International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 409-414
Published Online April 2020 in IJEAST (http://www.ijeast.com)

SPECTRUM SENSING AND SECURITY CONCERNS IN SOFTWARE-DEFINED RADIO AND COGNITIVE RADIO NETWORKS

T. L. Singal
Chitkara University Institue of Engineering and
Technology, Chitkara University, India

Abstract— **Cognitive radio networks (CRNs) enable to resolve the issue of radio spectrum scarcity by employing dynamic spectrum access (DSA) technique in next generation wireless networks. The cognitive radio (CR) yields additional bandwidth to support the demand for higher data rate and better quality wireless products and services. Several operational features of CRNs such as spectrum sensing, propagation criteria, probability of detection and system capacity have been explored in the recent past. However, requirement for providing adequate level of security is the main challenge for wide deployment of CRNs. The issues of security and robustness in CRNs have gained momentum recently. In this paper, an overview of spectrum sensing method with energy detection is given. But it is associated with probability of false alarm detection which leads to spectrum sensing errors. The implementation strategy for cooperative spectrum sensing with improved energy detection technique is discussed. This results in the optimal threshold level in order to obtain minimum spectrum sensing error (MSSE). An overview of various security concerns versus requirements in software defined radio (SDR) and cognitive radio networks is presented. Suggestions for countermeasures to address certain security concerns at different levels of implementation are also given. A thorough investigation covering all security aspects in CRNs is the need of the hour for obtaining the desired performance.**

Keywords— **Cognitive Radio Networks, Energy Detection, Software-Defined Radio, Spectrum Sensing, Security Concerns**

I. INTRODUCTION

The Internet data traffic over wireless communication infrastructures is increasing exponentially each day. It is mainly due to widespread usage of smart mobile phones for variety of online services with reduced subscription costs [1]. Several new user technologies for next generation wireless networks have emerged. Cognitive radio networks (CRNs) operate in an open wireless environment with random access to existing cellular and mobile communication networks [2]. In CRNs, the secondary users (unlicensed, also referred to as cognitive radios) can access the radio spectrum which is not being currently occupied by the primary users (licensed) in an opportunistic manner. Cognitive radios have the capability to adapt its radio transmissions (that is, frequencies, waveforms and protocols) according to the interference it sees [3]. This approach is commonly called dynamic spectrum access (DSA), which is implemented using sophisticated algorithms for flexible spectrum management.

Providing adequate level of security has been one of the major challenges for the wide deployment of CRNs, as the case in any wireless communication networks [4]. In general, CRNs must validate communication security requirements such as authorization, registration, authentication, privacy, data confidentiality, and network availability. Due to wireless nature of CRNs, various types of common security threats encountered in traditional wireless networks are also applicable here. These security threats include RF jamming at the physical layer, MAC address spoofing including spurious transmission of MAC frames and cheating on back-off rules, and traffic congestion [5]. But CRNs have their unique cognitive characteristics. So they face newer security threats and challenges such as primary user emulation attack (PUEA), beacon falsification (BF), spectrum sensing data falsification (SSDF), a small back-off window (SBW) in combination with SSDF, cross layer threats, software defined radio related hardware and software security issues [6], [7].

In CRNs, the spectrum access by the cognitive users depends solely on accurate spectrum sensing that poses a serious security threat. For better understanding of the operation and the possible security concerns in CRNs, energy detection strategies should be analyzed. With this objective, this paper begins with a brief overview of cooperative spectrum sensing using energy detection technique. The aspect related to probability of detection is discussed next. This forms the basis for investigation of the current studies available on security issues pertaining to cognitive radio networks. A detailed analysis of various security concerns under specific conditions is carried out with suggestions for countermeasures.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 393-400
Published Online April 2020 in IJEAST (http://www.ijeast.com)

II. RELATED LITERATURE

Recently, security aspects in CRNs have gained momentum. A lot of researchers have identified, analyzed and suggested several algorithms to countermeasure security attacks. An optimal obfuscation strategy [8] was proposed for location privacy and spectrum utilization efficiency that uses geolocation databases to share the spectrum in CRNs. The effect of passive attacks on capacity of primary and cognitive radio link rates was thoroughly analyzed [9]. Deliberations were carried out on new security attacks and challenges in energy detection based spectrum sensing [10]. Various inter-related CR security attacks and possible protection techniques were identified for further investigations [11]. Various security challenges, possible solutions and further research areas were presented [12].

Cross-layer attacks to TCP connection was discussed and a mitigation technique was proposed [13]. The issue of physical-layer security in a spectrum-sharing CRN was addressed from an information-theoretic perspective [14]. The disruptive effects of PUE attack on spectrum sensing in CRNs was demonstrated with suggestion for countermeasure scheme [15]. Different types of denial-of-service (DoS) attacks in CRNs have been presented [16]. Underlay paradigm in CRN offers less vulnerability to jamming attacks [17], and location-based defensive scheme has been proposed to counter PUE spoofing [18].

Various types of security attacks in dynamic spectrum access have been discussed [19]. Cross-layer security threats have been analyzed at higher level applications for using spectrum sensing [20], [21]. There is a need of thorough understanding of vital aspects of cognitive radio networks and analysis of security issues so as to devise methods to countermeasure them effectively.

III. ENERGY DETECTION BASED SPECTRUM SENSING

In CRNs, the key component is spectrum sensing which means collecting cognition about the radio environment. Spectrum is not limited to frequency band alone but the concept of spectrum space extends to space, time and code also. Likewise sensing includes detection of type of signals that occupy the spectrum, for example, carrier frequency, bandwidth, modulation, and waveform. At the physical radio communication level, situational awareness allows the cognitive user to optimise the transmission parameters with minimum interference to other users and maximizing its own throughput. Fig. 1 shows a typical process flow diagram of spectrum sensing with energy detection [22].

However, due to probability of false alarm or missed detection, access collision during spectrum sensing affects the throughput and quality of service for the primary users. This necessitates re-transmission which may cause delays.

In a multiuser CRN, the cognitive users are competing against each other for the unoccupied spectrum. In order to obtain more reliable and improved performance, cooperation among spatially dispersed secondary users reduces the sensing time and minimises the mutual interference. The performance is enhanced due to use of cooperative sensing that results from the deployment of the spatial diversity between the interpretations made by different CR users at different locations. This means more control messaging, and thereby an increase in the transmission overheads.

An implementation strategy of cooperative spectrum sensing with improved energy detection technique involves the use of fast Fourier transform (FFT). This method improves the spectrum sensing accuracy due to increase in signal-to-noise ratio. Thus, the minimum spectrum sensing error (MSSE) is obtained. This can be further improved by using the optimum algorithm known as Maximum-A-Posteriori (MAP) detector. [23].

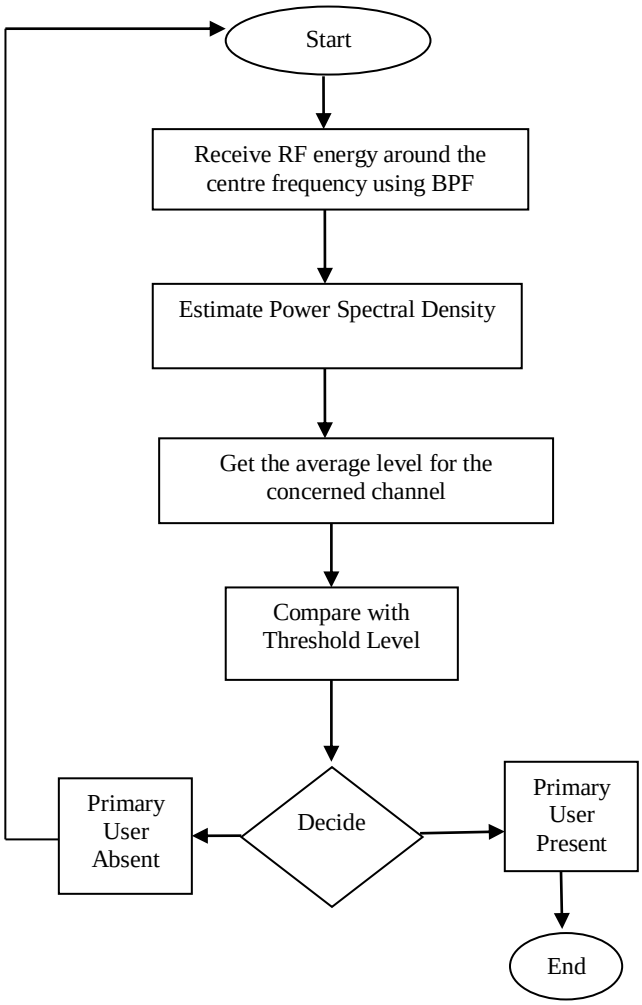

Fig. 1. Spectrum Sensing with Energy Detection

Thus, the fundamental characteristic of a cognitive radio is spectrum sensing which enables it to use it in an opportunistic manner. Distributed detection, sequential and quickest detection techniques are advanced spectrum sensing techniques for more effective and efficient spectrum exploration. Distributed detection techniques provide spatial diversity gains which avoid the hidden node problems as well as problems caused by shadowing and fading.

IV. SECURITY CONCERNS IN CRNS

In CRNs, cognitive radio nodes are secondary users that share the allocated spectrum of the licensed primary users. They have authorized access to the idle spectrum either on a limited- or no-interference basis to the transmissions of the

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 393-400
Published Online April 2020 in IJEAST (http://www.ijeast.com)

primary users as well as other cognitive users at that instant of time. This type of operating environment results into security concerns related to denial-of-service attacks. Accurate spectrum sensing by CRN's secondary users is the core feature but it also poses a major security threat to the overall reliable operation of the network. Energy detection based spectrum sensing is widely employed because there is no need of prior knowledge about presence of primary users. Moreover, this method is simple to implement with low computational overheads. There are mainly three classes of security attacks that manipulate the behavior of a cognitive radio network: sensory, belief, and self-propagating. These types of security attacks to cognitive radio networks are also referred to as cognitive radio viruses.

Most of different types of security concerns can affect both distributed as well as centralized types of cognitive radio networks. Commonly known security threats in cognitive radio are presented briefly in Table I [24].

TABLE I. SECURITY CONCERNS IN COGNITIVE RADIO

Description of Security Threat	Security Requirement
Unauthorized usage of allocated spectrum by malicious user or for DoS to Primary user	Regulatory framework be complied
Cognitive RF channel jamming, or cognitive control channel saturation, or cognitive radio node internal failure	System integrity be protected with robustness
Cognitive radio node altered by malicious user	Regulatory framework be complied, and system integrity be protected
Masquerading of a primary user or a cognitive radio node	Identities be verified as well as accounted for, confidentiality be protected, and access to resources be controlled
Hidden CR node problem	Regulatory framework be complied, and identities be verified
Cognitive messages altered by malicious user	Data integrity be protected, and identities be verified
Cognitive messages eavesdropped	Data confidentiality be protected
MAC layer of CRN disrupted	System integrity be protected, Identities be verified, and access to resources be controlled

A specific security threat to cognitive radio spectrum can affect the DSA mechanism – spectrum sensing, spectrum analysis and spectrum decision, all forming part of the cognitive cycle. When an incumbent signal is detected, cognitive radios perform spectrum hand-off which leads to more sensing time. Malicious and greedy CR nodes cause DoS attacks by transmitting fake incumbent signals. This may disrupt CRN operation severely. It is essential to identify and classify different categories of possible security concerns in cognitive radio and related protection requirements at various levels of operation.

Various security threats can be correlated to each other. Protection mechanism against security threats can be categorized based on CR nodes reputation, crypto-analysis of their authentication, sophisticated analysis for identification of masquerading signals and usage of geolocation databases of licensed CR users. A beacon signal may also be used to alert any secondary users by a primary user for any malicious use of spectrum.

Security threats against a subset of CR nodes can be more adverse in a cooperative network. This type of threat or attack is known as Primary User Emulation Attack (PUEA). It is quite effective in traditional DSA environments based on spectrum sensing with energy detection technique. However, the effect of PUEA is transient as it is only a sensory-manipulation attack. Advanced DSA algorithms operate on channel statistics for primary users. Spoofing primary user waveforms convert this attack into a belief-manipulation attack.

The probability of missed or false alarm detection is maximum in case the malicious CR users are very near to the secondary users. Malicious, greedy, or unintentionally misbehaving users report false observations for spectrum availability. This type of security threat is termed as spectrum sensing data falsification (SSDF) threat. This affects the spectrum decision part of the cognitive cycle. It is desirable to have minimum interference to primary users. This further necessitates collaboration between physical layer and MAC layer. Common control channel (CCC) enables CRs to exchange control information such as collaborative sensing (distributive and centralized), spectrum hand-off, channel negotiation, etc.

Spectrum management function is a critical function of a CRN using IEEE 802.22 MAC layer protocol for infrastructure-based CRNs as well as application or scenario specific protocols for ad-hoc CR networks. It can become the target of malicious users to cause DoS attacks. Security threats at MAC layer affects the spectrum analysis as well as spectrum decision aspects of the cognitive cycle. Multi-hop CRNs are more vulnerable to MAC spoofing (sending spurious messages to disrupt CRN operation), congestion and jamming attacks by creating RF interference. When malicious users transmit spurious beacon signals to disrupt spectrum sharing or synchronization between base stations of Wireless Regional Access Networks (WRANs). This type of security attack is known as Beacon Falsification (BF) attack.

Malicious users can launch security attacks targeting multiple layers (physical, MAC and others). Then these are called cross-layer security attacks which can affect the complete cognitive cycle. CRs with MAC layers using CSMA/CA are prone to small back-off window attack where malicious users monopolize bandwidth by choosing an incremental value for minimum contention window. When a PUEA or a SSDF security attack affects transport layer, it is known as lion attack [25]. This forces spectrum handoff unnecessarily which leads to degradation of the performance in terms of throughput of TCP connection. Another type of security threat can be to deny service to a cognitive user operating in TDMA environment.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 393-400
Published Online April 2020 in IJEAST (http://www.ijeast.com)

In DSA environments, PUEA is more prominent. In this, a malicious user can create a similar waveform as that used by the primary user in idle spectrum, thereby, denying spectrum use to cognitive users. A sensory manipulation attack is the main security concern that causes the SDR to select a sub-optimal configuration. However, its effect is transient only. Belief manipulation attack is another security concern when an attacker can cause temporary radio link degradation by injecting a jamming signal. In a cooperative type of CRN, security threats against a subset of cognitive nodes can result into contention-free spectrum access to the attackers.

Software defined radio (SDR) is the main component of cognitive radio which is highly configurable wireless communication device. It typically has specific waveform detectors, receiver sensors, and a programming interface. Security concerns in SDR becomes more serious since it performs a lot of mathematical modeling and simulation. It uses programmable digital signal processing to provide various radio functions in order to accommodate new capabilities and features. Moreover, SDR technology enables seamless radio operation by hiding implementation details from users. Table II depicts some of the security concerns which are common to SDR in CRNs [26].

TABLE II. SECURITY CONCERNS IN SDR

Description of Security Threat	**Security Requirement**
Malicious software introduced or waveform code altered	System integrity be protected
User or configuration data altered	Data integrity be protected
Configuration data or waveform data extracted	Data confidentiality be protected
Masquerading of valid software waveform	System integrity be protected, identities be verified, and access to resources be controlled
Repudiation of data	Data integrity be protected, and identities be verified
Failure of software or hardware	System integrity be protected with robustness
Real-time operating system (RTOS) software altered	System integrity be protected
User data extracted	Data integrity be protected
Framework software altered	System integrity be protected
Unauthorized use of SDR services	System integrity be protected, identities be verified, and access to resources be controlled

V. MITIGATION TECHNIQUES FOR SECURITY CONCERNS

Security aspects in CRNs recognizes threats as well as how the process of cognition itself enables to improve security. There are number of mitigation techniques and solutions which have been quite effective in thwarting the impact of security threats in CRNs. Most of these techniques are based on authentication and trust of CR nodes, detection of security threats using extensive digital signal processing, and SDR related security issues.

SDR security is equally important for proper functioning of the cognitive cycle. Security threats such as PUEA, SSDF, BF, CCC attacks and cross-layer attacks are possible through tampering of hardware or software parts of the SDR by malicious cognitive users. Cognitive reconfigurability, and capability give rise to newer security threats and mitigation techniques.

Newer security threats can affect both spatial and temporal behaviours of CRNs. A malicious cognitive user can mimic incumbent signals or create noise during the spectrum sensing periods by primary users.

There will be new challenges and security concerns as cognitive radio scales up the CRN stack. However, adverse manipulations at higher layers can be prevented by protecting data using better techniques of cryptography.

The mitigation techniques can be categorized depending on type of security threats in CR and SDR. Table III provides a brief account of different type of mitigation techniques versus nature of security threats, as described in previous sections, for CR and SDR [27].

TABLE III. MITIGATION TECHNQUES IN CR/SDR

Description of Mitigation Technique	**Nature of Security Threats in CR or SDR**
Framework to enforce spectrum policies	**CR** - Unauthorized use of spectrum bands for selfish use as well as DoS to primary users
Frequency hopping	**CR** - Jamming of RF channel used for delivery of cognitive messages
Authentication of CR nodes and Identification of masquerading threats using signal analysis	**CR** – Malicious alteration of a CR node or cognitive messages; Masquerading of a CR node or a primary user
Data fusion process of collaborative spectrum sensing	**CR** - Internal failure of a CR node or Hidden node problem
Robustness	**CR** - Saturation of the cognitive control channel
Verification of identities	**CR** - Disruption to the MAC layer of the CRN
System integrity protection	**CR** - Saturation of the cognitive control channel; Disruption to the MAC layer of the CRN
Confidentiality protection	**CR** - Eavesdropping of cognitive messages
Controlled access to	**CR** - Disruption to the MAC layer of the

resources	CRN
Trusted computing	**SDR –** Insertion of malicious software; Artificial consumption of resources; Alteration or destruction of waveform code, RTOS software or the software framework; Masquerading as authorized software waveform
Use of digital signatures for software modules	**SDR –** Insertion of malicious software; Alteration or destruction of waveform code; Masquerading as authorized software waveform
Software framework (middleware) of the SDR platform, or Data integrity functionality in the RTOS	**SDR –** Alteration or destruction of the configuration data; Extraction of configuration/user data or waveform data; Data repudiation
RTOS watchdog	**SDR –** Artificial consumption of resources
Use of secure administrative module and automatic calibration unit	**SDR -** Alteration or destruction of waveform code; Unauthorized use of SDR services
High assurance techniques	**SDR –** Software or hardware failures

VI. CONCLUSION

A cognitive radio employs sophisticated signal processing levels to ensure efficient spectrum utilization in next generation wireless networks. Security concerns in CRNs exist for primary users as well as cognitive users. Ideally, cognitive users should access the licensed spectrum meant for primary users on a non-interference basis. However, malicious cognitive radio users intend to cause severe DoS threats to primary users through RF interference. The paper has covered an extensive overview of various security concerns in SDR technology and CRN. Various types of mitigating techniques for thwarting the impact of security threats in CRNs have been summarized for further analysis. Additional techniques may include improved spectrum sensing algorithms, use of swarm intelligence and swarm optimization. A lot of investigation in the area of security aspects of CRNs is still required by the researchers working in this area.

VII. REFERENCES

[1] Morley J., Widdick K., and Hazas M. (2018). Digitalisation, energy and data demand: The impact of internet traffic on overall and peak electricity consumption, *Energy Research & Social Science, Elsevier,* Vol. 38, pp. 128-137.

[2] Umar R., and Sheikh A. (2013). A comprehensive study of spectrum awareness techniques for cognitive radio oriented wireless networks (CROWN), *Physical Communication 9, Elsevier,* pp. 148-170.

[3] Singal T. (2012). Analog and Digital Communications, 1st ed., *McGraw Hill Education,* pp. 867-868.

[4] Clancy T., and Goergen N. (2008). Security in cognitive radio networks: Threats and mitigation, *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications,* Singapore.

[5] Zhang Y., Xu G. and Xiaozhong Geng (2008). Security threats in cognitive radio networks, *10th IEEE International Conference on High Performance Computing and Communications,* Dalian China, pp. 1036-1041.

[6] Mathur C., and Subbalakshmi K. (2007). Security issues in cognitive radio networks: Towards self-aware networks, *Wiley,* New York, pp. 284-293.

[7] Singal T. (2013). Issues of interoperability among heterogeneous wireless communication networks, *International Journal of Computing and Business Research,* Vol. 4, Issue 2, pp. 1-10.

[8] Bhattarai S., Vaka P. and Park J. (2018). Thwarting location inference attacks in database-driven spectrum sharing, *IEEE Transactions on Cognitive Communications and Networking,* Vol. 4, No. 2, pp. 314-327.

[9] Arjoune Y., and Kaabouch N. (2019). A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions, *Sensors,* Basel Switzerland, Vol. 19(1), pp. 1-32.

[10] El-Hajj W., Safa H., and Guizani M. (2011). Survey of Security Issues in Cognitive Radio Networks, *Journal of Internet Technology,* Vol. 12, No. 2, pp. 1-18.

[11] Attar A. et. al. (2012). A survey of security challenges in cognitive radio networks: solutions and future research directions, *Proceedings of the IEEE,* Vol. 100, No. 12, pp. 3170-3171.

[12] Pei Y., et al. (2010). Secure communication over MISO cognitive radio channels, *IEEE Transactions on Wireless Communications,* Vol. 9, No. 4, pp. 1494-1502.

[13] Leon O., Juan H., and Soriano M. (2012). Cooperative detection of primary user emulation attacks in CRNs, *International Journal of Computer and Telecommunications Networking,* Vol. 56, Issue 14, pp. 3374-3384.

[14] Jin Z., Anand S., and Subbalakshmi K. (2009). Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, *ACM Mobile Computing and Communications Review, Special Issue on Cognitive Radio Technologies and Systems,* Vol. 13, No. 2, pp. 74-85.

[15] Murotake D., and Martin A. (2004). System threat analysis for high assurance software defined radios, *Proceedings of Technical Conference, SDR Forum,* Phoenix AZ.

[16] Jakimoski G., and Subbalakshmi K. (2009). Towards secure spectrum decision, *IEEE International Conference on Communications,* Dresden Germany, pp. 1-5.

[17] Chen R., Park J., and Reed J. (2012). Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead, *IEEE Communications Surveys and Tutorials,* Vol. 14, No. 2.

[18] Chen R., Park J., and Reed J. (2008). Defense against primary user emulation attacks in cognitive radio networks, *IEEE Journal on Selected Areas in Communications,* Vol. 26, Issue 1, pp. 25-37.

[19] Fragkiadakis A., et al. (2013). A survey on security threats and detection techniques in cognitive radio networks, *IEEE Communiactions Surveys and Tutorials,* Vol. 15, No. 1.

[20] Zhao C., et al. (2010). A PHY-layer authentication approach for transmitter identification in Cognitive Radio Networks, *International Conference on Communications and Mobile Computing,* Shenzhen China, Vol. 2, pp. 154-158.

[21] Yuan Z., et al. (2011). Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks, *IEEE Wireless Communications and Networking Conference,* Mexico, pp. 28-31.

[22] Arora K., Singal T. (2014). Cognitive Radio Network – Cooperative Spectrum Sensing with Energy Detection, *International Journal of Electronics and Communication Technology,* Vol. 5, Issue 4, Version Spl-1, pp. 26-30.

[23] Arora K., Singal T. (2015). Simulation of Probability of False Alarm and Probability of Detection in Cognitive Radio, *International Journal of Computer Science and Technology,* Vol. 6, Issue 1, Version Spl-1, pp. 37-41.

[24] Yu R., et al. (2016). Securing cognitive radio networks against primary user emulation attacks, *IEEE Network,* Vol. 30, Issue 6, pp. 62-69.

[25] Juan H., et al. (2011). Modelling the Lion attack in cognitive radio networks, *EURASIP Journal on Wireless Communications and Networks,* Article ID 242304, pp. 1-10.

[26] Raj S., and Sahu O. (2017). Countermeasures to security threats/ attacks on different protocol layers in cognitive radio networks: An overview, *International Conference on Smart Technologies for Smart Nation,* Bangalore, India.

[27] Kun Z., et al. (2010) Reputation-based cooperative spectrum sensing with trusted nodes assistance, *IEEE Communications Letters,* vol. 14, no. 3, pp. 226-228.