A Sophisticated Anti-Eavesdropping Strategy

Andrey Garnaev, *Member, IEEE*, and Wade Trappe, *Fellow, IEEE*

***Abstract*—Wireless networks are susceptible to malicious attacks, especially those involving eavesdropping. In this letter, we consider a new type of anti-eavesdropping strategy which, beyond the basic goal of increasing the secrecy rate, also wants to achieve this in the most unpredictable way for the adversary. We model the problem by a non-zero sum game where a control center (called the transmitter) must communicate with a group of nodes allocated in security zone in the presence of an adversary intent on eavesdropping upon this communication. The transmitter wants to find a trade-off between two goals: (a) to increase the expected secrecy rate, and (b) to maintain such secret communication in the most unpredictable way for the adversary. As a metric for unpredictability of the transmitter we consider the Shannon entropy of its strategy. We model this problem by a nonzero-sum, two-player resource allocation game. The equilibrium is found in closed form, and its dependence on communication network parameters is illustrated. Finally, weighting coefficients for the basic and secondary goals of the transmitter are optimized based on proportional fairness criteria.**

***Index Terms*—Eavesdropping, entropy, Nash equilibrium.**

I. Introduction

THE PROBLEM of establishing secret communication between a transmitter and a receiver is fundamental to building secure communication systems. Physical layer security problems have commonly been studied under the threat of passive eavesdroppers [1]–[3]. Some works have studied how an active eavesdropper with the dual capability of either eavesdropping passively or jamming any ongoing transmission can disrupt the security and reliability of wireless communications networks [4]–[11]. In all these works, the anti-eavesdropping strategy was focused on the basic goal to maximize the secrecy rate. In this letter, different from prior works, we design a new sophisticated anti-eavesdropping strategy which, beyond the basic goal of maintaining secret communication as measured by the expected secrecy rate, also has a secondary goal of achieving such communication in the most unpredictable way for the adversary. We model the problem by a non-zero sum game where a control center (called the transmitter) must communicate with a group of nodes allocated in secure zone in the presence of an adversary aimed at eavesdropping upon this communication. As a metric for the secret communication by the transmitter we consider the secrecy rate. Meanwhile, as a metric for unpredictability of the transmitter we consider the Shannon entropy of its strategy. We model this problem by a nonzero-sum, two-player resource allocation game. The equilibrium is found in closed form, and its dependence on communication network parameters is illustrated. Finally, we show how weighting coefficients for the basic and secondary goals of the transmitter could be optimized via a fairness approach.

Manuscript received March 7, 2022; accepted May 3, 2022. Date of publication May 12, 2022; date of current version July 11, 2022. This work was supported in part by the U.S. National Science Foundation under Grant CNS-1909186 and Grant ECCS-2128451. The associate editor coordinating the review of this article and approving it for publication was J. Lee. *(Corresponding author: Andrey Garnaev.)*

The authors are with WINLAB, Rutgers University, North Brunswick, NJ 08902 USA (e-mail: garnaev@yahoo.com; trappe@winlab.rutgers.edu).

Digital Object Identifier 10.1109/LWC.2022.3174573

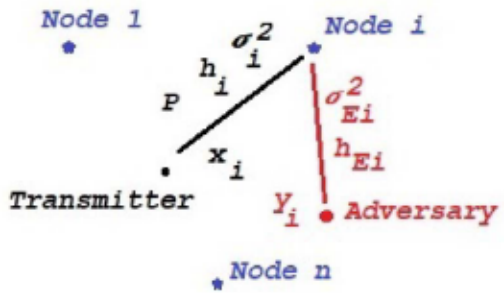

Fig. 1. Transmitter, nodes and adversary.

II. Communication Model

In this letter we consider a control center (transmitter) which must communicate with n nodes secretly in the presence of an adversary. The transmitter employs a separate channel for communication with each of the n nodes. As an example, it could be a (ground) control center which has to communicate with n drones engaged in performing a mission or task. An adversary intends to eavesdrop upon this communication, say, for further use of eavesdropped information to obstruct the control center's operation. The eavesdropping's technical characteristics might be such that it has restricted eavesdropping capability, i.e., the adversary may not be able to eavesdrop on all of the nodes at once. In this case the adversary changes from a passive adversary to an active one, since to eavesdrop effectively it must select which node (or, equivalently, channel) to eavesdrop upon. Then, if the adversary selects the same node to eavesdrop, say, node i, $i \in \mathcal{N} \triangleq \{1, \ldots, n\}$, that transmitter also selects to communicates with, then the secrecy rate [10] of the communication is given as follows:

$$\mathbb{CS}_i = \max\left\{\ln\left(1 + h_i P/\sigma_i^2\right) - \ln\left(1 + h_{Ei} P/\sigma_{Ei}^2\right), 0\right\}, \quad (1)$$

where P is the power level applied by the transmitter, h_i is the main channel gains between the transmitter and node i, and h_{Ei} is the eavesdropping channel gains between node i and the adversary, σ_i^2 and σ_{Ei}^2 are the corresponding background noise power levels (Fig. 1). Note that to maintain secret communication, the transmitter has to eliminate channels, which do not correspond such goal, i.e., any channel i such that $\mathbb{CS}_i = 0$.

That is why, without loss of generality, by (1), we consider only such channels that the following inequalities hold:

$$h_i/\sigma_i^2 > h_{Ei}/\sigma_{Ei}^2, \quad i \in \mathcal{N}. \tag{2}$$

A transmitter strategy is a vector of probabilities $x = (x_1, \ldots, x_n)$, where x_i is the probability of selecting node i to communicate with. An adversary strategy is a vector of probabilities $y = (y_1, \ldots, y_n)$, where y_i is the probability of selecting node i to eavesdrop upon. Using probabilities can be motivated by considering communication as a repeated process [12]. Then, the probabilities reflect frequencies with which transmitter communicates with nodes and the adversary eavesdrops upon them.

By (1) and (2), the expected secrecy rate, if the transmitter and adversary apply strategies x and y, respectively, is:

$$\mathbb{CS}(x, y) = \sum_{i \in \mathcal{N}} \Big(\ln(1 + h_i P/\sigma_i^2) - \ln(1 + h_{Ei} P/\sigma_{Ei}^2) y_i \Big) x_i. \tag{3}$$

Meanwhile, the expected "eavesdroppable" rate is:

$$v_A(x, y) = \sum_{i \in \mathcal{N}} \ln(1 + h_{Ei} P/\sigma_{Ei}^2) x_i y_i. \tag{4}$$

Traditionally, in secrecy communication problems, the transmitter has only the goal of maximizing its secrecy rate, while, the adversary wants to minimize it, or, equivalently, to maximize "eavesdroppable" rate.

III. Sophisticated Transmitter

The (sophisticated) transmitter wants to find a trade-off between two goals: (i) the basic one, to maximize the secrecy rate, and (ii) the secondary one, to achieve such secret communication in the most unpredictable way for the adversary. As a metric for the transmitter to confuse the adversary, we consider the Shannon entropy [13] of its strategy. Recall that the Shannon entropy, also known as information entropy for a random variable, in our case probability vector x, i.e., transmitter's strategy, reflects the average level of uncertainty inherent in its possible outcomes (the nodes selected to communicate to), and formally defined as:

$$H(x) = -\sum_{i \in \mathcal{N}} x_i \ln(x_i). \tag{5}$$

Here larger entropy reflects higher uncertainty about which node is selected by the transmitter to communicate to, or, equivalently, higher uncertainty for the adversary about the transmitter's choice. Maximal uncertainty is achieved for the uniformly distributed strategy. The payoff for such a transmitter is taken as a weighted sum of the entropy of its strategy and the expected secrecy rate, i.e.,

$$v_T(x, y) = w_T \mathbb{CS}(x, y) + w_E H(x), \tag{6}$$

where w_T and w_E are non-negative weighting coefficients.

The ratio $r_E \triangleq w_E/(w_E + w_T)$, operationally, reflects the uncertainty level implemented by the transmitter in its communication strategy, where $r_E = 1$ and $r_E = 0$ correspond maximal and minimal uncertainty levels, respectively.

Note that by introducing auxiliary notation we can present payoffs $v_T(x, y)$ and $v_A(x, y)$ in the following compact form:

$$v_T(x, y) = w_T \sum_{i \in \mathcal{N}} x_i (A_i - B_i y_i) - w_E \sum_{i \in \mathcal{N}} x_i \ln(x_i), \tag{7}$$

$$v_A(x, y) = \sum_{i \in \mathcal{N}} B_i x_i y_i, \tag{8}$$

where

$$A_i = \ln\Big(1 + h_i P/\sigma_i^2\Big), \; B_i = \ln\Big(1 + h_{Ei} P/\sigma_{Ei}^2\Big), \; i \in \mathcal{N}. \tag{9}$$

By (2) and (9), we have that

$$A_i > B_i, \quad i \in \mathcal{N}. \tag{10}$$

We look for a Nash equilibrium. Recall that (x, y) is a Nash equilibrium if and only if, for each pair of feasible strategies $(\tilde{x}, \tilde{y})$, the following inequalities hold:

$$v_T(\tilde{x}, y) \le v_T(x, y) \text{ and } v_A(x, \tilde{y}) \le v_A(x, y). \tag{11}$$

Denote this non-zero sum game by Γ.

Proposition 1: In the game Γ there exists at least one equilibrium.

Proof: By (8), $v_A(x, y)$ is linear on y. Meanwhile, by (7), $v_T(x, y)$ is an additively separable function of x_i, $i \in \mathcal{N}$ such that $\partial v_T^2(x, y)/\partial x_i^2 = -w_E/x_i < 0$. Thus, $v_T(x, y)$ is concave in x, and the result follows from Nash's theorem [12] since the set of feasible strategies for each player is compact. ∎

Further, we find equilibrium strategies in closed form using a constructive approach by solving the best response equations. Recall that, by (11), (x, y) is a Nash equilibrium if and only if each of these strategies is the best response to the other, i.e., (x, y) is

$$x = \underset{x}{\operatorname{argmax}}\, v_T(x, y), \tag{12}$$

$$y = \underset{y}{\operatorname{argmax}}\, v_A(x, y). \tag{13}$$

Note that (12) is a Non-Linear Programming (NLP) problem, meanwhile (13) is a Linear Programming (LP) problem.

IV. Explicit Form for the Equilibrium Strategies

In this section we derive the solution of the best response equations (12) and (13) as functions of the two auxiliary parameters ω and ν. The intuition beyond these parameters is: ν is the Lagrange multiplier for the NLP problem (12) and ω is the maximal "eavesdroppable" rate.

Proposition 2: In the game Γ, each pair of equilibrium strategies $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ for the transmitter and adversary, respectively, must have the following form:

$$x_i = x_i(\omega, \nu) \triangleq \begin{cases} e^{\frac{A_i w_T}{w_E} - 1 - \frac{\nu}{w_E}}, & i \in I_0(\omega, \nu), \\ \frac{\omega}{B_i}, & i \in I(\omega, \nu) \end{cases} \tag{14}$$

and

$$y_i = y_i(\omega,\nu) \triangleq \begin{cases} 0, & i \in I_0(\omega,\nu), \\ \frac{w_T A_i - w_E \ln\left(\frac{\omega}{B_i}\right) - \omega_E - \nu}{w_T B_i}, & i \in I(\omega,\nu), \end{cases} \quad (15)$$

where

$$I_0(\omega,\nu) \triangleq \left\{ i \in \mathcal{N} : B_i e^{\frac{A_i w_T}{w_E} - 1} \le \omega e^{\frac{\nu}{w_E}} \right\}, \quad (16)$$

$$I(\omega,\nu) \triangleq \left\{ i \in \mathcal{N} : B_i e^{\frac{A_i w_T}{w_E} - 1} > \omega e^{\frac{\nu}{w_E}} \right\}. \quad (17)$$

Moreover, the parameters ω and ν are solutions of the following equations

$$X(\omega,\nu) \triangleq \sum_{i\in\mathcal{N}} x_i(\omega,\nu) = 1, \quad (18)$$

$$Y(\omega,\nu) \triangleq \sum_{i\in\mathcal{N}} y_i(\omega,\nu) = 1 \quad (19)$$

such that the following conditions hold

$$\omega \in (0, \overline{B}] \text{ and } \nu \ge w_T \underline{D} - w_E \quad (20)$$

with

$$\overline{B} \triangleq \max_{i\in\mathcal{N}} B_i \text{ and } \underline{D} \triangleq \min_{i\in\mathcal{N}} (A_i - B_i). \quad (21)$$

Proof: By (8), (13) is a LP problem, and the adversary's feasible strategy $\boldsymbol{y}$ is the best response to a fixed transmitter's strategy $\boldsymbol{x}$ if and only if there is an ω such that

$$y_i \begin{cases} \ge 0, & B_i x_i = \omega, \\ = 0, & B_i x_i < \omega. \end{cases} \quad (22)$$

By (7), (12) is a NLP problem. To find the transmitter's best response $\boldsymbol{x}$ to a fixed adversary's strategy $\boldsymbol{y}$ we introduce the Lagrangian $\mathcal{L}_\nu(\boldsymbol{x})$ with ν is the Lagrange multiplier as follows:

$$\mathcal{L}_\nu(\boldsymbol{x}) = v_T(\boldsymbol{x},\boldsymbol{y}) + \nu\left(1 - \sum_{i\in\mathcal{N}} x_i\right). \quad (23)$$

Then, the transmitter's strategy $\boldsymbol{x}$ is the best response to the adversary's strategy $\boldsymbol{y}$ if and only if the following condition holds:

$$\frac{\partial \mathcal{L}_\nu(\boldsymbol{x})}{\partial x_i} = w_T(A_i - B_i y_i) - w_E - w_E \ln(x_i) - \nu \begin{cases} = 0, & x_i > 0, \\ \le 0, & x_i = 0. \end{cases} \quad (24)$$

By (24), we have that

$$x_i > 0, \quad i \in \mathcal{N}. \quad (25)$$

This, jointly with (24), implies that

$$w_T(A_i - B_i y_i) - w_E - w_E \ln(x_i) = \nu, \quad i \in \mathcal{N}. \quad (26)$$

By (22) and (26), we have that ω and ν, respectively, must be such that (20) holds.

By (25), only two cases arise to consider separately: (a) $y_i = 0$ and (b) $y_i > 0$.

(a) Let $y_i = 0$. Substituting such y_i into (22) and (26) imply, respectively, the following relations:

$$B_i x_i \le \omega \quad (27)$$

and

$$w_T A_i - w_E - w_E \ln(x_i) = \nu. \quad (28)$$

Solving (28) by x_i implies

$$x_i = \exp(A_i w_T/w_E - 1 - \nu/w_E). \quad (29)$$

Substituting (29) into (27) implies

$$B_i \exp(A_i w_T/w_E - 1 - \nu/w_E) \le \omega. \quad (30)$$

Thus, the assumption that $y_i = 0$ jointly with (29) and (30) imply the first rows in (14) and (15) with $I_0(\omega,\nu)$ given by (16).

(b) Let $y_i > 0$. Substituting such y_i into (22) implies

$$B_i x_i = \omega. \quad (31)$$

Thus, $x_i = \omega/B_i$. Substituting such x_i into (26) implies:

$$w_T B_i y_i = w_T A_i - w_E - w_E \ln(\omega/B_i) - \nu. \quad (32)$$

Substituting lower bound for y_i, i.e., $y_i = 0$, into (32) implies

$$w_T A_i - w_E - w_E \ln(\omega/B_i) - \nu > 0. \quad (33)$$

Finally, (31)-(33) imply the second rows in (14) and (15) with $I(\omega,\nu)$ given by (17). ■

V. Auxiliary Results

In this section we establish auxiliary monotonicity properties of the functions $X(\omega,\nu)$ and $Y(\omega,\nu)$, which allows us to prove the uniqueness of the equilibrium in the game Γ, as well as to derive an algorithm to find this equilibrium.

Proposition 3: The functions $X(\omega,\nu)$ and $Y(\omega,\nu)$ have the following properties:

(a) Function $Y(\omega,\nu)$ is continuous in both parameters ω and ν. Moreover, it is decreasing on both parameters while $Y(\omega,\nu)$ is positive.

(b) Function $X(\omega,\nu)$ is continuous in both parameters ω and ν. Moreover, it is increasing in ω and it is decreasing in ν.

(c) For each fixed ω there is the unique $\mathbb{N}(\omega)$ such that

$$Y(\omega,\mathbb{N}(\omega)) = 1. \quad (34)$$

Such $\mathbb{N}(\omega)$ can be found via the bisection method.

(d) Function $\mathbb{N}(\omega)$ is continuous and decreasing in ω.

(e) Function $X(\omega,\mathbb{N}(\omega))$ is continuous and increasing in ω.

(f) There is the unique root $\omega_* \in (0,\overline{B})$ of equation

$$X(\omega,\mathbb{N}(\omega)) = 1. \quad (35)$$

This root can be found via the bisection method.

Proof: First note that (15)-(17) and (19) imply (a). Similarly, (b) follows from (14) and (16)-(18). Then, (c) follows from (a). Meanwhile, (d) follows from (a) and (c). Finally, (b) and (d) imply (e). Meanwhile, (f) follows from (20) and (e). ■

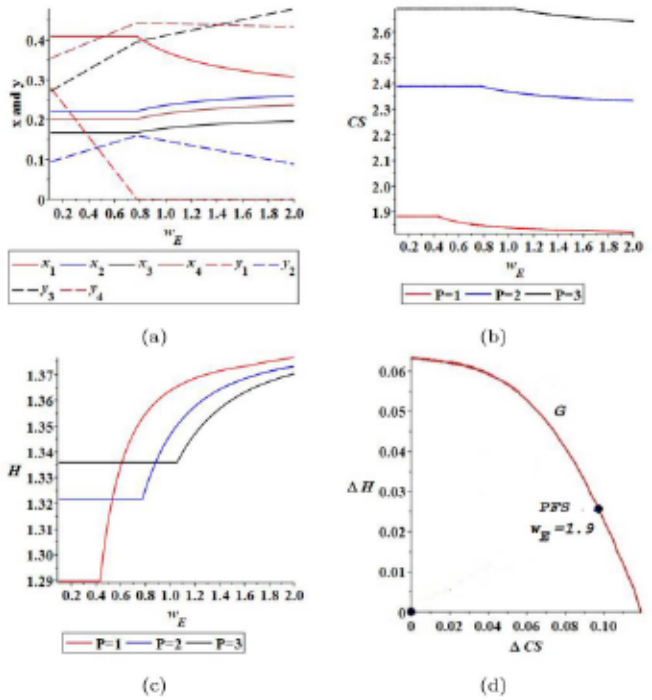

Fig. 2. (a) Equilibrium strategies, (b) secrecy rate, (c) entropy of transmitter's strategies as functions on w_E and (d) proportional fair solution.

VI. Uniqueness of Equilibrium

In this section we establish the uniqueness of the equilibrium and give it in closed form.

Theorem 1: In the game Γ, the Nash equilibrium is unique. Moreover, this unique equilibrium (x, y) is given as follows:

$$x = x(\omega_*, \mathbb{N}(\omega_*)) \text{ and } y = y(\omega_*, \mathbb{N}(\omega_*)), \tag{36}$$

where the vector-value functions $x(\omega, \nu)$ and $y(\omega, \nu)$ are given by Proposition 2, meanwhile the function $\mathbb{N}(\omega)$ and the unique value ω_* are given by Proposition 3.

Proof: The result follows directly from Proposition 2 and Proposition 3. ■

VII. Numerical Illustration

To illustrate how the equilibrium strategies in Theorem 1 depend on the weighting coefficients of the transmitter's payoff let us consider an example involving $n = 4$ nodes with main channel gains $h = (7.1, 5.9, 9.8, 10.6)$, eavesdropping channel gains $h_E = (0.9, 2.85, 5.7, 3.53)$, background noises $\sigma^2 = \sigma_E^2 = (1, 1, 1, 1)$, weighting coefficient $w_T = 1$ and implemented power level $P = 2$ by the transmitter.

Fig. 2(a) illustrates that the adversary's strategy is more sensitive to varying the weighting coefficient w_E than the transmitter's strategy. Smaller sensitivity of the transmitter's strategy is reflected by flat segments that arise for small weighting coefficient w_E, specifically, $w_E \leq 0.77$ when the set $I_0(\omega, \nu)$ becomes empty (see, Eqn. (14)). In this case, by (14), $x_i = 1/(\sum_{j\in\mathcal{N}}(B_i/B_j))$, $i \in \mathcal{N}$, i.e., $x = (0.41, 0.22, 0.17, 0.20)$ while $I_0(\omega_0, \nu)$ is empty with $\omega_0 = 1/(\sum_{j\in\mathcal{N}}(1/B_j)) = 0.42$. An increase in weighting coefficient w_E implies that the transmitter's strategy tends to a uniformly distributed strategy, i.e., the one with maximal entropy. Meanwhile, the adversary tends to focus eavesdropping efforts on the node with the maximal "eavesdroppable" rate, i.e., on node 3. Fig. 2(b) and Fig. 2(c) illustrate that an increase in power level by the transmitter leads to an increase in the upper-bound on the weighting coefficient w_E, where the transmitter's strategy is non-sensitive to such coefficient w_E. Also, the secrecy rate is non-increasing with respect to weighting coefficient w_E while the entropy is non-decreasing on this coefficient.

VIII. Optimization of Weighting Coefficients via Fairness Approach

In the previous section it was shown that an increase in the weighting coefficient w_E leads to an increase in the entropy of the transmitter's strategy and a decrease in the secrecy rate. Thus, a question arises: which weighting coefficient w_E is preferable for the transmitter to maintain both of the transmitter's goals: (a) the basic one, to communicate secretly, and (b) the secondary one, to do it the most unpredictable way? Note that, without loss of generality, we can assume that w_T is fixed since the transmitter's payoff (7) is a linear function of weighting coefficients (w_T, w_E).

We now show how proportional fairness [14] can be applied to find such trade-off between both transmitter's goals.

First, let us denote by x_{w_E} and y_{w_E}, the equilibrium strategies of the transmitter and adversary, respectively, parameterized by weighting coefficient w_E and given by Theorem 1. By Theorem 1, for w_E tending to infinity we have that the transmitter's strategy tends to a uniformly distributed one $x_\infty = (x_{1,\infty}, \ldots, x_{n,\infty}) = (1/n, \ldots, 1/n)$, which corresponds the maximum of entropy. Also, the adversary's strategy tends to $y_\infty = (y_{1,\infty}, \ldots, y_{n,\infty})$ such that $y_{i,\infty} = 1$ for such an i where B_i achieves its maximum, i.e., such i that $B_i = \overline{B}$ with $\overline{B}$ given by (21). Meanwhile, $y_{j,\infty} = 0$ for $j \neq i$. For the lower-boundary case of weighting coefficient w_E, i.e., $w_E = 0$, we have that the adversary's strategy $y_0 = (y_{1,0}, \ldots, y_{n,0})$ has a water-filling form. Specifically, $y_{i,0} = \max\{(A_i - \tilde{\nu})/B_i, 0\}$, $i \in \mathcal{N}$, where $\tilde{\nu}$ is the uniquely given by the condition that y_0 is a probability vector, i.e., $\sum_{i\in\mathcal{N}} \max\{(A_i - \tilde{\nu})/B_i, 0\} = 1$. Also, the transmitter's strategy is $x_{i,0} = 1/\sum_{j:A_j>\tilde{\nu}}(B_i/B_j)$ for $A_i > \tilde{\nu}$ and $x_{i,0} = 0$ for $A_i \leq \tilde{\nu}$ with $i \in \mathcal{N}$.

Let $\mathbb{CS}_{w_E} \triangleq \mathbb{CS}(x_{w_E}, y_{w_E})$ be the secrecy rate if the transmitter and adversary implement strategies x_{w_E} and y_{w_E}, respectively. Meanwhile, let $H_{w_E} \triangleq H(x_{w_E})$ be entropy of the transmitter's strategy x_{w_E}. The basic objective of the transmitter to increase secrecy rate can be modeled by the difference between current secrecy rate $\mathbb{CS}_{w_E}$ and the secrecy rate corresponding the strategy with the maximal entropy (i.e., the one when the transmitter focuses its efforts only on an increase in entropy), i.e., by the following payoff as function of w_E:

$$\Delta\mathbb{CS}_{w_E} = \mathbb{CS}_{w_E} - \mathbb{CS}_\infty. \tag{37}$$

The secondary objective of the transmitter to make its communication unpredictable can be modeled by the difference

between the current entropy H_{w_E} and the entropy H_0, when the transmitter focuses its efforts only on an increase in the secrecy rate, i.e., by the following payoff as function of w_E:

$$\Delta H_{w_E} = H_{w_E} - H_0. \tag{38}$$

Now we can introduce the set of all possible pair of transmitter's payoffs, i.e.,

$$G \triangleq \{(\Delta \mathbb{CS}_{w_E}, \Delta H_{w_E}) : w_E \geq 0\}. \tag{39}$$

This set is illustrated in Fig. 2(d) by the example considered in the previous section with implemented power level $P = 2$. Then, the trade-off weighting coefficient w_E via proportional fairness [14] as criteria can be found as the solution of the following optimization problem:

$$\max\{\ln(\Delta \mathbb{CS}_{w_E}) + \ln(\Delta H_{w_E}) : w_E \geq 0\}. \tag{40}$$

Solution of this optimization problem, i.e., proportional fair solution (PFS), can be found via the Nelder-Mead simplex algorithm [15]. In the considered example, it is $w_E = 1.9$, which corresponds to trade-off values of secrecy rate and entropy being equal to 2.33 and 1.37, respectively.

IX. Conclusion

In this letter, a new type of transmitter has been modeled, specifically, a sophisticated transmitter that has to communicate with a group of nodes allocated in a security zone in the presence of an adversary aimed at eavesdropping upon this communication. The sophisticated transmitter, beyond the basic goal of communicating secretly, also has a secondary goal to achieve such secret communication in the most unpredictable way. This scenario has been modeled by a non-zero sum resource allocation game. The expected secrecy rate has been used as payoff to model the transmitter's basic goal. Meanwhile, the entropy of the transmitter's strategy has been implemented as a payoff to model the transmitter's secondary goal. The equilibrium has been found in closed form, and its uniqueness has been proven. A higher level of sensitivity for the adversary's strategy with respect to network parameters compared to the transmitter's strategy has been established. The proven uniqueness of the equilibrium demonstrates the stability of the suggested transmission algorithm. Finally, the parameters of the transmitter's utility supporting its basic and secondary goals were optimized via a proportional fairness approach.

References

[1] L. Yin and H. Haas, "Physical-layer security in multiuser visible light communication networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 1, pp. 162–174, Jan. 2018.

[2] F. Tian *et al.*, "Secrecy rate optimization in wireless multi-hop full duplex networks," *IEEE Access*, vol. 6, pp. 5695–5704, 2018.

[3] A. Garnaev and W. Trappe, "Secret communication when the eavesdropper might be an active adversary," in *Multiple Access Communications (MACOM)* (Lecture Notes in Computer Sciences, 8715), M. Jonsson, A. Vinel, B. Bellalta, and E. Belyaev, Eds. Cham, Switzerland: Springer, 2014. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-10262-7_12#citeas

[4] X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Trans. Commun.*, vol. 65, no. 3, pp. 1379–1395, Mar. 2017.

[5] A. Mukherjee and and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[6] Z. Feng *et al.*, "Power control in relay-assisted anti-jamming systems: A Bayesian three-layer Stackelberg game approach," *IEEE Access*, vol. 7, pp. 14623–14636, 2019.

[7] K. Wang, L. Yuan, T. Miyazaki, Y. Chen, and Y. Zhang, "Jamming and eavesdropping defense in green cyber–physical transportation systems using a Stackelberg game," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4232–4242, Sep. 2018.

[8] A. Garnaev, M. Baykal-Gursoy, and H. V. Poor, "A game theoretic analysis of secret and reliable communication with active and passive adversarial modes," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2155–2163, Mar. 2016.

[9] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in MIMO channels," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2010, pp. 1695–1700.

[10] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Basar, "Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2011, pp. 119–124.

[11] H. Pang, L. Xu, Y. Zou, X. Wang, and K.-K. R. Choo, "Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10788–10799, Nov. 2018.

[12] G. Owen, *Game Theory*. New York, NY, USA: Academic, 1982.

[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY, USA: Wiley, 1991.

[14] I. Ahmed, A. Mohammed, and H. Alnuweiri, "On the fairness of resource allocation in wireless mesh networks: A survey," *Wireless Netw.*, vol. 19, no. 6, pp. 1451–1468, 2013.

[15] J. C. Lagarias, J. A. Reeds, M. H. Wright, and P. E. Wright, "Convergence properties of the Nelder–Mead simplex method in low dimensions," *SIAM J. Optim.*, vol. 9, no. 1, pp. 112–147, 1998.