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.

daubin@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 of 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-WT-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 ($i \in \{1, 2, \ldots, N\}$) channel inputs and output are given by

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

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
Similarly, the receiver gets an estimation of $Y_i$ for $i = 1, 2$. Let $\alpha_{i,j} = Var(\epsilon_{i,j})$.

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

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

(1.7)

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

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

(1.8)

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

$$X_{1,k} = \sqrt{\frac{P_1}{\alpha_{1,k-1}}} \epsilon_{1,k-1},$$  

(1.9)

and transmitter 2 sends

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

(1.10)

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

$$\rho_{k-1} = \frac{E[\epsilon_{1,k-1} \epsilon_{2,k-1}]}{\sqrt{\alpha_{1,k-1} \alpha_{2,k-1}}}$$  

(1.11)

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

(1.12)

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

$$\rho_1 = 0, \quad \rho_2 = 0,$$

$$\rho_k = \frac{\rho_{k-1}^2 - sign(\rho_{k-1}) \sqrt{P_1 P_2} (1 - \rho_{k-1}^2)}{\sqrt{(P_1 (1 - \rho_{k-1}^2) + \sigma^2) (P_1 (1 - \rho_{k-1}^2) + \sigma^2)}},$$

$$\alpha_{1,2} = \alpha_{1,1} = \frac{\sigma^2}{2P_1}, \quad \alpha_{2,2} = \frac{\sigma^2}{2P_2},$$

$$\alpha_{1,k} = \frac{\sigma^2}{P_1 + P_2 + 2\sqrt{P_1 P_2} |\rho_{k-1}| + \sigma^2},$$

$$\alpha_{2,k} = \frac{\sigma^2}{P_1 + P_2 + 2\sqrt{P_1 P_2} |\rho_{k-1}| + \sigma^2}.$$  

(1.13)

From (1.13), we can conclude that for $1 \leq k \leq N$, $\rho_k$ 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 $(R_1, R_2) \in C^{gmac-f}$.

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

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

(1.14)

where $X_{1,i}$, $X_{2,i}$, $\eta_i$ and $Y_i$ are defined to be the same as those in Subsection I-A, and $S_i \sim N(0, Q)$ 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

\[ X_{j,i} = \frac{Y_i}{\sqrt{12P_j^2}} + \frac{\eta_i}{\sqrt{12P_j^2}} \]  

\[ \text{where } \epsilon_{2,2} = \hat{\theta}_{2,2} - \theta_2 = \frac{\eta_i}{\sqrt{12P_2^2}}. \]  

Let $\alpha_{2,2} = Var(\epsilon_{2,2}) = \frac{\sigma^2}{12P_2^2}$. 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 $3 \leq k \leq N$, the receiver obtains $Y_k = X_{1,k} + X_{2,k} + \eta_k$ and gets an estimation of $\theta_j$ ($j = 1, 2$) by computing

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

\[ (1.7) \]

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

\[ \epsilon_{j,k} = \epsilon_{j,k-1} - \frac{E[Y_k \epsilon_{j,k-1}]}{E[Y_k^2]} Y_k. \]

\[ (1.8) \]
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

$$X_{1,i} = \sqrt{12P_1\theta_1}, \quad X_{2,i} = \varnothing, \quad X_{2,2} = \sqrt{12P_2\theta_2},$$

$$X_{1,3} = \sqrt{\frac{P_1}{\sigma^2} \eta_1}, \quad X_{2,3} = \sqrt{\frac{P_2}{\sigma^2} \eta_2}, \ldots$$

$$X_{1,N} = \sqrt{\frac{P_1(P_1 + P_2 + 2\sqrt{P_1P_2\rho_{N-2}} + \sigma^2)}{\alpha_{1,N-2}(P_2(1 - \rho_{N-2}^2) + \sigma^2)}} \cdot (\epsilon_{1,N-2} - \frac{\alpha_{1,N-2}(\sqrt{P_1 + \sqrt{P_1\rho_{N-2}}} \sigma)}{\alpha_{2,N-2}(P_1(1 - \rho_{N-2}^2) + \sigma^2)}) \cdot (X_{1,N-1} + X_{2,N-1} + \eta(N-1)),$$

$$X_{2,N} = \sqrt{\frac{P_2(P_1 + P_2 + 2\sqrt{P_1P_2\rho_{N-2}} + \sigma^2)}{\alpha_{2,N-2}(P_1(1 - \rho_{N-2}^2) + \sigma^2)}} \cdot (\epsilon_{2,N-2} - \frac{\alpha_{2,N-2}(\sqrt{P_2 + \sqrt{P_2\rho_{N-2}}} \sigma)}{\alpha_{2,N-2}(P_1(1 - \rho_{N-2}^2) + \sigma^2)}) \cdot (X_{1,N-1} + X_{2,N-1} + \eta(N-1)).$$

(2.3)

From (2.3) and the fact that $\rho_k$ 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 $\eta_1, \ldots, \eta_{k-1}$, and it is independent of the transmitted messages. For convenience, define

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

(2.4)

where $j = 1, 2$ and $3 \leq k \leq N$. By using (2.3) and (2.4),

$$\frac{1}{N}H(W_1, W_2 | Z^n) \text{ is bounded by}$$

$$\frac{1}{N}H(W_1, W_2 | Z^n) = \frac{1}{N}H(\theta_1, \theta_2 | Z^n) \geq \frac{1}{N}H(\theta_1, \theta_2 | Z^n, \eta_1, \ldots, \eta_N, \eta_{N-1} \ldots, \eta_2)$$

(2.5)

The secrecy capacity region $C_s^{\text{mac}-f}$ 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:** $C_s^{\text{mac}-f} = C^{\text{mac}-f}$, where $C^{\text{mac}-f}$ is given in (1.2).

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

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

where $X_{1,i}, X_{2,i}, Y_i, Z_i, \eta_i, \eta_{2,i}$ 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 $C^s_{\text{GMAC-NCSIT}}$. 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:** $C^s_{\text{GMAC-NCSIT}} = C^s_{\text{GMAC}}$, where $C^s_{\text{GMAC}}$ is given in (1.2).

**Proof:** First, note that $C^s_{\text{GMAC-NCSIT}}$ cannot exceed the capacity region of the same model without secrecy constraint, i.e., $C^s_{\text{GMAC-NCSIT}} \subseteq C^s_{\text{GMAC}}$. Next, as explained in Subsection I-B, [16] has shown that $C^s_{\text{GMAC-NCSIT}} = C^s_{\text{GMAC}}$. Then, it remains to show that any rate pair $(R_1, R_2) \in C^s_{\text{GMAC}}$ is achievable with the secrecy constraint (2.2). In fact, we argue below that the feedback coding scheme in Subsection I-B that achieves $C^s_{\text{GMAC-NCSIT}}$ also satisfies the secrecy constraint (2.2).

At time $3 \leq i \leq N$, the transmitted codewords $X_{j,i}$ ($j = 1, 2$) can be expressed as the functions of $\eta_i, ..., \eta_{i-1}$, 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.

![Figure 3. Capacity results on GMAC-WT with or without feedback and noncausal CSI at the transmitters.](image)

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

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

where $X_{1,i}, X_{2,i}, \eta_i, \eta_{2,i}, Y_i$ 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 $C^s_{\text{GMAC-WT}, \text{with feedback}}$, and the following Theorems 3-4 show the inner and outer bounds on $C^s_{\text{GMAC-WT}, \text{with feedback}}$.

**Theorem 3:** An inner bound $R^s_{\text{GMAC-WT}}$ on $C^s_{\text{GMAC-WT}}$ is given by

$$R^s_{\text{GMAC-WT}} = \bigcup_{0 \leq \rho \leq 1} \{(R_1, R_2) : R_1 \leq \frac{1}{2} \log(1 + \frac{\alpha P_2}{\sigma^2 + \alpha P_2}),$$

$$R_2 \leq \frac{1}{2} \log(1 + \frac{(1 - \alpha) P_2}{\sigma^2 + \alpha P_2}),$$

$$R_1 + R_2 \leq \frac{1}{2} \log(1 + \frac{P_1 + 2\sqrt{P_1 P_2 (1 - \alpha) \rho}}{\sigma^2 + \alpha P_2}) + \frac{1}{2} \log(1 + \frac{\alpha P_2}{\sigma^2 + \alpha P_2})\}.$$

**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 $\{1, 2, ..., 2^{NR_1}\}$ 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 $\alpha P_2$ 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 $\alpha P_2$ for $W_{12}$ is treated as channel noise. Now applying the feedback scheme in Subsection I-A, we can conclude that

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

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

$$R_{11} + R_{12} \leq \frac{1}{2} \log(1 + \frac{P_1 + 2\sqrt{P_1 P_2 (1 - \alpha) \rho}}{\sigma^2 + \alpha P_2}),$$

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

$$R_{12} \leq \frac{1}{2} \log(1 + \frac{\alpha P_2}{\sigma^2}) - \frac{1}{2} \log(1 + \frac{\alpha P_2}{\sigma^2 + \alpha P_2}) \quad \text{(3.5)}$$
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 $R^g_{\text{sec}}$ is achieved, and the proof is completed.

**Theorem 4:** An outer bound $C^g_{\text{sec}}$ on $C^g$ is given by

$$C^g_{\text{sec}} = \bigcup_{0 \leq \rho \leq 1} \{(R_1, R_2) : R_2 \leq \frac{1}{2} \log(1 + \frac{P_2(1-\rho^2)}{\sigma^2}), \quad R_1 + R_2 \leq \frac{1}{2} \log(1 + \frac{P_1 + P_2 + 2\sqrt{P_1 P_2 \rho}}{\sigma^2})\},$$

where $C^g_{\text{sec}}$ is also the capacity region of the GMAC with degraded message set and feedback.

**Proof:** First, note that the secrecy capacity region $C^g_{\text{sec}}$ is upper bounded by the capacity region $C^g$ 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 $C^g_{\text{sec}}$ for $P_1 = 1$, $P_2 = 1.5$, $\sigma^2 = 0.9$ and $\sigma^2 = 1.5$. 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.](image)

**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**


