Deep Learning for Spectrum Anomaly Detection in Cognitive mmWave Radios

Andrea Toma[1,2], Ali Krayani[1,2], 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: andrea.toma@ginevra.dibe.unige.it, ali.krayani@edu.unige.it
{lucio.marcenaro, carlo.regazzoni}@unige.it, yue.gao@qmul.ac.uk

***Abstract*—Millimeter Wave (mmWave) band can be a solution to serve the vast number of Internet of Things (IoT) and Vehicle to Everything (V2X) devices. In this context, Cognitive Radio (CR) is capable of managing the mmWave spectrum sharing efficiently. However, Cognitive mmWave Radios are vulnerable to malicious users due to the complex dynamic radio environment and the shared access medium. This indicates the necessity to implement techniques able to detect precisely any anomalous behaviour in the spectrum to build secure and efficient radios. In this work, we propose a comparison framework between deep generative models: Conditional Generative Adversarial Network (C-GAN), Auxiliary Classifier Generative Adversarial Network (AC-GAN), and Variational Auto Encoder (VAE) used to detect anomalies inside the dynamic radio spectrum. For the sake of the evaluation, a real mmWave dataset is used, and results show that all of the models achieve high probability in detecting spectrum anomalies. Especially, AC-GAN that outperforms C-GAN and VAE in terms of accuracy and probability of detection.**

***Index Terms*—Deep Learning, Anomaly Detection, Cognitive Radios, Millimeter Wave, Generative Models**

I. Introduction

The explosive rise in the number of wireless equipment, including Internet of Things (IoT) and Vehicle to Everything (V2X) devices will support tremendous wireless connectivity causing the spectrum scarcity [1], [2]. Millimetre Wave (mmWave) and Cognitive Radio (CR) are proposed to address such issue and increase the radio spectrum utilization [3]. CR allows the secondary users to sense frequently and access opportunistically the spectrum bands which are not in use by the primary licensed users and without damaging the quality of service [4]–[7]. The mmWave provides sizeable available bandwidth at high frequencies which operate in the range of 30 to 300 GHz, offering low latency and high-speed data connection [8], [9]. Such frequencies impose several limitations due to the fact that the signal will suffer from high propagation loss and get distorted due to raindrops and humidity absorption as well as its sensitivity to blockages, making the implementation of the mmWave communications possible to a few kilometres in small cells and heterogeneous networks which are efficient to serve the IoT and V2X scenarios [10], [11]. Besides, the fifth-generation (5G) technology will provide a system structure for these emerging V2X and IoT applications that require high reliability and strict delay for secure message delivery between transmitters and receivers which impose the need of an efficient hybrid access scheme for licensed and unlicensed spectrum in mmWave bands. Thus, CR has been proposed to manage the dynamic spectrum access in mmWave communications [12].

The Physical Layer Security in Cognitive mmWave Radios has attracted broad interest to achieve secured communications that involve multiple signal transmissions due to the shared wideband spectrum and the coexistence in tight integration with different wireless systems [13], [14]. Such open access medium and dynamic environment makes the system vulnerable to malicious users that aim to manipulate the radio spectrum by injecting anomalous signals and enforce the system to learn wrong behaviours that lead the radio to take mistaken actions [15], [16]. Autonomous learning is a crucial component in CR system to adapt to the perceived wireless environment and potentially maximize the utility of the available spectrum resources and allow the radio to take an optimal decision and act efficiently [17]. Therefore, precise detection of spectrum anomalies is crucial to enhance the physical layer security and improve the system's performance.

Spectrum anomaly detection has been explored in literature. However, it does not provide exhaustive work based on Deep Learning techniques, making it still a challenging task. The work in [18] investigates the wireless spectrum anomaly detection problem and design a module based on auto-encoder for feature extraction then performs initial unsupervised anomaly detection followed by anomaly feature module to optimize the feature extraction that is further used for active anomaly clustering and detection with user interaction. A deep predictive coding neural network for radio-frequency anomaly detection in wireless systems has been proposed in [19] where image sequences generated from the spectrum by monitoring real-time wireless signals. In [20], scaling deep learning models are built to capture spectrum usage patterns and use them as baselines to detect LTE spectrum usage anomalies resulting from faults and misuse. An adversarial auto-encoder using interpretable features as power spectral density data is proposed in [21] for wireless spectrum anomaly detection. In [19], [20], and [21], the data is relative to narrow ranges of frequencies and is represented by bidimensional spectrograms. Besides, anomalies are not related to changes in the dynamics of the signals. Indeed, in the abnormal spectrum, there is either an additional signal or the signal is corrupted concerning the normal situation. A framework with two different

applications, according to the dimensionality of the data, is presented in [22] where Dynamic Bayesian Network (DBN) and Generative Adversarial Network (GAN) are investigated as part of a self-awareness module with two levels in CR devices. Furthermore, in [22] it is shown that the approaches employing autonomous learning of deep features provide better results in the anomaly detection context with respect to conventional techniques, in particular the cyclostationary feature detector (CFD). Here, in the proposed framework for spectrum anomaly detection, we compare three deep generative models: the Conditional Generative Adversarial Network (C-GAN), the Auxiliary Classifier GAN (AC-GAN) and the Variational Auto Encoder (VAE). These generative models (C-GAN, AC-GAN and VAE) are investigated and employed in the mmWave communications enabled by CR to learn a representation of the dynamic spectrum following probabilistic reasoning. A generalized state vector, consisting of the signal feature (amplitude) extracted from the Stockwell Transform (ST) and the corresponding derivatives, is formed and used to construct the network that, consequently, detects any anomalous signals related to abnormal behaviours inside the radio spectrum. The motivation for using a generalized state vector is clarified in [22]. *To the best of our knowledge, this is the first time that the generalized state vectors are investigated as input data for a comparison between GAN and VAE models in the literature*. Making such a comparison lays the basis for an understanding of the mechanisms for each of these generative models capable of generating an anomaly measure, and highlighting strengths and weaknesses in the conventional GAN and VAE models.

The rest of this paper is organized as follows. We described the proposed framework in Section II and showed the experiments and results in Section III. Finally, in Section IV we conclude the paper by highlighting the future work.

II. Proposed Framework

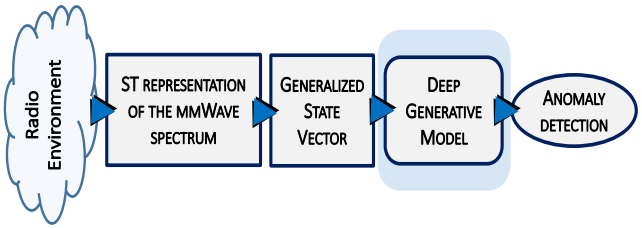
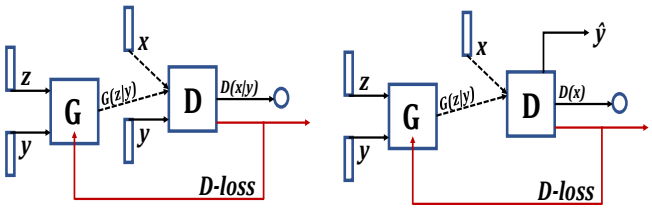


Fig. 1. The deep model-based anomaly detection scheme for CR

The general scheme of the proposed research is depicted in Fig. 1. The radio environment represents wireless communication in which transmissions are involved in the mmWave band. A CR system observes and gathers information about the spectrum occupancy where multiple signals dynamically occupy the available channels. However, processing and sensing such dynamic spectrum in the considered scenario requires suitable techniques. To this end, Stockwell Transform (ST) is used to extract the time-frequency representation of the spectrum following the approach proposed in [23]. From such



(a) Diagram of the C-GAN (b) Diagram of the AC-GAN

Fig. 2. Generative Adversarial Networks

representation, a generalized state vector is formed, as defined in [24]. It consists of the current state in terms of amplitude (A) and its first-order derivative ($\dot{A}$):

$$\mathbf{x} = [A_{ch,k},\ \dot{A}_{ch,k}]; \quad \text{ch} \in \{1, \ldots, N\} \tag{1}$$

where k is the time instant at which each value A related to the ch-th channel is extracted from ST and N is the total number of channels. From the generalized state vector, the proposed deep models presented in the following section will learn the dynamics of the radio environment and how they are evolving with time.

A. Conditional Generative Adversarial Network (C-GAN)

By conditioning the basic GAN model [25] on additional information $\mathbf{y}$ (e.g. class labels), it is possible to direct the data generation process. This model is called C-GAN [26] shown in Fig. 2(a).

Training Phase: the C-GAN consists of both a generative model G that captures the data distribution and a discriminative model D that estimates the probability of a sample comes from that data distribution. Both G and D can be represented by a non-linear mapping function that is learnt during the training phase. G maps a random noise $\mathbf{z}$ to data space $\mathbf{x}$. This mapping is represented by $G(\mathbf{z}|\mathbf{y})$. While D acts as a binary classifier and outputs a single scalar represented by $D(\mathbf{x}|\mathbf{y})$. The training procedure for G is to minimize the probability that D makes the correct decision. While D is trained to maximize the probability of correctly differentiating the training samples from generated samples. This framework corresponds to a two-player min-max game. The corresponding cost function is given by:

$$\min_G \max_D V(D,G) = \mathrm{E}_{\mathbf{x}\sim p_{data}(\mathbf{x})}[\log D(\mathbf{x}|\mathbf{y})] + \\ + \mathrm{E}_{\mathbf{z}\sim p_z(\mathbf{z})}[\log(1 - D(G(\mathbf{z}|\mathbf{y})))] \tag{2}$$

where $p_{data}(\mathbf{x})$ is the data distribution and $p_z(\mathbf{z})$ is the prior.

Testing Phase: the parameters of both G and D networks are not updated through the optimization of the cost function which is only utilized to detect deviations between prediction and observation, based on the following anomaly measurement:

$$\text{db0} = |l_{real} - l_{fake}| \tag{3}$$

where l_{real} is the loss computed at the discriminator when the input is the real data $\mathbf{x}$ while l_{fake} is the loss when the input is

the one generated by the generator from G($\mathbf{z}|\mathbf{y}$), respectively, and $|\cdot|$ represents the absolute value function.

B. Auxiliary Classifier GAN (AC-GAN)

Alternatively, the discriminator can be modified with reconstructing the class information $\hat{\mathbf{y}}$. In this way, the discriminator will contain an auxiliary decoder network that outputs the class label for the training data. This variant of the GAN architecture is called auxiliary classifier GAN (or **AC-GAN**) [27] and shown in Fig. 2(b).

Training Phase: G uses both the class labels $\mathbf{y}$ and the noise $\mathbf{z}$ to generate data samples (fake data), $\mathbf{x}_{fake}$. While, the discriminator computes both the probability distribution of the sources, $p(\mathbf{s}|\mathbf{x})$, and of the class labels, $p(\mathbf{y}|\mathbf{x})$ such that $D(\mathbf{x}) = (p(\mathbf{s}|\mathbf{x}), p(\mathbf{y}|\mathbf{x}))$. The source of the data, $\mathbf{s}$, refers to the decision of the discriminator, namely either real data, $\mathbf{s}_{real}$, or fake data, $\mathbf{s}_{fake}$. Consequently, the objective function consists of both the log-likelihood of the correct source, $L_{\mathbf{s}}$, and the log-likelihood of the correct class, $L_{\mathbf{y}}$, as follows:

$$L_{\mathbf{s}} = \mathrm{E}[\log p(\mathbf{s}_{real}|\mathbf{x}_{real})] + \mathrm{E}[\log p(\mathbf{s}_{fake}|\mathbf{x}_{fake})] \quad (4)$$

$$L_{\mathbf{y}} = \mathrm{E}[\log p(\hat{\mathbf{y}}|\mathbf{x}_{real})] + \mathrm{E}[\log p(\hat{\mathbf{y}}|\mathbf{x}_{fake})] \quad (5)$$

D maximizes the probability of correctly classifying real and fake samples ($L_{\mathbf{s}}$) and correctly predicting the class label ($L_{\mathbf{y}}$) of a real or fake sample ($L_{\mathbf{s}} + L_{\mathbf{y}}$). G minimizes the ability of the discriminator to discriminate real and fake samples while also maximizing the ability of the discriminator in predicting the class label of real and fake samples ($L_{\mathbf{y}} – L_{\mathbf{s}}$).

Testing Phase: as in C-GAN, in this phase the parameters of both G and D networks are not updated, and the anomaly measurement defined in eq.(3) is utilized to detect deviations where, in addition to the loss computed on data, both l_{real} and l_{fake} take also into account an auxiliary loss term from real and fake class labels, respectively.

C. Variational Auto Encoder (VAE)

Training Phase: VAEs learn a stochastic mapping between an observed data space $\mathbf{x}$, whose empirical distribution is typically complicated, and a latent space $\mathbf{z}$, whose distribution can be relatively simple [28]. $\mathbf{z}$ represents a compressed low dimensional representation of the input $\mathbf{x}$. VAEs consist of two models, the encoder or inference model, and the decoder or generative model (refer to Fig. 3). The generative model (decoder) learns the joint distribution $p_\theta(\mathbf{x}, \mathbf{z})$. The inference model (encoder) $q_\phi(\mathbf{z}|\mathbf{x})$, approximates the true but intractable posterior $p_\theta(\mathbf{z}|\mathbf{x})$ of the generative model. The model parameters of the decoder and encoder are denoted by θ and ϕ, respectively. While, μ and σ are the mean and standard deviation of the multivariate distribution $q_\phi(\mathbf{z}|\mathbf{x})$. $\varepsilon \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$ is a noise random variable. Ideally, the reconstructed input $\mathbf{x}'$ is approximately identical to $\mathbf{x}$, $\mathbf{x} \approx \mathbf{x}'$.

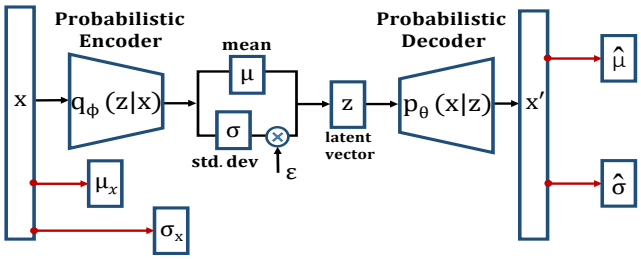


Fig. 3. Diagram of the VAE

VAEs provide a computationally efficient way for optimizing the generative model jointly with the corresponding inference model. The model parameters (ϕ), also called variational parameters, are optimized such that:

$$q_\phi(\mathbf{z}|\mathbf{x}) \approx p_\theta(\mathbf{z}|\mathbf{x}) \quad (6)$$

by using the Evidence Lower Bound (ELBO) which is the variational lower bound on the log-likelihood of the data. It includes the Kullback-Leibler (KL) divergence between $q_\phi(\mathbf{z}|\mathbf{x})$ and $p_\theta(\mathbf{x}, \mathbf{z})$. Maximization of the ELBO w.r.t. the parameters θ and ϕ, will approximately maximize the marginal likelihood $p_\theta(\mathbf{x})$ and minimize the KL divergence of the approximation $q_\phi(\mathbf{z}|\mathbf{x})$ from the true posterior $p_\theta(\mathbf{z}|\mathbf{x})$.

Testing Phase: the parameters θ and ϕ are not updated so that the encoder and decoder are the ones learned during training. In this phase, a way of measuring the similarity between the observation and prediction is related to the reconstruction error which gives the anomaly measurement $db0$ (refer to Fig. 3) computed as follows:

$$\mathrm{db0} = \left((\mu_x - \widehat{\mu})^T C_{\widehat{\sigma}^2}^{-1} (\mu_x - \widehat{\mu})\right)^8 \quad (7)$$

where μ_x is the mean vector from the input data with dimension d (for the sake of completeness, σ_x is the standard deviation vector from the input data), and $\widehat{\mu}$ and $\widehat{\sigma}$ are the mean and standard deviation vectors from the reconstructed data vector with the same dimension d. These quantities are the output of neural networks whose input is $\mathbf{x}$ and $\mathbf{x}'$, respectively. $C_{\widehat{\sigma}^2}^{-1}$ is a covariance matrix given by diag$(\widehat{\sigma}_1^2, \ldots, \widehat{\sigma}_d^2)$.

III. Experiments

The following experiments have been performed on the generative models described in Sec.II to demonstrate the practical feasibility of the proposed approach for spectrum anomaly detection. First, the mmWave testbed and the real dataset are described, then results are presented.

A. mmWave Testbed

The National Instruments mmWave Transceiver System, Fig.4, used to collect the dataset, is a Software Defined Radio (SDR) platform consisting of hardware equipment and application software that enables real-time over the air mmWave communications. The transceiver system is comprised of chassis, controllers, a clock distribution module, 192 MS/s Field-Programmable Gate Array (FPGA) modules, high-speed Digital-to-Analog Converters (DACs) and Analog-to-Digital Converters (ADCs) (3.072 GS/s), Local Oscillator (LO) and Intermediate Frequency (IF) modules, and mmWave radio heads (24.25 - 33.4 GHz) for up-conversion from 12 GHz IF

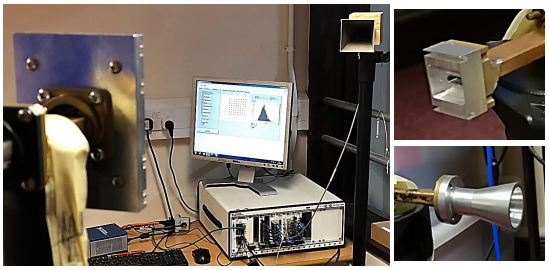
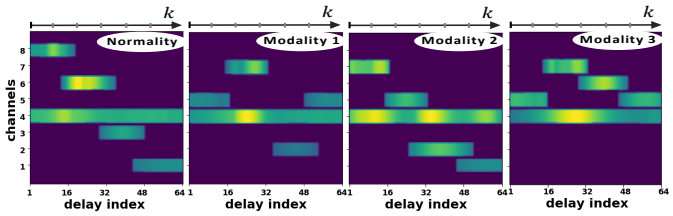
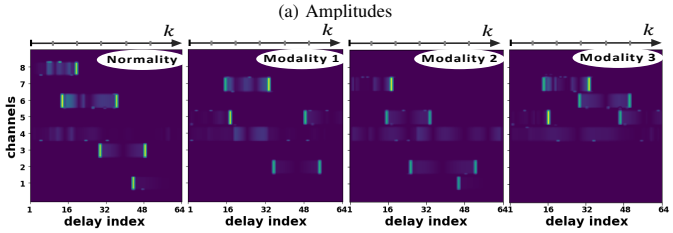


Fig. 4. The mmWave testbed setup.



(a) Amplitudes



(b) Derivatives

Fig. 5. Four patterns performed by the signals inside the spectrum

to mmWave band and down-conversion from mmWave band to 12 GHz IF. A detailed description can be found in [29]. The radio heads are connected to a Ka-band circular horn transmitting antenna (26-40 GHz) and a slot antenna at 28.5 GHz for receiving the signal [30], respectively. The mmWave transceiver operates at 28 GHz (central carrier frequency), and the analysed spectrum consists of 8×100 MHz channels with 800 MHz total bandwidth. Complex I/Q data is collected at base-band after the down-conversion process. Cyclic-Prefix Orthogonal Frequency Division Multiplexing (CP-OFDM) signals with 1200 sub-carriers are transmitted inside the mmWave band with 75 kHz sub-carrier spacing and 2048 FFT size. Different modulation schemes are supported (BPSK, QPSK, 16-QAM, and 64-QAM). The sampling frequency is 3.072 GS/s (12-14 bits). The system specifications relative to the observed spectrum and the signal pre-processing resulting in the images of Fig. 5 are summarized in details in Table I and Table II.

B. Real Dataset

The dataset is divided into two sets: one for the training phase which represents the normal behaviour (no malicious behaviour) of the signals inside the spectrum and the second is used during the testing phase including three different anomaly modalities in which the behaviour of the signal is different from the normal one. Fig.5(a) shows the time-frequency representation of the dynamic spectrum obtained by

TABLE I
DATA FROM THE SYSTEM SPECIFICATION DATASHEET

Maximum bandwidth	2 GHz
Central frequency	28 GHz in the mmWave band
Sampling Rate	3.072 GS/s, resampled to/from 153.6 MS/s
	3.072 GS/s ÷ 153.6 MS/s = 20
Spectrum of interest	800 MHz bandwidth (27.6 GHz - 28.4 GHz)
Channels (width)	8 (100 MHz)
	192 MS/s x 2 (I/Q) x 8 channels = 3.072 GS/s
OFDM signal	1200 subcarriers/channel with 75 kHz spacing for each subcarrier (75 kHz x 1200 = 90 MHz)
Symbol Rate	153.6 MS/s (oversampling on each channel, I/Q data)
FFT for OFDM	2048 points (153.6 MHz / 75 kHz)

TABLE II
SIGNAL PRE-PROCESSING SPECIFICATIONS

Samples for each burst (I/Q signals)	4096
Stockwell transform size	512
Dual-resolution ST (frequency-time index)	512 (f) x 64 (k)
Sub-channel division (frequency-time index)	128 (f) x 64 (k)

ST in terms of amplitude (only one snapshot for each modality is displayed due to space limitations). The k axis represents the time domain in terms of 64 shifts of the sliding window denoted as delay index. While the vertical axis represents the frequency domain consisting of 8 channels divided into 128 sub-channels. And the corresponding derivatives are shown in Fig.5(b). The generalized state vector is formed by inserting the values relative to each vertical line from ST representation and concatenated with the corresponding vertical line of the derivative. The state vector is thus composed of 256 elements (128 for amplitudes and 128 for the derivatives) at each time instant k.

Normality data: the normal behaviour consists of a fixed signal which occupies channel ch number 4 and a moving signal jumping at four different channels: sequentially 8, 6, 3, and 1 as shown in the first pattern of Fig. 5(a).

Testing data: testing patterns with 3 different behavior modalities are also shown in Fig. 5(a) and described as follows.

- Modality 1: a fixed signal is occupying *ch-4* and a moving signal jumps between *ch-5*, *ch-7*, *ch-2*, *ch-5*.
- Modality 2: a fixed signal is occupying *ch-4* and a moving signal jumps between *ch-7*, *ch-5*, *ch-2*, *ch-1*.
- Modality 3: a fixed signal is occupying *ch-4* and a moving signal jumps between *ch-5*, *ch-7*, *ch-6*, *ch-5*.

Specifically, in the observed spectrum, a signal is anomalous when its behaviour (or dynamics) is different from the one previously seen during the training phase. Namely, the strategy by which the signal jumps in the spectrum changes with respect to the normal behaviour. In this case, an anomaly is said to have happened. This could be due to a new device in the network or to a malicious user. In particular, our approach is capable of learning the dynamics of signals and, each time a change in the dynamics happens, the generative models

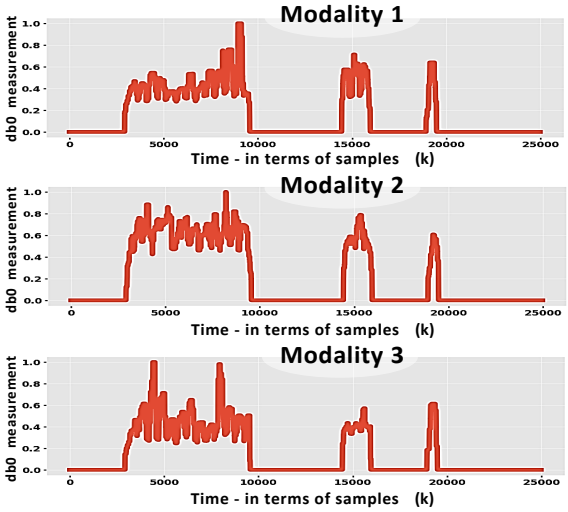


Fig. 6. Anomaly indicator (**C-GAN model**)

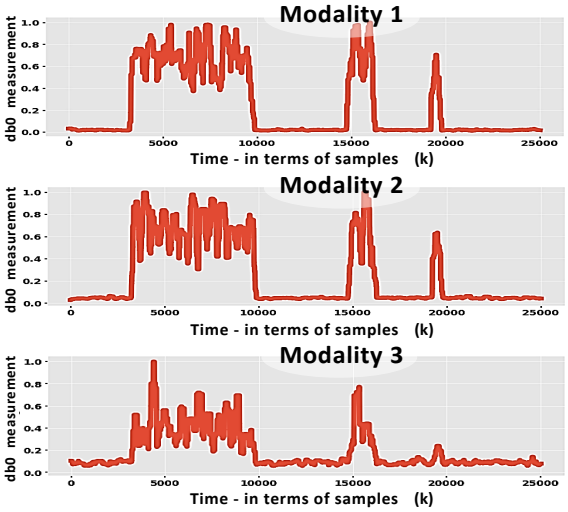


Fig. 8. Anomaly indicator (**AC-GAN model**)

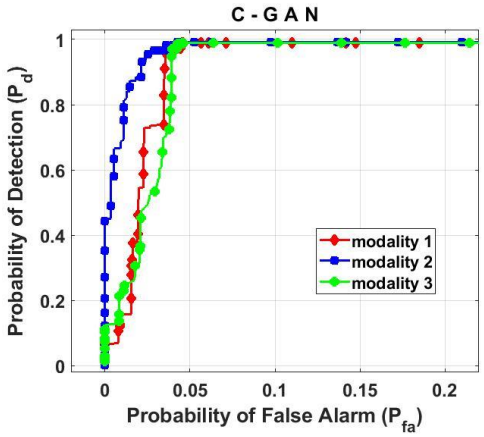


Fig. 7. ROC curves (**C-GAN model**)

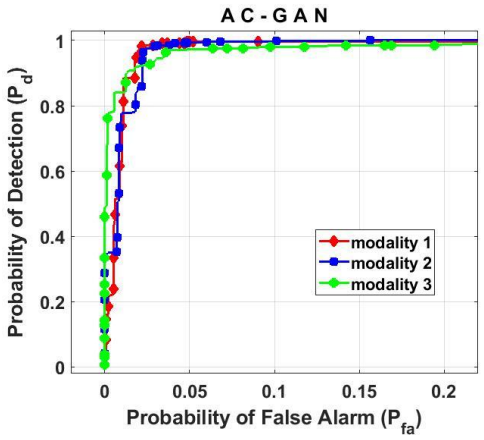


Fig. 9. ROC curves (**AC-GAN model**)

produce predictions that deviate from the observations that are classified as anomalies, as demonstrated in next section.

C. Results

1) Training of the generative models: the training data consists of 59520 *k-samples* in the time domain of the generalized state vector and 256 in the frequency domain for C-GAN, while 164480 *k-samples* and 256 for AC-GAN and VAE. By providing the normality data, *the generative models are learnt in an unsupervised way*. Indeed, in this work, the conditioning information, $\mathbf{y}$ consists of a fictitious input label because it is assigned the same value regardless of the input data $\mathbf{x}$ whether normal or anomalous. The training data is used to train neurons in the latent space of the networks, and it has been shown that in generative models, each neuron learns to detect specific types of features from the input data. Intrinsic clustering on input data is also obtained thanks to neurons that learn to detect similarity characteristics of groups of input samples. The Adam optimizer is used to train G and D of C-GAN and AC-GAN as well as the encoder and decoder of VAE. MSE loss is used as adversarial loss in C-GAN, while L^p loss (with p = 8) in AC-GAN which also includes a Cross-Entropy loss as an auxiliary loss. By setting p = 8, anomaly peaks (when an anomaly happens) and fluctuations (when signals in the spectrum follow a normal behaviour) in the indicator signal are optimized. The KL divergence is included in the loss function in VAE. Experiments have been performed on 'NVIDIA® GeForce® GTX 1080 Ti' GPU.

2) Testing of the generative models: in this phase 25280 *k-samples* in time domain and 256 in frequency domain forming the generalized state vector are tested and anomaly measurement is obtained (Figs. 6-8-10) for each of the 3 models and modalities. It can be seen that, when the deep model is given a generalized state vector as input, it is capable of detecting abnormal patterns, when they happen, in which malicious behaviour produces deviations of predictions from observations. This would be a novel approach by applying a generalized state vector to a deep model. These results can be

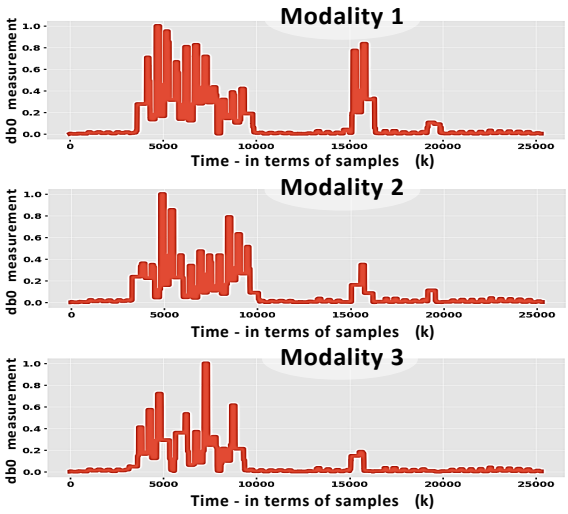


Fig. 10. Anomaly indicator (**VAE model**)

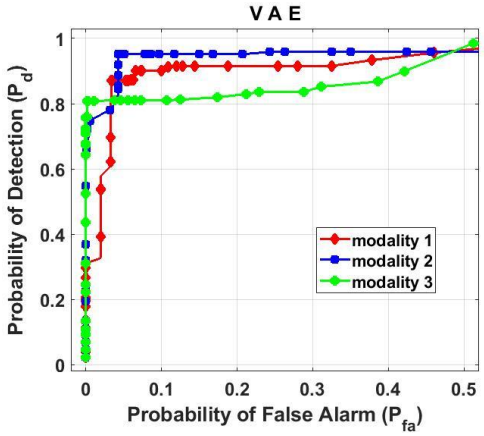


Fig. 11. ROC curves (**VAE model**)

analyzed by considering that groups of samples in the testing data could exhibit different types of features (anomalous situation) from the ones observed during the training of the generative network with normality data. In other words, since no neuron in the latent space was trained to detect these features, abnormality data cannot activate any neuron in the neural networks and the consequent deviation of prediction from observation produces high values of the abnormality measurements. Additionally, to evaluate the performance of the models, ROC curves are also shown in Figs. 7-9-11 that confirm that each of the deep model can provide high detection probability with low P_{fa}. In addition, the P_d can be optimized through a sensible choice of the threshold in the binary testing. Indeed, Area Under Curve (AUC) and Accuracy (ACC) values are extracted and listed in the Table III where the AC-GAN seems to provide better performance than C-GAN and VAE models. From another point of view, when GAN-based models are compared to VAE, it can be noticed that: in the first case, since the generator is trained to learn a mapping between a

TABLE III
AUC AND ACC VALUES FOR THE 3 DEEP LEARNING MODELS

		AUC	ACC
C-GAN	**modality 1**	0.9566	0.9657
	modality 2	0.9737	0.9696
	modality 3	0.9545	0.9668
AC-GAN	**modality 1**	**0.9741**	**0.9804**
	modality 2	**0.9751**	**0.9757**
	modality 3	**0.9742**	**0.9660**
VAE	**modality 1**	0.9365	0.9356
	modality 2	0.9577	0.9551
	modality 3	0.9232	0.9382

TABLE IV
COMPUTATIONAL TIMES FOR THE 3 DEEP LEARNING MODELS

Deep Learning Models	Training time [mm:ss]	Testing time [mm:ss]
C-GAN	15:16	01:36
AC-GAN	30:42	03:16
VAE	**15:09**	**01:00**

random noise vector, $\mathbf{z}$ in Fig. 2, and the generated data (by learning hidden, complex structure in the real data $\mathbf{x}$), then G is able to capture the dynamics in the real data. In the second case, a VAE model returns the posterior probability that an observation belongs to a specific cluster by learning the latent vector, $\mathbf{z}$ in Fig. 3. In this way, observations $\mathbf{x}$ from different clusters will correspond to different $\mathbf{z}$ vectors and the dynamics of $\mathbf{x}$ is captured according to the way and the time instants the vector $\mathbf{z}$ changes. In effect, learning from dynamic data as in the first case should provide better performance as confirmed by the results. Alternatively, an advantage of the VAE, with respect to GAN, is the possibility to exploit the encoder's output latent variables (μ and σ) that represent probabilistic distributions. Indeed, such variables can be clustered to learn temporal dependencies among them and draw a probabilistic graphical representation. The latent variables can also be used to reduce the complexity due to high dimensionality data in wideband RF spectrum. Finally, Table IV gives an idea about the time required to train and test the models under investigation. Among the 3 analysed models, VAE required less computational time to perform both training and testing processes, since KL is faster than MSE and L^p methods.

IV. CONCLUSION AND FUTURE WORK

This work has demonstrated the effective implementation of C-GAN, AC-GAN, and VAE models to detect mmWave spectrum anomalies in a CR system. A comparison framework is proposed between deep generative models learned from the generalized state vector which incorporates the signals amplitude and the corresponding derivative extracted from ST representation of the dynamic spectrum. Extensive experiments have been conducted on a real dataset collected by using a mmWave testbed. In all the tested modalities, anomaly measurements showed good performance for the three models, particularly the AC-GAN. ROC curves confirmed that

the probability of detection is high with a low false alarm probability. However, from computational time analysis, the VAE resulted in being faster than the other two networks. Moreover, in a VAE, the encoder's output latent variables could be clustered to learn temporal dependencies among them and draw a probabilistic graphical representation. These latent variables can also be used to reduce the complexity due to high dimensionality data. As future work, these approaches will be employed to characterize and classify the anomalous signals.

REFERENCES

[1] X. Liu and X. Zhang. NOMA-based Resource Allocation for Cluster-based Cognitive Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, pages 1–1, 2019.

[2] H. Xiao, D. Zhu, and A. T. Chronopoulos. Power Allocation With Energy Efficiency Optimization in Cellular D2D-Based V2X Communication Network. *IEEE Transactions on Intelligent Transportation Systems*, pages 1–11, 2019.

[3] Y. Song, W. Yang, X. Yang, Z. Xiang, and B. Wang. Physical Layer Security in Cognitive Millimeter Wave Networks. *IEEE Access*, 7:109162–109180, 2019.

[4] Z. Wei, B. Zhao, and J. Su. Cooperative Sensing in Cognitive Radio Ad Hoc Networks. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2019.

[5] Tripta, A. Kumar, and S. Saha. Estimator-Correlator based Spectrum Sensing with PU Signal Uncertainty in Full Duplex CRNs. In *2019 URSI Asia-Pacific Radio Science Conference (AP-RASC)*, pages 1–4, March 2019.

[6] L. Hu, R. Shi, M. Mao, Z. Chen, H. Zhou, and W. Li. Optimal energy-efficient transmission for hybrid spectrum sharing in cooperative cognitive radio networks. *China Communications*, 16(6):150–161, June 2019.

[7] C. Liu, X. Liu, and Y. Liang. Deep CNN for Spectrum Sensing in Cognitive Radio. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–6, May 2019.

[8] H. Zhao, J. Zhang, L. Yang, G. Pan, and M. Alouini. Secure mmWave Communications in Cognitive Radio Networks. *IEEE Wireless Communications Letters*, 8(4):1171–1174, Aug 2019.

[9] C. Chen, O. Kedem, C. R. C. M. d. Silva, and C. Cordeiro. Millimeter-Wave Fixed Wireless Access Using IEEE 802.11ay. *IEEE Communications Magazine*, pages 1–7, 2019.

[10] S. Vuppala, Y. J. Tolossa, G. Kaddoum, and G. Abreu. On the Physical Layer Security Analysis of Hybrid Millimeter Wave Networks. *IEEE Transactions on Communications*, 66(3):1139–1152, March 2018.

[11] K. Xiao, W. Li, M. Kadoch, and C. Li. On the Secrecy Capacity of 5G MmWave Small Cell Networks. *IEEE Wireless Communications*, 25(4):47–51, AUGUST 2018.

[12] Q. Huang, X. Xie, H. Tang, T. Hong, M. Kadoch, K. K. Nguyen, and M. Cheriet. Machine-Learning-Based Cognitive Spectrum Assignment for 5G URLLC Applications. *IEEE Network*, 33(4):30–35, July 2019.

[13] W. Yang, L. Tao, X. Sun, R. Ma, Y. Cai, and T. Zhang. Secure On-Off Transmission in mmWave Systems With Randomly Distributed Eavesdroppers. *IEEE Access*, 7:32681–32692, 2019.

[14] S. Wang, K. Huang, X. Xu, and S. Zhang. On the Reliability and Security Performance of Opportunistic Relay Selection in Millimeter Wave Networks. In *2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, pages 1–6, Aug 2018.

[15] S. Srinu, M. K. K. Reddy, and C. Temaneh-Nyah. Physical layer security against cooperative anomaly attack using bivariate data in distributed CRNs. In *2019 11th International Conference on Communication Systems Networks (COMSNETS)*, pages 410–413, Jan 2019.

[16] W. Wang and Z. Zheng. Hybrid MIMO and Phased-Array Directional Modulation for Physical Layer Security in mmWave Wireless Communications. *IEEE Journal on Selected Areas in Communications*, 36(7):1383–1396, July 2018.

[17] X. Zhou, M. Sun, G. Y. Li, and B. Fred Juang. Intelligent wireless communications enabled by cognitive radio and machine learning. *China Communications*, 15(12):16–48, Dec 2018.

[18] S. Rajendran, V. Lenders, W. Meert, and S. Pollin. Crowdsourced wireless spectrum anomaly detection. *IEEE Transactions on Cognitive Communications and Networking*, pages 1–1, 2019.

[19] 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.

[20] Zhijing Li, Zhujun Xiao, Bolun Wang, Ben Y. Zhao, and Haitao Zheng. Scaling Deep Learning Models for Spectrum Anomaly Detection. In *Proceedings of the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, Mobihoc '19, pages 291–300, New York, NY, USA, 2019. ACM.

[21] 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.

[22] 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, March 2020.

[23] A. Toma, T. Nawaz, L. Marcenaro, C. Regazzoni, and Y. Gao. Exploiting ST-Based Representation for High Sampling Rate Dynamic Signals. In *2nd International Conference on Wireless Intelligent and Distributed Environment for Communication*, pages 203–217, Cham, 2019. Springer International Publishing.

[24] K. Friston, B. Sengupta, and G. Auletta. Cognitive Dynamics: From Attractors to Active Inference. *Proceedings of the IEEE*, 102(4):427–445, April 2014.

[25] I.J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio. Generative Adversarial Networks. *ArXiv e-prints*, June 2014.

[26] M. Mirza and S. Osindero. Conditional Generative Adversarial Nets. *CoRR*, abs/1411.1784, 2014.

[27] A. Odena, C. Olah, and J. Shlens. Conditional Image Synthesis With Auxiliary Classifier GANs. *arXiv e-prints*, page arXiv:1610.09585, Oct 2016.

[28] D. P. Kingma and M. Welling. An Introduction to Variational Autoencoders. *CoRR*, abs/1906.02691, 2019.

[29] National Instruments. Introduction to the NI mmWave Transceiver System Hardware: http://www.ni.com/product-documentation/53095/en/, 2019.

[30] S. Alkaraki, Y. Gao, and C. Parini. High aperture efficient slot antenna surrounded by the cavity and narrow corrugations at Ka-band and Ku-band. *IET Microwaves, Antennas Propagation*, 12(12):1926–1931, 2018.