A Zero-Sum Game of Age of Information Over a Finite Horizon Between Sensor and Adversary

Aynur Cemre Aka
Dept. of Information Engineering
University of Padova, Italy
aynurcemre.aka@studenti.unipd.it

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

***Abstract*—We analyze the interplay between a sensor reporting real-time data and an adversary that wants to disrupt communication, modeled as a strategic agents in a zero-sum game. The value of the game is set as age of information (AoI) over a finite horizon, over which the sensor sends n reporting milestones as equally-spaced update instants. The adversary can choose to jam some of these milestones, while at the same time the sensor can adopt a defense mechanism (i.e., to increase the transmission power) also on a limited number of milestones, to protect them from the adversary's jamming. This implies that the adversary chooses the milestones to jam trying to circumvent the sensor's defenses, whereas the sensor wants to choose the same transmission instants as the adversary so as to prevent its jamming. These choices are performed in a simultaneous-move game, i.e., without knowledge of the opponent's choice, and the resulting AoI is computed. We discuss the value of the game at the Nash equilibrium, and the impact of the strategic degrees of freedom of the players.**

***Index Terms*—Age of information, zero-sum game, security, game theory.**

I. Introduction

The widespread diffusion of the Internet of Things (IoT) and the increased communication capabilities of next generation devices have led to an interconnected world, where countless devices can communicate and exchange real-time data with extremely low latency, opening up unprecedented opportunities [1]. Smart devices can be found in home appliances or industrial sensors, which enables a wide array of applications where real-time information are collected, processed, and transmitted [2]. The IoT's ability to monitor and control physical systems is expected to bring a revolution to healthcare, transportation, and agriculture systems. However, this vast network of connected devices also presents new challenges, particularly in managing the timeliness and security of the information being exchanged [3].

A critical concept in real-time data exchange is that of age of information (AoI), which quantifies the freshness of data available to the receiver [4]. Unlike traditional metrics such as latency or throughput, AoI focuses on the time elapsed since the last received update was generated, making it relevant for applications that require real-time decision-making [5]. In scenarios like autonomous driving [6], [7], industrial automation [8], [9], or health monitoring [10], maintaining low AoI is essential to ensure that the decisions are based on the most current and accurate data. As IoT networks grow in scale and complexity, optimizing AoI becomes a significant concern, especially in environments with high data traffic and dynamic conditions [11].

Given the critical role of AoI in ensuring the effectiveness of IoT applications, it becomes a valuable target for adversaries seeking to disrupt or manipulate these systems [12]. Attacks on AoI can take various forms, such as delaying the transmission of updates, injecting false data, or blocking the reception of critical information [13]. These attacks can degrade the quality of service, compromise safety, or lead to incorrect decision-making [14]. For instance, in a smart grid, delaying information about power consumption could cause inefficiencies in energy distribution [15], while in a health monitoring system, outdated data could lead to improper treatment decisions [16].

The vulnerability of AoI to attacks is particularly concerning in scenarios where the integrity and timeliness of information are key. As IoT systems continue to expand into critical infrastructures, the need for safeguarding AoI against potential threats becomes particularly acute [17]. This requires a comprehensive understanding of the AoI mechanisms, including the implementations of attack and defense strategies, but also their potential interaction in a game theoretic fashion. By addressing these challenges, we can ensure that IoT networks remain resilient, reliable, and capable of supporting the demands of an increasingly connected world [18].

In this paper, we consider a game-theoretic interaction between two agents: a sensor responsible for sending data updates and an adversary whose objective is to jam these transmissions. This interaction is modeled as a zero-sum static game, where the gain of one player results in an equivalent loss for the other [19]. The sensor and the adversary are both aware of each other's strategies and objectives, and their decisions are made simultaneously.

The available strategy set to both players comprises a discrete set of potential transmission instants, called *milestones* and set at regular intervals. These are the instants where the sensor is expected to transmit an update, which resets

979-8-3503-8359-1/24/$31.00

age of information (AoI). In addition, both the sensor and the adversary can choose these predefined time points to act [20]. The adversary aims to select some milestones to jam the transmission and preventing the AoI from being reset [21]. In turn, the sensor can defend some of these milestones by increasing the power level of the transmission, thereby avoiding the adversarial jamming [22]. Due to power limitations, the sensor cannot increase the transmission power in all milestones, and also does not know what transmissions are jammed by the adversary.

The outcome of each round is determined by the alignment of the chosen milestones. Whenever the sensor selects the same milestones of the adversary, the transmission is successful despite the jamming, and the AoI is reset, benefiting the sensor [23]. However, if a milestone is undefended, the transmission is jammed, leading to an increase in AoI, which is convenient for the adversary. Since this is a zero-sum game, the payoff for one player directly corresponds to the loss for the other, therefore we take AoI as the value of the game, with the adversary playing as a maximizer and the sensor as a minimizer [24]. In addition, theoretical properties hold for this kind of game, enabling the evaluation of the payoff at the Nash equilibrium (NE) as the most likely outcome that can be expected from rational players.

The rest of the paper is organised as follows. In Section II, we describe our game theoretic model. Numerical results showing the performance at the equilibrium are presented in Section III. Finally, Section IV concludes the paper.

II. System Model

We consider a status reporting from a remote sensor to a receiver, tracking some process of interest [6], [13]. Communication from the sensor occurs at regular intervals over a fixed time horizon, which without loss of generality can be normalized [20] and denoted as $[0, 1]$. We assume that the normal functioning of the system corresponds to sending n updates during this time interval, taking place at time instants in set $\mathcal{M} = \{1/(n+1), 2/(n+1), \ldots, n/(n+1)\}$. These predefined instants are referred to as *milestones* [25] and are the subject of the game theoretic interaction between the adversary and the sensor.

The resulting performance is evaluated through AoI, which is reflecting the freshness of the information at the receiver. In the absence of any jamming to these transmissions, the average AoI Δ over the horizon can be found as [5]

$$\Delta = \sum_{j=0}^{n} \frac{1}{2(n+1)^2} = \frac{1}{2(n+1)} \,. \tag{1}$$

However, the attacker attempts to disrupt some of these transmissions, and the sensor may also deploy defenses to mitigate the impact of the attacks. Neither the attacker nor the defender has complete knowledge of each other's actions. Both players choose a finite proper subset of milestones for their actions.

The game theoretic model works as a zero-sum static game of complete information [19] denoted as $\mathcal{G} = \{\mathcal{P}, \mathcal{S}, \mathcal{U}\}$, where $\mathcal{P} = \{\mathrm{A}, \mathrm{D}\}$ is the set of players, comprising the attacker A and the sensor (defender) D. Sets $\mathcal{S}$ and $\mathcal{U}$ contain the strategies and the utilities available to the players, respectively. Since this is a zero-sum game, the latter simply correspond to setting the resulting value of the average AoI Δ as the utility for A (the maximizing player), whereas D tries to minimize instead, and therefore chooses $-\Delta$ as the utility [26].

For what concerns the strategies, the attacker selects a proper subset of milestones, denoted as $\mathcal{A} \subset \mathcal{M}$, where we denote $a = |\mathcal{A}|$ as the number of attacks. It makes sense to consider the cases where a is strictly less than n, to respect Shannon's principle of information security (i.e., considering attackers that are not all-powerful). Similarly, the defender (sensor) D selects a set of time slots $\mathcal{D} \subset \mathcal{M}$, where we denote $d = |\mathcal{D}|$. The defender's objective is to contain the impact of the attacker. From a physical standpoint, this corresponds to injecting some extra security measurement, such as higher power, or anti-jamming through spread spectrum, in some transmissions. But once again, these cannot be applied to all the transmissions. In the following analysis, we will show the impact of variable a and d values.

The model for disruption of communication through jamming and defenses is as follows. We assume that the updates are always successful unless some jamming from the adversary intervenes. This is not restrictive, since including the impact of losses, which can be done following other papers [6], [21] as externalities has no effect on the game theoretic interplay. Whenever an attack is successful, i.e., it is launched in a milestone that is not defended by the sensor, the value of AoI is not reset to 0 and further increases with a linear pattern. If the attack is defended, instead, the instantaneous value of AoI drops to 0. This actually happens on all milestones where the sensor chooses to defend, even if there is no attack.

Thus, the value of AoI averaged over the whole horizon can be computed as

$$\Delta = \sum_{j=0}^{n} \frac{1}{2(n+1)^2} + \sum_{k \in \mathcal{K}} \frac{k^2}{(n+1)^2} \tag{2}$$

where $\mathcal{K}$ is a list of the number of consecutive successful attacks in the time horizon. For example, if no attack is successful, $\mathcal{K} = \emptyset$, whereas if the attacker is able to cause two consecutive successful attacks and then another (separate) attack, then $\mathcal{K} = [2; 1]$. Note that the position of successful attacks is order irrelevant, all that matters is whether the successful attacks are adjacent to one another, since this causes a greater increases to AoI [20].

Given the number of milestones n, the number of attacks a and defenses d, the game is fully defined and the outcome can be computed for any choice of the players in the resulting AoI. This immediately leads to the computation of the Nash equilibria (NEs) of the game [27]. The NEs represent the preferable joint strategy for both the attacker and the defender, where neither party can unilaterally improve their outcome by changing their strategy. In general, these have to be computed analyzing the utilities resulting from all possible attack-defense strategy pairs.

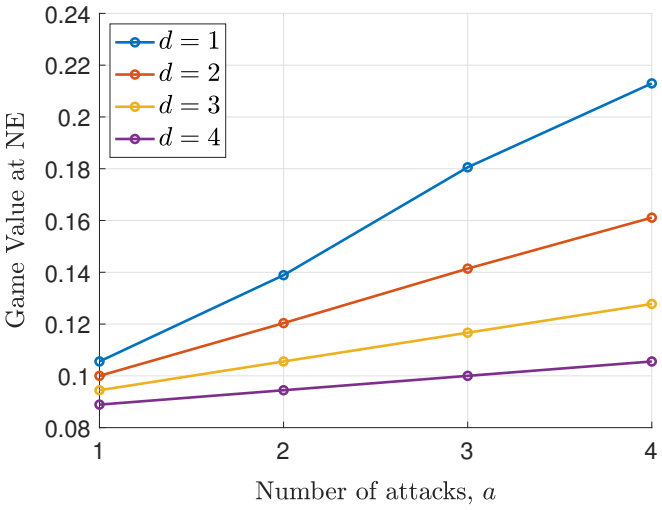

Fig. 1. Impact of the number of attacks and defenses on the game value at the Nash Equilibrium for a time horizon with $n = 5$ milestones.

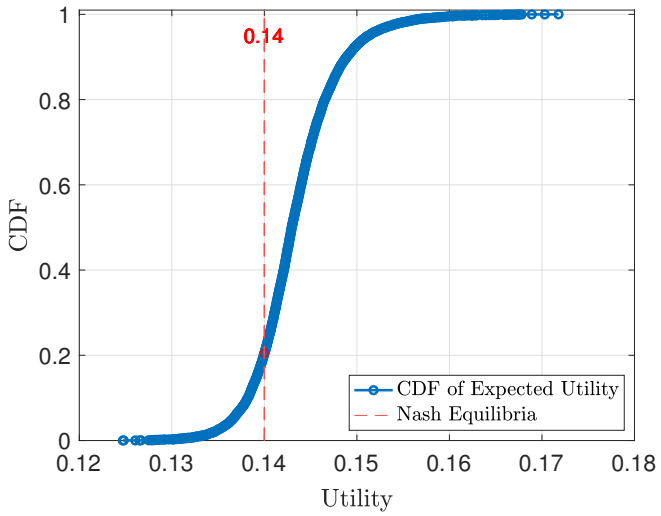

Fig. 2. Horizon with $n = 4$ milestones, $a = 2$, $d = 2$. CDF of the expected value (utility for the attacker) over 10^4 simulations. The red dashed line is the expected payoffs at the Nash Equilibria.

However, this is a zero-sum and therefore relatively easier to solve because all NEs in such games yield the same payoff, known as the game's value – conventionally, this is taken as the utility of the attacker. This simplifies the analysis since the focus shifts from finding multiple potential outcomes to identifying a single optimal value for each player, which can be computed with relatively low complexity as a standard optimization problem [26].

III. Numerical Results and Discussion

We present some results for the value of the game (i.e., the average AoI Δ) at the NE. As argued in the previous section, the specific choice of the NE does not influence the resulting value. However, it is worth noting that the complexity rapidly increases in n, not due to the task of finding the NE itself, but because the strategic choices are combinatorial and therefore increase as $\binom{n}{a}$ or $\binom{n}{d}$ for the attacker or the defender, respectively. Thus, the set of available strategies to each player rapidly increases in n.

Fig. 1 reports the game value at the NE for different numbers of attacks and defenses by the two players, for a scenario where $n = 5$ milestones are available. The x-axis represents the number of attacks a, and the y-axis represents the game value at NE. As observed, increasing the number of attacks increases the game value, especially when the defenses are fewer than the attacks (i.e., $d < a$). Increasing the number of defenses d has the opposite effect. Note that the average AoI Δ in the absence of any jamming would be 0.0833, as per (1).

This plot illustrates the critical balance between attack and defense strategies within the system, where both parties aim to optimize their respective outcomes over the given time horizon. It is interesting to note that increasing the degrees of freedom in the system leads to a generally lower value of the game. Indeed, aside from the case where $a = d = 1$, if a and d are equal to a certain j, the value of the game decreases in j. This seems to imply that the game becomes generally favorable to the defender as the number of the strategic choices increases.

It is actually common that, when an adversarial game introduces more strategic options, it often tends to be more favorable for the defender, particularly in security contexts [12]. When more choices are available, the defender can employ a diverse range of tactics to protect against attacks. Moreover, more strategic options in our scenario lead to the adversary's actions being less effective, since a significant AoI increase is obtained only if consecutive successful attacks are present, and also the denominator in (2) becomes lower in n. In general, a higher number of strategic options forces the adversary to spread the attacks, diluting the impact of any single strategic choice. Therefore, while a more complex strategic landscape can be challenging for both players, the principle of "security through diversity" provides the defender with a general advantage to tailor the strategies for a more robust defense.

This also suggests that a way to counteract a malicious jammer could be to choose sub-optimal milestones to transmit, so as to increase their number. It is immediate to see that, as stated by (1), the choice of n optimal milestones lies in regularly spaced intervals at values in $\mathcal{M}$ [20]. However, enlarging the set of available milestones, even if not all of them correspond to a transmission, may be a further way to increase the degrees of freedom of the system, and therefore to circumvent the malicious jammer.

Additionally, Fig. 2 shows the CDF of the attacker's expected utility, for a scenario of $n = 4$ milestones, with $a = 2$ attacks and $d = 2$ defenses. The x-axis reports the expected utility values of the attacker, while the y-axis gives the corresponding probability to achieve utility less than or

equal to that on the x-axis. The red dashed lines give the expected payoff at the NE, which in this setup gives a value (i.e., an expected AoI) of 0.14.

These results, computed with a simulation of 10^4 instances of the game, give a further insight. Specifically, the CDF values indicate that the NE roughly lies to the left of the median point of the distribution. Still, the oscillations are generally limited, as most of the AoI values are between 0.13 and 0.155, suggesting that the value of the game is a good representation of the expected AoI under many attack and defense games, even those that fluctuate around the NE without being precisely located at it.

Still, one can observe the presence of a longer tail of high AoI values, with a small but non-negligible frequency. This indicates that, in some cases, the AoI can be significantly higher. In practice, this reflects those scenarios where the attacker successfully disrupts the communication over multiple time slots without encountering sufficient defense. Hence, an alternative objective of the game for the defender may be taken as limiting the occurrence of these instances as much as possible. This can be a sensible objective for scenarios where the decision-making operation of the system control may be relatively insensitive to small AoI values, but can lead to problematic failures when the information is significantly obsolete [28].

IV. Conclusions

We studied a zero-sum static game between a sensor transmitting data updates and an adversary attempting to jam these transmissions. These players act as minimizer and maximizer of the transmission's AoI [19], [24]. They both choose from a finite set of predefined milestones, representing potential transmission instants. If a transmission is successfully jammed, AoI increases [21]. Otherwise, for the milestones that are successfully defended, or for those that are not attacked, AoI is reset to zero [25]. The game theoretic decision-making takes place since the two players are unaware of each other choices. For this scenario, we computed the NEs and discussed the resulting performance.

In particular, we highlighted how contrasting the jammer becomes easier for a defender when the set of available options increases. This suggests that the set of available transmission milestones may be increased to include suboptimal instants just to increase their number [22]. Further developments in this area could consider other forms of attack beyond jamming, such as false data injection [13].

At the same time, it is also possible to explore dynamic and adaptive strategies for both the sensor and the adversary, potentially incorporating elements of learning over repeated games. For example, the sensor might adjust its milestone selection strategy based on observed patterns in the adversary's behavior, leading to more resilient update schedules [29]. Similarly, the adversary could employ more sophisticated jamming techniques, such as stochastic or probabilistic approaches, to increase the unpredictability and effectiveness of its attacks.

Another avenue for research involves extending this study to more players, i.e., multiple adversaries or sensors [11]. This would introduce additional layers of complexity, such as cooperative or competitive strategies among agents, as well as uncertainty in the information that gives a Bayesian character to the game [27].

References

[1] E. Uysal, O. Kaya, A. Ephremides, J. Gross, M. Codreanu, P. Popovski, M. Assaad, G. Liva, A. Munari, B. Soret *et al.*, "Semantic communications in networked systems: A data significance perspective," *IEEE Netw.*, vol. 36, no. 4, pp. 233–240, 2022.

[2] N. Michelusi, K. Stamatiou, L. Badia, and M. Zorzi, "Operation policies for energy harvesting devices with imperfect state-of-charge knowledge," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2012, pp. 5782–5787.

[3] Q. Zhang, Z. Xu, X. Lan, J. Chen, J. He, W. Ma, and Q. Chen, "Optimal age of information and throughput scheduling in heterogeneous traffic wireless physical layer security communications," *IEEE Internet Things J.*, vol. 11, no. 13, pp. 23 644–23 660, 2024.

[4] 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, 2021.

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

[6] A. Baiocchi, I. Turcanu, N. Lyamin, K. Sjöberg, and A. Vinel, "Age of information in IEEE 802.11p," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag.*, 2021, pp. 1024–1031.

[7] M. Vicini, S. Albut, E. Gindullina, and L. Badia, "Decision making via game theory for autonomous vehicles in the presence of a moving obstacle," in *Proc. IEEE Int. Conf. Commun. Netw. Satellite (COMNETSAT)*, 2022, pp. 393–398.

[8] C.-F. Liu and M. Bennis, "Taming the tail of maximal information age in wireless industrial networks," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2442–2446, 2019.

[9] A. Berardo and N. M. Pugno, "A model for hierarchical anisotropic friction, adhesion and wear," *Tribology International*, vol. 152, p. 106549, 2020.

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

[11] W. Pan, Z. Deng, X. Wang, P. Zhou, and W. Wu, "Optimizing the age of information for multi-source information update in Internet of things," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 2, pp. 904–917, 2022.

[12] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surveys (CSUR)*, vol. 45, no. 3, pp. 1–39, 2013.

[13] V. Bonagura, S. Panzieri, F. Pascucci, and L. Badia, "Strategic interaction over age of incorrect information for false data injection in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 12, no. 1, 2025.

[14] L. Badia, M. Miozzo, M. Rossi, and M. Zorzi, "Routing schemes in heterogeneous wireless networks based on access advertisement and backward utilities for QoS support," *IEEE Commun. Mag.*, vol. 45, no. 2, pp. 67–73, 2007.

[15] 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. IEEE icSmartGrid*, 2023, pp. 01–06.

[16] L. Badia, V. Bonagura, F. Pascucci, V. Vadori, and E. Grisan, "Medical self-reporting with adversarial data injection modeled via game theory," in *Proc. IEEE Int. Conf. Commun. Signal Proc. Appl. (ICCSPA)*, 2012, pp. 5782–5787.

[17] I. Kahraman, A. Köse, M. Koca, and E. Anarım, "Age of information in Internet of things: A survey," *IEEE Internet Things J.*, vol. 11, no. 6, pp. 9896–9914, 2024.

[18] R. Hazra, M. Banerjee, and L. Badia, "Machine learning for breast cancer classification with ANN and decision tree," in *Proc. IEEE Inf. Tech. Elec. Mobile Commun. Conf. (IEMCON)*, 2020, pp. 0522–0527.

[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.* VDE, 2015, pp. 1–6.

[20] L. Badia, A. Zancanaro, G. Cisotto, and A. Munari, "Status update scheduling in remote sensing under variable activation and propagation delays," *Ad Hoc Networks*, vol. 163, p. 103583, 2024.

[21] S. Banerjee, S. Ulukus, and A. Ephremides, "Age of information of a power constrained scheduler in the presence of a power constrained adversary," in *Proc. IEEE Infocom Whshps*, 2023, pp. 1–6.

[22] G. D. Nguyen, S. Kompella, C. Kam, J. E. Wieselthier, and A. Ephremides, "Information freshness over an interference channel: A game theoretic view," in *Proc. IEEE Infocom*, 2018, pp. 908–916.

[23] R. Verma, S. J. Darak, V. Tikkiwal, H. Joshi, and R. Kumar, "Countermeasures against jamming attack in sensor networks with timing and power constraints," in *Proc. IEEE COMSNETS*, 2019, pp. 485–488.

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

[25] E. Đokanović, A. Munari, and L. Badia, "Harsanyi's equilibrium selection for distributed sources minimizing age of information," in *Proc. IEEE Medit. Commun. Comp. Netw. Conf. (MedComNet)*, 2024, pp. 1–4.

[26] D. Koller and N. Megiddo, "The complexity of two-person zero-sum games in extensive form," *Games Econ. behav.*, vol. 4, no. 4, pp. 528–552, 1992.

[27] G. Quer, F. Librino, L. Canzian, L. Badia, and M. Zorzi, "Inter-network cooperation exploiting game theory and Bayesian networks," *IEEE Trans. Commun.*, vol. 61, no. 10, pp. 4310–4321, 2013.

[28] M. Emara, H. Elsawy, and G. Bauch, "A spatiotemporal model for peak AoI in uplink IoT networks: Time versus event-triggered traffic," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 6762–6777, 2020.

[29] M. Li, C. Chen, C. Hua, and X. Guan, "Learning-based autonomous scheduling for AoI-aware industrial wireless networks," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 9175–9188, 2020.