Arvanitaki *et al. J Wireless Com Network* (2021) 2021:178
https://doi.org/10.1186/s13638-021-02046-7

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

# Performance analysis of congestion-aware secure broadcast channels

Antonia Arvanitaki[1*], Nikolaos Pappas[2], Niklas Carlsson[1], Parthajit Mohapatra[3] and Oleg Burdakov[4]

*Correspondence:
antonia.arvanitaki@liu.se
[1] Department of Computer and Information Science, Linköping University, Linköping, Sweden
Full list of author information is available at the end of the article

**Abstract**

Congestion-aware scheduling in case of downlink cellular communication has ignored the distribution of diverse content to different clients with heterogeneous secrecy requirements. Other possible application areas that encounter the preceding issue are secure offloading in mobile-edge computing, and vehicular communication. In this paper, we extend the work in Arvanitaki et al. (SN Comput Sci 1(1):53, 2019) by taking into consideration congestion and random access. Specifically, we study a two-user congestion-aware broadcast channel with heterogeneous traffic and different security requirements. We consider two randomized policies for selecting which packets to transmit, one is congestion-aware by taking into consideration the queue size, whereas the other one is congestion-agnostic. We analyse the throughput and the delay performance under two decoding schemes at the receivers, and provide insights into their relative security performance and into how congestion control at the queue holding confidential information can help decrease the average delay per packet. We show that the congestion-aware policy provides better delay, throughput, and secrecy performance for large arrival packet probabilities at the queue holding the confidential information. The derived results also take account of the self-interference caused at the receiver for whom confidential data is intended due to its full-duplex operation while jamming the communication at the other user. Finally, for two decoding schemes, we formulate our problems in terms of multi-objective optimization, which allows for finding a trade-off between the average packet delay for packets intended for the legitimate user and the throughput for the other user under congestion-aware policy.

**Keywords:** Broadcast channel, Queueing, Congestion control, Secrecy, Multi-objective optimization

## 1 Introduction

In many wireless networks such as cellular network and Internet of Things (IoT), it is required to serve users with different Quality Of Service (QoS). Congestion control has been used in the traditional network to improve the network performance such as delay and throughput. In this work, we consider a two-user broadcast channel with heterogeneous traffic characteristics and security requirements. This setup can capture the downlink scenario by a base station that serves simultaneously two different users, one with bursty traffic and security requirements and another one with delay tolerant traffic without secrecy constraints. Furthermore, the user who has secrecy requirements, has

also full-duplex capability and it can transmit jamming signals to increase its secrecy in the cost of self-interference. The work explores the impact of congestion on the performance of the broadcast channel with heterogeneous traffic with different secrecy requirements. The proposed system can be potentially used in applications such as secure offloading in mobile-edge computing scenarios, secure communication in vehicular networks, as well as secure downlink in cellular networks.

### 1.1 Related works

Most of the existing works in congestion control ignore the security requirement of the users. Physical layer secrecy has emerged as a promising approach for security in wireless communications [2]. The work in [3] has been instrumental in the development of various results in physical layer secrecy. It considers the problem of secure communication in the presence of a passive eavesdropper, where the trade-off between the transmission rate and equivocation at the eavesdropper has been explored. The result in [3] was subsequently extended for the broadcast channel [4] with a common and a private message. In [5], the physical layer security performance of a wireless ad hoc network is studied, where pairs of transmitters and receivers communicate, and the latter transmit a jamming signal to a number of eavesdroppers to facilitate secure communication. Various other network setups under physical layer secrecy constraints have been studied in the literature [6–9].

However, these results assume that users always have data to send and in such scenarios, stable throughput or stability region is a more meaningful metric to measure the performance of the system rather than secrecy capacity or secrecy rate. The work in [10] characterizes the stability region of the broadcast channel under different decoding schemes when there is no secrecy constraint at the receivers. The impact of secrecy constraint on the stability region has also been explored in [11]. In [1], the average packet delay in a two-user broadcast channel for different decoding schemes has been characterized with secrecy constraint at the receiver. In [12], the authors studied the problem of secure communication under different malicious attacks in the physical layer in a cognitive radio network, and they used Q-learning to adjust the transmission power of the secondary user. In [13], the authors investigated the problem of security in Internet of Vehicles (IoV) networks by proposing an intelligent edge-chain enabled access control framework to hinder compromised IoV devices from having access to centralized cloud and improve communication issues caused due to mobility of the IoV devices.

In such modern and complex wireless communication systems, there are dependencies among metrics. Therefore, the designer has to make a choice to favour one metric over another, depending on the application. Multi-objective optimization focuses on optimizing multiple objective functions and showing the trade-off among the metrics [14, 15]. The multi-objective approaches are successfully used in designing communication systems. For instance, in [16], the authors used multi-objective optimization to study the trade-off between the spectrum selection and the resource management in a cognitive radio network. In [17], a multi-objective optimization problem was formulated for optimizing the power control and the QoS components in a CDMA wireless communication system. The authors of [18] obtained a trade-off between the data rate and the transmission power in a cellular communication system.

To the best of our knowledge, the effect of secrecy on the congestion is not well understood and needs to be explored. The performance of queue holding the confidential data can degrade due to congestion and it is important to understand the impact of congestion on the secrecy performance. To explore this, we consider a two-user broadcast channel where one of the receivers having full-duplex capability need to be served with confidential data that are of bursty nature. The main contributions of the paper are described below.

### 1.2 Contribution

In this paper, we study a congestion-aware broadcast channel with random selection between two queues with different secrecy requirements under different decoding schemes at the receivers. The transmitter has two queues and it serves two users with different secrecy requirements: one queue has confidential data whereas the second queue has non-confidential data. The receiver to which confidential data needs to be served has full-duplex capability, and it transmits a jamming signal to hinder eavesdropping of its data at the other user. The queue holding the confidential can grow large due to congestion. Congestion occurs when the queue grows above a threshold. The contributions are summarized as follows.

We consider two schemes, a congestion-agnostic randomized policy, and a congestion-aware one for the selection of the packets that are transmitted by the source. When the source selects one packet from each queue, it applies superposition coding to transmit the two packets with a single transmission. In this case, we consider two decoding schemes at the receivers' side, treating interference as noise, and successive decoding. We then characterize the average queue size, and the average delay per packet. In addition, we characterize the throughput performance of the other user for both schemes. We numerically compare the impact of the transmission power and random access probability for packets intended for the legitimate user on the average packet delay for the sensitive traffic for different combinations of the decoding schemes. We show that congestion control at the queue holding confidential information can decrease the average delay per packet. Finally, we present the Pareto sets for the average packet delay for packets intended for the legitimate user and the throughput for the other user under congestion-aware policy for two decoding schemes, where we show the trade-off between them.

### 1.3 Structure of the paper

The rest of this paper is organized as follows. In Sect. 2, we present the system model and assumptions for the precedent stated problem. In Sect. 3, we provide the analysis for the congestion-agnostic and congestion-aware policies. In Sect. 4, we formulate two multi-objective optimization problems, where we study the trade-off between two performance metrics in case of congestion-aware policy. In Sect. 5, we provide numerical results, where we show the impact of different parameters on performance metrics for three different combinations of decoding schemes at the legitimate receiver and the eavesdropper. We also present the trade-off between the performance metrics with Pareto sets. In Sect. 6, we summarize our study.

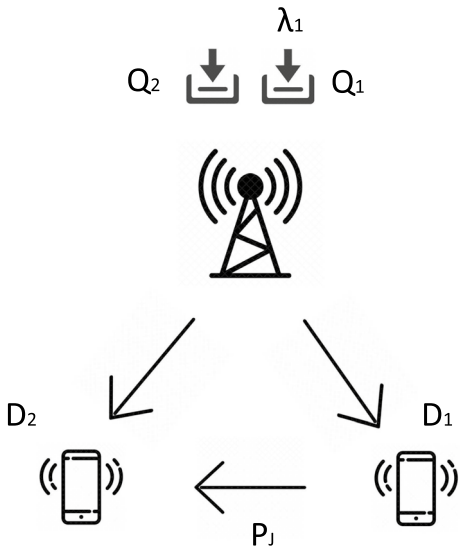


**Fig. 1** Two-user broadcast channel with secrecy constraints

## 2 System model

### 2.1 Network model

We consider a two-user broadcast channel (BC), where a single source $S$ is equipped with two queues $Q_i$ that contain traffic intended for two users (receivers) $D_i$, where $i = 1, 2$, as shown in Fig. 1. Here, $Q_i$ represents both the queue length of the queue that has packets for receiver $D_i$, and the queue itself. $Q_1$ stores packets intended for receiver $D_1$ and they have to be kept confidential from receiver $D_2$. Queue $Q_2$ has packets intended for receiver $D_2$. Time is assumed to be slotted. The confidential data is intended for the legitimate receiver and the non-confidential data is intended for the other receiver (Table 1).

We assume that the arrival process at queue $Q_1$ is Bernoulli with mean $\lambda_1$, so a packet arrives with probability $\lambda_1$ during a time slot. Queue $Q_2$ is assumed saturated, i.e., it never empties, this captures a delay tolerant traffic scenario, where $Pr(Q_2 = 0) \approx 0$; thus it overestimates the interference that is caused to the other transmission.

When queue $Q_1$ is non-empty, and queues $Q_1$ and $Q_2$ are selected with probabilities $q_1$ and $q_2$ respectively, source $S$ sends two messages in a single transmission using superposition coding, allocating power $P_1$ and $P_2$ for the packets from the first and the second queue respectively. The total power budget is $P_{\max}$, which means that $P_1 + P_2 = P_{\max}$. When $Q_1$ is empty, source $S$ sends with probability 1 the packet intended for receiver $D_2$, with a power $P_2$.[1] We assume that there is no packet dropping and $Q_1$ has infinite size. Furthermore, packets will be re-transmitted until they are received by their intended destination. During one time slot, a bursty queue can be in one of the following states: empty state, non-empty and active state, non-empty and inactive state. By active state we mean that a packet is selected to be transmitted. When the queue is non-empty, but the source does not select a packet from that queue, then the queue is inactive. Packet transmissions occur at the beginning of the time slot, while packet arrivals happen at the

[1] In an extension of this work we will consider power control schemes adapting to the state of the queues.

**Table 1** List of notations

| Notation | Definition |
|---|---|
| $Q_1$ | Queue holding the confidential information |
| $Q_2$ | Queue holding the non-confidential information |
| $q_1$ | Random access probability for packets in queue $Q_1$ |
| $q_2$ | Random access probability for packets in queue $Q_2$ |
| $B$ | Congestion limit for queue $Q_1$ |
| $\alpha$ | Path loss exponent |
| $\gamma_1$ | SNR/SINR threshold for the legitimate receiver |
| $\gamma_2$ | SNR/SINR threshold for receiver $D_2$ |
| $P_1$ | Power transmission for the legitimate receiver |
| $P_2$ | Power transmission for receiver $D_2$ |
| $P_J$ | 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 receiver $D_2$ |
| $d_{12}$ | Distance between the legitimate receiver and receiver $D_2$ |
| $P_{\max}$ | Total power budget |

end of the time slot. We assume that the transmission of acknowledgments (ACKs) are instantaneous and error-free.

### 2.2 Physical layer model

We assume that the legitimate receiver $D_1$ has full-duplex capability. This means it can receive and transmit packets at the same time, when necessary. In this work, SNR/SINR based physical layer based secrecy is considered to capture the confidential aspects of data associated with users [3–9, 11]. The SNR or SINR based secrecy metric allows the decoding ability of the unauthorized users in decoding confidential data. The full-duplex ability of the receiver $D_1$ can hinder the decoding of its intended message at receiver $D_2$ by sending a jamming signal. The receiver $D_1$ sends a jamming signal when $Q_1 > 0$, otherwise it is silent. The simultaneous transmission and reception at receiver $D_1$ causes self-interference. We assume that $D_1$ has imperfect self-interference cancellation, and the residual self-interference is modelled as a scalar $g$, where $g \in [0, 1]$. When $g = 0$, we have perfect self-interference cancellation, while there is no cancellation at receiver $D_1$ when $g = 1$ [19, 20]. The self-interference reduces the probability of packet reception by the legitimate receiver.

We assume Rayleigh fading for the channel between $S$ and receiver $D_i$, and between $D_1$ and $D_2$ as well. When queue $Q_1$ is non-empty and active, and queue $Q_2$ is active, source $S$ sends the signal $x[t] = x_1[t] + x_2[t]$. Then, $D_1$ and $D_2$ receive the signals $y_1[t]$ and $y_2[t]$ respectively at time slot $t$, given by

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

where $z_i$ $(i = 1, 2)$ is additive white Gaussian noise with zero mean and unit variance, $h_i$ is the channel gain from $S$ to $D_i$, $h_{12}$ 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 cancellation coefficient. When queue $Q_1$ is empty, or non-empty and non-active, the transmitted signal is $x[t] = x_2[t]$. A receiver can decode its intended packet 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).

We consider two different decoding schemes at receivers $D_1$ and $D_2$. Namely, treating interference as noise (TIN), and successive decoding (SD). When a receiver performs treating interference as noise, it decodes only the packet intended for it, while discarding the other packet. Successive decoding is a decoding scheme, where the receiver decodes first the packet not intended for it and then cancels its effect; then it decodes the intended packet. We assume different combinations of decoding schemes for each receiver apart from the case where both receivers perform successive decoding, because this case is not feasible. The success probability that receiver $D_1$ can successfully decode packets from queue $Q_1$, while receiver $D_2$ cannot decode the packet (remains secret) is denoted by $P(D^s_{1/\mathcal{T}})$, where $\mathcal{T}$ denotes the set of active queues, and $s$ indicates that a message is confidential. Furthermore, $P(D_{2/\mathcal{T}})$ represents the success probability that the other user can successfully decode packets from queue $Q_2$. The aforementioned probabilities differ for each decoding scheme are omitted here due to space limitations but they can be found in [11]. *The purpose of this work is to utilize these probabilities to study the effect of a congestion-aware scheme on throughput and delay for the considered setup under different secrecy requirements.*

## 3 Methods

In this section, we introduce two congestion policies for the two-user broadcast channel, the congestion agnostic and the congestion-aware policy and present the analysis for each of them.

### 3.1 Congestion-agnostic randomized policy

We provide the analysis for the throughput when the source randomly selects a packet from a non-empty queue as we discussed in the previous section (recall that $Q_2$ is assumed to be saturated here). Thus, $Q_2$ never empties and we have the following two cases.

1. $Q_1 = 0$: In this case, the source transmits a packet from queue $Q_2$ with probability 1. We denote the success probability for that transmission $P(D_{2/2})$.
2. $Q_1 > 0$: In this case, the source selects a packet from each queue with probability $q_1q_2$. Then, the success probability with secrecy requirement for $D_1$ is $P(D^s_{1/1,2})$, and the success probability for $D_2$ is $P(D_{2/1,2})$. With probability $q_1(1-q_2)$, a packet is selected only from $Q_1$ and the success probability is $P(D^s_{1/1})$. With $q_2(1-q_1)$, the source transmits a packet only from $Q_2$ .

Now, we can write the average service probability $\mu_1$ and the throughput $\mu_2$ as given below

$$\mu_1 = q_1q_2P(D^s_{1/1,2}) + q_1(1-q_2)P(D^s_{1/1}), \tag{2}$$

$$\mu_2 = q_2(1-q_1)P(Q_1>0)P(D_{2/2}) + +q_1q_2P(Q_1>0)P(D_{2/1,2}) + P(Q_1=0)P(D_{2/2}). \tag{3}$$

Since the traffic at $Q_1$ is bursty, the term $\mu_1$ denotes the service probability of that queue. If the queue is stable, $\lambda_1 < \mu_1$, then the throughput is $\lambda_1$, otherwise the throughput is $\mu_1$. Note that the stability condition $\lambda_1 < \mu_1$ can be rewritten as

$$q_1 > \frac{\lambda_1}{q_2P(D^s_{1/1,2}) + (1-q_2)P(D^s_{1/1})}. \tag{4}$$

On the other hand, since $Q_2$ is saturated, $\mu_2$ is the throughput.

Since $Q_1$ can be seen as a Geo/Geo/1 queue with arrival probability $\lambda_1$ and service probability $\mu_1$, we have that $P(Q_1>0) = \frac{\lambda_1}{\mu_1}$. Thus, (3) after some calculations can be written as

$$\mu_2 = P(D_{2/2}) - \frac{[1-q_2(1-q_1)]P(D_{2/2}) - q_1q_2P(D_{2/1,2})}{q_1q_2P(D^s_{1/1,2}) + q_1(1-q_2)P(D^s_{1/1})}\lambda_1. \tag{5}$$

Note that if $Q_1$ is unstable, then the throughput for the $D_2$ is given by

$$\mu_2 = q_2(1-q_1)P(D_{2/2}) + q_1q_2P(D_{2/1,2}). \tag{6}$$

### 3.2 Congestion-aware randomized policy

In this section, we introduce a congestion-aware protocol that takes into account the queue size at $Q_1$. A similar protocol was introduced in [21, 22], but in a different system setup. We consider a congestion limit $B$ for queue $Q_1$, $B$ affects the operation of the randomized policy described in the previous section as explained below.

- *If* $Q_1 = 0$: In this case, no packet from queue $Q_1$ is sent, and the source transmits a packet from queue $Q_2$ with probability 1. The saturated throughput is given by $\mu'_2 = P(D_{2/2})$.
- *If* $1 \le Q_1 \le B$: The source transmits a packet from queue $Q_i$ with a probability $q_i$, where $i = 1, 2$. The service probability for queue $Q_1$ is given by (2). The saturated throughput is given by

$$\mu''_2 = q_1q_2P(D_{2/1,2}) + q_2(1-q_1)P(D_{2/2}). \tag{7}$$

- *When* $Q_1 > B$: The source transmits a packet only from queue $Q_1$ with probability 1. The service probability for queue $Q_1$ is given by

$$\mu'_1 = P(D^s_{1/1}). \tag{8}$$

Given the probabilities of the above respective cases, the average service probability for $Q_1$, $\bar{\mu}_1$, is given by

$$\bar{\mu}_1 = \frac{P(1 \le Q_1 \le B)\mu_1 + P(Q_1 > B)\mu'_1}{P(1 \le Q_1 \le B) + P(Q_1 > B)}, \tag{9}$$

where $\mu_1$ and $\mu'_1$ are given by (2) and (8), respectively.

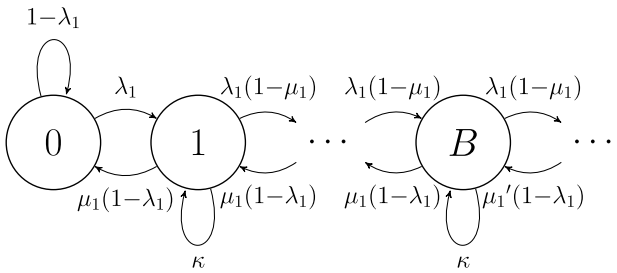


**Fig. 2** The Discrete Time Markov Chain (DTMC) that models the evolution of $Q_1$. The service probabilities $\mu_1$ and $\mu_1'$ are given by (2) and (8), respectively

The average throughout seen at receiver $D_2$ can be written as

$$\mu_2 = P(Q_1 = 0)P(D_{2/2}) + P(1 \leq Q_1 \leq B)\mu_2'', \tag{10}$$

where $\mu_2''$ is given by (7). As stated earlier in Sect. 2.2, the success probabilities $P(D^s_{1/\mathcal{T}})$ and $P(D_{2/\mathcal{T}})$, where $\mathcal{T}$ consists of the set of active queues, are given in [11].

In order to fully characterize the average service probability and the throughput, we proceed by modeling the evolution of $Q_1$ by a a discrete time Markov chain (DTMC) in order to calculate the probabilities $P(Q_1 = 0)$, $P(1 \leq Q_1 \leq B)$, and $P(Q_1 > B)$.

#### *3.2.1 Markov chain for the congestion control protocol*

The DTMC that models the evolution of $Q_1$ is depicted in Fig. 2. The number of the state denotes the amount of packets in the queue.

The steady-state distribution of the DTMC can be obtained by solving the flow-conservation equations along the lines of [22] and is given by

$$\pi_i = \begin{cases} \dfrac{(\mu_1-\lambda_1)(\mu_1'-\lambda_1)}{\mu_1\mu_1'-\lambda_1\mu_1-\lambda_1\left[\frac{\lambda_1(1-\mu_1)}{(1-\lambda_1)\mu_1}\right]^B(\mu_1'-\mu_1)}, & i = 0, \\ \dfrac{\lambda_1^i(1-\mu_1)}{(1-\lambda_1)^i\mu_1^i}\pi_0, & 1 \leq i \leq B, \\ \dfrac{\lambda_1^{B+1}(1-\mu_1)^B(1-\mu_1')^{i-1}}{(1-\lambda_1)^{B+i}\mu_1^B\mu_1^i}\pi_0, & i > B. \end{cases} \tag{11}$$

Thus, $P(1 \leq Q_1 \leq B) = \sum_{i=1}^{B} \pi_i$ is given by

$$P(1 \leq Q_1 \leq B) = \frac{\lambda_1\left(1-\xi^B\right)(\mu_1'-\lambda_1)}{\mu_1\mu_1'-\lambda_1\mu_1-\lambda_1\xi^B(\mu_1'-\mu_1)} \tag{12}$$

where $\mu_1$ is given by (2), $\mu_1'$ is given by (8), and $\xi = \frac{\lambda_1(1-\mu_1)}{(1-\lambda_1)\mu_1}$.

After replacing (12) in (10), we obtain the expression for the throughput of $D_2$. The expression $P(Q_1 = 0)$ is given by (11) and

$$P(Q_1 > B) = 1 - P(Q_1 = 0) - P(1 \leq Q_1 \leq B). \tag{13}$$

The average queue length under congestion control is $E[Q_1] = \sum_{i=1}^{\infty} i\pi_i$, after some calculations, we obtain

$$E[Q_1] = \frac{N_1 + N_2}{\mu_1\mu_1' - \lambda_1\mu_1 - \lambda_1\xi^B(\mu_1' - \mu_1)}, \tag{14}$$

where $N_1 = \lambda_1(1-\lambda_1)\mu_1\frac{\mu_1'-\lambda_1}{\mu_1-\lambda_1}\left[B\xi^{B+1} - \xi^B(B+1)+1\right]$,
and $N_2 = \xi^B\lambda_1(\mu_1-\lambda_1)\left[B + \frac{(1-\lambda_1)\mu_1'}{\mu_1'-\lambda_1}\right]$.

The average queue length for $Q_1$ without the congestion-aware protocol is given by

$$E[Q_1] = \frac{\lambda_1}{\mu_1 - \lambda_1}(1-\lambda_1). \tag{15}$$

#### *3.2.2 Delay Analysis for the legitimate user*

Here, we characterize the delay performance of the legitimate user for the cases without congestion control and with congestion control as described earlier. The average delay per packet consists of the queueing delay, $\bar{D}_{Q_1}$, and the transmission delay, $\bar{D}_T$.

The average transmission delay that a packet from $Q_1$ faces is given by

$$\bar{D}_T = \frac{1}{\bar{\mu}_1}, \tag{16}$$

where $\bar{\mu}_1$ is the probability of departure (or service probability) for the packet waiting in the head of the queue $Q_1$. For the case of congestion control, $\bar{\mu}_1$ is given by (9).

In congestion control, the average queue length is given by (14). The average queueing delay in $Q_1$ is given by

$$\bar{D}_{Q_1} = \frac{E[Q_1]}{\lambda_1}, \tag{17}$$

where $E[Q_1]$ is given by (14).

The average packet delay for receiver $D_1$ is given by

$$\bar{D}_1 = \bar{D}_{Q_1} + \bar{D}_T. \tag{18}$$

Similarly, we obtain the average delay per packet for the simple randomized policy described in Sect. 3.1.

## 4 Optimization problem

Here we consider the performance optimization problem for two-user broadcast channel from the viewpoint of multi-objective optimization. It is obviously desirable to have the average packet delay as small as possible and the average throughput for the eavesdropper as large as possible. However, these desires are in conflict because the two metrics, called as objective functions, depend on a join set of design parameters, referred to as decision variables. The multi-objective optimization allows for obtaining the so-called Pareto set. Every Pareto optimal solution, by definition, is not dominated by any other solution simultaneously in all objectives. The network designer can use the Pareto set for choosing specific parameter values which provides a trade-off between the objectives. We proceed now to formulating two bi-objective

optimization problems which are solved in a decentralized way by source $S$ and receiver $D_1$.

First, we consider a bi-objective optimization problem, where two metrics, the throughput of the eavesdropper and the average packet delay for packets intended for receiver $D_1$ are jointly optimized. The throughput for the eavesdropper, given by (10), is defined as the service probability for queue $Q_2$ when congestion control is used for queue $Q_1$, and it is desired to be maximized. The average packet delay for the legitimate receiver given by (18) is desired to be minimized. These two metrics are to be optimized by source $S$. Here the decision variables are $P_1$, $P_2$, $q_1$, and $q_2$. Since $P_1 + P_2 = P_{\max}$, they can be reduced to $P_1$, $q_1$, and $q_2$. The success probabilities in (18) and (10) can be found in [11]. The optimization problem is then defined as

$$\begin{aligned} &\min_{P_1,q_1,q_2} \ (\bar{D}_1, -\mu_2) \\ &\text{s.t} \quad P(Q_1 > B) \le P_{\text{con}}, \\ &\qquad P_{\min} \le P_1 \le P_{\max}, \\ &\qquad 0 < q_1 \le 1, \\ &\qquad 0 < q_2 \le 1, \end{aligned} \tag{19}$$

where $P(Q_1 > B)$ is given by (13), $P_{\text{con}}$ is the upper threshold for $P(Q_1 > B)$, $P_1$ is the transmission power for packets transmitted from queue $Q_1$, $P_{\max}$ is a power threshold for $P_1$, and $q_i$ is the probability that the source selects a packet from queue $Q_i$, where $i = 1, 2$.

Next, we formulate a second bi-objective optimization problem, which is solved by receiver $D_1$. The objective functions are the same as in the previous formulation, but here we have only $P_J$ as a decision variable, which is the jamming power that receiver $D_1$ uses to send the jamming signal to receiver $D_2$. The corresponding optimization problem is formulated as

$$\begin{aligned} &\min_{P_J} \qquad (\bar{D}_1, -\mu_2) \\ &\text{s.t} \qquad 0 \le P_J \le P'_{\max}, \end{aligned} \tag{20}$$

where $P'_{\max}$ is a power threshold for $P_J$.

## 5 Results and discussion

In this section, we evaluate numerically the analytical results presented in the previous sections. The metrics used to evaluate our proposed system are the average packet delay ($\bar{D}_1$), the saturated throughput ($\mu_2$), and the secrecy loss tolerance defined in [1]. The secrecy loss tolerance metric describes the trade-off between throughput and secrecy. For the congestion-agnostic policy, it is given by

$$f_{\text{ag}} = 1 - \frac{\mu_1}{\dot{\mu_1}}, \tag{21}$$

where $\dot{\mu_1} = q_1 q_2 P(D_{1/1,2}) + q_1(1 - q_2)P(D_{1/1})$, and $\mu_1$ is given by (2).

For the congestion-aware policy, the secrecy loss tolerance is given by

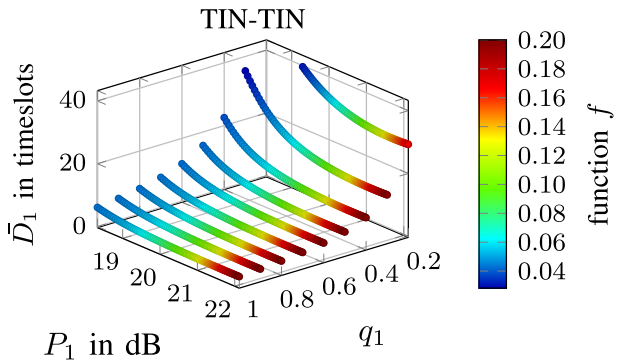


**Fig. 3** ($\bar{D_1}$, function $f_{\text{aw}}$) vs. ($q_1$, $P_1$), under congestion-aware randomized policy in TIN-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\max} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-TIN, $d_1 = 8.2$ m

$$f_{\text{aw}} = 1 - \frac{\bar{\mu_1}}{\hat{\mu}_1}, \tag{22}$$

where $\bar{\mu_1}$ is given by (9), and $\hat{\mu}_1$ is given by

$$\hat{\mu}_1 = \frac{P(1 \le Q_1 \le B)\mu_{1_\not}} + P(Q_1 > B)\mu'_{1_\not}}{P(1 \le Q_1 \le B) + P(Q_1 > B)}, \tag{23}$$

where$\mu_{1_\not}} = q_1 q_2 P(D_{1/1,2}) + q_1(1 - q_2)P(D_{1/1})$, and$\mu'_{1_\not}} = P(D_{1/1})$.

We solve the optimization problems in (19) and (20) by using PYMOO [23]. In the framework of PYMOO, we used NSGA-II [24], a multiobjective genetic algorithm.

The parameters of our system are the following: $\lambda_1 \in [0.1, 0.9]$ is the probability of a packet arrival in a time slot. $\alpha \in [2, 4]$ is the path loss exponent, where $\alpha = 2$ corresponds to free space and $\alpha = 4$ corresponds to lossy environments. $\gamma_1, \gamma_2 \in [-10\,\text{db}, +10\,\text{db}]$ are the SINR thresholds for receivers $D_1$ and $D_2$. $d_1$, $d_2$, $d_3$ $\in [0, 100\text{m}]$ are the distances between the source and each receiver, and the distance between the two receivers. $g \in [0, 1]$ is the residual self-interference, where $g = 0$, corresponds to perfect self-interference cancellation, and when $g = 1$ corresponds to no cancellation at receiver $D_1$ ($\beta \triangleq -10 \log g^2$ in dB). $P_J \in [0, 23\,\text{dB}]$ is the jamming power. $B \in [1, 20]$ is the congestion threshold in packets. $q_i \in [0, 1]$ is the random access probability for packets, where $i = 1$ refers to confidential data, and $i = 2$ refers to non-confidential data. $P_1 \in [0, 23\text{db}]$ is the transmission power for confidential packets. The parameters for our results are presented in the caption of Figs. 3, 4, 5, 6, 7 and 8.

In summary, the key points from the numerical results are the following.

- With the congestion-aware policy, $P_1$ affects the secrecy performance more than $\lambda_1$ and $q_1$ do. Function $f_{\text{aw}}$ is unaffected by $B$ in TIN-TIN and SD-TIN. In TIN-SD, higher $B$ leads to less secrecy.
- The congestion-aware policy provides better delay performance in TIN-TIN and SD-TIN for large $\lambda_1$, but for small $\lambda_1$ the two policies perform the same. IN TIN-

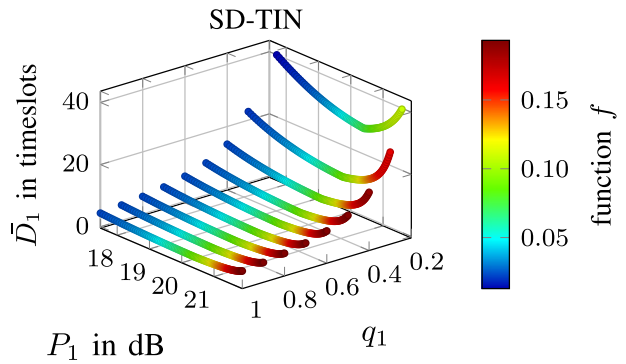


**Fig. 4** ($\bar{D_1}$, function $f_{\text{aw}}$) versus ($q_1$, $P_1$), under congestion-aware randomized policy in SD-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\text{max}} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In SD-TIN, $d_1 = 8.2$ m

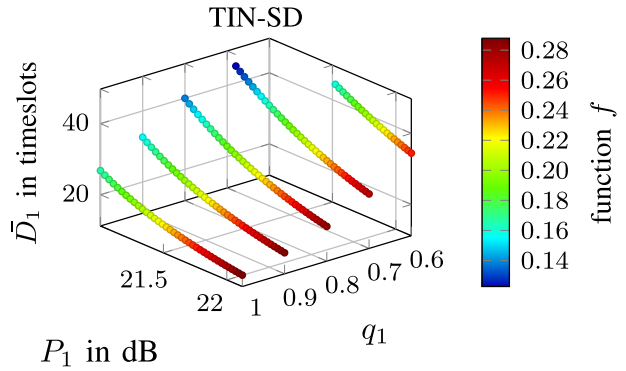


**Fig. 5** ($\bar{D_1}$, function $f_{\text{aw}}$) versus ($q_1$, $P_1$), under congestion-aware randomized policy in TIN-SD. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\text{max}} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-SD, $d_1 = 17.4$ m

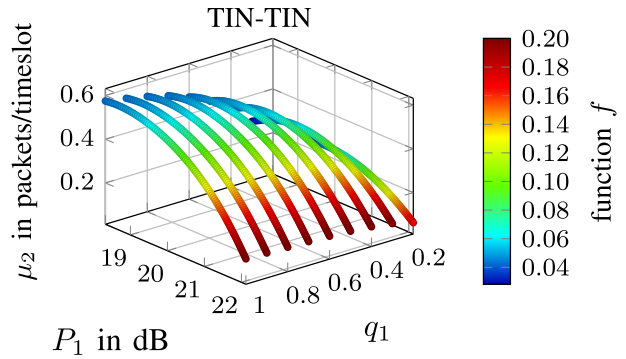


**Fig. 6** ($\mu_2$, function $f_{\text{aw}}$) versus ($q_1$, $P_1$), under congestion-aware randomized policy in TIN-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\text{max}} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-TIN, $d_1 = 8.2$ m

SD, the delay performance is better in the congestion-aware policy for any $\lambda_1$. In the congestion-aware policy, $\bar{D_1}$ increases as $B$ increases in TIN-TIN and SD-TIN

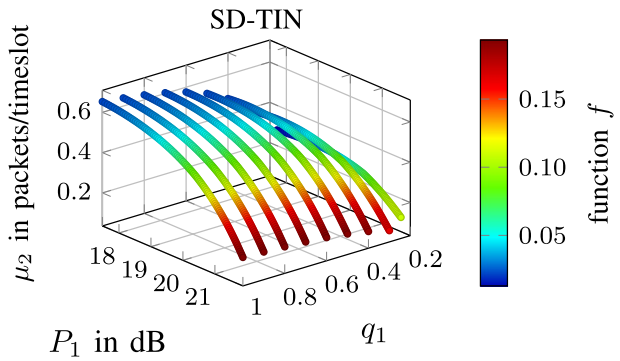


**Fig. 7** ($\mu_2$, function $f_{\text{aw}}$) versus ($q_1$, $P_1$), under congestion-aware randomized policy in SD-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\text{max}} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In SD-TIN, $d_1 = 8.2$ m

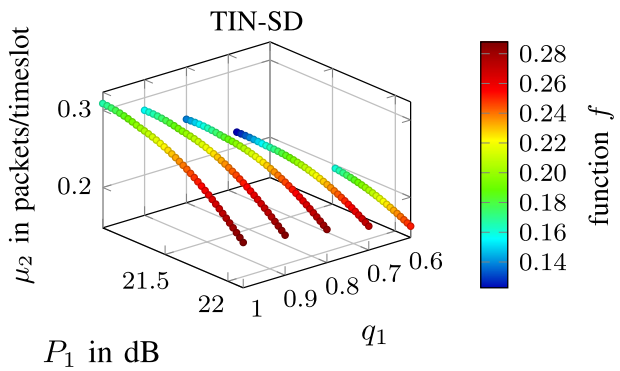


**Fig. 8** ($\mu_2$, function $f_{\text{aw}}$) versus ($q_1$, $P_1$), under congestion-aware randomized policy in TIN-SD. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $q_2 = 0.4$, $B = 6$ packets, $P_{\text{max}} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-SD, $d_1 = 17.4$ m

for small $B$. For large $B$, $\bar{D_1}$ is constant in TIN-TIN and SD-TIN. In TIN-SD, $\bar{D_1}$ keeps increasing as $B$ increases.

- The throughput performance is noticeably better in congestion-aware policy for TIN-TIN and SD-TIN. In TIN-SD, the congestion-aware policy performs better for small $\lambda_1$, but for larger $\lambda_1$, the congestion-agnostic policy achieves better results. The throughput performance remains unaffected when changing $B$ in TIN-TIN and SD-TIN. In TIN-SD, $\mu_2$ decreases for large $B$.
- The secrecy is less in congestion-aware policy in TIN-TIN and SD-TIN for large $\lambda_1$ and for any $\lambda_1$ in TIN-SD.
- We can achieve higher throughput performance and lower delay performance in SD-TIN as shown by the Pareto set for the optimization problem in (19) under congestion-aware policy.

To illustrate these findings, Figs. 3, 4, 5, 6, 7 and 8 present example results selected from a broader set of results. In particular, Figs. 3, 4 and 5 show how $\bar{D_1}$ and function $f_{\text{aw}}$ change when we change $P_1$ and $q_1$ for three combinations of decoding schemes:

TIN-TIN, SD-TIN, and TIN-SD. Here, we set $q_2 = 0.4$ and we change $q_1$ in the range [0, 1]. We also change $P_1$ in the range [0 dB, 23 dB]. The values of $q_1$ and $P_1$ that cause instability at queue $Q_1$ are not shown in the figure. Thus, the source transmits packets from both queues with the aforementioned probabilities, according to the congestion-aware randomized policy. We observe that $\bar{D_1}$ increases as $q_1$ decreases, because the average queuing delay is higher since more packets remain in queue $Q_1$. We also see that $\bar{D_1}$ decreases as $P_1$ increases in TIN-TIN and TIN-SD, because higher transmission power leads to higher probability of successful packet reception. In SD-TIN, $\bar{D_1}$ decreases as $P_1$ increases up to $P_1 = 20.5$ dB, and then it starts increasing, due to delay imposed by the successive decoding for decoding the packets. The values of $P_1$ not shown in the figure cause instability of queue $Q_1$, as explained earlier. We note that function $f_{\text{aw}}$ is affected more by $P_1$ than $q_1$. Specifically, function $f_{\text{aw}}$ increases when $P_1$ increases, meaning that higher $P_1$ leads to less secrecy of the system since the signal is stronger and the probability that the other user receives the signal is higher. We also observe that function $f_{\text{aw}}$ has the lowest value in SD-TIN, which means that we have more secrecy in this case. The reason is that the service probability is higher in SD-TIN, due to the proximity of receiver $D_1$ to the source.

Figures 6, 7 and 8 depict how $P_1$ and $q_1$ affect $\mu_2$ and function $f_{\text{aw}}$ for the cases of TIN-TIN, SD-TIN, and TIN-SD. We observe that $\mu_2$ decreases as $P_1$ increases, because $\mu_1$ is higher and receiver $D_1$ transmits a jamming signal with higher probability. We see that $\mu_2$ has the lowest value in TIN-SD for the aforementioned reason. When $q_1$ increases, $\mu_2$ also increases. This happens because $\mu_2$ depends on $q_1$ as shown in (7) and (10). This means that $\mu_2$ increases when queue $Q_1$ is non-empty, and both queues are selected with probabilities $q_1$ and $q_2$ respectively under the congestion-aware randomized policy. The values of $P_1$ and $q_1$ not shown in the figure lead to instability of queue $Q_1$, as described earlier. We also observe that function $f_{\text{aw}}$ increases as $P_1$ increases for the same aforementioned reason as in Figs. 3, 4 and 5. Function $f_{\text{aw}}$ has the lowest value in the case of SD-TIN (higher secrecy), because $\mu_1$ is higher due to better communication channel between the source and receiver $D_1$.

In Table 2, we see how $\bar{D_1}$, $\mu_2$, and functions $f_{\text{aw}}$ and $f_{\text{ag}}$ are affected by $\lambda_1$ and $P_1$ under two congestion policies for the cases of TIN-TIN, SD-TIN, and TIN-SD. We observe that the congestion-aware policy is significantly effective for large $\lambda_1$ in all aforementioned cases. For small $\lambda_1$, the delays for the two congestion policies are the same for TIN-TIN and SD-TIN. For TIN-SD, the delays are very close, but the congestion-aware policy has a better delay performance. The congestion-aware policy leads to more secrecy (low function $f_{\text{aw}}$) when $\lambda_1$ is large in TIN-TIN, but for small $\lambda_1$, the secrecy is the same for the two policies. As $P_1$ increases, $\bar{D_1}$ decreases for both policies. The same observations apply for SD-TIN, but higher $P_1$ leads to larger $\bar{D_1}$ for small $q_1$ when no congestion-aware policy is used in SD-TIN. In TIN-SD, we see that the congestion-aware policy leads to more secrecy for small $q_1$, because $\bar{\mu_1}$ is higher than $\mu_1$. The congestion-aware policy results in higher $\mu_2$ compared with $\mu_2$ in the congestion-agnostic aware policy. When $P_1$ increases, $\mu_2$ decreases in a significant volume. This happens because as $P_1$ increases, more packets are successfully received by receiver $D_1$, which transmits a jamming signal with higher probability to receiver $D_2$ to hinder successful confidential packet reception by the latter. As $\lambda_1$ increases in

**Table 2** Performance under different congestion policies

| | | | With congestion policy | | | No congestion policy | | |
|---|---|---|---|---|---|---|---|---|
| **Decoding** | $\lambda_1$ | $P_1$ **(in dB)** | $\bar{D}_1$ **(in timeslots)** | $\mu_2$ **(in packets/ timeslot)** | $f_{aw}$ | $\bar{D}_1$ **(in timeslots)** | $\mu_2$ **(in packets/ timeslot)** | $f_{ag}$ |
| TIN-TIN | 0.10 | 19.29 | 5.42 | 0.54 | 0.06 | 5.42 | 0.39 | 0.06 |
| | 0.10 | 21.58 | 4.22 | 0.26 | 0.16 | 4.22 | 0.19 | 0.16 |
| | 0.20 | 19.29 | 6.36 | 0.40 | 0.06 | 6.38 | 0.30 | 0.06 |
| | 0.20 | 21.58 | 4.63 | 0.20 | 0.16 | 4.63 | 0.15 | 0.16 |
| | 0.30 | 19.29 | 8.37 | 0.26 | 0.05 | 9.15 | 0.20 | 0.06 |
| | 0.30 | 21.58 | 5.41 | 0.14 | 0.16 | 5.44 | 0.10 | 0.16 |
| | 0.40 | 19.29 | 11.90 | 0.17 | 0.03 | 128.26 | 0.11 | 0.06 |
| | 0.40 | 21.58 | 7.10 | 0.09 | 0.15 | 7.83 | 0.06 | 0.16 |
| SD-TIN | 0.10 | 19.29 | 4.43 | 0.56 | 0.05 | 4.43 | 0.41 | 0.05 |
| | 0.10 | 21.58 | 5.44 | 0.25 | 0.17 | 5.44 | 0.18 | 0.17 |
| | 0.20 | 19.29 | 4.91 | 0.44 | 0.05 | 4.91 | 0.33 | 0.05 |
| | 0.20 | 21.58 | 6.38 | 0.17 | 0.17 | 6.41 | 0.13 | 0.17 |
| | 0.30 | 19.29 | 5.86 | 0.32 | 0.05 | 5.92 | 0.25 | 0.05 |
| | 0.30 | 21.58 | 8.37 | 0.10 | 0.16 | 9.23 | 0.07 | 0.17 |
| | 0.40 | 19.29 | 8.03 | 0.21 | 0.04 | 9.38 | 0.17 | 0.05 |
| | 0.40 | 21.58 | 11.60 | 0.05 | 0.12 | 166.05 | 0.02 | 0.17 |
| TIN-SD | 0.10 | 21.93 | 22.74 | 0.21 | 0.26 | 24.67 | 0.20 | 0.27 |
| | 0.10 | 22.12 | 20.98 | 0.19 | 0.28 | 22.27 | 0.18 | 0.29 |
| | 0.12 | 21.93 | 27.00 | 0.21 | 0.25 | 36.01 | 0.21 | 0.27 |
| | 0.12 | 22.12 | 24.68 | 0.19 | 0.27 | 30.38 | 0.19 | 0.29 |
| | 0.14 | 21.93 | 32.09 | 0.19 | 0.22 | 92.78 | 0.21 | 0.27 |
| | 0.14 | 22.12 | 29.17 | 0.19 | 0.25 | 57.99 | 0.21 | 0.29 |

TIN-TIN and SD-TIN, $\mu_2$ also decreases, because the probability of jamming is higher when receiver $D_1$ receives more packets.

Table 3 presents the impact of $P_1$, $B$, and $f_{aw}$ on $\bar{D}_1$ in TIN-TIN, SD-TIN, and TIN-SD. As shown, $B$ does not affect $\mu_2$, neither function $f_{aw}$ in TIN-TIN and SD-TIN. In TIN-SD, $\mu_2$ decreases as $B$ increases when $P_1$ is small. When $P_1$ is large, $\mu_2$ increases as $B$ increases, because large $B$ implies that the congestion policy adapts much later. We also note that function $f_{aw}$ increases as $B$ increases. In TIN-TIN, SD-TIN and TIN-SD, $\bar{D}_1$ increases when $B$ is small because the queuing delay increases. As $B$ increases, $\bar{D}_1$ increases but it is stable in TIN-TIN and SD-TIN for large $B$, whereas $\bar{D}_1$ increases as $B$ increases in TIN-SD.

Figures 9, 10 and 11 show the Pareto set for the optimization problem in (19) for the cases of TIN-TIN, SD-TIN, and TIN-SD. In SD-TIN, $-\mu_2$ has the highest value and $\bar{D}_1$ has the minimum value compared to TIN-TIN and TIN-SD due to the topology requirement of the successive decoding. We also observe that TIN-SD has the worst performance since both $-\mu_2$ and $\bar{D}_1$ have the lowest value compared to TIN-TIN and SD-TIN for the aforementioned reason.

Table 4 presents the solution for the optimization problem in (20). It has only one solution for each combination of decoding schemes, namely, $P_J^* = P_{\max}$. Comparing the optimal values of $D_1^*$, TIN-TIN has the lowest value of $D_1^*$, whereas TIN-SD has the

**Table 3** Performance in congestion-aware randomized policy when changing $B$ and $P_1$

| Decoding | $B$ (in packets) | $P_1$ (in dB) | $\bar{D}_1$ (in timeslots) | $\mu_2$ (in packets/timeslot) | $f_{aw}$ |
|---|---|---|---|---|---|
| TIN-TIN | 2 | 18.33 | 7.52 | 0.54 | 0.04 |
| | 2 | 21.88 | 4.21 | 0.19 | 0.18 |
| | 6 | 18.33 | 8.03 | 0.54 | 0.04 |
| | 6 | 21.88 | 4.23 | 0.19 | 0.18 |
| | 10 | 18.33 | 8.03 | 0.54 | 0.04 |
| | 10 | 21.88 | 4.23 | 0.19 | 0.18 |
| SD-TIN | 2 | 18.33 | 4.90 | 0.61 | 0.03 |
| | 2 | 21.88 | 6.53 | 0.17 | 0.19 |
| | 6 | 18.33 | 4.95 | 0.61 | 0.03 |
| | 6 | 21.88 | 6.85 | 0.17 | 0.19 |
| | 10 | 18.33 | 4.95 | 0.61 | 0.03 |
| | 10 | 21.88 | 6.85 | 0.17 | 0.19 |
| TIN-SD | 2 | 21.04 | 26.00 | 0.26 | 0.13 |
| | 2 | 22.12 | 16.69 | 0.17 | 0.25 |
| | 6 | 21.04 | 39.29 | 0.26 | 0.14 |
| | 6 | 22.12 | 21.10 | 0.19 | 0.28 |
| | 10 | 21.04 | 49.80 | 0.25 | 0.16 |
| | 10 | 22.12 | 22.18 | 0.19 | 0.29 |

**Table 4** Pareto optimal solution of the optimization problem in (20) for different decoding schemes

| Decoding | $P_J^*$ (in dB) | $D_1^*$ (in timeslots) | $-\mu_2^*$ (in packets/timeslot) |
|---|---|---|---|
| TIN-TIN | 23.00 | 4.24 | − 0.15 |
| SD-TIN | 23.00 | 7.83 | − 0.12 |
| TIN-SD | 23.00 | 21.81 | − 0.20 |

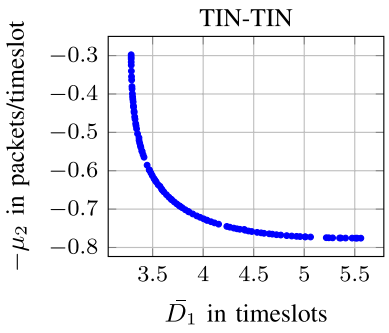


**Fig. 9** Pareto set for (19) in TIN-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1$, $\gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $B = 6$ packets, $P_{\max} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-TIN, $d_1 = 8.2$ m

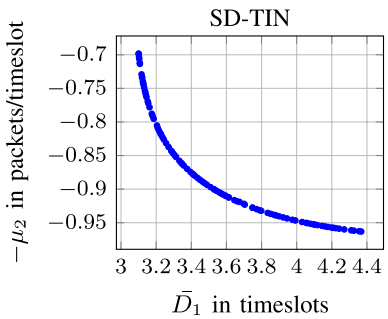


**Fig. 10** Pareto set for (19) in SD-TIN. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $B = 6$ packets, $P_{\max} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In SD-TIN, $d_1 = 8.2$ m

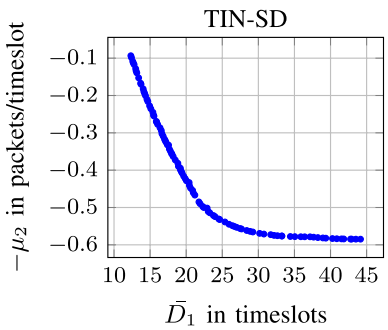


**Fig. 11** Pareto set for (19) in TIN-SD. The rest of the parameters are the following: $\lambda_1 = 0.1, \gamma_1 = -4.2$ dB, $\gamma_2 = -6.4$ dB, $\alpha = 2.2$, $\beta = 41$ dB, $P_J = 23$ dB, $B = 6$ packets, $P_{\max} = 23$ dB, $d_2 = 14.6$ m, and $d_{12} = 10$ m. In TIN-SD, $d_1 = 17.4$ m

largest value of $D_1^*$. Regarding $-\mu_2$, SD-TIN has the lowest value, whereas TIN-SD has the largest value.

## 6 Summary

Congestion can deteriorate the performance of communication networks leading to high packet delay. To address the problem of congestion in a two-user broadcast channel with contrasting traffic and security characteristics, we characterized the average packet delay for confidential traffic, and the throughput of the other user, and we proposed a congestion-aware randomized scheme. We showed that the proposed scheme can significantly improve the performance for the legitimate user.

**Acknowledgements**
This work was supported in part by Department of Science and Technology (DST), India—Swedish Research Council (VR Sweden).

**Authors' contributions**
AA carried out the analysis, evaluated numerically the results and drafted the manuscript. NP helped in the analysis and drafting the manuscript. NC and PM helped in drafting the manuscript. OB helped in the formulation of the multi-objective problem and drafting the manuscript. All authors read and approved the final manuscript.

**Funding**
Open access funding provided by Linköping University. CUGS (National Graduate School in Computer Science), IDA, Linköping University.

**Availability of data and materials**
Not applicable since no datasets were generated or analysed in the current article.

## Declarations

**Competing interests**
The authors declare that they have no competing interests.

**Author details**
[1]Department of Computer and Information Science, Linköping University, Linköping, Sweden. [2]Department of Science and Technology, Linköping University, Norrköping, Sweden. [3]Department of Electrical Engineering, Indian Institute of Technology, Tirupati, India. [4]Department of Mathematics, Linköping University, Linköping, Sweden.

Received: 27 April 2021 Accepted: 22 August 2021
Published online: 25 September 2021

**References**

1. A. Arvanitaki, N. Pappas, P. Mohapatra, N. Carlsson, Delay performance of a two-user broadcast channel with security constraints. SN Comput. Sci. **1**(1), 53 (2019)
2. A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: A survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
3. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
4. I. Csiszár, J. Körner, Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
5. T. Zheng, H. Wang, J. Yuan, Z. Han, M.H. Lee, Physical layer security in wireless ad hoc networks under a hybrid full-/half-duplex receiver deployment strategy. IEEE Trans. Wirel. Commun. **16**(6), 3827–3839 (2017)
6. P.K. Gopala, L. Lai, H. El Gamal, On the secrecy capacity of fading channels. IEEE Trans. Inf. Theory **54**(10), 4687–4698 (2008)
7. X. Zhou, M.R. McKay, B. Maham, A. Hjørungnes, Rethinking the secrecy outage formulation: a secure transmission design perspective. IEEE Commun. Lett. **15**(3), 302–304 (2011)
8. L. Zhang, H. Zhang, D. Wu, D. Yuan, Improving physical layer security for miso systems via using artificial noise, in IEEE Global Communications Conference (GLOBECOM), vol. 2015 (2015), p. 1–6
9. K. Chopra, R. Bose, A. Joshi, Secrecy outage of threshold-based cooperative relay network with and without direct links. EURASIP J. Inf. Secur. **2018**(1), 7 (2018). https://doi.org/10.1186/s13635-018-0077-8
10. N. Pappas, M. Kountouris, A. Ephremides, V. Angelakis, Stable throughput region of the two-user broadcast channel. IEEE Trans. Commun. **66**(10), 4611–4621 (2018)
11. P. Mohapatra, N. Pappas, J. Lee, T.Q.S. Quek, V. Angelakis, Secure communications for the two-user broadcast channel with random traffic. IEEE Trans. Inf. Forensics Secur. **13**(9), 2294–2309 (2018)
12. S. Lai, J. Xia, D. Zou, L. Fan, Intelligent secure communication for cognitive networks with multiple primary transmit power. IEEE Access **8**, 37 343-37 351 (2020)
13. Y. Liu, M. Xiao, S. Chen, F. Bai, J. Pan and D. Zhang, An intelligent edge-chain-enabled access control mechanism for ioV,in *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12231–12241. (2021). https://doi.org/10.1109/JIOT.2021.3061467
14. K. Miettinen, *Nonlinear Multiobjective Optimization* (1999)
15. M. Ehrgott, *Multicriteria Optimization* (2005)
16. R. Samano-Robles, A. Gameiro, Joint spectrum selection and radio resource management based on multi-objective portfolio optimization for cognitive radio networks, in *The First International Conference on Future Generation Communication Technologies* (2012), p. 22–27
17. M. Elmusrati, R. Jantti, H.N. Koivo, Multiobjective distributed power control algorithm for CDMA wireless communication systems. IEEE Trans. Veh. Technol. **56**(2), 779–788 (2007)
18. M. Elmusrati, H. El-Sallabi, H. Koivo, Applications of multi-objective optimization techniques in radio resource scheduling of cellular communication systems. IEEE Trans. Wirel. Commun. **7**(1), 343–353 (2008)
19. Z. Tong, M. Haenggi, Throughput analysis for full-duplex wireless networks with imperfect self-interference cancellation. IEEE Trans. Commun. **63**(11), 4490–4500 (2015)
20. N. Pappas, M. Kountouris, A. Ephremides, A. Traganitis, Relay-assisted multiple access with full-duplex multi-packet reception. IEEE Trans. Wirel. Commun. **14**(7), 3544–3558 (2015)
21. K. Jagannathan, E. Modiano, L. Zheng, On the role of queue length information in network control. IEEE Trans. Inf. Theory **57**(9), 5884–5896 (2011)
22. N. Pappas, M. Kountouris, Throughput of a cognitive radio network under congestion constraints: a network-level study, in *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)* (2014), p. 162–166
23. J. Blank, K. Deb, Pymoo: multi-objective optimization in python. IEEE Access **8**, 89 497-89 509 (2020)
24. K. Deb, A. Pratap, S. Agarwal, T. Meyarivan, A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput. **6**(2), 182–197 (2002)

## Publisher's Note