Eavesdropping Fresh Information: A Game Theoretical Approach in Dual Sender Networks

Alessandro Buratto, Aynur Cemre Aka, Shahla Sadeghzadeh, and Leonardo Badia
Dept. of Information Engineering, University of Padova, Italy
{alessandro.buratto.1@phd., aynurcemre.aka@studenti., shahla.sadeghzadehdarandash@studenti., leonardo.badia@}unipd.it

***Abstract*—We analyze Age of Information (AoI) within dual-sender networks, focusing on the strategic interplay between transmission rates and their optimization with eavesdropping concerns. Using a game-theoretical framework, we propose an objective function for each sender that jointly minimizes the age of information at the legitimate receiver and maximizes the same metric at the eavesdropper while avoiding congestion on the shared channel between senders. We derive numerical solutions for the choice of the offered traffic by the senders at the Nash Equilibrium (NE) considering a FCFS M/M/1 queuing model as the receiver's buffer. We demonstrate that the presence of multiple senders that need to contend limited resources for transmission leads to lower utilities for each of them, as they end up limiting their transmissions even when they are aware of the fact that the eavesdropper is not overhearing their information. These findings can be used to analyze the strategic interaction aimed at securing communications, from both the perspective of attackers and defenders.**

***Index Terms*—Age of Information; Dual-sender network; Communication system security; Game theory.**

I. Introduction

Age of information (AoI) is a popular metric to characterize the freshness of information in real-time applications, where the timeliness of data updates directly impacts decision-making and system performance. Packet congestion in networks can make it hard to deliver updates quickly. This problem has made people more interested in performance metrics such as AoI, which is emerging as a key end-to-end metric, providing a detailed description of the latency in systems and applications dedicated to status updates [1], [2]. When status updates are exchanged between a transmitter and receiver, the AoI value at the receiver side is calculated as

$$\delta(t) = t - \sigma(t)\,, \tag{1}$$

with $\sigma(t)$ being the time of the last update's creation. Assuming no delay in transmission and that each update contains new information, AoI grows linearly over time until a new update resets it to its initial value. Due to resource constraints, these updates can only occur occasionally [3], [4].

As the freshness of information is crucial in sensor networks and Internet of Things (IoT) scenarios, queueing systems serve as an effective model. With their mathematical foundation, they offer a flexible approach for studying information flows, which is largely unaffected by specific technologies or applications. This versatility makes them ideal for analyzing a wide range of areas, including healthcare, autonomous transport, and smart grids [5]. For simplicity, we focus on the M/M/1 queue with a first-come-first-served (FCFS) policy, but other systems could also be considered in future studies.

The scenario described in [6] involves a communication link with a sender named Alice, a legitimate receiver called Bob, and an eavesdropper, Eve. Alice transmits updates aimed at Bob, who processes them based on a FCFS order within a typical M/M/1 queue framework. Eve, intercepts these updates with an uniform and i.i.d. probability distribution over them. Even though Eve intercepts the updates, Bob continues to receive them; Eve processes these updates similarly to the legitimate receiver. Like Bob, Eve also keeps track of AoI, but her AoI value is calculated only based on the information she captures. Alice, understanding that Eve intercepts her transmissions, can manipulate the rate at which she sends out updates. By decreasing this rate, she can hinder Eve from obtaining timely information, though this simultaneously worsens Bob's AoI. Alice's challenge lies in navigating the trade-off between minimizing Bob's AoI and maximizing Eve's, aiming to strike an optimal balance between these divergent goals [7].

In this study, our objective is to explore the outcomes of the interaction between multiple sources or senders, specifically focusing on the optimal amount of data transmission without causing congestion on the network [8]. For this scenario, we examine the roles of two participants, named Alice and Amanda. In this context, the aim of timely updates is distinct from both maximizing system utilization and minimizing the delay in receiving status updates. Sending updates too quickly can overload the system, causing updates to queue up and delay. Conversely, reducing update frequency might minimize delay, but increases the risk that the receiver will obtain outdated information because of fewer updates. Thus, a balance is needed between update frequency and the freshness of information received [9].

In our analysis, we express the players' utility functions and determine the resulting Nash Equilibrium (NE). We show that there exists a single NE in mixed strategies. Moreover, this solution implies that senders reduce their offered traffic to avoid network congestion. These results can be used to analyze the strategic interaction aimed at securing communication, from both the attackers and the defender perspectives. Also, they can be exploited to understand the inefficiency of distributed actions by agents acting without any preliminary cooperation, but that are aware of the presence of other users. This reduction in performance can be expressed through the introduction of a novel metric named Multi-Sender Inefficiency (MSI), which captures the variation of the utility received by a sender that has the whole channel to itself and multiple senders that compete for the same resources. Finally, we can also envision extensions to broader strategic scenarios that possibly combine multiple objectives that go beyond the AoI. This would be the case where eavesdropping is not just undesirable, since it causes the AoI of the legitimate transmission to grow, but also exposes some security concerns of the system, in which case the strategic choice would also be related to prevent eavesdropping as much as possible [10], [11].

The remainder of this paper is organized as follows. Section II reviews previous research on queuing systems, the age of information and security. Section III details the system model and the game's formulation. Numerical results are presented in Section IV, and the paper is concluded in Section V.

II. Related Works

This paper expands on previous research by analyzing AoI in queueing systems, with a focus on traditional memoryless models [12], [13]. In an FCFS M/M/1 queue, AoI is influenced by the arrival rate (λ) and the service rate (μ), with stability ensured when the load factor $\rho = \lambda/\mu < 1$. This relationship underscores the AoI's dependency on maintaining an optimal balance between λ and μ for effective throughput [14].

Multiple works consider the optimization of AoI in different types of queues. Yates et al. [1] obtain closed-form expressions for the average AoI in multiple service scenarios of M/M/1 queues and derive optimal bounds for system requirements in which it is best to adopt the FCFS service or two particular variants of last-come first-served policies. Moltafet et al. [15] derive expressions for the AoI in the presence of multiple senders in the same queue. Nevertheless, they make critical assumptions on the non-independence of the incoming packets that are not suitable to our distributed scenario. Other authors [16], [17] study AoI in time-discrete queueing systems which differ from our scenario because we consider our queues to act in continuous time. In recent years, a branch of research has been focusing on other aspects of AoI in queueing systems, specifically on the peak AoI which is the maximum value achieved by the metric before it is reset to its initial value [18], [19]. In this work, we do not consider this metric as we are more interested in the steady-state average behavior.

Only a handful of more recent works consider the effect of eavesdropping on AoI [7], [20]. Following this branch of research, we include an eavesdropper, who aims to intercept the communications between sources and a legitimate receiver. In this scenario, the challenge for the source becomes to increase its transmission rate to reduce the receiver's AoI, but also to carefully plan the updates to increase as much as possible the one of the eavesdropper [7]. We expand on this idea by including a second sender that shares the same queue at the receiver as the original one. We study the interaction between the two by means of a game-theoretic approach. We formalize a duopoly in which sources aim at maximizing their own utilities by sharing a constrained amount of resources [21]. The literature offers multiple studies of applications of game theory to collaborative scenarios that range from participatory sensing [2], [22], [23] to link layer protocol analysis [24], [25]. Our contribution is also novel in this aspect, as the uncoordinated interaction between agents aware of the AoI has never been extensively studied in the presence of an eavesdropper.

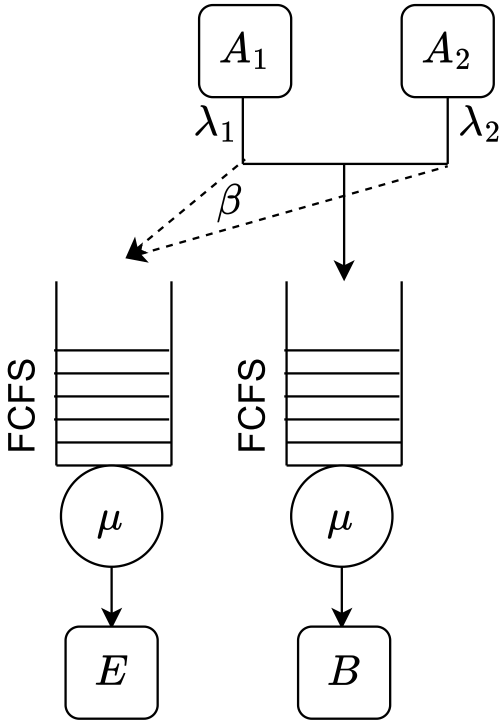

Fig. 1. Queuing system with dual transmitter (A_1) and (A_2), a legitimate receiver (B), and an eavesdropper (E).

In fact, most of the research on eavesdropping at the physical layer focuses on obtaining game-theoretic solutions in adversarial settings [26], [27] where the players need to actively counteract the presence of the eavesdropper that is considered an active entity in the game. Our approach also differs in the sense that the only *intelligent* actors are the sources who can control the information they send through the communication channel independently.

III. System Model

We consider a scenario in which two sources, Alice (A_1) and Amanda (A_2) send a data stream to a receiver Bob, who will be addressed as B, through a FCFS M/M/1 queueing system. A_1 and A_2 generate packets according to a Poisson process with rate λ_1 and λ_2 respectively. Similarly, the service time of B's queue is exponentially distributed with rate μ. Because the packets from the sources are i.i.d. the resulting queue is M/M/1 with arrival rate $\lambda = \lambda_1 + \lambda_2$ and total offered load

$$\rho = \frac{\lambda}{\mu} = \frac{\lambda_1}{\mu} + \frac{\lambda_2}{\mu} = \rho_1 + \rho_2 \, . \tag{2}$$

Moreover, an eavesdropper Eve (E) is present in the system, and tries to intercept data from either sender to the receiver with the ultimate goal of eavesdropping updates keeping its AoI as low as possible. We consider that each packet sent by A_1 and A_2 can be eavesdropped by E with a uniform probability of $\beta \in [0, 1]$. We thus consider that, on average, Eve also receives a fraction β of the in-flight packets towards Bob. Similarly to Bob, Eve also enqueues her packets in a FCFS M/M/1 queue with arrival rate that follows a Poisson process according to the thinning property [5] $\beta\lambda$ and service rate μ which we consider to be equal to B's. Thus, there is also a channel between the two sources and the eavesdropper with similar properties of the one between senders and receiver with load factor

$$\rho_E = \frac{\beta\lambda_1}{\mu} + \frac{\beta\lambda_2}{\mu} = \frac{\beta\lambda}{\mu} = \beta\rho \,. \tag{3}$$

A graphical representation of this scenario is shown in Fig. 1 where the arrival rates for two FCFS M/M/1 queues are explicitly shown.

In our scenario, only A_1 and A_2 are *intelligent* agents, as they have full control over their send rate λ_i. Moreover, they are aware of the presence of the eavesdropper and they know exactly what the value of probability β is, that is the probability that one of the packets they send over the channel is also delivered to E. We formalize their objective to minimize the AoI at Bob's side while maximizing the one at Eve's end. We can compute the AoI at the receiver side for A_1 in a FCFS M/M/1 system with multiple senders as [1]

$$\Delta_{1,B} = \frac{1}{\mu}\left(\frac{\rho_1^2(1-\rho\rho_2)}{(1-\rho(1-\rho_2)^3} + \frac{1}{1-\rho_2} + \frac{1}{\rho_1}\right) . \tag{4}$$

Similarly, the AoI at the eavesdropper side follows a similar expression

$$\Delta_{1,E} = \frac{1}{\mu}\left(\frac{\beta^2\rho_1^2(1-\beta^2\rho\rho_2)}{(1-\beta\rho(1-\beta\rho_2)^3} + \frac{1}{1-\beta\rho_2} + \frac{1}{\beta\rho_1}\right) . \tag{5}$$

The expressions for A_2 are easily computed swapping the roles of ρ_1 and ρ_2 in (4) and (5) due to the symmetries between the sources. Note that $\beta = 1$ implies that all traffic directed to B is intercepted by E, thus $\Delta_{1,E} = \Delta_{1,B}$.

We then need to combine the two metrics into a single utility expression for each of the sources. We decide to adopt a similar approach to [6] and apply Bergson's approach [28] to obtain the trade-off on the Pareto front for both sources

$$u_i(\rho_1, \rho_2) = \frac{\Delta_{i,E}}{(\Delta_{i,B})^{a+1}} \,, \qquad i = 1, 2 \quad , \tag{6}$$

where $a \in [0, \infty)$ is a parameter that controls the trade-off between the maximization of $\Delta_{i,E}$ and the minimization of $\Delta_{i,B}$. This is meant to avoid the undesirable outcome that one sender decides not to transmit thus maximizing the AoI at the eavesdropper, but also avoiding the reception of information to the legitimate receiver [6]. For this reason, we adopt the notation $a + 1$ as we cannot remove the contribution of $\Delta_{i,B}$ to the objective. This expression can be promptly converted to a linear combination of the source's objectives by taking the logarithms, but the product form best conveys the balancing between the two.

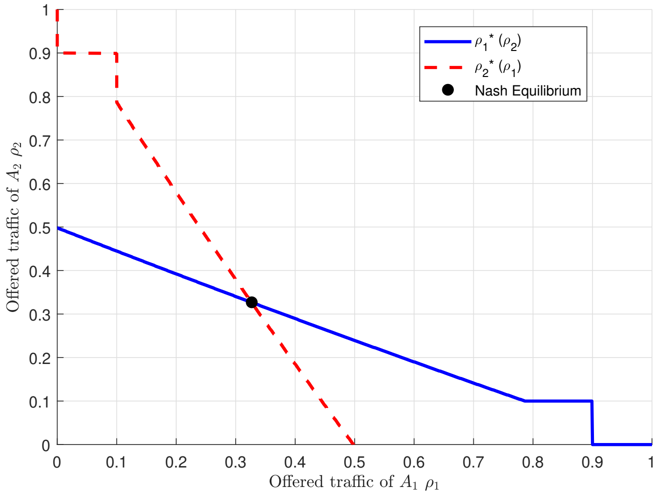

Fig. 2. Nash Equilibrium solution described as the intersection of the Pareto fronts of ρ_1 and ρ_2. Results obtained with $\beta = 0.2$ and $a = 5$.

In this scenario, the sources A_1 and A_2 need to compete for the offered traffic as a FCFS scheme is the best performing for $\rho \leq 1$, as discussed in [1]. For this reason, their interaction can be modeled as a duopoly in which two firms need to compete on the amount of output they will produce. The outcome of this interaction is a Nash Equilibrium where the choice of the traffic ρ_1 and ρ_2 is a best response to the unchanged decision of the other sender [21], [29].

This is translates mathematically to solving a system of partial differential equations

$$\begin{cases} \dfrac{\partial u_1(\rho_1, \rho_2)}{\partial \rho_1} = 0 \\ \dfrac{\partial u_2(\rho_1, \rho_2)}{\partial \rho_2} = 0 \end{cases} , \tag{7}$$

which can be solved numerically by fixing in an iterative fashion alternatively ρ_1 and ρ_2 and optimizing for the other variable. When convergence is reached, we obtain a single NE in mixed strategies. A graphical representation of this algorithm is presented in Fig. 2 where it is clearly visible that there is only one intersection between the two Pareto fronts of the offered rates, and this indicates the presence of a single NE.

We further define the Multi-Sender Inefficiency (MSI) which is a novel metric we introduce to measure the inefficiency of a NE solution when multiple senders are subject to the presence of an eavesdropper. Let us define $f(\rho)$ the utility gained by a single sender as obtained in [6]

$$f(\rho) = \frac{(\beta^3\rho^3 - \beta^2\rho^2 + 1)\rho^a(\rho-1)^{a+1}}{\beta(\beta\rho-1)(\rho^3-\rho^2+1)^{a+1}} \,. \tag{8}$$

With this definition the MSI is computed as

$$MSI = \frac{f(\rho)}{u_1(\rho_1^\star, \rho_2^\star)} \,. \tag{9}$$

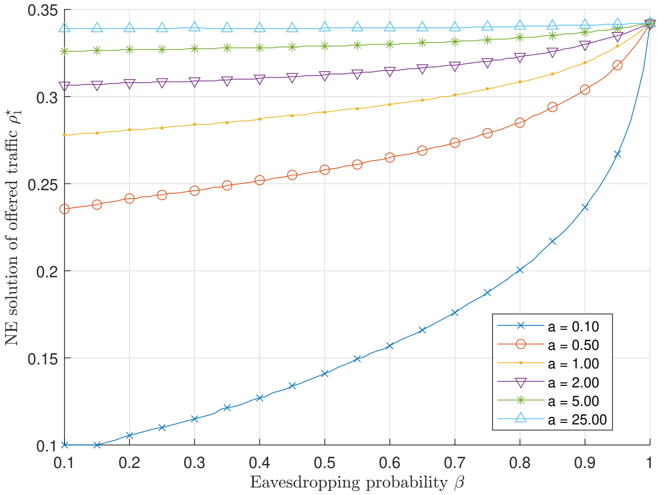

Fig. 3. Optimal offered traffic $\rho_1^\star$, as a function of eavesdropping probability β, for different values of trade-off parameter a.

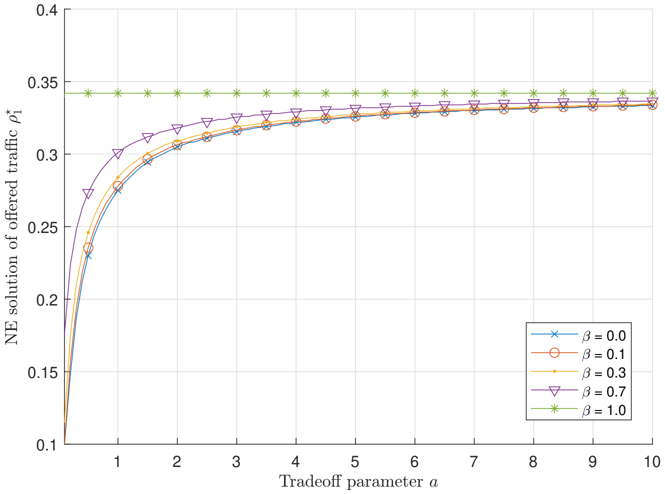

Fig. 4. Optimal offered traffic $\rho_1^\star$, as a function of trade-off parameter a, for different values of eavesdropping probability β.

It is worth noting that $MSI < 1$ indicates that multiple senders that act simultaneously can obtain better utilities when compared to a single sender meaning they can effectively reduce more the information gained by the eavesdropper. $MSI > 1$ indicates that a single sender obtains better utilities than multiple senders in the same scenario. Finally, $MSI = 1$ indicates that there is no difference in the utility available to senders if they are alone in the network or if they need to compete to send their data.

IV. Numerical Results

In this section we provide quantitative evaluations to previously defined equations. Without loss of generalization, in all the following results we will consider a normalized service rate $\mu = 1$, thus implying that $\rho = \lambda = \lambda_1 + \lambda_2$, otherwise all the results can be rescaled by a factor μ. In all the following plots we will focus only on the results for A_1 as the solutions are the same for A_2 because of the previously shown symmetries in the equations in Sec. III.

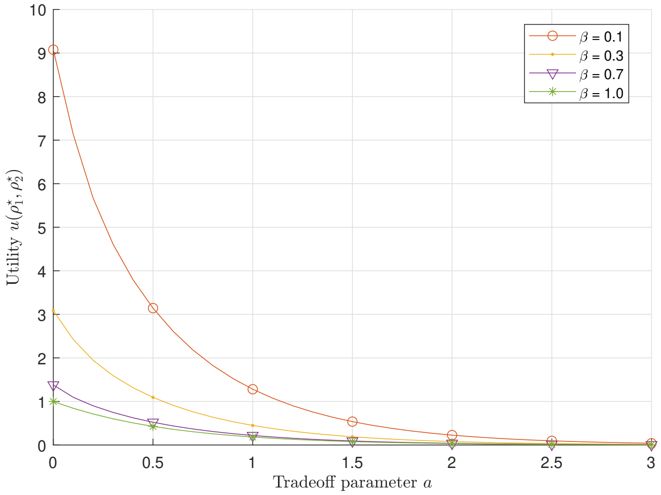

Fig. 5. Utility function evaluated at the optimal offered traffic $\rho_1^\star$, and optimal offered traffic $\rho_2^\star$ as function of the trade-off parameter a, for different eavesdropping probabilities β.

Fig. 3 shows the NE solution $\rho_1^\star$ as a function of the eavesdropping probability β for different values of the trade-off parameter a. For $\beta \to 0$ and $a \to 0$ also the offered traffic $\rho_1 \to 0$ thus implying that the sources prefer to transmit as little as possible when they know that the eavesdropper will likely not overhear any packet and the AoI minimization at Bob's side is not important with respect to the maximization of the AoI at Eve's side. It is also notable that increasing values of the trade-off parameter a leads to the linearization of the growth of the offered traffic as a function of the eavesdropping probability. At the limit, as $a \to \infty$ the NE solution for $\rho_1^\star \to 0.342$ for all values of β, indicating that this is the optimal value for which the AoI on Bob's side is minimized when neglecting the presence of an eavesdropper, in accordance with the solution for two independent servers at the NE reported in [1].

Fig. 4 displays the NE solution for $\rho_1^\star$ as a function of the trade-off parameter a for different values of β. As noted in Sec. III, $\beta = 1$ forces $\Delta_{1,E} = \Delta_{1,B}$, which means that the choice of ρ_1 at the NE is independent of the trade-off parameter a. For all other values of β, $a \to \infty$ states that the NE solution for $\rho_1^\star \to 0.342$ as discussed in Fig. 3. Not surprisingly, lower values for β also lead to lower values of load factors ρ_i, as senders know that they can maximize their utility with fewer transmissions.

Fig. 5 shows the utility obtained by each sender with the NE solutions for $\rho_1^\star$ and $\rho_2^\star$. Low values of β lead to higher utilities as the AoI of the eavesdropper is maximized more easily. This effect quickly vanishes for increasing values of the trade-off parameter a, and eventually the utility will approach 0 for every value of β.

Figs. 6-7 report the Multi-Sender Inefficiency as defined in (9). It is evident that for low values of the tradeoff parameter

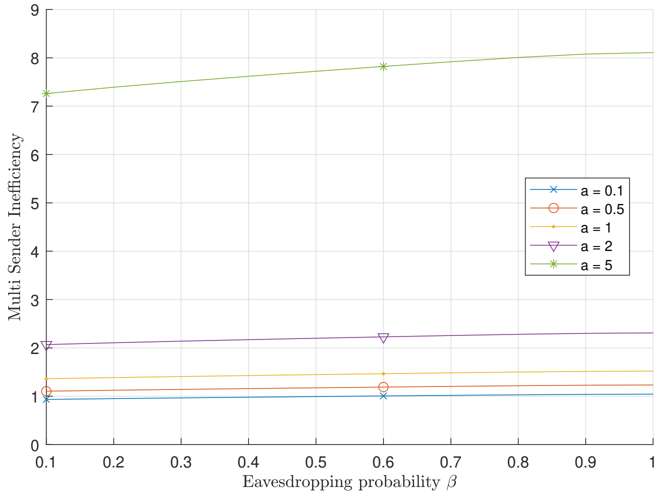

Fig. 6. MSI as a function of the eavesdropping probability β for different values of the trade-off parameter a.

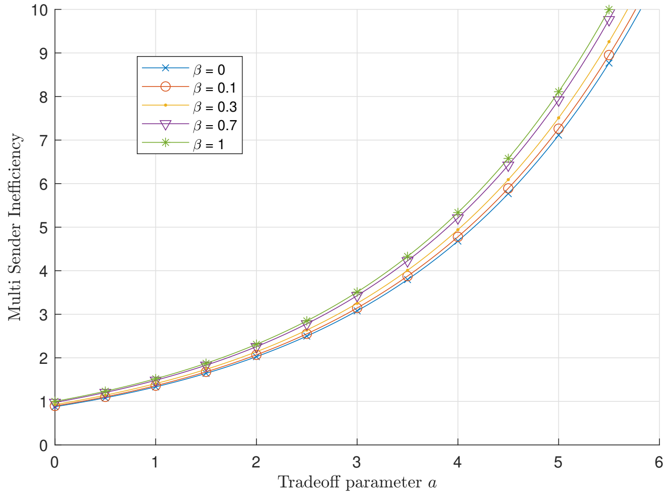

Fig. 7. MSI as a function of the eavesdropping probability β for different values of the trade-off parameter a.

a the utility achieved by a single sender is slightly lower than that of two concurrent senders. This advantage fades quickly for increasing values of a, hinting that the presence of multiple senders in the same network leads to each receiving less benefits from the distributed interaction. It should be noted that, while the choice of the probability of eavesdropping β does not change the MSI in an appreciable manner, this is not true for the trade-off parameter a as slight variations may considerably increase the value of the metric, as clearly shown in Fig. 6. This is possibly a consequence of the fact that the utility reported in Fig. 5 has a rapid decrease for low values of a and approaches zero faster than in the single-sender case. Moreover, a single sender tends to choose offered traffic values ρ higher than in scenarios where multiple agents need to share the same amount of resources.

V. Conclusions

In this paper, we analyzed AoI within dual-sender networks, using a game-theoretical framework to discuss the interaction between timely data transmissions and the need to protect against eavesdropping. We modeled an objective function for each sender that jointly minimizes the AoI at the legitimate receiver and maximizes the same metric at the eavesdropper while avoiding congestion on the shared channel between senders. We obtained numerical solutions for the choice of the offered traffic by the senders at the NE considering a FCFS M/M/1 queuing model as the receiver's buffer. We argue that the presence of multiple senders that need to contend limited resources for transmission leads to lower utilities for each of them, as they end up limiting their transmissions even when they are aware of the fact that the eavesdropper is not overhearing their information. Further contributions on the topic may include deeper considerations on security concerns that may arise with eavesdropping [10]. Possible solutions may include adversary setups [30] with friendly jammers and the inclusion of other metrics other than AoI in the utilities.

References

[1] 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.

[2] 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 Wkshps.*, 2023, pp. 1301–1306.

[3] C. Kam, S. Kompella, G. D. Nguyen, J. E. Wieselthier, and A. Ephremides, "On the age of information with packet deadlines," *IEEE Trans. Inf. Theory*, vol. 64, no. 9, pp. 6419–6428, Sep. 2018.

[4] 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, Jun. 2021.

[5] L. Badia, H. Duranoglu Tunc, A. Aka, R. Bassoli, and F. Fitzek, "Strategic interaction over age of information on a quantum wiretap channel," in *Proc. European Wireless Conf.*, 2023.

[6] L. Crosara, N. Laurenti, and L. Badia, "It is rude to ask a sensor its age-of-information: Status updates against an eavesdropping node," in *Proc. IEEE BalkanCom*, 2023.

[7] ——, "Age of information is not just a number: Status updates against an eavesdropping node," *Ad Hoc Networks*, vol. 155, p. 103388, 2024.

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

[9] R. D. Yates and S. Kaul, "Real-time status updating: Multiple sources," in *Proc. IEEE ISIT*, 2012, pp. 2666–2670.

[10] H. Chen, Q. Wang, P. Mohapatra, and N. Pappas, "Secure status updates under eavesdropping: Age of information-based physical layer security metrics," *arXiv*, 2020. [Online]. Available: https://arxiv.org/abs/2002.07340

[11] 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.

[12] L. Crosara and L. Badia, "A stochastic model for age-of-information efficiency in ARQ systems with energy harvesting," in *Proc. European Wireless Conf.*, 2021.

[13] L. Huang and E. Modiano, "Optimizing age-of-information in a multi-class queueing system," in *IEEE ISIT*. IEEE, 2015, pp. 1681–1685.

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

[15] M. Moltafet, M. Leinonen, and M. Codreanu, "On the age of information in multi-source queueing models," *IEEE Trans. on Comm.*, vol. 68, no. 8, pp. 5003–5017, 2020.

[16] N. Akar and O. Dogan, "Discrete-time queueing model of age of information with multiple information sources," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14 531–14 542, 2021.

[17] V. Tripathi, R. Talak, and E. Modiano, “Age of information for discrete time queues,” *arXiv preprint arXiv:1901.10463*, 2019.

[18] J. Xu and N. Gautam, “Peak age of information in priority queuing systems,” *IEEE Trans. Inf. Theory*, vol. 67, no. 1, pp. 373–390, 2020.

[19] J.-B. Seo and J. Choi, “On the outage probability of peak age-of-information for D/G/1 queuing systems,” *IEEE Comm. Lett.*, vol. 23, no. 6, pp. 1021–1024, 2019.

[20] M. Costa and Y. E. Sagduyu, “Timely and covert communications under deep learning-based eavesdropping and jamming effects,” *Journal of Communications and Networks*, vol. 25, no. 5, pp. 621–630, 2023.

[21] A. Fazeli and A. Jadbabaie, “Duopoly pricing game in networks with local coordination effects,” in *Proc. IEEE CDC*, 2012, pp. 2684–2689.

[22] V. S. Dasari, B. Kantarci, M. Pouryazdan, L. Foschini, and M. Girolami, “Game theory in mobile crowdsensing: A comprehensive survey,” *Sensors*, vol. 20, no. 7, p. 2055, 2020.

[23] L. Badia, M. Levorato, F. Librino, and M. Zorzi, “Cooperation techniques for wireless systems from a networking perspective,” *IEEE Wirel. Commun.*, vol. 17, no. 2, pp. 89–96, 2010.

[24] I. Stanojev, O. Simeone, U. Spagnolini, Y. Bar-Ness, and R. L. Pickholtz, “Cooperative arq via auction-based spectrum leasing,” *IEEE Trans. on Comm.*, vol. 58, no. 6, pp. 1843–1856, 2010.

[25] A. Buratto and L. Badia, “Analysis of age of information in slotted aloha networks with different strategic backoff schemes,” in *Proc. IEEE CAMAD*, 2023, pp. 87–92.

[26] Q. Zhu, W. Saad, Z. Han, H. V. Poor, and T. Başar, “Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach,” in *IEEE MILCOM*, 2011, pp. 119–124.

[27] Y. Luo, Z. Feng, H. Jiang, Y. Yang, Y. Huang, and J. Yao, “Game-theoretic learning approaches for secure D2D communications against full-duplex active eavesdropper,” *IEEE Access*, vol. 7, pp. 41 324–41 335, 2019.

[28] A. Bergson, “A reformulation of certain aspects of welfare economics,” *Quart. J. Econ.*, vol. 52, no. 2, pp. 310–334, Feb. 1938.

[29] M. Cappelletti, N. Cibin, and L. Badia, “Game-theoretic economic models of duopolies applied to green ICT design,” in *Proc. IEEE EPEC*, 2021, pp. 267–272.

[30] G. Perin, A. Buratto, N. M. Anselmi, S. Wagle, and L. Badia, “Adversarial jamming and catching games over AWGN channels with mobile players,” in *Proc. IEEE WiMob*, 2021, pp. 319–324.