Journal of Systemics, Cybernetics and Informatics (2022) 20(4), 30-33
https://doi.org/10.54808/JSCI.20.04.30

Secure Communications based on Cognitive Multidisciplinary Strategies

Mario LA MANNA
Evoelectronics
Rome, Italy

ABSTRACT[1]

The use of cognitive multidisciplinary strategies represents a powerful tool to allow a communication system to transmit and receive data in a secure way by working in parallel with other electromagnetic devices, sharing the same frequency channels, without being affected by malfunctions caused by unintentional or intentional interferences (e.g. jammers). The cognitive operation is possible by modeling the channel behavior and predicting future channel occupancy. The model of the electromagnetic environment is based on the observation of the spectrum occupancy over time and on suitable reinforced learning strategies to acquire the characteristics of the channel occupancy. The learning operation is paramount, as the prediction about channel occupancy is possible only after understanding the behavior of the concurrent emitters present in the scenario. This paper describes the concept of reinforced learning techniques, based on emitter classification and matching and on human in the loop agent. implemented on a number of real cases of emitter behavior. We show that, in selected study cases, our reinforced learning techniques based on cognitive multidisciplinary strategies can provide good performance, even in presence of a consistent number of concurrent transmitters.

Keywords: cognitive communications, reinforced learning, spectrum sharing, interference, jammer, network intrusion.

1. INTRODUCTION

The objective of this paper is to describe and evaluate a type of reinforced learning mechanism, which is capable to support the frequency sharing functions of a cognitive multidisciplinary communication system. This means that the communication system is capable to operate in frequency dense environments, without significant loss of efficiency and preventing intrusions and/or loss of data due to external attacks. An interesting case is that of a networked communication system working in a hostile environment (Fig, 1), where other emitters can produce unintentional interferences, and/or obscure the network communications (jamming), and/or attempting to enter the network. In order to cope with interferences, jamming and network intrusion, each node of the networked communication system has to be configured as a cognitive device.

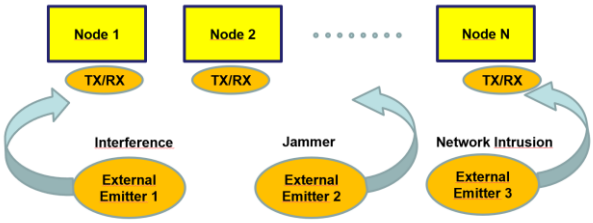

Fig. 1: Networked communication system in a hostile environment.

Such a device is composed of three main units, a Frequency Channel Modeling and Prediction Unit, a Transmit Signal Cognitive Unit and a Receive Signal Cognitive Unit. These units can be considered either as add-on units of a conventional communication device, or as substitutes of conventional units.

A typical structure of a cognitive multidisciplinary communication device is reported in Fig.2.

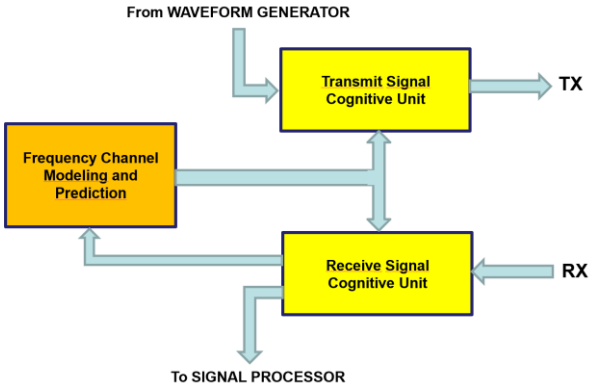

Fig. 2: Structure of a cognitive multidisciplinary communication device.

[1] I would like to thank Prof. Alessandro Trifiletti, University Sapienza, Rome, Italy, for his support in peer-editing this article.

The role of this device is manyfold. First of all, it monitors the environment, in order to discover if there are other emitters who are able to interfere with the communication packets transmitted/ received by the device. Then, after discovering the presence of these emitters, it adopts the suitable countermeasures to avoid the above interferences. The used countermeasures must be matched with the type of threat that has been discovered (e.g. unintentional interference, jammer, network intrusion, etc.). To accomplish this tasks, the communication packets are modified, by transforming the original packets into adaptive packets, to allow the coexistence of the device emissions with the concurrent emitters present in the environment. This feature of the Transmit Signal Cognitive Unit makes the communication device responsive to the dynamic characteristics of the external emitters. In the same way, the Receive Signal Cognitive Unit performs a type of adaptive processing of the received packets, whose goal is to filter the packets which are assumed to have been corrupted by the discovered existing threat. The main advantage of this mechanism is that the communication device can provide flexible TX/RX control, which can insure the network security, without significant degradation of the communications among the network nodes. In fact, the general strategy is based on the concept to avoid/ modify the transmission of the packets in the spectral regions of the interference/ jammer/ network intrusion.

The paper is organized as follows. Section 2 describes the reinforced learning technique that we use to predict the emitter behavior. Section 3 deals with the case study that we examine, which includes the scenario we are using and the types of emitters we have to cope with. Section 4 deals with the performance evaluation of the above case study and the extension to a general case. Section 5 summarizes the conclusions and final remarks.

2.THE REINFORCED LEARNING TECHNIQUE

This section deals with the description of the technique we use for the reinforced learning. In particular, Fig. 3 shows the flow diagram of the proposed algorithm. This algorithm is based on three main blocks, namely Emitter Modeling, Emitter Classification and Emitter Matching.

The scope of Emitter Modeling is to monitor the emitter behavior for a certain time, in order to model its behavior,

The scope of Emitter Classification is to assess the radiating model of the emitter, in order to recognize its specific behavior and classify this behavior, by relying on a number of predefined classes.

The scope of Emitter Matching is to harmonize the device characteristics (e.g. the characteristics of the communication packets) with the emitter features, in order to minimize the effects of interference/jammer/intrusion etc. caused by the external emitters.

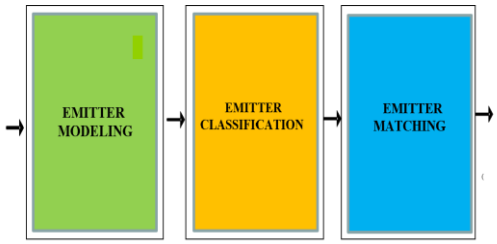

Figure 3.Block Diagram of the Reinforced Learning Algorithm.

Let us consider the case of jammer (Fig. 4), that represents the worst case. In this case, the reinforced learning algorithm goes through the following steps: jammer detection, jammer classification, jammer analysis, countermeasure evaluation and countermeasure selection. The effect of the adopted countermeasure returns back to the communication devices through the signals received by the environment and is evaluated as success or failure. The result of this evaluation is the basis for the learning process, as it will influence the countermeasure evaluation at the next steps. The presence of the Human in the Loop Agent in the evaluation process is a fundamental part of the reinforced learning process. It has been evaluated that including Human in the Loop in the decision process allows the fast convergence of the decision process and strongly facilitates the right choice of the best strategy to contrast the detected threat.

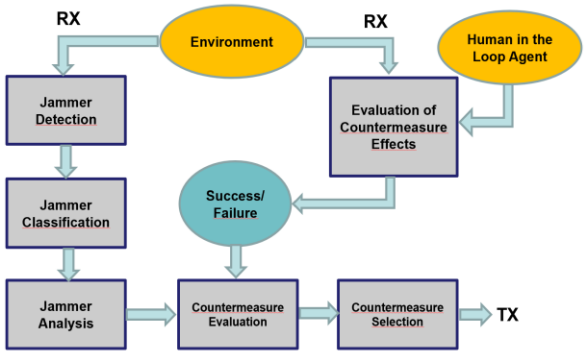

Figure 4. The Reinforced Learning Algorithm in case of jammer.

3. PERFORMANCE EVALUATION

In this section we evaluate the performance of the reinforced learning technique in the case of the worst type of threat, i.e. the presence of jamming emitters, which work in frequency hopping, i.e. emitters that can change their transmit frequency periodically inside their operating time.

We assume that the jammer sources perform frequency hopping into a period of some hundreds of microseconds, in order to disturb the communication service by interfering on the same frequencies. Due to the above threat, it is mandatory that the communication system can detect and neutralize the threat in a short time , i.e. a small fraction (e.g.10%) of the overall operating cycle (e.g. some seconds) of the external emitter.

In our case study, we evaluate the success of neutralization when the jammer has been reduced to less than 10% within 500 msec. (10% of the operating cycle, assumed to be 5 sec).

First of all, we examine the case of a single emitter, following four different radiating strategies: fixed channel, sequential hopping, periodic hopping and random hopping.

Sub-case 1. Fixed channel. The reinforced learning algorithm needs a limited time to perform emitter modeling and emitter classification. After classifying the emitter as a fixed channel emitter, the emitter matching action is simply to avoid to transmit/ receive on that channel.

Sub-case 2. Sequential hopping. The reinforced learning algorithm, after classifying the emitter as a sequential hopping emitter, transmits/ receives on a fixed channel and waits until the emitter reaches the same channel, in order to avoid that channel at that time. All the above operations need a limited transient time.

Sub-case 3. Periodic hopping. It is possible that the emitter performs sequential hopping, but on a limited set of channels. In this case, the machine learning algorithm has both to classify the emitter as a periodic emitter and to detect which channels make part of the periodic hopping. As a consequence, the learning time could be longer than before, but the strategy remains the same.

Sub-case 4. Random hopping. The emitter visits the available channels by following a random strategy. In this case, the machine learning algorithm, after classifying the emitter as a random emitter, starts transmitting/ receiving at random in one of the potentially shared channels. A possible convergence is reached only when the reinforced learning algorithm has found the channels with the lowest probability of access by part of the external emitters, in order to use those channels for transmitting/ receiving, thus minimizing the probability of being jammed. In this specific case, the presence of the Human in the Loop Agent, which represents a multidisciplinary mechanism, is paramount in the reduction of the time to neutralize jammer, due to the better efficiency of the learning process.

When the emitters are more than one, the same actions are carried out sequentially for the different emitters, for all the above four sub-cases.

In the most critical sub-case (sub-case 4, random hopping), a Montecarlo simulation has been used to estimate the time needed to neutralize the jammer. In particular, the performance evaluation has been carried out by simulating the frequency occupancy of the band between 1.05 GHz to 1.15 GHz (100 MHz band, subdivided into 25 channels, of 4 MHz each) over time. The time needed to neutralize the jammer has been estimated statistically, by using Montecarlo on ten thousand different iterations.

The simulation has been carried out by considering a total time of 500 msec. from the starting of the emitter action and the results have been evaluated on the basis of probability of the presence of jammer produced by the external emitters vs. time, i.e. the probability that this jammer has not yet been neutralized.

We have considered three scenarios with a number of emitters from 1 to 3 and 25 potentially shared channels (Figure 5, Figure 6 and Figure 7).

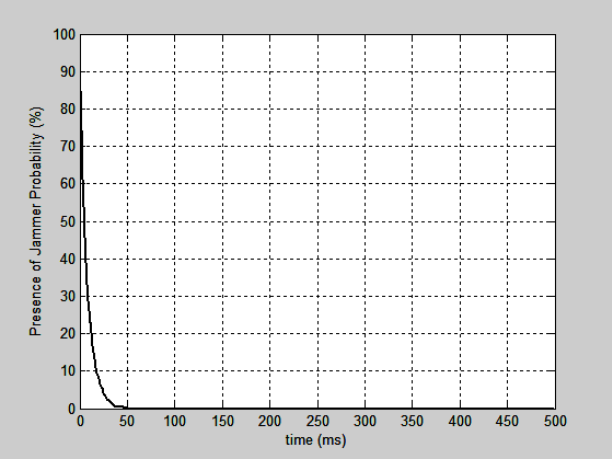

Figure 5. Probability of Presence of Jammer vs time (0-500 msec.) with 1 emitter and 25 potentially shared channels.

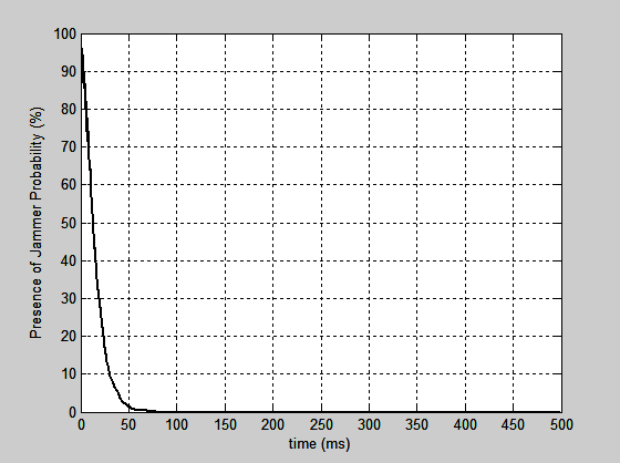

Figure 6 Probability of Presence of Jammer vs time (0-500 msec.) with 2 emitters and 25 potentially shared channels..

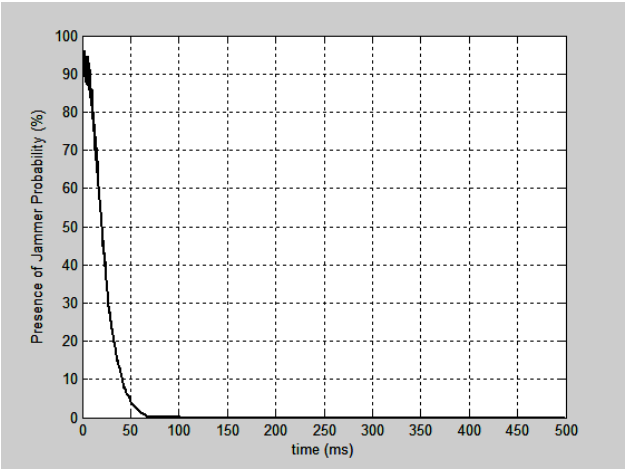

Figure 7. Probability of Presence of Jammer vs time (0-500 msec.) with 3 emitters and 25 potentially shared channels.

Furthermore, we have considered a more complex scenario, relative to a case where the communication band is 200 MHz and this band is shared with 10 external emitters. In this case, we have simulated a number of emitters from 1 to 10 and 50 potentially shared channels. With regard to these scenarios, the results of ten different cases (1-10 emitters) are synthetically reported in Fig.8 (10 cases from 1 to 10 emitters represented by 10 diagrams from left to right).

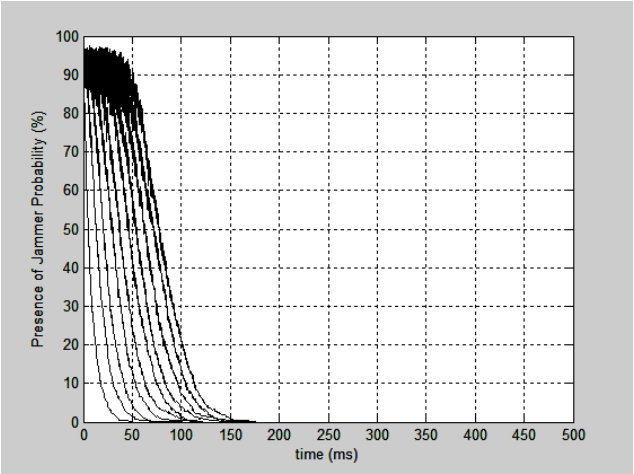

Figure 8. Probability of Presence of Jammer vs time (0-500 msec.) with 1-10 emitters and 50 potentially shared channels.

4. CONCLUSIONS

In this paper, we present a reinforced learning technique, based on cognitive multidisciplinary strategies, implemented on real cases of emitter behavior, namely fixed, sequential, periodical and random hopping. We have shown that, for the worst threat (jammer) and worst case (random hopping), the reinforced learning technique can provide very good jammer neutralization, even in presence of a consistent number of concurrent transmitters.

4. REFERENCES

[1] M. LaManna ”Urban Environment Monitoring: System and Technology Issues”, IMCIC 2012, 25-28 March 2012, Orlando, FL.

[2] M. LaManna “Data Fusion of Heterogeneous Sensors in Urban Environment Monitoring” IMCIC 2013, 9-12 July 2013, Orlando, FL.

[3] M. LaManna “Cost-Benefit Analysis of Automated Systems for the Control of Urban Critical Infrastructures” WMSCI 2015, 12-15 July 2015, Orlando, FL.

[4] M. LaManna “Man-Machine Synergy in Systems for Critical Infrastructure Protection” WMSCI 2019, 6-9 July 2019, Orlando, FL.

[5] M. LaManna “A Man-Machine Synergy Integrated Approach for Homeland Protection” WMSCI 2020, 13-16 September 2020, Orlando, FL.

[6] Papoulis, A., Probability, Random Variables, and Stochastic Processes, 2nd edition, McGraw-Hill, New York, 1984.

[7] B. Kamiński, M. Jakubczyk, P. Szufel "A framework for sensitivity analysis of decision trees". Central European Journal of Operations Research, 2017.

[8] R.J. Urbanowicz, J.H.Moore "Learning Classifier Systems: A Complete Introduction, Review, and Roadmap". Journal of Artificial Evolution and Applications. 2009.

[9] N.Friedman, D. Geiger, M. Goldszmidt "Bayesian Network Classifiers". Machine Learning, Nov. 1997.

[10] H.Zhang “The Optimality of Naive Bayes”, Florida Artificial Intelligence Research Society Conference, 2004.

[11] W. Daelemans, A. Van den Bosch, “Memory-Based Language Processing”. Cambridge University Press, 2005.