Robust Nash Equilibria of Age of Incorrect Information Games in Cyber-Physical Systems

Valeria Bonagura*, Chiara Foglietta†, Federica Pascucci*, and Leonardo Badia§
* University of Roma 3, 00146 Rome, Italy. Email: bonagura@uniroma3.it
† San Raffaele Roma Open University, 00166 Rome, Italy. Email: chiara.foglietta@uniroma5.it
§ University of Padova, 35131 Padova, Italy. Email: leonardo.badia@unipd.it

***Abstract*—This paper studies the impact of uncertainty in the attacker's cost on equilibrium behavior in adversarial systems competing over the age of incorrect information (AoII). We consider a game-theoretic framework in which a defender and an attacker select their activity levels so as to respectively minimize and maximize AoII, while incurring linear costs. Unlike standard formulations, the attacker's cost is assumed to be uncertain and known only within a bounded interval, reflecting incomplete information about the adversary's capabilities. To address this uncertainty, we adopt a robust game-theoretic approach and characterize the resulting Robust Nash Equilibrium (RNE), where players optimize their strategies against worst-case parameter realizations. We derive structural properties of the equilibrium and provide insights into how uncertainty affects both players' strategies and system performance. Numerical results show that the robust formulation leads to more conservative strategies and highlights the sensitivity of the equilibrium to the attacker's cost. The proposed framework provides a tractable and practically relevant tool for the design of security mechanisms under incomplete information.**

***Index Terms*—Cyber-physical systems; False data injection; Markov processes; Age of incorrect information; Robust Nash equilibrium.**

I. Introduction

Robust Nash equilibrium (RNE) extends the classical Nash equilibrium (NE) concept to strategic environments in which players face uncertainty in payoff functions or system parameters. Although the standard NE assumes that all players have perfect knowledge of the game structure, many real-world systems are characterized by incomplete or uncertain information on costs, utilities, or environmental conditions [1]. Robust game theory addresses this limitation by allowing players to optimize their strategies against the worst-case realization of uncertain parameters within a prescribed uncertainty set. The early foundations of this approach can be traced to the development of robust optimization in operations research [2], which was subsequently extended to game-theoretic settings.

In [3], a formal treatment of robust games and the notion of RNE was introduced, where games with uncertain payoff matrices were analyzed, showing that equilibrium strategies can be obtained by solving tractable robust optimization problems. In this framework, each player selects a strategy that maximizes its worst-case payoff given the strategies of the others, thereby obtaining resiliency to modeling errors and parameter uncertainty.

RNEs have since been applied in a variety of domains where uncertainty plays a critical role [4]. In wireless and communication networks, robust formulations have been used to address resource allocation problems with uncertain channel gains or interference levels, enabling distributed algorithms that remain stable even when the system parameters fluctuate [5]. Similar ideas have been explored in transportation and energy networks, where users must make routing or consumption decisions under uncertain demand or supply conditions [6], [7]. In economic and engineering systems, more broadly, robust equilibrium concepts provide a systematic way to design decentralized decision mechanisms that maintain desirable performance despite imperfect information about the environment [8], [9]. These applications illustrate how robust game-theoretic models bridge the gap between traditional equilibrium analysis and the uncertainty-aware design principles commonly used in modern optimization.

The robust equilibrium paradigm is particularly appealing in the context of network security problems, where the behavior and capabilities of adversarial agents are often uncertain or only partially observable [10]. In security-oriented network games, such as jamming, denial-of-service, or intrusion scenarios [11]–[13], defenders typically lack precise knowledge of attacker resources, strategies, or system vulnerabilities. RNE provides a principled framework for capturing this uncertainty by enabling agents to compute strategies that remain effective under worst-case assumptions about adversarial actions [14].

As a result, robust game-theoretic models can contribute to the design of defensive policies that maintain performance guarantees even in adversarial environments, making them a promising tool for the analysis and control of secure communication networks and cyber–physical systems [15].

In this work, we consider a false data injection (FDI) setting for a cyber-physical system (CPS) [16], where a source node has the objective of providing monitoring data to a destination that can enact control actions. In this context, it is important that the updates sent are both timely and accurate, thus reflecting the time-changing nature of the system as closely as possible. The key indicator used to assess system performance is, therefore, the age of incorrect information (AoII) introduced in [17] to this end.

We assume that an attacker can inject false data into the system, increasing the discrepancy between the real state of the system and its knowledge about it at the destination. This model was already analyzed by the authors in [18] but under the assumption of complete knowledge of the parameters, in particular the attacker cost that is revealed to be the key parameter in the equilibrium determining a threshold effect.

In this contribution, we address the impact of uncertainty in the attacker's cost on the equilibrium behavior of this problem. In particular, we assume that the attacker cost is not known even as a probability distribution, but is only known to lie within a bounded interval. This type of uncertainty naturally arises in practical security scenarios, where the defender may have only partial knowledge of the attacker's capabilities or constraints [19].

To capture this aspect, we adopt a robust game-theoretic formulation and study the resulting RNE. Under this approach, players optimize their strategies against the worst-case realization of uncertain parameters. This leads to a conservative but practically meaningful solution concept, especially in security applications where underestimating the adversary may result in severe performance degradation. Compared to Bayesian formulations, which require prior distributions over uncertain parameters [20], [21], the robust approach provides tractable and distribution-free guarantees.

We show how the RNE formulation leads players to seek conservative optimizations against worst-cases. Even though the structure of the equilibrium is qualitatively the same, and the predictive character of the game theoretic investigation is preserved, there is a higher variability of behavior in the parameter range that is worth considering when enacting practical security countermeasures.

The rest of this paper is organized as follows. Section II introduces the system model and formulates the game. Section III presents the robust equilibrium analysis and characterizes the resulting strategies. Section IV provides numerical results that illustrate the impact of uncertainty on system performance. Finally, Section V concludes the paper and outlines directions for future work.

II. Robust Nash Equilibrium

Consider a simultaneous-move game involving N players of set $\mathcal{N} = \{1, 2, \dots, N\}$, where each one of them $i \in \mathcal{N}$ chooses a strategy s_i from a set $\mathcal{S}_i$, which results in an outcome $\mathbf{s} = (s_1, s_2, \dots, s_N)$, also often denoted as (s_i, s_{-i}) to isolate player i, where $-i$ represents all players in $\mathcal{N}\setminus\{i\}$. Each player has its own evaluation of the outcome expressed through the *utility function* $u_i(\mathbf{s})$.

A strategy profile $\mathbf{s}^* = (s_i^*, s_{-i}^*)$ is a *Nash equilibrium* if no player can unilaterally improve its utility, i.e., [22]

$$u_i(s_i^*, s_{-i}^*) = \max_{s_i} u_i(s_i, s_{-i}^*), \quad \forall s_i \in \mathcal{S}_i,\ \forall i \in \mathcal{N}.$$

Now assume that the utility functions depend on an additional parameter $\eta \in \mathcal{H}$, representing uncertainty or noise, so that utilities are written as $u_i(\mathbf{s}, \eta)$.

According to the von Neumann–Morgenstern expected utility [23], players evaluate outcomes in expectation with respect to η. The NE definition naturally extends to

$$\mathbb{E}_\eta[u_i(s_i^*, s_{-i}^*, \eta)] = \max_{s_i} \mathbb{E}_\eta[u_i(s_i, s_{-i}^*, \eta)],\ \forall s_i \in \mathcal{S}_i, \forall i \in \mathcal{N}.$$

However, when no probabilistic information on η is available and only the uncertainty set $\mathcal{H}$ is known, one can use the concept of *robust Nash equilibrium* (RNE) [3], [24], defined by requiring each player to optimize against the worst-case realization of η. A strategy profile $\mathbf{s}^*$ is a RNE if

$$\min_{\eta\in\mathcal{H}} u_i(s_i^*, s_{-i}^*, \eta) = \max_{s_i\in\mathcal{S}_i} \min_{\eta\in\mathcal{H}} u_i(s_i, s_{-i}^*, \eta) \qquad (1)$$
$$\forall s_i \in \mathcal{S}_i,\ \forall i \in \mathcal{N}.$$

This formulation captures a conservative decision-making paradigm in which each player guarantees its performance under the most adverse realization of the uncertain parameter.

In many security problems, the interaction can be modeled as a game between a defender $\mathtt{D}$ and an attacker $\mathtt{A}$. The players choose nonnegative activity rates p and q, respectively, where p represents the defensive effort (e.g., transmission, monitoring, or protection rate) and q quantifies the intensity of the attack. Both players act on a common performance function $A(p, q)$, i.e., a KPI of the system [12], [18], [25]. We also assume that $A(p, q)$ is non-decreasing in p and non-increasing in q, and the attacker seeks to minimize it, whereas the defender seeks to maximize it.

The interaction is quasi-adversarial in that, in addition to their effect on $A(p, q)$, both players may incur a cost proportional to their activity [26]. Specifically, the defender and the attacker have utility functions

$$\begin{aligned} u_{\mathtt{D}}(p, q) &= \quad A(p, q) - Cp \\ u_{\mathtt{A}}(p, q) &= -A(p, q) - Kq\,, \end{aligned} \qquad (2)$$

where parameters $C > 0$ and $K > 0$ denote the *marginal costs of effort* of the defender and the attacker, respectively.

A typical uncertainty in security problems is that $\mathtt{A}$'s marginal cost parameter K may not be precisely known to the players because the characteristics of the attacker are blurry. For example, K may be known to lie within an interval $K \in [K_{\min}, K_{\max}]$. This uncertainty may be due to incomplete information about the attacker's resources, technology, or operational constraints [19].

A typical way to address this issue within a game theoretic framework is to include a Bayesian formulation [21], but this would require to estimate a prior distribution on the unknown parameters, which is sometimes challenging. A conservative approach (worst-case) would often be sufficient for practical purposes [2].

Thus, we can adopt a robust game-theoretic formulation in which each player optimizes against the worst-case realization of the uncertain parameter. In this setting, the attacker solves a max–min problem:

$$\max_{q} \quad \min_{K\in[K_{\min}, K_{\max}]} \big(A(p, q) - Kq\big), \qquad (3)$$

which, due to the linear dependence on K, yields the worst-case realization $K = K_{\max}$. Thus, the robust attacker behaves as if its cost were equal to the highest possible value.

However, this is the opposite of what is considered in security problems, where uncertainty about attack costs represents a problem for the defender [27]. Therefore, in a robust formulation, the defender evaluates the performance under $K = K_{\min}$, anticipating the most favorable conditions for the attacker.

III. Application Example: Robust NEs for False Data Injection in a Cyber-Physical System

We apply the concept of RNE to the false data injection (FDI) problem of [18]. In that scenario, a continuous-time status update system contains a source monitoring a process and sending data to a destination over a wireless channel. To formalize the notation, let $X(t) \in \mathcal{X}$ denote the state of the system at time t, where $\mathcal{X}$ is a countable set. The process $\{X(t)\}$ evolves as a continuous-time Markov chain and changes state with rate d, which is called *drift* and generically represents the variability of the system under observation. Let $\hat{X}(t)$ denote the estimate of the state of the system at the receiver. We are specifically interested in whether this estimate is correct or not and assume that $\mathcal{X}$ is sufficiently large to treat the probability that $X(t) = x_1$, $\hat{X}(t) = x_2 \neq x_1$, $X(t^+) = x_2$ *due to a drift* as negligible. In other words, it cannot happen that a wrong estimate at the destination is luckily corrected by a drift that changes the true state of the system to exactly that wrong estimate [28]. In contrast, $X(t) = \hat{X}(t)$ must necessarily be a consequence of a transmission from the source of true data about the state of the system.

The source perfectly observes the system and generates status updates whose transmissions occur according to a memoryless process with rate p, uncorrelated with drifts. Upon transmission, the estimate at the destination is updated instantaneously to the current state of the system, i.e., $\hat{X}(t^+) = X(t)$. Between successful updates, the estimate remains unchanged, but the state of the system can change due to drifts. Then $Y(t) := \mathbb{1}[X(t) \neq \hat{X}(t)]$, with $\mathbb{1}[\cdot]$ denoting the characteristic function, is a binary value that represents the incorrectness of what the destination knows about the state of the system at time t. In other words, $Y(t)$ describes whether the information available at the destination at time t is "incorrect" or "false." The process $\{Y(t)\}$ evolves as a binary-state continuous-time Markov process, whose transitions from 0 to 1 have rate d, and transitions from 1 to 0 have rate p.

The age of incorrect information (AoII) at time t is [17]

$$\Gamma(t) = t - z(t) \tag{4}$$

where $z(t)$ is the time of the first drift following the last generated update. If the last generation before time t happened at time $u(t)$, then $z(t) = \sup\{a : u(t) < a < t,\, Y(a) = 0\}$.

Under the previous assumptions on the dynamics of the source and the transmission process, the long-term average AoII $\bar{\Gamma}$ can be expressed as a function of the rates of update p and drift d. Observing how the system alternates between correct and incorrect estimation phases, and applying the renewal-reward theorem, yields

$$\bar{\Gamma} = \frac{d}{p(p+d)}. \tag{5}$$

Now, assume that an adversary is also present, maliciously injecting false data to the destination. True and false data are assumed to be indistinguishable, and the only countermeasure available to the source to withstand adversarial FDI is to send more true data. FDI occurs as a memoryless process, independent of transmission and drifts, with rate q. It is immediate to see that the role of the drift rate in (5) becomes now played by $d + q$, since false data injection causes $Y(t)$ to become 1, not due to a real system drift, but because $\hat{X}(t)$ is still not matching $X(t)$ anymore. The interaction between the transmitter and the adversary is modeled as a strategic game, as follows.

We take the resulting average AoII as

$$\bar{\Gamma}(p, q) = \frac{q + d}{p(p + q + d)} \tag{6}$$

as a function of p and q, instead we treat d as a known parameter. This is taken as $-A(p, q)$ in the general adversarial formulation of (2), the negative sign being due to the average AoII being something that the transmitter wants to *minimize*, and the adversary *maximize* instead.

Thus, players $\mathtt{D}$ and $\mathtt{A}$ are set as the source and adversary, seeking to maximize the following utilities:

$$\begin{aligned} u_{\mathtt{D}}(p, q) &= -\bar{\Gamma}(p, q) - Cp \\ u_{\mathtt{A}}(p, q) &= \bar{\Gamma}(p, q) - Kq\,, \end{aligned} \tag{7}$$

respectively, with C and K as their respective activity marginal costs.

This means that the transmitter selects the update rate p to minimize the average AoII plus a transmission cost Cp, while the adversary aims to degrade performance, i.e., to maximize the AoII, but also accounts for false data injection cost Kq. Thus, in the following we will denote C and K as the "marginal transmission cost" and the "marginal injection cost," respectively.

In [18], it is eventually found that the NE conditions are

$$\begin{aligned} p &= \begin{cases} (K + C)^{-1/2} & \text{if } K < ((K+C)^{1/2}+d)^{-2} \\ \sqrt{(d+p)^2(1-Cp^2)} & \text{otherwise} \end{cases} \\ q &= \begin{cases} -d - p + K^{-1/2} & \text{if } K < ((K+C)^{1/2}+d)^{-2} \\ 0 & \text{otherwise.} \end{cases} \end{aligned} \tag{8}$$

Note that some conditions are implicit as they do not admit a closed-form solution. However, they can be easily computed numerically.

We may want to investigate the *robustness* of this NE under uncertainty of the marginal injection cost K. Assume that this parameter falls in a certain range $(K_{\min}, K_{\max})$. According to the discussion in Section II, we assume three cases.

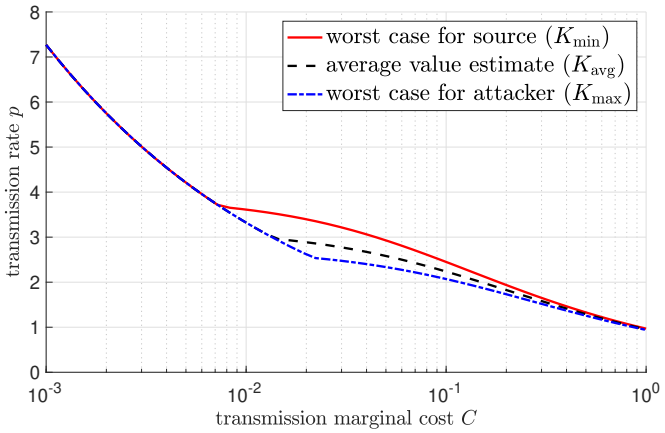

Fig. 1. Transmission rate p at the RNE vs. transmission cost C

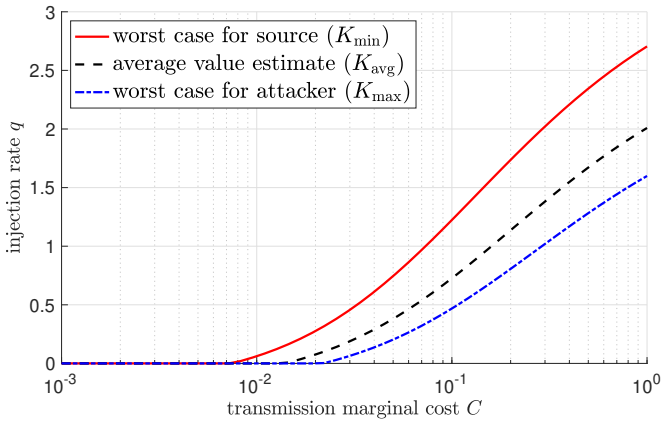

Fig. 2. Injection rate q at the RNE vs. transmission cost C

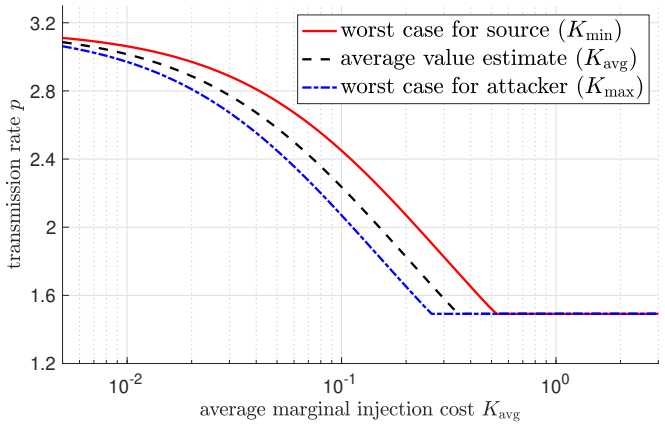

Fig. 3. Transmission rate p at the RNE vs. injection cost K

A possible approach would be to take the marginal injection cost as constantly equal to $K_{\text{avg}} = (K_{\max}+K_{\min})/2$. This is referred to as the "average value estimate," even though it is important to note this is meant as the *arithmetic average* between the minimum and maximum value of the range, and not necessarily as the statistical average. If all the values in this range are equally likely, i.e., K follows a uniform probability density, or, more loosely speaking, if its pdf is symmetric around the middle point, then K_{avg} is also the statistical average.

Another approach would be to assume a conservative FDI that chooses q according to the worst case for the attacker. Under appropriate monotonicity conditions, this was argued in Section II to correspond to imposing $K{=}K_{\max}$. This is actually confirmed for this specific case study, as visible from (8), since q is non-increasing in K, hence a larger K implies a lower q at equilibrium.

Instead, the source faces the most adverse scenario when the attacker is most aggressive, i.e., when the injection cost is minimal. This is especially true for the application scenario at hand, where the equilibrium in (8) has a threshold condition that requires K to be below a certain threshold for the attacker to be active [18]. Thus, the worst case scenario for the source corresponds to choosing $K{=}K_{\min}$, which means that if the threshold condition of the attacker is met only for a narrow range of K-values, the source always treat it as an active threat, even though it is probably often inactive.

In the following section, we will show some numerical quantification of the distance between the average value estimate and the two approaches from the perspective of a conservative attacker and a conservative transmitter.

IV. Numerical Results

We plot some sample results by considering the following numerical choices. We always take a drift rate $d = 0.2$ and a ratio $K_{\max}/K_{\min} = 2.0$. We will vary either parameter C or K (i.e., the marginal costs of the players) but unless otherwise specified, their default values are taken as 0.1 for both parameters.

Fig. 1 shows the variation of the transmission rate p of the source as a function of its marginal activity cost. Clearly, p is strictly decreasing in C, with a bi-modal pattern reflecting (8), especially with a threshold corresponding to whether the attacker is expected to be silent or not. Overall, the variability is relatively limited because even in the absence of an attacker, the source still needs to contrast the data drifts of the system.

Fig. 2, showing the equilibrium value of q versus C, mirrors some trends of the previous figure. However, the most striking trend is that a conservative approach of the source causes the attacker to be more aggressive. Moreover, the threshold required for the attacker to become active moves forward as we consider more conservative cases.

In Figs. 3 and 4, we change instead the value of the arithmetic average K_{avg} of the two extremes of the interval in which K lies. In both figures, it is visible how the increase of the cost causes p and q to become flat because the attacker is not active. However, this happens earlier for the curve displaying the worst case of the attacker, and later when the source is conservative instead. Moreover, an overall low value of K_{avg} implies high variability for the activity of the attacker (see Fig. 4), whereas the source is almost unaffected

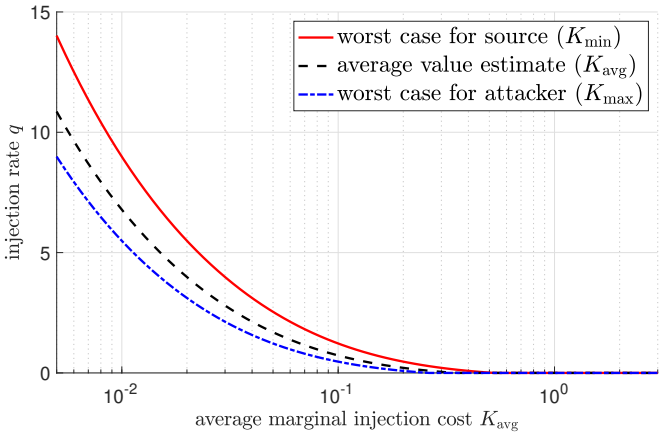

Fig. 4. Transmission rate q at the RNE vs. transmission cost K

as it must choose a high value of p anyways, and this choice becomes mostly limited by the marginal transmission cost C, instead. Conversely, when K_{avg} increases, the behavior of A becomes more similar between the three cases (it tends to decrease the FDI activity and eventually turns it off completely), while player D shows a more variable behavior with stronger oscillations, especially when approaching the switching point for the attacker's activty.

These numerical results highlight the impact of uncertainty in the attacker's cost on the equilibrium behavior of the system. In particular, the robust formulation leads to more conservative strategies, as the defender anticipates worst-case attack conditions, while the attacker accounts for the highest possible cost. Despite this conservatism, the qualitative structure of the equilibrium remains consistent in different parameter regimes, with players' strategies easily adapting to variations in system parameters.

Our results confirm that uncertainty can substantially affect system performance, especially in regimes where the equilibrium is sensitive to the attacker's cost. This underscores the importance of accounting for parameter uncertainty in the design of security mechanisms, as neglecting it may lead to overly optimistic performance predictions. Overall, the proposed robust framework provides a reliable and tractable approach to capturing these effects, offering valuable insights for the design of adversarial systems under incomplete information.

However, for the specific problem of FDI in a remote sensing system with the adversarial interaction focused on AoII, we see a general robustness of the qualitative trends observed across different parameter regimes. The exact equilibrium point varies with the system parameters and uncertainty bounds, but the overall structure of the interaction between the players remains consistent. The introduction of a robustness criterion in the presence of uncertainty leads to smooth adjustments in the equilibrium strategies, without abrupt transitions. This suggests that the proposed framework captures fundamental properties of adversarial systems that are not tied to specific parameter choices.

V. Conclusion

In this paper, we investigated the impact of uncertainty in the attacker's cost on the equilibrium behavior in adversarial and its repercussions for a specific case of FDI in CPSs, which allows a closed-form performance formulation through AoII [17]. We considered a game-theoretic model in which a defender and an attacker select their activity levels while acting on a shared performance metric and incurring linear costs. To account for incomplete information on the attacker's cost, we adopted a robust formulation and analyzed the resulting RNE [3].

Our analysis showed that uncertainty leads to more conservative strategies, as players optimize against worst-case parameter realizations. Despite this, the qualitative structure of the equilibrium is preserved and the system exhibits predictable behavior in different uncertainty regimes. The numerical results also highlighted the sensitivity of the equilibrium and the system performance to the attacker's cost, highlighting the importance of incorporating uncertainty in the design of defensive mechanisms [7].

Future work may extend this framework to more general settings, including multiple attackers, dynamic interactions, and alternative uncertainty models such as probabilistic or learning-based approaches [20].

References

[1] G. P. Crespi, D. Radi, and M. Rocca, "Insights on the theory of robust games," *Comput. Econ.*, vol. 65, no. 2, pp. 717–761, 2025.

[2] A. Ben-Tal, A. Nemirovski, and L. El Ghaoui, *Robust optimization*. Princeton university press, 2009.

[3] M. Aghassi and D. Bertsimas, "Robust game theory," *Math. Prog.*, vol. 107, no. 1, pp. 231–273, 2006.

[4] J. R. Marden and J. S. Shamma, "Game theory and distributed control," in *Handb. Game Th. Econ. Appl.* Elsevier, 2015, vol. 4, pp. 861–899.

[5] G. Scutari, F. Facchinei, J.-S. Pang, and D. P. Palomar, "Real and complex monotone communication games," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 4197–4231, 2014.

[6] M. Favero, C. Schiavo, A. Buratto, and L. Badia, "Price of anarchy for green digital twin enabled logistics," in *Proc. IEEE Symp. Comp. Commun. (ISCC)*, 2025, pp. 1–6.

[7] M. Passacantando and F. Raciti, "Optimal road maintenance investment in traffic networks with random demands," *Optimiz. Lett.*, vol. 15, no. 5, pp. 1799–1819, 2021.

[8] A. Nedic and A. Ozdaglar, "Distributed subgradient methods for multi-agent optimization," *IEEE Trans. Automat. Contr.*, vol. 54, no. 1, pp. 48–61, 2009.

[9] A. Nayyar, A. Mahajan, and D. Teneketzis, "Decentralized stochastic control with partial history sharing: A common information approach," *IEEE Trans. Automat. Contr.*, vol. 58, no. 7, pp. 1644–1658, 2013.

[10] M. Bloem, T. Alpcan, and T. Basar, "Intrusion response as a resource allocation problem," in *Proc. IEEE Conf. Decis. Contr.*, 2006, pp. 6283–6288.

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

[12] A. Garnaev and W. Trappe, "A jamming game with fair trade-off between SINR and power saving," in *Proc. IEEE Mediterr. Conf. Commun. Netw. (MeditCom)*, 2024, pp. 541–546.

[13] T. Marchioro, R. Saroui, and A. Olivereau, "Network intrusion response systems: towards standardized evaluation of intrusion response," in *Proc. Eur. Symp. Res. Comp. Sec. (ESORICS)*, 2025.

[14] L. Crosara, F. Ardizzon, S. Tomasin, and N. Laurenti, "Worst-case spoofing attack and robust countermeasure in satellite navigation systems," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 2039–2050, 2024.

[15] F. Mancini, L. Cannella, G. Messina, M. Centenaro, I. Di Pietro, A. Greco, S. Persia, F. Cuomo, and G. Bianchi, "5G security assurance: Lessons learned from 3GPP SCAS tests on virtualized network architectures." in *Proc. ITASEC/SERICS*, 2025.

[16] M. Ghaderi, K. Gheitasi, and W. Lucia, "A blended active detection strategy for false data injection attacks in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 168–176, 2021.

[17] A. Maatouk, S. Kriouile, M. Assaad, and A. Ephremides, "The age of incorrect information: A new performance metric for status updates," *IEEE/ACM Trans. Netw.*, vol. 28, no. 5, pp. 2215–2228, May 2020.

[18] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "Strategic interaction over age of incorrect information for false data injection in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 12, no. 1, pp. 872–881, 2025.

[19] L. Giaretta, T. Marchioro, E. Markatos, and S. Girdzijauskas, "Towards a realistic decentralized naive Bayes with differential privacy," in *Int. Conf. Smart Business Techn.* Springer, 2022, pp. 98–121.

[20] G. Quer, F. Librino, L. Canzian, L. Badia, and M. Zorzi, "Inter-network cooperation exploiting game theory and Bayesian networks," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4310–4321, 2013.

[21] V. Bonagura, L. Badia, C. Foglietta, F. Pascucci, and S. Panzieri, "A bayesian game-theoretic framework for false data injection in cyber-physical systems," *IEEE Transactions on Industrial Cyber-Physical Systems*, 2026.

[22] L. Badia, A. Zanella, and M. Zorzi, "A game of ages for slotted ALOHA with capture," *IEEE Trans. Mobile Comput.*, vol. 23, no. 5, pp. 4878–4889, 2024.

[23] P. Wakker and D. Deneffe, "Eliciting von Neumann-Morgenstern utilities when probabilities are distorted or unknown," *Manag. Sc.*, vol. 42, no. 8, pp. 1131–1150, 1996.

[24] C. Biefel, F. Liers, J. Rolfes, L. Schewe, and G. Zöttl, "Robust market equilibria under uncertain cost," *Eur. J. Oper. Res.*, vol. 302, no. 3, pp. 1230–1241, 2022.

[25] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier, and A. Ephremides, "Impact of hostile interference on information freshness: A game approach," in *Proc. WiOpt*, 2017.

[26] L. Badia, S. Merlin, A. Zanella, and M. Zorzi, "Pricing VoWLAN services through a micro-economic framework," *IEEE Wireless Commun.*, vol. 13, no. 1, pp. 6–13, Feb. 2006.

[27] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordónez, and M. Tambe, "Computing optimal randomized resource allocations for massive security games," in *Proc. Int. Conf. Auton. Agents Multiagent Syst. (AAMAS)*, 2009.

[28] F. Chiariotti, A. Munari, L. Badia, and P. Popovski, "Goal-oriented medium access with distributed belief processing," *IEEE/ACM Trans. Netw.*, vol. 34, pp. 1643–1658, 2026.