Strategic Interaction Over Age of Information on a Quantum Wiretap Channel

Leonardo Badia*†, Hilal Sultan Duranoglu Tunc†, Aynur Cemre Aka*, Riccardo Bassoli†, Frank H. P. Fitzek†
* Dept. of Information Engineering, University of Padova, Italy
† Deutsche Telekom Chair of Communication Networks, TU Dresden, Germany
{badia@dei.,aynurcemre.aka@studenti.}unipd.it, {hilal_sultan.duranoglu_tunc,riccardo.bassoli,frank.fitzek}@tu-dresden.de

***Abstract*—We investigate a scenario where a transmitter (Alice) sends information to a legitimate receiver (Bob) through a quantum channel in the presence of an eavesdropper (Eve). The information leaked to Eve is made unavailable to Bob, which causes the system to behave like a partially degraded wiretap channel. We consider Alice and Eve to be strategic players interested in minimizing the resulting age of information at Bob's and Eve's, respectively. We frame the resulting system as two M/M/1 queues, fed by the remaining information and the eavesdropped data, respectively, for which we can exploit well-known results. The strategic interaction among the players is captured by a game-theoretic formulation, where Alice chooses her data generation rate and Eve controls the interception probability, both subject to a cost for their action. We obtain a characterization of the resulting Nash equilibria, exploring the conditions for their existence depending on the cost parameters. The most important finding of our analysis lies in the evaluation of the price of anarchy, which is found to be extremely high in the presence of multiple Nash equilibria. Thus, the application of distributed management ought to be carefully controlled to avoid inefficient outcomes.**

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

I. Introduction

Age of Information (AoI) is a popular metric to characterize the freshness of information in real-time applications, where the timeliness of data updates directly impacts decision-making and system performance [1]–[3]. Its evaluation has gained significant attention and seen numerous studies in the context of queueing systems, thanks to the analytical characterizations made in seminal studies that have led to revitalizing this classic topic [4].

Queueing systems can model sensor networks and Internet of Things (IoT) scenarios, where the freshness of information is critical. In this case, the analysis of AoI is preferable to that of traditional performance metrics, such as delay, throughput, and queue length, which may not fully capture the timeliness aspect of information [5]. Also, due to their mathematical nature, queueing systems provide a versatile framework for studying the dynamics of information flows almost independent of the application or the technology used. For this reason, they are suited for studying heterogeneous domains such as healthcare systems, autonomous transportation, smart grids, and supply chain management, which are the target of upcoming 6G systems, as well as different emerging technological supports such as quantum, terahertz, or massive MIMO communications [6].

In this paper, we consider a quantum communication scenario, where we leverage theoretical results from queueing theory pertaining to AoI evaluations. We focus on a quantum wiretap channel [7] where an eavesdropper (Eve) can capture part of the information sent by a transmitter (Alice) to her legitimate receiver (Bob). We assume that information pieces that have been captured by Eve are not available to Bob. In quantum communications, this happens because Eve's interception would perturb the quantum superposition state of the transmission, which would allow Bob to recognize, and ultimately discard, the content that was tampered with [8]. More in general, our analysis can be applied to all those scenarios where the eavesdropping operation either materially takes the information carrier away and the physical support of the information is non-reproducible, or causes the information content to become inherently degraded for the intended receiver. The former case also happens, for example, in molecular communications [9], whenever the chemical compounds intercepted by the eavesdropper are withdrawn from the molecular channel.

Whatever the reason, the fact that Bob gets information through a partially degraded wiretap channel requires Alice to send updates more frequently to compensate for the loss of information caused by Eve [10]. We assume that Alice and Eve pay some costs for their actions, so they are prevented from indefinitely increasing their activities [11]. Note that Eve is just interested in acquiring fresh information so she does not need to capture the information sent by Alice in its entirety, since an AoI-minimal information flow is found at intermediate values that neither are too sporadic nor too frequent, as the former causes information to become stale but the latter would clog the queueing process [4]. As a result, Alice is similarly not required to indefinitely increase her transmission rate.

To better characterize the convergence of these objectives, we introduce a game theoretic approach where Alice and Eve are taken as strategic players, each interested in minimizing an AoI value – Eve wants to obtain fresh information for herself, whereas Alice wants to minimize the AoI of the remaining information that Bob gets after discarding what he recognizes was eavesdropped by Eve – also subject to a cost. We formalize the utilities of the players in such a case, and we compute the resulting Nash equlibria (NE).

This leads to investigate some interesting properties of the problem, such as the existence and number of the NEs, as well as their properties. We ultimately identify that the problem may possess multiple NEs, and a discussion of the resulting price of anarchy (PoA) is derived [12].

These results can be utilized to analyze the strategic interaction aimed at securing the communication, from both perspectives of attackers and defenders. Also, they can be exploited to understand the efficiency of distributed actions by agents acting without any preliminary cooperation, which is the purpose of quantifying the system efficiency through the lens of the PoA. Finally, we can also envision extensions to broader strategic scenarios possibly combining multiple objectives. This would be the case where the eavesdropping by Eve is not just undesirable since it causes the AoI of the legitimate transmission to grow, but also exposes some security concerns of the system, in which case the strategic choice would also be related to prevent the eavesdropping [13].

The rest of this paper is organized as follows. In Section II, we present the background of our work and discuss the related literature. Section III describes the resulting formulation of the game. Section IV shows numerical results. Finally, Section V concludes the paper.

II. Background

Consider Alice sending status updates to a legitimate receiver named Bob. AoI is a performance indicator that quantifies the freshness of information received, and can be computed as [1], [2]

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

where $u(t)$ is the instant when the receiver processed the last update before time t. In the following, we will distinguish between AoI values at different receivers (legitimate or not) by means of subscripts. For example, we denote with $\delta_{\mathrm{B}}(t)$ and $\delta_{\mathrm{E}}(t)$ the AoI values received by Bob and Eve, respectively. Other quantities will receive analogous subscripts when appropriate.

We assume that Alice generates updates according to a memoryless process with rate λ updates/second and Bob handles them with exponentially distributed times and FCFS policy. The resulting system is therefore an M/M/1 queue and we can exploit the seminal reference [4], where the average AoI $\Delta = \mathbb{E}[\delta(t)]$ for this kind of system was found as

$$\Delta = \lambda\big(\mathbb{E}[XT] + \mathbb{E}[X^2]/2\big)\,, \tag{2}$$

with X and T being the random interarrival time and system time of each generated update, respectively. For simplicity, in the following we consider a unitary service rate, i.e., $\mu = 1$ in the standard queueing system notations. Also according to [4], we then obtain

$$\Delta = 1 + \frac{1}{\lambda} + \frac{\lambda^2}{1-\lambda}\,. \tag{3}$$

Notice that, as already argued by [4], an AoI-optimal update generation rate is neither too strong nor too weak. More precisely, the minimum of (3) is found in $\lambda^* \approx 0.531$.

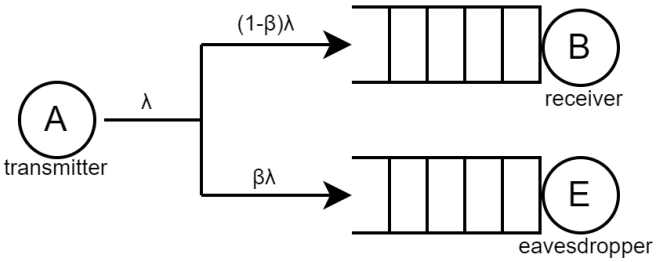

Fig. 1. Partially degraded wiretap channel with a transmitter (A), a legitimate receiver (B), and an eavesdropper (E).

In this paper, we apply this mathematical framework to a quantum wiretap channel [7]. Thus, we consider the additional presence of an eavesdropper (Eve). We assume that each update sent by Alice can be eavesdropped by Eve. For simplicity, this takes place according to an independent identically distributed (i.i.d.) Bernoulli process with parameter $\beta \in [0, 1]$. This means that each piece of information sent by Alice is eavesdropped by Eve with probability β, independent of what happened to the other transmissions.

Moreover, we assume that updates captured by Eve do not reach Bob. In quantum communications, Bob can detect what updates were eavesdropped by Eve and decides to ignore them. Thus, each update is either received by Bob or eavesdropped by Eve, with respective probabilities $1-\beta$ and β. Note the important difference with [10], due to the communication taking place over a quantum channel – in that study a classic channel was considered, therefore the probabilities of the packet being available at Bob's and Eve's were 1 and β, respectively. More complex models can also be adopted to evaluate the eavesdropping capacity obtained by Eve [14] as well as the reduced (secrecy) capacity of the legitimate quantum channel [8], but the essence of the strategic interaction will be the same.

Once again, for the purposes of our analysis it makes sense to assume that Bob's detection procedure of eavesdropped packets is near-perfect [15]. Also, the same model can be applied to, for example, cases where the physical communication medium is hijacked by Eve so that the update itself does not even reach Bob.

The eavesdropped packets are enqueued separately by Eve and processed with FCFS policy and exponentially distributed service with rate $\mu = 1$.

As a result, we are in the presence of not just one, but two M/M/1 queues, one at Bob's and another at Eve's end, respectively. The flow of updates generated by Alice with rate λ splits into two memoryless flows with rate $(1-\beta)\lambda$ and $\beta\lambda$, respectively. The resulting scenario is represented in Fig. 1.

The above problem represents an original extension of the theory. While the application of queueing theory to AoI investigations has been a fertile ground of investigations in the recent literature, most of the departures from the classic scenario relate to the extensions to different queueing systems, basically covering the entire variety of Kendall's notation for

what concerns the arrival or service processes, the buffer size, or the queueing policy, such as adding priorities or preemptions [1]–[3], [16]–[18]. Our evaluation is actually orthogonal to these variations. Thus, while we just analyze the M/M/1 queue for the sake of simplicity, any other different system can be considered as well, which is left for future studies.

The presence of an eavesdropping in the scenario can also be addressed as a security concern. Indeed, for those applications where AoI is relevant (mission-critical, real-time scenarios), security is likely to be another major concern. In this sense our contribution also relates to [10] and [13]. These papers study the problem of eavesdropping attacks, where the intended transmitter Alice has multiple objectives, namely, to keep the AoI value at Bob's side to be low, while at the same time maximizing the age of information for the updates captured by Eve. In general, this is achieved by *reducing* the transmission rate so as to leak the lowest possible information to the adversary.

In the scenario investigated in the present paper, Alice and Eve, while being later formalized as players in a non-cooperative game, are not directly adversaries but just competitors. Especially, neither of them wants to maximize the AoI of the other. As a result, the problem is inherently different, with the particular conclusion that Alice ought to *increase* the data injection rate instead, to compensate the updates lost due to Eve's action. Incidentally, this also marks a difference with a relatively restricted group of other papers, where a third party acts an adversary of Alice and Bob's, but is not interested in acquiring information. For example, in [19] a generic adversary is considered with the only goal to disrupt the legitimate communication exchange. Conversely, [20] considers that the communication exchange between Alice and Bob is closely monitored by a warden (Willie) that must be avoided.

III. System Model

Following [4], and according to the previous assumptions about the rate of update feeding each queue, we can denote the average age of information values at Bob's and Eve's sides, respectively, as Δ_{B} and Δ_{E}, and compute them as

$$\Delta_{\mathrm{B}}(\lambda,\beta) = 1 + \frac{1}{(1-\beta)\lambda} + \frac{(1-\beta)^2\lambda^2}{1-(1-\beta)\lambda}\,, \tag{4}$$

$$\Delta_{\mathrm{E}}(\lambda,\beta) = 1 + \frac{1}{\beta\lambda} + \frac{\beta^2\lambda^2}{1-\beta\lambda}\,. \tag{5}$$

Now, we frame a scenario of interaction between Alice (A) and Eve (E) in a game theoretic fashion [21]. Alice is taken as the only strategic agent in the party of the intended transmitter-receiver pair (Alice–Bob), as we treat Bob as passive, implying he has no control over the outcome. Conversely, A and E can modify both AoI values in (4)–(5) through their actions and are then taken as players in a static game of complete information, with continuous-space action sets. More precisely, the game is formalized as $\mathcal{G} = (\mathcal{N}, \mathcal{A}, \mathcal{U})$, where the set of players $\mathcal{N}$ consists of just A and E. We assume that A can tune the injection rate of generated data, so A's action is to choose $\lambda \in [0, +\infty)$. At the same time, E can instead choose the probability of eavesdropping $\beta \in [0, 1]$.

The objectives of the players relate to lower the AoI values on their side, i.e., Δ_{B} and Δ_{E} for A and E, respectively. However, it may be unrealistic to assume that they can both increase their activity without any consequence, so we also impose a cost to both players. The cost term is directly proportional to their action value, through a *unit price* coefficient, respectively denoted as c for Alice, and k for Eve. The precise choice of a proportional cost is related to framing the limitations of the players through shadow prices, i.e., Lagrange multipliers [11]. Moreover, we note that the AoI terms follow an opposite trend with respect to what usually considered in game theory as a *utility*, that is, a quantity that the players would like to increase. For this reason, we take the utilities as

$$\begin{aligned} u_{\mathrm{A}}(\lambda,\beta) &= [\Delta_{\mathrm{B}}(\lambda,\beta)]^{-1} - c\lambda \\ u_{\mathrm{E}}(\lambda,\beta) &= [\Delta_{\mathrm{E}}(\lambda,\beta)]^{-1} - k\beta\,. \end{aligned} \tag{6}$$

While other choices are possible (e.g., even just changing the sign of Δ in the utility definition would work), the definitions above have the advantage that the AoI values are positive and going to infinity in the worst case, so the first part of each player's utility definition is at least 0 [22]. The negative term representing the cost implies that the player is active only whenever her activity improves her AoI value, otherwise she just choose being inactive that results in zero utility.

The typical game theoretic approach [21] requires at this point to look for the NEs of the system, typically seen as the stable operation points from the perspective of strategic users. To this end, we observe that the choices of λ and β by A and E, respectively, are intertwined, and each player can compute her best response (BR) to the belief about the choice of the other. In particular, we can denote as $\lambda^\star(\beta)$ Alice's BR to the choice of Eve, whereas $\beta^\star(\lambda)$ is clearly the opposite (Eve's BR to Alice's choice). Formally:

$$\begin{aligned} \lambda^\star(\beta) &= \underset{\lambda\in[0,\infty)}{\arg\max}\; u_{\mathrm{A}}(\lambda,\beta)\,, \\ \beta^\star(\lambda) &= \underset{\beta\in[0,1]}{\arg\max}\; u_{\mathrm{E}}(\lambda,\beta)\,. \end{aligned} \tag{7}$$

It is immediate to verify [10] that the utilities are concave functions and therefore they admit a unique maximum in the definitions above. Moreover, the NEs are the strategy profiles for which these BR conditions are mutually satisfied, which can instead correspond to one or multiple points, depending on the unit prices c and k.

While the overall problem of finding such solutions is of limited numerical complexity, and therefore can be computed precisely, it is unfortunately difficult to find a precise analytical expressions for them, due to the inherent complications of solving (7) through an exact computations of the gradients and equating the curves. Thus, in the following we will resort to numerical evaluations.

As visible from the following sample results, the number of intersections can change depending on the values of c and k. For the case where $c = k = 0$, displayed in Fig. 2, the best

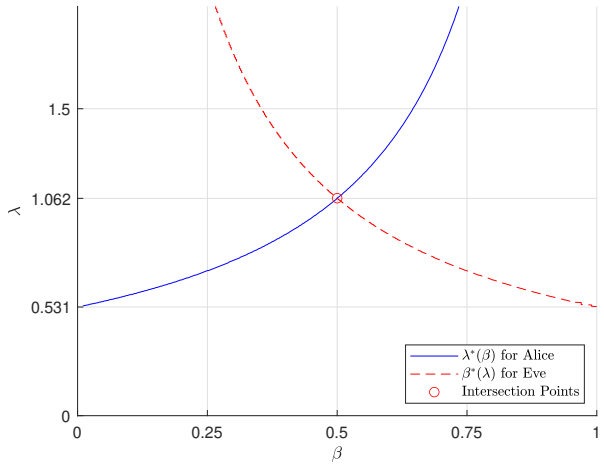

Fig. 2. Best responses of Alice and Eve's for c=0.0, k=0.0.

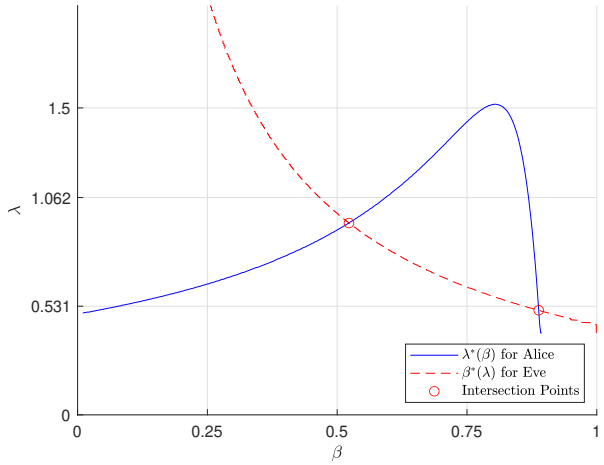

Fig. 3. Best responses of Alice and Eve's for c=0.1, k=0.1.

response of the players follow a monotonic behavior and have a single intersection. In this case, the solution is found for $\lambda = 1.062$, twice as much as the classic result from [4], and $\beta = 0.5$. That is, it is convenient for Alice to yield to the presence of Eve and just provide information for both receivers.

When the unit prices increase, the behavior at first just translates to lower and higher values for Alice and Eve, respectively. As the prices keep increasing, the curves bend and the number of intersections may increase. Fig. 3 shows that for $c = 0.1$, $k = 0.1$, there are two intersections. Thus, multiple intersections may be present, or none if the costs are increased further, in which case the BR of either player may degenerate to a border condition, e.g., $\lambda = 0$ or $\beta = 0$, which implies that the costs are too high for that player to be active – this condition is not very interesting for practical purposes.

If we limit the analysis to cases where the curve do intersect and the NEs do not degenerate, we find out that there is always one NE as the left-most of the intersection points in the graphs shown. In the following, we will refer to this as the *primary* NE of the system. Additional NEs are called *secondary* NE and are generally less efficient, as will be shown next via numerical computations.

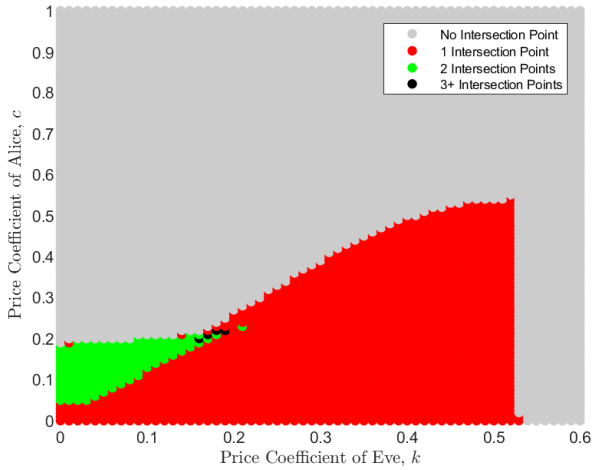

Fig. 4. Number of intersections for different unit prices of Alice and Eve

It becomes therefore interesting to investigate the PoA for our game, especially in the presence of multiple NE. While the literature contains slightly different definitions to translate the concept of PoA in practice, it always relates to computing the ratio between costs for inefficient equilibria vs. the best that can be achieved [12].

For the problem at hand, we precisely define the PoA following a similar rationale, as

$$\text{PoA} = \frac{u_{\text{A}}(\lambda_0, \beta_0) + u_{\text{E}}(\lambda_0, \beta_0)}{u_{\text{A}}(\lambda_{\text{w}}, \beta_{\text{w}}) + u_{\text{E}}(\lambda_{\text{w}}, \beta_{\text{w}})} \tag{8}$$

where the sum of the utilities of the players is chosen as an indicator of *social welfare* and also: $\lambda_{\text{w}}, \beta_{\text{w}}$ represents the worst possible NE, whereas λ_0, β_0 is the social optimum, i.e., the strategic choices that maximizes the welfare. As we will show in the next, the primary NE is also achieving the social optimum. Thus, the PoA is 1 in the presence of only one NE, but it might soar when the game admits multiple NEs, due to the very low welfare of secondary NEs.

IV. Numerical Results

In the following, we compute relevant quantities for different values of c and k, which are taken as system parameters. In particular, we sketch the numerical evaluations that lead to conclude that the primary NE is always the social optimum, and we compute the PoA in the presence of multiple equilibria.

Fig. 4 shows the number of intersection points of λ and β curves. In case c=0, there is a single intersection, even if k increases. Multiple NEs are present when c is larger than 0 but not too high and also k is contained. For too high costs, the problem degenerates into a trivial solution, as follows. If k is too high for the BRs to intersect, then Eve does not intercept any information and the equilibrium is at β=0. If c is too high instead, then Alice does not even transmit, so the equilibrium is at λ=0, β=0.

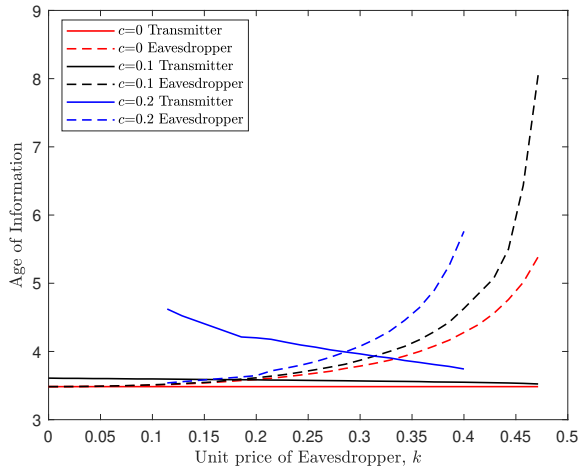

Fig. 5. AoI vs Eve's unit price for different unit prices of Alice, primary NE

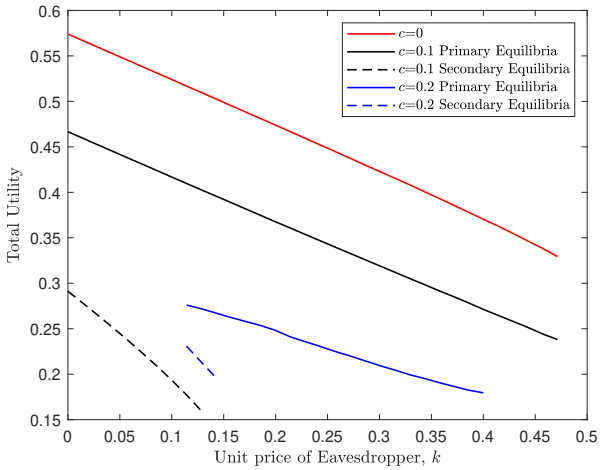

Fig. 7. Social welfare vs unit price of Eve for different unit prices of Alice.

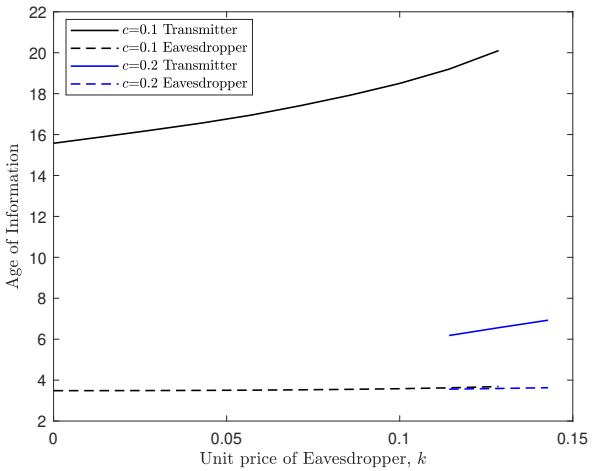

Fig. 6. AoI vs Eve's unit price for different unit prices of Alice, secondary NE

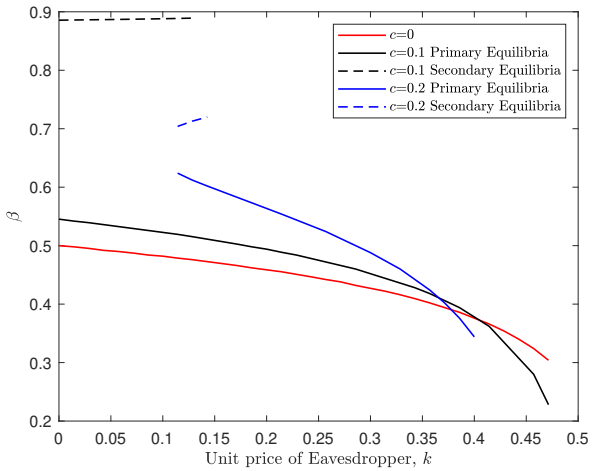

Fig. 8. Eavesdropping probability β for different prices

Fig. 5 plots AoI values at the primary NE vs k, for different values of c. AoI at Eve's increases in k, whereas AoI at Bob's decreases, but the latter trend is much more limited. Conversely, a higher c implies that *both* AoI values increase, which is a consequence of the parasitic behavior of Eve that must rely on Alice being able to transmit at low cost.

Fig. 6 shows instead the same plot but for the secondary NE, whenever present. It is interesting to observe the increasing behavior in Bob's AoI for an increasing k (the same holds for Eve but to a limited extent). This happens because the secondary NEs take place in the decreasing part of Alice's BR, but it is a sign that these NEs are inefficient. Comparing Figs. 5 and 6 makes it clear that the range of AoI values for the secondary NE(s) is much higher than that for the primary NE. This is further confirmed by Fig. 7 where the total welfare is shown. As a result, the total welfare at the primary NE point is always higher than the secondary, which implies that the primary NE is Pareto dominant and the social optimum [23]. Thus, when a single NE is present, the PoA is one. In case of multiple NEs, the PoA can be computed as the ratio between the total utility at the primary NE (also the social optimum) and the secondary NE. Fig. 7 also shows that the total welfare decreases with higher costs, with the only exception of the secondary NE, whose welfare increases in c, but this is a consequence of its aforementioned inefficiency.

Figs. 8 and 9 show the activity patterns of the players. For the primary NE, Fig. 8 shows that β decreases in k, at first slowly, then it drops down. Also, k increases in c, which is explained by Alice decreasing her rate of updates, which Eve counteracts by capturing them more often. In Fig. 9 a similar trend is shown for λ vs k, but the reason is different. Due to the presence of Eve, Alice starts with an enlarged transmission rate with respect to the optimal λ without eavesdropping, equal to 0.531 as per [4]. As parameter k increases, Eve is less active and Alice can relax her rate increase. Moreover, it can be seen, confirming the previous results, that the optimal λ decreases in c, and the secondary NEs generally correspond to inefficient allocations where β is much higher and λ is lower.

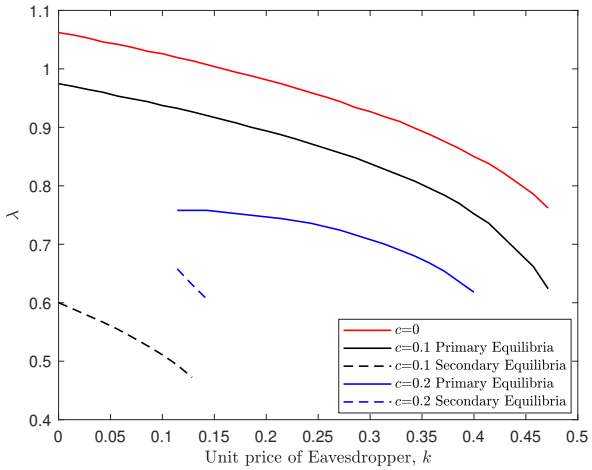

Fig. 9. Alice's transmission rate λ for different prices

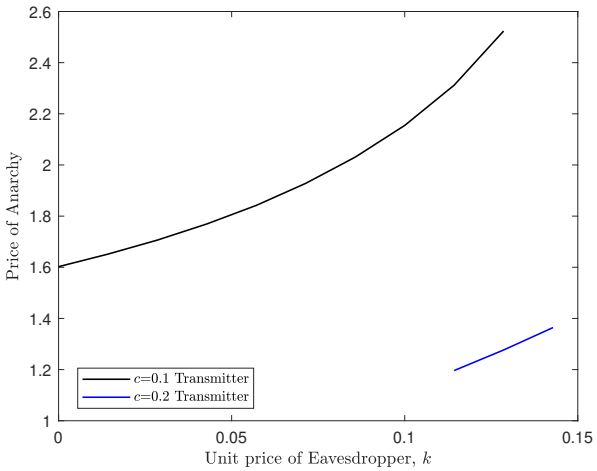

Fig. 10. PoA versus unit price of Eve for different unit prices of Alice

Finally, Fig. 10 evaluates the PoA, which exhibits a complex behavior. When only one NE is present, the PoA is 1. This signifies that the problem admits an efficient distributed solution, and in reality even achieves the social optimum. Conversely, when multiple NE are present, the PoA can be very high. In particular, this happens for relatively low values of c and k, albeit not zero.

V. Conclusions

We presented an analysis of a quantum wiretap channel seen as a queueing system, for which we introduced a game theoretic analysis of the interaction between the legitimate transmitter and an eavesdropper, of which the former is aware. The latter not only captures information, which is not a concern for this specific setup, but also reduces the amount of information transmitted to the intended receiver.

The strategic choices of the players depend on both AoI and a cost term to prevent perennial transmission and eavesdropping. For this scenario, we numerically quantified the number of NEs and the resulting PoA, as functions of the cost parameters in the transmission of the users.

Our results contribute to a better understanding of security in quantum communications, and can be extended to more complex cases with multiple objectives, such as simultaneously minimizing AoI and thwarting potential eavesdroppers.

References

[1] R. D. Yates, Y. Sun, D. R. Brown, S. K. Kaul, E. Modiano, and S. Ulukus, "Age of information: An introduction and survey," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 5, pp. 1183–1210, 2021.

[2] 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.

[3] 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, 2020.

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

[5] L. Crosara and L. Badia, "Cost and correlation in strategic wireless sensing driven by age of information," in *Proc. European Wireless*, 2022.

[6] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2384–2428, 2021.

[7] H. Boche, M. Cai, N. Cai, and C. Deppe, "Secrecy capacities of compound quantum wiretap channels and applications," *Phys. Rev. A*, vol. 89, no. 5, p. 052320, 2014.

[8] J. Wu, Z. Lin, L. Yin, and G.-L. Long, "Security of quantum secure direct communication based on Wyner's wiretap channel theory," *Quantum Engin.*, vol. 1, no. 4, p. e26, 2019.

[9] P. Hofmann, J. A. Cabrera, R. Bassoli, M. Reisslein, and F. H. Fitzek, "Coding in diffusion-based molecular nanonetworks: A comprehensive survey," *IEEE Access*, vol. 11, pp. 16 411–16 465, 2023.

[10] 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.

[11] L. Badia, S. Merlin, A. Zanella, and M. Zorzi, "Pricing VoWLAN services through a micro-economic framework," *IEEE Wireless Commun.*, vol. 13, no. 1, pp. 6–13, 2006.

[12] 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.

[13] 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

[14] G. Smith, "Quantum channel capacities," in *Proc. IEEE ITW*, 2010.

[15] G. Castro and R. V. Ramos, "Enhancing eavesdropping detection in quantum key distribution using disentropy measure of randomness," *Quantum Inf. Proc.*, vol. 21, no. 2, p. 79, 2022.

[16] 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, 2021.

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

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

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

[20] X. Lu, S. Yan, W. Yang, M. Li, and D. W. K. Ng, "Covert communication with time uncertainty in time-critical wireless networks," *IEEE Trans. Wireless Commun.*, vol. 22, no. 2, pp. 1116–1129, 2022.

[21] D. Bauso, *Game theory with engineering applications*. SIAM, 2016.

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

[23] 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.