Vulnerabilities in cognitive radio networks: A survey

Shameek Bhattacharjee, Shamik Sengupta, Mainak Chatterjee

Abstract

Cognitive radio networks are envisioned to drive the next generation wireless networks that can dynamically optimize spectrum use. However, the deployment of such networks is hindered by the vulnerabilities that these networks are exposed to. Securing communications while exploiting the flexibilities offered by cognitive radios still remains a daunting challenge. In this survey, we put forward the security concerns and the vulnerabilities that threaten to plague the deployment of cognitive radio networks. We classify various types of vulnerabilities and provide an overview of the research challenges. We also discuss the various techniques that have been devised and analyze the research developments accomplished in this area. Finally, we discuss the open research challenges that must be addressed if cognitive radio networks were to become a commercially viable technology.

1. Introduction

Spectrum allocation and management have traditionally followed a ‘command-and-control’ approach – regulators like the Federal Communications Commission (FCC) allocate spectrum to specific services under restrictive licenses. The restrictions specify the technologies to be used and the services to be provided, thereby constraining the ability to make use of new technologies and the ability to redistribute the spectrum to higher valued services. These limitations have motivated a paradigm shift from static spectrum allocation towards a more ‘liberalized’ notion of dynamic spectrum management in which non-license holders (i.e., secondary networks/users) can ‘borrow’ idle spectrum from those who hold licenses (i.e., primaries or primary networks/users), without causing harmful interference to the latter—a notion commonly referred to as dynamic spectrum access (DSA) or open spectrum access [1]. It is envisioned that DSA networks enabled with cognitive radio devices [24,35] will bring about radical changes in wireless communications that would opportunistically exploit unused spectrum bands. However, the open philosophy of the unmanaged/unlicensed spectrum makes the cognitive radio networks susceptible to events that prevent them from communicating effectively. Just like traditional radios, cognitive radios are not only susceptible to interference but also need spectrum assurance. Unlike traditional radios, cognitive radios constantly monitor the spectrum and intelligently share the spectrum in an opportunistic manner, both in licensed and unlicensed bands. The most important regulatory aspect of these networks is that unlicensed cognitive radios must relinquish their operating channels and move to another available channel as soon as they learn or sense the presence of a licensed user on that channel [11].

As spectrum is made available to unlicensed users, it is expected that all such users will follow the regulatory aspects and adhere to the spectrum sharing and access rules. However, the inherent design of cognitive radios exposes its configuration options to the controlling entity in an effort to make the operational parameters flexible and tunable. As a consequence, configurability and adaptability features open up avenues for manipulation as well. Moreover, problems arise when regulatory constraints are not followed. Also, learning by the cognitive radios is a feature that can be manipulated. A radio can be induced to learn false information by malicious or selfish entities, the effect of which can sometimes propagate to the entire network. It is apparent that the inherent design, flexibility and openness of opportunistic spectrum usage have opened avenues of attacks and made cognitive radio networks susceptible to various genres of vulnerabilities including non-compliance of regulations.

In this paper, we provide a comprehensive overview of the characteristics that make cognitive radio networks vulnerable. The vulnerabilities that arise from the inherent design and protocols of operation are discussed considering different perspectives like objectives, nature of impact, and nature of manipulation. We classify these vulnerabilities based on different criterion and...
understand the rationale behind threats or attacks that have been identified and their subsequent impact. We also provide insight on how vulnerabilities in system design could become potential threats. Subsequently, we discuss the current research developments that deal with ensuring security of cognitive radio networks for various types of attacks. Finally, we present some open research challenges related to trust, security, and protection of cognitive radio networks.

The rest of this survey is organized as follows. Section 2 provides an overview of the cognitive radio architecture and relates how the inherent design principles make them vulnerable to threats. Section 3 provides a classification of various vulnerabilities based on different criteria. Section 4 discusses the context in which each attack/threat is relevant and what their consequences are. In Section 5, the current research developments that have been proposed to mitigate different types of attacks are described and the significance of such developments is analyzed. In Section 6, we put forward some of the open research challenges that must be addressed to make cognitive radio networks commercially viable.

2. Architectural aspects and operational weaknesses

In this section, we present the architectural aspects of cognitive radios and the networks they create. In particular, we focus on the vulnerabilities and threats due to the cognitive functionalities and the architectural aspects of the network that make them prone to different genres of attack.

A typical cognitive radio consists of a sensor, a radio, a knowledge database, a learning engine, and a reasoning engine. A cognitive radio continuously learns from its surroundings and adapts its operational parameters to the statistical variations of incoming radio frequency (RF) stimulus [24]. A cognitive radio selects a set of parameters based on knowledge, experience, cognition, and policies. The parameters chosen optimize some objective function. In the cognitive domain, knowledge or cognizance is obtained from awareness of surroundings, based on input statistics from sensory observations and other network parameters. Optimization of the objective function(s) is governed by the cognitive engine which is shown in Fig. 1.

Cognitive radios usually have a programming interface that exposes the configuration options to a controlling entity. The controlling entity could be the service provider that deploys the cognitive radios (base station, access point, etc.) who needs to frequently change the operational parameters— for example, the operating band, access policies, transmission power, and modulation schemes [3,36]. As it is rather impractical to have physical connections with the cognitive radios, the programming of the radios is usually done over-the-air. In the absence of an infrastructure, there might not be any controlling entity and therefore the programming capability could be limited.

2.1. Cognition cycle

The cognition cycle for the cognitive radios is shown in Fig. 2 which primarily consists of three stages: observe, reason and learn, and act. In the observe stage, the radio takes input statistics from the RF environment, updates the knowledge base, and tries to learn the trends with an ultimate aim to optimize a certain objective function during the act stage. It can be noted that, false input statistics in the observe stage can induce incorrect inference, which when shared might propagate throughout the network. As far as learning is concerned, several algorithms based on machine learning, genetic algorithm, artificial intelligence, etc., can be used. With the accumulated knowledge, the radio decides on the operational parameters in such a way that maximizes the objective function at any time instance. At times, different combination of inputs are tried to see if there is a significant change in the objective function. The results are stored in the knowledge base and also fed to the learning algorithms for them to evolve over time.

2.2. Types of cognitive radios

There are three types of cognitive radios: (i) Policy radios, (ii) Procedural cognitive radios, and (iii) Ontological cognitive radios.

Policy radios are governed by a set of rules called the radio’s policy [2,6], where they choose a specific subset of rules that is based on factors like the radio’s location, the radio environment map, constraints imposed by primary spectrum holder, etc. Spectrum regulators need to ensure that unlicensed cognitive radios have minimal impact over licensed systems, and so there ought to be some implementation of rule based domain knowledge. These may be implemented during the manufacturing, programmed over the air, or configured by a user. The rules might change as the device changes location and falls under the jurisdiction of another primary network. Policy radios generally do not possess learning or reasoning engine. Open questions remain that deal with situations where the policy messages are altered which may lead to regulatory violations.

Procedural cognitive radios are those whose operational adaptation is based on observations by utilizing hard-coded algorithms [37], that specify the different actions necessary for different inputs. Procedural knowledge is summarized as a set of ‘if-then-else’ rules. Adaptive actions to be exercised are triggered by certain conditions or observations which may be traced to a pre-defined hard coded function. These are more flexible than the policy radios but not as intelligent as they work in a somewhat deterministic manner taking predictable actions when certain

---

The diagram illustrates the architectural overview of a cognitive radio, showing the relationship between different components such as knobs, dials, and cognitive radio engine. The objective function(s) influences policies, and the radio engine includes knowledge base, reasoning engine, and learning engine.
combinations of observations occur as inputs. An example of such
hard-coded algorithms is dynamic frequency selection using ge-
netic algorithm which triggers adaptations from observations
[41]. Since they do not have learning capabilities they are vulnera-
table to short-term attacks.

**Ontological cognitive radio** are by far the most flexible and intel-
ligent radios as they use reasoning as well as a learning engine
[2,7,36] as seen in Fig. 1. Often times the former radios are not con-
sidered as the classical ‘cognitive radio’ as they do not rely on any
form of artificial intelligence or the use ontological reasoning and
learning. Radio Knowledge Representation Language (RKRL) [36]
is usually used to describe the existence of entities and inter-rela-
tionships between them, and how they may be subdivided accord-
ing to similarities and differences which forms the basic tenets of
ontological reasoning. In cognitive radio paradigm, these ontolo-
gies facilitate the reasoning engine to infer the radio frequency
environment and make intelligent decisions. It is more proactive
as these radios add to their knowledge base how they arrived to
the current learning from the past cognition cycles and then uses
their own reasoning to deduce the next action which is not based
on any pre-determined logic. However, the same learning features
open avenues for manipulations which affect radio’s behavior to be
discussed in Section 3.

### 2.3. Types of networks: infrastructure vs. ad hoc

Cognitive radio networks can be classified into two broad categ-
ories based on whether there is an infrastructure support or not.

**Infrastructure based**: These are networks in the presence of a
central authority that controls the administration of the network
[3]. An example of an infrastructure based cognitive radio network
is the IEEE 802.22 wireless regional area network that resembles a
cellular network comprising a base station and consumer premise
equipments (CPEs). The base station acts as the data fusion center
for the spectrum sensed data that is reported by the CPEs. Based on
the gathered information, the base station allocates uplink and
downlink channels to the CPEs in its cell. Another example of such
a network is an access point with a set of cognitive radio enabled
nodes that are associated with it just like an IEEE 802.11 network
but where nodes are unlicensed.

**Ad hoc mode**: An infrastructure-less cognitive radio network is
like an ad hoc network that operates without a dedicated fusion
center or a channel allocation authority. In the absence of a central
authority, the cognitive radios make independent decisions with
regard to channel access, transmission power, and routing.

### 2.4. Operational aspects of a cognitive radio network

**Spectrum Decision**: Cognitive radio networks have to decide on
the availability of channels before they can use them [3,24,35].
The entity deciding on the occupancy compares the energy de-
tected on a channel with a threshold; if energy is greater than
the threshold, the channel is inferred to be occupied by a primary
or a secondary. This process is termed as local sensing as it is done
by a stand-alone cognitive radio. In an infrastructure based cogni-
tive radio network, the local sensing results are sent to the central
fusion center which combines the local results in accordance with
a suitable fusion algorithm. The local sensing result may also be
raw energy values; in which case the fusion center has to normal-
ize the energy vectors from each node. Generally for larger net-
works, the local sensing result is a binary vector of 1’s and 0’s,
where 1 denotes channel is occupied by a primary and 0 denotes
absence of primary. In contrast, in the ad hoc mode, the local sens-
ing results are sent to all neighbors. A radio fuses the local sensing
of its neighbors data before it can decide on the usage. The process
of fusing data from other radios usually entails cooperation, and
thus collaborative or cooperative sensing is usually employed.
However, there is always a difference (both temporal and spatial)
between the collected data and the result of the fusion. The possi-
bility of this difference can be exploited by the malicious nodes.

**Collaborative or Cooperative Sensing**: In collaborative and co-
erative spectrum sensing, radios share their sensed information
with others; hence the level of cooperation has a direct effect on
the efficiency of resource usage. This is because all radios are ex-
posed to typical wireless characteristics like signal fading and
noise which may result in wrong inference [12]. To reduce the level
of uncertainty, cognitive radio networks often employ spectrum
sensing, [21,22,34,43,44], where the spectrum decision is based on
fusion of opinions by a number of radios in the network. Such
dependence on information from other radios makes the collabora-
tion vulnerable to malicious radios which could provide misleading
data. Moreover, such spectrum usage sharing might indirectly
reveal the location information of a radio violating its location pri-
vacy rights. However, measures on preserving the location privacy

---

**Fig. 2. The cognition cycle.**
in cooperative spectrum sensing have been proposed in [30]. We will discuss how malicious nodes can jeopardize cooperative sensing in the Sections 3 and 4.

Self-Coexistence: The IEEE 802.22 standard defines several inter-base station (BS) dynamic resource sharing mechanisms that enable overlapping cells to share spectrum. In on-demand spectrum contention [23] (ODSC), a BS in need of spectrum (contention source) selectively contends for candidate channels of neighboring BSs (contention destinations). If the contention source wins the contention, it occupies the contended channels exclusively, while the contention destinations vacate those channels via channel switching. The non-exclusive spectrum sharing scheme does little to prevent self-interference among co-channel overlapping cells, which can render IEEE 802.22 networks to be useless [10]. Although the exclusive spectrum sharing scheme can avoid self-interference, it incurs heavy control overhead due to its channel contention procedure. There are a number of security vulnerabilities that arise due to the self-coexistence (existence of multiple overlapping cells). One of the objectives is to reduce interference between co-channel overlapping cells and provide acceptable QoS. The IEEE 802.22 networks have two mechanisms for maintaining the quality of service: (i) Resource Renting Mechanism: a non-exclusive spectrum resource sharing technique and (ii) On-Demand Spectrum Contention (ODSC): an exclusive spectrum sharing technique. The BS controls media access through a cognitive MAC layer (CMAC), that addresses the self-coexistence issues using inter-BS dynamic resource sharing mechanisms. The mechanisms in the security sub-layer are insufficient as they are mostly borrowed from the IEEE 802.16 networks which do not exhibit the unique coexistence features of IEEE 802.22 networks.

3. Classes of vulnerabilities

The open policies and programming interface of cognitive radios create certain vulnerabilities; moreover, the very architecture exposes the configuration options like inputs applied, the manipulation which may directly affect the learning process resulting in sub-optimal performance [17]. Configuration of operating parameters by unauthorized entities is always a possibility. In this section, we discuss the vulnerabilities in the radio design, and those that arise due to network operations, and subsequently classify different possible attacks based on various criteria.

The reasoning feature of ontological radios has both pros and cons. This is because if the radio sees spurious signal in observe stage, it affects the learning and hence the action radio takes in the Act stage. Although the intelligence and flexibility of the ontological cognitive radios allow them to act in a more proactive and optimal manner under various scenarios than policy radios, it also makes them vulnerable to avenues of attack. For example, when malicious elements mislead the learning process by manipulating statistics about the RF environment, there are pronounced long-term effects. Such repeated manipulations have pronounced long-term effects on reasoning and creates faulty knowledge base.

Compromising the controlling entity or the ways in which design and implementation are reconfigured leads to possible faulty policy incorporation. This type of radios are more inflexible and do not rely much on learning; thus not vulnerable to learning attacks. For example, a policy may specify the maximum transmission power to be used for different frequency bands that are specific to a location. As the device moves to new locations the controlling entity is supposed to supply the policy messages; in this case the maximum allowed transmit power on a band for that location. However, altering these policy messages or jamming them are possibilities. Since they do not have a reasoning engine and do not incorporate learning of statistical variations of RF environment, they are not vulnerable to attacks due to faulty manipulation of inputs. We classify the various categories of vulnerabilities as shown in Fig. 3 and discuss each of them.

3.1. Objective of adversarial attackers

The objectives of an attacker have a direct correlation with the way the attacks are launched, and therefore they determine the nature of attacks.

3.1.1. Selfish attacks

The attacker’s motive is to acquire more spectrum for its own use by preventing others from competing for the channels and unfairly occupying their share. In this type of attack, adversaries will defy the protocols and policies only if they are able to benefit from them.

3.1.2. Malicious attacks

The attacker’s only objective is to create hindrance for others and does not necessarily aim at maximizing own benefits. They do not have any rational objective and defy protocols and policies to just induce losses to others.

3.2. Impact of attack on the victims

3.2.1. Direct attack

In direct attacks, the objective of the adversary is denial or refusal of communication or service whenever possible. An example would be to somehow make the radio believe that primary incumbent is present, when in-fact the primary is not present. This is a classical example of denial of service attack where honest cognitive nodes are denied authorized access. Another example is jamming them by sending interfering signals on a channel agreed upon by a transmitter–receiver pair for data communication. We discuss several subclasses of such attacks in the next subsection.

![Fig. 3. Categories of vulnerabilities.](image-url)
3.2.2. Induced attack

In induced attacks, the attacks are related to policy violation and breach of regulation. There is usually a significant delay between the actual execution of the attack and its effect on the victim. It often has serious legal consequences as the effects are associated with breach of regulations and agreements. For example, inducing unauthorized spectrum access through a policy violation by making a radio believe that the primary is not present when in-fact the primary is present, thus causing a regulatory violation.

3.3. Based on the nature of manipulation

3.3.1. Sensory manipulation

As obvious from the term, the attack is done in such a way that sensors those sense the presence of primaries are provided with misleading information. Spoofing faulty sensor information will cause the radios to make incorrect decisions about spectral occupancy and may select configurations or set of parameters that provides sub-optimal performance. Primary user emulation attacks (discussed in the Section 4) is an example of sensory manipulation where the sensors perceive a spoofed signal that resemble the signal of a licensed user and is led to believe that spectrum is not available for use. This type of attack can be quickly launched and therefore is a type of immediate denial attack. The objective of attacks is to manipulate the Observe stage of the cognition cycle, such that the subsequent stages are affected.

(a) Direct sensory manipulation: Malicious nodes may alter sensory input statistics in such a manner so as to deny communication opportunities to others. For example, a malicious node can simply emit spurious signals with signal properties similar to that of a primary incumbent thereby impersonating the presence of the primary incumbent. Thus, a sensor would fail to detect the spectrum vacancy even when the primary is not transmitting. In effect, the Observe state can influence the Act state in the cognition cycle and as an outcome the sensor infers that a channel is not usable and hence a denial of service attack. (b) Induced sensory manipulation: Here, the sensory input is altered to make a sensor fail to identify the presence of the primary. This can be done by a variety of ways like raising the noise floor, masking signals, and advertising lower signal to noise ratio values during cooperative sensing. All these will make a radio believe that the primary is not present and will be tempted to use the channel which will induce interference to the primary. While the effect of interference is immediate, a radio may be banned after repeated occurrences of such induced interference. Thus, there is time lag between the time of execution of the attack and its effect to take place.

3.3.2. Belief manipulation

This type of attack can be aimed at procedural and ontological cognitive radios that use learning and experience. The radios learn to associate the temporal and spatial characteristics of the channel occupancy that are faulty. Another example would be that an attacker can introduce a jamming signal whenever a cognitive radio device switches to higher modulation rates, thus forcing it to operate on lower modulation rate. It is led to believe that switching to higher modulation rate causes interference and it employs lower data rates, and may never try higher data rates, given the past experience.

(a) Direct belief manipulation: This attack is closely related to cooperative spectrum sensing, where multiple radios may lie about their opinion on spectral occupancy. If such modified opinions are shared, the fusion outcome is wrong. Obviously the severity of such manipulation depends on how a node fuses the information. The secondary spectrum data falsification attack is an example of a direct belief manipulation in which spurious occupancy information is sent to honest radios.

(b) Induced belief manipulation: Here the learning radios associate wrong temporal and spatial characteristics of the RF environment and orient their functionalities and configurations to an operating state that results in a sub-optimal performance. As radios employ learning algorithms, case-driven memory and case-based learning, spurious inputs pollute the inference and knowledge base significantly. So when the learning stage is affected, the decision phase is also affected. For example, few dynamic spectrum access algorithms gather channel access statistics for PUs in an attempt to predict when the channel will be idle [16]. If attackers keep spoofing modified occupancy information on a channel, it will affect the long term behavior of the radio.

An illustrative example: A cognitive radio selects a set of inputs in such a way so as to produce system outputs that optimize some objective function. So while a radio is building its knowledge base from observations, the adversary attacks such that the observed value of the objective function decreases for that particular input. Repeated occurrences of this action will coax the radio into believing that certain options like higher modulation rates, certain power levels, frequencies encryption levels, lowers the objective function that yields sub-optimal performance. The fact that every cognitive radio aims to optimize an objective function is made use of, hence this type of attack is also called an objective function attack.

3.3.3. Sybil identities

A Sybil attack is a pervasive security threat where a single malicious node masquerades multiple identities, and behaves like multiple geographically distinct nodes [20]. Due to the presence of multiple small scale networks operated by multiple operators, it becomes difficult to maintain a standard database to record identity information thus making cognitive radio networks vulnerable to Sybil attacks. In a secondary network with multiple nodes competing for spectra, one attacker may generate multiple Sybil identities. Each such counterfeit identity request for spectrum thereby decreasing the fairness of spectrum usage for others and might even deny spectrum to deserving nodes.

3.3.4. Modifying messages of control and synchronization

In many dynamic resource sharing mechanisms there are messages exchanged for synchronization and resource contention. Modifying such control messages leads to various security issues. For example [10] discusses such vulnerabilities that arise from the protocols of self-coexistence where manipulation of control messages leads to the failure of self-coexistence.

(a) Beacon Falsification: The control messages used in self-coexistence are in the form of cell beacons. There are two types of beacons: (i) Base station (BS) beacons provide information about traffic schedule and current operating parameters which are shared between BS’s of neighboring cells; and (ii) Consumer Premise Equipment (CPE) beacons inform the BS it is currently subscribed with and information about traffic flow between the BS and the CPE. Since there exists no security mechanism for inter-cell beacon messages, such messages are susceptible to a number of security threats like unsanctioned modification that impair inter-cell spectrum contention and synchronization. Such an attack targeting inter-cell beacon is known as Beacon Falsification attack which alters messages of synchronization by inserting false frame offsets. Beacon Falsification attack aims to harness the loopholes in the On-Demand Spectrum Conten-
tion (ODSC) protocol [23] and impair the inter-cell contention process which is an exclusive spectrum sharing scheme for BSs that need more spectrum for higher workloads.

(b) Frame Offset Falsification: Inter-cell synchronization of Quiet Periods (QP) in IEEE 802.22 networks increases the spectrum sensing accuracies. Quiet period is the sensing slot where only sensing is performed and all network activities are shut. This synchronization facilitates reliable incumbent signal detection for overlapping cells. When a beacon transmitted by a BS is received by a neighboring BS, the neighboring BS registers the frame offset indicating the time stamp of reception. The neighboring BS synchronizes with the source BS by sliding its frames according to some convergence rule that depends on parameters like frame duration code, transmission and reception offsets. Insertion of false frame offsets leads to two neighboring BSs to calculate inaccurate frame sliding lengths leading to loss of synchronization. This might result in loss of sensing accuracy, the extent of which depends on the sensing mechanism being used.

3.3.5. Exploiting weaknesses in protocols of evacuation

The protocols of evacuation are used to govern the opportunistic usage of idle bands. The aim of the evacuation protocol is to advertise channels that have been evacuated by a primary. In [25], weaknesses in the channel evacuation protocols such as BOOST and ESCAPE are discussed. The BOOST protocol [52,53] is a physical layer signaling protocol which uses superposition of emitted radio power, thus averts the use of signaling through ordinary data frames and reduces the resources needed to support signaling. BOOST involves two logical sets of channels where one busy channel is paired with an idle channel. The protocol requires mobile terminals to send complex symbols at maximum power on busy channel is paired with an idle channel. The protocol requires mobile terminals to send complex symbols at maximum power on busy channel is paired with an idle channel. The protocol requires mobile terminals to send complex symbols at maximum power on.

4. Threats and attack categories

In the previous section, we discussed the different classes of vulnerabilities and their classification based on various perspectives. In this section, we study the attacks and threats triggered by those vulnerabilities. In Table 1, we provide the different types and subtypes of attacks and show the relation between nature of manipulation discussed in previous section.
Table 1
The different attacks and subtypes based on nature of manipulation.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Subtype</th>
<th>Nature of Manipulation</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary user emulation attack (PUEA) [14,15,26,31]</td>
<td>Denial PUEA</td>
<td>Direct sensory manipulation</td>
<td>Also called sensory link disruption</td>
</tr>
<tr>
<td></td>
<td>Induced PUEA</td>
<td>Induced sensory manipulation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coordinated PUEA</td>
<td>Sensory manipulation</td>
<td></td>
</tr>
<tr>
<td>Secondary spectrum data falsification [48,9,13,40,54,57]</td>
<td>Denial SSDF</td>
<td>Direct belief manipulation</td>
<td>Also sensory cooperation disruption</td>
</tr>
<tr>
<td></td>
<td>Induced SSDF</td>
<td>Induced belief manipulation</td>
<td>Also sensory cooperation disruption</td>
</tr>
<tr>
<td>Sybil attacks [46,47]</td>
<td>Sybil based PUEA</td>
<td>Sybil based identities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybil based SSDF</td>
<td>Sybil based identities</td>
<td></td>
</tr>
<tr>
<td>Disruptive CR jamming [28,29,38,39,50,56]</td>
<td>Communication disruption on transmission slot</td>
<td>Modifying messages of synchronization and control</td>
<td></td>
</tr>
</tbody>
</table>

4.1. Primary User Emulation Attacks (PUEA)

Primary User Emulation Attacks (PUEA) are attacks [26] in which the malicious nodes emit signals whose signal power and waveform characteristics are almost similar to the licensed primary transmitter. PUEA can be divided into different sub-genres based on impacts the adversary wants to achieve.

(a) Denial PUEA: An attacker emits spurious signals in absence of primaries, so that the radios believe that a primary is present and thus refrain from using the spectrum. This is an immediate/short term attack, where the radios are denied immediate use of the available channels as sensors are manipulated with faulty sensory inputs of the RF environment.

(b) Induce PUEA: Here a malicious user in the vicinity of a secondary can mask the primary signal by raising the noise floor, or it may transmit at low power masking signals if close to the secondary. With a higher noise floor, or equivalently a less Signal to Noise Ratio (SNR), a secondary will erroneously infer that a primary is not present and try to use the spectrum. This is a violation of spectrum regulations and sooner or later the radio may be banned.

(c) Coordinated PUEA: Multiple malicious nodes might launch attacks in a coordinated fashion on different channels simultaneously to disrupt as many networks as possible. After detecting the current channel to be occupied due to an emulated signal, the secondary will try to choose another from the set of candidate channels. Even after switching the secondary might not be able to find a suitable channel if many candidate channels are attacked. In the context of ontological cognitive radios, such coordinated PUEA attacks on candidate channels will degenerate the learning phase by associating a few channels to be statistically non-usable. Although, in reality, the spectrum may be available, the radios will be reluctant to use the candidate channels after a few learning periods, thus limiting their learning capabilities.

4.2. Jamming disruption attacks in DSA networks

Jamming is transmitting a signal to the receiving antenna on the same frequency as that of an authorized transmitter, thus hindering the legitimate reception by the receiving antenna [42]. In the context of cognitive radios, jamming is done during the data transmission. The difference between PUEA and jamming in DSA networks is the emission of primary like signals in the sensing slot in an effort to manipulate the sensors; while in jamming, disruption is realized in the data transmission slot.

Channel aggregation, fragmentation and bonding allow support of more users, increase spectrum utility and provide improved bandwidth if necessary [18,19]. However, there is a potential vulnerability introduced by these features. This is because the fragmented channels are no longer orthogonal, and the energy leakage increases. An attacker exploits the correlation between the non-orthogonal fragments, and causes a disruptive denial of service similar to jamming attacks. The key difference between jamming and disruption due to fragmentation is that an attacker can attack a different channel i, by spoofing power on another channel j which may be legally acquired by the attacker by capitalizing on the loss of orthogonality. In this case there might not be a total denial of service disruption but certainly would cause impaired QoS, loss in channel capacity, and decreased throughput. An analysis of service disruption caused by malicious attacker in an IEEE 802.22 network is provided in [5].

4.3. Secondary spectrum data falsification (SSDF) or Byzantine attacks

A Byzantine failure in secondary networks [4,13], may occur when radios are unable to correctly determine the presence of primaries due to attackers who modify spectrum sensing data. This attack exploits the cooperative nature of spectrum sensing where an attacker sends false spectrum data to the fusion center or data collector, thus inducing erroneous decisions on spectral usage. There are three ways in which a Byzantine attack can be launched.

(a) Denial SSDF: The adversary may advertise 0 (not occupied) as 1 (occupied) thus causing the fusion/channel allocation center to believe that primary is present, thus restricting channel access. This attack comes under both short term and denial attack, as interpreting empty spectrum as occupied means that a radio cannot use the spectrum with immediate effect.

(b) Induce SSDF: The adversary may advertise 1 as 0 thus causing harmful interference to primary incumbent. Repeated occurrence of such breach of policies may cause the radio to be barred temporarily or banned permanently from the network. Since repeated occurrence of this instance is necessary, it is a long term or induce attack. This is distinct from the previous case which was a denial attack and is achieved quickly.

(c) Sybil-based SSDF: A number of Sybil based malicious nodes with multiple unique counterfeit identities may spoof incorrect channel occupancy information and render incorrect spectrum decision. This type of attack spoofs an illusion that there are
nodes who have sensed a channel, when in reality there are no such nodes. Of course the occupancy information advertised by different logical Sybil interfaces have to be the same on a particular sensing cycle in order to mislead the entity deciding on the spectrum availability. A malicious Sybil node can out vote the honest users. In case a channel is allocated to the counterfeit node, it reduces spectrum utilization.

5. Mitigating vulnerabilities in cognitive radio networks

In this section we discuss the current research advances in countering various vulnerabilities and security threats in cognitive radio networks. We consider the attacks discussed in the previous section and provide some potential approaches to mitigate them.

5.1. Primary user emulation attack remedies

5.1.1. Transmitter signal location verification

This type of detection for PUEA is only restricted to secondary networks where primary incumbents are TV transmitters. The veracity of a received signal is examined by scrutinizing the location of the signal source i.e., whether the sensed received signal is coming from a known legitimate primary. The location verification procedure requires a set of GPS enabled trusted network entities called location verifiers (LVs). The LVs carry out the verification process with prior knowledge of the locations of all TV transmitters. The LVs may be either dedicated network devices or specialized secondary nodes. There are mainly two types of tests that determine the veracity of a signal: distance ratio test and distance difference test.

Distance Ratio Test (DRT): The distance ratio test [14] exploits the fact that there is a correlation between transmitter receiver distance and the received signal strength. It is easy to understand that the ratio between the received signal strength at two LVs depends only on the ratio between distances of respective LVs to the primary transmitter’s location. Thus with two or more LVs, the location of a TV transmitter can be verified. If both the ratios with respect to TV transmitter and received signal strength are close then the source is a legitimate transmitter, otherwise a PUEA attack has been launched. Though there could be some inaccuracies due to channel related effects, having more LVs or conducting the test multiple times reduces the error.

Distance Difference Test (DDT): The distance difference test [14] is a slightly better technique that utilizes the relative phase difference of received signal at two different LVs. The time difference between the two signals received at the LVs is measured and then converted to distance difference. If the distances are sufficiently close then the TV transmitter could be identified. However there are certain constraints associated with the DDT. Proper synchronization between the two LVs must be ensured. The geographical distance between two LVs participating in a verification round must be small enough in order for the DDT to be feasible. Also there is a possibility that an attacker might jam the synchronization signal which may provide incorrect results.

5.1.2. Examination of pdf of received signal

This kind of mitigation technique for PUEA [26] does not rely on localization of signal source; rather the examination of pdf of received signals is required to detect the occurrence of PUEA. The work in [26] assumes that there are multiple randomly scattered malicious nodes in a fading wireless environment and provides two mechanisms to test the pdf of received signals. Let us discuss two tests.

- Neyman Pearson Composite Hypothesis Test (NPCHT): The Neyman Pearson hypothesis test finds the probability of successful PUEA for a fixed probability of missed detection. The criterion allows to control or fix either one: the probability of false alarm or probability of missed detection. With malicious nodes uniformly and randomly located, NPCHT computes the pdf of received power at the secondary nodes due to the primary transmitter and for the malicious users. Given a fixed probability of missed detection, the NPCHT helps to decrease the chances of PUEA by comparing the ratios of these two probabilities with a predefined threshold. Based on whether the ratio is above or below the threshold, primary transmission and emulation attacks can be distinguished.
- Wald’s Sequential Probability Ratio Test (WSPRT): WSPRT or Wald’s SPRT is similar to NPCHT, but allows to set thresholds on both probabilities of false alarm and missed detection. WSPRT is a multi-stage iterative process where a set of observations is necessary to make a decision [49]. It is a finer test but takes more time requiring more than one observation. The test computes a ratio of the two probability distribution functions at each iterative step. The product of the ratios for n iterations gives the decision variable as:

\[ \Lambda_n = \prod_{t=1}^{n} \frac{p^{(m)}(x_i)}{p^{(P)}(x_i)} \]  \hspace{1cm} (1)

where \( p^{(m)}(x_i) \) is the pdf of total received power from all malicious nodes at the \( n \)th iteration, \( p^{(P)}(x_i) \) is the pdf of received power at a secondary due to the primary transmission, and \( x_i \) is the measured power at the \( i \)th iteration. The decision variable \( \Lambda_n \) is compared with two predefined thresholds \( T_1 \) and \( T_2 \), which are functions of tolerable levels of false alarm and missed detection probabilities. If \( \Lambda_n \) is less than \( T_1 \), a legitimate primary transmission is assumed. If \( \Lambda_n \) is greater than \( T_2 \), then a PUEA is detected. For any other case, it is necessary to take more observations. The authors also discuss the bounds on average number of observations required to make a decision on whether a PUEA has been launched or not. Results from [26] show that it is possible to achieve 50 percent reduction in probability of successful PUEA in WSPRT than from NPCHT.

5.1.3. Detection of puea using sensor networks

A method to detect the PUEA using an underlying wireless sensor network has been proposed in [15]. The verification scheme which has some similarities with DDT and DRT, uses a localization based defense (LocDef) by creating a received signal strength (RSS) map of the network with the help of a large number of sensors distributed across the network. The peak RSS values are compared with known locations of primary transmitters. The network is divided into grids and the corner intersection points are called pivot points. A “smoothened RSS value” is calculated by taking the median of RSS measurements obtained from all sensors that lie within a certain radius from a pivot point. The points that produce peaks of median values are supposed to be the locations of primaries. If a peak is observed in a region where there is no primary, then a PUEA is inferred.

5.1.4. Detection of PUEA using cryptographic and wireless link signatures

In [31], the mitigation of PUEA is dealt with authentication of the primary’s signal using cryptographic and wireless link signatures via a helper node usually placed in close proximity to the primary. Since regulations mandate that primaries cannot use cryptographic signatures, a helper node is used as a relay to enable a secondary to verify cryptographic signatures and wireless link signatures. Secondaries learn about the link signatures when helper node transmits signals on channels allocated to PU but not being
used. An authentication technique based on amplitude ratio of the multi-path components of a signal under scrutiny (incumbent or attacker’s) is proposed. The amplitude ratios are calculated using measurements on channel impulse response. If the amplitude ratio is less than a threshold then it is regarded as a spurious signal and discarded. Thus the helper node enabled with cryptographic signature can securely notify about the presence of primaries.

5.2. Byzantine attack remedies

5.2.1. Catchit: onion peeling approach

‘Catchit’ is a technique that helps preserve the correctness of spectrum decision in collaborative spectrum sensing even in the presence of multiple malicious nodes [54]. This heuristic can be described as an “onion peeling approach”, where the possibility of a node being malicious is calculated in a “batch-by-batch basis”, i.e., suspicious levels of all nodes involved are calculated at every time slot, and if at some point the suspicious level is greater than a certain threshold then that node is deemed to be malicious. The centralized decision center excludes the information from that particular node. The process is repeated until there are no more malicious nodes. A similar approach using Bayesian detection to progressively eliminate nodes based on past reports can be found in [55].

5.2.2. Robust distributed spectrum sensing using weighted sequential probability ratio

Robust distributed spectrum sensing is a method to ensure that the final spectrum decision is not affected by Byzantine attacks when multiple nodes participate in collaborative spectrum sensing in the presence of a centralized decision maker [13]. There are two issues that are considered for robust fusion. (i) Ensure bounds on both false alarm and missed detection probabilities and (ii) consider the previous history of behavior of individual sensing terminals. The first issue is taken care by a weighted decision variable derived from the WSPRT [48,49], (originally known as Abraham Wald’s SPRT) where the weight of the decision variable is a function of the reputation. The second aspect is taken care by reputation maintenance where the previous behavior of a terminal is incremented or decremented based on the decision variable. The weighted sequential ratio test is not be confused with WSPRT (Wald’s Sequential probability ratio test) discussed earlier, as weighted SPRT is a just a modification of a known method SPRT developed by Abraham Wald. Weighted SPRT uses weights over decision variables to account for reputation based on observed behavior. The final decision depends on whether the weighted decision variable is within the tolerable limits of false alarm and missed detection probabilities.

5.2.3. Abnormality detection using double sided neighbor distance algorithm

Catching attackers with the help of a technique popularly used in data-mining called the k-proximity algorithm has been proposed in [27]. This considers a single channel system with secondary in presence of a data fusion center and non-collaborative malicious nodes. The proposed algorithm finds outliers that lie far apart from most SUs in the history space. If the history of behavior is too close or too far from other histories, then an aberrant behavior is inferred.

5.2.4. Two-tier optimal-cooperation based secure spectrum sensing

A distributed spectrum sensing algorithm is presented in [51] that aims to mitigate each of the two types of attacks, namely PUEA and SSDF attacks. For PUEA, a user verification scheme on localization based defense is proposed. For SSDF a non-linear cooperation scheme which considers $M$-ary hypothesis, where $M$ is the no of primary transmitters, is proposed. As opposed to the works in [13,27], this paper introduces the concept of a 2-tier hierarchical centralized CRN, in order to optimize the energy and bandwidth consumed as well as decrease the computational complexity. Since reporting by a large number of secondaries results in high computation, energy, and management costs, such optimizations are necessary. Thus, special relay nodes which collect and compress local spectrum sensing help reduce costs.

5.2.5. Performance limits of cooperative sensing under Byzantine attacks

In [4], an analysis of collaborative and non-collaborative Byzantine attacks derived from [33] is presented. The paper aims to analyze the optimal attack strategies as well as issues of collaborative Byzantine attacks with a dedicated fusion center. Kullback–Leibler divergence (KL distance) is used as an objective function which malicious nodes seek to minimize. Given the probabilities of missed detection, false alarm, and the probabilities of true reporting for honest as well as malicious nodes, the paper provides the optimal fraction of malicious nodes required to make the fusion center incapable of making a correct decision. The aim of the malicious nodes is to introduce an error in the global decision on spectrum occupancy. The probability distribution function for the event that fusion center decides the result ($j=0/1$) on the hypothesis that PU is present (absent) is calculated and denoted as $X_j(Y_j)$. Both of them are functions of the fraction of malicious attackers in the system. The relative entropy or KL distance is a non-symmetric measure of the difference between the two distributions $X$ and $Y$ and is denoted by $D(X||Y) = \sum_{x \in X} X(x) \log \frac{X(x)}{Y(x)}$. The attackers attempt to reach a state where $D(X||Y)$ is zero, which is achieved for the optimal fraction of attackers. Subsequently, the paper discusses the best possible strategy for all the entities namely the Byzantine radios, honest radios and the fusion center. The interaction between them is modeled as a minimax game between Byzantines and fusion center and the best strategy for both players is the saddle point. The interaction is analyzed in light of two different performance aspects namely, the KL distance and probability of error. The saddle points in the context of KL distance for both independent and collaborative Byzantine attacks are derived.

5.2.6. Long term reputation based exclusion

A method proposed in [40] counters Byzantine attacks over a number of sensing periods, by accumulating the local decisions from each radio, and comparing it with the final decision at the fusion center in the same time window. The number of times the local decision from a radio is different from the final decision at fusion center is used as a reputation measure for a radio. If reputation measure is lower than a certain threshold the radio is isolated from the fusion process. The methodology assumes the usage of ‘l-out-of-K fusion rule’ where the final decision on a channel is decided based on what at least l out of K participating radios advertise. However, if the fraction of attackers is high, the fusion center cannot distinguish correctly.

5.2.7. Bio inspired consensus based cooperative sensing scheme in ad hoc CRN

In [57], a scheme that is derived from bio-inspired consensus algorithms is utilized for a consensus based cooperative sensing scheme in an ad hoc cognitive radio network to counter SSDF attacks or Byzantine failures. The lack of central authority makes ensuring security difficult as certain local information when spoofed impacts the radio behavior rather easily. In this method, RP statistics from immediate neighbors are used as state variables which are aggregated to deduce a consensus variable. The consensus variable is then used to make the decision over the detected energy and determine the presence or absence of the primary.
The sensing scheme works in the following fashion. All secondary nodes sense the spectrum and report their locally estimated energy level to their neighbors. With the gathered information, a node uses a selection criterion to exclude reports from nodes that are likely to be attackers. For any time instant, the exclusion/selection process uses the mean value of energy at the previous instant and compares the mean value with individual values from the neighbors. For a particular node, the set of neighbors whose reports suffer maximum deviation from the mean are excluded and the remaining nodes' reports are taken into consideration. This process of sharing, receiving, selecting, and updating continues until all states converge to a common value which is then compared with a certain threshold. If the common value is greater than the threshold, the spectrum is occupied else it is not occupied.

5.2.8. Trust based anomaly monitoring
In [8], a trust based monitoring mechanism is proposed that prevents harmful effects of Byzantine attacks in ad hoc CRNs. Using an anomaly detection technique, each node assigns a trust value to its neighboring nodes that shared occupancy reports. Unlike [57] where raw energy values are shared, binary values are used where 0 indicates channel is not occupied and 1 indicates channel is occupied. The trust is an index of how much trustworthy is a node's shared occupancy information is. Based on the calculated trust, a decision is made whether to consider a node's advertised spectrum occupancy information for fusion or not. The scheme does not require any additional information on identity information of neighbors. It may be noted that the idea is not to identify or isolate malicious nodes, but to ignore the reports from the malicious nodes for the fusion process.

5.2.9. Exploiting misleading information
In [9], the authors go a step further by not only evaluating the trustworthiness of nodes, but also exploiting misleading information sent by malicious nodes. First, a trust model is proposed that is based on the correlation between what information a node sends and the predicted values. Then, using a log weighted metric, malicious nodes are distinguished. Subsequently, selective inversion fusion and complete inversion fusion schemes are proposed that effectively combine not only the information sent by honest nodes but also utilize misleading information by malicious nodes. Results reveal better fusion results for inversion based fusion scheme for various input parameters.

5.3. Disruptive cognitive radio jamming remedies
5.3.1. Optimal sensing disruption of cognitive radio adversary
The work in [38] considers sensing link disruption and sensing cooperation disruption as two variants of the sensory manipulation attack. The attacker is considered as an external entity and not a part of the secondary system. The authors show that the optimal disruption strategy for spoofing that maximizes the number of false detections for secondaries is an equal power partial band spoofing strategy. For an attacker with a total power budget of \( P \), the optimal strategy is to transmit with power \( P/n \) on all the \( n \) channels to maximize the average number of false detections. This method also helps to determine the number of channels that should be targeted by the power constrained attacker.

5.3.2. Multi-tier proxy based cooperative defense strategy
A framework discussed in [50] explores collaborative jamming in a centralized network where multiple jammers try to deny communication of cognitive radios with the base station. The paper proposes multiple possible disruptive jamming strategies and subsequently a two-tier proxy based collaborative defense strategy. The probability that a user is jammed is similar to a hyper-geometric distribution that is used to calculate the spectrum availability rates at the jammer and the base station under different hopping strategies. In the two-tier architecture, users are divided into two classes: the proxy users which act as relay and followers. The proxy users are in between the followers and the BS. There are three stages of communication; followers connect to proxies (first stage) which in turn forward it to the BS (second stage) and then relay backward from BS to followers (third stage). Results show that the spectrum availability rate is higher when collaborative multi-tier proxy based defense strategy is employed.

5.3.3. Tradeoff between spoofing and jamming
The work in [39] assumes that the sensory manipulating adversaries have a constrained power budget and proposes intelligent optimal attack strategies. Spoofing is defined as the disruption energy launched over the sensing slot causing an incumbent emulation. Jamming is the energy emitted to disrupt once radios acquire bands and initiate communication. The paper shows how an adversary should utilize its power budget between spoofing and jamming so as to inflict maximum damage. The objective function is the average throughput of secondaries which is optimized from the adversary's perspective. Optimization is solved using a 2-step process. However both spoofing and jamming may not be possible at the same time. In such a case, the more effective one is employed depending on the context. Either spoofing or jamming can apply the equal power partial band strategy discussed in [38]. The observations throw light on the tradeoffs between spoofing and jamming under different conditions. Experiments show that when the number of users requesting spectrum is very less, the minimum average throughput is reached if entire energy is directed to jamming. As the number of users requesting the spectrum increases the average throughput monotonically decreases with increase in spoofing power which indicates that when demand is high the power budget should be allocated to spoofing.

5.3.4. Dogfight in spectrum: jamming and anti jamming in multichannel cognitive systems
A body of work in [28] discusses optimal attack strategies by fixing the secondary nodes strategies for primary user emulation attacks. The finite horizon game is modeled as a 2-player normal zero sum game with one stage and multistage. The same authors in [29] have focussed on the problem of jamming and escaping under unknown channel statistics and solved it as an adversarial multi-armed bandit problem. Lower bounds of performance for defenders, subject to several typical attack strategies, were derived for a single defender. The problem of Blind Dogfight is as follows: There are two adversarial groups; attackers and defenders. The attacker can observe rewards and payoffs for defenders, but the defenders are not able to observe any information for the attacker. So the defenders face a multi-armed bandit with an opponent with arbitrary strategies. The goal of solving the problem is to design a strategy for the defenders without information about channels, yet to ensure reasonable performance of spectrum sensing.

5.3.5. Adaptive anti jamming using non stochastic multi arm bandit problem
In [56], an adaptive online jamming resistant protocol for an ad hoc secondary network using non stochastic multi arm bandit problem (NS-MAB) is proposed in the form of learning algorithms and subsequent quantitative performance benefits are established. It is assumed that the priori probabilities of nature of occupancies and other network statistics are not available. The game is played among secondary sender, secondary receiver and a jammer with an objective to strike a balance between exploring and exploiting the best channels for transmission. The protocol is as follows: There are a fixed number of strategies for the sender and the receiver;
each strategy has a weight associated with it. Similarly each channel has a channel weight and a strategy is determined by all channels. Hence weight of strategy is the product of all channel weights.

5.4. Sybil attack

5.4.1. Sybil attacks implementation and defense

The work in [46] introduces the concept of Sybil attacks in IEEE 802.11 networks where a malicious node masquerades several distinct secondary nodes requesting spectrum with disparate identities. The statistics of beacon transmissions are accumulated and a defense strategy based on anomalies in beacon transmission intervals on the receiver side is proposed and implemented, both in presence and absence of interference from external sources. The mechanism employed to launch Sybil identities by a malicious node is through sending beacon frames embedded with different identity information to neighbor nodes. A testbed called SpiderRadio is used where each radio has two network interfaces: one for broadcast of WAN services and other for receiving and recording time stamps of beacons frames. The central idea is to emit beacon frames from one device with multiple SSIDs. The Sybil identity generation involves manipulation at two stages, namely beacon generation and beacon frame transmission. In each beacon frame, a different MAC address, SSID, and beacon interval field in frame body are generated. The transmission powers of each beacon are also varied using a transmission power control algorithm that achieves different receive signal strength (RSS) at the neighboring secondary nodes. The different header properties with obfuscated RSSs' capture the twofold essence of a successful Sybil attack. The Sybil attack generated may be either hardware based or software based, and therefore the authors propose defense strategy against both by examining time intervals between two consistent beacon frames.

5.4.2. Using sybil identities for primary user emulation and Byzantine attacks in DSA networks

In [47], a mechanism for a new Sybil based attack is implemented where an adversary is allowed to launch primary user emulation attack as well as Sybil based Byzantine attacks. Issues like allocation of Sybil identities for different attacks are investigated in the presence and absence of a reputation system. Both the secondary network and the malicious attackers have knowledge of candidate channels. The malicious attacker has two interfaces: (a) Sybil Saboteur (SybS), where the goal of is to launch Sybil based Byzantine attacks influencing spectrum decision at fusion center, and (b) Sybil Attacker (SybA), where the goal is to launch PUE attacks on candidate channels.

There are three Sybil interfaces with 3 distinct MAC addresses which are used to attack multiple candidate channels simultaneously. The attacker launches a PUEA by attacking a candidate channel with one interface for 250 ms and then switches to another channel using a different interface. An honest user who relinquishes one channel and moves to another candidate channel might not find a valid channel. This is termed as SybA or Sybil attacker. Along with this, the attacker is also capable of launching SybS or Sybil Saboteur where a single attacker node sends beacons with false reports to compromise the collaborative spectrum sensing. These counterfeit identities also request spectrum as different entities decreasing total spectrum efficiency.

6. Conclusions and future challenges

In this survey, we have explored the various vulnerabilities of cognitive radio networks. These vulnerabilities stem from not only the basic design philosophy but also from the flexibilities and opportunities these networks offer. We discussed the unique characteristics of cognitive radio operation that make it susceptible to sensory, belief, and other kinds of manipulation. We also revealed the weaknesses in operational aspects of a cognitive radio network that can be potentially exploited by malicious entities. We classified threats based on different objectives and their impacts. We also discussed the various techniques that have been devised to counter the threats and analyzed the research developments along similar lines.

However, the research to deal with vulnerabilities is still in its incipient stages and there are many open questions that need to be answered before a secure cognitive radio network could be deployed. For example, the lower layers of the protocol stack need to be defined and agreed upon. Else, the advantages obtained from features such as aggregation, fragmentation, and bonding will be offset. Also, there must be mechanisms to detect if any synchronization and control messages have been tampered with; thus securing the weaknesses in spectrum evacuation protocols.

It is to be noted that most modeling of adversaries in cognitive radio networks do not distinguish between selfish and malicious users for better tractability. However, the rationale and the attack strategies of these two kinds of adversaries are very different, both posing threats to the honest users. While there has been some research in traditional wireless networks where selfish and malicious users have been considered separately, the cognitive radio research is yet to establish an universally accepted framework. Moreover, in cognitive radio networks, there will always be honest users who have an incentive to acquire more spectrum when competition for spectrum is high, coaxing them to turn selfish during certain situations. Dealing with such momentary strategy deviations is challenging.

There is not much study that analyzes the coordination among attackers engaging in Byzantine attacks. Such study will help us understand on which channels the attackers agree to attack, how they change their strategies, and what factors determine the nature of attacking strategies. Better information fusion techniques must be used that can accurately fuse spectrum reports from multiple sources—some of which could be malicious. Further investigations are needed that can distinguish Sybil identities and better ways to associate multiple Sybil interfaces with the true transmitter.

Verifying authenticity in a large heterogeneous network with open source DSA nodes operated by multiple operators is another challenging problem. This calls for designing efficient authentication mechanisms, validation methodologies during deployment, and some frameworks that can authenticate identity and location information.

Defending both long-term and short-term attacks using learning techniques must be explored. As there will be no single learning technique that can learn and infer all events, appropriate and context-based learning mechanisms have to be adopted. Concepts from no-regret learning [58], Q-learning, and reinforcement learning [45] could be used to understand the nature of learning attacks in cognitive radio networks and effective mechanisms to defend against such threats must be devised.

References