Scientific Research Publishing

Journal of Computer and Communications, 2017, 5, 27-39
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Secure Cognitive Radio Communication for Internet-of-Things: Anti-PUE Attack Based on Graph Theory

Azar Hosseini[1], Bahman Abolhassani[1], Arezoo Hosseini[2]

[1]School of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran
[2]Pardis Nasibe-Shahid Sherafat, Farhangian University, Tehran, Iran
Email: st.azar.hosseini@gmail.com, abolhassani@iust.ac.ir, a.hosseini@cfu.ac.ir

How to cite this paper: Hosseini, A., Abolhassani, B. and Hosseini, A. (2017) Secure Cognitive Radio Communication for Internet-of-Things: Anti-PUE Attack Based on Graph Theory. *Journal of Computer and Communications*, **5**, 27-39.
https://doi.org/10.4236/jcc.2017.511003

Received: August 19, 2017
Accepted: September 10, 2017
Published: September 13, 2017

Abstract

Internet of Things (IoT) paradigm with strong impact on future life will be interconnected through Cognitive Radio Networks (CRNs). CRNs with Ubiquitous trait are highly promising to achieve interference-free and on-demand services. CRs are able to sense the spectral environment, to detect unoccupied bands, and to use them for signal transmissions. This opportunity encourages malicious Users to surpass CRs by Primary User Emulation (PUE) attack and use vacant spectrums. This paper proposes an unsupervised algorithm to distinguish CRs from PUs regardless of static and mobile user. Employing K-means and graph theory are coincident in our algorithm to improve detection outcomes. The edge of graph corresponding to the relation between signals is used and the result of comparison the signal properties is exposed to different clusters. The Receiver Operating Characteristic (ROC) and Detection Error Tradeoff (DET) of our proposed algorithm prove our claim.

Keywords

IoT, PUE, K-Means, Cognitive Radio

1. Introduction

Internet of Things can provide a ubiquitous network of connected devices and intelligent sensors for smart communications, and big data analytics has the potential to enable the movement for real-time control. IoT capable objects will be interconnected through wired and wireless communication technologies. However, cost-effectiveness issues and accessibility to remote users make wireless communication as a feasible solution [1]. The continuous growth of objects and smart sensors led to emerge cognitive capabilities. This emergence may be a suitable option for mitigating the fixed spectrum allocation, the interference in different bands, accessibility problems in every place, large volumes of data collection and transmission, license costs and power consumption.

A Cognitive radio Network (CRN) is a network comprising of CR devices that are equipped with cognitive capability and reconfigurability and built on the software-defined radio (SDR) [2]. They can adjust their own transmitter parameters such as power output, frequency, modulation and identify potential impairments to communicate quality in interference, path loss, shadowing and multipath fading. A CR is an intelligent wireless communicator that learns from its radio environment and adapts its internal states for starting or not starting radio transmission depending on the absence of the PU in the band. There are four major tasks for a cognitive radio: spectrum sensing to find vacant channels, spectrum sharing, spectrum mobility and spectrum management.

Due to the aforementioned tasks, a CR requires following enabling techniques:

- Bayesian signal processing (e.g. cognitive radar with the availability of a priori information),
- Dynamic programming,
- Learning machines with feedback (e.g. neural networks),
- Game-theoretic models,
- Cross layer protocol design.

Nowadays, PU detection is performed using one of the following three methods: transmitter detection, cooperative and interference detection. Four approaches are shown in **Figure 1** for transmitter detection, based on the knowledge on the transmitter signals, which are obtained through spectrum sharing. Cooperative is one of the methods for detecting PUs, in which information from CRs are sent to a common center for decision. The third method is interference detection between transmitter and receiver. Four ways are followed to identify the Malicious User (MU) by transmitter technique: Firstly, Matched Filter [3], the received signal in matched filter is processed by prior knowledge like mod-

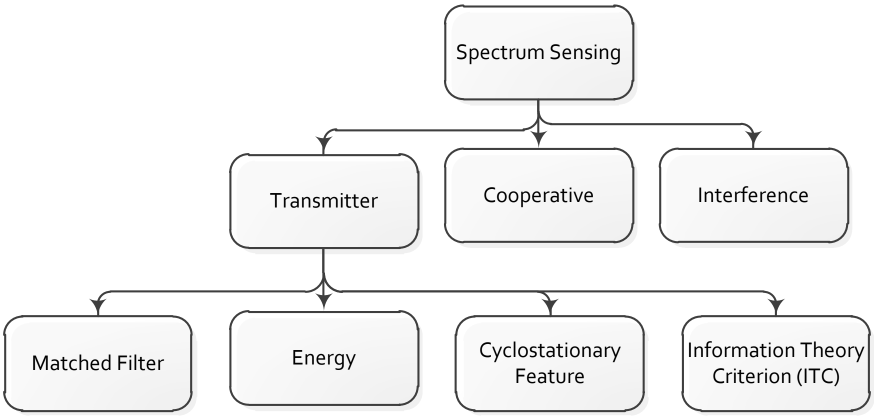

Figure 1. Spectrum Sensing techniques.

ulation. Secondly, Energy Detection [3] is highly recommended for distinguishing the known users, since unknown user utilizes various parameters which can cause errors in real signal detection such as mobility parameters and emulation attacks. Thirdly, Cyclostationary Features [3] introduce the signal features and their effects on signal processing. Finally, Information Theory Criterion (ITC) [4], which uses information theory to detect the PU transmitter. Our paper is based on feature extraction for clustering received signals to detect MUs.

Most common types of malicious user attacks are: 1) PUE attack, 2) Spectrum Sensing Data False (SSDF) [5] attack, 3) using vacant spectrum opportunity or transmitting noise in links (Jamming and Game theory), 4) secondary emulation and participating in spectrum sharing. In this scheme, we mainly focus on the security problem from PUE attacks in CRN. In this attack MUs emulate the PUs' transmitting signal and mislead the legitimate SUs to give up the spectrum band. For instance, if a MU is to be recognized as a PU, a TV broadcaster with specific modulation, rate and power, should transmit the same signal with exactly PU’s features. This scenario would not be endured for a long time because MU wants to transmit its own data and features. In recent approaches, MUs have been detected by knowing positions of other SUs and PUs, while the mobility of users makes the detection unsuccessful [6]. MU can be recognized by Feature Selection Algorithms (FSAs) like k-means and graph theory in the absence of training data.

This paper emphasizes graph theory to enhance the accuracy of clustering based on the unsupervised learning methods, while MUs’ traits lead to misclustering.

The remainder of this paper is organized as follows. Section 2 describes the K-means algorithm and its challenges for detecting MU. In Section 3, Graph theory is discussed. Section 4 introduces the dependence of signals and then details of the proposed algorithm are explained in Section 5. In Section 6, we survey the accuracy of the proposed algorithm to recognize a malicious user. In Section 7, we analytically evaluate the performance of the K-means method, and our proposed algorithm. Summary of the work and conclusions are presented in Section 8.

2. Enhanced K-Means Algorithm

Suppose that sparse points as delivered signals which may belong to PUs, SUs or MUs are scattered in one cluster. They have their own features such as power, mean, kurtosis of signals, or kurtosis of d/dt of signals, *rms* value, autocorrelation, which can be used for clustering process. For clustering received signals in a three dimensional space, three features can be employed.

One of the renowned clustering algorithms is k-means. It assigns a signal to a cluster whose center has the minimum distance from the object. The distance is calculated between received signals based on features which have been introduced on each axis. For instance, k-means algorithm considers *rms* values of each received signal denoted by rms_s for clustering them. Imagine that it declares the rms values of cluster centers by rms_n $n = 1, 2, \cdots, N$, then it should solve the following problem:

$$n_{opt} = \text{find}\left[\min_{n} \left| rms_s - rms_n \right|\right] \tag{1}$$

In the Equation (1), n_{opt} is the minimum distance among every two distances between two rms values. So, k-means algorithm assigns the received signal to cluster n_{opt}. This procedure is done for any received signal and it is assumed that the features (e.g. rms value) of cluster centers are known by k-means algorithm.

Noise, interference and Rayleigh fading channel may change features of the received signal. To combat this problem, we propose that k-means employs randomly three features of the received signal and find its distance from the three corresponding features of the cluster centers, then decides to which cluster the signal should be assigned. Figure 2 presents clustering of I = 30 received signals into N = 3 clusters, using three features: kurtosis of square of signal, kurtosis of d/dt of the signal, and autocorrelation of the signal [7]. In this example, PUn signal is BPSK, 16QAM and GMSK for n = 1, 2, 3, respectively. Cluster centers are shown by "o" in the Figure 2.

As stated by three features, all other kinds of received signals can be clustered. If one of these features causes the same value between clusters, this feature will be replaced randomly with other features of the signal. This procedure may be repeated a number of times until a received signal clustered into one of existing clusters.

3. Graph Theory

Wide range of wireless standards and relevant devices to communicate in IoT environment [8] can cause complexity in calculation and performance reduc-

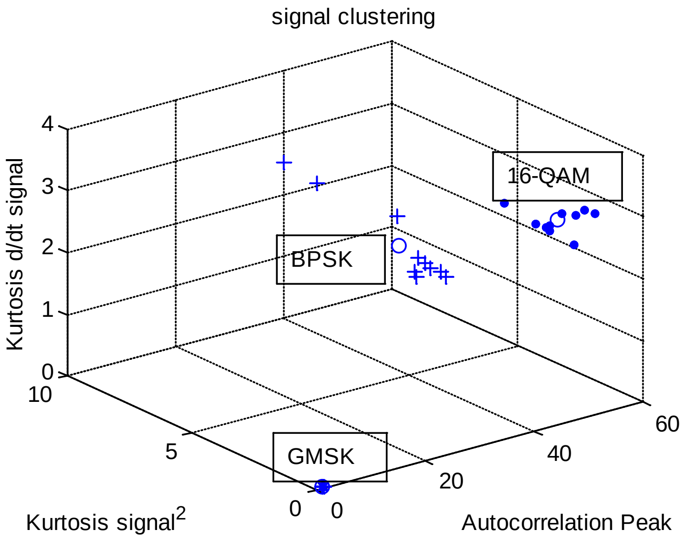

Figure 2. K-means clustering exhibition of signals with three modulations, cluster centers are shown by blue "o".

tion. To fix this problem we present a new pattern detection method based on the graph theory to distinct area like bipartite graph [9] and establish proper background to manage the influx of signals with diverse aspects in modulation and traits. A graph $G(v\varepsilon)$ is called bipartite while vertices v can be partitioned into N disjoint modulations with $\bigcup_{n=1}^{N} SIG_n = v$, and the edge set ε connect vertices from one to another modulation. Each cluster can construct its own features based on eliciting information from received signal. Let I'_n denotes the number of signals belonging to cluster n. Assume that cluster n collects the set of channels from all CRs in I'_n. Then, it can declare a bipartite graph, $G_n\left(\bigcup_{i_n=1}^{I'_n} sig_{i_n}, \bigcup_{j=n+1}^{N} \varepsilon_{i_{nj}}\right)$, which represents the relation between channels (**Figure 3**). An edge $\varepsilon_{12}\left(=\left(sig_{I_1}, sig_{I_2}\right); \varepsilon_{12} = \varepsilon_{21}\right)$ exists between a vertex sig_{i_1} (ЄSIG1) and a vertex sig_{i_2} (ЄSIG2). SIG1 is the set of I'_1 signals that belong to cluster "1" ($SIG_1 = \bigcup_{i_1=1}^{I'_1} sig_{i_1}$) and SIG2 is the set of I'_2 signals that belong to cluster "2" ($SIG_2 = \bigcup_{i_2=1}^{I'_2} sig_{i_2}$). Next section is focused on the edge ε as the relevance of signals.

We consider three standard modulations, namely, BPSK, 16-QAM and GMSK, but any other modulation can be easily included in the scheme. These modulations are representative of CDMA, WiFi and GPRS IoT standards respectively. Other related standards as well as their application in internet of things are exposed in **Table 1**.

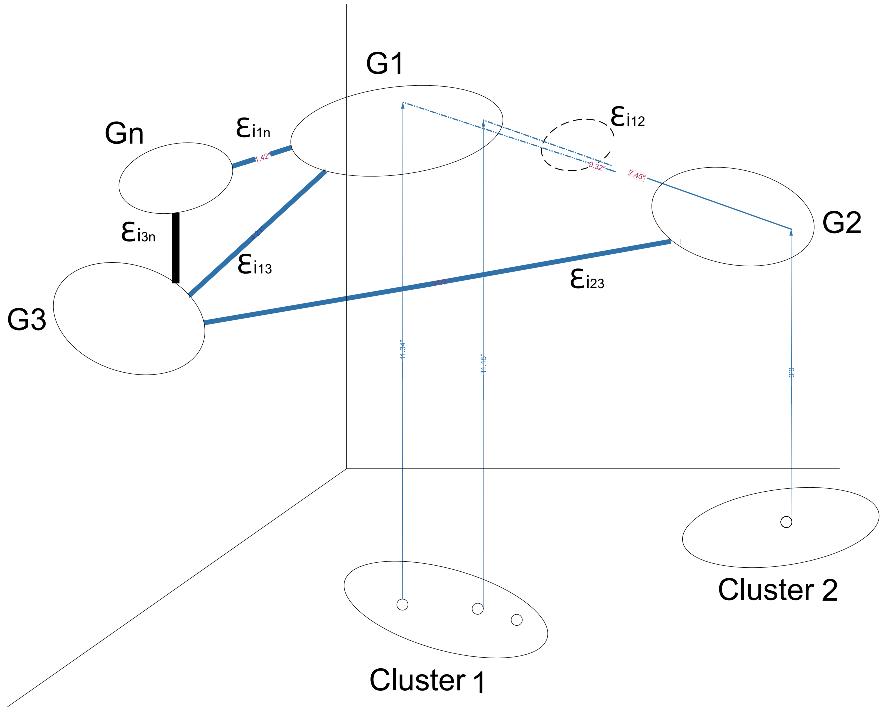

Figure 3. Graph-based representation between corresponding clusters.

Table 1. Application of modulations in IoT.

Proposed Modulations	Applications in IoT		
	Modulation	Standard/Protocol	Application areas in IoT
	BPSK	• CDMA • WiMAX (16d, 16e) • WLAN 11a, 11b, 11g, 11n • Satellite • DVB • Cable modem	To transmit the essential information of systems and low speed communication systems [8]
	16QAM	• Low power wide area network • WiFi • WiGi • TV white space	• digital terrestrial television using DVB-Digital Video Broadcasting • land mobile communications • envelopment (DOE) technique • LTE modes
	GMSK	• Positive Train Control • Wireless M-bus	EC-GPRS

4. Signals Relevance

The continuous growth of incoming signals means a continuous growth of features. Besides mentioned features which have been implied earlier, some other features like carrier frequency, signal bandwidth, symbol rate, modulation scheme and propagation channel exist as extra features of unknown incoming signals and channels. Increasing these features to the calculation led us to exceedingly complicated analysis. Hence, these recent features are ignored in “blind” channel modeling to cluster signals. In previous section, we discussed about edgeε that shows the relevance of two points and consequently relation between two clusters. In this paper, we use common features between two signals like signal to noise amplitude ratio (SNAR), bit error rate (BER) and others that shown in Table 2 as signals relevance.

According to the Figure 3, every two signals may have common area which called signal relevance. Good exemplar of this relationship could include signal to interference plus noise ratio (SINR), SNAR, BER, power, data rate, and others in Table 2. A few of these signal relevance are listed in the first column of this Table. For instance, two signals by their own mean (μ) and standard deviation (σ) have common value like SNAR that is calculated at second column in second line. On the other hand, SNAR may be related to the other signal relevance such as BER. Therefore BER can be calculated by SNAR which inserted in third column as Relation. To sum it up the third column is the result of relation between previous signal relevance. These computations with details in deeply manner about relationships can amend the discernment of clustering and mitigate suspicious analyses.

SNAR, BER and Power features can be used for the initial calculation and seeking the degree of membership.

Table 2. Ratio features and their relevance.

Ratios	Relevance		
	Typical signals relevance	Formula	Relation
	SINR	$\frac{T_0 \cdot c}{N + \sum_i I_i}$	BER, FER
	SNAR	$\frac{\mu_1 + \mu_2}{\sigma_1 + \sigma_2}$	BER
	BER	$0.5 \times erfc\left(sqrt\left(10 \wedge \left(\frac{\mu_1 + \mu_2}{20(\sigma_1 + \sigma_2)}\right)\right)\right)$	SNAR
		$Q\left(\sqrt{E(SINR_K)_\infty}\right)$	SINR
	Occupied Bandwidth	$R_S \cdot K(1+\alpha)$	S$_{\text{eff}}$, BER, Power, SINR, Data Rate
	Spectral Efficiency (S$_{\text{eff}}$)	$\frac{K}{K(1+\alpha)}$	Occupied Bandwidth, Power
	Frame Error Rate (FER)	$FER \le \sum_{m=t+1}^{n_{FEC}} \binom{n}{m} \mathrm{Pe}^m (1-P)^{n-m}$	SINR, Power
	Power	$\int \lvert Signal \rvert^2 \mathrm{d}t$	SINR
	Data Rate	$R_S \cdot K\left(\frac{K_{FEC}}{n_{FEC}}\right) \cdot \left(\frac{T_{TX}}{T_{TX} + T_{RX}}\right) \cdot \left(\frac{L}{L_{\max}}\right)$	Power, S$_{\text{eff}}$

R_S: Symbol Rate; T_0: Symbol Period ($1/R_S$); K: number of bits per symbol ($\log_2^M$); α: pulse shape filter roll-off factor (in this scheme, α = 0.5); $\frac{T_{TX}}{T_{RX}}$: amount of transmitting time to receiving in a TDD sys; $\frac{L}{L_{\max}}$: the number of bytes to maximum bytes in a packet; N: Noise Power; m: modulation order; c: carrier power; μ_i: the mean of signal i; σ_i: standard deviation of signal i.

5. Proposed Algorithm

Advent of cognition ability will change the future of communications. And bring new requirements of sources. The most proportion of sources will be allocated to data storage and data analyzing. These two factors should be handled by optimized algorithm of analyzing and organized information like that described in.

Machine learning and associated branches have a significant role in computing. In this paper, we try to step into optimal modes to reduce the adventure of sophisticated analyzing and heighten the accuracy of malicious detection by k-means clustering. K-means restricted to distance and threshold radius of cluster. But our algorithm by exhibiting a new way tried to escape from k-means' restrictions and its imprecise clustering. Initially, it alludes to thirteen features of signal which encompass Mean, The Standard Deviation (StdDev), Variance-Covariance (VAR), Kurtosis, Kurtosis of Square signal, Kurtosis of Derivation of signal, Skewness, Power, Average Power, StdDev of amplitude, StdDev of angle, Max Autocorrelation of signal and StdDev of absolute value of Phase change (StdDev_abs_PhaseChange). These features are momentous for stochastic chosen name for each axis which their impact have been explained in Section 2. First of all it uses Euclidian metrics (**Figure 4**) to follow k-means rule until facing

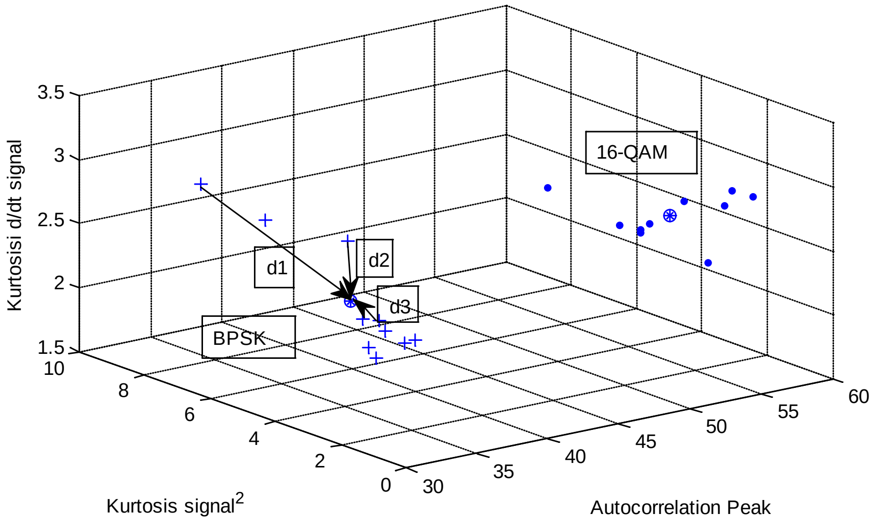

Figure 4. Defined distance between points and average in one cluster.

with inefficient measure of the distance criterion. Then, the procedure switches to compare the signal features and relevant features respectively. Aforementioned argument the Power of unknown signal will be compared with the average power of nearest cluster as a second stage. Third step dedicated to utilize the comparative features such as Signal-to-Noise Amplitude Ratio (SNAR) and Bit Error Rate (BER) and exploit their privileges to determine malicious user (extra explanation brought in Sections 3 and 4).

6. Verifying the Proposed Algorithm

Our algorithm attempts to discover patterns of malicious users. In this section we try to confirm whether this algorithm reflects the properties of MUs. The ROC curve is a fundamental tool for evaluating the algorithm's result. In a ROC curve the true positive rate is plotted in function of false rate for different cut-off points. Each possible cut-off point represents the discrimination between malicious cases and normal cases, there will be some cases with the malicious correctly detected as positive (TP = True Positive), but some cases with the malicious will be detected negative (FN = False Negative). On the other hand, some cases without the malicious will be correctly detected as negative (TN = True Negative), but some cases without the malicious will be detected as positive (FP = False Positive).

Our assumption about TN, FP, TP and FN is defined as follows:

$$\text{TN} := \sum_{n=1}^{N} P_n\left(Tr\middle|L\right) = \sum_{n=1}^{N} P\left(N'_{nn}\right) - \sum_{n=1}^{N}\sum_{q=n+1}^{N} P\left(N'_{nq}\right)\cdot P\left(N'_{qn}\right) \tag{2}$$

In Equation (2), L presents legal point and *Tr* is a representative of the threatening point. Each point falls into two categories, firstly, legal affiliation to CR, secondly, dependence on malicious users. Both of aspects have at least one acceptance value for signals relevance.

$P\left(N'_{nn}\right)$ is the probability of threatening points for cluster n and $P\left(N'_{nq}\right)$ is the probability of threatening points of cluster n for cluster q. These probabilities can be calculated with following equations:

$$P\left(N'_{nn}\right)=\frac{N'_{nn}}{I'_n};\quad P\left(N'_{nq}\right)=\frac{N'_{nq}}{I'_n};\quad P\left(N'_{qn}\right)=\frac{N'_{qn}}{I'_q}$$

$$\begin{aligned}\mathrm{FP}:=\sum_{n=1}^{N}P_n\left(L\middle|Tr\right)=\sum_{n=1}^{N}\left\{\left(\sum_{n=1}^{N}1-\left[P\left(N'_{nn}\right)+\prod_{q=1,q\neq n}^{N}P\left(N'_{nq}\right)\right]\right)\right.\\ \left.-\sum_{n=1}^{N}\sum_{q=n+1}^{N}1-\left[P\left(N'_{nq}\right)\cdot P\left(N'_{qn}\right)\right]\right\}\end{aligned}\tag{3}$$

$$\mathrm{TP}:=\sum_{n=1}^{N}P_n\left(Tr\middle|\neg L\right)=\frac{\sum_{n=1}^{N}\sum_{q=n+1}^{N}N'_{nq}}{SIG};\quad SIG=\sum_{n=1}^{N}card\left(\left[Sig_n\right]\right)\tag{4}$$

Finally, False Negative fraction:

$$\mathrm{FN}:=\sum_{n=1}^{N}P_n\left(L\middle|\neg Tr\right)=\frac{\sum_{n=1}^{N}1-P\left(N'_{nn}\right)}{SIG}\tag{5}$$

Figure 4 exhibits group of points according to their modulation on three-dimensional coordinate axes (accidentally chosen features) to clarify threatening point. Each group of points has own average which far from other points. If these distances have been introduced by average distance (dn) we can choose threatening point which is farther than dn.

To verify this idea, a point should be compared with others in Power, SNAR, BER, SINR and other signals relevance like what was stated in **Algorithm 1**.

7. Simulation Results

We generate 100 random signals corresponding to 100 trials for three clusters with three modulations, BPSK, 16QAM and GMSK. While the properties of these signals are: 1) $\alpha = 0.5$, 2) $R_s = 256$ kb/s for one level modulation, 3) $E_b/N_0 = 10$ and AWGN fading channel with 320 max doppler frequency. The ROC curve describes the detection performance of proposed and k-means algorithm. As can be seen from **Figure 5**, Proposed bipartite graph moved cut-off point (blue circle point) from (79, 21) to (83, 17). Validation results in this point show that proposed algorithm can detect PUE attack nearly 15 percent more efficient than the traditional K-means.

Two types of errors may be occurred during detection process. The first type is related to inaccurate sense occupied bandwidth by CR when PU is present. In this case, the subsequent transmissions of CRs will cause interference to the PU. The second type arises from inaccurate sense occupied bandwidth by CR when PU is absent. In addition to exploiting the transmission opportunities and use spectrum more efficiently, the cognitive structure needs to minimize the risk of malicious activities and restrict the probability of incorrect attack detection.

Algorithm 1. Malicious detection.

```
1) Input $\text{mod}_1, \text{mod}_2, \cdots, \text{mod}_N$ ; $N$ is the number of modulations
2) Input $sig_i$ ; $1 \le i \le q$
3) $\text{mod} = \{\text{mod}_1, \text{mod}_2, \cdots, \text{mod}_N\}$
4) Acquire $f_j$ ; $1 \le j \le 13$ for $sig_i$ and $feat^{13} = \{f_1, f_2, \cdots, f_{13}\}$ ; ( $f_j$ is signal feature).
5) Choose three random elements of $feat^{13}$ and assign them to $sig'_i$ .
   $$sig'_i = [f_t, f_h, f_p] ;\ t, h, p \in \{1, 2, \cdots, 13\}$$
6) Plot $sig'_i = [f_t, f_h, f_p]$ in 3D
7) Apply k-means clustering ($k$=$N$) for $sig_i$ ; $1 \le i \le q$
8) $[sig_i]$ is $i^{th}$ cluster and assume $I'_i = card([sig_i])$
9) $c_n = center[sig_n]$ ; $1 \le n \le N$
10) $d_n = \frac{1}{I'_i} \sum_{i=1}^{I'_i} |sig_i - C_n|$ ; $sig_i \in [sig_n]$
11) Receive $sig_{i+1}$ and do stage 4 to 6 then continue.
12) $d_{(i+1,n)} = \{|sig_{i+1} - c_n|, 1 \le n \le N\}$ and $T = \{d_{(i+1,1)}, \cdots, d_{(i+1,N)}\}$
13) $T_m = \min\{d_{(i+1,n)}, 1 \le n \le N\}$ , there exist $m$ , $1 \le m \le N$ such that $T_m \equiv d_{(i+1,m)}$
14) $T^m = \{d_{(i+1,n)} | 1 \le n \le N, n \ne m\}$ ; while $d_{(i+1,m)}$ is omitted.
15) If $d_{(i+1,m)} \le d_m$ thus $sig_{i+1} \in [sig_m]$ then go to stage 28.
16) Else compute the average power of $m^{th}$ cluster ( $P_m$ ) and $P_{i+1}$ as the power of $sig_{i+1}$ .
17) If $P_{i+1} \le P_m$ thus $sig_{i+1} \in [sig_m]$ then go to stage 28.
18) Else Calculate the average SNAR of cluster m,
   $$SNAR_m = \frac{1}{I'_m} \sum_{i=2}^{I'_m} \frac{\mu_{sig_{(i-1)m}} + \mu_{sig_{im}}}{\sigma_{sig_{(i-1)m}} + \sigma_{sig_{im}}}$$
   $\mu_{sig_{(i-1)m}}$ is the Mean and $\sigma_{sig_{(i-1)m}}$ is the Standard Deviation of $(i-1)^{th}$ signal from cluster m respectively.
19) Compute the average SNAR of $sig_{i+1}$ ,
   $$SNAR_{(i+1,m)} = \frac{1}{I'_m} \sum_{i=1}^{I'_m} \frac{\mu_{sig_{i+1}} + \mu_{sig_{(i+1,m)}}}{\sigma_{sig_{i+1}} + \sigma_{sig_{(i+1,m)}}}$$
20) If $SNAR_{(i+1,m)} \le SNAR_m$ thus $sig_{i+1} \in [sig_m]$ then go to stage 28.
21) Else calculate the average BER of cluster m,
   $$BER_m = \frac{1}{I'_m} \sum_{i=2}^{I'_m} 0.5 \times erfc\left( sqrt\left( 10 \wedge \left( \frac{\mu_{sig_{(i-1)m}} + \mu_{sig_{im}}}{20\left(\sigma_{sig_{(i-1)m}} + \sigma_{sig_{im}}\right)} \right) \right) \right)$$
22) $$BER_{(i+1,m)} = \frac{1}{I'_m} \sum_{i=1}^{I'_m} 0.5 \times erfc\left( sqrt\left( 10 \wedge \left( \frac{\mu_{sig_{i+1}} + \mu_{sig_{(i+1)m}}}{20\left(\sigma_{sig_{i+1}} + \sigma_{sig_{(i+1)m}}\right)} \right) \right) \right)$$
23) If $BER_{(i+1,m)} \le BER_m$ thus $sig_{i+1} \in [sig_m]$ then go to stage 28.
24) Else $T_m = \min(T^m) = \min\{d_{(i+1,n)} | 1 \le n \le N, n \ne m\}$ , there exist $1 \le m \le N-1$ such that $T_m = d_{(i+1,m)}$
25) If $T^m = \phi$ then go to stage 27.
26) Else go to stage 15.
27) Announce $sig_{i+1}$ is a malicious user.
28) Input another signal $sig_{i+1}$ = SIG go to stage 11.
```

An alternative to the ROC curve is the Detection Error Tradeoff (DET) graph, which plots the false negative rate (missed detections) vs. the false positive rate (false alarms) on non-linearly transformed x- and y-axes. Figure 6 demonstrates

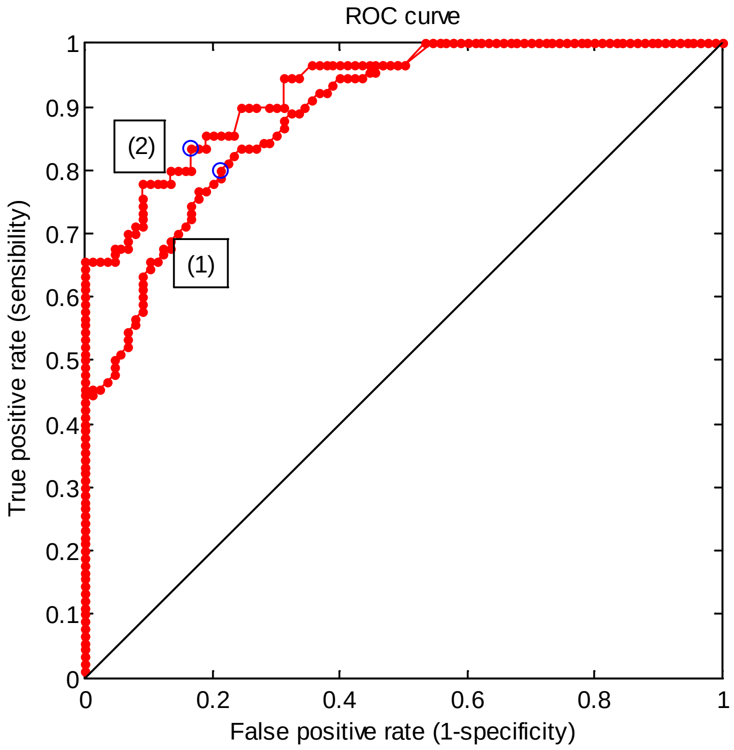

Figure 5. ROC curve for K-means Algorithm (1) and proposed Algorithm (2).

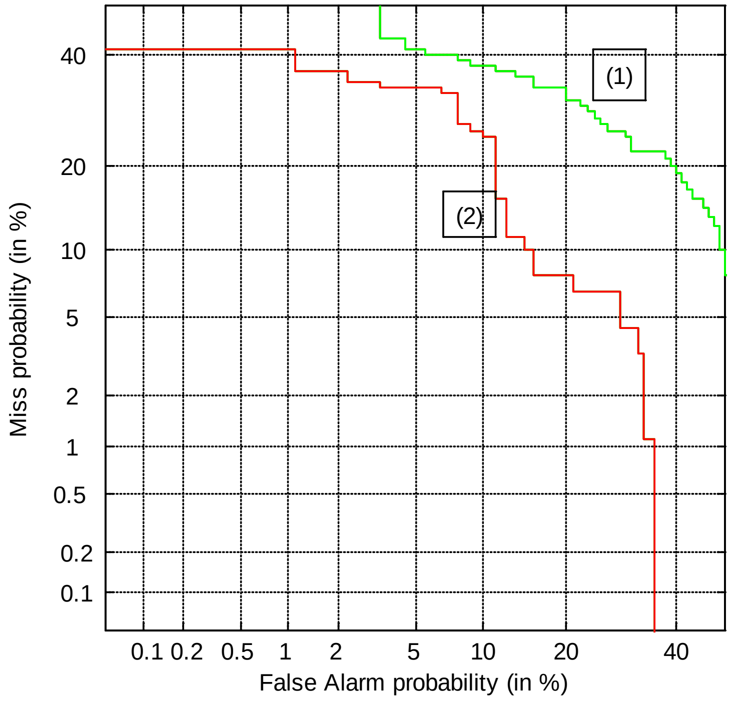

Figure 6. DET graph for K-means Algorithm (1) and proposed Algorithm (2).

that the proposed algorithm can identify malicious user with lower error probability in detection.

8. Conclusion

The new field of unsupervised learning in cognitive radios with a special emphasis on unique aspect of these radios-spectrum sensing provides novel opportunities to cluster. We strengthen the accuracy clustering while a malicious user wants to be a PU and opportunistically occupies licensed bandwidth. As claimed by the rules of graph-based, the edge of each cluster is defined by the relation between signals (Table 1). In each iteration or adding new signal as a point, besides comparison the distance between a point and the center of clusters, the value of signal properties like SNAR, BER and etc. should be compared with other points simultaneously. Despite highly accuracy, cognitive system may encounter data flood during reconfiguration. This problem has a fundamental role in operation phase and causes utilizing elaborate data center or separate layer for analyzing data and algorithm. The future research of this paper can focuses on optimizing algorithm and accelerating procedure.

Acknowledgements

This work was partially funded by *Iran Telecom* Research Center (*ITRC*) and Iran University of Science and Technology (IUST).

References

[1] Khan, A.A. (2016) When Cognitive Radio Meets the Internet of Things? *Wireless Communications and Mobile Computing Conference* (*IWCMC*), 2376-6506. https://doi.org/10.1109/IWCMC.2016.7577103

[2] Xiao, S., *et al.* (2009) Tamper Resistance for Software Defined Radio Software. *The* 33*rd Annual IEEE International Computer Software and Applications Conference* (*COMPSAC* 2009). https://doi.org/10.1109/COMPSAC.2009.58

[3] Hu, H. (2009) Cyclostationary Approach to Signal Detection and Classification in Cognitive Radio Systems. 5*th Chapter of Cognitive Radio Systems Edited by Wei Wang*, 51-76. https://doi.org/10.5772/7840

[4] Giorgetti, A., *et al.* (2011) Spectrum Holes Detection by Information Theoretic Criteria. 4*th International Conference on Cognitive Radio and Advanced Spectrum Management*, No. 66. https://doi.org/10.1145/2093256.2093322

[5] Hyder, C.S., *et al.* (2011) Defense against Spectrum Sensing Data Falsi Cation Attacks in Cognitive Radio Networks. *IEEE Transactions*, **59**, 774-786. https://doi.org/10.1109/TSP.2010.2091277

[6] Huang, L., *et al.* (2010) Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks. *IEEE International Conference on Communications and Mobile Computing*. https://doi.org/10.1109/CMC.2010.26

[7] Clancy, T.C., *et al.* (2011) Robust Signal Classification Using Unsupervised Learning. *IEEE Transaction on Wireless Communication*, **10**, 1289-1299. https://doi.org/10.1109/TWC.2011.030311.101137

[8] Khan, A.A. (2015) Cognitive Radio for Smart Grids: Survey of Architectures, Spec-

trum Sensing Mechanisms, and Networking Protocols*. IEEE Communications Surveys & Tutorials*, **18**, 860-898.

[9] Bradonjic, M. and Lazos, L. (2012) Graph-Based Criteria for Spectrum-Aware Clustering in Cognitive Radio Networks. *Elsevier Ad Hoc Networks*, **10**, 75-94. https://doi.org/10.1016/j.adhoc.2011.05.009