On the Anarchy of Multiple False Data Injectors for Age of Incorrect Information in Sensor Networks

Leonardo Badia and Thomas Marchioro
Dept. of Information Engineering (DEI), University of Padova, Italy
email: {leonardo.badia,thomas.marchioro}@unipd.it

***Abstract*—Sensor networks, especially when deployed in a field with little supervision, are vulnerable to a broad range of attacks. In this paper, we study a scenario where multiple competitive adversaries inject false content in the sensed data with the intent of impairing network control. We use game theory to analyze the different behavior of adversaries acting independently or in a coordinated fashion. This analysis ultimately results in the evaluation of efficiency metrics for the utility of uncoordinated attackers, based on the Age of Incorrect Information (AoII), which is compared to the coordinated case. Our numerical results show that generally the lack of coordination is detrimental for the two attackers. With the exception of few edge cases, competition leads the attackers to be more concerned with prevailing over each other than actually compromising the system.**

***Index Terms*—Age of Incorrect Information; Cyber physical systems; Data acquisition; Game theory; Security.**

I. Introduction

The technology for wireless sensors has rapidly progressed in recent years, which can be attributed to several key factors. The advancements in semiconductor technology the development of micro-electromechanical systems (MEMS) enable the miniaturization of sensors while maintaining high performance [1]. Additionally, the enhancement of communication protocols especially in the area of uncoordinated low-power access, such as LoRa [2], [3] or Zigbee [4], which has improved the reliability, range, and energy efficiency of wireless sensor networks [5]. This, in turn, has led to the integration of sensing and control in the Internet of things (IoT) to realize cyber-physical systems [6].

However, the increased capabilities of sensor networks go hand in hand with their susceptibility to tampering or unauthorized access, especially when the physical placement of sensors is in the open and difficult to monitor [7]. The distributed character of data generation, along with wireless data transmission, creates security issues that are less common in centralized wireline systems, posing threats of interception and eavesdropping [8], [9] as well as unauthorized access and false data injection [10]–[12].

In this paper, we focus on the last scenario by considering two adversaries injecting false data in the sensor readings with the purpose of corrupting the system operation. Their objective can be related to age of incorrect information (AoII), a metric proposed by [13] that increases linearly with the time elapsed since the injection of inaccurate information. The approach is general and can be applied to any other metric that relates to the deviation from the system normal operation, amplified over time [14].

We assume that the adversaries are competitive and uncoordinated, meaning that each of them wants the system to use their own false data, and not that of the other [15]. In other words, an attacker's utility increases as long as their injected data remains in the system, but this increase in utility is reset whenever the data is overwritten—either by the legitimate system control or by another attacker. Therefore, this kind of scenario requires to analyze decision-making in distributed and competitive environment, and we find that *game theory* would be the instrument of choice to that end [16], [17].

Game theory enables for the systematic analysis of strategic interactions between multiple agents with different goals. This type of analysis is often used to model cybersecurity problems, as it helps predicting rational strategies for an attacker and optimal defenses [18]. However, in the specific study presented in this paper, there is no strategic involvement from the network's perspective, meaning that the legitimate transmitter is not a player of the game. This makes our scenario not really adversarial (despite involving network security and attackers) [19]–[23], but rather competitive, since the strategic players, i.e., the malicious transmitters, desire to prevail over one another but not to disable the other's activity, if not indirectly.

This game theoretic model allows us to study how the lack of coordination impacts the attackers, unveiling whether their interaction can be seen as mutually reinforcing or merely antagonistic, ultimately making the system defense easier. This is computed through efficiency metrics, which quantify the decrease in utility caused by uncoordinated action, similar to the price of anarchy [24].

Our findings align with the general conclusion that, when the attackers have little margin for action, for example because their activity expenditure is high and/or the network control is tightly monitoring the network, their efficiency is close to 1. In such cases, it is not particularly significant whether they act in a coordinated manner or selfishly [25]. However, the broader the freedom of the attackers, whether due to limited system supervision or low malicious injection cost, the higher the anarchy of uncoordinated attacks. This conclusion leads to interesting implications for scenarios of environmental monitoring, especially in agriculture, forestry, or marine contexts, where the cost of supervising the network may be too high to be preemptively sustainable, yet strategic responses to attacks can be envisioned.

979-8-3503-6836-9/25/$31.00 ©2025 IEEE

The rest of this paper is organized as follows. In Section II, we review related work. Section III presents the system model, and Section IV analyzes it via game theory as a game of complete information. Numerical results are presented in Section V. Section VI concludes the paper.

II. Literature review

False data injection attacks are a problem well studied in the context of power grids [17], [26]. Indeed, these cyber-physical systems are vulnerable to maliciously injected false measurements that, while avoiding triggering threshold alarms [10], can lead to load shedding, as well as over- or under-voltage [7]. Because of this, some researchers have proposed game theoretical approaches, but the common setup is generally that of a single attacker and a single defender playing against each other [6], [27], [28].

For example, [27] investigates a zero-sum game where an attacker can perform the specific false data injection of load redistribution, whereas the network agent tries to defend by implementing a moving target strategy. Generally, even a static game like this results in a plethora of different Nash equilibria depending on the network parameters, as discussed in [28], which classifies them into six different typologies (sometimes even coexisting). The situation is complicated even more by [6] where a multi-stage dynamic game is considered instead.

In this paper, we take instead a more general approach that does not necessarily depend on the electrical aspects, but makes a general reference to the freshness of information in cyber-physical systems. To this end, the metric of choice is AoII, proposed in [13], which allows us to abstract from the specific implementation aspects of both the cyber-physical systems and the attacks performed within it. Indeed, AoII allows a direct connection with the mean absolute error, as discussed in [14], and in general expresses a balance between accuracy and timeliness of the information available in the system, a concept that is becoming increasingly popular for real-time content whose freshness is often quantified through age of information [15], [20], [29].

The main contribution of our analysis, i.e., to consider multiple attackers, is reminiscent of other game theoretic studies where the anarchy between multiple players acting in a distributed fashion is considered and some form of exogenous coordination is introduced to improve upon it [30], [31]. For example, [30] focuses on incentivizing distributed players in a crowdsourcing scenario to provide fresh information, whereas [31] considers the superimposition of reinforcement learning to increase data throughput.

However, for what concerns previous studies related to freshness of information, our studies is more similar to [15] and [29]. The latter reference [29] considers a scenario where two sources can both provide fresh status updates, however, if they both do so at the same time due to their lack of coordination, the redundant data causes the system to be inefficient. Conversely, [15] analyzes the case of two *competing* sources, each wanting to push their own updates. Our problem is similar to these approaches, but ultimately significantly differs from them since the focus is on two malicious agents that instead introduce *false* data, with the purpose of making the system information inaccurate and stale at the same time. In a sense, this combine both references previously mentioned, since the attackers are able to increase AoII (as in [29] they can both decrease AoI), yet they compete to push their own false data over the other, as in [15], even though the data are false here.

Finally, the system model leveraging a Markov chain switching between correct and wrong status information is reminiscent of [11], but with a fundamental difference, i.e., that paper considered two strategic players corresponding to the system manager and a single attacker. Conversely, here we have a passive (i.e., non strategic) legitimate transmitter, whereas the players of the game are both on the side of malicious agents, albeit they are competing and not collaborating with one another.

III. System model

A sensing scenario with just one attacker injecting false data can be considered alternatively reporting between two states of "correct" and "incorrect" status information [32]. The system finds itself in the "correct" operational state when legitimate status reports are performed by the sensor networks. When the attacker injects false data, the state transitions to "incorrect." When this happens, the correct system control is jeopardized, and a penalty known as AoII can be computed to characterize the resulting mixture of obsolescence and inaccuracy in the information [14].

The transition between states are chosen as memoryless, i.e., the time spent in each of the states is exponentially distributed. This gives a system description as a continuous-time Markov chain [11]. A graphical representation of the system is visible in Fig. 1, with the rate of transitions from correct to incorrect or vice versa have been generically denoted as p and q, respectively. The only condition on these terms is that they are positive real numbers for the chain to be recurrent.

The value of AoII at time t can be described as [13]

$$\delta(t) = \big(t - \varphi(t)\big)\chi(t) \tag{1}$$

where $\varphi(t)$ is the time of the last status update reception and $\chi(t)$ is a binary value being equal to 1 if the last update was malicious, 0 otherwise.

This metric can be considered as part of the objective for a malicious attacker. As an application, think of a monitoring system for an IoT outdoor scenario with little to no supervision for cost reasons. In many cases, false data can be conveyed rather easily, given the absence of cryptography or similar protection when deemed to expensive, not to mention that data collection of open environments is relatively easy and can lead to data falsification with minor effort from an attacker [33].

Thus, as the first component in the objective of an attacker, we include the expected value of the AoII $\Delta = \mathbb{E}_t\big[\delta(t)\big]$,

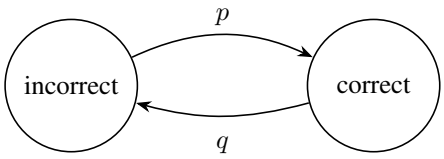

Fig. 1. General Markov representation of the system transitions.

which the attacker wants to maximize, so it is used in the goal function with a plus sign.

From standard derivations of Markov models, Δ can be promptly computed as [29]

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

where we wrote it as $\Delta(p,q)$ to emphasize the dependence on these two parameters. In (2), $1/2p^2$ represents the average cumulative penalty before a system reset. The denominator $1/p + 1/q$ is the average duration of a cycle between two system resets.

Additionally, we introduce a cost term associated with the injection of false data, which can be interpreted as an energy/effort expenditure, or any other limiting factors of the activity, which is taken proportional to the frequency [30]. This means that the utility of the players can be expressed as

$$u(p,q) = \Delta(p,q) - Kq\,, \tag{3}$$

where proportionally factor K can be referred as a unit cost of activity for the attackers.

We note that [11], [20], and [22] consider a similar system, where a strategic adversarial interaction is played by a transmitter choosing p and an adversary choosing q. Conversely, we focus here on a case where p is pre-set, yet multiple adversaries are present, which makes the analysis inherently different.

The reasoning above, as well as the expressions (2) and (3), still hold when we consider multiple attackers in the same scenario. However, it is worth noting that, if attackers are competitive, each of them only considers its own injected data as relevant, where every other transmissions by another attacker resets the AoII value.

In the following, we limit the analysis to 2 attackers, labeled 1 and 2, denoting their activity rates as x and y, respectively, as shown in figure 2. This can be promptly extended to a general case of N adversaries by replacing adversary 2 with the combination of a multitude of attackers, since transmissions are memoryless [25].

Since each malicious attacker considers only its own data to give an acceptable transition towards its intentionally wrong status operation, if we focus on attacker 1, we can keep the same equations as before but with x and y as the strategic decision parameters, setting $q = x$ and replacing p with $p+y$. This means that the utility function includes an expected AoII

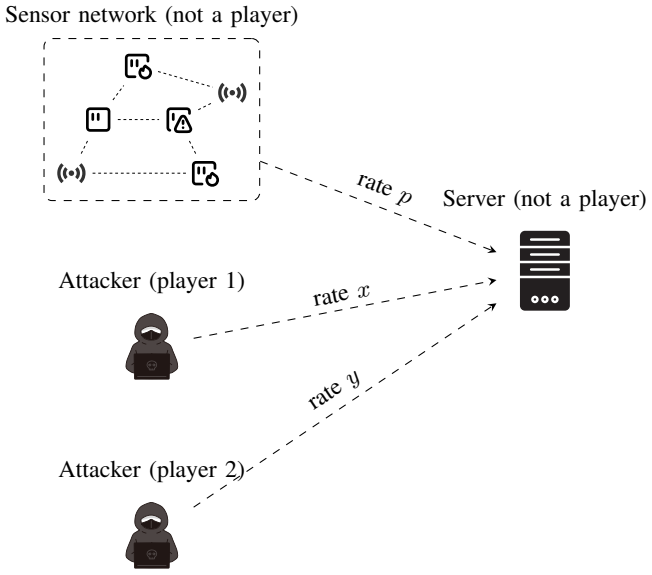

Fig. 2. Threat model analyzed in this paper.

term now written as $\Delta(x,y)$ that reads, after some algebraic rearrangements, as

$$\Delta(x,y) = \frac{x}{2(p+y)(p+x+y)}\,. \tag{4}$$

and the utility of attacker 1 being, as per (3), written as

$$u(x,y) = \Delta(x,y) - Ky. \tag{5}$$

Finally, we note that focusing on either attacker 1 or 2 is purely conventional. Due to symmetry, we can write the same equations for attacker 2 but swapping x and y.

IV. Game theoretic analysis

The aforementioned set of equations induces a game of complete information $\mathcal{G} = (\mathcal{P}, \mathcal{A}, \mathcal{U})$, whose normal form contains the set of players $\mathcal{P}$ as consisting of the two attackers, $\mathcal{A} = \mathbb{R}_+^2$ being the set of available actions, which are $x, y \in [0, +\infty)$, and the utilities in set $\mathcal{U}$ as per (5).

To "solve" the game, i.e., determine valid choices of x and y, we can preliminarily remark that, because of the aforementioned symmetry in the players, after setting any maximization, in the end $x = y$ must hold, since the two players are subject to identical conditions and follow the same utility function.

Thus, we seek for the Nash equilibrium (NE), which is a saddle point of the utilities, i.e., a point $(x,y) \in \mathbb{R}_+^2$ from which neither player wants to unilaterally deviate [29]. This results in setting

$$\frac{\partial u(x,y)}{\partial x} = 0 \quad \Rightarrow \quad \frac{\partial \Delta(x,y)}{\partial x} = K \tag{6}$$

which gives

$$\frac{1}{2(p+x+y)^2} = K\,. \tag{7}$$

The existence of at least one NE, and in this case its uniqueness, are direct consequences of game theoretic principles and can be proven through Glicksberg's theorem [34]. However, in the specific problem at hand, it is immediate to see this constructively, by applying symmetry $x = y$, which shows that the only solution to (7) satisfies

$$x = \frac{1/\sqrt{2K} - p}{2}\,. \tag{8}$$

where the last equation meets the requirement that $x \geq 0$ only if $K \leq (2p^2)^{-1}$.

This relationship implies that the adversaries require the cost being below a certain threshold value, which depends on p, to be active. Clearly, if their activity is too expensive, they prefer to choose $x = y = 0$. The fact that this threshold depends on p is also justified in light of the activity of the legitimate transmissions as contrasting the data injected by the adversaries at that rate [11].

However, as often happens in competitive setups [24], the NE is not the best possible choice for the players if they are allowed to agree on a coordinated strategy, or simply if they are controlled by the same agent. The optimal solution can be found by still leveraging symmetry, which corresponds to setting $x = y$ from the start, and taking the maximum value of the objective transformed into a single-variable function, i.e.,

$$\Delta(x) = \frac{x}{2(p+x)(p+2x)}\,. \tag{9}$$

where the optimum of $u(x) = \Delta(x) - Kx$ is found in

$$\frac{\partial u(x)}{\partial x} = 0 \quad \Rightarrow \quad \frac{\partial \Delta(x)}{\partial x} = K\,, \tag{10}$$

which implies

$$(2x^2 + 3xp + p^2)^2 K + 2x^2 - p^2 = 0\,. \tag{11}$$

Since the LHS of (11) is negative in $x = 0$, has a positive limit for $x \to +\infty$, and is monotonically increasing in x, it admits only one zero in the feasibility interval $x \in [0, +\infty)$. This is the optimal solution that can be found through numerical means. In the following, we are comparing the NE with the optimum and argue about the efficiency (or lack thereof) of the uncoordinated activity of the adversaries.

V. Numerical results

We quantitatively evaluate the impact of the competition between two adversaries by comparing: (a) their utility u_{NE} at the Nash equilibrium with (b) their utility at the optimum u^* and (c) the utility $\bar{u}$ of a single attacker with no competition. Furthermore, we measure the transmission rate x of the attackers and the AoII Δ across all three cases. We plot these metrics and analyze how they vary with different values of the attacker's transmission cost K and the controller's transmission rate p. We recall that utility, AoII, and transmission rate must be the same for the two attackers both at the NE and at the optimum. Therefore, in the plots we refer to a single attacker, who can be either of the two.

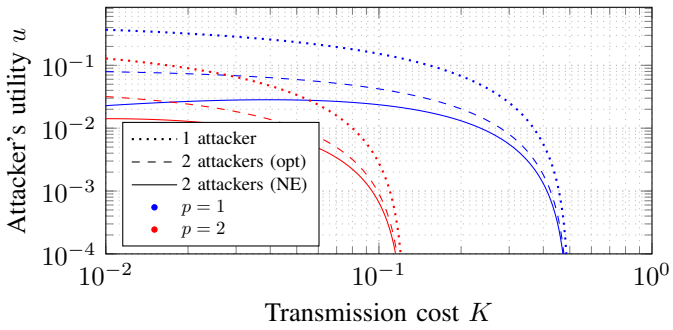

Fig. 3. Attacker's utility versus cost K.

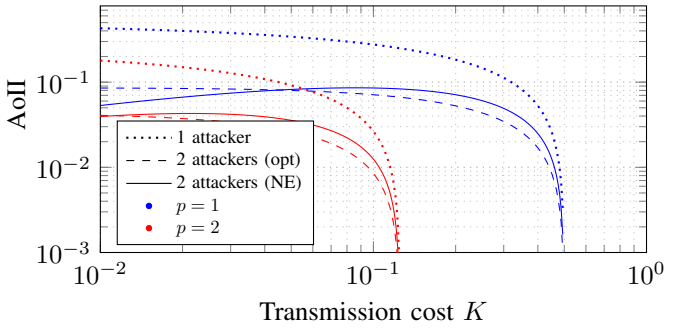

Fig. 4. AoII versus cost K.

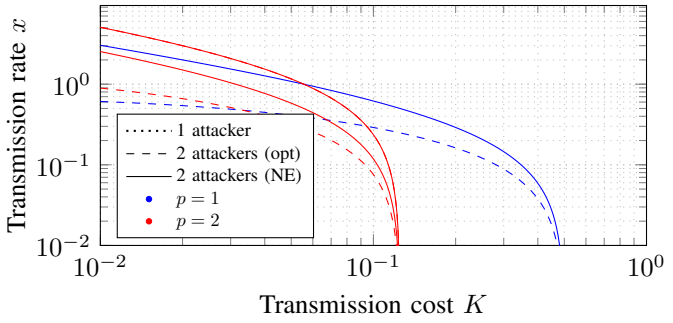

Fig. 5. Attacker's transmission rate versus cost K.

Fig. 3 compares the attacker utilities against the transmission cost K, for p fixed at 1 and 2. For better visualization, both axes are in logarithmic scale. In all the three cases, the utility reaches 0 at $K = (2p^2)^{-1}$, as previously discussed in Section IV. The behavior is monotonically decreasing for the 1-attacker case and the optimal 2-attacker case, but not for the Nash equilibrium. In the case of a single attacker, or if two attackers are coordinated, a lower transmission cost corresponds to a smaller AoII. However, at the NE, AoII does not approach its maximum when $K = 0$. Instead, the maximum AoII is found at an intermediate value between 0 and $(2p^2)^{-1}$. This specific value can be determined algebraically, but it does not yield a meaningful or easily interpretable expression. The intuition behind this is that, when the transmission cost is small, the adversaries face fewer constraints on their transmission capabilities, which leads to heightened competition between the two at the NE. Conversely, when K is higher, the transmissions of the adversaries are limited, forcing them

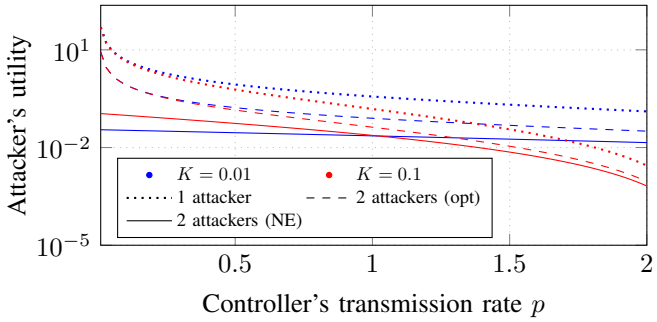

Fig. 6. Attacker's utility versus controller's rate p.

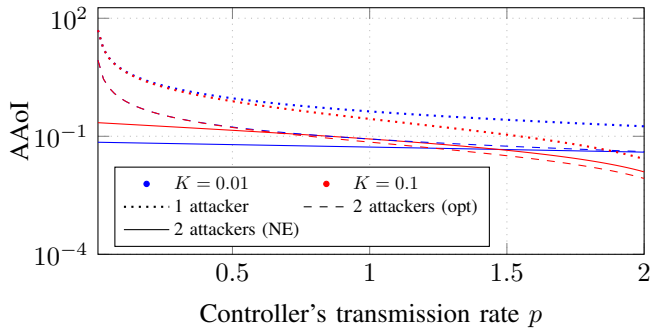

Fig. 7. AAoI versus controller's rate p.

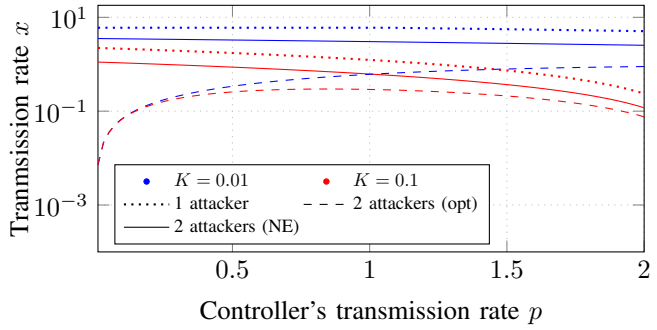

Fig. 8. Attacker's rate x versus controller's rate p.

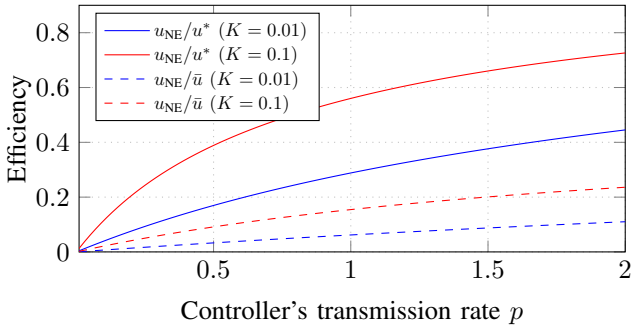

Fig. 9. Efficiency of the NE versus p.

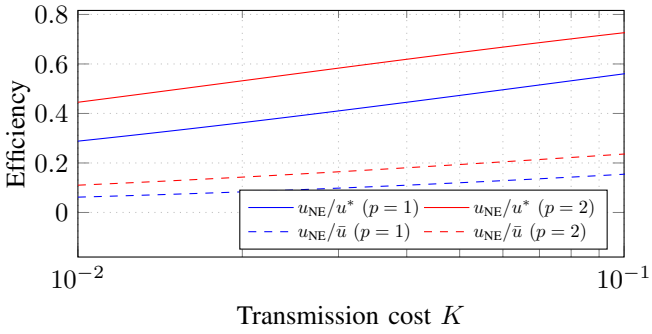

Fig. 10. Efficiency of the NE versus K.

to concede more bandwidth to one another. This results in an increase in AoII, as shown by Fig. 4. The attacker transmission rate at the NE, on the other hand, monotonically decreases with K, as shown in Fig. 5. This behavior can be easily deduced by the expression of x at the NE in (8).

The controller's transmission rate p also decreases the utility of the attackers. Fig. 6 displays the utility as a function of p in the interval $[10^{-2}, 2]$ with K fixed at 0.01 and 0.1. The x-axis follows a linear scale, whereas the y-axis is log-scaled.

When p approaches 0, the utility of a single attacker and two coordinated attackers increases indefinitely, leading to an infinite AoII. This phenomenon is illustrated in Fig. 7, which plots the AoII against p. Interestingly, this is not the case for two competing attackers at the NE, where the AoII cannot reach its maximum value, as determined by K (e.g., for $K = 0$ the peak value is $1/4$). This behavior is again attributed to the selfish nature of the competing agents [24]. In a cooperative scenario, for $p = 0$ the attackers can coordinate their transmission rate x to an arbitrarily small value, as shown in Fig. 8. However, in a competitive scenario, if one adversary chooses a low transmission rate, the other is incentivized to increase its own and enhance its utility. This implies that for $p \to 0$, the price of anarchy (PoA), i.e., the utility ratio u_{NE}/u^*, increases indefinitely.

The main takeaway from this evaluation is that competition between two adversaries with differing goals significantly limits their impact on the system. The PoA can become unbounded, and in turn this represents an efficiency limitation that we evaluated. To do this, we adopted two measures of efficiency, which are plotted in Figs. 9 and 10: the utility ratio between the two attackers at the Nash equilibrium and the optimum (i.e., the reciprocal of the PoA), and the utility ratio between two attackers at the Nash equilibrium and the single-attacker scenario. Both efficiency metrics exhibit similar behavior with respect to K and p. However, the trend is more pronounced in the comparison with the single-adversary case. In other words, the Nash equilibrium of multiple uncoordinated attackers is clearly less efficient than their optimal coordination (solid lines), but is performing particularly poorly if compared with the damage (dashed lines) that a single attacker concentrating all the resources in a single agent can cause to the network.

VI. Conclusions

We analyzed a system where multiple uncoordinated adversaries inject false data into a cyberphysical system with

the purpose of increasing AoII [11]. For this scenario, we computed the resulting NEs and discussed their efficiency.

Compared to a scenario where a single malicious agent is present, or multiple adversaries are fully coordinated, the resulting working point is less threatening for the system, which is in line with many similar game theoretic results. Shortly put, the absence of coordination can lead to inefficiencies, and this is true not only for legitimate nodes, but also for attackers lacking a common control [24].

Disorganized efforts among attackers can be detrimental, making them unable to increase AoII and leading to high energy expenditure [18]. Future work may expand on this point, considering alternative objectives or different game theoretic setups, such as involving a dynamic interaction.

ACKNOWLEDGMENT

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+).

REFERENCES

[1] H. A. Hamid and Z. Celik-Butler, "Self-packaged, flexible, bendable mems sensors and energy harvesters," *IEEE Sensors J.*, vol. 21, no. 11, pp. 12 606–12 617, 2021.

[2] D. Magrin, M. Capuzzo, and A. Zanella, "A thorough study of LoRaWAN performance under different parameter settings," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 116–127, 2019.

[3] A. Tolio, D. Boem, T. Marchioro, and L. Badia, "Spreading factor allocation in LoRa networks through a game theoretic approach," in *Proc. IEEE ICC*, 2020.

[4] H. Fitriawan, M. Susanto, A. S. Arifin, D. Mausa, and A. Trisanto, "ZigBee based wireless sensor networks and performance analysis in various environments," in *Proc. Int. Conf. Qual. Res. (QiR)*, 2017, pp. 272–275.

[5] A. Munari, "Modern random access: An age of information perspective on irregular repetition slotted ALOHA," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3572–3585, 2021.

[6] X. Yang, H. Zhang, H. Cheng, and C. Lu, "Multi-stage offensive and defensive game method for FDIA on power CPS," in *Proc. IEEE Conf. Ener. Internet Ener. Syst. Integr. (EI2)*, 2023, pp. 4164–4169.

[7] J. Ye, A. Giani, A. Elasser, S. K. Mazumder, C. Farnell, H. A. Mantooth, T. Kim, J. Liu, B. Chen, G.-S. Seo *et al.*, "A review of cyber–physical security for photovoltaic systems," *IEEE J. Emerg. Sel. Topics Power Elec.*, vol. 10, no. 4, pp. 4879–4901, 2021.

[8] W. Yang, Z. Zheng, G. Chen, Y. Tang, and X. Wang, "Security analysis of a distributed networked system under eavesdropping attacks," *IEEE Trans. Circuits Syst. II*, vol. 67, no. 7, pp. 1254–1258, 2019.

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

[10] M. Ghaderi, K. Gheitasi, and W. Lucia, "A blended active detection strategy for false data injection attacks in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 168–176, 2021.

[11] 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, pp. 347–352.

[12] S. Kriouile, M. Assaad, D. Gündüz, and T. Soleymani, "Optimal denial-of-service attacks against status updating," in *Proc. IEEE Int. Symp. Inf. Th. (ISIT)*, 2024, pp. 1–6.

[13] A. Maatouk, S. Kriouile, M. Assaad, and A. Ephremides, "The age of incorrect information: A new performance metric for status updates," *IEEE/ACM Trans. Netw.*, vol. 28, no. 5, pp. 2215–2228, 2020.

[14] 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, 2022.

[15] 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.

[16] L. Badia and A. Munari, "A game theoretic approach to age of information in modern random access systems," in *Proc. IEEE Globecom Worksh. (GC Wkshps)*, 2021, pp. 1–6.

[17] J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," *ACM Comput. Surv. (CSUR)*, vol. 52, no. 4, pp. 1–28, 2019.

[18] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach," *IEEE Trans. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[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 Conf.*, 2015.

[20] 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.

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

[22] A. Garnaev, W. Zhang, J. Zhong, and R. D. Yates, "Maintaining information freshness under jamming," in *Proc. IEEE INFOCOM Workshops*, 2019, pp. 90–95.

[23] T. Marchioro, N. Laurenti, and D. Gündüz, "Adversarial networks for secure wireless communications," in *Proc. IEEE ICASSP*, 2020, pp. 8748–8752.

[24] 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, 2021.

[25] L. Badia and L. Crosara, "Correlation of multiple strategic sources decreases their age of information anarchy," *IEEE Trans. Circuits Syst. II*, vol. 71, no. 7, pp. 3403–3407, 2024.

[26] A. Baiocco, C. Foglietta, and S. D. Wolthusen, "Delay and jitter attacks on hierarchical state estimation," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2015, pp. 485–490.

[27] B. Liu, H. Wu, and H. Zhang, "Countering AC load redistribution attacks in smart grids: The role of moving target defense in a defense-attack game," *IEEE Access*, vol. 12, pp. 118 060–118 071, 2024.

[28] M. Borgo, B. Principe, L. Spina, L. Crosara, L. Badia, and E. Gindullina, "Attack strategies among prosumers in smart grids: A game-theoretic approach," in *Proc. Int. Conf. Smart Grid (icSmartGrid)*, 2023, pp. 201–206.

[29] L. Badia, "Age of information from two strategic sources analyzed via game theory," in *Proc. Int. Wkshp Comp. Aided Model. Design Commun. Links Netw. (CAMAD)*, 2021, pp. 1–6.

[30] A. Buratto, A. Mora, A. Bujari, and L. Badia, "Game theoretic analysis of AoI efficiency for participatory and federated data ecosystems," in *Proc. IEEE ICC Workshops*, 2023, pp. 1301–1306.

[31] B. Brik, M. Esseghir, and L. Merghem-Boulahia, "On adjusting data throughput in IoT networks: A deep reinforcement learning-based game approach," *IEEE Internet Things J.*, vol. 11, no. 7, pp. 11 368–11 380, 2024.

[32] M. Rossi, L. Badia, and M. Zorzi, "SR ARQ delay statistics on N-state Markov channels with non-instantaneous feedback," *IEEE Trans. Wireless Commun.*, vol. 5, no. 6, pp. 1526–1536, 2006.

[33] S. Yfantidou, C. Karagianni, S. Efstathiou, A. Vakali, J. Palotti, D. P. Giakatos, T. Marchioro, A. Kazlouski, E. Ferrari, and Š. Girdzijauskas, "Lifesnaps, a 4-month multi-modal dataset capturing unobtrusive snapshots of our lives in the wild," *Scient. Data*, vol. 9, no. 1, p. 663, 2022.

[34] I. L. Glicksberg, "A further generalization of the Kakutani fixed point theorem, with application to Nash equilibrium points," *Proc. Am. Math. Soc.*, vol. 3, no. 1, pp. 170–174, 1952.