GNU Radio implementation for Multiuser Multi-Armed Bandit learning algorithms in IoT networks

Julio Manco-Vasquez¹, and Christophe Moy², Faouzi Bader¹

¹ IETR / CentraleSupélec Campus de Rennes, F-35510 Cesson-Sévigné, France, {JulioCesar.MancoVasquez, Faouzi.Bader} @CentraleSupelec.fr
² Univ Rennes, CNRS, IETR - UMR 6164, F-35000, Rennes, France
Christophe.Moy@Univ-Rennes1.fr

Abstract

Novel access schemes based on multi-armed bandit (MAB) learning approaches has been proposed to support the increasing number of devices in IoT networks. In the present work, a GNU radio framework is implemented to recreate an IoT network where IoT devices embedding MAB algorithms are able to learn the availability of the channel for their packet transmissions to the gateway. It allows to incorporate several IoT users recognized by an identifier (ID), and provides a gateway to handle a large number of IDs as well as the packet collisions among IoT devices. The experimental results show that the introduction of learning mechanism in access schemes can improve the performance of the network.

1 Introduction

Several efforts to introduce reinforcement learning algorithms tailored for low-power wide-area (LPWA) networks have been recently carried out [1, and references therein]. However, unlike opportunistic spectrum access (OSA) schemes, where several proof of concept based on MAB algorithms have been developed [2, and references therein], the experimental evaluation for IoT networks has been overlooked.

Previous works regarding the evaluation of MAB algorithms for OSA in decentralized networks do not take into account realistic transmissions between the primary and secondary users, and utilize particular toolboxes avoiding to run reproducible experiments. In this regard, a first proof of concept to assess the potential usage of MAB algorithms for IoT scenarios is provided in [1]. It is fully implemented in GNU radio, and we consider this initial effort to introduce features concerning an LPWA network. In doing so, the emulation of an IoT network to support a large number of users is addressed. Our testbed is composed of several IoT devices and a Gateway, where each IoT device following an ALOHA wireless protocol transmits a packet containing its ID, and waits for an ACK packet transmitted by the gateway, as it is shown in Fig. 1. For that end, a data packet structure is implemented to provide the required support for a multiuser scenario. Our demonstration shows that significant gains can be obtained, when a well-known MAB approach, an Upper-Confidence Bound (UCB) algorithm [1] is embedded in IoT devices.

2 Experimental setup

Our testbed is implemented using N210 USRPs connected to an Octoclock for time and frequency synchronization among the devices. Each USRP running a GNU radio application implements a transceiver composed of three GNU radio blocks. For instance, in an IoT user, a first block corresponding to the physical layer detects and demodulates the packets into QPSK symbols, after which a second block detects the ID within the ACK packet. In the last block, a new packet is created and transmitted through the frequency channel pointed out by the MAB algorithm, if it is embedded in the IoT device.

The implemented data packet structure is shown in Fig. 2, where a preamble is utilized for the packet detection and phase correction of the received signal, while the values in the field UP/DOWN allow the receivers at the gateway and the IoT user to only receive uplink and

In a similar way, it operates at the gateway side, where after demodulating the packet, an ID detection is carried out to identify the IoT user, and finally an ACK packet is created in the last block.
A data packet composed of a preamble, a field named UP/DOWN, and a user ID given by six blocks of QPSK symbols, $B_k$.

downlink packets, respectively. The ID user is defined by 6 blocks of QPSK symbols $B_k$ for $k \in [1, 6]$, which are assigned two possible constellation symbols. Then, a threshold is applied to the number of times that a symbol is received within each block $B_k$, so that a decision about the transmitted symbol is made. Hence a binary sequence of 6 bits are obtained, and consequently a total of 64 users can be supported.

### Results

We evaluate our demo in a scenario with a clear line of sight (LOS) by placing two IoT users and a gateway, all of them working at a carrier frequency of 433.5 MHz. Each IoT user embedding a UCB algorithm is able to select among four frequency channels and transmit packets of roughly 0.5 seconds following a LoRa standard. In Fig. 3, the implemented GNU radio companion (GRC) designs are depicted, where

*The length of the fields can be adjusted to support more users. In fact, our implementation allows to divide the blocks $B_k$ into chunks of symbols so as to convey more bits. Furthermore at higher sample rates, more symbols per block $B_k$ are available.*

For a more detailed illustration of the implemented UCB algorithm, the reader may refer to [1].

### Conclusion

We have presented a GNU radio implementation that recreates an IoT network for the evaluation of access policies based on reinforcement learning approaches. Our framework introduces a packet structure to handle a large number of IoT users that may incorporate MAB algorithms. Finally, the experimental results show that a UCB approach improves the performance of the IoT user. Furthermore, the modular design of the proposed framework allows the evaluation of any novel access policy, as well as the incorporation of other physical layers.

### References
