Strategic Status Updates in an Eavesdropping Game

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 analyze a system where a transmitter (Alice) sends status updates to a legitimate receiver (Bob), but a fraction of them can be captured by an eavesdropper (Eve). Alice is modeled as a strategic agent that follows a two-fold objective. First of all, she wants to minimize the average age of information at Bob's side. Yet, she also simultaneously attempts to maximize Eve's average age of information, so as to avoid that the eavesdropper captures valuable information. Both objectives are combined in a bargaining framework, so as to obtain their tradeoff that ultimately depends on the injection rate of Alice and the probability that Eve intercepts data. At the same time, Eve is also seen as a strategic agent that aims to minimize its own AoI, coming from stolen data, by tuning the eavesdropping probability but subject to a cost. We frame the interaction between Alice and Eve as a static adversarial game of complete information, and we derive and discuss the resulting equilibria. This extension of security aspects to the age of information framework enables a quantitative perspective with possible practical conclusions.**

***Index Terms*—Age of Information; Data acquisition; Game theory; Communication system security.**

I. Introduction

The freshness of status updates about the surrounding environment, quantified through age of information (AoI), is becoming extremely relevant for most applications envisioned for the upcoming 6th generation (6G) of wireless communications [1]–[3]. Among the key enablers of 6G, the technological convergence and the ability for the communication systems of making autonomous decisions thanks to artificial intelligence [4] rely on the exchange of up-to-date information.

To understand the definition of AoI, consider a system, where a transmitter sends status updates to a receiver, which processes them for a random time before using them. The propagation time from the transmitter to the receiver is taken as instantaneous, since it can be conglomerated in the processing time [5]. We also assume that all updates deliver fresh information to the receiver [6], [7].

Then, we define the AoI at the receiver's side at time t as [8]

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

where $\sigma(t)$ is the last instant prior to t when an update was finished being processed.

If updates arriving at the receiver's side while a previous one is still being processed are enqueued, we obtain an interesting line of research related to queueing systems. In this spirit, classic results from queueing theory, typically expressing throughput or delay, are revisited to focus on AoI, to obtain interesting conclusions through elegant closed-form evaluations. Most investigations in the literature expand basic systems, such as the M/M/1 queue studied in [8], to different arrival/service processes, buffer size, or queue policy [9]–[14].

We leverage these results for a different setup, where, beyond the communication between a transmitter (Alice) and a legitimate receiver (Bob), an eavesdropper (Eve) is added to the system. Alice generates memoryless status updates intended to reach Bob, which processes them for an exponentially distributed random time and with FCFS order. That is, the Alice–Bob system is a standard M/M/1 queue [8].

Eve intercepts the updates according to a binomial process with independent and identically distributed (i.i.d.) probability $\beta \in [0, 1]$. The eavesdropped updates are still received by Bob but also processed by Eve. Analogous to Bob, she has an AoI value based on the stolen information only.

Under this setup, we consider a game theoretic approach where Alice is a strategic agent. She is aware that Eve is stealing information and can control the generation rate of updates. She can tune it down to prevent Eve's from gaining too fresh information, but at the price of also increasing Bob's AoI value. Thus, Alice's objective is found as the barganing between two contrasting objectives, i.e., minimizing Bob's and maximizing Eve's expected AoI values [1].

Eve is also strategic, and tries to to maximize the freshness of her eavesdropped data, also including an activity cost in her objective. We use a game theory setup to study the competition between Alice and Eve, as selfish players, who strive for maximizing their own payoffs [15]. The analysis is interesting as the final outcome jointly depends on two parameters, the generation rate and the eavesdropping probability, which are each in exclusive control of either player. Thus, the interaction between Alice and Eve can be a static adversarial game of complete information [16].

As a result, we are able to highlight interesting conclusions, such as the optimal data generation rate chosen by Alice being, under proper conditions, a decreasing function of the probability β of data capture by Eve. Then, we derive the Nash Equilibriums (NEs) of the resulting system and we compare the obtained performance of both legitimate (Alice–Bob) and malicious (Eve) users at the NE with the case without a strategic adversary that only chooses a fixed β. In this sense, our study serves as a foundation to expand the age of information investigations to security considerations [17], [18].

The rest of this paper is organized as follows. In Section II, we review related work on queuing systems, age of information, security, and game theory, noting how all these aspects are sometimes considered together, but rarely all of them at once. In Section III, we outline the system model, formalized as an adversarial setup for which we introduce strategy and payoff of each player. This is studied in Section IV through game theory, deriving analytical results on the NEs. We present numerical results in Section V, and we conclude in Section VI.

II. Related Work

This paper extends the studies framing AoI in the context of queuing systems [9]–[14]. The AoI computation for an FCFS M/M/1 queue with arrival rate λ and service rate μ, whose load factor is then $\rho = \lambda/\mu$, is found in [8] and already interesting in itself, as a closed-form expression is obtained for the average AoI $\Delta = \mathbb{E}[\delta(t)]$ as

$$\Delta = \frac{1}{\mu}\left(1 + \frac{1}{\rho} + \frac{\rho^2}{1-\rho}\right). \tag{2}$$

This implies that the optimal average AoI is achieved for the load factor $\rho^\star \approx 0.531$. It follows that an AoI-optimal data generation must be sufficiently frequent, yet without congesting the server. For different queue disciplines, this may change and, in particular, preemption allows to circumvent the congestion at the receiver's buffer; thus, the AoI-optimal load factor is on the brink of instability [2]. Nevertheless, our analysis refers to a plain M/M/1 queue, and these numerical values are retrieved later; e.g., Alice's optimal generation rate in the absence of Eve is $\rho = \rho^*$. Hence, for other disciplines, the values change but a similar reasoning applies.

Quite surprisingly, opposed to the plethora of results available from standard queueing theory, there are relatively few investigations pertaining to security or confidentiality of AoI, which we believe to be of key importance for many 6G scenarios, especially for mission critical or tactical applications. Among these, in [19], a generic Internet of vehicles network is investigated and a vehicle-assisted verification is adopted. Here, AoI is used as a quantitative indicator of security, but the scenario focuses on sybil attacks and not eavesdropping.

In [20], the problem of keeping fresh information under passive eavesdropping attacks is considered. The authors study a source reporting the latest status of the system to an intended receiver, while thwarting a potential eavesdropper. To this end, two AoI-based metrics are introduced to characterize the secrecy performance of the considered system. Similar to our paper, they aim at computing the optimal generation rate of the transmitter, but under a stateful information, which allows for an optimization of the transmission schedule [7], [13]. In our approach, the choice of ρ is aimed instead at minimizing the average AoI from closed-form expressions.

Also, they consider a very specific objective, taken as the difference between the AoI values of the legitimate receiver and the eavesdropper, respectively. Such a choice may not be ideal, especially in the case very high values are considered – if the information at the legitimate receiver is stale, it may not be very useful that the AoI at the eavesdropper is just higher by a certain amount. For this reason, our application of Bergson's theory of social welfare may be preferable. This approach, which can be framed in the general context of Nash bargaining theory, was actually introduced for AoI problems in our previous paper [1]. Yet, notice that neither [20] nor [1] consider a game theoretic framework as we do here.

Finally, there are a few related references for what concerns applications of game theory to AoI. However, the literature is relatively limited at least in the context of security aspects. Most of the game theoretic approaches to AoI concern the datalink layer [21]–[23]. In these cases, multiple users are just competing but not adversarial. That is, they strive for accessing the channel, which is a scarce resource due to collisions or mutual interference, so as to keep their information fresh, but they do not benefit from the other players having high AoI. Therefore, aspects like security or confidentiality are not explored. However, our extension where data-capturing attackers are included in the systems would be an important aspect, especially for sensitive contexts in 6G networks.

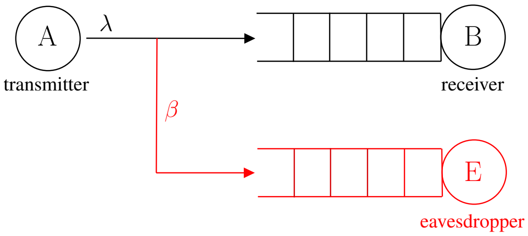

Fig. 1. Queuing system with a transmitter (A), a legitimate receiver (B), and an eavesdropper (E).

Few studies in the literature use game theory to analyze security problems combined with information freshness, and even when all these elements are considered (game theory, AoI, security), the focus is on adversarial service denial (e.g., jamming) [17], [24] rather than data confidentiality. In [18], an adversarial setup is considered with a jammer trying to increase AoI at the receiver's side; a dynamic game is established between two players, i.e., the attacker and the system controller. Other cases are analyzed in [25], comparing Nash and Stackelberg equilibria, and [26], with a focus on aerial channel and attacks related to both physical and medium access layers.

Studies that evaluate confidentiality and eavesdropping via game theory only quantify the secrecy rate [27], an aggregate measure that does not describe freshness, and is more related to throughput. Thus, our analysis goes through unexplored avenues, and can lead to original conclusions of practical interests in the field of information security.

III. System Model

With reference to Fig. 1, consider Alice (A) sending status updates to Bob (B) as data packets that can be intercepted and eavesdropped by Eve (E). Alice's primary objective is to minimize Bob's expected AoI, but due to Eve's presence, she may want to adjust the generation of status updates to Bob so as to cause the data captured by Eve to be stale. In other words, Alice seeks for combining two objectives: minimizing Bob's and maximizing Eve's expected AoI values.

The Alice–Bob system is taken as an M/M/1 queue with FCFS discipline; Alice generates packets according to a memoryless process of rate λ, which are processed by Bob with exponentially distributed times. For notational simplicity, we take a normalized rate $\mu = 1$ of service at Bob's, which implies that the offered load is $\rho = \lambda$. All the results can be expanded to different values of μ by re-introducing it as a multiplicative factor. The channel between Alice and Bob is error-free, i.e., every update sent by Alice is correctly received by Bob. This is not restrictive, and can be relaxed by rescaling ρ [7].

Each update packet generated by Alice at a random time t_j might be eavesdropped by Eve, 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 the packet 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 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, also with normalized service rate μ=1. Thus, we can compute two AoI values, related to receivers Bob (legitimate) and Eve (malicious). The first corresponds to the instantaneous freshness of data legitimately exchanged. From (1), it is

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

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

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

with $\sigma_{\mathrm{E}}(t)$ being the instant of reception of a packet that is also captured by Eve, and υ_j the service time at Eve.

The fact that Eve may capture some update packets implies that Alice realistically also desires, in addition to minimizing Bob's AoI, that the information reaching Eve is as old as possible. Thus, Alice has two competing objectives as

$$f_1(\lambda) = \frac{1}{\Delta_{\mathrm{B}}(\lambda)}\,, \qquad f_2(\lambda) = \Delta_{\mathrm{E}}(\lambda), \tag{5}$$

where $\Delta_{\mathrm{B}}(\lambda) = \mathbb{E}[\delta_{\mathrm{B}}(t)]$ and $\Delta_{\mathrm{E}}(\lambda) = \mathbb{E}[\delta_{\mathrm{E}}(t)]$ are the expected AoI values of Bob's and Eve's, respectively. These expressions are set in agreement with the criterion that utilities are generally taken as quantities to maximize [28]. However, as will be clear later, this choice is entirely modular, as the tradeoff between these objectives can be tuned by a specific parameter, and it does not quantitatively affect the result.

These two objectives are contrasting, 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. We follow Bergson approach, as done in [1] in setting a utility function u_{A} for Alice as a weighted product between objectives f_1 and f_2, which reformulates the tradeoff into a single function and sets a precise value on Pareto frontier of f_1 vs. f_2. Our choice is

$$u_{\mathrm{A}}(\lambda) = [u_1(\lambda)]^{a+1} u_2(\lambda) = \frac{\Delta_{\mathrm{E}}(\lambda)}{[\Delta_{\mathrm{B}}(\lambda)]^{a+1}}, \tag{6}$$

with $a \in (0, +\infty)$ tuning the trade-off between f_1 and f_2. We must assume that f_1 is slightly more important than f_2, since it would be easier for Alice to just maximize the latter by never updating, which is illogical: it would have $\Delta_{\mathrm{E}}(\lambda)$ but also $\Delta_{\mathrm{B}}(\lambda)$ to grow indefinitely. Thus, we set the exponent of f_1 in the trade-off as greater than or equal to 1, and we write it as $a+1$. The larger a, the more important f_1 versus f_2 in the trade-off. Setting $a \to +\infty$ corresponds to ignoring the presence of Eve, whereas $a \to 0^+$ means that the threat of the eavesdropping receives the highest importance. The specific choice of a governs the selection in the Pareto frontier.

IV. Game Theoretic Analysis

Game theory can frame multi-agent systems into a multi-objective optimization where each agent is driven by its own selfish objectives. For the context of AoI and security, two different stances are possible. In an adversarial context, one of the nodes is an attacker with the objective of maximizing the legitimate node's AoI. This approach would be good for jamming problems [18], [25]. Other papers [22], [23], [29] consider each source as uninterested in the other's performance, having the sole objective of minimizing its own AoI.

For our problem, both these approaches are taken for different players. The eavesdropper has no reason to alter the system's AoI, but rather, just wants to gain illegitimate access to fresh data. Thus, Eve's selfish goal is to minimize her own AoI. Conversely, Alice takes a mixed objective of sending fresh updates to Bob while leaving only stale information to Eve. Then, in spite of Eve being the attacker, the adversarial role is played by Alice, in a swap similar to that of friendly jamming problems [16].

We frame the interaction between Alice and Eve as a static adversarial game of complete information, assuming that Alice and Eve are the two players of the game. The former tunes the offered load $\lambda \in [0,1]$, while the latter chooses the eavesdropping probability $\beta \in [0,1]$.

Alice's utility function is taken from (6), but written as $u_{\mathrm{A}}(\lambda, \beta)$, with an explicit dependence on β, and results in

$$u_{\mathrm{A}}(\lambda, \beta) = \frac{(\beta^3\,\lambda^3 - \beta^2\,\lambda^2 + 1)\lambda^a\,(\lambda-1)^{a+1}}{\beta\,(\beta\,\lambda - 1)\,(\lambda^3 - \lambda^2 + 1)^{a+1}}\,, \tag{7}$$

where a is a positive real value tuning the tradeoff between $\Delta_{\mathrm{B}}(\lambda)$ and $\Delta_{\mathrm{E}}(\lambda, \beta)$. We remark that $\Delta_{\mathrm{E}}(\lambda, \beta)$ also includes an explicit strategic dependence on β, chosen by Eve, and also the choice of $u_{\mathrm{A}}(\lambda, \beta)$ includes an implicit cost for Alice, since λ cannot be indefinitely increased, as argued in Section III, or else Eve would always eavesdrop fresh information.

Eve wants to lower her average AoI of stolen data, but at the same time she is limited in the persistency of her eavesdropping by a *cost* associated to it, as directly proportional to β through a coefficient $c > 0$. Thus, Eve's ultimate objective is the minimization of the linear combination of her AoI and the eavesdropping cost. Her utility function is

$$u_{\mathrm{E}}(\lambda, \beta) = -\Delta_{\mathrm{E}}(\lambda, \beta) - c\beta = -1 - \frac{1}{\beta\lambda} - \frac{\beta^2\lambda^2}{1-\beta\lambda} - c\beta\,, \tag{8}$$

where the negative signs are due to that both the expected AoI and the cost are metrics to be minimized, while the utility is once again taken as a quantity to maximize [28].

To find the NEs $(\lambda_{\mathrm{NE}}, \beta_{\mathrm{NE}})$, for given values of a and c, we compute the best responses (BRs) as

$$\lambda^\star(\beta) = \underset{\lambda \in [0,1]}{\arg\max}\; u_{\mathrm{A}}(\lambda, \beta)\,, \tag{9}$$

$$\beta^\star(\lambda) = \underset{\beta \in [0,1]}{\arg\max}\; u_{\mathrm{E}}(\lambda, \beta)\,, \tag{10}$$

for Alice and Eve, respectively. Now, we must find a strategy profile for which the BR conditions are mutually satisfied. For given a and c, $\lambda^\star(\beta)$ is the only solution in $[0,1]$ of

$$\frac{\partial}{\partial\lambda}\, u_{\mathrm{A}}(\lambda, \beta) = 0\,, \tag{11}$$

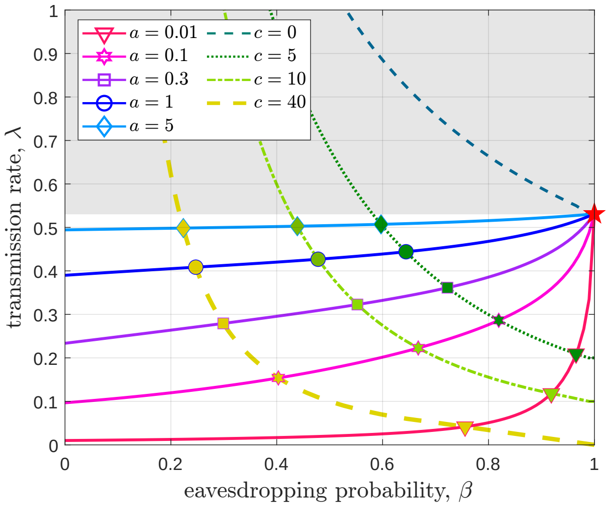

Fig. 2. Eve's BR function $\beta^\star(\lambda)$ (dashed lines) for different values of c, Alice's BR function $\lambda^\star(\beta)$ (solid lines) for different values of a. The NE points are denoted by the markers.

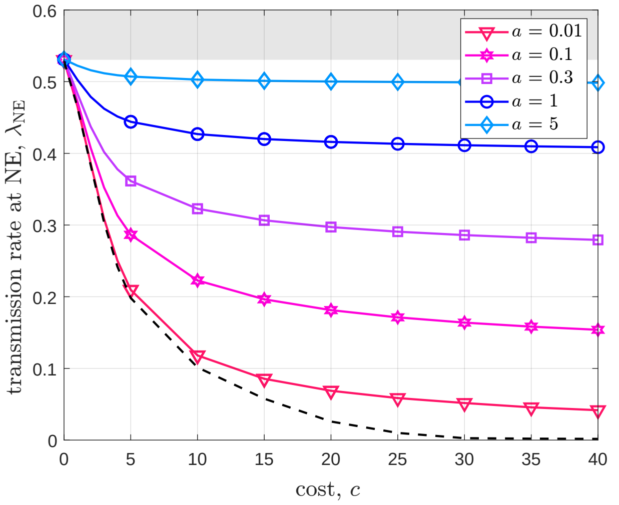

Fig. 3. Transmission rate at NE $\lambda_{\rm NE}$ versus the cost c, for different values of the trade-off parameter a. The black dashed line represents the limit for $a \to 0$.

that depends on β, while $\beta^\star(\lambda)$ is the solution of

$$\frac{\partial}{\partial \beta}\, u_{\rm E}(\lambda, \beta) = 0\,, \tag{12}$$

which depends on λ. According to [1], $u_{\rm A}(\lambda, \beta)$ is a concave function of λ; thus, (11) has only one solution $\lambda^\star(\beta)$. To prove the concavity of $u_{\rm E}(\lambda, \beta)$ with respect to β, for every value of λ, we compute its second order derivative in β as

$$\frac{\partial^2}{\partial \beta^2}\, u_{\rm E}(\lambda, \beta) = \frac{2\left(-3\beta^2\lambda^2 + 3\beta\lambda - 1\right)}{\beta^3\lambda(1-\beta\lambda)^3}\,, \tag{13}$$

where the denominator is always positive, and the numerator, for each value of β, describes a negative concave parabola which as maximum for $\beta = 1/(2\lambda)$, and

$$\max_{\beta}\, -3\beta^2\lambda^2 + 3\beta\lambda - 1 = -\frac{13}{4}\,,\ \forall \lambda. \tag{14}$$

We conclude that the second order derivative of $u_{\rm E}(\beta, \lambda)$ in β is negative for every λ, which implies that $u_{\rm E}(\beta, \lambda)$ is concave for every λ and, therefore, (12) has only one solution $\beta^\star(\lambda)$.

The NEs can be found through solving a system of two equations, one for each player's best response, in two unknowns, which can be done with numerical means.

V. Numerical Results

We present quantitative evaluations for the game played by Alice and Eve; the former tunes the transmission rate λ, while the latter chooses the eavesdropping probability β in a strategic fashion following a cost-minimizing strategy.

We discuss the impact that a fixed or strategically chosen eavesdropping probability β has on the average AoI at Bob's and Eve's, i.e., $\Delta_{\rm B}$ and $\Delta_{\rm E}$, respectively. When Eve is not present, since $\mu = 1$, the optimum transmission rate $\lambda^\star$ is equal to $\rho^\star = 0.531$ [8]. Thus, in the following results, the areas corresponding to $\lambda > \rho^\star$ are shaded, since a rational Alice will never choose a transmission rate larger than the optimal value in the absence of Eve.

Fig. 2 shows the best responses of Alice and Eve. The dashed lines represent Eve's best response $\beta^\star(\lambda)$ for different values of c, while the solid lines represent $\lambda^\star(\beta)$ for different values of a. The intersection points between solid and dashed lines are the solutions of both (11) and (12), thus they represent the NE $(\lambda_{\rm NE}, \beta_{\rm NE})$ of the game, for different values of the system parameters a and c. From the figure, we first see that when there is no cost in eavesdropping, i.e., $c = 0$, for all values of a the NE is always $\lambda_{\rm NE} = 0.531$ and $\beta_{\rm NE} = 1$. In this case, the problem degenerates to Eve persistently eavesdropping. Alice's goal becomes exclusively to minimize $\Delta_{\rm B}$, which is achieved by choosing $\lambda = 0.531$ [8]. Furthermore, we note that, when $a \to 0$, $\beta_{\rm NE} \to 1$ for every c, while, when $a \to +\infty$, $\lambda_{\rm NE} \to 0.531$ for every c. In the intermediate cases, with $0 < a < 1$ and $0 < c < 1$, the equilibria are obtained for $\lambda_{\rm NE} \in (0, 0.531)$ and $\beta_{\rm NE} \in (0, 1)$, which are further depicted in Figs. 3 and 4.

Fig. 3 shows the transmission rate at NE $\lambda_{\rm NE}$ versus the cost c, for different values of the trade-off parameter a. As can be seen, $\lambda_{\rm NE}$ is decreasing for an increasing cost parameter c, and approaches an asymptotic value. The latter is zero for $a \to 0^+$, see the dashed line, whereas it increases, so that when a is very high the curve also tends to 0.531 for high cost; in other words, $\lambda_{\rm NE}$ exhibits a flat trend. This occurs because, when $a \to 0^+$, it becomes a priority for Alice to maximize $\Delta_{\rm E}$ over minimizing $\Delta_{\rm B}$ and, for this reason, her optimal strategy is to choose a lower transmission rate λ. In the opposite case $a \to +\infty$, the minimization of $\Delta_{\rm B}$ becomes most relevant for Alice, who then chooses an transmission rate that approaches 0.531, i.e., the optimal value in the absence of Eve. Moreover, the value of $\lambda_{\rm NE}$ is also related to Eve's strategy β, as discussed below.

Fig. 4 shows the eavesdropping probability at NE $\beta_{\rm NE}$ versus the cost c, for different values of the trade-off parameter a. The value of $\beta_{\rm NE}$ decreases as c increases: this behavior is intuitive and implies that the higher the eavesdropping cost, the lower the fraction of intercepted packets by Eve. Thus,

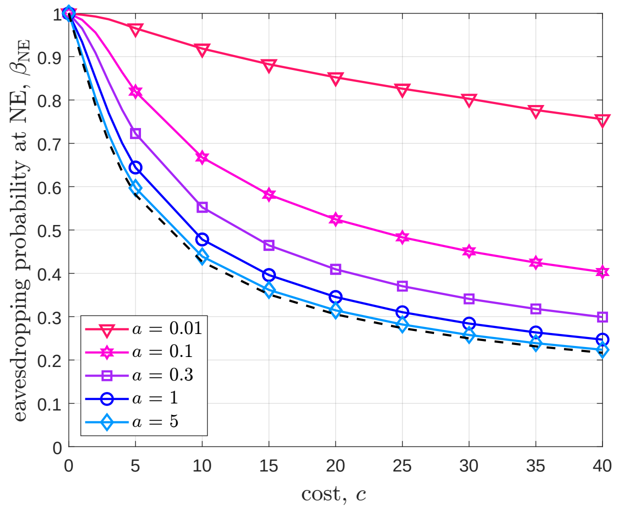

Fig. 4. Eavesdropping probability at NE β_{NE} versus the cost c, for different values of the trade-off parameter a. The black dashed line represents the limit for $a \to +\infty$.

combining the results of Figs. 3 and 4, the growth of the cost c causes a decrease in the value of β at the NE which, in turn, implies that Alice chooses a lower transmission rate λ. As a result, Alice and Eve shy away from transmitting and eavesdropping data, respectively. Moreover, Fig. 4 shows that, as a increases, the value of β_{NE} decreases more rapidly with increasing cost when a is high, and, as a increases, the curves moves quickly toward the dashed black line, which is the limit for $a \to +\infty$. In particular, when $a > 0.3$ and $c = 5$ a strategic Eve will choose to eavesdrop with probability $\beta_{\text{NE}} \in [0.6, 0.7]$, while, when $c = 20$, the eavesdropping probability at NE is approximately $\beta_{\text{NE}} \in [0.3, 0.4]$.

We use this result to compare the performance achieved by pair Alice-Bob versus that of Eve in the next Figs. 5–7. We consider a static behavior with fixed β by Eve, so that the optimum transmission rate $\lambda^\star$ is as derived in [1], compared with the strategic behavior at the NE. To allow for a direct comparison, and according to the numerical results of Fig. 4, the case of strategic Eve with $c = 5$ is compared with a fixed choice of $\beta = 0.6$, and similarly the case of $c = 20$ is compared with a static choice of $\beta = 0.3$.

Fig. 5 shows Eve's average AoI plus cost $\Delta_{\text{E}} + c\beta$ at NE for a strategic Eve (solid lines), and with optimum transmission rate $\lambda^\star$ for a fixed β (dashed lines), versus the trade-off parameter a. Given a cost c, the dashed line is above the solid one, i.e., if Eve chooses a fixed β for each value of a instead of optimizing it, she gets worse performance. For a given c, the difference between the curves for fixed and strategic β becomes negligible as a grows, as β_{NE} tends to the fixed β.

Fig. 6 shows Bob's average AoI Δ_{B} at NE for a strategic Eve (solid lines), and with optimum transmission rate $\lambda^\star$ for a fixed β (dashed lines), versus the trade-off parameter a. The black curve represents the minimum value of Δ_{B}, achieved when Eve is not present and Alice chooses $\lambda^\star = 0.531$ [8]. Fig. 6 shows that, when a grows, all the curves tend to the case without eavesdropping (black line). This happens since, as a grows, the optimal value λ (in both cases of static and strategic eavesdropping) tends to 0.531, as can be seen from Fig. 3.

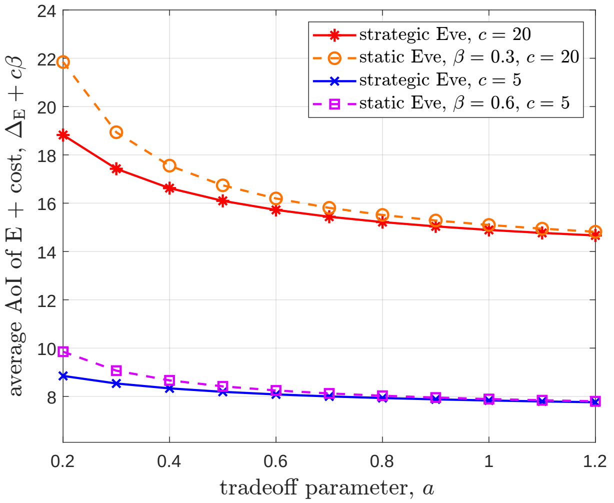

Fig. 5. Eve's average AoI plus cost $\Delta_{\text{E}} + c\beta$ at NE for a strategic Eve (solid lines), and with optimum transmission rate $\lambda^\star$ for a fixed β (dashed lines), versus the trade-off parameter a, for different values of the cost c.

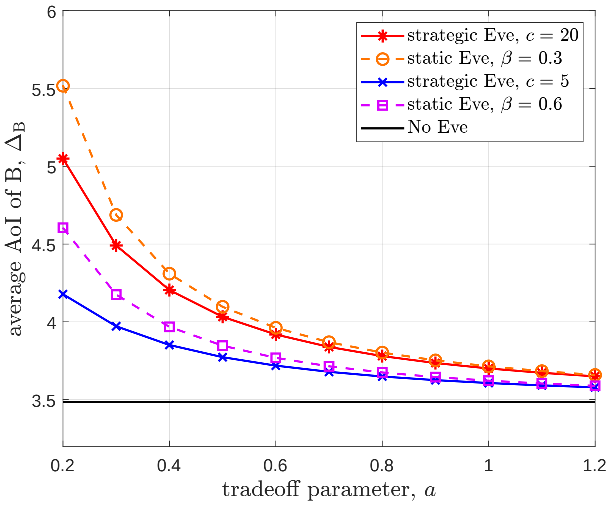

Fig. 6. Bob's average AoI Δ_{B} at NE for a strategic Eve (solid lines), and with optimum transmission rate $\lambda^\star$ for a fixed β (dashed lines), versus the trade-off parameter a, for different values of the cost c. The black curve represents the achievable performance when Eve is not present, and $\lambda = 0.531$.

Moreover, for a given c, either $c = 5$ or $c = 20$, we can see that the dashed curve is above the solid one. Thus, the fixed β value chosen by Eve causes a greater deterioration in Bob's AoI than the case where β is chosen strategically. However, as it was previously mentioned while discussing Fig. 5, by selecting a fixed β, Eve does not optimize its own performance. As a result, a fixed β may worsen the communication between Alice and Bob, but without Eve benefiting from it. On the other hand, a strategic Eve induces a deterioration on Alice's payoff function with respect to a static Eve, as Fig. 7 shows.

VI. Conclusions

We analyzed an AoI-aware exchange, between a transmitter (Alice) and a legitimate receiver (Bob), of status updates that

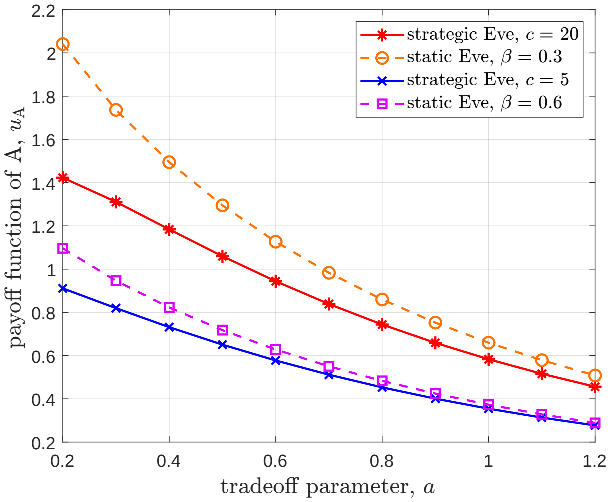

Fig. 7. Alice's payoff u_{A} at NE for a strategic Eve (solid lines), and with optimum transmission rate $\lambda^\star$ for a fixed β (dashed lines), versus the tradeoff parameter a, for different values of the cost c.

can be intercepted by an eavesdropper (Eve). We leveraged closed-form results for queuing systems, computing the AoI as functions of system parameters such as the update generation rate and the eavesdropping probability.

We formalized a game theoretic setup where Alice and Eve are two strategic players. The former wants to set an update generation rate to simultaneously lower the average AoI at Bob's and leave only stale information to Eve. These two objectives are combined according to Bergson's bargaining approach. At the same time, Eve's objective is chosen as the minimization of a penalty consisting of her own average AoI plus an activity cost. In general, the presence of Eve results in lowering the data generation/transmission rate by Alice. However, an eavesdropper with a strategic character may be less harmful to the legitimate transmission than a brute-force one, since its ultimate objective is just to capture information and not to hurt the transmission.

Our analysis can be extended by looking not only at the average values of AoI but also at the instantaneous values and the probability of Peak-AoI violation [30]. To this end, Alice may schedule the updates with full information on the AoI according to a stateful approach [7], and similarly Eve can follow different patterns for its eavesdropping according to her AoI value. Possible extensions include Bayesian approaches for when the presence of the eavesdropper is not known for sure, but Alice moves based on cost estimates for tracking the eavesdropper and detecting whether data was captured [15].

References

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

[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, May 2021.

[3] 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.

[4] R. Bassoli, F. H. Fitzek, and E. Calvanese Strinati, "Why do we need 6G?" *ITU J. Fut. Evolving Techn.*, vol. 2, no. 6, pp. 1–31, 2021.

[5] 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.

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

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

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

[9] 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.

[10] A. Soysal and S. Ulukus, "Age of information in G/G/1/1 systems: Age expressions, bounds, special cases, and optimization," *IEEE Trans. Inf. Theory*, vol. 67, no. 11, pp. 7477–7489, Nov. 2021.

[11] A. Kosta, N. Pappas, A. Ephremides, and V. Angelakis, "Non-linear age of information in a discrete time queue: Stationary distribution and average performance analysis," in *Proc. IEEE ICC*, 2020, pp. 1–6.

[12] 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.

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

[15] L. Prospero, R. Costa, and L. Badia, "Resource sharing in the Internet of Things and selfish behaviors of the agents," *IEEE Trans. Circuits Syst. II*, vol. 68, no. 12, pp. 3488–3492, Dec. 2021.

[16] L. Badia and F. Gringoli, "A game of one/two strategic friendly jammers versus a malicious strategic node," *IEEE Netw. Lett.*, vol. 1, no. 1, pp. 6–9, Mar. 2019.

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

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

[19] 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.

[20] 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

[21] 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.

[22] L. Badia and A. Munari, "A game theoretic approach to age of information in modern random access systems," in *Proc. IEEE Globecom Wkshps*, 2021.

[23] K. Saurav and R. Vaze, "Game of ages in a distributed network," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1240–1249, May 2021.

[24] 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.

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

[26] Y. Yang, W. Wang, R. Xu, G. Srivastava, M. Alazab, T. R. Gadekallu, and C. Su, "AoI optimization for UAV-aided MEC networks under channel access attacks: A game theoretic viewpoint," in *Proc. IEEE ICC*, 2022.

[27] C. Fan, H. Liu, B. Li, C. Zhao, and S. Mao, "Adversarial game against hybrid attacks in UAV communications with partial information," *IEEE Trans. Veh. Technol.*, vol. 71, no. 2, pp. 2204–2208, Feb. 2022.

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

[29] 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.

[30] F. Chiariotti, B. Soret, and P. Popovski, "Latency and peak age of information in non-preemptive multipath communications," *IEEE Trans. Commun.*, vol. 70, no. 8, pp. 5336–5352, Aug. 2022.