Leaked Age of Information of Preemptive Status Updates Against a Preemptive Eavesdropper

Pietro Meneghini and Leonardo Badia
Dept. Information Engineering, University of Padova, 35131 Padua, Italy
Email: pietro.meneghini.1@studenti.unipd.it, leonardo.badia@.unipd.it

***Abstract*—We consider a communication system where preemptive status updates are exchanged with a general objective of data freshness, e.g., for real-time industrial applications. The transmitter-receiver pair (Alice and Bob) is threatened by an eavesdropper (Eve) that probabilistically intercepts some of the exchanged messages. We model the system performance through the average age of information (AoI), leveraging known results from queueing theory. Alice tunes the status update generation according to a tradeoff between achieving low average AoI at Bob's side, while at the same time keeping Eve with stale leaked information. Unlike existing investigations, we focus on the case where preemption of status updates is performed by both receivers (legitimate or not), so that the considered queues are classified as M/M/1*, and we present the performance evaluation to include both freshness and confidentiality considerations.**

***Index Terms*—Age of information; Eavesdropping; Cybersecurity; Queueing theory.**

I. Introduction

Age of information (AoI) is a metric used to assess data freshness, defined as the time elapsed since the most recently received update was generated stated in [1]. When a monitor receives an update generated at time $\sigma(t)$, the AoI is [2]

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

This expression captures the information freshness, in that, if the monitor's last update is very recent, $\delta(t)$ will be small. AoI grows linearly with time and, whenever an update is generated and received, it resets to zero. We also assume, as commonly done in the literature, zero propagation delay, so whenever an update is generated from the transmitter, it is received immediately without delay, which then brings fresh information [3]. In [1] and [2] it is highlighted how AoI is different from traditional delay metrics, as it captures both the inter-update timing, as well as the service delays, providing a more complete definition of timeliness.

The concept of AoI has found application in a wide variety of fields such as e-health [4], satellite communications [5], smart agriculture [6], smart grids [7]. Yet, one of the most interesting concept is that of industrial applications [8], where strict delay constraints often lead to preemption policies in the queue to ensure timely delivery.

This work was supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP D33C22001300002, PE00000014 – program "SEcurity and RIghts in the CyberSpace" (SERICS), Spoke 4 - project "Innovative Security Paradigms for beyond 5G" (ISP5G+).

System characterization through AoI has led to a renewed interest in queueing theory, which allows for analytical evaluations. Indeed, age-related metrics have been derived for a number of different queueing systems, starting from the basic evaluations such as the average AoI of a first-come-first-served (FCFS) M/M/1 queue already explored in seminal papers [1].

Although other evaluations including peak AoI [9] or AoI violation probabilities [10] are also possible, in this paper we will concentrate on the average AoI, which we will refer to as Δ, and we will connect to queueing parameters such as the transmission rate λ, and the service rate μ. In [1], it is highlighted that to minimize the average AoI, an optimal offered load ($\rho = \lambda/\mu$) can be found. If alternative types of queue are chosen to describe Δ, different optimal values of ρ can be derived. In the M/M/1 case, for example, the optimal load ρ^* is found to be at $\rho \approx 0.531$. However, this no longer holds true if preemption is adopted by the monitor to only exploit the most recent update in the queue, and the queue becomes what [2] denotes as an M/M/1* queue. This may be actually more realistic in industrial scenario where status updates are usually tracked to notify working conditions and therefore preemption is useful to guarantee better system responsiveness [11].

In this paper, we apply such characterizations of AoI in queueing systems to a problem that in a way is similar to that outlined in [12], [13]. We consider a transmitter owned by Alice sending status updates to a legitimate receiver Bob. An eavesdropper, Eve, is present and is able to capture Alice's information with probability $\beta \in [0, 1]$. We assume that Alice knows about the presence of Eve and also knows the value of the eavesdropping probability β. We further suppose that every packet transmitted by Alice is successfully received by Bob. Alice tries to set a suitable transmission rate λ to find the best trade-off between trying to minimize Bob's AoI, while keeping Eve's updates as stale as possible, thus maintaining a tradeoff between freshness and confidentiality. However, while all previous papers refer to a more traditional M/M/1 queue, we consider that both Bob and Eve adopt preemption on their received updates, thus making them the end point of two M/M/1* queues.

For example, this approach can find practical implementations in remote industrial control systems (e.g., SCADA and industrial IoT) [14]. Sensor readings and control commands in such systems typically require submillisecond latencies,

which are usually exchanged through encrypted wireless links to ensure confidentiality [15]. Using preemptive queueing, the legitimate controller always sees the most up-to-date information, keeping its age of information at minimum [16]. Meanwhile, if an eavesdropper (Eve) captures these encrypted packets, the approach proposed in this paper allows more control to maintain a desired freshness gap between the controller and interceptor. In fact, optimizing the update rate guarantees that Bob's data is always ahead of Eve's, thus naturally improving secrecy of industrial communications.

To exploit the balance between the two contrasting goals, we will use an objective function derived from Bergson's social welfare theory [17]. This will allow us to derive with closed form solutions the optimal load factor ρ^*, thus finding the best strategies to maintain both quality and confidentiality in the communication scenario considered.

Lastly, we will discuss a sensitivity analysis by observing how the optimal offered load ρ^* behaves as the other parameters that characterize the change in the objective function.

II. Background

The derivations in [1], [2], and [18] contain closed-form expressions for the average AoI in queueing systems as a function of the transmission rate λ, service rate μ, with stability of the system ensured if $\rho = \lambda/\mu < 1$. In the present paper, we focus on a last-come-first-served (LCFS) M/M/1 queue with preemptive service policy, denoted as M/M/1* [2]. This means that any new update packet preempts any other packet currently in service, effectively discarding it. That is, the total number of packets in the system is at most one [19].

Our industrial communication scenario follows the representation of Fig. 1, where update packets sent by Alice to Bob can also be intercepted by an unauthorized eavesdropper, Eve, according to an independent and identically distributed binomial variable with probability β. We assume that both Bob and Eve are the end point of a queue with average service time $1/\mu$ and i.i.d. interarrival time with expected value $1/\lambda$. We treat AoI as a random process, thus allowing to define the average AoI as $\Delta = \mathbb{E}[\delta(t)]$. For the M/M/1* case, Δ can be computed as [2], [18], [20]

$$\Delta_{\text{M/M/1}^*} = \frac{1}{\mu}\left(1 + \frac{1}{\rho}\right). \tag{2}$$

This expression is minimized whenever $\rho \to 1^-$, which shows that we have optimal average AoI for a load $\rho \approx 1$. Such behavior means that in order to minimize $\Delta_{\text{M/M/1}^*}$ the transmitter has to continuously send updates, which is really different from the optimal and less aggressive strategy than ought to be used in an FCFS M/M/1 queue.

Recent research is linking the concept of AoI with security in networks where eavesdroppers might be present, therefore considering "Leaked AoI" as the freshness of information available to the unauthorized eavesdropper. The general strategy is to try to maintain high AoI at the eavesdropper's side. Complemented with traditional security measures such as encryption [21] or digital signatures [22], this represents a more basic way of not divulging confidential information.

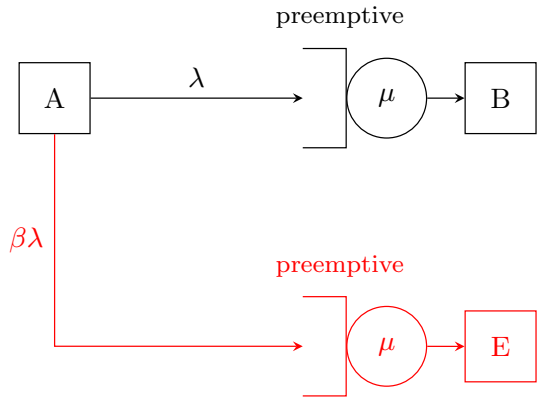

Fig. 1. Preemptive network setup with an empty queue: A queuing system comprising a transmitter (A), a legitimate receiver (B), and an eavesdropper (E). The figure illustrates that the queue remains empty; at any given time, only one client is present in the system, which is the one being served.

In [23], the authors study how to keep status updates secure under passive eavesdropping. They propose two new secrecy metrics based on age of information: Secrecy Age and Secrecy Age Outage Probability. To analyze the introduced metrics, a two-dimensional Markov chain is used, thanks to which they derive closed-form expressions for secrecy performance, further validating them through simulations.

The authors of [24] considered instead the perspective of the freshness advantage of the legitimate transmitter; in other words, they quantify through some closed form derivation the difference of AoI between an eavesdropper and the legitimate receiver, and implicitly assume it as a target of an optimization.

To optimize the freshness, security, and resilience of information in Internet of Everything (IoE) systems, in [25], AoI is incorporated with a two-layer scheduling according to an optimization framework that reduces delays and handles unpredictable edge device performance, also similar to [26]. With a machine learning system based on Bayesian reinforcement learning and a deep learning algorithm, optimal system strategies are derived.

Game-theoretical approaches have also been used on this matter. In [27], with a method and considerations similar to the present paper, the authors consider a setup with Alice, Bob, and Eve, with the aim of finding a suitable trade-off to maintain both efficiency and confidentiality in the channel. The system is modeled as an M/M/1 queue, framing the interaction between the transmitter and the eavesdropper as a static adversarial game of complete information, deriving analytical expressions to capture strategic behavior of the two players. Paper [28] extends this idea in a scenario in which two senders are considered sharing a common legitimate receiver. In this dual-sender setup, the transmitters must not only keep the updates secure from an eavesdropper but also compete with each other for limited channel resources.

The most similar contribution to the study presented in this paper is [12], with the main difference that both receiver and eavesdropper enqueue the update packets with an FCFS M/M/1 queue. They derive optimal transmission strategies in terms of the offered load ρ, varying the parameters of the proposed objective function derived from the Bergson social welfare framework. The work done in [13] goes one step further, considering a scenario where the unwanted receiver's service rate differs from the legitimate receiver's one. This leads to additional and sometimes counterintuitive conclusions in finding optimal policies in such conditions.

III. System Model

Consider the system of Fig. 1, where Alice (A) sends status updates to Bob (B), with the unwanted presence of an eavesdropper, called Eve (E), capturing packets transmitted by Alice with probability of success β. Alice generates update packets according to a Poisson process with rate λ, while Bob's service is exponentially distributed with rate μ, and handles packets with a preemptive policy [26]. Eve captures information with probability β; due to the properties of Poisson processes, this means that she also receives packets with a Poisson process of rate $\beta\lambda$, which are queued with an exponential service rate μ according to the queueing system M/M/1*.

For the sake of simpler notation, we set $\mu = 1$ for both receivers, thus making Bob's offered load $\rho_{\mathrm{B}} = \rho = \lambda$ and Eve's load $\rho_{\mathrm{E}} = \beta\rho = \beta\lambda$. Therefore, the numerical analysis presented in Section IV, varying ρ, will explicitly capture the changes in the generation rate λ. It is worth noting that more general evaluations for $\mu \neq 1$ can be promptly derived with proper rescaling. Comparison considerations for different service rates in the queues, which can be developed according to what outlined in [13], require a detailed analysis and are left for future work.

In the absence of the eavesdropper, the only purpose of Alice would be to choose the transmission rate so that Δ_{B} is minimized, i.e., $\lambda = \rho \to 1^{-}$. Using (2) the average AoI for Bob can be computed as

$$\Delta_{\mathrm{B}} = 1 + \frac{1}{\rho} = 1 + \frac{1}{\lambda}\,. \tag{3}$$

From now on, we will indifferently refer to ρ, which is also equal to λ, as the transmission rate, the update rate, or the offered load. Analogously, we can compute the average AoI at the eavesdropper's side

$$\Delta_{\mathrm{E}} = 1 + \frac{1}{\beta\rho}\,. \tag{4}$$

A. Objective Function

In our network configuration, Alice is the only agent who can make decisions. Her only possible action is to adjust the transmission rate $\lambda = \rho$ with which she intends to send updates. By doing so, she needs to find a good compromise to create a communication that relies on both quality and security. Basically, Alice should try to keep Δ_{B} low, but at the same time Δ_{E} high. This is non-trivial since they depend on the same parameter ρ. In fact, if we strictly think about creating a quality connection, we would need to find

$$\rho^{*} = \arg\min_{\rho}(\Delta_{\mathrm{B}}), \tag{5}$$

but this would also minimize Δ_{E}, which can create security problems. In contrast, if we solely rely on security, we would need to create our communication system with a source that has a load factor $\rho \to 0^{+}$. This, as expected, maximizes Eve's average AoI, but it does so also for the one of the legitimate receiver Bob, which is undesirable in a communication. We are therefore dealing with two conflicting objectives, which is the case of a multi-objective maximization problem.

The two conflicting goals, as in [13], can be described by the following utility functions

$$u_1(\rho) = \frac{1}{\tilde{\Delta}_B(\rho)}, \quad u_2(\rho) = \tilde{\Delta}_E(\rho), \tag{6}$$

where, in order to obtain treatable results even when dealing with infinity, the average AoI is upper bounded with a sufficiently large value which will be called M. Therefore, for Bob we get

$$\tilde{\Delta}_B(\lambda) = \min\{\Delta_B(\lambda), M\} \tag{7}$$

and for Eve

$$\tilde{\Delta}_E(\lambda) = \min\{\Delta_E(\lambda), M\}. \tag{8}$$

The choice of introducing an upper bound can also be legitimated in practical industrial scenarios [10], [13], where AoI values beyond a threshold can be considered useless.

To capture the best update strategy, we combine these two objectives in a single function. Analogously to [12], we follow a Bergson approach [17] to propose an objective function as a weighted ratio defined as

$$f(\rho) = [u_1(\rho)]^{a+1}\, u_2(\rho) = \frac{\tilde{\Delta}_{\mathrm{E}}(\rho)}{\left[\tilde{\Delta}_{\mathrm{B}}(\rho)\right]^{a+1}}, \tag{9}$$

which is a modified Nash bargaining solution [29]. The parameter $a \in (0, +\infty)$ can be referred to as trade-off parameter and will weigh the amount of value we intend giving into keeping Δ_{B} low. That is, having $a \to +\infty$ means ignoring the presence of the eavesdropper, while having $a \to 0^{+}$ means giving the eavesdropper the same importance of the receiver.

B. Critical Transition Point Derivation

In our system, when eavesdropping probability β is low, updates on Eve's side do not occur often on average, bringing her average AoI, Δ_{E}, to be upper bounded by the threshold M. This results in a change of behavior in the way optima evolve as β varies. As shown in Fig. 2, there is a point of particular interest, which will be called "critical load factor" indicated with ρ_{c}, that shows where this shift occurs. The transition appears whenever Δ_{E} changes from being $\Delta_{\mathrm{E}} < M$, to the condition $\Delta_{\mathrm{E}} = M$, which can be expressed as

$$1 + \frac{1}{\beta\rho} = M \tag{10}$$

Such situation can be described, rearranging (10), with the following equation

$$\beta\rho = \frac{1}{M-1}, \tag{11}$$

which, when satisfied for some β and some ρ, marks the shift in the behavior of the optimal transmission strategy, the one indicated by ρ_c. Since we know that at that point an optimum occurs, we have that ρ_c will be a root of our objective's derivative

$$\frac{d}{d\rho}f(\rho) = \frac{\rho^{a-1}\left([(a+1)\beta - 1]\,\rho + a\right)}{\beta\,(\rho+1)^{2a}}. \tag{12}$$

To find ρ_c, we use the necessary condition given by (11), expressing β as function of the load factor ρ

$$\beta = \frac{1}{\rho(M-1)}, \tag{13}$$

which can be substituted in the derivative expression and equated to zero

$$\frac{d}{d\rho}f(\rho) = \frac{\rho^{a}\left[1 + aM - (M-1)\rho\right]}{(\rho+1)^{2a}} = 0. \tag{14}$$

Solving the equation we can derive the numerical value at which the critical load factor occurs, i.e.

$$\rho_c = \frac{aM+1}{M-1}. \tag{15}$$

Using (13), we can also find the value of β for which the objective function has a maximum that arises exactly at ρ_c. This is given by

$$\beta_c = \frac{1}{\rho_c(M-1)} \tag{16}$$

A further discussion of this phenomenon with results will be provided in the following section.

IV. Results

We present a sensitivity analysis on the objective presented in Section III, to understand how preemption impacts the performance of the receivers (legitimate or eavesdropper), both modeled as an M/M/1* queue. We analyze the dependence on ρ^* as well as parameters β and a.

In Fig. 2, we plot the objective function $f(\rho)$ as a function of ρ where each curve corresponds to different values of the probability of eavesdropping β. The black dots highlight the maxima of each curve, having a black solid line connecting each maximum. Furthermore, a red dashed line highlights the position of the critical load factor ρ_c, that can be computed by means of (15) and (16). In this specific case (that is, at $a = 0.25$ and $M = 25$), we obtain $\rho_c \approx 0.302$ and $\beta_c \approx 0.138$, as shown in the graph. When $\beta = 0$ we are in the situation where Eve never intercepts packets, which leads to Δ_E always being "saturated" in $M = 25$. This behavior confirms the theory; in fact, for such a value of β, Eve never updates, thus making her AoI continuously grow, bringing her average AoI Δ_E greater than M. Consequently,

$$f(\rho) \approx \frac{M}{\left[\tilde{\Delta}_B(\rho)\right]^{a+1}} \tag{17}$$

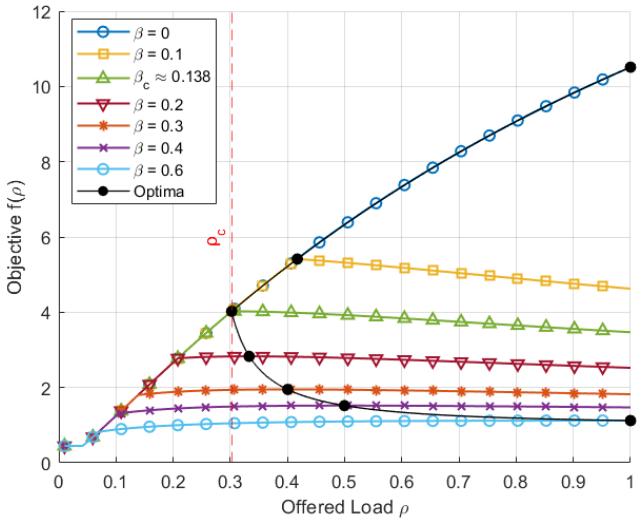

Fig. 2. Objective $f(\rho)$ as a function of the offered load ρ for different values of eavesdropping probability β, with tradeoff parameter $a = 0.25$ and upper bound $M = 25$

meaning that the only focus of the optimization can be Bob's average AoI. Since $\Delta_B(\rho)$ is minimized at $\rho \to 1$, the objective function is maximized at the same point. For moderate β, it can be noticed that the plots are "hill-shaped" and that the maximum occurs at an intermediate value of ρ. In fact, at small ρ Bob's average AoI is too large, which hurts the overall value of $f(\rho)$, while as ρ increases Δ_E diminishes lowering as well the objective. As β grows towards 1, the difference between the two receivers' average AoI becomes smaller and smaller. Therefore, the best strategy is now to pick a higher ρ, since trying to avoid eavesdropping becomes much more difficult or even impossible when $\beta = 1$. In the figure, it can be seen that already when $\beta = 0.6$ the optimal policy is to completely ignore the presence of Eve, which results in pushing the optimal load to its maximum, that is $\rho^* = 1$. Hence, we find that for high values of β, the objective function benefits more in maintaining a good quality connection with the legitimate receiver Bob rather than caring about the presence of the eavesdropper.

We focus on how the tradeoff parameter a influences the optimal load. In Fig. 3, we plot ρ^* as a function of eavesdropping probability β for different values of a. We recall that high Δ_E is capped at M, which in the figure results in a common trend that characterizes each plot in the optimal load factor ρ^*. This behavior is highlighted with a dashed red line that represents the critical offered load ρ_c as a function of β_c, calculated for different values of a. Function $\rho_c(\beta_c)$ follows almost exactly the curve of $a = 0$. In fact, for this value, the objective greatly rewards keeping Eve's average AoI high, which, for almost all values of β, results in having $\Delta_E > M$. Therefore, the best strategy is to keep ρ^* low, which further decreases as β increases. Conversely, when $\beta \approx 0$ we have no eavesdropping and the optimal policy is to have $\rho^* \approx 1$.

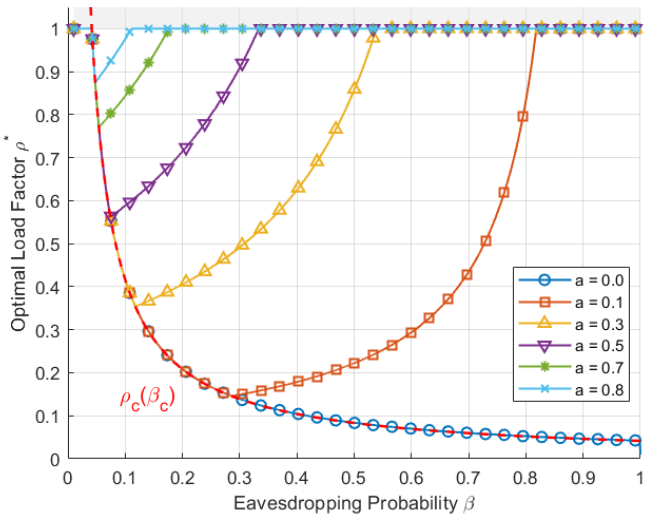

Fig. 3. Optimal offered load ρ^* as a function of eavesdropping probability β, for different values of tradeoff parameter a. The average AoIs are upper bounded by $M = 25$

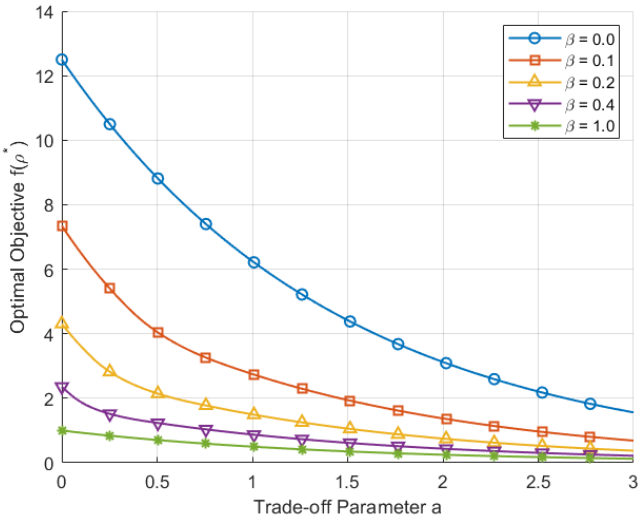

Fig. 4. Optimal $f(\rho^*)$ as a function of trade-off parameter a for different values of eavesdropping probability β and fixed upper bound $M = 25$

For a tradeoff parameter $a > 0$, the plots form a U shape: All curves, for low β, start at $\rho^* \approx 1$, the optimal load then drops for intermediate values of eavesdropping probability following the $\rho_c(\beta_c)$ red dashed line, and increases back to $\rho = 1$ as $\beta \to 1$. When higher values of a (e.g., $a = 0.8$) are considered, the system strongly prioritizes Bob's freshness, therefore ρ^* remains close to 1 across all values of β.

In Fig. 4, we compute the objective function at the optimal load, that is $f(\rho^*)$, as a function of a for different values of β. For all colored curves, as a grows, the objective $f(\rho)$ puts more weight on reducing Δ_B. Consequently, since driven by the same parameter ρ, also Δ_E inevitably diminishes, thus decreasing the product of the two utilities. At $\beta = 0$, Eve's average AoI is capped at M, so $f(\rho^*)$ can be quite large when the parameter a is small. In this case the objective function reaches its highest value. This shows that, when there is no eavesdropping (i.e., $\beta \to 0^+$), we are in the best case scenario. When all packets are intercepted, we have that $\Delta_E \approx \Delta_B$. Thus, we can rewrite the objective as

$$f(\rho) \approx \frac{1}{\left[\tilde{\Delta}_B(\rho)\right]^a}. \tag{18}$$

Now, the best that the transmitter can do is to solely focus on reducing Bob's average AoI. Therefore, in this case, the objective opts for a high optimal offered load, i.e. $\rho^* \approx 1$, also helping Eve to receive fresh updates. This results in the function remaining low across all values of a, also showing that total eavesdropping is the worst case scenario, hence confirming the theory. Eventually, as $a \to +\infty$, all curves converge to an optimal load $\rho^* = 0$.

Thus, when both legitimate and unauthorized receivers process their update packets with an M/M/1* queue, they both benefit from preemption. Thus, the optimal strategy often tends to prioritize communication performance (that is, minimizing Δ_B) even if it means that Eve gets fresh updates too, thus worsening the security of the system. This occurs because the objective function finds a greater benefit in optimizing Bob's average AoI, instead of keeping Eve's updates stale.

V. Conclusions

This paper highlighted the need for industrial communication systems to be both efficient and secure [8], [13], [25]; to this end, we analyzed a situation where status updates are exchanged between a transmitter and a receiver with the undesired presence of an eavesdropper. The main goal was to find a balance in keeping data fresh for the receiver and stale for the eavesdropper.

To solve this task, we used an objective function that integrated with a ratio the contrasting goals of the authorized receiver, and the one of the eavesdropper. Unlike the existing literature, we modeled the communication system using the M/M/1* policy to handle the packets that arrive at each receiver [2]. This model allowed us to derive closed-form solutions, which, provided together with numerical sensitivity analysis, point out that an optimal transmission strategy can be found for the fully preemptive scenario considered.

References

[1] S. Kaul, R. Yates, and M. Gruteser, "Real-time status: How often should one update?" in *Proc. IEEE Infocom*, 2012, pp. 2731–2735.

[2] 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.

[3] A. Munari and L. Badia, "The role of feedback in AoI optimization under limited transmission opportunities," in *Proc. IEEE Globecom*, 2022, pp. 1972–1977.

[4] L. Badia, V. Bonagura, F. Pascucci, V. Vadori, and E. Grisan, "Medical self-reporting with adversarial data injection modeled via game theory," in *Proc. Int. Conf. Commun. Signal Proc. Applic. (ICCSPA)*, 2024.

[5] L. Badia and A. Munari, "Satellite intermittent connectivity and its impact on age of information for finite horizon scheduling," in *Proc. IEEE Adv. Satellite Multimedia Syst. Signal Proc. Space Commun. (ASMS/SPSC)*, 2025.

[6] L. Crosara, A. Zancanaro, G. Cisotto, N. Laurenti, and L. Badia, "Analytical evaluation of age of information in networks of correlated sources," in *Proc. IEEE Wkhsp Metrology Agr. Forestry (MetroAgriFor)*, 2022, pp. 323–328.

[7] L. Fisser and A. Timm-Giel, "Minimizing age of information for distributed control in smart grids," in *Proc. IEEE SmartGridComm*, 2021.

[8] H. Wang, X. Xie, and J. Yang, "Optimizing average age of information in industrial IoT systems under delay constraint," *IEEE Trans. Ind. Informat.*, vol. 19, no. 10, pp. 10 244–10 253, 2023.

[9] 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.

[10] L. Hu, Z. Chen, Y. Dong, Y. Jia, L. Liang, and M. Wang, "Status update in IoT networks: Age-of-information violation probability and optimal update rate," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11 329–11 344, 2021.

[11] M. Yin, M. Yan, Y. Guo, and M. Liu, "Analysis of a pre-emptive two-priority queuing system with impatient customers and heterogeneous servers," *Mathematics*, vol. 11, no. 18, p. 3878, 2023.

[12] 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. Int. Balkan Conf. Commun. Netw. (BalkanCom)*, 2023.

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

[14] X. Wen, C. Chen, C. Ren, Y. Ma, M. Li, L. Lyu, and X. Guan, "Age-of-task-aware co-design of sampling, scheduling, and control for industrial iot systems," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 4227–4242, 2024.

[15] A. Tanveer, R. Sinha, and M. M. Y. Kuo, "Secure links: Secure-by-design communications in IEC 61499 industrial control applications," *IEEE Trans. Ind. Informat.*, vol. 17, no. 6, pp. 3992–4002, 2021.

[16] X. Zhang, X. Jia, H. Chang, and H. Tian, "Average age of information for multi-source single buffer preemption queueing model with packet dropping in service," in *Proc. IEEE Veh. Tech. Conf. (VTC Fall)*, 2024.

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

[18] 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, 2019.

[19] S. K. Kaul, R. D. Yates, and M. Gruteser, "Status updates through queues," in *Proc. IEEE CISS*, 2012, pp. 1–6.

[20] 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, 2016.

[21] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[22] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, p. 120–126, 1978.

[23] Q. Wang, H. Chen, P. Mohapatra, and N. Pappas, "Secure status updates under eavesdropping: Age of information-based secrecy metrics," in *Proc. IEEE Infocom Wkshps*, 2024.

[24] J. Zhang, H. Xu, A. Zheng, D. Cao, Y. Xu, and C. Lin, "Transmitting status updates on infinite capacity systems with eavesdropper: Freshness advantage of legitimate receiver," *Entropy*, vol. 27, no. 6, p. 571, 2025.

[25] 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, 2022.

[26] L. Badia, A. Baiocchi, A. Todini, S. Merlin, S. Pupolin, A. Zanella, and M. Zorzi, "On the impact of physical layer awareness on scheduling and resource allocation in broadband multicellular IEEE 802.16 systems," *IEEE Wirel. Commun.*, vol. 14, no. 1, pp. 36–43, 2007.

[27] L. Crosara, N. Laurenti, and L. Badia, "Strategic status updates in an eavesdropping game," in *Proc. European Wirel. Conf.*, 2023, pp. 290–295.

[28] A. Buratto, A. C. Aka, S. Sadeghzadeh, and L. Badia, "Eavesdropping fresh information: A game theoretical approach in dual sender networks," in *Proc. European Wirel. Conf.*, 2024, pp. 91–96.

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