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

Julio Manco-Vasquez, Christophe Moy, Faouzi Bader

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

Julio Manco-Vasquez[1], and Christophe Moy[2], Faouzi Bader[1]

[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 unlicensed bands. 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 channels 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 decentralized learning mechanism in access schemes can improve the performance of the IoT devices, both in terms of energy consumption and spectrum overload, thanks to radio collision mitigation.

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 limited in number and multi-devices conditions [3].

Previous works regarding the evaluation of MAB algorithms for OSA in decentralized networks do not take into account all aspects of realistic transmissions between the primary and secondary users. In this regard, a first proof of concept to assess the potential usage of MAB algorithms for channel selection in unlicensed bands for IoT scenarios is provided in [3]. It is fully implemented in GNU radio, and we consider this initial effort to introduce new 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.

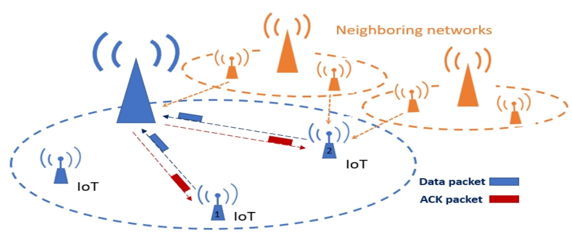

Figure 1: A LPWA scenario with IoT devices that aim to select the best channel for their transmissions to the gateway, while collisions among other IoT devices and interference from other networks may occur.

2 Experimental setup

Our testbed is implemented using N210 USRPs from Ettus/NI connected to an Octoclock for time and frequency synchronization among the devices. Each USRP running a GNU radio application implements a transceiver composed of dedicated 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 [1].

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

[1] In a similar design, 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.

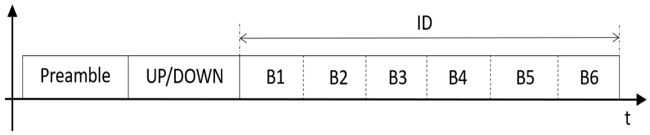

Figure 2: A data packet composed of a preamble, a field named UP/DOWN, and a user ID given by six blocks of QPSK symbols, B_k.

the gateway and the IoT user to discriminate between uplink and downlink packets. The ID user is defined

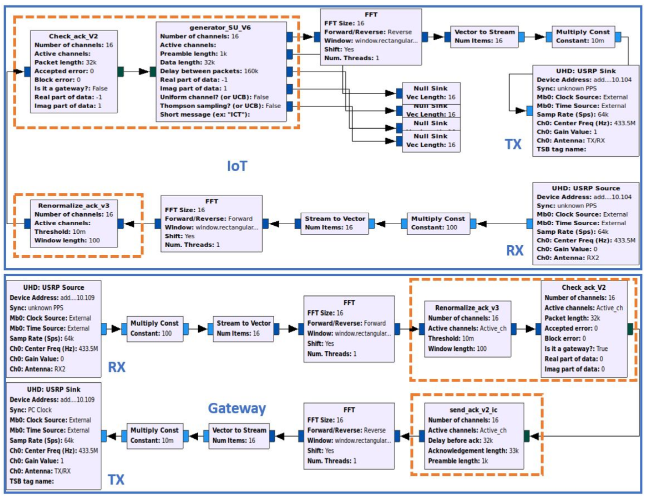

Figure 3: The GRC designs for the IoT device and the gateway are described at the top and bottom of the figure, respectively. The blocks corresponding to our framework are higlighted (in orange boxes) within the flowgraphs.

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 to detect a radio collision. Hence a binary sequence of 6 symbols of 1 bit are obtained, and consequently a total of 64 users can be supported [2].

3 Results

We evaluate our demo in a scenario by placing two IoT users and a gateway, all of them working at a carrier frequency of 433.5 MHz that can be arbitrary set at any value between 100 MHz and 6 GHz. Each IoT user embedding a UCB algorithm [3] is able to select among four frequency channels and transmit packets of roughly 0.5 seconds following a LoRa-like standard. In Fig. 3, the implemented GNU radio companion (GRC) designs are depicted, where a sample rate of 64 kbps, and 4×10^3 symbols for each block

[2] The length of the fields can be adjusted to support more users.

[3] For a more detailed illustration of the implemented UCB algorithm, the reader may refer to [3].

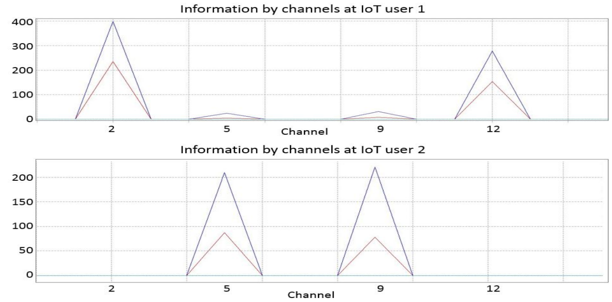

Figure 4: Number of times a channel is selected (curve in blue) and the number of successful transmissions (curve in red) for each channel and IoT users under heavy IoT traffic conditions.

B_k are configured. An FFT block of size 16 is employed to a provide a channel selection mechanism with four channels[4] indexed as 2, 5, 9, and 12. In this example, one of the IoT user is set to use the channels 9 and 12, whereas a second IoT user is able to choose among the four channels. The obtained results in Fig. 4 show that the second IoT user learns to select the available channels 2 and 12 (curve in blue), meaning that the gateway is able to handle the incoming packets by replying with the corresponding ACK packets. On the other hand, a gap is observed between the number of trials and successful transmission due to the collisions involved with the surrounding traffic generated by purpose to emulate the IoT networks density in unlicensed networks.

4 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

[1] R. Bonnefoi, C. Moy, and J. Palicot, "Improvement of the LPWAN AMI backhaul's latency thanks to reinforcement learning algorithms," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, p. 34, 2018.

[2] C. Robert, C. Moy, and H. Zhang, "Opportunistic Spectrum Access Learning Proof of Concept," in *SDR-WinnComm14 Wireless Innovation Conference,Schaumburg, Illinois, USA*, 11-13 March 2014.

[3] L. Besson, R. Bonnefoi, and C. Moy, "GNU Radio Implementation of MALIN: "Multi-Armed bandits Learning for Internet-of-things Networks"," in *IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2019.

[4] Note however that the FFT size is flexible, and it can incorporate up to 128 channels.