A survey on security issues in cognitive radio based cooperative sensing

Shivanshu Shrivastava\textsuperscript{1}  |  A. Rajesh\textsuperscript{2}  |  P. K. Bora\textsuperscript{2}  |  Bin Chen\textsuperscript{1}  |  Mingjun Dai\textsuperscript{1}  |  Xiaohui Lin\textsuperscript{1}  |  Hui Wang\textsuperscript{1}

\textsuperscript{1}College of Electronics and Information Engineering, Shenzhen University, Nanshan, Shenzhen, China
\textsuperscript{2}Department of Electronics and Electrical Engineering, Indian Institute of Technology Guwahati, Guwahati, India

\section*{Abstract}

Cognitive radio based cooperative spectrum sensing (CSS) is severely affected when some secondary users maliciously attack it. Two attacks regarded as key adversaries to the success of CSS are spectrum sensing data falsification (SSDF) and primary user emulation attack (PUEA). Defending SSDF and PUEAs has received significant attention in research in the past decade globally. This paper performs a state-of-the-art comprehensive survey of the researches on defending SSDF and PUEAs. First, the preliminaries like Hypothesis testing for detecting the primary user and different models of CSS are discussed briefly. Then a categorization of the defence mechanisms for defending both the attacks has been proposed as active and passive. Active mechanisms are suitable for an immediate defence in a limited time span, while passive mechanisms are suitable for flexible CSS systems that are ready to detect the attacks over a period of time and suppress them permanently by bringing changes in their underlying operations. An in-depth tutorial on both the defence mechanisms is provided from the perspectives of the secondary users throughput and the interference to the primary user. Finally, a detailed survey on the open research problems in this area and some possible solutions has been performed.

\section{INTRODUCTION}

Wireless communication devices need the electromagnetic spectrum to transmit information. The use of the spectrum is authorized by the government of a state or a territory \cite{1}. However, the available suitable spectrum is scarce for the number of wireless network operators present and there is a strong competition for it \cite{2}. Consequently, the spectrum is auctioned by the government to various network operators \cite{1}. Each winner of the auction is granted the full use of a particular part of the spectrum and is called the primary user (PU). Henceforth, the PUs hold the legitimate right over the part of the spectrum granted to them.

It has been found that in a given space and time span, most of the spectrum licensed by the government to the auction winners remains unused \cite{3}. A significant idea to solve this issue came from the Ph.D. dissertation of Joseph Mitola III \cite{4}. It proposed the design of a software radio (SR) capable of sensing its environment. Mitola termed such an SR as a cognitive radio (CR). A CR is an extension of an SR to learning about the RF bands, air interfaces, protocols, spatial and temporal patterns that moderate the use of the radio spectrum. Mitola’s thesis mainly proposed a radio knowledge representation language to use the learning capability of CR for increasing the spectrum efficiency. Based on this idea, the annual report of the FCC in 2003 \cite{5} proposed to apply the learning capabilities of a CR to allow dynamic spectrum allocation (DSA) among the wireless operators based on its availability. A significant research work on DSA was performed by Simon Haykin \cite{6} in 2005, which quantified Mitola’s work. Haykin suggested to accomplish DSA
by using CR technology for the unlicensed users. An unlicensed user was termed as a secondary user (SU). It was realized that a CR can be installed in an SU to sense the presence of the PU signal on its spectrum. This function was termed as spectrum sensing (SS). If the PU signal was found to be absent, its spectrum can be used by the SU. However, this usage was subject to a stringent condition that there should be no interference to the PU. If the PU signal is present, the SU should refrain from any kind of transmission.

Since [6] has been published, SS has emerged as a significant area of research [7, 8]. The most important objective of SS has been identified as accuracy, so that the PU should not suffer interference. However, the SS performed by an individual SU can be highly inaccurate in deep fading environments. To overcome this problem, a cooperation between more than one SU to sense the spectrum has been proposed [9–11]. This scheme is known as cooperative spectrum sensing (CSS). CSS is classified as centralized and decentralized [12]. In centralized CSS, the cooperating SUs report their data or decisions to a central body known as a fusion centre (FC) or a base station (BS). Based on these data or decisions, the FC forms its decision about the presence or the absence of the PU and broadcasts it to all the SUs. On the other hand, decentralized CSS is based on the sharing of data or decisions among all the cooperating SUs to arrive at a final decision. The focus here is mainly on centralized CSS.

CSS significantly improves the SS performance in deep fading environments. However, its performance depends on the data or decision of an individual SU. Any flaw in an individual SU’s data or decision can cause a significant error at the FC [13]. There can be various reasons for these flaws in the SU data or decision, like hardware malfunction, deep fading etc. A major reason for such a flaw is when an unlicensed transmitter misleads the SU ecosystem about the status of the PU spectrum for selfish reasons, by manipulating its air interfaces and transmitting fake signals in the environment. Such an unlicensed user is termed as a malicious user (MU) [11]. If the MU is a part of CSS, it can mislead the CSS system by deliberately reporting wrongly to the FC. Such security issues from MUs constitute one of the most significant concerns in CR systems [13].

The sensing capability enabled by the CRs gives way to the MUs to cause attacks. The openness of the lower layers adds advantage to the MUs. The MUs can sense the spectrum and transmit fake signals according to the spectrum status. If the honest SUs are misdirected and cease their transmissions, the MUs take the advantage and start using the spectrum.

There have been extensive researches on the possible malicious attacks [14–18]. These attacks have been named based on their strategies, like the receiver jamming attack, eavesdropping, authentication attacks, intruding attack, exogenous attack, and greedy attack. The receiver jamming attacks are caused when the MU affects the received signal-to-noise ratio (SNR) of the SU severely by transmitting absurd signals or noise over the channel. Eavesdropping is caused when the MUs overhear the SU and PU data and attack accordingly. Authentication attacks are caused when the MUs transmit fake signals to deceive the SUs, unlike jamming where the purpose of the MUs is to obstruct the channels of the SUs. Intruding attacks are caused when the MUs pose as legitimate SU nodes and mislead the system. Exogenous attacks are nearly similar to jamming attacks, while greedy attack can be seen as a combination of authentication and eavesdropping attacks.

The domain of attack strategies is reasonably broad. More specific attacks can be identified further and terminologies can be given to them based on their strategies. Broadly, most of these attacks can be classified under spectrum sensing data falsification (SSDF) attacks and the primary user emulation attacks (PUEAs). The attacks where the MUs misdirect the FC regarding the spectrum status by reporting to it wrongly are categorized as SSDF attacks. These attacks may cause the FC to declare the vacant spectrum as occupied or the occupied spectrum as vacant. On the other hand, the attacks where an MU misdirects other SUs and the FC regarding spectrum occupancy by transmitting emulated PU signals are categorized as PUEAs [19]. An MU causing PUEA is termed as a primary user emulator (PUE). Several researches propose counter mechanisms for these attacks. The objective of this paper is to perform a survey of the researches on SSDF attacks and PUEAs. Both the attacks have been studied for a CSS system, as they are more vulnerable to the attacks than individual CR systems. There are various counter mechanisms in the existing literature for these attacks [14–18]. We categorize the existing counter mechanisms as active and passive approaches. The active approach involves directly detecting the SSDF attacks and PUEAs with the help of some actions by the SU network towards the MUs. These actions involve detecting the location of the MUs by transmitting training signals, or installing hardware to detect the honesty and maliciousness of the incoming signals from the SUs by differentiating their strength, features or statistical properties. These approaches are advantageous where quickness is the primary need. However, the cost paid for quickness is temporariness of their impact. To counter SSDF attacks, they directly eliminate the malicious data reported by the attackers, by identifying anomalies in the statistical properties of the malicious data. They can eliminate the malicious data also by differentiating the location of its source from the locations of the PU and the SUs. Active schemes thwart the PUEAs by cancelling the PUE signal. They check the PUE signals for a tag already embedded in the PU signal. The PUE signals are eliminated if they do not possess the tag. The PUE signals are also identified based on the location of their source.

The passive approaches on the other hand resist the SSDF attacks and PUEAs with some changes in the underlying operations of CSS. These changes involve designing their spectrum sensing mechanism in a manner to mitigate the effects of the SSDF attacks on a particular parameter like the probability of false alarm or the probability of detection, and avoid the PUE signal. For defending SSDF attacks, they use the reputation of an SU based on this history of its reports and using game theoretic mechanism to maximize the utility parameter aimed at increasing the probability of detection. They counter the PUEAs by either suppressing the harmful effects on PUEAs or avoiding the PUE signals. The passive approaches do not counter the MUs head-on. However, they provide a more permanent defence to CSS than the active mechanisms. They are
advantageous for flexible systems, which can easily redesign their architecture.

The motivation of this paper is to present a state-of-the-art comprehensive survey of security aspects of the CR technology. Precisely, the most relevant security threats like SSDF and PUEAs, the related countermeasures like active and passive strategies, their working principles, and methodologies have been discussed in detail. Both the attacks and protection techniques apply to all three domains viz., commercial, public safety and military. The major motivations of the present work are as follows:

- Discuss in detail the taxonomies of the SSDF and PUEAs, their mechanisms and the corresponding attack parameters, which determine where, who, how, and when these attacks are launched.
- Propose a classification of existing defence algorithms to typical SSDF and PUEAs and provide an in-depth tutorial on the state-of-the-art defence schemes from the perspectives of throughput of the SU and interference to the PU, respectively.
- Analyse the spear-and-shield relation between the SSDF and PUEAs and defence from an interactive location based, statistical parameter based, attack signal avoidance based, damage suppression based, game-theoretical based perspectives.
- An analytical comprehensive survey of the current state-of-the-art researches for the detection of the SSDF and PUEAs.
- Discuss the open research challenges, present some possible solutions, and present future research directions in these research areas.

The rest of the paper is organized as follows: Section II illustrates the fundamental system model for spectrum sensing, CSS, types of CSS, and how the security attacks affect CSS. The fundamental models for SSDF and PUEAs are also explained here. Section III performs a survey on the counter strategies against SSDF attacks. Section IV presents the counter strategies against the PUEAs. Various categorizations like active and passive mechanisms for thwarting SSDF attacks and PUEAs are done within the respective sections. Section V provides a detailed explanation on the open research directions and Section VI concludes the paper.

2 | SYSTEM MODEL

2.1 | SSDF attacks

SSDF attacks are caused when the MUs misdirect the FC about the spectrum occupancy by reporting wrongly to it. When the PU spectrum is vacant, the MUs report to the FC that the PU spectrum is occupied. The FC broadcasts the honest SUs to cease their transmissions. The MUs may take the advantage of this situation by using the band for their own purpose. In the other scenario, the MUs may misdirect the FC to declare an occupied spectrum as unoccupied. Following this decision, the honest SUs may start transmitting which would cause a severe interference to the PU. The PU may impose penalty on the honest SUs and can also restrict them from further using its spectrum [20]. The MUs may take the advantage of this situation by getting the honest SUs punished.

2.2 | PUEAs

PUEAs are caused when the PUEs deceive the honest SUs and the FC by transmitting emulated PU signals. PUEs are classified as always-on and smart [21]. Always-on PUEs do not know about the status of the licensed spectrum. They seamlessly transmit emulated PU signals on the PU spectrum band. On the other hand, smart PUEs are capable of knowing the PU spectrum status by individual decision making or listening to other SUs. They plan and attack depending on the presence of the PU. As a result of the PUEAs, the honest SUs may get misdirected in deciding the spectrum status and report wrong decisions to the FC. If the PU is absent, the SUs mistake the PUE's signal to be coming from the PU and cease their transmissions. The PUE takes the advantage of this situation by transmitting on the vacant band. On the other hand, when the PU is present, the PUEs cause interference to it. Smart PUEs cause interference deliberately while always on PUEs do it in anyway. As a result, the PU may penalize the honest SUs and the PUE may take advantage of the situation.

2.3 | Mathematical models of SSDF Attacks and PUEAs

The mathematical models of SSDF attacks and PUEAs require the understanding of CSS. A CSS model has SUs placed randomly in the environment as shown in Figure 1. Each SU performs spectrum sensing on the frequency band allocated to the PU and reports its data or decision at the FC. The FC uses these data or decision values and makes a decision regarding spectrum occupancy. The decisions at individual SUs or at the FC are formed with the help of binary hypothesis testing problem.

Suppose an SU is lying in the vicinity of a PU base station. As the PU base station broadcasts wireless signals in the environment, the CR equipment installed in this SU receives an incoming signal sample and performs binary hypothesis testing to detect the presence of PU signal in it [6]. The process is explained as follows:
2.4 Hypothesis testing problem in CR

Let hypothesis $H_0$ denote the absence while $H_1$ denote the presence of the PU. The CRs make their decisions in favour of $H_0$ or $H_1$ based on the signal they receive from the PU base station. Let there be an SU in the vicinity of the PU and let $y(k)$ denote the signal it receives from the PU at the $k$th instant of time. The presence of the PU can be expressed in the binary hypothesis form as

$$
y(k) = h(k)y(k) + w(k) \quad H_1
$$
$$
y(k) = w(k) \quad H_0
$$

where $y(k)$ denotes the PU signal, $h(k)$ denotes the multipath channel fading component and $w(k)$ is the additive white Gaussian noise (AWGN) at the SU receiver. Now the CR installed in the SU uses an spectrum sensing mechanism to perform the binary hypothesis testing. There are many spectrum sensing techniques used for this purpose. The most famous primary user detection technique is energy detection. The focus in this survey is on the security attacks in energy detection based CR systems. Energy detection is a blind signal detection technique proposed in [22]. It does not need any knowledge of the characteristics of the signal. The CRs compute the energy of the incoming signal. Then, the computed energy is compared to a predefined threshold. If it is higher than the threshold, the decision is made in favour of $H_1$ otherwise $H_0$ is concluded. The calculation of the threshold is done using the Neyman–Pearson method [23]. The decision statistic in energy detection systems is the energy of $y(k)$ given as

$$
T_E = \frac{1}{K} \sum_{k=1}^{K} |y(k)|^2
$$

where $K$ is the number of samples considered for evaluating the energy. The SU compares $T_E$ in (2) to a predefined threshold $\lambda_E$ and decides $H_1$ or $H_0$ as follows

$$
T_E > \lambda_E \quad H_1
$$
$$
T_E < \lambda_E \quad H_0
$$

The probability of false alarm of the FC ($P_f$) is the probability of an SU making a false decision when the PU signal is absent. This means that the FC thinks that the PU is transmitting when in reality, it is not transmitting. Mathematically, $P_f$ is written as

$$
P_f = \Pr(T_E \geq \lambda_E | H_0)
$$

The closed form expression for $P_f$ obtained after solving (11) is obtained as

$$
P_f = Q_m(\sqrt{2}\gamma, \sqrt{\lambda_E})
$$

where $\gamma$ is the signal to noise ratio of the SU with the PU given as

$$
\gamma = \frac{|A|^2 \rho^2}{\sigma^2}
$$

where $A^2$ is the PU signal power. In (5), $Q_m(\cdot, \cdot)$ is the generalized Marcum $Q$-function given as

$$
Q_m(a, b) = \int_{b}^{\infty} x^{m-1} \exp \left(-\frac{x^2 + a^2}{2}\right) I_{m-1}(ax) dx
$$

where $I_{m-1}$ is the modified Bessel’s function of $(m-1)$th order.

Similarly, the probability of misdetection of the FC ($P_m$) is the probability of the FC making error in detecting the presence of the PU signal. This means that the FC thinks that the PU is not transmitting, when in reality it is transmitting. $P_m$ can be expressed mathematically as

$$
P_m = \Pr(T_E < \lambda_E | H_1)
$$

The closed form expression for $P_m$ obtained after solving (7) is given as

$$
P_m = \frac{\Gamma(u, \lambda / 2)}{\Gamma(u)}
$$

where $\Gamma(\cdot, \cdot)$ and $\Gamma(\cdot)$ are the incomplete and complete gamma functions respectively. Individual spectrum sensing can be inefficient due to presence of environmental obstacles. To overcome the limitation, cooperative spectrum sensing is carried out with the help of multiple SUs.

2.5 Cooperative spectrum sensing

The pathloss and multipath fading caused to the PU signal result into inaccurate sensing. Consequently, the SU can make a wrong decision about spectrum occupancy. This can cause a severe interference to the PU. As a counter measure, a cooperation among multiple SUs for sensing the spectrum has been proposed [24]. The process is called cooperative spectrum sensing (CSS). CSS is more prone to security attacks compared to individual spectrum sensing, as attacks can be launched more efficiently when attackers exist within the system. The main focus of this paper is on the effects of security issues on CSS and their counter mechanisms. CSS is necessitated for the CR sensing. The idea of CSS is to exploit the spatial diversity of the signal propagation environment. Exploiting spatial diversity was first proposed in refs. [25] and [26]. In CRs, diversity is obtained when different copies of the same signal are received by multiple antennas or multiple SUs [12] as a result of multipath diversity. The gain obtained by exploiting multipath diversity is called diversity gain. The idea of CSS is that out of the various copies of the PU signal received by different SUs, some copies would have suffered lesser attenuation while some copies would have suffered more attenuation. The SU receiving a highly attenuated signal is likely to make a wrong decision regarding spectrum occupancy. In this regard, if a decision is made by combining the individual decisions of the SUs, the bad decisions will be compensated by the decisions from the good paths, and the effects of attenuation can be mitigated. CSS significantly reduces the inaccuracy in spectrum sensing by a single user. Each SU shares its data or decisions with other
SU’s and forms its decision about the spectrum occupancy. It is mainly categorized as centralized and decentralized CSS. In centralized CSS, the SU’s fuse their individual data or decisions to a central body known as the FC, as shown in Figure 1. In decentralized CSS, there is no FC [27]. It is based on sharing of data or decisions among the SUs as shown in Figure 2. The focus of this work is more on centralized CSS systems as they have higher application due to their well-structured architecture.

In data fusion, the individual data of each SU is fused at the FC. For instance, if energy detection mechanism is followed by the SU’s, the global statistic is calculated by summing all the incoming $T_{Ei}$ values and forms a new global statistic $E_G$. The global statistic $E_G$ is compared to a threshold and a decision is formed by the FC on spectrum occupancy, which is known as the global decision. Let there be $N$ SU’s participating in CSS and $T_{Ei}$ denotes the energy value of the $i$th SU, the calculation of $E_G$ has been shown mathematically as

$$E_G = \sum_{i=1}^{N} T_{Ei}$$

(9)

The global statistic $E_G$ is compared to the global threshold value $\lambda_G$ and the decision on spectrum occupancy is obtained as

$$\frac{H_1}{H_0}$$

(10)

The decision fusion rule is implemented at the FC as

$$E_G < \lambda_G$$

(11)

In majority rule, if a minimum of $n$ SU’s transmit 1 to the FC, it decides hypothesis $H_1$. OR rule says that the FC decides in favour of hypothesis $H_1$ if at least 1 SU transmit 1 to the FC. If none of the SU’s transmit 1, it must decide $H_0$ as true. In majority rule, if a minimum of $N/2$ SU’s transmit 1 to the FC, it decides hypothesis $H_1$ as true otherwise it decides $H_0$. Let $D_i$ be the individual decision of the $i$th SU, where $D_i \in \{0, 1\}$, the decision fusion rule is implemented at the FC as

$$P_{md} = Pr(E_G < \lambda_G | H_0)$$

(12)

In decision fusion CSS, each SU transmits its binary decision to the FC in the form of 1s and 0s, where 1 indicates the presence and 0 indicates the absence of the PU. The FC follows AND, OR or the majority rule to form its decision regarding spectrum occupancy, where the PU presence is decided if $N$, 1, or $N/2$ SU’s transmit 1 to the FC respectively. The formulation of $P_{fa}$ and $P_{md}$ is similar to (11) and (12), with $E_G$ replaced by the sum of the binary decisions from the SU’s [12].

AND rule says that the FC decides in favour of hypothesis $H_1$ if all the $N$ SU’s participating in CSS transmit 1 to the FC. If $N-1$ or lesser number of SU’s transmit 1 to the FC, it decides in favour of hypothesis $H_0$. OR rule says that the FC decides in favour of hypothesis $H_1$ if at least 1 SU transmits 1 to the FC. If none of the SU’s transmit 1, it must decide $H_0$ as true. Let $D_i$ be the individual decision of the $i$th SU where $D_i \in \{0, 1\}$, the decision fusion rule is implemented at the FC as

$$P_{fa} = Pr\left(\sum_{i=1}^{N} D_i \geq n | H_0\right)$$

(13)

where $n = 1$ for OR, $n = N$ for AND, and $n = N/2$ for the majority rule.

$$P_{md} = Pr\left(\sum_{i=1}^{N} D_i < n | H_0\right)$$

(15)

2.5.1 Selection of the FC

The selection of the FC is based on the principle of trusted nodes in the network. We consider a mechanism where one of the cooperating SU’s is equipped to function as the FC. The choice of that SU is based on the merit of its decisions. In this regard, a trusted cooperating SU which has a history of reporting correct decisions is chosen. At any instant of time, when the decision of a cooperating SU is consistent with the global network decision, its reputation value will be increased. On the other hand, if it is not consistent with the global network decision, it will be decreased. The reputation value associated with any network is calculated as

$$r_i(k) = r_i(k-1) + (-1)^{P_{d}(k)+d(k)}$$

(16)
where \(d(k)\) is the value representing the global decision. If an SU is repeatedly reporting wrong values, it is discarded. The decision to discard an SU is decided by a discard threshold value \(\eta\). The \(i\)th SU is discarded for repeatedly making wrong decisions if \(r_i\) becomes less than \(\eta\). However, in fading environments, the possibility of an SU receiving attenuated information from the PU spectrum is high. Thus, it may fail to detect the PU spectrum correctly which will affect its merit which is based on the history of its decisions. In this regard, a threshold \(\Delta\) is additionally used to prevent the environment affected SUs. The reputation value of an SU is lowered only if it reaches a value lesser than \(\eta\). The node which has the highest reputation value is assigned as the FC. Generally devices like the server, the controlling unit, or the SU base station are able to maintain such a high reputation value. Thus, these devices are made the FC, where are the SUs report their individual data or decisions.

2.5.2 Election of spectrum head with the help of the cooperative spectrum sensing and transmission energy levels

After making the decision on the availability of the spectrum for SUs, the next step for the FC is allocation of the spectrum. The part of the spectrum used by the PU is wide and can be shared by multiple SUs. The FC divides the PU spectrum into various sub-carriers of different bandwidths. One cooperating SU is allotted one sub-carrier each. The significant issue is what strategy to follow the sub-carrier allocation. The objective of the FC is to allot the sub-carriers to the SUs in a manner that the achievable sum-rate of the SU system is maximized. In this regard, the transmission energy levels of the SUs becomes significant, as the data-rate of the SU is a function of the transmission energy level. Also the correct detection of the available sub-carrier is crucial for the maximization of the achievable sum-rate of the SU system. Thus, efficient usage of the energy levels of CSS plays a significant role in spectrum allocation.

To explain this mathematically, we consider a comprehensive scenario of \(n_1 = 1, 2, ..., N_1\) networks available where CSS is being performed. Let the \(k\)th sub-carrier be assigned to the \(m\)th SU under the coverage of \(k\)th base station within the \(n_1\)th network. The variable \(x_{n_1 \text{ sub}}\) indicates the happening of this situation by assuming a value 1 and when it assumes a value 0, it indicates that this event has not happened. The data transmission rate achieved by the \(m\)th SU while performing its transmission through the sub-carrier \(k\) within the network \(n\) and base station \(s\) is given as

\[
R_{n_1 \text{ sub}} = x_{n_1 \text{ sub}} D_{IC_{n_1 \text{ sub}}} \log_2 \left( 1 + \frac{P_{n_1 \text{ sub}} b_{n_1 \text{ sub}}}{N_0 B_0} \right)
\]

for \(n_1 = 1, 2, ..., N_1, s \in S, m \in M_{n_1}, k \in K_{n_1}
\]

where \(D_{IC_{n_1 \text{ sub}}} = 1\) means that the sub-carrier \(k\) is detected as a spectrum hole (a vacant part of the spectrum) in the network \(n_1\) base station \(s\). The correctness of \(D_{IC_{n_1 \text{ sub}}}\) largely depends on the energy levels of the CSS. Thus, the data rate of an SU is highly dependent on the energy levels of CSS as derived earlier in expression (9). Further, \(R_{n_1 \text{ sub}}\) represents the transmission energy level of the SUs. \(M_{n_1}, K_{n_1},\) and \(S_{n_1}\) are the sets of SUs, sub-carriers, and base stations within the network \(n_1\). The allotment of the \(k\)th sub-carrier to the \(m\)th SU is indicated by the variable \(x_{n_1 \text{ sub}}\).

The achievable sum-rate of the SU network is given as

\[
R = \sum_{n_1} \sum_{r} \sum_{m} \sum_{k} R_{n_1 \text{ sub}}
\]

The allotment of the sub-carrier (or the frequency sub-bands) is done to the SUs by optimizing the transmission energy level of the SUs \(P_{n_1 \text{ sub}}\) and the sub-carrier allocation variable \(x_{n_1 \text{ sub}}\) as

\[
\max_{x_{n_1 \text{ sub}} \in \{0, 1\}} R
\]

subject to

\[
\sum_{n_1} \sum_{r} \sum_{m} \sum_{k} x_{n_1 \text{ sub}} P_{n_1 \text{ sub}} D_{n_1 \text{ sub}} \leq p_{\text{max}}
\]

\[
\sum_{n_1} \sum_{r} \sum_{m} \sum_{k} R_{n_1 \text{ sub}} \leq 1, x_{n_1 \text{ sub}} \in \{0, 1\}
\]

\[
\sum_{n_1} \sum_{r} \sum_{m} \sum_{k} P_{n_1 \text{ sub}} \leq p_{\text{max}}
\]

\[
\sum_{n_1} \sum_{r} \sum_{m} \sum_{k} R_{n_1 \text{ sub}} \geq R_{\text{min}}
\]

2.6 Effects of security attacks in CSS

Apparently in CSS, the final belief of an SU about the spectrum occupancy depends on the data or decisions of other SUs. The belief may be formed with the help of the FC or by the sharing of the data or decisions among the SUs. In either case, it depends on other SUs. As mentioned earlier, it is possible that some SU in the network indulges in malpractices to misguide the spectrum sensing system for its selfish interests and such an SU is termed as a malicious user (MU) [28]. The MUs severely affect the signal processing and propagation characteristics of the sensing system. Their presence necessitates the redesigning of the sensing strategy of the SUs. As a result, the throughput of the SUs is degraded and the interference on the PU increases severely. There are different ways in which the MUs can launch attacks. These attacks have been classified into two categories which have been widely studied in researches: spectrum sensing data falsification (SSDF) attacks and primary user emulation attacks (PUEAs).
The following section describes the attack mechanism and mathematical models of SSDF and PUEAs, and how they affect CSS.

2.6.1 Mechanism of SSDF attacks

These attacks are caused in centralized CSS systems, as shown in Figure 3. They are the outcome of the Byzantine failure problem which is caused when a cooperating SU reports wrongly to the FC [29]. This false reporting may be due to hardware failure or a selfish intention of an SU. The false reporting due to selfish intentions is known as the SSDF attack [29, 30]. The MUs report falsely to misguide the FC regarding the spectrum status. On getting misdirected, the FC broadcasts the wrong decisions to the cooperating SUs. Hence, the entire network is misdirected regarding the spectrum status. If the FC gets misdirected, it will change its decision to 0 when the spectrum is occupied. This is done by sending a high energy value or sending a wrong decision to the FC. For these types of attacks, the interest of the attack detector will be in detecting the event \( X_3 \), denoted as \( X_n \).

As mentioned earlier, the SSDF attacks are caused when an MU inverts its true decision on the spectrum to make the FC change its decision to 0 when the spectrum is occupied. This is done by sending a high energy value or sending a wrong decision to the FC. For these types of attacks, the interest of the attack detector will be in detecting the event \( X_3 \), denoted as \( X_n \).

\[
X_0 = p_1[b(p_\mu(\lambda + (1 - \lambda)X_0(t - 1)) + (1 - p_\mu)(1 - \lambda)X_0(t - 1)) + (1 - b)p_\mu(\lambda + (1 - \lambda)X_0(t - 1)) + (1 - p_\mu)\beta(\lambda + (1 - \lambda)X_0(t - 1)) + (1 - p_\mu)\beta(\lambda + (1 - \lambda)X_0(t - 1)) + (1 - b)(1 - \mu)(1 - \lambda)X_0(t - 1)]
\]

The first term in (25) represents the frequency of event type 10 for the case when the PU signal is present. Multiplying \( b \) denotes honest SUs and the term \( p_\mu \) shows that the event 1 is due to the misdetection by honest SUs. On the other hand, \( b \) and \( 1 - p_\mu \) show that 10 happens even when there is no misdetection by the honest SUs. The terms \( (1 - b) \) and \( p_\mu \) show that the event 10 happens due to the MUs while misdetection is happening while \( b \) and \( 1 - b \) happen together show that 10 is happening because the MUs are inverting their decisions with probability \( \beta \).

On the other hand for detecting the SSDF attacks which make the FC change its decision to 0 when the spectrum is actually occupied, the event type 01 is to be singled out. The
PUEAs are more damaging than SSDF attacks, so much that they change the basic hypothesis testing model in (1). PUEs have been classified as always-on and smart. Always-on PUEs always transmit the emulated signals while smart PUEs transmit the emulated signals only when the PU is not transmitting. The hypothesis testing model in (1) for PUEAs becomes

\[ y(k) = h_p(k)x(k) + h_c(k)r(k) + w(k) \quad H_1 \]
\[ y(k) = h_c(k)x(k) + w(k) \quad H_0 \]

where \( h_p(k) \) and \( h_c(k) \) denote the channel fading component from the PU transmitter and the PUE transmitter respectively. \( s(k) \) is the PU signal which is emulated by the PUE. For smart PUEs, the hypothesis testing model is modified as

\[ y(k) = b_p(k)x(k) + h_c(k)r(k) + w(k) \quad H_{11} \]
\[ y(k) = b_c(k)x(k) + w(k) \quad H_{10} \]
\[ y(k) = b_p(k)x(k) + w(k) \quad H_{01} \]
\[ y(k) = w(k) \quad H_{00} \]

respectively. Hypotheses \( H_{00} \) and \( H_{11} \) denote the presence of neither PU signal nor PUE signal and the presence of both the signals respectively, while hypotheses \( H_{01} \) and \( H_{10} \) denote the presence of PUE signal but not the PU signal, presence of PU signal but not the PUE signal respectively. The mathematical definitions for \( P_a \) and \( P_{md} \) for the above hypothesis testing problems in (27) and (28) remain the same as defined in (11) and (12). However, the closed form expressions obtained after solving (11) and (12) for an honest SU system in (1) change completely when PUE is present. PUEAs severely affect the throughput of the SUs. They also increase interference to the PU. We categorize the counter mechanisms to PUEAs also as active and passive mechanisms. Active mechanisms aim at cancelling or suppressing the PUE signal by differentiating it from the PU signal. This differentiation is facilitated by differentiating the received signal strength (RSS), some features, location of the PU and the PUE [39–41]. The second approach is passive where instead of detecting the PUE signal, a specific damage done by the PUE on the SUs is suppressed [21, 42–44]. The counter strategies proposed in the existing literature to counter both the attacks have been detailed as follows.

For detecting the PUEs, a Strong Stackelberg equilibrium (SSE) based surveillance strategy has been followed [116]. The network manager performs the surveillance of the PU spectrum. The attacker is assumed to be rational enough to adapt to the surveillance strategy. The task of the network manager is to observe the spectrum and decide whether the signal occupying it is from the PU or from the PUE. A multi-channel is considered for surveillance. A game theoretic approach is formulated where the attacker and the network monitor are designated as the players. The attacker emulates the PUE signals while the network monitor, regarded as the defender, monitors the spectrum. The strategy set of the attacker over \( K_1 \) bands is
denoted by
\[ \sigma_A = \{ A_0, A_1, \ldots, A_{K_t-1} \} \] (29)

Similarly, the strategy set of the defender is written as
\[ \sigma_D = S_0, S_1, \ldots, S_{K_t-1} \] (30)

Based on these actions, the attacker and the defender receives certain pay-offs. Based on the pay-offs obtained by the defender, the primary user emulation attacks are detected. The variables that enable the calculation of the pay-offs are illustrated as follows:

**Attacker**

- \( C_A \) is the cost for attacking.
- \( G_A \) is the benefit of using the channel for any CR user at one data frame.
- \( P_A \) is the penalty value for being captured by the defender.

For the defender

- \( C_S \) is the cost for implementing the surveillance process.
- \( G_S \) is the benefit for detecting the attack.

The parameters \( C_A, G_A, P_A, C_S, G_S \) help in the formulation of the pay-off. After performing rigorous calculations, pay-offs are obtained in the form of these parameters for the various conditions on the actions of the PU and the PUE. For example if the defender is performing surveillance when the attacker is attacking when the PU is not transmitting, the defender receives a reward \(-C_A + G_A\). This reward is received by the defender only when it is correctly able to detect the attack. Similarly when the defender is performing surveillance when the attacker is attacking while the PU is transmitting, the reward obtained by the defender on correct detection is \(-C_A\). Similarly the attacks are detected in the other scenarios.

Further in [117], the mechanism has been extended to detecting the PUEAs with the help of the rewards obtained by the SUs. It is assumed that a penalty is imposed on the SUs when the PU suffers interference. The formulation of the reward obtained by an SU is given as

\[ U = R.1 \text{(Successful transmission)} - L.1 \text{(Transmission failure)} \]

\[ - B.1 \text{(Hopping cost)} - F.1 \text{(Busy channel)} \]

\[ - Q.1 \text{(Packet drop)} + E.1 \text{(Attacker detection)} \] (31)

The expected reward for the SUs is obtained as

\[ \overline{U} = \sum_{n=1}^{\infty} \delta^{n-1} U(n) \] (32)

where \( \delta \) represents the discount factor \( 0 < \delta \leq 1 \). The status of an SU is represented with a Markov chain model and the presence or the absence of the PUEA is determined. The utilities and payoffs defined can be used to identify PUEAs by identifying their effects the SU throughput under a Rayleigh flat fading channel [118]. Karimi et al. also derive a test statistic based on the generalized likelihood ratio test to differentiate the PUEs from the actual PU. An investigation on the damages caused by the smartness of the PUEAs has also been conducted and significant damage is found. Rathee et al. in [119] use the payoffs for the network manager, the PU and the SUs to propose a secure hand-off mechanism for identifying the PUEAs. It is achieved by introducing a coordinating CR user which computes the level of trust of each SU based on its behavioral characteristics. This method is further improved with the help of artificial neural network (ANN) in [120].

### 3 | COUNTER STRATEGIES AGAINST SSDF ATTACKS

As discussed earlier, the SSDF attacks are caused when one or more MUs transmit fake signals to misdirect the SUs performing CSS [11, 34]. These attacks can be caused by a single MU, multiple MUs independently, or multiple MUs in collusion. As mentioned earlier, the counter mechanisms for these attacks have been categorized as active and passive approaches. Active approaches include location identification based and statistical approaches while passive approaches include reputation-based mechanisms, game theoretic, and damage suppression-based approaches. Location-based approaches counter the SSDF attacks by identifying the locations of the PU, the SUs, or MU. Statistical approaches differentiate the statistical properties of the MUs’ data with the honest SUs’ data. The statistical tests are based on outlier rejection from a sample of data. An outlier is a value in a data-set having different statistical properties. The incoming data to the FC from the cooperating SUs follow a specific statistical distribution. A random low or high value transmitted by an MU belongs to a different distribution and behaves as an outlier. Using statistical tests, these outliers can be identified and discarded. Different statistical tests have been reported in the literature [45, 46]. Reputation based mechanisms depend on the previous history of the SU node. The reporting of the SUs is compared with a trusted SU. Based on the previous history of the reported decisions, the SU nodes are assigned weight values. The SU nodes repeatedly giving values similar to the values of the trusted node are weighed high. The main challenge in these mechanisms is to identify the trusted SU. In game theoretic approaches, the SUs, the PU, and the FC are regarded as players. Their actions are termed as strategies and the outcome of their actions are termed as utilities or payoffs. To counter the security threats with game theoretic approaches, the benefits obtained by an SU in reporting honestly or maliciously are termed as honest and malicious utilities. The objective in these approaches is to maximize the honest utilities and minimize the malicious utilities, so that the SUs do not turn malicious. In damage suppression, instead of detecting the MUs, a particular damage of the SSDF attacks is identified and minimized. The damage can be caused on the PU or the SUs. The various mechanisms to counter the active attacks in the research literature are explained next.
3.1 Active methods

Active methods aim at directly eliminating the malicious readings or detecting the MUs. The prominent active methods are location identification based approaches and statistical approaches. We brief about the existing works in each of these approaches as follows:

3.1.1 Location identification based approaches

Location identification based mechanisms counter the SSDF attacks by identifying the locations of the PU, the SU or MU. The idea of using localization based approaches for countering MUs can be attributed to the Ma et al. in [14], where the localization of PUs has been carried out. They have aimed to locate the PU which helps in reducing interference to it and in detecting MUs. Ma et al. also design location aware mechanism access control protocol and show significant throughput gains.

There are two kinds of algorithms for localization: range based algorithms and range free algorithms. The range free algorithms are less accurate but simple to implement, whereas range based algorithms are accurate but complicated to implement. Ma et al. have obtained a simple to implement and accurate algorithm and term it as semi-range algorithm. They have mainly focused on how MUs are affecting the localization of the PU.

The above concept can be used by the MUs can be used to geo-locate the position of the SUs from their sensing reports [15]. This leakage of the location of the SUs is considered as the privacy leakage of the SUs. The defence against privacy leakage is carried out in two steps viz., the privacy preserving sensing report aggregation (PPSRA) and the distributed dummy report injection (DDRI) protocols to prevent the privacy leakage. These two steps are together named as privacy preserving CSS. The PPSRA uses cryptographic techniques with which the FC can get the final result from each SU without needing its calculated individual value. Subsequently, the DDRI algorithm provides differential location privacy for SUs. A single service provider (SP) has been considered as a central entity serving a group of SUs.

When multiple SPs are considered, they are used for performing CSS. Each SP has the perfect knowledge of the group of SUs it is serving. In [31], the attackers constitute of the SUs and the SPs. The information of the SUs is shared with every entity in the network. The malicious SPs and SUs can misuse this information to geo-locate the honest SUs and compromise with their location privacy. To counter such privacy leakage, a privacy preservation framework termed as PrimCos is proposed. In this mechanism, before executing CSS, the original data is transferred to a privacy preserving form that pre-
serves the statistical information. Additionally, the SPs share perturbed sensing data by adding a random noise to it. The perturbation hides the exactness of the data and prevents its leakage. However, the reconstruction of the perturbed data is challenging and remains an open research problem. The complexity of this system is another challenge, as sensing is a time bound process. The proposed mechanism gives the SUs sufficient protection for privacy and incentivizes them to share their data. Nevertheless, the accuracy in the localization of the PUs is severely affected, particularly when they are mobile. In [32], such effects are studied for a system facing SSDF attacks by tracking the mobile PUs. The accuracy in the localization of PU is severely affected under the attacks. The objective is to suppress the attacks from the MUs by tracking the mobile PUs. However, it becomes challenging when MUs manipulate the data, because localization largely depends on the sensing results of the SUs. To face this challenge, the authors propose sequential Monte Carlo combined with shadow fading estimation (SOLID) for attack/fault tolerant mobile PUs. This mechanism integrates sequentially Monte Carlo estimation based target tracking with shadow fading estimation. The sequential Monte Carlo estimation based tracking uses the sensing reports of the SUs iteratively to track the location of the PU. The shadow fading estimation part of the mechanisms refers to estimating the shadow fading correlation in the sensing reports induced by the PU’s mobility. When the shadow fading estimation is integrated with sequential Monte Carlo estimation based tracking, the effects of MUs on localizing the PU is significa-

TABLE 3 Active defence mechanisms for PUEAs

| Defence mechanism       | Principle                                                                 | Available works       | Limitations and open research issues                                                                 |
|-------------------------|---------------------------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------|
| Location based defence  | With signal characteristics, the source of the signal is verified for being the PU | References [39, 75–77] | Depend on matching the RSS and DOA of the signals from the transmitter with those from the PU.         |
| Fingerprint authentication | A tag, dependent of the PU signal, is added in it. The tag acts as an authentication information of the PU. | References [17, 18, 41, 78–89] | Successful implementation of this mechanism is complex as it involves the insertion of the tag in the PU signal. |
cantly reduced. In [47], the authors aim to detect the honest SUs in a CSS rather than MUs. The authors aim to form a cluster with no MUs with a fast searching algorithm and propose a scheme based on clustering the honest SUs with a fast sensing algorithm. The proposed fast sensing algorithm groups the SUs into different clusters. The clusters transmit their decisions about the presence of the PU to the FC. From the decisions of various clusters, their distances from the PU is estimated. This estimated distance is compared to the actual distance and the corresponding error is calculated. If the error associated with a cluster is below a predefined threshold, it is regarded as honest with no malicious sensor. Such a cluster is categorized as a trusted cluster. Next, the FC decides the status of the PU channel only with the information shared by the trusted clusters.

### 3.1.2 Statistical test based approaches

The signals transmitted by MUs are likely to follow different distributions from that of the signals transmitted by the SUs. This difference in the statistical distribution can be exploited to detect the signals of the MUs. In statistical attack prevention mechanisms, the difference in the statistical properties of the honest SUs and the MUs is observed [33, 34]. These attack prevention mechanisms were first introduced in [33] where the authors consider distributed detection in the presence of cooperative Byzantine attacks. These attacks are launched by Byzantine sensors which have been reprogrammed deliberately to send fictitious observations to the FC. To counter these attacks, the authors propose to obtain the optimal attacking distributions for the Byzantine sensors that minimizes the detection error exponent. Subsequently, the smallest error exponent is obtained that signifies the power of the attack. The smallest error exponent is further used to obtain the minimum fraction of Byzantine attackers that are capable of damaging successful

| Defence mechanism | Principle | Available works | Limitations and open research issues |
|-------------------|-----------|----------------|-------------------------------------|
| Suppressing the harmful effects of the PUEAs | In these approaches, a particular harm to the SU system done by the PUEAs is countered. By nature, these mechanisms are identical to the Damage suppression based approaches for defending the SSDF attacks. | References [21, 42, 44, 96, 97] | The suppressing harmful effects of PUEAs based defence mechanisms focus on a very narrow subset of damages. The other damages remain untouched or may even result in deteriorating them. Though a constraint may be put on the deteriorating parameters, but still these mechanisms fail to make a comprehensive defence strategy. |
| Avoiding the signals from the PUE | These approaches aim to avoid the PUE signals, rather than detecting them or suppressing the harmful effects done by them. Generally they are based on wideband channels which facilitate hopping over different channels. The challenge addressed in these mechanisms for the SUs to identify the presence of the PUE signal on a particular channel without latency and hop on a different channel. | References [98–106] | The mechanism of avoiding PUE signals is difficult to be implemented on a narrow channel. Generally they need hopping on multiple number of channels to avoid the PUE signal. They are also subject to a prior detection of the PUE signal. |

PU detection at the FC. Using this idea for detecting MUs in CSS can be attributed to the work in [46]. As mentioned earlier, MUs transmit fake data to the FC which can be a constant or any other random value. Hence, the data from the MUs is likely to follow a distribution different from the SUs’ data. The fundamental idea of [46] is outlier detection, where the data from MUs are treated as outliers [46]. The basic notion followed here to detect outliers is done on the basis of outlier factor $o_i$ which is the difference with the mean of the data ($\mu_i$) divided by the standard deviation ($\sigma_i$) of the data, given as $o_i = \frac{T_{ij} - \mu_i}{\sigma_i}$, for $0 \leq i \leq N$. If the $o_i$ associated with the $i$th data is greater than a threshold value, then that data value is regarded as an outlier. However, this method has a limitation that it is dependent on $\mu_i$ and $\sigma_i$, which are contaminated by the outliers. To overcome this limitation, a bi-variate estimate based outlier factor calculation is proposed. The bi-variate estimate is based on assigning penalty values to each cooperating SU. It depends on the number of iterations where positive and negative changes in the data values of the SUs happen. The penalty assigned to the $i$th SU $P_i[k]$ is given as

\[ P_i[k] = \sum_{k' \in S_k[k]} (\sigma_i [k' - 1] + o_i^- [k']) + \sum_{k' \in L_k[k]} (\sigma_i [k' - 1] + o_i^+ [k']) \]  

\[ o_i^- [k'] = \begin{cases} \frac{T_{ij} - \mu_i}{\sigma_i}; & T_{ij} < \mu_i \\ 0; & \text{otherwise} \end{cases} 

\[ o_i^+ [k'] = \begin{cases} \frac{T_{ij} - \mu_i}{\sigma_i}; & T_{ij} > \mu_i \\ 0; & \text{otherwise} \end{cases} \]
where $S[k]$ and $\Delta[k]$ are the sets of iterations for which $\Delta μ[k] = \Delta μ[k] - \Delta μ[k-1]$ is positive and negative respectively.

The above mechanism is subject to the challenging requirement of a priori knowledge of the environment, as the incoming SU's data at the FC depends on the channel gain between the respective SU and the FC. This limitation can be overcome by modifying the statistical test to detecting the statistical differences between the CSS decision and the individual SU decisions. In [48], the authors propose an algorithm based on the Kruskal-Wallis test to detect the MUs without any a priori knowledge. This test is a non-parametric method for testing whether samples originate from the same distribution. The proposed algorithm uses the statistical differences between the cooperative decision and the individual SU decisions. The statistical mechanisms can use Bayesian approach if the FC has some knowledge about the strategy of the MUs. In [49], a Bayesian approach is followed to detect the MUs. The authors assume some knowledge about the strategy of MUs's data to be available with the FC. Since, it is assumed that the MUs’ strategy is known, the a posteriori probability of their attacks can be known with reverse engineering on some captured MUs and hence all MUs are detected subsequently. The Bayesian approach is an efficient mechanism to detect the MUs, however, depends on the a priori knowledge of the SUs. This dependence is overcome in [16], where it is shown that it is always possible to detect the MUs when they attack individually, even when the information on their strategy is not available. Attacking individually means that the MUs are not aware about the responses of other SUs. When the MUs know or can hear other SUs, a strategy has been formulated such that the SUs are never detected by them. Then, a strategy is formulated for detecting the MUs. The prior condition for this strategy is availability of the knowledge of $P_{H}$ and $P_{F}$. The condition for this strategy is to have the knowledge $P_{H}$ and $P_{F}$. The authors point that practically the strategies of the MUs cannot be known a priori, particularly for a system when the MUs can hear other SUs and modify their attacks accordingly. Hence, the mechanisms proposed will fail to detect the MUs. To overcome the challenge of the unknown strategies of the MUs, a data mining technique to detect abnormalities has been proposed in [16]. This technique is fundamentally the application of the outlier detection method in (35)–(37) without the requirement of the a priori information on the MUs. Finally, the sensing reports of the SUs are kept in high dimension space and the possible abnormalities are detected. The idea of this work is to place the sensing reports of the SUs in a high dimension space and detect possible abnormalities.

CR systems are generally based on wideband sensing as PU is likely to hold license over a wide spectrum band. The study of security issues on widebands is thus significant. In [50], Srinu et al. study wide band sensing under SSDF attacks. The wide band is divided into multiple bands. They propose to predict the PU signal status on the multiple bands by integrating the entropy and cyclic properties of the received signal. The presence of MUs complicates accomplishing this proposal. The MUs are eliminated by designing by designing the generalized extreme statistical deviate and adjust boxplot methods by using uncertainty and autocorrelation properties of the signals. It is found that the proposed mechanism is efficient in eliminating the MUs. In [51], Tang et al. have aimed to save the CR-mobile ad hoc networks (MANETs) from security risks. The proposed scheme is a bio-inspired consensus algorithm. It takes the inspiration from self-organising behaviour of the birds, fishes, ants, honeybees or other animals in groups. Engineering algorithms have been formulated on the basis of the behaviour of animals in groups in the existing researches [52–54]. Studying the difference between the communication at the higher level and the animals at the lower level, the authors generate fundamental insights at the group decision at the higher level and individual communication. The algorithm makes the use of the local communication between the SUs. The major advantage of the algorithm is its low cost. Also the failure of a local SU node does not lead to the failure of the complete system. The basic requirement of this algorithm is to use the local communication and the group level communication model, to strike out the unwanted signals inserted by the SSDF attacks, and then make the correct decision about the presence of the PU which can be viewed as the multi agent coordination system. The summary of [51] is that it is local communication added to the global decision. He et al. in [55] propose a statistical approach based on identifying the abnormal statistical spectrum sensing behaviours to suppress the malicious activities. Two hidden Markov models (HMM) have been adopted for the behaviours of the honest SUs and the MUs. The detection of the MUs is achieved by differentiating between the models. Due to the abnormal statistical characteristics, the HMM of attackers will be different from that of the honest SUs. Some features of the HMM will depict the difference. The algorithm is about inferring those different features regarded as the HMM parameters to facilitate the detection of the MUs. Active mechanisms are efficient for performing moment-to-moment MU detection and elimination. However, as they require complex hardware designs for implementation, their application may be difficult in certain systems. The next study is performed on passive attack prevention mechanisms for defending SSDF attacks.

### 3.2 Passive methods

In passive methods, the SUs or the FC make changes in their own detection strategies which minimize the damages caused by the MUs [35–38]. Passive methods include reputation based approaches, game theoretic approaches, and damage suppression. We briefly describe the major works done in each of these approaches below:

#### 3.2.1 Reputation based mechanisms

The reputation based mechanisms are mainly followed in centralized CSS systems [56, 74]. The honesty is decided after observing the alignment of its decisions with the decisions of the FC over a period of time. In [55], existing data fusion techniques are investigated for their resistance towards the
Byzantine Failure problem. Then, they propose a new algorithm which uses a variable number of samples rather than using a fixed number of samples. The reputation based mechanisms are based on a “reputation value” $r_i$. The $i$th SU participating in CSS is given a reputation $r_i$, which depends on the history of the truthfulness of its decisions. The history is recorded over a period of time, where $r_i$ is updated as $r_i \leftarrow r_i + (-1)^{D_i + D}$. The weighted decision rule followed for applying CSS is given as

$$w_i = f(r_i) = \begin{cases} 0 & r_i \leq -g \\ \frac{r_i + g}{\text{max}(r_i + g)} & r_i > -g \end{cases}$$

where the variable $g$ fulfills the requirement that enough weight is allocated to the SU that has a slightly negative reputation value, which can happen due to the environmental attenuations.

A general reputation based algorithm known as the sequential probability ratio test (SPRT) [57], is given as

$$\frac{\sum_{i=1}^{N} w_i D_i < n}{\sum_{i=1}^{N} w_i D_i > n}$$

The accuracy brought by considering more number of local SS reports can be further enhanced by considering more number of samples. The authors in [36] aim to restrict the damage caused by the MUs by considering more samples. They proposed the enhanced WSPrT (EWSPrT) and enhanced weighted sequential zero/one test (EWZOT) which are robust against SSDF attacks. The EWSPrT and the EWZOT reduce the sample requirements for suppressing the effects of the MUs. However, large number of samples causes high data overhead. In [37], a reputation based approach is followed to detect the MUs. The system model contains multiple MUs and it is assumed that the number of MUs are known. An onion peeling approach, where the suspicious levels are calculated for each SU, is applied to detect the MUs. If the suspicious level is less than a threshold then the SU is regarded as honest. If the suspicious level crosses the threshold, its report is eliminated from decision making. The test is applied till there are no MUs left in the network. However, having the knowledge of the MUs is a strong assumption.

In [38], the performance limits of CSS under the SSDF attacks have been analysed when the information on the number MUs is not available. The authors show that above certain fraction of MUs, it is impossible for any reputation based attack strategy to counter them. The authors propose a new reputation based scheme. It is assumed that the attackers do not have the knowledge other SUs in the network and are dependent only on their own decisions. The attack prevention strategies also aim at countering collaborative attacks. The proposed schemes are basically reputation based countering schemes designed by counting the mismatches between an SU’s decisions and the FC’s decision. After performing this operation for a period of time, the Byzantines are removed from the data.

The efficiency of the defence mechanisms deteriorate in mobile CRN systems. The fluctuations in the channel gains caused to the mobility of SUs causes reporting errors at the FC, which affect the respective SU’s reputation. In [74] and [56], the mobile CRNs under attacks have been considered. The existing researches to mitigate the attacks were proposed for static CRNs. These algorithms for static CRNs cannot be applied for mobile CRNs, because they need localization information. If those algorithms are applied to mobile CRNs, the honest SUs having bad path-loss would be charged. For mobile CRNs, the authors propose to use two trust parameters: location reliability and malicious intention (LRMI). A high LR signifies the location of an SU having less path-loss whereas MI signifies to the intention of the SUs. It is observed that the proposed scheme improves both the MU detection rate and the PU detection.

In [58], the effect of multiple MUs on the energy efficiency along with the detection accuracy of the CR has been studied. A low overhead symmetric cryptographic mechanism based protocol to address SSDF attacks under a trade-off between the energy efficiency and the security of the CRN is given. An optimal number of security bits needed to maximize the energy efficiency has been derived. The authors show that the effects of MUs on energy efficiency depend on the fusion rule, which is used to form the global decision. Detecting the cause of abnormality in the data is challenging. The patterns of distortion brought by environmental obstacles and maliciousness are
not always differentiable. The authors in [59] rely on the consistency of the system states estimated by each SU. The proposed scheme removes the abnormalities in the data of the various sensors irrespective of the cause of the deviations in the abnormal reports. System states refer to the path loss exponent [60] and the PU signal power. The MUs do not have control over these parameters. The authors propose iterative state estimation (IRIS) scheme to detect the abnormalities in the data. The IRIS scheme does two examinations: the received signal power and the pathloss exponent of the path. By examining each sensor’s result, the scheme finds the measurement residual, which indicates the deviation of the PU signal power and the path loss from their normal values. In [61], the authors use combinatorial optimization identification (COI) [62] to counter the SSDF attacks. The proposed technique is a complement to the previously proposed IRIS technique. The authors have studied the attack scenario where IRIS does not work. The IRIS may also remove a good data sample having a large residual while keeping a compromised data sample. As a prevention mechanism, the authors propose COI to complement the IRIS. The limitation has also been overcome in [63] where the authors design a reputation based classifier to classify the SUs and the MUs. The classification is based on more than the traditional two divisions of honest and malicious. Such classification helps to handle the case when different honest SUs have different individual P’s and P’s and there are multiple types of MUs. An iterative expectation maximization algorithm is used to make this classification, calculate global P and P, and reliably detect the PU for the sensing system under the attacks. Their assumption is that the MUs are less in number than the SUs. Except this assumption, no prior knowledge at the FC has been assumed. The MUs can be classified on various grounds like having bad signal and channel characteristics. The MUs have been divided on causing more than one type of attacks. This is done with only few divisions from the CRs while in traditional reputation based classifiers large number of SUs cannot classify the SUs perfectly. The proposed mechanism outperforms other reputation based mechanisms particularly for large number of SUs.

Reputation based methods also help to identify the SU node near to the FC. The detection system near to the decision node is identified with the consistency in the correctness of its decisions. When the decisions of a node suffer lesser pathloss, they remain uncorrupted. Pathloss varies inversely with the distance. The relationship between the transmit and received powers as per the pathloss model is given as [122]

\[ P_t = P_t \left( \frac{\sqrt{G_t \lambda}}{4\pi d} \right)^2 \]  

(40)

where \( \sqrt{G_t} \) is a constant and is the product of the transmit and receive antennas field radiation patterns in the line of sight (LOS) direction and \( \lambda \) is the signal wavelength. Thus, a node constantly reporting correct decisions is quite likely near to the decision node as it is suffering less path loss.

The major challenge here is to recognize that which node has a lesser path loss with the decision node. In this regard, the reputation of the cooperating nodes is observed. A node having a high reputation value quite likely is located near to the decision node. The reputation value is based on the trust of a node. In this regard, sliding window based trust mechanism has been used. It observes the consistency in the correctness of the decisions from an SU for a duration of \( T \) time slots. A sliding window accommodates the time slots 1 to \( T \). A time period of \( K \) such windows is considered. As the sliding window slides on the time scale, its indexing changes from sliding window 1 to sliding window \( K \). The sliding window \( K \) accommodates the time slots \((K-1)T \) to \( KT \). Within the time period \( T \) slots of each sliding window, the number of matches between the decision of an SU and that of the FC is denotes as \( k_{sw} \). Each window has a trust value associated with it and is given as

\[ P(V_{T+1} = 1 | N(T) = k_{sw}) = \frac{k_{sw} + 1}{T + 2} \]  

(41)

where \( V_T \) is an index showing the match between the local SU decision and the global decision of the FC.

For \( K \) sliding windows, there are \( K \) trust values. The weighing factor of the \( i \)th sliding window, denoted by \( \lambda_i \), is given as

\[ \lambda_i = \frac{i + 1}{K + 1} \]  

(42)

The trust value of the \( m \)th SU is given as

\[ R_m = \frac{k_{sw} + 1}{T + 2} \]  

(43)

At the sliding window \( K \), the long term accumulated weighted trust of the \( m \)th SU, denoted by \( R_m' \), is given as

\[ R_m' = \frac{\sum_{i=1}^{K} \lambda_i R_m}{\sum_{i=1}^{K} \lambda_i} \]  

(44)

A cumulative weighted average is helpful to characterize long term behaviours or strategies of an SU. A number of research works can be found on the above concept. It has been used for cluster based reputation formulation to detect intrusion attacks in [123], generalized Byzantine attack and defence in [124, 125] for the analysis of attack strategies in the absence of defence and implementing suitable defence strategy in [126], for the removal of anomalous values from the data fusion process in [127], for the removal of malicious data in heterogeneous and ultra-dense networks in [128], for implementing a Bayesian inference based sliding-window trust mechanism in [129] analysing a cost benefit trade-off in Byzantine attacks in CSS in [130] and detecting MUs in non-orthogonal multiple access based systems in [131].

3.2.2 Game theoretic approach

In the game theoretic approaches, the CR communication systems are analysed with game theory [64–66]. The FC and the SUs make changes in their detection strategies as per the
outcome of the game. In a general game theoretic set up, the SUs, the PU, and the FC are regarded as players. Their actions are termed as strategies and the outcome of their actions are termed as utilities or payoffs. The benefits obtained by an SU in reporting honestly and maliciously are termed as honest and malicious utilities respectively. A general objective in this approach is to maximize the honest utility and minimize the malicious utility, so that the SUs refrain from turning malicious.

The honest utility for an SU is defined as

$$E_{U_i}(n) = P((D \leq n - 1) \cap H_i) \left(1 - P_{PU} \right) \frac{U_{SU}}{N}$$

$$+ P((D \leq n - 1) \cap H_i) \left(1 - P_{PU} \right) \frac{U_{SU}}{N}$$

$$+ \left(1 - P_{PU} \right) \left(\frac{U_{SU} - C_p}{N} + P_{PU} \frac{-C_p}{N}\right)$$

(45)

where $P_{PU}$ is the probability of error between the PU transmitter and the PU receiver when collisions happen, $P_{PU}$ is the probability of error when there is no collision, $U_{SU}$ is the utility of the SU when it performs successful transmission, $C_p$ is the collision penalty imposed by the PU on the FC which is divided among the N cooperating SUs. The next step is the formulation of the malicious utility $G_{U_i}(m, n)$ seen by the MUs as

$$G_{U_i}(m, n) = P((D = n) \cap H_i) S_p \frac{U_{SU}}{m}$$

$$- P((D = n) \cap H_i) \frac{C_p}{N}$$

(46)

where $S_p = 1 - P_{PU}$ and $m$ is the number of MUs. The general condition for an MU to attack is when it sees,

$$G_{U_i}(m, n) > E_{U_i}(n)$$

(47)

Based on the above condition, the bounds on $C_p$ are derived for defending the attacks from the MUs under different scenarios. The $m$ MUs form an attack strategy to get the highest possible damage to the honest SUs. The attack strategy is made with the help of game theory.

Designing efficient defence mechanisms with Game Theory requires a thorough understanding of the behaviour of the MUs. In [64], colluded denial of service (DoS) attacks have been studied. The authors perform the security study from the perspective of the MUs. The colluded malicious activity has been studied in single and multiple stages. These attacks are performed with a game theoretic approach. The attackers maximize their utility in a group rather than maximizing their individual utilities. In a single stage scenario, a cooperative game is formulated where the malicious nodes aim to attack as many secondary networks as possible while putting a minimum constraint on the cost or penalty they have to pay. The theoretical expression for the net pay-off has been formulated for the MUs and the optimal strategy is derived for them. In a multistage discrete time scenario, the Markov chain model for the dynamic behaviour of MUs has been formulated. The Markov chain models the change of the states. It is proved that as the system reaches the steady state, the net payoff becomes independent of the switching probability and becomes dependent on the number of SUs. Finally the authors obtain the optimal number of malicious users to carry out attacks successfully. The colluded DoS attacks have been countered in [67], where the effects of coordinated DoS on identity management (IdM) systems have been minimized. It is a damage suppression approach and will be explained in the next section. In [65], the authors have investigated an attack scenario where the SUs can access a single frequency band at a time and they hop among the different channels. They study the communication between the SUs and the MUs to find the optimum hopping strategy for the SUs using the Markov decision process. The hopping strategy is aimed towards countering the jamming attacks. Initially, the analysis is done for a perfect knowledge of the channels. Subsequently, two schemes have been proposed for the SUs to gain the knowledge of the adversaries. This knowledge enables them to handle attacks. The authors have also considered the case when the SUs can use all the channels simultaneously. The anti-jamming game is redefined for this case and the problem is modelled as Colonel Blotto game where random power allocation is the defence strategy. These games are zero sum games where players are tasked to distribute limited resources over several objects. The Nash Equilibrium has been established for this game which minimizes the worst-case damage.

In [66], the authors have modelled the jamming and anti-jamming processes as Markov decision processes. Following this approach, the SUs are able to counter the attacks from the MUs and maximize their pay-off function. First the authors use first policy iteration [68] method. However, the method is computationally expensive. Hence, the authors use Q function method to solve the problem.

3.3 Damage suppression approach

In this approach, a particular damage caused by the MU to a specific entity of the SU network is detected and is reduced [69–73]. Unlike the above approaches, it does not depend on detection, localization or down weighting of the MU. The affected entity can be the PU, the energy harvesting scheme, the channel coordination, the secrecy of the data etc.

Damage suppression approaches have been widely studied in the literature. In [69], the damage caused by the MUs to the PU has been reduced. The SUs get the favour from the PU to use its spectrum only when the SUs secure the PU communication from the MUs present in the system. Hence, the SUs behave as “jammer” for the MUs. The mechanism has been carried out in two hops. In the first hop the SU transmitter sends the information to the relay set and the SU receiver acts as a friendly jammer to disturb the overhearing of the MUs. In the second hop, the relay transmits the information to the SU receiver and the SU transmitter acts as a friendly jammer to disturb the overhearing of the MUs.

A clear advantage offered by this mechanism is that the possibly disturbing SU service from the perspective of the PU is
brought into a rather beneficial service. The possibly disturbing SU service from the perspective of the PU is brought into a rather beneficial service. The damage done by the MUs to the PU is minimized with the help of the SUs, however, the main objective of this work is to maintain any compromise in the secrecy of the SU. Optimal relay selection, time allocation, and power allocation are obtained for protecting the secrecy rate of the SUs while at the same time maintaining the minimum secrecy rate of the PU. Note that the damage caused due to secrecy leakage is reflected in the outage probability of the SU network. The secrecy rate is defined as the difference between the transmitter-receiver data rate and the transmitter-eavesdropper data rate. The normalized secrecy rates of the PU transmitter-receiver and the PU transmitter-eavesdropper are given as

\[ \gamma_{PT-PR} = \log_2(1 + \frac{P_{PT}h_{PT-PR}}{N_0B + I^2_{PR}}) \]  

and

\[ \gamma_{ST-SR} = \log_2(1 + \frac{P_{ST}h_{ST-SR}}{N_0B + I^2_{SR}}) \]  

where subscripts PT, PR, and e denote the primary transmitter, the primary receiver, and the eavesdropper respectively, and \( \gamma_{PT-PR} \) and \( \gamma_{ST-SR} \) are the SINRs at the PR and at the eavesdropper respectively, given as

\[ \gamma_{PT-PR} = \frac{P_{PT}h_{PT-PR}}{N_0B + I^2_{PR}} \]  

\[ \gamma_{ST-SR} = \frac{P_{ST}h_{ST-SR}}{N_0B + I^2_{SR}} \]

where \( P_{PT} \) is the transmit power of the PU transmitter, \( h_{a \rightarrow b} \) is the channel gain on the link \( a \rightarrow b \) link, and \( I_a \) is the interference on the node \( a \). \( a \) and \( b \) are dummy variables. Similarly, the secrecy rate of the SU transmitter-receiver link is given as

\[ \epsilon_{ST-SR} = \log_2(1 + \frac{\gamma_{ST-SR}}{1 + \gamma_{ST-e}}) \]  

where

\[ \gamma_{ST-e} = \frac{P_{ST}h_{ST-e}}{N_0B + I^2_{SR}} \]  

Depending on the damage to be reduced, \( \epsilon_{PT-PR} \) and \( \epsilon_{ST-SR} \) can be maximized or can be used for applying constraints over them.

Enhancing the secrecy performance in terms of data rate is a robust way to reduce the damage caused by the MUs. An outage probability analysis can be another way to reduce these damages. In [72], the secrecy performance is investigated in terms of an outage probability. A relay scheme is proposed to prevent eavesdropping and assist transmission from the CR transmitter to CR receiver. It is shown that the physical layer secrecy is significantly improved by increasing the number of relays. Another security issue addressed here is that a CR enabled SU turning malicious as it can sense the environment. This capability can be used to launch attacks. This increases the chances of a CRN to have more attacks than a normal communication system. The broadcast system also increases the chances to overhear secure communications.

The capability of the MUs to launch attacks considerably increases when they have energy harvesting capability. This issue is addressed in [70], where the MUs harvest energy for their operations like the honest SUs. The issue addressed is that MUs can also harvest energy for their operations like the honest SUs. The authors have formulated a throughput optimization problem under MU attacks as a Markov Decision process. Then a new solution based on deception tactics to stop smart MUs has been presented. Further, a learning algorithm for multiple SUs to find an optimal transmission policy has been designed. It is shown that these learning algorithms are effective in stopping smart MUs. In damage control mechanisms, the reliability in the coordination of channels plays a significant role. The damages caused by the attacks cause disruptions in the coordination of the channels. A preventive mechanism in this regard exists in [71], where the focus is on the coordination of channels in spectrum sharing systems in the presence of MUs. Reliable coordination of the channels is very important in CRNs. This coordination may be smooth until all the CRs in the SU network are honest. However, if the SUs start behaving contrary to their channel assignment, then such benefits associated with the channel coordination are negated. The authors in [71] focus on the dilemmas that occur in the coordination because of the attacks. The first dilemma is with the PU when it thinks that the SU is honest. On the other hand, if it thinks that the SU is malicious then it has to choose a band from a larger set of bands which invites more interferences. Similarly, there are dilemmas associated with the SUs about what the PU thinks about it. If the PU has a positive opinion about the SU, then the SU is allowed to transmit on the PU band. However, if the SU has a malicious image, then it will transmit on the SU band only. Corresponding to these beliefs, a game has been formulated and a game theoretic approach has been followed to solve the problem accordingly. The players are the PU, the SU, and the SP. The authors consider an example of two secondary service providers (SPs) with their own set of SUs. Suppose, each SP has been allotted a channel. The SPs will be benefitted in protecting its SUs from any possible interference. Similarly, they will get other benefits in harming the other channels. So, there are a set of strategies which the SUs can play. This reference also comes in the category of game theoretic approaches. However, since the authors aim to suppress the damage of SSDF attacks on the channel coordination, we have explained it in the damage suppression approaches category. In [67], the damage caused by the coordinated DoS attacks on the identity management (IdM) systems [64] has been minimized. IdM systems provide authentication authorities critical data. Through IdM systems, the SUs can authenticate at the single and multiple domains without providing additional information. IdM systems also help in reducing the complexity in the management of the data. They benefit many large systems like cyber-physical systems, smartgrids, and vehicular ad hoc networks. However, coordinated DoS attacks can severely affect IdM systems. The authors in [67] present
scheme for DoS attacks mitigation by their organization and optimization of the IdM system (SAMOS). This scheme is based on adaptive reorganizations and optimization of the IdM systems’ components to thwart DoS attacks. The coordinated DoS attack strategy has been considered from [64] and SAMOS aims at thwarting it. It is found that SAMOS is efficient in this purpose. A significant issue for the damage suppression attack prevention mechanisms is the optimal decision fusion rule for minimizing a damage caused by the MUs. In decision fusion rule based CSS, the optimal value of n has been obtained by obtaining and using the attack strength [73]. This ratio comes out to be the probability of an SU of being malicious. The optimal value of n minimizes the Bayes risk. However for data fusion, this issue remains unstudied.

4 COUNTER STRATEGIES AGAINST PUEAS

PUEAs are launched when the MUs attack by transmitting the emulated PU signal. The PUEAs severely compromise the functioning of the SU network. There are many existing and ongoing researches to defend the SU network from PUEAs. We categorize the major proposed mechanisms as active and passive approaches.

4.1 Active methods

The active methods aim at cancelling or suppressing the PUE signal by differentiating the power or a feature of the PUE signal from the PU signal. The active methods are mainly categorized into three mechanisms based on the nature of implementation as the Location based defence mechanisms, Finger print detection mechanism, and Game theoretic approach. We discuss here the major studies performed in the literature and possibilities offered by them for further research.

4.1.1 Location based defence mechanism

The first widely used mechanism for detecting PUEAs is location based defence mechanism. It is based on transmitter verification performed by identifying the location of the respective transmitter. The most fundamental work in this category has been done on detecting a PUE is in [39]. Here, the authors have focused on the vacant TV bands, since the FCC has recognized the TV bands suitable for the initial application for CR technology. These TV bands experience lower dynamic traffic compared to the cellular networks. In this paper, a transmitter verification scheme termed as LocDef (localization based defence) has been proposed. In this scheme, the source of the signal is verified for being the PU by observing the signal characteristics. The location information of the PU has been used to differentiate between the PU and the PUE signal characteristics. The authors assume a stationary and known PU location. To implement this scheme, LocDef uses a non-iterative localization scheme. This method primarily depends on the modelling of the received signal from the PUE. The LocDef approach is based on calculating the mean RSS at two different points.

For illustrating the basic LocDef model, let us consider two SUs SU_1 and SU_2. The location of the PU transmitter is assumed to be known to both the SUs. They also consist self equipped localization units which help them to identify their own locations. Let their location coordinates be (x_1, y_1) and (x_2, y_2). Each SU receives the signal from the attacker and can record its respective received signal strength (RSS), which is modelled by statistical log-loss signal propagation model as

\[ P_i(dBm) = P_t(dBm) - \alpha \log(d) - s, \]  

where \( P_i \) is the RSS in dBm, \( P_t \) is the transmission signal strength in dBm, \( d \) is the transmitter receiver distance, and \( \alpha \) is the path loss constant. \( s \) represents the standard deviation associated with the degree of shadow fading, and it is assumed that it is the same for both the SUs as they are very close to each other. The SUs can interact with each other. Let the RSSs at the SU_1 and SU_2 be \( RSS_1 \) and \( RSS_2 \). With the measured values of \( RSS_1 \) and \( RSS_2 \), we can have

\[ \eta = \frac{d_{\text{attacker, SU}_2}}{d_{\text{attacker, SU}_1}} = 10 \frac{\text{RSS}_1-\text{RSS}_2}{\alpha} = 10 \frac{\Delta \text{RSS}}{\alpha} \]  

where \( d_{\text{attacker, SU}_1} \) and \( d_{\text{attacker, SU}_2} \) represent the distance from the attacker to the SU_1 and SU_2. If the position of the attacker is (x, y), then

\[ \eta \sqrt{(x - x_1)^2 + (y - y_1)^2} = \sqrt{(x - x_2)^2 + (y - y_2)^2}. \]  

The trace of the attacker is calculated as

\[ \text{radius} = \frac{\eta d_{12}}{\eta^2}, \text{centre} = \left( \frac{\eta^2 x_1 - x_2}{\eta^2 - 1}, \frac{\eta^2 y_1 - y_2}{\eta^2 - 1} \right), \eta \neq 1, \]  

In line with this mechanism, the RSS can be exploited in different ways to identify the PUE. Received signal strength indicators (RSSI) based learning mechanisms have been found efficient in detecting the PUEs [75]. The authors propose a technique based on particle swarm optimization algorithm and the RSSI for the PU/PUE position detection to increase the detection accuracy and decrease the probability of false alarms. The accuracy of the location for detecting the PUEs can be improved with estimation techniques. Two criteria have been used to obtain total number of co-channel transmitters in the primary system [76]. The first criterion is the net MMSE criterion, which uses Cramer–Rao lower bound on location accuracy. In [76], the authors present two criteria to determine the total number of co-channel transmitters in the primary system. The first criterion is the net MMSE criterion, which uses the Cramer–Rao lower bound on localization accuracy. The second criterion is the information theoretic criterion, the minimum description length. Although only signal strength measurements have been considered, the approach can be generalized to include other
types of observations (e.g., time and angle information) with independent measurements in additive noise.

The security attacks can advance to the next level by making their own malicious base stations. As a result, they can subvert the cell association process of the genuine base stations. A stochastic geometry framework can be used to efficiently handle random locations of the honest base stations and malicious base stations and analyse the impact of these attacks [77]. The conditional probability of the RLF given a suboptimal association triggered by MBSs has been derived analytically and the theoretical results using simulations have been verified. This paper also presents insights on the appropriate ranges of thresholds for MUs seeking association with LBSs and claiming RLF using the conditional RLF probability triggered by MBS attacks.

Location based PUEA detection can prove inefficient if the SUs further manipulate their signals and mislead the detector about their locations. To overcome these limitations, fingerprint based mechanisms have been widely used as prevention mechanisms for PUEA.

### 4.1.2 Finger print based authentication

Fingerprint based mechanisms use signature embedded in the PU signal to detect its authentication. The SUs check the embedded signature in the incoming signal and discard it if they find discrepancy in it. The signature or the fingerprint can be a feature of the signal or an external tag embedded in the signal. Thus the fingerprint can be dependent on the PU signal [17], or independent of it [78].

A fingerprint dependent on the PU signal is transmitted concurrently with its data. It is added in the PU signal by superimposing a secret modulation in the transmitted PU signal without requiring additional bandwidth. The designing of the authentication finger print system has to be performed at the physical layer, as performing it at the higher layers will require the PU and the SUs to follow the same protocol. A PU signal-independent fingerprint is better than a dependent one. Here, a fingerprint termed as an authentication tag is developed in the first stage and in the second stage, the developed tag is embedded with the PU signal as shown in Figure 6.

In the first stage, a tag is developed and in the second, the developed tag is embedded with the PU signal. At the receiver, the PUE signals are checked for the tag and if they do not possess it, they are cancelled out. The fundamental fingerprint authentication model is shown in

A tag is inserted in the PU signal at the transmitter. This tag has to be detected by the SU to know that the incoming signal is from the PU or the PUE. The PU transmit signal from (1) with tag embedded can be written as $s(k) = g(t, x)$ where $x$ is the transmit symbol and $t$ is the embedded tag bit, given as $t \in \{0, 1\}$. Thus, $g(0, x)$ and $g(1, x)$ denote the transmitted signal for $t \in \{0, 1\}$. It is assumed that $g(0, x) \in S_1$ and $g(1, x) \in S_1$, where $S_0$ and $S_1$ denote sets. If $\tilde{t}$ is the tag bit detected by the SU, the detection error probability is

$$P_e = Pr(\tilde{t} \neq t)$$ (58)

For successfully detecting the PUE, involves $P_e$ must be minimized at the SU which is done with the help of a Bayesian detector. The corresponding detection rule is formulated as

$$\gamma = \begin{cases} 0 & \text{if } Pr(y(k)|x(k) \in S_0) > Pr(y(k)|x(k) \in S_1) \\ 1 & \text{otherwise} \end{cases}$$ (59)

The above ML detection is solved depending on the distribution of the fading gain $h(k)$ in (1).

This method explores possibilities of using device specific features like device ID, MAC address, radio metrics like amplitude, frequency, and bandwidth as the fingerprints of the PUs. These features can also be used to determine the total number of transmitting devices in the PU spectrum [18]. The method proposed in [18] is non-parametric since the number of devices needs not be known a priori. After forming the fingerprints, the authors adopt the infinite Gaussian mixture model (IGMM) and propose a modified collapsed Gibbs sampling method to classify the extracted finger prints based on Bayesian classification. In the first module, the authors first check the phase of the signal and the carrier frequency of the signal because these properties are unique for the transmitter. Then they check the MAC address and from the MAC ID database, they differentiate it. The second module checks the signal ID. If the PUE transmits from the same ID but a different fingerprint, it is detected. It is found that the proposed classification efficiently detects the PUEs. The proposed mechanism is independent of the number of transmitters, hence it needs not to be estimated.

The efficiency of the PUEAs is enhanced to the next level if they are capable of detecting the channels which are to be used by the SUs and attack accordingly. A fingerprint based mechanism proposed to counter such PUEAs is based on allowing the SUs to share the messages among themselves [41]. Here, the RSS from the PU is considered as the signature or the fingerprint. The PUEs are assumed to have the capability to detect channels which are going to be used by the SUs and attack accordingly. A fingerprint based mechanism proposed to counter such PUEAs is based on allowing the SUs to share the messages among themselves [41].
other SUs. The distribution of the RSS from the PU and the suspect are used to perform these operations. The belief calculation is performed iteratively until the SUs converge to a common belief about the PUE. Then, the PUE is detected and its signal characteristics are broadcast to the CRs in the network. Finally, the SUs are able to avoid the PUE’s signal. In [79], a game theoretic framework has been proposed to discard the PUEs. The authors formulate a non-cooperative multistage game between the SUs and PUEs. The strategy of the SUs and PUEs are different. The SUs leave the spectrum on the arrival of the PU. But the PUE tries to interfere with it while also trying to keep the SUs away. A novel belief updating system for updating the SUs belief about the PUs has been proposed as the game evolves. It is shown that the proposed belief updating system achieves satisfactory performance for the SUs in terms of recognizing the true PUs and cancelling out the signals from the PUEs. The relationship between the energy level of the RF signal and the acoustic information of the primary signal can be exploited to detect the PUEs, particularly when the primary signal is the TV signal. This relationship is very difficult to mimic. The approach has been exploited in [80], where microphones and TVs are the designated PUs. Further, RF fingerprinting has been studied experimentally to detect the PUEs [90]. Low cost CRs have been considered for detecting the PUEs. Investigations have been performed on the distortions made by low-end CR receivers in the RF fingerprints. It is concluded that RF fingerprint can be concluded only when the CRs have high end receivers.

In fingerprint based approaches, the a priori knowledge on the PU signal is an obvious limitation. A direct approach in this regard could be observing the externally visible characteristics of the PU signals and using them as fingerprints. However, the characteristic should not be mimicable. In [81], the PUE detection is performed by the acquisition and the reconstruction of the PU signal activity pattern. This technique acquires the activity pattern of the signal through SS. For example the ON and OFF periods of the signal may be acquired as the activity pattern. Then, it reconstructs the signal with a signal reconstruction model and checks it for any error. By examining a reconstruction error, the signals from a PU or a PUE are differentiated. The paper aims to overcome the limitations of location based identification and fingerprint methods which need knowledge about the signal characteristics or the location of the PUE. Similarly in [85], a fingerprint mechanism independent of any previous knowledge about the system. The authors use the statistical characteristics of the users to address one of the important kinds of attacks called primary user emulation attack (PUEA).

In the proposed scheme, the received power statistics of the CR users is used to detect the PUEA. Pu et al. in [82] detect the motion-related feature vectors of PUs in the FFT of its signal to differentiate PUE from it. A database where the signal from the PU is given is referred. The authors record the data from the incoming signal and compare it to the data from the database. For further classification, they feed this data to a covariance descriptor with the help of a neural algorithm. The covariance descriptor classifies the incoming signal database with the existing signal database to detect the PUEs. In [83], two strategies have been proposed for the detection of the PUEs. The first strategy is a channel surveillance process to check for the presence of the PUEs. The second strategy is aimed at detecting new transmission opportunities for the PUEs. An extra sensing process has been implemented to carry out the second strategy. The PUEs have been categorized as selfish, malicious, and mixed. The selfish PUEs aim for transmitting whereas malicious PUEs only aim to cause problem for the SUs, like obstructing the operation of the CR network. The mixed PUEs launch attacks in both the forms. In this process, the channel has been sensed and if an SU signal is found on the channel, it indicates that it is being used by a selfish PUE. After the sensing time, if the FC sees a channel is free which was declared busy after the sensing process, it was attacked by a PUE. It is found that it is possible to retrieve the opportunity of using the attacked channel by sensing it again after the sensing time finishes. Hence, an extra sensing process has been proposed. Essentially, the selfish PUE keeps transmitting throughout the sensing and the transmission periods of the SU whereas the smart PUEs transmit only for the sensing time. The authors have studied this problem with a game theoretic approach. The PUEs and the defenders are considered players and the Nash equilibrium has been derived for all the three attackers (malicious, selfish and mixed PUEs).

Certain inherent parameters in the PU signal like the minimum eigenvalue (EME) [86] can be used to mitigate PUEA through less spatial correlated secondary users (SUs). The SUs are selected based on their spatial correlation characteristics in log-normal shadow fading environment. Hence, the detection performance is improved. Simulation results show that the proposed method mitigates the PUEA effectively with lesser number of SUs.

Another significant mechanism has been proposed by employing an underlay RF fingerprint in the PU signal [87]. The fingerprint is introduced as an underlay waveform on the top of the header of the legitimate PU signal. This underlay waveform is consistent of wider bandwidth and higher baud rate than those of the original primary users signal. As a direct result, the underlay waveform exhibits a unique and different cyclostationary feature than that of the primary user signal. At the CR, a sophisticated cyclostationary analysis algorithm, combined with a primary user signal cancellation, is capable of revealing this unique cyclostationary feature to authenticate and validate the identity of the legitimate PU. The PUE attack signal, on the other hand, will not reveal this cyclostationary feature and fail to pass the authentication.

Further, a hybrid PUEA detection method has been proposed [88], where two kinds of wireless channel characteristics between the transmitter and the receiver, the Doppler spread and the variance of the received signal power, are utilized to infer the source of the received signal. In the CRN with mobile SU, the Doppler spread between the SU and the primary user (PU) may differ from that between the SU and the primary user emulator (PUE) because of different relative velocities. However, the performance of the PUEA detection method based on Doppler spread may be affected the relative position between the SU and the PUE. In order to make the detection performance be unaffected the relative position
between the SU and PUE, the variance of the received signal power is also used as the signature of the transmitter.

In [89], the authors propose a reliable AES-encrypted DTV scheme, in which an AES-encrypted reference signal is generated at the TV transmitter and used as the sync byte of each DTV data frame. By allowing a shared secret between the transmitter and the receiver, the reference signal can be regenerated at the receiver and used to achieve accurate identification of authorized primary users. The effectiveness of the proposed approach through both theoretical derivation and simulation examples has been analysed. It is shown that with the AES-encrypted DTV scheme, the primary user can be detected with high accuracy and low false alarm rate under primary user emulation attacks. It should be emphasized that the proposed scheme requires no changes in hardware or system structure except for a plug-in AES chip. Potentially, it can be applied to today’s DTV system directly to mitigate primary user emulation attacks, and achieve efficient spectrum sharing.

4.1.3 Game theoretic approach

In these approaches, the PUEs are actively cornered by formulating optimal strategies with the help of game theory. Generally, the PU, the SU and the PUE act as the players. They formulate strategies based on maximizing the rewards received by them respectively. In a typical setup, the PUEs may design strategies to maximize their rewards while the SUs and the PU play strategies to thwart these attacks.

In these approaches, the perfectness of information shared between players having common interest players a significant role. The evolution of the imperfect information exchange to perfect information exchange between the SUs viz. players has been studied in [91], where a game theoretical framework is proposed to study the primary user emulation attack (PUEA) on cognitive radio nodes as a game of imperfect information between the SUs, who do not exchange game information between them against the adversaries generating the PUEA and to define optimal strategies with minor computational demands. When the SU challenges the PU emulator successfully, updating the information on a cloud-based database enables the rest of the network to know the identity of PUE. As the game evolves, the grand coalition of the SUs acts as the one without collaboration against the PU emulator playing a winning strategy. The performance of the game for optimal strategies is equal to the performance of the collaborative methods for PUEA detection.

A possibility to be explored with game theoretic approaches is that whether the PUEAs can be mitigated by allowing an interaction between the SUs and the PUEs. In [92], the interaction between the PUE attacker and the secondary user is modelled as a constant-sum differential game which is called PUE attack game. The secondary user’s objective is to find the optimal sensing strategy so as to maximize its overall channel usability, while the attacker’s objective is to minimize the secondary user’s overall channel usability. The Nash equilibrium solution of this PUE attack game is deprived, and the optimal anti-PUE attack strategy is obtained. Numerical results demonstrate the trajectories of the secondary user’s optimal channel sensing strategies over time, and also shows that: by following the differential game solution, the secondary user can always optimize its channel usability when confronting PUE attacks. For illustrating the model considered for the game theoretic approach, let the number of channels which can be at most be tested by the SU be $M$ and the number of channels which can be attacked by the PUE attacker be $N$. The strategy of the SU $u(t)$ is defined as the portion of $M$ channels, denoted as $u(t) \in \left[\frac{1}{M}, 1\right]$. The strategy of the attacker $v(t)$ is denoted as $v(t) \in [0, 1]$. The left boundary of $v(t)$ is 0, as the attacker can decide whether to attack or not. The probability with which each PU channel will be sensed is given as $\frac{M u(t)}{K}$. On the other hand, the probability with which each channel will be attacked will be $\frac{N v(t)}{K}$. At a time instant $t$, the total number of available channels which are sensed by the SU but not attacked by the attacker is denoted as

$$x_s = \frac{M u(t)}{K} \left(1 - \frac{N v(t)}{K}\right) K$$

$$x_a = M u(t) - \frac{M N}{K} u(t) v(t)$$

The number of channels which are successfully attacked (sensed and attacked), is denoted as:

$$x_s = \frac{M u(t) N v(t)}{K} K$$

$$x_a = M u(t) v(t)$$

At the time instant $t$, the pure usability of channels for the SU is defined as

$$\zeta_5 \propto \zeta_3$$

For the time period of the cognitive radio network $[0, T]$, the total pure usability for an SU will be $\int_0^T (\zeta_5(t) - \zeta_3(t)) dt$. The total power consumption for an SU is defined as $\mu \int_0^T M u(t) dt$, where $\mu$ is the unit power consumption for sensing one channel. Thus, the overall utility for an SU is given as

$$J_s = \int_0^T [\zeta_5(t) - \zeta_3(t)] dt - \mu \int_0^T M u(t) dt$$

Similarly, total pure usability for the PUE and the overall utility are given as $\int_0^T (\zeta_4 - \zeta_3) dt$ and

$$J_a = \int_0^T [\zeta_4(t) - \zeta_3(t)] dt - \psi \int_0^T N v(t) dt$$
The SUs and the attackers fulfil their own objectives by maximizing or minimizing the expressions in (65) and (66) or their derivatives. In [93], a dynamic secure routing game framework to effectively combat jamming attacks in distributed cognitive radio networks has been proposed. First, a stochastic multi-stage zero-sum game framework based on the directional exploration of ad hoc on-demand distance vector (AODV) algorithms has been proposed. The zero-sum game captures the conflicting goals between malicious attackers and honest nodes and considers packet error probability and delay as performance metrics. The game-theoretic routing protocol guarantees a performance level given by the value of the game. Distributed Boltzmann–Gibbs learning is used for an on-line routing algorithm, in which the users do not have the knowledge of the attackers and the utility function. Instead, the users learn the payoffs based on their past observations. Simulations are used to illustrate the proposed routing mechanism and compare the algorithm with fictitious-play learning. Unlike typical distributed routing algorithms such as AODV routing, the proposed secure routing algorithm supports a novel recovery of routing path failure against unknown attackers.

The game theoretic approach has been extended to formulate a multi-channel surveillance game between the selfish attack and the surveillance process in multi-channel CRNs [94]. The sequence-form representation method is adopted to determine the Nash equilibrium (NE) of the game. It is shown that performing the obtained NE surveillance strategy significantly mitigates selfish PUEA. Later it has been pointed that the network managers could adopt a surveillance process on the disallowed channels for identifying illegal channel occupation of selfish PUEA [94], and hence mitigating selfish PUEA. Determining surveillance strategies, particularly in multi-channel context, is necessary for ensuring network operation fairness. In this paper, the authors formulate a game, called multi-channel surveillance game, between the selfish attack and the surveillance process in multi-channel CRNs. The sequence-form representation method is adopted to determine the NE of the game.

In [95], the problem is analysed within a Bayesian game framework, in which users are unsure of the legitimacy of the claimed type of other users. It is shown that depending on radios’ beliefs about the fraction of PUs in the system, a policy maker can control the occurrence of emulation attacks by adjusting the gains and costs associated with performing or checking for emulation attacks.

### 4.2 Passive methods

The passive approaches have been applied in two ways:

1. Suppressing one or more harmful effects of PUEAs on the SU network rather than directly cancelling its signal with the help of the channel state information (CSI) of the PUE with the PU or the SU with the PU.
2. Avoiding the signals from the PUE using the CSI of the PU or the PUE.

![FIGURE 7 Point diagram of primary user emulation attacks (PUEAs)](Image)

Passive approaches largely depend on the channel based signatures of the PU-SU link. It is defining the path between the PUE and the FC [120]. Let us consider a part of Figure 4 containing the PUE, one SU and the PU, as shown in Figure 7.

Detecting PUEAs can be done with the help of transmitter specific features or with the help of channel-specific features. The latter method detects the PUEs by estimating the received signal power at the SU. The received signal power after the signal traverses a path of distance \( r \), denoted by \( P_r \), will be proportional to \( r^{-\alpha} \), where \( \alpha \) is the path loss coefficient. \( P_r \) is also proportional to a shadowing random variable \( G \), which is given as, \( G = e^{\beta} \). Thus,

\[
P_r = P_r r^{-\alpha} e^{\beta}
\]

where \( \beta \) follows a normal distribution \( \beta \sim \mathcal{N}(0, \sigma^2) \). An SU receives signals from the PU with \( E_1, E_2, \ldots, E_n \), where \( n \) is the number of observed signals. Then \( E_1, E_2, \ldots, E_n \) is i.i.d. and follow the same distribution as \( P_r^{(v)} \), where

\[
P_r^{(v)} = P_r r^{-\alpha} e^{\beta}
\]

As shown in Figure 7, \( r_1 \) is the distance of the PU from the SU. The next step will be to estimate the statistical parameters of \( P_r^{(v)} \). It is done as

\[
u_r = E \left( P_r^{(v)} \right) = P_r r^{-\alpha} e^{\frac{1}{2} \sigma^2 \sigma_p^2}
\]

\[
\sigma_r^2 = \text{Var} \left( P_r^{(v)} \right) = P_r^2 r^2 e^{\sigma^2 \sigma_p^2 - 1}.
\]

The estimation of \( \nu_r \) and \( \sigma_r^2 \) will be performed as

\[
\hat{\nu}_r = \frac{1}{n} \sum_{i=1}^{n} y_i
\]

\[
\hat{\sigma}_r^2 = \frac{1}{n} \sum_{i=1}^{n} \left( y_i - \frac{1}{n} \sum_{j=1}^{n} y_j \right)^2
\]
A large $n$ gives accurate estimation of $\nu$ and $\sigma_d^2$. The detection of PUE is done as

$$
\text{Signal is from PU if } |P_d - \hat{\nu}_d| \leq k\sqrt{\sigma_d^2} \\
\text{Signal is from PUE if } |P_d - \hat{\nu}_d| > k\sqrt{\sigma_d^2}
$$

(73)

The difference between the passive approaches and the active approaches is that the passive approaches are independent of the features, the RSS, the external tagging, or the classification of the PU or the PUE. Secondly, the active approaches may have to make some modifications in their sensing strategies after detecting the PUE, like cancelling its signals. However, the passive approach follows the normal sensing integrated with a mechanism for the suppression of a particular damage caused by the PUE signal or its avoidance with the help of CSI. Following are some of the major works with passive approaches with the above applications:

### 4.3 Suppressing the harmful effects of the PUEAs

In these approaches, a particular harm to the SU system done by the PUEAs is countered. In approach, these mechanisms are identical to the Damage suppression based approaches for defending the SSDF attacks. The harmful effects can be in the form of throughput degradation, increased interference to the PU, or the combination of both. In [21], the channel information is used to minimize the damage caused by the PUEAs to the robustness of a CSS system. The paper considers a basic cooperative model with an always-on PUE. The expressions for $P_d$ and $P_{fa}$ are obtained for a CSS system where a PUE is present. Then, $P_d$ is maximized with a bound on $P_{fa}$ to obtain the optimal weights for performing CSS. The optimal weights are functions of the channel gains of the PU and the PUE with the SU. This leads to the minimization of the damages caused by PUEAs on the detection performance of CSS. The authors in [42] and [44] investigate the harmful effects of smart PUEAs on the CSS network. Smart PUEAs attack only when the PU is absent. The degradation caused by the PUEAs is accounted as probability of error $P_e$, which is defined as the sum of $P_{fa}$ and $1 - P_d$. Decision fusion CSS has been considered and both aim at minimization of $P_e$. The parameter optimized for achieving the minimum $P_e$ is the transmission time. The difference between the works is that the authors in [42] perform this optimization for $n$ out of $N$ decision fusion systems whereas, the authors in [44] perform it for OR and AND rule based decision fusion systems. Alahmadi et al. in [96] aim at countering the damages caused by PUEAs on energy harvesting in an OFDM modulation based CR system. A DTV signal has been considered and the P2 pilot symbols are generated using an advance algorithm for encryption. The main aim of this research is sum-rate-maximization of the energy harvesting based SU system facing PUEAs. The sum-rate is the sum of the downlink transmission and the uplink transmission of the SUs. Alahmadi et al. minimize the interference of the PUEAs which affect the sum-rate for the SUs. The basic hypothesis model shown in (27) is considered in these mechanisms. First the particular damaged caused by the PUEAs. Next, this damage is suppressed with the help of weighted PUEAs. The weight values are designed in a manner to suppress the damages. Ideally, the weighted CSS scheme is carried out by making the weighted sum of the individual energy values transmitted by the SUs to the FC. However, here the weighted CSS scheme is slightly changed for mathematical simplicity. The individual signals from the SUs $y_i(k), i \in \mathcal{N}$ are added with weights assigned to each of them as

$$
y(k) = \sum_{i=1}^{N} w_i y_i(k)
$$

(74)

Now the energy is calculated as

$$
E_G = \sum_{i=1}^{K} y(k)
$$

(75)

The probability of false alarm and mis detection are obtained as

$$
P_{fa} = \frac{\Gamma(K - \frac{E_G}{\sigma_0^2})}{\Gamma(K)}
$$

(76)

$$
P_d = \frac{\Gamma(K - \frac{E_G}{\sigma_i^2})}{\Gamma(K)}
$$

(77)

where $\Gamma(\cdot, \cdot)$ and $\Gamma(\cdot)$ are the upper incomplete Gamma function and Gamma function respectively. The damage considered here is that the decrement caused in $P_d$ because of PUEAs. To suppress this damage, the maximization of $P_d$ has been carried out with a constraint on $P_{fa}$.

The Neymann–Pearson method now has dual tasks: the calculation of the decision threshold and the calculation of beamforming vector values $w$. The objective here is to minimize the effects of PUEAs as

$$
\max \ P_{\text{dfc}}(\lambda, w)
$$

subject to

$$
P_{\text{fc}}(\lambda, w) > \hat{\nu}_d
$$

(79)

where $P_{\text{fc}} = Pr(F_{\text{beam}} > \lambda | H_0)$ and $P_{\text{dfc}} = Pr(F_{\text{beam}} > \lambda | H_1)$ are the probabilities of false alarm and detection respectively. These values were functions of the channel gains on the PUSU and the PUE-SU link, $b_{af}$ and $b_{det}$, respectively. The optimal beamforming vector values were obtained as

$$
w_{\text{opt}} = (\phi^{-1} b_{\text{det}})^{1/2}
$$

(80)

where $\phi = \sigma_d^2 I + \sigma_2^2 I, H_{ij} = b_{det}h_{ij}^T$ for $[h_{ij}, h_{i2}, ..., h_{iN}]^T$. The above idea of the selection of CSS has been exploited in
various research works with different objectives. For example, it has been used for the minimization of energy consumption in [131], to study the statistical characteristics of the incoming data at the FC for PUEA avoidance in [132], for adaptive cooperative sensing to reduce sensing overhead while not affecting the sensing accuracy requirements in [133], to enable the assistance of the SUs in CSS for malicious attack suppression in [134] for obtaining the optimal voting rule and the optimal number of samples for performing CSS in the presence of MUs in [135], for the application of the maximum ratio combining in CSS for MU detection in [136], for the application of a heuristic algorithm, which chooses the optimal subset of cognitive sensors with minimum average energy consumption for CSS in [137], to use physical layer fingerprints in a multi-path Rayleigh fading channel for the mitigation of MUs in CSS [138, 139], and for the application of generalized likelihood ratio test and Rao test for suppressing the effects of MUs in CSS [140].

The expressions in (76) and (77) can be used to control the harms on different aspects of CSS. A significant aspect of CSS is its overall throughput. The lesser the $P_{fa}$ higher is the throughput of the system. Minimization of $P_{fa}$ can lead to maximization of the throughput. In [97], the focus is on the damage caused by the PUE on the throughput of the CSS system. The throughput of a CSS system is reflected in it $P_{th}$. Lower the $P_{fa}$ higher is the CSS throughput. Thus, the objective in [97] was the minimization of $P_{fa}$ in (76) with a constraint on $P_{th}$ in (77). Total error minimization is another objective widely studied within this category of attack defence mechanism. Total error is formulated with the sum of $P_{fa}$ and $1 - P_{th}$.

A significant requirement is reducing the damages of the PUEAs on the throughput of the SU at the network level. This study is performed in [107] by analysing the call blocking and dropping performance, where the authors develop the first centralized protocol. The authors developed the first centralized protocol to help SUs fuse their individual detection results with the help of a centralized controller, to better mitigate PUEA. Here, a distributed spectrum decision protocol in which SUs make individual spectrum decisions is developed and then individual sensing results with their one-hop neighbours to increase resilience to PUEA are exchanged. This protocol has been termed as NEAT: Neighbour assisted spectrum decision protocol. A detailed analysis of the protocol in terms of the probability of successful PUEA under Byzantine attacks has also been presented, where the malicious users can lie about their individual sensing results. It is shown that with negligible communication overhead, the proposed protocol reduces the probability of successful PUEA by up to three orders of magnitude in the presence of Byzantine attacks.

4.4 Avoiding the PUE signal

These approaches aim to avoid the PUE signals, rather than detecting them or suppressing the harmful effects done by them. Generally they are based on wideband channels which facilitate hopping over different channels. The challenge addressed in these mechanisms for the SUs to identify the presence of the PUE signal on a particular channel without latency and hop on a different channel. The authors in [98] and [99] combat PUEAs with a game theoretic approach. The authors assume that the channel statistics like channel availability probability are known a priori. The proposed idea is that the SUs will escape the PUEAs by randomly hopping on the available channels. Such random hopping is unlikely to be detected by the PUEs, and hence they will fail to harm the SUs. However, this creates a dog fight between the PUEs and the SUs. The work is aimed at studying the dogfight in accessing the spectrum, which refers to random hopping over the frequency bands to get access to them for their transmission. The fundamental model considered in these works is the Markov Chain model. Each band is either in busy or in idle state, denoted by B and I respectively. The busy state refers to the presence and idle state to the absence of the PU signal on the band. The probability that a channel $m$ is idle in an arbitrary time slot is denoted by $p_{m}$ and is given as

$$p_{m} = \frac{Q_{m}}{Q_{m} + Q_{B}}$$ (81)

where $Q_{B}$ and $Q_{m}$ are the state transition probabilities from state B to state I and from state I to state B, respectively. The $i$th SU formulates its action $u_{i}$ to avoid the PUE signals. The objective of the SUs is to act cooperatively and reach the Nash Equilibrium. The unique Nash equilibrium is attained when

$$u_{i} = \begin{cases} \frac{1}{\sum_{j=N-K+1}^{N} \frac{1}{p_{j}}}, & i = M - K + 1, \ldots, N, \\ 0, & i = 1, \ldots, M - K \end{cases}$$ (82)

where $M$ is the number of channels and $K$ is given as

$$K = \arg \max_{K} \left| \frac{1}{\sum_{j=N-K+1}^{N} \frac{1}{p_{j}}} \right|$$ (83)

The authors in [100] and [101] address the similar objective of [98] and [99] but for an unknown channel. In [100] and [101], the channel availability probability is unknown, and a blind dogfight algorithm has been proposed. To solve this issue, the algorithm of the adversarial bandit problem is adapted. The proposed works are passive defence based on the assumption that there are multiple channels available. The objective here is to intelligently use those multiple channels to avoid the PUEAs. In [102], the PUEs have been viewed as attackers which can behave as a PU or an SU. The authors assume that other SUs do not know about their fellow SUs or the PU. To check their knowledge about the PU or their fellow SUs, a Bayesian game has been formulated which depends on the SUs’ belief about a fraction of PUs. A policy maker can control the gains and costs associated with performing or checking for PUEAs. The authors derive conditions for the Nash equilibrium, the
conditions which throw light of some important facts such as whether the honest SUs will exist with PUEAs, with what probability PUEAs launch attacks, under what conditions the PUEAs are discouraged, with what probability the radios will challenge the license of other radios etc. These results can be used to determine appropriate policies to keep the rate of PUEAs low.

Another approach for PUE signal avoidance has been proposed in [103], where the PUE attacks only when no one is sensing the channel. A new room of vulnerability in the conventional sensing approaches where the PUE attacks only when no one is sensing the channel has been introduced in [103]. This attack will decrease the channel utilization by SUs and create a Denial of Service (DoS) situation for victim SUs. This attack has been named as off-sensing attack. The authors also propose an analytical model to analyse the impact of the off-sensing attack in a CRN.

In [104], the PUE signal avoidance has been studied without any prior knowledge on the primary user activity characteristics and the secondary user access strategies. They formulate the problem as a non-stochastic online learning problem where the PUE attacker needs to dynamically decide the attacking channel in each time slot based on its attacking experience in previous slots. The challenge in the considered problem is that the PUE attacker cannot observe the reward on the attacked channel because it never knows if a secondary user ever tries to access it. To solve this challenge, they propose an attack-but observe-another (ABOA) scheme, in which the PUE attacker attacks one channel in the spectrum sensing phase, but observes at least one other channel in the data transmission phase. The authors propose two online learning algorithms, EXP3-DO and OPT-RO, to dynamically decide the attacking and observing channels.

In [105], before avoidance, the authors attempt to characterize the PUEA. This is done by estimating the channel parameter and transmission power of the primary user or the BS with MLE. The PUE then transmits the false signal by emulating these characters to spoof other honest cognitive users making the wrong decisions. For PUEA avoidance, an expectation maximization based algorithm has been proposed by estimating the channel parameters. In the proposed approach, the difference of the parameters of primary channel and attack channel to achieve the accurate detection through a simple iterative algorithm has been utilized.

In [106], PUEA avoidance is carried out by first characterizing received power at good secondary user. This is done by using a flexible log-normal sum approximation. The received power thus characterized is used to determine the probability of successful PUEA on each secondary user, which is used to develop the proposed protocol. Simulation results demonstrate that the proposed protocol can significantly reduce the probability of successful PUEA under Byzantine attacks (i.e., when the malicious users intentionally provide false spectrum decisions), while still following the spectrum evacuation etiquette.

It can be concluded that the most fundamental impact of the security attacks is on the throughput of the SUs. The interference on the PU signals also increases severely. The impact on the SU throughput occurs as security attacks can cause the SUs to think that the PU signal is present when the spectrum is vacant from the PU signal. Consequently, the SUs cease their transmissions. In the other case, security attacks make the SUs believe that the PU signal is absent on a frequency band, when it is actually present. The SUs transmit on the respective band and cause interference to the PU. As a result, the PU signal suffers interference. Due to this interference, it can also impose a penalty on the SUs. It can be seen that both the active and passive mechanisms are being followed to counter the SSDF and PUE attacks. Both these mechanisms have certain advantages and disadvantages in countering SSDF and PUE attacks respectively. The active mechanisms counter the attacks head-on. They ensure a nearly instantaneous elimination of the corrupt data. However, the FC has to constantly be active in identifying the type of anomaly and its elimination. This may lead to an increased functional load on the FC. Passive mechanisms, on the other hand, are based on gradual suppression of the corrupt data over a time span. They are achieved with changes in the existing FC circuit which ensures malicious data suppression in the long term. However, operational latency can at times prove to be a disadvantage with them. In summary, for quick action, active mechanisms are recommended, whereas for robustness, passive mechanisms are recommended. The limitations with these approaches open a wide scope for further researches.

5 | OPEN RESEARCH DIRECTIONS

As mentioned above, the approaches surveyed have certain shortcomings which opens many new research problems. The problems are based on increasing efficiency of their fundamental mechanisms and rectifying the problems created with their application respectively. These research problems have been explained as follows:

5.1 | Active counter mechanisms for SSDF attacks

Several open research issues exist in active counter mechanisms for SSDF attacks. Location based defence mechanisms are effective but depend on the location identification of the PU for detecting the attacker. The location of the PU from each SU is transmitted to the FC via. their $P_m$s. During this process, the MUs can overhear the SUs and can make the estimate of the locations of the PU and the SU. This information leakage is known as location privacy leakage.

The primary limitation in statistical data based detection mechanisms is caused due to the confidence level of the statistical mechanism followed. The confidence level is the threshold till which a data value is considered to be an outlier. A narrow confidence level ensures that a data value is regarded as outlier even with a slight deviation from the distribution of the other data values. This ensures robustness in detecting the outlying data from the MUs. However, in case when an SU lies in a deep faded environment, the data value it transmits to the FC
Similar limitations exist with fingerprint based detection approaches. The SUs detect the authenticity of the PU signal with the help of its fingerprint inserted in the form of a tag. However, successful implementation of this mechanism is complex. It involves the insertion of the tag in the PU signal which is then communicated to the SU. When the SU receives the PU signal, it performs ML detection to check the similarity of the tag in the PU signal with the one communicated to it earlier. ML detection largely depends on the estimated channel gain between the PU transmitter and the SU receiver. Thus, the mechanism is susceptible to the channel estimation error. Efficient designing of low complex fingerprint mechanism without compromising on the accuracy remains an open research problem.

### 5.4 Passive counter mechanisms for PUEAs

Passive counter mechanisms have a wide scope of further research. The suppressing harmful effects of PUEAs based defence mechanisms focus on a very narrow subset of damages. The other damages remain untouched or may even result in deteriorating them. For example [19] focuses on the interference to the PU, but have to skip the effects on the SU throughput. Similarly, [52] focuses on the energy harvesting issues, while [97] focuses on the SU throughput leaving other issues untouched. Though a constraint has been put on the interference to the PU, but still these mechanisms fail to make a comprehensive defence strategy.

The mechanism of avoiding PUE signals is difficult to be implemented on a narrow channel. Generally they need hopping on multiple number of channels to avoid the PUE signal. They are also subject to a prior detection of the PUE signal. It must be noted that these attack mechanisms offer a huge scope for the application of learning algorithms, as they are highly dependent on moment-to-moment updates on the channels.

### 5.5 Some possible solutions

Following are some possible solutions to the problems presented:

- Prevention before attack. It aims to make a targeted reinforcement considering networks’ vulnerability, which will enhance the system’s inborn robustness to attack. For example, selectively improve critical nodes’ security levels. In consequence, the attack cost is increased while attack effectiveness declines.
- Appropriate counterattack. First of all, offending is coordinated with traditional defence schemes including bad data detection. After a certain period, the knowledge of malicious users’ behaviours are gradually obtained and the network develops the capacity of launching counterattack. Here, the counterattack means that users identified as malicious ought to be in certain punishment, which will improve users’ responsibility widely neglected by users due to the openness of the underlying protocols.
• The location aware schemes were studied which are capable of countering intelligent attacks taking advantage of the mobility of the PU and the SUs. Intelligent attackers will take advantage of the mobility characteristic to launch more intangible and powerful attack, which deserves considerable attention and is a challenging problem for defense. Besides, both PUs and SUs can be mobile and the problem can be more complex. This requires defense schemes to be location-aware. It will be a common thing in CRNs that the scenarios are time-varying due to, e.g., the mobility of PUs and/or SUs, the variation of attack behaviors and PU activities, etc. Correspondingly, efficient defense schemes should dynamically adapt to time-varying scenarios. Specifically, in mobile CRNs, every SU’s sensing environment is time-varying and when evaluating the confidence level of a SU’s sensing report, location diversity must be taken into consideration.

6 DISCUSSIONS AND LIMITATIONS

The work discussed various defense mechanisms for countering SSDF attacks like reputation based mechanisms and statistical test based mechanisms. For countering SSDF attacks, reputation based mechanism depend on the prior information of the environment as they depend on calculating the Likelihood function of the received signal. Also these mechanisms can suppress the colluded attacks only in a sequential manner. Consequently, their computational complexity is increased considerably. Statistically based mechanisms have a limitation that the SUs transmitting abnormal sensing reports, due to the environmental losses are tagged as outliers. In heterogeneous networks, the presence of MUs affects the correct estimation of cell boundaries. Smaller the cells, higher is the disparity in the reports of the SUs. However, the presence of MUs can result into higher disparity and affects the correct estimation of the cell size. In case of PUEAs, the use of analytical models for the received power for attack detection can lead to large number of samples and long sensing times, which is difficult to achieve in highly dynamic environment. The RSS based mechanisms depend on separate sensor networks which increases the costs related to deployment and maintenance. Also they assume fixed transmission power for the signals transmitted from the MUs. In signature based mechanisms to detect the PU, modification of the PU signals and the need of a certification authority are necessary. Also, it can be affected to the vulnerabilities related to encryption and description of the PU data. In the mechanisms related to the modelling of PUEAs, the position of the attacker the distances between the PU, the SUs and the attacker have to be known in advance.

7 CONCLUSION

This paper performs a state-of-the-art survey of the defense mechanisms for mitigating security attacks in cognitive radio systems. In the beginning, the preliminaries of CSS have been briefly presented for general readers. Key CR operations like hypothesis testing and different types of CSS have been presented here. Next, the mechanisms of SSDF and PUEAs have been discussed. The different situations and the intentions of the attackers and their effects on CSS are discussed in detail. We showed the effects of SSDF and PUEAs on the throughput of the SU system and on the interference to the PUs. Then, a detailed study on the defense mechanisms for both these attacks was performed. The defense mechanisms were categorized as active and passive, based on the nature of their defense strategy. In a nutshell, active mechanisms directly detect and eliminate the MU, whereas passive mechanisms are based on bringing changes in the underlying operations of the CSS to mitigate the effects of the attacks. Finally, a detailed illustration of the open research problems and some possible solutions to these problems have been presented. It is envisioned that searching for new defense mechanisms for SSDF and PUEAs is a fruitful research area.

ACKNOWLEDGEMENT

This work is supported by fund of National Key Research and Development Program under the project number 2019YFB1803305, the Natural Science Foundation of China under Grant 61575126 and Grant 62071304, the Fund of Shenzhen Basic Research (JCYJ20170818091801577, JCYJ20190808120415280, 20200826152915001), the Natural Science Foundation of Guangdong under Grant 2018A0303130131 and Grant 2020A151501381.

ORCID
Shivanshu Shrivastava https://orcid.org/0000-0001-9313-4232
Bin Chen https://orcid.org/0000-0003-1208-6676

REFERENCES

1. McMillan, J.: Why auction the spectrum? Telecommun. Policy 19(3), 191–199 (1995)
2. Jain, R.: Spectrum auctions in India: lessons from experience. Telecommun. Policy 25(10), 671–688 (2001)
3. Federal Communications Commission, Spectrum Policy Task Force, ET Docket No. 02-135 (2002)
4. Mitola, J.: Cognitive radios: An integrated agent for software defined radio. Ph.D. Dissertation, Royal Institute of Technology (KTH), Stockholm (2000)
5. Federal Communications Commission, Notice of Proposed Rule Making and Order, ET Docket No.03-108 (2003)
6. Haykin, S.: Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas Commun. 23(2), 201–220 (2005)
7. Tandra, R., Sahai, A.: SNR walls for signal detection. IEEE J. Sel. Topics Signal Process. 2(1), 4–17 (2008)
8. Gandetto, M., Regazzoni, C.: Spectrum sensing: A distributed approach for cognitive terminals. IEEE J. Sel. Areas Commun. 25(3), 546–557 (2007)
9. Ganesan, G., Li, Y.: Cooperative spectrum sensing in cognitive radio, part I: Two user networks. IEEE Trans. Wirel. Commun. 6(6), 2204–2213 (2007)
10. Xiong, G., Kishore, S.: Cooperative spectrum sensing in cognitive radio networks under gaussian fusion channels. In: 2009 43rd Annual Conference on Information Sciences and Systems, pp. 675–680, IEEE, Piscataway, NJ (2009)
11. Mishra, S.M., Sahai, A., Brodersen, R.W.: Cooperative sensing among cogni-
tive radios. In: 2006 IEEE International Conference on Communicati-
ons, pp. 1658–1663, IEEE, Piscataway, NJ (2006)
12. Ghasemi, A., Sousa, E.S.: Collaborative spectrum sensing for opportunis-
tic access in fading environments. In: First IEEE International Sympo-
sium on New Frontiers in Dynamic Spectrum Access Networks, 2005.
DySPAN 2005., pp. 131–136, IEEE, Piscataway, NJ (2005)
13. Sahai, A., Hoven, N., Tandra, R.: Some fundamental limits on cognitive
radio. In: Allerton Conference on Communication, Control, and Com-
puting, Monticello, II, 29 September–1 October 2004
14. Ma, Z., et al.: A semi range-based iterative localization algorithm for
cognitive radio networks. IEEE Trans. Veh. Technol. 59(2), 704–717
(2010)
15. Li, S., et al.: Location privacy preservation in collaborative spectrum sens-
ing. In: 2012 Proceedings IEEE INFOCOM, pp. 729–737, IEEE, Piscat-
away, NJ (2012)
16. Li, H., Han, Z.: Catch me if you can: An abnormality detection approach
for collaborative spectrum sensing in cognitive radio networks. IEEE
Trans. Wirel. Commun. 9(11), 3554–3565 (2010)
17. Yu, P.L., Baras, J.S., Sadler, B.M.: Physical-layer authentication. IEEE
Trans. Inf. Forensics Secur. 3(1), 38–51, 2008.
18. Nguyen, N.T., Zheng, R., Han, Z.: On identifying primary user emulation
attacks in cognitive radio systems using nonparametric bayesian classifi-
cation. IEEE Trans. Signal Process. 60(3), 1432–1445 (2012)
19. Chen, R., Park, J.: Ensuring trustworthy spectrum sensing in cognitive
radio networks. In: 2006 1st IEEE Workshop on Networking Technolo-
gies for Software Defined Radio Networks, pp. 110–119, IEEE, Piscat-
away, NJ (2006)
20. Duan, L., et al.: Attack prevention for collaborative spectrum sensing in
cognitive radio networks. IEEE J. Sel. Areas Commun. 30(9), 1658–1665
21. Duan, L., et al.: Attack prevention for collaborative spectrum sensing in
cognitive radio networks. IEEE J. Sel. Areas Commun. 30(9), 1658–1665
2012
22. Chen, C., Cheng, H., Yao, Y.: Cooperative spectrum sensing in cogni-
tive radio networks in the presence of the primary user emulation attack.
IEEE Trans. Wirel. Commun. 10(7), 2135–2141 (2011)
23. Kay, S.M., Fundamentals of Statistical Signal Processing: Estimation The-
ory. Prentice-Hall PTR, Upper Saddle River, NJ (1998)
24. Letaief, K.B., Zhang, W.: Cooperative communications for cognitive radio
networks. Proc. IEEE 97(5), 878–893 (2009)
25. Sendonaris, A., Erkip, E., Aazhang, B.: User cooperation diversity. part i.
System description. IEEE Trans. Commun. 51(11), 1927–1938 (2003)
26. Sendonaris, A., Erkip, E., Aazhang, B.: User cooperation diversity. part ii.
Implementation aspects and performance analysis. IEEE Trans. Commun.
51(11), 1939–1948 (2003)
27. To, B.L., et al.: Decentralized cooperative spectrum sensing for cogni-
tive radio ad-hoc network: Hidden terminal awareness approach. In: 2012
11th International Conference on Information Science, Signal Process-
ing and their Applications (ISSPA), pp. 146–151, IEEE, Piscataway, NJ
2012
28. Mishra, S.M., Sahai, A., Brodersen, R.W.: Cooperative sensing among cogni-
tive radios. In: 2006 IEEE International Conference on Communicati-
ons, pp. 1658–1663, IEEE, Piscataway, NJ (2006)
29. Chen, R., Park, J., Bian, K.: Robust distributed spectrum sensing in cog-
nitive radio networks. In: IEEE INFOCOMM 2008 - The 27th Conference
on Computer Communications, pp. 1876–1884, IEEE, Piscataway, NJ
2008
30. Chen, C., et al.: A game-theoretical anti-jamming scheme for cognitive
radio networks. IEEE Network 27(3), 22–27 (2013)
31. Mousavifar, S.A., Leung, C.: Centralized collision attack in cognitive
radio collaborative spectrum sensing. In: 2014 IEEE 80th Vehicular
Technology Conference (VTC2014-Fall), pp. 1–6, IEEE, Piscataway, NJ
2014
32. Wu, Y., et al.: Anti-jamming games in multichannel cognitive radio net-
works. IEEE J Sel. Areas Commun. 30(1), 4–15 (2012)
33. Marano, S., Matta, V., Tong, L.: Distributed detection in the presence of
byzantine attacks. IEEE Trans. Signal Process. 57(1), 16–29 (2009)
34. Kaligineedi, P., Khabbazian, M., Bhargava, V.K.: Secure cooperative sens-
ing techniques for cognitive radio systems. In: 2008 IEEE International
Conference on Communications, pp. 3406–3410, IEEE, Piscataway, NJ
2008
35. Chen, R., Park, J., Bian, K.: Robust distributed spectrum sensing in cog-
nitive radio networks. In: IEEE INFOCOM 2008 - The 27th Conference
on Computer Communications, pp. 1876–1884, IEEE, Piscataway, NJ
2008
36. Zhu, F., Xiong, S.: Enhanced robust cooperative spectrum sensing in cog-
nitive radio. J. Commun. Networks 11(2), 122–133 (2009)
37. Wang, W., et al.: Detecting malicious nodes in collaborative spectrum
sensing. In: GLOBECOM 2009-2009 IEEE Global Telecommunications
Conference, pp. 1–6, IEEE, Piscataway, NJ (2009)
38. Rawat, A.S., et al.: Collaborative spectrum sensing in the presence of
byzantine attacks in cognitive radio networks. IEEE Trans. Signal Pro-
cess. 59(2), 774–786 (2011)
39. Chen, R., Park, J., Reed, J.H.: Defense against primary user emulation
attacks in cognitive radio networks. IEEE J. Sel. Areas Commun. 26(1),
25–37 (2008)
40. Yuan, Z., et al.: Defense against primary user emulation attacks
using belief propagation of location information in cognitive
radio networks. In: 2011 IEEE Wireless Communications and Net-
working Conference, pp. 599–604, IEEE, Piscataway, NJ (2011)
41. Yuan, Z., et al.: Defeating primary user emulation attacks using belief
propagation in cognitive radio networks. IEEE J. Sel. Areas Commun.
30(10), 1850–1860.56 (2012)
42. Saber, M.J., Sadadough, S.M.: Optimisation of cooperative spectrum
sensing for cognitive radio networks in the presence of smart primary
user emulation attack. Trans. Emerg. Telecommun. Technol. 28(1), e2885
(2017)
43. Saber, M.J., Sadadough, S.M.S.: Optimal energy detection in cognitive
radio networks in the presence of malicious users. In: ICCKEE 2013, pp.
173–177, IEEE, Piscataway, NJ (2013)
44. Haghighat, M., Sadadough, S.M.S.: Cooperative spectrum sensing for cog-
nitive radio networks in the presence of smart malicious users. AEU-Int.
J. Electron. Commun. 68(6), 520–527 (2014)
45. Kalamkar, S.S., Banerjee, A., Roychowdhury, A.: Malicious user sup-
pression for cooperative spectrum sensing in cognitive radio net-
works using dixon's outlier detection method. In: 2012 National Con-
ference on Communications (NCC), pp. 1–5, IEEE, Piscataway, NJ
2012
46. Kaligineedi, P., Khabbazian, M., Bhargava, V.K.: Malicious user detection
in a cognitive radio cooperative sensing system. IEEE Trans. Wirel.
Commun. 9(8), 2488–2497 (2010)
47. Ghaznavi, M., Jamshidi, A.: A reliable spectrum sensing method in the
presence of malicious sensors in distributed cognitive radio network.
IEEE Sens. J. 15(3), 1810–1816 (2015)
48. Adelantado, F., Verkouikis, C.: A non-parametric statistical approach
for malicious users detection in cognitive wireless ad-hoc networks.
In: 2011 IEEE International Conference on Communications (ICC), pp.
1–5 (2011)
49. Wang, W., et al.: Attack-proof collaborative spectrum sensing in cog-
nitive radio networks. In: 2009 43rd Annual Conference on Infor-
mation Sciences and Systems, pp. 130–134, IEEE, Piscataway, NJ
2009
50. Srinu, S., Sabat, S.L.: Cooperative wideband sensing based on entropy
and cyclic features under noise uncertainty. IET Signal Process. 7(8),
655–663 (2013)
51. Tang, H., et al.: Distributed consensus-based security mechanisms in
cognitive radio mobile ad hoc networks. IET Commun. 6(8), 974–983 (2012)
52. Ren, W., Beard, R.W.: Consensus seeking in multiagent systems under
dynamically changing interaction topologies. IEEE Trans. Automat.
Control 50(5), 655–661 (2005)
53. Xiao, L., Boyd, S., Lall, S.: A scheme for robust distributed sensor fusion
based on average consensus. In: IPSN 2005 Fourth International Sym-
posium on Information Processing in Sensor Networks, 2005, pp. 63–70,
IEEE, Piscataway, NJ (2005)
54. Huang, M., Manton, J.H.: Stochastic consensus seeking with measurement noise: Convergence and asymptotic normality. In: 2008 American Control Conference, pp. 1337–1342, IEEE, Piscataway, NJ (2008)

55. He, X., Dai, H., Ning, P.: Hmm-based malicious user detection for robust collaborative spectrum sensing. IEEE J. Sel. Areas Commun. 31(11), 2196–2208 (2013)

56. Wald, A.: Sequential tests of statistical hypotheses. Ann. Math. Statist. 6(2), 171–186 (1945)

57. Soltanmohammadi, E., Naraghi-Pour, M.: Fast detection of malicious behavior in cooperative spectrum sensing. IEEE J. Sel. Areas Commun. 32(3), 377–386 (2014)

58. Tan, Y., Sengupta, S., Subbalakshmi, K.P.: Analysis of coordinated denial-of-service attacks in IEEE 802.22 networks. IEEE J. Sel. Areas Commun. 29(4), 890–902 (2011)

59. Chen, C., et al.: A game-theoretical anti-jamming scheme for cognitive radio networks. IEEE Network 27(3), 22–27 (2013)

60. Monticelli, A., Wu, F.F., Yen, M.: Multiple bad data identification for state estimation by combinatorial optimization. IEEE Power Eng. Rev. PER-6(7), 73–74 (1986)

61. Nasif, A.O., Mark, B.L.: Measurement clustering criteria for localization of multiple transmitters. In: 2009 43rd Annual Conference on Information Sciences and Systems, pp. 341–345, IEEE, Piscataway, NJ (2009)

62. Feng, S., Kwon, H.M., Mukherjee, A.: Stochastic geometry analysis of reference signal spoofing attack in wireless cellular networks. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6, IEEE, Piscataway, NJ (2016)

63. Bolle, M., Chen, B., Du, W.K.: Physical layer spectrum usage authentication in cognitive radio: Analysis and implementation. IEEE Trans. on Information Forensics and Security 10(10), 2225–2235 (2015)

64. Tan, Y., Sengupta, S., Subbalakshmi, K.P.: Primary user emulation attack in dynamic spectrum access networks: a game-theoretic approach. IET Commun. 6(8), 964–973 (2012)

65. Chen, S., Zeng, K., Mohapatra, P.: Hearing is believing: Detecting wireless microphone emulation attacks in white space. IEEE Trans. Veh. Technol. 63(9), 4372–4382 (2014)

66. Nguyen-Thanh, N., et al.: Surveillance strategies against primary user emulation attack in cognitive radio networks. IEEE Trans. Wirel. Commun. 14(9), 4981–4993 (2015)

67. Rehman, S.U., Sowerby, K.W., Coghill, C.: Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. IET Commun. 8(8), 1274–1284 (2014)

68. Ghaznavi, M., Jamshidi, A.: Defence against primary user emulation attack using statistical properties of the cognitive radio received power. IET Commun. 11(9), 1535–1542.61 (2017)

69. Das, D., Das, S.: Eigenvalue detection based method to mitigate pue attacks in multichannel cognitive radio networks. In: 2013 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6, IEEE, Piscataway, NJ (2013)

70. Chakravarthy, R., et al.: Primary user authentication of cognitive radio network using underlay waveform. In: 2017 Cognitive Communications for Aerospace Applications Workshop (CCAA), pp. 1–5, IEEE, Piscataway, NJ (2017)

71. Li, Y., et al.: A primary user emulation attack detection scheme in cognitive radio network with mobile secondary user. In: 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1076–1081, IEEE, Piscataway, NJ (2016)

72. Alahmadi, A., et al.: Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. In: 2013 IEEE Global Communications Conference (GLOBECOM), pp. 3229–3234, IEEE, Piscataway, NJ (2013)

73. Rehman, S.U., Sowerby, K.W., Coghill, C.: Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios. IET Commun. 8(8), 1274–1284 (2014)

74. Kakalou, I., Psannis, K.E.: Coordination without collaboration in imperfect games: The primary user emulation attack example. IEEE Access 6, 5402–5414 (2018)

75. Hao, D., Sakurai, K.: A differential game approach to mitigating primary user emulation attacks in cognitive radio networks. In: 2012 IEEE 26th International Conference on Advanced Information Networking and Applications, pp. 495–502, IEEE, Piscataway, NJ (2012)

76. Zhu, Q., Song, J.B., Basar, T.: Dynamic secure routing game in distributed cognitive radio networks. In: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, pp. 1–6, IEEE, Piscataway, NJ (2011)

77. Xu, D., et al.: Mitigating primary emulation attacks in multi-channel cognitive radio networks: A surveillance game. In: 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1–6, IEEE, Piscataway, NJ (2016)

78. Thomas, R.W., et al.: A bayesian game analysis of emulation attacks in dynamic spectrum access networks. In: 2010 IEEE Symposium on New
Frontiers in Dynamic Spectrum (DySPAN), pp. 1–11, IEEE, Piscataway, NJ (2010)
96. Alahmadi, A., et al.: Subband puea detection and mitigation in ofdm-based cognitive radio networks. IEEE Trans. Inf. Forensics Secur. 10(10), 2131–2142 (2015)
97. Shrivastava, S., Rajesh, A., Bora, P.: Defense against primary user emulation attacks from the secondary user throughput perspective. AEU-Int. J. Electron. Commun. 84, 131–143 (2018)
98. Li, H., Han, Z.: Dogfight in spectrum: Jamming and anti-jamming in multichannel cognitive radio systems. In: GLOBECOM 2009-2009 IEEE Global Telecommunications Conference, pp. 1–6, IEEE, Piscataway, NJ (2009)
99. Li, H., Han, Z.: Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part i: Known channel statistics. IEEE Trans. Wirel. Commun. 9(11), 3566–3577 (2010)
100. Li, H., Han, Z.: Blind dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems with unknown channel statistics. In: 2010 IEEE International Conference on Communications, pp. 1–6, IEEE, Piscataway, NJ (2010)
101. Li, H., Han, Z.: Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems part ii: Unknown channel statistics. IEEE Trans. Wirel. Commun. 10(4), 274–283.63 (2011)
102. Thomas, R.W., et al.: Understanding conditions that lead to emulation attacks in dynamic spectrum access. IEEE Commun. Mag. 49(3), 32–37 (2011)
103. Hossain, M., Xie, J.: Impact of off-sensing attacks in cognitive radio networks. In: GLOBECOM 2017-2017 IEEE Global Communications Conference, pp. 1–6, IEEE, Piscataway, NJ (2017)
104. Dabaghchian, M., et al.: Online learning-based optimal primary user emulation attacks in cognitive radio networks. In: 2016 IEEE Conference on Communications and Network Security (CNS), pp. 100–108, IEEE, Piscataway, NJ (2016)
105. Liu, L., Zhang, Z., Li, J.: Em-based algorithm for defeating against primary user emulation attacks in cognitive wireless networks. In: 2016 2nd IEEE International Conference on Computer and Communications (ICCC), pp. 1450–1455, IEEE, Piscataway, NJ (2016)
106. Jin, Z., Anand, S., Subbalakshmi, K.P.: Robust spectrum decision protocol against primary user emulation attacks in dynamic spectrum access networks. In: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp. 1–5, IEEE, Piscataway, NJ (2010)
107. Jin, Z., et al.: Neat: A neighbor assisted spectrum decision protocol for resilience against puea. In: 2014 IEEE Conference on Communications and Network Security, pp. 44–52, IEEE, Piscataway, NJ (2014)
108. Marchang, N., Taggu, A., Patra, A.K.: Detecting byzantine attack in cognitive radio networks by exploiting frequency and ordering properties. IEEE Trans. Cognit. Commun. Networking 4(4), 816–824 (2018)
109. Wu, J., et al.: Cost-benefit tradeoff of byzantine attack in cooperative spectrum sensing. IEEE Syst. J. 14(2), 2532–2543 (2020)
110. Hashlamoun, W., Brahma, S., Varshney, P.K.: Mitigation of byzantine attacks on distributed detection systems using audit bits. IEEE Trans. Signal Inf. Process. over Networks 4(1), 18–32 (2018)
111. Hashlamoun, W., Brahma, S., Varshney, P.K.: Audit bit based distributed byzianen attack detection in the presence of byzaintines. IEEE Trans. Signal Inf. Process. over Networks 4(4), 643–655 (2018)
112. Zhang, L., et al.: Defending against byzantine attack in cooperative spectrum sensing: Defense reference and performance analysis. IEEE Access 4, 4011–4024 (2016)
113. Nie, G., et al.: Byzantine defense in collaborative spectrum sensing via bayesian learning. IEEE Access 5, 20089–20098 (2017)
114. Fu, Y., He, Z.: Bayesian-inference-based sliding window trust model against probabilistic ssf attack in cognitive radio networks. IEEE Syst. J. 14(2), 1764–1775 (2020)
115. Ta, D., et al.: Strategic surveillance against primary user emulation attacks in cognitive radio networks. IEEE Trans. Cognit. Commun. Networking 4(3), 582–596 (2018)
116. Hossain, M., Xie, J.: Hide and seek: A defense against off-sensing attack in cognitive radio networks. In: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, pp. 613–621, IEEE, Piscataway, NJ (2019)
117. Karimi, A., Taherpour, A., Cabric, D.: Smart traffic-aware primary user emulation attack and its impact on secondary user throughput under rayleigh flat fading channel. IEEE Trans. Inf. Forensics Secur. 15, 66–80 (2020)
118. Rathee, G., et al.: A secure spectrum handoff mechanism in cognitive radio networks. IEEE Trans. Cognit. Commun. Networking 6(3), 959–969 (2020)
119. Rathee, G., et al.: Handoff security using artificial neural networks in cognitive radio networks. IEEE Internet of Things Magazine 3(4), 20–28 (2020)
120. Chen, Z., et al.: Modeling primary user emulation attacks and defenses in cognitive radio networks. In: 2009 IEEE 28th International Performance Computing and Communications Conference, pp. 208–215, IEEE, Piscataway, NJ (2009)
121. Goldsmith, A.: Wireless Communications. Cambridge University Press, Cambridge (2005)
122. Rina, K., et al.: Can clustering be used to detect intrusion during spectrum sensing in cognitive radio networks? IEEE Syst. J. 12(1), 938–947 (2018)
123. Wu, J., et al.: Generalized byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks. IEEE Access 6, 53272–53286 (2018)
124. Wu, J., et al.: Robust reputation management mechanism in cooperative spectrum sensing. Electron. Lett. 55(21), 1128–1130 (2019)
125. Wu, J., et al.: Analysis of byzantine attack strategy for cooperative spectrum sensing. IEEE Commun. Lett. 24(8), 1631–1635 (2020)
126. Gao, R., et al.: A cooperative spectrum sensing scheme in malicious cognitive radio networks. In: 2019 IEEE Globecom Workshops (GC WKSHPS), pp. 1–5, IEEE, Piscataway, NJ (2019)
127. Ahmad, I., et al.: Trust and reputation management for securing collaboration in 5G access networks: The road ahead. IEEE Access 8, 62542–62560 (2020)
128. Fu, Y., He, Z.: Bayesian-inference-based sliding window trust model against probabilistic ssf attack in cognitive radio networks. IEEE Syst. J. 14(2), 1764–1775 (2020)
129. Wu, J., et al.: Cost-benefit tradeoff of byzantine attack in cooperative spectrum sensing. IEEE Syst. J. 14(2), 2532–2543 (2020)
130. Xia, S., et al.: Malicious user detection in non-orthogonal multiple access based on spectrum analysis. IEEE Signal Process. Lett. 27, 1390–1394 (2020)
131. Banerjee, A., Maiti, S.P.: On energy minimization in cooperative spectrum sensing using lrt in presence of emulation attack. In: 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6, IEEE, Piscataway, NJ (2016)
132. Ghaznavi, M., Jamshidi, A.: Defence against primary user emulation attack using statistical properties of the cognitive radio received power. IET Communications 11(9), 1555–1542 (2017)
133. Dai, Z., et al.: Adaptive cooperative sensing with low overhead for cognitive radio networks. In: 2013 IEEE Global Communications Conference (GLOBECOM), pp. 1173–1178 (2013)
134. Pongcharoenkan, Z., et al.: Efficient collaborative spectrum sensing under the smart primary user emulation attacker network. In: 2015 IEEE Global Communications Conference (GLOBECOM), pp. 1–7, IEEE, Piscataway, NJ (2015)
135. Saber, M.J., Sadough, S.M.S.: Optimal energy detection in cognitive radio networks in the presence of malicious users. In: ICCKE 2013, pp. 173–177, IEEE, Piscataway, NJ (2013)
136. Yang, J., et al.: Cooperative spectrum sensing against attacks in cognitive radio networks. In: 2014 IEEE International Conference on Information and Automation (ICIA), pp. 71–75, IEEE, Piscataway, NJ (2014)
137. Monemian, M., Mahdavi, M., Omidi, M.J.: Optimum sensor selection based on energy constraints in cooperative spectrum sensing for cognitive radio sensor networks. IEEE Sens. J. 16(6), 1829–1841 (2016)
138. Kudu, R.D., Karde, P.P., Thakare, V.M.: Performance of css cognitive radio networks under primary user emulation attack. In: 2017 Interna-
139. Gao, N., et al.: Robust collaborative spectrum sensing using phy-layer fingerprints in mobile cognitive radio networks. IEEE Commun. Lett. 21(5), 1063–1066 (2017)

140. Zhang, L., et al.: Spectrum sensing under spectrum misuse behaviors: A multihypothesis test perspective. IEEE Trans. Inf. Forensics Secur. 13(4), 993–1007 (2018)

How to cite this article: Shrivastava S, Rajesh A, Bora PK, Chen B, Dai M, Lin X, Wang H. A survey on security issues in cognitive radio based cooperative sensing. IET Commun. 2021;15:875–905. https://doi.org/10.1049/cmu2.12131