Smart Jammer Detection for Self-Aware Cognitive UAV Radios

Ali Krayani[1,2], Mohamad Baydoun[1], Lucio Marcenaro[1], Yue Gao[2] and Carlo S.Regazzoni[1]
DITEN, University of Genova, Italy[1]
CIS, Queen Mary University of London, UK[2]
email addresses: {ali.krayani, mohamad.baydoun}@edu.unige.it
{lucio.marcenaro, carlo.regazzoni}@unige.it, yue.gao@qmul.ac.uk

***Abstract*—Cellular connectivity for a massive number of Unmanned Aerial Vehicles (UAVs) will overcrowd the radio spectrum and cause spectrum scarcity. Incorporating Cognitive Radio (CR) with UAVs (Cognitive-UAV-Radios) has been proposed to overcome such an issue. However, the broadcasting nature of CR and the dominant line-of-sight links of UAV makes the Cognitive-UAV-Radios susceptible to jamming attacks. In this paper, we propose a framework to detect smart jammer, which locates and attacks the UAV commands with low Jamming-to-Signal-Power-Ratio (JSR). Smart jammer is more challenging than the types of jammers that always require high power values. Our work focuses on learning a Dynamic Bayesian Network (DBN) to model and analyze the signals' behaviour statistically. A Markov Jump Particle Filter (MJPF) is employed to perform predictions and consequently detect jamming signals. The results are satisfactory in terms of detection probability and false alarm rate that outperform the conventional Energy Detector approach.**

***Index Terms*—UAV, CR, DBN, LTE, JAMMER**

I. Introduction

Telecommunication researchers are focusing on Unmanned Aerial Vehicles (UAVs) due to their attractive features such as dynamic deployment ability, high mobility and availability of Line-of-Sight (LoS) links facilitating wireless broadcast and supporting high data rate transmissions [1]. UAVs are already being studied for 4G LTE (Long Term Evolution) [2] and they are expected to play an important role in the upcoming 5G technology as mentioned in [3]. UAVs can be used as Flying Base Stations for improving reliability, coverage and capacity of wireless networks or as Aerial Users by connecting them to a cellular system [4]. According to the Federal Aviation Administration (FAA) report, the fleet of connected UAVs will be more than doubled from an estimated 1.1 million in 2017 to 2.4 million units by 2022 [5]. This huge number of connected UAVs will overcrowd the spectrum bands and lead to spectrum scarcity. Incorporation of Cognitive Radio (CR) and UAVs, which we refer to as the Cognitive-UAV-Radios has been proposed to mitigate the spectrum scarcity problem [6], [7].

CR can sense, learn and adapt to the environmental modifications by optimizing its operating parameters based on observations and previous experiences. However, due to the radio propagation and broadcasting nature, CRs are vulnerable to jamming attacks [8]. Moreover, the situation could be worse in CRs, where a smart jammer with cognitive abilities can estimate system parameters and manipulate radio spectrum, thus forcing CR to learn wrong behaviours and take non-optimal actions, consequently. In addition, due to the dominant LoS communication links, UAVs are more vulnerable to terrestrial jammers [9].

Several researchers investigated the problem of jamming attacks on CRs and UAV communications [8], [10]–[12]. Accurate and timely detection of anomalies (e.g. jammer attacks) is the first essential step to protect the Cognitive-UAV-Radios effectively. Anomaly detection has been addressed in several works through a machine learning data-driven approach [13]–[16]. Authors in [13] proposed an unsupervised anomaly detection method for the CR using long-short-term memory mixture density networks applied to time series data by considering only the In-Phase (I) components of digital radio transmissions. However, discarding the Quadrature (Q) components will impose some limitations on analysing how the signal dynamics are changing with time at both I and Q channels and causes confusion in identifying some samples (e.g. two samples might have the same I with different Q values). The work proposed in [14] uses an adversarial auto-encoder relying on features (as power spectral density, signal bandwidth and center frequency) which require an additional effort to be extracted and could be inconvenient in the UAV scenario. The methods proposed in [15], [16] are based on video frame predictor and Convolutional Neural Networks (CNN), respectively; this requires the generation of video frames and waveforms images that can be unfeasible at the UAV level, because of the battery and power consumption limitations.

CR can detect, classify and predict efficiently after it has achieved a certain degree of Self-Awareness (SA) (includes spectrum awareness) [17]. A basic SA module should include the following abilities: *i)* autonomous learning $Generative\ Models$ by simultaneously observing CR states and related environmental changes; *ii)* deciding whether communications between the device itself and other devices are occurring according to a pre-learned normal behaviour ($Abnormality\ Detection$); *iii)* applying $Abnormality\ Mitigation$ strategies or $Incrementally\ learning$ new models that describe different dynamic situations not included in pre-learned experiences; *iv)* learning $Interactive\ Models$ of the causality

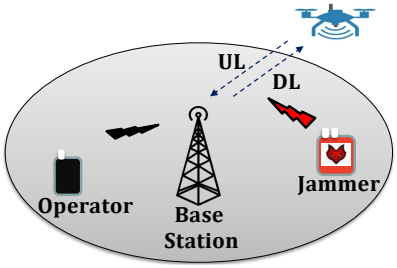


Fig. 1. Illustration of the system model

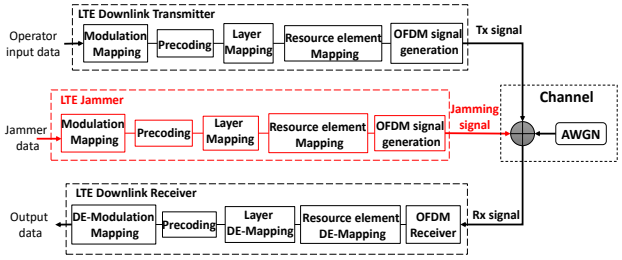


Fig. 2. Illustration of the Propagation Model

and interactions between different users (e.g. cognitive device and jammer) or between multiple signals received by the cognitive user (e.g. LTE and GPS signals). Introducing SA to CR systems enhances the physical layer security through radio spectrum anomalies detection and decision-action process improvement.

This paper will focus on the first two functionalities of the SA module. Like in [18], a jammer detection framework is proposed based on learning Generative Models as Dynamic Bayesian Network (DBN). Our proposed approach differs from [18], since *1)* it investigates a new scenario based on the integration of CR and UAV communications; *2)* it copes with more complex attacks by considering smart jammers dynamically injecting disturbance signals and attacking with low power (JSR $\leq$ 0 dB); *3)* it uses the Growing-Neural-Gas (GNG) unsupervised technique to cluster the data; *4)* it formulates an effective Generalized State Vector which improves the learning process.

The remainder of the paper is organized as follows: section II describes the system model, while the proposed jammer detection approach is illustrated in section III. Experimental results are reported in section IV and conclusions are drawn in section V.

II. System Model

The system model (see Fig. 1) consists of a Base Station (BS) and a UAV with a 4G antenna and GPS receiver. A human operator controls the UAV through LTE cellular system. Commands are sent to the UAV through BS using the Downlink (DL) channel. We consider the DL channel under the threat of a terrestrial jammer which aims to send false commands to alter the trajectory and take control of the UAV. The propagation model consisting of the LTE downlink transmitter, receiver and jammer is shown in Fig. 2. In standard LTE the downlink transmission is based on the Orthogonal Frequency Division Multiplexing (OFDM) scheme.

The BS continuously sends a Radio Frame (RF) of 10 ms duration to the active users (already synchronized with BS) in the cell. Each RF is composed of 10 subframes of 1 ms duration each, denoted by indices ranging from 0 to 9. In this work, we focus on FDD-RF structure type 1 where the Primary Synchronization Signal (PSS) and the Secondary Synchronization Signal (SSS) along with the Broadcast Channel (BCH) are located within the 0^{th} subframe. The PSS and SSS are repeated in the 5^{th} sub-frame. While the User Data plus the Channel State Information (CSI) are located in all of the 10 sub-frames. Each sub-frame is divided into two 0.5 ms slots where the first slot contains the Downlink Control Information (DCI). The BS allocates a specific number of sub-carriers to the user for a predetermined time which are referred to as Physical Resource Blocks (PRBs).

A PRB is defined as consisting of 12 consecutive sub-carriers of 180 kHz in the frequency domain for 1 slot (0.5 ms) duration. Slots composed of either 6 or 7 OFDM symbols, depending on whether the normal or extended cyclic prefix is employed. A PRB is the smallest element of resource allocation assigned by the BS scheduler forming a total of $12 \times (6\ or\ 7)$ Resource Elements (REs). We supposed that the GPS measures the 3D position every 50 ms and the UAV receives one PRB every 50 ms as well (assuming that the BS follows the third allocation scheme for UAV command & control (C2) data as mentioned in [19]) since the 3GPP specifies that efficient management of a UAV would require a maximum of 100 kb/s for C2 data, latency of 50 ms and inter-arrival time (defined also as Transmission Time Interval TTI) of 100 ms [20]. The commands (Pitch, Yaw, and Roll) are sent in the PRB over 9 consecutive sub-carriers in the frequency domain within 1 OFDM symbol in the time domain. We call these REs as a Resource Vector (RV) as shown in Figs. 3-4. The remaining sub-carriers and OFDM symbols of the PRB are related to other information sent to the UAV. For our analysis, only the RV is considered in which we are interested in studying the command signals only. However, this can be simply extended to consider the whole PRB in future investigation. We assume that the jammer is smart and is aware of the transmission protocol and the resource allocation strategy performed by the BS. Hence, the jammer can locate and identify the PRBs allocated to the UAV inside the radio spectrum and attacks it consequently. In our study, the data is extracted after the OFDM receiver where the output of this block consists all the Resource Elements (REs) which represent the time-frequency grid. At this level the UAV can scan and sense the whole REs of the grid.

III. Proposed Jammer Detection Framework

Based on the system model described in section II, the UAV can sense the received PRBs allocated by the BS and extract the RV consequently. The method aims to provide the

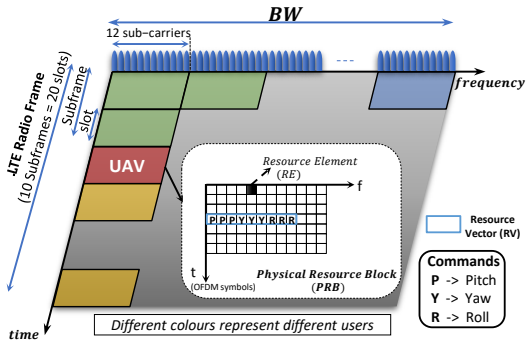


Fig. 3. LTE Physical resource allocation and Radio Frame structure

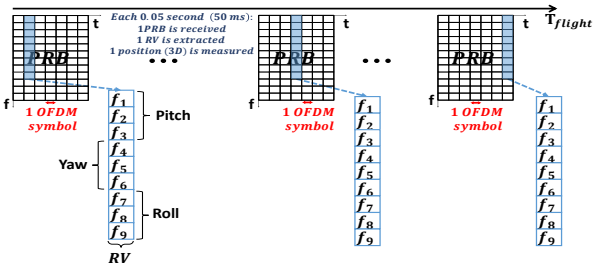


Fig. 4. Timing of the PRBs and RVs received by the UAV

UAV with the capability to learn the dynamic behaviour of the signal by observing such resources. These observations can be expressed in a probabilistic way and represented as a DBN. Additionally, the proposed approach allows performing predictions of the future RVs that lead to a better understanding of the radio spectrum and detecting malicious behaviours.

A. Forming the Generalized State Vector (GSV)

To analyse the dynamics of the received signal (received commands) statistically, we generate a set of Generalized State Vectors (GSVs) $\mathbf{X}$ consisting of all the components of the RV at each time instant t and the corresponding derivatives as shown in Fig. 5. The state vector is 36-dimensional, and it is defined as follows:

$$\tilde{X}_t = [I_{f_1}, \ldots, I_{f_9}, Q_{f_1}, \ldots, Q_{f_9}, \dot{I}_{f_1}, \ldots, \dot{I}_{f_9}, \dot{Q}_{f_1}, \ldots, \dot{Q}_{f_9}], \quad (1)$$

where $\tilde{X}_t \in \mathbf{X}$ and I, Q are in-phase and quadrature components of the signal at different frequencies while $\dot{I}$, $\dot{Q}$ are the corresponding derivatives. The derivatives are considered in order to understand the rule in which the commands are changing as the time evolves. Incorporating I-Q elements which belong to different sub-carriers in the same GSV will certainly improve the learning process. Since in OFDM the data stream is transmitted in parallel over multiple sub-carriers, exploiting such correlation between data can help in learning the dynamic evolution of the signal over time in a better way.

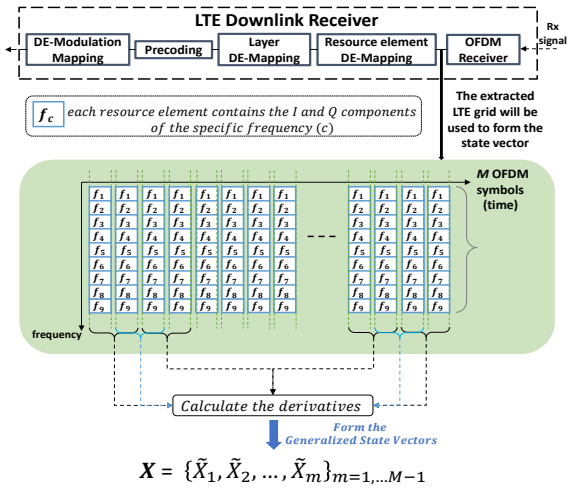


Fig. 5. Data extraction and generation of the Generalized State Vectors

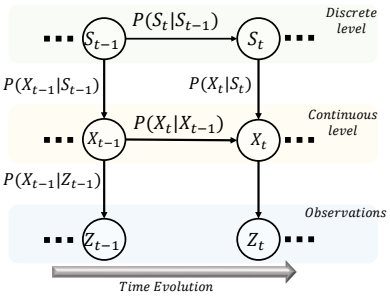


Fig. 6. Proposed Dynamic Bayesian Network (DBN).

B. Learning the DBN model (Training Process)

The DBN provides a graphical representation and inference mechanisms at different levels in which two consecutive temporal slices (time instants) are used to model a set of dynamic rules. In this work, we proposed a switching DBN consists of three levels as shown in Fig. 6. The lowest level stands for the observations model $\mathbf{Z}$, while the continuous $\tilde{\mathbf{X}}$ and discrete $\mathbf{S}$ states correspond to the medium and top levels of inference, respectively. Discrete and continuous variables are connected by links (arcs) that characterize the conditional probabilities and explain the causality among them. The conditional dependencies involved in the network are the following: ***1)*** the probability to obtain the observation given the signal's state $P(Z_t|\tilde{X}_t)$. Such inference can be calculated by referring to the observation model

$$Z_t = H\tilde{X}_t + n_t. \quad (2)$$

$H = [H_1\ H_2]$ is the observation matrix where $H_1 = [I_{18}\ 0_{18}]$, $H_2 = [0_{18}\ 0_{18}]$ and n_t is the measurement noise which is assumed to be zero mean gaussian noise with covariance R_t such that $n_t \sim \mathcal{N}(0, R_t)$. ***2)*** The probability of obtaining a future signal's state given the previous state $P(\tilde{X}_t|\tilde{X}_{t-1})$, here inference can be made by using the dynamic model which is

defined in the following form:

$$\tilde{X}_t = A\tilde{X}_{t-1} + BU_{S_{t-1}} + w_t, \quad (3)$$

where $A = [A_1 \ A_2]^\intercal$ is the transition matrix while $A_1 = [I_{18} \ 0_{18}]$ and $A_2 = [0_{18} \ 0_{18}]$. In addition, $B = [I_{18} \ 0_{18}]^\intercal$ is the control model and U_{S_t} is the control vector which consists of the rules of which the signal will follow, once is being inside a discrete region S_t and it is defined as $U_{S_t} = [\dot{I}_{f_1}, \ldots, \dot{I}_{f_9}, \dot{Q}_{f_1}, \ldots, \dot{Q}_{f_9}]$. w_t is the process noise which is assumed to be drawn from a zero multivariate normal distribution with covariance σ_t such that $w_t \sim \mathcal{N}(0, \sigma_t)$. ***3)*** the probability $P(\tilde{X}_t|S_t)$ of being in the signal's state $\tilde{X}_t$ given the super-state S_t related to the discrete regions of the signal. ***4)*** the probability $P(S_t|S_{t-1})$ of transiting from super-state (S_{t-1}) to (S_t) by referring to the transition matrix (Π).

The DBN representation of the signal's behaviour can be learned by following the successive steps:

Learning super-states. The GSVs (**X**) corresponding to a clean signal (without jamming attacks) will be fed as input to an unsupervised learning technique. In this work, we used the Growing Neural Gas (GNG) to cluster the signal without any prior knowledge about its nature. GNG is an incremental neural network that learns the relation between a given set of input patterns and adapts the topological structure based on nearest neighbour relationships and local error measurements. GNG shows higher flexibility in representing the input data if compared to fixed size networks like the Self Organizing Maps (SOMs). GNG encodes the GSVs into discrete components producing a set of super-states (or neurons) **S** that represent the quasi-similar OFDM symbols, where $\mathbf{S} = \{ S_1, S_2, \ldots, S_L\}$ and L is the total number of super-states. L is selected based on the investigation done in [21].

Learning super-states Properties. After obtaining the super-states, properties as mean value ξ_S, covariance matrices Σ_S and boundary region uncertainty ψ_S of each super-state are calculated.

Learning Transition Matrix (Π). by observing the active super-states inside the spectrum over a certain number of OFDM symbols in the time domain, it is possible to obtain a (Π) that represent the probabilities of changing current super-state $P(S_t|S_{t-1}, t)$ taking in consideration the time spent in each super-state before moving to the new one.

C. MJPF Filtering (Testing Process)

The Markov Jump Particle Filter (MJPF) firstly proposed in [22] is here employed to perform predictions at different inference levels of the DBN by using a combination of Particle Filters (PFs) and Kalman Filters (KFs). The probability of transitions between super-states $P(S_t|S_{t-1})$ is used to make inferences of future predictions at the discrete level by means of PF. The PF generates a set of particles corresponding to the predicted super-state S_t^*. For each particle we employed a KF to predict the future state as pointed out in Eq. 3 (i.e. $P(\tilde{X}_t^*|\tilde{X}_{t-1}^*(S_t^*))$), where $(.)^*$ indicates the considered particle. The prediction at the continuous level and the performance of the KF depend on the predicted super-state (S^*)

Algorithm 1: MJPF

Input: $\Pi, \mathbf{S}, \xi_S, \psi_S, \Sigma_S \leftarrow$ Learned variables
$Z_t \leftarrow$ Testing measurements t = 1,...,T
$N \leftarrow$ Total number of particles

for *t = 1 to T* $\leftarrow$ *Time evolution* **do**
  for *n = 1 to N* $\leftarrow$ *Particles* **do**
    $w_n = \frac{1}{N} \leftarrow$ weight of the particle
    `Prediction at Discrete Level`
    if *t == 1* $\leftarrow$ *Initial State* **then**
      Sample $\tilde{X}_1$ from initial prior density $P(\tilde{X}_1)$
      $\tilde{X}_t = \tilde{X}_1 \leftarrow$ current state
      Estimate $\tilde{S}_t^*$ from $P(\tilde{X}_t|S_t)$
    else $\leftarrow$ Remaining States
      Predict $\tilde{S}_n^*$ by referring to Π
      $\tilde{X}_t$=$\tilde{X}_{t-1} \leftarrow$ current state
    Calculate $d(\tilde{X}_t, \xi_{S_{t-1}}) \leftarrow$ euclidean distance
    if $1 - (\frac{d(\tilde{X}_t, \xi_{S_{t-1}})}{\psi_S}) < 0 \leftarrow$ *outside the model* **then**
      $U_{S_{t-1}} = 0$ & $P_{t-1|t-1} = R_t \leftarrow$ process noise
    else
      $U_{S_{t-1}} = U_{S_{t-1}^*}$ & $P_{t-1|t-1} = \Sigma_{S_{t-1}^*}$
    `Prediction at Continuous Level`
    $\tilde{X}_t = A\tilde{X}_{t-1} + BU_{S_{t-1}} \leftarrow$ state
    $P_{t|t-1} = AP_{t-1|t-1}A^\intercal + \sigma_{t-1} \leftarrow$ covariance
    $\hat{Z}_t = (Z_t - H_t\tilde{X}_t)$
    $K_t = P_{t|t-1}H_t^\intercal(HP_{t|t-1}H + R_t)^{-1}$
    $update$:
    $\hat{X}_t = \tilde{X}_t + K\hat{Z}_t \leftarrow$ updated state
    $\hat{P}_{t|t} = (1 - K_tH_tP_{t|t-1}) \leftarrow$ updated covariance
    Calculate abnormality signals db1 & db2
    $w_n = \frac{w_n}{db1+db2}$
  SIR resampling

Output: db1 & db2

performed by PF (based on Π). Therefore, a wrong prediction at the super-state level will lead to wrong predictions at the continuous level and consequently overall degradation of the MJPF performance. The posterior probability $P(\tilde{X}_t|Z_t, S_t^*)$ is estimated according to current observation Z_t and the update is performed by using:

$$P(\tilde{X}_t|Z_t, S_t^*) = \frac{P(\tilde{X}_t|Z_{t-1}, S_t^*)P(Z_t|\tilde{X}_t^*, S_t^*)}{P(Z_t|Z_{t-1})}. \quad (4)$$

The MJPF is augmented with respect to basic definition by an additional step for computing the abnormality signals based on the Bhattacharyya distance between prediction $p(\tilde{X}_t^*|\tilde{X}_{t-1}^*(S_{t-1}^*))$ and

- probability of being inside the predicted super-state of particle $p(\tilde{X}_t^*|S_t^*)$:

$$db1 = -\ln \int \sqrt{p(\tilde{X}_t^*|\tilde{X}_{t-1}^*(S_{t-1}^*))p(\tilde{X}_t^*|S_t^*)}d\tilde{X}_t^*; \quad (5)$$

- evidence $p(Z_t|\tilde{X}_t^*)$ to have solutions near the measurement:

$$db2 = -\ln \int \sqrt{p(\tilde{X}_t^*|\tilde{X}_{t-1}^*(S_{t-1}^*))p(Z_t|\tilde{X}_t^*)}d\tilde{X}_t^*; \quad (6)$$

$db1$ indicator corresponds to the discrete level of the DBN, and its value is related to the similarity between the prediction of the state and the likelihood to be in the predicted super-state. If the predicted state is out of the learned model (outside the super-state) or is far away from the super-state's center, $db1$ will provide a high abnormality signal; otherwise, it will provide low abnormality signal. On the other hand, $db2$ indicator corresponds to the continuous level of the DBN and its value is related to the similarity between the state prediction and the continuous state evidence corresponding to the new observation in each super-state. The weight W_t^* of the particle S_t^* is calculated (taking into account the abnormality measurements $db1$ and $db2$, the weight of a specific particle will increase as the abnormality level decrease and viceversa; to favorite particles with low abnormality that represent well prediction) and then normalized by considering the Sequential Importance Resampling (SIR) technique. The logic of the MJPF is reported in Algorithm 1, showing the different steps of the filter to perform predictions and consequently detect abnormalities.

IV. Experimental Results

We use simulated data to evaluate the proposed Framework. First, the trajectory of a quadcopter UAV is simulated based on [23]. A relation is studied between the commands and velocities of the UAV at different angles (Pitch, Yaw and Roll) to generate the appropriate bits for simulating the LTE signal and vice versa, from the jammed LTE signal the altered trajectory is extracted. The LTE signal is generated with respect to the 3GPP standard requirements and the parameters defined in table I. The flight time of the UAV is T_{flight}*=30 sec* consisting of 600 samples due to the fact that the position is measured by the GPS every 50 ms. In addition, the UAV receives a PRB every 50 ms and extracts the RV that contains a set of commands sent over 9 consecutive frequencies in 1 OFDM symbol. Thus during the T_{flight} the UAV will receive 600 sets of commands, corresponding to 600 OFDM symbols in time domain (Fig. 3). And each received set of commands will indicate how the UAV will move in the 3D space. The

TABLE I
LTE Simulation Parameters

Parameter	Value
BW	1.4 MHz
Duplex mode	FDD
Δf	15 kHz
Number of PRBs per BW	6
Sampling frequency	1.92 Mhz
N_{FFT}	128
OFDM symbols per slot	7
CP length	normal
SNR	15 dB
Modulation	QPSK
Channel	AWGN
Total Radio Frames	600

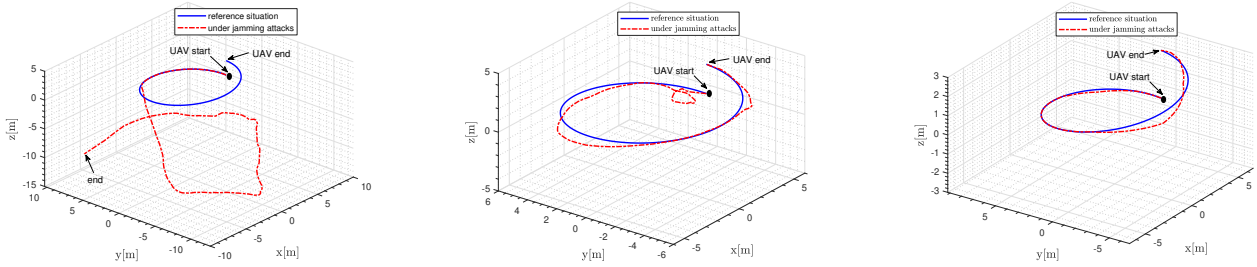
output of the QPSK modulator for both the normal signal and the jammer is normalized based on the average power. The normal signal has average power $P_S = 1$. While, the average power of the jammer is $P_J = 1/n$. The Jamming-to-Signal-Power-Ratio (JSR) is calculated as: $JSR = \frac{P_J}{P_S}$.

Four different situations are considered, one related to the normal signal, and the rest are concerning the smart jammer behaviour and the JSR values.

- **Reference Situation**: represents the normal behaviour of the signal related to the original commands sent by the operator as shown in Fig. 8(a) (because of space limitation, we visualize only 3 frequencies) which is used to learn the DBN model. The UAV trajectory during the normal situation is depicted in Fig. 7 (in blue color).
- **Situation 1**: the JSR is equal to 0 dB where the power of the jammer is $P_J = 1$ considering $n = 1$ and the signal's power is $P_S = 1$. The jamming signal is consecutive starting from time *t = 15 sec* till *t = 30 sec* as shown in Fig. 8(b). Where the altered UAV trajectory during the jamming attacks is shown in Fig. 7(a) (dashed red trajectory).
- **Situation 2**: the JSR is equal to -3 dB where the power of the jammer is $P_J = \frac{1}{2}$ considering $n = 2$ and the power of the normal signal is $P_S = 1$. Here the jammer behaves in a dynamic way by attacking from *t = 0.05 sec* till *t = 5 sec*, from *t = 10 sec* till *t = 15 sec* and from *t = 20 sec* till *t = 25 sec* as shown in Fig. 8(c). Therefore affecting the commands to change the UAV's trajectory as shown in Fig. 7(b).
- **Situation 3**: the JSR is equal to -4.7 dB where $P_J = \frac{1}{3}$ considering $n = 3$ and $P_S = 1$. The jammer behaves in a dynamic way by attacking from *t = 5 sec* till *t = 10 sec* and from *t=15 sec* till *t=30 sec* as shown in Fig. 8(d) and alters the UAV's trajectory as depicted in Fig. 7(c).

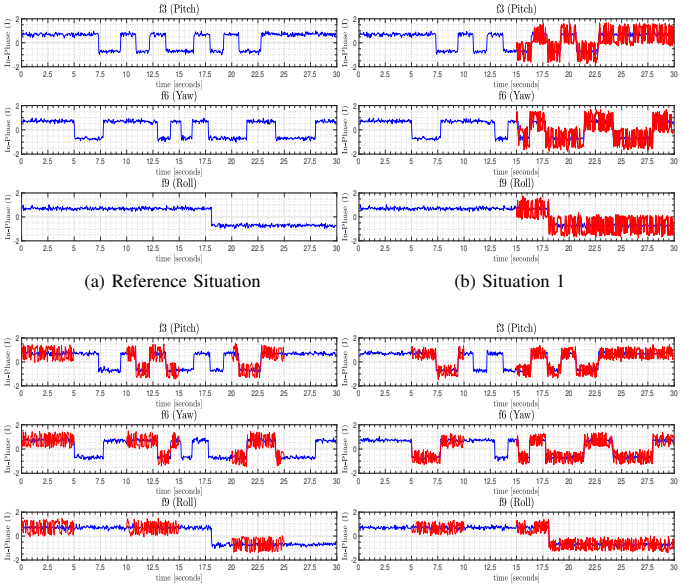
The proposed approach aims to predict future OFDM symbols at different frequencies (defined as RV) simultaneously. Such predictions are performed by applying the MJPF filter on the previously acquired knowledge (the learned DBN) by the Cognitive-UAV-Radio. Testing new observations Z_t and predicting eventually, could follow the same rules with which the dynamic model has been learned from previous experience when the jammer was absent or could deviate due to the new rules caused by the jammer. The MJPF provides two abnormality measurements (see Eqs. 5 - 6) to identify whether the new signals are following the learned rules or not.

Figs. 8(b-c-d), represent the testing data including jammer attacks on the LTE signal related to the situations mentioned previously. Consequently, Fig. 9 shows the abnormality signals at the two inference levels. At the discrete level, if the probability that the predicted RV is inside the predicted super-state is high, the filter will provide a low abnormality signal otherwise the filter will provide high abnormality signal. At the continuous level, if the probability of having the prediction near the measurement (or the likelihood which is the probability of how much the prediction is confirmed by the observation) is high the abnormality signal is low and viceversa. As shown in Fig. 9, the filter provides high abnormality signals in the time instants where the jammer is attacking



(a) Situation 1 (b) Situation 2 (c) Situation 3

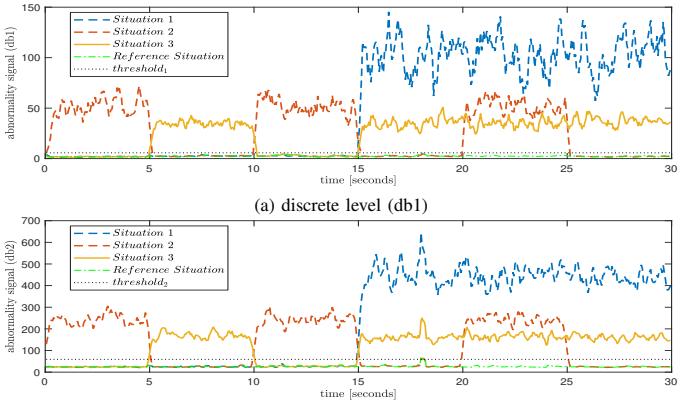
Fig. 7. UAV trajectory in different situations



(a) Reference Situation (b) Situation 1

(c) Situation 2 (d) Situation 3

Fig. 8. Normal (blue) and Jammed (red) command signals



(a) discrete level (db1)

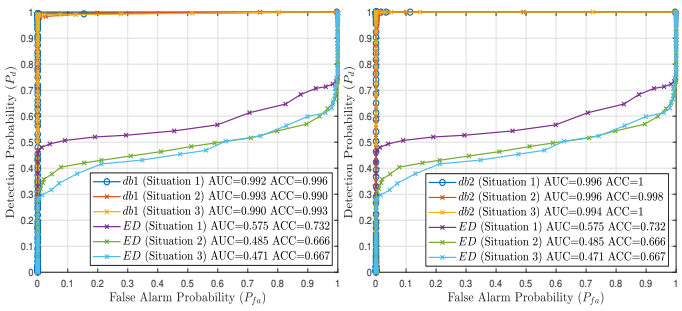
(b) continuous level (db2)

Fig. 9. Abnormality Signals: *db1* and *db2*

and low abnormality signals (near zero) when the jammer is off. Moreover, the abnormality signal's level may vary from one situation to the other. For instance, $db1$ (values above threshold) in situation 1 is greater than the other situations since the jammer is attacking with higher power with respect to situation 2 and 3, which means that it will shift more the signal towards the boundary of the predicted super-state.

It is worth to note that there is a difference between the filter's performance (state estimation using predictions and updates) and the abnormality signals provided by it. If the filter doesn't predict well it may provide high abnormality signals too, even if the jammer is absent. To this purpose, the clean signal without jamming attacks is tested by the MJPF to evaluate the filter's performance and it is obvious from Fig. 9 that the abnormality signal during this situation (reference situation) is very low which verifies the filter's ability in predicting the OFDM symbols at 9 frequencies correctly. Optimized thresholds can be obtained by implementing the MJPF using the normal signal (without jamming attacks). At the discrete level, the threshold can be obtained by calculating that the mean value of the $db1$ signal plus the standard deviation, while at the continuous level the mean value of $db2$ plus its standard deviation will represent the second threshold.

In order to evaluate the performance of the proposed framework, we used a range of confidence thresholds to build the corresponding ROC curves along with the Area Under Curve (AUC) and Accuracy (ACC). The ROC curves in Fig. 10 (a)-(b) shows that the MJPF filter can provide high detection probability (P_d) with low P_{fa} at both levels considering different JSR values (0 dB, -3 dB and -4.7dB) and compared with the conventional Energy Detector (ED). The high detection probabilities can be explained by the fact



(a) discrete level (db1) (b) continuous level (db2)

Fig. 10. ROC curves (DBN vs. ED)

that the predictions performed at the higher level by PF were precise and accurate almost of the time (30 sec related to 600 OFDM symbols) considered in the analysis.

Further experiments are tested by decreasing the JSR till $-16dB$ and considering $P_J = 1/n$ where $n = [1, \ldots, 40]$. In all these experiments the jammer attacks dynamically from *t = 5 sec* till *t = 10 sec*, from *t=15 sec* till *t=20 sec*, and from *t=25 sec* till *t=30 sec*. Fig. 11 showed that the proposed method can still detect with high detection probability even when the jammer attacks with very low power.

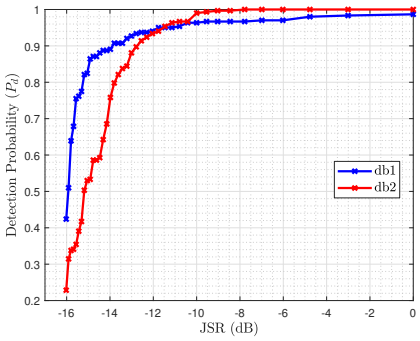


Fig. 11. Probability of detection vs. JSR

V. Conclusion and Future Work

We proposed a probabilistic framework based on learning switching dynamic models to detect a smart jammer that can locate the PRBs allocated to the UAV inside the radio spectrum and consequently attack the control commands with low JSR, which is more difficult to detect compared with the traditional types of jammers who attack with high JSR. We tested the work on simulated LTE signals, and the performance was evaluated by using the ROC curves. Additionally, in this paper we showed how efficient is the proposed method considering only Additive White Gaussian Noise (AWGN) Channel by assuming that the communication link between the base station and the UAV is always Line-of-Sight (LOS). However, multi-path fading and Non-line-of-Sight (NLOS) conditions will be investigated and tested in future work.

Multiple jammer characterization and classification as well as learning the interaction between the LTE signal and GPS signal will be studied in future work to achieve new functionalities of the Self-Awareness module, which will further enhance the Cognitive-UAV-Radios physical layer security.

References

[1] B. Li, Z. Fei, and Y. Zhang. UAV Communications for 5G and Beyond: Recent Advances and Future Trends. *IEEE Internet of Things Journal*, 6(2):2241–2263, April 2019.

[2] W. Xia, M. Polese, M. Mezzavilla, G. Loianno, S. Rangan, and M. Zorzi. Millimeter Wave Remote UAV Control and Communications for Public Safety Scenarios. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–7, June 2019.

[3] 3GPP. *https://www.3gpp.org/release-17*, 2019.

[4] M. Mozaffari, W. Saad, M. Bennis, Y. Nam, and M. Debbah. A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems. *IEEE Communications Surveys Tutorials*, 21(3):2334–2360, thirdquarter 2019.

[5] A. Fotouhi, H. Qiang, M. Ding, M. Hassan, L. G. Giordano, A. Garcia-Rodriguez, and J. Yuan. Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. *IEEE Communications Surveys Tutorials*, pages 1–1, 2019.

[6] G. M. D. Santana, R. S. Cristo, C. Dezan, J. Diguet, D. P. M. Osorio, and K. R. L. J. C. Branco. Cognitive Radio for UAV communications: Opportunities and future challenges. In *2018 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 760–768, June 2018.

[7] N. u. Hasan, W. Ejaz, U. Farooq, I. Baig, and M. Zghaibeh. Adaptive Error Control Framework for a Multihop Cognitive Radio based UAVs for Disaster Management. In *2019 IEEE 5th International Conference on Mechatronics System and Robots (ICMSR)*, pages 87–91, May 2019.

[8] M. K. Hanawal, D. N. Nguyen, and M. Krunz. Cognitive Networks with In-band Full-duplex Radios: Jamming Attacks and Countermeasures. *IEEE Transactions on Cognitive Communications and Networking*, pages 1–1, 2019.

[9] G. Zhang, Q. Wu, M. Cui, and R. Zhang. Securing UAV Communications via Joint Trajectory and Power Control. *IEEE Transactions on Wireless Communications*, 18(2):1376–1389, Feb 2019.

[10] H. Noori and S. S. Vilni. Defense Against Intelligent Jammer in Cognitive Wireless Networks. In *2019 27th Iranian Conference on Electrical Engineering (ICEE)*, pages 1309–1314, April 2019.

[11] H. Wang, J. Chen, G. Ding, and J. Sun. Trajectory Planning in UAV Communication with Jamming. In *2018 10th International Conference on Wireless Communications and Signal Processing (WCSP)*, pages 1–6, Oct 2018.

[12] K. Pärlin, T. Riihonen, and M. Turunen. Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems. In *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, pages 1–6, May 2019.

[13] M. Walton, M. Ayache, L. Straatemeier, D. Gebhardt, and B. Migliori. Unsupervised Anomaly Detection for Digital Radio Frequency Transmissions. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 826–832, Dec 2017.

[14] S. Rajendran, W. Meert, V. Lenders, and S. Pollin. Unsupervised Wireless Spectrum Anomaly Detection With Interpretable Features. *IEEE Transactions on Cognitive Communications and Networking*, 5(3):637–647, Sep. 2019.

[15] N. Tandiya, A. Jauhar, V. Marojevic, and J. H. Reed. Deep predictive coding neural network for rf anomaly detection in wireless networks. In *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, May 2018.

[16] M. A. Conn and D. Josyula. Radio Frequency Classification and Anomaly Detection using Convolutional Neural Networks. In *2019 IEEE Radar Conference (RadarConf)*, pages 1–6, April 2019.

[17] A. Toma, A. Krayani, M. Farrukh, H. Qi, L. Marcenaro, Y. Gao, and C. S. Regazzoni. AI-Based Abnormality Detection at the PHY-Layer of Cognitive Radio by Learning Generative Models. *IEEE Transactions on Cognitive Communications and Networking*, 6(1):21–34, 2020.

[18] M. Farrukh, A. Krayani, M. Baydoun, L. Marcenaro, Y. Gao, and C. S. Regazzoni. Learning a Switching Bayesian Model for Jammer Detection in the Cognitive-Radio-Based Internet of Things. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pages 380–385, April 2019.

[19] H. C. Nguyen, R. Amorim, J. Wigard, I. Z. KováCs, T. B. Sørensen, and P. E. Mogensen. How to Ensure Reliable Connectivity for Aerial Vehicles Over Cellular Networks. *IEEE Access*, 6:12304–12317, 2018.

[20] J. Stanczak, D. Kozioł, I. Z. Kovács, J. Wigard, M. Wimmer, and R. Amorim. Enhanced Unmanned Aerial Vehicle Communication Support in LTE-Advanced. In *2018 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–6, Oct 2018.

[21] A. Krayani, M. Farrukh, M. Baydoun, L. Marcenaro, Y. Gao, and C. S.Regazzoni. Jammer detection in M-QAM-OFDM by learning a Dynamic Bayesian Model for the Cognitive Radio. In *2019 27th European Signal Processing Conference (EUSIPCO)*, pages 1–5, 2019.

[22] M. Baydoun, D. Campo, V. Sanguineti, L. Marcenaro, A. Cavallaro, and C. Regazzoni. Learning switching models for abnormality detection for autonomous driving. In *2018 21st International Conference on Information Fusion (FUSION)*, pages 2606–2613, July 2018.

[23] N. Michael, D. Mellinger, Q. Lindsey, and V. Kumar. The GRASP Multiple Micro-UAV Testbed. *IEEE Robotics Automation Magazine*, 17(3):56–65, Sep. 2010.