Gaussian WTC was found in [6], where the classical Schalkwijk-Kailath (SK) feedback scheme [7] for the Gaussian channel was shown to achieve the secrecy capacity of the Gaussian WTC with feedback. Later, [8]- [9] showed that some modified SK schemes also achieve the secrecy capacities of variations of the Gaussian WTC with feedback.

Although the impact of feedback has been well studied in the basic wiretap channels as reviewed above, such a topic is mostly open for multi-user wiretap channels. In this paper, we focus on the Gaussian multiple-access wiretap channel models, and study how the feedback affects the secrecy capacity region. We summarize our contributions as follows.

We first study the Gaussian multiple-access wiretap channel (GMAC-WT) with feedback. [14] studied such a channel without a wiretapper (GMAC with feedback) and showed that a generalized SK scheme achieves the capacity region. By using this generalized SK scheme, we prove that the *secrecy* capacity region equals the capacity region of the same model without secrecy constraint. Such a result is in parallel to that in [6], which showed that the *secrecy* capacity of the single user Gaussian wiretap channel with feedback equals the capacity of the same model without secrecy constraint.

We then study the GMAC-WT with noncausal channel state information at the transmitters (GMAC-WT-NCSIT) and feedback. In [16], a variation of the generalized SK scheme in [14] was shown to achieve the capacity region of the GMAC-NCSIT with feedback. By using the feedback scheme in [16], we prove that the *secrecy* capacity region of the GMAC-WT-NCSIT with feedback equals the capacity region of the same model without secrecy constraint. Numerical results show that the feedback enhances the *secrecy* capacity regions of the GMAC-WT [10]- [11] and the GMAC-WT-NCSIT [18].

We further study the GMAC-WT with degraded message set and propose a new feedback scheme, which combines the generalized SK scheme in [14] and the random binning scheme for the wiretap channel [2]. We show that though this new scheme cannot achieve the capacity region of the same model without secrecy constraint, the perfect secrecy of the private message can be guaranteed without loss of any rate.

I. Preliminaries

A. GMAC with feedback

For the GMAC with noiseless feedback (see Figure 1), the i-th ($i \in \{1, 2, ..., N\}$) channel inputs and output are given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_i, \tag{1.1}$$

where $X_{1,i}$ and $X_{2,i}$ are the channel inputs subject to the average power constraints P_1 and P_2, respectively, Y_i is the channel output, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$ is the channel noise and is

The work of B. Dai was supported by the National Natural Science Foundation of China under Grants 61671391, the Open Research Fund of the State Key Laboratory of Integrated Services Networks, Xidian University, under Grant ISN21-12, and the 111 Project No.111-2-14. 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.

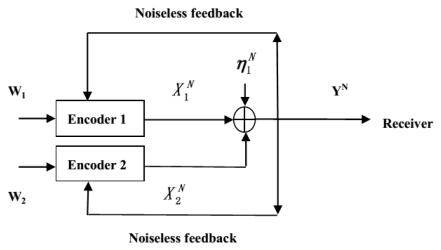

Fig. 1. The GMAC with feedback.

i.i.d. across the time index i. For $j = 1, 2$, the transmitted message W_j represents the message sent by transmitter j, and is uniformly distributed over its alphabet $\{1, 2, ..., 2^{NR_j}\}$ (here R_j is the transmission rate of W_j). At each time i, $X_{j,i}$ is a function of the message W_j and the feedback $Y^{i-1} = (Y_1, ..., Y_{i-1})$ for $j = 1, 2$.

The capacity region $\mathcal{C}^{gmac-f}$ of the GMAC with noiseless feedback was determined in [14] and it is given by

$$\begin{aligned}
&\mathcal{C}^{gmac-f} \\
&= \bigcup_{0\le\rho\le 1} \left\{ (R_1, R_2) : R_1 \le \frac{1}{2}\log\left(1 + \frac{P_1(1-\rho^2)}{\sigma^2}\right), \right. \\
&R_2 \le \frac{1}{2}\log\left(1 + \frac{P_2(1-\rho^2)}{\sigma^2}\right), \\
&\left. R_1 + R_2 \le \frac{1}{2}\log\left(1 + \frac{P_1 + P_2 + 2\sqrt{P_1P_2}\rho}{\sigma^2}\right) \right\}. \quad (1.2)
\end{aligned}$$

The capacity achieving scheme is described below.

Since W_j $(j = 1, 2)$ takes the values in $\mathcal{W}_j = \{1, 2, ..., 2^{NR_j}\}$, we 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 (here note that for sufficiently large N, the variance of θ_j approximately equals $\frac{1}{12}$). At time 1, transmitter 2 sends no signal and transmitter 1 sends

$$X_{1,1} = \sqrt{12P_1}\theta_1. \quad (1.3)$$

The receiver obtains $Y_1 = X_{1,1} + \eta_1$, and gets an estimation of θ_1 by computing

$$\hat{\theta}_{1,1} = \frac{Y_1}{\sqrt{12P_1}} = \theta_1 + \frac{\eta_1}{\sqrt{12P_1}} = \theta_1 + \epsilon_{1,1}, \quad (1.4)$$

where $\epsilon_{1,1} = \hat{\theta}_{1,1} - \theta_1 = \frac{\eta_1}{\sqrt{12P_1}}$. Let $\alpha_{1,1} \triangleq Var(\epsilon_{1,1}) = \frac{\sigma^2}{12P_1}$.

At time 2, transmitter 1 sends no signal and transmitter 2 sends

$$X_{2,2} = \sqrt{12P_2}\theta_2. \quad (1.5)$$

Similarly, the receiver gets an estimation of θ_2 by computing

$$\hat{\theta}_{2,2} = \frac{Y_2}{\sqrt{12P_2}} = \theta_2 + \frac{\eta_2}{\sqrt{12P_2}} = \theta_2 + \epsilon_{2,2}, \quad (1.6)$$

where $\epsilon_{2,2} = \hat{\theta}_{2,2} - \theta_2 = \frac{\eta_2}{\sqrt{12P_2}}$. Let $\alpha_{2,2} \triangleq Var(\epsilon_{2,2}) = \frac{\sigma^2}{12P_2}$. The receiver sets $\hat{\theta}_{1,2} = \hat{\theta}_{1,1}$, so that $\epsilon_{1,2} = \epsilon_{1,1}$ and $\alpha_{1,2} = \alpha_{1,1}$.

At time $3 \le k \le N$, the receiver obtains $Y_k = X_{1,k} + X_{2,k} + \eta_k$, and gets an estimation of θ_j $(j = 1, 2)$ by computing

$$\hat{\theta}_{j,k} = \hat{\theta}_{j,k-1} - \frac{E[Y_k\epsilon_{j,k-1}]}{E[Y_k^2]}Y_k. \quad (1.7)$$

Define $\epsilon_{j,k}$ as $\hat{\theta}_{j,k} - \theta_j$, then (1.7) yields that

$$\epsilon_{j,k} = \epsilon_{j,k-1} - \frac{E[Y_k\epsilon_{j,k-1}]}{E[Y_k^2]}Y_k. \quad (1.8)$$

Meanwhile, for time $3 \le k \le N$, transmitter 1 sends

$$X_{1,k} = \sqrt{\frac{P_1}{\alpha_{1,k-1}}}\epsilon_{1,k-1}, \quad (1.9)$$

and transmitter 2 sends

$$X_{2,k} = \sqrt{\frac{P_2}{\alpha_{2,k-1}}}\epsilon_{2,k-1} \cdot sign(\rho_{k-1}), \quad (1.10)$$

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

$$\rho_{k-1} \triangleq \frac{E[\epsilon_{1,k-1}\epsilon_{2,k-1}]}{\sqrt{\alpha_{1,k-1}\alpha_{2,k-1}}}, \quad (1.11)$$

$$sign(\rho_{k-1}) = \begin{cases} 1, & \rho_{k-1} \ge 0, \\ -1, & \rho_{k-1} < 0. \end{cases} \quad (1.12)$$

Here note that [14] showed that for $3 \le k \le N$, we have

$$\begin{aligned}
&\rho_1 = 0,\ \rho_2 = 0, \\
&\rho_k = \frac{\rho_{k-1}\sigma^2 - sign(\rho_{k-1})\sqrt{P_1P_2}(1-\rho_{k-1}^2)}{\sqrt{(P_1(1-\rho_{k-1}^2)+\sigma^2)(P_2(1-\rho_{k-1}^2)+\sigma^2)}}, \\
&\alpha_{1,2} = \alpha_{1,1} = \frac{\sigma^2}{12P_1},\ \alpha_{2,2} = \frac{\sigma^2}{12P_2}, \\
&\alpha_{1,k} = \alpha_{1,k-1}\frac{P_2(1-\rho_{k-1}^2)+\sigma^2}{P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{k-1}| + \sigma^2}, \\
&\alpha_{2,k} = \alpha_{2,k-1}\frac{P_1(1-\rho_{k-1}^2)+\sigma^2}{P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{k-1}| + \sigma^2}.
\end{aligned} \quad (1.13)$$

From (1.13), we can conclude that for $1 \le k \le N$, ρ_k and $\alpha_{j,k}$ $(j = 1, 2)$ are independent of the transmitted messages. In [14], it has been shown that the decoding error of the above coding scheme is arbitrarily small if $(R_1, R_2) \in \mathcal{C}^{gmac-f}$.

B. GMAC-NCSIT with feedback

For the GMAC-NCSIT with noiseless feedback (see Figure 2), the i-th channel inputs and output are given by

$$Y_i = X_{1,i} + X_{2,i} + S_i + \eta_i, \quad (1.14)$$

where $X_{1,i}$, $X_{2,i}$, η_i and Y_i are defined to be the same as those in Subsection I-A, and $S_i \sim \mathcal{N}(0, Q)$ is the independent Gaussian state interference and is i.i.d. across the time index i. At time i, $X_{j,i}$ $(j = 1, 2)$ is a function of the message

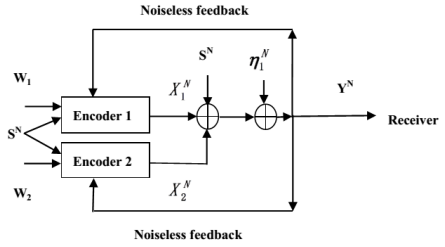

Fig. 2. The GMAC-NCSIT with feedback.

W_j, the feedback Y^{i-1} and the state S^N. The capacity region $\mathcal{C}^{gmac-s-f}$ of the GMAC-NCSIT with noiseless feedback was established in [16], which equals $\mathcal{C}^{gmac-f}$ (see (1.2)). This indicates that the state interference can be perfectly cancelled. The capacity-achieving scheme of $\mathcal{C}^{gmac-s-f}$ is also similar to that of $\mathcal{C}^{gmac-f}$ in Subsection I-B, and the details can be referred to [16].

II. Secrecy Capacity Regions of GMAC-WT with Feedback and GMAC-WT-NCSIT with Feedback

A. GMAC-WT with feedback

For the GMAC-WT with feedback, the i-th ($i \in \{1, 2, ..., N\}$) channel inputs and outputs are given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_i,\ Z_i = Y_i + \eta_{2,i}, \qquad (2.1)$$

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 eavesdropper, respectively, and $\eta_i \sim \mathcal{N}(0, \sigma^2)$, $\eta_{2,i} \sim \mathcal{N}(0, \sigma_2^2)$ are the channel noises and are i.i.d. across the time index i. The channel input $X_{j,i}$ ($j = 1, 2$) is a (stochastic) function of the message W_j and the feedback Y^{i-1}. An achievable secrecy rate pair (R_1, R_2) is an achievable rate pair that satisfies an additional weak secrecy constraint, i.e.,

$$\frac{H(W_1, W_2|Z^N)}{N} \geq R_1 + R_2 - \epsilon. \qquad (2.2)$$

The *secrecy* capacity region $\mathcal{C}_s^{gmac-f}$ of the GMAC-WT with feedback is composed of all such achievable secrecy rate pairs. Our first result as given in the following theorem establishes that the secrecy constraint does not reduce the capacity of GMAC with feedback.

Theorem 1: $\mathcal{C}_s^{gmac-f} = \mathcal{C}^{gmac-f}$, where $\mathcal{C}^{gmac-f}$ is given in (1.2).

Proof: First, note that $\mathcal{C}_s^{gmac-f}$ cannot exceed the capacity region of the same model without secrecy constraint, i.e., $\mathcal{C}_s^{gmac-f} \subseteq \mathcal{C}^{gmac-f}$. Then, it remains to show that any rate pair $(R_1, R_2) \in \mathcal{C}^{gmac-f}$ is achievable with the secrecy constraint (2.2). In fact, we show below that the feedback coding scheme achieving $\mathcal{C}^{gmac-f}$ satisfies the secrecy constraint (2.2).

From Subsection I-A, we know that at time i ($1 \leq i \leq N$), the transmitted codewords $X_{j,i}$ ($j = 1, 2$) can be expressed as

$$\begin{aligned}
&X_{1,1} = \sqrt{12P_1}\theta_1,\ X_{2,1} = X_{1,2} = \emptyset,\ X_{2,2} = \sqrt{12P_2}\theta_2,\\
&X_{1,3} = \sqrt{\frac{P_1}{\sigma^2}}\eta_1,\ X_{2,3} = \sqrt{\frac{P_2}{\sigma^2}}\eta_2, ...\\
&X_{1,N} = \sqrt{\frac{P_1(P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{N-2}| + \sigma^2)}{\alpha_{1,N-2}(P_2(1-\rho_{N-2}^2) + \sigma^2)}} \cdot\\
&(\epsilon_{1,N-2} - \frac{\sqrt{\alpha_{1,N-2}}(\sqrt{P_1} + \sqrt{P_2}|\rho_{N-2}|)}{P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{N-2}| + \sigma^2}(X_{1,N-1}\\
&+X_{2,N-1} + \eta_{N-1})),\\
&X_{2,N} = \sqrt{\frac{P_2(P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{N-2}| + \sigma^2)}{\alpha_{2,N-2}(P_1(1-\rho_{N-2}^2) + \sigma^2)}} \cdot\\
&(\epsilon_{2,N-2} - \frac{\sqrt{\alpha_{2,N-2}}(\sqrt{P_2} + \sqrt{P_1}|\rho_{N-2}|)sign(\rho_{N-2})}{P_1 + P_2 + 2\sqrt{P_1P_2}|\rho_{N-2}| + \sigma^2} \cdot\\
&(X_{1,N-1} + X_{2,N-1} + \eta_{N-1})). \qquad (2.3)
\end{aligned}$$

From (2.3) and the fact that ρ_k and $\alpha_{j,k}$ ($j = 1, 2$ and $1 \leq k \leq N$) are independent of the transmitted messages (see (1.13)), we can conclude that for $3 \leq k \leq N$, $X_{j,k}$ is a function of η_1,...,η_{k-1}, and it is independent of the transmitted messages. For convenience, define

$$X_{j,k} = f_{j,k}(\eta_1, ..., \eta_{k-1}), \qquad (2.4)$$

where $j = 1, 2$ and $3 \leq k \leq N$. By using (2.3) and (2.4), $\frac{1}{N}H(W_1, W_2|Z^N)$ is bounded by

$$\begin{aligned}
&\frac{1}{N}H(W_1, W_2|Z^N) = \frac{1}{N}H(\theta_1, \theta_2|Z^N)\\
&\geq \frac{1}{N}H(\theta_1, \theta_2|Z^N, \eta_1, ..., \eta_N, \eta_{2,3}, ..., \eta_{2,N})\\
&\overset{(a)}{=} \frac{1}{N}H(\theta_1, \theta_2|\sqrt{12P_1}\theta_1 + \eta_1 + \eta_{2,1}, \sqrt{12P_2}\theta_2\\
&+\eta_2 + \eta_{2,2}, \sqrt{\frac{P_1}{\sigma^2}}\eta_1 + \sqrt{\frac{P_2}{\sigma^2}}\eta_2 + \eta_3 + \eta_{2,3}, ...,\\
&f_{1,N}(\eta_1, ..., \eta_{N-1}) + f_{2,N}(\eta_1, ..., \eta_{N-1})\\
&+\eta_N + \eta_{2,N}, \eta_1, ..., \eta_N, \eta_{2,3}, ..., \eta_{2,N})\\
&= \frac{1}{N}H(\theta_1, \theta_2|\sqrt{12P_1}\theta_1 + \eta_{2,1}, \sqrt{12P_2}\theta_2 + \eta_{2,2})\\
&= \frac{1}{N}(H(\theta_1, \theta_2) - h(\sqrt{12P_1}\theta_1 + \eta_{2,1}, \sqrt{12P_2}\theta_2 + \eta_{2,2})\\
&+h(\eta_{2,1}, \eta_{2,2}|\theta_1, \theta_2))\\
&\overset{(b)}{=} \frac{1}{N}(H(\theta_1, \theta_2) - h(\sqrt{12P_1}\theta_1 + \eta_{2,1})\\
&-h(\sqrt{12P_2}\theta_2 + \eta_{2,2}) + h(\eta_{2,1}) + h(\eta_{2,2}))\\
&\overset{(c)}{\geq} R_1 + R_2 - (\frac{1}{2N}\log(1 + \frac{P_1}{\sigma_2^2}) + \frac{1}{2N}\log(1 + \frac{P_2}{\sigma_2^2})),
\end{aligned} \qquad (2.5)$$

where (a) follows from (2.1) and (2.3), (b) follows from the fact that θ_1, θ_2, $\eta_{2,1}$ and $\eta_{2,2}$ are independent of each other, and (c) follows because $H(\theta_j) = NR_j$ ($j = 1, 2$), the variance of θ_j equals $\frac{1}{12}$ as N tends to infinity, and θ_j is independent

of $\eta_{2,j}$. Choosing sufficiently large N, the secrecy constraint (2.2) is proved, which completes the proof. ■

B. GMAC-WT-NCSIT with feedback

For the GMAC-WT-NCSIT with feedback, the i-th ($i \in \{1,2,...,N\}$) channel inputs and outputs are given by

$$Y_i = X_{1,i} + X_{2,i} + S_i + \eta_i,\ Z_i = Y_i + \eta_{2,i}, \quad (2.6)$$

where $X_{1,i}$, $X_{2,i}$, Y_i, Z_i, η_i, $\eta_{2,i}$ are defined to be the same as those in Subsection II-A, the state S_i is defined to be the same as that in Subsection I-B. At time i, $X_{j,i}$ ($j = 1,2$) is a (stochastic) function of the message W_j, the state S^N and the feedback Y^{i-1}. The *secrecy* capacity region of the GMAC-WT-NCSIT with feedback is denoted by $\mathcal{C}_s^{gmac-s-f}$. Our following result shows that the state corruption as well as the secrecy constraint do not reduce the capacity region of the GMAC with feedback.

Theorem 2: $\mathcal{C}_s^{gmac-s-f} = \mathcal{C}^{gmac-f}$, where $\mathcal{C}^{gmac-f}$ is given in (1.2).

Proof: First, note that $\mathcal{C}_s^{gmac-s-f}$ cannot exceed the capacity region of the same model without secrecy constraint, i.e., $\mathcal{C}_s^{gmac-s-f} \subseteq \mathcal{C}^{gmac-s-f}$. Next, as explained in Subsection I-B, [16] has shown that $\mathcal{C}^{gmac-s-f} = \mathcal{C}^{gmac-f}$. Then, it remains to show that any rate pair $(R_1, R_2) \in \mathcal{C}^{gmac-f}$ is achievable with the secrecy constraint (2.2). In fact, we argue below that the feedback coding scheme in Subsection I-B that achieves $\mathcal{C}^{gmac-s-f}$ also satisfies the secrecy constraint (2.2). At time $3 \le i \le N$, the transmitted codewords $X_{j,i}$ ($j = 1,2$) can be expressed as the functions of η_1,...,η_{i-1}, which are similar to the expressions in (2.3). Then following the steps similar to these in (2.5), we can prove the secrecy constraint (2.2), which completes the proof. ■

The following Figure 3 compares various capacity results with $P_1 = 1$, $P_2 = 1.2$, $Q = 1$, $\sigma^2 = 0.1$, $\sigma_2^2 = 1.5$. It can be seen that feedback enhances the *secrecy* capacity regions of GMAC-WT and GMAC-WT-NCSIT.

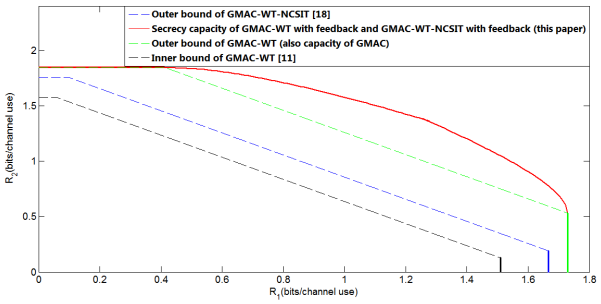

Fig. 3. Capacity results on GMAC-WT with or without feedback and noncausal CSI at the transmitters.

III. Feedback Scheme for GMAC-WT with Degraded Message Set

Consider the GMAC-WT with degraded message set and feedback. The i-th ($i \in \{1,2,...,N\}$) channel inputs and outputs are given by

$$Y_i = X_{1,i} + X_{2,i} + \eta_i,\ Z_i = Y_i + \eta_{2,i}, \quad (3.1)$$

where $X_{1,i}$, $X_{2,i}$, η_i, $\eta_{2,i}$, Y_i and Z_i are defined to be the same as those in Subsection II-A. A common message W_1 taking values in $\{1,2,...,2^{NR_1}\}$ is known by both transmitters, and a private message W_2 taking values in $\{1,2,...,2^{NR_2}\}$ is only known by the second transmitter. At time i, the channel input $X_{1,i}$ is a (stochastic) function of W_1 and the feedback Y^{i-1}, and $X_{2,i}$ is a (stochastic) function of W_1, W_2 and the feedback Y^{i-1}. The *secrecy* capacity region of this model is denoted by $\mathcal{C}_s^{g-f}$, and the following Theorems 3-4 show the inner and outer bounds on $\mathcal{C}_s^{g-f}$.

Theorem 3: An inner bound $\mathcal{R}_s^{g-f}$ on $\mathcal{C}_s^{g-f}$ is given by

$$\begin{aligned}\mathcal{R}_s^{g-f} = \bigcup_{\substack{0\le\rho\le 1\\ 0\le\alpha\le 1}} \{(R_1,R_2): R_1 \le\ & \\ \frac{1}{2}\log(1+\frac{\alpha P_2 + P_1(1-\rho^2)}{\sigma^2}) - \frac{1}{2}\log(1+\frac{\alpha P_2}{\sigma^2+\sigma_2^2}),& \\ R_2 \le \frac{1}{2}\log(1+\frac{(1-\alpha)P_2(1-\rho^2)}{\sigma^2+\alpha P_2}),& \\ R_1+R_2 \le \frac{1}{2}\log(1+\frac{P_1+P_2+2\sqrt{P_1P_2(1-\alpha)}\rho}{\sigma^2}) & \\ -\frac{1}{2}\log(1+\frac{\alpha P_2}{\sigma^2+\sigma_2^2})\}.&\end{aligned}$$

Proof: Split the common message W_1 into two sub-messages W_{11} and W_{12}, where W_{1j} ($j = 1,2$) takes values in $\{1,2,...,2^{NR_{1j}}\}$ and $R_{11} + R_{12} = R_1$. The sub-message W_{11} is transmitted by Transmitter 1, and W_{12} together with W_2 are transmitted by Transmitter 2. Transmitter 2 uses power αP_2 to transmit W_{12}, and power $(1-\alpha)P_2$ to transmit W_2. Classical random binning coding scheme [2] for the wiretap channel is applied to the sub-message W_{12}, and the coding scheme for W_{11} and W_2 is the same as that for the messages W_1 and W_2 in GMAC with feedback (see Subsection I-A), where the power αP_2 for W_{12} is treated as channel noise. Now applying the feedback scheme in Subsection I-A, we can conclude that

$$R_{11} \le \frac{1}{2}\log(1+\frac{P_1(1-\rho^2)}{\sigma^2+\alpha P_2}), \quad (3.2)$$

$$R_2 \le \frac{1}{2}\log(1+\frac{(1-\alpha)P_2(1-\rho^2)}{\sigma^2+\alpha P_2}), \quad (3.3)$$

$$R_{11}+R_2 \le \frac{1}{2}\log(1+ \frac{P_1+(1-\alpha)P_2+2\sqrt{P_1P_2(1-\alpha)}\rho}{\sigma^2+\alpha P_2}), \quad (3.4)$$

is achievable. Since W_{11} and W_2 can be decoded with high probability if (3.2)-(3.4) are satisfied, the receiver subtracts the corresponding terms from received signal, yielding only the codeword of W_{12} added to the channel noise. From [2], we can conclude that if

$$R_{12} \le \frac{1}{2}\log(1+\frac{\alpha P_2}{\sigma^2}) - \frac{1}{2}\log(1+\frac{\alpha P_2}{\sigma^2+\sigma_2^2}) \quad (3.5)$$

is satisfied, W_{12} is achievable with perfect secrecy. Combining $R_{11}+R_{12}=R_1$, (3.2), (3.3), (3.4) and (3.5), the region $\mathcal{R}_s^{g-f}$ is achieved, and the proof is completed. ■

Theorem 4: An outer bound $\mathcal{C}_s^{g-f-out}$ on $\mathcal{C}_s^{g-f}$ is given by

$$\begin{aligned}&\mathcal{C}_s^{g-f-out}\\&=\bigcup_{0\le\rho\le 1}\{(R_1,R_2): R_2\le\frac{1}{2}\log(1+\frac{P_2(1-\rho^2)}{\sigma^2}),\\&R_1+R_2\le\frac{1}{2}\log(1+\frac{P_1+P_2+2\sqrt{P_1P_2}\rho}{\sigma^2})\},\end{aligned}\quad(3.6)$$

where $\mathcal{C}_s^{g-f-out}$ is also the capacity region of the GMAC with degraded message set and feedback.

Proof: First, note that the *secrecy* capacity region $\mathcal{C}_s^{g-f}$ is upper bounded by the capacity region $\mathcal{C}^{g-f}$ of the same model without secrecy constraint, namely, the GMAC with degraded message set and feedback. Next, from [17] and [14], we can check that feedback does not increase the capacity region of the GMAC with degraded message set, which equals the region given in (3.6). Thus the proof is completed. ■

The following Figure 4 plots the bounds on $\mathcal{C}_s^{g-f}$ for $P_1=1$, $P_2=1.5$, $\sigma^2=0.9$ and $\sigma_2^2=1.5$. From Figure 4, one can see that the maximum rate R_2 of the inner bound equals the maximum R_2 of the outer bound, which indicates that the perfect secrecy of the private message W_2 can be guaranteed without the loss of any rate.

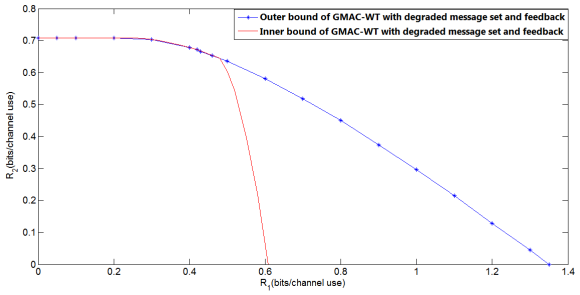

Fig. 4. Capacity bounds on the GMAC-WT with degraded message set and feedback.

IV. Conclusion and Future Work

This paper shows that the Ozarow's SK type feedback scheme and its variation for GMAC and GMAC-NCSIT with feedback (not designed with consideration of secrecy) already achieve secrecy by themself. Such an inherent secrecy nature of the SK-type GMAC schemes is a new finding to the community and thus is the major contribution of this paper. Another contribution of this paper is the derivation of inner and outer bounds on the *secrecy* capacity region of the GMAC-WT with degraded message set and feedback, and these bounds indicate that the perfect secrecy of the private message can be achieved without loss of any reliable transmission rate.

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. Another one is to investigate whether the generalized feedback approach in [19] can be applied to the GMAC-WT with feedback. The last one is about the finite blocklength regime, which deserves attention even in the single user wiretap case where a modified SK scheme motivated by [20] might be useful.

References

[1] R. Ahlswede, N. Cai, "Transmission, identification and common randomness capacities for wire-tap channels with secure feedback from the decoder," book chapter in *General Theory of Information Transfer and Combinatorics*, LNCS 4123, pp. 258-275, Berlin: Springer-Verlag, 2006.
[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.
[3] B. Dai, Y. Luo, "An improved feedback coding scheme for the wiretap channel," *IEEE Trans. Inf. Forensics and Security*, vol. 14, No. 1, pp. 262-271, 2019.
[4] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 1, pp. 1-10, 1976.
[5] C. Wei, L. Yu, B. Dai, "Some new results on the Gaussian wiretap feedback channel," *Entropy*, vol. 21, no. 9, pp. 817-828, 2019.
[6] D. Gunduz, D. R. Brown and H. V. Poor, "Secret communication with feedback," *International Symposium on Information Theory and Its Applications, (ISITA)*, 2008.
[7] 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.
[8] 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.
[9] B. Dai, C. Li, Y. Liang, Z. Ma, S. Shamai (Shitz), "The dirty paper wiretap feedback channel with or without action on the state," *IEEE International Symposium on Information Theory (ISIT)*, pp. 657-661, 2019.
[10] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735-2751, 2008.
[11] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747-5755, 2008.
[12] T. Cover, S. K. Leung-Yan-Cheong, "A rate region for multiple access channels with feedback," *IEEE Trans. Inf. Theory*, vol. 27, no. 3, pp. 292-298, 1981.
[13] R. Venkataramanan, S. S. Pradhan, "A new achievable rate region for the multiple-access channel with noiseless feedback," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8038-8054, 2011.
[14] 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.
[15] L. Dikstein, H. H. Permuter, S. Shamai, "MAC with action-dependent state information at one encoder," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 173-188, 2015.
[16] A. Rosenzweig, "The capacity of Gaussian multi-user channels with state and feedback," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 4349-4355, 2007.
[17] 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.
[18] A. Sonee and G. A. Hodtani, "On the secrecy rate region of multiple-access wiretap channel with noncausal side information," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 6, pp. 1151-1166, 2015.
[19] G. Bassi, P. Piantanida and S. Shamai (Shitz), "The wiretap channel with generalized feedback: secure communication and key generation," *IEEE Trans. Inf. Theory*, vol. 65, No. 4, pp. 2213-2233, 2019.
[20] R. G. Gallager, B. Nakiboglu, "Variations on a theme by Schalkwijk and Kailath," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 6-17, 2010.