Controlling Age of Incorrect Information Violation Under Data Drift and Strategic Attacks

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

***Abstract*—We study a control system where sensor measurements are transmitted to a remote station. Information may become outdated due to system drift or compromised by malicious false data injection. To quantify the impact of staleness and inaccuracy in the information at the receiver's side, we use Age of Incorrect Information (AoII). In particular, we consider the Excess AoII above a certain threshold as our key objective to minimize, which we argue to be a sensible goal for many real-time control systems. We adopt a game-theoretic framework to model the strategic interaction between a transmitter, which aims to minimize both Excess AoII and transmission costs, and a malicious agent, which seeks to maximize the same Excess AoII metric while minimizing its own costs. Our analysis reveals the existence of a Nash equilibrium for this game, and we investigate how the system parameters influence the adversary's decision to attack, identifying the conditions under which an attack becomes advantageous or not.**

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

I. Introduction

Real-time control in remote sensing is essential for cyber-physical systems, as applications like industrial automation, healthcare monitoring, and critical infrastructure management require timely and accurate data [1]–[3]. Rapid data processing enables effective decision-making and reduces risks associated with outdated or incorrect information, which can lead to harmful decisions [4].

However, remote sensing and real-time control are susceptible to noise and interference, which can be exacerbated by data drift caused by changing conditions or malicious interventions [5].

In response to the growing demand for low latency in real-time applications, the concept of Age of Information (AoI) was introduced over a decade ago in seminal works such as [6]. This concept has recently been extended to the Age of Incorrect Information (AoII) [7], which quantifies the impact of information staleness and inaccuracy. AoII serves as a multi-faceted penalty metric that combines the increase in information staleness with its divergence from the true value, making it particularly suitable for systems where status updates occur only during dynamic changes [8].

In applications involving remote sensing, a critical challenge is the selection of the transmission rate. This choice must balance the freshness of the data with the associated costs of communication [9]. A higher transmission rate can lead to more timely updates, thus reducing AoI and improving decision making. However, it also incurs greater operational costs, which can be a significant concern in resource-constrained environments.

Moreover, communication over networks is not immune to cyberattacks that can compromise the integrity of transmitted data [10]. Such attacks can alter the communication process, leading to the dissemination of incorrect or outdated information. Therefore, it is essential to make informed choices about transmission strategies that not only enhance data freshness, but also improve the security of the communication process. Implementing robust security measures and adaptive transmission strategies can help mitigate the risks posed by potential cyber threats, ensuring that the system remains resilient and reliable in the face of adversarial conditions.

Various adaptations of AoI have emerged to capture different perspectives relevant to network control objectives. For instance, [11] suggests that while limited increases in AoI are unavoidable, it is more pragmatic to focus on reducing the probability that information staleness exceeds certain threshold requirements. AoI violations can be defined as instances in which the staleness of information exceeds a predetermined limit, which can be related to the instantaneous AoI value or the peak age [12].

Multi-source systems can be scheduled to ensure guarantees on (peak) AoI violations, as demonstrated in [13]. The penalty for a violation can be quantified by measuring the probability that AoI exceeds the threshold, similar to an outage [14], or by measuring the extent to which AoI exceeds this threshold, which we refer to as *excess AoI*.

Recent research has also explored the vulnerability of status update systems to cyberattacks, including denial-of-service attacks and eavesdropping. For instance, [15] investigated optimal jamming policies in status update systems, demonstrating that threshold-based strategies are effective for both AoI and AoII metrics from the attacker's perspective. In contrast, [16] examined the trade-off between AoI at legitimate receivers and eavesdroppers, employing a social welfare framework to optimize updates and balance information freshness with security.

Our approach is different since it considers a scenario where both the system controller and malicious attackers act as *strategic* players, leading to a game-theoretic framework

[17]–[21]. This setup allows us to explicitly focus on an adversarial context, where the interaction between the system and an attacker is modeled as a dynamic game, establishing the existence of a unique stationary equilibrium [18].

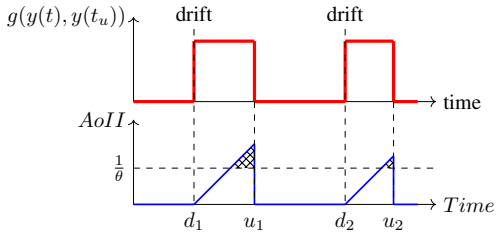

Fig. 1. Age of Incorrect Information

A. Proposed Metric: Excess AoII

We propose *Excess Age of Incorrect Information (Excess AoII)* as a new performance metric that captures the impact of both outdated and inaccurate information in remote monitoring systems. In contrast to classical AoI or AoII, Excess AoII introduces a threshold-based evaluation, penalizing the system only when the inaccuracy becomes critical, i.e., when it exceeds a predefined tolerance level.

Let $y(t)$ represent the true value of the quantity monitored at time t, and $y(t_u)$ the most recent value received by the remote system at the update time t_u. The *instantaneous AoII* is defined as:

$$\delta(t) = (t - t_d) \cdot g(y(t), y(t_u)), \tag{1}$$

where t_d is the most recent time instant when the system enters an incorrect state due to a change (or *drift*) in the monitored value, and $g(y(t), y(t_u)) \in \{0, 1\}$ is a binary indicator of correctness. Specifically, $g(y(t), y(t_u)) = 1$ if the received value $y(t_u)$ no longer matches the current state $y(t)$, and 0 otherwise.

We assume that once $g(\cdot)$ becomes 1 (that is, the information is incorrect), it remains so until a new accurate update is received. The frequency at which drifts occur is modeled using a parameter called *drift rate*, denoted as d, which represents the average number of incorrect state transitions per unit time (i.e., the reciprocal of the expected time between successive drifts).

To isolate and quantify only significant inaccuracies, we introduce a threshold $1/\theta$, corresponding to the maximum tolerable AoII. The Excess AoII metric is defined as:

$$\delta_{1/\theta}(t) = \left(\delta(t) - \frac{1}{\theta}\right) \cdot \mathbf{1}_{\{\delta(t) \geq \frac{1}{\theta}\}}, \tag{2}$$

where $\mathbf{1}_{\{\delta(t) \geq \frac{1}{\theta}\}}$ is the indicator function, equal to 1 when AoII exceeds the threshold, and 0 otherwise. Thus, the Excess AoII captures only those periods during which the receiver is exposed to outdated and incorrect information beyond the acceptable limit.

Fig. 1 illustrates how the Excess AoII corresponds to the shaded regions above the threshold line. These areas highlight the severity and duration of unacceptable information inaccuracies.

We study this metric in a game-theoretic framework, where a system controller chooses a transmission rate p to minimize Excess AoII and its associated costs, while a malicious agent attempts to increase the metric by injecting false updates at a rate q. The interaction between the two strategic entities forms the basis for our analysis.

B. Paper Contributions

The key contributions of this paper are as follows.

I. We introduce *Excess AoII*, a threshold-based metric that extends AoII to focus on periods of critical system inaccuracy.
II. We formulate a *game-theoretic model* between a transmitter and a strategic attacker, where each agent aims to optimize their utility based on Excess AoII and associated costs
III. We prove the *existence and uniqueness* of a Nash Equilibrium (NE) in the strategic interaction and provide explicit expressions for the optimal update and injection rates.
IV. We analyze how system parameters such as *drift rate*, *cost coefficients*, and the *threshold* impact strategic behavior and the conditions under which attacks become profitable.
V. Through simulations, we show that our approach offers actionable insights into *update scheduling and cybersecurity*, particularly in cyber-physical systems exposed to false data injection.

C. Paper Organization

The subsequent sections of this paper are organized as follows: In Section II, we define our system model. Section III analyzes the strategic interaction between the transmitter and the attacker using game theory. In Section IV, we present numerical simulations to gain insight into how the NE is influenced by various parameters of the system. Finally, Section V concludes the paper and summarizes our findings.

II. System Model

We consider the following dynamical system:

$$\begin{cases} \dot{x}(t) &= f(x(t), u(t)) \\ y(t) &= h(x(t)), \end{cases} \tag{3}$$

where $x(t) \in \mathbb{R}^n$ represents the plant state, $u(t) \in \mathbb{R}^p$ is the control input, and $y(t) \in \mathbb{R}$ is the output at time t. The functions $f(\cdot)$ and $h(\cdot)$ denote the state transition and output selection functions, respectively. We assume that the sensor measurements acquired in the filed, must be communicated to a remote station (e.g., a SCADA system) by transmitting the output measurement $y(t)$ with an average rate p. For simplicity, our analysis concentrates on scalar output measurements; however, many real-world applications involve

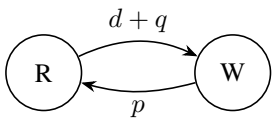

Fig. 2. Continuous-time Markov process illustrating the transitions between states representing the Age of Incorrect Information.

vector outputs, which we plan to explore in future research. We assume no propagation delay between the controller and the remote station, allowing for time synchronization. As time progresses, sensor information can become outdated or incorrect due to natural phenomena, termed *system drift*, or malicious actions like *false data injection*. In this context, with the term *drift*, we refer to the time after which a measurement no longer accurately reflects the system's state due to being outdated. To model this, we assume that the intervals between successive drifts follow an exponential distribution with a mean of d, representing the *average drift rate*. In other words, d denotes the average time for the function $g(\cdot)$, defined in (1), to reach a value of 1. Conversely, information can also become incorrect due to the actions of a malicious agent who performs false data injection at a rate q. From the perspective of the receiver, as depicted in Fig. 2, we can model the system using a Markov chain with two distinct states: Right (R) and Wrong (W). The system is in the R state when the information available at the receiver correctly represent the current state of the system, while it is in the W state when the latest available information do not correctly represent the current state of the system anymore due to a system drift or a malicious update.

We aim to measure the average duration the system spends above threshold when in the W state of the Markov chain. This duration is represented by the average area of the upper triangles in Fig. 1 over a complete period, which corresponds to the interval between two successive successful updates. To quantify this, we consider the expected value of Excess AoII, denoted as $\Delta_{\frac{1}{\theta}} = \mathbb{E}_t[\delta_{\frac{1}{\theta}}(t)]$:

$$\Delta_{\frac{1}{\theta}} = \max\left\{0,\ \frac{\frac{1}{2}\left(\frac{1}{p}-\frac{1}{\theta}\right)^2}{\frac{1}{d+q}+\frac{1}{p}}\right\}.$$

Note that $\Delta_{\frac{1}{\theta}} = 0$ when $p > \theta$, which means that legitimate updates are performed before allowing the system to exceed the threshold.

Both the transmitter and the malicious agent incur costs when transmitting updates. For the transmitter, the cost is C, which is proportional to the transmission rate p. For the malicious agent, the cost is K, which is proportional to the injection rate q. These costs can be understood as energy expenditures or shadow prices.

We model the strategic decision-making process using a game theoretic approach. In particular, we formulate a maximization task in which the utility function of the transmitter T and the malicious agent M are:

$$u_{\mathrm{T}}(p,q) = -\Delta_{\frac{1}{\theta}} - C\cdot p, \quad u_{\mathrm{M}}(p,q) = \Delta_{\frac{1}{\theta}} - K\cdot q\,. \quad (4)$$

Here, $u_{\mathrm{T}}(p,q)$ represents the utility of the transmitter that wants to minimize the sum of $\Delta_{\frac{1}{\theta}}$ and its transmission costs by properly selecting the transmission rate p. Instead, $u_{\mathrm{M}}(p,q)$ is the utility of the malicious agent, seeking to maximize $\Delta_{\frac{1}{\theta}}$ but also limiting the cost undertaken for malicious injections by selecting the injection rate q.

III. Game Theoretic Analysis

The interaction between the transmitter T and the malicious agent M can be formalized as a static game of complete information, denoted as $\mathcal{G} = (\mathcal{P}, \mathcal{A}, \mathcal{U})$. Here, the set of players is defined as $\mathcal{P} = \{\mathrm{T}, \mathrm{M}\}$, with player T choosing an action $p \in [0,\infty)$ and player M selecting an action $q \in [0,\infty)$. The utility set is represented as $\mathcal{U} = \{u_{\mathrm{T}}, u_{\mathrm{M}}\}$. This setup is common knowledge among the players. The game is classified as *static* because each player makes their choice independently, without knowledge of the other's action.

Remark 1. It is important to clarify that the term *static* in this context refers exclusively to the nature of the game between the transmitter T and the malicious agent M, and not to the physical system being monitored. While the underlying system evolves dynamically over time (e.g., due to drift), the game is static because both strategic players select their actions, namely, the transmission rate p and the injection rate q, once at the beginning of the game. Thus, the game captures a one-shot strategic interaction, independent of the temporal evolution of the monitored process.

The most desirable outcome for both players is typically characterized by the NE.

Theorem 1 (*Existence of a NE*)**.** The 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. The uniqueness follows directly from the monotonicity of the utility functions for both players across their entire action range. This property guarantees that the ε-fixed point to which they converge is consistent. □

The NE conditions for the specific formulation can be derived numerically by solving the following equations [22]:

$$\frac{\partial u_{\mathrm{M}}(p,q)}{\partial q} = 0 \qquad \frac{\partial u_{\mathrm{T}}(p,q)}{\partial p} = 0, \quad (5)$$

which yield:

$$\frac{\partial \Delta_{\frac{1}{\theta}}}{\partial q} = K \qquad \frac{\partial \Delta_{\frac{1}{\theta}}}{\partial p} = -C. \quad (6)$$

Rearranging the term in $\frac{\partial \Delta_{\frac{1}{\theta}}}{\partial q} = K$ leads to a second-degree equation in q:

$$\frac{(p-\theta)^2}{2(d+p+q)^2\theta^2} = K. \tag{7}$$

Solving this equation yields two solutions, of which only one is viable since the other is negative for all values of K:

$$q = -d - p + \frac{\theta - p}{\sqrt{2K}\theta}. \tag{8}$$

Substituting this expression for q into $\frac{\partial \Delta_{\frac{1}{\theta}}}{\partial p} = -C$ and rearranging produces another second-degree equation in p:

$$K - \frac{1}{2}\left(\frac{1}{p^2} - \frac{1}{\theta^2}\right) + \frac{\sqrt{2K}}{\theta} = -C. \tag{9}$$

This equation also presents two solutions, one being negative for all possible values of C. Thus, the equilibrium conditions yield:

$$p = \frac{\theta}{\sqrt{1 + 2\theta\sqrt{2K} + 2\theta^2(C+K)}}. \tag{10}$$

Consequently, the NE is expressed as:

$$\begin{aligned} p &= \frac{\theta}{\sqrt{1 + 2\theta\sqrt{2K} + 2\theta^2(C+K)}}, \\ q &= -d - p + \frac{\theta - p}{\sqrt{2K}\theta}. \end{aligned} \tag{11}$$

In (11), the expression for p is always positive. For q to also be positive, the injection cost term K must be sufficiently small. If q is negative, it indicates that the attacker does not get any benefit and chooses to remain inactive.

The injection cost term K must therefore balance the natural drift rate d, the transmission rate p, and the threshold θ. If these terms grow excessively large, q can remain positive only if K is sufficiently low. This emphasizes the trade-offs among the various factors influencing the system dynamics.

To ensure that q is positive, a necessary condition is that p be less than θ. Mathematically, this is expressed as:

$$p = \frac{\theta}{\sqrt{1 + 2\theta\sqrt{2K} + 2\theta^2(C+K)}} < \theta, \tag{12}$$

which is satisfied if:

$$\sqrt{1 + 2\theta\sqrt{2K} + 2\theta^2(C+K)} > 1. \tag{13}$$

This condition is always fulfilled, suggesting that under attack conditions, it is not advantageous for the transmitter to excessively increase the transmission rate to keep AoII below the threshold $1/\theta$, as this would incur excessive costs.

Further, it is essential to determine the appropriate values for K to ensure that player M actively participates in the game, i.e., that (11) accurately represents the NE of the system.

Notably, p is strictly monotonic in θ, leading to the limit:

$$\lim_{\theta\to\infty} p = \frac{1}{\sqrt{2(C+K)}} \tag{14}$$

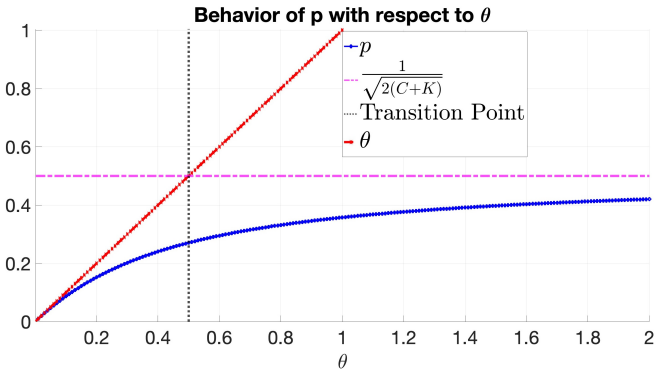

Fig. 3. Upper bound on the transmission rate p with respect to θ.

Note that the expression for p in (14) aligns with the analysis in [22]. Specifically, as θ approaches infinity, it signifies that the acceptable time for the system to remain in the W state is zero. In addition, we have derived an upper bound for p, which is θ. Therefore, we consider the upper bound for p to be

$$\bar{p} = \min\{\theta, \frac{1}{\sqrt{2(C+K)}}\} \tag{15}$$

This behavior is also illustrated in Fig. 3.

When p can be approximated as $\frac{1}{\sqrt{2(C+K)}}$, the analysis remains consistent with previous work [22]. Thus, we conclude that there exists a critical value K^* such that if $K > K^*$, then $q = 0$.

To ensure that $q > 0$, we need to satisfy

$$-d - p + \frac{\theta - p}{\sqrt{2K}\theta} > 0,$$

which simplifies to:

$$\sqrt{2K} < \frac{1}{\theta}\cdot\frac{\theta - p}{d+p} = \frac{1}{d+p} - \frac{p}{\theta}\cdot\frac{1}{d+p}.$$

Given that $p < \theta$ implies $0 < \frac{p}{\theta} < 1$, we can conclude that

$$\sqrt{2K} < \frac{1}{d+p} < \frac{1}{d+\theta}.$$

This establishes a critical cost K^* for the adversary to be active in the game as

$$K^* = \frac{0.5}{(d+\theta)^2}.$$

This means that if $K < K^*$ the malicious agent will participate in the game. When this happens, the problem reduces to a single player optimization where the transmitter selects the transmission rate as

$$p = \text{argmax}_p\{-\Delta_{\frac{1}{\theta}} - C\cdot p\}.$$

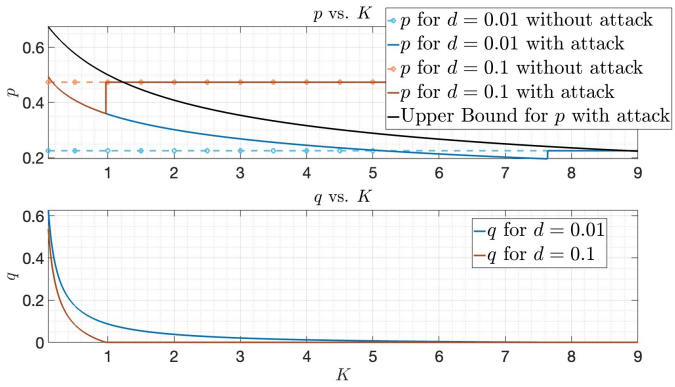

Fig. 4. Comparison of strategic update rate p with and without a malicious agent, $C = 1$ and $\theta = 5$. The black line indicates the upper bound for p computed through (15).

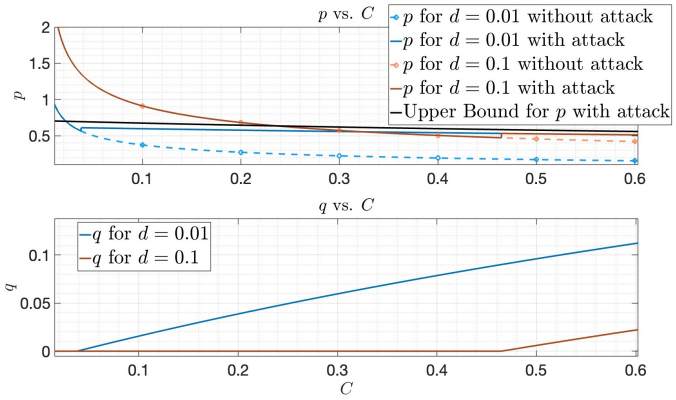

Fig. 5. Comparison of strategic update rate p with and without a malicious agent, $K = 1$ and $\theta = 5$. The black line indicates the upper bound for p computed through (15).

Combining these results together, at the NE the transmission and injection rates are

$$p = \begin{cases} \dfrac{\theta}{\sqrt{1 + 2\theta\sqrt{2K} + 2\theta^2(C+K)}} & \text{if } K < K^* \\ \text{argmax}_p\{-\Delta_{\frac{1}{\theta}} - C \cdot p\} & \text{otherwise} \end{cases} \tag{16}$$

$$q = \begin{cases} -d \ - \ p \ + \ \dfrac{\theta - p}{\sqrt{2K\theta}} & \text{if } K < K^* \\ 0 & \text{otherwise} \end{cases}, \tag{17}$$

IV. Numerical Results

This section presents the numerical application of the NE derived in equations (16) and (17), along with the conclusions of Theorem 1. The results quantify the game-theoretic interactions between a controller, which minimizes the Excess AoII at a remote receiver, and an adversary that injects false data, which seeks to maximize the Excess AoII, with both aiming to minimize their associated costs.

Fig. 4 illustrates the relation between the transmitter rate p and the adversary injection rate q at the NE as a function of the adversary injection cost K, with $C = 1$ and $\theta = 5$. In the presence of an adversarial agent, the transmitter increases its transmission rate in response to the adversary's actions. However, as the injection cost K increases, the adversary decreases its injection rate q, prompting the transmitter to reduce its transmission rate. Eventually, the transmitter approaches the attack-free transmission rate as the adversary's injection rate converges to zero. The black line represents the upper bound for p computed through equation (15), which holds only when the adversary's injection rate q is non-zero. When $q = 0$, the problem reduces to a single-player optimization problem, making the bound irrelevant.

In Fig. 5, the strategic update rate p is shown as a function of the transmission cost C, with fixed values $K = 1$ and $\theta = 5$. As in the previous figure, the presence of the adversary results in an increased transmission rate. As parameter C increases, the cost burden forces the transmitter to reduce its rate until it stabilizes. Notably, (16) shows that the transmission rate under attack is independent of the drift rate d, which explains the consistency of the transmission rate across varying drift rates when the system is under attack. The black line once again represents the upper bound for p from equation (15), applicable only when $q \neq 0$.

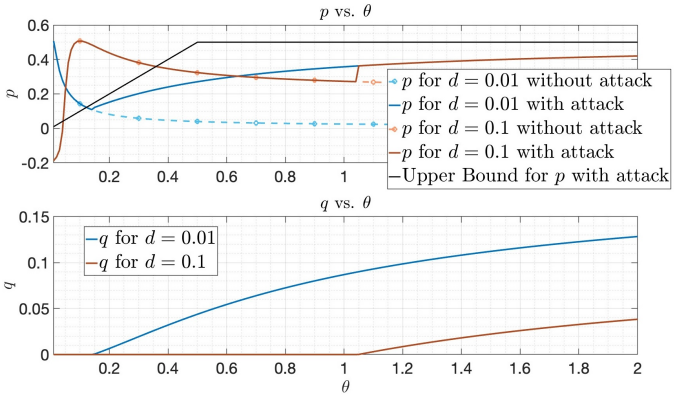

Fig. 6. Comparison of strategic update rate p with and without a malicious agent, $K = 1$ and $C = 1$. The black line indicates the upper bound for p computed through (15).

Finally, Fig. 6 depicts the relation between the transmission rate p and the adversary's injection rate q at the NE as a function of the threshold θ, with $K = 1$ and $C = 1$. As θ varies, an interesting pattern emerges: without attack, a smaller θ leads to a rapid increase in the transmission rate, especially when the drift rate d is low. However, for larger values of θ, the transmission rate decreases more rapdily. Under attack, the transmission rate increases, but larger values of θ favor the adversary. A θ of zero signifies an infinite acceptable threshold, making it impossible for the malicious agent to compromise the system. In contrast, as θ increases, the acceptable threshold decreases, enabling the malicious agent to more easily compromise the system while making it more costly for the transmitter to defend.

V. Conclusions

We examined a scenario in which a transmitter sends information to a receiver over a network vulnerable to injection attacks. The presence of the attacker can be detected, but not blocked. To counteract the attacks, the transmitter can increase its activity.

We utilized game theory to model the interaction between the transmitter and the adversary. The malicious agent incurs a cost that is directly proportional to its activity rate, which corresponds to the percentage of blocked updates. Instead, the legitimate agent faces a cost that is proportional to its transmission rate. The malicious agent's objective is to maximize the Excess AoII at the receiver while minimizing its own costs. In contrast, the legitimate agent aims to minimize the Excess AoII metric at the receiver and its own costs. Through our analysis, we computed the unique NE, which is guaranteed to exist under the given conditions.

Our findings indicate that the presence of the adversary leads to an increase in the transmission rate p. Moreover, a higher threshold $1/\theta$ encourages the adversary to refrain from intervening; the higher the threshold, the more challenging it becomes for the malicious agent to compromise the communication to an acceptable level. Importantly, our analysis reveals the existence of a threshold K^*. If $K > K^*$, the malicious agent chooses not to intervene. This result provides valuable information on resource allocation strategies that aim to reduce the likelihood of attacks.

Appendix A
Proof of the Existence of the NE

Proof. The utilities described by (5) are continuous and resemble polynomial functions. In line with the adversarial framework of our study, these utilities exhibit a strict monotonic behavior with respect to the actions chosen by the respective players. Specifically, $u_{\mathrm{T}}(p, q)$ strictly increases with p for a fixed q, as $u_{\mathrm{M}}(p, q)$ does with q for a fixed p. Additionally, these utilities are concave, i.e., their first and second derivatives are positive and negative, respectively [23]. Consequently, we can apply Glicksberg's theorem [24], which generalizes Nash's theorem to continuous cases.

In more detail, the NE can be identified as a 0-Nash equilibrium, which is an ε-Nash equilibrium for $\varepsilon{=}0$. This equilibrium is the limit point of a sequence of actions that alternate between the players' best responses, with ε-convergence to a fixed point ensured by the properties of continuity, monotonicity, and concavity mentioned above. □

References

[1] S. Misra, C. Roy, T. Sauter, A. Mukherjee, and J. Maiti, "Industrial Internet of things for safety management applications: A survey," *IEEE Access*, vol. 10, pp. 83 415–83 439, 2022.

[2] G. Cisotto, A. V. Guglielmi, L. Badia, and A. Zanella, "Joint compression of EEG and EMG signals for wireless biometrics," in *Proc. IEEE Globecom*, 2018, pp. 1–6.

[3] M. Mendula, A. Bujari, L. Foschini, and P. Bellavista, "A data-driven digital twin for urban activity monitoring," in *Proc. IEEE ISCC*, 2022.

[4] T. Soleymani, J. S. Baras, and K. H. Johansson, "Stochastic control with stale information–part i: Fully observable systems," in *Proc. IEEE Conf. Decis. Control (CDC)*, 2019, pp. 4178–4182.

[5] O. A. Wahab, "Intrusion detection in the IoT under data and concept drifts: Online deep learning approach," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 19 706–19 716, 2022.

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

[7] 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.

[8] 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.

[9] X. Zheng, S. Zhou, and Z. Niu, "Urgency of information for context-aware timely status updates in remote control systems," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 11, pp. 7237–7250, 2020.

[10] E. D. Knapp, *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier, 2024.

[11] L. Hu, Z. Chen, Y. Dong, Y. Jia, L. Liang, and M. Wang, "Status update in IoT networks: Age-of-information violation probability and optimal update rate," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 329–11 344, 2021.

[12] R. Devassy, G. Durisi, G. C. Ferrante, O. Simeone, and E. Uysal, "Reliable transmission of short packets through queues and noisy channels under latency and peak-age violation guarantees," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 721–734, 2019.

[13] K.-Y. Lin, Y.-C. Huang, and Y.-P. Hsu, "Scheduling for periodic multi-source systems with peak-age violation guarantees," *IEEE J. Sel. Areas Commun.*, vol. 71, no. 12, pp. 7102–7116, 2023.

[14] A. Franco, B. Landfeldt, and U. Körner, "Analysis of age of information threshold violations," in *Proc. ACM MSWiM*, 2019, pp. 163–172.

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

[16] L. Crosara, N. Laurenti, and L. Badia, "Age of information is not just a number: Status updates against an eavesdropping node," *Ad Hoc Networks*, vol. 155, p. 103388, 2024.

[17] 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.

[18] Y. Xiao and Y. Sun, "A dynamic jamming game for real-time status updates," in *Proc. IEEE INFOCOM Workshops*, 2018, pp. 354–360.

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

[20] 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.

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

[22] 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.

[23] 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.

[24] 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.