Delay Performance of a Two-User Broadcast Channel with Security Constraints

Antonia Arvanitaki¹ · Nikolaos Pappas² · Parthajit Mohapatra³ · Niklas Carlsson¹

Received: 22 July 2019 / Accepted: 6 December 2019 / Published online: 21 December 2019
© The Author(s) 2019

Abstract

In this paper, we consider the two-user broadcast channel with security constraints. We assume that a source broadcasts packets to two receivers, and that one of them has secrecy constraints, i.e., its packets need to be kept secret from the other receiver. The receiver with secrecy constraint has full-duplex capability, allowing it to transmit a jamming signal to increase its secrecy. We derive the average delay per packet and provide simulations and numerical results, where we compare different performance metrics for the cases when both receivers treat interference as noise, when the legitimate receiver performs successive decoding, and when the eavesdropper performs successive decoding. The results show that successive decoding provides better average packet delay for the legitimate user. Furthermore, we define a new metric that characterizes the reduction on the success probability for the legitimate user that is caused by the secrecy constraint. The results show that secrecy poses a significant amount of packet delay for the legitimate receiver when either receiver performs successive decoding. We also formulate an optimization problem, wherein the throughput of the eavesdropper is maximized under delay and secrecy rate constraints at the legitimate receiver. We provide numerical results for the optimization problem, where we show the trade-off between the transmission power for the jamming and the throughput of the non-legitimate receiver. The results provide insights into how channel ordering and encoding differences can be exploited to improve performance under different interference conditions.

Keywords Broadcast channel · Delay · Queueing · Security constraints

Introduction

Due to the broadcast nature of the wireless medium, communication over a wireless channel is susceptible to eavesdropping. Secure communication is one of the critical issues

for current and future wireless networks, and physical layer secrecy has emerged as a promising approach for ensuring secure communication over wireless channels in the last decade.

Most of the works in physical layer secrecy assume that users have always data to transmit. However, in many practical scenarios, the arrival of data is bursty in nature and the notion of stable throughput or region becomes a meaningful measure for such scenarios [2–6]. However, the exact characterization of delay is rather difficult, even in small multiple access networks, and remains unexplored in most cases [6].

Related Work

The broadcast channel has been studied extensively with and without secrecy constraints in the existing literature [7–11]. In [7], the problem of secure communication is investigated for the broadcast channel, where the transmitter needs to send a confidential message to one of the receivers and also needs to send a common message to both of the receivers. The role of cooperation for secure communication when using a broadcast channel is studied in [9]. The effects on

This work was presented in part in [1].

✉ Nikolaos Pappas
nikolaos.pappas@liu.se
Antonia Arvanitaki
antonia.arvanitaki@liu.se
Parthajit Mohapatra
parthajit@iittp.ac.in
Niklas Carlsson
niklas.carlsson@liu.se

¹ Department of Computer and Information Science, Linköping University, Linköping, Sweden

² Department of Science and Technology, Linköping University, 60174 Norrköping, Sweden

³ Department of Electrical Engineering, Indian Institute of Technology, Tirupati, India

the capacity of the broadcast channel without secrecy constraints are studied in [10, 11]. However, characterizing the capacity and communication latency of a broadcast channel, even without secrecy constraints, is still an open problem.

The role of fading in secure communication has been explored in [8, 12]. In [8], the problem of secure communication is considered over a wiretap channel where the channel between different communicating nodes undergo quasi-static fading. In [8], it is shown that in the presence of fading, the legitimate transmitter can communicate securely even when the eavesdropper has a better SNR than the legitimate receiver. The impact of fading on the secrecy capacity of the broadcast channel has been explored in [12]. The effect of fading on secrecy for other communication models can be found in [13–15].

The problem of secure communication over multihop wireless networks has also been investigated [16–19]. Lai and Garnal [16] explores security enhancement through the use of relay nodes. In [17], it is shown how the intrinsic properties of multilevel wireless networks can be exploited to support network secrecy. The impact of secrecy constraints on the throughput of large-scale decentralized network has been analyzed in [18]. In [19], the scalability of physical layer-based approaches, which exploit the dynamics of wireless fading channels, is studied for a large wireless network.

Recently, there has been rapid growth in the area of supporting real-time applications, which means that there is a need to provide delay-based guarantees. For many future wireless networks, security and delay are required to be considered jointly for the performance analysis of the networks. At the same time, decoding ability of the users can impact the performance of the users significantly. To explore the impact of security and delay constraint on the performance, we have considered a two-user broadcast channel (BC) under various decoding schemes. The transmitter has two queues, where one of the queues has confidential data and the other queue has non-confidential data. The work also considers different traffic conditions at the queues. In particular, the delay performance is analyzed for the BC with secrecy constraint under various decoding schemes such as both the receivers treat interference as noise and one of the receivers treat interference as noise and the other receiver performs successive decoding.

Contribution

In this paper, we study the average delay performance of a two-user broadcast channel with security constraints and different traffic conditions at the queues. It is assumed that the receiver whose packets require secrecy has full-duplex capability. Hence, the receiver can send a jamming signal to hinder decoding of the sensitive information at the

non-legitimate receiver. However, the full-duplex operation of the receiver results in self-interference at its own receiver, which can hamper decoding of its own message. The delay performance of the system depends on the secrecy constraint as well as on the jamming power and degree of self-interference cancelation at the receiver. The main contribution of this paper is to characterize the average delay performance for the legitimate receiver; in addition, we introduce a new metric that characterizes the reduction on the success probability for the legitimate user that is caused by the secrecy constraint. This metric can also characterize the tradeoff between secrecy and achieved throughput without secrecy. The paper also formulates an optimization problem, where the throughput of the receiver that does not have a secrecy constraint is maximized under delay and secrecy rate constraints for the legitimate receiver. To the best of our knowledge, the delay performance of a two-user broadcast channel with security constraints using different decoding schemes and different queue conditions (saturated queue and non-saturated queue), and a metric that characterizes the trade-off between secrecy and throughput performance has not been explored in the existing literature. In this work, we show how different decoding schemes can affect performance metrics such as average packet delay, saturated throughput, and the average queue size.

Structure of the Paper

The remainder of this paper is organized as follows. In the next section, we present some prior work used in the proposed method. In the subsequent section, we introduce the throughput analysis for different decoding schemes, and traffic at the source, followed by which we characterize the delay performance of the legitimate user. Before the concluding section, we provide numerical and simulation results, where we compare different performance metrics for different decoding schemes, and traffic at the source. Finally, we conclude the paper.

System Model

We consider a two-user broadcast channel (BC), where a single source S sends packets from two separate queues Q_i to two different users (receivers) D_i , where $i = 1, 2$, as shown in Fig. 1. Here, we use Q_i to denote both the queue size of the queue that holds the packets for receiver D_i and to refer to the queue itself. Queue Q_1 holds sensitive information; thus, these packets must be kept secret from D_2 . In contrast, queue Q_2 contains non-sensitive packets intended for receiver D_2 . Time is assumed to be slotted.

The arrival process at Q_1 is assumed to be Bernoulli with mean λ_1 ; thus, within a given time slot, a packet arrives

Fig. 1 The system model where queue Q_1 has bursty traffic with arrival rate λ_1 and a queue Q_2 which is saturated. Receiver D_1 transmits a jamming signal of power P_J to receiver D_2 to hinder eavesdropping

with probability λ_1 . Queue Q_2 is assumed to be saturated, thus it can capture the case of heavy traffic scenario, where $Pr(Q_2 = 0) \approx 0$, thus it can overestimate the interference that is caused to the other transmission.

When queue Q_1 is non-empty, source S transmits two messages in a single time slot using superposition coding. When queue Q_1 is empty, source S sends the packet intended for receiver D_2 , with power P_2 . The total power budget at the source is $P_{\max}$. The capacity of both queues is infinite, i.e., there is no packet dropping. Moreover, it is assumed that packets not successfully transmitted in a time slot will be retransmitted until they are received by their intended destination. Packet transmission occurs at the beginning of the time slot. Finally, the packet arrivals happen at the end of the time slot. It is assumed that the transmission of acknowledgement (ACKs) is instantaneous and error free.

We assume that the legitimate receiver D_1 has full-duplex capability, i.e., it can receive and transmit simultaneously. Hence, receiver D_1 can send a jamming signal to receiver D_2 to prevent D_2 from decoding the packet that is intended for D_1 . Thus, we assume that D_1 transmits a jamming signal when $Q_1 \neq 0$, otherwise is silent. In this work is assumed that D_1 is aware of the state of its intended queue, this can be achieved by the transmission of a control packet only when that queue is empty. We assume that this transmission is instantaneous and error free. The simultaneous transmission and reception at D_1 causes self-interference. It is assumed that the self-interference cancelation at receiver D_1 is imperfect and that the residual self-interference is modelled as a scalar g , where $g \in [0, 1]$. For $g = 0$, we have perfect self-interference-based cancelation, whereas for $g = 1$, there is no cancelation at receiver D_1 [20–22].

We assume that the channel between source S and receiver D_i is subject to Rayleigh fading. The signals that are received at the receivers, when both queues are non-empty, are as follows:

$$\begin{aligned} y_1[t] &= h_1 x[t] + g x_J[t] + z_1[t], \\ y_2[t] &= h_2 x[t] + h_{12} x_J[t] + z_2[t], \end{aligned} \quad (1)$$

where z_i ($i = 1, 2$) is additive white Gaussian noise with zero mean and unit variance, h_i is the channel gain from source S to receiver D_i , h_{12} is the channel gain from D_1 to D_2 , x_i is the signal that the source S transmits to the receiver D_i , x_J is the jamming signal, and g is the self-interference cancelation coefficient. Note that x_1 and x_2 are independent. Due to the transmission of the jamming signal, the self-interference affects the reception of the sensitive information by the legitimate receiver. The source transmits the signal $x[t] = x_1[t] + x_2[t]$, when both queues have packet, t indicates the time slot. When queue Q_1 is empty, the transmitted signal is $x[t] = x_2[t]$. We also assume that both receivers have multipacket reception (MPR) capabilities. Specifically, a receiver can decode its intended transmission even when both queues are active and two packets are transmitted in a time slot based on the received signal-to-interference and noise ratio (SINR)/signal-to-noise ratio (SNR).

The probability that the legitimate receiver can successfully decode the packets originated by queue Q_1 and that the eavesdropper cannot decode the packet is denoted by $Pr(D_{1/T}^s)$, where T denotes the set of the queues containing messages, and s indicates the event that a message intended for receiver D_1 contains confidential information. Moreover, $Pr(D_{2/T})$ represents the probability that the eavesdropper can successfully decode the packets transmitted by queue Q_2 . The mentioned probabilities depend on the decoding scheme and in the next section we will provide their exact characterization.

Throughput Analysis

We consider two schemes to decode the packets that are intended for receiver D_i : *successive decoding* and *treating interference as noise*. In the successive decoding scheme, the receiver first decodes the unintended packet and cancels its effect before decoding the intended packet. In the case of treating interference as noise, the receiver decodes the intended packet by treating the other packet as noise. Based on the different decoding schemes at the receivers, we consider three cases. In the first case, we consider that both of the receivers treat interference as noise. In the second case, we assume that receiver D_1 performs successive decoding and receiver D_2 treats interference as noise. In the third case, receiver D_2 performs successive decoding and receiver D_1 treats interference as noise. Finally, we note that the case where both receivers D_1 and D_2 perform successive decoding is infeasible in terms of power allocation for the two receivers as shown in [4]. In the following, the aforementioned cases are presented with

different traffic assumptions at Q_1 and Q_2 , in contrast with [5], where the case where one queue has bursty traffic and other queue has saturated traffic is not considered.

Queue Q_1 Has Bursty Traffic, While Queue Q_2 Is Saturated

In this case, the average service probabilities for queues Q_1 and Q_2 are given, respectively, by

$$\mu_1 = Pr(D_{1/1,2}^s), \quad (2)$$

$$\mu_2 = Pr(Q_1 > 0)Pr(D_{2/1,2}) + Pr(Q_1 = 0)Pr(D_{2/2}). \quad (3)$$

The probability of success $Pr(D_{2/2})$ is given by

$$Pr(D_{2/2}) = Pr\{SNR_2 \geq \gamma_2\} = \exp\left(-\frac{\gamma_2 d_2^\alpha}{P_2}\right), \quad (4)$$

where $SNR_2 = P_2|h_2|^2 d_2^{-\alpha}$, with P_2 being the transmit power, h_2 being the Rayleigh block fading channel gain from source S to receiver 2, d_2 being the distance between source S and receiver D_2 , and α being the path loss exponent. When both queues Q_1 and Q_2 are non-empty, the probability that the SINR requirement is satisfied depends on the decoding scheme. Table 1 summarizes the notations used in the following equations.

The probability that queue Q_1 is empty is given by

$$Pr(Q_1 = 0) = 1 - \frac{\lambda_1}{Pr(D_{1/1,2}^s)}. \quad (5)$$

From (2) and (5), we can obtain the service probability for queue Q_2 , given by

$$\mu_2 = Pr(D_{2/2}) - \frac{Pr(D_{2/2}) - Pr(D_{2/1,2})}{Pr(D_{1/1,2}^s)} \lambda_1. \quad (6)$$

Below we present the three cases regarding the decoding schemes at the receivers and provide the success probabilities.

Case 1 (Both receivers treat interference as noise) The probability of success that the legitimate receiver decodes the packet transmitted by source S to the legitimate receiver is given by

$$Pr(D_{1/1,2}^s) = \exp\left(-\frac{\gamma_1 d_1^\alpha}{P_1 - \gamma_1 P_2} (1 + P_J g^2)\right) \times \left\{1 - \exp\left(-\frac{\gamma_1 d_2^\alpha}{P_1 - \gamma_1 P_2}\right) [1 + \gamma_1 \frac{P_J}{P_1 - \gamma_1 P_2} \left(\frac{d_2}{d_{12}}\right)^\alpha]^{-1}\right\}, \quad (7)$$

Table 1 List of notations

Notation	Definition
α	Path loss exponent
γ_1	SNR/SINR threshold for the legitimate receiver
γ_2	SNR/SINR threshold for the eavesdropper
P_1	Power transmission for the legitimate receiver
P_2	Power transmission for the eavesdropper
P_J	Jamming power
g	Residual self-interference
d_1	Distance between the source S and the legitimate receiver
d_2	Distance between the source S and the eavesdropper
d_{12}	Distance between the legitimate receiver and the eavesdropper
$P_{\max}$	Total power budget

with P_1 being the transmit power for the legitimate receiver, h_1 being the Rayleigh block fading channel gain from source S to receiver D_1 , d_1 being the distance between source S and receiver D_1 , P_2 being the transmit power for the eavesdropper, α being the path loss exponent, P_J being the jamming power, g being the residual self-interference, h_{12} being the Rayleigh block fading channel gain between the two receivers, and d_{12} being the distance between receiver D_1 and receiver D_2 . Equation (7) is nonzero when $\frac{P_1}{P_2} > \gamma_1$.

The probability of success that the legitimate receiver can decode the packets intended for it without the secrecy constraint, $Pr(D_{1/1,2})$, is given by

$$Pr(D_{1/1,2}) = \exp\left(-\frac{\gamma_1 d_1^\alpha}{P_1 - \gamma_1 P_2}\right), \quad (8)$$

when $P_1 > \gamma_1 P_2$.

The probability of success $Pr(D_{2/1,2})$ is given by

$$Pr(D_{2/1,2}) = \frac{\exp\left(-\frac{\gamma_2 d_2^\alpha}{P_2 - \gamma_2 P_1}\right)}{1 + \gamma_2 \frac{P_J}{P_2 - \gamma_2 P_1} \left(\frac{d_2}{d_{12}}\right)^\alpha}, \quad (9)$$

and it is nonzero when $\frac{P_2}{P_1} > \gamma_2$. If we want to consider the system without secrecy constraints, then we replace $P_J = 0$ in (9). The derivations for (7) and (9) are based on the Rayleigh fading assumption [5].

Case 2 (Receiver D_1 performs successive decoding and receiver D_2 treats interference as noise) In this case, $Pr(D_{1/1,2}^s)$ is given by

$$Pr(D_{1/1,2}^s) = \exp \left(-\max \left\{ \frac{\gamma_2(1+g^2P_J)d_1^\alpha}{P_2-\gamma_2P_1}, \frac{\gamma_1(1+g^2P_J)d_1^\alpha}{P_1} \right\} \right) \times \left[1 - \exp \left(-\frac{\gamma_1 d_2^\alpha}{P_1 - \gamma_1 P_2} \right) \right] \times \left\{ 1 + \gamma_1 \frac{P_J}{P_1 - \gamma_1 P_2} \left(\frac{d_2}{d_{12}} \right)^\alpha \right\}^{-1}. \quad (10)$$

The details of the proof can be found in [5].

The probability of success $Pr(D_{1/1,2})$ that the legitimate receiver can decode the packets intended for it without secrecy is given by

$$Pr(D_{1/1,2}) = Pr \left(\frac{P_2|h_1|d_1^{-\alpha}}{1+P_1|h_1|d_1^{-\alpha}} \geq \gamma_2, P_1|h_1|d_1^{-\alpha} \geq \gamma_1 \right). \quad (11)$$

After some simplifications, $Pr(D_{1/1,2})$ is given by

$$Pr(D_{1/1,2}) = \begin{cases} \exp \left(-\frac{\gamma_2 d_1^\alpha}{P_2 - \gamma_2 P_1} \right), & \text{if } \gamma_2 P_1 < P_2 \leq P_1 \frac{\gamma_2(1+\gamma_1)}{\gamma_1}, \\ \exp \left(-\frac{\gamma_1 d_1^\alpha}{P_1} \right), & \text{if } P_2 > P_1 \frac{\gamma_2(1+\gamma_1)}{\gamma_1}. \end{cases} \quad (12)$$

Case 3 (Receiver D_1 treats interference as noise and receiver D_2 performs successive decoding) In this case we consider that receiver D_2 has the capability to perform successive decoding. Since the eavesdropper has the capability to perform successive decoding, then if it fails, it makes sense to assume that it will try to decode the packet by treating interference as noise. Thus, by following the same methodology as in [5], $Pr(D_{1/1,2}^s)$ is given by

$$Pr(D_{1/1,2}^s) = \exp \left(-\frac{\gamma_1 d_1^\alpha}{P_1 - \gamma_1 P_2} (1 + P_J g^2) \right) \times \left[\frac{\exp \left(-\frac{\gamma_2 d_2^\alpha}{P_2 - \gamma_2 P_1} \right)}{1 + \frac{\gamma_2 P_J}{P_2 - \gamma_2 P_1} \left(\frac{d_2}{d_{12}} \right)^\alpha} - \frac{\exp \left(-\frac{\gamma_1 d_2^\alpha}{P_1} \right)}{1 + \gamma_1 \frac{P_J}{P_1} \left(\frac{d_2}{d_{12}} \right)^\alpha} \right] + \exp \left(-\frac{\gamma_1 d_1^\alpha}{P_1 - \gamma_1 P_2} (1 + P_J g^2) \right) \times \left(1 - \exp \left(-\frac{d_2^\alpha}{\max \left\{ \frac{P_2}{\gamma_2} - P_1, \frac{P_1}{\gamma_1} - P_2 \right\}} \right) \right) \times \left\{ 1 + \frac{d_2^\alpha}{\max \left\{ \frac{P_2}{\gamma_2} - P_1, \frac{P_1}{\gamma_1} - P_2 \right\}} P_J d_{12}^{-\alpha} \right\}^{-1}. \quad (13)$$

The probability of success $Pr(D_{1/1,2})$ that the legitimate receiver can decode its packets without secrecy constraints is given by

$$Pr(D_{1/1,2}) = Pr \left(\frac{P_1|h_1|^2 d_1^{-\alpha}}{1 + P_2|h_1|^2 d_1^{-\alpha}} \geq \gamma_1 \right), \quad (14)$$

and its expression is given by (8).

In the following, we will provide the expression for the success probability for receiver 2. Here, receiver 2 first attempts to decode its intended packet by successive decoding. If this fails, it decodes by treating interference as noise. Following the same methodology as in [5] we obtain

$$Pr(D_{2/1,2}) = \exp \left(-\frac{\gamma_2 d_2^\alpha}{P_2 - \gamma_2 P_1} \right) \left[1 + \gamma_2 \frac{P_J}{P_2 - \gamma_2 P_1} \left(\frac{d_2}{d_{12}} \right)^\alpha \right]^{-1} + \frac{\exp(-\gamma_2')}{1 + \gamma_2' P_J d_{12}^{-\alpha}} - \frac{\exp(-\gamma_2'')}{1 + \gamma_2'' P_J d_{12}^{-\alpha}}, \quad (15)$$

where $\gamma_2' \triangleq \min \left\{ \frac{\gamma_1 d_2^\alpha}{P_1 - \gamma_1 P_2}, \frac{\gamma_2 d_2^\alpha}{P_2} \right\}$ and $\gamma_2'' = \frac{\gamma_2 d_2^\alpha}{P_2 - \gamma_2 P_1}$. The probability of success $Pr(D_{2/2})$ is given by (4).

Remark 1 Previously we provided the success probabilities for both cases of secrecy and without secrecy constraints for the legitimate user for several decoding schemes. It is interesting to show the reduction on the success probability for the legitimate user that is caused by the secrecy constraint. Thus, we define the following function f

$$f = 1 - \frac{Pr(D_{1/1,2}^s)}{Pr(D_{1/1,2})}. \quad (16)$$

This function can also model the tolerance on the loss of secrecy to increase the throughput performance, in our case this can be achieved by adjusting the jamming power or the power allocation at the transmitter. This function provides a design factor for our system since it allows to tune the percentage of throughput loss we are willing to sacrifice to impose security constraints for the legitimate user. As $P(D_{1/1,2}^s) \leq P(D_{1/1,2})$, following holds $0 \leq f \leq 1$. In this case, we assume that the feasibility conditions are satisfied so that we do not encounter the case where $P(D_{1/1,2}) = 0$. When $f = 0$, there is no loss due to the secrecy constraints when both the queues have data to send.

Remark 2 The expression for f can be obtained for various decoding schemes using the results in this section. In the following, the expression for f is obtained when both the receivers treat interference as noise. Thus, f is given by

$$f = 1 - \exp\left(-\frac{\gamma_1 d_1^\alpha P_J g^2}{P_1 - \gamma_1 P_2}\right) \times \left\{ 1 - \frac{\exp\left(-\frac{\gamma_1 d_2^\alpha}{P_1 - \gamma_1 P_2}\right)}{1 + \frac{\gamma_1 P_J}{P_1 - \gamma_1 P_2} \left(\frac{d_2}{d_{12}}\right)^\alpha} \right\}. \quad (17)$$

If $P_J = 0$, then we have

$$f = \exp\left(-\frac{\gamma_1 d_2^\alpha}{P_1 - \gamma_1 P_2}\right). \quad (18)$$

In this case, f reduces to the probability that the eavesdropper can decode correctly the packet of the legitimate user if we did not impose security constraint.

In Sect. 4, we will utilize function f as a constraint in an optimization problem.

Both Queues Have Bursty Traffic

In this case, we consider that the queue Q_2 is no longer saturated, but instead has bursty traffic with arrival rate λ_2 . The average service probabilities for queues Q_1 and Q_2 when they have both bursty traffic are given, respectively, by

$$\mu_1 = \Pr(Q_2 > 0) \Pr(D_{1/1,2}^s) + \Pr(Q_2 = 0) \Pr(D_{1/1}^s), \quad (19)$$

$$\mu_2 = \Pr(Q_1 > 0) \Pr(D_{2/1,2}) + \Pr(Q_1 = 0) \Pr(D_{2/2}). \quad (20)$$

As we can see, the average service rate given by (19) and (20) depends on the queue size of Q_2 and Q_1 respectively. Thus, queues Q_1 and Q_2 are coupled, which makes it difficult to compute the average service rates μ_1 and μ_2 . The coupling of the queues can be tackled by applying the stochastic dominance technique, as in [2]. The stochastic dominance technique is based on the construction of dominant systems, where the queue with no packets transmits “dummy” packets and the other one behaves as in the original system. After applying the stochastic dominance technique we can obtain the stability conditions, which was the study of the work in [5]. Here, we focus on the delay performance of this system and more specifically on the delay performance for the legitimate user with secrecy constraints when queue Q_2 does not empty, thus it can overestimate the interference that is caused to the other transmission.

Delay Analysis for the Legitimate User

In this section, we will characterize the delay performance of the legitimate user. Delay has two components, the queueing delay and the transmission delay.

The average transmission delay of a packet from queue Q_1 when it is transmitted by source S to the legitimate receiver is given by

$$\bar{D}_T = \frac{1}{\mu_1}, \quad (21)$$

where μ_1 is the probability of departure for a packet waiting in queue Q_1 .

The average queue size Q_1 , if the queue is stable, is given by

$$\bar{Q}_1 = \frac{\lambda_1}{\mu_1 - \lambda_1} (1 - \lambda_1). \quad (22)$$

Proof: See “Appendix A”.

By Little’s law, the average waiting time of a packet in queue Q_1 is given by

$$\bar{D}_{Q_1} = \frac{\bar{Q}_1}{\lambda_1} = \frac{\frac{\lambda_1}{\mu_1 - \lambda_1} (1 - \lambda_1)}{\lambda_1} = \frac{1}{\mu_1 - \lambda_1} (1 - \lambda_1). \quad (23)$$

The average packet delay for the legitimate receiver is given by

$$\bar{D}_1 = \bar{D}_{Q_1} + \bar{D}_T = \frac{1}{\mu_1 - \lambda_1} (1 - \lambda_1) + \frac{1}{\mu_1}. \quad (24)$$

Optimization Problem

Here, we will consider the maximization of the throughput of the eavesdropper with delay constraints for the legitimate receiver and also a constraint regarding the f function defined in (16). The throughput for the eavesdropper is given by (6). The decision variables for the optimization problem are P_1 , P_2 , and P_J . Since $P_1 + P_2 = P_{\max}$, the optimization variables are reduced to P_1 and P_J . Then, the optimization problem is defined as follows

$$\begin{aligned} \max_{P_1, P_J} & \Pr(D_{2/2}) - \frac{\Pr(D_{2/2}) - \Pr(D_{2/1,2})}{\Pr(D_{1/1,2}^s)} \lambda_1 \\ \text{s.t.} & \bar{D}_1 \leq D^*, \\ & f \leq f^*, \\ & 0 \leq P_1 \leq P_{\max}, \\ & 0 \leq P_J \leq P'_{\max}, \end{aligned} \quad (25)$$

where $\bar{D}_1 \leq D^*$ is the average delay constraint for the legitimate user, f^* is the threshold for the function f given by (16), and the constraint $f \leq f^*$ denotes that the success probability loss due to secrecy for the legitimate user cannot be above f^* . Furthermore, we assume that the arrival probability for the traffic of the legitimate user is fixed and equals to λ_1 . The expressions for the success probabilities depend on the decoding schemes as presented in the previous section.

This optimization problem can model the case where a base station serves simultaneously two users with different secrecy requirements. We want to maximize the throughput seen by the user without secrecy requirements and at the same time to keep the delay for the user with secrecy requirements below a threshold. We also tune the secrecy tolerance depending on the requirements of the legitimate user.

The optimization problem in (25) is nonlinear due to the exponential factors in the equations for the success probabilities. We solve it numerically in the next section by utilizing the MATLAB solver (*fmincon*).

Numerical and Simulation Results

In this section, we provide numerical evaluation of the analytical results presented in the previous sections, in addition, we confirm the accuracy of our analysis with simulation results. Specifically, we study the impact of the jamming power P_j , the transmission power P_1 , and the arrival rate λ_1 on the average packet delay $\bar{D}_1$, given in (24), on the saturated throughput μ_2 , given in (6), on the probability that queue Q_1 is empty, given in (5), and on the average queue size, given in (22). The average packet delay is a significant metric in a physical layer security application with partial jamming; it determines how often the legitimate receiver transmits a jamming signal in order to preserve the secrecy of its packets from an eavesdropper. When the legitimate receiver transmits a jamming signal frequently, the saturated throughput decreases, since the legitimate receiver causes interference to the eavesdropper. Even in the case where the eavesdropper does not receive the packets intended for the legitimate receiver, the legitimate receiver transmits a jamming signal because it has no knowledge about the channel state of the eavesdropper. The saturated throughput is another important metric; it has the maximum value if the legitimate receiver does not transmit jamming signals to the eavesdropper. The saturated throughput decreases as the jamming signal is transmitted more often. It is desirable that the probability that queue Q_1 is empty has a high value and a small average queue size for a given arrival probability, since the goal is to transmit all the packets from queue Q_1 to the legitimate receiver.

For our evaluation, we performed numerical evaluation and simulations in MATLAB R2016a. We consider the scenario where queue Q_1 has bursty traffic, while queue Q_2 is saturated. Under the aforementioned scenario, we consider three cases, and all numeric results are presented together with the corresponding simulation results when queue Q_2 is saturated. In the first case, both receivers treat interference as noise. Here, the distances between source S and the two receivers are $d_1 = 10$ m, $d_2 = 11$ m, and $d_{12} = 11$ m. In the

second case, receiver D_1 performs successive decoding since it is closest to source S , and receiver D_2 treats interference as noise. In the third case, receiver D_1 treats interference as noise, and receiver D_2 performs successive decoding. Here, the distances between source S and the receivers are $d_1 = 11$ m, $d_2 = 10$ m, $d_{12} = 11$ m, where receiver D_2 is closest to source S and performs successive decoding.

The reason why we consider the first topology is that we have that the distance between the legitimate user and the transmitter is shorter than the distance between the eavesdropper and the transmitter. Furthermore, as also explained in [5], we need to have an asymmetric setup to reveal gains from the superposition coding and the successive decoding. In the second case, we consider the case where the eavesdropper is closer to the transmitter compared to the legitimate user, and also the eavesdropper can perform successive decoding, so satisfying the secrecy requirements is more challenging in this case. Thus, this case can stress the secrecy performance of the legitimate user.

For each of the aforementioned experiments, we have three sub-cases. First, we change the jamming power at the legitimate receiver, while keeping the transmission power to the legitimate receiver and the eavesdropper constant ($P_1 = P_2 = 20$ dB) for different values of λ_1 and β . Second, we change the transmission power to the legitimate receiver and the eavesdropper, while the jamming power at the legitimate receiver is kept constant ($P_j = 20$ dB) for different values of λ and β . In the third case, we change λ_1 while keeping the transmission power constant for both the legitimate receiver and the eavesdropper ($P_1 = P_2 = 20$ dB) for different values of P_j . For our simulation results, each simulation was run 10 times, with each simulation lasting over 10^7 time slots, and the average value of the performance metrics were then reported. The simulation parameters are shown in Table 2. For each experiment, the sum of the transmission powers to the legitimate receiver and the eavesdropper are equal to the total power budget, $P_{\max}$. We measure the residual self-interference in dB ($\beta \triangleq -10 \log g^2$). The arrival probabilities are chosen such that $\lambda_1 < \mu_1$, which means that the system is stable.

We summarize the key points from the numerical and simulation results as following:

- Increasing the jamming power affects negatively both the delay performance and the saturated throughput regardless the decoding scheme.
- The delay performance can considerably be improved in the case when receiver D_1 performs successive decoding, while receiver D_2 treats interference as noise, since receiver D_1 is closer to the source in this decoding scheme.
- Another way to increase the saturated throughput is by lowering the secrecy level, in other words, by increasing

Table 2 List of simulation parameters

Parameters	Value
Simulation time	10^7 time units
α	2.2
γ_1	0.5
γ_2	0.4
$P_{\max}$	23.01 dB
β	40 dB, 180 dB

the value of f^* in the case when receiver D_1 performs successive decoding, while receiver D_2 treats interference as noise. Receiver D_2 can also benefit by achieving a higher throughput when the value of D^* is small in the aforementioned decoding scheme.

Both Receivers Treat Interference as Noise

In Figs. 2, 3, 4, 5, 6, 7, 8 and 9, both receivers treat interference as noise, and queue Q_2 is saturated. In Figs. 2, 3 and 4, we change P_J when both queues treat interference as noise. Figure 2 presents the average packet delay vs. the jamming power at the legitimate receiver for different values of λ_1 and β . The average packet delay decreases as the jamming power increases since the service probability increases as the jamming power increases as shown by (7) and (24). It should be noted that the simulation results validate the analytic expressions. To illustrate the uncertainty in the simulation values, Table 3 presents confidence intervals for the case $\lambda_1 = 0.09$ and $\beta = 40$ dB. Since the confidence intervals are also relatively tight, we have decided not to show these for the rest of the results in this paper. Instead, we only report average values from the simulations. Moreover, we can see that the average packet delay increases as the arrival probability at Q_1 increases. This happens because the waiting time of packets at queue Q_1 increases. The average packet delay also increases when β is small, which means that the self-interference cancellation technique is insufficient, resulting in retransmissions of the packets. Figure 3 presents the saturated throughput vs. the jamming power at the legitimate receiver for different values of λ_1 and β . An increase in jamming power leads to a decrease in the saturated throughput, as shown by (6). We can also see that the saturated throughput increases as the arrival rate at Q_1 decreases, since the legitimate receiver transmits a jamming signal more often as the number of packets entering queue Q_1 increases. We can also see that the saturated throughput increases as β increases, which means that a small self-interference residual (g) leads to an increase in the saturated throughput. In Fig. 4, we measure the probability that Q_1 is empty vs. P_J . We observe that the probability of Q_1 being

Table 3 T confidence intervals

P_J	$\bar{D}_{1,Numerical}$	$\bar{D}_{1,Analytical}$	95% Confidence Interval
11.55	15.78	15.79	[15.77, 15.80]
14.56	15.44	15.44	[15.43, 15.46]
16.32	15.19	15.19	[15.17, 15.21]
17.57	15.01	15.01	[14.99, 15.03]
18.54	14.87	14.87	[14.85, 14.88]
19.33	14.76	14.76	[14.74, 14.78]
20.00	14.69	14.67	[14.67, 14.70]

Fig. 2 Average packet delay vs. jamming power at the legitimate receiver when both receivers treat interference as noise **Fig. 3** Average saturated throughput vs. jamming power at the legitimate receiver when both receivers treat interference as noise

empty increases as P_J increases. The reason is that a high P_J contributes to high service probability due to security constraints that are satisfied. We can also see that a high β

Fig. 4 Probability that Q_1 is empty vs. jamming power at the legitimate receiver when both receivers treat interference as noise

Fig. 5 Average packet delay vs. transmission power at the legitimate receiver when both receivers treat interference as noise

corresponds to a higher probability that queue Q_1 is empty. The reason is that a large β means that the self-interference residual (g) is small, which in turn means that there are fewer retransmissions of the confidential packets.

In Figs. 5 and 6, we change the transmission power of the legitimate receiver. The average packet delay vs. the transmission power at the legitimate receiver and the average queue size vs. the transmission power at the legitimate receiver are presented for different values of λ_1 and β . The transmission powers are in the range $[19.29, 20.00]$ because they satisfy the constraints $\frac{P_1}{P_2} > \gamma_1$ and $\frac{P_2}{P_1} > \gamma_2$ in (7) and (9), respectively. The average packet delay decreases as the transmission power at the legitimate receiver increases, since source S uses more power for the transmission. We can also

Fig. 6 Average queue size vs. transmission power at the legitimate receiver when both receivers treat interference as noise

Fig. 7 Average packet delay vs. transmission power at the legitimate receiver when both receivers treat interference as noise

see that the average packet delay increases as λ_1 increases, since there are more packets in queue Q_1 waiting for transmission. Another observation is that the average packet delay is higher when β is smaller. Thus, the average packet delay is higher due to more packet retransmissions, since the self-interference cancelation is not sufficient. In Fig. 6, we see that the average queue size decreases as the transmission power increases. This is reasonable since the more power source S uses to transmit the packets, the greater the likelihood that they will be received successfully. As λ_1 increases, the number of packets entering queue Q_1 also increases, thereby increasing the average queue size. The average queue size is also higher in the case where β is small,

Fig. 8 Optimal saturated throughput vs. delay threshold when both receivers treat interference as noise and $f^* = 0.2$

Table 4 Optimal $\bar{P}_J$ for $f^* = 0.2$ and different values of D^* and λ_1 when both receivers treat interference as noise

D^*	λ_1	$\bar{P}_J^*$
[5, ..., 50]	0.014	20.177
[5, ..., 50]	0.016	20.177
[5, ..., 50]	0.019	20.177

Fig. 9 Optimal saturated throughput vs. f threshold when both receivers treat interference as noise and $D^* = 50$ timeslots

Table 5 Optimal $\bar{P}_J$ for $D^* = 50$ time slots and different values of f^* and λ_1 when both receivers treat interference as noise

f^*	λ_1	$\bar{P}_J^*$
[0, ..., 1]	0.014	19.294
[0, ..., 1]	0.016	19.294
[0, ..., 1]	0.019	19.294

meaning that the self-interference cancellation is insufficient. In Fig. 7, we can see the penalty on the delay performance due to secrecy constraints in comparison to the case when there is not secrecy constraints and both receivers treat interference as noise. Specifically, we note that the average packet delay is higher in the case where there is secrecy. This happens due to retransmission of packets.

We also evaluate the optimization problem in (25), in which both receivers treat interference as noise. In Fig. 8, the optimal saturated throughput vs. the delay threshold is presented. For obtaining the optimal saturated throughput, we get the optimal jamming power for $f^* = 0.2$ and different values of D^* and λ_1 in Table 4. Since $f^* = 0.2$, it means that the required secrecy level is high. We can see that the optimal saturated throughput increases as the delay threshold increases. This happens because as D^* increases, the probability that receiver D_1 transmits a jamming signal decreases. In Fig. 9, the optimal saturated throughput vs. the f threshold is presented. For obtaining the optimal saturated throughput, we get the optimal jamming power for $D^* = 50$ timeslots and different values of f^* and λ_1 in Table 5. The optimal saturated throughput increases as f^* increases, since smaller f^* implies less secrecy.

Receiver D_1 Performs Successive Decoding and Receiver D_2 Treats Interference as Noise

In Figs. 10, 11, 12, 13, 14, 15, 16 and 17, receiver D_1 performs successive decoding and receiver D_2 treats interference as noise. In Figs. 10, 11 and 12, we change P_J for different values of λ_1 and β . In Fig. 10, we observe that the average packet delay decreases as P_J decreases and it increases as λ_1 increases as shown by (10), (24), and (21). Comparing Fig. 2 with Fig. 10, we can see that the successive decoding for receiver D_1 leads to smaller average packet delay in comparison with the case where both receivers treat interference as noise for the same λ_1 and P_J . In Fig. 11, we see that the saturated throughput decreases as P_J increases. In contrast with Fig. 3, we see that the saturated throughput with the same values of λ_1 and P_J is higher in the case where receiver D_1 performs successive decoding. This is justified by the fact that the service probability is higher in this case due to the successive decoding. In Fig. 12, we see the probability that the queue Q_1 is empty vs. P_J , where it increases as P_J increases and it increases as λ_1 decreases as shown by (5) and (10). If we compare this figure with the respective one in the case where both receivers treat interference as noise in Fig. 4, we can see that the probability is higher when using successive decoding. This is justified by the fact that receiver D_1 has a better link.

In Figs. 13 and 14, we see the average packet delay vs. the transmission power at receiver D_1 and the average queue size vs. the transmission power at receiver D_1 when D_1 performs

Fig. 10 Average packet delay vs. jamming power at the legitimate receiver when D_1 performs successive decoding and D_2 treats interference as noise

Fig. 12 Probability that Q_1 is empty vs. jamming power at the legitimate receiver when D_1 performs successive decoding and D_2 treats interference as noise

Fig. 11 Saturated throughput vs. jamming power at the legitimate receiver when D_1 performs successive decoding and D_2 treats interference as noise

Fig. 13 Average packet delay vs. transmission power when D_1 performs successive decoding and D_2 treats interference as noise

successive decoding and D_2 treats interference as noise, respectively. The transmission powers are in the range $[19.29, 20.00]$ because they satisfy the constraints $\frac{P_1}{P_2} > \gamma_1$ and $\frac{P_2}{P_1} > \gamma_2$ in (7) and (9) respectively. In Fig. 13, we see that the average packet delay decreases slightly at $P_1 = 19.60$ dB and it increases for $P_1 > 19.60$ dB. Moreover, we observe that the average packet delay increases as λ_1 increases and as β decreases. The reason is that higher arrival probability leads to increasing packets in queue Q_1 and small β implies a limited ability to cancel out self-interference, which leads to an increase in the average packet delay due to packet retransmissions. Comparing Figs. 5 and 13, we see that the

average packet delay decreases as P_1 increases in the case of where both receivers treat interference as noise. Another observation is that we have significantly smaller average packet delay when successive decoding is used, which is due to better channel between source S and receiver D_1 . In Fig. 14, we see that the average queue size decreases slightly at $P_1 = 19.60$ dB and it increases as P_1 increases as shown in (10) and (22). Furthermore, we see that the average queue size increases for larger values of λ_1 and for smaller values of β . Comparing Fig. 6 with Fig. 14, we can see that, when the receiver performs successive decoding, the average queue size increases as P_1 increases, while in the case when both receivers treat interference as noise, the average queue size decreases as P_1 increases.

Fig. 14 Average queue size vs. transmission power when D_1 performs successive decoding and D_2 treats interference as noise

Fig. 15 Average packet delay vs. transmission power when D_1 performs successive decoding and D_2 treats interference as noise

In Fig. 15, we can see that the average packet delay is higher as P_1 increases when there is secrecy, but decreases when there is no secrecy. The reason is that since receiver D_1 is closer to the source, a high transmission power leads to a low average packet delay when there is no secrecy.

We also evaluate the optimization problem in (25) when receiver D_1 performs successive decoding and receiver D_2 treats interference as noise. In Fig. 16, the optimal saturated throughput vs. the delay threshold is presented. For obtaining the optimal saturated throughput, we get the optimal jamming power for $f^* = 0.2$ and different values of D^* and λ_1 in Table 6. Since $f^* = 0.2$, it means that there is high secrecy at receiver D_2 . We can see that the optimal saturated

Fig. 16 Optimal saturated throughput vs. delay threshold when receiver D_1 performs successive decoding and receiver D_2 treats interference as noise and $f^* = 0.2$

Table 6 Optimal $\bar{P}_J$ for $f^* = 0.2$ and different values of D^* and λ_1 when receiver D_1 performs successive decoding and receiver D_2 treats interference as noise

D^*	λ_1	$\bar{P}_J^*$
[5, ..., 50]	0.014	19.924
[5, ..., 50]	0.016	19.892
[5, ..., 50]	0.019	19.950

Fig. 17 Optimal saturated throughput vs. f threshold when receiver D_1 performs successive decoding and receiver D_2 treats interference as noise and $D^* = 50$ timeslots

Table 7 Optimal $\bar{P}_J$ for $D^* = 50$ timeslots and different values of f^* and λ_1 when receiver D_1 performs successive decoding and receiver D_2 treats interference as noise

f^*	λ_1	$\bar{P}_J^*$
[0, ..., 1]	0.014	19.952
[0, ..., 1]	0.016	19.946
[0, ..., 1]	0.019	19.950

Fig. 18 Average packet delay vs. jamming power at the legitimate user when D_1 treats interference as noise and D_2 performs successive decoding

throughput, increases as the delay threshold increases, since the probability receiver D_1 transmits a jamming signal to receiver D_2 decreases. Figure 17 presents the optimal saturated throughput vs. f threshold. For obtaining the optimal saturated throughput, we get the optimal jamming power for $D^* = 50$ time slots and different values of f^* and λ_1 in Table 7. We see that the optimal saturated throughput increases as f increases, because higher f^* means that there is less secrecy.

Receiver D_1 Treats Interference as Noise and Receiver D_2 Performs Successive Decoding

In Figs. 18, 19, and 20, we change P_j for different values of λ_1 in the case where receiver D_1 treats interference as noise while receiver D_2 is more powerful and performs successive decoding. Specifically, in Fig. 18, we see that the average packet delay decreases as P_j increases and it increases as λ_1 increases as shown in (13), (21), and (24). Comparing Figs. 2 and 10 with Fig. 18, we can see that the case when receiver D_2 performs successive decoding has a higher average packet delay than the other two cases. Figure 19 presents the saturated throughput vs. jamming power. As we can see, the saturated throughput decreases quickly as P_j increases and it decreases as λ_1 increases as shown in (6) and (13). Comparing Figs. 3 and 11 with Fig. 19, we can see that the case where receiver D_2 performs successive decoding achieves the highest saturated throughput of the three cases. This can be justified since receiver D_2 is geographically closer to source S , and thus it has a better channel. In Fig. 20, the probability that Q_1 is empty vs. jamming power is presented. The probability increases as P_j increases and as β increases, and decreases as λ_1 increases as shown in (5) and

Fig. 19 Saturated throughput vs. jamming power at the legitimate user when D_1 treats interference as noise and D_2 performs successive decoding

Fig. 20 Probability that Q_1 is empty vs. jamming power at the legitimate user when D_1 treats interference as noise and D_2 performs successive decoding

(13). When we compare Figs. 4 and 12 with Fig. 20, we see that the probability has the lowest value in the case where receiver D_2 performs successive decoding.

In Figs. 21 and 22, we have the average packet delay vs. the transmission power at source S for receiver D_1 and the average queue size vs. the transmission power at source S for receiver D_1 when D_2 performs successive decoding and D_1 treats interference as noise. The transmission powers are in the range $[19.29, 20.00]$ because they satisfy the constraints $\frac{P_1}{P_2} > \gamma_1$ and $\frac{P_2}{P_1} > \gamma_2$ in (7) and (9), respectively. In Fig. 21, we can see the average packet delay vs. the transmission power P_1 for different values of λ_1 and β . As we can notice, the average packet delay decreases as P_1 increases and

Fig. 21 Average packet delay vs. transmission power when D_1 treats interference as noise and D_2 performs successive decoding

Fig. 23 Average packet delay vs. transmission power when D_1 treats interference as noise and D_2 performs successive decoding

Fig. 22 Average queue size vs. transmission power when D_1 treats interference as noise and D_2 performs successive decoding

increases as λ_1 increases as shown in (13), (21), and (24). In Fig. 22, we can see the average queue size vs. the transmission power P_1 for different values of λ_1 and β . We can see that the average queue size decreases as P_1 and λ_1 increase, and increases as β decreases as shown in (13), and (22). Comparing Figs. 6 and 14 with Fig. 22, we observe that the average queue size decreases as P_1 increases when both receivers treat interference as noise and when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding, but increases as P_1 increases when receiver D_1 performs successive decoding.

In Fig. 23, we see that the average packet delay is higher in the case where there is no secrecy. Specifically, we can see that when receiver D_2 performs successive decoding and,

Fig. 24 Optimal saturated throughput vs. delay threshold when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding and $f^* = 0.2$

thus is closer to the source, the average packet delay for receiver D_1 is considerably higher in the case where there is secrecy.

We also evaluate the optimization problem in (25) when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding. In Fig. 24, the optimal saturated throughput vs. the delay threshold is presented. For obtaining the optimal saturated throughput, we get the optimal jamming power for $f^* = 0.2$ and different values of D^* and λ_1 in Table 8. We can see that the optimal saturated throughput is constant between [5, 10] timeslots, but it increases when $D^* > 10$ timeslots. The reason is that the probability

Table 8 Optimal $\bar{P}_J$ for $f^* = 0.2$ and different values of D^* and λ_1 when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding

D^*	λ_1	$\bar{P}_J^*$
[5, ..., 50]	0.014	21.537
[5, ..., 50]	0.016	21.452
[5, ..., 50]	0.019	21.451

Fig. 25 Optimal saturated throughput vs. f threshold when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding and $D^* = 50$ timeslots**Table 9** Optimal $\bar{P}_J$ for $D^* = 50$ timeslots and different values of f^* and λ_1 when receiver D_1 treats interference as noise and receiver D_2 performs successive decoding

f^*	λ_1	$\bar{P}_J^*$
[0, ..., 1]	0.014	20.911
[0, ..., 1]	0.016	20.911
[0, ..., 1]	0.019	20.911

that receiver D_1 transmits a jamming signal to receiver D_2 decreases, as a result optimal saturated throughput increases. Figure 25 presents the optimal saturated throughput vs. f threshold. For obtaining the optimal saturated throughput, we get the optimal jamming power for $D^* = 50$ timeslots and different values of f^* and λ_1 in Table 9. We see that the optimal saturated throughput increases as f increases, because as f^* increases there is less secrecy.

Conclusion

This paper presents an analysis of delay for a two-receiver broadcast scenario with security constraints. Specifically, a source transmits both confidential and non-confidential data to two receivers, while the legitimate receiver transmits a jamming signal to the eavesdropper in order to prevent the latter from decoding the former's packets. A delay analysis

is provided and the saturated throughput is maximized with packet delay and secrecy rate constraints for the legitimate receiver. We provide numerical results where we show that the use of successive decoding at the legitimate receiver outperforms the cases where the eavesdropper performs successive decoding and when both receivers treat interference as noise. Thus, different decoding schemes affect the performance metrics differently. This allows us to exploit the channel ordering to provide better performance. For example, in cases where the interference from the other receiver is strong, performing successive decoding is desirable, and when the interference is sufficiently weak it is better to treat the interference as noise.

Acknowledgements Open access funding provided by Linköping University.

Compliance with Ethical Standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Appendix A

Markov Chain

The Markov chain (DTMC) that describes the queue evolution is presented in Fig. 26. Each state represents the number of packets in the queue Q_1 . At each time slot, the

Fig. 26 The discrete time Markov Chain (DTMC) for the evolution of Q_1

departures take place before the arrivals. The queue stays in state 0, when no arrivals happen. When a new packet arrives in queue Q_1 , there is a transition to state 1 with probability λ_1 . The transition from state 1 to state 0 happens with probability $\mu_1(1 - \lambda_1)$, where a packet departure happens but no packet arrives in the current time slot. The queue length remains in the same state with probability $\kappa = \lambda_1\mu_1 + (1 - \lambda_1)(1 - \mu_1)$, where both a packet arrival and a packet departure happen, or where neither happens. The transition for packet arrivals to state 2 happens with a probability $\lambda_1(1 - \mu_1)$, where a packet arrives in the queue but there is no packet departure. The same applies for packet arrivals for the rest of the states. Next, we derive the steady-state distribution of the Markov chain.

To compute the steady-state distribution π , we have to solve for $\pi = \pi P$, where P is the transition matrix, which is equivalent to

$$\pi_i = \pi_{i-1}P_{i-1,i} + \pi_i P_{ii} + \pi_{i+1}P_{i+1,i}, \quad i > 0, \quad (26)$$

$$\pi_0 = \pi_0 P_{00} + \pi_1 P_{1,0}. \quad (27)$$

For $i = 0$, we obtain $\pi_0 = \pi_0 P_{00} + \pi_1 P_{1,0} \Rightarrow \pi_1 = \frac{\lambda_1}{\mu_1(1-\lambda_1)} \pi_0$.

For $i = 1$, we get $\pi_1 = \pi_0 P_{0,1} + \pi_1 P_{11} + \pi_2 P_{2,1} \Rightarrow \pi_2 = \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right] \pi_0$.

For $i = 2$, it is $\pi_2 = \pi_2 P_{1,2} + \pi_2 P_{22} + \pi_3 P_{3,2} \Rightarrow \pi_3 = \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^2 \pi_0$.

In addition, the above equations have to satisfy the constraint $\sum_i \pi_i = 1$. By substituting the aforementioned expressions for the steady-state distribution to the above constraint, we obtain $\pi_0 + \frac{\lambda_1}{\mu_1(1-\lambda_1)} \pi_0 + \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right] \pi_0 + \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^2 \pi_0 + \dots = 1$. Solving for π_0 , we get the stationary probability of being in the state 0, which is given by $\pi_0 = 1 - \frac{\lambda_1}{\mu_1}$. Thus, the steady-state distribution is given by

$$\pi_i = \begin{cases} \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^{i-1} \pi_0, & i > 0, \\ 1 - \frac{\lambda_1}{\mu_1}, & i = 0. \end{cases} \quad (28)$$

The average queue size can be calculated by

$$\begin{aligned} E[Q_1] &= \sum_{i=0}^{\infty} i \pi_i \\ &= \sum_{i=1}^{\infty} i \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^{i-1} \pi_0 \\ &= \pi_0 \sum_{i=1}^{\infty} i \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^{i-1} \\ &= \left(1 - \frac{\lambda_1}{\mu_1} \right) \sum_{i=1}^{\infty} i \frac{\lambda_1}{\mu_1(1-\lambda_1)} \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^{i-1} \\ &= \left(1 - \frac{\lambda_1}{\mu_1} \right) \frac{\lambda_1}{\mu_1(1-\lambda_1)} \sum_{i=1}^{\infty} i \left[\frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^{i-1} \\ &= \left(1 - \frac{\lambda_1}{\mu_1} \right) \frac{\lambda_1}{\mu_1(1-\lambda_1)} \frac{1}{\left[1 - \frac{\lambda_1(1-\mu_1)}{\mu_1(1-\lambda_1)} \right]^2}. \end{aligned} \quad (29)$$

After some simplifications, (29) takes the form

$$E[Q_1] = \frac{\lambda_1}{\mu_1 - \lambda_1} (1 - \lambda_1). \quad (30)$$

References

1. Arvanitaki A, Pappas N, Mohapatra P, Carlsson N. Delay performance of a two-user broadcast channel with security constraints. In: Global Information Infrastructure and Networking Symposium (GIIS), Oct. 2018. p. 1–5.
2. Rao RR, Ephremides A. On the stability of interacting queues in a multiple-access system. *IEEE Trans Inf Theory*. 1988;34(5):918–30.
3. Pappas N, Kountouris M, Ephremides A. The stability region of the two-user interference channel. In: *IEEE Information Theory Workshop (ITW)*, Sep. 2013. p. 1–5.
4. Pappas N, Kountouris M, Ephremides A, Angelakis V. Stable throughput region of the two-user broadcast channel. *IEEE Trans Commun*. 2018;66(10):4611–21.
5. Mohapatra P, Pappas N, Lee J, Quek TQS, Angelakis V. Secure communications for the two-user broadcast channel with random traffic. *IEEE Trans Inf Forensics Secur*. 2018;13(9):2294–309.
6. Dimitriou I, Pappas N. Stable throughput and delay analysis of a random access network with queue-aware transmission. *IEEE Trans Wirel Commun*. 2018;17(5):3170–84.
7. Csiszar I, Korner J. Broadcast channels with confidential messages. *IEEE Trans Inf Theory*. 1978;24(3):339–48.

8. Barros J, Rodrigues MRD. Secrecy capacity of wireless channels. In: *IEEE international symposium on information theory (ISIT)*, July 2006. p. 356–360.
9. Ekrem E, Ulukus S. Secrecy in cooperative relay broadcast channels. *IEEE Trans Inf Theory*. 2011;57(1):137–55.
10. Marton K. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans Inf Theory*. 1979;25(3):306–11.
11. Fayolle G, Gelenbe E, Labetoulle J. Stability and optimal control of the packet switching broadcast channel. *J ACM*. 1977;24(3):375–86.
12. Jafarian A, Vishwanath S. The two-user Gaussian fading broadcast channel. In: *IEEE international symposium on information theory*, Jul. 2011. p. 2964–2968.
13. Liu T, Mukherjee P, Ulukus S, Lin S, Hong YP. Secure degrees of freedom of mimo rayleigh block fading wiretap channels with no csi anywhere. *IEEE Trans Wirel Commun*. 2015;14(5):2655–69.
14. Khisti A, Tchamkerten A, Wornell GW. Secure broadcasting over fading channels. *IEEE Trans Inf Theory*. 2008;54(6):2453–69.
15. Jiang K, Jing T, Li Z, Huo Y, Zhang F. Analysis of secrecy performance in fading multiple access wiretap channel with sic receiver. In: *IEEE International Conference on Computer Communications (INFOCOM)*, May 2017. p. 1–9.
16. Lai L, Gamal HE. The relay-eavesdropper channel: cooperation for secrecy. *IEEE Trans Inf Theory*. 2008;54(9):4005–19.
17. Lee J, Conti A, Rabbachin A, Win MZ. Distributed network secrecy. *IEEE J Sel Areas Commun*. 2013;31(9):1889–900.
18. Zhou X, Ganti RK, Andrews JG, Hjørungnes A. On the throughput cost of physical layer security in decentralized wireless networks. *IEEE Trans Wirel Commun*. 2011;10(8):2764–75.
19. Vasudevan S, Goeckel D, Towsley DF. Security-capacity trade-off in large wireless networks using keyless secrecy. In: *ACM international symposium on mobile ad hoc networking and computing (MobiHoc)*, 2010. p. 21–30.
20. Pappas N, Ephremides A, Traganitis A. Relay-assisted multiple access with multi-packet reception capability and simultaneous transmission and reception. In: *IEEE information theory workshop*, Oct. 2011. p. 578–582.
21. Tong Z, Haenggi M. Throughput analysis for full-duplex wireless networks with imperfect self-interference cancellation. *IEEE Trans Commun*. 2015;63(11):4490–500.
22. Pappas N, Kountouris M, Ephremides A, Traganitis A. Relay-assisted multiple access with full-duplex multi-packet reception. *IEEE Trans Wirel Commun*. 2015;14(7):3544–58.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.