Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

Comprehensive survey on security challenges and solutions in cognitive radio networks

Elizabeth Atieno Otieno *

Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, 40601, Bondo.

Global Journal of Engineering and Technology Advances, 2024, 21(01), 001–037

Publication history: Received on 08 August 2024; revised on 27 September 2024; accepted on 29 September 2024

Article DOI: https://doi.org/10.30574/gjeta.2024.21.1.0177

Abstract

Cognitive Radio (CR) technology offers dynamic spectrum access, allowing for more efficient use of the radio frequency spectrum. While this innovation addresses spectrum scarcity, it introduces significant security and privacy concerns. This paper examines key vulnerabilities in cognitive radio networks (CRNs), including spectrum sensing data falsification, primary user emulation attacks, and denial-of-service attacks, which exploit the adaptive and opportunistic nature of CR systems. In addition, privacy challenges arise from the frequent sharing of location, identity, and spectrum usage data. This paper explores existing security frameworks, mitigation strategies, and privacy-preserving techniques, emphasizing the need for robust cryptographic methods, trust management, and real-time intrusion detection systems. The paper concludes by identifying open research areas that need attention to develop secure, resilient CRNs while preserving user privacy.

Keywords: Cognitive Radio Networks; Spectrum Sensing; Attacks; Security Vulnerabilities; Privacy Preservation; Intrusion Detection Systems**.**

1. Introduction

The growing demand for wireless communication has led to an increasing scarcity of available radio frequency spectrum [1], which is traditionally regulated and statically allocated. Conventional spectrum allocation policies often result in underutilized frequency bands [2], contributing to inefficient spectrum usage. The CR technology has emerged as a promising solution to address this problem by enabling dynamic spectrum access [3]. According to [4], CRNs are intelligent systems capable of sensing their surrounding environment, detecting unused spectrum (also known as spectrum holes or white spaces), and dynamically adjusting their transmission parameters to utilize these gaps without interfering with licensed or primary users (PUs). Fig.1 shows a typical cognitive cycle.

---

* Corresponding author: Elizabeth Atieno Otieno

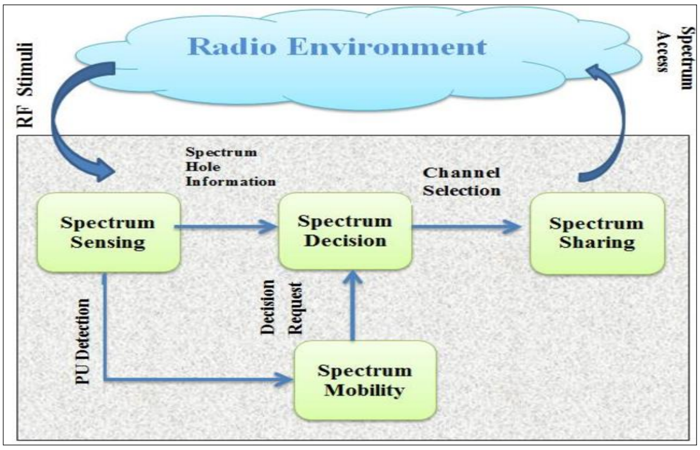

Figure 1 Typical cognitive cycle

CRNs operate based on the cognitive cycle [5], which involves three key functions: spectrum sensing, spectrum management, and spectrum sharing. Spectrum sensing [6] allows CR devices, also known as secondary users (SUs), to detect unused spectrum, while spectrum management facilitates efficient [7] allocation of these resources. Fig.2 shows a Block diagram of cognitive radio.

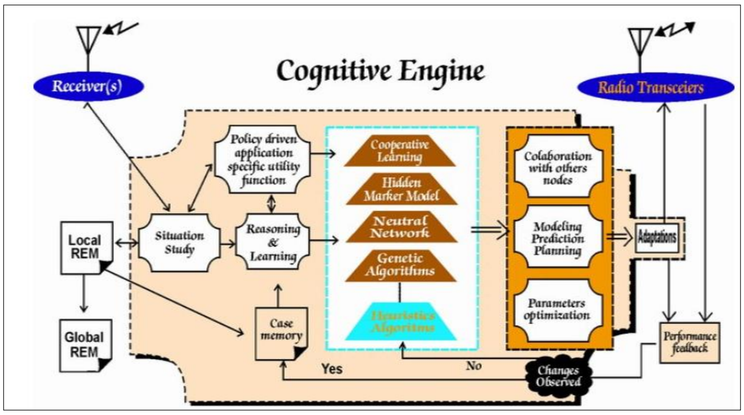

Figure 2 Cognitive radio block diagram

Spectrum sharing ensures that secondary users can coexist harmoniously with primary users without causing harmful interference [8], [9]. These capabilities allow CRNs to achieve a more efficient utilization of spectrum resources and contribute to the overall improvement of wireless communication systems.

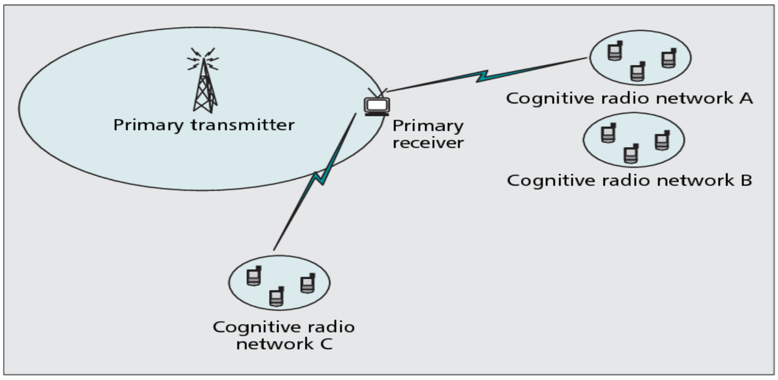

Figure 3 Spectrum sensing

Despite the many advantages of CR technology, its dynamic and opportunistic nature introduces a range of security and privacy challenges [10]-[13]. The openness and flexibility of CRNs make them susceptible to various types of attacks, which could severely impact the integrity, availability, and confidentiality of communications [14]. Adversaries can exploit the inherent characteristics of cognitive radio systems to launch attacks that compromise both the security and privacy of users. Fig.3 gives a depiction of a typical spectrum sensing in CRNs.

One of the primary security concerns in CRNs is the spectrum sensing data falsification (SSDF) attack [15], where malicious users intentionally report false spectrum sensing results to mislead the network about the availability of spectrum. This can lead to suboptimal spectrum allocation, degrade the overall network performance, and even cause disruptions for legitimate primary users [16]. Additionally, primary user emulation (PUE) attacks [17] pose another critical threat, in which attackers mimic the behavior of primary users to monopolize spectrum resources [18] or disrupt communication between secondary users, as shown in Fig. 4. Denial-of-service (DoS) attacks are also prevalent in CRNs [19], where malicious users attempt to overwhelm the network by jamming or otherwise disrupting spectrum sensing or access processes.

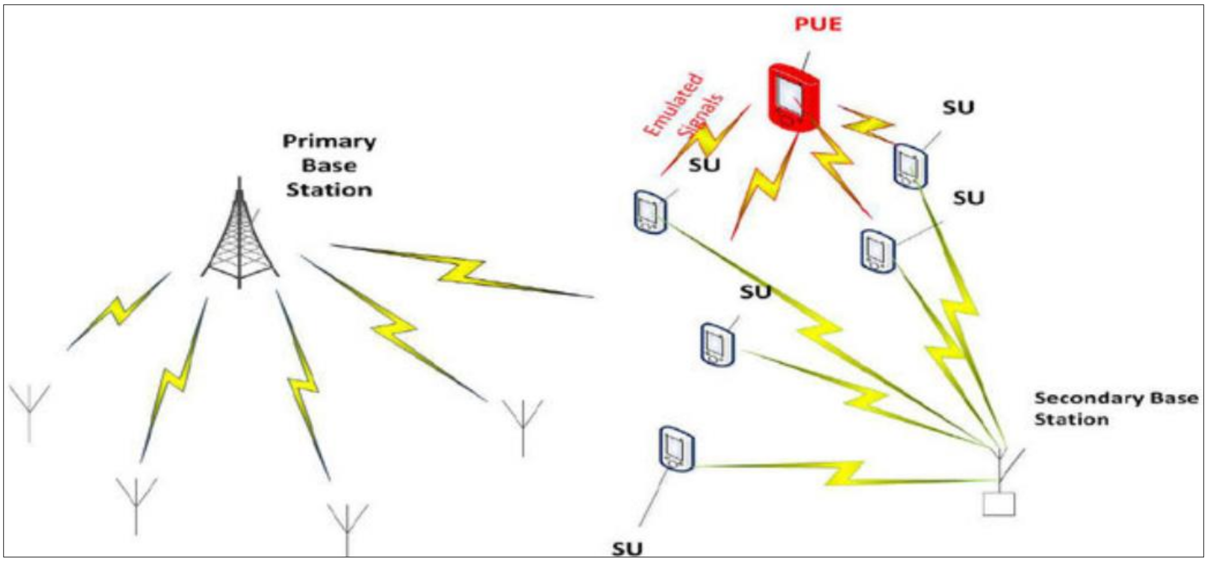

Figure 4 Primary user emulation attack

Privacy issues in CRNs are equally significant. Due to the need for frequent and real-time sharing of information such as spectrum usage patterns, location, and identity data, cognitive radio systems are vulnerable to privacy breaches [20]-[23]. The ability of attackers to infer sensitive information from spectrum sensing activities or communication patterns can expose users to privacy risks [24]. For example, an adversary could monitor spectrum usage to track the location of a CR device or identify a user's communication habits, leading to potential identity theft or targeted attacks.

In this context, ensuring robust security and privacy protection mechanisms in CRNs is essential for their widespread adoption and effective operation [25], [26[. Addressing these concerns requires a multifaceted approach, combining cryptographic methods, trust management schemes, and intrusion detection systems (IDS) to mitigate potential risks [27]. Security mechanisms need to safeguard the integrity and authenticity of spectrum sensing data, protect primary and secondary users from emulation attacks, and ensure the availability of communication channels in the presence of adversarial behavior [28]-[30].

In terms of privacy, techniques such as privacy-preserving spectrum sensing, anonymization of user identity, and secure location-based services can help protect user data while maintaining the functional requirements of cognitive radio networks [31]-[35]. However, implementing these solutions comes with challenges, including balancing the trade-offs between security, privacy, and system performance [36]. Therefore, this paper aims to provide an in-depth exploration of the security and privacy issues in CRNs, highlighting key vulnerabilities, attack vectors, and potential mitigation strategies. The paper also discusses existing frameworks and propose future research directions that could enhance the security and privacy of cognitive radio systems. By addressing these challenges, this work paves the way for the development of resilient, secure, and privacy-preserving cognitive radio networks that can efficiently meet the growing demands of wireless communication.

1.1. Motivation

The advent of CRNs represents a transformative shift in wireless communication, promising unprecedented levels of spectrum efficiency and adaptability. By allowing dynamic spectrum access and enabling radios to intelligently adapt to changing network conditions, CRNs have the potential to address the growing demand for wireless communication and alleviate spectrum scarcity. However, this technological advancement brings with it a host of security and privacy challenges that need to be thoroughly addressed.

Growing demand for spectrum and communication flexibility: The exponential growth in wireless communication devices and services has led to an increased demand for spectrum resources [37], [38]. Traditional static spectrum allocation methods are becoming insufficient to meet this demand. CRNs offer a solution by enabling more efficient and flexible spectrum usage. This capability not only maximizes the utilization of available spectrum but also facilitates the deployment of new applications and services. However, the very flexibility that makes CRNs attractive also introduces significant security and privacy concerns [39] that must be addressed to ensure the reliable and safe operation of these networks.

Complexity of dynamic spectrum access: CRNs operate in a highly dynamic environment where spectrum availability can change rapidly [40], [41]. Cognitive radios must make real-time decisions about spectrum access and usage based on constantly evolving conditions. This dynamic nature creates opportunities for sophisticated attacks, such as spectrum sensing data falsification (SSDF) and primary user emulation (PUE) [42]. These attacks can undermine the integrity of spectrum access and disrupt communication services. Understanding and mitigating these security threats is crucial to maintaining the functionality and trustworthiness of CRNs.

Privacy concerns in cooperative spectrum sensing: Cooperative spectrum sensing, a key feature of CRNs, involves multiple radios sharing their sensing data [43] to improve spectrum detection accuracy. While this cooperation enhances network performance, it also raises significant privacy concerns [44]. Users must share sensitive information about their spectrum usage patterns and, potentially, their location and behavior [45]. Protecting this sensitive information from unauthorized access and ensuring user privacy is essential to fostering trust and encouraging participation in cooperative sensing activities.

Evolving threat landscape: The security and privacy landscape in CRNs is continually evolving, with new threats and attack vectors emerging as technology advances [46]-[48]. For instance, the rise of machine learning and artificial intelligence [49] introduces new types of attacks that can exploit vulnerabilities in CRN protocols. Similarly, the potential future impact of quantum computing on cryptographic security presents an additional layer of concern [50]. Addressing these evolving threats requires ongoing research and adaptation of security and privacy measures to stay ahead of potential adversaries.

Need for robust and scalable solutions: Current security and privacy solutions for CRNs often face challenges related to scalability and efficiency [51]. As CRNs grow in size and complexity, it becomes increasingly important to develop solutions that can handle large-scale networks without compromising performance. Lightweight cryptographic protocols, scalable trust management systems, and efficient privacy-preserving techniques are essential to ensuring that security and privacy measures are effective and practical for deployment in real-world CRNs [52]-[55].

Therefore, the motivation for this paper stems from the critical need to address the security and privacy challenges associated with the deployment and operation of Cognitive Radio Networks. As CRNs continue to evolve and become integral to modern wireless communication infrastructure, ensuring their security and privacy is paramount to their success and widespread adoption. This paper seeks to advance the understanding of these issues and provide actionable insights to help secure and protect CRNs in the face of emerging threats and evolving technological landscapes.

1.2. Main Contributions

This paper presents a comprehensive exploration of security and privacy issues in CRNs, offering valuable insights into the challenges and solutions associated with securing these dynamic and flexible communication systems. The primary contributions of this paper are as follows:

Detailed analysis of security and privacy challenges: This paper provides an in-depth examination of the unique security and privacy challenges faced by CRNs. It identifies and elaborates on key issues, including spectrum access security, cooperative spectrum sensing vulnerabilities, and the protection of user identity and location data. The discussion highlights the complexities introduced by the decentralized and adaptive nature of CRNs, offering a nuanced understanding of the threats and risks involved.

Overview of existing security and privacy frameworks: The paper systematically reviews existing frameworks and solutions designed to address security and privacy concerns in CRNs. It covers various approaches, including cryptographic methods, trust management systems, and privacy-preserving techniques. By presenting the strengths and limitations of these frameworks, the paper provides a comprehensive overview of current practices and their applicability to CRNs.

Identification of open research challenges: This work identifies several open research challenges in the realm of CRN security and privacy. It addresses issues such as dynamic spectrum management, privacy in cooperative spectrum sensing, and trust management in decentralized environments. Additionally, the paper highlights emerging threats, including machine learning-based attacks and quantum computing, and emphasizes the need for ongoing research to develop effective solutions.

Proposed directions for future research: The paper outlines potential directions for future research to advance the state of security and privacy in CRNs. It suggests areas for further investigation, including the development of adaptive and scalable solutions, the enhancement of lightweight cryptographic protocols, and the exploration of novel privacy-preserving techniques. These proposed research directions aim to address the current limitations and challenges identified in the paper.

The remainder of this paper is organized as follows: section 2 describes the basic building blocks of CRNs while Section 3 discusses the security challenges in CRNs, detailing the various attack types and their potential impact. Section 4 explores privacy concerns and the associated risks in cognitive radio systems. Section 5 reviews existing security and privacy frameworks and countermeasures. Section 6 highlights open research challenges, and Section 7 concludes the paper with a discussion on the future of secure and privacy-preserving CRNs.

2. Cognitive Radio building blocks

The basic building blocks of Cognitive Radio (CR) enable the technology's ability to sense the radio environment, make decisions based on the sensed data, and adapt dynamically to changing conditions. The architecture of a conventional cognitive radio network is shown in Fig.5.

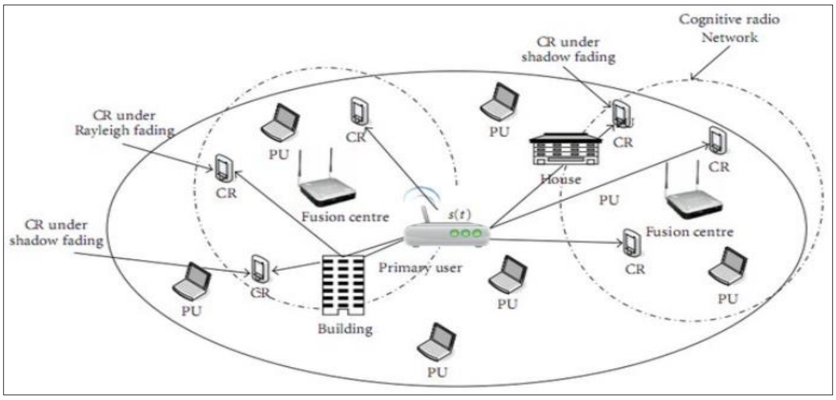

Figure 5 Cognitive radio network architecture

These building blocks work together to create a system capable of optimizing spectrum usage without interfering with licensed or primary users. The key building blocks of cognitive radio are:

2.1. Radio Environment Sensing (Spectrum Sensing)

Spectrum sensing is one of the most crucial components of cognitive radio, enabling it to monitor and assess the surrounding radio environment [56]. The goal of spectrum sensing is to detect unused portions of the spectrum (known as spectrum holes or white spaces) that can be exploited by secondary users without interfering with primary users [57]. The spectrum sensing techniques include:

Energy detection: The most common method, where the CR measures the energy in a frequency band and compares it to a threshold to determine the presence of a signal [58].

Matched filtering: A technique requiring prior knowledge of the primary user's signal [59]. It correlates the received signal with a known signal to detect the presence of the primary user with high accuracy.

Cyclostationary feature detection: This technique exploits the periodic features of modulated signals to detect the presence of a primary user [60], even in low signal-to-noise ratio conditions.

Cooperative sensing: Involves multiple cognitive radios collaborating to improve detection accuracy by sharing their sensing information [61].

2.2. Spectrum decision-making and analysis

Once spectrum holes are identified, the CR must decide whether and how to access them. Spectrum decision-making involves selecting the most appropriate frequency band, modulation scheme, and transmission power based on the characteristics of the available spectrum and the needs of the secondary user [62]-[64]. Fig. 6 gives an illustration of Spectrum Decision-Making in CRNs.

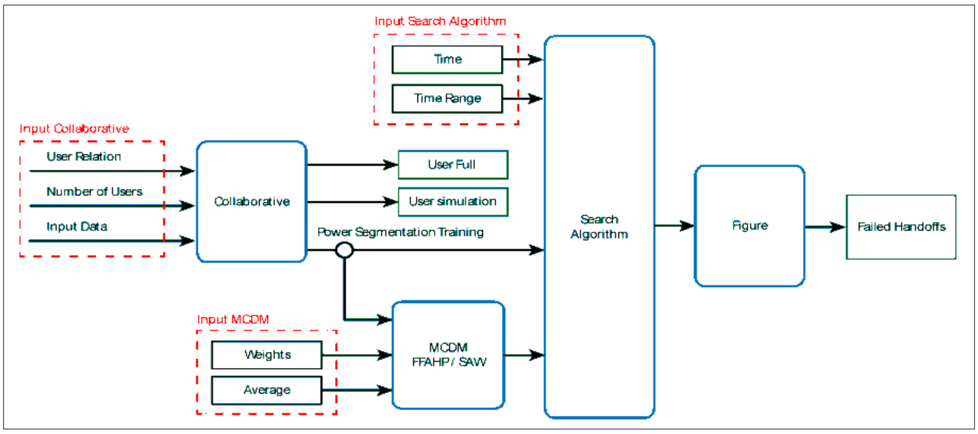

Figure 6 Spectrum Decision-Making in Collaborative Cognitive Radio

This block uses information from spectrum sensing to:

- Evaluate the quality of available spectrum in terms of signal strength, noise levels, and interference.
- Predict future spectrum availability based on historical patterns or real-time environmental changes.

Choose the most appropriate spectrum band for communication to meet the secondary user's quality-of-service (QoS) requirements, while avoiding interference with primary users.

2.3. Spectrum sharing

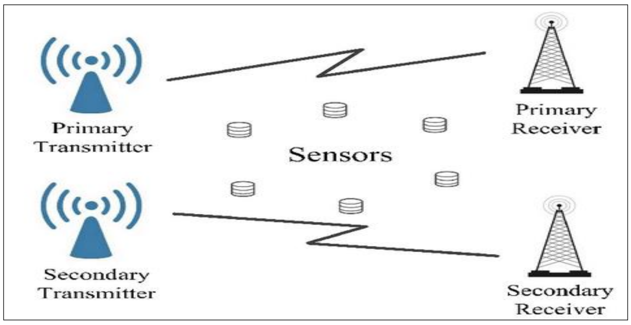

Figure 7 Cognitive radio Spectrum sharing

Spectrum sharing ensures that cognitive radios can coexist with both primary users and other secondary users without causing harmful interference [65], [66]. Fig. 7 gives an illustration of spectrum sharing in CRNs. It is essential to manage the efficient allocation and sharing of spectrum resources among multiple users, especially when multiple secondary users attempt to access the same spectrum band. The main functions of spectrum sharing include:

Dynamic Spectrum Access (DSA): Allows secondary users to opportunistically access spectrum holes as long as they do not interfere with primary users [67].

Interference management: Prevents harmful interference by coordinating access [68] among secondary users and ensuring that communication activities do not disrupt primary users [69].

Resource allocation: Distributes available spectrum among multiple secondary users based on demand, priority, or fairness criteria [70].

The Two major spectrum sharing models are:

Centralized spectrum sharing: Managed by a central authority or base station that allocates spectrum to secondary users based on sensing results and coordination rules [71].

Distributed spectrum sharing: Cognitive radios self-organize and negotiate access to spectrum without centralized control [72], using protocols like game theory or auction-based mechanisms.

2.4. Spectrum Mobility (Handover)

Spectrum mobility, or spectrum handover, is the process by which a cognitive radio moves from one frequency band to another [73]. This is necessary when a primary user becomes active on a previously unused band, requiring the secondary user to vacate the spectrum and switch to an available channel [74], as shown in Fig.8.

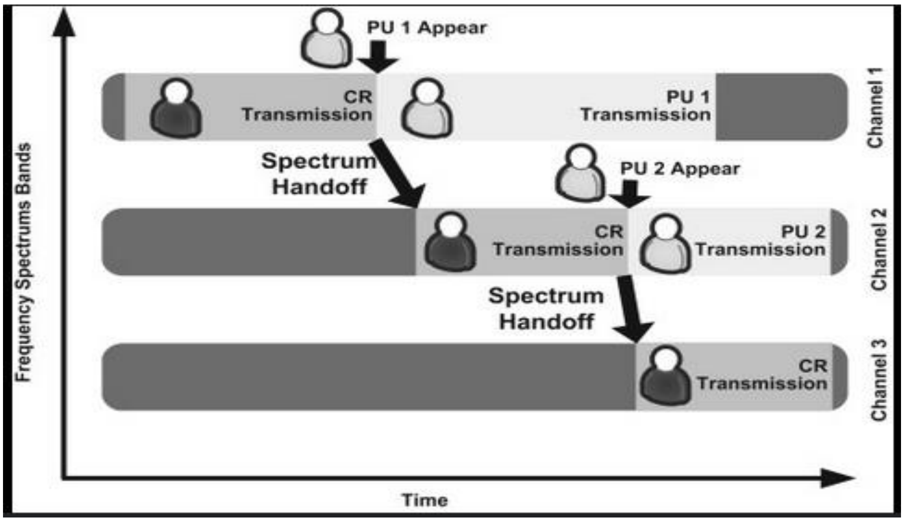

Figure 8 Spectrum handoff in cognitive radio networks

Spectrum mobility ensures that communication continues seamlessly despite the dynamic nature of spectrum usage. The challenges in spectrum mobility include:

Fast detection of primary user activity: Cognitive radios must quickly detect when a primary user reclaims the spectrum to minimize interference [75].

Seamless handover: The handover process must be smooth to avoid disruptions or degradation in communication quality during spectrum transitions [76].

2.5. Cognitive Engine (Learning and Reasoning)

The cognitive engine is the intelligence behind cognitive radio. It is responsible for learning, reasoning, and decision-making, enabling the system to adapt dynamically to changes in the environment [77], [78]. Fig.9 shows an illustration of the cognitive engine architecture. The cognitive engine leverages machine learning and artificial intelligence (AI) techniques [79] to optimize its performance over time by learning from past experiences and making predictions about future spectrum conditions. The key functions of the cognitive engine include:

Learning: The engine can learn from historical data, such as spectrum usage patterns, environmental changes, and primary user behavior, to make informed decisions [80]. Learning techniques include supervised, unsupervised, and reinforcement learning.

Reasoning: The cognitive radio applies decision-making algorithms to determine how to act based on the current spectrum environment and its objectives [81], such as maximizing throughput or minimizing interference.

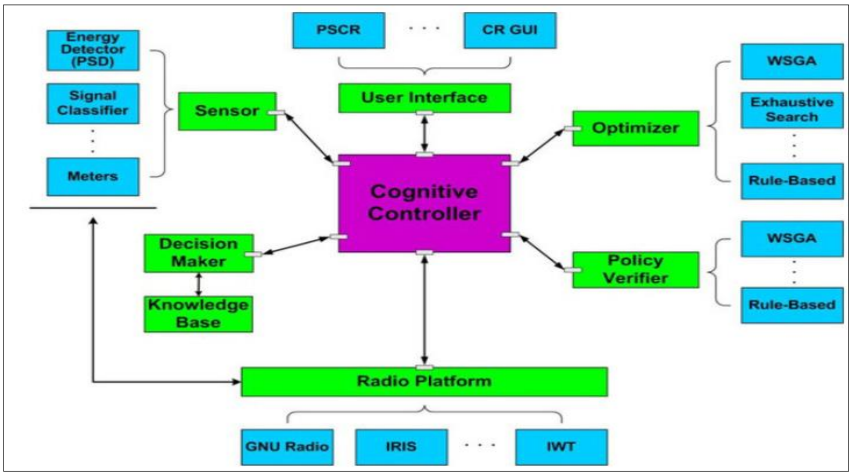

Figure 9 Cognitive engine architecture

Adaptation: The cognitive engine dynamically adjusts transmission parameters (frequency, power, modulation) based on the sensed environment and current system goals, ensuring optimal communication [82].

2.6. Radio Frequency (RF) front-end

The RF front-end is the hardware component responsible for transmitting and receiving signals across multiple frequency bands [83], as shown in Fig.10. Since cognitive radios must operate over a wide range of frequencies, the RF front-end must be flexible and capable of tuning to various frequencies dynamically [84]. The RF front-end includes:

Antenna: A wideband or tunable antenna that can operate across a broad spectrum range.

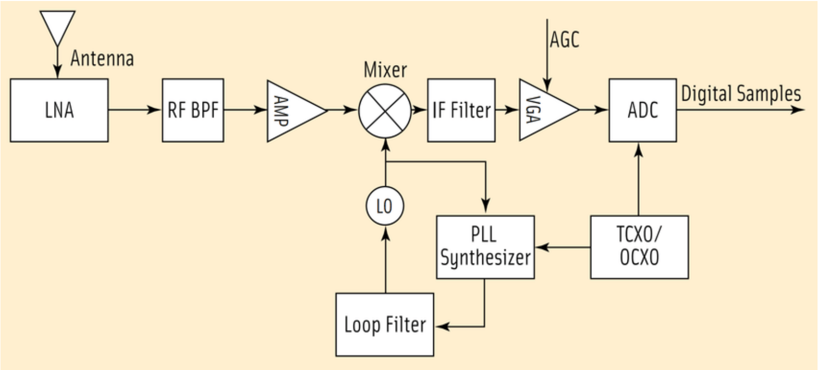

Figure 10 GPS receiver radio frequency front-end

Mixer: Converts incoming signals from RF to baseband and outgoing signals from baseband to RF for transmission.

Amplifier: Enhances weak signals received from the antenna for further processing.

Analog-to-Digital Converter (ADC): Converts analog RF signals into digital format for processing by the cognitive engine.

Digital-to-Analog Converter (DAC): Converts digital signals back into analog format for transmission over the airwaves.

2.7. Policy engine

The policy engine ensures that the cognitive radio adheres to regulatory constraints and operational policies [85]. Cognitive radios operate in environments regulated by spectrum authorities, which impose rules on how spectrum can be accessed and used. The policy engine ensures compliance with these rules, preventing unauthorized spectrum access [86] and ensuring legal operation. The functions of the policy engine include:

Regulatory compliance: Ensures that cognitive radios follow spectrum usage policies set by regulatory bodies [87], such as avoiding interference with licensed users and complying with power limits.

Operational policies: Defines how the cognitive radio should behave under various conditions [88], such as prioritizing emergency communication or adhering to organizational policies for spectrum access.

2.8. Security and privacy modules

Cognitive radios must have robust security mechanisms to prevent attacks that exploit the dynamic nature of spectrum access [89]-[92]. Security and privacy modules are responsible for protecting against malicious behavior such as:

Primary User Emulation (PUE) attacks: Where a malicious user pretends to be a licensed user [93], preventing legitimate secondary users from accessing the spectrum.

Spectrum Sensing Data Falsification (SSDF): Where attackers provide false sensing data to manipulate the network's spectrum decisions [94].

Privacy breaches: Protection of sensitive information like user identity and location, which may be exposed through spectrum usage patterns [95].

These basic building blocks work together to provide a dynamic and intelligent system capable of optimizing spectrum usage. The integration of spectrum sensing, decision-making, sharing, mobility, and learning functions allows cognitive radios to make real-time adjustments and maximize communication performance. However, as CR technology advances, it is essential to address associated challenges, particularly in the areas of security, privacy, and regulatory compliance. These building blocks form the foundation for the development and deployment of efficient, resilient, and secure cognitive radio networks.

3. Security challenges in CRNs

The CRNs represent a transformative approach to wireless communication by dynamically accessing underutilized spectrum. However, the flexibility and adaptability that make CRNs so powerful also introduce significant security challenges [96], [97]. The openness of CRNs, their reliance on cooperative behavior, and the dynamic nature of spectrum access make them vulnerable to a variety of security threats [98]. The security challenges in CRNs span across different layers of the network, impacting spectrum sensing, data transmission, spectrum sharing, and user privacy.

This section provides an extensive discussion of the security challenges in CRNs, focusing on key vulnerabilities, attack vectors, and the need for effective security mechanisms.

3.1. Primary User Emulation (PUE) attacks

One of the most significant threats in CRNs is the PUE attack, where a malicious secondary user mimics the behavior of a primary user to occupy or monopolize spectrum resources [99], [100]. A typical primary user emulation is illustrated in Fig.11. In CRNs, secondary users are required to vacate the spectrum whenever a primary user becomes active. Attackers can exploit this rule by pretending to be a primary user, thereby forcing legitimate secondary users off the spectrum [101].

By faking the presence of a primary user, the attacker forces secondary users to vacate the spectrum, allowing the attacker to monopolize the band for their own transmissions. This not only disrupts the efficient use of the spectrum but also undermines the core functionality of cognitive radio, which relies on accurate spectrum sensing to avoid interference with legitimate primary users. Detecting and mitigating PUE attacks is critical for maintaining secure and efficient spectrum usage in cognitive radio networks.

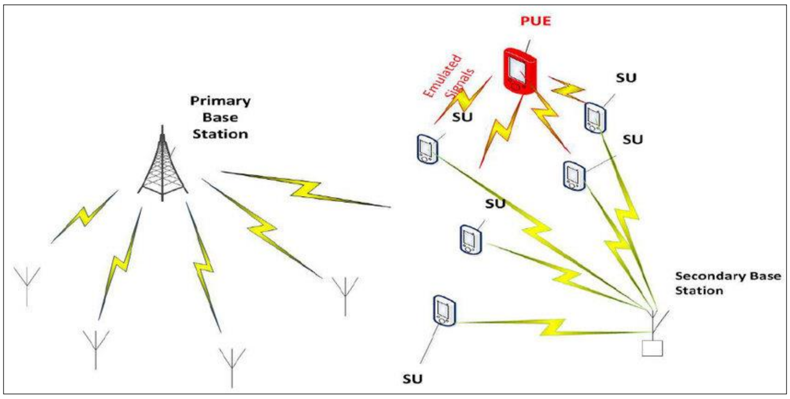

Figure 11 PUE attack model

Attack mechanism: The attacker transmits signals that resemble the transmission characteristics of a primary user. Upon detecting these signals, legitimate secondary users vacate the spectrum, assuming the presence of a primary user [102], [103]. The attacker either monopolizes the spectrum for its own use or causes a denial-of-service (DoS) [104] for legitimate secondary users by blocking their access to available spectrum. The impacts of these attacks include the following:

Denial-of-spectrum attack: Legitimate secondary users are prevented from accessing available spectrum [105], degrading the overall efficiency of the CRN.

Interference: If the attacker mimics the primary user's signal characteristics incorrectly, this may cause harmful interference to actual primary users [106], as shown in Fig.12.

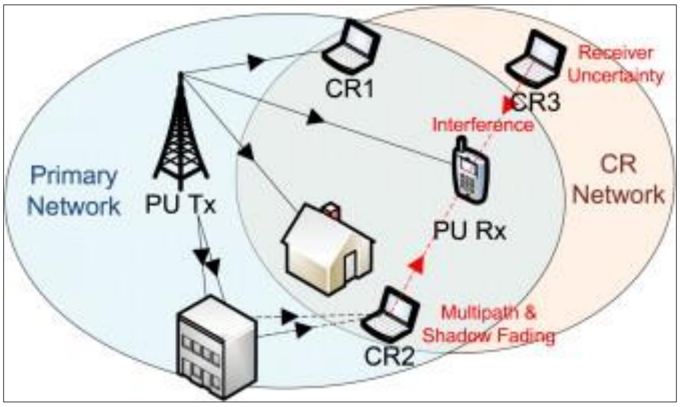

Figure 12 Interference in CRNs

Cognitive radios are designed to intelligently detect and utilize underused frequency bands, adjusting their transmission parameters to avoid causing interference to primary users (licensed users of the spectrum). However, interference can still occur if the cognitive radio inaccurately senses the spectrum or if multiple cognitive radios compete for the same band, leading to a clash in signal transmission. Effective interference management, through techniques like dynamic spectrum access and cooperative spectrum sensing, is crucial to optimizing cognitive radio performance.

3.2. Spectrum Sensing Data Falsification (SSDF) Attacks

Spectrum Sensing Data Falsification (SSDF) or data manipulation attacks are a class of security threats where malicious users deliberately falsify their spectrum sensing reports [107]-[109]. A conventional spectrum sensing data falsification attack is depicted in Fig.13. CRNs often rely on cooperative spectrum sensing, where multiple secondary users collaborate to make more accurate spectrum access decisions.

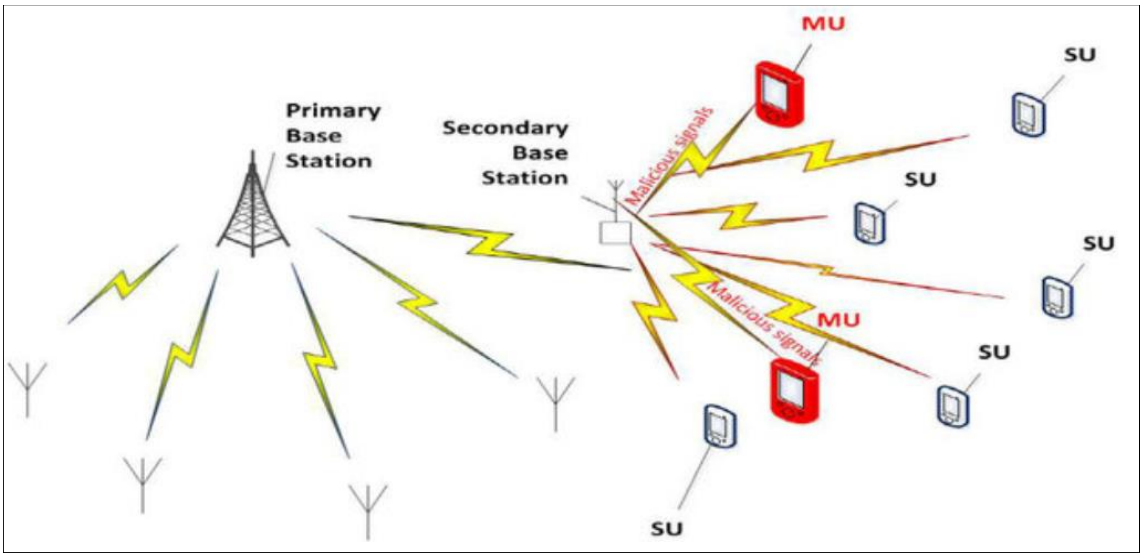

Figure 13 Spectrum sensing data falsification attack

In an SSDF attack, adversaries manipulate sensing data [110] to deceive the network, causing inefficiencies in spectrum allocation.

Attack mechanism: Malicious users submit falsified sensing data to either report spectrum as occupied when it is not or report it as free when it is occupied [111], [112]. In cooperative sensing, the false data skews the aggregated sensing results, leading to poor spectrum decisions by the network. The effects of these attacks can include the following:

False vacating: Legitimate secondary users vacate the spectrum unnecessarily [113], reducing the network's efficiency.

Interference: Secondary users may be encouraged to transmit on a frequency band already occupied by a primary user [114], causing interference.

DoS attacks: Attackers can cause widespread denial of service by influencing the network to make incorrect spectrum allocation decisions [115], [116].

3.3. Denial-of-Service (DoS) attacks

CRNs are vulnerable to various forms of DoS attacks, which can disrupt the normal operation of the network by overwhelming it with excessive traffic or by blocking access to the spectrum [117], [118]. DoS attacks are particularly concerning in CRNs because the dynamic nature of spectrum access makes it challenging to maintain continuous communication under attack conditions.

Attack mechanism: Attackers can launch DoS attacks by jamming the spectrum sensing process [119], flooding the network with false requests, or monopolizing spectrum resources through PUE attacks or SSDF attacks. Jamming can be performed by injecting noise signals into the spectrum to prevent legitimate users from detecting the availability of free spectrum or by disrupting the communication between secondary users [120], [121]. The probable repercussions of these attacks include:

Spectrum unavailability: Legitimate users are prevented from accessing available spectrum resources, leading to reduced network throughput and increased latency [122], [123].

Network congestion: The network's resources, such as bandwidth and processing power, are consumed by the attack [124], reducing its ability to serve legitimate users.

3.4. Eavesdropping and privacy breaches

CRNs often require frequent and real-time sharing of information, such as spectrum usage patterns, location data, and communication details, between users and network controllers [125]-[127]. This creates opportunities for eavesdropping and privacy breaches [128] as shown in Fig.14. Here, where attackers can intercept communication or infer sensitive information from the shared data.

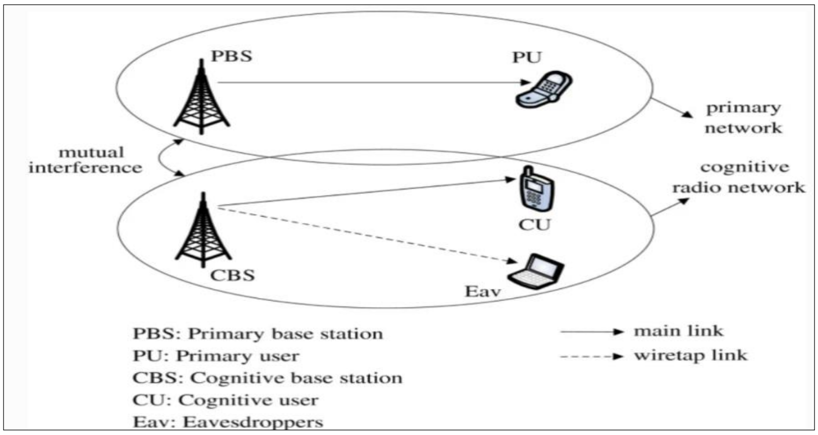

Figure 14 Eavesdropping in CRNs

Attack mechanism: Attackers passively monitor the communication between CR devices to gather information about user identity, location, and behavior [129]. The attacker may also analyze spectrum usage data to infer patterns of communication or to track the movements of a user over time. The impacts of these security challenges may include the following:

Privacy invasion: Attackers can gain access to personal or sensitive information about users [130], leading to potential identity theft, unauthorized surveillance, or location tracking.

Traffic analysis: Even if the communication is encrypted, attackers can perform traffic analysis to infer details about the users' communication patterns or the type of communication being carried out [131].

3.5 Jamming attacks

Jamming attacks involve the deliberate interference with the radio signals in CRNs [132], disrupting communication by overwhelming the network with noise or unwanted signals. As shown in Fig.15, these attacks can target either the spectrum sensing process or the data transmission phase.

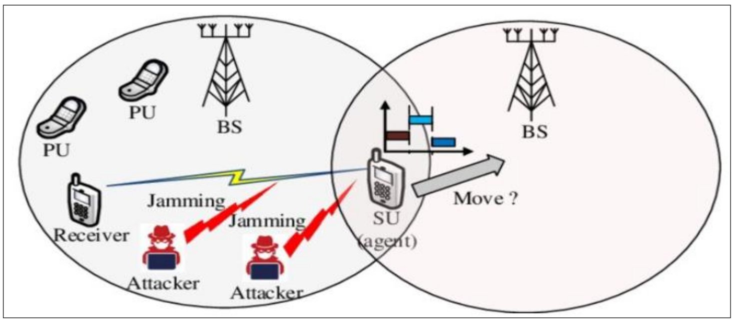

Figure 15 Jamming attacks in CRNs

Attack mechanism: Attackers transmit high-power noise signals or signals similar to the primary user's signal to disrupt the ability of secondary users to sense the spectrum accurately or to communicate effectively [133]. Jamming can be done selectively (targeting specific frequencies) or randomly (across a wide range of frequencies). The possible effects may encompass:

Spectrum sensing disruption: Jamming during the sensing phase can prevent secondary users from detecting spectrum availability, leading to inefficient spectrum usage [134] or missed communication opportunities.

Communication disruption: Jamming during data transmission can result in dropped packets, reduced throughput, and increased latency [135], [136].

3.5. Malicious selfish behavior

CRNs rely on cooperative behavior, particularly during spectrum sensing and sharing processes [137], [138]. However, selfish users may act maliciously by misreporting spectrum sensing data or monopolizing spectrum resources to improve their own performance at the expense of others, as shown in Fig.16 below.

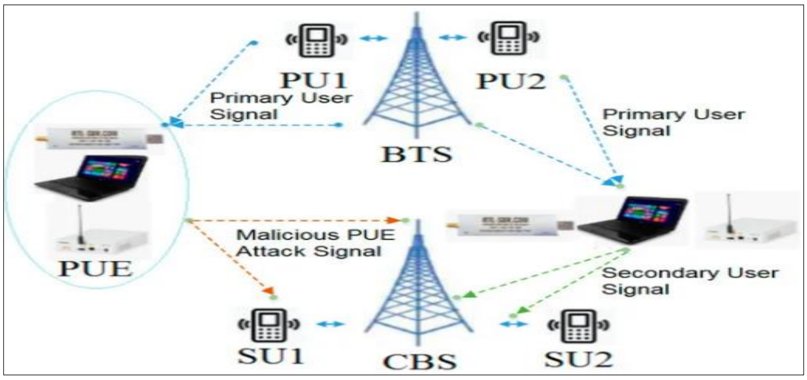

Figure 16 Malicious selfish behavior in CRNs

Attack mechanism: Selfish users may underreport or overreport their spectrum sensing results, making it more difficult for other users to access available spectrum [139]. They may also refuse to vacate the spectrum when a primary user becomes active or delay the vacating process to maximize their own spectrum usage. The impacts include the following:

Reduced network efficiency: Selfish behavior disrupts the fairness of spectrum allocation, leading to inefficient use of resources [140].

QoS degradation: Legitimate users may experience reduced quality of service due to the selfish actions of malicious users [141]. Table 1 presents some of the mitigation strategies for each of these security challenges.

Table 1 CRNs security mitigation strategies

Security challenges	**Mitigation challenges**
PUE Attacks	*Cryptographic authentication*: Involves verification of the identity of the primary user through cryptographic techniques can prevent unauthorized users from emulating primary users [142]. *Signal characteristics analysis*: concerned with differentiating between legitimate and fake primary users by analyzing the physical-layer properties of the signal (e.g., location, signal strength, or modulation features) [143]. *Location verification*: involves the verification of the location of the user transmitting the primary user's signal and cross-referencing it with known primary user locations [144].
SSDF Attacks	*Trust-based Systems*: Assigning trust values to users based on their past behavior allows the system to weigh sensing data from reliable users more heavily than from potentially malicious users [145]. *Outlier detection*: Statistical techniques can be used to detect and discard abnormal sensing data [146] that deviates significantly from the expected pattern. *Secure cooperative sensing protocols*: Implementing cryptographic mechanisms to ensure the authenticity and integrity of sensing data before it is shared or aggregated [147].
DoS Attacks	*Spread spectrum techniques*: Spread spectrum and frequency hopping can reduce the effectiveness of jamming attacks [148] by making it harder for the attacker to predict the spectrum band being used by legitimate users.

	Rate limiting: Limiting the rate at which users can send requests for spectrum access helps mitigate flooding-based DoS attacks [149]. *Detection and reaction systems*: Implementing real-time monitoring systems to detect unusual traffic patterns or jamming signals allows the network to react by reallocating resources or switching to more secure communication channels [150].
Eavesdropping and Privacy leaks	*Encryption*: Using strong encryption techniques ensures that even if attackers intercept the communication, they cannot understand the content of the messages [151], [152]. *Anonymous spectrum sensing*: Techniques that allow users to participate in spectrum sensing without revealing their identity can help protect user privacy [153]. *Obfuscation techniques*: Introducing randomness or noise into the data being shared (e.g., through dummy traffic or location obfuscation) [154] can make it harder for attackers to infer useful information from eavesdropped data.
Jamming Attacks	*Adaptive frequency hopping*: CR devices can hop between different frequency bands when jamming is detected [155], reducing the impact of the attack. *Spread spectrum techniques*: Techniques like frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS) can make it difficult for attackers to jam the entire communication range effectively [156]. *Jamming detection systems*: Real-time monitoring of the spectrum for unusual interference patterns can help detect jamming attacks early [157], allowing the network to respond by switching channels or adjusting transmission parameters.
Malicious Selfish Behavior	*Reputation and trust systems*: Building a reputation system that tracks user behavior over time can help penalize selfish users by reducing their spectrum access priority or trust levels [158]. *Incentive-based mechanisms*: Designing incentive mechanisms to reward cooperative behavior and penalize selfish actions encourages users to act in the network's best interest [159].

It is important to note that security challenges in CRNs arise due to the network's open and dynamic nature [160], the reliance on cooperative sensing, and the complexity of managing spectrum access in real-time.

4. Privacy concerns in CRNs

CRNs bring transformative advancements in wireless communication through their ability to dynamically access underutilized spectrum. However, while CRNs offer numerous benefits like enhanced spectrum efficiency and adaptive network management [161], they also introduce significant privacy concerns. These challenges primarily stem from the frequent exchange of sensitive information (such as spectrum usage patterns, user location, and network behavior) that is necessary for the functioning of the CRN [162]. The dynamic, distributed nature of these networks opens multiple avenues for privacy breaches, making it essential to address privacy issues comprehensively.

This section provides an extensive discussion of the privacy challenges in CRNs, examining how various elements of the network can expose users to privacy risks and what countermeasures can be implemented to protect user data.

4.1. User location privacy

One of the most significant privacy concerns in CRNs is the protection of user location information. CRNs often rely on location-aware services and spectrum sensing [163], where the geographical location of users plays a critical role in determining spectrum availability and access priority. Attackers can exploit this feature to track the physical movement of users, leading to serious privacy violations. The attack mechanisms include:

Traffic analysis: By observing spectrum access patterns and signal propagation characteristics, an attacker can infer the location of CR devices [164], [165]. This can be done even if the actual communication is encrypted, as the radio signal's physical properties can give away location-related information.

Location disclosure: In cooperative spectrum sensing, users may be required to share their location information with nearby users or base stations. Malicious users or adversaries can intercept this data [166], either directly from the communication or by analyzing the metadata associated with the sensing reports.

The impacts of user location privacy can be:

Tracking: Continuous tracking of a user's location can enable adversaries to create detailed movement profiles [167], which can be used for surveillance, stalking, or other malicious purposes.

Geographical targeting: Attackers can target users in specific geographic locations for location-based attacks, such as injecting malicious information or launching denial-of-service (DoS) attacks [168] aimed at users in a particular area.

Personal security risks: Location privacy breaches can also pose physical security risks, as users' movements and patterns become exposed to malicious actors [169].

4.2. Identity privacy

Identity privacy in CRNs refers to the protection of users' identities during spectrum sensing, sharing, and communication processes [170]. Given the cooperative and often decentralized nature of CRNs, users frequently exchange information with other users, base stations, or access points. If proper privacy measures are not in place, this can lead to the exposure of users' identities, making them susceptible to targeted attacks or tracking [171]. The attack techniques include the following:

User profiling: By continuously monitoring the network activities of a particular user, attackers can link various communication sessions to a specific user [172], revealing their identity. Even if the communication content is encrypted, side-channel information such as transmission timing, frequency, and power can be used for profiling [173].

Packet sniffing: Adversaries can intercept data packets in the network and attempt to link them to a particular user [174] by analyzing metadata (e.g., IP addresses or unique device identifiers).

Cooperative sensing exploitation: In cooperative spectrum sensing, where multiple users collaborate to detect available spectrum, attackers can analyze the sensing reports to identify specific users based on the unique characteristics of their transmissions or by correlating reports over time [175].

The repercussions of Identity privacy include:

Targeted attacks: Once a user's identity is known, adversaries can launch targeted attacks, such as DoS or jamming attacks [176], aimed specifically at disrupting that user's communication.

Data correlation: By linking different communication sessions to the same user, attackers can build comprehensive profiles that include not only the user's identity but also their communication habits, location, and preferences [177], [178].

Impersonation attacks: If attackers can uncover a user's identity, they may attempt to impersonate the user in future communication sessions [179], leading to spoofing attacks or unauthorized access to network resources.

4.3. Spectrum usage pattern privacy

In CRNs, users' spectrum usage patterns—such as the frequency bands they use, the times they access the spectrum, and the duration of their transmissions—can reveal sensitive information about their behavior, preferences, and even the content of their communication [180], [181]. Attackers can exploit this information to infer details about a user's activities or to predict future communication patterns, leading to potential privacy breaches [182]. The various attack mechanisms include:

Behavioral profiling: By analyzing spectrum usage over time, attackers can create a profile of a user's communication behavior, identifying regular access patterns (e.g., specific times of day when the user is most active, preferred frequency bands, or transmission power levels) [183], [184].

Traffic inference: Even without accessing the content of communication, an attacker can infer the type of communication (e.g., voice calls, video streaming, or file transfers) based on the spectrum usage patterns [185], such as bandwidth consumption and transmission duration.

Usage prediction: Attackers can predict future spectrum usage by analyzing historical data [186]. This enables preemptive attacks, such as occupying spectrum bands before the user can access them or launching targeted interference during known active periods.

The probable effects of spectrum usage pattern privacy can be:

Privacy invasion: Detailed behavioral profiles built from spectrum usage patterns can reveal private information about users [187], such as their daily routines, work habits, or even the type of communication they engage in (e.g., business vs. personal).

Denial-of-Service (DoS) and jamming attacks: Predicting future spectrum usage allows attackers to launch targeted DoS or jamming attacks at critical times [188], causing disruptions in communication when the user is most reliant on the network.

Security breaches: In critical applications, such as military or governmental communication, revealing spectrum usage patterns could compromise the security of the communication [189], leading to espionage or sabotage.

4.4. Privacy in cooperative sensing and sharing

Cooperative spectrum sensing is a key feature of CRNs, allowing multiple users to collaborate to improve the accuracy of spectrum sensing. However, cooperative sensing introduces significant privacy risks [190], as users are often required to share potentially sensitive information (such as their location, spectrum usage, and sensing results) with other users and the network infrastructure. The various attack techniques:

Sensing data exploitation: In cooperative sensing, attackers can collect and analyze the sensing data shared by users to extract private information [191], such as user location, identity, and communication behavior. Even if the shared data does not contain explicit personal information, it can still be exploited through traffic analysis or correlation attacks.

Collusion attacks: Malicious users may collude to share their sensing data and coordinate their actions to extract more detailed information about other users, potentially violating their privacy [192].

Untrusted third parties: In scenarios where the cooperative sensing data is aggregated and processed by third-party entities (e.g., spectrum brokers or network operators), there is a risk that these entities could misuse the data or fail to adequately protect it from privacy breaches [193].

The possible impacts of privacy in cooperative sensing and sharing include the following:

Privacy leakage: Sensitive information about users’ spectrum usage, location, and communication behavior can be exposed to malicious users [194], untrusted third parties, or even legitimate users who exploit their access to the cooperative sensing data.

Loss of trust: Users may lose trust in the network if they believe that their private information is being improperly accessed or shared [195], leading to reduced participation in cooperative sensing, which in turn affects the overall performance of the CRN.

Vulnerabilities to insider attacks: In cooperative sensing, trusted users can act as insiders who misuse their privileged access to exploit private information for malicious purposes [196], including blackmail, espionage, or unauthorized surveillance. Table 2 gives a summary of some of the mitigation strategies for these privacy challenges.

It is clear that privacy challenges in CRNs are multifaceted and arise from the dynamic, decentralized, and cooperative nature of these networks. User location privacy, identity privacy, spectrum usage pattern privacy, and privacy in cooperative sensing all present significant risks that must be addressed to protect users' sensitive information [212], [213]. As CRNs continue to evolve and become more widely adopted, it is essential to develop robust privacy-preserving mechanisms [214] that can mitigate these challenges without compromising the performance and flexibility of the network. Effective solutions will involve a combination of encryption, anonymization, obfuscation, and trust management techniques to safeguard user privacy in the face of increasingly sophisticated threats.

Table 2 CRNs privacy mitigation strategies

Privacy challenges	**Mitigation challenges**
User location privacy	*Location obfuscation*: Techniques that add noise or modify the accuracy of location information shared with other users or the network [197]. For example, a user could report an approximate or anonymized location, instead of their precise geographical coordinates. *Encryption of location data*: Encrypting location data during transmission to prevent unauthorized access or interception [198]. Only trusted entities should be able to decrypt the actual location. *Dummy location generation*: The introduction of fake or "dummy" location reports can be used to confuse attackers and make it difficult to pinpoint the real location of the user [199].
Identity privacy	*Anonymous spectrum sensing*: Implementing anonymous spectrum sensing protocols that allow users to participate in cooperative sensing without revealing their identities [200]. This can be achieved using cryptographic techniques such as zero-knowledge proofs or anonymous credentials. *Identity obfuscation*: Temporarily changing user identifiers (such as MAC addresses or pseudonyms) during communication can help prevent long-term tracking or profiling by adversaries [201]. *Group-based communication*: Group-based or collaborative spectrum access protocols can help obfuscate individual identities [202] by allowing users to participate in the network as part of an anonymous group, rather than as identifiable individuals.
Spectrum usage pattern privacy	*Randomized spectrum access*: By randomizing the times and frequencies at which users access the spectrum, CRNs can make it more difficult for attackers to analyze and predict usage patterns [203]. Users can periodically switch between different frequency bands and vary their transmission parameters to obfuscate their behavior. *Privacy-preserving traffic analysis*: Implementing privacy-preserving algorithms that add noise or randomness to the reported spectrum usage patterns can reduce the likelihood of successful traffic analysis by adversaries [204]. *Encrypted spectrum sensing reports*: Encrypting spectrum sensing reports and other network metadata can help protect spectrum usage information from being intercepted and analyzed by malicious users [205].
Privacy in cooperative sensing and sharing	*Privacy-preserving sensing protocols*: Implementing privacy-preserving cooperative sensing protocols that allow users to participate in spectrum sensing without revealing sensitive information [206]-[208]. This can be achieved using techniques like homomorphic encryption, differential privacy, or secure multi-party computation. *Data minimization*: Limiting the amount of sensitive information that users are required to share during cooperative sensing [209]. For example, users may share only aggregate or anonymized data [210] rather than detailed sensing reports. *Trust management systems*: Developing trust management frameworks that evaluate the behavior and reputation of users participating in cooperative sensing [211]. These systems can reduce the risk of privacy breaches by ensuring that only trusted users have access to sensitive data.

5. Existing security and privacy frameworks

CRNs introduce complex security and privacy challenges due to their dynamic, decentralized, and flexible nature. To address these concerns, researchers and practitioners have developed various frameworks aimed at safeguarding CRNs against security threats and protecting user privacy. These frameworks provide mechanisms for spectrum management, user authentication, secure communication, and privacy-preserving spectrum sensing. This section presents an extensive discussion of existing security and privacy frameworks for CRNs, focusing on key approaches, techniques, and solutions that have been proposed or implemented in the literature.

5.1. Cryptographic frameworks for secure communication

Cryptography plays a critical role in securing communication in CRNs, providing protection against unauthorized access, data tampering, and identity theft [215], [216]. Given the openness and dynamic nature of spectrum access in CRNs, cryptographic frameworks have been adapted to ensure secure communication, particularly in cooperative spectrum sensing and dynamic spectrum sharing.

5.1.1. Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is a widely adopted framework in CRNs to secure communication between cognitive radio (CR) devices [217]. PKI provides secure key management, digital signatures, and encryption through the use of asymmetric keys [218], [219]. In CRNs, PKI can be used for secure spectrum sensing data exchange, authentication of primary and secondary users and protection of control messages transmitted between CR nodes.

5.1.2. Lightweight cryptographic solutions

Given the limited computational resources of CR devices, lightweight cryptographic frameworks have been developed for CRNs [220]-[222]. These frameworks aim to provide the necessary security while reducing the computational burden on CR devices. The examples include elliptic curve cryptography (ECC) and lightweight symmetric key algorithms (e.g., AES in lightweight mode) [223]. These are designed to be less resource-intensive while maintaining a high level of security.

5.2. Trust-based frameworks

CRNs rely heavily on cooperation among users, especially for spectrum sensing and sharing. However, this opens the door to malicious behavior, such as spectrum sensing data falsification (SSDF) attacks [224], where malicious users provide false information to mislead the network. To address this, trust-based frameworks have been introduced to evaluate and manage user behavior, ensuring that only trusted users influence network decisions [225], [226].

5.2.1. Reputation-based trust models

Reputation-based trust frameworks rely on past behavior to evaluate the trustworthiness of a user [227], [228]. In these models, users are assigned trust scores based on their actions, such as accurate spectrum sensing or adherence to spectrum-sharing rules. In CRNs, users who consistently provide accurate sensing data or follow spectrum-sharing policies receive higher trust scores. Users with low trust scores are either excluded from cooperative sensing or their input is given less weight in decision-making processes. The examples of these models include the following:

Bayesian trust models: These models use probabilistic reasoning to update trust values based on user behavior [229].

Game-theoretic approaches: In game theory-based models, trust is dynamically adjusted based on users' actions over time, rewarding cooperative behavior and penalizing malicious or selfish actions [230].

5.2.2. Subjective logic-based trust models

Subjective logic-based frameworks extend reputation models by incorporating subjective opinions in trust evaluation [231]. These models are useful in scenarios where trust cannot be quantified precisely, and they allow CR devices to form trust relationships based on subjective beliefs about other users' behavior.

5.3. Privacy-preserving frameworks

Privacy is a major concern in CRNs, especially in cooperative spectrum sensing where users share information about their location, behavior, and spectrum usage. To address this, privacy-preserving frameworks [232] have been developed, focusing on protecting user data while enabling the cooperative nature of the network.

5.3.1. Differential privacy

Differential privacy is a statistical technique that provides strong privacy guarantees by introducing noise into the data being shared [233]. In the context of CRNs, differential privacy is applied to protect spectrum sensing reports and usage patterns from revealing sensitive user information [234]. When users participate in cooperative spectrum sensing, they can apply differential privacy to ensure that their individual contributions to the sensing result cannot be inferred, even by an adversary with access to the aggregated data.

5.3.2. Homomorphic encryption

Homomorphic encryption allows computations to be performed on encrypted data without needing to decrypt it first [235]. This property is useful in CRNs for protecting user privacy during spectrum sensing and sharing [236]. In CRNs, users can encrypt their spectrum sensing data and share it with a central entity (e.g., a spectrum broker) that performs computations (such as aggregating the data) on the encrypted values. The results of these computations can then be decrypted by authorized users, without exposing the individual sensing data.

5.3.3. Privacy-Preserving Cooperative Spectrum Sensing (PPCSS)

Privacy-Preserving Cooperative Spectrum Sensing (PPCSS) frameworks are specifically designed to protect user privacy in cooperative spectrum sensing [237]. These frameworks ensure that users can contribute to the sensing process without revealing sensitive information [238], such as their location or spectrum usage patterns. The various techniques in PPCSS include:

Obfuscation: Users can obfuscate their sensing reports by adding noise or masking certain details [239], making it harder for attackers to infer private information.

Secure Multi-Party Computation (SMPC): SMPC allows multiple users to contribute to a joint computation (such as spectrum sensing) without revealing their individual inputs [240]. This ensures that the sensing results are accurate while preserving the privacy of each user's data.

5.4. Game-theoretic security frameworks

Game theory has been extensively applied to CRNs to model and address security and privacy challenges [241]. Game-theoretic frameworks treat security and privacy as strategic interactions between rational users (or attackers) who aim to maximize their utility while adhering to network rules.

5.4.1. Non-cooperative game theory

In non-cooperative game theory, users are treated as independent entities who act selfishly to maximize their own spectrum usage or network utility [242]. Game-theoretic models can be used to detect and mitigate malicious behavior, such as SSDF attacks or PUE attacks [234]. Non-cooperative games are used to model interactions between legitimate users and attackers. By analyzing the payoffs associated with different strategies, the network can identify optimal responses to mitigate the impact of attacks [235]. The examples of these applications include the following:

Jamming games: Non-cooperative games have been used to model jamming attacks, where attackers and legitimate users compete for control of the spectrum [244]. The game identifies optimal strategies for users to avoid jamming and continue communication.

Sensing data manipulation games: Game theory can model how malicious users falsify sensing data [245], allowing the network to develop counter-strategies that minimize the impact of such attacks.

5.4.2. Cooperative game theory

In cooperative game theory, users work together to maximize the overall performance of the CRN, rather than acting selfishly. Cooperative games are useful for modeling trust relationships and encouraging collaborative spectrum sensing [246], [247]. Cooperative game theory can be used to encourage users to share their spectrum resources and participate in cooperative spectrum sensing by offering incentives or rewards for good behavior. Table 3 presents some of strengths and weaknesses of these existing security and privacy frameworks.

Evidently, the existing security and privacy frameworks for CRNs address a wide range of challenges, including secure communication, trust management, privacy preservation, and protection against malicious behavior. Cryptographic techniques, trust-based frameworks, privacy-preserving mechanisms, and game-theoretic models all contribute to securing CRNs in various ways. However, the dynamic and decentralized nature of CRNs requires ongoing research and innovation to develop more efficient and effective solutions. Future frameworks will need to balance security and privacy requirements with the performance constraints of CRNs, particularly in resource-limited environments like mobile or IoT networks.

Table 3 Existing security and privacy frameworks

Framework	Strengths	Weaknesses
Public key infrastructure	PKI provides strong security guarantees, including non-repudiation, confidentiality, and integrity [248]. It is particularly useful in large-scale CRNs where users dynamically join or leave the network.	The main challenge with PKI in CRNs is the computational overhead associated with key generation, distribution, and validation, especially in resource-constrained environments like mobile devices.
Lightweight cryptographic solutions	Lightweight cryptography improves the performance of CRNs by minimizing latency and power consumption, making them suitable for mobile and battery-powered CR devices [249].	While lightweight cryptography is efficient, it may not always provide the same level of security as traditional algorithms [250], especially in highly adversarial environments.
Reputation-based trust models	Reputation-based systems reduce the impact of malicious users in cooperative spectrum sensing [251], thus improving the overall security and performance of the CRN.	The accuracy of these models can be affected by collusion among malicious users who work together to manipulate trust scores. Furthermore, trust systems may require extensive monitoring, which can introduce communication overhead.
Subjective logic-based trust models	Subjective logic allows for flexibility in trust management [252], as it can handle uncertain or incomplete information. It also enables CR devices to adapt trust levels dynamically based on new evidence.	These models require complex algorithms to process subjective opinions and update trust values, which can increase computational complexity.
Differential privacy	Differential privacy provides a robust mathematical framework for protecting user data while allowing for accurate sensing results [253]. It is particularly effective in large-scale networks with many users.	The trade-off between privacy and accuracy is a key challenge. Adding too much noise can reduce the accuracy of spectrum sensing, while too little noise can compromise privacy. Balancing these factors requires careful tuning of privacy parameters.
Homomorphic encryption	Homomorphic encryption provides strong privacy guarantees because the data remains encrypted throughout the entire process [254]. This eliminates the risk of data exposure during transmission or computation.	Homomorphic encryption is computationally intensive, which can make it impractical for resource-constrained devices in CRNs. Recent advancements have focused on developing more efficient algorithms, but this remains an area of ongoing research.
PPCSS	PPCSS frameworks enable secure and private participation in cooperative spectrum sensing [255], improving the overall performance and fairness of the network.	These frameworks often require complex cryptographic operations or additional communication overhead [256], which can increase the latency and energy consumption in the network.
Non-cooperative game theory	Game-theoretic frameworks provide a mathematical approach to analyzing complex security interactions in CRNs [257]. They can be used to design adaptive defense mechanisms that adjust based on the behavior of attackers.	The challenge with non-cooperative games is ensuring that all users follow the network rules. Malicious users may not act rationally or may collude to exploit the system. Additionally, game-theoretic models can be computationally intensive.
Cooperative game theory	Cooperative game theory fosters collaboration among users, improving spectrum utilization and security [258]. It can also be used to design fair and efficient resource allocation mechanisms.	Encouraging cooperation among users can be difficult in adversarial environments, where some users may attempt to cheat the system for personal gain. Trust management systems must be in place to prevent such behavior.

6. Open research challenges

As CRNs continue to evolve and expand, ensuring robust security and privacy remains a critical concern [259]. The dynamic, decentralized, and adaptive nature of CRNs introduces unique challenges that current solutions struggle to fully address. This section explores several open research challenges in the security and privacy domain for CRNs, highlighting areas where further investigation is needed to improve the resilience and trustworthiness of these networks.

6.1. Dynamic Spectrum Management and Security

Dynamic Spectrum Management (DSM) is a key feature of CRNs, allowing users to adaptively access available spectrum bands based on real-time conditions [260]. However, the dynamic nature of spectrum access introduces several security challenges:

Adaptive attack strategies: As CRNs continuously adapt their spectrum usage, attackers can exploit this flexibility to launch sophisticated attacks, such as SSDF or PUE attacks. Attackers may also use adaptive jamming techniques [261] that vary based on the spectrum management policies.

Future research directions encompasses the development of robust mechanisms to detect and mitigate adaptive attacks in real-time. Research is needed to create models and algorithms that can anticipate and counteract evolving attack strategies while maintaining efficient [262] spectrum management.

Spectrum handoff security: Spectrum handoff, where a cognitive radio switches from one frequency band to another, can be exploited by attackers to disrupt communication or eavesdrop on sensitive data [263].

Future research works involves the investigation of secure spectrum handoff protocols that ensure the integrity and confidentiality of data during the transition between spectrum bands. Solutions should address potential vulnerabilities introduced during handoff processes.

6.2. Privacy in cooperative spectrum sensing

Cooperative Spectrum Sensing (CSS) relies on multiple users sharing their spectrum sensing data to improve accuracy. However, this sharing introduces privacy risks:

Privacy-preserving sensing data aggregation: Ensuring that users can participate in cooperative sensing without disclosing sensitive information about their location, behavior, or communication patterns [264].

Probable research directions involves the development of advanced privacy-preserving techniques, such as secure multi-party computation (SMPC) and differential privacy, to aggregate sensing data while protecting individual user privacy. Research should focus on optimizing these techniques for real-time applications.

Trade-offs between privacy and accuracy: Balancing the need for privacy with the accuracy of spectrum sensing results [265]. Excessive privacy measures can degrade sensing performance, while insufficient measures can expose sensitive information.

Future research directions encompass the investigation of methods that dynamically adjust the level of privacy based on the specific requirements of the sensing task and the sensitivity of the data. Developing adaptive privacy models that can maintain high sensing accuracy while protecting user privacy.

6.3. Trust management in decentralized networks

Trust Management is crucial for ensuring reliable operation in decentralized CRNs where users interact without a central authority:

Robust trust evaluation mechanisms: Designing trust models that accurately evaluate user behavior and detect malicious actions in a decentralized environment [266]. Current models may be susceptible to collusion attacks or manipulation by malicious users.

Probable research directions will involve exploring advanced trust evaluation techniques, such as blockchain-based systems for immutable trust records and decentralized trust management frameworks. Research should also focus on enhancing trust models to handle diverse and dynamic network conditions.

Scalability and adaptability of trust systems: Ensuring that trust management systems can scale to large numbers of users and adapt to changes in the network topology and user behavior [267].

Feasible research directions have to do with the development of scalable trust management solutions that can efficiently handle large-scale CRNs and adapt to changes in network conditions. Investigating algorithms that balance computational efficiency with the accuracy of trust assessments.

6.4. Security of lightweight and resource-constrained devices

CRNs often involve lightweight and resource-constrained devices that may not support traditional security measures:

Lightweight cryptographic solutions: Implementing cryptographic solutions that provide sufficient security while being efficient enough for devices with limited computational and energy resources [268].

Feasible research directions entails the advancement of lightweight cryptographic algorithms and protocols that can offer strong security guarantees without imposing significant computational overhead. Research should focus on optimizing encryption and authentication mechanisms for resource-constrained CR devices.

Energy-efficient security protocols: Balancing security requirements with the energy constraints of CR devices [269], especially in battery-powered scenarios.

Research directions in this domain entails designing energy-efficient security protocols that minimize the impact on device battery life while maintaining robust protection against attacks [270]. Investigating novel approaches to reduce energy consumption in security operations, such as low-power encryption techniques.

6.5. Security and privacy in multi-tenant CRNs

Multi-Tenant CRNs involve multiple operators or users sharing the same network infrastructure, each with different security and privacy requirements:

Isolation and segregation of resources: Ensuring that the activities of one tenant do not interfere with or compromise the security and privacy of other tenants [271]. Proper isolation mechanisms are needed to prevent cross-tenant data leakage or interference.

Possible research directions have to do with the development of mechanisms for secure resource isolation and segregation in multi-tenant CRNs. This includes designing virtualized network environments that maintain security boundaries between tenants and prevent unauthorized access to shared resources.

Tenant-specific security policies: Implementing and enforcing security policies that cater to the specific needs of different tenants, while maintaining overall network integrity [272].

Future research work may investigate policy management frameworks that can handle diverse security and privacy requirements in multi-tenant environments. Research should focus on dynamic policy enforcement and conflict resolution between tenant-specific policies.

6.6. Vulnerability to emerging threats

Emerging Threats such as advanced persistent threats (APTs), machine learning-based attacks, and quantum computing pose new challenges for CRNs:

Machine learning-based attacks: Machine learning techniques can be used by attackers to develop sophisticated attacks, such as predicting spectrum usage patterns or evading detection by adaptive security mechanisms [273], [274].

Future research efforts should be devoted towards exploring methods to defend against machine learning-based attacks [275], including the development of machine learning algorithms for intrusion detection and anomaly detection in CRNs.

Quantum computing threats: Quantum computing has the potential to break many traditional cryptographic algorithms [276], posing a significant threat to CRNs.

Research directions in this domain will encompass the investigation of post-quantum cryptographic algorithms and protocols that can withstand attacks from quantum computers [277]-[279]. Research should focus on transitioning to quantum-resistant security measures while maintaining compatibility with existing CRN infrastructure.

In a nutshell, there are a number of open research challenges in CRNs security and privacy which requires a multidisciplinary approach. This may encompass a combination of advances in cryptography, trust management, privacy-preserving techniques, and emerging technologies [280]. As CRNs continue to evolve and integrate into various applications, ongoing research is crucial to developing effective solutions that balance security, privacy, and performance. Collaborative efforts among researchers, practitioners, and industry stakeholders will be essential to tackling these challenges and ensuring the resilience and trustworthiness of future CRNs.

7. Conclusion

The rapid evolution and deployment of Cognitive Radio Networks (CRNs) introduce significant opportunities for optimizing spectrum utilization and enhancing communication flexibility. However, this dynamic and decentralized nature also presents complex security and privacy challenges that must be addressed to ensure the robustness and trustworthiness of these networks. Throughout this paper, various dimensions of security and privacy issues in CRNs have been explored, including the fundamental architectural elements of cognitive radios, the inherent security and privacy challenges, and existing frameworks designed to mitigate these issues. Key security concerns encompass the protection of spectrum access, secure communication, and the integrity of cooperative spectrum sensing. On the privacy front, challenges include safeguarding users' location data, identity, and spectrum usage patterns while participating in cooperative sensing and sharing activities. Existing frameworks, such as cryptographic solutions, trust management systems, and privacy-preserving techniques, offer valuable tools for addressing these challenges. Cryptographic methods, including public key infrastructure (PKI) and lightweight cryptographic algorithms, provide essential security functions but must be tailored to the resource constraints of CR devices. Trust management frameworks, such as reputation-based and subjective logic models, play a crucial role in ensuring cooperation and mitigating malicious behavior. Privacy-preserving techniques, such as differential privacy and homomorphic encryption, are vital for protecting sensitive user data during spectrum sensing and sharing. Despite the progress made, several open research challenges remain. Dynamic spectrum management, privacy in cooperative spectrum sensing, trust management in decentralized networks, and the security of lightweight devices are areas that require ongoing investigation. Additionally, emerging threats such as machine learning-based attacks and quantum computing pose new risks that demand innovative solutions. To address these challenges effectively, future research should focus on developing adaptable and scalable solutions that can operate within the constraints of CRNs while maintaining high levels of security and privacy. Collaborative efforts among researchers, industry stakeholders, and policymakers are essential to advance the state of the art and ensure the secure and private operation of CRNs in diverse applications. Therefore, the journey towards securing and preserving privacy in CRNs is ongoing. Continued innovation and rigorous research are imperative to overcome the current limitations and to address the evolving threats in this dynamic field. By leveraging the insights and advancements discussed in this paper, the players can work towards building more resilient and privacy-conscious CRNs that meet the demands of tomorrow's wireless communication landscape.

References

[1] Olaleye DS, Oloye AC, Akinloye AO, Akinwande OT. Advancing green communications: the role of radio frequency engineering in sustainable infrastructure design. International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS). 2024;13(5):113.

[2] Alsaedi WK, Ahmadi H, Khan Z, Grace D. Spectrum options and allocations for 6G: A regulatory and standardization review. IEEE Open Journal of the Communications Society. 2023 Aug 7.

[3] Ahmad WS, Radzi NA, Samidi FS, Ismail A, Abdullah F, Jamaludin MZ, Zakaria M. 5G technology: Towards dynamic spectrum sharing using cognitive radio networks. IEEE access. 2020 Jan 13;8:14460-88.

[4] Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Sixth generation (6G) cognitive radio network (CRN) application, requirements, security issues, and key challenges. Wireless Communications and Mobile Computing. 2021;2021(1):1331428.

[5] Solomon AM, Jayakumari J. Improving User Satisfaction for Next Generation CRN using Utility Proportional Fairness based Resource Allocation Approach. In2024 International Conference on Advancements in Power, Communication and Intelligent Systems (APCI) 2024 Jun 21 (pp. 1-6). IEEE.

[6] Pandian P, Selvaraj C, Priyanga S. Spectrum Sensing and Sharing for Internet of Things. InSpectrum and Power Allocation in Cognitive Radio Systems 2024 (pp. 224-240). IGI Global.

[7] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[8] Candal-Ventureira D, González-Castaño FJ, Gil-Castineira F, Fondo-Ferreiro P. Coordinated allocation of radio resources to Wi-Fi and cellular technologies in shared unlicensed frequencies. IEEE Access. 2021 Sep 24;9:134435-56.

[9] Pandit S, Singh G, Pandit S, Singh G. Cognitive radio communication system: spectrum sharing techniques. Spectrum Sharing in Cognitive Radio Networks: Medium Access Control Protocol Based Approach. 2017:1-33.

[10] Comert C, Gul OM, Kulhandjian M, Touazi A, Ellement C, Kantarci B, D'Amours C. Secure design of cyber-physical systems at the radio frequency level: Machine and deep learning-driven approaches, challenges and opportunities. Artificial Intelligence for Cyber-Physical Systems Hardening. 2022 Nov 24:123-54.

[11] Miranda RF, Barriquello CH, Reguera VA, Denardin GW, Thomas DH, Loose F, Amaral LS. A review of cognitive hybrid radio frequency/visible light communication systems for wireless sensor networks. Sensors. 2023 Sep 12;23(18):7815.

[12] Shuaib K, Barka E, Al Hussien N, Abdel-Hafez M, Alahmad M. Cognitive radio for smart grid with security considerations. Computers. 2016 Apr 28;5(2):7.

[13] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[14] Chandrakant AC, Patil KP. Analysis of Various Attacks in Cognitive Radio Network and Security Provisions. In2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS) 2024 Apr 17 (pp. 36-43). IEEE.

[15] Mthulisi V, Issah N, Semaka MS. Spectrum sensing data falsification attack reputation and Q-out-of-M rule security scheme. InProceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London, Volume 2 2022 (pp. 11-25). Springer Singapore.

[16] Paul A, Mishra AK, Shreevastava S, Tiwari AK. Deep reinforcement learning based reliable spectrum sensing under SSDF attacks in cognitive radio networks. Journal of Network and Computer Applications. 2022 Sep 1;205:103454.

[17] Dong Q, Chen Y, Li X, Zeng K, Zimmermann R. An adaptive primary user emulation attack detection mechanism for cognitive radio networks. InSecurity and Privacy in Communication Networks: 14th International Conference, SecureComm 2018, Singapore, Singapore, August 8-10, 2018, Proceedings, Part I 2018 (pp. 297-317). Springer International Publishing.

[18] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[19] Lebepe M, Velempini M. Evaluation of denial of service attacks in software defined-cognitive radio networks. InInternational Conference on Ad Hoc Networks 2021 Nov 24 (pp. 49-62). Cham: Springer International Publishing.

[20] Lei H, Jiang J, Yang H, Park KH, Ansari IS, Pan G, Alouini MS. Trajectory and power design for aerial CRNs with colluding eavesdroppers. IEEE Transactions on Vehicular Technology. 2024 Aug 2.

[21] Yamini B, Beslin PP, Anish TP, Gracelin SB, Dinesh MG, Nalini M, Siva SR. Advancements in Cognitive Radio Networks: Protocols, Architectures, Challenges, and Future Perspectives. InSpectrum and Power Allocation in Cognitive Radio Systems 2024 (pp. 1-17). IGI Global.

[22] Zeng Y, Li X, Yang X, Xu Q, Wang D. A practical privacy preserving protocol in database-driven cognitive radio networks. InInformation Security and Privacy: 23rd Australasian Conference, ACISP 2018, Wollongong, NSW, Australia, July 11-13, 2018, Proceedings 23 2018 (pp. 634-648). Springer International Publishing.

[23] Rachakonda LP, Siddula M, Sathya V. A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond). High-Confidence Computing. 2024 Mar 12:100220.

[24] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[25] Ul Hassan M, Rehmani MH, Rehan M, Chen J. Differential privacy in cognitive radio networks: a comprehensive survey. Cognitive Computation. 2022 Mar;14(2):475-510.

[26] Deebak BD, Al-Turjman F, Zahmatkesh H. An efficient lightweight privacy-preserving scheme for secondary users in cognitive radio networks. InSustainable Networks in Smart Grid 2022 Jan 1 (pp. 233-253). Academic Press.

[27] Al-Rjoob AM, Ababnah AA, Al-Mistarihi MF, Darabkh KA. Physical-layer security for primary users in 5G underlay cognitive radio system via artificial-noise-aided by secondary users. International Journal of Computers and Applications. 2024 Jul 24:1-3.

[28] Muchandi N, Khanai R, Muchandi M. Cooperative Sensing Assisted Cross layer QoS Assured Routing in Cognitive Radio Adhoc Networks: Ensuring Security and Privacy. International Journal of Intelligent Engineering & Systems. 2024 Jan 1;17(1).

[29] Li W, Chen G, Zhang X, Wang N, Lv S, Huang J. When Industrial Radio Security Meets AI: Opportunities and Challenges. IEEE Transactions on Industrial Informatics. 2024 Jun 24.

[30] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[31] Seliem M, Elgazzar K, Khalil K. Towards privacy preserving iot environments: a survey. Wireless Communications and Mobile Computing. 2018;2018(1):1032761.

[32] Sampaio S, Sousa PR, Martins C, Ferreira A, Antunes L, Cruz-Correia R. Collecting, processing and secondary using personal and (pseudo) anonymized data in smart cities. Applied Sciences. 2023 Mar 16;13(6):3830.

[33] Li H, Pei Q, Zhang W. Location privacy-preserving channel allocation scheme in cognitive radio networks. International Journal of Distributed Sensor Networks. 2016 Jul 14;12(7):3794582.

[34] Sabir B, Yang S, Nguyen D, Wu N, Abuadbba A, Suzuki H, Lai S, Ni W, Ming D, Nepal S. Systematic Literature Review of AI-enabled Spectrum Management in 6G and Future Networks. arXiv preprint arXiv:2407.10981. 2024 Jun 12.

[35] Li Y, Xiao Y, Liang W, Cai J, Zhang R, Li KC, Khan MK. The security and privacy challenges toward cybersecurity of 6G networks: A comprehensive review. Computer Science and Information Systems. 2024(00):16-.

[36] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[37] Iyer S, Patil A, Bhairanatti S, Halagatti S, Pandya RJ. A survey on technological trends to enhance spectrum-efficiency in 6g communications. Transactions of the Indian National Academy of Engineering. 2022 Dec;7(4):1093-120.

[38] Shayea I, Azmi MH, Rahman TA, Ergen M, Han CT, Arsad A. Spectrum gap analysis with practical solutions for future mobile data traffic growth in Malaysia. IEEE Access. 2019 Jan 6;7:24910-33.

[39] Grissa M, Hamdaoui B, Yavuz AA. Location privacy in cognitive radio networks: A survey. IEEE Communications Surveys & Tutorials. 2017 Apr 12;19(3):1726-60.

[40] Abbas G, Abbas ZH, Baker T, Waqas M. Spectrum efficiency in CRNs using hybrid dynamic channel reservation and enhanced dynamic spectrum access. Ad Hoc Networks. 2020 Oct 1;107:102246.

[41] Hlophe MC, Maharaj BT. AI meets CRNs: A prospective review on the application of deep architectures in spectrum management. IEEE Access. 2021 Aug 11;9:113954-96.

[42] Parhizgar N, Jamshidi A, Setoodeh P. Defense against spectrum sensing data falsification attack in cognitive radio networks using machine learning. In2022 30th International Conference on Electrical Engineering (ICEE) 2022 May 17 (pp. 974-979). IEEE.

[43] Duaa Fadhel Najem, Nagham Abdulrasool Taha, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Junchao Ma and Dhafer G. Honi. Low-Complexity and Secure Clustering-Based Similarity Detection for Private Files. TEM Journal, 13(2), 2341-2349 (2024).DOI: 10.18421/TEM133-61

[44] 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 Communications. 2021 Apr;15(7):875-905.

[45] Nasser A, Al Haj Hassan H, Abou Chaaya J, Mansour A, Yao KC. Spectrum sensing for cognitive radio: Recent advances and future challenge. Sensors. 2021 Mar 31;21(7):2408.

[46] Khan R, Kumar P, Jayakody DN, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials. 2019 Aug 8;22(1):196-248.

[47] Porambage P, Gür G, Osorio DP, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society. 2021 May 10;2:1094-122.

[48] Lamssaggad A, Benamar N, Hafid AS, Msahli M. A survey on the current security landscape of intelligent transportation systems. IEEE Access. 2021 Jan 8;9:9180-208.

[49] Xu X, Patibandla RL, Arora A, Al-Razgan M, Awwad EM, Nyangaresi VO. An Adaptive Hybrid (1D-2D) Convolution-based ShuffleNetV2 Mechanism for Irrigation Levels Prediction in Agricultural Fields with Smart IoTs. IEEE Access. 2024 Apr 3.

[50] Dixit S. The Impact of Quantum Computing on Cryptographic Security Protocols. Advances in Nonlinear Variational Inequalities. 2024 Aug 24;27(3):558-70.

[51] Aouedi O, Vu TH, Sacco A, Nguyen DC, Piamrat K, Marchetto G, Pham QV. A survey on intelligent Internet of Things: applications, security, privacy, and future directions. IEEE Communications Surveys & Tutorials. 2024 Jul 18.

[52] Velliangiri S, Manoharn R, Ramachandran S, Venkatesan K, Rajasekar V, Karthikeyan P, Kumar P, Kumar A, Dhanabalan SS. An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography. IEEE Transactions on Industrial Informatics. 2021 Dec 31;18(9):6494-502.

[53] Theodore SK, Gandhi KR, Palanisamy V. A novel lightweight authentication and privacy-preserving protocol for vehicular ad hoc networks. Complex & Intelligent Systems. 2021 Oct:1-1.

[54] Alshudukhi JS, Al-Mekhlafi ZG, Mohammed BA. A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography. IEEE Access. 2021 Jan 20;9:15633-42.

[55] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[56] Muzaffar MU, Sharqi R. A review of spectrum sensing in modern cognitive radio networks. Telecommunication Systems. 2024 Feb;85(2):347-63.

[57] Fernando X, Lăzăroiu G. Spectrum sensing, clustering algorithms, and energy-harvesting technology for cognitive-radio-based internet-of-things networks. Sensors. 2023 Sep 11;23(18):7792.

[58] Luo J, Zhang G, Yan C. An energy detection-based spectrum-sensing method for cognitive radio. Wireless Communications and Mobile Computing. 2022;2022(1):3933336.

[59] Dannana S, Chapa BP, Rao GS. Spectrum sensing using matched filter detection. InIntelligent Engineering Informatics: Proceedings of the 6th International Conference on FICTA 2018 (pp. 497-503). Springer Singapore.

[60] Kumar BA, Hima Bindu V, Swetha N. User detection using cyclostationary feature detection in cognitive radio networks with various detection criteria. InInternational Conference on Innovative Computing and Communications: Proceedings of ICICC 2020, Volume 2 2021 (pp. 1013-1029). Springer Singapore.

[61] Huang T, Yin X, Li X. Energy-efficient and intelligent cooperative spectrum sensing algorithm in cognitive radio networks. International Journal of Distributed Sensor Networks. 2022 Sep;18(9):15501329221125119.

[62] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[63] Giral D, Hernández C, Rodríguez-Colina E. Spectrum decision-making in collaborative cognitive radio networks. Applied Sciences. 2020 Sep 28;10(19):6786.

[64] Rao AL, Ramesh B, Jain A, Alzubaidi LH, Barolia PA. The Role of Cognitive Radio in Optimizing Spectrum Utilization. In2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT) 2024 Apr 6 (pp. 176-182). IEEE.

[65] Ghodhbane RM. A Mixed Spectrum Sharing Strategy for Cognitive Radio Systems. In2021 International Conference on Smart Applications, Communications and Networking (SmartNets) 2021 Sep 22 (pp. 1-6). IEEE.

[66] Briones-Reyes A, Vásquez-Toledo LA, Prieto-Guerrero A, Aguilar-Gonzalez R. Mathematical evaluation of spectrum sharing in cognitive radio networks for 5G systems using Markov processes. Computer Networks. 2020 Dec 9;182:107521.

[67] Kumar G, Kumar S, Shrivastava A, Srivastava AP, Badhoutiya A, Pant R. Dynamic Spectrum Access in Cognitive Radio Networks: A Reinforcement Learning Approach. In2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) 2024 Feb 21 (pp. 1-6). IEEE.

[68] Al Sibahee MA, Ma J, Nyangaresi VO, Abduljabbar ZA. Efficient Extreme Gradient Boosting Based Algorithm for QoS Optimization in Inter-Radio Access Technology Handoffs. In2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) 2022 Jun 9 (pp. 1-6). IEEE.

[69] Zaheer O, Ali M, Imran M, Zubair H, Naeem M. Efficient resource allocation for 5G/6G cognitive radio networks using probabilistic interference models. Physical Communication. 2024 Jun 1;64:102335.

[70] Al-Medhwahi M, Hashim F, Ali BM, Sali A, Alkholidi A. Resource allocation in heterogeneous cognitive radio sensor networks. International Journal of Distributed Sensor Networks. 2019 Jul;15(7):1550147719851944.

[71] Mishra S, Singh SS, Mishra BS. A comparative analysis of centralized and distributed spectrum sharing techniques in cognitive radio. Computational Intelligence in Sensor Networks. 2019:455-72.

[72] Hawa M, AlAmmouri A, Alhiary A, Alhamad N. Distributed opportunistic spectrum sharing in cognitive radio networks. international journal of communication systems. 2017 May 10;30(7):e3147.

[73] Premalatha M, Singh N. Increased Efficient Usage of Power in Cognitive Radio Networks Utilizing Hybridized Handover of Spectrum. In2024 5th International Conference for Emerging Technology (INCET) 2024 May 24 (pp. 1-5). IEEE.

[74] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[75] Arshid K, Jianbiao Z, Hussain I, Pathan MS, Yaqub M, Jawad A, Munir R, Ahmad F. Energy efficiency in cognitive radio network using cooperative spectrum sensing based on hybrid spectrum handoff. Egyptian Informatics Journal. 2022 Dec 1;23(4):77-88.

[76] Qasim HH, Abidin HZ, Abdullah SA. Handover management in vehicle communication: applications, techniques, issues, and challenges: a review. Bulletin of Electrical Engineering and Informatics. 2024 Oct 1;13(5):3167-86.

[77] Joshi N, Arora N, Yadav H, Sharma SC. AI-Driven Cognitive Radio Networks for Transforming Industries and Sectors Towards a Smart World. InRecent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors 2024 Sep 10 (pp. 1-35). Singapore: Springer Nature Singapore.

[78] Babu CR, Balakrishnan A, Ramana K, Singh S, Ra IH. Elite-CAM: An Elite Channel Allocation and Mapping for Policy Engine over Cognitive Radio Technology in 5G. Sensors. 2022 Jul 2;22(13):5011.

[79] Moon P, Yenurkar G, Nyangaresi VO, Raut A, Dapkekar N, Rathod J, Dabare P. An improved custom convolutional neural network based hand sign recognition using machine learning algorithm. Engineering Reports. 2024:e12878.

[80] Venkatesan M, Kulkarni AV, Menon R. Learning Strategies in Cognitive Radio Involving Soft Computing Techniques. Cognitive Radio, Mobile Communications and Wireless Networks. 2019:233-57.

[81] Wang Y, Ye Z, Wan P, Zhao J. A survey of dynamic spectrum allocation based on reinforcement learning algorithms in cognitive radio networks. Artificial intelligence review. 2019 Mar 15;51:493-506.

[82] Zhang J, Li J. Spatial Cognitive Engine Technology. Elsevier; 2023 Jun 15.

[83] Miranda RF, Barriquello CH, Reguera VA, Denardin GW, Thomas DH, Loose F, Amaral LS. A review of cognitive hybrid radio frequency/visible light communication systems for wireless sensor networks. Sensors. 2023 Sep 12;23(18):7815.

[84] Sen P, Bozorgi F, Harutyunyan A, Noll Barreto A, Nimr A, Fettweis G. RF front-ends for ISAC—design challenges and potential solutions. InIntegrated Sensing and Communications 2023 Jul 19 (pp. 507-535). Singapore: Springer Nature Singapore.

[85] Medeisis A, Holland O, Holland O, Basaure A, Medeisis A, Sydor J, Cremene L, Więcek D, Haddad Y, Holland O, Anskaitis A. Policy Suggestions for the Way Forward for CR. InCognitive Radio Policy and Regulation: Techno-Economic Studies to Facilitate Dynamic Spectrum Access 2014 Feb 13 (pp. 349-381). Cham: Springer International Publishing.

[86] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[87] Oyewobi SS, Djouani K, Kurien AM. A review of industrial wireless communications, challenges, and solutions: A cognitive radio approach. Transactions on Emerging Telecommunications Technologies. 2020 Sep;31(9):e4055.

[88] Kiran NC. Cognitive radios. InTowards Wireless Heterogeneity in 6G Networks 2024 (pp. 70-86). CRC Press.

[89] Zemo FD, Bakkali S. A survey on security threats in cognitive radio networks based on cooperative spectrum sensing. International Journal of Communication Networks and Distributed Systems. 2024;30(4):433-66.

[90] Marinho J, Granjal J, Monteiro E. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal on Information Security. 2015 Dec;2015:1-4.

[91] Ahuja P, Sethi P, Chauhan N. A comprehensive survey of security threats, detection, countermeasures, and future directions for physical and network layers in cognitive radio networks. Multimedia Tools and Applications. 2024 Mar;83(11):32715-38.

[92] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[93] Olaleru GI, Ohize HO, Dauda US, Isaac YO, Obiajulu OJ, Folashade A. A Systematic Review of the Primary User Emulation Attack in the Cognitive Radio Network. In2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG) 2024 Apr 2 (pp. 1-7). IEEE.

[94] Thulasimani L, Hyils Sharon Magdalene A. Lessening Spectrum Sensing Data Falsification Attack by Weighted Fuzzy Clustering Means Using Simulation Annealing in Cognitive Radio Networks. InInternational Conference on Advances in Electrical and Computer Technologies 2021 Oct 1 (pp. 423-435). Singapore: Springer Nature Singapore.

[95] Amsaveni A, Bharathi M. Security Threats and Privacy Challenges in Millimeter-Wave Communications. InNext Generation Wireless Communication: Advances in Optical, mm-Wave, and THz Technologies 2024 Jul 24 (pp. 13-33). Cham: Springer Nature Switzerland.

[96] Salameh HB, Abdel-Razeq S, Al-Obiedollah H. Integration of cognitive radio technology in NOMA-based B5G networks: State of the art, challenges, and enabling technologies. IEEE Access. 2023 Feb 6;11:12949-62.

[97] Madbushi S, Raut R, Rukmini MS. Security issues in cognitive radio: A review. Microelectronics, Electromagnetics and Telecommunications: Proceedings of ICMEET 2015. 2016:121-34.

[98] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[99] Muñoz EC, Pedraza GC, Cubillos-Sánchez R, Aponte-Moreno A, Buitrago ME. PUE Attack Detection by Using DNN and Entropy in Cooperative Mobile Cognitive Radio Networks. Future Internet. 2023 May 31;15(6):202.

[100] Pari D, Natarajan J. Defense against SSDF Attack and PUE Attack in CR-Internet of Vehicles (IoVs) for Millimeter Wave Massive MIMO Beamforming Systems. Symmetry. 2022 Nov 22;14(12):2472.

[101] Batool R, Bibi N, Muhammad N, Alhazmi S. Detection of primary user emulation attack using the differential evolution algorithm in cognitive radio networks. Applied Sciences. 2022 Dec 31;13(1):571.

[102] Khan MS, Jibran M, Koo I, Kim SM, Kim J. A double adaptive approach to tackle malicious users in cognitive radio networks. Wireless Communications and Mobile Computing. 2019;2019(1):2350694.

[103] Al-Dulaimi OM, Vlâdeanu C, Martia A, Al-DulaimiMohammed AM, Al-Dulaim MK. Cognitive radio using spectrum sensing by cooperative two secondary users. InIOP conference series: Materials science and engineering 2021 Feb 1 (Vol. 1094, No. 1, p. 012031). IOP Publishing.

[104] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[105] Vadivukkarasi S, Santhi S. A novel hybrid learning based Ada Boost (HLBAB) classifier for channel state estimation in cognitive networks. International Journal of Dynamics and Control. 2021 Mar;9(1):299-307.

[106] Elghamrawy SM. Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. Future generation computer systems. 2020 Aug 1;109:479-87.

[107] Wan R, Ding L, Xiong N, Zhou X. Mitigation strategy against spectrum-sensing data falsification attack in cognitive radio sensor networks. International Journal of Distributed Sensor Networks. 2019 Sep;15(9):1550147719870645.

[108] Yao J, Cao J, Zheng Q, Ma J. Pre-processing of incomplete spectrum sensing data in spectrum sensing data falsification attacks detection: a missing data imputation approach. Iet Communications. 2016 Jul;10(11):1340-7.

[109] Mapunya S, Makgolane B, Velempini M. Investigating the Effectiveness of Spectrum Sensing Data Falsification Attacks Defense Mechanisms in Cognitive Radio Ad Hoc Networks. InInternational Conference on Ad Hoc Networks 2021 Nov 24 (pp. 72-80). Cham: Springer International Publishing.

[110] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[111] Hwang J, Kim J, Sung I, Yoo D, Kim K. Fast and Accurate Detection of Malicious Users in Cooperative Spectrum Sensing Network. Wireless Personal Communications. 2021 May;118:1709-31.

[112] Gul N, Qureshi IM, Elahi A, Rasool I. Defense against malicious users in cooperative spectrum sensing using genetic algorithm. International Journal of Antennas and Propagation. 2018;2018(1):2346317.

[113] Rawat DB, Song M, Shetty S. Dynamic spectrum access for wireless networks. Springer International Publishing; 2015 Mar 9.

[114] Safdar GA, Ur-Rehman M, Muhammad M, Imran MA, Tafazolli R. Interference mitigation in D2D communication underlaying LTE-A network. IEEE Access. 2016 Oct 25;4:7967-87.

[115] Dalmazo BL, Marques JA, Costa LR, Bonfim MS, Carvalho RN, da Silva AS, Fernandes S, Bordim JL, Alchieri E, Schaeffer-Filho A, Paschoal Gaspary L. A systematic review on distributed denial of service attack defense mechanisms in programmable networks. International Journal of Network Management. 2021 Nov;31(6):e2163.

[116] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA. Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance. Plos one. 2024 Jan 23;19(1):e0296781.

[117] Lebepe M, Velempini M. Mitigation of Denial of Service Attacks in Software-Defined Cognitive Radio Networks. In2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD) 2021 Aug 5 (pp. 1-5). IEEE.

[118] Chuku E, Kouvatsos D. Detection of Network Congestion and Denial of Service (DoS) Attacks in Cognitive Radio Networks. In2019 7th International Conference on Future Internet of Things and Cloud (FiCloud) 2019 Aug 26 (pp. 377-384). IEEE.

[119] Amjad MF, Afzal H, Abbas H, Subhani AB. AdS: An adaptive spectrum sensing technique for survivability under jamming attack in Cognitive Radio Networks. Computer Communications. 2021 Apr 15;172:25-34.

[120] Abdolkhani N, Khalek NA, Hamouda W. Deep Reinforcement Learning for EH-Enabled Cognitive-IoT Under Jamming Attacks. IEEE Internet of Things Journal. 2024 Sep 10.

[121] Jaichandran R, Bharathi PS, Meenakshi B, Anushya A, Devi VB. The Defense Against Jamming Attack in Cognitive Radio Networks: Energy Efficiency Management Perspective. Microprocessors and Microsystems. 2021 Apr 1;82:103816.

[122] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[123] Mu H, Hu T. Cognitive radio and the new spectrum paradigm for 5G. Spectrum Access and Management for Cognitive Radio Networks. 2017:265-86.

[124] Hassani MM, Berangi R. A new congestion control mechanism for transport protocol of cognitive radio sensor networks. AEU-International Journal of Electronics and Communications. 2018 Feb 1;85:134-43.

[125] Ogbodo EU, Dorrell D, Abu-Mahfouz AM. Cognitive radio based sensor network in smart grid: architectures, applications and communication technologies. IEEE Access. 2017 Sep 6;5:19084-98.

[126] Senthilkumar S, Geetha Priya C. A review of channel estimation and security techniques for CRNS. Automatic Control and Computer Sciences. 2016 May;50:187-210.

[127] Hu F, Chen B, Zhu K. Full spectrum sharing in cognitive radio networks toward 5G: A survey. IEEE Access. 2018 Feb 5;6:15754-76.

[128] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11; 2(3): 399-406.

[129] Salahdine F, Kaabouch N. Security threats, detection, and countermeasures for physical layer in cognitive radio networks: A survey. Physical Communication. 2020 Apr 1;39:101001.

[130] Jain AK, Sahoo SR, Kaubiyal J. Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems. 2021 Oct;7(5):2157-77.

[131] Bahramali A, Soltani R, Houmansadr A, Goeckel D, Towsley D. Practical traffic analysis attacks on secure messaging applications. arXiv preprint arXiv:2005.00508. 2020 May 1.

[132] Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. IEEE communications surveys & tutorials. 2022 Mar 14;24(2):767-809.

[133] Lavaud C, Gerzaguet R, Gautier M, Berder O, Nogues E, Molton S. Whispering devices: A survey on how side-channels lead to compromised information. Journal of Hardware and Systems Security. 2021 Jun;5:143-68.

[134] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[135] Salameh HA, Almajali S, Ayyash M, Elgala H. Spectrum assignment in cognitive radio networks for internet-of-things delay-sensitive applications under jamming attacks. IEEE Internet of Things Journal. 2018 Mar 20;5(3):1904-13.

[136] Salameh HB, Al-Quraan M. Securing delay-sensitive CR-IoT networking under jamming attacks: Parallel transmission and batching perspective. IEEE Internet of Things Journal. 2020 Apr 2;7(8):7529-38.

[137] Mousa SH, Ismail M, Nordin R, Abdullah NF. Effective Wide Spectrum Sharing Techniques Relying on CR Technology toward 5G: A Survey. J. Commun.. 2020 Feb;15(2):122-47.

[138] Balachander T, Krishnan MM. Efficient utilization of cooperative spectrum sensing (CSS) in cognitive radio network (CRN) using non-orthogonal multiple access (NOMA). Wireless Personal Communications. 2022 Dec;127(3):2189-210.

[139] Zhang Z, Sun Y, Sabharwal A, Chen Z. Impact of channel state misreporting on multi-user massive mimo scheduling performance. InIEEE INFOCOM 2018-IEEE Conference on Computer Communications 2018 Apr 16 (pp. 917-925). IEEE.

[140] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[141] Kampitaki DG, Economides AA. Selfishness in mobile ad-hoc networks: A literature review on detection techniques and prevention mechanisms. IEEE Access. 2023 Aug 14.

[142] Mohamed MI, Hassan MF, Safdar S, Saleem MQ. Adaptive security architectural model for protecting identity federation in service oriented computing. Journal of King Saud University-Computer and Information Sciences. 2021 Jun 1;33(5):580-92.

[143] Xie X, Wang W. Detecting primary user emulation attacks in cognitive radio networks via physical layer network coding. Procedia Computer Science. 2013 Jan 1;21:430-5.

[144] Ebendt R, Touko Tcheumadjeu LC. An approach to geometry-based dynamic location referencing. European Transport Research Review. 2017 Sep;9:1-30.

[145] Mousa H, Mokhtar SB, Hasan O, Younes O, Hadhoud M, Brunie L. Trust management and reputation systems in mobile participatory sensing applications: A survey. Computer Networks. 2015 Oct 29;90:49-73.

[146] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[147] Khan AU, Javaid N, Khan MA, Ullah I. A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things. Cluster Computing. 2023 Apr;26(2):945-60.

[148] Shahid MF, Mehmood K, Mohsin M, Saleem A, Yaqoob S, Bashir W. Taxonomy of Physical Layer Jamming Techniques and Strategies for Security Enhancement in Wireless Communication: A Comprehensive Survey.

[149] Benmoussa A, Kerrache CA, Lagraa N, Mastorakis S, Lakas A, Tahari AE. Interest flooding attacks in named data networking: survey of existing solutions, open issues, requirements, and future directions. ACM Computing Surveys. 2022 Dec 15;55(7):1-37.

[150] Li M, Zhu L, Zhang Z, Lal C, Conti M, Alazab M. User-defined privacy-preserving traffic monitoring against n-by-1 jamming attack. IEEE/ACM Transactions on Networking. 2022 Mar 23;30(5):2060-73.

[151] Drăguşin SA, Bizon N, Boştinaru RN. Comprehensive Analysis Of Cyber-Attack Techniques And Vulnerabilities In Communication Channels Of Embedded Systems. In2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) 2024 Jun 27 (pp. 1-12). IEEE.

[152] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[153] Vinod M, Sharma I, Singh G. Optimal sensing duration and threshold selection approach in cognitive radio networks with cooperative spectrum sensing. International Journal of Communication Systems. 2024:e5959.

[154] Alyami M, Alghamdi A, Alkhowaiter MA, Zou C, Solihin Y. Random segmentation: New traffic obfuscation against packet-size-based side-channel attacks. Electronics. 2023 Sep 9;12(18):3816.

[155] Chi Z, Li Y, Liu X, Wang W, Yao Y, Zhu T, Zhang Y. Countering cross-technology jamming attack. InProceedings of the 13th ACM conference on security and privacy in wireless and mobile networks 2020 Jul 8 (pp. 99-110).

[156] Tiwari RG, Misra A, Agarwal AK, Khullar V. Communication jamming in body sensor network: A review. In2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART) 2021 Dec 10 (pp. 135-139). IEEE.

[157] Osanaiye O, Alfa AS, Hancke GP. A statistical approach to detect jamming attacks in wireless sensor networks. Sensors. 2018 May 24;18(6):1691.

[158] Bennaceur J, Idoudi H, Saidane LA. Hierarchical game-based secure data collection with trust and reputation management in the cognitive radio network. Computers & Electrical Engineering. 2021 Dec 1;96:107463.

[159] Wang EK, Chen CM, Yiu SM, Hassan MM, Alrubaian M, Fortino G. Incentive evolutionary game model for opportunistic social networks. Future generation computer systems. 2020 Jan 1;102:14-29.

[160] Al Sibahee MA, Abduljabbar ZA, Luo C, Zhang J, Huang Y, Abduljaleel IQ, Ma J, Nyangaresi VO. Hiding scrambled text messages in speech signals using a lightweight hyperchaotic map and conditional LSB mechanism. Plos one. 2024 Jan 3;19(1):e0296469.

[161] Khasawneh M, Azab A, Alrabaee S, Sakkal H, Bakhit HH. Convergence of IoT and cognitive radio networks: A survey of applications, techniques, and challenges. IEEE Access. 2023 Jul 10;11:71097-112.

[162] Aslam MM, Du L, Zhang X, Chen Y, Ahmed Z, Qureshi B. Research Article Sixth Generation (6G) Cognitive Radio Network (CRN) Application, Requirements, Security Issues, and Key Challenges.

[163] Padhy A, Joshi S, Bitragunta S, Chamola V, Sikdar B. A survey of energy and spectrum harvesting technologies and protocols for next generation wireless networks. IEEE Access. 2020 Dec 23;9:1737-69.

[164] Fu Y, He Z. Massive SSDF attackers identification in cognitive radio networks by using consistent property. IEEE Transactions on Vehicular Technology. 2023 Mar 8;72(8):11058-62.

[165] Khalek NA, Tashman DH, Hamouda W. Advances in Machine Learning-Driven Cognitive Radio for Wireless Networks: A Survey. IEEE Communications Surveys & Tutorials. 2023 Dec 21.

[166] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[167] Lee NJ. Freedom of Movement: Protecting the Right to Travel from Location Tracking Interference. Drexel L. Rev.. 2024;16:187.

[168] Gadallah WG, Ibrahim HM, Omar NM. A deep learning technique to detect distributed denial of service attacks in software-defined networks. Computers & Security. 2024 Feb 1;137:103588.

[169] Asuquo P, Cruickshank H, Morley J, Ogah CP, Lei A, Hathal W, Bao S, Sun Z. Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures. IEEE Internet of Things Journal. 2018 Mar 27;5(6):4778-802.

[170] Lai H, Xu L, Zeng Y. An efficient location privacy-preserving authentication scheme for cooperative spectrum sensing. IEEE Access. 2020 Sep 7;8:163472-82.

[171] Haber MJ, Rolls D. Identity attack vectors. InIdentity Attack Vectors: Strategically Designing and Implementing Identity Security, Second Edition 2024 Mar 31 (pp. 109-118). Berkeley, CA: Apress.

[172] Al Sibahee MA, Nyangaresi VO, Abduljabbar ZA, Luo C, Zhang J, Ma J. Two-Factor Privacy Preserving Protocol for Efficient Authentication in Internet of Vehicles Networks. IEEE Internet of Things Journal. 2023 Dec 7.

[173] Park J, Rahman F, Vassilev A, Forte D, Tehranipoor M. Leveraging side-channel information for disassembly and security. ACM Journal on Emerging Technologies in Computing Systems (JETC). 2019 Dec 18;16(1):1-21.

[174] Qiu H, Dong T, Zhang T, Lu J, Memmi G, Qiu M. Adversarial attacks against network intrusion detection in IoT systems. IEEE Internet of Things Journal. 2020 Dec 30;8(13):10327-35.

[175] Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS. A survey on sensor-based threats and attacks to smart devices and applications. IEEE Communications Surveys & Tutorials. 2021 Mar 8;23(2):1125-59.

[176] Niroumand FJ, Bonab PA, Sargolzaei A. Security of Connected and Autonomous Vehicles: A Review of Attacks and Mitigation Strategies. SoutheastCon 2024. 2024 Mar 15:1197-204.

[177] Liu H, Wang Y, Liu J, Yang J, Chen Y, Poor HV. Authenticating users through fine-grained channel information. IEEE Transactions on Mobile Computing. 2017 Jun 22;17(2):251-64.

[178] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[179] Sultana R, Hussain M. Mitigating primary user emulation attack in cognitive radio network using localization and variance detection. InProceedings of First International Conference on Smart System, Innovations and Computing: SSIC 2017, Jaipur, India 2018 (pp. 433-444). Springer Singapore.

[180] Piran MJ, Pham QV, Islam SR, Cho S, Bae B, Suh DY, Han Z. Multimedia communication over cognitive radio networks from QoS/QoE perspective: A comprehensive survey. Journal of Network and Computer Applications. 2020 Dec 15;172:102759.

[181] Ding G, Jiao Y, Wang J, Zou Y, Wu Q, Yao YD, Hanzo L. Spectrum inference in cognitive radio networks: Algorithms and applications. IEEE Communications Surveys & Tutorials. 2017 Sep 11;20(1):150-82.

[182] Zeng Y, Xu L, Yang X, Yi X, Khalil I. Lightweight privacy preservation for secondary users in cognitive radio networks. Journal of Network and Computer Applications. 2020 Jul 15;162:102652.

[183] Veksler VD, Buchler N, Hoffman BE, Cassenti DN, Sample C, Sugrim S. Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. Frontiers in psychology. 2018 May 15;9:691.

[184] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31;47(6).

[185] Bou-Harb E, Ghani N, Erradi A, Shaban K. Passive inference of attacks on CPS communication protocols. Journal of information security and applications. 2018 Dec 1;43:110-22.

[186] Luo Z, Zhao S, Lu Z, Xu J, Sagduyu YE. When attackers meet AI: Learning-empowered attacks in cooperative spectrum sensing. IEEE Transactions on Mobile Computing. 2020 Oct 12;21(5):1892-908.

[187] Park S, Matic A, Garg K, Oliver N. When simpler data does not imply less information: A study of user profiling scenarios with constrained view of mobile HTTP (S) traffic. ACM Transactions on the Web (TWEB). 2018 Jan 27;12(2):1-23.

[188] Wang Q, Sun H, Hu RQ, Bhuyan A. When machine learning meets spectrum sharing security: Methodologies and challenges. IEEE Open Journal of the Communications Society. 2022 Jan 26;3:176-208.

[189] Hamamreh JM, Furqan HM, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2018 Oct 25;21(2):1773-828.

[190] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[191] Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the internet of things: a comprehensive review. Sensors. 2023 Apr 19;23(8):4117.

[192] Hallyburton RS, Hunt D, Luo S, Pajic M. A Multi-Agent Security Testbed for the Analysis of Attacks and Defenses in Collaborative Sensor Fusion. arXiv preprint arXiv:2401.09387. 2024 Jan 17.

[193] Wen Y, Liu L, Li J, Li Y, Wang K, Yu S, Guizani M. Covert Communications Aided by Cooperative Jamming in Overlay Cognitive Radio Networks. IEEE Transactions on Mobile Computing. 2024 Jun 26.

[194] Qu K, Ye J, Li X, Guo S. Privacy and Security in Ubiquitous Integrated Sensing and Communication: Threats, Challenges and Future Directions. IEEE Internet of Things Magazine. 2024 Jun 27;7(4):52-8.

[195] Alkaeed M, Qayyum A, Qadir J. Privacy preservation in Artificial Intelligence and Extended Reality (AI-XR) metaverses: A survey. Journal of Network and Computer Applications. 2024 Aug 2:103989.

[196] Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, Abduljaleel IQ. A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. Plos one. 2024 Apr 25;19(4):e0301277.

[197] Liu J, Zhang C, Lorenzo B, Fang Y. DPavatar: A real-time location protection framework for incumbent users in cognitive radio networks. IEEE Transactions on Mobile Computing. 2019 Feb 5;19(3):552-65.

[198] Balakumar D, Nandakumar S. Cognitive Radio Spectrum Sensing-Based QAM Technique Using Blockchain. International Journal of Distributed Sensor Networks. 2023;2023(1):7225260.

[199] Zhu R, Xu L, Zeng Y, Yi X. Lightweight Privacy Preservation for Securing Large-Scale Database-Driven Cognitive Radio Networks with Location Verification. Security and Communication Networks. 2019;2019(1):9126376.

[200] Balakumar D, Sendrayan N. Enhance the Probability of Detection of Cooperative Spectrum Sensing in Cognitive Radio Networks Using Blockchain Technology. Journal of Electrical and Computer Engineering. 2023;2023(1):8920243.

[201] Givehchian H, Bhaskar N, Redding A, Zhao H, Schulman A, Bharadia D. Practical obfuscation of BLE physical-layer fingerprints on mobile devices. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 2867-2885). IEEE.

[202] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[203] Zheng M, Liang W, Yu H, Sharif H. Utility-based opportunistic spectrum access for cognitive radio sensor networks: joint spectrum sensing and random access control. IET Communications. 2016 Jun;10(9):1044-52.

[204] Zhang C, Zhu L, Xu C, Du X, Guizani M. A privacy-preserving traffic monitoring scheme via vehicular crowdsourcing. Sensors. 2019 Mar 13;19(6):1274.

[205] Yang J, Lim H. Deep learning approach for detecting malicious activities over encrypted secure channels. IEEE Access. 2021 Mar 9;9:39229-44.

[206] Zeng Y, Xu L, Yang X, Yi X, Khalil I. Privacy-preserving aggregation for cooperative spectrum sensing. Journal of Network and Computer Applications. 2019 Aug 15;140:54-64.

[207] Goyat R, Kumar G, Saha R, Conti M. Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities. Cluster Computing. 2024 Jul;27(4):4823-39.

[208] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11;10:26257-70.

[209] Ye J, Kang X, Liang YC, Sun S. A trust-centric privacy-preserving blockchain for dynamic spectrum management in IoT networks. IEEE Internet of Things Journal. 2022 Jan 13;9(15):13263-78.

[210] Gadotti A, Rocher L, Houssiau F, Creţu AM, de Montjoye YA. Anonymization: The imperfect science of using data while preserving privacy. Science Advances. 2024 Jul 17;10(29):eadn7053.

[211] Zhu R, Boukerche A, Long L, Yang Q. Design Guidelines on Trust Management for Underwater Wireless Sensor Networks. IEEE Communications Surveys & Tutorials. 2024 Apr 16.

[212] Tyagi AK, Nair MM, Niladhuri S, Abraham A. Security, privacy research issues in various computing platforms: A survey and the road ahead. Journal of Information Assurance & Security. 2020 Jan 1;15(1).

[213] Rao PM, Deebak BD. Security and privacy issues in smart cities/industries: technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing. 2023 Aug;14(8):10517-53.

[214] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[215] Pöpper C, Batina L. Applied Cryptography and Network Security. InProceedings of the 22nd International Conference, ACNS 2024.

[216] Kumar A, Jayakody DN, Upadhyay RK. Secure and Reliable IoT Communication in Underlay CRN With Imperfect CSI. IEEE Internet of Things Journal. 2024 Mar 1.

[217] Heinl MP, Pursche M, Puch N, Peters SN, Giehl A. From Standard to Practice: Towards ISA/IEC 62443-Conform Public Key Infrastructures. InInternational Conference on Computer Safety, Reliability, and Security 2023 Sep 11 (pp. 196-210). Cham: Springer Nature Switzerland.

[218] Shewajo FA, Boualouache A, Senouci SM, El-Korbi I, Brik B, Fante KA. Integrating Blockchain Technology with PKI for Secure and Interoperable Communication in 5G and Beyond Vehicular Networks. In2024 IEEE 21st Consumer Communications & Networking Conference (CCNC) 2024 Jan 6 (pp. 998-1001). IEEE.

[219] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[220] Sucasas V, Althunibat S, Radwan A, Marques H, Rodriguez J, Vahid S, Tafazolli R, Granelli F. Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks. Security and Communication networks. 2015 Dec;8(18):3978-94.

[221] Soundararajan S, Nithya B, Nithya N, Vignesh T. Block chain espoused adaptive multi-scale dual attention network with quaternion fractional order meixner moments encryption for cyber security in wireless communication network. Wireless Networks. 2024 Feb 21:1-7.

[222] Tsantikidou K, Sklavos N. Threats, Attacks, and cryptography frameworks of cybersecurity in critical infrastructures. Cryptography. 2024 Feb 25;8(1):7.

[223] Sirajuddin M, Ravela C, Krishna SR, Ahamed SK, Basha SK, Basha NM. A Secure Framework based On Hybrid Cryptographic Scheme and Trusted Routing to Enhance the QoS of a WSN. Engineering, Technology & Applied Science Research. 2024 Aug 1;14(4):15711-6.

[224] Miao L, Di X, Huo ZM, Sun ZX. Research on spectrum sensing data falsification attack detection algorithm in cognitive Internet of Things. Telecommunication Systems. 2022 Jun;80(2):227-38.

[225] Akhtar SI, Rauf A, Amjad MF, Batool I. Inter-Cloud Data Security Framework to Build Trust Based on Compliance with Controls. IET Information Security. 2024;2024(1):6565102.

[226] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec;39(10):e13126.

[227] You X, Hou F, Chiclana F. A reputation-based trust evaluation model in group decision-making framework. Information Fusion. 2024 Mar 1;103:102082.

[228] Ullah F, Salam A, Amin F, Khan IA, Ahmed J, Zaib SA, Choi GS. Deep Trust: A Novel Framework for Dynamic Trust and Reputation Management in the Internet of Things (IoT) Based Networks. IEEE Access. 2024 Jun 4.

[229] Hosseinnezhad M, Azgomi MA, Dishabi MR. A probabilistic trust model for cloud services using Bayesian networks. Soft Computing. 2024 Jan;28(1):509-26.

[230] Abdalzaher MS, Seddik K, Elsabrouty M, Muta O, Furukawa H, Abdel-Rahman A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. Sensors. 2016 Jun 29;16(7):1003.

[231] Javed S, Sajid A, Kiren T, Khan IU, Dewi C, Cauteruccio F, Christanto HJ. A subjective logical framework-based trust model for wormhole attack detection and mitigation in Low-Power and Lossy (RPL) IoT-Networks. Information. 2023 Aug 29;14(9):478.

[232] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[233] Zhang K, Zhang Y, Sun R, Tsai PW, Hassan MU, Yuan X, Xue M, Chen J. Bounded and unbiased composite differential privacy. In2024 IEEE Symposium on Security and Privacy (SP) 2024 May 19 (pp. 972-990). IEEE.

[234] Rahman MH, Mowla MM, Shanto S. Differential privacy enabled deep neural networks for wireless resource management. Mobile Networks and Applications. 2022 Oct;27(5):2153-62.

[235] Su G, Wang J, Xu X, Wang Y, Wang C. The Utilization of Homomorphic Encryption Technology Grounded on Artificial Intelligence for Privacy Preservation. International Journal of Computer Science and Information Technology. 2024 Mar 13;2(1):52-8.

[236] Zhang M, Wang L, Zhang X, Wang Y, Sun W. Fully Privacy-Preserving and Efficient Clustering Scheme based on Fully Homomorphic Encryption. InICC 2024-IEEE International Conference on Communications 2024 Jun 9 (pp. 2694-2700). IEEE.

[237] Vo V, Dayaratne T, Haydon B, Yuan X, Lai S, Abuadbba S, Suzuki H, Rudolph C. Security and Privacy of 6G Federated Learning-enabled Dynamic Spectrum Sharing. arXiv preprint arXiv:2406.12330. 2024 Jun 18.

[238] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[239] Thirumalaisamy M, Basheer S, Selvarajan S, Althubiti SA, Alenezi F, Srivastava G, Lin JC. Interaction of secure cloud network and crowd computing for smart city data obfuscation. Sensors. 2022 Sep 21;22(19):7169.

[240] Pillai SE, Polimetla K. Enhancing Network Privacy through Secure Multi-Party Computation in Cloud Environments. In2024 International Conference on Integrated Circuits and Communication Systems (ICICACS) 2024 Feb 23 (pp. 1-6). IEEE.

[241] Agnew D, Boamah S, Bretas A, McNair J. Network Security Challenges and Countermeasures for Software-Defined Smart Grids: A Survey. Smart Cities. 2024 Aug 2;7(4):2131-81.

[242] Caso G, Alay Ö, Ferrante GC, De Nardis L, Di Benedetto MG, Brunstrom A. User-centric radio access technology selection: A survey of game theory models and multi-agent learning algorithms. IEEE Access. 2021 Jun 7;9:84417-64.

[243] Thangjam S, Kumar N, Kumar S. A Survey on Prevention of the Falsification Attacks on Cognitive Radio Networks. InIOP Conference Series: Materials Science and Engineering 2021 (Vol. 1033, No. 1, p. 012021). IOP Publishing.

[244] Mohammed MA, Hussain MA, Oraibi ZA, Abduljabbar ZA, Nyangaresi VO. Secure Content Based Image Retrieval System Using Deep Learning. J. Basrah Res.(Sci.). 2023 Dec 30;49(2):94-111.

[245] Subbulakshmi P, Prakash M, Ramalakshmi V. Honest auction based spectrum assignment and exploiting spectrum sensing data falsification attack using stochastic game theory in wireless cognitive radio network. Wireless Personal Communications. 2018 Sep;102:799-816.

[246] Muhammed D, Anisi MH, Zareei M, Vargas-Rosales C, Khan A. Game theory-based cooperation for underwater acoustic sensor networks: Taxonomy, review, research challenges and directions. Sensors. 2018 Feb 1;18(2):425.

[247] Dasari VS, Kantarci B, Pouryazdan M, Foschini L, Girolami M. Game theory in mobile crowdsensing: A comprehensive survey. Sensors. 2020 Apr 6;20(7):2055.

[248] Khan NA. PKI-Based security enhancement for IoT in 5G networks. InInventive Computation and Information Technologies: Proceedings of ICICIT 2021 2022 Jan 18 (pp. 217-225). Singapore: Springer Nature Singapore.

[249] Yan S, Wang X, Xu L. Rollout algorithm for light-weight physical-layer authentication in cognitive radio networks. IET Communications. 2020 Nov;14(18):3128-34.

[250] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9;3(5):364.

[251] Luo X. Secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks. IEEE Access. 2020 Jul 20;8:131361-9.

[252] Mannix K, Gorey A, O'Shea D, Newe T. Sensor network environments: A review of the attacks and trust management models for securing them. Journal of Sensor and Actuator Networks. 2022 Aug 8;11(3):43.

[253] Xue W, Shen Y, Luo C, Xu W, Hu W, Seneviratne A. A differential privacy-based classification system for edge computing in IoT. Computer Communications. 2022 Jan 15;182:117-28.

[254] Li S, Zhao S, Min G, Qi L, Liu G. Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things. IEEE Internet of Things Journal. 2021 Mar 24;9(16):14542-50.

[255] Tran TT, Kong HY. Exploitation of spatial diversity in a novel cooperative spectrum sharing method based on PAM and modified PAM modulation. Journal of Communications and Networks. 2014 Jun;16(3):280-92.

[256] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InApplied Cryptography in Computer and Communications: Second EAI International Conference, AC3 2022, Virtual Event, May 14-15, 2022, Proceedings 2022 Oct 6 (pp. 46-64). Cham: Springer Nature Switzerland.

[257] Poonam, Nagpal CK. A game theory based solution for security challenges in CRNs. 3D Research. 2018 Mar;9:1-24.

[258] Mian NA. Role of Game Theory in Utilizing the Spectrum in Cognitive Radio Networks. Journal of Computing & Biomedical Informatics. 2024 Jun 1;7(01):654-65.

[259] Awin FA, Alginahi YM, Abdel-Raheem E, Tepe K. Technical issues on cognitive radio-based Internet of Things systems: A survey. IEEE access. 2019 Jul 19;7:97887-908.

[260] Kokkinen H, Järvenpää M, Peltotalo S, Reis–Kivinen A. Experiment of Dynamic Spectrum Management for 5G Drone-Based Tactical Bubble. In2024 International Conference on Military Communication and Information Systems (ICMCIS) 2024 Apr 23 (pp. 01-10). IEEE.

[261] Zhou Q, Niu Y. From Adaptive Communication Anti-Jamming to Intelligent Communication Anti-Jamming: 50 Years of Evolution. Advanced Intelligent Systems. 2024:2300853.

[262] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[263] Vaduganathan L, Neware S, Falkowski-Gilski P, Divakarachari PB. Spectrum Sensing Based on Hybrid Spectrum Handoff in Cognitive Radio Networks. Entropy. 2023 Aug 31;25(9):1285.

[264] Xu C, Lu R, Wang H, Zhu L, Huang C. PAVS: A new privacy-preserving data aggregation scheme for vehicle sensing systems. Sensors. 2017 Mar 3;17(3):500.

[265] Alonso RM, Plets D, Deruyck M, Martens L, Nieto GG, Joseph W. Multi-objective optimization of cognitive radio networks. Computer Networks. 2021 Jan 15;184:107651.

[266] AlMarshoud M, Sabir Kiraz M, H. Al-Bayatti A. Security, privacy, and decentralized trust management in VANETs: a review of current research and future directions. ACM Computing Surveys. 2024 Jun 22;56(10):1-39.

[267] Lu Z, Qu G, Liu Z. A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems. 2018 Apr 23;20(2):760-76.

[268] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec;11(4):66.

[269] Alghamdi A, Al Shahrani AM, AlYami SS, Khan IR, Sri PA, Dutta P, Rizwan A, Venkatareddy P. Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network. Wireless Networks. 2024 Aug;30(6):5851-66.

[270] Prasad R. Enhanced energy efficient secure routing protocol for mobile ad-hoc network. Global Transitions Proceedings. 2022 Nov 1;3(2):412-23.

[271] Islam MN, Kundu S. IoT security, privacy and trust in home-sharing economy via blockchain. Blockchain Cybersecurity, Trust and Privacy. 2020:33-50.

[272] Blanc G, Kheir N, Ayed D, Lefebvre V, de Oca EM, Bisson P. Towards a 5G security architecture: Articulating software-defined security and security as a service. InProceedings of the 13th International Conference on Availability, Reliability and Security 2018 Aug 27 (pp. 1-8).

[273] Singh J, Wazid M, Das AK, Chamola V, Guizani M. Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey. Computer Communications. 2022 Aug 1;192:316-31.

[274] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[275] Rosenberg I, Shabtai A, Elovici Y, Rokach L. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR). 2021 May 23;54(5):1-36.

[276] Buchanan W, Woodward A. Will quantum computers be the end of public key encryption?. Journal of Cyber Security Technology. 2017 Jan 2;1(1):1-22.

[277] Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, Leichenauer S, Hidary J, Venables P, Hansen R. Transitioning organizations to post-quantum cryptography. Nature. 2022 May 12;605(7909):237-43.

[278] Grote O, Ahrens A, Benavente-Peces C. A review of post-quantum cryptography and crypto-agility strategies. In2019 International Interdisciplinary PhD Workshop (IIPhDW) 2019 May 15 (pp. 115-120). IEEE.

[279] Käppler SA, Schneider B. Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. Proceedings of the Society. 2022 Jun 20;84:61-71.

[280] Satybaldy A, Nowostawski M. Review of techniques for privacy-preserving blockchain systems. InProceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure 2020 Oct 6 (pp. 1-9).