It Is Rude to Ask a Sensor Its Age-of-Information: Status Updates Against an Eavesdropping Node

Laura Crosara, Nicola Laurenti, and Leonardo Badia
Dept. of Information Engineering (DEI), University of Padova, Italy
email: {laura.crosara.1@phd. , nicola.laurenti@ , leonardo.badia@ }unipd.it

Abstract—We consider periodical status updates between a transmitter and a legitimate receiver, in the presence of an eavesdropper that is sometimes able to capture pieces of information. We assume that, in the absence of such a threat, the connection between the transmitter and the receiver is controlled by the transmitter with the aim to minimize the age of information at the receiver's side. However, if the presence of an eavesdropper is known, the transmitter may further tune the generation rate of status updates to trade off the age of information values acquired by the eavesdropper and the receiver, respectively. To analyze this problem, we first propose a metric that combines both objectives according to a Bergson social welfare framework, and then we solve the problem of finding the optimal generation rate as a function of the probability of data capture by the eavesdropper. This enables us to derive notable and sometimes counter-intuitive conclusions, and possibly establish an extension of the age of information framework to security aspects from a performance evaluation perspective.

Index Terms—Age of Information; Data acquisition; Modeling; Communication system security.

I. INTRODUCTION

Age of information (AoI) has become a performance indicator adopted frequently to quantify the freshness of status updates from remote transmitters [1]. Many sensing applications require to track real-time content and, more than the average delay or the sheer throughput, their most important requirement is that the exchanged data be fresh.

Whenever a transmitter and receiver exchange status updates, the AoI at the receiver is defined as [2]

$$\delta(t) = t - \sigma(t) \qquad (1)$$

where $\sigma(t)$ is instant of generation of the last received update. As normally done in this kind of analysis [3], [4], we consider zero propagation delay in the exchange, so time instants can be indifferently computed at the transmitter's or the receiver's side, and that whenever an update is generated at the transmitter's side, it always conveys fresh information [5]. Resource limitations imply that updates can only be performed sporadically, obtaining a trend of $\Delta(t)$ that is linearly growing until an update is performed, which resets the AoI to 0.

Queueing systems are among the first models investigated under this lens, already in some seminal papers on the topic [2]. Even the study of a simple M/M/1 queue highlights the following beautiful conclusion. If we assume that the transmitter generates updates with exponentially independent and identically distributed (i.i.d.) inter-generation times, with

tunable rate λ, and the service of the queue, also a memoryless process, has rate μ, so that the offered load is $\rho = \lambda/\mu$, the lowest AoI is achieved at a certain intermediate value, which is less straightforward than the delay- or throughput-optimizing conditions that are $\rho \to 0^+$ and $\rho \to 1^-$, respectively. This reasoning can be extended to more complex systems by changing the queue policy [6], [7] or explicitly including other aspects such as medium access control [8]–[10].

In the present paper, we want to add a new twist, by including a confidentiality objective related to the adversarial presence of an eavesdropper. To frame the problem in a classic setup, we consider a transmitter owned by Alice sending status updates to Bob, who plays the role of a legitimate receiver. Alice can tune the generation rate of update packets and the service procedure is according to a standard M/M/1 queue with *first-come-first-served* (FCFS) policy [11]. However, in addition to the aforementioned actors, an eavesdropper is present, aptly named Eve, who has the ability to capture information sent by Alice to Bob. We assume that all updates from Alice are received by Bob, but each of them has probability $\beta \in [0, 1]$ of being eavesdropped by Eve.

We further assume that Alice is aware of Eve's presence and knows the value of β. This changes the objective of the exchange from just sending fresh updates to Bob, to also including a *further* goal of leaving only stale information to Eve. Thus, the main contribution of this paper is a reformulation of the problem with a new objective function that chooses a point over the Pareto frontier of these two contrasting objectives according to Bergson's theory of social welfare [12]. This allows for an extension of the analytical framework to determine how the optimal load factor is influenced by Eve's probability of data capture.

We discuss quantitative results and highlight important conclusions, such as the optimal generation rate being, under proper conditions, a decreasing function of the probability of data capture. More in general, our investigation may set the basis for the extension of the age of information framework to security issues with analytical instruments.

The rest of this paper is organized as follows. In Section II, we discuss models from the literature for AoI of queuing systems, since our analysis piggybacks on them, and we also review the (actually few) efforts made to conjugate AoI and security aspects. Section IV describes our proposed extension, from two different standpoints; first, we identify a trade-off

between minimizing the AoI of the legitimate receiver and maximizing that of the eavesdropper, and then we solve it through an entirely analytical framework. Section V presents numerical results. Finally, we conclude in Section VI.

II. RELATED WORK

Many studies evaluate the AoI in queuing systems, for various settings but especially based on classic memory-less systems with different disciplines [13]–[15].

The FCFS M/M/1 queue presents a compelling behavior for what concerns its AoI. On one hand, it is well known that its throughput is related to its stability, i.e., the arrival rate λ and the service rate μ must satisfy $\rho = \lambda/\mu < 1$, and a high throughput is achieved whenever ρ approaches 1. On the other hand, the delay is minimized when ρ is close to 0. The AoI can be optimized by offering a traffic in an intermediate condition, even though the server is slightly biased towards being busy over being idle and so the optimal load factor ρ is actually $\rho^\star \approx 0.531$ [2]. In other words, optimizing the AoI in an M/M/1 queue implies seeking for non-aggressive management, where λ is significantly lower than μ, so there is already a self-limitation imposed to the data generation.

The quite elegant analytical results presented by Kaul and Yates in [2], and subsequent contributions [16], are important sources of inspiration for the present work. In particular, the full expression of the average AoI $\Delta = \mathbb{E}[\delta(t)]$ for an M/M/1 queue with FCFS policy is [2]

$$\Delta = \lambda\big(\mathbb{E}[XT] + \mathbb{E}[X^2]/2\big) = \frac{1}{\mu}\left(1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}\right), \quad (2)$$

where X and T are random variables equal to the interarrival time and system time of an update packet, respectively.

Some side remarks involve that there are substantially equivalent expressions, at least for what concerns the extensions meant in the present paper, to the cases of M/D/1, D/M/1, G/M/1, and so on, as well as with switching the discipline of the queue to *last-come-first-served* (LCFS), adding preemption, and more [7], [13], [14], [17]. For the purposes of our study, all of these evaluations can be considered equivalent, so we will just deal with the simpler M/M/1 queue.

Very few studies in the literature combine security and/or game theory with information freshness, and most of them just focus on mutual interference [18] or intentional jamming [19], [20]. The subject of confidentiality is rarely explored together with AoI, which is surprising since many mission critical applications rely on timely exchanges, which an attacker may want to intercept, forge, or modify. Paper [21] proposes to use AoI as an integrated quality of service and security indicator to discriminate the validity of a hash key in a urban rail communication-based train control data communication systems. However, the AoI is not used as a performance metric, but rather as a tool to improve secrecy. Similarly, [22] analyzes a generic Internet of Vehicles (IoV) network and designs a vehicle-assisted batch verification system. Differently from [21], they present a performance evaluation of AoI as a quantitative indicator of security.
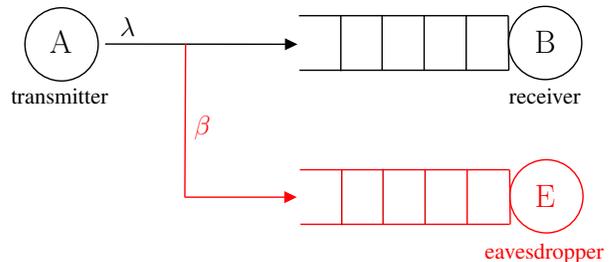

Fig. 1. Queuing system with a transmitter (A), a legitimate receiver (B), and an eavesdropper (E).

In [23], the transmission system considers various scattered packets with some network coding connecting them, so that the receiver can decode the message after receiving k packets out of n, but with the additional objective of preventing an eavesdropper from decoding that number of packets first.

The closest contribution we can find to our proposed approach is [24], where authors study the problem of maintaining information freshness under passive eavesdropping attacks. They consider a similar scenario, where a source sends its latest status to an intended receiver, while protecting the message from being overheard by an eavesdropper. Two AoI-based metrics are defined to characterize the secrecy performance of the considered system. Also akin to our analysis, they obtain similar performance curves, on which they find the optimal data injection rate. However, there are some notable differences with the present paper, which make our analysis simpler and more general. First of all, they consider a discrete time axis with stateful information, which allows for an optimization of the transmission schedule [5], [13]. We take a more basic approach where we tune the arrival rate λ of the queue. Since λ is a continuous variable, our linear optimization is without any discretization effect. Moreover, they consider a tradeoff between the AoI performance at the intended receiver and at the eavesdropper, based on their difference. Instead, we investigate this from a wider perspective based on Bergson's theory of social welfare [12] that allows to weigh the importance of contrasting the eavesdropper versus obtaining fresh information at the receiver.

Finally, combining conflicting objectives into a social welfare function according to Bergson's approach predates but is actually similar to the more well known contribution of Nash barganing [25]. Our specific choice corresponds to a product (that can be changed into a linear combination through logarithmic transformations) where exponential coefficients are tunable. The underlying point is that neither of the objectives can dominate over the other in a Pareto sense, but focusing on their product allows to identify a specific point on the Pareto frontier.

III. PROBLEM DEFINITION

We consider a system as depicted in Fig. 1, where a transmitter (Alice) sends status updates to a receiver (Bob). Alice can tune the generation rate of update packets and the service

procedure is according to an FCFS M/M/1 queue. We add a twist to this scenario adding an eavesdropper (Eve), that may capture data packets sent by Alice to Bob.

In the absence of Eve, Alice objective would be to minimize the AoI at Bob's receiver, to keep the information available to Bob as fresh as possible. However, if the presence of Eve is known, Alice may adjust the generation rate of status updates to increase the AoI at Eve's receiver. Therefore, Alice seeks for a tradeoff between two objectives, i.e., minimizing the AoI available to Bob and maximizing the AoI at Eve's side.

A typical real-world scenario that could be cast into our system is represented, for instance, by a open communication environment, which makes wireless transmissions more vulnerable than wired communications to malicious attacks [26], [27]. In particular, an eavesdropper can manage to intercept data whenever Alice and Bob cannot establish a secure communication channel. Tactical networks [28] are also an important application for our analysis.

To sum up, we are going to address the following points.

1) Define an appropriate confidentiality-aware objective function, which takes into account the two contrasting purposes of Alice, namely minimizing the average AoI at Bob's receiver, while keeping the average AoI at Eve's receiver as large as possible
2) Find the optimal generation rate of update packet for Alice, according to the objective function above
3) Show and discuss quantitative results, highlighting counter-intuitive conclusions, considering different scenarios and system parameters.

IV. ANALYTICAL MODEL

We consider the system described in Section III, where a transmitter (Alice) sends periodical update packets to a legitimate receiver (Bob) through a FCFS M/M/1 packet queue. Each update transmitted by Alice carries new information that resets the AoI at Bob's side. Alice generates packets according to a Poisson process of rate λ and service time of Bob's queue is exponentially distributed with rate μ, providing an offered load $\rho = \lambda/\mu$. It is not restrictive to normalize Bob's service capacity as $\mu = 1$, so that $\lambda = \rho$; otherwise, all the results can be rescaled by a factor μ. We assume that the channel between Alice and Bob is error-free, so that every update packet sent by Alice is correctly received by Bob, although in this basic framework it would be possible to account for erasures of status updates by simply modifying ρ accordingly.

Moreover, we consider the presence of an eavesdropper, referred to as Eve (E), which attempts to capture the information exchanged between the transmitter and the receiver. We assume that each update packet transmitted by Alice is independently eavesdropped by Eve according to an i.i.d. statistics, with eavesdropping probability $\beta \in [0, 1]$. Consequently, we can consider that a fraction β of the transmitted packets are received also by Eve. According to the thinning property [29], packets arrival at Eve's queue follow a Poisson process with rate $\beta\lambda$. Akin to Bob, Eve enqueues her packets in a FCFS M/M/1 queue

with service rate μ, equal to that of Bob. The load factor in the channel between Alice and Eve is $\rho_{\mathrm{E}} = \beta\rho$.

A. Confidentiality Aware Objective Function

In our scenario, Alice is assumed to be the only intelligent agent, since she can choose her transmission rate λ, while Eve and Bob are passive entities. We further assume that Alice is aware of Eve's presence and knows the value of β. In a scenario where no eavesdropper is present, the purpose of the transmitter will be to tune the value of ρ to obtain an AoI value at the legitimate receiver Bob that is as small as possible. However, the presence of an eavesdropper who captures a fraction of the transmitted packets implies that Alice wants the information available to Eve to be as old as possible, in addition to minimizing Bob's AoI. Therefore, Alice has two competing objectives described by the utility functions

$$u_1(\rho) = \frac{1}{\Delta_{\mathrm{B}}(\rho)}, \qquad u_2(\rho) = \Delta_{\mathrm{E}}(\rho), \qquad (3)$$

where $\Delta_{\mathrm{B}}(\rho) = \mathbb{E}[\delta_{\mathrm{B}}(t)]$ and $\Delta_{\mathrm{E}}(\rho) = \mathbb{E}[\delta_{\mathrm{E}}(t)]$ represent the expected AoI at Bob's and Eve's receivers, respectively.

From Alice's perspective, it is beneficial to increase either of these utilities, or both. However, they are contrasting objectives as is clear from the following reasoning. Indeed, the values of $\delta_{\mathrm{B}}(t)$ and $\delta_{\mathrm{E}}(t)$ increase until Alice generates a data packet. When a new data packet is transmitted, two situation can occur: (i) the packet is received by both Bob and Eve, this happens with probability β. In this case, at the current time instant $\delta_{\mathrm{B}}(t)$ and $\delta_{\mathrm{E}}(t)$ are reset to zero; (ii) the packet is received only by Bob, this happens with probability $1 - \beta$. In this case, at the current time instant only $\delta_{\mathrm{B}}(t)$ is reset to zero while $\delta_{\mathrm{E}}(t)$ continues to increase. This means that, whenever $\delta_{\mathrm{B}}(t)$ is lowered, $\delta_{\mathrm{E}}(t)$ can decrease too, since Eve's capture of data cannot be controlled or forecast by Alice.

Thus, to maximize the two competing utilities of (3), we reformulate the problem defining a new objective function that sets a precise value on Pareto frontier created by u_1 and u_2, i.e., the set of values for which u_1 cannot be increased without lowering u_2, or vice versa. This choice is made following Bergson's approach [12], where we set an ultimate objective function f to be a weighted product between the two utilities u_1 and u_2, which is a modified Nash bargaining solution [25]

$$f(\rho) = [u_1(\rho)]^{a+1} u_2(\rho) = \frac{\Delta_{\mathrm{E}}(\rho)}{[\Delta_{\mathrm{B}}(\rho)]^{a+1}}, \qquad (4)$$

with $a \in (0, +\infty)$ being a parameter that controls the trade-off between u_1 and u_2. Note that in the choice of the exponent of u_1 we must assume that this objective cannot be eliminated; otherwise, we would reach a trivial allocation where Alice never updates. This would consistently obtain a very high $\Delta_{\mathrm{E}}(\rho)$ but would also have $\Delta_{\mathrm{B}}(\rho)$ to grow indefinitely, which goes against the motivation of the setup in the first place. Thus, the objective of delivering fresh data to Bob cannot be avoided and the exponent in the trade-off must be greater than or equal to 1. Hence, we write it as $a + 1$, where the larger a, the more important u_1 versus u_2 in the trade-off. Moreover,

$a \to +\infty$ corresponds to ignoring the presence of Eve, while $a \to 0^+$ means that the threat of the eavesdropping receives the highest importance, and Alice just wants to minimize the ratio $\Delta_B(\rho)/\Delta_E(\rho)$ instead of $\Delta_B(\rho)$ itself. Therefore, the specific choice of a governs the selection of the optimal point in the Pareto frontier.

B. Optimal Offered Load

The full expressions for $\Delta_B(\rho)$ and $\Delta_E(\rho)$ when $\mu = 1$ can be computed from (2) as

$$\Delta_B(\rho) = 1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}, \tag{5}$$

for the legitimate channel between Alice and Bob, and

$$\Delta_E(\rho) = 1 + \frac{1}{\beta\rho} + \frac{\beta^2\rho^2}{1-\beta\rho}. \tag{6}$$

for the eavesdropper channel between Alice and Eve. The optimal offered load ρ maximizing the objective $f(\rho)$ is

$$
\begin{aligned}
\rho^\star &= \arg\max_\rho f(\rho) = \arg\max_\rho \frac{\Delta_E(\rho)}{[\Delta_B(\rho)]^{a+1}} \\
&= \arg\max_\rho \frac{1 + \frac{1}{\beta\rho} + \frac{\beta^2\rho^2}{1-\beta\rho}}{\left(1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}\right)^{a+1}} \\
&= \arg\max_\rho \frac{(\beta^3\rho^3 - \beta^2\rho^2 + 1)\rho^a(\rho-1)^{a+1}}{\beta(\beta\rho-1)(\rho^3-\rho^2+1)^{a+1}}
\end{aligned}
\tag{7}
$$

Equation (7) can be solved by computing the derivative of $f(\rho)$. It is worth noting that, when $\beta \to 0^+$, the derivative $f'(\rho)$ approaches

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

where $g(\rho)$ is the 4-th degree polynomial

$$g(\rho) = (a+2)(\rho^4 - 2\rho^3 + \rho^2) - (2a+1)\rho + a. \tag{9}$$

Therefore, when $\beta \to 0^+$, the optimal load factor at the limit is obtained as the only real solution of $g(\rho) = 0$ in the interval $(0, \mu)$. The function $g(\rho)$ is continuous in the interval $(0, \mu)$ and it takes value of opposite sign at the boundaries

$$g(0) = a > 0, \tag{10}$$
$$g(\mu) = -(a+1) < 0. \tag{11}$$

Therefore, according to the intermediate value theorem, a real value $\tilde{\rho} \in (0, 1)$ such that $g(\tilde{\rho}) = 0$ must exist. Moreover, the first order derivative of $g(\rho)$ is

$$g'(\rho) = 2\rho(a+2)(\rho-1)(2\rho-1) - 2a - 1, \tag{12}$$

which is negative for every $\rho \in (0, 1)$. Consequently, the solution $\tilde{\rho}$ is unique and can be found numerically. For example, in the case of $a = 1$, we have

$$3(\rho^2 - 2)(\rho^2 + 1) + 1 = 0, \tag{13}$$
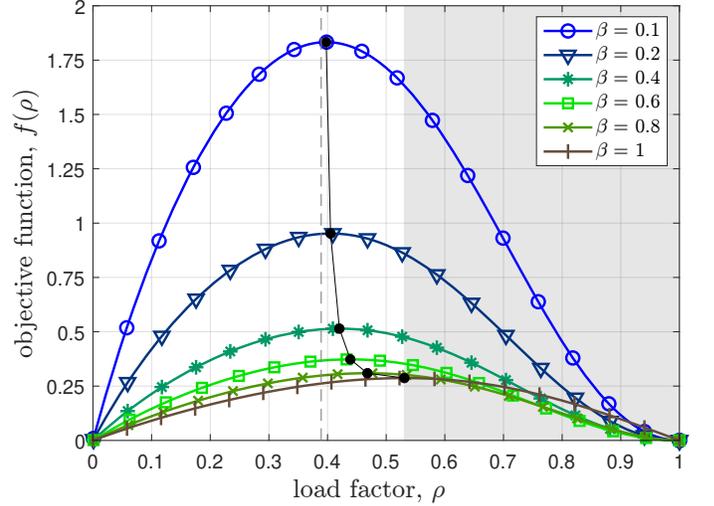
and the solution is found at $\rho \approx 0.389$.

Fig. 2. Objective $f(\rho)$, as a function of the load factor ρ, for different values of eavesdropping probability β, with weight $a = 1$. The black line connects the maximizing points $\rho^\star$. The dashed black line reports $\rho = 0.389$.

V. NUMERICAL RESULTS

We present quantitative evaluations to express the consequences of the derivations above. The scenario considered includes a transmitter (Alice) and a receiver (Bob), whose communication is intercepted by an eavesdropper (Eve). Eve independently intercepts data packets with probability β. For sake of normalization, we consider both Bob's and Eve's service capacities to be $\mu = 1$. We will discuss how the optimal load factor $\rho^\star$, obtained maximizing the objective function $f(\rho)$ in (7), is influenced by Eve's probability of data capture β and the trade-off parameter a.

If Eve does not intercept any packet, i.e. $\beta = 0$, we expect $\rho^\star = 0.531$, which is the AoI minimizing value for the load factor with normalized service capacity [2]. When packets are eavesdropped with i.i.d. probability $\beta > 0$, we expect that the optimal load factor decreases, therefore $\rho^\star \leq 0.531$ for any value of β. For this reason, in all the results that follow, the areas corresponding to $\rho^\star > 0.531$ are shaded.

Fig. 2 shows the objective function $f(\rho)$, as a function of ρ for different values of β when $a = 1$. The black line connects the maximum point of each curve, reached when $\rho = \rho^\star$, while the dashed black line reports the value $\tilde{\rho} = 0.389$. First of all, we note that the curves are bell-shaped with a very pronounced maximum when β is small. When β rises, the curves get flatter, this happens because, when β tends to 1, the two functions Δ_B and Δ_E get closer, and Alice has narrower margins to reach her objectives. When $\rho = 1$, all the curves go to zero. As the black line in Fig. 2 shows, the value of $\rho^\star$ tends to 0.531 as β increases, and decreases with β, tending towards a vertical asymptote at $\rho < 0.531$, displayed as the black dashed line in the figure, whose numerical value is the solution of (12). For the specific case of this figure where $a = 1$, the asymptotic value shown by the vertical dashed line is $\tilde{\rho} = 0.389$.
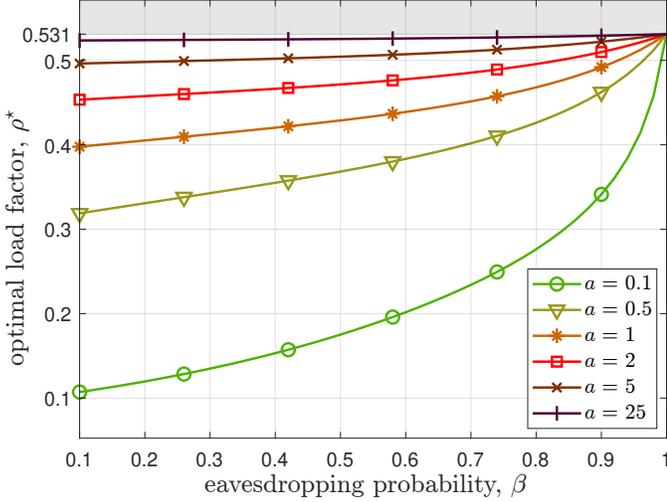
Fig. 3. Optimal load factor $\rho^\star$, as a function of capture probability β, for different values of weight a.
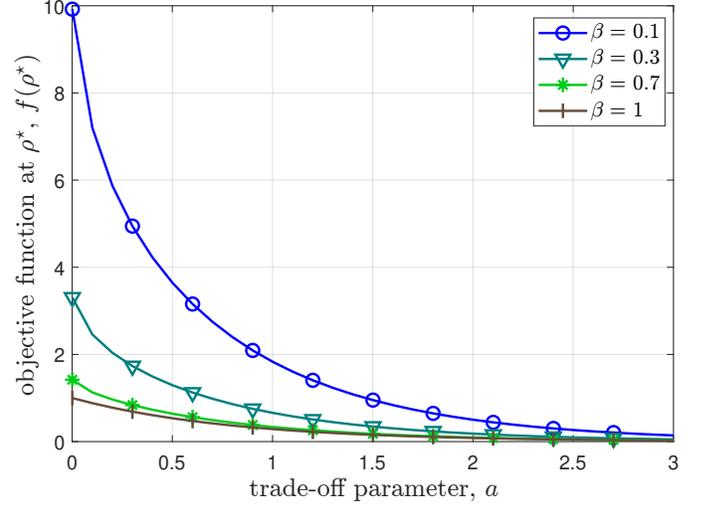

Fig. 4. Objective function $f(\rho)$ evaluated at the optimal load factor $\rho^\star$, as a function of weight a, for different eavesdropping probabilities β.

Interestingly, the lower β, the lower $\rho^\star$, which, at first glance, may seem counter intuitive, yet this behavior has the following explanation. If β tends to 1 the eavesdropper often intercepts the packets transmitted by Alice, so the only sensible objective for Alice is to keep $\Delta_{\rm B}$ low, which is achieved by choosing $\rho = 0.531$. If β decreases, the second objective takes over, and Alice transmits less frequently, choosing $\rho < 0.531$, to prevent Eve from intercepting. Above all, if $\Delta_{\rm B}$ is low and $\Delta_{\rm E}$ high, Alice should wait before transmitting a new packet because the effect can be to reset both $\Delta_{\rm B}$ and $\Delta_{\rm E}$. As a side note, in our analysis Alice only chooses the transmission rate λ, and she does not perform a real-time optimization based on the instantaneous values of the $\Delta_{\rm B}$ and $\Delta_{\rm E}$. Yet, it is expected that in a stateful optimization [5], [24] (left for future research) this phenomenon will be seen with even more clarity.

Fig. 3 shows the optimal load factor $\rho^\star$ as a function of β, for different values of a. One can see that the optimal value $\rho^\star$ approaches zero when the values of β and a are low. In other words, if the main objective for Alice is to have a large ratio of Eve's AoI versus Bob's, and Eve is rarely capable of eavesdropping data, the best strategy for Alice is also to update very rarely. This means that in Fig. 2 the dashed vertical grey line would move to the left as a decreases. Conversely, when the value of a rises, $\rho^\star$ tends to 0.531 for every β, thus

$$\lim_{a \to +\infty} \rho^\star = 0.531, \quad \forall \beta \in [0,1]. \tag{14}$$

Hence, the black dashed line in Fig. 2 would move to the left as a increases. When $\beta = 1$, $\rho^\star = 0.531$ for all $a > 0$.

Fig. 4 shows the objective function $f(\rho)$ evaluated at the optimal load factor $\rho^\star$, as a function of a, for different values of β. We note that when $a \to 0^+$, the value of the objective function at the optimal point $f(\rho^\star)$ tends to $1/\beta$ for every value of β, i.e.,

$$\lim_{a \to 0^+} f(\rho^\star) = \lim_{a \to 0^+} \frac{\Delta_{\rm E}(\rho^\star)}{[\Delta_{\rm B}(\rho^\star)]^{(a+1)}} = 1/\beta, \tag{15}$$
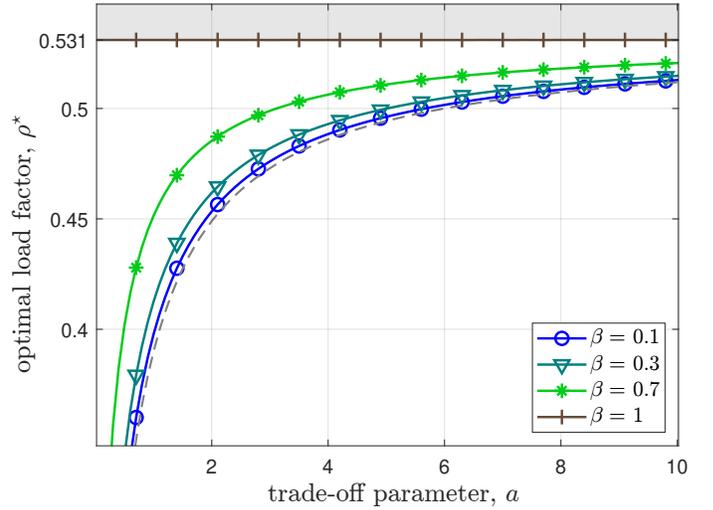
Fig. 5. Optimal load factor $\rho^\star$, as a function of weight a, for different eavesdropping probabilities β. The black dashed line is the limit for $\beta \to 0^+$.

whereas, when $a \to +\infty$, $f(\rho^\star) \to 0^+$ for all values of β.

Fig. 5 shows the optimal load factor $\rho^\star$, as a function of a, for different values of β. For all the curves, the value of $\rho^\star$ moves toward 0 when a tends to zero, i.e.,

$$\lim_{a \to 0^+} \rho^\star = 0, \quad \forall \beta \in [0,1), \tag{16}$$

for every value of β, provided it is less than 1 (whereas for $\beta = 1$ the curve degenerates in a constant optimal choice of $\rho^\star = 0.531$). Moreover, we also plot a black dashed line to represents the limit for $\beta \to 0^+$. Notably, all curves with a relatively small (but not necessarily infinitesimal) values of β, such as $\beta = 0.3$ in the figure, approach this asymptotic trend quite closely, thereby implying that for a low eavesdropping

probability, the optimal behavior of the transmitter is always the same, and ultimately determined by the sole value of a, i.e., the level of importance attributed to one objective versus the other. We believe that this may lead to interesting conclusions about the optimal transmission policy for fresh status updates in the presence of an eavesdropper whenever the success rate of data capturing is relatively low, even in the case it is not accurately known.

VI. Conclusions

We analyzed a scenario of status updates between a transmitter and a legitimate receiver, considering also the presence of an eavesdropper that is sometimes able to intercepts data packets. For this purpose, we leveraged existing analytical results for queuing systems, where the AoI is computed as a function of the load factor.

We assume that the transmitter is aware of the eavesdropper and wants to set an efficient data injection rate that simultaneously achieves low AoI at the intended receiver but keeps the information of the eavesdropper stale. To analyze this problem, we proposed to combine both objectives according to a Bergson social welfare framework, then we solved the problem of finding the optimal load factor as a function of the probability of data capture by the eavesdropper.

The main conclusion is that, in order to account for this additional objective of leaking only stale information to the eavesdropper, the transmitter has to decrease its data generation rate, lowering the load factor. Especially, if the predominant goal of the transmitter is to keep the eavesdropper at bay, the load factor tends to zero even for small values of the probability of data capture by the eavesdropper. More in general, the present framework can be used as an adjustable approach for different cases of interests in practical contexts.

Envisioned extensions of the present paper include the analysis of an optimized schedule with stateful information [5], also investigating the costs for tracking the eavesdropper and detecting whether data was actually captured. Moreover, a natural follow-up would be to consider the analysis of this adversarial setup from a game theoretic standpoint [30], with an eavesdropper that is able to strategically regulate the data capture probability. Finally, an extension to pervasive data networks, especially for what concerns the scalability of the analysis, is key to bring the present investigation in the context of future generation communication systems [31].

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, May 2021.

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

[3] S. Kaul, M. Gruteser, V. Rai, and J. Kenney, "Minimizing age of information in vehicular networks," in *Proc. IEEE SAHCN*, 2011, pp. 350–358.

[4] Y. Wang, S. Wu, L. Yang, J. Jiao, and Q. Zhang, "To preempt or not: Timely status update in the presence of non-trivial propagation delay," in *Proc. IEEE VTC Fall*, 2020.

[5] A. Munari and L. Badia, "The role of feedback in AoI optimization under limited transmission opportunities," in *Proc. IEEE Globecom*, 2022.

[6] L. Crosara and L. Badia, "Cost and correlation in strategic wireless sensing driven by age of information," in *Proc. Eur. Wirel.*, 2022.

[7] J. P. Champati, R. R. Avula, T. J. Oechtering, and J. Gross, "Minimum achievable peak age of information under service preemptions and request delay," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1365–1379, May 2021.

[8] 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.

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

[10] O. T. Yavascan and E. Uysal, "Analysis of slotted ALOHA with an age threshold," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1456–1470, May 2021.

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

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

[13] M. Moltafet, M. Leinonen, and M. Codreanu, "Average AoI in multi-source systems with source-aware packet management," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1121–1133, Feb. 2020.

[14] M. Costa, M. Codreanu, and A. Ephremides, "On the age of information in status update systems with packet management," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 1897–1910, Apr. 2016.

[15] L. Crosara and L. Badia, "A stochastic model for age-of-information efficiency in ARQ systems with energy harvesting," in *Proc. Eur. Wirel.*, 2021.

[16] R. D. Yates and S. K. Kaul, "The age of information: Real-time status updating by multiple sources," *IEEE Trans. Inf. Theory*, vol. 65, no. 3, pp. 1807–1827, Mar. 2018.

[17] R. Talak and E. H. Modiano, "Age-delay tradeoffs in queueing systems," *IEEE Trans. Inf. Theory*, vol. 67, no. 3, pp. 1743–1758, Mar. 2020.

[18] 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.

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

[20] S. Banerjee and S. Ulukus, "Age of information in the presence of an adversary," in *Proc. IEEE Infocom Wkshps*, 2022.

[21] X. Wang, L. Liu, L. Zhu, and T. Tang, "Joint security and QoS provisioning in train-centric CBTC systems under sybil attacks," *IEEE Access*, vol. 7, pp. 91 169–91 182, Jul. 2019.

[22] T. Jing, H. Yu, X. Wang, and Q. Gao, "Joint timeliness and security provisioning for enhancement of dependability in Internet of Vehicle system," *Int. J. Distrib. Sens. Netw.*, vol. 18, no. 6, Jun. 2022.

[23] A. Asheralieva and D. Niyato, "Optimizing age of information and security of the next-generation Internet of everything systems," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 20 331–20 351, Oct. 2022.

[24] 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

[25] J. F. Nash, Jr, "The bargaining problem," *Econometrica*, vol. 18, no. 2, pp. 155–162, Apr. 1950.

[26] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[27] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[28] P. Thanh, T. Hoan, H. Vu-Van, and I. Koo, "Efficient attack strategy for legitimate energy-powered eavesdropping in tactical cognitive radio networks," *Wirel. Netw.*, vol. 25, pp. 3605—3622, Feb. 2019.

[29] N. Benvenuto and M. Zorzi, *Principles of communications networks and systems*. Wiley, 2006.

[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.

[31] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of things: a survey," *Fut. Gen. Comp. Syst.*, vol. 56, pp. 684–700, Mar. 2016.