AN ENERGY HARVESTED COGNITIVE NETWORK COMBINING COOPERATIVE SENSING AND SAP ATTACK ANALYSIS

V.P.SONA, PG SCHOLAR
DEPARTMENT OF INFORMATION TECHNOLOGY,
PSNA COLLEGE OF ENGINEERING AND
TECHNOLOGY.DINDIGUL, INDIA
sonavpandian@gmail.com

K.SELVARAJ, ASSOCIATE PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
PSNA COLLEGE OF ENGINEERING AND
TECHNOLOGY DINDIGUL,INDIA
kselvaraj@psnacet.edu.in

Abstract-Cognitive Radio (CR) innovation is utilized for future remote range portion to enhance the utilization of the authorized groups. Primary User Emulation (PUE) is one of the discovered attacks for CR networks. Primary User Emulation (PUE) attack means that an attacker sends primary-user-like signals during the spectrum sensing period such that honest secondary users leave the corresponding channels, which causes a serious threat to cognitive radio systems. It significantly increases the spectrum access failure probability. This deft range access by the optional clients manages a consistent settling on of choices to decide when to detect the essential direct with a specific end goal to identify the condition of essential action. The optional task is constantly obliged by the requirement for shielding the essential client from obstruction and furthermore by vitality restrictions. The end goal to plan Energy Efficient and Energy Harvesting (EEH) Cooperative Spectrum Sensing (EEH-CSS), fundamental constraints must be considered: 1) Two main practical protocols are proposed in the literature namely; Time Switching (TS) protocol and Power Splitting (PS) protocol 2) Energy Half-Duplex (EHD) constraint which prevents the batteries from charging and discharging at the same time,3) Heterogeneous cooperative spectrum sensing model , and to propose a novel PUE detection system, termed Signal activity Pattern Acquisition and Reconstruction System (SPARS).

Keywords CR, PUE, EEH, EEH-CSS, TS, PS, EHD, SPARS

I.INTRODUCTION

Current data networking technology limits a network’s ability to adapt, often resulting in sub-optimal performance. Limited in state, scope and response mechanisms, the network elements (consisting of nodes, protocol layers, policies and behaviors) are unable to make intelligent adaptations. Communication of network state information is stifled by the layered protocol architecture, making individual elements unaware of the network status experienced by other elements. Any response that an element may make to network stimuli can only be made inside of its limited scope. The adaptations that are performed are typically reactive, taking place after a problem has occurred. According to the FCC (Federal Communications Commission) recent report on spectrum utilization, measurement data shows that licensed frequency bands are heavily under-utilized. As a way of making more efficient use of the limited frequency resource, researchers have been studying cognitive radios, devices that can adapt their operating characteristics to the channel condition, as a candidate for secondary spectrum access. A cognitive radio is a wireless communication device that intelligently utilizes any available side information about the (a) activity, (b) channel conditions, (c) encoding strategies or (d) transmitted data sequences of primary users with which it shares the spectrum. In light of the kind of accessible system side data alongside the administrative limitations, optional clients look to underlay, overlay, or join their signs with those of essential clients without fundamentally affecting these clients. In the next section we describe these different cognitive radio paradigms in more detail. The fundamental capacity limits for each of these paradigms are discussed in later sections.

Cognitive Radio Network Paradigms

There are three main psychological feature radio network paradigms underlay, overlay, and interweave. The underlay paradigm permits secondary users to control if the interference they cause to primary users is below a given threshold or meets a given sure on primary user performance degradation. In overlay systems the secondary users overhear the transmissions of the first users, and then use this information along with refined signal process and coding techniques to take care of or improve the performance of primary users, whereas also getting some further information measure for their own communication. Under the ideal conditions, subtle encryption and decryption ways permit each of the secondary and first users to get rid of all or a part of the interference caused by different users. In interweaving systems, the secondary users observe the absence of primary user signals in area, time, or frequency, and opportunistically communicate throughout these absences. For each of the three ideal models, if there are numerous auxiliary clients then these clients must share data transfer capacity among themselves and additionally with the essential clients, subject to their given intellectual worldview. This offers to ascend the Medium Access Control (MAC) issue among auxiliary clients like what emerges among clients in customary remote systems. Given this likeness, MAC conventions that have been proposed for optional clients inside a specific worldview are regularly gotten from traditional MAC conventions. Furthermore, various auxiliary clients may transmit to a solitary optional recipient, as in the uplink of a cell or satellite framework, and one optional client may transmit to different auxiliary beneficiaries, as in the comparing downlink. The underlay paradigm appeared in Figure1.1 orders that simultaneous essential and optional transmissions may happen just if the impedance created by the auxiliary transmitters at the essential recipients is beneath some satisfactory limit. Instead of deciding the correct impedance it causes, an optional client can spread its flag over a wide transfer speed with the end goal that the obstruction control phantom thickness is beneath the clamor floor at any essential client area. These spread signs are then dispread at every one of their planned optional recipients. This spreading procedure is the premise of both spread range and ultra wideband (UWB) correspondence. On the other hand, the optional transmitter can be extremely moderate in its yield energy to guarantee that its flag stays underneath the recommended obstruction edge.

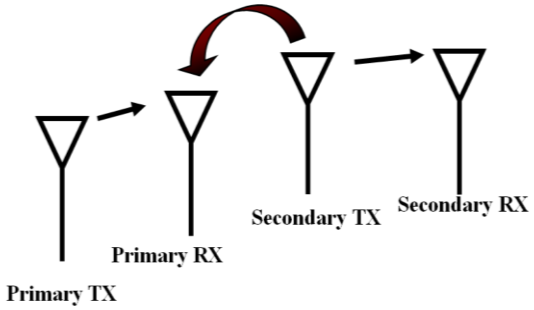


Fig:1.1 Underlay Paradigm

II.RELATED WORKS

Using Sybil Identities for Primary User Emulation and Byzantine Attacks in DSA Networks

The new kind of denial of service attack in dynamic spectrum access networks – Sybil enabled attack. During this attack, the assaulter not solely launches the Primary User Emulation (PUE) attacks however conjointly creates and infiltrates multiple Sybil identities to compromise the choice creating method of the secondary network via Byzantine attacks. We additionally investigate the ideal assault technique from the point of view of the malignant aggressor, i.e., the ideal allotment of Sybil interfaces for various assaults[12], to boost the effect on the optional system. The assault models are broke down under two distinct situations: with also, without a reputation mechanism in the system combination focus.

Hybrid Energy Harvesting-Based Cooperative Spectrum Sensing and Access in Heterogeneous Cognitive Radio Networks

A hybrid energy harvesting SU (EH-SU) model which can harvest energy from both renewable sources, e.g., solar, and ambient radio frequency signals. A heterogeneous EEH CSS scheme is first proposed to handle EH-SUs with non-identical harvesting, sensing, and reporting characteristics by permitting them to sense and report at different sensing accuracy. Formulating the energy state evolution of EH-SUs with and without EHD constraint, we analyze the asymptotic activity behavior of a single EH-SU by deriving the theoretical upper bound for the chance of being active to sense and transmit[19]. Thereafter, we develop a convex framework to find maximum achievable total throughput by optimizing the asymptotic active probability, sensing duration, and detection threshold of each SU subject to above constraints.

Dogfight in Spectrum: Combating Primary User Emulation Attacks in Cognitive Radio Systems, Part I: Known Channel Statistics

The diversion between protecting optional user(s) and an aggressor in a multichannel psychological radio framework has been demonstrated as a dogfight game diversion in range. For the single assailant and single optional client case in a solitary round, It displayed the dogfight in range as a zero-sum game and have gotten the Nash unique equilibrium, as well as the Anti Jamming Efficiency[11]. For the instance of different auxiliary clients, we have examined the Nash equilibrium for the two instances of decentralized and concentrated controls. The connected structure of Partially Observable Markov Decision Process (POMDP) to the instance of multi-arrange dogfight by settling the guard methodology of optional client.

Defense against Primary User Emulation Attacks Using Belief Propagation of Location Information in Cognitive Radio Networks

The Belief Propagation (BP) based protection technique against PUE assault is utilized as a part of CR networks. Each auxiliary client ascertains the nearby capacities in light of RSS estimations, figures the messages, trades messages with the neighboring clients, and figures the convictions until merging. At that point, the PUE attacker will be identified by the mean of the final beliefs in view of a belief threshold[13]. At last, all the optional clients in the system will be advised about the qualities of the attackers signal, and maintain a strategic distance from the aggressors essential imitating motion later on. It demonstrates the proposed system focalizes quick, even in extensive scale systems, furthermore, it is extremely successful and proficient to distinguish the PUE attacker**.**

Online Learning-Based Optimal Primary User Emulation Attacks in Cognitive Radio Networks

To learn the optimal PUE attack methodologies with no earlier information on the essential client movement attributes and the optional client get to methodologies. To define the issue as a non-stochastic web based learning issue where the attackers need to progressively choose the attacking channel direct the each availability in view of its attacking involvement in past openings. The PUE attacker can't watch the reward on the attacked channel since it never knows whether an auxiliary client ever tries to get to it. To fathom this test, we propose an Attack But to Observe- Another (ABOA) plot, in which the attacker attacks one channel in the spectrum sensing stage, yet sees in any event one other divert in the information transmission stage. Two non-stochastic web based learning-based assaulting calculations, EXP3 with deterministic observation (EXP3-DO) and Optimal Online-Learning with Uniformly Randomized Observation (OPT-RO)[18], which select the watching channel deterministically in view of the attacking channel and uniform arbitrarily, separately. EXP3-DO utilizes a current hypothetical structure and is suboptimal. OPT- RO depends on the new proposed hypothetical structure and is ideal.

III.PROPOSED SYSTEM

In this paper, we propose a novel PUE detection system, termed Signal activity Pattern Acquisition and Reconstruction System. Different from current solutions of PUE detection, the proposed system does not need any a priori knowledge of Primary Users (PUs), and has no limitation on the type of PUs that are applicable. It acquires the activity pattern of a signal through spectrum sensing, such as the ON and OFF periods of the signal. Then it reconstructs the observed signal activity pattern through a reconstruction model. By examining the reconstruction error, the proposed system can smartly distinguish a signal activity pattern of a PU from a signal activity pattern of an attacker. Our motivation is that while an attacker can cheat on the signal itself, it cannot cheat on its objective, i.e., causing DoS to the CRN. An attacker can transmit a PU signal, but its SAP is expected to be different from the ones of PUs. Therefore, the attacker aims to significantly decrease the channel availability to the CRN, e.g., by increasing the ON periods and/or decreasing the OFF periods. Thus the attacker creates a different SAP from PUs. On the other hand, if an attacker also cheats on its SAP, i.e., manipulates its spectrum occupation to be similar to the one of PUs, we argue that such a ‘mild’ PUE attack is tolerable by the CRN, and hence defeats the DoS objective of the attacker. This is because a CRN usually selects the operation channels with low spectrum occupation by PUs.

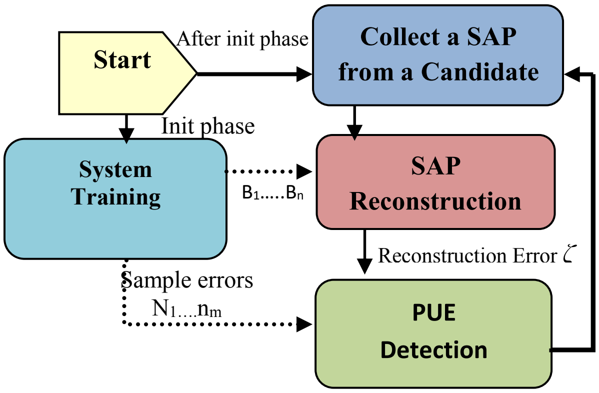


Fig.3.1 SPARS Architecture.

The main idea of SPARS is to use a set of *n* vectors **B**1*, . . . ,***B**n ∈ R*k*, which are called *bases* in this paper, to reconstruct a SAP. Specifically, let a column vector ***Y*** ∈ R*k* denote a SAP. Our objective is to reconstruct ***Y*** using bases ***B***1*, . . . ,**Bn*** as

$$\Upsilon=E+\sum_{i=1}^{n} \boldsymbol{B}_i \, W_i \quad \ldots\ldots\ldots\ldots\ldots..(1)$$

Where Wi ($1 \leq i \leq n$) is the weight associated with base $\boldsymbol{Bi}$ to compose $\boldsymbol{Y}$. The bases $\boldsymbol{B}1, \ldots, \boldsymbol{Bn}$ are carefully learned through a training process to capture the essential features of the SAPs of PUs. For the reconstruction model in (1) to be a good model, it is typically not a determined system, but an over determined or underdetermined system. Hence the reconstruction of a SAP results in a reconstruction error, which is utilized by SPARS to detect PUE attack. This is because the SAPs of PUs can be reconstructed by (1) very well, i.e., with a small reconstruction error, as the bases have captured the essential features of such SAPs. On the other hand, as discussed in Section 1, the SAPs of attackers would have different features from the SAPs of PUs, since the attackers aim to cause severe DoS to the CRN. Therefore, if we use the bases to reconstruct a SAP of an attacker, it would turn out that the reconstruction cannot be performed well, i.e., we would have a large reconstruction error. Thus, from the reconstruction error, we can tell if the transmitter of SAP $\boldsymbol{Y}$ is an attacker or a PU. Fig. 1 illustrates the architecture of SPARS. It consists of three modules: system training, *SAP* reconstruction, and PUE detection. In the initial CRN setup phase, an SU passively performs spectrum sensing to collect a set of SAPs from PUs for the purpose of training SPARS. This set of SAPs is called the training data set. The system training module learns the bases $\mathbf{B}1, \ldots, \mathbf{B}n$ from the training data set. After learning the bases, the system training module also computes the reconstruction errors for the training data set, $\eta1, \ldots, \eta m$, called the sample errors in the figure. This module can be re-run periodically to update the training data set and the bases. After SPARS is trained, then an SU can use it for PUE detection. Suppose the SU wants to find if there is an attacker in a candidate channel. It first collects a SAP from this channel. Then the SU uses the SAP reconstruction module of SPARS to reconstruct this SAP using the learned bases $\mathbf{B}1, \ldots, \mathbf{B}n$, and compute the reconstruction error ζ for this SAP. Next, the PUE detection module is used to Check if ζ falls in a tolerance interval of the sample errors $\eta1, \ldots, \eta m$, which have been obtained in the initial system training. If it does not fall in the tolerance interval, then this SAP is treated from an attacker, and the transmitter of this SAP is alarmed as an attacker. Both the SAP reconstruction and the system training rely on a good SAP reconstruction model. The system training needs the model to select the best bases $\mathbf{B}1, \ldots, \mathbf{B}n$ for the purpose of SAP reconstruction in the future. On the other hand, the SAP reconstruction module needs the model to select best weights $W1, \ldots, Wn$ to minimize the reconstruction error.

Algorithm Steps :

```
if CRN is in the initial setup phase then
    Passively carry out spectrum sensing to collect SAPs,denoted as $\boldsymbol{X}1, \ldots, \boldsymbol{Xm}$.
    for $1 \leq i \leq m$ do
        Calculate the mean $\mu i$, and variance mean for SAP $X_{i.}$
    end for
    Compute the sample mean and variance of vector
    Compute the tolerance limit of the ON periods mean
    Compute the lower tolerance limit of the OFF periods mean
    Compute the sample mean and variance of vector
    Compute the tolerance limit of the variance.
end if
loop
    For a SAP $\boldsymbol{Y}$ collected from a candidate channel, compute the mean and variance
    if      SAP $Y$ is from a PU. Alarm = NO
    else    SAP $Y$ is an attacker . Alarm = Yes
    end if
end loop
```

Hybrid Energy Harvesting

We consider EH-SUs with the ability of harvesting energy from renewable sources (e.g. solar) and ambient RF/wireless signals (e.g., primary signals). Simultaneous wireless information and power transfer technique has been recently proposed where the receiver is able to use the radio frequency signal simultaneously for information and energy harvesting

Time Switching (Ts) Protocol and Power Splitting (Ps) Protocol

Two main practical protocols are proposed in the literature namely; Time Switching (TS) protocol and Power Splitting (PS) protocol. In the TS protocol, the energy harvesting node switches over time between the energy harvester equipment and the information decoder. While in PS protocol, a portion of the received signal is used for energy harvesting and the remaining is used for the information processing

Energy Half-Duplex (EHD)

Energy Half-Duplex (EHD) constraint which prevents SUs from charging and discharging simultaneously. This constraint can be mitigated by the exploitation of two identical ultra-capacitors such that while the first one charges from harvested energy, the second discharges to supply continuous power for sensing and transmission tasks.

Heterogeneous Cooperative Spectrum Sensing Model

At the beginning of each slot, cooperating SUs first determine whether to be in the *active mode* to involve in CSS and data transmission or to be in the *passive mode* to solely harvest energy, which is denoted by

$$am \triangleq f0(passive);\ 1(active)$$

Harvested Energy in Time Slot

$$E^{h,t}_{m}= \begin{cases} (1-a^{t}_{m})X^{t}_{m}T & ,a^{t,o}_{m,}\ C_{t\ ,\ \varphi t} \text{ for EHS} \\ a^{t}_{m}X^{t}_{m}\ (T-T_{m)} & ,\ a^{t,1}_{m,}C_{\ t\ ,\ \varphi t} \text{ for EHS} \\ a^{t}_{m\varphi t}\quad X^{t}_{m(}T-\Gamma) & ,\ a^{t,o}_{m,}\ C_{t\ ,\ \varphi t} \text{ for EHS} \\ a^{t}_{m}\,C_{t\ \varphi t}\ X^{t.RF}_{m}\,(\Gamma\ -T_{m)} & ,\ a^{t,1}_{m,}C^{1}_{\ t,\ \varphi}\ {}^{1}_{t} \text{ for EHS} \\ 0 & \end{cases}$$

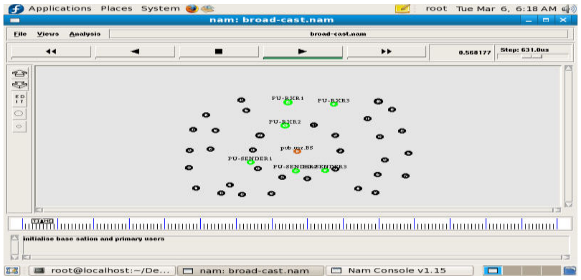
IV. MODULES AND DESCRIPTION

A.SAP Reconstruction Model:

A determined model has poor performance for reconstructing arbitrary input data , because it targets only the training data during system training. In other words, fig 4.1 demonstrates the determined model captures all features of the training data, some of which are actually not desirable when reconstructing the future input data, as they represent deviations of training data from a typical input data. Therefore, it is desirable to design an over determined or underdetermined model in practice. In this paper, we adopt an underdetermined model, which is robust to noise and other interference of the data. An underdetermined model also has other desirable features such as greater flexibility to reconstruct the input data. With an underdetermined model, we do not get an exact representation of ***Y*** by ***B***1, . . . ,***B**n* and W1, . . . ,Wn. Instead, we get an approximate representation of ***Y*** with an error term ***E*** = [E1, . . . , Ek]T. In other words, as an underdetermined model, becomes

$$\Upsilon=E+\sum_{i=1}^{n} B_{i}\ W_{i}$$

where the number of bases *n* is larger than the number of elements *k* in ***Y***. Furthermore, to prevent overfitting, a sparse model that uses only a small number of bases to reconstruct the input data is preferred over a complex model that uses a majority of bases to reconstruct the input data. use a matrix ***B*** = [***B***1, . . . ,***Bn***] to denote the bases and a column vector ***W*** = [W1, . . . ,Wn]T to denote the weight.

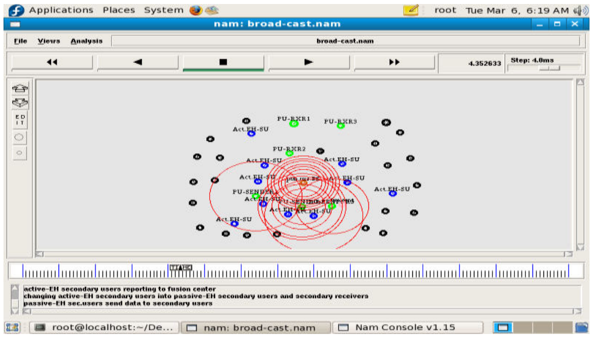


```
initialise base sation and primary users
```

Fig 4.1 Capturing the Features of Training Data

B.SPARS Training:

To train SPARS to obtain an optimal set of bases ***B****, we need a set of training data, i.e., a set of SAPs. We can collect the training data in the initial setup phase of the CRN. At the beginning of CRN setup, each SU passively performs spectrum sensing on each channel to collect the SAP information (ON and OFF periods) of every PU signal transmitter. In this initial sensing phase, the transmitters of PU signal are expected to be (genuine) PUs. This is because in this phase, the selfish SUs would not launch PUE attack, since data transmission is not started yet, and they do not get any benefit for occupying a channel. Furthermore, a malicious attacker would not be aware of a CRN being set up in the field, since the SUs are not transmitting. Hence, the PUE attack in the initial CRN setup phase is relieved by the selection of operation channels. Therefore, we assume that during the initial sensing phase of a CRN setup, there is no PUE attack, so that the training data set consists of SAPs of PUs. After the CRN is set up, Fig 4.2 demonstrates the training data set can be continuously updated by randomly incorporating the SAPs which are recognized as from PUs by SPARS.



```
active-EH secondary users reporting to fusion center
changing active-EH secondary users into passive-EH secondary users and secondary receivers
passive-EH sec.users send data to secondary users
```

Fig 4.2 Training Data Set Incorporating the Signal Activity Pattern

C.PUE Detection:

We use the SSE ζ to measure the normality of SAP ***Y***. We introduce a technique called tolerance interval to test normality of SAP ***Y***. The tolerance interval is similar to the quantile, but has a benefit that it can be computed from the sample mean and variance, without needing the actual mean and variance. We can obtain the SSE sample mean and variance from $\eta 1, \ldots, \eta m$, which have been obtained in last section for reconstructing the training data set ***X***, since each training data ***Xi*** is a random SAP sample. Given the tolerance interval $[-\infty, \tilde{\gamma}]$, we test SAP ***Y*** by examining the SSE ζ . If ζ falls in the tolerance interval, i.e., $\zeta \leq \tilde{\gamma}$, then ***Y*** is a normal SAP. Otherwise, ***Y*** is an abnormal SAP and the corresponding signal transmitter is alarmed as an attacker.

V.CONCLUSION

The PUE detection system termed SPARS, which acquires the Signal Activity Pattern (SAP) of the Primary User signal transmitters. It uses a SAP reconstruction model to reconstruct a determined SAP associated finds if the SAP belongs to associate attacker supported the reconstruction error. Completely different from current solutions on the PUE detection, SPARS doesn't want a priori information of PUs, and has no limitation on the kind of applicable PUs. The performance analysis indicates that SPARS is strong and effective to sight each straight and smart PUE attackers, despite the fact that the good attackers might forge the SAPs. The heterogeneous EEH-CSS theme subject to basic EEH-CSS constraints. It had been shown that taking the various harvests, sensing, and news characteristics of EH-SUs into thought can yield a stronger performance in terms of realizable throughput, energy consumption, and so likelihood of being active. Since the active likelihood of associate degree EH-SU is extremely dependent on harvest home, sensing, and news attributes, we analyzed the straight line behavior of being active for one EH-SU, which is then generalized to planned heterogeneous EEH-CSS theme. Given a possible set of Secondary users, deciding the best set of cooperating EH-SUs is of the essence to achieve most realizable total outturn.

VI.REFERENCES

[1] S. Park and D. Hong, "Achievable throughput of energy harvesting cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1010–1022, 2014.

[2] E. C. Y. Peh *et al.*, "Optimization of cooperative sensing in cognitive radio networks: A sensing-throughput tradeoff view," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5294–5299, Nov. 2009.

[3] S. Yin *et al.*, "Achievable throughput optimization in energy harvestingcognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 3, pp. 407–422, Mar. 2015.

[4] H. Liu *et al.*, "Optimal cooperative spectrum sensing strategy in cognitive radio networks exploiting rf-energy harvesting," in *proc. IEEE WCSP*, 2015, pp. 1–5.

[5] K. Li *et al.*, "Energy-harvesting cognitive radio systems cooperating for spectrum sensing and utilization," in *proc. IEEE GLOBECOM*, 2015.

[6] S. Luo *et al.*, "Optimal save-then-transmit protocol for energy harvesting wireless transmitters," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1196–1207, Mar. 2013.

[7] A. Celik, A. Alsharoa, and A. Kamal, "Hybrid energy harvesting cooperative spectrum sensing in heterogeneous crns," in *proc. IEEE GLOBECOM Workshops*, Dec. 2016.

[8] A. Celik and A. E. Kamal, "Green cooperative spectrum sensing and scheduling in heterogeneous cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 2, no. 3, pp. 238–248, Sept 2016.

[9] A. Celik and A. E. Kamal, "More spectrum for less energy: Green cooperative sensing scheduling in crns," in *proc. IEEE ICC*, 2015.

[10] Y. Mao, Y. Luo, J. Zhang, and K. B. Letaief, "Energy harvesting small cell networks: feasibility, deployment, and operation," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 94–101, June 2015.

[11] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, Part II: Unknown channel statistics," *IEEE Trans. Wireless Commun.*, vol. 10, no. 1, pp. 274–283, Jan. 2011.

[12] Y. Tan, K. Hong, S. Sengupta, and K. Subbalakshmi, "Using Sybil identities for primary user emulation and byzantine attacks in dsa networks," in *Proc. IEEE GLOBECOM*, Houston, TX, USA,2011.

[13] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *Proc. IEEE WCNC*,Cancun, Mexico, 2011.

[14] N. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Trans. Signal Process.*, vol. 60, no. 3,pp. 1432–1445, Mar. 2012.

[15] R. Chen, J.-M. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive

radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

[16] S. Chen, K. Zeng, and P. Mohapatra, "Hearing is believing: Detecting mobile primary user emulation attack in white space," in *Proc. IEEE INFOCOM*, 2011

[17] J. Wright, A. Yang, A. Ganesh, S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 31, no. 2, pp. 210–227, Feb. 2009.

[18] Monireh Dabaghchian *et al.*," Online Learning-Based Optimal Primary User Emulation Attacks in Cognitive Radio Networks," IEEE Conference on Communications and Network Security (CNS),2016.

[19] Abdulkadir Celik *et al.*," Hybrid Energy Harvesting-Based Cooperative Spectrum Sensing and Access in Heterogeneous Cognitive Radio Networks," IEEE Transactions on Cognitive Communications and Networking,2016.