Strategic Control Against an Intruder for Timely and Accurate Updates to a Reactive Receiver

Valeria Bonagura*†, Stefano Panzieri*, Federica Pascucci*, and Leonardo Badia§
∗ University of Roma 3, 00146 Rome, Italy. Email: { valeria.bonagura, stefano.panzieri, federica.pascucci} @uniroma3.it
† Politecnico of Bari, 70125 Bari, Italy. Email: vbonagura@phd.poliba.it
§ Dept. University of Padova, 35131 Padova, Italy. Email: leonardo.badia@unipd.it

Abstract—**Remote sensing is a key component of control for cyber-physical systems, and is susceptible to the injection of false data by adversaries. We consider a transmitter sending status updates about a physical process to a receiver, incurring a cost for each transmission. We use a two-state Markov chain to represent whether the receiver has correct information about the process or not. In normal conditions, transitions to the wrong state happen because the physical process drifted away from the last reported value and the transmitter did not update the receiver yet. However, an adversary can also inject false data to increase the rate of such a transition. The receiver cannot tell the malicious updates apart from the legitimate ones, but, upon detecting a higher arrival rate of data, can counteract it by requesting additional legitimate updates from the transmitter. The ensuing interaction can be examined using game theory, treating both the receiver and the adversary as strategic players. Specifically, they act as a minimizer and a maximizer, respectively, of the age of incorrect information at the receiver's side, while also minimizing their activity costs. We analyze the equilibria of the game and evaluate the impact of strategic decision-making on the system performance.**

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

I. Introduction

Cyber-physical systems (CPS), combining physical components with communication networks, represent a paradigm to provide new functionalities for remote control, especially in the context of critical infrastructures or industrial facilities [1], [2]. For example, within the industrial environment, programmable logic controllers (PLCs), regularly used to control the physical process, can periodically transmit updates to a remote supervisory control and data acquisition (SCADA) system [3]. This allows operators to monitor the evolution of the physical processes without needing on-site presence.

Unfortunately, this fusion of the physical and cyber realms introduces potential complexities, most notably an expanded attack surface for cyber threats [4]. The expansion of the network communication, together with the lack of human assistance, is prone to cybersecurity vulnerabilities, such as jamming, eavesdropping, and false data injection [5]–[9].

This has prompted research into the performance evaluation of status update exchanges over communication channels. A metric widely used in the recent literature to quantify the information timeliness at the receiver's side is Age of Information (AoI) [10], [11], defined as the time elapsed since the last received update. AoI is useful to assess whether the receiver can make appropriate control decisions since it has fresh information available. However, it is often not appropriate for scenarios where relevant new information is scarce and sporadic. Indeed, AoI assumes that every status update is bringing relevant information, whereas, in typical industrial systems, updates may be unnecessary unless system conditions change [12].

To account for this discrepancy, some researchers proposed age of incorrect information (AoII) [13], which measures the time elapsed since the first change in the process state after receiving an update. This may be more relevant in systems where information accuracy is critical, such as control or safety-related applications [14], [15], as a high AoII can indicate that the information being used is inaccurate [16].

We consider a scenario involving the exchange of state updates between a transmitter and a receiver over a network, considering the presence of a malicious agent injecting false data in the communication. The receiver is assumed to be unable to distinguish between regular and malicious data, but it can overall react to the anomaly, and implement a corrective action. This scenario is versatile and applicable to various cyber-physical systems in IoT or tactical environments.

The transmitter sends updates to the receiver so as to monitor the current system state. The transmission rate is set to minimize AoII at the receiver's side, yet the malicious agent's intervention increases AoII. The receiver is reactive, i.e., it can not only detect the anomalously larger data rate when the attack occurs but also intervene by requesting the transmitter to increase the rate of updates. This setup calls for a game-theoretic approach [17], [18], where the receiver and the adversary act as rational agents with opposite objectives: minimizing and maximizing AoII. The resulting game is non-zero-sum, as both players incur transmission costs in addition to their objective related to AoII [19].

Our key finding is that, under rational behavior, the adversary's attacks can be reasonably contained. This analysis is valuable for improving the security of CPSs and can guide

Project co-founded by the European Union - Next Generation Eu - under National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Investment 3.3- Decree No. 352 (9^{th} April 2022) of Italian Ministry of University and Research - Concession Decree No. 2153 (28^{th} December 2022) of the Italian Ministry of University and Research, Project code D93D22001390001, within the Italian National Program PhD Programme in Autonomous Systems (DAuSy)

further investigations into strategic interactions [20].

The rest of this paper is organized as follows. Section II discusses the state of the art. Section III introduces the system model, and Section IV presents the game theoretic analysis. Numerical results are shown in Section V. The paper is finally concluded in Section VI.

II. Related Work

AoII expands the AoI concept to combine information freshness and correctness, weighing the drift toward incorrect data with an increasing function of elapsed time [13]. Previous research [12], [16], [21] primarily focused on enhancing AoII performance or reading it as an extrapolation of error and delay metrics. For example, [12] considers AoII minimization through proper scheduling of updates, whereas [21] explores the minimization of AoII by optimizing slotted ALOHA parameters. Conversely, [16] discusses the relationship between reporting errors and AoII for specific signals and updating policies, i.e., random updates and linear piecewise signals in the former, and a binary Markov source and different update policies in the latter.

Differently from these previous studies, we consider an adversarial setup that is studied through game theory [17]. Game theory is a powerful tool that has been successfully used in cyber-physical systems to model strategic interactions and refine agent behavior. For instance, it has found extensive application in multi-robot systems coordination [18] or the shared exploration of structured workspaces like building floors [14]. Nevertheless, the literature is scarce for what concerns addressing AoII within the overall problems of data security and adversarial scenarios.

Most existing game theoretic approaches for AoI and AoII just consider symmetric problems with competing sources trying to deliver their own data under limited resources or mutual interference [22]. From the perspective of security, this can only serve to evaluate situations like privacy-preserving crowdsensing, but does not address malicious strategic agents. When adversarial attacks are considered, they most often focus on jamming [5], [7], [23], rather than malicious data injection [8]. This contrasts with our research, which addresses the latter more sophisticated attack.

Our study introduces an original perspective by applying game theory to analyze the counterposition between a legitimate agent and an adversary, considering their strategic interplay in the context of AoII and malicious data injection. This is reminiscent of other studies previously performed by some of the authors, such as [6], where we considered a similar interaction but taking place between a legitimate transmitter and an eavesdropper, so that the ultimate task of the attacker is to compromise data confidentiality but not their integrity.

In [9], we also studied false data injection for vehicular networks, which is a context where accuracy and timeliness of data is important. However, the payoff of the players is not directly related to AoII and the entire strategic interaction is much simpler than what we did here. Conversely, [4] explores the techniques to detect and counteract malicious injections in practice, but does not take a game theoretic stance, since the adversary is not reacting to the network defenses.

Finally, in [19] we considered a scenario similar to the one analyzed in this paper. We utilized game theory for a game over a two-state Markov chain, with an adversarial setup of two players acting as minimizer and maximizer of AoII, respectively. However, there is an important difference related to the reactive role of the receiver in the present paper. Indeed, that previous analysis just considered all the strategic capabilities for the legitimate network agent as concentrated at the transmitter's side. In the present study, we consider the additional feature of the receiver detecting the increased data injection and triggering countermeasures from the transmitter. As we will show in the mathematical analysis, this changes the equilibrium conditions significantly and allows for different outcomes to be achieved, whereas in [19] the only way to defeat the adversary is to hope that its cost is too high. This makes our approach particularly relevant in the context of CPSs, since it may lead to constructive implementations of network defense mechanisms.

III. System Model

In this study, we investigate a transmitter that periodically sends updates to a receiver. For example, the transmitter could be a PLC sending system output and control input updates to a remote SCADA system for plant monitoring.

At time t^*, an adversary gains access to the communication channel and injects false updates to the receiver at a certain rate. The receiver cannot distinguish between false and legitimate updates but can detect anomalies attributed to the adversary's actions. Unlike our previous work [19], where we assumed the transmitter was initially aware of the adversary, we now consider a more realistic scenario where anomaly detection triggers corrective action. Upon detecting anomalies, the receiver requests the transmitter to increase its transmission rate. We assume the adversary can access the communication channel but not vice versa.

The following equations mathematically describe the underlying dynamics of the system:

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

In this context, the variable $x(t)$ represents the state of the system at time t, $u(t)$ signifies the control input, and $y(t)$ denotes the output at time t. The $f(\cdot)$ and $h(\cdot)$ represent the state transition and output selection functions, respectively.

The transmitter sends updates to a receiver denoted as R within our framework. The communication involves transmitting the output measurement $y(t)$ with a rate p. We assume negligible propagation delay between the transmitter and the receiver, enabling us to work with time calculations from either end of the communication channel.

AoI is employed to gauge the timeliness of the information. At time t, it is defined as

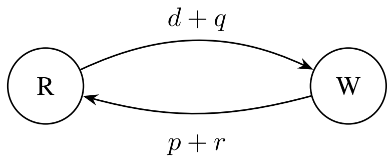

Fig. 1. Continuous time Markov process with the respective rates of moving from one state to one another. The sum of d (i.e., the natural drift rate) and q (i.e., the transmission rate for the malicious agent M) gives the transition rate from R to W. The sum of p (i.e., the natural drift rate of the physical system) and r (i.e., that is, the increase of transmission rate requested by R) gives the transition rate from W to R.

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

Here, t_u represents the time corresponding to the reception of the most recent update just before time t, inclusively.

To model the system's behavior effectively, we introduce a continuous-time Markov chain with two states: "right" (R) and "wrong" (W). Transitions between these states depend on system dynamics and actions, as illustrated in Fig. 1. The malicious entity termed an "adversary" (M), can increase transitions to state W at a rate denoted by q. However, the receiver can respond by requesting the transmitter to increase its transmission rate, boosting transitions to state R. The transmission rate increase is denoted by r. If the nominal transmission rate is p, after the corrective action, it becomes $p + r$.

In our model, the corrective action implemented by the receiver R is driven toward the general objective of minimizing its AoII, whose value $\delta(t)$ at time t is defined as

$$\delta(t) = f(k) \cdot g(y(t), y(t_u), y(t_m)), \tag{3}$$

where function $g(\cdot, \cdot, \cdot)$ quantifies the discrepancy between the current system output $y(t)$, the most recent correct update transmitted $y(t_u)$, and the latest false update sent by the malicious agent M, denoted as $y(t_m)$. The function $f(\cdot)$ incorporates the penalties that increase as the discrepancy measured by $g(\cdot, \cdot, \cdot)$ escalates.

We consider a specific form of $g(\cdot, \cdot, \cdot)$:

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

This function quantifies the disparity between the present system output $y(t)$, the most recent correct update $y(t_u)$, and a defined threshold ϑ. Following a system drift or a malicious transmission, we assume this disparity persists until a new update occurs.

The linear time-increasing penalty $f(\cdot)$ is defined as:

$$f(t) = t - t_d \tag{5}$$

where t_d is the last time-instant over a period where $g(y(t), y(t_u), y(t_m)) = 0$. To gain insight into the system's dynamics, we analyze the expected value of AoII, represented as $\Delta = \mathbb{E}_t\big[\delta(t)\big]$, computed as:

$$\begin{aligned} \Delta &= \frac{1/(2 \cdot (p + r)^2)}{1/(p + r) + 1/(d + q)} \\ &= \frac{d + q}{2(p + r)(d + p + q + r)} \end{aligned} \tag{6}$$

In (6), the numerator $1/2(p + r)^2$ represents the average area below the AoII function, specifically denoted by (4), within a given period. In fact, choosing a linear function $f(t)$ as (5), the area to be calculated is that of a triangle. The denominator $1/(p + r) + 1/(d + q)$ signifies the expected value of the time elapsed between two consecutive updates, referred to as a period. See also [19] for further details. Furthermore, we introduce cost terms associated with the nominal transmission rate of the transmitter, the increase of transmission rate requested by agent R, and the injection of false data by agent M. These terms can be interpreted as energy expenditures or limiting factors on the frequency of their activities. We assume that these costs are linearly proportional to their activity rate, denoted as r and q for agents R and M, respectively. The linear coefficients (representing the unit prices) are denoted as $K > 0$ for the transmission rate increase and $\alpha K > 0$ for the malicious injection.

Based on these definitions, we formulate utility functions for both the receiver and the malicious agent:

$$u_{\mathrm{R}}(q, r) = -\Delta - K \cdot r, \quad u_{\mathrm{M}}(q, r) = \Delta - \alpha K \cdot q. \tag{7}$$

In this context, $u_{\mathrm{R}}(q, r)$ represents the utility function for the receiver, aiming to minimize the combined metric of the expected AoII and the cost of increasing the transmission rate. Conversely, $u_{\mathrm{M}}(q, r)$ is the utility function for the malicious agent to maximize the expected AoII experienced by the transmitter while considering the associated cost of malicious injections.

In ideal conditions, where no malicious entities exist, the transmitter can arbitrarily choose the transmission rate p, and in this paper, we assume that it does so to minimize AoII. However, we assume the transmitter faces a transmission cost Jp, i.e., proportional to p with unit price J, when transmitting. To find the optimal transmission rate p, we can optimize a single-variable function that balances AoII and the associated transmission cost:

$$p = \arg\max_{p} \{-\Delta - J \cdot p\} \tag{8}$$

where in Δ, $r = 0$ and $q = 0$. Note, that (8) is a single-player optimization, and is not involved in the strategic interaction.

In our previous work [19], we showed that in the absence of a malicious agent, there is only one value of p that maximizes (8), which is

$$p = \frac{1}{6}\left(-3d + \sqrt{3}\sqrt{s} + \frac{3\sqrt{\frac{d^2}{3} + \frac{1}{3}s + \frac{2\sqrt{3}d}{J\sqrt{s}}}}{J}\right). \tag{9}$$

where:

$$s = d^2 + \frac{d^4 J}{t} + \frac{t}{J}$$

and

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

Table I lists the notation used.

TABLE I
NOTATION SUMMARY

Parameter	Symbol
Cost of increasing the transmission rate	K
Injection cost for the malicious agent	αK
Nominal transmission cost for the transmitter	J
Natural drift rate of the physical system	d
Variable	**Symbol**
Nominal transmission rate for transmitter	p
Increase of transmission requested by R	r
Injection rate for M	q

IV. Game-Theoretic Analysis

We designate the receiver and the adversary as two rational agents, denoted as R and M, respectively. We assume that upon the commencement of an adversary's attack, the receiver can promptly detect the adversary's presence and take corrective actions.

Due to the simultaneous presence of R 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 $\mathcal{P} = \{\mathrm{R}, \mathrm{M}\}$, their respective set of actions $\mathcal{A}$ where player R chooses $r \in [0, \infty)$ and M chooses $q \in [0, \infty)$, and the utility set $\mathcal{U} = \{u_{\mathrm{R}}, u_{\mathrm{M}}\}$.

We characterize the game as *static*, which implies that the players just choose one value of their action independently and unbeknownst to each other. The sustainable outcome for a distributed control is typically characterized as the Nash equilibrium (NE).

For the specific game under exam, the NE obeys the properties formalized by the following theorem.

Theorem 1 (*Existence and Uniqueness of the NE*)**.** Game $\mathcal{G}$ admits a unique NE.

The proof is provided in Appendix A.

Now, we are ready to derive numerically the NE for the problem at hand. To this end, we simultaneously maximize the objectives of the two agents, which is equivalent to set:

$$\frac{\partial u_{\mathrm{M}}(q,r)}{\partial q} = 0 \qquad \frac{\partial u_{\mathrm{R}}(q,r)}{\partial r} = 0 \tag{10}$$

which implies:

$$\frac{\partial \Delta}{\partial q} = \alpha K \qquad \frac{\partial \Delta}{\partial r} = -K. \tag{11}$$

Rearranging these terms in (11) gives:

$$\begin{cases} q = \frac{1}{\sqrt{2\alpha K}} - d - p - r \\ r = \frac{1}{\sqrt{(1+\alpha)2K}} - p \end{cases} . \tag{12}$$

Within (12), K and α must be such that the requirement that q and R are positive is met. If (12) results in $q < 0$, the adversary has no advantage in injecting false data and is silent. Similarly, if (12) results in $r < 0$, for the receiver is too expensive to take countermeasures and increase the transmission rate.

From the second equation in (12), we obtain that if

$$K < \frac{1}{2\alpha p^2} - 1$$

then the receiver gains an advantage in requesting the transmitter to increase the transmission rate.

In other terms, considering the second equation in (12), we can write

$$r + p = \frac{1}{\sqrt{(1+\alpha)2K}} . \tag{13}$$

We can interpret $\frac{1}{\sqrt{2K(1+\alpha)}}$ as a saturation point for the transmitter's transmission rate. When p alone equals this saturation point, pushing the transmission rate any higher becomes unfeasible.

From the first equation in (12), we know that the malicious agent gains an advantage in transmitting if $q > 0$, and therefore

$$\frac{1}{\sqrt{2K}} \left(\frac{\sqrt{1+\alpha} - \sqrt{\alpha}}{\sqrt{\alpha(1+\alpha)}} \right) - d > 0 .$$

And, defining

$$h(\alpha) = \left(\frac{\sqrt{1+\alpha} - \sqrt{\alpha}}{\sqrt{\alpha(1+\alpha)}} \right) ,$$

we conclude that the malicious agent gains an advantage in transmitting if

$$h(\alpha) > d\sqrt{2K}.$$

Note that

$$\frac{\partial h(\alpha)}{\partial \alpha} = \frac{-1 - 2a - a^2 + a^{\frac{3}{2}}\sqrt{1+a}}{2\sqrt{1+a}(a(1+a))^{\frac{3}{2}}} < 0 ,$$

holds for all $\alpha > 0$, and this implies that $h(\alpha)$ is monotonically decreasing.

Based on those observations, the NE is as follows:

$$q = \begin{cases} \frac{1}{\sqrt{2\alpha K}} - d - p - r & \text{if } h(\alpha) > d\sqrt{2K} \\ 0 & \text{otherwise} \end{cases} \tag{14a}$$

$$r = \begin{cases} \frac{1}{\sqrt{(1+\alpha)2K}} - p & \text{if } K > \min\{\frac{1}{2\alpha p^2} - 1, \frac{h^2(\alpha)}{2d^2}\} \\ 0 & \text{otherwise} \end{cases} . \tag{14b}$$

V. Numerical Results

In Fig. 2, we plot the optimal transmission rate p in the absence of an adversary versus the nominal transmission cost J, as resulting from (8). From this plot, it is visible that for higher values of the drift rate, the optimal solution is to increase the transmission rate to reduce the average AoII

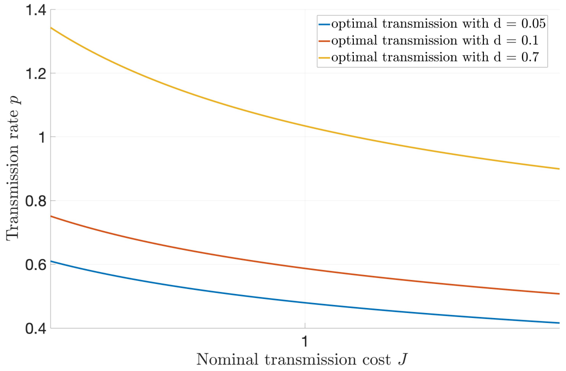

Fig. 2. Optimal transmission rate p in the absence of an adversary.

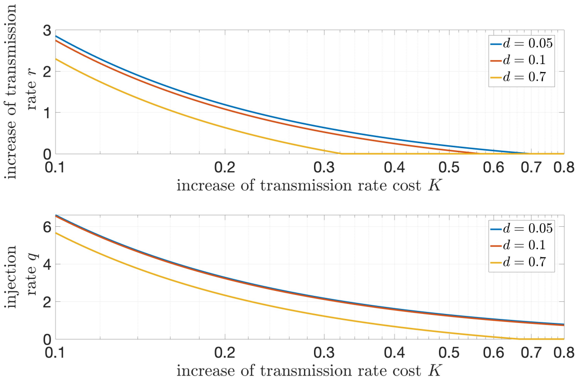

Fig. 3. Increase of transmission rate R and injection rate q at NE, for $\alpha = 0.5$. The nominal transmission cost for the receiver was set $J = 1$, thus (8) results in p=$[0.4791, 0.5869, 1.0341]$ for d=$[0.05, 0.1, 0.7]$, respectively.

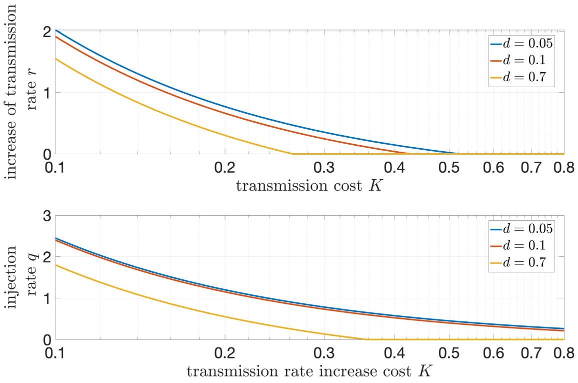

Fig. 4. Increase of transmission rate R and injection rate q at NE, for $\alpha = 1$. The nominal transmission cost for the receiver was set $J = 1$, thus (8) results in p=$[0.4791, 0.5869, 1.0341]$ for d=$[0.05, 0.1, 0.7]$, respectively.

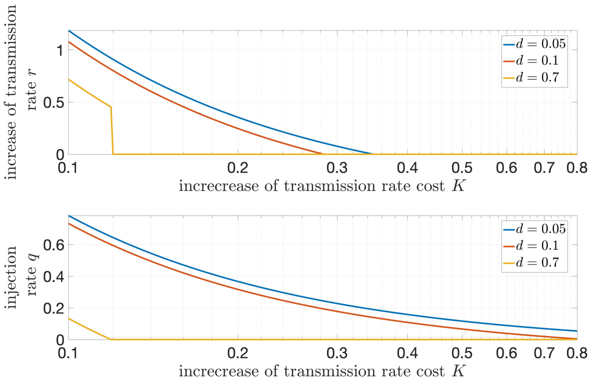

Fig. 5. Increase of transmission rate R and injection rate q at NE, for $\alpha = 2$. The nominal transmission cost for the receiver was set $J = 1$, thus (8) results in p=$[0.4791, 0.5869, 1.0341]$ for d=$[0.05, 0.1, 0.7]$, respectively.

at the receiver. On the other hand, as the transmission cost increases, the optimal transmission rate decreases.

Figs. 3, 4, and 5 analyze how the data injection attack affects the NE, depending on the cost of increasing the transmission rate, the injection cost, and the network drift. These figures consider scenarios where the injection cost of the adversary, compared to the cost of increasing the transmission rate, is halved, the same, or doubled, respectively. The plots show the values of p and R at NE versus the cost of increasing the transmission rate, and all three scenarios were analyzed in the case where the drift rate d is 0.05, 0.1, and 0.7.

As also emerged when analyzing Fig. 2, the effect of increasing the drift rate is an increase in the transmission rate. For the adversary, on the other hand, having a higher drift rate implies that the receiver more frequently has incorrect information about the current state of the system, thus implying a lower injection rate. This phenomenon can be seen in all three analyzed cases. The effect of an increase in the adversary injection rate, on the other hand, is a leftward shift of the K threshold value that causes the adversary to not intervene. In Figs. 3, 4 the rate R goes to zero before the injection rate does, and this implies that for a range of values for K, the adversary will inject false data without allow the legitimate agent to intervene. Only in Fig. 5, for $d = 0.7$ the injection rate q go to zero faster than the increase of transmission rate R, and therefore in our simulations this is the only scenario where the receiver can defend for all possible values of K.

VI. Conclusions

We analyzed a CPS, where a transmitter sends updates to a receiver, and an adversary can compromise the communication by sending malicious updates to the receiver. We assume that the receiver can detect the attacker's presence but cannot differentiate between genuine and fake updates.

To counteract this attack, the receiver can request an increase in the transmission rate from the transmitter.

We modeled the interaction between the transmitter and the adversary using game theory. The malicious agent incurs a cost that is proportional to the rate of injection, while the legitimate agent incurs a cost that is proportional to the increase in the transmission rate. The objective of the malicious agent is to maximize AoII at the receiver while minimizing its own cost. The legitimate agent aims to minimize AoII at the receiver and its own cost. We computed the NE, which is both unique and guaranteed to exist in our scenario.

This reveals that three possible scenarios can unfold based on the system parameters, such as the nominal drift rate, transmission cost, increase in transmission rate, and injection cost. In the first scenario, the receiver can successfully request an increase in the transmission rate, thereby reducing the attack's impact on the system. Alternatively, it may be too costly to request an increase in the transmission rate, allowing the adversary to intervene without hindrance. Finally, it may also be too costly for the adversary to intervene.

This underscores the importance of vigilant monitoring to detect potential threats early and to remain aware of their presence. Furthermore, future research can expand upon these findings by considering more general scenarios and exploring advanced strategic interactions.

Appendix A
Proof of the existence and uniqueness of the NE

Existence: The utilities in (7) are continuous and rational. Consistent with our adversarial framework, they display a strictly monotonic response to the choices made by the respective players. In other words, for a fixed value of one parameter, $u_{\mathrm{T}}(r, q)$ is strictly increasing in the other parameter, while $u_{\mathrm{M}}(r, q)$ is strictly increasing in the opposite parameter. Furthermore, these functions possess concave properties, i.e., the first and second derivatives are positive, and negative, respectively [24]. Thus, Glicksberg's theorem [25] guarantees the existence of a NE in the continuous domain.

Such an NE can be identified as a ”0-Nash equilibrium,” which is effectively an ε-Nash equilibrium with ε set to 0. This serves as the limiting point of a sequence of actions that alternates between the best responses of the players. The ε-convergence to a fixed point is guaranteed by the properties of continuity, monotonicity, and concavity.

Uniqueness: It directly results from the utilities maintaining monotonic behavior across their entire range. As a result, the ε-fixed point they converge to remains constant, ensuring the existence of a single solution.

References

[1] V. Bonagura, C. Foglietta, S. Panzieri, and F. Pascucci, “Advanced intrusion detection system for industrial cyber-physical systems,” *IFAC-PapersOnLine*, vol. 55, no. 40, pp. 265–270, 2022.

[2] A. Buratto, B. Yivli, and L. Badia, “Machine learning misclassification within status update optimization,” in *Proc. IEEE COMNETSAT*, 2023.

[3] S. Yin, S. X. Ding, X. Xie, and H. Luo, “A review on basic data-driven approaches for industrial process monitoring,” *IEEE Trans. Ind. Electron.*, vol. 61, no. 11, pp. 6418–6428, 2014.

[4] V. Bonagura, C. Foglietta, S. Panzieri, and F. Pascucci, “Enhancing industrial cyber-physical systems security with smart probing approach,” in *Proc. IEEE CSR*, 2023, pp. 387–393.

[5] S. Bhattacharya and T. Başar, “Game-theoretic analysis of an aerial jamming attack on a UAV communication network,” in *Proc. IEEE ACC*, 2010, pp. 818–823.

[6] L. Crosara, N. Laurenti, and L. Badia, “It is rude to ask a sensor its age-of-information: Status updates against an eavesdropping node,” in *Proc. IEEE BalkanCom*, 2023.

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

[8] B. K. Sethi, A. Singh, S. Mohanty, D. Singh, and R. Misra, “Game theoretic smart residential buildings energy management system under false data injection attack,” *IEEE Internet Things J.*, vol. 10, no. 1, pp. 110–119, 2022.

[9] L. Crosara, M. Brocco, C. Cavalagli, X. Wu, E. Gindullina, and L. Badia, “Data injection in a vehicular network framed within a game theoretic analysis,” in *Proc. IEEE MedComNet*, 2023, pp. 25–28.

[10] 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.

[11] L. Badia, “Analysis of age of information under SR ARQ,” *IEEE Commun. Lett.*, vol. 27, no. 9, pp. 2308–2312, Sep. 2023.

[12] 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.

[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] K. Skrzypczyk, “Game theory based task planning in multi robot systems,” *Int. J. Simul.*, vol. 6, no. 6, pp. 50–60, 2005.

[15] U. Michieli and L. Badia, “Game theoretic analysis of road user safety scenarios involving autonomous vehicles,” in *Proc. IEEE PIMRC*, 2018, pp. 1377–1381.

[16] 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.

[17] L. Prospero, R. Costa, and L. Badia, “Resource sharing in the Internet of Things and selfish behaviors of the agents,” *IEEE Trans. Circuits Syst. II*, vol. 68, no. 12, pp. 3488–3492, Dec. 2021.

[18] Y. Meng, “Multi-robot searching using game-theory based approach,” *Int. J. Adv. Robotic Syst.*, vol. 5, no. 4, p. 44, 2008.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] 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.

[25] 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.