*URSI GASS 2021, Rome, Italy, 28 August - 4 September 2021*

# Artificial Intelligence for Jamming Mitigation in IoT Networks: LoRaWAN Field Measurements Using IoTligent

Christophe MOY
Univ Rennes, CNRS, IETR - UMR 6164, F-35000, Rennes, France, christophe.moy@univ-rennes1.fr

## Abstract

This paper gives the results of the implementation of decentralized artificial intelligence algorithms embedded in IoT devices in order to make them behave smartly against radio jamming conditions in the unlicensed bands. Whatever jamming source is (IoT devices, other interferers in the ISM band, propagation conditions, or malicious radio interferers aiming at denial of service), the proposed solution gives the ability to smart IoT devices, named IoTligent, to choose transmitting in channels which are not jammed and therefore obtain a better transmission success rate towards the gateway and the network. In case of retransmission mode, it directly improves battery lifetime of the devices. In the illustrated scenario, the percentage of successful transmission improves from 65% (obtained for a reference device) to 93% for IoTligent devices during the initial learning phase and rapidly (after just a few tens of transmissions) up to 96%, with a theoretical limit of 100% in the long term. Results are given for a LoRaWAN network but would be the same with any other IoT standard in unlicensed bands.

## 1 Introduction

We proposed last year the first results of the implementation of artificial intelligence algorithms on IoT devices deployed in a real LoRaWAN network in the town of Rennes, France. We named this decentralized solution based on reinforcement learning: IoTligent [1]. The first goal of this approach is to mitigate radio collisions that will occur in unlicensed bands when the number of IoT devices reaches expected forecasts of 10s of billions of IoT devices by year 2020 [2]. However, if the results of [1] demonstrated the efficiency of the proposed solution, the real conditions of the experiments did not permit to completely decide on experimental constraints.

As we were in real network conditions open to public use, we could not indeed know the number of devices and the traffic load they generated in the surrounding environment of the experiment. There was some balance in the spectrum “quality-in-the-large” and IoTligent could detect it and cope with it. We can just make the hypothesis that the inhomogeneity of occupancy of the radio channels was probably not due to a great number of IoT devices transmitting in the ISM band in the area of Rennes. So the results of [1] effectively demonstrated the efficiency of the proposed solution, but maybe for other reasons than spectrum scarcity due to the high density of IoT devices. Other systems also use the ISM 868 MHz band, such as remote keys, but we hardly can imagine these sporadic and short term transmissions could provoke such a spectrum scarcity. The main reason is probably due to propagation issues. Objects were located at the limit of LoRa gateways range (around 15 km with mostly urban and partly suburban conditions). What is surprising with this hypothesis is that the three considered channels were very close and it would be hard to explain why conditions were so different in the three cases. Note that the proposed solution could also be used as a countermeasure to malicious radio attacks for denial of service (DoS).

Anyway, our goal was reached: obtain better transmission success rate for IoTligent device compared to a normal device in the context of a LoRaWAN network, in case of spectrum inhomogeneity in the radio channels. However we propose in the current paper to keep on validating these observations, by generating interference with mastered probability of occurrence in several channels, in order to check if IoTligent devices are able to avoid these channels, and how fast they can do it. Therefore, we propose in this paper to generate artificial jamming radio signals in a real LoRaWAN network, whatever they would be IoT signals or interferences of any other kind, or due to a degradation on propagation conditions in a given radio channel or malicious radio attacks. Seven channels are considered this time, within three of them are partially jammed

We first remind briefly in the next section the proposed solution based on artificial intelligence and the results obtained in previous paper. Then Section 3 details the experimental set-up we built in order to make these new experiments. Finally, section 4 gives results which confirm the pertinence of the proposed solution for radio jamming mitigation in unlicensed band IoT networks.

## 2 Proposed solution*: IoTligent*

IoTligent is based on previous work made in the field of Cognitive Radio [3] [4] for Opportunistic Spectrum Access (OSA) issue, a specific case of Dynamic Spectrum Access (DSA) [5]. It has been introduced in 2010 [6] that OSA can be modeled as a Multi-Armed Bandit (MAB) issue and solved in theory at least by Upper Confidence Bound (UCB) algorithm [7][8]. Numerous papers have investigated bandit algorithms for OSA since, on many different aspects: Markovian environment models, multi-players, non-stationary environments, new algorithms, etc. However, we have made the only investigations that have demonstrated the success of that solution in practice, thanks to Proof-of-Concept (PoC) on OSA demonstrators running the algorithms with real radio signals in lab conditions, such as in [9] and [10].

Then IoT spectrum access in unlicensed bands has also been modeled as a MAB issue and the pertinence of bandit algorithms has been also demonstrated for IoT radio collisions mitigations in simulations [11], at PoC level [12] and in real LoRaWAN network conditions [1]. The results of the current paper aim at validating IoTligent approach for generic jamming reasons, whatever they are due to ultra-dense IoT scenario where many radio collisions occur in unlicensed bands, or propagation disagreement concerning specific channels, in order to reproduce and better understand what was observed in real network conditions in [1].

Bad transmissions (or receptions) are a main drawback in IoT since it directly affects the IoT devices' battery autonomy. Indeed, transmission is the most energy-consuming operation made by most of IoT devices. It can roughly represents a factor 2 to 4 compared to the energy necessary at reception and 4 to 5 orders of magnitude times higher than sleep mode (for LoRa, see Semtech SX1272/73 datasheet). So, each IoT device transmission that is not received, or each retransmission, has a high cost for IoT battery lifetime and IoT network efficiency. This could be, for instance, the goal of a malicious attacker aiming at DoS.

## 3 Experimental setup

### *3.1 Proposed artificial intelligence solution*

IoTligent is based on reinforcement learning algorithms such as UCB, as proposed in [6]. Refer to [1] for the details in IoT and LoRa context. Reinforcement learning is based on a feedback loop that gives a success measure of experience. In the IoT context we propose to use the acknowledgement (ACK) sent by the gateway to the IoT device. Before each transmission, IoTligent device selects within k channels, the one with highest UCB index $B_k(t) = X_k(t) + A_k(t)$ with $X_k$, the empirical mean of transmission success, i.e. of ACK received by the IoTligent devices from the gateway, and $A_k$ a bias made to obtain mathematical proofs of convergence [8]. Then only $X_k$, which is a simple mean and $A_k$, which is a factor obtained with half a dozen of operations (depending on bandit algorithm), have to be computed and stored for each channel, once for each transmission. So, IoTligent relies on a specific kind of artificial intelligence (AI) algorithm, which is so simple to implement that it can be applied in a decentralized manner, i.e. at IoT device side. It adds indeed almost no extra overhead (processing, memory, energy consumption). Moreover, as the radio conditions may be quite different at gateway side and devices side, it is important that device can make decisions before transmitting (and consuming energy). Whereas it involves artificial intelligence algorithms, the proposed solution provides energy savings compared to a mis-transmission.

### *3.2. Hypothesis*

One main justification for IoTligent is that it imposes no change on normal LoRaWAN protocol [13] neither in terms of extra retransmission, nor extra-power to be sent, nor extra data to be added in frames.

Only condition is to use an acknowledged mode for IoT. The hypothesis that radio "channels" (there are no official channels in ISM bands) are not all jammed by surrounding radio signals (IoT or not) with the same probability, is due to the superposition of many independent IoT networks at the same place. As the propagation conditions that affect the channels, it is not possible to predict it in time and space how events happen for each IoT device, so the need to learn on the field.

## 4 Results

Experiments are done with Pycom LoRa devices and a 8 channels LoRaWAN Multitech gateway, but we do not use the 869.5 MHz channel often used for downlink as it has a 10% duty cycle band. Jamming is generated with SDR (software defined radio) USRP platforms, with the capability to choose channels and percentage of time the jamming signals are activated. Jamming signals are a set of pure sub-carriers here. In order to avoid interference in the 868 MHz, the experiments are done in an anechoic chamber and Faraday cage.

### *4.1 Experimental scenario*

The experimental conditions are presented in TABLE I on 7 channels of 200 kHz in European ISM band at 868 MHz. This illustrates the case of LoRaWAN spectrum where 3 channels are jammed, either used by surrounding devices, or malicious radio attackers or due to propagation conditions in the area, and 4 channels are let interference-free. Experiments are made in parallel on one reference IoT device with a usual behavior, i.e. randomly transmitting through channels, and one IoTligent device. Both operate at the same time and the same transmission period in the same conditions for fair comparison. Of course, they probably do not transmit at exactly the same millisecond. Anyway, we can consider that they are not interfering the one with the other if they are transmitting in the same channel. Channel bandwidth is set to 125 kHz for both.

The goal of the experiment is to verify if the proposed solution makes IoTligent devices:

- avoid transmitting in jammed channels,
- avoid more and more jammed channels with time, thanks to learning,
- adapt to changing conditions in the environment,

and to check if:

- learning is not a drawback at the beginning, when learning is not yet achieved,
- learning time is fast compared with IoT lifetime,
- total successful transmissions is really better for IoTligent devices than for reference IoT devices.
- IoTligent devices equally balance their transmissions between unjammed channels.

TABLE I. CHANNEL JAMMING TIME PERCENTAGE DUE TO AMBIENT IOT TRAFFIC, CHANNELS CHARACTERISTICS OR MALICIOUS ATTACKS.

| Channel | % of jamming | Frequency (in MHz) | Figure color |
|---|---|---|---|
| #0 | 0 % | 866.9 | dark blue |
| #1 | 0 % | 867.1 | red |
| #2 | 0 % | 867.3 | yellow |
| #3 | 40 % | 867.5 | green |
| #4 | 40 % | 867.7 | purple |
| #5 | 0 % | 867.9 | light blue |
| #6 | 40 % | 868.1 | dark green |

### *4.2 Interpretation*

Global results of the experiment are given in TABLE II. The objects performance has been measured during 475 transmissions. We can see that the reference IoT devices did not receive 166 times the acknowledgement sent by the gateway, for a mean 65,1 % of success. During the same period, IoTligent device just lost 33 ACK and reached 93% of success.

TABLE II. COMPARED RESULTS AT THE END OF THE EXPERIMENT BETWEEN REFERENCE IOT DEVICE AND IOTLIGENT DEVICE IN TERMS OF PERCENTAGE OF SUCCESS (I.E. ACK RECEIVED BY THE DEVICE).

| | Reference IoT | IoTligent |
|---|---|---|
| Nb of iterations | 475 | 475 |
| Nb of no ACK | 166 | 33 |
| % of success | 65,1 % | 93,1% |

TABLE III is a sum-up of the experiment and all the results which will be further detailed in the following figures. We can see that contrary to the reference IoT device, the IoTligent device did not go through the channels uniformly. Thanks to the learning algorithm, and contrary to the reference IoT device, it privileged the use of channels #0, #1, #2 and #5. Indeed the choice made by the algorithm is partly built on the empirical mean of successes obtained in each channel, which make these channels obviously better than the 3 others. The result is that IoTligent device used ten times more each of the unjammed channels than the others during the total duration of the experiment.

TABLE III. COMPARED RESULTS AT THE END OF THE EXPERIMENT BETWEEN REFERENCE IOT DEVICE AND IOTLIGENT DEVICE IN TERMS OF NUMBER OF TRANSMISSIONS (TX) AND PERCENTAGE OF SUCCESS ON EACH CHANNEL.

| | Reference IoT | | IoTligent | |
|---|---|---|---|---|
| Channel | % of success | Nb of Tx | % of success | Nb of Tx |
| #0 | 95,8 % | 72 | 98,2 % | 110 |
| #1 | 94,2 % | 69 | 99,1 % | 116 |
| #2 | 92,6 % | 68 | 98,2 % | 109 |
| #3 | 28,3 % | 67 | 25 % | 12 |
| #4 | 32,4 % | 68 | 20 % | 10 |
| #5 | 97 % | 66 | 97,2 % | 109 |
| #6 | 10,8 % | 65 | 11,1 % | 9 |

TABLE IV shows that the results of TABLE III are underestimated as they encounter also learning phase which occurs at the beginning of the experiment. Indeed, as the proposed algorithm requires no previous training, it starts from scratch. However, learning is very fast. We can see in TABLE IV that on the last 100 iterations over 475 of this experiment, 96% of the transmissions have been made in the unjammed channels only. The percentage of success which is expected in theory in the long term is 100% as IoTligent device should more and more only transmit in the jamming-free channels.

TABLE IV. RESULTS OF THE REFERENCE IOT DEVICE AT THE END OF EXPERIMENTS, I.E. ON THE LAST 100 ITERATIONS, IN TERMS OF NUMBER OF TRANSMISSIONS AND PERCENTAGE OF SUCCESS ON EACH CHANNEL.

| Channel | % of success | Nb of Tx |
|---|---|---|
| #0 | 100 % | 24 |
| #1 | 100 % | 24 |
| #2 | 100 % | 23 |
| #3 | 0 % | 1 |
| #4 | 66,7 % | 3 |
| #5 | 95,8 % | 24 |
| #6 | 0 % | 1 |

### *4.3 Detailed results through time*

The following figures enable to observe what happened trough time during the experiment. Figure 1 represents the evolution of the number of times each channel has been chosen by IoTligent through time. We can see that rapidly (after 10 to 20 transmissions only), IoTligent did just concentrate on the use of the 4 unjammed channels. Other 3 jammed channels are just tried form time to time, in order to see if they had been rejected due to bad luck untill now. Note that sometimes, a good transmission may occur also in these 3 channels as they are jammed only 40% of time. Remark that the same curve for reference IoT device would show all 7 channels roughly following the same regular ramp from 0 to around 70, as seen on TABLE III.

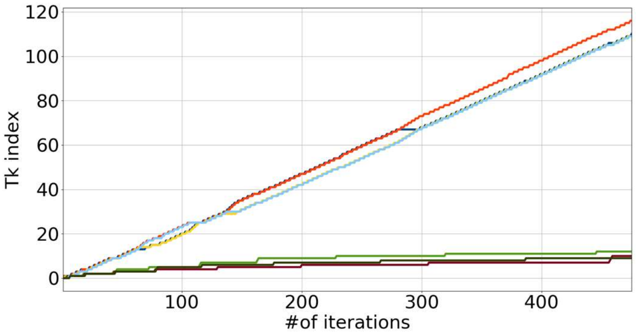

Fig. 1. Evolution of $T_k(t)$, the number of selections of each channel k through time, for IoTligent device.

The empirical mean $X_k(t)$ of IoTligent device in Figure 2 reveals the success rate measured by IoTligent. For unknown reasons, which prove that these results are experimental and not simulated, we can see that some but few transmissions were not acknowledged also in the 4 unjammed channels. They should be constant at 100%. However, they converge to nearly 99% as seen in column 4 of TABLE III, which does not make results derive.

For the 4 jammed channels, average percentage of success can be better approached on Figure 3 as more attempts have been made by reference IoT device on these channels than IoTligent device which avoided them as much as possible. We can see that the number of steps is much higher for the green, purple and dark green curves on Figure 3 than on Figure 2.

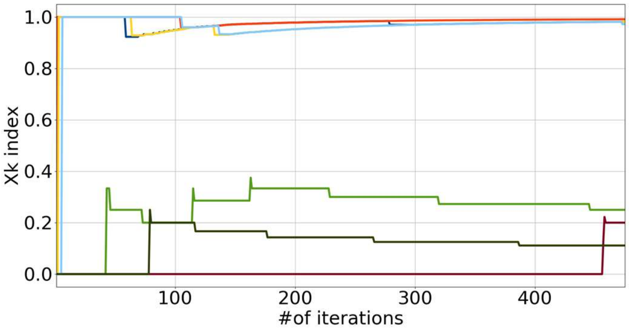

Fig. 2. Evolution of $X_k(t)$, the empirical mean of each channel k through time, for IoTligent device.

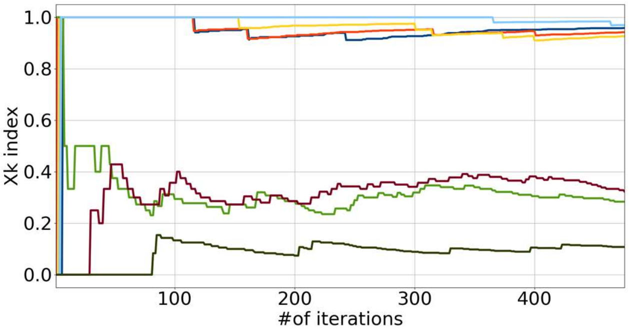

Fig. 3. Evolution of $X_k(t)$, the empirical mean of each channel k through time, for reference IoT device.

## 8. Conclusion

This paper gives results of the implementation of learning algorithms on devices deployed in a real IoT LoRaWAN network. These results could be obtained with any other IoT technology in ISM bands. We can now answer the questions asked in section 4.1: IoTligent devices clearly avoid transmitting more and more with time in jammed channels. Learning is never degrading the performance of IoTligent device, compared to reference device. Learning is just less efficient at the beginning but it rapidly improves the performance, at the scale of a few 10s of transmissions. As it is a much shorter period than IoT lifetime, this guarantees that IoTligent device is benefiting from learning most of the time. Learning is so fast that if surrounding conditions are changing (interfered channels change), a simple reset on learning enables to adapt to changing conditions. Equal balance between good channels is achieved, avoiding the concentration of all IoTligent devices in the same channel. To sum-up, IoTligent transmissions have a success rate much better than usual IoT devices which should spend a lot of energy due to retransmission, or a lot of quality of service due to the bad reception of their signals by the gateway, whatever the jamming reason: radio collisions with other IoT devices, malicious radio attacks and/or propagation issue.

## 9. Acknowledgment

Author would like to thank Laurent Toutain from IMT Atlantique and Acklio Company, as well as Guillaume Delbarre and Yalla Diop for their technical support on LoRa network and Pycom programming.

## 10. References

[1] C. Moy, “IoTligent: First World-Wide Implementation of Decentralized Spectrum Learning for IoT Wireless Networks”, *URSI AP-RASC*, New Delhi, India, 9-14 March 2019.

[2] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security andprivacy issues in Internet-of-Things”, *IEEE Internet Things Journal*, vol.4, no. 5, pp. 1250–58, Oct. 2017

[3] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," in *IEEE Personal Communications*, vol. 6, no. 4, Aug 1999.

[4] J. Mitola, Cognitive radio: An integrated agent architecture for software defined radio. PhD Thesis, Royal Inst of Technology (KTH) (2000)

[5] Q. Zhao and A. Swami, "A Survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives", *IEEE ICASSP*, 1349-1352, April 2007.

[6] W. Jouini, D. Ernst, C. Moy and J. Palicot, "Upper Confidence Bound Based Decision Making Strategies and Dynamic Spectrum Access", *IEEE ICC,* Cape Town, South Africa, May, 2010

[7] T. L. Lai and H. Robbins, “Asymptotically efficient adaptive allocation rules,” Advances in Applied Mathematics, vol. 6, no. 1, pp. 4–22, 1985.

[8] P. Auer, N. Cesa-Bianchi, and P. Fischer, “Finite-time analysis of the multiarmed bandit problem”, Machine Learning, volume 47, number 2-3, May 2002.

[9] C. Moy, “Reinforcement Learning Real Experiments for Opportunistic Spectrum Access”, *Karlsruhe Workshop on Software Radio*, Karlsruhe, Germany, March 2014.

[10] C. Moy, J. Palicot, and S. J. Darak, “Proof-of-Concept System for Opportunistic Spectrum Access in Multi-user Decentralized Networks”, *EAI Endorsed Trans. on Cognitive Communications*, vol. 2, 2016.

[11] R. Bonnefoi, L. Besson, C. Moy, E. Kaufmann, J. Palicot, "Multi-Armed Bandit Learning in IoT Networks: Learning helps even in non-stationary, settings", *CrownCom'17*, Lisbon, Portugal, Sep. 2017.

[12] L. Besson, R. Bonnefoi, C. Moy, *"MALIN: Multi-Armed bandit Learning for Iot Networks with GRC*: A TestBed Implementation and Demonstration that Learning Helps", ICT'2018, France, June 2018.

[13] N. Sornin, M. Luis, T. Eirich and A. L. Beylot “LoRaWAN specification”, LoRa Alliance, Jan. 2015.