Strategic Interaction Over Age of Incorrect Information for False Data Injection in Cyber-Physical Systems

Valeria Bonagura, *Student Member, IEEE,* Stefano Panzieri, Federica Pascucci, *Senior Member, IEEE,* and Leonardo Badia, *Senior Member, IEEE*

Abstract—Ambient monitoring through remote sensing is the first required step of many control operations in cyber-physical systems to enable accurate decision-making by network intelligence. We consider a controller that sends status updates about a process to a receiver, incurring a cost when doing so. The process is dynamical, implying that the information the receiver has may become outdated due to a natural drift of the process. To determine the correctness of the information at the receiver, we model this interaction using a Markov Chain with two states, namely right (R) and Wrong (W). The controller can restore the receiver status to R by performing a new transmission, which comes at a cost. The staleness of information, when the system state is erroneous, is quantified through the average value of the age of incorrect information metric. Moreover, an adversary may inject false data at a price to make the information available at the receiver less fresh, which can only be contrasted by additional measurements by the controller. This results in a game played by strategic agents, namely the controller and the adversary. The adversary's objective is to maximize the time the receiver is in the W state of the Markov Chain, while the controller's objective is to minimize it. We provide a mathematical formulation of this strategic interaction using Game-Theory, demonstrating the existence of a Nash equilibrium. In our analysis, we discuss the role of different system parameters and the implications on the resulting system performance, providing a quantitative evaluation of the parameter ranges where an adversary can be effectively counteracted is an important guideline to improve security of cyber-physical systems.

Index Terms—Cyber-physical systems; Cyberattack; False data injection; Markov processes; Age of information; Age of incorrect information; Game theory.

1 Introduction

Remote sensing, the acquisition of information from a distance, plays an important role in cyber-physical systems (CPSs), providing up-to-date environmental data for enhanced monitoring, control, and decision-making. Its integration contributes to the efficiency, reliability, and responsiveness of various domains such as smart cities, transportation, energy management, and eHealth monitoring [1], [2], [3]. As a fundamental step in network control, remote sensing involves data acquisition, transmission, processing, and fusion, leading to informed control decisions within CPSs.

However, the physical deployment of sensing units exposes them to potential tampering or unauthorized access, presenting security challenges that are not as prevalent in centralized components. Vulnerabilities in data transmission, often relying on wireless communication, introduce risks such as interception, eavesdropping, or unauthorized access [4].

While existing research focuses on detecting and preventing attacks through secure communication protocols, authentication mechanisms, and tamper-resistant strategies [5], [6], false data injection (FDI), particularly in stealthy or replay attacks [7], poses a distinct challenge. Unlike typical security measures, our paper explores strategic interactions between an adversary injecting false data and a system controller aiming to mitigate the attack's impact. FDI, though unavoidable, can be countered by increasing the effort required by the adversary, resulting in a game-theoretic approach [8], [9], [10], [11].

Framed as an adversarial game [12], our approach uses the average age of incorrect information (AoII) as the objective. AoII measures the time elapsed since inaccurate information was last updated, crucial for assessing the impact of FDI on the timeliness of decision-making in CPSs [13]. Unlike the age of information (AoI), AoII emphasizes the delay between an event and the system's acknowledgement of that change, making it pertinent for FDI scenarios [14]. Successful FDI can elevate AoII, leading to compromised system behaviour. To formalize the problem, we incorporate

- *Manuscript received XXX.*
- *Project co-founded by the European Union - Next Generation Eu - under National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Incestment 3.3- Decree No. 352 (9^{th} April 2022) of Italian Ministry of University and Research - Concession Decree No. 2153 (28^{th} December 2022) fo the Italian Ministry of University and Research, Project code D93D22001390001, within the Italian National Program PhD Programme in Autonomous Systems (DAuSy)*
- *V. Bonagura, S. Panzieri, and F. Pascucci are with the Department of Civil, Computer Science and Aeronautical Technologies Engineering, University Roma Tre, 00146 Rome, Italy.*
  E-mail: valeria.bonagura@uniroma3.it; stefano.panzieri@uniroma3.it; federica.pascucc@uniroma3.it.
- *V. Bonagura is also with the Dept. of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy.*
  E-mail: vbonagura@phd.poliba.it
- *L. Badia is with the Dept. of Information Engineering, University of Padova, 35131 Padova, Italy.*
  E-mail: leonardo.badia@unipd.it

a drift into the process tracked by remote sensing, causing inaccuracies over time. While the controller requests measurements to minimize AoII, adversary-induced FDI increases the drift and AoII. Introducing costs for both players prevents an undesirable scenario where both players increase their activity without consequence, making our game a non-zero sum [15].

Our analysis reveals that containment of the adversary is possible, depending on associated costs and the natural drift rate. When an adversary faces high costs, it remains inactive. Conversely, if the cost of injection for the adversary is low compared to the cost of transmission for the legitimate user, the system performance is compromised. Yet, this situation prompts the network controller to respond strategically. The subsequent findings enhance our comprehension of FDI dynamics within cyber-physical systems. [16].

The remainder of this paper is organized as follows. Section 2 reviews related literature. Section 3 introduces the system model, analyzed using game theory. Numerical results are presented in Section 4, followed by conclusions in Section 5.

1.1 Paper Contributions

In this study, we analyze a sensing scenario involving the exchange of status updates between a controller and a receiver. Notably, this scenario unfolds in the presence of a malicious agent, termed the *adversary*, equipped with the ability to inject false data. The adversary aims to maximize damage to the targeted system, represented by the *receiver*. In contrast, the controller endeavors to minimize the inflicted damage, setting the stage for a compelling game-theoretic interaction. Our study introduces a novel approach to counter false data injection attacks, leveraging game theory to model and understand the strategic interactions between these agents. Our contributions can be summarized as follows.

Markov Modeling of the Adversarial Interaction. We formulate the strategic interaction from the receiver's standpoint using a Markov Chain comprising two states: "right" (R) and "wrong" (W). The state is W when the available information fails to accurately reflect reality and R otherwise. Transitions between these states hinge on the system dynamics and the actions of the involved agents. The adversary aims to maximize a penalty depending on the receiver's duration in the W state while the controller endeavors to minimize it.

Game-Theoretic Analysis. We approach the interaction through the lens of game theory. The controller and the legitimate agent can determine the transmission and injection rates, respectively. This paper assumes that this decision-making process is driven by maximizing a utility function. For the controller, this utility function encapsulates the imperative to minimize the time the receiver spends in state W, while for the adversary, it reflects the objective to maximize this duration. The game is non-zero-sum since both agents are constrained by a transmission cost that limits the rate. We establish the existence of a unique Nash Equilibrium for the considered game.

System Parameter Analysis. In our analysis, we examine the influence of various system parameters on the resultant system performance. Offering a quantitative assessment of the parameter ranges within which an adversary can be effectively countered serves as a crucial guideline for enhancing the security of cyber-physical systems.

Indeed, there exists an extensive body of literature on security threats in cyber-physical systems, including discussions on the potential interactions between FDI attackers and systems, as highlighted in works such as [17], [18]. However, what sets our study apart is our characterization of these interactions in a *strategic* manner, utilizing the lens of game theory [19]. In our approach, the evaluation goes beyond merely considering the attacker's planning of malicious actions. Instead, we incorporate the decision-making process of both the attacker and the network operator. This includes developing and implementing countermeasures by the network operator, to which the attacker responds, and so forth. By adopting this strategic perspective, we provide a more nuanced and detailed mathematical framework for modelling smart attacks, encompassing multiple layers of interactions between the involved parties.

2 Related Work

Among the security challenges faced by CPSs, FDI is one of the most troublesome. In [16], a comprehensive discussion of this kind of problem was given, and it was especially highlighted how a sufficiently smart and system-aware attacker could elude detection under proper assumptions. This is the fundamental motivation of our analysis since we consider a game theoretic setup [9], in which the system controller can only increase the rate of measurements performed to compensate for false data injected in the network.

Most of the literature exploring FDI in CPSs is primarily interested in either giving taxonomies of the problem or finding joint detection and control schemes to overcome the problem. For example, [7] combines a watermarked signal and a nonlinear static auxiliary function to limit the disclosure resources of the adversary and obtain an unidentifiable moving target. Such a strategy is effective against a broad class of FDI attacks.

In [4], coding the sensor reading was proposed so that stealthy false data injection attacks are detected by increasing the estimation residues under intelligent data injection attacks. The problems of malicious sensor detection and secure estimation are considered in [6], where optimal filtering and learning are proposed to exclude malicious sensor observations and detect injection attacks.

Analogously, [5] propose a secure control scheme based on moving target defence and reinforcement learning, where attack detection and isolation schemes are designed to locate and exclude the compromised actuators accurately. This last paper introduces some strategic elements in the algorithm design through a reinforcement learning approach. This implies the assumption that nodes can control their choices to optimize their benefit, which is the crucial ingredient of game theory [9]. Another approach is considered in [20], but only from the attacker's perspective.

When both the adversary and the controller are strategic, we obtain a game theoretic perspective such as that of [8], similar to our study. In that paper, an infinite horizon linear quadratic Gaussian system is considered, where an attacker injects malicious data. False alarm probability is regarded as the reward, which the controller and the attacker want to minimize and maximize, respectively. This marks a difference from our approach since we consider an AoII-based reward, which implies that instead of just minimizing the probability that the information about the system is wrong, we also account for its persistence. Another difference is that instead of analyzing a zero-sum game, like is done there, we also include costs in the operation of the players.

Game theory is a powerful tool to model security problems, design robust control for network systems, and identify strategies against attackers. At the same time, game theoretic approaches exist for AoI [2], [21]. Yet, these aspects (security, AoI, and game theory) are rarely seen together. For the most, game theoretic approaches for AoI analyze symmetric problems with mutual interference conditions [10], [15], [22], or the need for privacy-preserving crowdsensing [23]. Fewer papers address AoI or AoII about performance losses related to lack of security, and they do so only for less sophisticated attacks such as jamming, i.e., preventing the system from being updated to the recent value [11], [24].

The main novelty of this paper is to use the AoII metric instead of AoI, to connect the system control with its semantic meaning. This is a recent idea proposed for the first time in [13], to weigh the time elapsed since the last drift that makes the state information no longer up-to-date. It can be seen as a generalization of shaping the concept of AoI with different penalties, as argued in [25].

Nevertheless, all the main contributions discussing AoII to date only focus on the original definition with a linear penalty for aging [14], [26], [27], [28]. We adopt this approach as well, considering AoII as a quantity that is reset to zero after each successful update, and stays at that value as long as the monitored process does not significantly change. Whenever the last update no longer accurately describes the status of the environment, either because a natural variation occurred or the attacker injected false data, we have a linear AoII increase as a negative reward (i.e., a penalty) [29].

Some investigations of AoII revolve around the relationship between the mean absolute error in the reports of a specific (piecewise linear) signal over a noisy channel and AoII [14]. Other studies consider the minimization of AoII through proper setup of slotted ALOHA parameters [26] or proper scheduling of updates [27].

Finally, [28] and [29] consider a real-time tracking of a Markov chain, similar to our scenario. However, we are not interested in characterizing the source but in understanding the impact of adversarial attacks. Hence, our analysis will be limited to a two-state Markov chain, not because the system state is binary, but because we need to distinguish whether the information available at the controller is accurate. This can represent a system with any number of states, where all that matters is whether the controller is aware of what form the system is in, and the probability that the system reverts to correct information after drift is negligible.

3 System model

In this section, we present our system model, which revolves around a dynamical system described by the equations:

$$\begin{cases} \dot{x}(t) &= f(x(t), u(t)) \\ y(t) &= h(x(t)), \end{cases} \tag{1}$$

Here, $x(t)$ represents the plant state, $u(t)$ is the control input, and $y(t)$ is the output at time t. The functions $f(\cdot)$ and $h(\cdot)$ denote the state transition and output selection functions, respectively. In this framework, $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^p$, $y(t) \in \mathbb{R}$. The control input $u(t)$ is generated by a network controller N that communicates with a remote station (e.g., a SCADA system) by transmitting the output measurement $y(t)$. For the sake of simplicity, we assumed that the output measurement is scalar. Still, the problem could be easily adapted to the vector case by conducting the same analysis for each of the outputs. We assume no propagation delay between the controller and the remote station, allowing us to compute time on either end.

The value of age of information (AoI) at time t is

$$\gamma(t) = t - t_u \,, \tag{2}$$

where t_u is the time corresponding to the reception of the most recent update before time t, inclusive.

To capture the model of this behaviour, we introduce a continuous-time Markov chain with two states: "right" (R) and "wrong" (W). The transitions between these states depend on system dynamics and actions, as illustrated in Fig. 1. In particular, a malicious agent M, also called "adversary," can increase the frequency of transitions to state W, to cause havoc in the system. After every update, Age of Information (AoI) linearly increases. However, the information available at the receiver might still correctly represent the system's state. As an extension of the AoI metric, in [10] the Age of Incorrect Information (AoII) was introduced. The primary goal of AoII is to assess the amount of time the receiver possesses incorrect information. This concept is formalized by multiplying a cost function, denoted as $\ell(\cdot)$ in our paper, which increases over time, and an information penalty function, denoted as $g(\cdot)$, capturing the disparity between the current information available at the receiver and the actual process state. Our research is centred around discerning whether the information available at the receiver remains accurate or has deviated due to natural drift or malicious updates. Consequently, our metric of interest is AoII, not AoI. AoI is inadequate for modelling false data injection, as adversarial interventions of this nature solely elevate AoII without affecting AoI. Based on the definition provided in [13], the value of the AoII at time t is:

$$\delta(t) = \ell(t) \cdot g(y(t), y(t_u), y^a(t_m)) \,, \tag{3}$$

where, $g(\cdot, \cdot, \cdot)$ quantifies the discrepancy between the actual system output $y(t)$, the last correct update transmitted $y(t_u)$, and the most recent false sensor reading sent by malicious agent M, $y^a(t_m)$. The function $\ell(\cdot)$ imposes penalties as the discrepancy $g(\cdot, \cdot, \cdot)$ increases.

Notably, our specific formulation employs a basic expression of AoII, where the information penalty function is binary (taking values of 0 or 1) based on the correctness or incorrectness of the information, and the time-increasing penalty function is linear. In particular,

$$g(y(t), y(t_u), y^a(t_m)) = \begin{cases} 1 & \text{if } |y(t) - y(t_s)| \geq \vartheta \\ 0 & \text{otherwise} \end{cases} \,, \tag{4}$$

where $t_s = \max\{t_u, t_m\}$ is the index of the last time instant the receiver received an update, without distinguish-

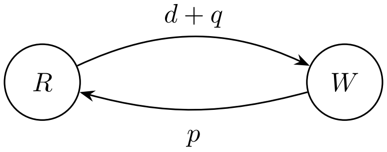


Fig. 1. Continuous time Markov process with the respective rates of moving from one state to one another.

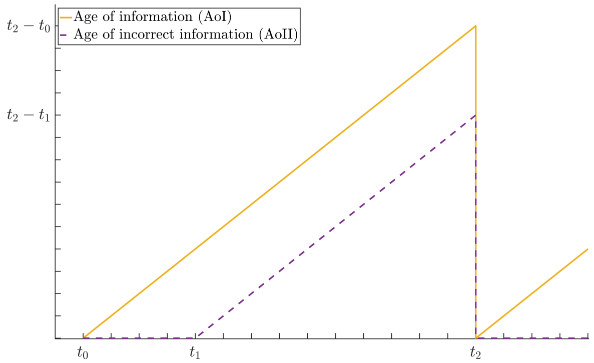


Fig. 2. Age metrics are initialized to 0 at t_0. From that instant onwards, AoI increases linearly, whereas AoII initially stays at 0 (status is obsolete but correct). At t_1, AoII starts increasing as well due to drift. At t_2, the status is refreshed. For any $t \in (t_1, t_2)$, AoI and AoII are $t - t_0$ and $t - t_1$, respectively.

ing between legitimate and malicious. If $t_s = t_m$, then $y(t_s) = y^a(t_m)$, otherwise $y(t_s) = y(t_u)$. This function reflects the gap between the current system output $y(t)$, the last update available at the receiver, and a threshold ϑ. We assume that, following a drift or a malicious transmission, $|y(t) - y(t_s)| > \vartheta$ until a legitimate update takes place.

The linear time-increasing penalty function $\ell(\cdot)$ is

$$\ell(t) = t - t_d,$$

where t_d is the last time-instant over a period where $g(y(t), y(t_u), y^a(t_m)) = 0$. Despite its apparent simplicity, this formulation serves a crucial purpose in our analysis. Indeed, with our proposed formulation, AoII is zero when the receiver possesses correct information. Subsequently, it increases linearly when the receiver acquires erroneous information and continues to rise until a new legitimate update occurs. Hence, AoII measures the time elapsed since the last drift, whether a natural occurrence or maliciously induced one. To better clarify the difference between AoI and AoII, see Fig. 2. The figure provides a comparative illustration of AoI and AoII in a straightforward scenario where a drift (either naturally present or maliciously induced by an adversary) occurs at time t_1, while at t_2 a new legitimate update is performed. The age metrics are initialized to 0 at t_0. Starting from that moment, AoI exhibits a linear increase, while AoII remains at 0 initially (indicating an obsolete but correct status). At t_1, AoII begins to increase due to the drift. At t_2, the status is refreshed. For any $t \in (t_1, t_2)$, AoI and AoII are represented as $t - t_0$ and $t - t_1$, respectively.

The system parameters involved in the transitions are the following. We set the measuring rate of the controller as p, which corresponds to the rate by which the system enters state R, since the measuring action sets the information about the states as correct. Afterwards, the information slowly becomes stale but is still correct, until either a system drift or a malicious injection by the adversary occurs, since these events send the system state to W. We denote the rate of (natural) drift of the system as d and the rate of malicious injection by an adversary as q. We further assume that natural drifts, malicious injections, and reading by the controllers all happen according to memoryless processes independent of each other. Thus, the transition from W to R happens with rate p, whereas that from R to W has rate $d+q$, see Fig. 2.

We consider the expected value of the AoII $\Delta = \mathbb{E}_t[\delta(t)]$ meant as a time average. From standard derivations of Markov models, Δ can be promptly computed as [15]

$$\Delta = \frac{1/(2 \cdot p^2)}{1/p + 1/b}, \tag{5}$$

where $b = d + q$. In (5), $1/2p^2$ represents the average area below the AoII function, specifically denoted by (3), within a given period. To provide a visual reference, this corresponds to the area of the purple triangle in Fig. 2. On the other hand, the denominator $1/p + 1/b$ signifies the expected value of the time elapsed between two consecutive updates, referred to as a period. This metric accounts for the average time between two updates, balancing the update rate p with the total rate b of system drift and malicious data injection. Additionally, we introduce respective cost terms associated with transmission of controller N and false data injection of adversary M. These terms can be interpreted as energy expenditures or limiting factors on their frequency of activity. We assume that both cost incurred by these agents are linearly proportional to their activity rate, i.e., p and q for N and M, respectively.

The linear proportionality between the activity rates (transmission and injection rates) and the associated costs can be grounded in both mathematical and technical reasons. It can be seen, for example, as a shadow price, that is, as a Lagrange multiplier associated to the constraint of a maximum allowed activity [30]. At the same time, it can also be seen as associated to energetic or computational expenditures [10], [15], where a linear relationship in the frequency of activity is expected. By maintaining a linear proportionality assumption, our model captures the essence of resource constraints, making it a pragmatic choice for scenarios where energy considerations play a significant role. The linear coefficient is denoted as $C > 0$ for the controller and $K > 0$ for the adversary.

With these definitions, we formulate utility functions for both controller and malicious agent as

$$u_{\mathrm{N}}(p, q) = -\Delta - C \cdot p, \quad u_{\mathrm{M}}(p, q) = \Delta - K \cdot q\,. \tag{6}$$

Here, $u_{\mathrm{N}}(p, q)$ represents the utility of the controller, aiming to minimize the sum of the expected AoII and its transmission costs, while $u_{\mathrm{M}}(p, q)$ is the utility of the malicious agent, seeking to maximize the expected AoII of the controller but also limiting the cost undertaken for the malicious injections.

In the absence of an adversary, the controller's optimal transmission rate p is determined by balancing the cost term $C \cdot p$ and the natural drift rate d, which ultimately result in maximizing the single-variable function

$$u_{\mathrm{N}}(p, 0) = -\Delta - C \cdot p\,, \tag{7}$$

which implies that, without M in the network, the problem boils down to just a single-agent optimization.

However, due to the simultaneous presence of N and M, their interaction can be formalized as a static game of complete information $\mathcal{G} = (\mathcal{P}, \mathcal{A}, \mathcal{U})$, defined by the set of players $\mathcal{P} = \{\mathrm{N}, \mathrm{M}\}$, their respective set of actions $\mathcal{A}$ where player N chooses $p \in [0, \infty)$ and M chooses $q \in [0, \infty)$, and the utility set $\mathcal{U} = \{u_{\mathrm{N}}, u_{\mathrm{M}}\}$. All of this is common knowledge among the players. Characterizing the game as *static* implies that the players choose one value of their action independently and unbeknownst to each other. The most desirable outcome for the players is typically characterized by the Nash equilibrium (NE). The NE obeys the properties formalized by the following theorems for the specific game under exam.

Theorem 1 (*Existence of an NE*)**.** Game $\mathcal{G}$ admits a NE.

The proof is provided in Appendix A.

Corollary 1.1 (*Uniqueness of the NE*)**.** The NE is also unique.

Proof. This is a direct consequence of the utility function of the controller and the adversary being both monotonic over their entire span. This ensures that the ε-fixed point to which they converge is always the same. □

For the specific formulation at hand, the NE conditions can be numerically derived by looking at the critical points of the analytical expressions, which implies to solve the following conditions [3]

$$\frac{\partial u_{\mathrm{M}}(p,q)}{\partial q} \;=\; 0 \qquad \frac{\partial u_{\mathrm{N}}(p,q)}{\partial p} \;=\; 0\,, \tag{8}$$

which imply

$$\frac{\partial \Delta}{\partial q} \;=\; K \qquad \frac{\partial \Delta}{\partial p} \;=\; -\,C. \tag{9}$$

Rearranging the terms in $\frac{\partial \Delta}{\partial q} = K$ results in a second-degree equation with respect to q:

$$\frac{1}{2\left(d+p+q\right)^2} = K\,.$$

Solving this equation is straightforward and yields two solutions, one negative for all possible values of K. Therefore, the only viable solution to our problem is given by

$$q = -d - p + \frac{1}{\sqrt{2K}}.$$

Substituting this expression for q into $\frac{\partial \Delta}{\partial p} = -C$ and rearranging the terms, we obtain a second-degree equation with respect to p:

$$K - \frac{1}{2p^2} = C.$$

Once again, it is straightforward that this equation has two solutions, one of which is negative for all possible values of C. We conclude that at the equilibrium

$$p = \frac{1}{\sqrt{2K + 2C}}.$$

Thus, the NE is

$$\begin{aligned} p \;&=\; \frac{1}{\sqrt{2K+2C}}, \\ q \;&=\; -\,d\,-\,p\,+\,\frac{1}{\sqrt{2K}}. \end{aligned} \tag{10}$$

In (10), K must be sufficiently small to ensure that q is positive. If the mathematical solution of (10) yields a value of q less than zero, it implies that the attacker gains no benefit from the manipulated data and therefore chooses to remain silent. In this case the NE still exists, but the condition degenerates to the border points of the feasibility intervals, in particular q is equal to 0 and the optimal update frequency p is reduced to a single-agent optimization problem that maximizes $u_N(p, 0)$ as per (7).

Hence, in (10), the injection cost term K is balanced against the natural drift d and the transmission rate p. If these terms become too large, q can only remain positive if K is low enough. This highlights the trade-off between the different factors influencing the system dynamics.

Taking a broader perspective, we can explore the range of appropriate values for K, ensuring that player M actively participates in the game and (10) accurately reflects the NE of the system. From (10), if $K > d^{-2}/2$, it is impossible to get $q > 0$.

Even if $K < d^{-2}/2$, it might be inconvenient for the adversary to transmit, as it must also hold

$$-\,d\,-\,\frac{1}{\sqrt{2K+2C}}\;+\;\frac{1}{\sqrt{2K}} > 0. \tag{11}$$

Considering that K and C are positive and so is d, the following theorem states that a threshold value K^* exists that defines the border between the conditions for the NE to lie in an inner point or to degenerate at the border. In more detail, if $K > K^*$, the cost is too high for the adversary and it does not really partake in the interaction, leaving the only drift to the natural rate d.

Theorem 2 (*Existence and uniqueness of* K^*)**.** For all $C \in (0, \infty)$ and $d \in (0, \infty)$, a value K^* exists such that for $K < K^*$,

$$-d\,-\,\tfrac{1}{\sqrt{2K+2C}}\;+\;\tfrac{1}{\sqrt{2K}} > 0,$$

holds.

The proof is provided in Appendix B.

This result implies that player M will avoid transmitting if $K > K^*$ since the cost is too high. According to (10), a higher transmission cost for the controller lowers the transmission rate p. Thus, the theorem implies that for the adversary to conveniently transmit, the controller's update rate must be low enough to undermine the system.

To sum up, the NE conditions are

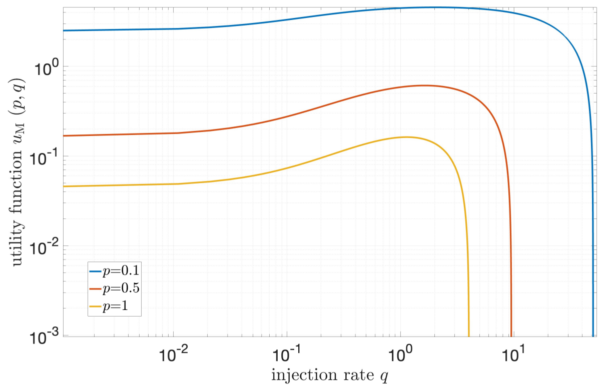


Fig. 3. Utility $u_{\mathrm{M}}(p,q)$ for $C = 1$, $K = 0.1$, $d = 0.1$, and $p = 0.1,\ 0.5,\ 1$.

$$p = \begin{cases} \dfrac{1}{\sqrt{2K+2C}} & \text{if } K < K^* \\[2ex] \frac{1}{6}\left(-3d + \sqrt{3}\sqrt{s} + \dfrac{3\sqrt{\frac{d^2}{3}+\frac{1}{3}s+\frac{2\sqrt{3}d}{C\sqrt{s}}}}{C}\right) & \text{otherwise} \end{cases} \tag{12}$$

$$q = \begin{cases} -d \ - \ p \ + \ \dfrac{1}{\sqrt{2K}} & \text{if } K < K^* \\ 0 & \text{otherwise} \end{cases}, \tag{13}$$

where

$$s = d^2 + \frac{d^4 C}{r} + \frac{r}{C},$$

and

$$r = \left(\frac{27d^2C}{2} + d^6C^3 + \frac{3}{2}\sqrt{3}\sqrt{d^4C^2(27+4d^4C^2)}\right)^{\frac{1}{3}}.$$

Those equations are derived in one case by resolving the static game where N and M are involved, while in the other by maximizing (7) i.e., the objective function of the controller when the malicious agent is not playing the game.

4 Numerical Results

This section demonstrates the application of the derived NE (12)-(13) and Th. 1, illustrating how the equilibrium changes with variations in the system parameters. Specifically, it examines a setting involving a strategic interaction between a controller and an adversary injecting false data. Both agents strategically pursue their objectives within the framework of reducing and increasing AoII at a remote station, respectively. Concurrently, they aim to minimize their respective costs due to their activities. We start by exploring the utility functions, namely $u_{\mathrm{M}}(p,q)$ and $u_{\mathrm{N}}(p,q)$, representing the malicious agent and the controller's objectives, respectively. These are graphically depicted in Figs. 3 and 4, offering insights across various parameter combinations of p and q.

Fig. 3 demonstrates how the malicious agent strategically selects its activity rate q to maximize its utility $u_{\mathrm{M}}(p,q)$ under different fixed values of p. As the transmission rate p increases, the maximum of the utility $u_{\mathrm{M}}(p,q)$ decreases. This phenomenon arises because the higher the transmission rate, the lower the average AoII at the receiver. This implies a lowering of the value of the utility function of the malicious agent. Similarly, Fig. 4 provides insights into how the controller strategically adjusts its activity rate p to maximize its utility $u_{\mathrm{N}}(p,q)$ for different fixed values of q. As the injection rate q increases, the maximum of $u_{\mathrm{N}}(p,q)$ decreases. This is because the controller has to transmit more often to minimize AoII, resulting in higher costs.

Figs. 6 and 5 illustrate the strategic transmission rate

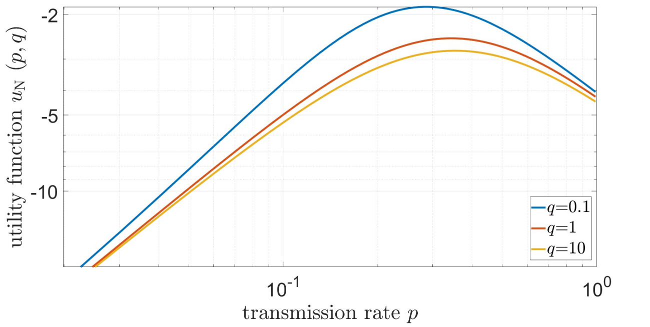


Fig. 4. Utility $u_{\mathrm{N}}(p,q)$ for $C = 1$, $K = 0.1$, $d = 1$, and $q = 0.1, 1, 10$.

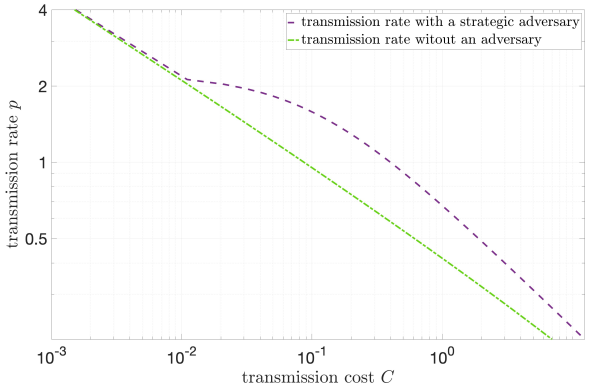


Fig. 5. Comparison of strategical update rate p with and without a malicious agent, $K = 0.1$ and $d = 0.5$

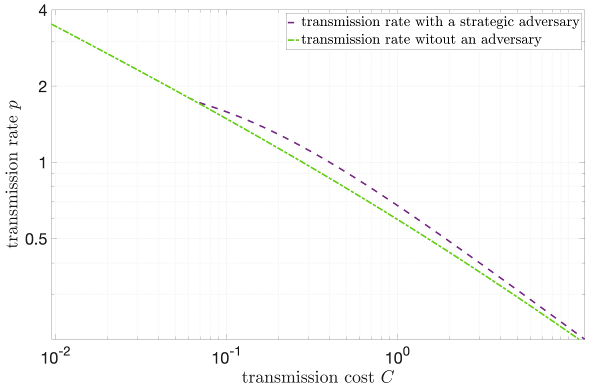


Fig. 6. Comparison of strategic update rate p with and without a malicious agent, $K = 0.1$ and $d = 1$.

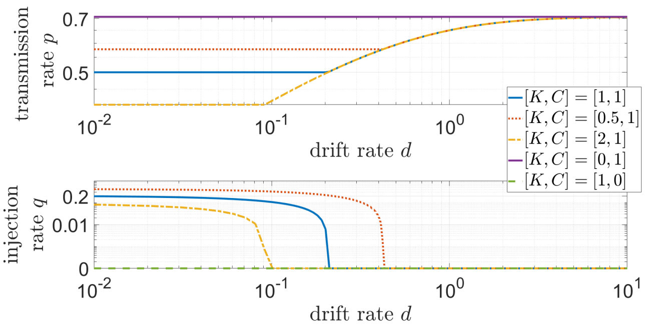


Fig. 7. Transmission and Injection rate at the NE to the change of drift rate d.

p at the NE versus the cost parameter C indicating the transmission cost of the legitimate user. The two figures consider a constant natural drift rate d, equal to 0.5 and 1, respectively. Also, we compare the situations with or without a strategic adversary, where in the former case the cost for the adversary is constant and equal to $K = 0.1$. These figures show that, when the adversary is absent, the activity of the transmitter follows a linearly decreasing relationship with its cost, being just aimed at counteracting the natural drift of the system. This is the same behavior observed if an adversary is present but the cost of the transmitter is low. Indeed, the strategic adversary possesses complete knowledge on these parameters and realizes that it is pointless to contrast a transmitter that can transmit very often to balance both the natural drift and the malicious injections. However, the curves show a transition in an angular point when the transmission costs C and K satisfy Theorem 2. At this point, the adversary becomes active and forces the transmitter to a higher activity. While the transmission probability still decreases with cost C, the transmitter is facing an increased drift due to the malicious adversary, which results in the inflation of the curve to higher values of p. A comparison of the figures show that this phenomenon is stronger if the natural drift of the system is lower, since in this case the presence of the adversary has a stronger impact.

Figs. 8 and 9 show the impact of strategic behaviour on the transmission and injection rates. As the transmission cost for the malicious agent increases, the injection rate q decreases, discouraging the adversary from injecting data. Moreover, as the natural drift rate d increases, the injection rate decreases, necessitating a higher update rate from the controller N to counteract the malicious injections.

Our findings highlight that the strategic selection of injection and transmission rates can mitigate the impact of misleading data injection. The presence of the malicious agent becomes less threatening if it incurs higher costs for data injection. A proper increase in the controller's activity rate can significantly curtail the impact of data injection.

Furthermore, we discuss the evolution of the Markov Chain depicted in Fig. 1 according to the outcome of the game. The average residence time in the ”wrong” (W) state corresponds to the average AoII Δ. However, for certain applications, the peak AoII may be more interesting, which corresponds to the maximum dwell time in state W, instead.

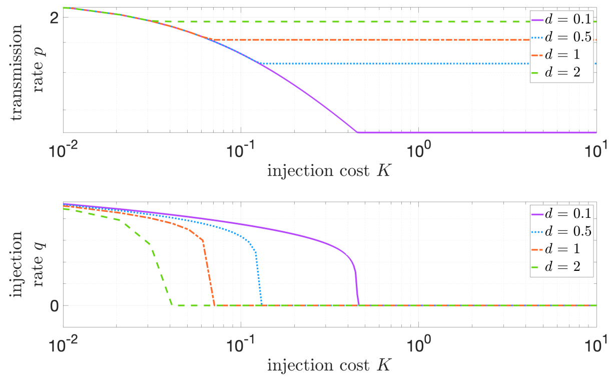


Fig. 8. Transmission rate p and injection rate q at the NE, for $C = 0.1$ and $d \in \{0.1, 0.5, 1, 2\}$.

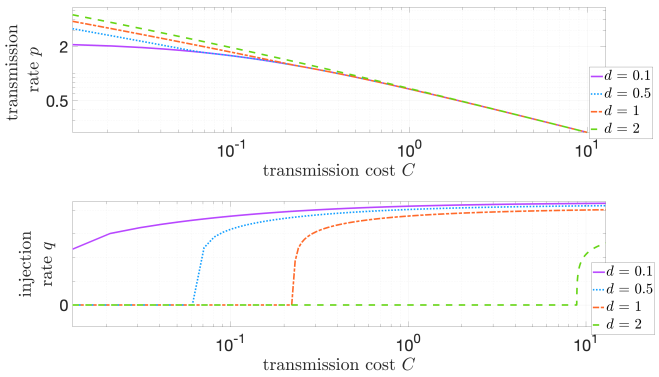


Fig. 9. Transmission rate p and injection rate q at the NE, for $K = 0.1$ and $d \in \{0.1, 0.5, 1, 2\}$.

Fig. 10 presents the cumulative distribution function of the probability of transitioning out of the W state over time. In scenarios with low costs of FDI, the controller strategically increases its update rate, resulting in a shorter duration spent in state W. Conversely, when both transmission and injection costs are high, both agents tend to reduce their transmission frequency, leading to longer dwell times in the W state, which may be critical for the peak AoII.

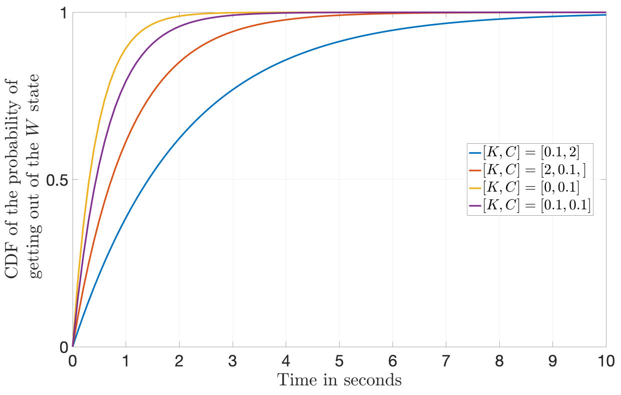


Fig. 10. Cumulative Distribution Function of the probability of getting out of W at NE as game-theoretic characteristic parameters change.

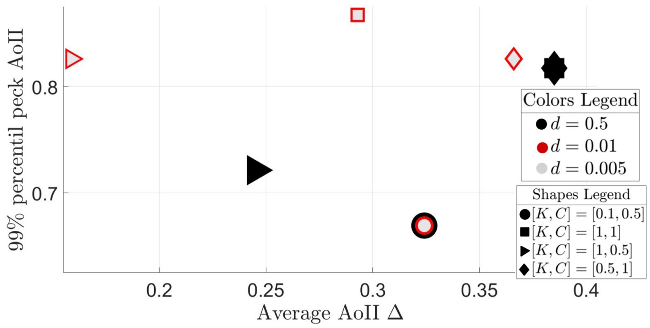


Fig. 11. On the abscissa, the mean AoII, and on the ordinate, is the 99% percentile of the peak AoII.

Fig. 11 illustrates the variations in average AoII and peak AoII at the NE, as the characteristic parameters of the system change. We observe that the peak AoII increases as the natural drift rate d decreases, while the average AoII decreases. Note that optimizing the peak AoII was not a primary objective in this study, but alternative strategic choices could potentially improve this parameter.

5 Conclusions

We analyzed a setting where a controller and a remote station exchange status updates over a network, while facing a malicious agent that sends fake updates. Using game theory, we studied the controller and adversary interaction [17].

The malicious agent aims to maximize AoII at the remote station while minimizing its own cost. At the same time, the controller seeks to minimize AoII at the remote station and its own cost. We computed the NE, which is both unique and guaranteed to exist in our setting. This reveals conditions where the adversary remains inactive, simplifying the problem to a regular nonlinear optimization. Even when the adversary is active, the controller's policy can achieve relatively unchanged performance compared to scenarios without the adversary.

Our analysis emphasizes the importance of vigilant monitoring to detect threats early and underscores the significance of further exploration of strategic scenarios. Future research can build upon these findings by considering more general scenarios [23]. Overall, we are able to shed light on the dynamics of controller-adversary interactions and enables the exploration of strategic scenarios.

Appendix A
Proof of the existence of an NE

Proof. The utilities defined by (8) are continuous, polynomial-like functions. Coherently with the adversarial setup set in our study, they follow a strictly monotonic behavior of the action chosen by the player they refer to. In other words, $u_{\mathrm{N}}(p, q)$ is strictly increasing in p for fixed q and $u_{\mathrm{M}}(p, q)$ is strictly increasing in q for fixed p. Moreover, they are also concave, i.e., the first and second derivatives are positive and negative, respectively [30].

As a result, we can invoke Glicksberg's theorem [31] that extends Nash' theorem to the continuous case.

In more detail, the NE can be found as a 0-Nash equilibrium, i.e., an ε-Nash equilibrium for ε=0 that is the limit point of a sequence of actions that alternates between best responses of the players, whose ε-convergence to a fixed point is guaranteed by the aforementioned properties of continuity, monotonicity, and concavity. □

Appendix B
Proof of the existence and uniqueness of K^*

Proof. By manipulating (11), we obtain the following inequality:

$$2K < \left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2}.$$

Adding $2C$ to both sides of the inequality, we have:

$$2K + 2C < \left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2} + 2C.$$

Substituting $\alpha = \sqrt{2K+2C}$, we can rewrite the inequality as

$$\alpha^2 < \left(\frac{1}{\alpha} + d\right)^{-2} + 2C.$$

For simplicity, define $f(\alpha) = \alpha^2$ and $g(\alpha) = \left(\frac{1}{\alpha} + d\right)^{-2} + 2C$.

We will show that there exists a unique value α^* such that $f(\alpha^*) = g(\alpha^*)$, and

$$\begin{cases} f(\alpha) < g(\alpha) & \text{if } \alpha < \alpha^* \\ f(\alpha) > g(\alpha) & \text{if } \alpha > \alpha^* \end{cases}$$

when $C, d \in (0, \infty)$. Note that α can only take positive values, so our interval of interest is $\alpha \in (0, \infty)$.

To prove this, we first show that $f(\alpha)$ and $g(\alpha)$ are continuous and differentiable in the interval $\alpha \in (0, \infty)$. $f(\alpha)$ is defined for every α and is therefore a continuous function, whereas $g(\alpha)$ is defined for $\alpha \neq -\frac{1}{d}$. Since d is a positive scalar and α only takes positive values, $g(\alpha)$ is also continuous in the interval of interest.

Next, consider their first order partial derivatives:

$$\begin{cases} \frac{\partial f(\alpha)}{\partial \alpha} = 2\alpha \\ \frac{\partial g(\alpha)}{\partial \alpha} = -\frac{2d}{(1+\alpha d)^3} + \frac{2}{(1+\alpha d)^2} \end{cases}.$$

Again, $\frac{\partial f(\alpha)}{\partial \alpha}$ is defined for every α and is therefore continuous. $\frac{\partial g(\alpha)}{\partial \alpha}$ is defined for $\alpha \neq -\frac{1}{d}$. Since d is positive and α only takes positive values, $\frac{\partial g(\alpha)}{\partial \alpha}$ is continuous in the interval of interest. Hence, both functions are continuous and differentiable in the interval.

Furthermore, by mathematical manipulation, it can be shown that both derivatives are strictly greater than 0 in the interval of interest, implying that they are monotonically increasing.

Through further mathematical manipulations, we can establish that $\frac{\partial f(\alpha)}{\partial \alpha} < \frac{\partial g(\alpha)}{\partial \alpha}$ for $\alpha \in (0, \infty)$. This implies that in the interval of interest, the function $f(\alpha)$ grows faster than the function $g(\alpha)$, and therefore $f(\alpha)$ and $g(\alpha)$ can intersect at most in one point.

Let us consider the limits of $f(\alpha)$ and $g(\alpha)$ as α tends to 0 from the right:

$$\lim_{\alpha \to 0^+} f(\alpha) = 0\,,$$

$$\lim_{\alpha \to 0^+} g(\alpha) = 2C$$

thus, it is clear that $f(0^+) < g(0^+)$. Next, consider the limits of $f(\alpha)$ and $g(\alpha)$ as α tends to $+\infty$, i.e.,

$$\lim_{\alpha \to +\infty} f(\alpha) = +\infty\,,$$

$$\lim_{\alpha \to +\infty} g(\alpha) = \frac{1}{d^2} + 2C\,.$$

Since C and d are both in $(0, \infty)$, it is clear that $f(\infty) > g(\infty)$. By the intermediate value theorem, we conclude that there exists at least one α^* such that $f(\alpha^*) = g(\alpha^*)$ in the interval $\alpha \in (0, \infty)$. Combining this with the fact that $\alpha^2 = 2K + 2C$, and $K, C \in (0, \infty)$, we conclude that for a given transmission cost C, there exists a unique K^* such that

$$K^* = \frac{\alpha^{*2} - 2C}{2}.$$

This completes the proof.

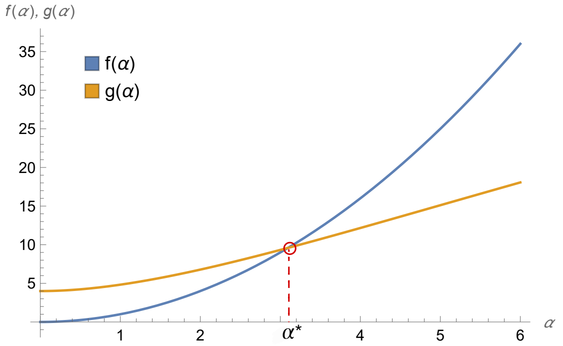


Fig. 12. $f(\alpha)$ and $g(\alpha)$ plot setting $d = 1$ and $C = 2$

.

□

References

[1] M. Robba, G. Ferro, R. Su, C. G. Cassandras, K. H. Johansson, and A. M. Annaswamy, "Guest editorial – special issue on smart city-networks," IEEE Trans. Control Netw. Syst., vol. 9, no. 4, pp. 1572–1575, 2022.

[2] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T. Qiu, and R. Y. Kwok, "Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach," IEEE J. Sel. Areas Commun., vol. 39, no. 2, pp. 463–478, Feb. 2021.

[3] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "A game of age of incorrect information against an adversary injecting false data," in Proc. IEEE CSR, 2023.

[4] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," IEEE Trans. Control Netw. Syst., vol. 4, no. 1, pp. 106–117, 2016.

[5] C. Wu, W. Yao, W. Pan, G. Sun, J. Liu, and L. Wu, "Secure control for cyber-physical systems under malicious attacks," IEEE Trans. Control Netw. Syst., vol. 9, no. 2, pp. 775–788, 2022.

[6] A. Chattopadhyay and U. Mitra, "Security against false data-injection attack in cyber-physical systems," IEEE Trans. Control Netw. Syst., vol. 7, no. 2, pp. 1015–1027, 2019.

[7] 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.

[8] R. Zhang and P. Venkitasubramaniam, "False data injection and detection in LQG systems: A game theoretic approach," IEEE Trans. Control Netw. Syst., vol. 7, no. 1, pp. 338–348, Mar. 2020.

[9] Y. Huang, J. Chen, L. Huang, and Q. Zhu, "Dynamic games for secure and resilient control system design," Nat. Sc. Rev., vol. 7, no. 7, pp. 1125–1141, 2020.

[10] K. Saurav and R. Vaze, "Game of ages in a distributed network," IEEE J. Sel. Areas Commun., vol. 39, no. 5, pp. 1240–1249, May 2021.

[11] A. Garnaev, W. Zhang, J. Zhong, and R. D. Yates, "Maintaining information freshness under jamming," in Proc. IEEE Infocom Wkshps, 2019.

[12] 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.

[13] 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.

[14] S. Saha, H. S. Makkar, V. B. Sukumaran, and C. R. Murthy, "On the relationship between mean absolute error and age of incorrect information in the estimation of a piecewise linear signal over noisy channels," IEEE Commun. Lett., vol. 26, no. 11, pp. 2576–2580, Nov. 2022.

[15] L. Badia, "Age of information from two strategic sources analyzed via game theory," in Proc. IEEE CAMAD, 2021.

[16] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in Prep. Wkshps SCS, vol. 1, 2010.

[17] M. Tian, Z. Dong, and X. Wang, "Analysis of false data injection attacks in power systems: A dynamic bayesian game-theoretic approach," ISA transactions, vol. 115, pp. 108–123, 2021.

[18] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," International Journal of Electrical Power & Energy Systems, vol. 104, pp. 169–177, 2019.

[19] M. Cao, "Merging game theory and control theory in the era of AI and autonomy," Nat. Sc. Rev., vol. 7, no. 7, pp. 1122–1124, Jul. 2020.

[20] L. Guo, H. Yu, and F. Hao, "Optimal allocation of false data injection attacks for networked control systems with two communication channels," IEEE Trans. Control Netw. Syst., vol. 8, no. 1, pp. 2–14, 2020.

[21] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in Proc. IEEE Infocom, 2012, pp. 2731–2735.

[22] 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.

[23] Y. Yang, B. Zhang, D. Guo, R. Xu, C. Su, and W. Wang, "Age of information optimization for privacy-preserving mobile crowdsensing," IEEE Trans. Emerg. Topics Comput., vol. 12, no. 1, pp. 281–292, 2024.

[24] S. Kriouile, M. Assaad, D. Gündüz, and T. Soleymani, "Optimal denial-of-service attacks against status updating," arXiv preprint arXiv:2403.04489, 2024.

[25] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, "Age of information: An introduction and survey," IEEE J. Sel. Areas Commun., vol. 39, no. 5, pp. 1183–1210, May 2021.

[26] A. Nayak, A. E. Kalør, F. Chiariotti, and P. Popovski, "A decentralized policy for minimization of age of incorrect information in slotted ALOHA systems," in Proc. IEEE ICC, 2023.

[27] Y. Chen and A. Ephremides, "Scheduling to minimize age of incorrect information with imperfect channel state information," Entropy, vol. 23, no. 12, p. 1572, Nov. 2021.

[28] C. Kam, S. Kompella, and A. Ephremides, "Age of incorrect information for remote estimation of a binary Markov source," in Proc. IEEE Infocom Wkshps, 2020.

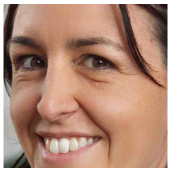
[29] S. Kriouile and M. Assaad, "Minimizing the age of incorrect information for real-time tracking of Markov remote sources," in Proc. IEEE ISIT, 2021, pp. 2978–2983.

[30] 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.

[31] I. Glicksberg and O. Gross, Notes on Games over the Square, ser. Annals of Mathematics Studies. Princeton University Press, 1950, vol. 28, pp. 173–183.

Valeria Bonagura (ST'23) received the M.sc in Automation Engineering in 2022 from University of Roma Tre, Italy, where she is currently pursuing the Italian National Ph.D programme in Autonomous Systems (DAUSY), under the supervision of Prof. Stefano Panzieri and Prof. Federica Pascucci. Her main research interests include distributed systems, distributed estimation, and model-based fault and anomaly detection.

Stefano Panzieri (M'92) received the M.sc degree in electronic engineering and the Ph.D. degree in systems engineering from the University of Roma La Sapienza, Rome, Italy, in 1989 and 1994, respectively. He is a Full Professor at the Department of Civil, Computer Science and Aeronautical Technologies Engineering of the University of Roma Tre of Rome, where he directs the Models for Critical Infrastructure Protection Laboratory (MCIP lab). His research interests are in the field of industrial control systems, robotics and sensor fusion.



Federica Pascucci (Senior Member, IEEE) received the Laurea degree (M.S.) in computer science and automation engineering from the University Roma Tre, Rome, Italy, in 2000, and the Ph.D. degree in system engineering from the University of Rome “La Sapienza,” Rome, in 2004. She has been an Assistant Professor with the University of Roma Tre since 2005, where she is currently an Associate Professor. Her research interests include wireless sensor networks, indoor localization, cyber–physical systems, industrial control systems, and critical infrastructure protection

Leonardo Badia (Senior Member, IEEE) received the Ph.D. in information engineering from the University of Ferrara, Italy, in 2004. From 2002 to 2003, he was at the RST Labs (currently, Wireless@KTH), Royal Institute of Technology, Sweden. In 2006, he joined the IMT Institute for Advanced Studies, Lucca, Italy. In 2011, he moved to the University of Padua, Italy, where he is currently Associate Professor. His research interests include mathematical analysis of wireless networks, cross-layer optimization, and applications of game theory to wireless communications. He is an active referee of scientific journals and TPC member for conferences in the areas of communications and networking.