Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Adaptive packet scheduling over a wireless channel under constrained jamming

Antonio Fernández Anta [a], Chryssis Georgiou [b], Dariusz R. Kowalski [c], Elli Zavou [a,d,*]

[a] IMDEA Networks Institute, Avda. del Mar Mediterráneo 22, 28918, Madrid, Spain
[b] University of Cyprus, 1678 Nicosia, Cyprus
[c] University of Liverpool, Liverpool, United Kingdom
[d] Universidad Carlos III de Madrid, 28911 Madrid, Spain

ARTICLE INFO

Article history:
Received 31 October 2016
Received in revised form 27 April 2017
Accepted 21 June 2017
Available online xxxx
Communicated by K. Censor-Hillel

Keywords:
Packet scheduling
Online algorithms
Wireless channel
Unreliable communication
Adversarial jamming
Adversarial Queuing Theory

ABSTRACT

In this work we consider the communication over a wireless link, between a sender and a receiver, being disrupted by a jammer. The objective of the sender is to transmit as much data as possible to the receiver in the most efficient way. The data is sent as the payload of packets, and becomes useless if the packet is jammed. We consider a jammer with constrained power, defined by parameters ρ and σ, which represent the rate at which the adversary may jam the channel, and the length of the largest burst of jams it can cause, respectively. This definition translates to the Adversarial Queuing Theory (AQT) constraints, typically used for packet arrivals.

We propose deterministic algorithms that decide the length of the packets sent in order to maximize the goodput rate; i.e., the amount of useful payload successfully transmitted over time. To do so, we first define and study a static version of the problem, which is used as a building block for the dynamic problem. We start by assuming packets of the same length and characterizing the corresponding quasi-optimal length. Then, we show that by adapting the length of the packets, the goodput rate can be improved. Hence, we develop optimal adaptive algorithms that choose the packet lengths depending on the jams that have occurred up to that point in time, in order to maximize the total payload transmitted successfully over a period T in the presence of up to f jams.

1. Introduction

Motivation. Transmitting data over wireless media in a fast and reliable way, has been attracting a lot of attention from the research community for quite some time now [3,7,11,12,15,20,24,25,28–30], and continues to increase its popularity, especially due to the increment of usage of mobile devices (e.g., smart phones, tablets). One of the many challenges of wireless communication, depending on the specific model and applications, is to cope with disruptions, especially when they are caused intentionally, e.g., by malicious jamming devices. Some of the research efforts already done in addressing this challenge, have looked in different assumptions and constraints (e.g., [4–6,13,16,20,23–25,28]) and will be further discussed in the Related Work part of this section.

* Corresponding author at: IMDEA Networks Institute, Avda. del Mar Mediterráneo 22, 28918, Madrid, Spain.
E-mail address: elli.zavou@imdea.org (E. Zavou).

http://dx.doi.org/10.1016/j.tcs.2017.06.020
0304-3975/

In our work we look at a wireless communication over a single channel between a sender and a receiver, being "watched" and disrupted by a malicious, adversarial jammer. The sender's goal is to fully transmit over the channel as much data possible in the most efficient way, despite the jams. More precisely, the sender has a potentially unbounded amount of data to be transmitted. Each packet sent contains a *header* of fixed size h and some *payload* whose size, l, depends on the scheduling algorithm used. Note that this payload counts towards the total size of the actual data to be transmitted. For simplicity and without loss of generality we assume that $h = 1$. We also consider *constant bit rate* for the channel (and hence constant bandwidth), which means that the transmission time of each packet is proportional to its size (in particular, a packet of size $l + 1$ takes $l + 1$ time units to be transmitted in full). What is more, when a packet is jammed, it needs to be retransmitted; hence we assume a feedback mechanism that informs the sender when a jam occurs. Our objective is to define optimal scheduling algorithms that decide the length of the packets to be sent, in particular their payload, so that they maximize the amount of data transmitted in time.

We assume that the adversary has complete knowledge of the packet scheduling algorithm and it decides on how to jam the channel dynamically. However, the jamming power of the adversary is constrained by two parameters, ρ and σ, whose values depend on technological aspects. Parameter ρ represents the rate at which the adversary can jam the channel and σ the largest size of a burst of jams that can be caused. More precisely, parameter σ represents the maximum number of "error tokens" available for the adversary to use at any point in time, and ρ represents the rate at which new error tokens become available (one at a time). Each error token models the ability of the adversary to jam one packet. This adversarial model could represent a jamming entity with limited resource of rechargeable energy, e.g., malicious mobile devices [1,2] or battery-operated military drones [14,18]. In these cases, σ represents the capacity of the battery (in packets that can be jammed) and ρ the rate at which the battery can be recharged (for instance, with solar cells). We call this model *dynamic*, due to the unpredictability and dynamic nature of the adversary and the channel jams.

To evaluate the scheduling algorithms considered, we use the *goodput rate* as our efficiency measure; successful transmission rate achieved. Under this model, we first show upper and lower bounds on the transmission time and goodput rate when the sender sends packets of the same length throughout the execution (uniform case), not taking into account the history of jams. The interesting question then is whether this bound can be surpassed by adapting the packet length depending on the channel jams. Considering first the case of $\sigma = 1$, we propose an adaptive scheduling algorithm that changes the packet length based on the feedback on jammed packets, and show that it can achieve better goodput and transmission time with respect to the uniform case, for most values of ρ. However, the analysis technique used for the case $\sigma = 1$ turned out not to be easily generalized for cases where $\sigma > 1$. Devising an optimal solution for the overall problem seems to be a challenging task.

In order to better understand the above problem and lay the groundwork for obtaining its optimal solutions, we also consider a simpler version of the problem, for which we define a corresponding model, called *static*. In particular, we focus on a specific time interval of length T, and instead of assuming that new error tokens are continuously arriving we assume a fixed number of error tokens f. The sender's objective now is to correctly transmit the maximum amount of data, considering the jamming power of the adversary. The adversary is constrained only by parameter f; the maximum number of errors (packet jams) it can introduce in the corresponding interval T (all tokens are available from the very beginning of the interval). Hence, given T and f, we want to maximize the total *useful payload* transmitted within the interval of interest.[1]

We then use the static model as a building block for the solution of the dynamic one. More details on the two models and our assumptions are detailed in Section 2.

In a previous work [4], we studied the impact of adversarial errors on packet scheduling, focusing on the long term competitive ratio of throughput, named *relative throughput*. We explored the effect of feedback delay and proposed algorithms that achieve close to optimal relative throughput under worst-case errors, and adversarial or stochastic packet arrivals. Part of the motivation to this work, was the question whether the upper bound of the relative throughput could be exceeded when the power of the adversary is constraint, one of the main differences with this work. Another difference is that in the current work the packet sizes are chosen by the sender, whereas in the previous one they were given. And last but not least, in [4], jammed packets were not retransmitted; the objective was to route packets as fast as possible and not strive to have each packet transmitted. In the current work, the choice of the packet size is precisely the most critical part from the side of the sender. Thus, we focus in devising scheduling algorithms for the decision of packet length to be used and conduct worst-case analysis for the efficiency measures.

Contributions. In this work, we first introduce our *dynamic*, AQT-based adversarial jamming model in wireless networks. AQT has been widely used for restricting packet arrivals in similar settings (see related work below). However, not much research has been done that considers the possibility of exploring its effects in the intent to "damage" a network. We compare our model with the few that have considered similar approaches in the related work below. As already mentioned, our approach of constrained adversarial jamming could be used to model battery-operated malicious devices that have bounded battery capacity and specific recharging rate. In Section 2, we formalize the constrained adversarial jamming model we consider, which we call *dynamic*, as well as the *static* version of the model (focusing on their differences), that is used as a

[1] Since we assume that the transmission time of each packet is equal to its length, it follows that T is an absolute upper bound on the useful payload transmitted.

Please cite this article in press as: A. Fernández Anta et al., Adaptive packet scheduling over a wireless channel under constrained jamming, Theoret. Comput. Sci. (2017), http://dx.doi.org/10.1016/j.tcs.2017.06.020