Ambiguous Data Injection Impacting Age of Incorrect Information: A Bayesian Game Analysis

Leonardo Badia*, Valeria Bonagura†‡, Chiara Foglietta†, and Erjol Sulku*
*Dept. Information Engineering, University of Padova, 35131 Padua, Italy
†Dept. Civil, Computer Science, Aeronautical Technologies Engineering, University Roma Tre, 00146 Rome, Italy
‡Dept. of Electrical and Information Engineering, Polytechnic of Bari, 70125 Bari, Italy
Email: leonardo.badia@unipd.it, valeria.bonagura@uniroma3.it, chiara.foglietta@uniroma3.it, erjol.sulku@studenti.unipd.it

***Abstract*—We use Bayesian game theory to investigate the interaction between a system controller and an additional unknown agent in a cyber-physical system. The system controller performs some monitoring for real-time operation management, with the aim of minimizing the age of incorrect information (AoII). The additional agent reports some extra information, which ideally can serve to aid the controller and meet the same objective of decreasing AoII, but it is uncertain whether these actions are useful or correspond to (possibly international) false data injection in the system. The controller only has information in terms of probability of the legitimacy of this extra agent through a common prior, and also knows that, in case it is malicious, it will try to increase AoII instead. Our analysis reveals that, under rational behavior, an adversary can effectively masquerading as a sensor injecting legitimate data, as the controller can hardly distinguish the behavior of a true helper from that of an attacker. However, under variable data drift, the strategic behavior of the external agent can give away their type.**

***Index Terms*—Cybersecurity; Real-time applications; Sensor networks; Age of incorrect information; Bayesian game theory.**

I. Introduction

Cyber-physical systems (CPS) seamlessly blend physical processes with sensing, communication, and control features, providing real-time applications for many environments, from autonomous vehicles and smart grids to industrial automation and remote healthcare [1]–[3]. As they expand to multiple sensing units, they shift from point-to-point architectures to more complex interconnected networks consisting of sensing, computing, and actuating nodes. This enables distributed data collection and collaborative decision making, greatly enhancing system coverage, scalability, and responsiveness. This multifaceted structure allows a CPS to tackle more complex real-time tasks, but also significantly expands the attack surface, making it challenging to detect, isolate, and defend against malicious manipulations such as false data injection [4]–[6].

In the context of real-time services, a suitable metric that can be used to quantify both accuracy and freshness of the exchanged information is age of incorrect information (AoII). Introduced by [7], AoII at time t is quantified by the value that we write as $\delta(t)$, corresponding to the difference between the current time index and that of the last time $\sigma(t)$ the system information was still considered accurate. If $s(t)$ denotes the actual state of the monitored system at time t, and $\hat{s}(t)$ the last received estimate of the state at the destination, it is assumed that, whenever there is an explicit report about the state of the system by one of the monitoring sensors at times $\tau_1, \tau_2, \ldots$, then $\delta(t)$ is set to 0 since in that case $s(\tau_j) = \hat{s}(\tau_j)$. Whenever $\hat{s}(t)$ differs from $s(t)$ by more than a tolerance value ε, the system information is no longer accurate, and $\delta(t)$ grows linearly until a new status report resets it to 0. Formally,

$$\begin{aligned} \delta(t) &= t - \sigma(t) \qquad (1)\\ \text{where: } \sigma(t) &= \min\{t > \tau^{(t)} : |s(t) - \hat{s}(t)| > \varepsilon]\}\,, \\ \tau^{(t)} &= \max_j\{\tau_j < t\}\,. \end{aligned}$$

AoII is a joint characterization of key aspects of data reliability and timeliness [8], useful for industrial control and safety-related applications, where inaccurate and/or obsolete information may cause the system to malfunction [9]. We consider a system alternating between a binary "right" or "wrong" condition. Transitions between states are caused by status reporting by a system controller and natural changes in the systems (called "drift"). The former causes a wrong state information to become right, and the latter does the opposite.

In a single-agent system, these are the only ways the state can change. However, for multisensor scenarios, there may be additional agents injecting data, and we assume that these supports the monitoring, as they correctly report about the system state, or correspond to intentional false data injection [10]. We assume that these actions contribute accordingly to the correct measurement rate of the system or to the data drift [11], respectively. Moreover, minimizing AoII is no longer the only objective to consider, as if a malicious agent injecting false data is present, it will try to maximize AoII instead, to pilot the system operation outside of a correct management.

This interaction can be framed with game theory [12]–[15], specifically in an adversarial setup. Whenever the information on these extra sensors available to the system controller is incomplete, an extension to Bayesian game theory is required [16], [17]. This happens not only because it is not known to the controller whether they will inject correct or false data but

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP D33C22001300002, PE00000014 – program "SEcurity and RIghts in the CyberSpace" (SERICS), Spoke 4 - project "Innovative Security Paradigms for beyond 5G" (ISP5G+).

also, according to the discussion above, since their objective and strategic gameplay will be different.

From this background, we analyze the case where a system controller N tries to achieve a low expected AoII $\Delta = \mathbb{E}[\delta(t)]$, and is at the same time subject to cost limitations, so it also seeks to minimize its own activity. An external node X is present in the system and offers an aid to monitor the system, which decreases AoII, allowing the controller to save effort. Node X is under a similar cost limitation, so it actually tries to minimize the sum of Δ and its activity cost. However, it can be suspected that X is malicious and tries to inject false data, increasing Δ rather than decreasing it. As seen in the following, this interaction develops into a Bayesian game, where the two players N and X decide their activity rate, and X has a private type (good/evil) describing its behavior.

It is found that the game admits a unique Bayesian Nash equilibrium (BNE), which is computed and discussed. Beyond the values resulting from the BNE, a point of interest is whether the controller is able to tell the two types of X apart [18], [19]. It is interesting to see that changing the values of the costs is not particularly revealing to the nature of X. However, if N is able to modify the system drift (i.e., the rate at which the system state naturally changes and becomes incorrect), it may obtain a way to identify malicious sources.

The remainder of this paper is organized as follows. In Section II, we review related works. Section III presents the system model and our Bayesian game theoretic analysis. We present results in Section IV, and conclusions in Section V.

II. Related work

The approaches to modeling AoI and AoII under attack through game theory found in the literature generally assume that the adversary is persistently malicious [2], [10], [11], [20]–[23], with extensions possibly involving multiple adversaries competing to attack [13]. A more niche line of research involves studies in which a non-malicious extra node is considered; e.g., [24] considers a relay corroborating the information sent by a source and possibly increasing information freshness. However, the relay is always collaborative, and game theory is invoked only due to the desire of both agents (the controller and the relay) to contain their activity costs.

Scenarios with ambiguous external nodes that possibly involve an extension to Bayesian games are not common. Most of the time, the goal is instead to remove the uncertainty through detection techniques. A preliminary study in this sense is found in [16], which focuses on identifying critical nodes that are more vulnerable to attacks, with particular reference to smart grids, which are highly sensitive to false data injection. In [25], [26], this is pushed forward to encompass the most advanced techniques involving automated reasoning.

Some contributions [17]–[19], [27], [28] use adversarial Bayesian games for cyberphysical security. In these papers, a CPS is under attack and the controller has incomplete information about the adversary. The uncertainty is related to the technology, location, or energy level of the attacker and the nature of the attack is different, corresponding to a denial of service/jamming in [17] and [19], while in [18] and [28] it can include false data injection but without influencing AoII. Finally, in [27] the Bayesian element relates to whether the opponent will adapt its behavior or not, but the scenario still only focuses on jamming and does not consider AoII.

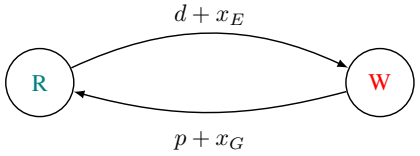

Fig. 1. Continuous time Markov chain describing $z(t)$, i.e., the state of the system being accurate or not.

In contrast, we ground our analysis in [11], where the strategic gameplay revolves around the goal of minimizing AoII for the system controller, while also including costs associated with the activity of the players. For that analysis, though, complete information is available to both players, and the scenario with incomplete information about the nature of the attacker has not yet received a characterization.

III. System Model

We consider a CPS where we track the correctness of the monitored information using a binary state model, where the state of the information at the destination is right (R) or wrong (W). According to the previous notation introduced in (2), these states correspond to $|s(t) - \hat{s}(t)|$ being less than or more than ε, respectively. We follow the model introduced in [11], where the transitions between states are treated as memoryless, and therefore a continuous-time Markov process captures the dynamics of information correctness.

Let $z(t) \in \{\mathrm{R}, \mathrm{W}\}$ denote the value of this binary state at time t. Note that $z(t)$ is different from the actual state of the system $s(t)$, since our assessment is related to the AoII value, which abstracts from the numerical measurements and only considers whether they are correct or not. The model used for $z(t)$ and its transitions is represented in Fig. 1.

Transitions between states R and W occur due to (i) natural drift and (ii) player-induced actions. The former describes that condition R will inevitably deteriorate, as after a while the system state will no longer be accurately known. This means that the Markov chain has a transition from R to W with rate d describing that the system information becomes inaccurate on average after a time $1/d$. In contrast, each measurement sent by the controller reports accurate state information. We assume that the controller measures and reports according to a Poisson (memoryless) process whose average interarrival time is $1/p$, which implies a transition from W to R with rate p. It is not restrictive to assume that updates are always successful, as any unreliability in the update channel can be absorbed into a rescaled p value, as discussed in [29].

In a similar non-Bayesian model introduced in [11], we formulated a static game between a controller and an adversary. In that model, the adversary injects false data at a certain rate q, and the controller updates the state of the monitored

system at a rate p. The goal of the controller is to minimize AoII while keeping the communication cost low, while the adversary seeks to increase AoII while considering the cost of disruption. The interaction is modeled using utility functions:

$$u_N(p,q) = -\Delta - Cp, \quad u_M(p,q) = \Delta - Kq, \tag{2}$$

with Δ being the expected AoII, and C, K are unit costs (prices) for the controller and the adversary, respectively. Transitions from W to R occur with a rate p (decided by the controller), while the transition rate from R to W is $d+q$.

Here, we adopt an extended model, where an external agent referred to as *player X* transmits additional information of *ambiguous* nature. The impact of these depends on X's type, but the true nature of player X is not directly known to the controller, introducing an element of uncertainty into the system. Player X injects data with rate x and can belong to one of two types: (i) Type G (Good): a cooperative participant that can reinforce the controller's information with more useful updates; (ii) Type E (Evil): an adversarial agent attempting to degrade information quality by injecting wrong data. We point out that this corresponds to having two parameters associated with player X, denoted as x_G and x_E. When player X is good, $x_G > 0$ and $x_E = 0$. Otherwise, $x_E > 0$ and $x_G = 0$. However, as visible in Fig. 1, this changes the placement of the transitions and extends the original model (where x_G was never present) to a case where another player, other than the controller, can affect the transition from W to R. Since all transitions are memoryless and based solely on current observations, the process $z(t)$ still forms a Markov chain [9].

From a Bayesian game theory perspective, the controller holds belief $\theta \in [0,1]$ that player X is of type G and $1-\theta$ that it is of type E. This model gives rise to a game with incomplete information. A similar uncertainty structure has been used in the recent literature to characterize cyberthreats and cooperative behavior in age-sensitive systems [5], [18].

We define an interaction according to type-specific objectives, where a Type G player injects helpful information at a rate x_G, to further reduce AoII through timely updates. Conversely, a Type E player injects misleading or corrupt data at a rate x_E, attempting to increase AoII and degrade system performance. The presence of such an ambiguity creates challenges for the controller, which must make decisions without knowing the true intent of player X.

The controller does not directly know the type of player X, but instead maintains a belief distribution over possible types. As in any Bayesian game framework, some shared information is still required for the players to interact. In this case, while only player X knows its own type, the controller is informed about the probability distribution over the types of player X. In our case, this corresponds to knowing the value of θ, which is common knowledge among players. In game-theoretic speech, the value of θ is said to be a *common prior* [30].

Let $\Delta_G(p, x_G)$ and $\Delta_E(p, x_E)$ represent the expected AoII when player X is of Type G or Type E, respectively. These are derived from the steady-state probabilities of the underlying Markov chain, as introduced in [11]. The controller seeks to minimize an expected AoII, weighted by its belief:

$$\mathbb{E}[\Delta(p)] = \theta \cdot \Delta_G(p, x_G) + (1-\theta) \cdot \Delta_E(p, x_E)\,.$$

The controller's utility function is thus:

$$u_N(p; x_G, x_E) = -\mathbb{E}[\Delta(p)] - C \cdot p \tag{3}$$

where C is the non-negative unit cost of N for transmitting updates. Player X's utility can be defined in a similar way, but with a dependence on player X's type, to represent that type G wants to minimize AoII, whereas type E wants to maximize it, and both types want to keep their activity costs low.

Thus, we formulate the interaction between the network controller and player X as a Bayesian game. Unlike complete-information frameworks where all system parameters are common knowledge, here some information is only known to one of the players. Player X has two possible types, and the specific type is known to player X but unknown to the controller. The interaction among these players leads to a Bayesian NE, where (i) the controller chooses the update rate p^* to maximize its expected utility; (ii) each type of player X chooses its injection rate (x_G^*, x_E^*) to best respond to p^*.

Formally, the Bayesian game is a quadruple $(\mathcal{P}, \mathcal{T}, \mathcal{S}, \mathcal{U})$ [30], consisting of the following. Set $\mathcal{P}$ contains the players, i.e., the controller N and an external player X. Set $\mathcal{T}$ includes the types, where player N is not typed and player X has a private type $t_X \in \{G, E\}$, with G being a helpful agent (e.g., a cooperative relay or another legitimate source) and E representing a malicious agent (e.g., injecting incorrect information). The strategies are contained in $\mathcal{S}$, and are the status update rate $p \in \mathbb{R}_+$ for the controller N, whereas player X selects an injection rate $x_t \in \mathbb{R}_+$ that actually depends on its type t_X, ultimately describing whether X is collaborative or malicious [17]. This means that the strategy of X is a pair of non-negative real values, (x_G, x_E). We note that the latter corresponds to a type agent representation of a Bayesian player [30], where different types can be considered as split players.

The utilities in $\mathcal{U}$ are instead defined as follows. First, we denote the average AoII for type $t \in \{G, E\}$ as $\Delta_t(p, x_t)$. The system's expected AoII is then:

$$\mathbb{E}[\Delta(p, x_G, x_E)] = \theta \cdot \Delta_G(p, x_G) + (1-\theta) \cdot \Delta_E(p, x_E)\,. \tag{4}$$

Moreover, the controller incurs a cost $C \cdot p$ for maintaining update rate p, and its utility is as in (3). Instead, player X has type-specific objectives, i.e., its type G (helpful) seeks for minimizing AoII ans its own injection cost, thus its utility is

$$u_G(x_G; p) = -\Delta_G(p, x_G) - K \cdot x_G \tag{5}$$

where the negative sign describes that u_G is to be maximized, and K is a non-negative unit cost parameter (price of activity) defined similar to C, see (2). Type E (malicious) has a similarly structured objective and the same price K, but aims to maximize AoII while minimizing its own cost, hence

$$u_E(x_E; p) = \Delta_E(p, x_E) - K \cdot x_E\,. \tag{6}$$

Let π_W^t denote the stationary probability of being in state W under player type $t \in \{G, E\}$. We obtain:

$$\pi_W^E = \frac{d + x_E}{d + x_E + p}, \quad \pi_W^G = \frac{d}{d + p + x_G}$$

The AoII terms in (4), (5), and (6) are derived from the expected time spent in state W before being corrected as:

$$\Delta_E(p, x_E) = \frac{\pi_W^E}{\lambda_{WR}^E} = \frac{d + x_E}{p(d + x_E + p)} \tag{7}$$

$$\Delta_G(p, x_G) = \frac{\pi_W^G}{\lambda_{WR}^G} = \frac{d}{(p + x_G)(d + p + x_G)}, \tag{8}$$

with the λ terms representing the return rate to R.

These expressions capture that malicious injection increases the frequency of errors, whereas supporting transmissions accelerate recovery to the correct system regime. Both events influence the steady-state and transient behavior of the system.

The controller, unable to observe the realized type, evaluates the expected AoII as per (4) and chooses an update rate $p \in \mathbb{R}_+$ to minimize a trade-off between the expected AoII and communication cost from (3), i.e.,

$$u_N(p; x_G, x_E) = -\left[\theta\Delta_G(p, x_G) + (1-\theta)\Delta_E(p, x_E)\right] - Cp\,.$$

Taking the derivative with respect to p yields the first-order condition for optimality:

$$\frac{du_N}{dp} = -\left[\theta \cdot \frac{\partial \Delta_G}{\partial p} + (1-\theta) \cdot \frac{\partial \Delta_E}{\partial p}\right] - C = 0$$

This condition reflects the marginal benefit of the controller in reducing AoII versus the marginal cost C. The controller reacts to its belief θ about the type of player X, increasing p when malicious behavior is more likely (that is, x_E is high), and reducing p when player X is more likely to cooperate.

To find the best response of player X, we note that its utility depends on its type $t \in \{\mathrm{G}, \mathrm{E}\}$ as (5) and (6), respectively. In both cases, the optimal injection rate x_t^* satisfies:

$$\frac{du_t}{dx_t} = \pm \frac{\partial \Delta_t}{\partial x_t} - K = 0 \tag{9}$$

where the $+$ sign is for type E, who wants to increase AoII, the $-$ sign is for G, who wants to reduce AoII, and Δ_t follows (7) or (8) depending on t being E or G, respectively.

Despite using different expressions for the two types of player X, we can draw conclusions analogous to the case where X is certainly malicious as in [11]. The derivative of Δ_t in (9) follows K at the equilibrium, which captures the sensitivity to the activity cost. Whatever the expression, increasing x_t exhibits diminishing returns for both types of player X. Thus, we obtain a threshold-like behavior. Each type of player X only finds it worthwhile to inject when the marginal impact on AoII is significant enough to offset the associated cost K. For example, type G may remain idle if the controller is already updating frequently, while type E becomes more aggressive when the controller is passive.

Thus, a BNE (p^*, x_G^*, x_E^*) exists when: (i) the controller maximizes $u_N(p)$ based on current beliefs and type-dependent responses; (ii) each type of player X chooses its best response to p^*. Hence, the BNE satisfies a fixed-point relationship:

$$p^* = \arg\max_p \left[-\theta\Delta_G(p, x_G^*(p)) - (1-\theta)\Delta_E(p, x_E^*(p)) - Cp\right] \tag{10}$$

This implies that despite the complication caused by the types of player X, a solution can be found by reasoning in the expected values. This is in line with the principles of von Neumann-Morgenstern utilities to work in expectation [30]. Thus, it is immediate that a BNE exists and is unique, which can be obtained by solving (10) using numerical methods.

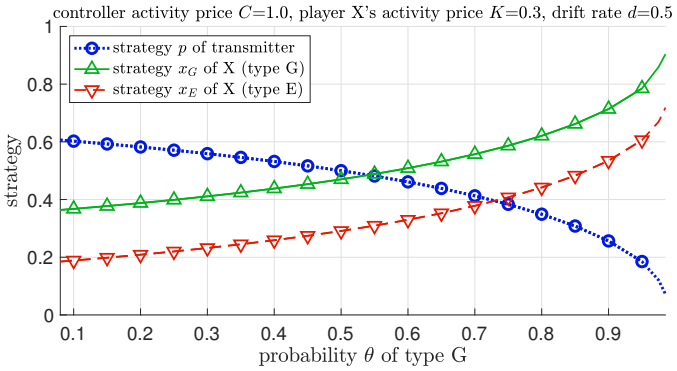

Fig. 2. Strategies of the players vs. prior of X's type being G θ, for controller activity price C=1.0, player X's activity price K=0.3, drift rate d=0.5.

IV. Results

We present numerical evaluations of the BNE to highlight some interesting trends. The objective of our evaluations are the strategic choices of the players, namely, the activity rate p for the controller N and the activity rates x_t for the external player X, distinguishing the two values x_G and x_E depending on the type of player being G or E, respectively.

The first parameters of interest are the unit costs of activity, denoted as C and K for the controller N and the additional player X, respectively. This means that the utility of player N is decreased by Cp, and similarly the utility of player X is decreased by Kx (note that the unit cost is the same for both types of player X, since they are never present at the same time). Also relevant are the probability θ that player X is of type G and the default drift rate d, always present in the system even in the absence of an adversary.

In Fig. 2, we report the strategies of the players versus the prior θ, i.e., the probability of player X being of type G. This highlights a subtle result of Bayesian game theory: when θ increases, the controller tends to trust player X more and decreases its own data transmission rate p. This implies that both the good and evil versions of player X increase their activity as θ increases. Type G does so to genuinely contribute more to the decrease of AoII in the system, whereas type E sees a window of opportunity to attack the system more often. Note that the latter circumstance is less likely since θ is high; yet, it implies a particularly advantageous situation for the rare malicious attackers that are unexpected due to the controller expecting a good player X due to the value of the prior.

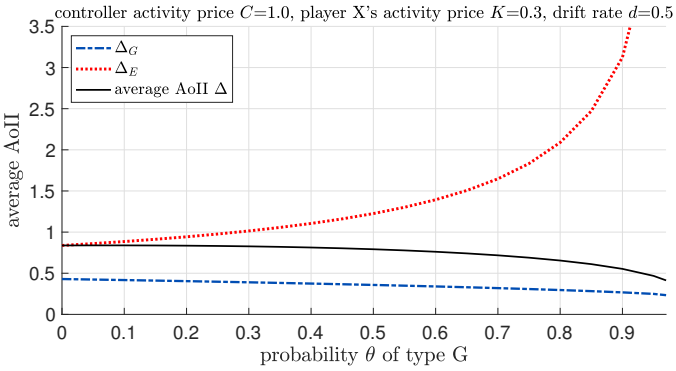

Fig. 3. Expected AoII vs. prior of X's type being G θ, for controller activity price C=1.0, player X's activity price K=0.3, drift rate d=0.5.

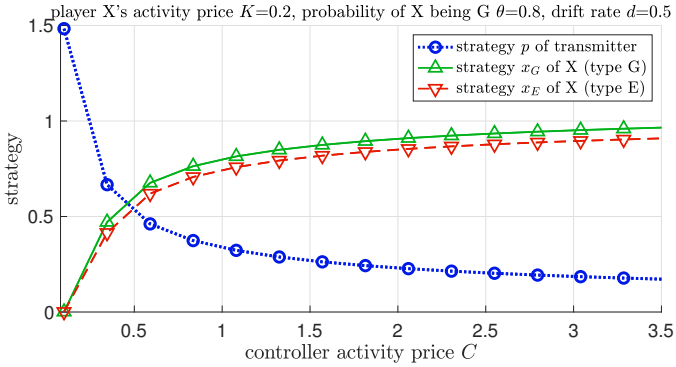

Fig. 4. Strategies of the players vs. controller activity price C, for player X's activity price K=0.2, prior of X's type being G θ=0.8, drift rate d=0.5.

Fig. 3 shows that the trend of the expected AoII is relatively flat. The figure also shows the individual contributions Δ_E and Δ_G, which are interesting only for high θ, where Δ_E soars, yet the overall Δ decreases since the contribution of Δ_E to it is minimal. These trends show that the behavior of both types is often similar, making it difficult to tell them apart.

Fig. 4 displays the strategies of the players versus the unit cost C of the controller's activity. The trend is similar to the previous figure, since increasing C causes player N to be less active; consequently, player X increases its data injection. In Fig. 5, we display the strategies of the players versus the unit cost K of player X's activity. Here, the trend of player X's activity is obviously reversed (it decreases its activity in both types, since they share the same K). For the specific values chosen, player N slightly increases its activity and also x_E drops to 0 sooner than x_G, but these are due to our numerical choice of $\theta = 0.8$, a relatively high value, implying that it is likely that player X is good. However, these trends suggest that neither the variations of C nor K are good indicators to distinguish the types of player X. This weakens one conclusion of [11], i.e., that increasing K can prevent system attacks (but it can also block support from goodwill collaborators).

A better way to distinguish types can be through changes in drift rate d, as visible from Fig. 6. Here, we show the strategies of the players versus d, whose variations are a giveaway for the

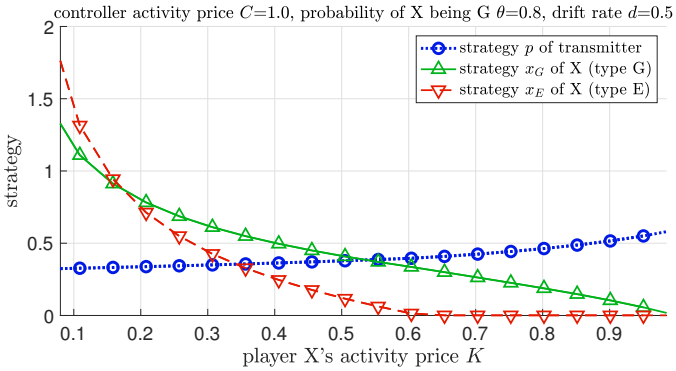

Fig. 5. Strategies of the players vs. player X's activity price K, for controller activity price C=1.0, prior of X's type being G θ=0.8, drift rate d=0.5.

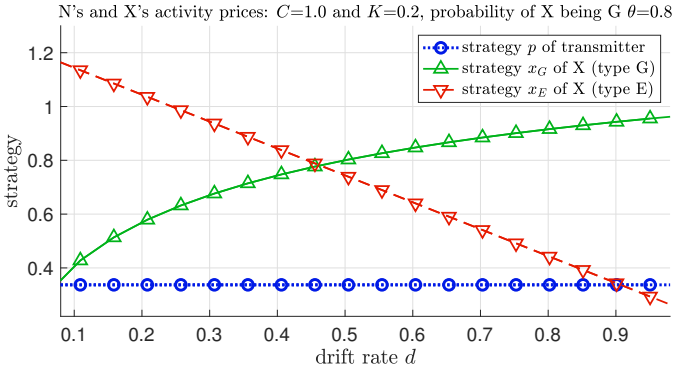

Fig. 6. Strategies of the players vs. drift rate d, for controller activity price C=1.0, player X's activity price K=0.2, prior of X's type being G θ=0.8.

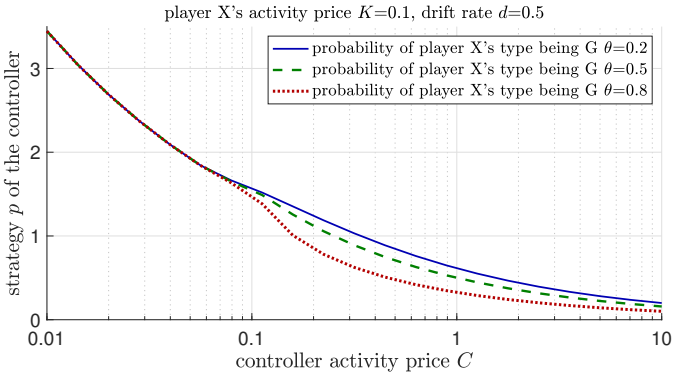

Fig. 7. Controller strategy p vs. activation price C, for different priors of X's type being G θ, player X's activity price K=0.1, drift rate d=0.5.

malicious type. Specifically, when d increases, a collaborative player of type G increases its activity, whereas a player of type E decreases it. This is in line with the finding of [11], showing that malicious players are less active under frequent drifts, as they represent a deterioration of the system's accuracy that comes for free, whereas player X's activity has a unit cost K. However, a collaborative player X would be willing to pay this cost to beneficially decrease AoII [24]. Thus, if the system can control or is aware of drift variations, it can exploit this to distinguish the types of an external player.

Finally, Fig. 7 shows another interesting trend that aligns with Bayesian game theory. In the figure, we focus on the controller N and plot its strategy p versus its cost, for different values of the prior θ. A clear threshold effect is visible in that, regardless of θ, the controller always adopts the same strategy when C is low. As C increases, a point is reached in which N becomes concerned with costs and differentiates its strategy based on how confident it is that player X can provide true support, i.e., the curves separate with those with high θ being lower. Identifying this point precisely and characterizing it analytically may be interesting, as it can represent a vulnerability of the system in which the controller is willing to rely on external agents.

V. Conclusions

We discussed the strategic interaction between a CPS controller and an additional source X that can be collaborative or attempting an FDI attack. The controller's objective is to minimize the average AoII [7]; depending on its nature, X further decreases or increases AoII.

We modeled the decision making of the controller and the two types of player X via Bayesian game theory, discussing the BNE and whether the controller can discriminate legitimate or malicious sources [6], [18]. The BNE always sees an increase in the activity of player X, regardless of its type, when the price value C of the controller increases. This happens because a legitimate additional source intervenes to assist, whereas a malicious one tries to exploit this opportunity to harm the network, knowing that no strong counter-reaction is expected. Similarly, player X decreases its activity when its own price K increases. This means that these parameters are hardly useful in discriminating the behavior of the players.

However, a variation in the drift rate can has different effects on assistive and malicious nodes. The former type increases its activity in the presence of more frequent drifts, a behavior that is not sustained by the latter. Clearly, malicious nodes can enact more sophisticated deceptions (e.g., sometimes supporting the controller), and also attack data integrity in a non-memoryless fashion, hitting harder when they see that the system is vulnerable [20]. The analysis of these complex interactions is an interesting direction left for future work [5].

References

[1] J. Guo, L. Li, J. Wang, and K. Li, "Cyber-physical system-based path tracking control of autonomous vehicles under cyber-attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 5, pp. 6624–6635, 2022.

[2] L. Badia, V. Bonagura, F. Pascucci, V. Vadori, and E. Grisan, "Medical self-reporting with adversarial data injection modeled via game theory," in *Proc. Int. Conf. Commun. Signal Proc. Appl. (ICCSPA)*, 2024.

[3] J. Bae, "An overview of false data injection attack against cyber-physical power systems," *Comput. Syst. Netw. Telec.*, vol. 2, no. 1, pp. 1–8, 2023.

[4] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2158–2169, 2018.

[5] H. Li, S. Amin, Y. Shoukry, and H. V. Poor, "Cyber deception games in cyber-physical systems: A survey," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 3, pp. 1175–1190, 2022.

[6] 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.

[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, 2020.

[8] S. Kriouile and M. Assaad, "Minimizing the age of incorrect information for real-time tracking of Markov remote sources," in *Proc. IEEE Int. Symp. Inf. Th. (ISIT)*, 2021, pp. 2978–2983.

[9] 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.

[10] 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.

[11] 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.

[12] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," *ACM Comput. Surveys*, vol. 50, no. 2, pp. 1–37, 2017.

[13] L. Badia and T. Marchioro, "On the anarchy of multiple false data injectors for age of incorrect information in sensor networks," in *Proc. IEEE Wirel. Commun. Netw. Conf. (WCNC)*, 2025.

[14] Y. Li, D. Shi, and T. Chen, "False data injection attacks on networked control systems: A Stackelberg game analysis," *IEEE Trans. Autom. Control*, vol. 63, no. 10, pp. 3503–3509, 2018.

[15] J. Li, X.-M. Li, G. Chen, X.-J. Peng, and H. Li, "Optimal tracking control for cyber-physical systems under mixed attacks via game-theoretical Q-learning," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 11 944–11 954, 2025.

[16] S. Mangalwedekar, P. Bansode, F. Kazi, and N. Singh, "A Bayesian game-theoretic defense strategy for false data injection attacks in smart grid," in *Proc. IEEE India Counc. Int. Conf. (INDICON)*, 2017.

[17] N. Yi and J. Xu, "Defense strategy selection based on incomplete information game for the false data injection attack," *Int. J. Syst. Sc.*, vol. 55, no. 14, pp. 2897–2913, 2024.

[18] B. Yan, Z. Jiang, P. Yao, Q. Yang, W. Li, and A. Zomaya, "Game theory based optimal defensive resources allocation with incomplete information in cyber-physical power systems against false data injection attacks," *Protection Control Modern Power Syst.*, vol. 9, no. 2, pp. 115–127, 2024.

[19] 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 Wirel. Conf.*, 2015.

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

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

[22] P. Perazzo, M. Paladini, and A. Vecchio, "Connectivity and energy consumption of cyber-physical systems under Wi-Fi attack," in *Proc. IFIP Wirel. Mob. Netw. Conf. (WMNC)*, 2024, pp. 55–59.

[23] J. Doncel and M. Assaad, "Can attacks reduce age of information?" *Perf. Eval.*, p. 102498, 2025.

[24] F. Chiariotti and L. Badia, "Strategic age of information aware interaction over a relay channel," *IEEE Trans. Commun.*, vol. 72, no. 1, pp. 101–116, 2024.

[25] L. Xin, G. He, and Z. Long, "Stealthy false data injection attacks detection and classification in cyber-physical systems using deep reinforcement learning," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 141–153, 2025.

[26] L. Xi, X. Tian, M. He, and C. Cheng, "False data injection detection in power system based on LOSSA-AdaBoostDT," *Protection Control Modern Power Syst.*, vol. 10, no. 3, pp. 55–64, 2025.

[27] A. Garnaev, A. P. Petropulu, W. Trappe, and H. V. Poor, "A jamming game with rival-type uncertainty," *IEEE Trans. Wirel. Commun.*, vol. 19, no. 8, pp. 5359–5372, 2020.

[28] Y. Wang, W. Xing, J. Zhang, L. Liu, and X. Zhao, "Remote state estimation under DoS attacks in CPSs with arbitrary tree topology: A Bayesian Stackelberg game approach," *IEEE Trans. Signal Inf. Proc. Netw.*, vol. 10, pp. 527–538, 2024.

[29] L. Badia, "A Markov analysis of selective repeat ARQ with variable round trip time," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2184–2187, 2013.

[30] S. Tadelis, *Game theory: an introduction*. Princeton Univ. Press, 2013.