The Degraded Gaussian Many-Access Wiretap Channel

Rémi A. Chou
Department of Electrical Engineering and Computer Science
Wichita State University
Wichita, KS 67260
remi.chou@wichita.edu

Aylin Yener
Department of Electrical Engineering
The Pennsylvania State University
University Park, PA 16802
yener@ee.psu.edu

***Abstract*—The Gaussian multiple-access wiretap channel when the number of transmitters grows unbounded and at most linearly with the blocklength is studied. Its capacity region is characterized when the eavesdropper channel is degraded and when the transmitters' activities are random. Unlike the conventional Gaussian multiple-access wiretap channel, the capacity region is independent of the power of the transmitters and depends only on the sum of the message lengths of the transmitters.**

I. Introduction

Emerging communication applications, including sensors networks and Internet of Things, often involve a large number of devices or users that seek to simultaneously transmit over the same medium. For such settings, multiuser information theory that accounts for a number of users that can grow unbounded with the blocklength is needed. Previous works that have proposed and investigated this setting include [1] for a noiseless binary adder channel, [2], [3] for Gaussian multiple-access channels under synchronous transmission, [4] for degraded broadcast channels, and [5] for Gaussian multiple-access channels under asynchronous transmission.

In this paper, we propose and study a model that brings information-theoretic security to this setting. That is, we are interested in providing security guarantees against eavesdropping when a large number of users can transmit over the same channel. As the initial model, we study the degraded Gaussian multiple-access wiretap channel [6] when the number of synchronous transmitters grows unbounded and at most linearly with the blocklength, n. We also consider random transmitter activities. The main challenges in this setting compared to the multiple-access wiretap channel in the conventional multi-user setting [7] are (i) the uncertainty on the exact number of active transmitters, which requires some sort of transmitter identification in the decoding process at the legitimate receiver and a careful consideration in the security analysis, and (ii) the scaling of the number of transmitters with n, which requires a new notion of capacity and prevents straightforward applications of standard tools such as joint typicality coding or Fano's inequality, as already noticed in [2].

The remainder of the paper is organized as follows. We formally define the problem in Section II. We present our main results in Section III and present their proofs in Sections IV, V. Finally, we provide concluding remarks in Section VI. Some proofs are omitted or sketched due to space constraints.

II. Problem Statement

Notation: For any $a \in \mathbb{N}^*$, define $[\![1,a]\!] \triangleq [1,a] \cap \mathbb{N}$. The indicator function is denoted by $\mathbb{1}\{\omega\}$, which is equal to 1 if the predicate ω is true and 0 otherwise. For $R \in \mathbb{R}_+$, let $\mathbb{B}_0^n(R)$ denote the ball of radius R centered in 0 in $\mathbb{R}^n$ under the Euclidian norm. For a binary sequence w, let $\mathrm{wt}(w)$ denote the Hamming weight of w. Let H_b denote the binary entropy. Finally, let $\bigtimes$ denote the Cartesian product.

Let $n \in \mathbb{N}$. Let $G \in \mathbb{N}$ and define $\mathcal{G} \triangleq [\![1,G]\!]$. Let l_n be the number of transmitters and define $\mathcal{L}_n \triangleq [\![1,l_n]\!]$ the set of all transmitters. Similar to Reference [2], we assume that there exists G groups of transmitters $(\mathcal{G}_g)_{g\in\mathcal{G}}$ that form a partition of $\mathcal{L}_n$ such that transmitters in $\mathcal{G}_g$ have a power constraint equal to P_g, $g \in \mathcal{G}$. We also assume that for $g \in \mathcal{G}$, $|\mathcal{G}_g| = \beta_g l_n$ with $\sum_{g\in\mathcal{G}} \beta_g = 1$. The l_n transmitters wish to communicate secret messages to a legitimate receiver in the presence of an eavesdropper over a degraded memoryless multiple-access wiretap channel [7] modeled as

$$Y^n \triangleq \sum_{g\in\mathcal{G}} \sum_{l\in\mathcal{G}_g} X_{g,l}^n + N_Y^n, \tag{1}$$

$$Z^n \triangleq \sum_{g\in\mathcal{G}} \sum_{l\in\mathcal{G}_g} \sqrt{h} X_{g,l}^n + N_Z^n, \tag{2}$$

where Y^n is the channel output observed by the legitimate receiver, Z^n is the channel output observed by the eavesdropper, $h \in]0,1[$, $X_{g,l}^n$, $g \in \mathcal{G}$, $l \in \mathcal{G}_g$, is the signal emitted by transmitter l in group $\mathcal{G}_g$ satisfying the power constraint $\|X_{l,g}^n\|^2 \triangleq \sum_{j=1}^n (X_{l,g})_j^2 \leqslant nP_g$, and N_Y^n and N_Z^n are sequences of independent and identically distributed Gaussian noises with variances $\sigma_Y^2 = 1$, $\sigma_Z^2 = 1$, respectively. Similar to [2], we model random access to the channel by assuming that each user in group $\mathcal{G}_g$, $g \in \mathcal{G}$, is independently active with probability $\alpha_{g,n}$ with $\lim_{n\to\infty} \alpha_{g,n} = \alpha_g \in [0,1]$. We denote by A_g the sequence of indices corresponding to active users in $\mathcal{G}_g$, and define $A \triangleq (A_g)_{g\in\mathcal{G}}$. Note that the channel model described in (1), (2) generalizes both the degraded Gaussian multiple-access wiretap channel [7] and the Gaussian many-access channel [2]. The model is depicted in Figure 1, we

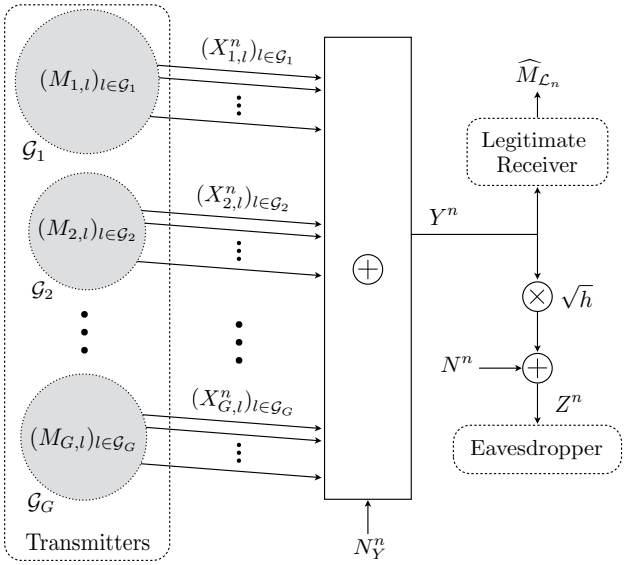

Fig. 1: Degraded Gaussian many-access wiretap channel. N^n is a sequence of n independent zero-mean Gaussian random variables with variance $1-h$.

term it the degraded *Gaussian many-access wiretap channel* (G-MnAC-WT).

Definition 1. *Let $n \in \mathbb{N}$. A $\left((2^{\upsilon_g(n)})_{g\in\mathcal{G}}, n\right)$ code $\mathcal{C}_n$ for the degraded G-MnAC-WT consists of*

- *l_n messages sets $\mathcal{M}_{g,l} \triangleq [\![0, 2^{\upsilon_g(n)}]\!]$, $g \in \mathcal{G}$, $l \in \mathcal{G}_g$;*
- *l_n stochastic encoders, $e_{g,l} : \mathcal{M}_{g,l} \to \mathbb{B}_0^n(\sqrt{nP_g})$, $g \in \mathcal{G}$, $l \in \mathcal{G}_g$;*
- *One decoder, $d : \mathbb{R}^n \to \bigtimes_{g\in\mathcal{G}, l\in\mathcal{G}_g} \mathcal{M}_{g,l}$;*

and operates as follows. If transmitter $l \in \mathcal{G}_g$, $g \in \mathcal{G}$, is active, then it encodes with $e_{g,l}$ a message $M_{g,l} \in \mathcal{M}_{g,l}\backslash\{0\}$, distributed according to $p_{M_{g,l}}(m|l \in A_g) \triangleq 2^{-\upsilon_g(n)}$ for $m \in [\![1, 2^{\upsilon_g(n)}]\!]$. If transmitter $l \in \mathcal{G}_g$, $g \in \mathcal{G}$, is inactive, then one considers that the message $M_{g,l} = 0$ is encoded with a codeword made of n zeros such that $p_{M_{g,l}}(0|l \notin A_g) \triangleq 1$. The result of the encoding is a codeword of length n, which is sent to the legitimate receiver over the channel described by (1), (2)*. Then, the legitimate receiver forms from his n channel output observations an estimate $\widehat{M}_{\mathcal{L}_n} \triangleq (\widehat{M}_{g,l})_{g\in\mathcal{G}, l\in\mathcal{G}_g}$ of the messages $M_{\mathcal{L}_n} \triangleq (M_{g,l})_{g\in\mathcal{G}, l\in\mathcal{G}_g}$. We also define $M_{A_g} \triangleq (M_{g,l})_{l\in A_g}$, $g \in \mathcal{G}$, and $M_A \triangleq \left(M_{A_g}\right)_{g\in\mathcal{G}}$.*

Definition 2. *A message length tuple $(\upsilon_g(n))_{g\in\mathcal{G}}$ is achievable, if there exists a sequence of $\left((2^{\upsilon_g(n)})_{g\in\mathcal{G}}, n\right)$ codes for the G-MAnC-WT such that*

$$\lim_{n\to\infty} \mathbb{P}[\widehat{M}_{\mathcal{L}_n} \neq M_{\mathcal{L}_n}] = 0 \text{ (reliability)},$$

$$\lim_{n\to\infty} \frac{1}{n} H(M_{\mathcal{L}_n}|AZ^n) \geqslant \frac{1}{n} H(M_{\mathcal{L}_n}|A) \text{ (equivocation)}.$$

Remark. *Observe that only confidentiality of the messages of the active users from the eavesdropper is sought. The identities of the active users are not required to be kept secret.*

Definition 3. *The message length capacity region for the degraded G-MAnC-WT is defined as the set of all message length tuples $(\upsilon_g(n))_{g\in\mathcal{G}}$ such that for any $\epsilon > 0$, the message length tuple $((1-\epsilon)2^{\upsilon_g(n)})_{g\in\mathcal{G}}$ is achievable.*

III. Main Results

We first state our results for the case $G = 1$, i.e., uniform power constraint for all users, in Theorem 1. The achievability can be found in Sections IV and the converse follows from Theorem 2. For Theorem 1, we omit the subscript $g = 1$.

Theorem 1 ($G = 1$)**.** *Define $k_n \triangleq \alpha_n l_n$ and assume that $\limsup_{n\to\infty} l_n = +\infty$, $\limsup_{n\to\infty} k_n = +\infty$, $l_n = O(n)$, $k_n = O(n)$, there exists $\delta_0 > 0$ such that $\lim_{n\to\infty} l_n e^{-k_n^{1-\delta_0}} = 0$. The message length capacity when $G = 1$ is*

$$L(n) \triangleq \frac{n}{2k_n} \log\left(\frac{1}{h}\right).$$

The achievability proof of the following result for $G \geqslant 1$ can be obtained using time sharing, and builds upon the proof of Theorem 1. The converse proof is presented in Section V.

Theorem 2 ($G \geqslant 1$)**.** *For $g \in \mathcal{G}$, define $k_n^{(g)} \triangleq \alpha_{g,n}\beta_g l_n$ and assume that $\limsup_{n\to\infty} l_n = +\infty$, $\limsup_{n\to\infty} k_n^{(g)} = +\infty$, $l_n = O(n)$, $k_n^{(g)} = O(n)$, there exists $\delta_0 > 0$ such that $\lim_{n\to\infty} l_n e^{-(k_n^{(g)})^{1-\delta_0}} = 0$. The message length capacity region is*

$$\mathcal{C} \triangleq \left\{ (L^{(g)}(n))_{g\in\mathcal{G}} : \sum_{g\in\mathcal{G}} k_n^{(g)} L^{(g)}(n) \leqslant \frac{n}{2} \log\left(\frac{1}{h}\right) \right\}.$$

When the number of active users is bounded we have the following result proved in Appendix A.

Proposition 1. *For $g \in \mathcal{G}$, assume that $k_n^{(g)}$ is bounded and $\limsup_{n\to\infty} l_n = +\infty$. Then, any achievable message length tuples $(L^{(g)}(n))_{g\in\mathcal{G}}$ must satisfy for all $g \in \mathcal{G}$, $\lim_{n\to\infty} L^{(g)}(n)_{g\in\mathcal{G}}/n = 0$.*

IV. Achievability of Theorem 1

A. Coding Scheme

Fix $\epsilon \in]0, \min(1, P)[$. Let $n \in \mathbb{N}^*$ and define $n_1 \triangleq \epsilon n$, $n_2 \triangleq (1-\epsilon)n$, $\delta_n \triangleq k_n^{-a}$, $a \in]0, \delta_0/2[$. Define also $\widetilde{\upsilon}(n) \triangleq (1-\epsilon)\frac{n}{2(1+\delta_n)k_n} \log(1 + (1+\delta_n)k_n(hP-\epsilon))$ and $\upsilon(n) \triangleq (1-\epsilon)\frac{n}{2(1+\delta_n)k_n} \log(1 + (1+\delta_n)k_n(P-\epsilon)) - \widetilde{\upsilon}(n)$.

Codebook construction: Each user $l \in \mathcal{L}_n$ generates a codebook independently as follows. Generate one sequence $\mathbf{C}_l^{(1)}$ of length n_1 that will be used as signature, $2^{\upsilon(n)+\widetilde{\upsilon}(n)}$ sequences $\left(\mathbf{C}_l^{(2)}(m, \widetilde{m})\right)_{(m,\widetilde{m})\in\mathcal{M}\times\widetilde{\mathcal{M}}}$ of length n_2 with $\mathcal{M} \triangleq [\![1, 2^{\upsilon(n)}]\!]$, $\widetilde{\mathcal{M}} \triangleq [\![1, 2^{\widetilde{\upsilon}(n)}]\!]$, whose components are i.i.d. according to a zero-mean Gaussian distribution with variance $P-\epsilon$. Form $2^{\upsilon(n)+\widetilde{\upsilon}(n)}$ sequences $(\mathbf{C}_l(m, \widetilde{m}))_{(m,\widetilde{m})\in\mathcal{M}\times\widetilde{\mathcal{M}}}$, where $\mathbf{C}_l(m, \widetilde{m}) \triangleq \left(\mathbf{C}_l^{(1)} || \mathbf{C}_l^{(2)}(m, \widetilde{m})\right)$.

Encoding: If Transmitter $l \in \mathcal{L}_n$ is active, then it encodes the message pair $(M_l, \widetilde{M}_l)$, chosen uniformly at random in

$\mathcal{M} \times \widetilde{\mathcal{M}}$, as $\mathbf{C}_l(M_l, \widetilde{M}_l)$ and sends it over the channel. One interprets $\mathbf{0} \in \mathbb{R}^n$ as the signal sent when Transmitter $l \in \mathcal{L}_n$ is inactive.

Decoding: Similar to [2], we split the observations $\mathbf{Y}$ of the legitimate receiver in two sequences $\mathbf{Y}^{(1)} \triangleq Y^{1:n_1}$, $\mathbf{Y}^{(2)} \triangleq Y^{n_1+1:n}$. Define also $\mathbf{N}_Y^{(1)} \triangleq N_Y^{1:n_1}$, $\mathbf{N}_Y^{(2)} \triangleq N_Y^{n_1+1:n}$, $\mathbf{C}^{(1)} \triangleq \underset{l}{\|} \mathbf{C}_l^{(1)} \in \mathbb{R}^{n_1 \times l_n}$, where concatenation is over $l \in \mathcal{L}_n$, $\mathbf{C}^{(2)} \triangleq \underset{l}{\|} \underset{(m,\widetilde{m})}{\|} \left[\mathbf{C}_l^{(2)}(m, \widetilde{m})\right] \in \mathbb{R}^{n_2 \times (l_n |\mathcal{M}||\widetilde{\mathcal{M}}|)}$, where concatenation is over $l \in \mathcal{L}_n$ and $(m, \widetilde{m}) \in \mathcal{M} \times \widetilde{\mathcal{M}}$. Let $\mathbf{S}^{(1)} \in \{0,1\}^{l_n}$, whose components are independent Bernoulli random variables with parameter α_n, represents the transmitters activity. Let $\mathbf{S}^{(2)} \triangleq [\|_{l \in \mathcal{L}_n} \mathbf{S}_l^T]^T$ where $\mathbf{S}_l \in \{0,1\}^{|\mathcal{M}||\widetilde{\mathcal{M}}|}$ indicates the message chosen by transmitter $l \in \mathcal{L}_n$ such that

$$\mathbb{P}[\mathbf{S}_l = \mathbf{0}] = 1 - \alpha_n,$$
$$\mathbb{P}[\mathbf{S}_l = \mathbf{e}_{m,\widetilde{m}}] = \frac{\alpha_n}{|\mathcal{M}||\widetilde{\mathcal{M}}|}, \forall (m, \widetilde{m}) \in \mathcal{M} \times \widetilde{\mathcal{M}},$$

where $\mathbf{e}_{m,\widetilde{m}} \in \{0,1\}^{|\mathcal{M}||\widetilde{\mathcal{M}}|}$ is the all-zero vector with a single component equal to one in position $(m-1)|\widetilde{\mathcal{M}}|+\widetilde{m}$. Hence,

$$\mathbf{Y}^{(1)} = \mathbf{C}^{(1)}\mathbf{S}^{(1)} + \mathbf{N}_Y^{(1)},$$
$$\mathbf{Y}^{(2)} = \mathbf{C}^{(2)}\mathbf{S}^{(2)} + \mathbf{N}_Y^{(2)}. \tag{3}$$

Next, similar to [2], decoding is operated in two steps.

1) User identification: Let $\mathbf{x}^*$ be a solution to the following optimization

$$\min \|\mathbf{Y}^{(1)} - \mathbf{C}^{(1)}\mathbf{x}\|_2^2 \text{ subject to}$$
$$\mathbf{x} \in \{0,1\}^{l_n}, \mathrm{wt}(\mathbf{x}) \leqslant (1+\delta_n)\alpha_n l_n.$$

The receiver determines an estimate of the set of active users as $\widehat{\mathcal{A}} \subset \mathcal{L}_n$, the set of indices of the non-zeros entries of $\mathbf{x}^*$.

2) Message reconstruction: Let $(\mathbf{s}_l^*)_{l \in \mathcal{L}_n}$ be a solution to the following optimization

$$\min \|\mathbf{Y}^{(2)} - \mathbf{C}^{(2)}[\mathbf{s}_1^T, \ldots, \mathbf{s}_{l_n}^T]^T\|_2^2 \text{ subject to}$$
$$\mathbf{s}_l \in \{0,1\}^{|\mathcal{M}||\widetilde{\mathcal{M}}|}, \mathrm{wt}(\mathbf{s}_l) = \mathbb{1}\{l \in \widehat{\mathcal{A}}\}, l \in \mathcal{L}_n.$$

For $l \in \widehat{\mathcal{A}}$, the index of the non-zero entry of $\mathbf{s}_l^*$ corresponds to the estimated message $(\widehat{m}_l, \widehat{\widetilde{m}}_l)$ for transmitter l. Define $\widehat{m}_{\widehat{\mathcal{A}}} \triangleq (\widehat{m}_l)_{l \in \widehat{\mathcal{A}}}$ an estimate of $m_{\mathcal{A}} \triangleq (m_l)_{l \in \mathcal{A}}$ and $\widehat{\widetilde{m}}_{\widehat{\mathcal{A}}} \triangleq (\widehat{\widetilde{m}}_l)_{l \in \widehat{\mathcal{A}}}$ an estimate of $\widetilde{m}_{\mathcal{A}} \triangleq (\widetilde{m}_l)_{l \in \mathcal{A}}$.

B. Coding Scheme Analysis

Let C_n denote the random codebook used by the transmitters and the legitimate receiver.

Probability of error analysis: Define the event $\mathcal{E} \triangleq \{\widehat{\mathcal{A}} = \mathcal{A} \text{ and } \mathrm{wt}(\mathbf{S}^{(2)}) \leqslant (1+\delta_n)k_n\}$. We have

$$\begin{aligned} P_e(C_n) &\triangleq \mathbb{P}\left[\widehat{M}_{\mathcal{L}_n} \neq M_{\mathcal{L}_n}\right] \\ &\leqslant \mathbb{P}\left[\widehat{M}_{\mathcal{L}_n} \neq M_{\mathcal{L}_n} | \mathcal{E}\right] + \mathbb{P}\left[\mathcal{E}^c\right] \\ &= \mathbb{P}\left[\widehat{M}_{\widehat{\mathcal{A}}} \neq M_{\mathcal{A}} | \mathcal{E}\right] + \mathbb{P}\left[\mathcal{E}^c\right] \\ &\leqslant \mathbb{P}\left[\widehat{M}_{\widehat{\mathcal{A}}} \neq M_{\mathcal{A}} | \mathcal{E}\right] + \mathbb{P}\left[\widehat{\mathcal{A}} \neq \mathcal{A}\right] \\ &\quad + \mathbb{P}\left[\mathrm{wt}(\mathbf{S}^{(2)}) > (1+\delta_n)k_n\right]. \end{aligned}$$

We next bound the three term in the right-hand side of the last equation. By Chernoff bound (e.g. [8, Proposition 2.4]), $\mathbb{P}\left[\mathrm{wt}(\mathbf{S}^{(2)}) > (1+\delta_n)k_n\right] \leqslant e^{-k_n\delta_n^2/3} = e^{-k_n^{1-2a}/3}$. Next, by the proof of [2, Theorem 2] for some constants $c_1, c_2 > 0$ and n large enough $\mathbb{P}\left[\widehat{\mathcal{A}} \neq \mathcal{A}\right] \leqslant l_n e^{-c_1 k_n} + e^{-k_n^{1-2a}/3} + (1 - k_n/l_n)^{l_n} + k_n^2 e^{-c_2 k_n}$ – note that the choice of δ_n is different than in [2, Theorem 2] but still ensures $\lim_{n\to\infty} \delta_n \log k_n = 0$. Finally, since $\upsilon(n) + \widetilde{\upsilon}(n) = (1-\epsilon)\frac{n}{2(1+\delta_n)k_n}\log(1 + (1+\delta_n)k_n(P-\epsilon))$, by the proof of [2, Theorem 4], for some constants $c_3, c_4 > 0$ and n large enough, $\mathbb{P}\left[\widehat{M}_{\widehat{\mathcal{A}}} \neq M_{\mathcal{A}} | \mathcal{E}\right] \leqslant \mathbb{P}\left[(\widehat{M}_{\widehat{\mathcal{A}}}, \widehat{\widetilde{M}}_{\widehat{\mathcal{A}}}) \neq (M_{\mathcal{A}}, \widetilde{M}_{\mathcal{A}}) | \mathcal{E}\right] \leqslant k_n e^{-c_4 k_n} + k_n e^{-c_3 n}$. Hence, for n large enough, once can show that

$$\mathbb{P}\left[\widehat{M}_{\mathcal{L}_n} \neq M_{\mathcal{L}_n}\right] \xrightarrow{n\to\infty} 0,$$

by using $\limsup_{n\to\infty} k_n = +\infty$, $k_n = O(n)$, and $\lim_{n\to\infty} l_n e^{-k_n^{1-\delta_0}} = 0$.

Equivocation analysis: Assume that M_A is given and let $(\widetilde{\mathbf{x}}_l)_{l \in \mathcal{L}_n}$ be a solution to the following optimization

$$\min \|\mathbf{Z}^{(2)} - \mathbf{C}^{(2)}[\mathbf{x}_1^T, \ldots, \mathbf{x}_{l_n}^T]^T\|_2^2 \text{ subject to}$$
$$\mathbf{x}_l \in \{0,1\}^{|\mathcal{M}||\widetilde{\mathcal{M}}|}, \mathrm{wt}(\mathbf{x}_l) = \mathrm{wt}(\mathbf{x}_l(M_l)) = \mathbb{1}\{l \in \mathcal{A}\}, l \in \mathcal{L}_n,$$

where we have defined $\mathbf{x}_l(M_l)$ as the sequence of components of $\mathbf{x}_l$ whose indices are in the range $[\![(M_l - 1)|\widetilde{\mathcal{M}}|+1, M_l|\widetilde{\mathcal{M}}|]\!]$. For $l \in \mathcal{A}$, the index of the non-zero entry of $\widetilde{\mathbf{x}}_l$ corresponds to the estimate $\breve{M}_l$ of message $\widetilde{M}_l$ for transmitter l. Define $\breve{M}_{\mathcal{A}} \triangleq (\breve{M}_l)_{l \in \mathcal{A}}$.

Define the event $\widetilde{\mathcal{E}} \triangleq \{\mathrm{wt}(\mathbf{S}^{(2)}) \leqslant (1+\delta_n)k_n\}$. Since $\widetilde{\upsilon}(n) = (1-\epsilon)\frac{n}{2(1+\delta_n)k_n}\log(1 + (1+\delta_n)k_n(hP-\epsilon))$, by the proof of [2, Theorem 4], for some constant $c_4 > 0$ and for n large enough,

$$\mathbb{P}\left[\breve{M}_{\mathcal{A}} \neq \widetilde{M}_{\mathcal{A}} | \widetilde{\mathcal{E}}\right] \leqslant k_n e^{-c_6 k_n} + k_n e^{-c_5 n}. \tag{4}$$

Define $X_{\text{sum}}^n \triangleq \sum_{g \in \mathcal{G}, l \in \mathcal{G}_g} X_{g,l}^n$. We have

$$\begin{aligned} &I(M_{\mathcal{L}_n}; Z^n | AC_n) \\ &\overset{(a)}{=} I(M_A \widetilde{M}_A; Z^n | AC_n) - I(\widetilde{M}_A; Z^n | M_A AC_n) \\ &= I(M_{\mathcal{L}_n} \widetilde{M}_{\mathcal{L}_n}; Z^n | AC_n) - H(\widetilde{M}_A | M_A AC_n) \\ &\quad + H(\widetilde{M}_A | Z^n M_A AC_n), \end{aligned} \tag{5}$$

where (a) holds because $I(M_{\mathcal{L}_n}; Z^n | AC_n) = I(M_A; Z^n | AC_n)$. We next bound the three terms in the right-hand side of (5). We have

$$\begin{aligned} I(M_{\mathcal{L}_n} \widetilde{M}_{\mathcal{L}_n}; Z^n | AC_n) &\overset{(b)}{\leqslant} I\left(X_{\text{sum}}^n; Z^n | AC_n\right) \\ &\overset{(c)}{\leqslant} I\left(X_{\text{sum}}^n; Z^n\right) \\ &\overset{(d)}{\leqslant} \frac{n_2}{2}\log(1 + k_n(hP-\epsilon)), \end{aligned} \tag{6}$$

where (b) holds because $M_{\mathcal{L}_n}\widetilde{M}_{\mathcal{L}_n}-(A,C_n,X_{\text{sum}}^n)-Z^n$ forms a Markov chain, (c) holds because $(A,C_n)-X_{\text{sum}}^n-Z^n$ forms a Markov chain, (d) holds by the proof of [2, Lemma 1]. Next, we have

$$\begin{aligned}
&H(\widetilde{M}_A|M_AAC_n)\\
&\overset{(e)}{=} H(\widetilde{M}_A|AC_n)\\
&\overset{(f)}{\geqslant} H(\widetilde{M}_A|AC_nB=1)\mathbb{P}[B=1]\\
&\geqslant (1-\delta_n)k_n\widetilde{v}(n)\mathbb{P}[B=1]\\
&\overset{(g)}{\geqslant} (1-\delta_n)k_n\widetilde{v}(n)(1-e^{-k_n^{1-2a}/2})\\
&\overset{(h)}{\geqslant} (1-\delta_n)^2\frac{n_2}{2}\log(1+k_n(hP-\epsilon))(1-e^{-k_n^{1-2a}/2}), \quad (7)
\end{aligned}$$

where (e) holds because $\widetilde{M}_A-(A,C_n)-M_A$ forms a Markov chain, (f) holds because $H(\widetilde{M}_A|AC_n)\geqslant H(\widetilde{M}_A|AC_nB)\geqslant H(\widetilde{M}_A|AC_nB=1)\mathbb{P}[B=1]$ where we have defined $B\triangleq\mathbb{1}\{\text{wt}(\mathbf{S}^{(2)})\geqslant(1-\delta_n)k_n\}$, (g) holds by Chernoff bound (e.g. [8, Proposition 2.4]), (h) holds because by definition $\widetilde{v}(n)\geqslant\frac{n_2}{2(1+\delta_n)k_n}\log(1+k_n(hP-\epsilon))\geqslant(1-\delta_n)\frac{n_2}{2k_n}\log(1+k_n(hP-\epsilon))$. Next, we have

$$\begin{aligned}
&H(\widetilde{M}_A|Z^nM_AAC_n)\\
&\overset{(h)}{\leqslant} H(\widetilde{M}_A\widetilde{E}|Z^nM_AAC_n)\\
&\leqslant 1+H(\widetilde{M}_A|Z^nM_AAC_n\widetilde{E}=1)\\
&\quad+H(\widetilde{M}_A|Z^nM_AAC_n\widetilde{E}=0)\mathbb{P}[\widetilde{E}=0]\\
&\overset{(i)}{\leqslant} 1+H(\widetilde{M}_A|Z^nM_AAC_n\widetilde{E}=1)+l_n\widetilde{v}(n)e^{-k_n^{1-2a}/3}\\
&\overset{(j)}{\leqslant} 2+k_n^2(e^{-c_6k_n}+e^{-c_5n})(1+\delta_n)\widetilde{v}(n)+l_n\widetilde{v}(n)e^{-k_n^{1-2a}/3}, \quad (8)
\end{aligned}$$

where in (h) we have defined $\widetilde{E}\triangleq\mathbb{1}\{\text{wt}(\mathbf{S}^{(2)})\leqslant(1+\delta_n)k_n\}$, (i) holds by Chernoff bound (e.g. [8, Proposition 2.4]), (j) holds by Fano's inequality and (4). Hence, from (5)–(8), we have

$$\begin{aligned}
&I(M_{\mathcal{L}_n};Z^n|AC_n)\\
&\leqslant\frac{n_2}{2}\log(1+k_n(hP-\epsilon))\left[1-(1-\delta_n)^2(1-e^{-k_n^{1-2a}/2})\right]\\
&\quad 2+\widetilde{v}(n)\left[k_n^2(e^{-c_6k_n}+e^{-c_5n})(1+\delta_n)+l_ne^{-k_n^{1-2a}/3}\right]\\
&\leqslant\frac{n}{2}\log(1+k_nhP)\left[2\delta_n+(1+\delta_n^2)e^{-k_n^{1-2a}/2}\right]+2\\
&\quad+\widetilde{v}(n)\left[k_n^2(e^{-c_6k_n}+e^{-c_5n})(1+\delta_n)+l_ne^{-k_n^{1-2a}/3}\right]\\
&\overset{(k)}{\leqslant}\frac{n}{2}\log(1+(1+\delta_n)k_nhP)\left[2\delta_n+(1+\delta_n^2)e^{-k_n^{1-2a}/2}\right.\\
&\quad\left.+k_n(e^{-c_6k_n}+e^{-c_5n})+\frac{l_n}{k_n}e^{-k_n^{1-2a}/3}\right]+2\\
&\overset{(j)}{=} o(n),
\end{aligned}$$

where (k) holds by definition of $\widetilde{v}(n)$, and (j) holds because $\lim_{n\to\infty}l_ne^{-k_n^{1-\delta_0}}=0$, $\lim_{n\to\infty}\delta_n\log k_n=0$, $\limsup_{n\to\infty}k_n=+\infty$, and $k_n=O(n)$.

Achievable message length: We have

$$\begin{aligned}
&v(n)\left(\frac{n}{2k_n}\log\left(\frac{1}{h}\right)\right)^{-1}\\
&=\frac{1-\epsilon}{\log\left(\frac{1}{h}\right)(1+\delta_n)}\log\frac{1+(1+\delta_n)k_n(P-\epsilon)}{1+(1+\delta_n)k_n(hP-\epsilon)}\\
&\xrightarrow{n\to\infty}1-\epsilon.
\end{aligned}$$

Hence, for any $\epsilon'>0$, for n large enough and ϵ small enough we have

$$v(n)\geqslant(1-\epsilon')\left(\frac{n}{2k_n}\log\left(\frac{1}{h}\right)\right).$$

Finally, by Markov's inequality, we conclude that there exists a codebook $\mathcal{C}_n$ such that $\lim_{n\to\infty}\frac{1}{n}I(M_{\mathcal{L}_n};Z^n|A\mathcal{C}_n)+P_e(\mathcal{C}_n)=0$.

V. Converse of Theorem 2

We consider a coding scheme that satisfies the requirements of Definition 2. We have

$$\begin{aligned}
&\sum_{g\in\mathcal{G}}\left[l_n\alpha_n^{(g)}\beta_g\log|\mathcal{M}_g|+l_n\beta_gH_b(\alpha_n^{(g)})\right]\\
&=H(M_{\mathcal{L}_n})\\
&=H(M_{\mathcal{L}_n}|Z^n)+H(M_{\mathcal{L}_n}|Y^n)-H(M_{\mathcal{L}_n}|Y^n)\\
&\quad+I(M_{\mathcal{L}_n};Z^n)\\
&\overset{(a)}{=} I(M_{\mathcal{L}_n};Y^n|Z^n)+H(M_{\mathcal{L}_n}|Y^n)+I(M_{\mathcal{L}_n};Z^n)\\
&\overset{(b)}{\leqslant} I(X_{\mathcal{L}_n}^n;Y^n|Z^n)+H(M_{\mathcal{L}_n}|Y^n)+I(M_{\mathcal{L}_n};Z^n)\\
&\overset{(c)}{\leqslant} I(X_{\mathcal{L}_n}^n;Y^n|Z^n)+H(M_{\mathcal{L}_n}|Y^n)+H(A)\\
&\quad+I(M_{\mathcal{L}_n};Z^n|A)\\
&\overset{(d)}{=} I(X_{\mathcal{L}_n}^n;Y^n)-I(X_{\mathcal{L}_n}^n;Z^n)+H(M_{\mathcal{L}_n}|Y^n)+H(A)\\
&\quad+o(n)\\
&\overset{(e)}{=}\text{h}(Y^n)-\text{h}(Z^n)+H(M_{\mathcal{L}_n}|Y^n)+H(A)+o(n)\\
&\overset{(f)}{\leqslant}\text{h}(Y^n)-\frac{n}{2}\log\left[2\pi e\left(1-h+\frac{h2^{2\text{h}(Y^n)/n}}{2\pi e}\right)\right]\\
&\quad+H(M_{\mathcal{L}_n}|Y^n)+H(A)+o(n)\\
&\overset{(g)}{\leqslant}\frac{n}{2}\log\left[\frac{1+\sum_{g\in\mathcal{G}}k_n^{(g)}P_g}{1+h\sum_{g\in\mathcal{G}}k_n^{(g)}P_g}\right]+H(M_{\mathcal{L}_n}|Y^n)+H(A)\\
&\quad+o(n), \quad (9)
\end{aligned}$$

where (a) holds because $M_{\mathcal{L}_n}-Y^n-Z^n$, (b) holds because $M_{\mathcal{L}_n}-X_{\mathcal{L}_n}^n-Y^n-Z^n$, (c) holds because $I(M_{\mathcal{L}_n};Z^n)\leqslant I(M_{\mathcal{L}_n}A;Z^n)=I(A;Z^n)+I(M_{\mathcal{L}_n};Z^n|A)$, (d) holds because $X_{\mathcal{L}_n}^n-Y^n-Z^n$ and by the equivocation condition, (e) holds because $\text{h}(Y^n|X_{\mathcal{L}_n}^n)=\sum_{i=1}^n\text{h}(Y_i|X_{\mathcal{L}_n,i})=\sum_{i=1}^n\text{h}(Z_i|X_{\mathcal{L}_n,i})=\text{h}(Z^n|X_{\mathcal{L}_n}^n)$, (f) holds by the entropy power inequality, similar to [7], [9], as due to the degradedness of the channel, one can write $\text{h}(Z^n)=\text{h}(\sqrt{h}Y^n+\sqrt{1-h}N^n)$ with N^n a vector of n independent variables distributed

according to a standard normal distribution, (g) holds because $x \mapsto x - \frac{n}{2}\log\left[2\pi e\left(1-h+\frac{h2^{2x/n}}{2\pi e}\right)\right]$ is non-decreasing and

$$\begin{aligned}\mathrm{h}(Y^n) &= I(Y^n; X^n_{\text{sum}}) + \mathrm{h}(Y^n|X^n_{\text{sum}}) \\ &= I(Y^n; X^n_{\text{sum}}) + \frac{n}{2}\log(2\pi e) \\ &\leqslant \frac{n}{2}\log\left[1+\sum_{g\in\mathcal{G}} l_n\beta_g\alpha_n^{(g)}P_g\right] + \frac{n}{2}\log(2\pi e), \quad (10)\end{aligned}$$

where the proof of (10) is omitted. Next, we upper-bound the second term in the right-hand side of (9) as

$$\begin{aligned}&H(M_{\mathcal{L}_n}|Y^n) \\ &\overset{(h)}{\leqslant} \sum_{g\in\mathcal{G}} H(M_g|Y^n) \\ &\overset{(i)}{\leqslant} \sum_{g\in\mathcal{G}} \Big[4P_e(n)(k_n^{(g)}\upsilon_g(n) \\ &\qquad + k_n^{(g)} + l_n\beta_g H_b(\alpha_n^{(g)})) + \upsilon_g(n) + 2\Big] \\ &\leqslant \sum_{g\in\mathcal{G}} \Big[4P_e(n)(k_n^{(g)}\upsilon_g(n) + O(n)) + \upsilon_g(n) + 2\Big] \\ &\leqslant \sum_{g\in\mathcal{G}} \left[4P_e(n)(k_n^{(g)}\upsilon_g(n) + O(n)) + \frac{k_n^{(g)}}{\min\limits_{g'\in\mathcal{G}} k_n^{(g')}}\upsilon_g(n) + 2\right], \quad (11)\end{aligned}$$

where (h) holds because conditioning reduces entropy, (i) holds by [2, Lemma 2], where $P_e(n) \triangleq \mathbb{P}[\widehat{M}_{\mathcal{L}_n} \neq M_{\mathcal{L}_n}]$. Hence, since $H(A) = \sum_{g\in\mathcal{G}} l_n\beta_g H_b(\alpha_n^{(g)})$, we have from (9) and (11)

$$\begin{aligned}&\sum_{g\in\mathcal{G}} k_n^{(g)}\upsilon_g(n) \\ &= \sum_{g\in\mathcal{G}} l_n\alpha_n^{(g)}\beta_g \log|\mathcal{M}_g| \\ &\leqslant \frac{n}{2}\log\left[\frac{1+\sum_{g\in\mathcal{G}} k_n^{(g)}P_g}{1+h\sum_{g\in\mathcal{G}} k_n^{(g)}P_g}\right] + \left(\sum_{g\in\mathcal{G}} k_n^{(g)}\upsilon_g(n)\right) \\ &\qquad \times \left(4P_e(n) + \left(\min_{g'\in\mathcal{G}} k_n^{(g')}\right)^{-1}\right) + o(n). \quad (12)\end{aligned}$$

Finally, one can show from (12) that for any $\epsilon > 0$ and n large enough

$$\sum_{g\in\mathcal{G}} k_n^{(g)}\upsilon_g(n) \leqslant (1+\epsilon)\frac{n}{2}\log\left(\frac{1}{h}\right).$$

VI. Concluding remarks

We defined the degraded Gaussian many-access wiretap channel and derived its capacity region when the number of transmitters grows unbounded and at most linearly with the blocklength. Similar to the many-access Gaussian channel and unlike the multiple-access wiretap channel, the capacity region is independent from the power of the transmitters and only depends on the sum rate of achievable message lengths. Our results also prove that joint detection (of the active transmitters) and decoding is not necessary and that performing detection then decoding is optimal. Additionally, the detection phase (for the regime where the numbers of users grows at most linearly with the blocklength) has a negligible impact on the message length that can be transmitted.

Several extensions of our results are currently under investigation including the treatment of non-degraded channels, strong secrecy, and a number of users that grows faster than linearly with the blocklength.

Appendix A
Proof of Proposition 1

Assume $P > 0$, $h < 1$, and define $f : \mathbb{R}_+^* \to \mathbb{R}, x \mapsto \log\left(\frac{1+xP}{1+xhP}\right)$. We will use the following lemma.

Lemma 1. *f is strictly concave. Hence, for any $x > 0$, $\frac{1}{2}f(2x) < f(x)$.*

By contradiction, assume that there exists a vector of achievable message lengths $(L_g^*(n))_{g\in\mathcal{G}}$ such that $\lim_{n\to\infty} L_{g_0}^*(n)/n = C$ for some $g_0 \in \mathcal{G}$ and some $C > 0$. Assume that the transmitters are set to transmit with the message lengths $(L_g^\dagger(n))_{g\in\mathcal{G}}$ where $L_g^\dagger(n) \triangleq L_g^*(n)$ and $L_{g_0}^\dagger(n) \triangleq \frac{n}{2k_0}f(k_0) < nC$, where $k_0 \in \mathbb{N}^*$ is large enough - such k_0 exists because $lim_{x\to+\infty} f(x)/x = 0$. With probability at least $\delta(n) \triangleq \binom{\beta_{g_0}l_n}{2k_0}(\alpha_{g_0,n})^{2k_0}(1-\alpha_{g_0,n})^{\beta_{g_0}l_n-2k_0}\prod_{g\neq g_0}(1-\alpha_{g,n})^{\beta_g l_n}$, the number of active users is at least $2k_0 \in \mathbb{N}^*$ for group $\mathcal{G}_{g_0}$ and 0 for all the other groups. Since $lim_{n\to\infty}\delta(n) > 0$ and, by Lemma 1, $L_{g_0}^\dagger(n) = \frac{n}{2k_0}f(k_0) > \frac{n}{4k_0}f(2k_0)$, where $\frac{n}{4k_0}f(2k_0)$ is the maximal message length for the conventional multiple-access wiretap channel with $2k_0$ transmitters, the error probability is bounded away from 0.

References

[1] S.-C. Chang and E. Weldon, "Coding for T-user multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 25, no. 6, pp. 684–691, 1979.

[2] X. Chen, T.-Y. Chen, and D. Guo, "Capacity of Gaussian many-access channels," *IEEE Trans. Inf, Theory*, vol. 63, no. 6, pp. 3516–3539, 2017.

[3] Y. Polyanskiy, "A perspective on massive random-access," in *IEEE Int. Symp. on Inf. Theory*, 2017, pp. 2523–2527.

[4] T.-Y. Chen, X. Chen, and D. Guo, "Many-broadcast channels: Definition and capacity in the degraded case," in *IEEE Int. Symp. Inf. Theory*, 2014, pp. 2569–2573.

[5] S. Shahi, D. Tuninetti, and N. Devroye, "On the capacity of strong asynchronous multiple access channels with a large number of users," in *IEEE Int. Symp. Inf. Theory*, 2016, pp. 1486–1490.

[6] E. Tekin, S. Serbetli, and A. Yener, "On secure signaling for the Gaussian multiple access wire-tap channel," in *Proc. 39th Annu. Asilomar Conf. Signals, Syst., Comput.*, 2005, pp. 1747–1751.

[7] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5747–5755, 2008.

[8] D. Angluin and L. G. Valiant, "Fast probabilistic algorithms for hamiltonian circuits and matchings," *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 155–193, 1979.

[9] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.