Chapter 10
Security Issues in Cognitive Radio Ad Hoc Networks

Mahendra Kumar Murmu and Awadhesh Kumar Singh

Abstract The cognitive radio network (CRN) is an interesting variant of opportunistic networks. It is gaining steep popularity due to its peculiar capability in mitigating spectrum scarcity problem. Due to the same reason it has different security challenges than other wireless and opportunistic networks, in particular. The chapter accounts security-related research issues, domains of study, security implications and various approaches proposed in the literature to handle them. In the interest of space, the illustration provides crisp summary of the topic instead of exhaustive presentation.

Keywords CRAHNs · Security · Threats · Attack · QoS

1 Introduction

1.1 Background

The widespread availability of affordable wireless devices has led to notable growth and popularity of wireless networks. Thus, the numbers of wireless applications and their size as well as complexity are consistently increasing and consequently the rise in demand for wireless spectrum too. On the contrary, according to FCC (Federal Communications Commission), a US-based spectrum regulation agency reports 15–85% of assigned spectrum is suffering from underutilization due to sporadic and geographical variations [1]. Therefore, it is the need of the hour to exploit the available spectrum intelligently. The cognitive radio network (CRN) has emerged as a solution to the problem. It uses dynamic spectrum allocation (DSA) methodology [2] and software-defined radio (SDR) to allow wireless devices to switch from one frequency band to another at marginal cost, and the wireless

M. K. Murmu (✉) · A. K. Singh
Department of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India

© Springer Nature Switzerland AG 2020

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_10

spectrum is utilized opportunistically. To implement it there are four basic steps, namely, spectrum sensing, spectrum management, spectrum sharing and spectrum mobility. The nodes in CRNs are of two types: primary user (PU) that owns the spectrum and secondary user (SU) that uses it, opportunistically. Therefore, the SU node needs to be aware of the behavioural activity of the primary user in order to form a reasonably stable network [3]. The CRN is alternatively called cognitive radio ad hoc network (CRAHN) or cognitive radio mobile ad hoc network [4, 5].

The CRAHN is a type of wireless network. Therefore, several security concerns in CRAHNs are similar to the security concerns in other computer networks [6–9]. However, the additional communication complexity, due to asynchronous sensing, optimization of cooperative sensing, localization, joint spectrum decision, reconfiguration framework, etc., and the security vulnerabilities in CRAHNs are a bit different.

The chapter presents security issues in the decentralized architecture where the SU nodes are communicating with each other in ad hoc manner. The physical specification of these types of network can be found in IEEE 802.11 b/c/g/f/h [10–14] and IEEE 802.16 [15]. The SU node performs various operations (e.g. spectrum sensing, spectrum sharing, spectrum mobility and spectrum management) collaboratively. The architecture also encompasses the coexistence of single or multiple wireless networks operating in different unlicensed bands. The CRAHN inherits general features, from mobile ad hoc network (MANET), such as lack of central control, node mobility, dynamic topology, wireless connectivity, etc.; however, the features like spectrum mobility and limited authorization are specific to CRAHN that have distinguishable security implications. For example, the effective channel utilization by a CRAHN node may be compromised by frequent interference from licensed users that may lead to malfunction or compromised system performance, and the network may be subjected to congestion, interference and jamming [1, 4].

1.2 Cognitive Radio Ad Hoc Networks

The CRAHNs may be viewed in two parts, as shown in Fig. 10.1. The primary network consists of three categories: licensed-I, licensed-II and unlicensed band. The network over unused band of PU(s) is referred as xG ad hoc network, also called CRAHN [1, 4, 16]. The CRAHNs consist of a collection of autonomous SU nodes. The SU node is equipped with cognitive as well as reconfiguration capability. The cognitive capability handles spectrum sensing and spectrum mobility and the spectrum reconfiguration capability handles spectrum sharing and spectrum management. Due to sensing ability, a node learns about the environment, finds spectrum holes and records it. The set of channel(s) available at SU is called the local channel set (LCS). If any pair of SUs has sensed a common channel, it is called common control channel (CCC) and the cumulative set of channels sensed by all participating SUs is called global channel set (GCS). The SUs are capable enough to take a decision on the basis of their local observation(s). The dotted

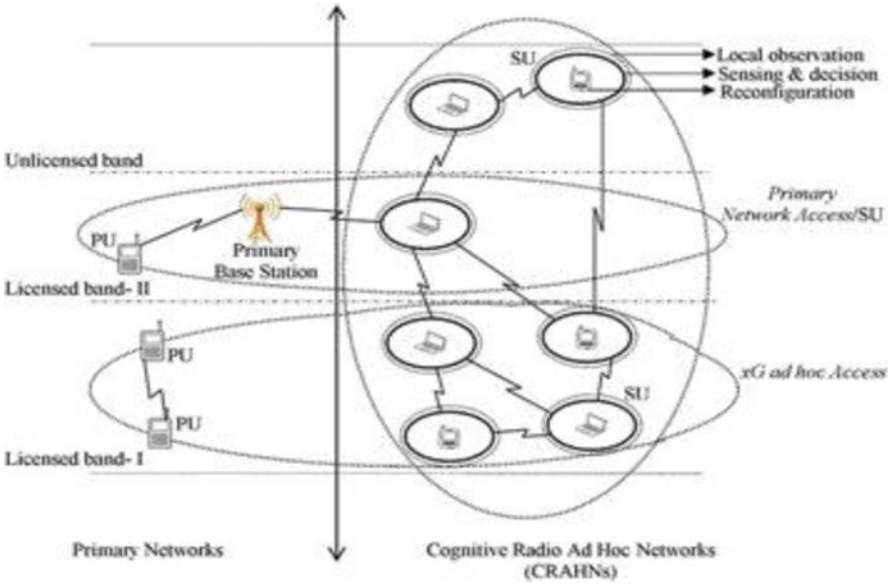

Fig. 10.1 Architecture block diagram of CRAHNs

circle around the SU node represents the range for local observation. The bold circle denotes the range of learning and decision making on the basis of local observations. The SU node is equipped with a reconfiguration device to adopt the environment. Due to autonomous behaviour, the SU node lacks complete topological information. This may result in collision with other SUs as well as PU. Therefore, the SU nodes cooperate and collaborate in order to form a network. In a connected component, the SU nodes may observe spectrum holes from one or more radio environment(s). Similarly, an SU belonging to one network may be connected to another SU that may belong to another network.

The connected SU nodes employ basic operations in the following manner in CRAHNs:

- *Spectrum sensing*: The spectrum sensing states that the devices are capable to sense their radio environments and choose the most suitable band and switch to the best available transmission mode (e.g. modulation type) in the free band [1]. The SU node performs sensing operation individually or cooperatively to detect the PU transmission. The sensing parameters of SU include the channel detection time, sensing band and channel move time. An SU may rely on a weak portion of PU band or free band. In spectrum sensing, the focus of the research has been transmission-based detection, cooperative detection and interference-based detection [1]. The primary objective of using these techniques is to detect the interference with PU. The signal transmitted by SU should not interfere with PU. Due to arbitrary appearance of PU, the SU nodes need to find spectrum holes in opportunistic manner.

- *Spectrum analysis*: Spectrum analysis deals with the identification of the capacity of spectrum holes. The secondary user analyses various characteristics of the network such as capacity, bit error rate and latency to achieve highly reliable as well as spectral efficient communication. The spectrum characterization is affected by several factors such as interference, path loss, wireless link error, link layer delay and hidden terminal problem [4]. However, most disastrous is the arbitrary appearances of PU in the networks. In such case, the SU node may share their information within connected component and find suitable alternate spectrum.
- *Spectrum decision*: The spectrum decision refers to the selection of most appropriate spectrum hole for transmission. It may be taken by a single secondary user or output by several cooperating SU nodes. The spectrum decision process comprises of spectrum characterization, spectrum selection and reconfiguration [1]. Once network characteristics have been analysed, the SU node reconfigures the spectrum operating frequency with the most suitable spectrum hole. In cooperative spectrum decision, the intended spectrum switching may be done *a priori* on the basis of feedback information received from SU neighbours.

1.3 Application of CRAHNs

Recently, the cognitive radio network has drawn the attention of the research community because it supports many interesting applications [17]; refer to Fig. 10.2. Like other ad hoc networks, CRAHN can be used in diverse areas, such as military, personal, commercial and emergency. However, some key applications of CRAHNs include the following:

- *Defence services*: The CRAHN was initially tested in military defence laboratory in USA. Spectrum mobility is a fundamental property of CRAHNs that enhances information security inherently. However, in other ad hoc networks forced spectrum mobility needs to be implemented in order to improve security in walky-talky, wars, terrorist attacks, sensors and other strategic applications.
- *Commercial application*: The CRAHNs have been tested for TV band as major commercial usage. The CRAHN has become a fundamental building block in 4G, LTE and advanced networks that cater pervasive computing environments. The network supports cognitive users seamlessly and ubiquitously to execute applications and to communicate with other users in an anytime anywhere manner.
- *Cellular services*: The CRAHN is useful in providing mobile services due to its capability to operate, on any network and over any service, despite service and network being non-cognitive. The number of subscribers, supported by a cell, can be increased using CRAHNs. Further, CRAHNs enhance the quality of communication over cellular services.

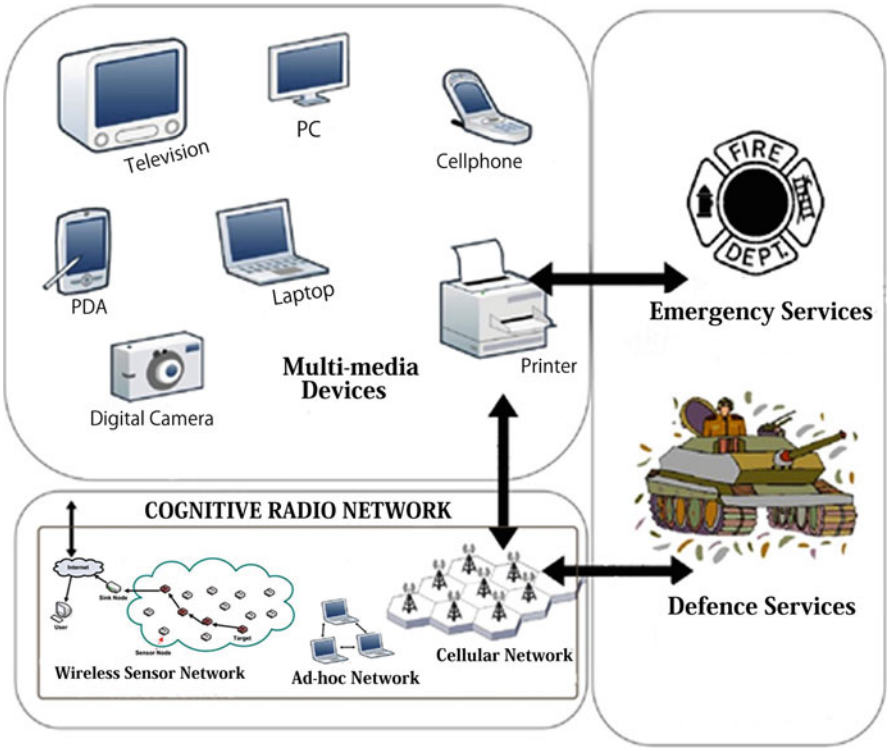

Fig. 10.2 Applications of CRAHNs

- *Emergency services*: The CRAHNs can be used to address traffic burst at disaster and rescue sites during flood, earthquake, volcanic eruption and mining.

1.4 Research Issues in CRAHNs

The following are the major research issues in cognitive radio networks [1, 4, 18]:

- *Security*: The cognitive radio nodes are connected through unused channels in the network. The wireless media is shared and thus the operational environment is unsecure. Also, it faces physical vulnerability that raises multiple security concerns in cognitive radio networks.
- *Quality of services*: The CRAHN falls in the category of opportunistic networks. The network components are required to be active for a sufficiently long time to guarantee the quality of service requirements. The QoS requirements are quantified in terms of reliability, delay, jitter and QoS-aware routing.

- *Mobility*: There are two types of mobility in CRAHN: node mobility and spectrum mobility. The SU nodes take mobility-related decisions on the basis of self-intelligence. They look for resources in the radio environment to form a network. The spectrum mobility causes further dynamism in the network due to forced channel switching by SU nodes.
- *Medium access*: The cognitive radio network is a collection of secondary user nodes. Any two nodes are neighbours iff they exist within their communication range and are tuned on at least one common channel. The nodes may be deployed arbitrarily in a region. The prime source of interference is the presence of licensed user. In addition, there are many other types of interferences that affect overall system throughput, e.g. distributed operations, hidden terminals, exposed nodes, access delay, real-time traffic support and resource reservation.
- *Routing*: The available bandwidth capacity is finite and various applications compete for it. The selection of appropriate radio resource from the available list is appreciable to accomplish the transmission. Some highlights need to be taken care of. Therefore, few entities need careful consideration, e.g. bandwidth utilization, error handling and resource constraint.
- *Data dissemination model*: Spectrum accessibility is affected by licensed user in both variants of the CRAHN, i.e. underlay as well as overlay network. The poor accessibility of the spectrum increases latency that may adversely affect robustness, efficiency, scalability, security and group management.
- *Topology*: Due to node and spectrum mobility, CRAHN suffers frequent topology changes that amount to unpredictability of node location, computational latency, termination detection, etc.
- *Interference*: The interference in CRAHN is not only due to licensed user, it is also caused by environmental conditions, terrestrial situations and many other factors.

The above-listed issues adversely affect the performance of CRAHN. However, the distributed services running on CRAHN are expected to guarantee some desired level of performance and efficiency.

1.5 General Security Objectives

The objective of security is to improve network effectiveness and reliability by preserving information while performing transmission on the fly. In general, the communication systems-based CR technology must validate the communication security requirements [10–12, 15, 19, 20], such as *data confidentiality*, *privacy*, *integrity*, *availability*, *identification*, *registration*, *authentication*, *authorization*, *access control* and *non-repudiation*. The *confidentiality* ensures that the network data is strongly protected from malicious user and cannot be read by unauthorized users. *Integrity* refers to the SU node detecting any intentional or unintentional changes to the original data made by the malicious user in transit. *Availability*

ensures that SU nodes and individuals can access spectrum holes when need be. *Access control* defines the spectrum holes that are available to the unlicensed user for their opportunistic use. If the licensed user appears, the unlicensed user needs to compromise with its network control. *Identification* ensures that an SU user/device must allow to participate with its tamper-proof identification. Identification of node or resources, i.e. channel, data and message, must be protected through robust keying mechanism. *Authentication* is used to prevent unauthorized users to access spectrum holes. *Authorization* states that though PU node influence the network control policy, the SU nodes have the permission to control the network access in opportunistic manner which is described by the level of authorization for each entity. *Non-repudiation* allows either the sender or receiver of the SU node to deny a transmitted message. An interruption of malicious user may misguide the SU node and hence deny transmitting of messages, since it has already been received [21].

However, the details of the security requirements of CRAHNs have been included in a separate section.

The rest of the chapter is organized as follows. Section 2 describes security background of CRAHNs. Section 3 explains various types of attacks in CRAHNs. Section 4 presents modern security approaches and we conclude the chapter in Sect. 5.

2 The Security Background

2.1 Domains of Security Study in CRAHN

In cognitive radio networks, a selfish or malicious user may modify the air interface to mimic a primary user or secondary user. It can mislead a legitimate node during spectrum sensing, spectrum sharing, spectrum mobility and spectrum management. The CRAHNs can be segregated into the following domain on the basis of their security requirements [22–29]:

- *The physical network boundaries*: It is the study of configuration of physical network, i.e. spectrum holes with the SU devices. The available WANs and LANs must support and use the wireless specification of 802.22 and 802.11 b/c/g/f/h and IEEE 802.16 that provide the cognitive radio functionalities.
- *The liabilities areas*: The traditional insurance policies cover general failures in wireless networks. However, CRAHN may suffer new failures, unwanted risks, threats or attacks during operational transmissions. This study identifies additional liabilities to frame the policy that can ensure effective utilization of cognitive radio ad hoc networks.
- *The functionalities fields*: It is the study of data networking and the software that separates and abstracts the elements defined by software-defined radio (SDR)-equipped system. The objective is to disallow the malicious programmed module to interfere with the original results.

- *The criticality of applications and data*: It deals with the effective utilization of networks and wireless WANs or LANs in all areas of applications. However, due to additional challenges in CRN, the communications become tedious. Therefore, the issues related to the transmission need further study to frame an effective utilization policy.
- *Potential geographical limits*: The geographical variation limits the potential of network usage. The CRAHN may be deployed in some critical terrain that may adversely affect the reliability and imposed new geographical limits. The study of these varieties helps in defining the new usage potential and applicability.
- *Traffic and capacity needs/availability*: It is the study of performance or measures of network availability. It helps in accounting the consistent volume of data transmission.
- *Continuity and recovery needs*: It is the study of failure-free system design. Though it is difficult to achieve, a better resource management and resilient backup mechanism are useful to achieve design objectives.
- *Business application domain*: It is the study of application areas. The efficient and effective utilization of spectrum may scale up the reachability and widen the network application area.
- *Business support domain*: It is the study of ACID (atomicity, consistency, isolation and durability) property while performing business transactions in CRAHNs.
- *Development and testing domains*: It deals with the quantification of possible test spaces (e.g. learning parameters, essential testing knowledge) within the system that ensure desired outputs with minimal resources. Furthermore, the optimum learning for spectrum selection and testing knowledge reduces redundancy and decreases the risk probability in the connected component.
- *Production domains*: It is the study of compatibility and feasibility with other platforms. The interoperability-related issues are more challenging in CRAHNs [30].
- *Alarm management domain*: It is the study to identify distinguishing events in the process of learning and reconfiguration. It is important to maintain the system integrity in transit. Better alarm management reduces the network as well as system delay and also it can minimize the risk factor in CRAHNs.
- *Managerial and administrative responsibilities*: The information security managers are responsible to protect user data from security breaches. The suitably well-drafted guidelines and designed security protocols may ensure information safety and avoid severe failure(s).

2.2 Classical Security Method

The basic security model of CRAHN is illustrated in Fig. 10.3. The security effectiveness of the network can be estimated in terms of security capacity. The security capacity reduces due to attacks in the networks. It may be of two kinds

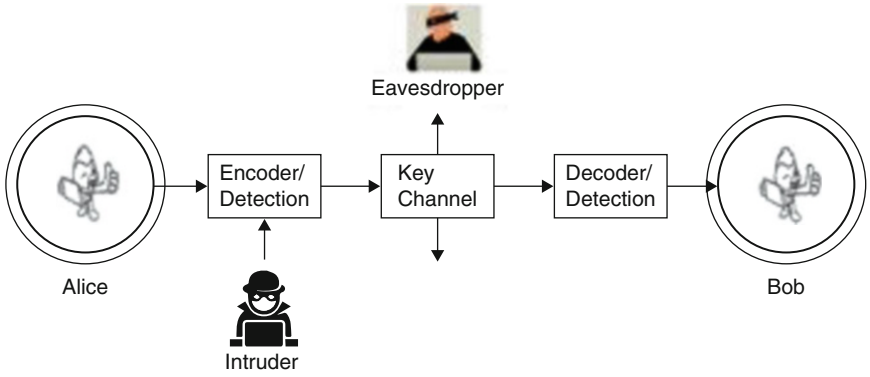

Fig. 10.3 Security model in CRAHNs

such as active attack and passive attack. Assume Alice and Bob are the two entities, i.e. transmitter and receiver, respectively, where secure transmission is going on. The transreceiver may be a legitimate user, e.g. secondary user or primary user. The attacker may try to modify the original information in transit. We denote Intruder and Eavesdropper as the active and passive attacker, respectively, in the figure. A legitimate user is required to transmit information using encrypted key(s). The receiver decrypts the information using the decryption key [31]. If the shared encryption key is known to all the recipients, it is called public key encryption, and if it is known only to the intended user, it is called private key encryption. The key(s) are used to validate the user. Every authorized recipient (secondary user) must be capable enough to synchronize and demodulate the original signal.

2.3 The Security Requirements in CRAHNs

The security requirements in CRAHNs [10–12, 15, 19, 20] are follows:

- *Confidentiality*: It assures that a legitimate SU node has the authority to access the spectrum holes provided there is no PU interference. To achieve this objective, SU needs to pass through a verification procedure that identifies the data transmission participants uniquely. Similarly, the channel identification procedure uses keys to protect it from an unauthorized user [10, 11, 19].
- *Integrity*: A false signal generated by a malicious user on a particular channel may misguide an SU node. The malicious user may hold that channel for a while and modify the original data. In the network, both the parties, i.e. *sender* and *receiver*, may use a robust keying mechanism to protect the data [10, 11, 19].
- *Availability*: A malicious user may attempt to mislead the PU as well as SU by keeping spectrum holes continuously in busy state. Therefore, SU nodes need to

apply an appropriate sensing mechanism so that it can identify the interference caused due to malicious user [10, 11, 19].

- *Access control*: The SU node has temporary access over some control channels in the network. The SU node may apply a robust keying mechanism (e.g. *key management*) to protect control channels from possible threats. The mechanism ensures access to control channels in case of possible attack on the network resources [10, 20].
- *Identification*: Most of the networks use standard naming convention (e.g. *bar-code*) to uniquely identify an SU node and channel. A tamper-proof mechanism may be used to protect various entities and the keys can be shared among legitimate participants [20].
- *Authentication*: An SU node needs to perform careful analysis of signals. It must be capable enough to protect its available spectrum hole from the noise injected by the attacker(s). A robust encryption-decryption method may be used to protect data from unauthorized access [15].
- *Authorization*: The SU nodes must have recent updates about the radio environment and behavioural activity of PU nodes. Using authorization key, the SU node controls the spectrum access within their connected component. Every legitimate user must have freedom to access all kinds of resources [15].
- *Non-repudiation*: The interference from a malicious user may mislead SU nodes by pretending that a message has already been received and hence there is no need to transmit it [20].

2.4 Security Issues in CRAHNs

The SDR-equipped secondary user node is capable enough to implement various radio functionalities like modulation/demodulation, signal generation, signal processing and signal coding. It is embedded in software and therefore it provides the highest degree of flexibility and reconfiguration capability for channel assignment and to adjust the transmission parameters to cater various communication services. The devices are intelligent enough to learn the radio environment during the window of opportunity to access the spectrum holes. The security issues [31] in CRAHN may be classified in the following categories:

- *High priority to primary user signals*: The licensed user signal has the highest priority to avoid interference in it. CRAHN is a distributed structure where SU nodes are connected using unused spectrum owned by the primary user. Due to stringent sensitivity of the licensed user, an unlicensed one has several sensing methods such as matched filter detection, energy-based and cyclostationary feature detection. In matched filter detection, PU signal such as the modulation type and order, the pulse shape and the packet format is known to the SU user. It performs better because the PU information is accurate and thus requires less time to achieve high processing gain. In energy detector, the SU node does not have a priori knowledge about the PU signals. If licensed user appears, the SU

node avoids the interference by selecting the noise floor as thresholds. However, the technique performs weak for spread spectrum signal. The cyclostationary feature detection uses advanced filtering to detect PU signals. The CRN network is under opportunistic category and thus it may suffer high unreliability [3, 32, 33].

- *Arbitrary behaviour of primary user*: Generally, there is lack of knowledge about PU behaviour in the environment. The interference model only provides the feedback to minimize the interference, not the location information of the primary user. In the literature, there are some methods available to handle the localization problem. However, there is no significant progress on this front. The mobile licensed users arbitrarily grab the spectrum in time, space and frequency domain, and consequently the networks may be interrupted or disconnected prematurely affecting the QoS requirements adversely [19].
- *Hidden terminal problem*: In CRAHNs, the SU nodes cooperatively interact with each other. The licensed user is either skipped or the SU node rarely bothers about its location information. The SU node detects PU availability on the basis of local observation of licensed user-transmitted signals. By default, weak signal is assumed to be interfered one. The SUs are assigned three distinct bands such as control, data channel and busy tone band. It is configured in such a way so that the data transmission can take place only after control is established. In the open environment the spectrum may be affected due to reasons like environmental and terrestrial situation or unwanted objects. This also creates communication interference between the SUs or with the licensed fusion centre [13].
- *Asynchronous sensing*: The SU nodes must have high accuracy sensing capability so that it can sustain the PU interference in the first place as well as detect interference due to other temporal variations. Also, the SU node should be able to detect interference due to other SUs [13].
- *Synchronization requirement*: The CRAHNs consist of a collection of autonomous SU nodes. Every node relies on spectrum holes on the radio environment. Once the unused spectrum is found, the SU node needs synchronization in terms of node activities and channel allocation to accomplish communication or computations. If PU appears, the requirement of time synchronization may play a decisive role. In centralized CRN, the sensing results are relayed to the base station which aggregates and determines the presence of PU transmissions. On the other hand, in decentralized networks, the SU nodes cooperatively maintain and share their sensing-related information among themselves to aggregate and determine the presence of PU transmissions. The latency of PU detection is a key concern. As soon as the PU is detected, the SU node must notify their neighbours in order to ensure the application continuity. In a decentralized system, despite an SU being out of sync with other SUs, the rest of the SUs would detect the energy transmitted from the out of sync one and forward the information to a local coordinator [2].
- *Opportunistic spectrum access*: Generally, the CRAHNs exist for a short span of time because it is highly dependent on the licensed user activity. An SU node may be misguided due to bad functional or non-functional system design. As

a result, the window of opportunity to access the spectrum hole is inefficiently utilized [2].

- *Lack of CCC*: Once the SU wakes up, it initiates search for control channels across the entire spectral band. However, a malicious user may engage control channel intentionally. Thus, the SU nodes may not find the spectrum holes and the whole network may collapse [4].
- *Selfish behaviour of a node*: Sometimes, the malicious entities may tend to occupy extra bandwidth and other resources or may block other nodes from acquiring specific resources. The strict control over such selfish act of malicious users is also a challenge in CRAHN [31].

2.5 Generic Security Challenges in CRAHNs

The network security is an important challenge in cognitive radio ad hoc networks [16, 21]. In general, most of the security challenges are found related to the physical, data link and network layer. Therefore, numerous approaches exist in the literature. However, another higher-layer security challenge is an open research problem. The security attacks in CRAHNs have been categorized according to layers as follows:

A. Physical layer

The physical layer security challenges listed in the literature [22, 23, 34] are as follows:

- *Legitimate user emulation attack* (*LUEA*): The unauthorized user transmits special signals and pretends as an authorized SU node on the channels which are not being used by the licensed user. An attacker node disallows the legitimate SU node the spectrum access.
- *Learning attack* (*LA*): The SU nodes adjust learning parameters in the radio environment. The SU has the right to maximize the data transfer rate and also it may enhance the level of security in the network. The unauthorized user may feed false learning parameters to the legitimate SU node, and therefore, an authorized SU node may start transmission on the false channel.
- *Jamming attack* (*JA*): The attacker may generate high-frequency signal and they may flood a single or multiple channels. Consequently, the ongoing communication on that channel is interrupted. This type of attacks can be easily detected by the SU node.
- *Eavesdropping* (*ED*): The malicious node continuously senses the radio environment for available spectrum holes. After detection, the attacker will increase the secrecy among PU from the legitimate user or reduce the frequency due to listening secret information while transmission is in progress.

B. Link Layer

The link layer-related security challenge can be found in [12, 27].

- *Channel jamming* (*CJ*): If a malicious user occupies the channel and prevents the PU from receiving control message, it is called channel jamming. The attacker interrupts the PU, uses all the channels and hence blocks the services. The types of jammers are as follows: deceptive jammer, constant jammer, random jammer and reactive jammer.
- *Denial of services* (*DoS*): An attacker may reduce the channel utilization and copy the MAC control frames by launching of DoS attack on the common control channel. The PU finds the channel busy and consequently denies channel access for transmission of data.
- *Collision attacks* (*CA*): A malicious node may send collision attack on the CCC and disregard MAC specifications. The attacker may transmit the noise packets on CCC which causes collision with other legitimate users transmitting on that channel. The receiver node may be misguided due to incorrect signal.

C. Network Layer

The network layer-related security challenges have been illustrated in [24, 25].

- *HELLO flood attack* (*HFA*): The attacker may communicate to all other SU nodes in the connected component using HELLO beacons. The attacker may easily misguide the legitimate SU nodes.
- *Sybil attack* (*SybA*): The attacker may influence the network using sybil attack that hides the SU nodes' identities. The attacker may send signal to PU and alter the decision-making process. This may result in inefficient channel access in CRAHNs.
- *Ripple effect attack* (*REA*): When the spectrum hole is switched to SU, the legitimate user would transfer flawed information with it which leads to disordered state. This type of attack is called REP attack. The attack may alter the actual energy consumption and elongate the time to operate; consequently, the sensing result is affected.

D. Cross-Layer

The cross-layer security challenges are detailed in [26].

- *Lion attacks* (*LnA*): The lion attack is observed when, namely, primary user emulation attacks (PUEA) target the physical layer that causes logical disconnection of TCP link with the SU node. It may increase packet loss. Therefore, we may arise for packet retransmission either due to time out or if due to distorted connections.
- *Routing information jamming* (*RIJ*): When the SU nodes share routing information among themselves, a handoff may be required to continue transmission. During this phase, the attacker may stimulate the spectrum handoff and stop reconfiguration.
- *Small back-off window attacks* (*SBW*): The malicious node may influence the SU to decrease its window size. This may adversely affect the storage capacity of SUs leading to reduced throughput.

3 Attacks in CRAHNs

Unlike other wireless networks, the CRAHNs are vulnerable to many types of attacks especially during the sensing phase. Broadly, the attacks in CRAHN are classified into two categories: *active* and *passive*. An attack is called active if an SU node behaves as attacker to affect the network security, for example, if a malicious user has successfully decrypted the identification key of a legitimate SU node and took authorization control to misguide other SUs. Similarly, a malicious node may emulate as PU, while other SUs are not able to detect it. On the other hand, an attack is called passive one if the attacker's intent is to affect a network node to deviate from specified behaviour. The passive attack should be handled proactively as it may block a passive attacker from switching to an active one; in case, it has intent. Because the extent of damage caused by passive attacker may be ignorable during sensing decision, it may not be ignorable in case of active one.

The design of a proactive assessment mechanism, which avoids an attacker to switch its state from passive to active, is an open research problem. An inefficient proactive assessment may pop up many issues related to spectrum sensing, sharing, mobility and management. Thus, the objective of application requirements must be well charted so that the SU may apply an appropriate sensing method that may help in taking interference preventive decisions. In CRAHN, the attackers have been classified into three categories: malicious users, greedy users and unintentionally behaving user. The malicious users may send false observations in order to mystify other SUs that may trigger band evacuation by legitimate SUs or cause interference to PUs. The greedy users monopolize specific bands by reporting continuous occupancy by incumbent signals. The unintentionally misbehaving users may supply false observations about band availability due to some hardware malfunction or software bug.

There are three types of attacks that are specific to CRAHN, namely, primary user emulation attacks [32], spectrum sense data falsification attacks (SSDFA) and beacon falsification attacks (BFA). The PUEAs are localization-related attacks where an SU node may have been misguided by the malicious user due to false sensing results, for example, emission of signal from the PU node. It is a physical layer-related attack. The SSDFA-type attack may interfere an ongoing communication between a pair SU by an unauthorized user.

A jamming attack or congestion attack may affect a channel by a malicious user. It is a link layer-related attack. The BFA is related with the beacon authentication schemes where an unauthorized user may generate a beacon signal and claim itself as legitimate one. A malicious user may generate a false alarm to conflict legitimate user for their spectrum resource. The attacker behaviour may further be classified in the following categories, like misbehaving, selfish, cheating and malicious. The misbehaving user does not abide by the rules set by the network authority. The selfish user wants to hold the network resources for its own use and it does not concern about other network users whether they benefit from the network. The cheating user does not share correct information about the network resources that are

needed to ensure desired quality of service (QoS). The malicious users purposefully target the network to degrade the QoS as well as network efficiency.

4 The Security Approaches

- *Spectrum-aware approach* (*SAA*): Spectrum mobility is one of the unique features in CRAHNs. The mobile SU node dynamically adjusts the tuning parameter using the functional operations such as spectrum sensing, spectrum mobility, spectrum sharing and spectrum management. The SU node needs to work upon cross-layer methodology approach and incorporate spectrum mobility in order to exchange state information during communication. Therefore, the behavioural analysis of the spectrum by learning [15, 20] may be helpful to protect information from possible attack.
- *Hammer model framework* (*HMF*): The SU node suffers from network jamming [35], alteration of channel information, masquerading of a PU, masquerading of SU, etc. In such a case, efficiency of channel utilization may be degraded. This type of threats is related to the denial of service attack. The hammer model framework [15] has been used to prevent information from DoS-related threats.
- *Propagation-based methodology* (*PBM*): The CRAHNs is a highly dynamic network. Due to its spectral variations, the CR technology enormously opens up a large portion of the spectrum access opportunity for communication. Every portion of the band has a sufficient spectrum agility for communication. However, it may adversely affect the communication as it is difficult to detect PU appearance. The hidden terminal problem may arise very frequently. The proposed method [30] suggests to monitor the spectrum at runtime that maps the spectrum in 'multidimensional' space and frequency domain in order to predict with high accuracy. The model reduces the chances of possible threats from malicious users.
- *Robust security model* (*RSM*): In CRAHNs, the SU nodes cooperate and collaborate to communicate with each other [14]. Therefore, a reliable and robust security protocol needs to be designed in order to increase the effectiveness of the network. The protocols aware of Byzantine generals' problem [36] may be a rightful approach to achieve robustness. Such design protocols have been used to provide fault tolerance in distributed system and can be used to enhance reliability of cognitive radio ad hoc networks. The design approach [20] may provide security solutions against attackers in cognitive radio ad hoc networks as well.
- *Selfish attack detection methods* (*COOPON*): The cognitive radio nodes in COOPON [14] may detect the attacks of selfish SUs toward multiple channel access using cooperation of other legitimate neighbouring SUs. In CRAHNs, the participating SUs exchange the sensed channel information among them. If any receiver SU finds discrepancy of figure in its neighbourhood, it considers SU as attacker in the network.

- *Distance analysis method* (*DAM*): The SU node measures the distance metrics and accesses that information cooperatively in the connected component. The data manager accounts trusted value using collected distance information [37]. If the SU node finds any discrepancy, it considers the neighbouring node as malicious in CRAHNs.
- *Strategic surveillance* (*SS*): The strategic surveillance [33] refers to the strategic analysis of interaction between defender and attackers through network manager. The manager strategically observes the behavioural activity of attackers and forces the attacker to commit on strategic line.
- *Location-based defence* (*LocDef*) method [3]: The method relies on sharing and comparing the estimated localization information with the already known location information of PU. If the SU node finds any mismatch in the estimated value, it notifies the node as malicious.

5 Conclusions

The CRAHN is significantly different from other wireless networks, and due to its tremendous application potential, it is evolving as the technology of future. Although the objective of the chapter was to account the security issues in CRAHNs, the illustration is helpful for beginners in setting their future research goals on security vulnerability in order to enhance effectiveness and reliability of CRAHNs. Furthermore, the content is intended to trigger the reader to develop insight about network vulnerability, security requirements and implications and to invent new approaches that may combat various types of adversaries that target CRAHNs.

References

1. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., & Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks, 50*(13), 2127–2159.
2. Granelli, F., Pawelczak, P., Prasad, R. V., Subbalakshmi, K. P., Chandramouli, R., Hoffmeyer, J. A., & Berger, H. S. (2010). Standardization and research in cognitive and dynamic spectrum access networks: IEEE SCC41 efforts and other activities. *IEEE Communications Magazine, 48*(1), 71.
3. Orumwense, E. F., Oyerinde, O., & Mneney, S. H. (2017). Improved cooperative spectrum sensing under primary user emulation attacks in cognitive radio networks. *Journal of Engineering Research, 5*(3), 1–18.
4. Akyildiz, I. F., Lee, W. Y., & Chowdhury, K. R. (2009). CRAHNs: Cognitive radio ad hoc networks. *Ad Hoc Networks, 7*(5), 810–836.
5. Mansoor, N., Islam, A. M., Zareei, M., Baharun, S., Wakabayashi, T., & Komaki, S. (2015). Cognitive radio ad-hoc network architectures: A survey. *Wireless Personal Communications, 81*(3), 1117–1142.

6. Gupta, B. B., Agrawal, D. P., & Yamaguchi, S. (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. Pennsylvania: IGI Global. https://doi.org/10.4018/978-1-5225-0105-3.
7. Ko, H., Mesicek, L., Choi, J., Choi, J., & Hwang, S. (2018). A study on secure contents strategies for applications with DRM on cloud computing. *International Journal of Cloud Applications and Computing (IJCAC), 8*(1), 143–153. https://doi.org/10.4018/IJCAC.2018010107.
8. Wang, L., Li, L., Li, J., Li, J., Gupta, B. B., & Liu, X. (2018). Compressive sensing of medical images with confidentially homomorphic aggregations. *IEEE IoT Journal, 6*, 1402. https://doi.org/10.1109/JIOT.2018.2844727.
9. Gupta, B. B., Agrawal, D. P., & Wang, H. (2018). *Computer and cyber security: Principles, algorithm, applications, and perspectives* (p. 666). Boca Raton, FL: CRC Press, Taylor & Francis.
10. Fragkiadakis, A. G., Tragos, E. Z., & Askoxylakis, I. G. (2013). A survey on security threats and detection techniques in cognitive radio networks. *IEEE Communications Surveys and Tutorials, 15*(1), 428–445.
11. Holcomb, S., & Rawat, D. B. (2016, March). Recent security issues on cognitive radio networks: A survey. In *SoutheastCon* (pp. 1–6). Piscataway, NJ: IEEE.
12. Salameh, H. B., Almajali, S., Ayyash, M., & Elgala, H. (2018). Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks. *IEEE Internet of Things Journal, 5*, 1904.
13. Yucek, T., & Arslan, H. (2009). A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Communications Surveys and Tutorials, 11*(1), 116–130.
14. Jo, M., Han, L., Kim, D., & In, H. P. (2013). Selfish attacks and detection in cognitive radio ad-hoc networks. *IEEE Network, 27*(3), 46–50.
15. Baldini, G., Sturman, T., Biswas, A. R., Leschhorn, R., Godor, G., & Street, M. (2012). Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead. *IEEE Communications Surveys and Tutorials, 14*(2), 355–379.
16. Nagpal, C. K. (2018). A game theory based solution for security challenges in CRNs. *3D Research, 9*(1), 11.
17. Meghanathan, N., & Reddy, Y. B. (2013). *Cognitive radio technology applications for wireless and mobile ad hoc networks*. IGI Global book series in AWTT. https://doi.org/10.4018/978-1-4666-4221-8.
18. Agarwal, S., Shakya, R. K., Singh, Y. N., & Roy, A. (2012). DSAT-MAC: Dynamic slot allocation based TDMA MAC protocol for cognitive radio networks. In *International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1–6).
19. Khasawneh, M., & Agarwal, A. (2017). A collaborative approach for monitoring nodes behavior during spectrum sensing to mitigate multiple attacks in cognitive radio networks. *Security and Communication Networks, 2017*, 1.
20. Mathur, C. N., & Subbalakshmi, K. P. (2007). Security issues in cognitive radio networks. In *Cognitive networks: Towards self-aware networks* (pp. 284–293). Hoboken, NJ: Wiley.
21. Akram, M. W., Salman, M., Shah, M. A., & Ahmed, M. M. (2017, September). A review: Security challenges in cognitive radio networks. In *Automation and computing (ICAC)* (pp. 1–6). Piscataway, NJ: IEEE.
22. Ren, K., Zhu, H., Han, Z., & Poovendran, R. (2013). Security in cognitive radio networks. *Proceedings of IEEE Network, 27*, 2–3.
23. Kang, T., & Guo, L. (2015). Physical layer security in cognitive radio based self-organization network. *Mobile Networks and Applications, 20*(4), 459–465.
24. Bouabdellah, M., Kaabouch, N., El Bouanani, F., & Ben-Azza, H. (2018). Network layer attacks and countermeasures in cognitive radio networks: A survey. *Journal of Information Security and Applications, 38*, 40–49.
25. Babu, B. R., Tripathi, M., Gaur, M. S., Gopalani, D., & Jat, D. S. (2015, May). Cognitive radio ad-hoc networks: Attacks and its impact. In *Emerging Trends in Networks and Computer Communications (ETNCC)* (pp. 125–130). IEEE.

26. Hossain, A., & Sarkar, N. I. (2015, November). Cross layer rendezvous in cognitive radio ad-hoc networks. In *Telecommunication Networks and Applications Conference* (*ITNAC*) (pp. 149–154). IEEE.
27. Soliman, J. N., Mageed, T. A., & El-Hennawy, H. M. (2017, December). Taxonomy of security attacks and threats in cognitive radio networks. In *Electronics, Communications and Computers* (*JAC-ECC*), *2017 Japan-Africa Conference on IEEE* (pp. 127–131).
28. Attar, A., Tang, H., Vasilakos, A. V., Yu, F. R., & Leung, V. C. (2012). A survey of security challenges in cognitive radio networks: Solutions and future research directions. *Proceedings of the IEEE, 100*(12), 3172–3186.
29. Kim, H. (2013). Privacy preserving security framework for cognitive radio networks. *IETE Technical Review, 30*(2), 142–148.
30. Nuallain, E. O. (2008, October). A proposed propagation-based methodology with which to address the hidden node problem and security/reliability issues in cognitive radio. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08 IEEE* (pp. 1–5).
31. Jianwu, L. I., Zebing, F., Zhiyong, F., & Ping, Z. (2015). A survey of security issues in cognitive radio networks. *China Communications, 12*(3), 132–150.
32. Jiang, Q. M., Chen, H. F., Xie, L., & Wang, K. (2017). On detecting primary user emulation attack using channel impulse response in the cognitive radio network. *Frontiers of Information Technology and Electronic Engineering, 18*(10), 1665–1676.
33. Ta, D. T., Nguyen-Thanh, N., Maillé, P., & Nguyen, V. T. (2018). Strategic surveillance against primary user emulation attacks in cognitive radio networks. *IEEE Transactions on Cognitive Communications and Networking, 4*, 582.
34. Shah, H. A., & Koo, I. (2018). A novel physical layer security scheme in OFDM-based cognitive radio networks. *IEEE Access, 6*, 29486.
35. Ho-Van, K., & Do-Dac, T. (2018). Reliability-security trade-off analysis of cognitive radio networks with jamming and licensed interference. *Wireless Communications and Mobile Computing, 2018*, 1.
36. Lamport, L., Shostak, R., & Pease, M. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS), 4*(3), 382–401.
37. Feng, J., Zhang, M., Xiao, Y., & Yue, H. (2018). Securing cooperative spectrum sensing against collusive SSDF attack using XOR distance analysis in cognitive radio networks. *Sensors, 18*(2), 370.