Age of Information is Not Just a Number: Status Updates Against an Eavesdropping Node

Laura Crosara*, Nicola Laurenti, Leonardo Badia[1]

University of Padova, Dept. of Information Engineering, 35131 Padova, Italy

Abstract

We consider status updates exchanged between a transmitter and a legitimate receiver, also including an eavesdropper that captures pieces of information. In the absence of such a threat, the connection between the transmitter and the receiver is controlled by the transmitter with the aim of delivering fresh information at the receiver's side quantified through the age of information. Due to the presence of the eavesdropper, the transmitter may further tune the generation rate of status updates to trade off the ages of information acquired by the eavesdropper and the receiver, respectively. We combine both objectives according to a Bergson social welfare framework and we solve the problem of finding the optimal generation rate as a function of the probability of data capture by the eavesdropper. We consider the age of information minimization task in the context of queuing systems, at first assuming equal service rates at the legitimate receiver and the eavesdropper, then analyzing scenarios where the eavesdropper's service rate is different. 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.

Keywords: Age of Information; Data acquisition; Modeling; Communication system security.

1. Introduction

Age of information (AoI) has become a performance indicator adopted frequently to quantify the freshness of status updates from remote transmitters [1, 2]. Many sensing applications are required 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.

*Corresponding author

Email addresses: laura.crosara.1@phd.unipd.it (Laura Crosara), nicola.laurenti@unipd.it (Nicola Laurenti), leonardo.badia@unipd.it (Leonardo Badia)

[1] This is an extended version of [1] published at IEEE BalkanCom 2023.

Whenever a transmitter and receiver exchange status updates, the value of AoI at the receiver is [3]

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

where $\sigma(t)$ is the instant of reception of the last update. As normally done in this kind of analysis [4, 5], we consider zero propagation delay in the exchange, so time instants can be indifferently computed at the transmitter's or the receiver's side. Note that considering a nonzero propagation delay results in a shift of the service time. Moreover, the impact of propagation delay has already been analyzed in [6] and is out of scope for this paper. We also adopt a generate at will model, implying that every update, when generated at the transmitter's side, conveys fresh information [7].

Queueing systems are among the first models investigated under this lens, already in some seminal papers on the topic [3]. Even the study of a simple M/M/1 queue highlights the following important conclusion. If 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 in the stability range $\rho \in [0, 1)$. This 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 [8, 9] or explicitly including other aspects such as medium access control [10, 11, 12].

In the present paper, we 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 [13]. 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. All updates from Alice are received by Bob, but each of them has probability $\beta \in [0, 1]$ of being eavesdropped by Eve.

We assume that Alice is aware of Eve's presence and knows the value of β [2]. 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 [14, 15, 16]. We analyze and simulate the scenario where Eve's and Bob's queues have the same service rate $\mu = 1$. Then, we also consider the case where the service rate in Eve's queue is either higher or lower than the service rate in Bob's queue.

Thus, the first contribution of this paper is a reformulation of the problem with a new objective function that chooses a point over the Pareto frontier of

[2] We remark that, in most scenarios, it is unlikely that Alice learns the specific packet captured by Eve. So, we adopt a worst-case approach for Alice and Bob, where they only have access to the statistical behavior of Eve.

these two contrasting objectives according to Bergson's theory of social welfare [17]. This allows for an extension of the analytical framework to determine how the optimal transmission probability is influenced by Eve's probability of data capture.

The second contribution is the analysis of the optimal transmission rate when the attacker and legitimate receiver queues have different service rates, which leads to some interesting and non-trivial conclusions about how Alice can counteract the presence of Eve.

Finally, we discuss quantitative results and highlight important conclusions, such as the optimal transmission probability chosen by Alice being, under proper conditions, a decreasing function of the probability β of data captured by Eve. In general, our investigation may set the basis for the extension of the AoI framework to security issues with analytical instruments.

The rest of this paper is organized as follows. In Section 2, 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, especially for what concerns covert communications against eavesdropping. We present the system model in Section 3; at 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 4 presents numerical results. Finally, we conclude in Section 5.

2. Related Work

Many studies evaluate AoI in queuing systems, for various settings but especially based on classic memoryless systems with various disciplines [12, 18, 19].

The FCFS M/M/1 queue presents a compelling behavior for what concerns its AoI. In a stable system for which the arrival rate λ and the service rate μ satisfy $\rho = \lambda/\mu < 1$, the highest throughput is achieved whenever ρ approaches 1, whereas the delay is minimized when ρ is close to 0. Conversely, AoI can be optimized by offering 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 $\rho_0 \approx 0.531$ [3]. In other words, optimizing AoI in an M/M/1 queue implies seeking non-aggressive management, where λ is significantly lower than μ, so there is already a self-limitation imposed on the data generation.

This and other quite elegant analytical results presented by Kaul and Yates in [3], and subsequent contributions [20], 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 [3]

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

where random variables X and T are 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 [9, 12, 18, 21]. For the purposes of our study, we will just deal with the simpler M/M/1 queue, even though the analysis can be promptly extended to other kinds of queues.

Security issues are rarely explored together with AoI, and most of the studies consider adversaries that resort to jamming [22, 23]. Hence, the objective of the attackers is seen as increasing AoI of legitimate communication, as opposed to capturing information for themselves. In this sense, these frameworks are prone to investigations through adversarial game theory [24, 25], by considering a maximizer of AoI, as opposed to the legitimate transmitter being a minimizer.

Instead, the subject of confidentiality is seldom explored together with AoI, despite many mission critical applications relying on timely exchanges, which an attacker may want to intercept, forge, or modify. This would be inherently different from jamming, and likely incompatible with it [26].

Among the few contributions on this matter, [27] proposes AoI as an integrated indicator of the quality of service and security to discriminate the validity of a hash key in urban rail communication-based train control data communication systems. However, AoI is not used as a performance metric, but rather as a tool to improve secrecy, and it is only regarded from the perspective of the legitimate users. In [28], instead, a generic Internet of Vehicles network is investigated and a vehicle-assisted batch verification system is adopted. Here, AoI is used as a quantitative indicator of security, but the scenario considers sybil attacks and not eavesdropping.

In [29], 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 focus of their analysis is therefore to exploit a proper inter-dependence among the packets, whereas in our analysis we take a more general stance where all packets are independent in content (and possibly, independently eavesdropped as well).

Physical layer security techniques to achieve protection against an eavesdropper, also considering AoI in the analysis, are introduced in [30], where a framework for covert full-duplex communication in block Rayleigh fading channels is proposed, with a requirement on information freshness. This means that artificial noise is transmitted to confuse the eavesdropper and the transmit probability of the informative signal containing status updates is adjusted to maximize the error probability of detection at the eavesdropper, yet subject to a constraint of minimum average AoI. While the model is unlike ours, one can see some resemblance to our analysis, in that the goal of contrasting the eavesdropper should not prevent the transmitter from sending informative status updates every now and then. However, in our approach, there is no injection of additional noise and the average AoI is minimized rather than just being a constraint.

On this same line, [31] also considers AoI minimization in a covert communication between a transmitter and its legitimate receivers when an eavesdropper is present in the area. The scenario is still from a physical layer perspective, i.e., focusing on the uncertainty about the physical locations of the eavesdropper and using successive interference cancellation for non-orthogonal medium access. The optimization also considers how to regulate the transmit power of the legitimate communication, to ensure negligible probability of interception by the eavesdropper, in addition to whether to transmit or not. This leads to a completely different analysis from ours, where once again AoI enters the model just through a constraint, however, considered here as applied to all the legitimate receivers.

In [14], the approach is more similar to ours, since that paper also deals with the optimization of status update scheduling against an eavesdropper. However, it makes different assumptions from our scenario: in particular, the eavesdropper is subject to energy harvesting constraints and the transmitter is aware of the specific AoI value achieved by the eavesdropper at all times, which allows for a stateful policy to be derived as the solution of a Markov decision process. In the present paper instead, we assume that the transmitter is only aware of the probability that the eavesdropper captures a packet, but not whether it succeeds on a per-packet basis. A further difference is that the authors of [14] consider a specific tradeoff between the two objectives, i.e., they minimize AoI of the legitimate communication but consider AoI of the eavesdropper as a constraint, i.e., it must stay below the pre-defined threshold. Clearly, this imposes a threshold behavior in the stateful policy. Conversely, we also consider these different objectives but the mediation between them is made tunable through a parameter.

The closest contribution we can find to our proposed approach is [15], where authors study the problem of maintaining information freshness under passive eavesdropping attacks. They consider a scenario where a source sends its latest status to an intended receiver while protecting the message from being overheard by an eavesdropper, and define two AoI-based metrics 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, some notable differences make our analysis simpler and more general. First of all, they consider a discrete time axis and assume stateful scheduling, which allows for an optimization of the transmission rate [7, 18]. In our approach, we tune the arrival rate λ of the queue a priori and, 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 [17] that allows us to weigh the importance of contrasting the eavesdropper versus obtaining fresh information at the receiver.

Combining conflicting objectives into a single function according to Bergson's approach predates but is actually similar to the better known contribu-

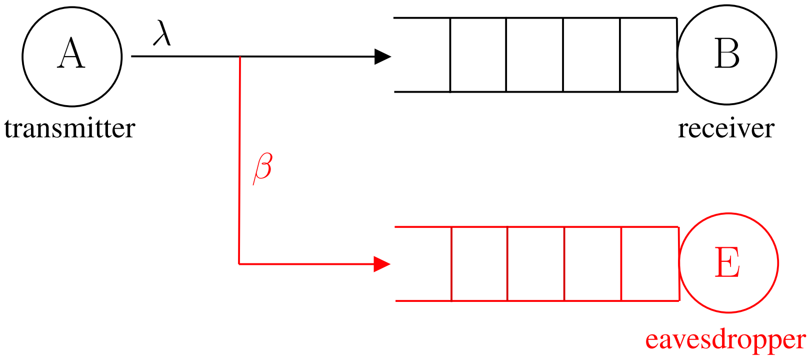

Figure 1: Queuing system with a transmitter (A), a legitimate receiver (B), and an eavesdropper (E).

tion of Nash bargaining [32]. 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 identifies a specific point on the Pareto frontier.

3. System Model

We consider a system as depicted in Figure 3, where Alice (A) is a transmitter sending status updates to her receiver, Bob (B). Alice can tune the generation rate of update packets and the service procedure is according to an FCFS M/M/1 queue. Within this scenario, we also include Eve (E), an eavesdropper that may capture data packets sent by Alice to Bob.

In the absence of Eve, Alice's objective would be to minimize Bob's AoI, to keep the information available to him as fresh as possible. If the presence of Eve is known, Alice may adjust the generation rate of status updates to cause the data captured by Eve to be stale. We will quantify this through Eve's AoI. Therefore, Alice seeks a tradeoff between two objectives, i.e., minimizing Bob's AoI while at the same time maximizing AoI at Eve's side.

A typical real-world scenario that could be cast into our system is represented, for instance, by an open communication environment, which makes wireless transmissions more vulnerable than wired communications to malicious attacks [16, 33]. In particular, an eavesdropper can manage to intercept data whenever Alice and Bob cannot establish a secure communication channel.

The connection between Alice and Bob is expressed by an M/M/1 queue with FCFS discipline, that is, Alice generates packets according to a Poisson process of rate λ and the service time of Bob's queue is exponentially distributed with unit rate, providing an offered load $\rho = \lambda$. It is not restrictive to normalize Bob's service capacity, otherwise, all the results can be rescaled by the service rate. The channel between Alice and Bob is taken as error-free so that every

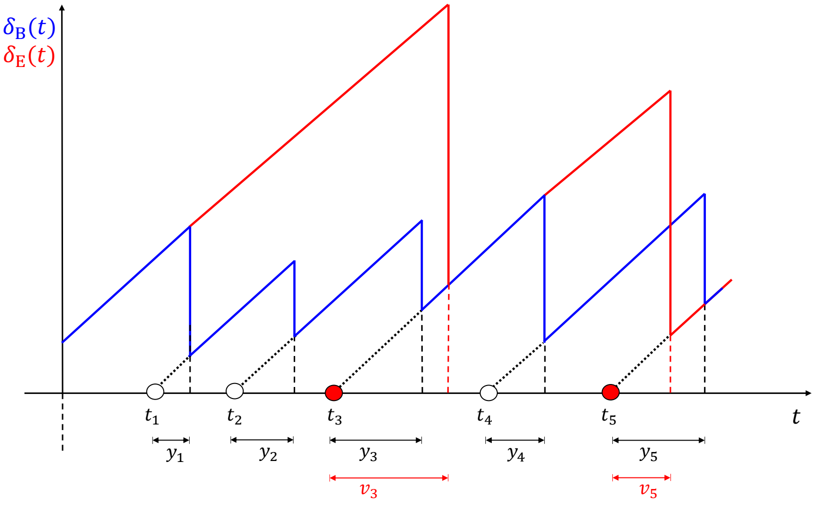

Figure 2: A possible realization of the instantaneous AoI process for Bob (in blue) and Eve (in red). Packet arrival instants from the source, Alice, are marked by circles, white for $\xi_j = 0$, red for $\xi_j = 1$, i.e. the packet j is eavesdropped by Eve.

update packet sent by Alice is correctly received by Bob. However, note that our framework can accommodate losses by adjusting the offered load ρ.

We consider that each update packet generated by Alice at a random time t_j might be eavesdropped by Eve. This happens according to a binary random variable $\xi_j \in \{0,1\}$ that follows an i.i.d. statistics, i.e., ξ_j can be either 1, implying that packet j is eavesdropped with probability $\beta \in [0,1]$, or 0 with probability $1-\beta$. Consequently, we refer to β as the eavesdropping probability, and it follows that the average fraction of packets captured by Eve is also equal to β. Moreover, packet arrivals at Eve's queue follow a Poisson process with rate $\beta\lambda$. Akin to Bob, Eve queues her packets in a FCFS M/M/1 queue with service rate μ. The load factor in the channel between Alice and Eve is $\eta = \beta\lambda/\mu$.

This configuration results in distinguishing between Bob's and Eve's AoI. The former denotes the instantaneous freshness of data legitimately exchanged, and is defined from (1) as

$$\delta_{\mathrm{B}}(t) = t - \sigma_{\mathrm{B}}(t)\,, \quad \sigma_{\mathrm{B}}(t) = \max\{t_j : t_j + y_j < t\}\,, \tag{3}$$

where y_j is the service time of the j-th packet at Bob, while the latter is written as

$$\delta_{\mathrm{E}}(t) = t - \sigma_{\mathrm{E}}(t)\,, \quad \sigma_{\mathrm{E}}(t) = \max\{t_j : t_j + \upsilon_j < t,\, \xi_j = 1\}\,, \tag{4}$$

with $\sigma_{\mathrm{E}}(t)$ being the instant of reception of a packet that is also captured and processed by Eve, with υ_j the service time at Eve. The instantaneous AoI at Bob and Eve is shown in Fig. 2.

3.1. Confidentiality Aware Objective Function

In our first scenario, Alice is the only intelligent agent, since she can choose her transmission rate λ, while Eve and Bob are passive entities. Alice is aware of Eve's presence and knows the value of β. 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

$$u_1(\lambda) = \frac{1}{\widetilde{\Delta_\mathrm{B}}(\lambda)}\,, \qquad u_2(\lambda) = \widetilde{\Delta_\mathrm{E}}(\lambda), \tag{5}$$

where to avoid troubles with infinity, we upper bound the average AoI value, i.e.,

$$\widetilde{\Delta_\mathrm{B}}(\lambda) = \min\{\Delta_\mathrm{B}(\lambda), M\}\,,\;\; \widetilde{\Delta_\mathrm{E}}(\lambda) = \min\{\Delta_\mathrm{E}(\lambda), M\}\,, \tag{6}$$

with M being a properly large value, and $\Delta_\mathrm{B}(\lambda) = \mathbb{E}[\delta_\mathrm{B}(t)]$ and $\Delta_\mathrm{E}(\lambda) = \mathbb{E}[\delta_\mathrm{E}(t)]$ representing the expected AoI of Bob's and Eve's, respectively. So, in the analyzed scenario the average AoI is probabilistically upper bounded by M, whose value should be chosen to obtain a low probability $\mathrm{P}[\Delta_\mathrm{B}(\lambda) > M]$ for either λ close to 0 or 1, and a low probability $\mathrm{P}[\Delta_\mathrm{E}(\lambda) > M]$ for λ close to 0 or μ. We took the expressions of the utilities in (5) in agreement with the utility functions being generally taken as quantities to maximize [34]. However, as will be clear later, this choice is entirely modular, as the tradeoff between the two objectives can be tuned by a specific parameter, and it does not quantitatively affect the result.

Finally, note that setting an upper bound to the AoI at Eve, so that Δ_E saturates to M, implies the existence of a minimum service rate value, below which Δ_E never falls below M. To make our analysis meaningful, it is therefore necessary to choose the value of M opportunely, or, equivalently, to verify the performance of the system only for values of μ above the minimum service rate. Thus, we write the following theorem.

Theorem 1. *For a given M, the minimal service rate μ_0 that guarantees $\Delta_\mathrm{E}(\lambda) < M$ for some $\lambda \in [0,1]$ is*

$$\mu_0 = \frac{\Delta_0}{M}\,, \tag{7}$$

where $\Delta_0 = 3.484$ is the minimal average AoI for a unitary service rate obtained when $\lambda = \rho_0 = 0.531$, as proved in [3].

Proof. Following the results obtained in [3], the load factor that minimizes the average AoI is computed seeking for the only solution in the interval $[0,1]$ of the 4th degree equation $\eta^4 - 2\eta^3 + \eta^2 - 2\eta - 1 = 0$, that is $\eta = \rho_0$, which, for a generic service rate μ at Eve, gives $\Delta_\mathrm{E} = \Delta_0/\mu$. So, in order for our analysis to be meaningful (i.e., Δ_E is not saturated to M for every choice of λ and β), the minimal average AoI must be below M, so the service rate μ must be such that

$$\min_\lambda \Delta_\mathrm{E}(\lambda) = \frac{\Delta_0}{\mu} < M \tag{8}$$

is satisfied. Therefore, the minimal service rate μ_0 is given by (7).

From Alice's perspective, it is beneficial to increase either of utilities u_1 and u_2, or both. However, these are contrasting objectives since Alice cannot prevent Eve's eavesdropping, therefore a packet that is meant to refresh the status at Bob's may also lower Eve's AoI if captured. To combine the two competing utilities of (5), we reformulate the problem defining a new objective function that sets a precise value on the 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 [17], where an ultimate objective function f is chosen as a weighted product between the two utilities u_1 and u_2, i.e., a modified Nash bargaining solution [32]

$$f(\lambda) = [u_1(\lambda)]^{a+1} u_2(\lambda) = \frac{\widetilde{\Delta_{\mathrm{E}}}(\lambda)}{[\widetilde{\Delta_{\mathrm{B}}}(\lambda)]^{a+1}}, \tag{9}$$

with $a \in (0, +\infty)$ being a parameter that controls the trade-off between u_1 and u_2. 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 $\Delta_{\mathrm{E}}(\lambda)$ but would also have $\Delta_{\mathrm{B}}(\lambda)$ 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 $\Delta_{\mathrm{B}}(\lambda)/\Delta_{\mathrm{E}}(\lambda)$ instead of $\Delta_{\mathrm{B}}(\lambda)$ itself. The specific choice of a governs the selection of the optimal point in the Pareto frontier.

3.2. Optimal Offered Load

The full expressions for $\Delta_{\mathrm{B}}(\lambda)$ and $\Delta_{\mathrm{E}}(\lambda)$, considering a unitary service rate for Bob and a service rate indicated by μ for Eve, are computed from (2) as

$$\Delta_{\mathrm{B}}(\lambda) = \begin{cases} 1 + \frac{1}{\lambda} + \frac{\lambda^2}{1-\lambda} & \text{when } \lambda < 1\,, \\ +\infty & \text{otherwise}\,, \end{cases} \tag{10}$$

for the legitimate channel between Alice and Bob, and

$$\Delta_{\mathrm{E}}(\lambda) = \begin{cases} \frac{1}{\mu} + \frac{1}{\beta\lambda} + \frac{\beta^2\lambda^2}{\mu^2(\mu-\beta\lambda)} & \text{when } \beta\lambda < \mu\,, \\ +\infty & \text{otherwise}\,, \end{cases} \tag{11}$$

for the eavesdropper channel between Alice and Eve. The optimal transmission rate λ maximizing the objective $f(\lambda)$, when $\Delta_{\mathrm{B}}(\lambda), \Delta_{\mathrm{E}}(\lambda) < M$, is

$$\begin{aligned} \lambda^{\star} &= \arg\max_{\lambda} f(\lambda) = \arg\max_{\lambda} \frac{\Delta_{\mathrm{E}}(\lambda)}{[\Delta_{\mathrm{B}}(\lambda)]^{a+1}} \\ &= \arg\max_{\lambda} \frac{\frac{1}{\mu} + \frac{1}{\beta\lambda} + \frac{\beta^2\lambda^2}{\mu^2(\mu-\beta\lambda)}}{\left(1 + \frac{1}{\lambda} + \frac{\lambda^2}{1-\lambda}\right)^{a+1}} \\ &= \arg\max_{\lambda} \frac{(\beta^3\,\lambda^3 - \beta^2\,\lambda^2 + \mu^3)\lambda^a\,(1-\lambda)^{a+1}}{\beta\,\mu^2\,(\mu - \beta\,\lambda)\,(\lambda^3 - \lambda^2 + 1)^{a+1}}\,. \end{aligned} \tag{12}$$

One can solve (12) by computing the derivative of $f(\lambda)$. Notably, when $\beta \to 0^+$, the derivative $f'(\lambda)$ approaches

$$f'(\lambda) \to \frac{g(\lambda)(\lambda - \lambda^2)^a}{\lambda\,\beta\,(\lambda^3 - \lambda^2 + 1)^{a+2}}\,, \tag{13}$$

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

$$g(\lambda) = (a+2)(\lambda^4 - 2\lambda^3 + \lambda^2) - (2a+1)\lambda + a. \tag{14}$$

Therefore, when $\beta \to 0^+$, the optimal load factor at the limit is obtained as the only real solution of $g(\lambda) = 0$ in the interval $(0,1)$. The function $g(\lambda)$ is continuous in the interval $(0,1)$ and takes values of opposite sign at the boundaries

$$g(0) = a > 0, \tag{15}$$

$$g(1) = -(a+1) < 0. \tag{16}$$

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

$$g'(\lambda) = 2\lambda(a+2)(\lambda-1)(2\lambda-1) - 2a - 1\,, \tag{17}$$

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

$$3(\lambda^2 - 2)(\lambda^2 + 1) + 1 = 0\,, \tag{18}$$

and the solution is found at $\lambda \approx 0.389$.

When $\Delta_{\mathrm{E}} > M$ and $\Delta_{\mathrm{B}} < M$, then

$$\lambda^{\star} = \arg\max_{\lambda} \frac{M}{\Delta_{\mathrm{B}}(\lambda)^{a+1}} = \arg\min_{\lambda} \Delta_{\mathrm{B}} = 0.531\,, \tag{19}$$

where the last step follows from the results in [3]. In the opposite case, in which $\Delta_{\mathrm{E}} < M$ and $\Delta_{\mathrm{B}} > M$, we have

$$\lambda^{\star} = \arg\max_{\lambda} \frac{\Delta_{\mathrm{E}}(\lambda)}{M^{a+1}} = \arg\max_{\lambda} \Delta_{\mathrm{E}}(\lambda) = 0\,. \tag{20}$$

Note that it may be convenient for Alice to saturate the value of $\widetilde{\Delta_{\rm E}}$, i.e., obtain the highest possible value $\widetilde{\Delta_{\rm E}} = M$, while keeping $\Delta_{\rm B} < M$, when possible, as better explained by the following theorems. We remark that the value of $\widetilde{\Delta_{\rm E}}$ can be saturated by choosing a high or low enough transmission rate only when Eve's queuing system is M/M/1 with FCFS policy, and there is no preemption or packet dropping.

Theorem 2. *Given the system parameters M and a, for every $\mu > \mu_0$ as derived in Theorem 1, there exist two values of η such that $\widetilde{\Delta_{\rm E}} = M$. We indicate with $\eta^- \in [0, \rho_0)$ and $\eta^+ \in (\rho_0, 1]$ these two values, and we have that*

$$\widetilde{\Delta_{\rm E}}(\lambda) = M \iff \eta \in [0, \eta^-] \cup [\eta^+, +\infty) \,. \tag{21}$$

To each value of η^- and η^+ are associated two functions, respectively,

$$\lambda^-(\beta) = \frac{\mu\eta^-}{\beta}\,, \quad \lambda^+(\beta) = \frac{\mu\eta^+}{\beta}\,, \tag{22}$$

such that, for a given β,

$$\Big(\lambda = \lambda^-(\beta)\Big) \vee \Big(\lambda = \lambda^+(\beta)\Big) \Rightarrow \widetilde{\Delta_{\rm E}}(\lambda) = M\,, \tag{23}$$

Proof. We can equivalently express $\Delta_{\rm E}(\lambda)$ as a function of η instead of λ, and we have that $\Delta_{\rm E}(\eta)$ is a convex function of η in the interval $[0, 1]$, with minimum for $\eta = \rho_0$ and $\Delta_{\rm E}(\eta) \to \infty$ at the boundaries. Moreover, $\mu < \mu_0$ guarantees that $\Delta_{\rm E}(\eta) < M$ for some $\eta \in (0, 1)$. Thus, $\eta^- \in [0, \rho_0)$ and $\eta^+ \in (\rho_0, 1]$ always exist. Moreover, given η^- and η^+, the transmission rates $\lambda^-(\beta)$ and $\lambda^+(\beta)$ that guarantees $\Delta_{\rm E} = M$ are obtained from $\eta^- = \beta\lambda^-/\mu$ and $\eta^+ = \beta\lambda^+/\mu$, respectively.

Furthermore, we observe that there are certain conditions on β and μ for which the optimal transmission rate is ρ_0 (i.e. Bob's optimal transmission rate in the absence of Eve) that allows for the lowest value Δ_0 for his average AoI. These conditions are summarized in the following theorem.

Theorem 3. *Given M, the optimal transmission rate is $\lambda^\star = \rho_0$ when any of the following conditions is met:*

a) $(\beta = \mu) \wedge (\mu \leq 1)\,,$
b) $\beta \leq \beta^- = \mu\eta^-/\rho_0\,,$
c) $(\beta \geq \beta^+ = \mu\eta^+/\rho_0) \wedge (\mu \leq \rho_0)\,,$

where a) yields to $\widetilde{\Delta_{\rm E}}(\lambda^\star) = \widetilde{\Delta_{\rm B}}(\lambda^\star) = \Delta_0$, while when b) or c) hold we have $\widetilde{\Delta_{\rm E}}(\lambda^\star) = M$ (i.e., Eve's AoI saturates to the highest possible value) and $\widetilde{\Delta_{\rm B}}(\lambda^\star) = \Delta_0$ (i.e., the lowest possible value for Bob's AoI).

Proof. Concerning condition a), from (12), considering $\mu = \beta$, we obtain

$$\lambda^\star = \arg\max_{\lambda} \frac{1}{\beta}\frac{1}{\Delta_{\rm B}(\lambda)^a} = \arg\min_{\lambda} \Delta_{\rm B}(\lambda) = \rho_0\,, \tag{24}$$

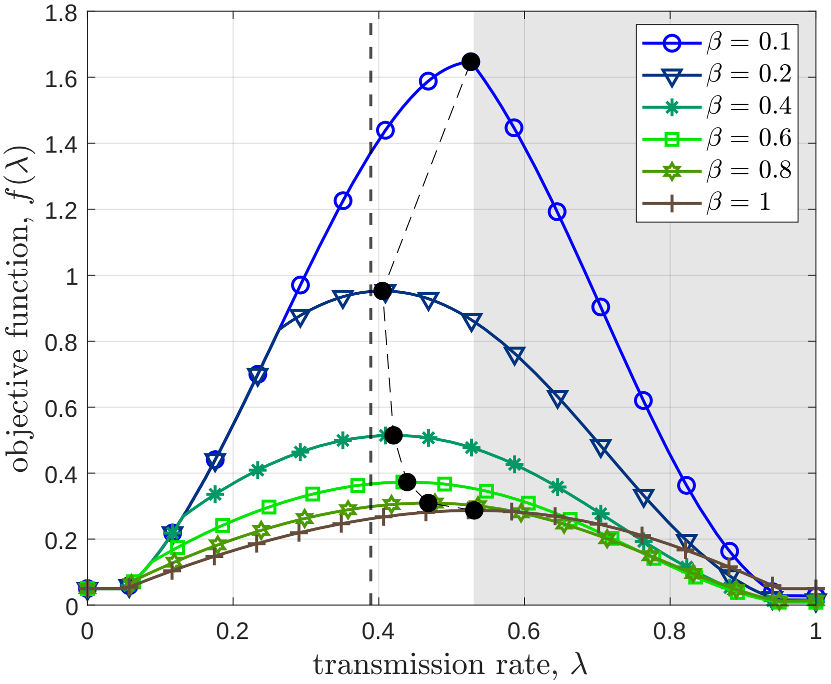

Figure 3: Objective $f(\lambda)$, as a function of the transmission rate λ, for different values of eavesdropping probability β, with weight $a = 1$ and $M = 20$. The black line connects the maximizing points $\lambda^\star$. The dashed black line reports $\lambda = 0.389$.

and $\eta = \beta\lambda^\star/\mu = \lambda^\star = \rho_0$, which implies $\widetilde{\Delta_{\mathrm{E}}}(\lambda^\star) = \widetilde{\Delta_{\mathrm{B}}}(\lambda^\star) = \Delta_0$. Instead, for condition b) we have that for any value of μ there exists a low enough value β^- of the eavesdropping probability below which Alice acts as Eve is not present. This value can be found solving $\lambda^- = \mu\eta^-/\beta = \rho_0$, for β that gives $\beta^- = \mu\eta^-/\rho_0$. Similarly, for c) we find β^+ from $\lambda^+ = \mu\eta^+/\beta = \rho_0$.

4. Numerical Results

In this section, we present quantitative evaluations to express the consequences of what has been derived in Section 3 for a scenario involving the interplay of Alice, Bob, and Eve.

We assume that the only active agent is Alice, who also knows the eavesdropping probability β. At first, we study the case where the service rates of Bob and Eve are the same, with both unitary values. Then, we consider the case where Eve's normalized service rate μ is different from that of Bob, and we analyze both situations of $\mu < 1$ and $\mu > 1$.

4.1. Equal service rate

We discuss how the optimal transmission probability $\lambda^\star$, obtained maximizing the objective function $f(\lambda)$ in (12), is influenced by Eve's probability of data capture β and the trade-off parameter a when $\mu = 1$.

If Eve does not intercept any packet, i.e., $\beta = 0$, we expect $\lambda^\star = 0.531$, which is the AoI minimizing value for the transmission probability with normalized service capacity [3]. When each packet is independently eavesdropped with probability $\beta > 0$, and $\mu = 1$, we expect that the optimal transmission probability decreases, therefore $\lambda^\star \leq 0.531$ for any value of β. For this reason, in the results that follow, the areas corresponding to $\lambda^\star > 0.531$ are shaded.

Figure 3 shows the objective function $f(\lambda)$, as a function of λ for different values of β when $a = 1$. The black line connects the maximum point of each curve, reached when $\lambda = \lambda^\star$, while the dashed black line reports the value $\tilde{\lambda} = 0.389$. First of all, the curves are bell-shaped with a very pronounced maximum when β is small. When β rises, the curves get flatter; in fact, when β tends to 1, Δ_{B} and Δ_{E} get closer, and Alice has narrower margins to trade between these objectives. When $\lambda = 1$, all the curves go to zero. As the black line in Figure 3 shows, the value of $\lambda^\star$ tends to 0.531 as β increases, and decreases with β, tending towards the vertical asymptote at $\lambda < 0.531$, displayed as the black dashed line in the figure, whose numerical value is the solution of (17). However, when β is very low, $\lambda^\star = \rho_0$, as anticipated in point b) of Theorem 3. For the specific case of this figure where $a = 1, \mu = 1$, the asymptotic value shown by the vertical dashed line is $\tilde{\lambda} = 0.389$.

Interestingly, the lower β, the lower $\lambda^\star$, which, at first glance, may seem counterintuitive, yet this behavior has the following explanation. If β tends to 1 the eavesdropper intercepts almost every packet transmitted by Alice, so the only sensible objective for Alice is to keep Δ_{B} low, which is achieved by choosing $\lambda = 0.531$. If β decreases, the second objective takes over, and Alice transmits less frequently, choosing $\lambda < 0.531$, to prevent Eve from intercepting. However, when $\beta \leq \beta^-$, Bob saturates Eve's AoI choosing $\lambda^\star = \rho_0$, as pointed out in Theorem 3. In particular, for $\mu = 1$ we have $\eta^- = 0.0531$, so $\beta^- = 0.1$. Above all, if Δ_{B} is low and Δ_{E} high, Alice should wait before transmitting a new packet because the effect can be to reset both Δ_{B} and Δ_{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 Δ_{B} and Δ_{E}. Yet, it is expected that in a stateful optimization [7, 15] (left for future research) this phenomenon will be seen with even more clarity.

Fig. 4 shows the optimal transmission probability $\lambda^\star$ as a function of β, for different values of a. One can see that the optimal value $\lambda^\star$ moves toward $\lambda^-(\beta) = \eta^-/\beta$ when a tends to zero, for every value of β, provided it is less than 1. 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 more rarely and, thus, saturate Eve's average AoI. Conversely, when the value of a rises, $\lambda^\star$ tends to 0.531 for every β. When $\beta = 1$, $\lambda^\star = 0.531$ for all $a > 0$.

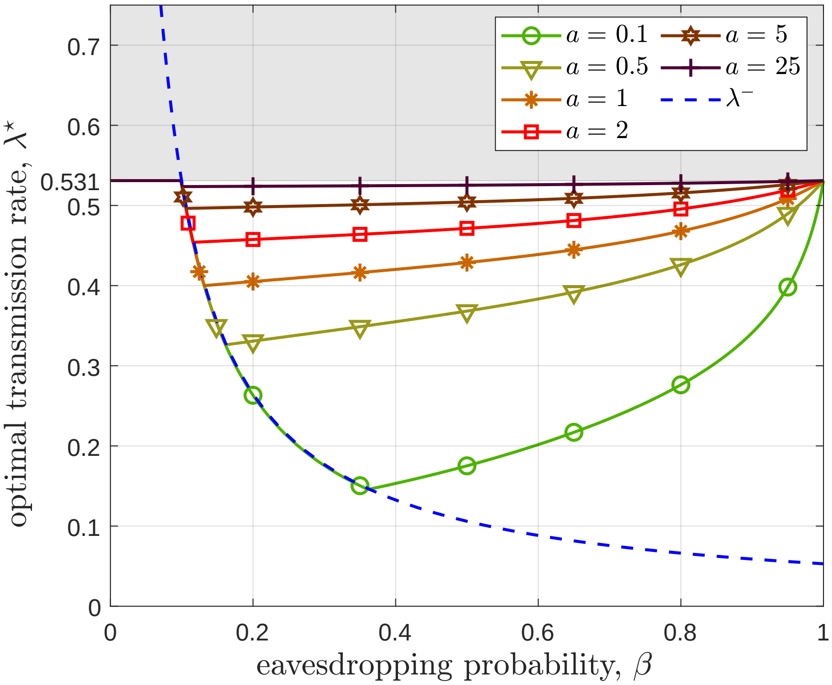

Figure 4: Optimal transmission probability $\lambda^{\star}$, as a function of capture probability β, for equal service rates $\mu = 1$, different values of weight a and $M = 20$.

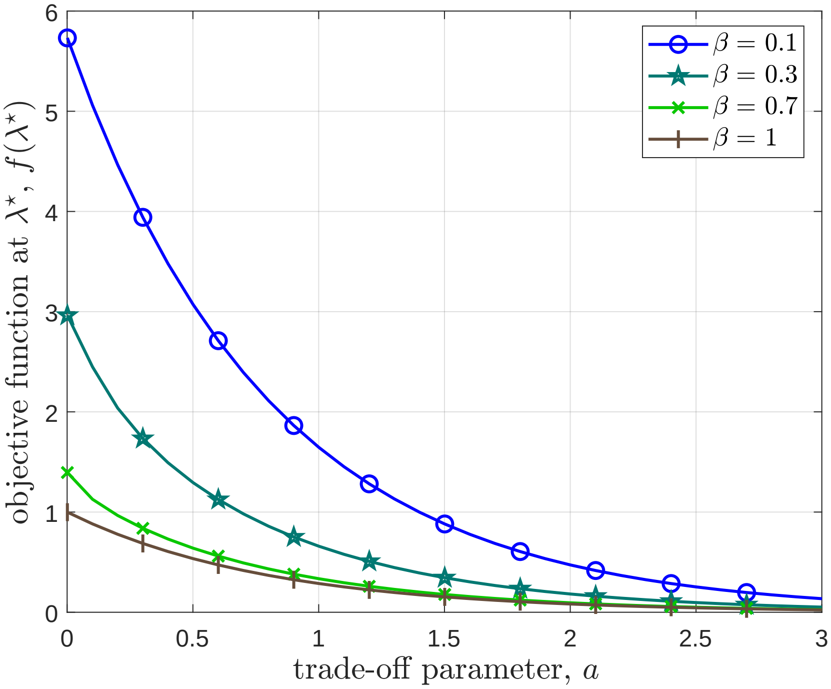

Figure 5: Objective function $f(\lambda)$ evaluated at the optimal transmission rate $\lambda^\star$, as a function of weight a, for equal service rates $\mu = 1$, different eavesdropping probabilities β and $M = 20$.

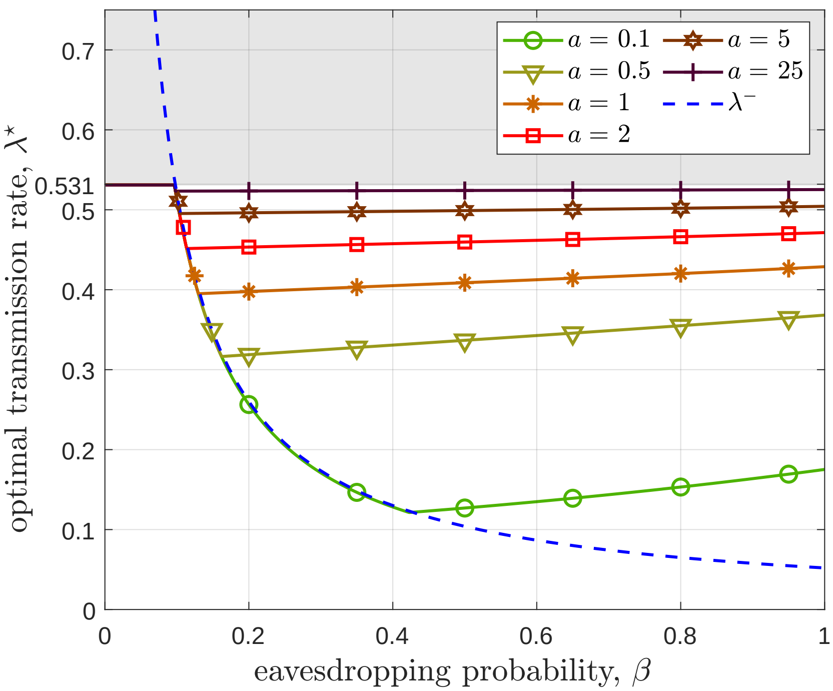

Figure 6: Optimal transmission rate $\lambda^\star$, as a function of the capture probability β, for different values of weight a, with service rate at Eve $\mu = 2$ and $M = 20$.

Fig. 5 shows the objective function $f(\lambda)$ evaluated at the optimal transmission rate $\lambda^\star$, as a function of a, for different values of β. Since $\beta^- = 0.1$, all the curves for $\beta < \beta^-$ are identical to that for $\beta = 0.1$ (the blue curve), that is

$$\beta \leq \beta^- \Rightarrow f(\lambda^\star) = f(\rho_0) = \frac{\Delta_0}{M^{a+1}}\,. \tag{25}$$

4.2. Higher eavesdropper service rate

When the service rate μ at Eve's queue is higher than Bob's service rate, i.e., $\mu > 1$, then as β tends to 1, there is no value of $\lambda \in [\lambda^+, 1]$ such that $\widetilde{\Delta_{\mathrm{E}}} = M$. This happens because Eve's queue is always faster than Bob's, and therefore, even when β is high, the latter cannot make Δ_{E} saturate while at the same time keeping his queue stable.

Figure 6 shows the optimal transmission rate $\lambda^\star$, as a function of the capture probability β, for different values of a, with service rate at Eve $\mu = 2$ and $M = 20$. We see that, for $\beta = 1$, the curves do not converge to the point $(1, 0.531)$ and are more flat than those in Figure 4. Moreover, the optimal transmission rate $\lambda^\star$ is strictly below ρ_0 for every $\beta > \beta^- = 0.098$. When $\beta \leq \beta^-$, we have that $\lambda^\star = \rho_0$, as proved in Theorem 1. Finally, when β is low, then $\lambda^\star$ is equal to λ^-, depicted by the blue dashed curve. Also $\lambda^\star$ moves toward the $\lambda^-(\beta)$ curve when a goes to zero, for every $\beta > \beta^-$.

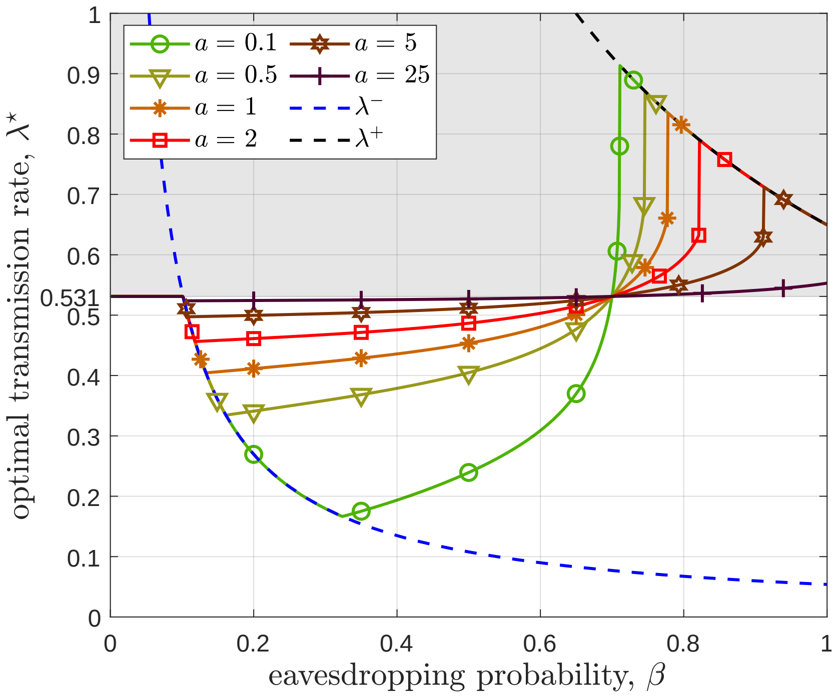

Figure 7: Optimal transmission rate $\lambda^\star$, as a function of capture probability β, for different values of weight a, with service rate at Eve $\mu = 0.7$ and $M = 20$.

4.3. Lower eavesdropper service rate

We analyze the case when Eve's service rate μ is lower than Bob's service rate, i.e., $\mu < 1$. Since in Theorem 3, the condition c) is valid only when $\mu < \rho_0$, we distinguish between two operational cases, $\mu = 0.7$ and $\mu = 0.4$.

Figures 7 and 8 show the value of $\lambda^\star$, as a function of the eavesdropping probability β, for different values of a, $M = 20$, and when Eve's service rate is, respectively, $\mu = 0.7$ and $\mu = 0.4$. As proved in Theorem 3, and as already shown for $\mu \geq 1$, we have that for $\beta < \beta^-$ the optimal transmission rate is $\lambda^\star = \rho_0$. The values of β^- for $\mu = 0.7$ and $\mu = 0.4$ are, respectively, 0.102 and 0.108. In both figures, we can see that the optimal transmission rate coincides with ρ_0 also when $\beta = \mu$, as proved in Theorem 3, and in this case $\widetilde{\Delta_\mathrm{E}}(\lambda^\star) = \widetilde{\Delta_\mathrm{B}}(\lambda^\star) = \Delta_0$.

When $\mu = 0.7$, from Figure 7 we see that as a tends to zero, the value of $\lambda^\star$ tends to $\lambda^-(\beta)$ for $\beta \in (\beta^-, \mu)$, and to $\lambda^+(\beta)$ for $\beta \in (\mu, 1]$. We note a similar behavior when $\mu = 0.4$. In fact, from Figure 8, we note that $\lambda^\star$ tends to $\lambda^-(\beta)$ for $\beta \in (\beta^-, \mu)$, and to $\lambda^+(\beta)$ for $\beta \in (\mu, \beta^+)$, with $\beta^+ = 0.656$[3]. For $\beta \geq \beta^+$ the optimal transmission rate is $\lambda^\star = \rho_0$. Thus, when Eve's service

[3] We remark that $\mu = 0.4$ is the only case among the analyzed ones, where $\beta^+ \leq 1$. In fact, a sufficient condition to obtain $\beta^+ \leq 1$ is $\mu \leq \rho_0$.

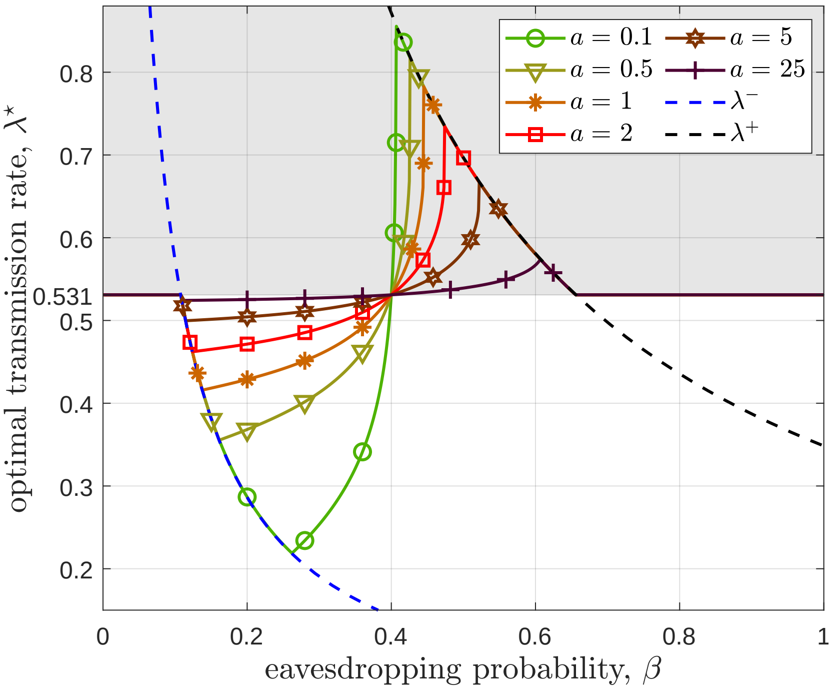

Figure 8: Optimal transmission rate $\lambda^\star$, as a function of capture probability β, for different values of weight a, with service rate at Eve $\mu = 0.4$ and $M = 20$.

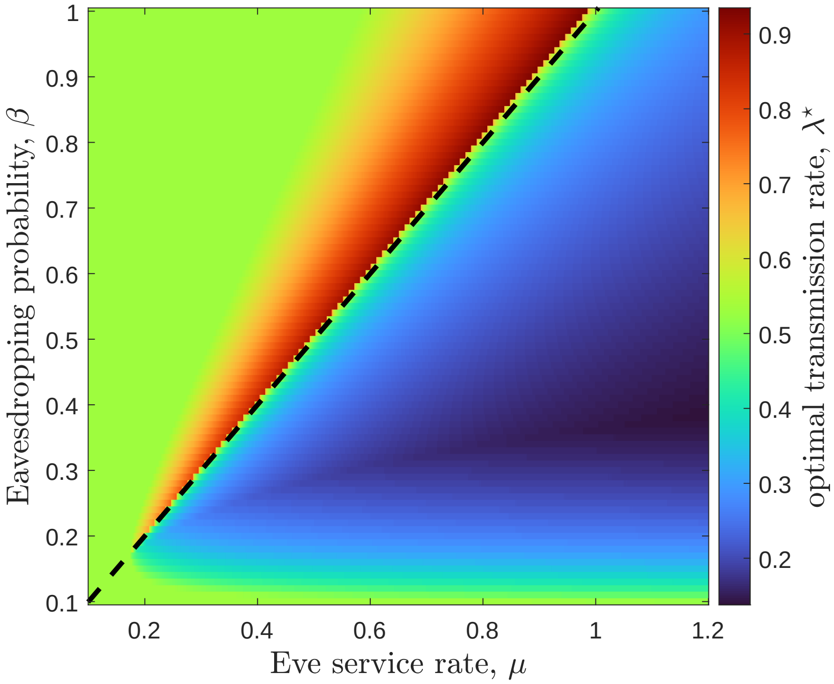

Figure 9: Optimal transmission rate $\lambda^\star$, for different values of the eavesdropping probability β and Eve's service rate μ, for $a = 0.1$ and $M = 20$. The dashed line represents $\beta = \mu$.

rate is lower than ρ_0, Bob's can saturate Eve's average AoI and obtain the best possible average AoI for his queue, when the eavesdropping probability is either sufficiently low or sufficiently high, i.e., $\beta \in [0, \beta^-] \cup [\beta^+, 1]$.

4.4. Comparison

Finally, we compare the optimal transmission rate obtained with different values of the eavesdropping probability β and Eve's service rate $\mu \in [0.1, 1.2]$. Figure 9 shows $\lambda^\star$, for different values of β and μ, when $a = 0.1$ and $M = 20$. The dashed line represents $\beta = \mu$. We can see that for $\mu < 0.2$ Bob chooses to transmit with $\lambda^\star = \rho_0$ for any β. This is due to the notably low service rate of Eve. Consequently, Eve does not pose any substantial threat to Alice and Bob. In response, Alice tends to overlook her presence and opts to transmit with the optimal λ in the absence of Eve. When μ increases, Bob chooses $\lambda^\star = \rho_0$ only for $\beta = \mu$, or for sufficiently high or low eavesdropping probability, i.e., $\beta \leq \beta^- \wedge \beta \geq \beta^+$. Indeed, when $\beta = \mu$, the offered load at Bob and Eve is equivalent. Consequently, Alice ignores Eve and transmits at rate ρ_0. This pattern also holds for extremely low β, where Eve's presence holds little concern for Alice, as well as for exceedingly high β, where Eve eavesdrops numerous packets. In such a scenario, Alice finds herself unable to mitigate this effect, leading her to focus solely on optimizing Bob's AoI. Lower values for the

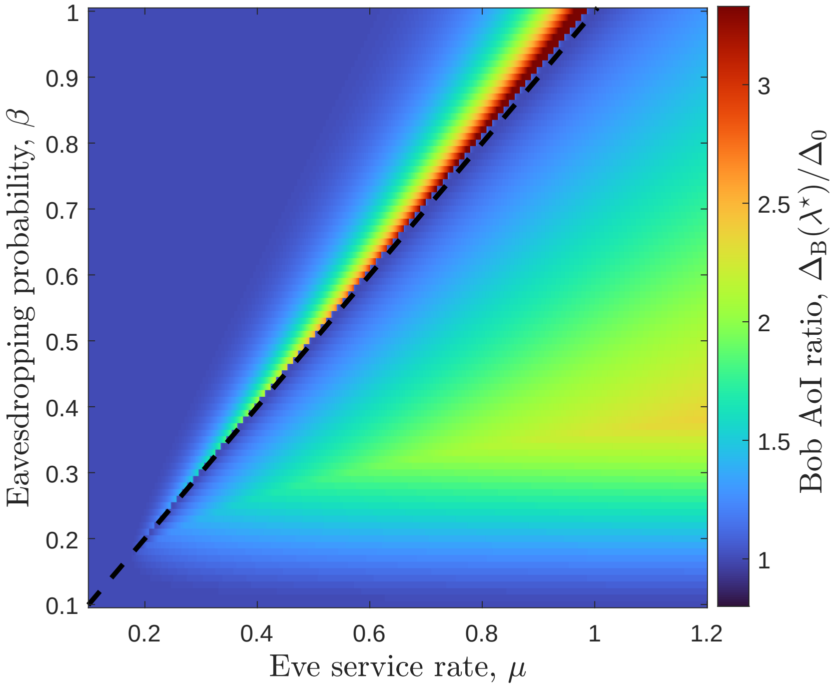

Figure 10: Ratio between Bob's average AoI $\Delta_\mathrm{B}(\lambda^\star)$ and Δ_0, for different values of the eavesdropping probability β and Eve's service rate μ, for $a = 0.1$ and $M = 20$. The dashed line represents $\beta = \mu$.

transmission rate are chosen by Bob when $\mu < \beta$, while higher values are chosen when $\mu > \beta$.

A similar observation arises looking at Figure 10, which shows the ratio between Bob's average AoI, i.e., $\Delta_\mathrm{B}(\lambda^\star)/\Delta_0$, for different values of the eavesdropping probability β and Eve's service rate μ, when $a = 0.1$ and $M = 20$. A high value of the ratio means that the performance achieved by Bob in terms of average AoI is degraded by the presence of Eve. We see that, when Bob chooses $\lambda^\star = \rho_0$, the ratio is 1, while when $\lambda^\star$ differs from the optimal one in the absence of Eve the ratio value increases and, therefore, the performance is worse. Finally, from Figure 10 we note that the average AoI at the legitimate receiver is degraded with respect to the case where no eavesdropper is present, and the impact of this is strongest when the service rate of Eve is approaching the eavesdropping probability (from the left).

5. Conclusions

We have analyzed a scenario of status updates between a transmitter and a legitimate receiver, considering the presence of an eavesdropper that is sometimes able to intercept data packets. For this purpose, we leveraged existing analytical results for queuing systems [3, 20], where AoI is computed as a function of the data injection rate by the transmitter.

We assume that the transmitter is aware of the eavesdropper and wants to set an efficient injection rate that simultaneously achieves low AoI at the intended receiver but keeps the eavesdropper information stale. To analyze this problem, we propose to combine both objectives according to a Bergson social welfare framework [17], and have solved the problem of finding the optimal transmission probability as a function of the probability of data capture by the eavesdropper.

The main conclusion is that the additional objective of leaking only stale information to the eavesdropper can be achieved with a proper remodulation of the data injection rate by the transmitter [14]. Specifically, when the primary objective of the transmitter is to thwart the eavesdropper, the transmission probability approaches zero, even for minimal probabilities of data capture by the eavesdropper. Furthermore, in scenarios where the service rate at the eavesdropper matches the eavesdropping probability, or when the eavesdropping probability is extremely high or low, the transmitter opts to ignore the eavesdropper's presence. This decision results in achieving an optimal transmission rate equivalent to the one in the absence of Eve. Moreover, the performance in terms of AoI at the legitimate receiver is degraded most with respect to the nominal case when the eavesdropper service rate is slightly below the eavesdropping probability.

The present framework can be used as an adjustable approach for different cases of interest in practical contexts. For instance, it can be open to game theoretic extensions [25], where the strategic behavior of the transmitter and/or the eavesdropper can be analyzed.

Acknowledgment

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE0000001 - program "RESTART").

References

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

[2] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, S. Ulukus, Age of information: An introduction and survey, IEEE J. Sel. Areas Commun. 39 (5) (2021) 1183–1210.

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

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

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

[6] A. Zancanaro, A. Munari, G. Cisotto, L. Badia, Impact of transmission delays over age of information under finite horizon scheduling, in: Proc. IEEE CAMAD), 2023.

[7] A. Munari, L. Badia, The role of feedback in AoI optimization under limited transmission opportunities, in: Proc. IEEE Globecom, 2022.

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

[9] J. P. Champati, R. R. Avula, T. J. Oechtering, J. Gross, Minimum achievable peak age of information under service preemptions and request delay, IEEE J. Sel. Areas Commun. 39 (5) (2021) 1365–1379.

[10] A. Munari, Modern random access: an age of information perspective on irregular repetition slotted ALOHA, IEEE Trans. Commun. 69 (6) (2021) 3572–3585.

[11] L. Badia, A. Zanella, M. Zorzi, A game of ages for slotted ALOHA with capture, IEEE Trans. Mobile Comput. (2024). doi:10.1109/TMC.2023.3298716.

[12] M. Costa, M. Codreanu, A. Ephremides, On the age of information in status update systems with packet management, IEEE Trans. Inf. Theory 62 (4) (2016) 1897–1910.

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

[14] F. Yuan, S. Tang, D. Liu, AoI-based transmission scheduling for cyber-physical systems over fading channel against eavesdropping, IEEE Internet Things J. (2023). doi:10.1109/JIOT.2023.3307351.

[15] H. Chen, Q. Wang, P. Mohapatra, N. Pappas, Secure status updates under eavesdropping: Age of information-based physical layer security metrics, arXiv (2020).
URL https://arxiv.org/abs/2002.07340

[16] Y. Zou, J. Zhu, X. Wang, L. Hanzo, A survey on wireless security: Technical challenges, recent advances, and future trends, Proc. IEEE 104 (9) (2016) 1727–1765.

[17] A. Bergson, A reformulation of certain aspects of welfare economics, Quart. J. Econ. 52 (2) (1938) 310–334.

[18] M. Moltafet, M. Leinonen, M. Codreanu, Average AoI in multi-source systems with source-aware packet management, IEEE Trans. Commun. 69 (2) (2020) 1121–1133.

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

[20] R. D. Yates, S. K. Kaul, The age of information: Real-time status updating by multiple sources, IEEE Trans. Inf. Theory 65 (3) (2018) 1807–1827.

[21] R. Talak, E. H. Modiano, Age-delay tradeoffs in queueing systems, IEEE Trans. Inf. Theory 67 (3) (2020) 1743–1758.

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

[23] S. Banerjee, S. Ulukus, Age of information in the presence of an adversary, in: Proc. IEEE Infocom Wkshps, 2022.

[24] Y. Xiao, Y. Sun, A dynamic jamming game for real-time status updates, in: Proc. IEEE Infocom Wkshps, 2018, pp. 354–360.

[25] L. Crosara, N. Laurenti, L. Badia, Strategic status updates in an eavesdropping game, in: Proc. European Wireless, 2023.

[26] A. Garnaev, W. Trappe, The eavesdropping and jamming dilemma in multi-channel communications, in: Proc. IEEE ICC, 2013, pp. 2160–2164.

[27] X. Wang, L. Liu, L. Zhu, T. Tang, Joint security and QoS provisioning in train-centric CBTC systems under sybil attacks, IEEE Access 7 (2019) 91169–91182.

[28] T. Jing, H. Yu, X. Wang, Q. Gao, Joint timeliness and security provisioning for enhancement of dependability in Internet of Vehicle system, Int. J. Distrib. Sens. Netw. 18 (6) (Jun. 2022).

[29] A. Asheralieva, D. Niyato, Optimizing age of information and security of the next-generation Internet of everything systems, IEEE Internet Things J. 9 (20) (2022) 20331–20351.

[30] Y. Wang, S. Yan, W. Yang, Y. Cai, Covert communications with constrained age of information, IEEE Wireless Commun. Letters 10 (2) (2020) 368–372.

[31] S. S. Hosseini, P. Azmi, N. Mokari, Minimizing average age of information in reliable covert communication on time-varying channels, IEEE Trans. Veh. Technol. (2023). doi:10.1109/TVT.2023.3303674.

[32] J. F. Nash, Jr, The bargaining problem, Econometrica 18 (2) (1950) 155–162.

[33] Y. Zhu, L. Wang, K.-K. Wong, R. W. Heath, Secure communications in millimeter wave ad hoc networks, IEEE Trans. Wireless Commun. 16 (5) (2017) 3205–3217.

[34] L. Badia, M. Zorzi, On utility-based radio resource management with and without service guarantees, in: Proc. ACM MSWiM, 2004, pp. 244–251.