Learning a Switching Bayesian Model for Jammer Detection in the Cognitive-Radio-Based Internet of Things

Muhammad Farrukh[1,2], Ali Krayani[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: {muhamad.farrukh, ali.krayani, mohamad.baydoun}@ginevra.dibe.unige.it
{lucio.marcenaro, carlo.regazzoni}@unige.it, yue.gao@qmul.ac.uk

***Abstract*—The proliferation of interconnected objects in the Internet of Things (IoT) can be benefit from integration of cognitive radio (CR) technologies at the network level. IoT networks equipped with cognitive capabilities can help to effectively alleviate the problem of spectrum scarcity. However, the IoT network can suffer from jammer attacks that interfere with user transmissions and disrupt communications. In this paper, we consider a CR-IoT network based on Orthogonal Frequency Division Multiplexing (OFDM) modulation scheme and a reactive jammer is hypothesized to be present in the network. A jammer detection method is proposed that is based on learning a switching Dynamic Bayesian Network (DBN) from normal OFDM data transmissions that is capable to detect abnormal situations. The proposed model is shown to be capable to detect and locate multiple jammers. The comparison with a conventional energy detection shows the validity of the proposed approach.**

***Index Terms*—Cognitive Radio, IoT, OFDM, Dynamic Bayesian Network**

I. Introduction

Recent developments in information technologies and machine to machine communications, brought a new technology which is deployed to intelligently connect different objects in a network, i.e. IoT. Typical objects in IoT networks are sensors, actuators, mobile phones and other devices, which are equipped with powerful data capabilities and use standard protocols to access any service at any time by using ideally any available path, service and network. IoT is an emerging technology which is penetrating into many fields such as industrial manufacturing, logistics process, transportation, health care, automation, and many more [1]. In IoT, objects are either connected through wired or wireless networks, however, wireless networks provide cost-effective and remote access solution as compared to the wired network [2]. The IoT objects might generate massive data as they exchange information in order to remain connected and access services. This increases spectrum resources requirements and creates a bottleneck in the IoT network. If a static spectrum allocation policy is adopted, the problem of spectrum scarcity might arise [3]. Current trends of research have drawn attention to incorporate Cognitive Radio (CR) in the IoT network and it is expected that devices in IoT will be supplied with cognitive capabilities to deal with spectrum scarcity problem [4]. Spectrum measurements show that most of the time, the radio spectrum is not being used by the licensed user and remains vacant. CR exploits vacant spaces to enhance spectrum utilization by assigning unused spectrum to other unlicensed users in the network. CR has been implemented in many applications such as mobile communication, wireless sensor networks, and radio-based smart grids [5]. CR makes radio systems intelligent by allowing them to sense, learn and adopt the best possible transmission strategy in a given operating environment. However, an adaptive physical layer modulation technique such as OFDM is necessary for CR to execute required tasks [6]. OFDM, due to its unique features, is broadly used in new wireless technologies. An OFDM modulation has been adopted in the Wireless Local Area Network standards such as IEEE 802.11a, IEEE 802.11g, IEEE 802.11n, IEEE 802.22 Wireless Regional Area Network based on CR in TV White Spaces (TVWS) and Long Term Evolution (LTE) mobile network. Moreover, to provide larger coverage area with the low-cost operation for thousands of connected objects in IoT, IEEE 802.11ah has been proposed in recent years which employs OFDM [7]. The use of CR has already been advocated for many IoT applications as an imminent solution and in this scenario, IoT objects act as secondary users to opportunistically access the primary user's spectrum whenever this is free [8]. To achieve the goals of CR-IoT network, protecting such network from various malicious attacks is a basic yet challenging issue [9]. IoT network suffers from various jammer attacks due to its heterogeneous nature [10]. CR network uses some of the characteristics of the radio network to address security challenges, however traditional radio networks may differ from one another with respect to the different strategies that are being adopted by each network to mitigate malicious attacks. This variation in using different strategies comes from the fact that each network is exposed to a dynamic environment and the CR network is more vulnerable to the security threats as compared with other radio networks

978-1-5386-4980-0/19/$31.00 ©2019 IEEE

due to its unique features. CR network attacks include Primary User Emulation (PUE), Spectrum sensing data falsification, denial of services, spoofing attacks and jamming. This last type of attack is considered to be the most frequent and menacing: Jammer attacks disrupt the communication and reduce the bandwidth of the CR network [11]. The security solution in the CR network aims to detect jammer and mitigate its effect. Accordingly, several methods have been studied and proposed such as classification, signature-based, and Anomaly-Based Detection (ABD) [12]. In [8], channel assignment technique is presented to address the issues of jammer attack in CR-IoT network. In [13], it is emphasized to exploit the statistical properties of the users in the CR network to learn the behavior of each user and make an inference. Such method of inference can be used to predict the state of a user in the network through a learning process. In this perspective, the ABD method has been studied and proposed to detect malicious attacks by using machine learning techniques [14].

The focus of this work is to analyze signals behaviour by using Dynamic Bayesian Networks realizing a Probabilistic Switching Model consisting of two hidden levels for each temporal slice and to detect malicious signals inside the spectrum for the CR-IoT network. The inference at continuous and discrete levels of the spectrum is achieved by using a combination of Particle filter (PF) for the 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 abnormality detection in autonomous driving. Self Organizing Maps (SOMs) [16] are applied to obtain discrete regions of the spectrum named as superstates. PF is used to compute transitions between superstates and predict discrete future states, while KF is implemented to predict the next states at continuous level inside a certain region corresponding to a given superstate. After learning the DBN model for the given spectrum under no jammer attacks, a testing set is used to evaluate the signal which is affected by a jamming interference.

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

Performances of a CR-IoT network can deteriorate due to malicious attacks. Therefore, there has been a major concern to detect such kind of devastating attacks which threaten normal operation of CR-IoT network. In this paper, jammer detecting and locating method is introduced based on a probabilistic model trained with wireless data corresponding to normal situations. Atya $et\ al.$ [17] proposed Jammer Interference Mitigation Scheme (JIMS) to avoid the jammer effects in OFDM communication system. Rahbari $et\ al.$ [18] presented the randomization of preamble technique in OFDM based 802.11 system to mitigate jammer attacks. The implementation of additional FFT module in parallel of OFDM block with wider window to reduce jamming effects in IEEE 802.11 Wi-Fi system is introduced in [19]. Nawaz $et\ al.$ [20] presented jammer detection algorithm for CRs. For ABD system discussed in Section I, CR network uses various features of the signals such as signal to noise ratio (SNR), traffic flow, signal modulation, packet delivery ratio (PDR), sensing threshold and signal strength (SS) to learn the behavior of the users under normal and jamming conditions [8]. In [11] authors used SS and PDR to implement ABD technique. Learning of the network is accomplished by using SS and PDR under no jamming conditions in learning phase. During the testing phase, jammer detection is done by comparing the normal and abnormal situations by using the baseline profile. In [21] authors formulated optimal power allocation scheme under jamming attacks. Jararweh $et\ al.$ [22] provided more comprehensive solution to detect jammer in the CR network. Both methods are not applicable for IoT applications because former employs many nodes to perform ON/OFF line monitoring and anomaly behavior analysis, latter uses constant jammer model which is energy-hungry. In [23], a modified Q-learning is proposed for jammer mitigation in the CR networks. In our work, we consider the amplitude and phase of the received OFDM signal rather than relying on complex features and learn the DBN model. As a result, this does not put extra burden on objects in CR-IoT network to perform spectrum sensing and features selection tasks. Moreover, learning is faster because very few objects are involved to monitor the environment.

III. System Model

The CR-IoT network based on IEEE 802.11 ah is considered for this work in which object signals are OFDM modulated. The OFDM symbols $X(k)$ which consist of N sub-carriers can be represented in time domain as

$$x(t) = \sum_{k=1}^{N} X(k) e^{j2\pi kt/N}, \tag{1}$$

the received OFDM signal can be written as

$$r(t) = h(t) \otimes x(t) + w(t), \tag{2}$$

where $h(t)$ is the channel response, $x(t)$ is transmitted signal and $w(t)$ is additive white Gaussian noise (AWGN) with zero mean and power spectral density σ_w^2.

For our proposed system which is illustrated in Fig.1, we consider reactive jammer equipped with cognitive capabilities. The jammer can detect and attack any of the sub-carrier in OFDM signal by injecting its power. Let us assume that OFDM signal consisting of $N \times M$ grid is transmitted, where N and M are the numbers of sub-carriers and symbols respectively and a jammer attacks one of the sub-carriers of the transmitted OFDM signal. At the receiver side of OFDM, FFT output is taken to form a state vector (Eq.3) for the proposed model which is explained in the end of this section. We choose FFT output due to two reasons: First, to analyze the signal statistically by using amplitude and

phase information. Second, an anti-jamming technique can be implemented to detect jammer before the signal goes to demodulation and mitigate jammer effect at this level, thus reducing receiver complexity. The perfect synchronization is assumed between transmitter and receiver, hence there is no frequency offset between OFDM symbols. For any given sub-carrier consisting of M symbols, there is temporal evaluation between consecutive symbols which allow to describe how amplitude and phase values are dynamically changing in a specific sub-carrier. Therefore, we can define the state vector at each time instant k as,

$$X_k = [\, a \; p \; \dot{a} \; \dot{p} \,] \tag{3}$$

where a, p are amplitude and phase while $\dot{a}$, $\dot{p}$ are corresponding derivatives.

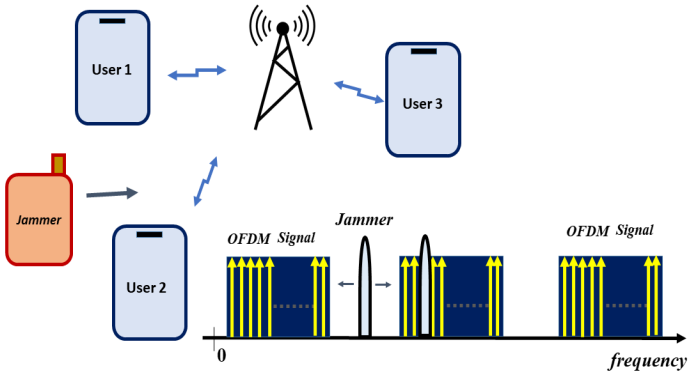

Fig. 1. Spectrum of the OFDM modulated users in CR-IoT Network while jammer tries to jam sub-carrier in the OFDM signal of the users by varying its power

IV. Proposed Method

A. Switching Dynamic Bayesian Network

After obtaining a set of state vectors describing the behaviour of the receiver in the spectrum when a normal situation (without jammer) is considered, it is proposed to learn a Switching Dynamic Bayesian Network (SDBN) model which is shown in Fig.2, for modeling and predicting the dynamical system over time. DBN enables to include dependencies between involved random variables as time evolves and also facilitates the representation of different inference levels. Consequently, here the lowest level of inference corresponds to the observed received carrier amplitude and phase Z_k. States, X_k, represent a medium inference level which encodes continuous information. Super-states S_k correspond to the top level of inference which manifest the discretization of the continuous states. 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 switching DBN, four steps are done, such that:

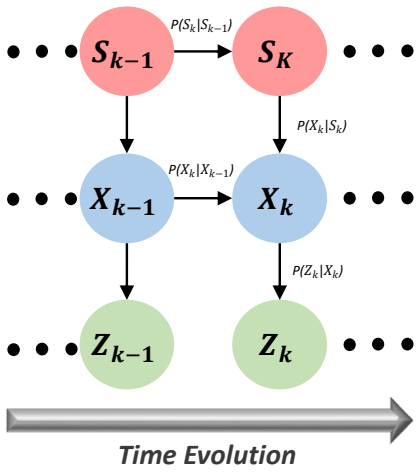

Fig. 2. Proposed DBN model comprises of two parts: (Discrete and Continuous) to detect jammer in the Spectrum

Learning superstates. To learn the superstates, we employed a SOM that receives X_k and produces a set of learned superstates $\boldsymbol{S}$ where similar information (quasi-constant derivatives) are valid, such that:

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

where $S_k \in \boldsymbol{S}$ and L is the total number of superstates.

Learn discrete transition models. By observing the activated superstate over time, it is possible to estimate a set of temporal transition matrices encoding the probabilities of passing from a current superstate to another one. Such matrices take into consideration the time spent in current superstate for encoding transition probabilities, facilitating the estimation of $P(S_k|S_{k-1}, t_k)$, where t_k encodes the time spent in the current superstate S_{k-1}.

Regions properties. A region S_k is represented by the variables ξ_{S_k}, Q_{S_k} and $\psi_{S_k^i}$ which encode the mean value, the covariance matrix of clustered states and a threshold value where linear models are valid, respectively. Such a threshold is defined in [15].

Learn continuous models. This work expresses the evolution in time of state vector based on quasi-constant derivatives models. Such type of model can be written as a function of the previously obtained regions S_k, such that:

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

where $A = [A_1 \;\; A_2]$ 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}.

To make inferences by employing the learned DBN (refer Fig.2), we proposed to use a probabilistic switching model called Markov Jump Particle filter (MJPF) [15]. Such filter uses Particle filter for inferring 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). In this work, by applying MJPF, it is possible to detect Jammer. Two abnormality measurements are defined for detecting the jammer, based on the Bhattacharrya distance between prediction $p(X_k^*|X_{k-1}^*(S_k^*))$ and

- probability of being inside the predicted superstate of particle $p(X_k^*|S_k^*)$.

$$db1 = -\ln \int \sqrt{p(X_k^*|X_{k-1}^*(S_k^*))p(X_k^*|S_k^*)}dX_k^*; \quad (7)$$

- evidence $p(z_k|X_k^*)$ to have solutions near the measurement:

$$db2 = -\ln \int \sqrt{p(X_k^*|X_{k-1}^*(S_k^*))p(Z_k|X_k^*)}dX_k^*; \quad (8)$$

where, $(.)^*$ indicates the considered particle and (S_k^*) means that the prediction depends on the superstate. The value of $db1$ relates to the similarity between prediction of the state and the likelihood to be in the predicted superstate. The value of $db2$ relates to the similarity between the state prediction and the continuous state evidence related to the new observation in each superstate.

B. Adaptive Energy Detector

Conventional Energy Detector (ED) has been the most popular spectrum sensing method used in CR due to its simplicity. It compares the signal energy with a predefined threshold to decide if the spectrum is occupied or not. Subsequently, we use adaptive version of ED in order to provide a fair comparison with the proposed DBN. The detection is based on two hypotheses:

$$H_0 : \quad r(t) = s(t) \quad (9)$$

and

$$H_1 : \quad r(t) = s^J(t) \quad (10)$$

$r(t)$ is the received OFDM symbol. H_0 represents the hypothesis of a normal situation when the symbol is not attacked, while H_1 represents the hypothesis of an abnormal situation when the jammer has attacked the symbol. The decision of H_0 and H_1 is based on a predefined threshold T compared with the energy of each received sample. The performance of the ED is evaluated based on the probability of detection (P_d) which is calculated as follows

$$P_d = P(E_{s_i} > T) \quad i = 1, 2, ..., M \quad (11)$$

where E_{s_i} is the energy of the detected symbol i. We adopt the traditional ED provided with a small memory, giving it a statistical knowledge of the symbol amplitude before and after jamming. This knowledge gives us an adaptive threshold which is able to detect the jammer. The threshold is obtained by calculating the difference values between the amplitude of the attacked symbols before and after jamming, such that,

$$D_i = ||s_i - s_i^J|| \quad (12)$$

where s_i represent the symbol before jamming and s_i^J after jamming. Accordingly, the result is a set of euclidean distance $\boldsymbol{D}$ related to the symbols under attack, such that,

$$\boldsymbol{D} = \{D_1, D_2, \ldots, D_M\}, \quad (13)$$

The threshold (T) is calculated as follows

$$T = |E(\boldsymbol{D})|^2 \quad (14)$$

Where E is the mean value of ($\boldsymbol{D}$).

V. Experimental Setup and Results

A. Data source

For our experiments, OFDM signal based on IEEE 802.11ah configurations is assumed to be under consideration. The data is generated and modulated using 16-QAM, mapped onto 64 sub-carriers, followed by cyclic prefix (CP) addition and transformed into the time domain by using IFFT. The received signal is assumed to be affected by AWGN. After CP is stripped off and FFT is performed, the output data is divided into two sets: one contains only the clean data (No jammer attack) for the training phase and the second set consists of the data affected by the jammer attack for the testing phase. The jammer attacks any of the sub-carriers in the OFDM signal according to the following scenarios.

- Scenario 0 ($Normal\ Situation$): This scenario is used to learn the DBN model as shown in Fig. 3 for the normal behavior of the CR network by applying the clean data during the training phase. The learned DBN is utilized later on the other scenarios to determine the deviations of the new behavior from the normal situation. After learning the normal situation during the $training\ phase$ we define different scenarios to test the proposed method ($testing\ phase$). The anomalies are detected based on the abnormality measurements as mentioned in section IV.
- Scenario 1 ($Single\ Jammer\ attack$): When the jammer attempts to disrupt the transmission of the primary user by attacking one symbol of the OFDM sub-carrier as shown in Fig.4.
- Scenario 2 ($Multiple\ Jammer\ attacks$): In this case, the jammer attacks different symbols of the OFDM sub-carrier, Fig.5.
- Scenario 3 ($Jammer\ attack\ with\ low\ power$): In this case, the jammer attacks single symbol of the OFDM sub-carrier with low power, Fig.6.

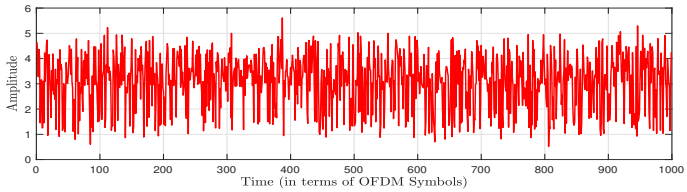

Fig. 3. Scenario 0 : Clean data (Normal Situation)

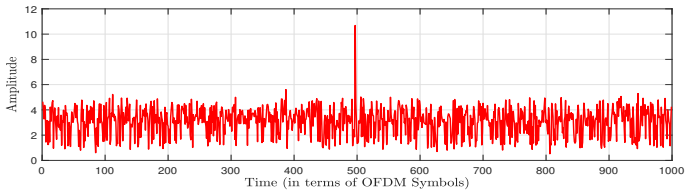

Fig. 4. Scenario 1: Single attack

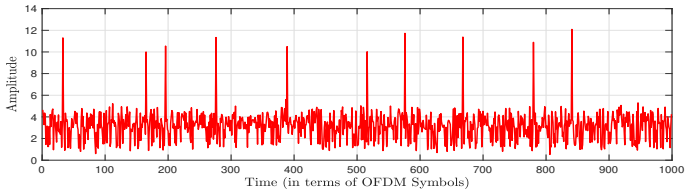

Fig. 5. Scenario 2: Multiple attacks

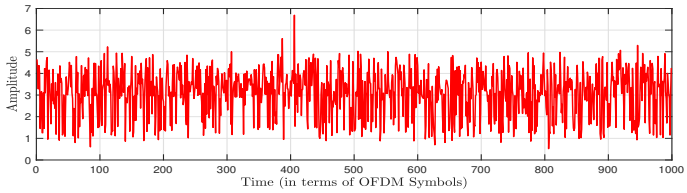

Fig. 6. Scenario 3: Single attack with low power

B. DBN Results

Here, we evaluated the performance of our DBN model under three different scenarios mentioned previously. The detection of the abnormal situation is based on a calculated threshold for each abnormality measurement.

Fig. 4 depicts the observation of scenario 1 where a single attack is present in the sub-carrier. By observing the abnormality measurements, it is possible to detect and locate the attacked symbol in that sub-carrier by comparing it with the threshold. The high peak means an abnormality and it is greater than threshold as displayed in Fig.7 and Fig.8. In this case we are able to detect the jammer at discrete and continuous levels.

In scenario 2 the jammer attacks multiple symbols. Our model is able to detect multiple attacks at discrete and continuous levels as shown in Fig. 9 and Fig. 10.

The jammer in Scenario 3 attacks one symbol with lower power. In this situation, it is possible to detect jammer only at discrete level (db1) as indicated in Fig. 11, while at continuous level (db2) our method is not able to detect the attack, Fig.12.

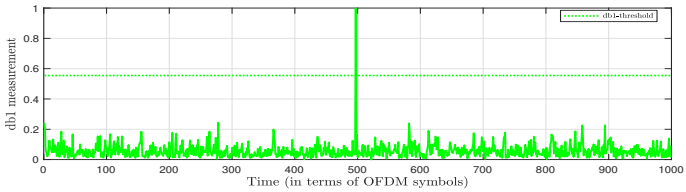

Fig. 7. Scenario 1: Abnormality measurement (db1)

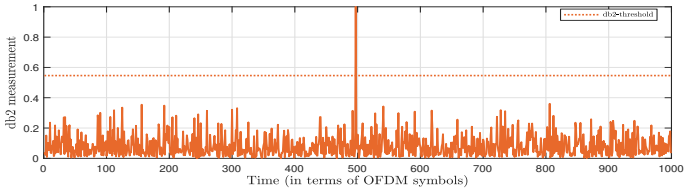

Fig. 8. Scenario 1: Abnormality measurement (db2)

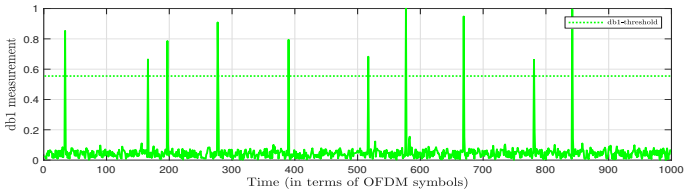

Fig. 9. Scenario 2: Abnormality measurement (db1)

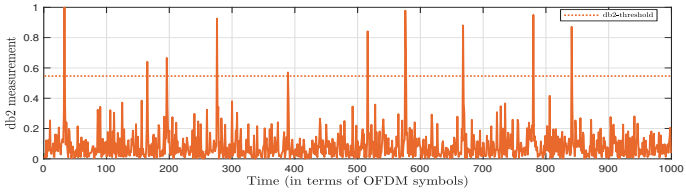

Fig. 10. Scenario 2: Abnormality measurement (db2)

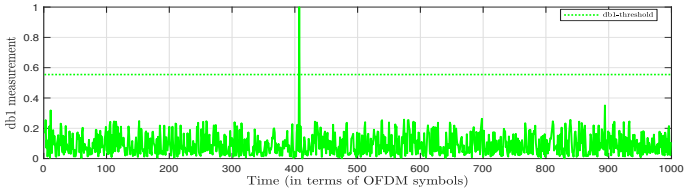

Fig. 11. Scenario 3: Abnormality measurement (db1)

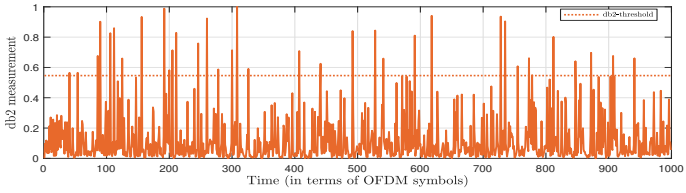

Fig. 12. Scenario 3: Abnormality measurement (db2)

C. Comparison between DBN and Adaptive ED

For ED we use the same data as for DBN in order to see the difference between the two systems. As discussed in the

previous sections, our proposed DBN model is based on a statistical analysis of the sensed sub-carrier, it can predict and estimate future states and deals with the whole OFDM symbols. On the other hand, the conventional energy detector receives signal and performs energy test statics for a given time instant. To make a fair comparison between the two systems we provided the ED with a limited memory for memorizing previous and current state (before and after an attack) of the symbol. The scenarios mentioned before are done to see how our proposed DBN perform with different situations regarding the jammer (changing its power, increasing the number of attacks). We compare the adaptive ED with DBN by plotting the Probability of detection with respect to the number of attacks. The performance of ED degrade as the

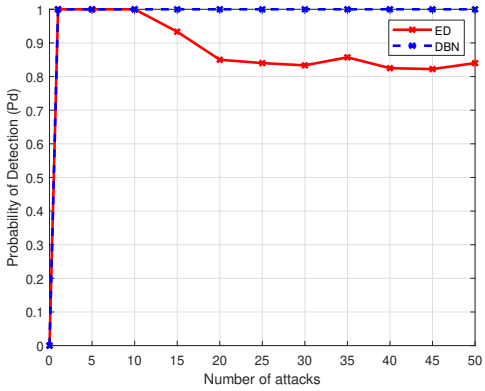

Fig. 13. Performance of ED and DBN in terms of P_d as the number of attacks increases

attacks increase where DBN is always able to detect attacks with stable performance as shown in Fig.13. The advantage of our proposed DBN model with respect to the adaptive ED is that it is able to detect and locate attacked symbol in the sub-carrier, where the adaptive ED is not apt to identify affected symbols. This is due to the fact that ED has a limited memory which allows it to sample observed symbol at a given time instant.

VI. Conclusion and Future Work

In this paper, we present a method to learn DBN model in CR-IoT network for OFDM modulated signals. The main strength of the proposed model lies in a fact that it identifies single or multiple affected symbols of OFDM sub-carrier which are attacked by jammer with either high or low power. Moreover, proposed method can be deployed in different wireless standards based on OFDM. As an extension of the future work, we will deal with multiple OFDM sub-carriers under various jammer attacks. Additionally, interaction between user and jammer will be studied to further improve the developed model by using real dataset.

References

[1] A. A. Khan, M. H. Rehmani, and A Rachedi. Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions. *IEEE Wireless Communications*, 24, 06 2017.

[2] M. Nitti, M. Murroni, M. Fadda, and L. Atzori. Exploiting Social Internet of Things Features in Cognitive Radio. *IEEE Access*, 4:9204–9212, 2016.

[3] 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*, 6:12858–12867, 2018.

[4] Y. Gao, Z. Qin, Z. Feng, Q. Zhang, O. Holland, and M. Dohler. Scalable and Reliable IoT Enabled by Dynamic Spectrum Management for M2M in LTE-A. *IEEE Internet of Things Journal*, 3(6):1135–1145, Dec 2016.

[5] F. Akhtar, M. H. Rehmani, and M. Reisslein. White space: Definitional perspectives and their role in exploiting spectrum opportunities. *Telecommunications Policy*, 40, 02 2016.

[6] H. A. Mahmoud, T. Yucek, and H. Arslan. OFDM for cognitive radio: merits and challenges. *IEEE Wireless Communications*, 16(2):6–15, April 2009.

[7] V. Banos, M. S. Afaqui, E. Lopez, and E. Garcia. Throughput and Range Characterization of IEEE 802.11ah. *IEEE Latin America Transactions*, 15(9):1621–1628, 2017.

[8] 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*, 5(3):1904–1913, June 2018.

[9] X. Tang, P. Ren, and Z. Han. Jamming Mitigation via Hierarchical Security Game for IoT Communications. *IEEE Access*, 6:5766–5779, 2018.

[10] Y. Chen, Y. Li, D. Xu, and L. Xiao. DQN-Based Power Control for IoT Transmission against Jamming. In *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, pages 1–5, June 2018.

[11] Z. M. Fadlullah, H. Nishiyama, N. Kato, and M. M. Fouda. Intrusion detection system (ids) for combating attacks against cognitive radio networks. *IEEE Network*, 27(3):51–56, May 2013.

[12] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein. Aldo: An anomaly detection framework for dynamic spectrum access networks. In *IEEE INFOCOM 2009*, pages 675–683, April 2009.

[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*, 66(4):3143–3157, 2017.

[14] S. Fayssal and S. Hariri. Anomaly-based protection approach against wireless network attacks. In *IEEE International Conference on Pervasive Services*, pages 193–195, July 2007.

[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)*, pages 2606–2613, July 2018.

[16] T. Kohonen. *Self-Organizing Maps, ser. Physics and astronomy online library*. Springer Berlin Heidelberg, 2001.

[17] A. O. F. Atya, A. Aqil, S. Singh, I. Broustis, K. Sundaresan, and S. V. Krishnamurthy. Exploiting Subcarrier Agility to Alleviate Active Jamming Attacks in Wireless Networks. *IEEE Transactions on Mobile Computing*, 14(12):2488–2501, Dec 2015.

[18] H. Rahbari and M. Krunz. Rolling Preambles: Mitigating Stealthy FO Estimation Attacks in OFDM-based 802.11 Systems. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 118–126, Oct 2016.

[19] G. Romero, V. Deniau, and E. P. Simon. Mitigation Technique to Reduce the Wi-Fi Susceptibility to Jamming Signals. In *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*, pages 1–3, May 2018.

[20] T. Nawaz, L. Marcenaro, and C. S. Regazzoni. Stealthy jammer detection algorithm for wide-band radios: A physical layer approach. In *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pages 79–83, Oct 2017.

[21] S. D'Oro, E. Ekici, and S. Palazzo. Optimal power allocation and scheduling under jamming attacks. *IEEE/ACM Transactions on Networking*, 25(3):1310–1323, June 2017.

[22] Y. Jararweh, H. A. Bany Salameh, A. Alturani, L. Tawalbeh, and H. Song. Anomaly-based framework for detecting dynamic spectrum access attacks in cognitive radio networks. *Telecommun. Syst.*, 67(2):217–229, February 2018.

[23] 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)*, pages 1–7, May 2015.