Jammer detection in M-QAM-OFDM by learning a Dynamic Bayesian Model for the Cognitive Radio

Ali Krayani[1,2], Muhammad Farrukh[1,2], Mohamad Baydoun[1], Lucio Marcenaro[1], Yue Gao[2] and Carlo S.Regazzoni[1]
Department of Electrical, Electronics and Telecommunication Engineering and Naval Architecture, University of Genova, Italy[1]
School of Electronic Engineering and Computer Science (EECS), Queen Mary University of London, UK[2]
email addresses: {ali.krayani, muhamad.farrukh, mohamad.baydoun}@ginevra.dibe.unige.it
{lucio.marcenaro, carlo.regazzoni}@unige.it, yue.gao@qmul.ac.uk

***Abstract*—Communication and information field has witnessed recent developments in wireless technologies. Among such emerging technologies, the Internet of Things (IoT) is gaining a lot of popularity and attention in almost every field. IoT devices have to be equipped with cognitive capabilities to enhance spectrum utilization by sensing and learning the surrounding environment. IoT network is susceptible to the various jamming attacks which interrupt users communication. In this paper, two systems (Single and Bank-Parallel) have been proposed to implement a Dynamic Bayesian Network (DBN) Model to detect jammer in Orthogonal Frequency Division Multiplexing (OFDM) sub-carriers modulated with different M-QAM. The comparison of the two systems has been evaluated by simulation results after analyzing the effect of the self-organizing map's (SOM) size on the performance of M-QAM modulation.**

***Index Terms*—Cognitive Radio, IoT, OFDM, Dynamic Bayesian Network, Kalman Filter, Particle Filter.**

I. Introduction

A new paradigm in the information and communication field known as IoT connects a wide variety of ubiquitous objects [1]. IoT is shaping real-world assets by providing unique features to remain interconnected with anything at any place and time by using any available network [2]. It has been advocated to deploy wireless technology to connect objects in IoT. However, this gives rise to the problem of spectrum scarcity as many devices intend to utilize spectrum in order to remain connected. Hence, technological trends are shifting to integrate Cognitive Radio (CR) into IoT. CR is an emanating technology which has been developed to eradicate the spectrum scarcity problem [3]. Devices in IoT must be equipped with the cognitive capabilities to refrain from insufficient utilization of spectrum [4]. CR is an intelligent system that can sense, learn and adapt to the environmental modifications by regulating optimally its operating parameters based on the observation and previous experience. For CR to achieve the required aforementioned objectives, the physical layer needs to be highly flexible and adaptable. To this purpose, OFDM has been recognized as an attractive transmission modulation technique for CR systems. In OFDM, all the elements of the time-frequency grid can be scanned without any extra hardware by exploiting the Fast Fourier Transform (FFT), which simplifies the sensing process of the operating spectrum. Furthermore, OFDM can be adapted to different transmission environments by simply changing some parameters as FFT size, modulation and transmission power, achieving good adaptation and scalability. Moreover, since OFDM modulation is successfully implemented in various technologies such as Wireless Local Area Network (LAN) standards (IEEE 802.11a, 11g, 11n, 11ac, 11ad, 11ah) and Long Term Evolution (LTE), it will be easy for CR employing OFDM to inter-operate with such technologies [5]. CR-IoT network suffers from various kind of malicious attacks. Such kind of attacks aims to disrupt communication, deplete the bandwidth and seize transmission. Therefore, to achieve CR-IoT network objectives, providing secure communication under jamming attacks is a basic yet challenging task [6]. Several methods have been studied and proposed to detect jammer attacks in CR-IoT network. These include signature based method, anomaly based detection and classification. In this perspective, anomaly-based detection method has been studied and proposed to detect malicious attacks by using machine learning techniques [7]. In [8] deep auto-endcoders are deployed to identify abnormal signals in wireless spectrum whereas, machine learning based anomaly detection method is formulated in [9]. In [10] jammer attacks in CR-IoT network are addressed by using channel assignment technique. For practical IoT systems, machine learning based security techniques are explored and discussed in detail [11]. In [12], benefits of implementing OFDM modulation in IoT network are highlighted. In CR, it is imperative to learn legitimate and non-legitimate user's behaviors to make inferences about their states inside the spectrum by exploiting statistical properties [13]. In this way, we can better predict user's activities in the spectrum as time evolves. Furthermore, jammer's behavior can also be exploited in a much more vivid way.

This paper is motivated by previous work on detecting jammer [14]. Nonetheless, this paper differs from previous work since *i)* It focus on investigating multiple sub-carriers modulated with different M-ary QAM in the OFDM signal under jammer attacks in the CR-IoT network. The general objective while considering multiple sub-carriers is to track the jammers behavior and analyze how it is jumping between different sub-carriers, to detect the attacked frequency and predict what will be the next sub-carrier that the jammer might attack in the next time instant. *ii)* Jammer detection is achieved by implementing

two proposed systems Single and Bank-Parallel DBN. *iii)* Analyze the performance of the learned models (Single and Bank-Parallel) in an unsupervised way in order to understand the difference between the two systems and evaluate the experimental results. Additionally, effect of changing SOM size in relation with QAM modulation is analyzed and results are shown.

The proposed DBN realizes a Probabilistic Switching Model (PSM) which provides an agility to draw inference for each time slice about the spectrum at discrete and continuous levels by employing a combination of Particle Filter (PF) for discrete level and Kalman Filter (KF) for the continuous level. The combined approach is called as Markov Jump Particle Filter (MJPF), was first presented in [15] for different sensory data abnormality detection. A test set is used to evaluate the signal which is affected by a jamming interference and both proposed methods are capable to detect jammer attack.

The reminder of the paper is organized as follows. Section II describes related work. Sections III and IV present the system model and the proposed method, respectively. Experimental results are discussed in section V. In section VI, conclusion and future work are highlighted.

II. Related Work

CR-IoT network is vulnerable to the various jamming attacks. Consequently, the performance of the network declines and eventually becomes the worst under devastating attacks. In this paper, probabilistic model based jammer detection method is presented. In [16], authors formulate a novel encryption scheme employing OFDM for a system to combat various attacks. In [17], authors present eavesdropping-resilient OFDM system based on sub-carriers interleaving and allocation relying on channel state information. The joint time and power allocation schemes are presented to improve security rate of OFDM system against jamming attacks [18]. In [10], it is highlighted that the anomaly-based approach is better to detect jammer behavior and, various CR features such as signal modulation, signal power, centre frequency, channel bandwidth, carrier sense threshold and bit error rate, can be used to evaluate the performance of the network under normal operation. The signal strength (SS) and packet delivery ratio (PDR) are exploited during the learning phase of the network under no jamming attacks [19]. During the testing phase, the jammer is accompanied by a normal signal and detection is done by comparing jammer presence against the baseline profile. In [20], authors proposed anomaly based detection method which uses K-mean clustering for mobile network. In [21], authors provided anomaly detection method to countermeasure the effects of jammer in CR network. In [22], jammer's behaviour is learned by implementing Q-learning algorithm. The work [21] involves many nodes in data processing to perform anomaly behavior analysis. Therefore, it is not well-suited for the CR-IoT network. Moreover, [22] engages many tiny nodes in learning jammer behavior which raises energy-constrained issues. Consequently, it can't be deployed in a CR-IoT network. In this work, we consider two readily available features (amplitude and phase) of the received OFDM signal and learn the DBN model, unlike the work presented in [19] which relies on SS and PDR and doesn't provide practical implementation aspects of the system. Moreover, it is shown that IoT devices use radio channel bandwidth, channel gain and receive jammed power to implement the Q-learning algorithm [11]. On the contrary, we rely on two simple characteristics of the received signal by taking an inherited advantage of the FFT module inside the OFDM signal which gives amplitude and phase of the signal. Hence, processing is much more convenient and well-suited for CR-IoT network.

III. System Model

We consider a CR-IoT network consisting of a group of Cognitive Radio Users (CRUs) and a jammer trying to disrupt the communication as shown in Fig. 1. CRUs sense the spectrum continuously and try to detect abnormal situation. The radio spectrum contains OFDM waveforms based on IEEE 802.11ah standard, which is adopted in this work. OFDM divides the band channel into many narrower sub-carriers allowing different users to transmit simultaneously with different orthogonal frequencies. The OFDM modulated signal consists of a set of N sub-carriers:

$$\boldsymbol{C} = \{C_1, C_2, \ldots, C_N\}, \tag{1}$$

each sub-carrier is divided into Q symbols in time domain, forming a $N \times Q$ time-frequency grid. In the previous work [14] only one sub-carrier is picked to employ the proposed method supposing that OFDM use 16-QAM for all the sub-carriers in the set (1). Instead, here we consider multiple sub-carriers modulated with different QAM (4, 16, 64, and 256-QAM according to the standard IEEE 802.11ah). Exploiting FFT output which consists of amplitude and phase of each symbol makes the spectrum sensing easier and less complex where CRUs can scan the entire grid. Moreover, by using the Amplitude and Phase information at this level, permits to implement a jammer detection technique before demodulation of the signal which reduces the receiver complexity. The jammer attacks at different time instants by jumping from one frequency into another. We assume that there is a perfect synchronization between the transmitter and receiver. To evaluate the dynamics of the amplitudes and phases related to consecutive symbols and how they are evolving with time we consider the derivatives ($\dot{a}$, $\dot{p}$) of both amplitudes (a) and phases (p), and the generalized state vector can be defined at each time instant k for a specific sub-carrier as,

$$X_{k,C_n} = [\ a\ p\ \dot{a}\ \dot{p}\ ] \quad n = \{1, 2, \ldots, N\}, \quad C_n \in \boldsymbol{C} \tag{2}$$

A set of generalized state vectors corresponding to each sub-carrier is defined as:

$$\boldsymbol{X} = \{X_{k,C_1}, X_{k,C_2}, \ldots, X_{k,C_N}\}, \tag{3}$$

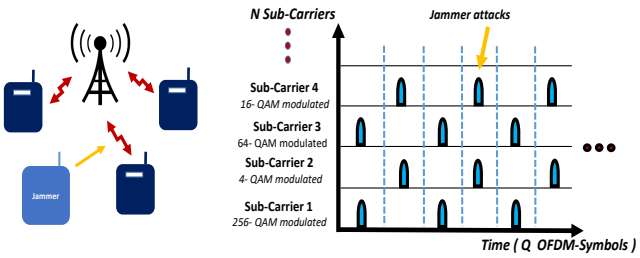


Fig. 1: Spectrum of the M-ary QAM modulated OFDM users in the CR-IoT Network under jammer attacks

IV. Proposed Method

The proposed method follows several processes that lead to detect abnormality behaviours in the spectrum, including the Offline Learning Process and the Online Testing Process. Two systems have been proposed *Single* and *Bank-Parallel* to deal with multiple sub-carriers where the Processes mentioned previously are used in both systems to learn the DBN model and obtain the abnormality indicator, respectively.

A. Offline Learning Process

The Dynamic Bayesian Network (DBN) model which is shown in Fig.2 is learned after obtaining a set of state vectors which describe signal behaviour in the spectrum under normal situation (without jammer). DBN enables to include dependencies between involved random variables as time evolves. DBN facilitates the representation of different inference levels related to the spectrum's dynamics. Consequently, here the lowest level of inference corresponds to measurements Z_k related to the observed received carriers in terms of amplitude and phase. States of the spectrum, X_k, represent a medium inference level which encodes continuous information of the spectrum. Super-states S_k corresponds to the top level of inference, which consists of the discretization of continuous information. Additionally, arrows represent conditional probabilities between the involved variables. Vertical arrows facilitate to describe causalities between both, continuous and discrete levels of inference and observed measurements. Horizontal arrows explain temporal causalities between hidden variables.

In order to learn the super-states, we employed a SOM that use as input the states of the spectrum and produce a set of super-states $\boldsymbol{S}$ including similar information (quasi-constant derivatives),

$$\boldsymbol{S} = \{S_1, S_2, \ldots, S_L\}, \tag{4}$$

where $S_k \in \boldsymbol{S}$ and L is the total number of superstates. A temporal transition matrix can be estimated by observing the activated superstate over time and encode the probabilities $P(S_k|S_{k-1}, t_k)$ of moving from a current superstate to another one (S_k), considering the time t_k spent in the current superstate (S_{k-1}). Each super-state is characterized by a mean value and covariance matrix.

To analyze and make inferences about a dynamic system, two models are required: the measurement model that maps observation into states and the dynamic model that describes the evolution of the state with time, and it can be written as:

$$X_k = AX_{k-1} + BU_{S_{k-1}} + w_k, \tag{5}$$

where S_k is the previous obtained region, $A = [A_1 \;\; A_2]$ is a dynamic model matrix: $A_1 = [I_2 \;\; 0_{2,2}]^\intercal$ and $A_2 = 0_{4,2}$. I_n represents a square identity matrix of size n and $0_{l,m}$ is a $l \times m$ null matrix. $B = [I_2 \Delta k \;\; I_2]^\intercal$ is a control input model. w_k represents the prediction noise. The variable $U_{S_{k-1}}$ is a control vector that encodes the spectrum's action when it is inside a superstate S_k, such that:

$$U_{S_k} = [\dot{a}_{S_k} \quad \dot{p}_{S_k}]^\intercal, \tag{6}$$

Accordingly, it is possible to estimate the probability of obtaining a future spectrum's state given its present state $P(X_k|X_{k-1}, S_{k-1})$ for each superstate S_{k-1}.

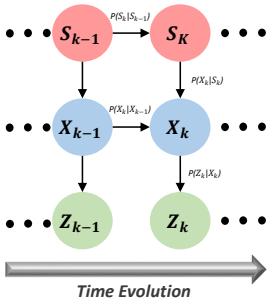


Fig. 2: Proposed DBN model to detect jammer in the Spectrum

B. Online Testing Process

To infer and detect the jammer, we proposed to use the MJPF introduced in Section I. As mentioned before, the MJPF uses Particle filter to make inferences at discrete levels. Additionally, each considered particle employs a Kalman Filter corresponding to the dynamic model learned for the corresponding value of the superstate (Eq.5) at the continuous level. As abnormal measurement we use the $db1$ defined in [15].

C. Single Dynamic Bayesian Network

As shown in the figure 3, we use the set of state vectors corresponding to each sub-carrier in (Eq.3) to learn a single DBN. During the Offline Learning Process, $\boldsymbol{X}$ is considered as input of the SOM which outputs a set of neuron $\boldsymbol{S}$. In this approach $\boldsymbol{S}$ consists of the discretization of the entire spectrum. However, single DBN keeps a memory of the spectrum's behaviour in time and frequency domain. Additionally, a single abnormality indicator is provided during the online Process.

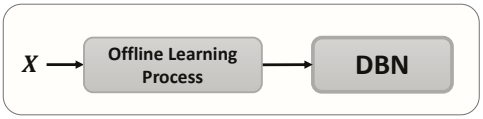


Fig. 3: Single DBN system

D. Bank-Parallel Dynamic Bayesian Network

In this approach, we don't have any correlation between the sub-carries, where the spectrum's behaviour at each sub-carrier X_{k,C_n} is processed individually (Fig 4). Accordingly, for each X_{k,C_n} we learn a DBN, such as:

$$\boldsymbol{DBN} = \{DBN_1, DBN_2, \ldots, DBN_N\}, \tag{7}$$

In the online process a MJPF is applied on each DBN_n providing an Abnormality signal, such as:

$$\boldsymbol{db1} = \{db1_1, db1_2, \ldots, db1_N\}, \tag{8}$$

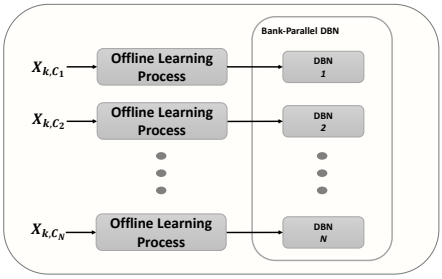


Fig. 4: Bank-Parallel DBN system

V. Experimental Setup and Results

A. Data Source

We use the OFDM system based on IEEE 802.11ah standard. We use a simulated OFDM signal consists of N = 64 sub-carriers and Q = 1000 symbols. The source generates random independent data. Each sub-carrier of the OFDM signal is modulated with different QAM modulation. For our experiments, we pick four sub-carriers with different QAM modulation (4, 16, 64, 256). The received signal is assumed to be affected by additive white Gaussian noise (AWGN) with zero mean and power spectral density σ_w^2. Data is cleaved into two data sets: first set contains clean data (without jammer attacks) which is used during training phase and the second one includes jammer's attacks which is used during testing, immediately after cyclic prefix (CP) is removed and FFT is performed on received data. We consider that jammer launches attacks into multiple sub-carriers with equal power.

B. Performance evaluation of M-ary QAM with SOM size

The performance of Single and Bank-Parallel DBN models are evaluated under multiple attacks and results are shown in terms of ROC curves which consist of Probability of Detection (P_d) and Probability of False Alarm (P_f), and Area Under Curve (AUC). The abnormality measurement ($db1$) is used to calculate the (P_d) and (P_f) respectively. (P_d) is the the number of times where abnormalities (related to jammer attacks) are correctly identified, while (P_f) are the times where anomalies are wrongly assigned to normal symbols. Fig. 5 illustrates the ROC curve obtained from Single DBN when a different number of neurons is selected. It is evident from Fig. 5 and Tab. I that 1024 neurons are the most appropriate for a Single DBN. Whereas, Fig. 6a, 6b, 6c and 6d present Bank-Parallel DBN ROC curves. For every ROC curve, each DBN deploys different QAM and optimum SOM size is analyzed. In case of 4-QAM, the optimum SOM size is 4 (see Fig. 6a and Tab. II). In 16-QAM is 4 (refer Fig. 6b and Tab. II). For 64-QAM, is 8 (see Fig. 6c and Tab. II), and for 256-QAM is 8 (refer Fig. 6d and Tab. II). We believe that the optimum number of neurons depend on the data and the number of symbols. For the simulated data used in our experiments and from the obtained results we can notice that the Bank-Parallel system performs well for a small number of neurons, where the Single system performs well for a large number of neurons. This is due to the fact that Single-DBN use the generalized state vector consisting a large number of samples ($4Q$ symbols), which is 4 times the number of symbols used in Bank-Parallel system.

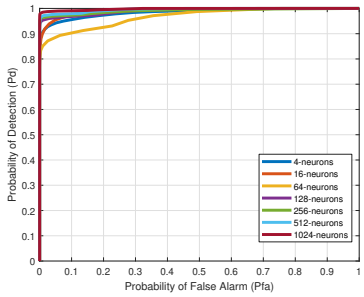
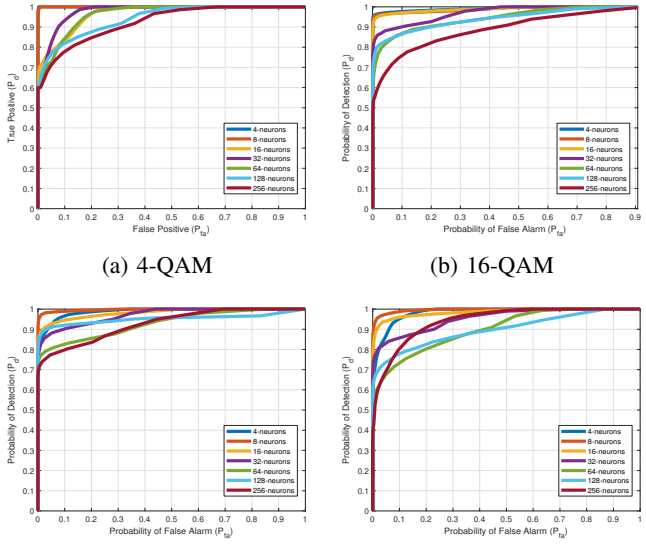


Fig. 5: ROC for a **Single-DBN** under attacks while varying SOM size

SOM size	4	16	64	128	256	512	1024
AUC (%)	98.95	99.75	99.05	99.89	99.71	99.93	**99.95**

TABLE I: Precision measurements for a **Single-DBN**



(a) 4-QAM (b) 16-QAM

(c) 64-QAM (d) 256-QAM

Fig. 6: ROC for an individual DBN in **Bank-Parallel-DBN** employs different M-QAM under attacks while varying SOM size

AUC (%)	SOM size 4	8	16	32	64	128	256
4-QAM	**99.99**	99.89	96.65	97.82	96.64	98.23	96.38
16-QAM	**99.86**	99.79	99.51	99.7	97.46	96.51	91.76
64-QAM	99.16	**99.89**	99.61	99.67	96.31	95.11	97.13
256-QAM	98.55	**99.83**	98.87	99.2	96.1	91.36	95.35

TABLE II: Precision measurements for a **Bank-Parallel-DBN**

C. Comparison between Single and Parallel DBN

After using the optimum number of neurons obtained previously to make a fair comparison between the two systems. The performance of both systems is somehow similar as shown in Fig. 7. We can deploy either of the proposed method depending on the receiver complexity and specific task. For instant, Single DBN learns single vocabulary for all sub-carriers, whereas, Bank-Parallel DBN learns multiple vocabularies corresponds to each sub-carrier which increases complexity. Subsequently, implementing bank parallel DBN is suitable for the source characterization tasks. Tracking the jammer and keeping its profile history in the entire spectrum is much more convenient in Single DBN.

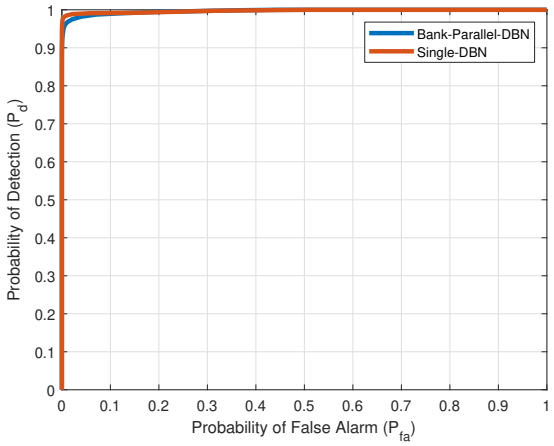


Fig. 7: Performance comparison between **Single-DBN** and **Bank-Parallel-DBN** in terms of ROC

VI. Conclusion and Future work

In this work, we present a jammer detection method in multiple OFDM sub-carriers by using two different systems. Sub-carriers are modulated with different M-QAM and optimum SOM size is selected for each QAM modulation based on the probability of detecting multiple attacks. As a conclusion we have learned that using the two systems, Single DBN and Bank-parallel DBN, exhibits similar performance under multiple attacks. The results presented in this work provide an understanding to further investigate the dynamic behaviour of the jammer in order to track its activity inside the spectrum and characterize it.

References

[1] W. Ejaz and M. Ibnkahla. Multiband Spectrum Sensing and Resource Allocation for IoT in Cognitive 5G Networks. *IEEE Internet of Things Journal*, Feb 2018.

[2] R. Han, Y. Gao, C. Wu, and D. Lu. An Effective Multi-Objective Optimization Algorithm for Spectrum Allocations in the Cognitive-Radio-Based Internet of Things. *IEEE Access*, 2018.

[3] A. A. Khan, M. H. Rehmani, and A. Rachedi. When Cognitive Radio meets the Internet of Things? In *International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sep. 2016.

[4] X. Zhang, Y. Ma, H. Qi, Y. Gao, Z. Xie, Z. Xie, M. Zhang, X. Wang, G. Wei, and Z. Li. Distributed Compressive Sensing Augmented Wideband Spectrum Sharing for Cognitive IoT. *IEEE Internet of Things Journal*, Aug 2018.

[5] H. A. Mahmoud, T. Yucek, and H. Arslan. OFDM for cognitive radio: merits and challenges. *IEEE Wireless Communications*, April 2009.

[6] X. Tang, P. Ren, and Z. Han. Jamming Mitigation via Hierarchical Security Game for IoT Communications. *IEEE Access*, 2018.

[7] S. Fayssal and S. Hariri. Anomaly-based Protection Approach against Wireless Network Attacks. In *IEEE International Conference on Pervasive Services*, July 2007.

[8] Qingsong Feng, Yabin Zhang, Chao Li, Zheng Dou, and Jin Wang. Anomaly detection of spectrum in wireless communication via deep auto-encoders. *The Journal of Supercomputing*, Jul 2017.

[9] 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 2018 - Proceedings*, 2018.

[10] H. A. Bany Salameh, S. Almajali, M. Ayyash, and H. Elgala. Spectrum Assignment in Cognitive Radio Networks for Internet-of-Things Delay-Sensitive Applications Under Jamming Attacks. *IEEE Internet of Things Journal*, June 2018.

[11] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, Sep. 2018.

[12] R. Melki, H. N. Noura, M. M. Mansour, and A. Chehab. An Efficient OFDM-based Encryption Scheme Using a Dynamic Key Approach. *IEEE Internet of Things Journal*, 2019.

[13] W. Han, H. Sang, X. Ma, J. Li, Y. Zhang, and S. Cui. Sensing statistical primary network patterns via Bayesian network structure learning. *IEEE Transactions on Vehicular Technology*, 2017.

[14] Muhammad Farrukh Shahid, Ali Krayani, Mohamad Baydoun, Lucio Marcenaro, Yue Gao, and Carlo 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 2019)*, Limerick, Ireland, April 2019.

[15] 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)*, July 2018.

[16] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong. Design of an OFDM Physical Layer Encryption Scheme. *IEEE Transactions on Vehicular Technology*, March 2017.

[17] H. Li, X. Wang, and J. Chouinard. Eavesdropping-Resilient OFDM System Using Sorted Subcarrier Interleaving. *IEEE Transactions on Wireless Communications*, Feb 2015.

[18] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin. Wireless Powered Cooperative Jamming for Secure OFDM System. *IEEE Transactions on Vehicular Technology*, Feb 2018.

[19] Z. M. Fadlullah, H. Nishiyama, N. Kato, and M. M. Fouda. Intrusion detection system (IDS) for combating attacks against cognitive radio networks. *IEEE Network*, May 2013.

[20] M. S. Parwez, D. B. Rawat, and M. Garuba. Big Data Analytics for User-Activity Analysis and User-Anomaly Detection in Mobile Wireless Network. *IEEE Transactions on Industrial Informatics*, Aug 2017.

[21] Yaser Jararweh, Haythem A. Bany Salameh, Abdallah Alturani, Loai Tawalbeh, and Houbing Song. Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks. *Telecommunication Systems*, Feb 2018.

[22] F. Slimeni, B. Scheers, Z. Chtourou, and V. Le Nir. Jamming mitigation in cognitive radio networks using a modified Q-learning algorithm. In *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2015.