Medical Self-Reporting With Adversarial Data Injection Modeled via Game Theory

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

Valeria Bonagura, Federica Pascucci
University Roma Tre, Italy
{valeria.bonagura,federica.pascucci}@uniroma3.it

Valentina Vadori, Enrico Grisan
London South Bank University, UK
{vadoriv,grisane}@lsbu.ac.uk

***Abstract*—We present a game theoretic analysis of a personal e-health system, where a user reports self-measured data to a collection center. Our focus lies on addressing the challenge of potential mistakes in the reported data, a common issue for untrained users in e-health scenarios. The system alternates between the states of correct or erroneous data about the user being available at the collection center. Our goal function is related to age of incorrect information, a measure of the staleness of the information content. It linearly increases as time spent in the erroneous state elapses further. In this scenario, we introduce an additional malicious agent that injects erroneous measurements with the objective of exacerbating the staleness of information. This leads to an adversarial game between the user of interest and the malicious agent, the equilibrium of which we discuss. We derive closed-form expressions based on the system parameters, providing insights into the parametric ranges where the impact of the adversary is most menacing.**

***Index Terms*—Personalized medicine; Medical self-reporting; False data injection; Age of incorrect information; Game theory**

I. Introduction

Among the applications of cyber-physical systems, a cornerstone is represented by personalized medicine, where individual well-being is supported by customized technological solutions leveraging portable devices, ubiquitous communications, and advanced data interpretation, possibly powered by machine learning (ML) [1]–[4]. This technological paradigm often requires a change in approach for data collection, from concentrated medical examinations and observations, where intense data sampling is performed by trained personnel, to patient-generated data obtained through self-reporting [5].

This certainly offers multiple advantages, for example, in terms of richness and coverage of the patient conditions, as well as a general feeling of the data collection being less invasive and also more satisfactory for the patients themselves [6]. Thus, self-reporting medical data can be seen as an empowerment of individuals to contribute information and make them more active in the therapeutic process. However, such a patient-centric approach also introduces a complex set of challenges, prominently featuring concerns related to data accuracy, integrity, and security [7], [8].

One of the main issues revolves around the correctness of self-reported data, as patients become active participants in documenting their health journey. This raises critical questions about the reliability of the information provided and, subsequently, the efficacy of medical decisions based on such data [9]. Moreover, as the healthcare landscape embraces digital platforms and interconnected systems, the vulnerability to security breaches becomes a pressing concern [10], [11]. In particular, the threat of false data injection looms large, posing significant risks to the integrity of personalized medicine initiatives. Indeed, the presence of a malicious agent injecting false data can wreak havoc on the network management as it further aggravates the problems of erroneous data reporting by the individual users, changing it from a random nuisance into an intentional service disruption [12].

Within this context, we employ the methodology of *game theory* to shed light on the potential pitfalls associated with inaccurate data reporting and the associated security challenge posed by malicious agents, with a precise focus on false data injection. Specifically, we consider a two-state system, where the state changes depend on the actions of the involved participants, from an individualistic perspective [13], [14].

Correct data reporting puts the system in the "right" state to reflect that the data collection center has accurate information about the patient. An erroneous reporting puts instead the system in the "wrong" state. Reported values are correct or erroneous with independent and identically distributed (i.i.d) probabilities [15]. We consider that the system can transition to an erroneous state due to a natural drift, reflecting the underlying dynamics of the patient's condition. This implies that patients must continue to report their own data over time to maintain the accuracy of the system [16], which is similar to channel-dependent scheduling in wireless communications [17]. Finally, we consider the possible presence of an adversary that can inject inaccurate data, thus increasing the rate of transitions to the "wrong" state.

Such a system incurs an operating penalty that can be quantified through the average value of the age of incorrect information (AoII) [18]. The latter refers to a recently proposed metric that combines the inaccuracy in the system's knowledge with how this inaccuracy worsens over time due to staleness. In medical applications, this metric is particularly problematic as it represents the timeliness (or lack thereof) of intervention in a medical emergency whenever it is needed.

This work was supported by the Italian PRIN project 2022PNRR "DIGIT4CIRCLE," project code P2022788KK, and by Next Generation EU, under National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Investment 3.3 - Project code D93D22001390001 (DAuSy).

This results in a game played by strategic agents, namely the legitimate user and the adversary [19]. Our analysis discusses the role of different system parameters and the implications on the resulting system performance. The evaluation of the parameter ranges where the adversary can be effectively counteracted can eventually serve to obtain practical results to improve security in cyber-physical systems [20], [21].

The rest of this paper is organized as follows. In Section II, we analyze similar models taken from the literature, giving game theoretic investigations of information freshness in competing and possibly adversarial systems. Section III gives a system description and presents the analysis with numerical and closed-form derivations of the Nash equilibria. We present numerical evaluations in Section IV, and we finally conclude in Section V.

II. Related work

Upcoming technologies like the 6th generation (6G) of mobile communications promise to boost the current sensing, transmission, and interaction capabilities of medical interconnected devices [10], opening unprecedented possibilities to smart health services. However, the increase in transmission ranges and the availability of pervasive communications also come together with the option for an adversary to maliciously inject data in the system [4].

Most of the literature discussing false data injection actually revolves around the classification of different use cases or practical techniques to counteract the problem. For instance, physical layer techniques such as watermarking or partial self-jamming [22] can be employed to limit the ability of an adversary to imitate legitimate content.

In [20], a mechanism for secure estimation is proposed based on optimal filtering and learning to exclude malicious injections. Reference [12] proposes a detection-oriented coding to reveal false data injection attacks through estimation residues.

Instead of investigating ways to counteract false data injection through technical means, in this paper, we admit it as a possibility and seek an evaluation of its impacts. This is motivated by the remark that personal medical monitoring devices are very often insecure and subject to external intrusions or tampering, as argued in [23]. For this reason, we admit that an adversary may inject false values in our systems, and we evaluate the consequences of this hazard, as well as estimating if this can be properly counteracted by an increased activity by the user to obtain a more faithful monitoring.

To obtain a quantitative evaluation, we use an approach based on AoII, a metric proposed for the first time in [18], corresponding to a linear penalty increase during the time intervals where the state information is incorrect. Such a metric can be seen as a generalization of the age of information [24], a performance metric that is enjoying popularity to quantify the freshness of data exchanged over sensing networks.

However, in its original formalization, AoII was considered as just due to system drifts or changes of state in the system. The added element of our analysis is that we analyze the incorrectness of information when intentionally caused by an adversary. At the same time, the reporting user is also assumed to be strategic and contrasting false data injection (e.g., increasing the activity rate). This leads to a game theoretic approach similar to [21], which presents a strategic analysis of false data injection. However, in that paper, the players act as minimizer/maximizer of the false alarm probability, whereas we consider an AoII-based reward, which also accounts for how long the information is kept in the wrong state, and we include the cost of activity in the game.

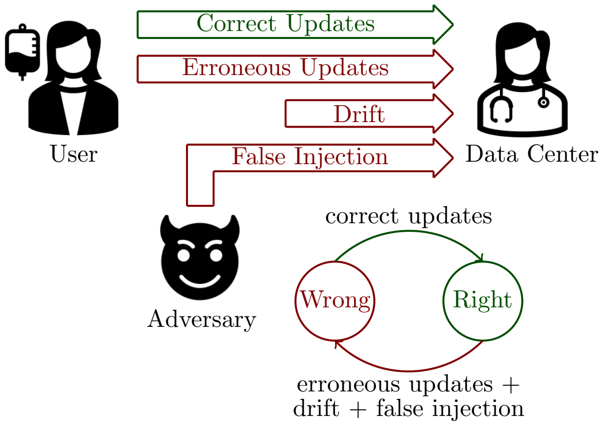

Fig. 1. System model.

While game theoretic approaches exist for AoI [8], [25]–[27], they mostly consider access in resource-constrained scenarios and not adversarial setups. Moreover, [28] actually involves a system where a third party acts to assist the communication from the reporting user instead of harming it. The present analysis considers instead an adversarial setup with false data injection and is based on our previous contribution made in [15]. However, it has the notable difference that the system state changes to the wrong state also by the effect of erroneous self-reporting by the individual user, which is a key problem in personal e-health systems [7]. Because of this, the building equations are different. In particular, while the solution concept is analogously through the Nash equilibrium, the proposed approach allows us to evaluate the impact of the failure rate on the performance metrics.

We remark that similar game theoretic approaches to the one used here can also be employed for different kinds of attack other than false data injection, specifically *jamming*, where the malicious agent destroys the user-generated content, thereby increasing the failure rate [19], [29], or *eavesdropping*, where the adversary is interested in capturing private information sent by the user [30], [31], which can be both serious source of concerns in medical self-reporting applications.

III. System analysis

The system under investigation is displayed in Fig. 1. In our model, we consider a remote user performing medical self-measurements to monitor health conditions and sending the resulting medical data to a collection data center, which can be a hospital or a physician. However, the data sent are not always correct due to the following undesired effects: (i) mistakes in the measurements by the remote user, so that they do not really reflect real medical conditions; (ii) a system drift reflecting the system dynamics, so that the values change and, while the measurements were previously correct, are no longer so; and finally, (iii) possible false data injection by an adversary.

Effects (i) and (ii) are described through stochastic processes that can be regarded as unintentional and, therefore, independent of each other. Conversely, (iii) can be present if an adversary intentionally attacks the system.

As a result, whenever a correct update is delivered to the data center, the system state transits to the "right" state since the monitoring platform now has correct medical information on the user. Conversely, all the events of erroneously reported update, data drift, or malicious injection cause the opposite transition towards the "wrong" state. If we assume all of these transitions to occur with memoryless dynamics (e.g., drifts or data reporting happen at random instants whose intervals are exponentially distributed), this reasoning can lead to a representation as a two-state continuous-time Markov chain. However, it is important to note that even in the case of more complex scenarios, similar reasoning can lead to a slightly more intricate Markov chain representation. Nevertheless, this representation still maintains the same fundamental features as discussed above.

We assume that the user transmits updates at a rate t, with a failure rate f. Therefore, the generation rates of correct and erroneous updates are $(1-f)t$ and ft, respectively. Additionally, we consider a drift rate d and a malicious injection rate of q by the adversary, as described in [15]. Note that the analysis in [15] assumed, unlike our approach here, that the updates were always successful.

We assume that all transitions from injected false data, erroneous updates, or data drifts are substantially equivalent, as they all have the effect of leading the system to an "wrong" state. Consequently, the receiving station cannot distinguish false data from erroneous legitimate updates. However, it is straightforward to include this consideration by treating q as the "net injection rate" that escapes detection from the data center.

Further, we assume that transmissions from the user and false data injection by an adversary incur a cost proportional to their rate through a constant parameter that can be seen as a price (i.e., cost per unit rate) [26]. The meaning of such a cost can be connected to the energy expenditure, which would be proportional to the activity rate, or just seen as a *shadow price*, i.e., the Lagrange multiplier of the constraint limiting the activity to indefinitely increase [14]. We denote these prices as C and K for the legitimate user and the adversary, respectively, in accordance with [15]. A summary of the notation for these parameters is reported in Table I.

TABLE I
NOTATION FOR THE ANALYSIS

Quantity	Symbol
transmission rate from the user (R)	t
failure probability of a user update	f
injection rate from the adversary (M)	q
system drift rate	d
transition rate → Wrong	$b = ft + q + d$
transition rate → Right	$p = (1-f)t$
transmission price for the user	C
transmission price for the adversary	K
average age of incorrect information (AoII)	Δ

Since our proposed model involves a recurring Markov chain, where the system alternates between two states, one can focus on the cycles between the hits of the "right" state. Thus, it is immediate to derive the average AoII, denoted as Δ, as the average reward obtained over a cycle divided by the duration of the cycle itself [28], which leads to [15]

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

where $b = ft+q+d$ is the rate of transitions towards the wrong state, whereas $p = (1-f)t$ is the rate of transitions towards the correct state. This means that (1) can be rewritten as

$$\Delta = \Delta(t,q) = \frac{ft + d + q}{2(1-f)t(t+d+q)} \,. \tag{2}$$

In light of this, we can take the actions of the reporting user R, as well as the malicious agent M, as guided by *utility functions*, respectively defined as follows

$$u_{\mathrm{R}}(t,q) = -\Delta(t,q) - C\cdot t, \quad u_{\mathrm{M}}(t,q) = \Delta(t,q) - K\cdot q \,. \tag{3}$$

In these definitions, we take inspiration from adversarial setups that are commonly modeled in game theory as *zero-sum* games [19]. Yet, our model here is not zero-sum in that we also include a cost term proportional to the player's activity through the respective prices.

These definitions mean that if the adversary is not present and therefore $q = 0$, the optimal transmission rate of the reporting user, which we denote as t_0, can be determined through a single variable maximization of $u_{\mathrm{R}}(t,0)$. Since in our model this is a rational function that is continuously differentiable, we can compute t_0 by imposing

$$\frac{\partial u_{\mathrm{R}}(t,0)}{\partial t} = 0 \qquad \Rightarrow \quad \frac{\partial \Delta(t,0)}{\partial t} = -C \,. \tag{4}$$

In general, this leads to an equation that can be solved numerically. However, if $d \to 0$, which is the case for a slowly drifting process, then the optimal transmission rate is only limited by failures. This can be seen as a lower bound, and we can write

$$t_0 \geq \lim_{d\to 0} t_0 = \sqrt{\frac{f}{2(1-f)C}} \tag{5}$$

Instead, to evaluate the outcome when false data injection is present ($q \neq 0$), since this is controlled by a different agent than the reporting user and whose objective is also clearly different, we need to resort to a game theoretic setup.

Specifically, we frame the problem as a *static game of complete information* [26], which means that two players choose an action independently and unbeknownst to each other, and the outcome of the game is determined by their *joint* choices. In making their choice, the players have complete information about the possible results, but they do not know each other's choice. Still, the usual approach of game theory is that a desirable outcome for the players can be obtained as the Nash equilibrium, seen as a point where no unilateral deviation by either player is convenient. In our formalization, the set of players is $\{\mathrm{R}, \mathrm{M}\}$, their respective actions are their activity rates t and q, both chosen as non-negative real values, and their utility functions are u_{R} and u_{M} as per (3).

Thus, the NE equations can be derived as [28]

$$\frac{\partial u_{\mathrm{M}}(t,q)}{\partial q} \;=\; 0\,, \qquad \frac{\partial u_{\mathrm{R}}(t,q)}{\partial t} \;=\; 0\,, \tag{6}$$

resulting in

$$\frac{\partial \Delta(t,q)}{\partial q} \;=\; K\,, \qquad \frac{\partial \Delta(t,q)}{\partial t} \;= -C. \tag{7}$$

The first condition leads to the convenient result

$$t + d + q = \frac{1}{\sqrt{2K}} \tag{8}$$

whereas the second obtains

$$C = \frac{1}{2(1-f)}\left(\frac{1}{t^2} - \frac{1-f}{(t+d+q)^2}\right). \tag{9}$$

It must be remarked that (8) is valid only if the resulting value for q is non-negative, thus this equation imposes $K < (t+d+q)^{-2}/2$, otherwise the optimal choice of the adversary is to be inactive ($q = 0$), and we fall back in the single-agent optimization as per (5). The practical interpretation of this condition is that there is an upper limit $\mathcal{K}_{\max}$ for the false data injection price, and if $K > \mathcal{K}_{\max}$, there will be no malicious activity since a strategic adversary will realize that it is not convenient to further increase the system's AoII with respect to what the failures and the natural drift already do (at no cost to the adversary). This underlines the importance of *system-awareness* in the opportunistic selfish behavior by the adversary [17].

If $K \leq \mathcal{K}_{\max}$, combining (8) into (9) obtains

$$t = [2(C+K)(1-f)]^{-1/2}\,. \tag{10}$$

which highlights an increase in activity with respect to (5), whereas of course if $K > \mathcal{K}_{\max}$ then $t = t_0$.

It may be useful to get an estimate of the upper limit $\mathcal{K}_{\max}$, since it is a quantification of the amount of defense that the network operator has to put in place to prevent malicious activities so that there is no adversarial injection if the price of adversarial activity is beyond that value. This can be achieved numerically based on the information provided above, although it is possible to derive closed-form bounds.

It may be tempting to consider the case of a vanishing system drift $d \to 0$, in which case we can immediately find an estimate $\widetilde{\mathcal{K}}_0$ by imposing $\sqrt{2K} < t^{-1}$ and taking the expression of t from (10), resulting in

$$0 \leq K < \widetilde{\mathcal{K}}_0 = \frac{C(1-f)}{f}\,. \tag{11}$$

However, this bound is very loose if d is small but non-zero because the actual condition is

$$\frac{1}{\sqrt{2K}} > \frac{1}{\sqrt{2(C+K)(1-f)}} + d$$

and the two sides of the inequality have a constant bias that only depends on d and is non-vanishing when its value is non-zero, even if small.

A tighter bound can be found by reordering the terms as

$$2dK\sqrt{f\widetilde{\mathcal{K}}_0 + K(1-f)} < f(\widetilde{\mathcal{K}}_0 - K) \tag{12}$$

where we neglected the term in d^2 but not that in d. Clearly, if $d = 0$ then we fall back to the previous upper bound $K < \widetilde{\mathcal{K}}_0$, but if we instead impose $\sqrt{K} = x$ we can solve the third degree inequality resulting from (12):

$$2d\sqrt{1-f}x^3 + (2d\sqrt{f\widetilde{\mathcal{K}}_0} + f)x^2 - f\widetilde{\mathcal{K}}_0 < 0 \tag{13}$$

whose associated equation only admits one positive solution α, the LHS term being always strictly increasing in $x \in [0, \infty)$, and its values at 0 and ∞ being negative and positive, respectively. This means that (13) gives a tighter upper bound $\widetilde{\mathcal{K}}_1 = \sqrt{\alpha}$ on the values of K where adversarial activities are possible, whenever $K < \widetilde{\mathcal{K}}_1$.

IV. Numerical evaluations

We present numerical evaluation samples derived from the computations discussed in the previous section. In all the plots, the transmission price for the reporting user R is set at $C = 1.0$, and the system drift is $d = 5 \cdot 10^{-2}$. While these specific values were used for the sake of illustration, the analysis is inherently general and can seamlessly accommodate other values as needed.

In the plots, we consider two different values of the failure probability $f \in \{f_1, f_2\}$. Specifically, we set $f_1 = 0.1$ and $f_2 = 0.3$. Such values correspond to $\mathcal{K}_{\max} \approx 2.464$ and $\mathcal{K}_{\max} \approx 1.421$, respectively, as determined numerically. Moreover, the upper bounds computed in the preceding section are $\widetilde{\mathcal{K}}_0 = 9.0$ for f_1 and $\widetilde{\mathcal{K}}_0 = 2.33$ for f_2. However, these bounds are shown to be particularly loose. Alternatively, tighter upper bounds are provided by $\widetilde{\mathcal{K}}_1 = 2.590$ for f_1 and $\widetilde{\mathcal{K}}_1 = 1.446$ for f_2.

Fig. 2 illustrates the transmission rate t of the reporting user R at the NE. It demonstrates that when the price of adversarial activities surpasses $\mathcal{K}_{\max}$, the adversary is absent, and t can be set solely based on the value t_0, determined by drifts and failures. However, if the price of adversarial activities falls below $\mathcal{K}_{\max}$, making malicious injection favorable for the attacker, the reporting user is compelled to compensate by increasing activity. Notably, even in scenarios with relatively lower failure rates, the resulting value of t might exceed the one observed when the failure rate is higher, but no adversary is present. This underscores the notion that a strategic adversary can inflict more substantial damage than a higher failure probability alone.

The activity rate q of the malicious player M is depicted in Fig. 3. The figure presents the ratio between q and t to gauge

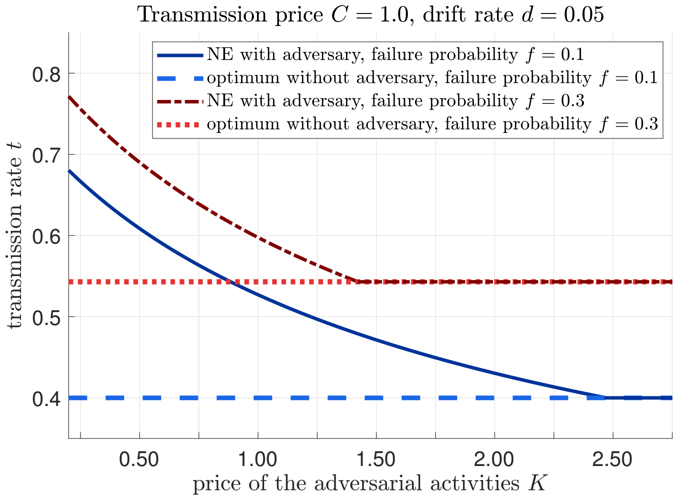

Fig. 2. Transmission rate t by the reporting user vs the price of adversarial activities K, with and without an adversary

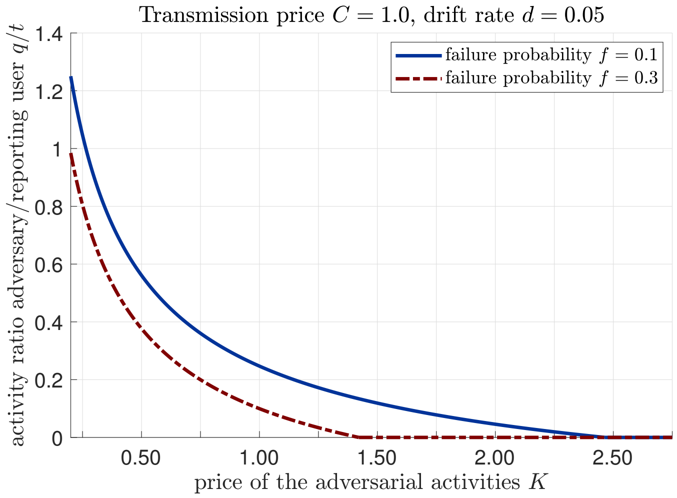

Fig. 3. Ratio of transmission rates of the adversary and the reporting user q/t, as a function of the price of adversarial activities K.

this in proportion to the data exchange rate, indicating that, except when the price K is exceptionally low—wherein the activity of M escalates—typically, the injection rate of false data is lower than t. As elucidated in the analysis, when the price rises beyond $\mathcal{K}_{\max}$, the adversary refrains from attacking, leading to a drop in its activity rate to 0. It is worth noting that the adversary remains active (i.e., $q > 0$) when K and C are comparable. In such instances, albeit restricted to a fraction of t, the attacker finds it convenient to cause damage (and, as will be observed in the next figure, this action proves to be successful and increases AoII). This implies that it would be crucial for the network manager to implement measures that make malicious injections more costly for the attacker than legitimate reporting from the user.

Finally, Fig. 4 shows the average AoII of the system. The trend mirrors that of Fig. 2, starting from a higher value and then saturating to an asymptote corresponding to the case without an adversary when K reaches $\mathcal{K}_{\max}$. However, this highlights the non-trivial property that, due to the adversary's presence, an increased transmission rate by the reporting user still corresponds to a *higher* AoII, rather than a lower one. This once again reaffirms the criticality of the presence of an adversary in the system, ultimately deteriorating the system performance even in the presence of strategic countermeasures. Therefore, the optimal approach to control it is by implementing system protections that make it prohibitively expensive for the attacker to intervene.

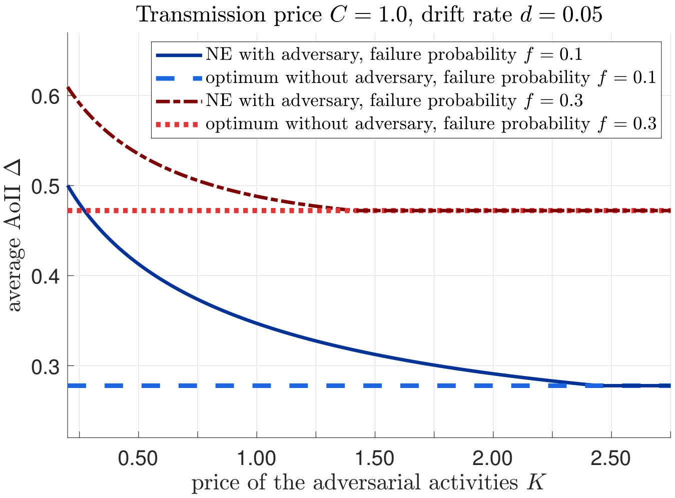

Fig. 4. Average AoII of the system vs the price of adversarial activities K, with and without an adversary.

A very active adversary can make a system with a low failure rate worse than one with a higher failure rate but no adversary. This is evidenced by the intersection of the NE curve for a failure rate of $f = 0.1$ with that for $f = 0.3$ in the absence of an adversary. Additionally, the earlier saturation of the AoII, albeit at a higher value, for a higher failure probability is explained by the observation that when the transmission is already noisy, the adversary finds it less advantageous to further disrupt it [15].

This happens because failures do not impose any cost on the adversary, whereas false data injection comes at a price. Therefore, the adversary is active only when deemed convenient. This highlights the possibility that system management might intentionally degrade system performance slightly to enhance its defense against attacks. While this approach may be justified if the primary goal of system control is stability and predictability rather than maximizing performance, it is essential to acknowledge that it ultimately diminishes overall system performance. One could then argue that an effective strategy to mitigate false data injection might involve convincing adversaries that the system is inherently unreliable, thereby deterring further intervention. Hence, the real takeaway lesson is that attacks are performed based on the malicious adversary's awareness of the system [17]. This highlights the importance of secrecy not only for the exchanged contents, but even for the global system characteristics, and possibly prompts further exploration within game theory, specifically concentrating on the Bayesian beliefs of the players and configurations that enhance system security [11].

V. Conclusions

We investigated a security problem concerning medical self-reporting data, with the objective of minimizing the average AoII [18]. This entails maximizing the accuracy and timeliness of reported information, even in the presence of an adversary injecting false data. The problem was formulated as an adversarial game involving status updates between the legitimate user and the adversary [21].

Our study involved a game-theoretic analysis of the interaction between two players, the user and the adversary. We derived closed-form expressions revolving around the modeling of the system as a two-state Markov chain with variable transition rates. These rates are controlled by the actions of the players, who, constrained by transmission costs, aim to minimize or maximize the average AoII [15].

We computed the NE and demonstrated that the adversary may remain inactive if its cost is prohibitively high. In such cases, optimal system control merely needs sporadic updates. However, if the cost is within an acceptable range, the activity of both players increases, leading to higher expected AoII.

We successfully established connections of various parameters, including the resulting expected AoII, the data injection rates by the legitimate user and the adversary, as well as the valid range for the adversary transmission price where the adversary is active, with the quantitative characteristics of the system. This enables a practical evaluation in closed form.

Future research could explore extended scenarios encompassing other forms of attack, as well as more advanced strategic interactions between the players. This could include incomplete information and Bayesian games [13], [19].

References

[1] J. Andreu-Perez, D. R. Leff, H. M. Ip, and G.-Z. Yang, "From wearable sensors to smart implants—toward pervasive and personalized healthcare," *IEEE Trans. Biomed. Eng.*, vol. 62, no. 12, pp. 2750–2762, Dec. 2015.

[2] L. Squarcina, F. M. Villa, M. Nobile, E. Grisan, and P. Brambilla, "Deep learning for the prediction of treatment response in depression," *J. Affective Disorders*, vol. 281, pp. 618–622, Feb. 2021.

[3] G. Cisotto, A. V. Guglielmi, L. Badia, and A. Zanella, "Classification of grasping tasks based on EEG-EMG coherence," in *Proc. IEEE Healthcom*, 2018.

[4] S. Zafar, M. Nazir, T. Bakhshi, H. A. Khattak, S. Khan, M. Bilal, K.-K. R. Choo, K.-S. Kwak, and A. Sabah, "A systematic review of bio-cyber interface technologies and security issues for Internet of bio-nano things," *IEEE Access*, vol. 9, pp. 93 529–93 566, 2021.

[5] G. Demiris, S. J. Iribarren, K. Sward, S. Lee, and R. Yang, "Patient generated health data use in clinical practice: a systematic review," *Nursing Outlook*, vol. 67, no. 4, pp. 311–330, 2019.

[6] Y. Lin, J. Ye, M. Jin, and Y. Zheng, "Applications of non-invasive sensor devices to personalised health care," *J. Engin.*, vol. 2020, no. 11, pp. 1139–1147, Nov. 2020.

[7] C. Thapa and S. Camtepe, "Precision health data: Requirements, challenges and existing techniques for data security and privacy," *Comput. biol. med.*, vol. 129, p. 104130, Feb. 2021.

[8] 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.

[9] L. N. Hodes and K. G. Thomas, "Smartphone screen time: inaccuracy of self-reports and influence of psychological and contextual factors," *Comput. Human Behav.*, vol. 115, p. 106616, Feb. 2021.

[10] E. Batista, P. Lopez-Aguilar, and A. Solanas, "Smart health in the 6G era: bringing security to future smart health services," *IEEE Commun. Mag.*, 2024, early access.

[11] A. V. Guglielmi and L. Badia, "Analysis of strategic security through game theory for mobile social networks," in *Proc. IEEE CAMAD*, 2017.

[12] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding schemes for securing cyber-physical systems against stealthy data injection attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, Mar. 2017.

[13] 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.

[14] A. MacKenzie and S. Wicker, "Selfish users in ALOHA: a game-theoretic approach," in *Proc. IEEE VTC Fall*, vol. 3, 2001, pp. 1354–1357.

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

[16] M. Chen, D. Cui, H. Haick, and N. Tang, "Artificial intelligence-based medical sensors for healthcare system," *Adv. Sens. Res.*, vol. 3, no. 3, p. 2300009, 2024.

[17] L. Badia, A. Baiocchi, A. Todini, S. Merlin, S. Pupolin, A. Zanella, and M. Zorzi, "On the impact of physical layer awareness on scheduling and resource allocation in broadband multicellular IEEE 802.16 systems," *IEEE Wireless Commun.*, vol. 14, no. 1, pp. 36–43, 2007.

[18] 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.

[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 Wireless Conference*, 2015.

[20] A. Chattopadhyay and U. Mitra, "Security against false data-injection attack in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 7, no. 2, pp. 1015–1027, Jun. 2020.

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

[22] S. Soderi, L. Mucchi, M. Hämäläinen, A. Piva, and J. Iinatti, "Physical layer security based on spread-spectrum watermarking and jamming receiver," *Trans. Emerg. Telecommun. Techn.*, vol. 28, no. 7, p. e3142, Jul. 2017.

[23] M. Kintzlinger and N. Nissim, "Keep an eye on your personal belongings! the security of personal medical devices and their ecosystems," *J. Biomed. Inf.*, vol. 95, p. 103233, Jul. 2019.

[24] 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.

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

[26] L. Badia and A. Munari, "A game theoretic approach to age of information in modern random access systems," in *Proc. IEEE Globecom Wkshps*, 2021.

[27] 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.

[28] 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, Jan. 2024.

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

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

[31] X. Li, J. Xu, H.-N. Dai, Q. Zhao, C. F. Cheang, and Q. Wang, "On modeling eavesdropping attacks in wireless networks," *J. Comput. Sc.*, vol. 11, pp. 196–204, 2015.