View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Archivio istituzionale della ricerca - Università di Padova

UNIVERSITÀ DEGLI STUDI DI PADOVA

Università degli Studi di Padova

Padua Research Archive - Institutional Repository

A Game of One/Two Strategic Friendly Jammers Versus a Malicious Strategic Node

Original Citation:

Availability:
This version is available at: 11577/3300448 since: 2019-05-09T10:58:55Z

Publisher:

Published version:
DOI: 10.1109/LNET.2019.2893536

Terms of use:
Open Access

This article is made available under terms and conditions applicable to Open Access Guidelines, as described at http://www.unipd.it/download/file/fid/55401 (Italian only)

(Article begins on next page)

A Game of One/Two Strategic Friendly Jammers versus a Malicious Strategic Node

Leonardo Badia, *Senior Member, IEEE,* Francesco Gringoli, *Senior Member, IEEE*

***Abstract*—We present a game-theoretic analysis of the interaction between a malicious node, attempting to perform unauthorized radio transmission, and friendly jammers trying to disrupt the malicious communications. We investigate the strategic behavior of the jammers against a rational malicious node and highlight counterintuitive results for this conflict. We also analyze the impact of multiple friendly jammers sharing the same goal but acting without coordination; we find out that this scenario offers a better payoff for the jammers, which has some strong implications on how to implement friendly jamming.**

***Index Terms*—Friendly jamming; network security; wireless LAN; game theory.**

I. Introduction

FREQUENCY jamming, usually performed to disrupt wireless communications, can also be used for good, namely to block unauthenticated transmissions, such as injection attacks; this is often referred to as *friendly jamming* [1]. We analyze the scenario of a local wireless network, e.g., in a campus or a public premise, challenged by a malicious node, whose activity can jeopardize network operation or whose radio access is forbidden: think of a student communicating to cheat during exams. To block it, the network dispatches one or more friendly jammers that reactively look for forbidden frames and jam their payloads [2]. The effectiveness of the friendly jammers depends on many aspects, such as their ability to monitor the channel, frequency hopping patterns, synchronization issues, and so on [3]. They also have multiple ways to disrupt unauthorized communications, e.g., jamming data packets or interfere with the reception of acknowledgments [4]. We abstract from all these elements and just consider an average success / failure rate of the jamming.

We frame the resulting conflict as an *Entry game*, a setup often used in economic scenarios, e.g., the telecommunication market [5]. Our goal is to infer results for effective security techniques, and prompt for extensions in practical contexts. First, we derive the mixed strategy Nash equilibrium of the entry game in closed form. One unexpected conclusion involves the dependences on the transmission cost, assumed identical for the jammer and the malicious node, and the reward that the latter gets for a successful attack. The frequency of attacks is proportional to the transmission cost, while the jamming probability decreases with it. Conversely, a higher reward leads to lower attack and higher jamming probabilities. These exploits stem from the strategic behavior of the players and will be discussed and justified. It is also noted that the jammer obtains a strictly negative average payoff.

Moreover, we consider *two* friendly jammers with the same purpose of defeating the attacker but also being strategic and uncoordinated, i.e., each may prefer to save the transmission cost and let the unwarranted transmissions be jammed by the other [6]. We derive the Nash equilibrium in closed form, with the interesting twist that the transmission cost term is now replaced by the square root of the transmission cost times the reward for a successful attack. As a result, the probability of malicious transmissions is increased, while the jamming probability is decreased. In addition, while the previous scenario was not strategically sustainable for the jammers due to a negative payoff, the one with multiple jammers might be, as long as the transmission cost is limited (as a rule of thumb: at most 20% of the reward for a successful jamming).

II. Related Work

A long-standing branch of research focuses on friendly jamming, mostly aimed at its implementation. For instance, [2] analyzed friendly jamming in wireless LANs, and [3] demonstrated the ease of implementation of friendly jamming with off-the-shelf smartphones. A proper signal design may be used to scramble only malicious transmissions but be harmless against legitimate ones [7]. In our scenario, jammers interact with the malicious node only; hence, we assume that they just increase the noise floor to lower channel capacity [8]. We do not deal with implementation details, nor we distinguish between different kinds of jamming, as exhaustively done in [4]; these are possible extensions for future work.

Other contributions [1], [9], [10] use game theory to study jamming problems, since they involve multiple players (usually limited in number) with different objectives and acting without coordination, and it is relatively easy to quantify the outcomes [9]. This last paper also offers a detailed discussion on how to evaluate game theoretic payoffs related to the quality of service of the network under jamming, so the reader is referred to it as a complement of our analysis in this sense.

Other studies [1] consider incentives for the jammers to contribute to network security against eavesdropping, e.g., as a bargain between the network and volunteering friendly jammers. The network negotiates incentives to support information secrecy and defeat the eavesdroppers [10]. Thus, jammers benefit from contributing to security purely based on their own utility. Yet, in these studies the malicious node is not strategic and does not react to the strategic jammers.

Manuscript received ....
##########################

L. Badia is with DEI, Dept. of Information Engineering, University of Padova, Italy. E-mail: leonardo.badia@unipd.it.

F. Gringoli is with DII, Dept. of Information Engineering, University of Brescia, Italy. E-mail: francesco.gringoli@unibs.it.

TABLE I
MAIN SYSTEM PARAMETERS

Parameter	Symbol
Transmission cost for all nodes	c
Reward for successful malicious transmission	r
Failure probability of jamming action	f
Benefit for successful jamming action	set to 1

Instead, we consider the malicious node as a concerned third party, i.e., a strategic player that makes decisions as best responses [8]. Another difference with the literature is that we also consider multiple uncoordinated jammers. This is akin to [6], where many agents acting toward a common goal, but without coordination and driven by strategic interests, were shown to suffer a limited efficiency loss; yet, this may no longer hold when their task involves a strategic adversary. All these differences justify our novel analysis.

III. Game Theoretic Analysis, One Jammer

Consider a complete information game between a network agent N and a malicious node M. The latter wants to perform unauthorized radio communications, whereas the former monitors the channel looking for unwarranted transmissions, and tries to prevent M's from communicating and/or increase the airtime for the legitimate nodes of an enterprise network. Thus, N acts as a *reactive friendly jammer* [3], and it is sensible to assume complete information, meaning that both players are mutually aware of each other and their objectives.

We formulate a static (one-shot) game that concentrates the strategic interplay in one interaction. In a static game, players separately choose their only move, which avoids synchronization issues [2]. A static game is generally the first building block of more advanced formulations, such as multiple interactions studied as repeated games [11]; however, this requires a discussion on the activity/frequency hopping pattern of the transmitter, and what does the jammer know about it. Extensions through Bayesian games [6] would allow for players being uncertain of each other's presence, or having multiple objectives, such as transmitters being in a variable number and/or performing both legitimate and malicious activity, or jammers choosing between just disrupting communications or detecting malicious nodes first [12]. All these studies are left for future work beyond the present investigation.

The values in Table I, set as generic parameters, are common knowledge among the players; one can follow [9] for their exact quantification. We denote as c the cost spent for transmitting, assumed identical for both players, as their transmitters likely use a similar circuitry, e.g., a standard WiFi card, possibly purposely programmed for jamming. We reckon that N's jamming may be unsuccessful; we abstract its average failure rate with probability f. As argued before, f accounts for all technical aspects related to jamming success or failure.

Also, we set a *reward* for node M, denoted as r, earned if its malicious actions succeed. This value reflects the incentive for M to transmit, despite being aware that it can be jammed, in which case it will just pay cost c. Similarly, we consider the returning utility for the friendly jammer, and we assume that whenever M is successful and gains r, player N suffers a loss of the same amount [8]. By contrast, the *benefit* for stopping the malicious actions of player M is in principle a different quantity, which can even be the outcome of a game theoretic bargain between the network administrator and the friendly jammers [10]. Without loss of generality, and for the sake of a simpler notation, we set this value to 1; changing it would be equivalent to rescale all the other values.

TABLE II
NORMAL-FORM (PAYOFF MATRIX) OF GAME $\mathcal{J}_1$

		Malicious node M: **E**	Malicious node M: **O**
Network agent N	**J**	$(1-f)-fr-c,\ fr-c$	$-c,\ 0$
	A	$-r,\ r-c$	$0,\ 0$

The interaction between N and M is set as a static entry game $\mathcal{J}_1$ of complete information [5]. This is a potential foundation for extensions e.g., to Bayesian or dynamic games [6], [9], which are left for future work. We assign two available actions to both players, which allows for a closed form solution. The malicious node M can *enter* (action denoted as **E**), that is, to perform unwarranted transmission, or stay out (action **O**), i.e., to feign transmission but actually avoid it; this is the correct action if M believes that the friendly jamming is active. In practice, node M enacts a probabilistic mixture of these two actions, which quantify its *transmission probability*. Similarly, N can friendly jam (action **J**) or abstain from it, e.g., to save energy (action **A**). The mixing of these actions results in the *jamming probability*. This setup is akin to others in the field of security: it is worth mentioning that the sole presence of the legitimate player as a watchdog (even not taking any actual countermeasure) may deter the malicious player from entering.

Players independently choose their strategies, which jointly determine their payoffs: for strategy pair (n, m), player $\mathtt{X}\in\{\mathtt{N},\mathtt{M}\}$ gets $u_{\mathtt{X}}(n, m)$. Table II shows the normal form of $\mathcal{J}_1$. In more detail, whenever M stays out, its payoff is 0. If it enters, its payoff has a $-c$ term and depends on the jamming outcome. If N is not jamming, then M gets a reward r. Since N's jamming fails with probability f, outcome (**J**,**E**) results in N and M earning $(1-f)-fr-c$ and $fr-c$, respectively. [1]

Table II requires this sensibility condition: $fr \leq c \leq r$. If either side is violated, M's action is obvious, as **E** or **O** are dominant strategies, respectively. It must also hold that

$$f \leq \frac{1+r-c}{1+r} \tag{1}$$

or jamming is too rarely successful and N always plays **A**.

Under these conditions, $\mathcal{J}_1$ has no pure strategy Nash equilibria, thus it must exist an equilibrium in mixed strategies, as per the Nash theorem [11], where N plays **J** with probability j and **A** with probability $1-j$, while M mediates between **E** and **O** with probabilities ε and $1-\varepsilon$, respectively.

Theorem 1: To derive j and ϵ in closed form, impose $\mathbb{E}[u_{\mathtt{N}}(0,\varepsilon)]=\mathbb{E}[u_{\mathtt{N}}(1,\varepsilon)]$ and $\mathbb{E}[u_{\mathtt{M}}(j,0)]=\mathbb{E}[u_{\mathtt{M}}(j,1)]$.

Proof: This result follows the *Indifference Principle* [11], which states that a player reaching a Nash equilibrium with a mixture of strategies x_1 and x_2 with respective probabilities

[1] These outcomes are accessible to both players. Indeed, the network can eavesdrop to the malicious transmission to see whether it was successful (e.g., acknowledgments are sent, or the packets sent progress forward).

ξ and $1-\xi$, $0<\xi<1$, achieves the same expected payoff by playing x_1 (or x_2) alone, i.e., $\xi=0$ (or $\xi=1$), if all other players do not change their strategies. ■

Hence, if $\mathtt{M}$ chooses transmission probability ε, $\mathtt{N}$ must have the same expected payoff when playing either **J** or **A**, thus

$$(1-f-fr-c)\varepsilon - c(1-\varepsilon) = -r\varepsilon \;\Rightarrow\; \varepsilon = \frac{c}{(1+r)(1-f)}. \quad (2)$$

and similarly

$$j = \frac{1-c/r}{1-f}, \quad \text{with } j \le 1 \text{ due to (1).} \quad (3)$$

These results closely relate with the strategic behavior of the players. If cost c increases, the malicious node becomes *more* active, since it is more expensive for the jammer to counteract the attacks, and this is common knowledge among the players. Also, the impact of reward r may seem surprising: the larger r, the lower the transmission probability ε and instead the higher the jamming probability j. The explanation is that the mixed strategy equilibrium sets indifference between the players' alternatives. Knowing that r is large, $\mathtt{N}$ prefers to pay the transmission cost and jam more often; thus, $\mathtt{M}$'s transmission probability decreases. Also, $\mathbb{E}[u_{\mathtt{M}}(j,\varepsilon)]=0$ because of the indifference with playing **O**, whereas for the jammer

$$\mathbb{E}[u_{\mathtt{N}}(j,\varepsilon)] = j\varepsilon(1+r)(1-f) - \varepsilon r - jc = \frac{-cr}{(1+r)(1-f)} \quad (4)$$

which is always negative; hence, $\mathtt{N}$ may arguably not find it sustainable to partake in the game with the only incentive being a benefit of $+1$ when $\mathtt{M}$ is successfully jammed.

IV. Game Theoretic Analysis, Two Jammers

The analysis can be extended to multiple friendly jammers. For tractability, we consider 2 jammers, but most of the implications can be qualitatively extended to a higher number. The game, now called $\mathcal{J}_2$, involves two friendly jammers $\mathtt{N}_1$ and $\mathtt{N}_2$, and malicious node $\mathtt{M}$. As before, the available actions are **J** and **A** for the jammers, **E** and **O** for the malicious node. The jammers act with the same purpose of disrupting transmissions from $\mathtt{M}$, but are also strategic in that they prefer to be inactive, and avoid paying the transmission cost, if the other is already successfully jamming. The jammers have the same transmission cost c, also identical to that of $\mathtt{M}$, and the same failure rate f. Actually, the latter may be questionable as success of jamming is strongly dependent, for example, on the positions of the nodes [2]. However, the value of f, which is common knowledge, represents an average estimate rather than the actual failure rate of a specific jamming instance. Thus, for the problem at hand it is sensible to have the same f for $\mathtt{N}_1$ and $\mathtt{N}_2$. Also, we assume they jam independently, so when both jammers are active the overall failure rate is f^2.

The payoffs for $\mathcal{J}_2$ can be extrapolated from $\mathcal{J}_1$ and the normal form expands to three dimensions; for visualization purposes, we split it in two according to the action of $\mathtt{N}_1$ and only show $\mathtt{N}_2$'s and $\mathtt{M}$'s payoffs; $\mathtt{N}_1$'s payoff is inferred by symmetry considerations. If $\mathtt{N}_1$ plays **A**, the game falls back to $\mathcal{J}_1$, as there is only one jammer ($\mathtt{N}_2$) that can contrast $\mathtt{M}$.

Table III shows payoffs $u_{\mathtt{N}_2}(n_1,n_2,m)$ and $u_{\mathtt{M}}(n_1,n_2,m)$. A mixed strategy Nash equilibrium exists, analogous to $\mathcal{J}_1$, but with more involuted equations involving 3 players. To solve

TABLE III
Payoff matrix of game $\mathcal{J}_2$, only players $\mathtt{N}_2$ and $\mathtt{M}$.

if Network agent $\mathtt{N}_1$ plays **J**:

		Malicious node $\mathtt{M}$: **E**	**O**
Network agent $\mathtt{N}_2$	**J**	$(1-f^2)-f^2r-c,\ f^2r-c$	$-c,\ 0$
	A	$(1-f)-fr,\ fr-c$	$0,\ 0$

if Network agent $\mathtt{N}_1$ plays **A**:
same payoffs of $\mathtt{N}_2$ and $\mathtt{M}$ as per game $\mathcal{J}_1$ (Table II)

in closed form, we exploit symmetry and assume that both jammers play **J** with the same probability j, while $\mathtt{M}$ transmits with probability ε. We set indifference for $\mathtt{M}$ in the expected payoffs $\mathbb{E}[u_{\mathtt{M}}]$ when playing **E** and **O** (the latter is 0), i.e.

$$j^2(f^2r-c) + 2j(1-j)(fr-c) + (1-j)^2(r-c) = 0 \quad (5)$$
$$\Rightarrow \Big(j(1-f)-1\Big)^2 - \frac{c}{r} = 0 \qquad \Rightarrow \quad j = \frac{1-\sqrt{c/r}}{1-f}$$

The difference from (3) is the square root term, due to the presence of two uncoordinated jammers. Compare it, e.g., with [6], where an analogous result was derived for two uncoordinated agents executing a task. Since $c/r \le 1$, replacing it with $\sqrt{c/r}$ implies a decrease in the jamming probability; both jammers are aware of each other's presence in the network and know they may restrain from intervening if the other is active. However, this reduced jamming rate is almost negligible if c is high, which apparently contrasts with immediate intuition. The explanation is again in the strategic behavior, as both jammers know that for high transmission cost it is less convenient to be active, which implies that the *other* jammer may stay inactive.

With analogous computations, ε at the equilibrium can be derived. The key is to assume $\mathtt{N}_1$ jamming with probability j, and $\mathtt{M}$ entering with probability ε. Applying Theorem 1 to $\mathtt{N}_2$, gives $\mathbb{E}[u_{\mathtt{N}_2}(j,0,\varepsilon)] = \mathbb{E}[u_{\mathtt{N}_2}(j,1,\varepsilon)]$ leading to

$$-c = f^2(1+r)\varepsilon j + f(1+r)\varepsilon - 2f(1+r)\varepsilon j - \varepsilon(1-j)(1+r)$$
$$\Rightarrow \varepsilon j(1+r)(1-f)^2 - \varepsilon(1+r)(1-f) + c = 0$$
$$\Rightarrow \varepsilon = \frac{c}{(1+r)(1-f)(1-j+jf)} \quad \Rightarrow \quad \varepsilon = \frac{\sqrt{cr}}{(1+r)(1-f)} \quad (6)$$

after exploiting (5). It is akin to (2) with $\sqrt{cr}$ replacing c.

The expected payoff of each jammer $\mathbb{E}[u_{\mathtt{N}}(j,j,\varepsilon)]$ is

$$\varepsilon - jc - \frac{c}{1-f}\Big(1-j(1-f)\Big)^2 = \frac{1}{1-f}\left(\frac{\sqrt{cr}}{1+r} - c\right) \quad (7)$$

which, remarkably, is positive if $c < r/(1+r)^2$. This implies that $\mathcal{J}_2$ has a threshold γ for the transmission cost allowing for a positive expected payoff for the jammers if $c<\gamma$. Since $\gamma = r/(1+r)^2$, it does not change much for $r \in [0.5, 2]$, being between $2/9 \approx 0.222$ and 0.25. In other words, if transmission cost c is about 5 times lower than the benefit of successful jamming, there exists a sustainable profit for the jammers, over a broad range of values for r. This result is significantly different from $\mathcal{J}_1$; it is also due to the fact that *both* jammers get the benefit when $\mathtt{M}$ is jammed, even if they are inactive. Indeed, this "money-for-nothing" gives a better appeal to the game from the jammer's standpoint and may hint at desirable

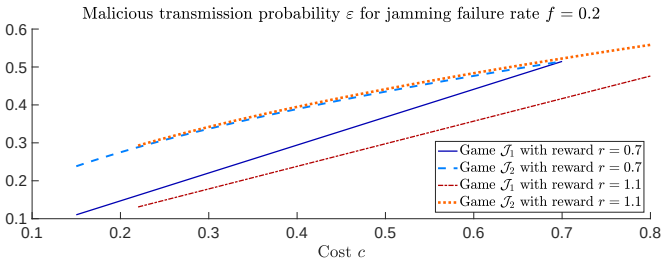

Fig. 1. Transmission probability ε vs. cost c.

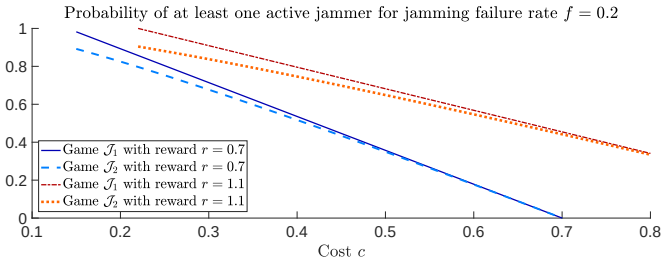

Fig. 2. Active jamming probability: j in $\mathcal{J}_1$, $2j-j^2$ in $\mathcal{J}_2$; vs. cost c.

design criteria for friendly jamming. However, the width of transmission cost values that are below threshold γ very much depends on the jamming failure rate f, since $fr < c$ and (1) must hold; this means that if f is too high, the problem is sensible only for values of c that are above threshold.

For visual aid, we report in Fig. 1 the transmission probability ε of the malicious node and in Fig. 2 the probability of at least one active jammer (equal to j for $\mathcal{J}_1$ and $2j-j^2$ for $\mathcal{J}_2$). The transmission probability of $\mathtt{M}$ increases with c, because the jamming probability decreases; thus, $\mathtt{M}$ is jammed less often, but gets a lower profit $r-c$ in these cases. Node $\mathtt{M}$ is also more aggressive in $\mathcal{J}_2$ than in $\mathcal{J}_1$. On one hand, in $\mathcal{J}_2$ the probability of being jammed is about the same as in $\mathcal{J}_1$, but the failure rate is lower when both jammers are active (f^2 instead of f); on the other hand, $\mathtt{M}$ can count on the lack of coordination among the jammers. A bigger reward r leads to a more frequent jamming in both $\mathcal{J}_1$ and $\mathcal{J}_2$; while this discourages the malicious node when facing a single jammer, in game $\mathcal{J}_2$ the opposite happens, and $\mathtt{M}$ transmits more often, relying on the lack of coordination of the jammers. Remarkably, r has little impact on the transmission probability ε in $\mathcal{J}_2$, since its dependence is through $\sqrt{r}/(1+r)$ that does not vary much in the considered range, as said before.

Finally, Fig. 3 shows the expected payoff of the jammers, which is always negative and decreasing in c and r for $\mathcal{J}_1$, while for $\mathcal{J}_2$ becomes positive in the narrow region with cost c below $\gamma = r/(1+r)^2$, and is impacted little by r.

V. Conclusions and Future Work

We formulated a friendly jamming problem in the context of game theory and we derived closed form solutions for its Nash equilibrium. We found interesting trends in the transmission probability of the malicious node as well as the jamming by the network agents. We further extended the conclusions to multiple uncoordinated jammers. In this scenario, despite an increased surveillance, the malicious node tries to transmit more often, relying on the lack of coordination among the

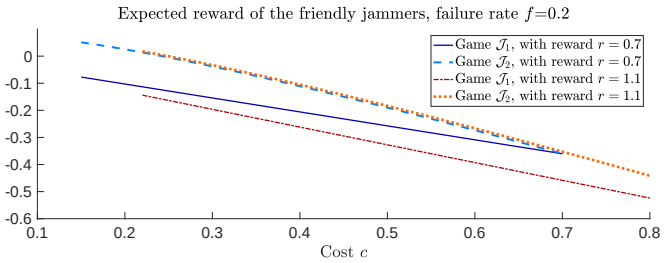

Fig. 3. Expected payoff of the friendly jammers vs. cost c.

jammers; however, security is better sustainable since the expected payoff of the jammers can be positive, as long as the transmission cost is below a threshold of 0.22–0.25 times the benefit of successful jamming over a broad range of values.

Some extensions are worth mentioning and currently under investigation. First, one may evaluate the parameters from a real application perspective. Moreover, we considered perfectly rational strategic players, immediately aware of the consequences of their actions; yet, within a practical jamming testbed [3], one may think of experiments to verify whether human players exhibit (game theoretic) rational behavior.

Finally, the formulation can be expanded. For example, the illegitimate transmitter may perform channel hopping [2], discontinued activity, or other sophisticated countermeasures to avoid being caught [4]. To do so, we can extend the problem toward *dynamic games* [9], where the game unfolds over multiple iterations, or *Bayesian games* [6], where players have different types. This goes beyond the scope of the present analysis, but may be considered in future investigations.

References

[1] H. Zhu, M. Ninoslav, M. Debbah, A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," *Proc. IEEE Gamenets*, 2009.

[2] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. B. Schmitt, "Friendly jamming on access points: Analysis and real-world measurements," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6189-6202, 2016.

[3] M. Schulz, F. Gringoli, D. Steinmetzer, M. Koch, and M. Hollick, "Massive reactive smartphone-based jamming using arbitrary waveforms and adaptive power control," *Proc. ACM WiSec*, pp. 111-121, 2017.

[4] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: a survey," *Int. J. Ad Hoc Ub. Comput.*, vol. 14, no. 4, pp. 197-215, 2014.

[5] F. Teng, D. Guo, and M. L. Honig, "Sharing of unlicensed spectrum by strategic operators," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 3, pp. 668-679, 2017.

[6] A. V. Guglielmi and L. Badia, "Bayesian game analysis of a queueing system with multiple candidate servers," *Proc. IEEE CAMAD*, 2015.

[7] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," *IEEE Symp. on Security and Privacy (SP)*, pp. 174-188, 2013.

[8] M. Scalabrin, V. Vadori, A. V. Guglielmi, and L. Badia, "A zero-sum jamming game with incomplete position information in wireless scenarios," *Proc. European Wireless*, 2015.

[9] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux,"Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, 2011.

[10] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134-145, 2013.

[11] M. Osborne, *An introduction to game theory*. Oxford Univ. Press, 2009.

[12] X. Liu, M. Dong, K. Ota, L. T. Yang, A. Liu, "Trace malicious source to guarantee cyber security for mass monitor critical infrastructure," *J. Comput. Syst. Sci.*, vol. 98, pp. 1-26, 2018.