# Security Challenges in Cognitive Radio Networks

Hanen Idoudi, Kevin Daimi, and Mustafa Saed

*Abstract***— Cognitive radio network (CRN) is an evolving concept aiming at more efficiently exploiting the available spectrum for opportunistic network usage. Deploying Cognitive Radio Networks raises several open issues and security concerns. CRNs suffer from both classical wireless networks vulnerabilities and threats, and new threats related to their inherent functionalities. In this paper, an overview of the cognitive radio networks and their security challenges will be provided. Both, the traditional and new security threats that emerged from these promising networks are addressed. The paper will also focus on the Primary User Emulation (PUE) attack as one of the main specific attacks targeting CRNs and analyze some proposed countermeasure. Furthermore, CRN security requirements are introduced.**

*Index Terms***— Cognitive Radio Networks, security threats, security countermeasures, security requirements**

## I. Introduction

COGNITIVE radio is an emerging paradigm, which was conceived to overcome the shortage of the unlicensed spectrum bands (2.4GHz and 5GHz). Recent studies conducted by the Federal Communication Commission (FCC) showed that many licensed spectrum bands, such as the TV bands, are underutilized whereas the unlicensed one are overcrowded [19]. New emerging schemes, such as IEEE 802.22, propose to exploit these white bands for data transmission as long as no licensed users are accessing them.

In the world of networking, spectrum is considered a decisive and critical resource. Most of the spectrum needed for wireless communication has been assigned. However, there is evidence indicating that abundant segments of the radio spectrum are not deployed for a substantial duration of time. This has piloted the innovation of cognitive radio technology as a solution for the inconveniences created as a result of this fixed spectrum allocation. This will enhance spectrum effectiveness through handling inefficient usage of licensed spectrum since radio equipment can identify the spectrum availability within their environment and invest the unused spectrum (spectrum holes) by licensed primary users (PUs) and reallocate it to secondary users (SUs) [17], [18], [23], [24], and [26].

Cognitive radio is based on the idea of allowing unlicensed users to use licensed bands while safeguarding the priority of primary licensed users. Cognitive radio networks (CRNs) are hence composed of two types of users, licensed users or primary users (PUs) and unlicensed users (secondary users) (SUs). Primary users have access priority to the spectrum. Secondary users have cognitive radio capabilities allowing them to detect available channels and switching to them whenever they are not used by a primary user. Secondary users have to cater for the highest priority of PUs by detecting their presence and terminating their communications immediately to avoid any interference with PUs.

Cognitive radio networks are envisioned to alleviate the shortage of spectrum by defining more smart and flexible wireless networks that can dynamically optimize spectrum usage. The utilization of such networks is still a challenging problem that raises several open research paradigms. Securing communications in CRN is one among these open challenges.

The open and dynamic feature of cognitive radio network causes cognitive radio systems to be vulnerable to various malicious attacks. In other words, the cognitive radio paradigm introduces entirely new classes of security threats and challenges. Securing wireless networks has never been an easy task. However, securing cognitive radio networks is even more complicated and challenging. This is because network security professionals have to deal with both the traditional wireless security threats and the newly added threats specific to CRNs. In addition to the traditional threats, such as denial of service (DoS), eavesdropping, spoofing, and tampering, new threats include jamming, primary user emulation (PUE), and spectrum mangers attacks [3], [10], [13], [16], [20], [22], and [27]. These can lead to the complete dysfunction of CRN. Therefore, strong security is essential to make cognitive radio a viable and reliable concept. Countermeasures are needed to ensure secondary users of the spectrum and primary users (incumbents) are fully protected.

In this paper, a brief overview of the cognitive radio networks is provided, and the security concerns and vulnerabilities that threaten such kind of networks are pointed out. Some focus will then be placed on the Primary User Emulation (PUE) attack including analyzing some proposed countermeasure. Finally, CRN security requirements are highlighted. Fig. 1 depicts the security threats and requirements investigated in this paper.

Manuscript received February 26, 2014, revised March 19, 2014.

H. Idoudi is with the National School of Computer Science of University of Manouba, Tunisia (phone: 216-975-80291; fax: 216-716-00449 e-mail: hanen.idoudi@ensi.rnu.tn).

K. Daimi is with Computer Science and Software Engineering, the University of Detroit Mercy, Detroit, MI 48221 USA (e-mail: daimikj@udmercy.edu).

M. Saed is with the HATCI Electronic Systems Development, Hyundai-Kia America Technical Center, Superior Township, MI 48198 USA (e-mail: msaed@hatci.com).

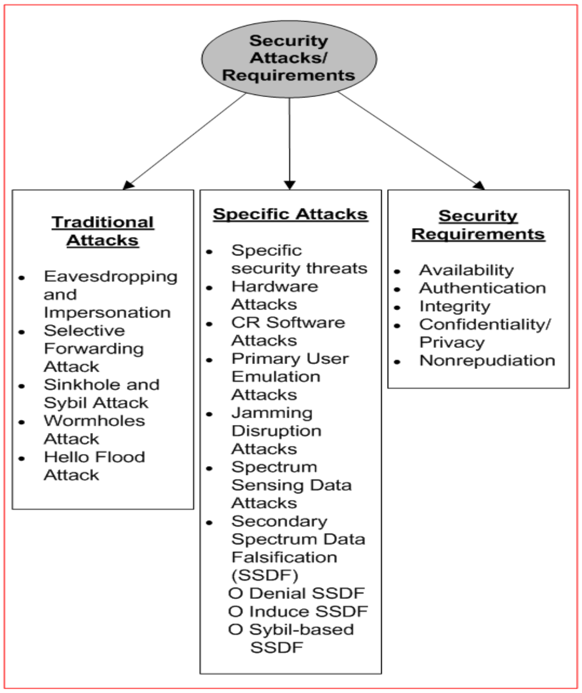


Fig. 1. Selective security attacks and requirements

## II. Cognitive Radio Networks Overview

In the early days of wireless networking, each wireless service was allotted a fixed frequency band for sole usage. With this static spectrum allocation policy and the exponentially growing demand for radio spectrum, the remaining spectrum available for the new services is being depleted. Nevertheless, recent studies conducted by the Federal Communication Commission (FCC) showed that the unlicensed spectrum (2.4GHz band) is congested whereas many licensed spectrums are still underutilized in both spatial and temporal domains. Even in the most crowded area near downtown Washington, DC, where both government and commercial spectrum use is intensive, only 38% of the licensed spectrum remains occupied and the remainder of spectrum resource (white space/spectrum hole) is unexploited [19]. In addition, the insufficient bandwidth and the growth of the unlicensed wireless technologies, such as IEEE 802.11b/g, Bluetooth, and Mobile Internet, augment interference and limit the quality of service (QoS) that can be attained. Consequently, the spectrum allocation authorities widely opened the door for licensed spectrum bands and engaged in new innovative technologies to permit dynamic use of the underutilized spectrum.

The cognitive radio (CR) technology is emerging as an effective solution to allow other users to share the underutilized spectrum provided that licensed users are not impacted. The accessibility to a frequency band depends on the activity of the licensed user. Such spectrum sharing is called dynamic spectrum access (DSA).

The FCC defines cognitive radio as, "A radio or system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, and access secondary markets**"** [9].

The spectrum-agile CR devices are capable of detecting the spectrum bands currently unused by licensed users, switching frequencies throughout a wide spectrum range, and adapting their communication parameters based on the network and user demands. Fig. 2 summarizes the CR functions. Several spectrum sensing techniques for CR are presented by Yucek et al [25]. These features empower the CR users to have opportunistic access to untaken licensed spectrum and greatly enhance the utilization of spectrum resource.

In cognitive radio networks (CRN), there are two types of users: licensed and unlicensed users. Licensed users, or primary users (PU), are those users who have privileges or legacy rights on the deployment of a specific part of the spectrum. The TV broadcast bands provide an obvious example of licensed spectrum. Unlicensed users (secondary users (SU) or cognitive users), are allowed to utilize this spectrum without instigating interferences to PUs. Like any other new technology, standards are a necessity. IEEE 802.22 is a standard for Wireless Regional Area Network (WRAN) using white spaces in the TV frequency spectrum [8], [11].

To enable devices to opportunistically access the vacant licensed frequency bands, Dynamic Spectrum Access (DSA) as a technique for radio regulation is applied. To coordinate spectrum sharing between primary users and cognitive radio systems, scheduling algorithms are needed to allow users to dynamically select the available spectrum.

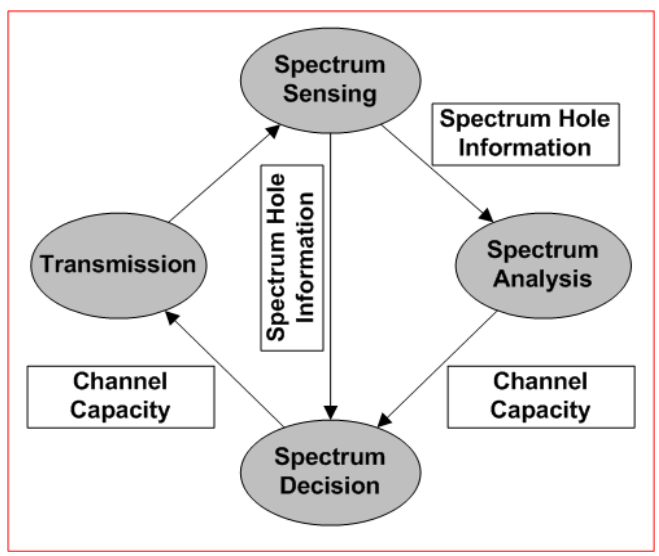


Fig. 2. Cognitive Radio Architecture

In infrastructure-based architecture, a CR node cannot establish links with other CR nodes outside its one-hop communication range. The information observed and gathered by each CR node is forwarded to the central CR-

 

Base Station (BS). Thus, a CR-base station can circumvent interference with primary networks. Furthermore, the base station (BS) can be solely responsible for the PUs detection and for spectrum analysis and decision making. The BS notifies CR nodes about the available spectrum to employ or the presence of a PU. This sort of architecture can relieve CR nodes from all decision making on cognitive functions execution. Generally speaking, this is the most appropriate architecture for cognitive wireless sensor networks, in which CR nodes are sensors with limited energy and computational resources, and have to rely on the coordinating base station.

Sensing and decision making can be totally distributed among all CR nodes, which have to cooperate to discover the PU, detect the most suitable available channel, and negotiate routing decision. This leads to an ad hoc architecture.

## III. Traditional Security Threats

Security of CRN communications is one of the most critical issues to deal with. CRNs suffer from many security threats due to their inherent characteristics. As is the case with all kinds of wireless networks, CRNs are more vulnerable to security threats originating from their open communication environment than wired networks. Attacks on wireless nodes privacy may involve different strategies including eavesdropping, impersonation, and traffic analysis. These attacks may harm wireless networks in general and CRN among them. Below, some of these attacks are explored.

### *A. Eavesdropping and Impersonation*

In passive eavesdropping attack, the attacker silently listens to the CRN wireless communications to extract useful information about the sessions including the communicating parties, PUs, and SUs, and uses that information to launch a replay attack or an impersonation attack. In an impersonation attack, the attacker uses a legitimate CR node identity in the wireless network and establishes communications with other CR nodes by providing its fake identity. In this case, the BS notifies CR nodes within the hop about the presence of a PU without realizing it is a fake one (attacker).

### *B. Selective Forwarding Attack*

Within a selective forwarding attack, malicious CR nodes may refuse to forward certain messages originating from an authentic CR node or the BS, and possibly destroying them to ensure that they are not propagated any further beyond that real CR node. A simple form of this attack is when a malicious CR node behaves like a black hole and declines to forward every packet it receives to other CR nodes.

### *C. Sinkhole and Sybil Attack*

Attackers advertise incorrect information to other participating CR nodes, such as high quality route to a sink, in case of cognitive sensor networks [5]. An attacker can actually provide this kind of route connecting all CR nodes to real sink and then selectively drop packets intended to other CR nodes. Sybil attack consists of a possible single CR node that pretends to be present at different locations of the network. The malicious node illegitimately presents multiple identities to other CR nodes in the network. Pretending to be at various locations (moving node) can fool the BS and other CR nodes into believing it is a legitimate note. In addition, this moving capability makes it harder to detect the malicious node.

### *D. Wormholes Attack*

Wormholes may convince two CR nodes to be neighbors when in fact they are far away from each other. This implies that identities and real addresses (locations) of such CR nodes will be disturbed. Well placed wormhole can completely muddle routing functionalities through impacting network topology by delivering routing information to the CR nodes before it would reach them via multi hop routing. Wormholes may be used in conjunction with Sybil attack.

### *E. Hello Flood Attack*

In a Hello Flood attack, attackers can broadcast HELLO message to CR nodes to establish a connection and then advertise high-quality route to sink. Some routing protocols use link layer acknowledgments. This helps attackers to spoof acknowledgements to convince other nodes that a weak link between nodes or hops is strong or that a dead CR node is alive. As a result, a weak link may be designated for routing forcing packets sent through that link to other nodes to be lost or corrupted.

## IV. Specific security threats

Due to their specific operational functions, CRNs suffer from new kinds of attacks that threaten their primary goals in addition to the traditional threats [15]. A number of these attacks are discussed below. A survey of CRN attacks and countermeasures for such attacks are provided in [2], [10].

### *A. Hardware Attacks*

Hardware attacks attempts to damage the hardware of some CR nodes or alter their functions. The impact of such attacks can range from totally shutting down a CR node, or leading it to transmit signals in a wrong frequency band. Furthermore, it can cause CR nodes to not properly participate in vital spectrum management collaborative decision making processes. This may give rise to incomplete or incorrect decisions, which can demoralize the network.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

### B. *CR Software Attacks*

Like any other software, CR software is subject to various attacks. However, due to the specific characteristics of CRNs, attacks on their software will have even higher impact. Software attacks can completely paralyze CRNs. As a first precaution, tamper-resistance and virus detection techniques should be incorporated to deter any malicious software installations. This also applies to any needed software download from trusted servers. With software attacks, there is a great need to enforce authentication and authorization, and protect the integrity of software installation to deter eavesdropping.

### C. *Primary User Emulation Attacks*

Using masquerading attacks or a PU Emulation Attack (PUE), a malicious adversary may masquerade a PU by replicating its characteristics and signal. This attack is uncomplicated to perform due to the flexibility of the cognitive radio of any CR node [5], and [12].

When a denial PUE attack occurs, the malicious node forces other SUs to stop their communications and avoid using this frequency based on the false impression that a PU is occupying it. This attack leads to a denial of service (DoS) following the attacker spreading false information preventing any SUs from acquiring useful communications.

Another PUE attack is the induced PUE attack. In this case an attacker may spread a high signal or noise in the vicinity of an SU to prevent an SU from detecting the PU presence. While in Coordinated PUE attack**,** multiple malicious nodes might coordinate to simultaneously launch attacks on different channels to disorder as many CRNs as possible. After detecting the current channel to be occupied due to an emulated signal, the SU will try to switch to another available channel. The secondary user (SU) might not be able to find a proper channel when multiple candidate channels are attacked. Within context of ontological cognitive radios, such coordinated PUE attacks on candidate channels will corrupt learning by coupling few channels to be non- operational.

### D. *Jamming Disruption Attacks*

Jammers transmit a signal to the receiving antenna of the CR with the same frequency as that of an authorized transmitter, and thus thwarting the legitimate reception through the receiving antenna. In the context of cognitive radios, jamming is performed during data transmission. While executing an unauthorized spectrum handling, the attacker may disregard the existence of primary users (PUs) and competes with them to access the same channel. This selfish conduct can cause a DoS attack for the primary users through interfering with their authorized communications.

### E. *Spectrum Sensing Data Attacks*

Counterfeiting spectrum sensing data is a high risk attack within the spectrum management process in charge of allocating appropriate bands to users. As a result of this attack, spectral analysis will be incorrect resulting in the wrong decisions of assigning improper bands to PUs and SUs. Improper bands will cause the CRN's activity to deteriorate. If no measures are enforced, the transmission characteristics of various bands will be incorrectly determined, and thus opening the door for further attacks and diminishing CRN functionality.

### F. *Secondary Spectrum Data Falsification (SSDF)*

A Byzantine failure (Secondary spectrum data falsification) may occur when nodes are unable to correctly detect the presence of PUs due to erroneous spectrum sensing data as a result of an attack. This attack abuses the cooperative nature of the spectrum sensing function when an attacker forwards false spectrum data to the fusion center or data collector causing erroneous decisions on spectral usage. There are three ways in which a Byzantine attack can be launched.

1) *Denial SSDF*
The adversary may advertise that a channel is unavailable. This forces the fusion/channel allocation center to suppose that the primary user is present. Consequently, channel access is restricted.

2) *Induce SSDF*
The adversary may falsely advertise that a channel is not occupied. Hence, harmful interference to PUs is incurred.

3) *Sybil-based SSDF*
In this attack, malicious attackers offer other nodes the impression that some CR nodes are implementing the required sensing functionalities. This leads legitimate nodes to rely on malicious nodes assuming that these nodes are accountable for sensing and communicating the right information on PU existence.

## V. PUE ATTACKS COUNTERMEASURES

PUE is one of the most detrimental attacks on CRN. If a malicious or selfish node apes the signal characteristics of a PU, it will impair both PUs and SUs by meddling with the former and thwarting the latter from accessing the channel. Chen et al [6] used simulations to show that a PUE attack can meritoriously take away bandwidth from legitimate SUs, and a malicious PUE attack can significantly diminishes the link bandwidth accessible to legitimate SUs.

To defend against PUE attacks, the identity of the transmitting source needs to be distinguished accurately. Three main approaches are proposed, localization, signal detection and authentication.

A scheme for PU identification relying on PU location was presented in [7]. Their proposal was based on the fact that for numerous cases, PU's locations are known. In IEEE 802.22 standard, transmitters are TV towers, which are fixed and predefined. SUs are only allowed to use white TV channels. The proposed methodology defined an architecture based on trusted location verifiers (LVs), which are responsible for verifying whether a signal is being transmitted by a PU or an attacker emulating a PU. This is achieved by searching its location in the known PUs locations database. Identifying the transmitter location can be obtained either by the Distance Ratio Test (DRT) technique, which is based on received signal strength measurements, or by the Distance Difference Test (DDT) method, which is based on signal phase difference.

Authors in [6] focused on counter-measuring the PUE threat by proposing a transmitter verification scheme called *LocDef* (Localization Based Defense). It verifies whether a given signal is of an incumbent transmitter by guessing its location and observing its signal characteristics. *LocDef* carries out transmitter verification following three steps: verification of signal characteristics, measurement of received signal energy level, and localization of the signal source. It uses RSS-based (Received Signal Strength) localization and relies on the relationship between signal strength and a transmitter location. To collect the RSS measurements, an underlying Wireless Sensor Network (WSN) was used.

Both techniques can be misled if an attacker transmits from a close location to a real PU. Furthermore, an attacker can collect enough statistical information on a PU's signal to replicate its characteristics. Also, these techniques are not applicable when completely mobile networks are used.

Authentication is an alternative efficient solution to distinguish real PUs and mitigate PUE attacks. Chandrashekar et al [4] defined a PU authentication system in order to provide SUs with secure and reliable information about PU activity. This system relies on a network of "helpers" which are deployed to assist with PUs localization and detection. Cryptographic signatures are used to secure communications [14].

An analytical model for detecting Primary User Emulation attacks was introduced in [1]. The authors used simplified propagation models to compute the probability of a successful PU emulation. An authentication method based on a network of monitoring nodes is another approach [5]. Monitoring nodes verify the origin of PU signals based on the received signal strength (RSS) measurements. If the anticipated location of a PU deviates from the actual PU location by some threshold, the signal is assumed to be emulated.

The above mentioned authentication methods are subject to some limitations. FCC specifications state that no modifications are allowed on the PU network. This makes authenticating the PU a very challenging endeavor. Moreover, mobility of SUs and PUs is not handled properly in existing solutions. Further work to deter PUE attacks is undoubtedly needed.

## VI. CRN SECURITY REQUIREMENTS

### A. *Availability*

Within CRNs, the Base stations (BSs) should ensure the availability of spectrum needed by PUs and SUs. BSs should be equipped with the needed security measures to deter DoS attacks including distributed DoS.

### B. *Authentication*

To ensure that CRN devices and components are communicating with a legal party, PUs, SUs, and other devices, authenticating them is essential. This applies to BS authenticating CRNs and CRNs authenticating each other. All components involved in the CRNs must be able to identify other legitimate devices and systems. Various cryptographic techniques are used for this purpose. CRNs should be capable of preventing or at least detecting various attacks on cryptographic protocols including man-in-the-middle attack.

### C. *Integrity*

It is demanding to ensure that the messages sent by BS, CRN, PU, or SU have not been modified when arriving at their destination. This assurance entitles that the messages received have not been through any modification, insertion, deletions, or replay on its way to its destination. Commands and signals issued by various constituents of the CRN are critical messages, and therefore, need to be clear of any modifications. Cryptographic hash functions and MACS need to be adopted to ensure message integrity.

### D. *Confidentiality/Privacy*

PUs and SUs are interested in keeping their communications confidential. They want to ensure that their messages are only disclosed to the authorized CRNs, PUs, and SUs. In many applications, such as healthcare applications, privacy is essential. CRNs should adopt cryptology to enforce privacy.

### E. *Nonrepudiation*

Communicating parties with the CRN infrastructure do not want the receiver to deny receiving a message (destination nonrepudiation), and the sender to deny sending a message (source destination). Cryptology can be deployed to ensure, for example, that a CRN cannot deny it has received a request for spectrum from PUs and SUs, and a CRN cannot deny a message received from a BS.

## VII. CRN SECURITY ENHANCEMENTS

In this section, possible security enhancements to cognitive radio networks are suggested.

1) For passive eavesdropping attack, messages need to be encrypted and time stamped and nonce added to prevent replays. PUs and SUs will verify the message and only accept it if it is verifiable. To prevent impersonation attack, anonymous IDs are recommended. The BS or CRN node will issue anonymous IDs for all PUs and SUs. These anonymous IDs will be changed at the same time the encryption key is changed. Even if this anonymous ID is captured, the attacker will not know whose ID it is to impersonate.
2) To counter attack a selective forwarding attack, the CR node or BS can establish a timing limit. If this limit is exceeded and the PU or SU has not received the message, it will inform the BS through another secure node. The BS will then resend the message using that route or another one if needed. Certainly, messages must be encrypted so that the malicious CR will not extract any useful information from the message.
3) To prevent an attacker from actually providing a false high quality route to a sink in case cognitive sensor networks are used, CR nodes can request certificates. These certificates could be issued by BS or by a Cognitive Radio Network Authority. In addition, CR nodes can forward the info about that high quality sink to the BS for verification.
4) To thwart the possibility of a single CR node pretending to be present at different locations of the network (Sybil attack), anonymous IDs need to be used and changed frequently. In addition, requiring certificates is necessary to further counter measure this attack.
5) To counter measure the possibility of Wormholes, the BS must provide each node with the anonymous IDs of the neighboring nodes and the distances from each one of these nodes. All this information must be encrypted. Any wormhole trying to convince two distant CR nodes that they are neighbors will fail when they check their list of anonymous IDs and distances to verify that claim.
6) For Hello Flood attack, certificates and authentication need to be enforced. Furthermore, routing protocols that use link layer acknowledgments must be replaced by more secure protocols.
7) To account for hardware attacks, hardware encryption must be provided. This prevents attackers from accessing the hardware of node, and consequently will not be able to shut down a CR node.
8) To resist software attacks, tamper-resistance, intrusion detection systems, and virus detection techniques should be incorporated to deter any malicious software installations.
9) Dealing with primary user emulation attack is not easy. However, the most important characteristics could be hashed or digitally signed. Therefore, the destination node will verify these characteristics first before responding. This can apply to the signal too. Further details are provided in section V above.
10) As mentioned above, jammers transmit a signal to the receiving antenna of the CR with the same frequency as that of an authorized transmitter. CRs should check IDs, certificates, and possibly authenticate the transmitting node whenever a signal with the same frequency is received.
11) Byzantine attack should be mitigated with enforced authentication schemes between sensing SUs and the fusion center. The fusion center must verify any sensing information received from CR nodes in order to assess their integrity. Authenticating CR nodes can avoid receiving and using misleading information about PU activities, which can be disseminated by malicious nodes. In case of completely distributed and cooperative sensing, PKI schemes should be established to manage identity verification.

## VIII. CONCLUSION

Available spectrum, which is a very valuable resource in wireless communication systems, has been exhausted by the static spectrum allocation policy. Cognitive radio is a promising concept which uses the available spectrum more efficiently through opportunistic spectrum deployment. Security is one of most critical concerns in these networks because of their inherent vulnerabilities. Safeguarding the priory of access to primary users is of utmost concern in CRNs. Hence, it is not surprising that the Primary User Emulation attack has drawn considerable attention. As security has a significant priority in CR networks, the security threats that face CRN were discussed, and some of the PUE countermeasures were analyzed. Furthermore, ensuring that the CRN security requirements are satisfied is a vital issue facing our security measures.

## REFERENCES

[1] S. Anand, Z. Jin, and K. Subbalakshmi, “An analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks,” *in Proc. 3rd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Chicago, IL, 2008, pp. 1–6.

[2] S. Bhattacharjeea, S. Sengupta, and M. Chatterjeea, “Vulnerabilities in Cognitive Radio Networks: A Survey,” *Computer Communications*, Vol. 36, No. 13, 2013, pp. 1387–1398.

[3] J. L. Burbank, “Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security,” *in Proc. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008)*, Singapore, 2008, PP. 1-7.

[4] S. Chandrashekar, and L. Lazo, “A Primary User Authentication System for Mobile Cognitive Radio Networks,” *in Proc. 3rd International Symposium on Applied Sciences in Biomedical and* Communication Technologies (ISABEL), Rome, 2010, pp. 1-5.

[5] O. B. Akan, O. B. Karli and O. Ergul, Cognitive Radio Sensor Networks, IEEE network, vol.23, 2009, pp.34-40.

[6] R. Chen, J. Park, and J. H. Reed, “Defense against Primary User Emulation Attacks in Cognitive Radio Networks,” IEEE Journal on Selected Areas in Communications, Vol. 26, No. 1, 2008, pp. 25-37.
[7] R. Chen, and J. Park, “Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks,” in Proc. First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, VA, 2006, pp.110-119.
[8] C. Cordeiro, K. Challapali, D. Birru and N. S. Shanka, “IEEE 802.22: The First Worldwide Wireless Standard based on Cognitive Radios,” *in Proc. First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Baltimore, MD, 2005, pp. 328-337.
[9] Federal Communications Commission, Notice of Proposed Rule-Making and Order: “Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies,” ET Docket No.03-108, 2005.
[10] G. A. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, “A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks,” *IEEE Communications Surveys and Tutorials*, Vol. 15, No. 1, 2013, pp. 428-445.
[11] IEEE 802.22 Standard, Available: http://www.ieee802.org/22/.
[12] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks Using Hypothesis Testing,” *ACM Mobile Computing and Communications Review*, Vol. 13 No. 2, 2009, pp. 74–85.
[13] X. Li, and W. Cadeau , “Anti-Jamming Performance of Cognitive Radio Networks,” *in Proc. 45th Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, 2011, pp. 1-6.
[14] Y. Liu, P. Ning, and H. Dai, “Authenticating Primary Users’ Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures,” *in Proc. The 2010 IEEE Symposium on Security and Privacy*, Oakland, CA, 2010, pp. 286–301.
[15] M. Mangai, S. Sundaram, N. Fernando, V. Daniel, and S. Babu, “A State of the Art Review on Various Security Threats in Cognitive Radio Networks,” *International Journal of Computer Science and Mobile Computing*, Vol. 2, No. 12, 2013, pp. 128-144.
[16] G. Mao, and L. Zhu, “An investigation on security of cognitive radio networks,” *in Proc. International Conference on Management and Service Science (MASS)*, Wuhan, 2011, pp. 1-4.
[17] O. Olabiyi, A. Annamalai and L. Qian, “Leader Election Algorithm for Distributed Ad-Hoc Cognitive Radio Networks,” *in Proc. the 9th Annual IEEE Consumer Communications and Networking Conference - Wireless Consumer Communication and Networking*, Las Vegas, NV, 2012, pp. 859-863.
[18] R. Pal, D. Idris, K. Pasari, N. Prasad, “Characterizing Reliability in Cognitive Radio Networks,” *in Proc. First International Symposium on Applied Sciences on Biomedical and Communication Technologies, (ISABEL '08)*, Aalborg, 2008, pp. 1-6.
[19] M. Pan, C. Zhang, P. Li, and Y. Fang, “Joint routing and link scheduling for cognitive radio networks under uncertain spectrum supply,” *in Proc. IEEE INFOCOM*, Shanghai, 2011, pp. 2237-2245.
[20] A purva N. Mody, R. Reddy, T. Kiernan, and T. Brown, “Security in Cognitive Radio Networks: An Example Using the Commercial IEEE 802.22 Standard,” *in Proc. IEEE Military Communications Conference (MILCOM 2009)*, Boston, MA, 2009, pp. 1-7.
[21] Y. Saleem, A. Bashir, E. Ahmed, J. Qadir, and A. Baig , “Spectrum-Aware Dynamic Channel Assignment in Cognitive Radio Networks,” *in Proc. International Conference on Emerging Technologies (ICET)*, Islamabad, 2012, pp. 1-6.
[22] G. A. Safdar, and M. O’Neill, “Common Control Channel Security Framework for Cognitive Radio Networks,” *in Proc. IEEE 69th Conference on Vehicular Technology*, Barcelona, 2009, pp. 1-5.
[23] S. Sengupta, and K. P. Subbalakshmi, “Open Research Issues in Multi-Hop Cognitive Radio Networks,” *IEEE Communications Magazine*, Vol. 51, No. 4, pp. 168-176, 2013.
[24] M. Youssef, M. Ibrahim, M. Abdelatif, L. Chen, and A. V. Vasilakos, “Routing Metrics of Cognitive Radio Networks: A Survey,” *IEEE Communications Surveys and Tutorials*, Vol. 16, No. 1, pp. 92-109, 2014.
[25] T. Yucek, and H. Arslan, “A Survey of Spectrum Sensing Algorithms for Cognitive Radio Applications,” *IEEE Communications Surveys and Tutorials*, Vol. 11, No. 1, pp. 116-130, 2009.
[26] Y. Zhao, M. Song, and C. Xin, “FMAC: A Fair MAC Protocol for Coexisting Cognitive Radio Networks,” *in Proc. IEEE Conference on Computer and Communications (INFOCOM)*, Turin, 2013, pp. 1474-1482.
[27] Y. Zou, X. Wang, and W. Shen, “Physical-Layer Security with Multiuser Scheduling in Cognitive Radio Networks,” *IEEE Transactions on Communications*, Vol. 61, No. 12, pp. 5103-5113, 2013.

ISBN: 978-988-19252-7-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)