Spectrum Sharing Security and Attacks in CRNs: a Review

Wajdi Alhakami, Ali Mansour and Ghazanfar A. Safdar
Department of Computer Science and Technology, University of Bedfordshire
Luton, LU1 3JU, United Kingdom

***Abstract*—Cognitive Radio plays a major part in communication technology by resolving the shortage of the spectrum through usage of dynamic spectrum access and artificial intelligence characteristics. The element of spectrum sharing in cognitive radio is a fundamental approach in utilising free channels. Cooperatively communicating cognitive radio devices use the common control channel of the cognitive radio medium access control to achieve spectrum sharing. Thus, the common control channel and consequently spectrum sharing security are vital to ensuring security in the subsequent data communication among cognitive radio nodes. In addition to well known security problems in wireless networks, cognitive radio networks introduce new classes of security threats and challenges, such as licensed user emulation attacks in spectrum sensing and misbehaviours in the common control channel transactions, which degrade the overall network operation and performance. This review paper briefly presents the known threats and attacks in wireless networks before it looks into the concept of cognitive radio and its main functionality. The paper then mainly focuses on spectrum sharing security and its related challenges. Since spectrum sharing is enabled through usage of the common control channel, more attention is paid to the security of the common control channel by looking into its security threats as well as protection and detection mechanisms. Finally, the pros and cons as well as the comparisons of different CR-specific security mechanisms are presented with some open research issues and challenges**.

Keywords—Dynamic Spectrum Access; Spectrum Sharing; Common Control Channel; Cognitive Radio Networks

I. INTRODUCTION

Cognitive Radio (CR) [1] technology promises to intelligently solve the issues in conventional wireless technology related to their limited and under-utilised spectrum [2]. This problem has become an issue of great concern given the continued increase in wireless devices that use unlicensed bands to operate, which has resulted in overcrowding, leading to inefficient use of the spectrum [3-5]. Therefore, CR provides a resolution to spectrum inefficiency and the shortage on these bands by allowing CR users (secondary users (SUs)) to opportunistically access vacant spectrum space [6]. This results in providing great opportunities for a rising number of SUs to use these bands through an optimised approach for utilising radio resources [7-8].

radio networks' (CRN) technology has its own intrinsic fundamental approach and principles for dynamic operation within the environment, unlike in the conventional wireless approach, which is based on the static radio frequency spectrum with fixed licensed users (primary users (PUs)) and fixed channels [9]. This indicates that the cognitive ability and reconfiguration capability are the core elements that make CR an advanced technology, which grants dynamic access to the unused spectrum for both licensed and unlicensed users through certain characteristics: adoption, awareness, modification, capability of learning, observation, and communication in realistic environments [10-16]. These characteristics provide reliable communication among CR users anytime and anywhere as a smart and intelligent choice to operate dynamically through artificial intelligence algorithms, such as spectrum sensing, spectrum sharing, and spectrum mobility [13, 17]. Moreover, they differentiate this new CR technology from existing wireless technologies. Due to these sophisticated features, the CR approach is known as Dynamic Spectrum Access (DSA) or Dynamic Spectrum Management (DSM) [8,18], in recognition of the potential to realise dynamically different paradigms within a network.

However, generally DSA is considered a big challenge to implement because of its dynamic behaviour and nature, such as different frequency, geographical location, and time of operation [19-20]. Also, SUs might utilise the licensed spectrum and encounter PUs who have diverse transmission characteristics. Moreover, in comparison to known security issues that exist in wireless networks, CRNs are more exposed to threats from targeted, intelligent malicious strategies [21-22]. This poses security challenges in preventing any definite or predictable risks from occurring.

As long as spectrum sharing is one of the fundamental aspects of the CR to provide access channels and sharing resources, this overview paper mainly focuses on the spectrum sharing security of the cognitive radio MAC layer. So far, most of the literature focuses on general aspects of CRNs security in spectrum sensing and spectrum mobility-related areas. But the security of spectrum sharing has received very little research coverage. It is very important to conduct thorough research to gain a broader and clearer overview of its techniques and security-related issues.

Therefore, this overview paper firstly provides details about the spectrum sharing classification, to show the differences of the mechanism, operation, and techniques. Subsequently, it focuses and gives detailed insights into the threats and attacks that are launched in the common control channel (spectrum sharing) part of MAC layer of CRNs. In addition, it investigates and includes the recent techniques that have been developed in this area in terms of protection and detection.

This paper is organised as follows: Section 2 briefly demonstrates the CR main functions and section 3 looks into the security challenges in cognitive radio's core functions, especially in spectrum sharing, i.e. common control channel security. Section 4 discusses common security threats to both traditional wireless and cognitive radio networks. It then concludes by outlining security threats specific to CR networks. Section 5 introduces the existing security methods for achieving secure communications in both centralised and ad hoc CRNs. Section 6 identifies some open research issues and challenges before the paper is concluded in section 7.

II. Cognitive Radio Core Functions

There are four fundamental functions which the CRN device must perform, as shown in Figure 1 and as stated below [8, 23]

1) ***Spectrum sensing*** *identifies the parts of the accessible spectrum and senses the presence of the PU operating in the licensed band.*

2) ***Spectrum management*** *determines the best channel to establish communication.*

3) ***Spectrum sharing*** *sets up a coordination access among users on the selected channel.*

4) ***Spectrum mobility*** *vacates the channel in case the PU is detected.*

One failure can easily affect and result in deterioration of the communication or introduce vulnerabilities to the network.

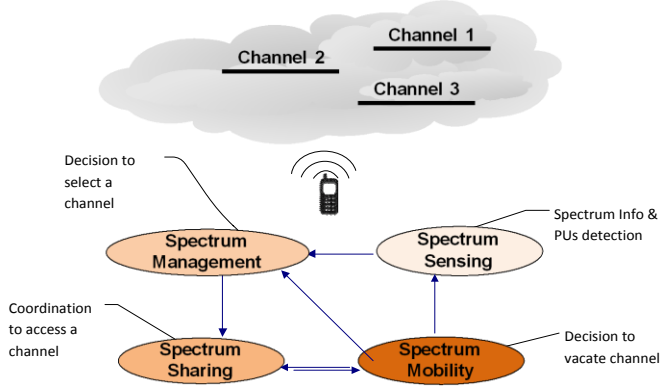

Fig. 1. Cognitive radio main functions

These embedded functions have a strong relationship between them for the process of establishing an efficient communication, considering the regulations and policies that govern CRNs. Each function influences another one by providing the necessary information required during the process of reaching a final decision. For instance, once the spectrum is sensed, in order to identify the available point of access, there are two possible decisions that can be taken: If the PU is detected then the process will be discontinued; if they are not, the obtained information will move forward to the next stage. The spectrum management function then decides and selects the proper channel for the communication. Once the channel is chosen, users are directed to access it by providing their information. During a successful communication, spectrum mobility remains ready for any changes that resulted from the appearance of a PU by a regular check of the spectrum sensing, or from other alterations to the environment in terms of the current allocation that is provided by spectrum management and spectrum-sharing elements [8, 24].

As long as CRNs have a set of nodes that interact with each other using determined policies, regulations, and sophisticated protocols [25], they have different capabilities [22, 26] relating to the spectrum awareness of the network operation and spectrum context, defined regulations and policies, quality of service (QoS), and user requirements for requesting traffic load capacity, resilience, and security. This means that cognitive nodes are able to dynamically reconfigure themselves according to the current environment in order to transmit and receive on different frequencies, in addition to supporting a variety of transmission access technology schemas [2, 27]. Another capability is resource management, which plays an important role in collaborating to assign the vacant network spectrum management resources, whether these are internal to the current network or external to conventional wireless networks [8, 28].

Spectrum sharing generally can be classified into three major criteria, based on the network architecture, access technology, and allocation behaviour (Figure 2). Descriptions of these classifications as follows:

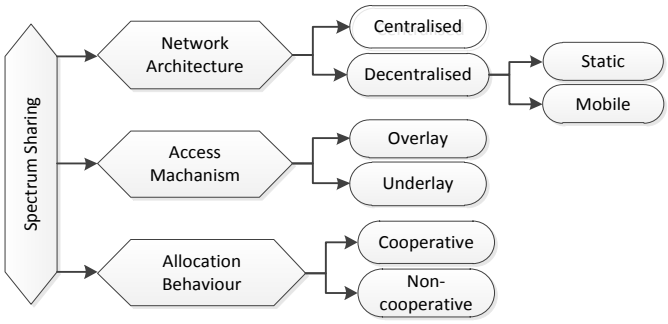

Fig. 2. Spectrum sharing classfications

The first technique is based on the network architecture, whether it is a centralised or distributed system (Figure 3). In centralised networks such as IEEE 802.22 cognitive radio, a base station governs and senses the free channel information from neighbours' nodes within range and performs the final decision on the availability of a channel. Unlike ad hoc CR networks, CR nodes generate and utilise a common spectrum allocation for the information exchange about available channels [8, 22]. Even though the centralised entity has the advantages of addressing better efficiency, the main drawback is that a single point of failure can be easily launched to the central entity [8]. More classifications can be added to ad hoc networks, classifying them into static and mobile networks. These apply in wireless sensor networks as a static form and in MANET (Mobile Ad-hoc Network) as mobile ad hoc networks in which a set of autonomous mobile terminals are liberated to move to other existing hybrid networks [29, 30] (more details about comparing the spectrum sharing mechanisms in both centralised and distributed architectures are discussed in [31]).

The second technique is based on allocation behaviour, whether it is cooperative or uncooperative. In the cooperative method, CR users are responsible for coordinating the

functionalities of the cognitive network in order to ensure the optimisation of the spectrum utilisation and improving network efficiency through the exchange of information. However, in non-cooperative systems, CR users are not responsible for coordinating the cognitive functionalities with other cognitive devices. Instead, they implement these functions on their own [24, 32]. The main difference between these two methods is relatively clear: the first approach essentially requires the exchange of information; hence a common control channel (CCC) is required to facilitate the information exchange. However, in the second approach, the cognitive nodes do the network functions tasks on their own without the need for any collaboration from other cognitive users. This would make the task more challenging and difficult for a cognitive user. In addition, this can affect the performance due to reasons like lower efficiency, slower sharing of spectrum resources allocation, and less reliability than the cooperative technique [8, 16, 24, 33].

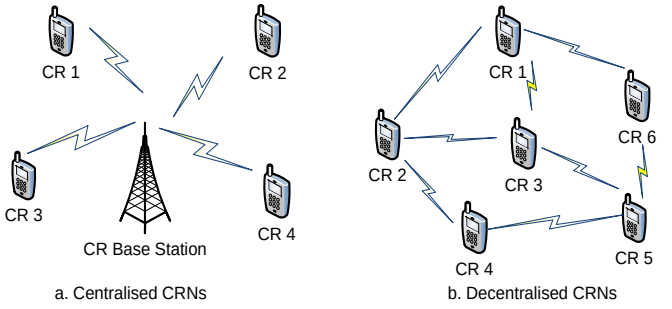

Fig. 3. Cognitive radio architecture

The last classification is access technology, whether it is an overlay or underlay approach [22, 24, 26, 34]. In the overlay approach a SU utilises the spectrum without sharing with a PU. This is in contrast to the underlay approach, in which both PUs and SUs utilise the licensed spectrum at the same time [35-38], with strict power control implemented by the CR users not to interfere with the PUs.

III. Security Callenges in CRN Core Functions

Due to the key differences in their specifications when compared to traditional wireless networks, cognitive radio networks face certain unique challenges in terms of their continued effective use and their vulnerability to outside attack. These particular characteristics of CRNs involve the need for additional implementation of specific functions, such as proper sensing protocols, correct decision making, appropriate switching, and the provision of sufficient access for the sharing of the resources required to operate each particular function. These challenges can be classified into four main areas, which will be described in greater detail in the following subsections:

A. Spectrum Challemges in Spectrum Sensing

The fact that spectrum sensing is responsible for sensing channels and the provision of accurate results means that CRNs must overcome certain specific challenges. The challenges broadly pertain to the ways in which a cognitive user detects and differentiates between PUs and SUs. This is of great importance as attackers may be able to emulate the signals of the PUs, thereby increasing the likelihood of false alarms being triggered. In addition, the hidden node problem may be another issue that can lead to a failure to detect the PUs, which would result in unacceptable shadow fading [6, 39].

B. Spectrum Challenges in Spectrum Management

An incorrect decision made by the spectrum management is a significant issue that could arise relatively easily. Also, the inherent complexity of the protection techniques is a key requirement to providing reliable and secure transmission of information among users. It is possible for an attacker to easily forge or tamper with the transmitted information, which would affect the correctness of any decisions made by the spectrum management.

C. Security Challenges in Spectrum Mobility

The requirement for a seamless handoff from one channel to another also constitutes a significant challenge for cognitive users when an attacker launches a threat to hinder or prevent this integral and flawless switching by occupying the available channels. This kind of attack could potentially increase the waiting time involved in achieving a proper handoff. This increase is certainly unacceptable to the PUs, who wants to utilise their assigned channels.

D. Security Challenges in Spectrum Sharing

The dynamic environment in MANET network architecture leads to more challenges and security issues arising due to the lack of the central entity which usually provides security and key management among users [40]. The control channels selection in decentralised cognitive radio networks decreases the probability of successful communication among SUs due to authenticity and validity. As discussed in [11], SUs are the non-licensed users and attackers easily exploit them and by escalating their privileges, they might damage the spectrum and the traffic of the PUs as well. Moreover, without security, this issue becomes more critical when cognitive nodes use the spectrums only when PUs are not available or not using their licensed bands. Moreover, selecting data channel(s) for exchange of data among SUs without the authenticity of the SUs is another issue that needs to be addressed in CRNs, especially for maintaining the links if a PU returns to the licensed channel.

Much research has been conducted into developing security in centralised CRNs [1-3]. However, the issue is that no research has been carried out on addressing the authentication in decentralised CRNs and its requirements, especially providing authentication of confidentiality, non-repudiation, and integrity, which are considered the main security elements in cognitive radio technology.

IV. Security Threats

Although cognitive radio is similar to the traditional wireless network, using a wireless medium instead of a wire to transmit information, it faces different vulnerabilities, which has resulted in the discarding of the communication process among end users [41-42]. These vulnerabilities can leads to varied threats, which can be classified into two different categories: the first relates to common security threats in both conventional wireless and CR networks, and the second category is specific to CRN users.

A. Common Security Threats in Conventional Wireless and CR Networks

In traditional wireless technology, radio channels are used to establish communication and transmit information between communicating nodes and access points (APs) or base stations (BSs). They are used in cognitive networks to address several similar functionalities. The transmitted information can be sensitive, such as the user's identity, the user's privacy, allocation and signaling information, as well as key information. However, an attacker using a range of techniques such as eavesdropping, forgery, and masquerading attacks can easily intercept the communication during the transmission process [9, 13]. An effective security mechanism must be applied to protect data transmission from malicious behaviour like eavesdropping and information tampering [29]. Therefore, as far as data protection is concerned, different security measurements can be used for protection, detection, and countermeasures based on wireless security protocols such as WEP, WPA, and WPA2 in conventional wireless networks and EAP, AES, and 3DES in WiMAX. These security protocols are designed with encryption levels of different strengths being used according to the importance of the information being secured. Figure 4 shows the most common threats in both traditional wireless and CR networks.

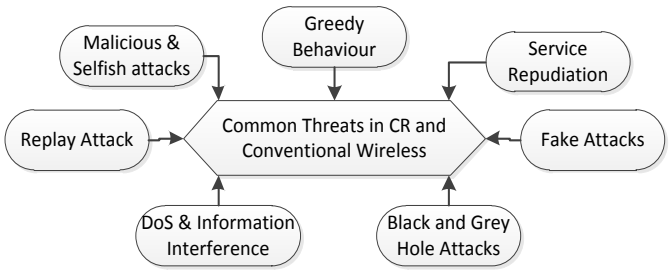

Fig. 4. Common security threats in conventional wireless and CR Networks

1) Fake Attacks

In the infrastructures of wireless networks, BSs or APs act as central entities that are connected wirelessly to end terminals. In order to establish communication, some information is exchanged through a radio channel between the end terminal device and the central entity. This information includes the identity data belonging to the procedures of the network control, network services and network access. A malicious user can obtain this information by wiretapping and then pose as a legitimate user. The purpose of this fake attack is a malicious user accesses the network and obtaining a network service or to launch an attack against the network [13, 43-44]. Therefore, cryptographic encryption schemes are generally used to protect the transmitted messages.

2) Information Tampering

This is a serious attack that causes change, modification, replacement, or deletion of the information before it is received at its intended destination [43], and that result in misleading the receiver, who can thus make a wrong decision. Alteration significantly affects message integrity, which is unacceptable for legitimate users and network policies. However, this type of attack generally occurs in a situation where a cooperative terminal is needed to forward the information [13, 45-46].

3) Service Repudiation

In this attack, when the connection is achieved between two nodes, one user denies transmitting their information for two reasons: repudiation for the communication service to deny usage of the network, which requires payment for the network usage, and repudiation for the communication content to refuse the transmission of their content. For example, when transactions are made in a commercial process, the user refuses to pay. To overcome these issues, proof-of-origin evidence can be used against a particular individual for sending or receiving messages. Identity, authentication, and cryptography encryption schemas are presently used to prevent unpredictable or hidden issues arising [13, 47].

4) Replay Attack

The key purpose of this attack at the MAC layer is to obtain effective information by intercepting and retransmitting the same signed information sent to a particular node over a period of time in order to build trust with the receiver. This gives an advantage to the attacker, granting them access to new useful information like user passwords, which then enables unauthorised access to resources and control network licenses, etc [13, 48-52]. Therefore, in order to overcome this attack, the timestamp procedure is recommended because of the message validation involved [52].

5) Denial of Service and Information Interference

While electromagnetic waves are essential in order to gain wireless information from users, recent advanced hardware technologies can involve a higher transmitted power in the communication process at the physical layer. It is, therefore, possible for an attacker to use this transmitter power to block the ordinary transmission and create interference and noise in the communication procedure, thereby decreasing the capacity of the wireless BS resources and equipment. This can also lessen user access through a BS terminal. Therefore, the interference of information procedures is likely to have a critical social impact [53]. An example of this occurred in 2001, which the satellite communication service was interrupted due to the high power caused by locating a VSAT terminal [13, 50].

6) Greedy Behaviour Attack

During the channel negotiation process in both centralised and decentralised multi-hop networks, an attacker intends to maximise their throughput of using a spectrum through manipulating and changing the parameters of the MAC layer protocol [54-57]. This is achieved by reporting false information regarding the available channel, which causes throughput collapse for other users. For instance, in decentralised networks, if a greedy user attempts to misbehave by starving the neighbouring node, the intermediate user will be affected and banned from transmitting its messages [13].

7) Malicious and Selfish Behaviour Attacks

In malicious behaviour, the attacker makes other cognitive users to make handoff from the current channel. This generally causes degrading of the network performance [29, 41, 57-58]. However, in selfish behaviour, the attacker intends to maximise their throughput by using a spectrum to disturb the normal process [59].

8) Black and Grey Hole Attacks

Both black and grey hole attacks exist in decentralised networks, where an attacker pretends to be the destination node. Therefore, a sender can be easily deceived and start transmitting packets. The rate of dropping the transmitting packets is used to distinguish between these two attacks. In a black hole, the malicious user obtains all the transmitted packets; however, in the grey behaviour attack, a malicious user drops part of these transmitted packets [29, 60-66].

B. Specific Security Threats in CR Networks

Several potentially serious threats to network performance which increase spectrum availability to malicious users have been highlighted by researchers investigating CRN technology [9, 13, 67]. Moreover, due to the unique characteristics of CRNs, they are more exposed to security threats which are usually not faced by conventional wireless technology. Therefore, security mechanisms play an important role in maintaining the network that is potentially affected by these kinds of threats [13]. Malicious attacks are well known threats that target all layers in the CRN [9, 13] with their own behaviour, which can affect network performance by attacking a particular layer. Some of the main security threats related to CRNs are identified in Figure 5.

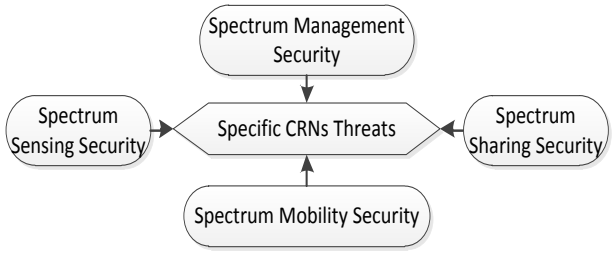

Fig. 5. Specific security threats in CRNs

1) Security in Spectrum Sensing

Spectrum sensing is a major aspect of CRNs environments, providing the spectrum information about the appearance of the PU and the available channels [12, 32-33, 68]. Therefore, it is subjected to the most prevalent attacks that bring the network performance down by reporting the false results of the PU detection. As long as the security in spectrum sensing is concerned with controlling the network operation, attackers have their own malicious behaviour strategies, focusing instead on degrading the network spectrum performance by causing collisions or occupying the spectrum. This can result in potential security vulnerabilities that enable denial of service (DoS) attacks to be launched easily [67]. Thus serious attacks can occur at this level of the spectrum, which are called primary users interference (PUI) and primary user emulation (PUE).

In PUE, an attacker can simulate a signal that resembles the signal of the PU, thereby misleading the SU [2, 12, 18, 58, 69-73]. In this case, the attacker has a chance to focus on the physical layer, pretending to be an authorised user by sending CR signals that are similar to PU signals, allowing them to deceive other SUs. This increases the availability of spectrum to the malicious user. The authors of [6, 41, 74] have proposed a simulation technique used by a malicious user, which involves a multiple stage attack that demonstrates the general influence on the network performance and other special effects on the SUs. Additionally, the authors' experiment results showed how the relationship between the performance improvements can be associated with the bands' availability and vice versa. However, in PUI, the attacker breaks the rules of the CRN mechanism by affecting network performance through interfering with PUs within the network. This forces the PU to use spectrum with noise and unavailable frequency band [13]. This is also called a jamming message attack or lion attack, where an attacker transmits high signal power to disturb the PUs through TCP connection [9, 41, 43, 75].

Several researchers have investigated and proposed algorithms to detect malicious behaviours in cooperative sensing of the spectrum in order to improve security in this stage. A detection scheme based on a past test report obtained through calculating the suspected point of secondary users, and computing the value of trust behaviour mechanism, is proposed in [74]. The proposed algorithm is able to distinguish malicious from honest users within a network. However, [76] presented a data mining technique without needing priori information about a secondary user to detect misbehaviours. In addition, [67] explained that changing the spectrum modulation system strategy and protecting the location information of the PU, and using proactive techniques in transmission, can help to prevent DoS attacks at this stage.

2) Security in Spectrum Management

Spectrum management is considered to be the second task after obtaining the result from spectrum sensing. Once the available bands are allocated, spectrum management determines the proper spectrum for communications based on the desired characteristics for quality of service (QoS) [22]. However, this stage cannot be safe from attacks. A forgery attack or tampering attack is designed to attack this particular level of the network element and involves the attacker transmitting incorrect spectrum sensing information to the data collection centre in order to deceive the secondary user, encouraging the wrong decision from spectrum management, which enables the malicious user to utilise the channel with superlative adaptive purpose [13, 67].

3) Security in Spectrum Mobility

This stage refers to the mandatory process of seamlessly switching (handoff) from a current channel to another available one due to channel occupancy by the PU. With the appearance of the PU to utilise their assigned channel, a SU must vacate and select another available channel to initiate a new connection, resulting in greater energy consumption [22, 67, 77-78].

However, from a security perspective, the availability of spectrum is reduced when there are a large number of malicious users, and this limited availability affects other legitimate SUs, who are required to vacate the current channel due to the appearance of the PU and to select another available channel [53, 78]. Moreover, a failed handoff to a proper channel may occur when an attacker forces SUs to vacate the channel by pretending to be the PU. As a consequence, it results in slower communication and requires additional time to resume the process of the communication [18, 22, 69].

4) Security in Spectrum Sharing

As long as spectrum sharing is crucial to maintaining effective communication in traditional wireless networks through the application of the Medium Access Control (MAC) method, it is an area of great interest for a number of researchers, who have proposed different solutions for sharing the spectrum [80, 81-83]. These solutions include a non-dedicated common control channel [84], a hopping-based control channel [85] and a dedicated CCC, also known as a Dynamic Local Common Control Channel (DLCC) [86] (Figure 6). These approaches focus on achieving a proper level of sharing among cognitive users. In this paper, a brief explanation of the first two approaches has been given, while the third approach is the main one which is considered in detail.

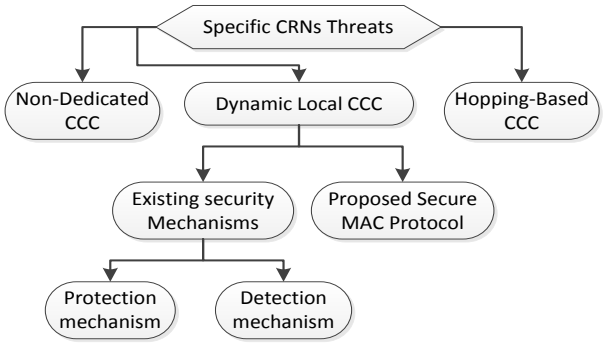

Fig. 6. Specific security threats in CRNs

a) Non-dedicated CCC

In this approach, a predefined non-dedicated CCC is assumed among a set of SUs. Hence, a number of CRN MAC protocols are designed for predicting that a CCC is already recognised and allocated to those SUs. Industrial, scientific and medical (ISM) or underlay ultra-wideband that is identified as unlicensed band can be the appropriate place to implement a control channel for cognitive users in order to exchange the control information [78, 80, 88].

b) Hopping-based Control Channel

This approach requires a predefined channel hopping sequence that is determined among SUs in order to achieve the hopping process over the existing licensed channels [87]. Both the cognitive sender and receiver necessitate time and channel synchronisation [5]. During this process, a proper channel is determined to be utilised to transmit data through exchange of control information between the sender and the receiver. Once successful control information is exchanged between both SUs, they end the hopping process and start with the second phase of transmitting data. After the completion of the data transmission phase, the synchronisation requests are recurred with the hopping sequence [23, 80].

c) Dynamic Local CCC

The CCC technique is one of the methods used to facilitate the functional sharing process between two SUs in distributed cooperative CRNs.

In distributed cooperative systems, CCC is established between both the sender and the receiver for establishing a handshaking protocol [14, 54, 80, 82, 84, 90-91]. In addition, CCC can be used to communicate with a base station through an existing centralised entity system [92]. It is also employed to include the related information that has resulted from the spectrum sensing. Due to these effective functionalities, a number of researchers believe that CCC designed procedures can play a major role in promoting the initial exchange of information processes among cognitive nodes.

However, from a security viewpoint, no spectrum sharing classifications, which are discussed in section 2, are secure against any malicious behaviour while they are not supported with security mechanisms for protection and detection (see table 1). Generally the attackers' intention is to determinate an effective strategy that exposes a predictable risk. For instance, when CCC is used in the cooperative method of decentralised CRNs for exchanging information about the available channels and the selected channel for data transmission between SUs, it is more prone to various attacks based on selfish and malicious behaviours [41-42]. Because it is regarded as a valuable structure for the attacker to access the channel and gain the most sensitive information, a key approach for some types of attackers involves applying a PUE attack. Moreover, it is more exposed to other attack types such as eavesdropping and DoS, which can be launched easily due to existing weaknesses within the MAC layer, where poor authentication and an existing lack of encryption mechanisms enable an attacker to detect available channels that they can occupy to forge or drop MAC frames, as shown in Figure 7 [41, 56, 90].

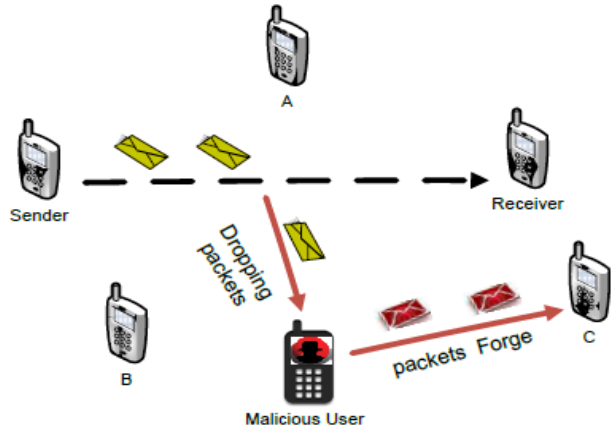

Fig. 7. Malicious activities in decentralised CRNs

Another vulnerability in a CCC is where an attacker forges the transmitted packets to another path and causes collisions. As a consequence, this impedes the network performance and launches a DoS attack. Once a CCC is saturated by attackers, a large number of forged packets are generated to block the exchange of the control information, enabling DoS attacks to be easily launched against the network, hence affecting its performance.

Moreover, an author in [56] suggests that encryption must be applied between legitimate SUs for the exchange of control information; otherwise, it can be readable by attackers of other cognitive users. Also, it can protect the exchanged control information over the channel from predictable control channel hopping sequences, thereby preventing itself from being saturated [13, 92].

TABLE I. OVERVIEW OF THE ATTACKS OCCURRING AT DIFFERENT CR FUNCTIONS

Attack Name	CR function	Description
Forgery & Data tamper	Spectrum Sensing	Spectrum Management system makes wrong decision by receiving the attackers' sensing information
Overlapping		An attacker impacts other networks by transmission to a specific network
Denial of Service		An adversary user decreases the availability of the spectrum bandwidth by blocking the communication, through creating noise spectrum signals which cause interference with PUs
Lion or Jamming message		An attacker transmits high signalling power to disturb the PU or the secondary user which results forcing the cognitive user to hop to different channel to utilise
Spectrum Sensing Data Falsification		In collaborative spectrum sensing, a collaboration technique used among CR nodes to generate and utilise a common spectrum allocation for the exchange of information about available channels. However adversary node gives false observations information to other users.
Eavesdropping	Spectrum Sharing	Weaknesses within the layer due to the poor authentication and no existing encryption mechanisms
Denial of Service & masquerade		Repetition of the frequent packets that result in overcrowding the channel which is being busy to be utilised by legitimated users
Selfish Behaviour or selfish masquerade attack		an attacker does not follow the normal communication process for maximising their throughput, saving energy or gaining unfair beneficial access of using spectrums through injecting frequent anomalous behaviour
Key depletion		An attacker attempts to break the cipher by repetition of the session key
Forgery Attack		Lack of authentication mechanism leads to the occurrence of modification and forgery on MAC CR Frames which result in the launch of DoS attacks
Biased Utility	Spectrum Management	An attacker tries to reduce the bandwidth of other SUs in order to obtain more bandwidth by changing the spectrum parameters
False feedback		An attacker secretes the incidence of the PU in order to disturb the information sensing of other SUs

V. RELTAED WORKS (EXISTING SECURE COMMUNICATION SCHEME IN CRNS)

Since the layers within CRNs have their own characteristics and parameters [74, 93], they are vulnerable and allow an attacker to make a decision to launch a specific attack for the purpose of degrading the whole network performance. In MAC layer frames, an adversary has a variety of aims for misbehaving and launching such an attack. For instance, a denial of the channel service is one of the serious threats that lead to the network degradation between both sender and receiver. This attack occurs when the attacker saturates the CCC till it becomes weak for attacking [8]. In addition, selfish behaviour is another example of an attack that can also exist in the MAC layer, in which an attacker does not follow the normal process of communication. Therefore, in order to provide a defence against these threats, security mechanisms are required in the MAC layer to provide authentication, authorisation and availability (AAA) in the CRNs. Incorporating these security features can lead to the exchange of complete and reliable secure MAC frames among cognitive users [9, 13, 94]. Thus, several studies have been conducted for secure MAC protocols in CRNs [11, 14-15, 94-101]. They are classified into two categories, based on protection and detection techniques for addressing the security requirements and to defend the existing security issues in MAC protocols in CRNs.

A. Protection Mechanism in CRNs

In general, a number of researchers [11, 15, 94-97, 99-100] have made efforts to address the security requirements and provide secure communication among SUs by applying different security mechanisms, such as authentication and authorisation access by different techniques, within a CRN. Their proposed procedures include digital signatures, certification authority (CA), and trust-based third parties entities like server and base stations. While these solutions may be effective in some ways, they have some drawbacks.

1) Digital Signature

In [11, 15, 99] proposed different protection systems based on applying a digital signatures for protecting the network from DoS attacks and providing secure communication. Their approaches involve the activities of a CA, PUs, and both PUs' and SUs' base stations. However, the main differences of these mechanisms are that the BSs are connected to the CA using wire links in [15], while in the [99] approach, an asymmetric key scheme instead of a CA is mainly used.

2) Certificate Authority

Another effective traditional approach-based CA on the application layer for achieving the same purpose of authentication is presented in [100, 101]. The proposed method uses both EAP-TTLS (for establishing a secure connection) and EAP-SIM (for authenticating the user) algorithms.

3) Trust Values Procedures

Other techniques based on trust values procedures are proposed in [95-96] to address and analyse the issues within CRNs. Based on this, the trust value will be calculated, which leads to the decision that will either allow the current user to utilise the available licensed channel or not.

4) Other Framework Architectures

Security for authentication and authorisation architecture frameworks have been proposed in [94, 97]. Both techniques require third-party entities for appropriate access policies to the spectrum. Authors in [94] use a technique based on processing user identification in the system and providing the user preferences to third parties according to privacy rules. Based on this, the user will be authenticated and then will determine whether or not a data port would be used. However the subsequent architecture in [97] consists of two layers, which are up-layers for authentication purpose and encryption techniques, while the physical layer is for securing and protecting the spectrum.

Overall, while these proposed mechanisms are effective in some way for protecting the networks from forgery and DoS attacks, they are not applicable in a decentralised environment

because a third-party node is incorporated in order to verify the identity and provide security key managements to end users. Therefore, the security and challenges in decentralised CRNs still arise and require defensive techniques for securing communication among cognitive users. Table 2 demonstrates the pros and cons of the proposed protection mechanisms.

TABLE II. PROTECTION MECHANISMS IN COGNITIVE RADIO NETWORKS

Proposed Mechanism	pros/ cons	Description
User identification	pro	Low complexity by generating two virtual ports for secure transmission: the first is for control traffic information and another is for data transmission which is blocked by default unless the user has been authenticated.
	con	It requires a third party to provide information like user preferences
Digital signature & certificate authority	Pro	Low complexity and using the basic architectures of symmetric and asymmetric key infrastructures.
	Con	It has not been simulated and tested to proof the security. It also does not work in Ad-hoc environment due to being based on centralised entities.
Certificate authority	Pro	Effective security mechanism due to identifying and verifying the user and the server respectively.
	Con	Requires a third-party to verify the user identity. Also the mechanism has not been simulated and tested to ensure security against malicious behaviours.
Trust values	Pro	It is an additional procedure that can be built on the top of other security techniques to increase the level of the protection and detection in term of secure communication.
	Con	Requires a third party procedure is to provide previous information of a node. Moreover, when a new node joins the network, the CA will not be able to provide reference for that particular user. Hence the mechanism does not operate in strong fixed level of the authentication for all cognitive users equally.

B. Detection schemes in CRNs

Authors in [14, 98,102] have focused on the detection mechanisms in CRNs. Their proposed techniques address a variety of attacks caused by malicious and selfish behaviours, and the pros and cons of these mechanisms are illustrated in table 3.

1) Selfish behaviour

Selfish behaviour detection techniques for the CCC are proposed in [14, 103], where a puzzle punishment model is applied for bad behaviour activities in a situation where a receiver is asked for a new hidden channel that has not been included previously. Thus, the sender would be a suspicious case. Therefore, the receiver applies the puzzle punishment to detect whether the sender is a selfish node or not. If the sender node solves the puzzle, they will be considered as a legitimate user and communication will be resumed normally; otherwise, the communication will be disconnected. Another technique called Cooperative neighboring cognitive radio Nodes (COOPON) is applied among a group of neighbouring users to detect selfish nodes who broadcast fake channel lists. Consequently, neighbouring users can detect the selfish users by comparing the transmitted channel list of the target user with their lists.

2) Timing parameters

Another detection mechanism was proposed in [102]. They presented a mechanism that relies on timing parameters at MAC layer. When the negotiation phase is taking place, the node, which receives a request, sets up timing parameters for controlling the time interval. This forces the sender to transmit data without getting a higher rate. If the sender does not obey and sends packets more frequently, the receiver node takes action against the sender. Then the receiver node analyses the sender's misbehaviour and broadcasts the information over the current network.

3) Anomalous spectrum usage attacks (ASUAs)

The others in [98] presented a cross-layer technique for CRNs for detecting ASUAs. Collecting the information on both the physical and network layers provides an awareness of the current spectrum. It operates against the PUE and jamming attacks to provide successful access to the spectrum.

TABLE III. DETECTION MECHANISMS IN COGNITIVE RADIO NETWORKS

Proposed Mechanism	pros/cons	Description
Selfish activity	Pro	applied in both CCC and data channel which decreases the potential of misbehaviour in different stages of the network
	Con	focuses only on detecting selfish behavior and does not provide the complete secure communication between sender and receiver
timing parameter	Pro	Detecting misbehaving nodes during the negotiation phase. It helps to maintain the channel from getting saturated.
	Con	-Theoretical and has not been simulated and tested to provide the detection scheme results. -Weak against eavesdropping and forgery attacks especially once the FCL is not hidden which is exploited to launch Jamming attacks.
Anomalous Spectrum Usage Attacks	Pro	Combining both physical and network layers for detecting malicious users give a better achievement instead of selecting only a layer
	Con	Focuses only on the detection approach and does not consider a significant protection scheme against both jamming and PUE attacks mobility.

C. Comparisons of the Presented Schemes

Incorporating the security requirements; authentication, confidentiality, non repudiation and data integrity in CRNs can lead to the exchange of complete and reliable secure MAC frames among cognitive users [9, 13, 92]. For instance, while the proposed digital signature, trust value and certificate authority procedures are different in terms of their operations (see the protection schemes in section V), the security requirements are considered for providing defense against most of the MAC threats such as DoS, Forgery, eavesdropping and spoofing in centralised CRNs. In contrast, both puzzle punishment and COOPON approaches consider only selfish behaviour among the other MAC attacks such as DoS, forgery, eavesdropping, and spoofing in decentralized CRNs. However, they are effective in selfish behaviour's detection

due to the cooperation between a group of cognitive users which involve identifying selfish users in COOPON technique and demand of solving the puzzle to resume the communication in puzzle punishment system. Moreover, the timing parameter procedure easily addresses DoS attack due to the presence of the centralised entity, which controls the cognitive users' communication. Table 4 gives information about achieving the security requirements and addressing the MAC layer attacks for each proposed scheme in both centralised and decentralised CRNs.

TABLE IV. COMPARISION OF THE PRPOSED SECURITY SCHEMES IN CRNS

	Puzzle punishment	COOPON	Digital Signature	Trust value	CA	Timing parameter
Authentication			√	√	√	
Integrity			√	√	√	
DoS			√	√	√	√
Forgery			√	√	√	
Eavesdropping & Spoofing			√	√	√	
Confidentiality			√	√	√	
Non-repudiation			√	√	√	
Selfish	√	√				
Architecture	Ad-Hoc	Ad-Hoc	Centralised	Centralised	Centralised	Centralised

VI. OPEN RESEARCH AREAS AND CHALLENGES

As long as secure communication is crucial for the exchange of information between SUs, the primary security concerns in decentralised CRNs are authentication and data confidentiality. Compromising on these elements can potentially lead to the modification, forgery or eavesdropping of the MAC frames in CR networks, which could, in turn, increase the chance of DoS attacks that would adversely affect the performance of the network. However, these security factors in ad hoc CRNs have received relatively little attention in the literature, perhaps due to their complex nature and dynamic topology [104]. These must be investigated properly in order to meet the security needs of the CRNs' technology. Further research is required in order to support the security requirements, especially to provide authentication assurance for the authorised access. These requirements assist in maintaining secure communication and enable the provision of available resources in distributed multi-hop CR environments, while simultaneously avoiding external threats. Moreover, a proper high-level encryption method is required to support secure communication between end users, although due consideration should be given to the inherent power limitations of the devices. This issue is also important because of the lack of a central entity that provides security and key management to end users. Thus, the implementation of a secure CR MAC protocol must involve the design and implementation of a robust, secure system that can achieve authentication, availability, confidentiality, integrity, non-repudiation, anonymity, and authorisation for granting security demands. This is of fundamental importance because CR users need to incorporate security by all possible means to ensure the protection of the relatively vulnerable network operations.

VII. CONCLUSION

Cognitive radio networks are a remarkable area for researchers due to their use of intelligent technology for providing a solution that utilises the available spectrum efficiently. However, security is a crucial aspect of CRNs to achieve successful communication between cognitive users. Due to some unique characteristics in CRNs, different new threats to CR functions exist, such as PUE and PUI in spectrum sensing, Tampering attacks in spectrum management, failed handoffs in spectrum mobility, and MAC threats like eavesdropping, forgery, and selfish behaviour attacks in spectrum sharing are other threats. Therefore, CRN is far more exposed to security threats than those facing the conventional wireless technology. This paper presented a comprehensive survey about the challenges and security in CRNs. The information is presented as a hierarchical structure, starting with challenges and then threats in spectrum sensing, spectrum management, and spectrum mobility. A major portion of the paper has been dedicated to spectrum sharing because it has been the main motivation behind this overview. Moreover, it introduced the spectrum sharing mechanisms: Non-dedicated CCC, hopping-based control channel and more details about the common control channel were chosen for investigation and highlighted the potential existing threats and vulnerabilities. The paper also highlighted several potentially serious threats to network performance in both centralised and ad hoc CRNs. As a result, the most recent detection and protection mechanisms were discussed in terms of their pros and cons and compared for the purpose of addressing the security issues in CRNs. Finally, some open research issues and challenges were presented, which must be met to ensure secure operation of CRNs.

For future work, a hybrid secure MAC protocol for CRN is proposed in [105]. The protocol is analysed and designed for addressing the security requirements, such as authentication, confidentiality, integrity, and non-repudiation. It also addresses most of the security issues in decentralised CRN, such as spoofing, eavesdropping, and forgery attacks. Therefore, the implementation stage of the proposed protocol is in progress in order to provide results that will be compared with others belonging to different secure protocols.

ACKNOWLEDGMENT

The first author would like to acknowledge the Saudi Ministry of Higher Education for supporting his PhD scholarship.

REFERENCES

[1] Cordeiro, C., Challapali, K., Birru, D., Shankar, N., (*2005*) "IEEE 802.22: The first worldwide wireless standard based on cognitive radios," in *New Frontiers in Dynamic Spectrum Access Networks,. DySPAN. First IEEE International Symposium on,* 2005, pp. 328-337.

[2] Shin, K., Kim, H., Min. A., Kumar, A., (2010) "Cognitive radios for dynamic spectrum access: from concept to reality," *Wireless Communications, IEEE,* vol. 17, no. 6. pp. 64-74.

[3] Wang, H., Qin. H., Zhu. L., (2008). "A survey on MAC protocols for opportunistic spectrum access in cognitive radio networks,". in

Computer Science and Software Engineering, 2008 International Conference on, pp. 214-218.

[4] Cao, L., Zheng. H., (2008) "Distributed Rule-Regulated Spectrum Sharing," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 1, pp. 130-145

[5] Zhao, Q., Tong. L., Swami. A., Chen. Y., (2007) "Decentralized cognitive MAC for opportunistic spectrum access in ad hoc networks: A POMDP framework," *Selected Areas in Communications, IEEE Journal on*, vol. 25,no.3, pp. 589-600,.

[6] Chen, R., Park, J., Hou, Y., Reed, J., (2008) "Toward secure distributed spectrum sensing in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 50-55.

[7] Lin, F., Hu, Z., Hou, S., Yu, J., Zhang, C., Guo, N., Wicks, M., Qiu, R., and Currie, K., (2011) "Cognitive radio network as wireless sensor network (II): Security consideration,"in *Aerospace and Electronics Conference NAECON, Proceedings of 2011 IEEE National*, pp.324-328.

[8] Baldini, G., Sturman, T., Biswas, A., Leschhorn, R., Godor, G., and Street, M., (2012)"Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead," *Communications Surveys & Tutorials, IEEE*, vol. 14, no, 2. pp. 355-379

[9] Zhang, X. and Li, C., (2009) "The security in cognitive radio networks: A survey," in *IWCMC '09: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, Leipzig, Germany, pp. 21–24.

[10] Zhen-dong, W., Hui-qiang, W., Guang-sheng, F., Bing-yang, L., Xiao-ming, C., (2010) "Cognitive networks and its layered cognitive architecture," in *Internet Computing for Science and Engineering (ICICSE), Fifth International Conference on*, pp. 145-148.

[11] Sanyal, S., Bhadauria, R. and Ghosh, C., (2009) "Secure communication in cognitive radio networks," in *Computers and Devices for Communication. CODEC. 4th International Conference on, ,* pp. 1-4.

[12] Yucek, T. and Arslan, H., (2009) "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 1, pp. 116-130,.

[13] Tang, L., and Wu, J., (2012)"Research and Analysis on Cognitive Radio Network Security," *April 2012*, vol. 4, pp. 120-126,.

[14] Wu, H., and Bai, B., (2011) "An improved security mechanism in cognitive radio networks," in *Internet Computing & Information Services (ICICIS), 2011 International Conference*, pp. 353-356.

[15] Parvin, S., and Hussain, F.. (2011), "Digital signature-based secure communication in cognitive radio networks,". in *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2011 International Conference on*, pp. 230-235.

[16] Gao, Z., Zhu, H., Li, Shuai., Du, S., Li, Xu., (2012) , "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE* , vol.19, no.6, pp.106-112,

[17] He, A., Bae, K., Newman, T., Gaeddert, J., Kim, Kyouwoong., Menon, R., Morales-Tirado, L., Neel, J., Zhao, Y., Reed, J., Tranter, W., (2010) "A Survey of Artificial Intelligence for Cognitive Radios," *Vehicular Technology, IEEE Transactions on*, vol. 59, no. 4, pp. 1578-1592,.

[18] Chen, R., Park, Jung-Min,. Reed, J., (2008)"Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no, 1. pp. 25-37.

[19] Datla, D., Wyglinski, A., Minden, G., (2009) "A Spectrum Surveying Framework for Dynamic Spectrum Access Networks," *Vehicular Technology, IEEE Transactions*, vol. 58, no, 8. pp. 4158-4168.

[20] Li, X., Chen, J., and Ng, F., (2009) "Secure transmission power of cognitive radios for dynamic spectrum access applications," in *Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on*, 2008, pp. 213-218.

[21] Burbank, J., (2008) "Security in cognitive radio networks: The required evolution in approaches to wireless network security," in *Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference*, pp. 1-7.

[22] Zhang, Y., Xu, G., Geng, X., (2008)"Security threats in cognitive radio networks," in *High Performance Computing and Communications, HPCC '08. 10th IEEE International Conference*, pp. 1036-1041.

[23] Domenico, A., Strinati, E., Benedetto, M., (2012) "A Survey on MAC Strategies for Cognitive Radio Networks," *Communications Surveys & Tutorials, IEEE*, vol. 14, no. 1, pp. 21-44.

[24] A. Umamaheswari., V. Subashini. and P. Subhapriya.,(2012)"Survey on performance, reliability and future proposal of cognitive radio under wireless computing," in *Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference*, pp. 1-6.

[25] Kamruzzaman, S.,Alam, M., (2010). "Dynamic TDMA Slot Reservation Protocol for QoS Provisioning in Cognitive Radio Ad Hoc Networks". *World Academy of Science, Engineering and Technology* , 449-791

[26] Ji, Zhu., and Liu, K., (2007) "cognitive radios for dynamic spectrum access - Dynamic Spectrum Sharing: A Game Theoretical Overview," *Communications Magazine, IEEE*, vol. 45, no, 5. pp. 88-94.

[27] Akyildiz, I., Lee, W., and Chowdhury, K., (2009)"CRAHNs: Cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810-836, 7.

[28] [28] Wei, W., (2011)"The research of cognitive communication networks," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference*, pp. 1-5.

[29] Soleimani, M., and Ghasemi, A., (2011) "Detecting black hole attack in wireless ad hoc networks based on learning automata," in *Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference* , pp. 514-519.

[30] Aboudagga, N., Refaei, M., Eltoweissy, M., Dasilva, L., Quisquater, J., (2005) "Authentication protocols for ad hoc networks taxonomy and research issues," in *Q2SWinet '05 Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and mobile Networks*, ACM New York, NY, USA, pp. 96 - 104.

[31] Salami, G., Durowoju, O., Attar, A., Holland, O., Tafazolli, R., and Aghvami, H., (2011) "A Comparison Between the Centralized and Distributed Approaches for Spectrum Management," *Communications Surveys & Tutorials, IEEE*, vol. 13, no, 2. pp. 274-290.

[32] Ejaz, W., Hasan, N., Kim, H., and Azam, M., (2011) "Fully distributed cooperative spectrum sensing for cognitive radio ad hoc networks," in *Frontiers of Information Technology (FIT), 2011*, pp. 9-13.

[33] Wang, W.,(2009) "Spectrum sensing for cognitive radio," in *Intelligent Information Technology Application Workshops, 2009. IITAW '09. Third International Symposium*, pp. 410-412.

[34] Arkoulis, S., Kazatzopoulos, L., Delakouridis, C. Marias, G., (2008) "Cognitive spectrum and its security issues," in *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. the 2nd International Conference*, pp. 565-570.

[35] Zhao, Q., Swami, A., (2007) "A survey of dynamic spectrum access: Signal processing and networking perspectives," in *Acoustics, Speech and Signal Processing,. ICASSP. IEEE International Conference*, pp. 1349-1352.

[36] Manosha, K., Rajatheva, N., Latva-aho, M., (2011) "Overlay/Underlay Spectrum Sharing for Multi-Operator Environment in Cognitive Radio Networks," *Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd* , pp.1-5, 15-18 May 2011,

[37] Senthuran, S.; Anpalagan, A.; Das, O. (2012), "Throughput Analysis of Opportunistic Access Strategies in Hybrid Underlay-Overlay Cognitive Radio Networks,"*Wireless Communications,IEEE Transactions on* , vol.11, no.6, pp.2024-2035, June 2012,

[38] Wyglinski, M., Nekovee, M., Hou, T., (2010). Cognitive Radio Communications and Networks: Principles and Practice.(2010 Elsevier)

[39] Akyildiz, I., Lee, W., Vuran, M., and Mohanty, S., (2008)"A survey on spectrum management in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no 4, pp. 40-48.

[40] Yu, F., and Tang, H., (2010)"Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks ," *Springer Science+Business Media, LLC*, vol. 16, no. 8, pp. 2169–2178,

[41] León, O., Hernández-Serrano, J., and Soriano, M.,(2010) "Securing cognitive radio networks," vol. 23, pp. 633-652,

[42] Fragkiadakis, A., Tragos, E., Askoxylakis, I., (2012) "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 1, PP, pp. 1-18.

[43] Sampath, A., Dai, H., Zheng, H., Zhao, B., (2007) "Multi-channel jamming attacks using cognitive radios," *Computer Communications & Networks. Proceedings of 16th International Conference*, pp. 352-357.

[44] Song, Y., Zhou, K., & Chen, X. (2012). "Fake BTS Attacks of GSM System on Software Radio Platform". *journal of networks, vol. 7, no. 2 , 7*, 275-281.

[45] Terence, J., (2011), "Secure route discovery against wormhole attacks in sensor networks using mobile agents," *Trendz in Information Sciences and Computing (TISC), 3rd International Conference on* , pp.110-115.

[46] Robles, R., Haas, J., Chiang, J., Hu, Y., Kumar, P., (2010), "Secure topology discovery through network-wide clock synchronization," *Signal Processing and Communications (SPCOM), International Conference*, pp.1-5, 18-21 July 2010,

[47] Rai, A., Tewari, R., & Upadhyay, S. (2010). "Different Types of Attacks on Integrated MANET-Internet Communication". *International Journal of Computer Science and Security* , vol. 4, no. 3, pp. 265-274

[48] Li, L., Kidston, D., Vigneron, P., Mason, P. (2011), "Replay attacks and detection in tactical MANETs," *Communications, Computers and Signal Processing (PacRim), IEEE Pacific Rim Conference on* , pp.226-231,

[49] Goyal, P. Batra, S., Singh, A., (2010). "A Literature Review of Security Attack in Mobile Ad-hoc Networks". *International Journal of Computer Applications* , vol. 9, no. 12, pp. 0975 – 8887

[50] Enneya, N., Baayer. A., Elkouttbi, M., (2011). "A Dynamic Timestamp Discrepancy against Replay Attacks in MANET". *Informatics Engineering and Information Science* ,vol 254, pp. 479-489

[51] Goyal, P., Parmar, V., & Rishi, R. (2011). "MANET: Vulnerabilities, Challenges, Attacks, Application". *IJCEM International Journal of Computational Engineering & Management, Vol. 11* , pp . 2230-7893.

[52] Baayer, A., Enneya, N., & Elkoutbi, M. (2012). "Enhanced Timestamp Discrepancy to Limit Impact of Replay Attacks in MANETs". *Journal of Information Security*, vol 3 , pp. 224-230.

[53] Jakimoski, G., and Subbalakshmi, K., (2008) "Denial-of-service attacks on dynamic spectrum access networks," in *Communications Workshops, 2008. ICC Workshops '08. IEEE International Conference*, pp. 524-528.

[54] Attar, A., Tang, H., Vasilakos, A., Yu, F. and Leung V., (2012) "A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions," *Proceedings of the IEEE,*vol. 100, no. 12, pp. 3172-3186

[55] [55] Djahel, S., Abdesselam, F., Turgut, D., (2009) "An effective strategy for greedy behavior inwireless ad hoc networks," in *Global Telecommunications Conference,. GLOBECOM 2009.IEEE*, pp. 1-6.

[56] Zhu, L., and Zhou, H., (2008) "Two types of attacks against Cognitive radio network MAC protocols," in *Computer Science and Software Engineering, 2008 International Conference*, pp. 1110-1113.

[57] Guang, L., Assi, C.,(2006) "Mitigating smart selfish MAC layer misbehavior in ad hoc networks," in *Wireless and Mobile Computing, Networking and Communications, (WiMob'2006). IEEE International Conference*, pp. 116-123.

[58] Chaczko, Z., Wickramasooriya, R., Klempous, R., Nikodem, J., (2010) "Security threats in cognitive radio applications," in *Intelligent Engineering Systems ,14th International Conference*, pp. 209-214.

[59] Akkarajitsakul, K., Hossain, E., Niyato, D., Kim, D., (2011) "Game Theoretic Approaches for Multiple Access in Wireless Networks: A Survey," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 3, pp. 372-395.

[60] Kariya, D., Kathole, A., and Heda, S., (2012) "Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method," vol. 2, no. 1, pp. 2250-2459.

[61] Yi, P., Zhu, T., Liu, N., Wu, Y. Li, J.,(2012) "Cross-layer Detection for Black Hole Attack in Wireless Network," vol. 8, no. 10, pp. 4101- 4109.

[62] Jhaveri R., Patel, S., and Jinwala, D.,(2012) "A novel approach for Gray Hole and Black Hole attacks in mobile ad hoc networks," in *Advanced Computing & Communication Technologies (ACCT), 2nd International Conference*, pp. 556-560.

[63] [63] Jhaveri R., Patel, S., Jinwala, D., (2012), "DoS attacks in mobile ad hoc networks: A survey," in *Advanced Computing & Communication Technologies (ACCT),Second International Conference*, pp. 535-541.

[64] Joshi, A., Agrawal, K., Arora, D. and Shukla, S., (2011) "Efficient Content Authentication in Ad-Hoc Networks-Mitigating DDoS Attacks," vol. 23, no. 4, pp. 0975 – 8887.

[65] Cai, J., Yi, P., Chen, J., Wang, Z., Liu, N., (2010)"An adaptive approach to detecting black and gray hole attacks in ad hoc network," in *Advanced Information Networking & Applications (AINA), 24th IEEE International Conference*, pp. 775-780.

[66] Xiaopeng, G., Wei, C., (2007) "A novel gray hole attack detection scheme for mobile ad-hoc networks," in *Network & Parallel Computing Workshops NPC, IFIP International Conference*, pp. 209-214.

[67] Mao, H., and Zhu, L., (2011)"An investigation on security of cognitive radio networks," in *Management and Service Science (MASS), 2011 International Conference*, pp. 1-4.

[68] Zhe, C., Guo. N., Qiu, C., (2010)"Demonstration of real-time spectrum sensing for cognitive radio," IEEE Communications Letters, *2010 - milcom*, vol, 14., no. 10., pp. 323-328.

[69] Jin, Z., Anand, S., and Subbalakshmi, K., (2012) "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," *Communications, IEEE Transactions on*, vol. 60, no, 9, pp. 635-2643

[70] Yuan, Z., Niyato, D., Li, H., Song, J., and Han, Zhu., (2012)"Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal*, vol. 30, no, 10, pp. 1850-1860

[71] Zhou, X., Xiao, Y., Li, Y., (2011)"Encryption and displacement based scheme of defense against primary user emulation attack," in *Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference*, pp. 44-49.

[72] Huang, L., Xie, L., Yu, H., Wang, W., and Yao, Y., (2010)"Anti-PUE attack based on joint position verification in cognitive radio networks," in *Communications and Mobile Computing (CMC), 2010 International Conference*, pp. 169-173.

[73] Anand, S., Jin, Z., and Subbalakshmi, K.,(2008) "An analytical model for primary user emulation attacks in cognitive radio networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium*, pp. 1-6.

[74] Wang, W., Li, H., Sun, Y., and Han, Z., (2009)"Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Information Sciences and Systems, 2009. CISS 2009. 43rd Annual Conference*, pp. 130-134.

[75] Wu. Y, Wang. B., Ray, L., and Clancy, T., (2012)"Anti-Jamming Games in Multi-Channel Cognitive Radio Networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no, 1, pp. 4-15,

[76] Li, H., Han, Zhu.,(2010)"Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," *New Frontiers in Dynamic Spectrum, IEEE Symposium*, pp. 1-12.

[77] Feng, W., Cao, J., Zhang, C., Liu, C., (2009) "Joint optimization of spectrum handoff scheduling and routing in multi-hop multi-radio cognitive networks," in *Distributed Computing Systems. ICDCS. 29th IEEE International Conference*, pp. 85-92.

[78] Song, Y., Xie, J., (2012) "ProSpect: A Proactive Spectrum Handoff Framework for Cognitive Radio Ad Hoc Networks without Common Control Channel," *Mobile Computing, IEEE Transactions on* , vol.11, no.7, pp.1127-1139, July 2012

[79] Akyildiz, I., Lee, W., Vuran, M., Mohanty, S., (2008)"A survey on spectrum management in cognitive radio networks," *Communications Magazine, IEEE*, vol. 46, no 4, pp. 40-48.

[80] A, H., Salameh, B., and Krunz, M., (2009) "Channel access protocols for multihop opportunistic networks: challenges and recent developments," *Network, IEEE*, vol. 23, no 4, pp. 14-19,.

[81] Brik, V., Rozner, E., Banerjee, S., Bahl, P., (2005) "DSAP: A protocol for coordinated spectrum access," *New Frontiers in Dynamic Spectrum Access Networks.1st IEEE International Symposium*, pp. 611-614.

[82] Ma, L., Han, X., and Shen, C., (2005)"Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks," in *New Frontiers in Dynamic Spectrum Access Networks. DySPAN. First IEEE International Symposium*, pp. 203-213.

[83] Sankaranarayanan, S., Papadimitratos, P., Mishra, A. Hershey, S., (2005)"A bandwidth sharing approach to improve licensed spectrum

utilization," in *New Frontiers in Dynamic Spectrum Access Networks,. DySPAN 2005. First IEEE International Symposium*, pp. 279-288.

[84] Kondareddy, Y., Agrawal, P., Sivalingam, K., (2008), "Cognitive Radio Network setup without a Common Control Channel," *Military Communications Conference,.MILCOM. IEEE* ,pp.1-6, 16-19 Nov. 2008

[85] Lin, Z., Liu, H., Chu, X., Leung, Y., (2011), "Jump-stay based channel-hopping algorithm with guaranteed rendezvous for cognitive radio networks," *INFOCOM, 2011 Proceedings IEEE*., pp.2444-2452.

[86] Romero, E., Mouradian, A., Blesa, J., Moya, J., and Araujo, A., (2012)"Simulation framework for security threats in cognitive radio networks," *Communications, IET*, vol. 6, no. 8, pp. 984-990.

[87] Song, Y., Xie, J., (2012) "ProSpect: A Proactive Spectrum Handoff Framework for Cognitive Radio Ad Hoc Networks without Common Control Channel," *Mobile Computing, IEEE Transactions on* , vol.11, no.7, pp.1127-1139, July 2012

[88] Salameh, H.B.; Krunz, M.; Younis, O.; (2008), "Distance- and Traffic-Aware Channel Assignment in Cognitive Radio Networks," *Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON '08. 5th Annual IEEE Communications Society Conference on* , vol., no., pp.10-18, 16-20 June 2008

[89] Shih, C., Wu, T., Liao, W., (2010) , "DH-MAC: A Dynamic Channel Hopping MAC Protocol for Cognitive Radio Networks," *Communications (ICC), IEEE International Conference*, pp.1-5.

[90] Safdar, G., and O'Neil, M., (2012) "A novel common control channel security framework for cognitive radio networks," *Int. J. of Autonomous and Adaptive Communications Systems*, vol. 5 No: 2, pp. 125 - 145.

[91] Kahraman, B., and Buzluca, F., (2010)"Protection and fairness oriented cognitive radio MAC protocol for ad hoc networks (PROFCR)," in *Wireless Conference (EW), 2010 European*, 2010, pp. 282-287.

[92] Bian, K. and Park, J.,(2006)"MAC-layer misbehaviors in multi-hop cognitive radio networks," *In Proceedings of the 2006 US-Korea Conference on Science, Technology and Entrepreneurship (UKC2006). National Science Foundation Under Grant CNS-0524052.*

[93] Ci, S., and Sonnenberg, J., (2007)"A cognitive cross-layer architecture for next-generation tactical networks," in *Military Communications Conference, 2007. MILCOM 2007. IEEE*, pp. 1-6.

[94] Prasad, N., (2008) "Secure cognitive networks," in *Wireless Technology, 2008. EuWiT 2008. European Conference*, pp. 107-110.

[95] Parvin, S., Han, S., Tian, B., Hussain, F., (2010), "Trust-based authentication for secure communication in cognitive radio networks,"in *Embedded and Ubiquitous Computing (EUC), IEEE/IFIP 8th International Conference*, pp. 589-596.

[96] Parvin, S., Hussain, F., (2012) "Trust-based Security for Community-based Cognitive Radio Networks",. 26th IEEE International Conference on Advanced Information Networking and Applications, pp. 518-525

[97] .Li Zhu; Huaqing Mao, "Unified Layered Security Architecture for Cognitive Radio Networks," *Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific* , vol., no., pp.1,4, 25-28 March 2011

[98] Sorrells, C; Potier, P; Qian, L; Li, X., (2011) "Anomalous spectrum usage attack detection in cognitive radio wireless networks," in *Technologies for Homeland Security (HST), 2011 IEEE International Conference*, 2011, pp. 384-389.

[99] Mathur, C., Subbalakshmi, K., (2007), "Digital signatures for centralised DSA networks"*Consumer Communications & Networking Conference, CCNC. 4th IEEE*

[100] Zhu, L., Mao, H., (2010) "Research on authentication mechanism of cognitive radio networks based on certification authority," in *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, 2010, pp. 1-5.

[101] Zhu, L., Mao, H., (2011), "An Efficient Authentication Mechanism for Cognitive Radio Networks," *Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific*, pp.1-5, 25-28 March 2011,

[102] Shaukat, R., Khan, S., Ahmed, A., (2008) "Augmented security in IEEE 802.22 MAC layer protocol,"in *Wireless Communications, Networking & Mobile Computing,. '08. 4th International Conference*, pp 1-4.

[103] Jo, M., Han, L., Kim, D., In, H.P., (2013) "Selfish attacks and detection in cognitive radio Ad-Hoc networks," *Network, IEEE* , vol.27, no.3, pp.46,50,

[104] Goyal, P., Parmar, V., & Rishi, R. (2011). "MANET: Vulnerabilities, Challenges, Attacks, Application". *IJCEM International Journal of Computational Engineering & Management, Vol. 11* , pp . 2230-7893.

[105] Alhakami, W.; Mansour, A.; Safdar, G.A.; Albermany, S., "A secure MAC protocol for Cognitive Radio Networks (SMCRN)," *Science and Information Conference (SAI), 2013* , pp.796,803, 7-9 Oct. 2013