A Game of Age of Incorrect Information Against an Adversary Injecting False Data

Valeria Bonagura, Stefano Panzieri, Federica Pascucci
University of Roma 3, 00146 Rome, Italy
Email: {valeria.bonagura, stefano.panzieri, federica.pascucci}@uniroma3.it

Leonardo Badia
University of Padova, 35131 Padova, Italy
Email: leonardo.badia@unipd.it

***Abstract*—Remote sensing enables fast and cost-effective data collection and monitoring, but can be subject to the injection of false data by adversaries. We consider a remote transmitter that is sending status updates about a process to a receiver, incurring a cost when doing so. The system is modeled as transiting between two conditions, implying that the receiver may start with correct knowledge about the process, but this information may become obsolete due to a natural drift of the process toward another regime and the lack of updates by the transmitter. In normal conditions, the transmitter would estimate the age of incorrect information (AoII), a metric proposed in the literature to quantify the time elapsed from the last instant in which the receiver had correct knowledge about the process, to determine the required frequency of updates, balancing it with the transmission cost. We assume the presence of an adversary that may increase the process drift, also incurring its own cost when doing so. The resulting interaction can be analyzed through game theory, with the transmitter and the adversary as strategic players. We present an analysis to determine the conditions for the costs paid by the players and the consequences of their actions on the resulting system performance.**

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

I. Introduction

In recent years, remote sensing technology has seen significant advancements towards the development of high-resolution sensors, possibly combined with drones [1] or satellites [2]. The resulting cyber-physical systems are capable of collecting and transmitting real-time data and enable a fine-graned context awareness that can be used for many applications. Non-invasive and cost-effective sensing technologies can be employed for monitoring different natural and artificial environments, including land and water resources, agriculture, smart cities, eHealth, and the Internet of things (IoT) [3], [4], also proving themselves to be a valuable asset for tactical networks, emergency situations, and disaster management.

At the same time, the issue of the vulnerability of remote sensing arises whenever malicious agents desire to prevent the network control from effective actions. An attacker can be injecting malicious data in the sensing process, with the intent to cause false alarms, or, worse, hide an emergency [5]–[7].

A widely studied approach in the last few years about remote sensing concerns the performance evaluation of the exchange of status updates over a communication channel between a transmitter, often integrated with the remote sensor, and a receiver. The reference metric is often chosen as the age of information (AoI), a quantification of how up-to-date the information about the monitored process is, defined as the time elapsed since the last received update [8]–[10].

AoI just describes the freshness of the content, and implicitly assumes that the environment is highly mutable, thus, every new update is relevant. In some situations, the ambient information is varying slowly and sending status updates would not be required if the system conditions are unchanged. This is especially true in emergency situations: as long as the system operates normally, no update is required. Whenever there is a malfunction, and an alert is to be raised, it is important to do so in a timely manner. Thus, some researchers have proposed the use of the age of incorrect information (AoII) in these cases [11].

AoII is related to AoI and is used to measure for how long the receiver possesses information that is no longer up-to-date. It is defined as the time elapsed from the first time the status of the process changed, *after* an update was received. AoII is relevant in systems where the information is critical and a high level of accuracy is required, such as in control or safety-related applications. A high AoII can indicate that the system is not operating correctly, and that the information being used may not be accurate [12]. Research on AoII is still relatively new, but there have been a few studies that have looked at the impact of different system configurations on the AoII [13].

We analyze a sensing scenario involving status update exchanges between a controller and a remote station over a network in the presence of a malicious agent, referred to as the *adversary*, able to inject false data. This setup is versatile and can be applied to many cyber-physical systems in the IoT or tactical environments.

The controller is assumed to track a process of interest that, even in the absence of the adversary, is subject to a natural drift. The rate of transmission to the remote station ought to be regulated to minimize AoII [14], [15]. However, the intervention of the malicious agent strengthens said drift, and therefore increases AoII. This scenario calls for a game theoretic characterization [1], [3], [9], [10], [16] where the controller and the adversary are modeled as rational agents, with the contrasting objectives to minimize and maximize AoII, respectively. We obtain a sum static game of complete information with an adversarial setup, i.e., played by a minimizer vs. a maximizer (the controller and the adversary,

respectively) [17], [18]. The game is *non zero sum* [19], implying that the utility functions of the two players are not just taken as opposite, or equal to AoII, but we also include a transmission cost for both players. Besides being a standard practice for game theoretic analysis of distributed network agents, adding a cost term is also required to avoid the trivial outcome where the two players simply indefinitely increase their activity [20].

We can characterize the strategic interaction among the players, focusing on the impact of the adversary on AoII and the countermeasures required by the network controller to counteract its increases. The main finding is that, if both players are rational, the attacks of the adversary can be reasonably contained. The extent of this conclusion actually depends on the natural drift of the system; since this corresponds to a baseline increase of AoII that must be counteracted anyways, and comes at no cost for the adversary, it does not make sense for the latter to be overly active unless its transmission cost is low. Thus, for reasonable choices of the parameters, i.e., except for the cases where the adversary has no limitations and therefore cannot be defeated, a tailored increase of the transmission rate by the network controller can prevent from an extreme outburst of AoII. This can be a precious finding to further expand the investigations about strategic interactions in security of cyber-physical systems [21].

The rest of this paper is organized as follows. In Section II, we review related work on AoII and game theoretic interactions. Section III gives a technical description of the system, and its analytical characterization. In Section IV, we solve the interaction between the rational agents as a non zero sum static game of complete information. Section V displays the numerical results, and Section VI concludes the paper.

II. Related Work

The concept of AoII as a metric to better connect status updates with their semantic meaning is quite recent. It was proposed for the first time in [11], where the authors discuss the option to weigh the time elapsed after a correct information drifts toward an incorrect state, resulting in an increasing AoII. This can also be framed in the broader context of shaping AoI as discussed in [22], where different penalties are considered as opposed to the linear increase of standard AoI.

Still, in most follow-up contributions [12]–[15] the definition of AoII follows the original proposal of [11], i.e., to combine a constant weight to represent incorrect information with a linear ageing. We will adopt this approach as well and consider an AoII term that stays at zero after receiving an update, as long as the status update correctly describes the process being monitored. After that point, whenever the process drifts towards a different value and therefore the last update is no longer descriptive of the real status of the system, we have a linear increase of the AoII as a penalty term [23].

In this form, or under minor variations, AoII has received dedicated studies for different scenarios of interest. For example, [14] considers its minimization through a proper scheduling of updates. Other recent contributions investigate the relationship between the mean absolute error in the reports of a specific (piecewise linear) signal over a noisy channel and AoII [13], as well as the minimization of AoII through proper setup of slotted ALOHA parameters [15].

Finally, [12] and [23] consider a real-time tracking of a Markov system, which is similar to what done in the present paper. However, we abstract from the specific chain, still retaining its Markov characteristics, as we are not primarily interested in the source characterization but rather in the impact of adversarial attacks. For this reason, we consider a two-state Markov chain not to represent a binary status, but rather to distinguish whether the information about the process at the receiver's side matches reality or not. In other words, our system is an abstract representation of an arbitrary number of states, where the only concern is whether the status is accurately tracked and the probability that the system reverts back to a correct information after a drift is negligible.

Another original element of this paper is the use of game theory for AoII in the context of an adversary injecting false information. Game theory is in general a powerful tool for modeling, analyzing, and optimizing the behavior of agents in cyber-physical systems, and can be used to design efficient and robust control strategies [24].

For example, in a multi-robot system, game theory can be used to design coordination strategies that optimize task performance [1]. This depends on the efficiency of the resulting Nash equilibrium (NE), which may allow to approach the problem from a decentralized perspective [16].

Alternatively, game theory can be used to model and analyze security aspects of cyber-physical systems, to model the interactions between attackers and defenders, and identify efficient strategies [18]. Indeed, while there exist various game theoretic approaches for AoI [3], [9], [20], [22], the literature is very scarce for applications that involve security aspects.

The only approaches concern the case of AoI under mutual interference conditions [10], [19] or jamming [17]. In this case, the action of the adversary is more limited compared to what we consider here, since we consider malicious data injection [5], and also, we focus on AoII instead. In this sense, our more advanced objectives with respect to the literature are not just a mere theoretical advancement, but make particular sense in light of the increased strategic capabilities of nodes in cyber-physical environments [21].

III. System Model

We consider a networked control system whose dynamics is, for simplicity, described in a scalar domain as

$$\begin{cases} \dot{x}(t) &= ax(t) + u(t) \\ y(t) &= x(t) \end{cases} \tag{1}$$

where $x(t)$, a, $u(t)$, $y(t)$ are real numbers representing the plant state, open-loop gain of the plant, control input end output, respectively, at time t. The control signal $u(t)$ is generated with a memory-less control policy and is therefore only dependent on $y(t)$; thus, the process $x(t)$ is Markov [12].

The controller, in addition to generating a control signal $u(t)$, communicates with a remote station (e.g., a SCADA system) sending the measurement of the output $y(t)$. In this work, we neglect the propagation delay between the controller and the remote station, so the time can be computed indifferently on the transmitter or the receiver side [25].

When the controller sends the output measure to the remote station, the latter performs an update of the stored value of the system's output. Thus, AoI at time t is [8]

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

where t_u is the last time instant corresponding to the reception of the last update before t, inclusive.

After an update, the AoI linearly increases as time goes by. However, the reported value might still describe the correct system state. In certain scenarios [11], we may want to explore whether the status is still correct or has become wrong due to a drift. This can be modeled through a continuous time Markov chain with two states, namely, right (R) and wrong (W), whose transitions are as follows.

The information at the remote station's side can become inaccurate due to a natural drift, whose rate d determines the transition from R to W. Additionally, we assume that the adversary can decrease the time spent in state R (and therefore increasing AoII) by increasing the drift rate by a term $q > 0$, which corresponds to the injection rate of false data that compromise the SCADA functionality.

Transitions from W to R happen instead because the controller sends updates to the remote station, which occurs with rate $p > 0$. It is not restrictive to assume that the updates are always successful, since in case they can be missed with a certain probability, one can correspondingly re-scale the value of p [25]. The remote system is aware that a malicious agent is present, but is unable to distinguish between the updates sent by the controller and the malicious agent.

We remark that characterizing the actions of the involved rational agents (the controller and the adversary) just through their activity rates p and q is a standard approach that allows to define a clear-cut strategic action of these agents as players in a game [9], [10], [19]. From the mathematical standpoint, the system respects the Markov property as all the three events of an update from the controller, a natural drift, and false data injection by the adversary are independent of one another, so the transitions are memoryless, and the two last ones just sum up to cause the transition rate from R to W be equal to $d+q$. The resulting Markov model is summarized in Fig. 1.

The receiver possesses a correct measure of the output of the system until a drift occurs or a malicious agent sends false sensor reading. From the perspective of the controller, the objective is to minimize AoII defined as [11]

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

where $g(\cdot,\cdot,\cdot)$ is a function that reflects the gap between the real output of the system in time slot t i.e., $y(t)$, the last correct update sent by the controller to the remote station in time slot t_u i.e, $y(t_u)$ and the last false sensor reading sent by the malicious agent to the remote station at t_m i.e, $y(t_m)$. Function $f(\cdot)$ is non-decreasing and plays the role of penalizing the system as $g(\cdot,\cdot,\cdot)$ increases.

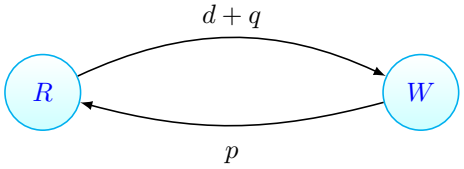

Fig. 1. Illustration of a continuous time Markov process with the respective rates of moving to one state to one another

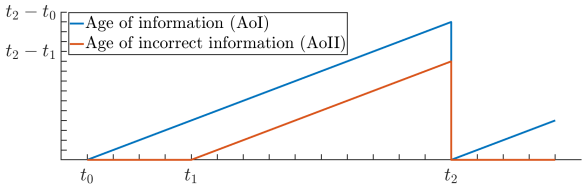

Fig. 2. Age metrics are initialized to 0 at t_0. From that instant onwards, AoI increases linearly, whereas AoII initially stays at 0 (status is obsolete but correct). At t_1, AoII starts increasing as well due to a drift. At t_2, status is refreshed. For any $t \in (t_1, t_2)$, AoI and AoII are $t-t_0$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

We first derive a closed form of AoII in the scenario without an adversary, then we introduce the malicious agent and discuss its impact. We consider the expected value of the AoII $\Delta = \mathbb{E}_t\big[\delta(t)\big]$ meant as a time average. To compute Δ, we exploit functions $g(\cdot,\cdot,\cdot)$ and $f(\cdot)$ introduced in (3). For example, we can use

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

where $t_s = \min(t_u, t_m)$ and $\vartheta > 0$ is an arbitrary threshold. This is an adequate choice when the remote system performance is immune to small mismatches between $y(t)$ and $y(t_s)$ [11]. We assume that, following a drift or a malicious transmission, $|y(t) - y(t_s)| > \vartheta$ until an update takes place. We define t_d as the index of the last instant where $g(y(t), y(t_u), y(t_m))$ was equal to 0, i.e., the index of first instant after the last update where a drift or a malicious injection occurred. For AoII, we use a linear $f(\cdot)$ defined as [11]

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

Fig. 2 shows a comparison between AoI and AoII for a sample situation where a drift (either naturally present or maliciously induced by an adversary) occurs at time t_1, while at t_2 a new update is performed.

With $\delta(t)$ so defined, the expected value Δ can be computed by averaging over a *period* between any two subsequent updates, thus obtaining

$$\Delta = \frac{1/(2 \cdot p^2)}{1/p + 1/b} \tag{6}$$

where $b = d + q$. In (6), the numerator $1/2p^2$ is the average area below the AoII in a period, whereas the denominator

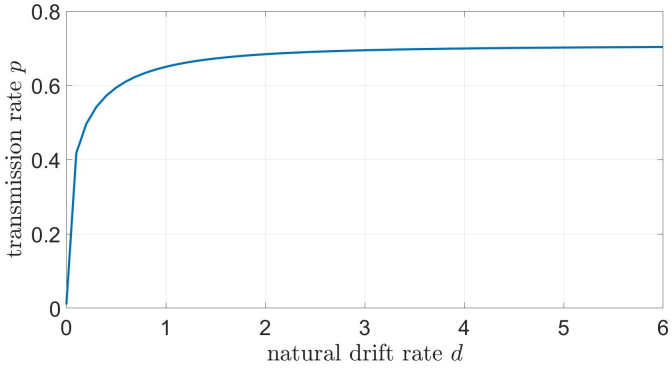

Fig. 3. Optimal transmission rate with transmission cost $C = 1$ and natural drift rate $d = 0.5$

$1/p + 1/b$ is the expected value of the time elapsed between two adjacent updates.

The controller can achieve a very low AoII with a high p, i.e., updating very often. However, we assume that sending transmissions to the remote station has a cost proportional to p through a coefficient C that can be interpreted as either related to energy expenditure or just as a shadow price accounting for any factor that limits the updating frequency [16].

If no adversary is present in the system, the optimal transmission rate p is just obtained from balancing the cost term $C \cdot p$ and the drift average rate d, solving an unconstrained optimization of the controller's utility function defined as

$$u_{\mathrm{N}}(p) = -\Delta - Cp. \tag{7}$$

A graphical representation of a possible optimal transmission rate is shown in Fig. 3. One can see that, the larger the natural drift d, the larger the optimal p. Yet, the curve saturates for high d, due to transmission costs that make it inconvenient to further increase the transmission rate.

With an adversary trying to compromise communication, the term Δ also depends on q, and the utility in (7) must be written as $u_{\mathrm{N}}(p, q)$. We assume that the adversary incurs a cost Kq, with direct proportionality to the injection rate q through a coefficient $K > 0$, limiting its false data injection. The utility of the adversary, whose aim is a high AoII, can be written as

$$u_{\mathrm{M}}(p, q) = \Delta - Kq. \tag{8}$$

The symbols used for the parameters are reported in Table I.

TABLE I
SUMMARY OF THE NOTATIONS

Parameter	**Symbol**
Transmission cost for sensors	C
Injection cost for malicious agent	K
Natural drift rate of the physical system	d
Variable	**Symbol**
Transmission rate for sensors	p
Injection rate for malicious agent	q

IV. Game theoretic analysis

We denote the controller and the adversary as two rational agents N and M, respectively. They play a static game of complete information with continuous valued actions p and q, both chosen in $(0, \infty)$. A static (one-shot) game concentrates the strategic interplay in one interaction, where agents selfishly follow their own utilities [26], which are $u_{\mathrm{N}}(p, q)$ and $u_{\mathrm{M}}(p, q)$. Values p and q are determined by N and M, respectively, independently and unbeknownst of each other.

The NE is derived from

$$\frac{\partial u_{\mathrm{M}}(p,q)}{\partial q} = 0 \qquad \frac{\partial u_{\mathrm{N}}(p,q)}{\partial p} = 0 \tag{9}$$

which implies

$$\frac{\partial \Delta}{\partial q} = K \qquad \frac{\partial \Delta}{\partial p} = -C. \tag{10}$$

Rearranging the terms in (10) gives

$$\begin{cases} p = \dfrac{1}{\sqrt{2K + 2C}} \\ q = -d - p + \dfrac{1}{\sqrt{2K}}. \end{cases} \tag{11}$$

Within (11), K must be low enough to meet the requirement that q is positive. If $q < 0$, the adversary has no advantage in injecting false data, and is actually silent. In that case, the optimal update frequency p reduces to a single-agent optimization maximizing (7). Thus, in (11), the injection cost term K is contrasted by the natural drift d and the transmission rate p: whenever they are too large, q is positive only if K is very low. More in general, we can discuss the choice of values for K such that player M is taking part in the game and (11) correctly represents the NE.

From (11), if $K > d^{-2}/2$, it is impossible to get $q > 0$. Even if $K < d^{-2}/2$, it might be inconvenient for the adversary to transmit, as it must also hold

$$-d - \frac{1}{\sqrt{2K + 2C}} + \frac{1}{\sqrt{2K}} > 0. \tag{12}$$

Rearranging (12), we get $K < \left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2}/2$, which is easy to check despite a term K being in both sides of the inequality, as K, C, and d are parameters known to both the controller and the adversary. Thus, if

$$K > \frac{1}{2} \min \left[\left(\frac{1}{\sqrt{2K + 2C}} + d \right)^{-2}, d^{-2} \right], \tag{13}$$

then the adversary has no advantage in transmitting. Since $(2K + 2C) > 0$, it is immediately verified that the right-hand side of (13) is always $\left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2}/2$. Thus, the NE conditions are

$$p = \begin{cases} (2K + 2C)^{-0.5} & \text{if } K < \left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2}/2 \\ \sqrt{(d+p)^2(1-2Cp^2)} & \text{otherwise} \end{cases} \tag{14}$$

$$q = \begin{cases} -d - p + \dfrac{1}{\sqrt{2K}} & \text{if } K < \left(\frac{1}{\sqrt{2K+2C}} + d\right)^{-2}/2 \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

where the second part of (14) comes from minimizing (7).

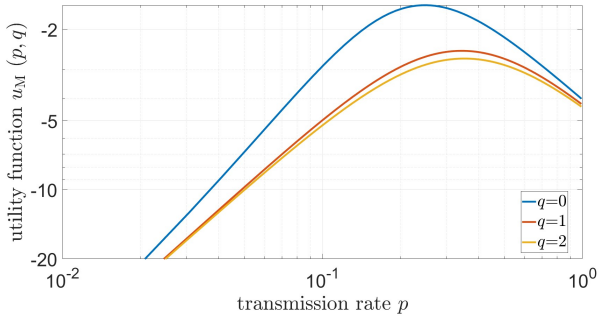

Fig. 4. Utility $u_{\mathrm{M}}(p,q)$ for $C=4$, $K=0.1$, $d=0.1$, and $q=0,1,2$.

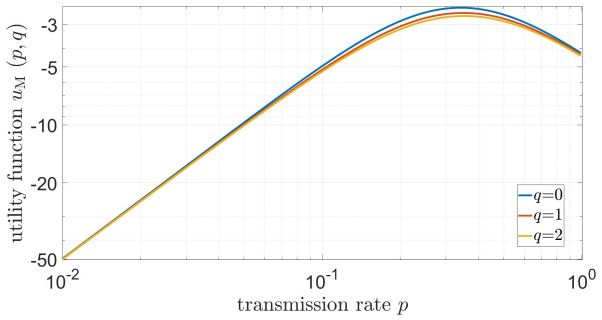

Fig. 5. Utility $u_{\mathrm{M}}(p,q)$ for $C=4$, $K=0.1$, $d=1$, and $q=0,1,2$.

V. Numerical Results

We evaluate the system performance at NE for the controller and the malicious agent being strategic agents driven by $u_{\mathrm{N}}(p,q)$ and $u_{\mathrm{M}}(p,q)$, respectively. This means that the controller wants to minimize AoII at the remote station, while the adversary wants to maximize it, but at the same time they both try minimizing their individual activity costs.

Figs. 4 and 5 investigate how the controller can choose its activity rate and show that utility $u_{\mathrm{M}}(p,q)$ with fixed q has a maximum in p. As the injection rate q increases, the maximum of $u_{\mathrm{M}}(p,q)$ decreases. This is due to the fact that the controller has to transmit more often to minimize AoII, resulting in higher costs. The figures investigate a different natural drift rate: $d=0.1$ and $d=1$ for Figs. 4 and 5, respectively. From their comparison, it is also inferred that as d increases, the NE in the presence of the adversary tends to approach the optimal value in its absence.

Figs. 6 and 7 show the strategic value of p depending on the presence (or not) of player M in the game at a fixed natural drift rate d (for which, we considered different values of 0.1 and 1, respectively) and injection cost K. The adversary causes an increase in the strategic transmission rate of the controller, and as its transmission cost increases, the difference between the two cases decreases. This is because a high transmission cost makes it inconvenient for the controller to increase the transmission rate, which is advantageous for the adversary. The results also show that as the natural drift d increases, the effect of the adversary on the NE decreases.

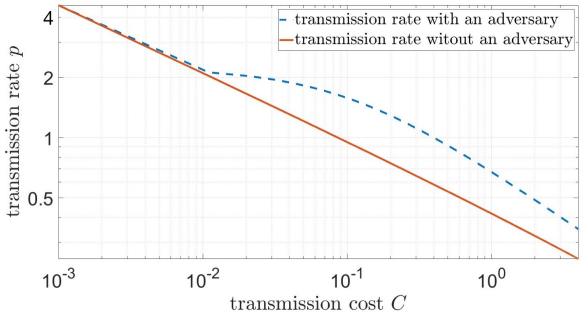

Fig. 6. Comparison of strategical update rate p with and without a malicious agent, $K=0.1$ and $d=0.1$

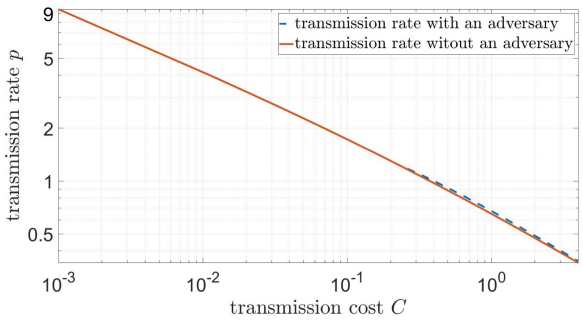

Fig. 7. Comparison of strategic update rate p with and without a malicious agent, $K=0.1$ and $d=1$.

Figs. 8 and 9 show the effect of the strategic behavior. In Fig. 8, as the transmission cost for player M increases, q decreases until it reaches 0, at which point it is no longer convenient for the adversary to inject data. Also, as the drift rate d increases, the injection rate agent decreases according to (15). This implies that when the malicious agent transmits, the lower the drift rate, the higher the update rate required to the controller to contrast the malicious injections. Fig. 9 shows that, as the transmission cost for the controller increases, it gets more convenient for the adversary to transmit. In accordance with (15) and its related discussion, as the drift rate increases, the value of q chosen by a strategic player decreases.

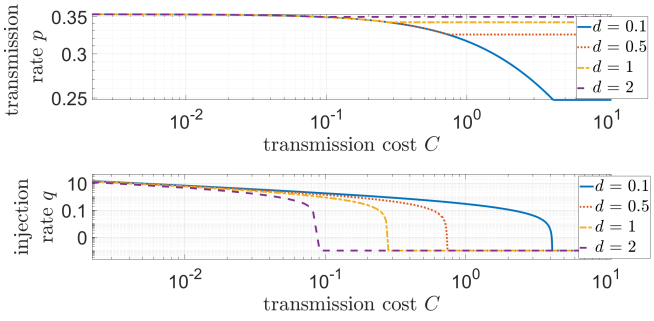

Fig. 8. Transmission rate p and injection rate q at the NE, for $C=4$ and $d\in\{0.1,0.5,1,2\}$.

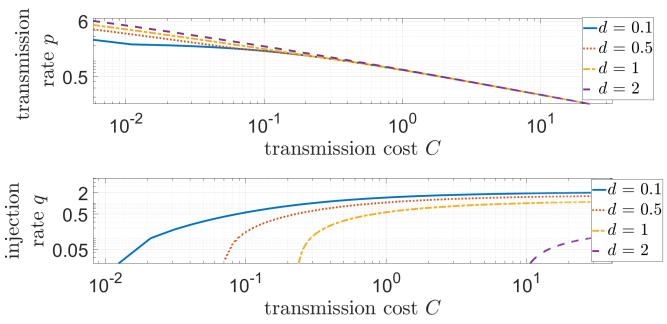

Fig. 9. Transmission rate p and injection rate q at the NE, for $K = 0.1$ and $d \in \{0.1, 0.5, 1, 2\}$.

Overall, the main takeaway message from our results is that false data injection can be effectively counteracted. First, there is a wide range of scenarios where the adversary ends up being inactive (essentially, due to high costs). The threat of data injection is concrete only if it comes at a very low cost, and even in this case, it can be strongly limited by a proper increase of the activity rate of the controller.

However, our analysis considers a scenario with complete information, especially meaning that the controller is aware of the presence of the adversary in the game. Hence, another insight gained is about the importance of monitoring for external data injected. All of these aspects can be seen as interesting extensions for future work, especially in the context of more advanced game-theoretic approaches, leveraging for example on Bayesian games [18].

VI. Conclusions

We investigated a scenario involving status updates between a controller and a remote station over a network in the presence of a malicious agent that sends fake status updates.

We provided a game theoretic description of the interaction between the controller and the adversary. The latter seeks to maximize AoII at the remote station and minimize its own cost, whereas the former wants to minimize AoII at the remote station and its own cost. We computed the NE, which is guaranteed to exist and be unique. The NE implies certain conditions that may cause the adversary to be inactive and the problem to revert to a plain nonlinear optimization. Even when this does not happen, our formulation as a static game of complete information gives an advantage for the controller that, for the same transmission and injection costs, does not significantly change its policy because of the adversary. This also stresses the importance of a careful monitoring to discover the presence of a potential threat beforehand and be aware of its presence. Future investigations may extend these results to more general scenarios and advanced strategic interactions.

References

[1] E. Camuffo, L. Gorghetto, and L. Badia, "Moving drones for wireless coverage in a three-dimensional grid analyzed via game theory," in *Proc. IEEE APCCAS*, 2021, pp. 41–44.

[2] E. Recayte and A. Munari, "Caching at the edge: Outage probability," in *Proc. IEEE WCNC*, 2021.

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

[4] A. Zancanaro, G. Cisotto, and L. Badia, "Modeling value of information in remote sensing from correlated sources," in *Proc. IEEE MedComNet*, 2022, pp. 47–53.

[5] B. Kumar and B. Bhuyan, "Using game theory to model DoS attack and defence," *Sādhanā*, vol. 44, no. 12, p. 245, Nov. 2019.

[6] 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.

[7] B. Li, H. Li, Q. Sun, and R. Lv, "Optimal control of false information clarification system under major emergencies based on differential game theory." *Comput. Intell. Neurosc.*, vol. 2022, Sep. 2022.

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

[9] L. Badia, A. Zanella, and M. Zorzi, "Game theoretic analysis of age of information for slotted ALOHA access with capture," in *Proc. IEEE Infocom Wkshps*, 2022.

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

[11] A. 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

[18] V. Vadori, M. Scalabrin, A. V. Guglielmi, and L. Badia, "Jamming in underwater sensor networks as a Bayesian zero-sum game with position uncertainty," in *Proc. IEEE Globecom*, 2015.

[19] 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.

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

[21] 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.

[22] 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.

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

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

[25] L. Badia, "A Markov analysis of selective repeat ARQ with variable round trip time," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2184–87, Nov. 2013.

[26] 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.