The Degraded Gaussian Multiple Access Wiretap Channel with Selfish Transmitters: A Coalitional Game Theory Perspective

Remi A. Chou and Aylin Yener

Wireless Communications and Networking Laboratory (WCAN)
The School of Electrical Engineering and Computer Science
The Pennsylvania State University, University Park, PA 16802.
remi.chou@psu.edu *yener@engr.psu.edu*

***Abstract*—We study the degraded Gaussian multiple access wiretap channel with selfish transmitters, i.e., they are each solely interested in maximizing their individual secrecy rate. The question then arises as to whether selfish transmitters can increase their individual secrecy rate by participating in a collective, i.e, multiple access, protocol instead of operating on their own. If yes, the question arises if there is a protocol that satisfies all the participating transmitters, in the sense that no transmitter has an incentive to deviate from the protocol. We answer these questions in the positive utilizing coalitional game theory. In particular, we show that cooperation is in the best interest of all transmitters and that there exist protocols that incentivize all transmitters to participate. Furthermore, we determine a unique, fair, and stable achievable secrecy rate allocation.**

I. Introduction

We study secure communication over a degraded Gaussian multiple access wiretap channel (GMAC-WT) [1]. The information-theoretic problem formulation for secure communication over the GMAC-WT enables establishing fundamental limits of achievable rate-tuples, under the assumption of altruistic legitimate entities. That is, the underlying assumption is one of full cooperation where transmitters work together to achieve the largest secure rate region. An equally valid scenario could be that the transmitters are interested only in maximizing *their individual* secure rates. This can lead to a conflict of interests and fairness issues among transmitters as they try to capture limited resources for their benefit. Only certain rate-tuples, if any, would be acceptable by selfish transmitters. A large body of the literature has considered similar questions in multiuser communication problems by means of game theory, see, for instance, [2], [3] for the Gaussian multiple access channel and [4], [5] for interference channels. We also refer to [6] and references therein for the treatment of broader classes of multiuser communication problems.

We treat the problem of selfish transmitters over the GMAC-WT by means of a coalitional game theory framework. We refer to [7] for an introduction to coalitional game theory, and to [8] for a review of some of its applications to telecommunications. The coalitional game we define is inspired by the game formulation of [2] for the Gaussian multiple access channel, which is recovered as a special case of our game. Note that the GMAC-WT with selfish users is also considered in [9] but via non-cooperative game theory and with the assumption that all users follow a specific transmission strategy. Our paper is also related to [10] as we characterize the worst behavior that a group of users can adopt to prevent confidential communication between the other users and the legitimate receiver.

Our contribution can be summarized as follows. We cast the problem of selfish transmitters over the GMAC-WT as a coalitional game. We show that there exist collective protocols for which no transmitter has an incentive to deviate, in particular, we show that the core of the game we have defined is non-empty and intersects known achievable regions for the GMAC-WT. Using the axiomatic solution concept introduced in [2], we determine a unique, fair, and stable secrecy rate allocation. As a byproduct, we obtain achievability regions for the degraded GMAC-WT in presence of an eavesdropper that can arbitrarily jam the main channel.

The remainder of the paper is organized as follows. We define in Section II a coalitional game for the GMAC-WT with selfish transmitters. We study the properties of the game and its core in Section III. In Section IV, we propose as a solution for a fair allocation, an achievable secrecy rate allocation that is shown to belong to the core of the game and that satisfies a series of axioms. We end the paper with concluding remarks in Section V. Most proofs are sketched or some omitted due to space constraints.

Notation: Throughout the paper, define $[\![a,b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. The components of a vector, X^n, of size $n \in \mathbb{N}$, are denoted by subscripts, i.e., $X^n \triangleq (X_1, X_2, \ldots, X_n)$. For $x \in \mathbb{R}$, define $[x]^+ \triangleq \max(0, x)$. The power set of $\mathcal{S}$ is denoted by $2^{\mathcal{S}}$. Unless specified otherwise, capital letters designate random variables, whereas lowercase letters designate realizations of associated random variables, e.g., x is a realization of the random variable X. For any set $\mathcal{S} \subset \mathbb{N}$, and any sequence $(R_s)_{s\in\mathcal{S}}$ of real numbers we use the notation $R_{\mathcal{S}} \triangleq \sum_{s\in\mathcal{S}} R_s$.

This work was supported in part by NSF grant CNS-1314719.

978-1-5090-4096-4/17/$31.00 ©2017 IEEE

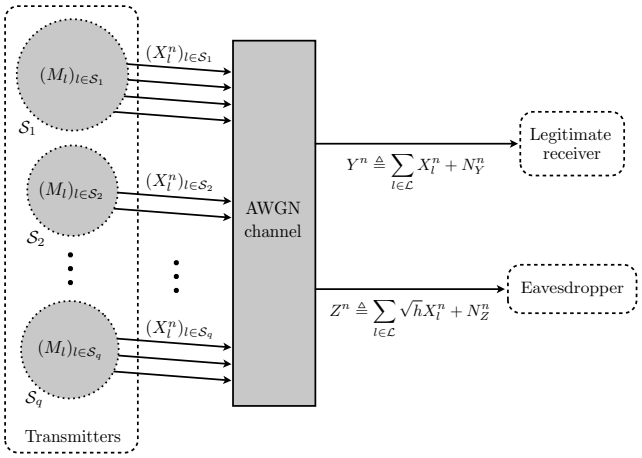

Fig. 1. Degraded Gaussian Wiretap Channel, where the transmitters form q coalitions.

II. Problem statement and game definition

We consider the GMAC-WT with L transmitters. In the remainder of the paper, we let $\mathcal{L} \triangleq [\![1, L]\!]$ denote the set of transmitters. More specifically, we consider the following channel model, put under standard form [1],

$$Y^n \triangleq \sum_{l\in\mathcal{L}} X_l^n + N_Y^n, \tag{1a}$$

$$Z^n \triangleq \sum_{l\in\mathcal{L}} \sqrt{h} X_l^n + N_Z^n, \tag{1b}$$

where $h < 1$, i.e., we consider the degraded setting as in [1]. Y^n and Z^n are the channel outputs observed by the legitimate receiver and the eavesdropper, respectively, for $l \in \mathcal{L}$, X_l^n is the signal by transmitter l satisfying the power constraint $\|X_l^n\|^2 \triangleq \sum_{i=1}^n X_i^2 \leqslant n\Gamma_l$ and that encodes a message M_l with rate R_l. N_Y^n and N_Z^n are independent and identically distributed Gaussian noise sequences with unit variances σ_Y^2, σ_Z^2, respectively. We define a coding scheme and achievable rates for our channel model following the scheme in [2] over $k \in \mathbb{N}$ encoding blocks of length n to allow time-sharing, with the following constraints:

$$\lim_{n\to\infty} \mathbb{P}[\widehat{M}_{\mathcal{L}} \neq M_{\mathcal{L}}] = 0 \text{ (reliability)}, \tag{2a}$$

$$\lim_{n\to\infty} \frac{1}{nk} H(M_{\mathcal{L}}|Z^{kn}) \geqslant \frac{1}{nk} H(M_{\mathcal{L}}) \text{ (equivocation)}, \tag{2b}$$

where $M_{\mathcal{L}}$ represents all the message sent by the transmitters, $\widehat{M}_{\mathcal{L}}$ is the estimate of $M_{\mathcal{L}}$ formed by the receiver, and Z^{kn} is all the observations of the eavesdropper. We assume that the transmitters are selfish, i.e., they are solely interested in maximizing their own secrecy rate. The transmitters could potentially form *coalitions* to achieve this goal as depicted in Figure 1, in the sense that subsets of agents can agree on a multiple access protocol before the actual information transmission to the receiver occurs. As would be the case for GMAC-WT the members of a given coalition do not alter the multiple access protocol they agreed on once transmission commences. The questions we would like to address are as follows. (i) Can the transmitters benefit from forming coalitions? (ii) If yes, can the transmitters find a consensus about which coalitions to form despite their selfish nature? (iii) If such consensus exists, how should the secrecy sum-rate of each coalition be allocated among its transmitters? To answer these questions, we define a game corresponding to our problem as follows. For $l \in \mathcal{L}$, let $\mathcal{A}_l$ corresponds to the set of strategies that transmitter l can adopt, and let $\pi_l(a_{\mathcal{L}})$ be the payoff of transmitter l, i.e., its secrecy rate, when the strategies $a_{\mathcal{L}} \in \bigtimes_{l\in\mathcal{L}} \mathcal{A}_l$ are played by all the transmitters. We next adopt a coalitional game theory framework by associating with each potential coalition of transmitters $\mathcal{S} \subseteq \mathcal{L}$ a worth $v(\mathcal{S})$. As detailed in Section III, the function v will allow us to study stability of coalitions formed by the transmitters, where stability of a coalition means that there is no incentive to merge with another coalition or to split in smaller coalitions. Two potential choices for the worth $v(\mathcal{S})$ of coalition $\mathcal{S} \subseteq \mathcal{L}$ are the following, [11], [12]

$$\max_{a_{\mathcal{S}}} \min_{a_{\mathcal{S}^c}} \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{S}^c}), \tag{3}$$

$$\min_{a_{\mathcal{S}^c}} \max_{a_{\mathcal{S}}} \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{S}^c}), \tag{4}$$

where the quantity in (3) corresponds to the payoff that coalition $\mathcal{S}$ can ensure to its members regardless of the strategies adopted by the member of $\mathcal{S}^c$, and the one in (4) to the payoff that coalition $\mathcal{S}^c$ cannot prevent coalition $\mathcal{S}$ to receive; see [12] for a detailed explanation of the subtle difference between these two notions in general. Observe that, for our problem, both quantities are equal since for any $\mathcal{S} \subseteq \mathcal{L}$, there exists $a^*_{\mathcal{S}^c} \in \bigtimes_{i\in\mathcal{S}^c} A_i$ such that for any strategies $a_{\mathcal{S}} \in \bigtimes_{i\in\mathcal{S}} A_i$, we have

$$\sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{S}^c}) \geqslant \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a^*_{\mathcal{S}^c}).$$

Note that the signals of the transmitters in $\mathcal{S}^c$ can be considered as a single signal of power up to $(\sum_{l\in\mathcal{S}^c} \sqrt{\Gamma_l})^2$ from the receiver perspective. We can thus consider the following strategy $a^*_{\mathcal{S}^c}$: the transmitters in $\mathcal{S}^c$ collude against coalition $\mathcal{S}$ by acting as a mega jammer with power upper bounded by $(\sum_{l\in\mathcal{S}^c} \sqrt{\Gamma_l})^2$ and by revealing their transmitted sequences to the eavesdropper. Using the terminology of [11], the game is *clear*, i.e., equality holds between (3) and (4).

To summarize, we cast the problem as a coalitional game $(\mathcal{L}, v)$ where the value function is defined as

$$v : 2^{\mathcal{L}} \to \mathbb{R}^+, \mathcal{S} \mapsto \max_{a_{\mathcal{S}}} \min_{a_{\mathcal{S}^c}} \sum_{i\in\mathcal{S}} \pi_i(a_{\mathcal{S}}, a_{\mathcal{S}^c}), \tag{5}$$

such that $v(\mathcal{S})$ corresponds to the maximal secrecy sum-rate achievable by coalition $\mathcal{S}$ when *no specific strategy is assumed* for the transmitters in $\mathcal{S}^c$.

III. Properties of the game and characterization of its core

We first provide the following characterization of the value function, whose proof relies on techniques to study arbitrar-

ily varying channels [13], polymatroid properties, and [14, Lemma 1]. We omit the proof of Theorem 1 due to space limitations and note that it involves a GMAC-WT model similar to the one reported in [15], generalized to $L > 2$, and on the special case of the degraded channel.

Theorem 1. *Let $\mathcal{S} \subseteq \mathcal{L}$. We have*

$$v(\mathcal{S}) = \left[\frac{1}{2}\log\left(\frac{1+h_{\Lambda_{\mathcal{S}^c}}\Gamma_{\mathcal{S}(\Lambda_{\mathcal{S}^c})}}{1+h\Gamma_{\mathcal{S}(\Lambda_{\mathcal{S}^c})}}\right)\right]^+, \tag{6}$$

where for any $\mathcal{S} \subseteq \mathcal{L}$, $\Lambda_{\mathcal{S}^c} \triangleq \left(\sum_{l\in\mathcal{S}^c}\sqrt{\Gamma_l}\right)^2$, $h_{\Lambda_{\mathcal{S}^c}} \triangleq (1+\Lambda_{\mathcal{S}^c})^{-1}$, $\mathcal{S}(\Lambda_{\mathcal{S}^c}) \triangleq \{l \in \mathcal{S} : \Gamma_l > \Lambda_{\mathcal{S}^c}\}$, $\Gamma_{\mathcal{S}} \triangleq \sum_{l\in\mathcal{S}}\Gamma_l$.

We now review the notion of superadditivity.

Definition 1. *A game $(\mathcal{L}, v)$ is superadditive if $v : 2^{\mathcal{L}} \to \mathbb{R}^+$ is such that*

$$\forall \mathcal{S}, \mathcal{T} \subseteq \mathcal{L}, \mathcal{S}\cap\mathcal{T} = \emptyset \implies v(\mathcal{S}) + v(\mathcal{T}) \leqslant v(\mathcal{S}\cup\mathcal{T}). \tag{7}$$

Property 1. *The game $(\mathcal{L}, v)$ defined in* (5) *is superadditive.*

Superadditivity implies that there is an interest in forming a large coalition to obtain a larger secrecy sum-rate, however, this large coalition might not be in the individual interest of the transmitters, and can thus be unstable. A useful concept to overcome this complication is the core of the game.

Definition 2 (e.g. [7])**.** *The core $\mathcal{C}(v)$ of a superadditive game $(\mathcal{L}, v)$ is the following set*

$$\left\{(R_l)_{l\in\mathcal{L}} : \sum_{l\in\mathcal{L}} R_l = v(\mathcal{L}) \text{ and } \sum_{i\in\mathcal{S}} R_i \geqslant v(\mathcal{S}), \forall \mathcal{S} \subset \mathcal{L}\right\}. \tag{8}$$

Observe that for any point in the core, the grand coalition, i.e., the coalition $\mathcal{L}$, is in the best interest to all transmitters, since the set of inequality in (8) ensures that no coalition of agents can increase its secrecy sum-rate by leaving the grand coalition. Observe also that for any point in the core the maximal secrecy sum-rate $v(\mathcal{L})$ for the grand coalition is achieved. In general, the core of a game can be empty. However, we will show that the game $(\mathcal{L}, v)$ defined in (5) has a non-empty core.

Definition 2 further clarifies the choice of the value function v. A coalition $\mathcal{S}$ wishes to be associated with a value $v(S)$ as large as possible, while the transmitters outside $\mathcal{S}$ wish $v(S)$ to be as small as possible to demand a higher share of $v(\mathcal{L})$. The latter transmitters achieve their goal by waiving a threat argument, which consists in arguing that they could adopt the strategy that minimizes $v(S)$, whereas coalition $\mathcal{S}$ achieves its goal by arguing that it can always achieve the secrecy sum-rate of Theorem 1, irrespective of the strategy of transmitters in $\mathcal{S}^c$. This formulation is generically termed as alpha effectiveness or alpha theory [11], [12]. It has also been used in [2] for the Gaussian multiple access channel and in [16] for many-to-one secret-key generation.

We next characterize a subset of the core that is achievable by the transmitters.

Theorem 2. *The core of the game $(\mathcal{L}, v)$ contains the following achievable rate-tuples*

$$\mathcal{C}^*(v) \triangleq \left\{(R_l)_{l\in\mathcal{L}} : R_{\mathcal{L}} = \frac{1}{2}\log\left(\frac{1+\Gamma_{\mathcal{L}}}{1+h\Gamma_{\mathcal{L}}}\right), \text{ and } \forall \mathcal{S}\subset\mathcal{L}, R_{\mathcal{S}} \leqslant \left[\frac{1}{2}\log\left(\frac{1+\Gamma_{\mathcal{S}}}{1+h\Gamma_{\mathcal{S}}}\right)\right]^*\right\}. \tag{9}$$

Proof. The fact that the rate-tuples defined in (9) are achievable follows from [1]. We now show that $\mathcal{C}^*(v) \subset \mathcal{C}(v)$. Let $\mathcal{S} \subseteq \mathcal{L}$ and assume $v(\mathcal{S}) > 0$, i.e., $h_{\Lambda_{\mathcal{S}^c}} > h$. Let $(R_l)_{l\in\mathcal{L}} \in \mathcal{C}^*(v)$, we have

$$\begin{aligned}
R_{\mathcal{S}} &= v(\mathcal{L}) - R_{\mathcal{S}^c} && \text{(10a)}\\
&\geqslant v(\mathcal{L}) - \frac{1}{2}\log\left[\frac{1+\Gamma_{\mathcal{S}^c}}{1+h\Gamma_{\mathcal{S}^c}}\right] && \text{(10b)}\\
&= \frac{1}{2}\log\left[\left(1+\frac{\Gamma_{\mathcal{S}}}{1+\Gamma_{\mathcal{S}^c}}\right)\left(1+\frac{h\Gamma_{\mathcal{S}}}{1+h\Gamma_{\mathcal{S}^c}}\right)^{-1}\right] && \text{(10c)}\\
&\geqslant \frac{1}{2}\log\left[\left(1+\frac{\Gamma_{\mathcal{S}}}{1+\Gamma_{\mathcal{S}^c}}\right)(1+h\Gamma_{\mathcal{S}})^{-1}\right] && \text{(10d)}\\
&\geqslant \frac{1}{2}\log\left[\left(1+\frac{\Gamma_{\mathcal{S}(\Lambda_{\mathcal{S}^c})}}{1+\Lambda_{\mathcal{S}^c}}\right)\left(1+h\Gamma_{\mathcal{S}(\Lambda_{\mathcal{S}^c})}\right)^{-1}\right] && \text{(10e)}\\
&= v(\mathcal{S}), && \text{(10f)}
\end{aligned}$$

where (10a) and (10b) hold by definition of $\mathcal{C}^*(v)$, (10e) holds by definition of $\Lambda_{\mathcal{S}^c}$ and because when $h_{\Lambda_{\mathcal{S}^c}} > h$, $x \mapsto \log\left(\frac{1+xh_{\Lambda_{\mathcal{S}^c}}}{1+xh}\right)$ is increasing. Hence, $(R_l)_{l\in\mathcal{L}} \in \mathcal{C}(v)$. ∎

IV. Stable and fair allocation

Although we have found in Theorem 2 achievable rate-tuples that belong to the core of the game, the question of choosing a specific point in the core remains. It is critical to satisfy all transmitters, since an unsatisfied transmitter, even with a relatively lower power constraint, could jam and, depending on the channel parameters, prevent achievability of *any positive secrecy rate* by the other transmitters, irrespective of their power constraints. We use the solution concept introduced in [2] to define a fair secrecy rate allocation. We will then show (i) existence and uniqueness, (ii) achievability, and (iii) membership to the core of this allocation.

Definition 3 ([2])**.** *A fair secrecy rate allocation $\{R_l^*(v)\}_{l\in\mathcal{L}}$ should satisfy the following axioms.*

(i) ***Efficiency****: The maximal secrecy sum-rate is achieved $\sum_{l\in\mathcal{L}} R_l^*(v) = v(\mathcal{L})$.*

(ii) ***Symmetry****: The labeling of the players should not influence the secrecy rate allocation. More specifically, let $\pi \in \mathrm{Sym}(L)$, where $\mathrm{Sym}(L)$ is the symmetric group on $\mathcal{L}$, and let πv be the game with value function that maps $\mathcal{S} \subseteq \mathcal{L}$ to $v(\{\pi(s) : s \in \mathcal{S}\})$. Then, for any $\pi \in \mathrm{Sym}(L)$, for any $l \in \mathcal{L}$, $R_l^*(v) = R_{\pi(l)}^*(\pi v)$.*

(iii) ***Envy-freeness****: For $i, j \in \mathcal{L}$, if $\Gamma_i > \Gamma_j$ and player i decides to conserve energy and only use the power Γ_j, then player i should receive the same secrecy rate allocation than player j. More specifically, let $v^{i,j}$ be the*

same game as v when the power constraint of player i is Γ_j, then one should have $R_i^*(v^{i,j}) = R_j^*(v)$.

We now show that for our problem there is a unique secrecy rate allocation as axiomatized in Definition 3. We assume the sequence $(\Gamma_l)_{l\in\mathcal{L}}$ decreasing by relabeling the players if necessary.

Proposition 1. *There exists a unique secrecy rate allocation $\{R_l^*(v)\}_{l\in\mathcal{L}}$ that satisfies the three axioms of Definition 3. Moreover, for $l \in \mathcal{L}$*

$$R_l^*(v) = \frac{1}{l}\left[\frac{1}{2}\log\left[\frac{1+l\Gamma_l+\Gamma_{l+1:L}}{1+h(l\Gamma_l+\Gamma_{l+1:L})}\right] - R_{l+1:L}^*(v)\right]. \tag{11}$$

Proof. The proof is similar to [2, Theorem 5.1]. Define for $x \in [0,1]$, for $l \in \mathcal{L}$

$$\phi_{x,l}(v) \triangleq \frac{1}{l}\left[\frac{1}{2}\log\left[1+x(l\Gamma_l+\Gamma_{l+1:L})\right] - \sum_{i=l+1}^{L}\phi_{x,i}(v)\right] \tag{12}$$

Some manipulations, similar to [2, Eq.(8)], gives that for any $x \in [0,1]$, for any $l \in \mathcal{L}\backslash\{L\}$

$$\phi_{x,l}(v) - \phi_{x,l+1}(v) = \frac{1}{2l}\log\left[\frac{1+x(l\Gamma_l+\Gamma_{l+1:L})}{1+x(l\Gamma_{l+1}+\Gamma_{l+1:L})}\right], \tag{13}$$

and, as shown in [2, Lemma 1], that for any $x \in [0,1]$, for any $l, l' \in \mathcal{L}$ such that $\Gamma_l > \Gamma_l'$

$$\phi_{x,l}(v^{l,l'}) = \phi_{x,l'}(v). \tag{14}$$

Define now the following secrecy rate allocation for $l \in \mathcal{L}$

$$R_l^*(v) \triangleq \phi_{1,l}(v) - \phi_{h,l}(v). \tag{15}$$

From (15), efficiency is easily seen by choosing $l = 1$ in (12), symmetry follows from (13), and envy-freeness follows from (14). The proof of uniqueness is identical to the proof of [2, Theorem 5.1]. ∎

We now show that the secrecy rate allocation $\{R_l^*(v)\}_{l\in\mathcal{L}}$ from Definition 3 is achievable and belongs to the core.

Theorem 3. *The secrecy rate allocation $\{R_l^*(v)\}_{l\in\mathcal{L}}$ defined in* (11) *is such that*

$$\forall \mathcal{S} \subseteq \mathcal{L}, 0 \leqslant R_{\mathcal{S}}^*(v) \leqslant \frac{1}{2}\log\left(\frac{1+\Gamma_{\mathcal{S}}}{1+h\Gamma_{\mathcal{S}}}\right). \tag{16}$$

Hence, by Theorem 2, $\{R_l^*(v)\}_{l\in\mathcal{L}}$ is achievable because it is in $\mathcal{C}^*(v)$ and belongs to the core because $\mathcal{C}^*(v) \subset \mathcal{C}(v)$.

Proof. In the following we use the notation $\Gamma_{i:j} \triangleq \sum_{l=i}^{j}\Gamma_l$ for any $i, j \in \mathbb{N}$. We first prove that for any $l \in \mathcal{L}$, $R_l^*(v) > 0$. Define for $k \in \mathbb{N}^*$, $h_1, h_2 \in [0,1[$, such that $h_1 < h_2$, $a \in \mathbb{R}_+$

$$f_{k,h_1,h_2,a} : \mathbb{R}_+ \to \mathbb{R}, x \mapsto \frac{1}{2}\log\left[\frac{1+h_1(kx+a)}{1+h_2(kx+a)}\right]. \tag{17}$$

For $l \in [\![1, L-1]\!]$,

$$\begin{aligned} R_l^*(v) - R_{l+1}^*(v) &= \frac{f_{l,h,1,\Gamma_{l+1:L}}(\Gamma_{l+1}) - f_{l,h,1,\Gamma_{l+1:L}}(\Gamma_l)}{l} && \text{(18a)}\\ &\geqslant 0, && \text{(18b)} \end{aligned}$$

where (18a) holds by (13) and (15), and (18b) holds because $\Gamma_{l+1} \leqslant \Gamma_l$ and $f_{l,h,1,\Gamma_{l+1:L}}$ is decreasing.Then,

$$\begin{aligned} R_L^*(v) &= -f_{L,h,1,0}(\Gamma_L) && \text{(19a)}\\ &> 0, && \text{(19b)} \end{aligned}$$

where (19a) holds by (13) and (15), (19b) holds because $h < 1$. Hence, by (18b) and (19b), for any $l \in \mathcal{L}$, $R_l^*(v) > 0$.

Next, we prove by induction that

$$\forall \mathcal{S} \subseteq \mathcal{L}, R_{\mathcal{S}}^*(v) \leqslant \frac{1}{2}\log\left(\frac{1+\Gamma_{\mathcal{S}}}{1+h\Gamma_{\mathcal{S}}}\right). \tag{20}$$

Clearly, (20) is true when $L = 1$. We assume that (20) is true for $L = K \in \mathbb{N}^*$, we will show that (20) is true for $L = K+1$. Let v be the game with $L = K+1$ users. We let $v^{(-j)}$ denote the game v by removing user $j \in [\![1, K+1]\!]$.

One can show that for any $l \in [\![1, K+1]\!]$, for any $j \in [\![1, K+1]\!]\backslash\{l\}$,

$$R_l^*(v) < R_l^*(v^{(-j)}). \tag{21}$$

Finally, for any $\mathcal{S} \subsetneq [\![1, K+1]\!]$, there exist $j_{\mathcal{S}} \in [\![1, K+1]\!]\backslash\mathcal{S}$ such that

$$\begin{aligned} R_{\mathcal{S}}^*(v) &< R_{\mathcal{S}}^*(v^{(-j_{\mathcal{S}})}) && \text{(22a)}\\ &< \frac{1}{2}\log\left(\frac{1+\Gamma_{\mathcal{S}}}{1+h\Gamma_{\mathcal{S}}}\right). && \text{(22b)} \end{aligned}$$

where (22a) holds by (21), and (22b) holds by induction hypothesis. ∎

We next bound the ratio of the secrecy rates of two transmitters by studying the influence of the noise level at the legitimate receiver and at the eavesdropper. More specifically, we assume $\sigma_Y^2 \leftarrow \omega\sigma_Y^2$ and $\sigma_Z^2 \leftarrow \omega\sigma_Z^2$, $\omega \in \mathbb{R}_+$ such that after normalization for any $l \in \mathcal{L}$, $\Gamma_l \leftarrow \omega^{-1}\Gamma_l$. Let $v^{(\omega)}$ denote the game with these new parameters. We obtain the same qualitative property as in [2, Section 5.5], namely, when the signal-to-noise ratio is high for all transmitters, they all obtain similar secrecy rates, whereas when the signal-to-noise ratio is low, they obtain secrecy rates proportional to their power constraints.

Proposition 2. *We assume the sequence $(\Gamma_l)_{l\in\mathcal{L}}$ decreasing by relabeling the players if necessary. For any $l \in [\![1, L-1]\!]$ such that $\Gamma_l \neq \Gamma_{l+1}$,*

$$\omega : \mathbb{R}_+^* \to \mathbb{R}, \mapsto \frac{R_l^*(v^{(\omega)})}{R_{l+1}^*(v^{(\omega)})}$$

is increasing and its image is $\left[1, \frac{\Gamma_{l'}}{\Gamma_l}\right]$. Hence, the secrecy rate allocation $\{R_l^*(v)\}_{l\in\mathcal{L}}$ defined in (11) *satisfies for $l, l' \in \mathcal{L}$*

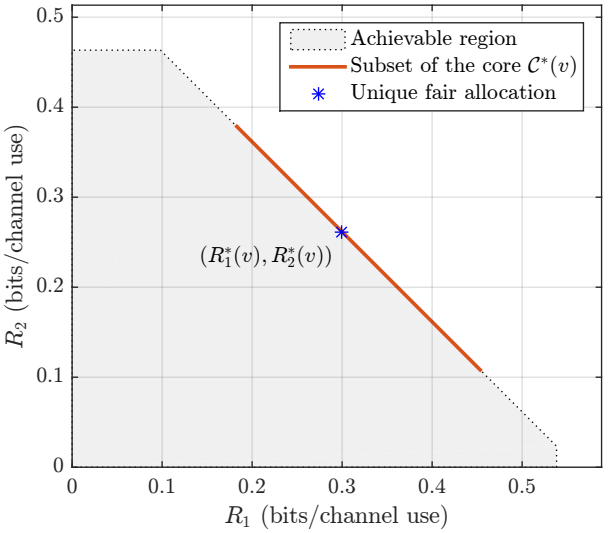

Fig. 2. Representation of a known achievable region [1], a subset of the core $\mathcal{C}^*(v)$ defined in Theorem 2, and the allocation $(R_1^*(v), R_2^*(v))$ defined in Proposition 1 for two transmitters with power constraints $(\Gamma_1, \Gamma_2) = (2, 1.4)$ and $h = 0.3$.

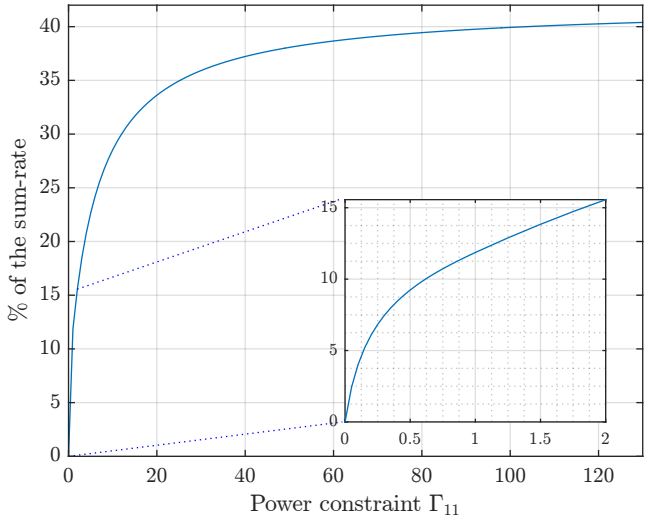

Fig. 3. We assume $L = 11$, $\Gamma_i = i \cdot 10^{-1}$ for $i \in [\![1, 10]\!]$ and $h = 0.1$. The percentage of the secrecy sum-rate to which Transmitter 11 is entitled, according to Proposition 1, is represented in function of its power constraint Γ_{11}.

$$\textit{such that } \Gamma_{l'} \geqslant \Gamma_l, \quad 1 \leqslant \frac{R_{l'}^*(v)}{R_l^*(v)} \leqslant \frac{\Gamma_{l'}}{\Gamma_l}. \tag{23}$$

We illustrate Theorem 2, Proposition 1, and Theorem 3 in Figure 2 with an example when $L = 2$. We also depict in Figure 3 the percentage of the sum-rate to which a user is entitled, according to Proposition 1, given its power constraint for an example with $L = 11$.

V. Concluding Remarks

We have studied the Gaussian multiple access wiretap channel with selfish transmitters. Although a collective protocol can increase the individual secrecy rate of the transmitters, it can, at the same time, lead to conflict of interests. To address serving selfish users, we have considered a coalitional game in which the worth of a given coalition is determined under information-theoretic guarantees, i.e., the worth associated with a coalition is computed with no restrictions on the strategies that the users outside the coalition can adopt. We have concluded that the grand coalition is in the best interest of all users and stable, in the sense that no coalition of transmitters has any incentive to leave the grand coalition. We have also determined a fair secrecy rate allocation, and showed its uniqueness, achievability, and its membership to the core of the game.

Note that it is possible to generalize the model by considering untrusted transmitters over the channel. All our results carry over to this case albeit this significantly complicates the analysis. In particular, one cannot invoke [1] in the proof of Theorem 2 anymore. Note also that the problem in the case of non-degraded channels remains open.

References

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

[2] R. La and V. Anantharam, "A game-theoretic look at the Gaussian multiaccess channel," *DIMACS series in discrete mathematics and theoretical computer science*, vol. 66, pp. 87–106, 2004.

[3] V. Gajic and B. Rimoldi, "Game theoretic considerations for the Gaussian multiple access channel," in *IEEE Int. Symp. Inf. Theory*, 2008, pp. 2523–2527.

[4] R. Berry and D. Tse, "Shannon meets Nash on the interference channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2821–2836, 2011.

[5] X. Liu and E. Erkip, "A game-theoretic view of the interference channel: Impact of coordination and bargaining," *IEEE Trans. Inf. Theory*, vol. 57, no. 5, pp. 2805–2820, 2011.

[6] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game theory in wireless and communication networks: theory, models, and applications*. Cambridge University Press, 2012.

[7] B. Peleg and P. Sudhölter, *Introduction to the theory of cooperative games*. Springer Science & Business Media, 2007, vol. 34.

[8] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Başar, "Coalitional game theory for communication networks," *IEEE Signal Process. Magazine*, vol. 26, no. 5, pp. 77–97, 2009.

[9] H. Ge, R. Xu, and R. Berry, "Secure signaling games for Gaussian multiple access wiretap channels," in *IEEE Int. Symp. Inf. Theory*, 2015, pp. 111–115.

[10] K. Banawan and S. Ulukus, "Achievable secrecy rates in the multiple access wiretap channel with deviating users," in *IEEE Int. Symp. Inf. Theory*, 2016, pp. 2814–2818.

[11] G. Jentzsch, "Some thoughts on the theory of cooperative games," *Advances in Game Theory, Annals of Mathematical Studies*, no. 52, pp. 407–442, 1964.

[12] L. Shapley and M. Shubik, "Game theory in economics - Chapter 6: Characteristic function, core, and stable set," *RAND R904/6-NSF*, 1973.

[13] I. Csiszár and P. Narayan, "Capacity of the Gaussian arbitrarily varying channel," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 18–26, 1991.

[14] R. Chou and A. Yener, "Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming," in *IEEE Int. Symp. Inf. Theory*, 2016, pp. 983–987.

[15] R. Chou and A. Yener, "The Gaussian multiple access wiretap channel when the eavesdropper can arbitrarily jam," in *IEEE Int. Symp. Inf. Theory*, 2017.

[16] R. Chou and A. Yener, "A game theoretic treatment for pair-wise secret-key generation in many-to-one networks," in *IEEE Int. Symp. Inf. Theory*, 2017.