Multimedia Tools and Applications (2024) 83:32715–32738
https://doi.org/10.1007/s11042-023-16642-w

A comprehensive survey of security threats, detection, countermeasures, and future directions for physical and network layers in cognitive radio networks

Pooja Ahuja[1] · Preeti Sethi[1] · Naresh Chauhan[1]

Received: 5 July 2022 / Revised: 12 May 2023 / Accepted: 23 August 2023 /
Published online: 23 September 2023

Abstract
Cognitive radio is providing the solution to the challenges of spectrum scarcity. The central idea behind this technology is to use spectrum without interfering with the rights of primary users, allowing multiple users to use the spectrum at the same time. Thus, the goals are to avoid high-cost spectrum resetting and improving overall spectrum utilization. This technology brings the TCP/IP protocol stack's Physical, Data Link, and Network Layers up to date with reference to Cognitive radio technology. Furthermore, due to the dynamic nature of cognitive radio Networks, these can be easily physically or mentally hurt, influenced, or attacked: to a slew of new security flaws. We concentrated on various attacks that target the Physical, Medium Access Control, and Network layers in this paper. A comparison of current defenses against outside and inside attacks is also included, as is a discussion of the current detection mechanisms and their countermeasures. Moreover, the systematic review is conducted to look into various attack vectors or malicious activities that may degrade the performance of cognitive radio networks. In addition to this, various paper discusses various recent tools and techniques that can be used to diagnose potential threats on wireless ecosystem. This survey also highlights the fundamental security challenges for cognitive radio networks.

Keywords Cognitive radio · Data Link · Radio networks · Spectrum scarcity · Network

1 Introduction

People are ready to access information and services whenever they want and from any location thanks to the fast development of mobile and wireless devices. Thus, there lies a greater tendency to adopt a human-centric perspective, which calls for more effective and prompt communication.

✉ Pooja Ahuja
ahujap316@gmail.com

[1] Department of Computer Engineering, J.C. BOSE University of Science and Technology, YMCA, Faridabad, Haryana, India

Additionally, in the ensuing decades, an immense number of smart terminals will have access to the internet, and the IoT (Internet of Thing) and other linked and wireless devices will produce additional data. This will result in increased Network congestion and an unequal distribution of resources since the ISM (Industrial, Scientific and Medical Network) band, which is unlicensed and free, would become congested. The static spectrum allocation method won't be able to keep up with the rising demand for spectrum resources as a result. Consequently, a need for the new dynamic spectrum utilization that has more coverage, capacity, and connectivity.

According to the FCC (Federal Communications Commission) survey, a significant number of spectrum resources have varying degrees of idealness in terms of time and space dimensions due to the static spectrum allocation strategy [1].

Traditional methods for utilizing licensed spectrum include multiplexing techniques like FDMA, TDMA, CDMA, and MIMO, which allow additional users but cannot address the issue of spectrum scarcity [2]. (Mitola & Maguire,1999) developed and initially coined the term, "Cognitive Radio" [3], in this context, while later described it as, "*an intelligent wireless communication system which is capable to monitor usage of the neighboring spectrum and exploiting the idle spectrum without impacting the ongoing transmission*" [4]. According to the FCC, Primary Users are licensed and non-licensed users known as Cognitive\ Secondary Users. Additionally, these secondary users have the capacity to sense whether a spectrum is vacant and instantly leave it when a Primary User attempts to access it again. Furthermore, the capacity for reconfiguration aids in adjusting in accordance with the findings of spectrum sensing.

The cross-layer design that Cognitive Radio Network uses also allows them to carry out their primary tasks of Spectrum Sharing & sensing to improve spectrum efficiency. More specifically, the application layer is in charge of handling the application Quality of Service needs, whereas the transport and Network layers are in charge of routing and reconfiguring the Networks, respectively. Furthermore, the Physical and Data Link layers [5, 6] carry out spectrum detection and sharing.

Every tier in the aforementioned TCP/IP protocol stack's functions for Cognitive Radio Network is vulnerable to different kinds of security risks. Due to their dynamic character, which could negatively interfere with regular operations, Cognitive Radio network are more susceptible to cyberattacks [8]. The many vulnerabilities, assaults, and defenses aimed at the various Cognitive radio Network tiers are covered in-depth in this article. Furthermore, some of these assaults are novel because to the peculiar characteristics of Cognitive radio Network, while others have been carried over from conventional wireless Networks. This article provides a comprehensive survey of various attacks encountered on different layers of TCP/IP protocol stacks for Cognitive Radio networks. The classification of attacks is performed on the basis of different layers like Physical layer attacks in CRN include Primary emulation user, Objective function, overlapping secondary user and jamming attacks [9–11]. Likewise, the attacks targeted on MAC layers are as control channel saturation, control channel jamming and spectrum sensing data falsification attacks [12]. Similarly, attacks targeted on network layer are host addressing attacks, IP datagram fragmentation attacks and Routing attacks [13, 14].

This article describes numerous risks that fall within the categories of internal and external attacks. Additionally, inside assaults are those that are launched by unauthorized people, who may be trusted or untrusted. Additionally, an intrusive party can break secrecy by making outside attacks. Several researchers have proposed various threat detection algorithms over computer networks in order to improve customer confidentiality and service availability. Below Table 1 shows the relevant abbreviations used.

Table 1 Relevant abbreviations

CRN	Cognitive Radio Network
SU	Secondary/Cognitive Users
PL	Physical Layer
PU	Primary Users
SSDF	Spectrum Sensing Data Falsification
NWL	Network Layer
SS	Spectrum Sensing
QoS	Quality of Service
PUE	Primary User Emulation
DOS	Denial of Service
MAC	Medium Access Control
NW	Network
SS	Spectrum Sharing

The paper has seven sections. In Section 2, we investigate how assaults in Cognitive radio Network target Physical and Data Link layers, in Section 3, we examine attacks aimed at Cognitive radio Network's Network layers. We examine several assaults detections and their countermeasures in Section 4. In Sections 5 and 6, we contrast a number of currently proposed mechanisms for defending against both Outsider & Insider threats respectively. We conclude with a succinct summary and recommendations for the future. In addition to this organization of this paper with brief description of various attacks encountered in different layers with their counter measures is shown below in Fig. 1.

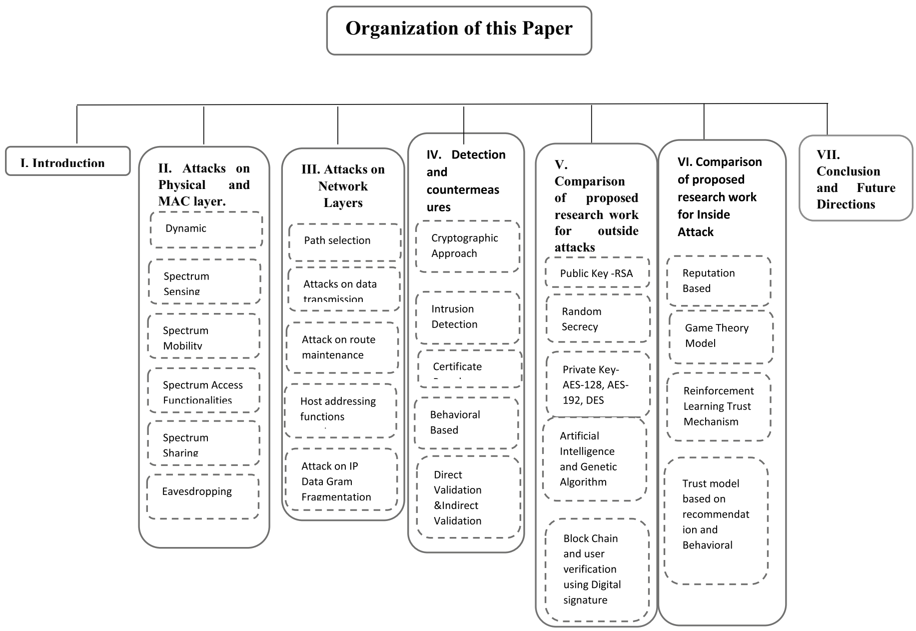

Fig. 1 Organization of this paper

2 Attacks on the Physical and MAC Layers

The Physical Layer is in charge of sending bit streams from sender to receiver. The Physical Layer is responsible for modulation, signal detection, and frequency selection. The channel is accessed and controlled above its media access control layer [8, 8]. It includes spectrum detection, spectrum sharing, spectrum access, spectrum decision-making, and spectrum mobility. In the case of CRN, the MAC protocol is designed differently because it must sense the radio environment and configure accordingly. These, like any other layer, are vulnerable easily to variety of attacks. Because the functionalities of the physical and media access control layers overlap, they either directly or indirectly affect each other. As a result, any harmful activity related to the PL has an impact on the functioning of the MAC and vice versa. Due to the sheer dynamic nature of spectrum access, it is vulnerable to eavesdropping, belief manipulation attacks, malicious traffic injection, and attacks on various spectrum e.g., access, sensing, allocation, and sharing functionality [9]. Attacks in each of the preceding categories are further classified as Dynamic Spectrum, Belief Manipulation, Eavesdropping, Spectrum Sensing, Spectrum sharing and Malicious Traffic Injections. Attacks on Physical and MAC Layer is shown in below Fig. 2.

2.1 Physical and Link-Layer attacks

Attacks in each of the preceding categories are further classified as Dynamic Spectrum, Belief Manipulation, Eavesdropping, Spectrum Sensing, Spectrum sharing and Malicious Traffic Injections.

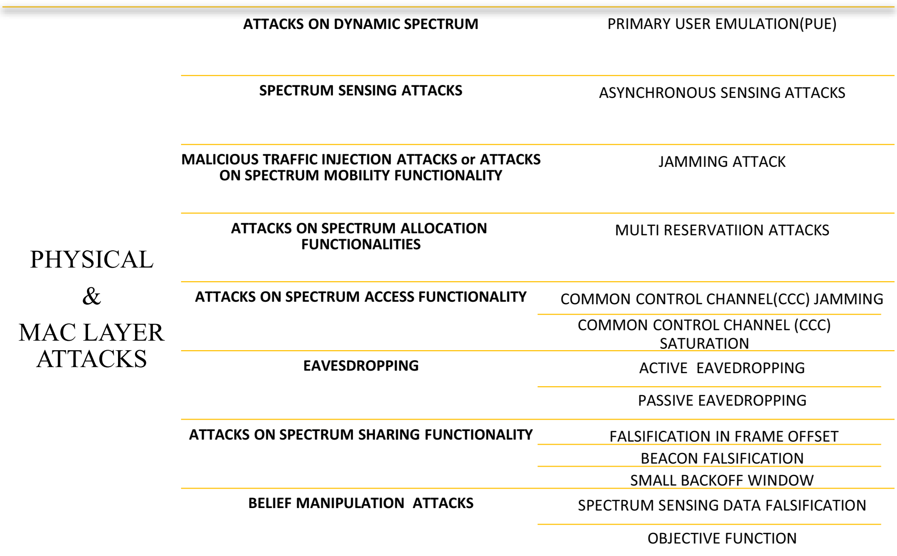

Fig. 2 Attacks on Physical and MAC Layer

a. ***Spectrum Dynamic Nature Attacks***

These attacks are designed to prevent the SU from dynamically accessing available spectrum holes. Primary User Emulation is a well-known example of this type of attack (PUE).

b. ***Primary User Emulation***

A primary user attack is a serious threat in which a malicious or selfish user imitates the PU signal in order to prevent SU from gaining access to the free channel. This kind of attack disrupts PU, trying to prevent it from using the PU channel and compelled it to vacate it on a regular basis [11]. These attacks are typically carried out by malicious or self-interested users, and they have a significant impact on spectrum sensing attacks. These types of attacks can be detected using techniques such as spectrum sensing, belief propagation method, data and feature-based, intrusion detection system, learning-based, and compressive sensing. Avoiding PUE attacks requires the use of cryptographic, game theory, or a combination of the two [13–17].

c. ***Belief Manipulation Attack***

These attacks are carried out in a cooperative environment in which the malicious user manipulates radio parameters, resulting in incorrect decision making. The most common attacks in this category are spectrum sensing data falsification and objective function manipulation attacks.

d. ***Spectrum Sensing Data Falsification (SSDF)***

SSDF is also known as a Byzantine attack. It is similar to cooperative spectrum sensing, in which multiple Sus work together to detect a frequency band. Furthermore, these malicious users provide false spectrum sensing results in order to gain control and degrade network performance. These types of attacks increase the possibility of false signaling [18].

Methods such as user reputation, onion peeling, and data mining can be used to detect SSDF attacks. SSDF attacks can be avoided by employing metrics based on reputation or trust [19].

e. ***Objective Function Manipulation Attack***

An objective Function attack is carried out by adjusting the radio parameters required to calculate the objective function, such as bandwidth, modulation type, frame size, coding rate, power, frequency, and so on. These attacks are detected using Optimization, Intrusion Detection Scheme, Alarms, and Voting Based Algorithm [20].

f. ***Eavesdropping***

In the wireless scenario, an attacker can fine-tune their receiver to the proper frequency to capture signals disseminated by legitimate users, overhear the information transmission, and inject the unwanted message into the network [21]. These attacks can be carried out on either the network or physical layers [22–24].

Eavesdropping attacks are classified as either active or passive. In passive eavesdropping attacks, the intruder overhears sensitive information and reacts or creates a false identity. A Passive eavesdropper, on the other hand, only acts as a spy [25].

Cryptographic solutions are typically used to combat eavesdropping attacks [26]. Furthermore, according to recent research, passive eavesdropping attacks can be detected by a device known as ghostbuster, which can detect leak signals during ongoing transmission and also aid in the detection of hidden presence in the network [27].

Eavesdropping attacks can be avoided by employing relay-based techniques, artificial noise injection, spoofing-based techniques, and multi-antenna-based security-oriented beamforming techniques [28, 29].

g. ***Malicious Traffic Injection***

This type of attack involves inserting unwanted messages into the network, causing congestion. A jamming attack is an example of a malicious traffic injection attack. In these attacks, malicious users continuously broadcast high-energy signals to obstruct legitimate users and force them to receive unwanted packets that consume a lot of bandwidth, resulting in network denial of service (DOS) [30, 31].

3 Attacks targeting network layer

Furthermore, the network layer functionalities are the same in traditional and cognitive radio networks. Routing is the fundamental function of the network layer, which is further subdivided into three major processes: path determination, data packet forwarding, and route maintenance [38]. Furthermore, in a Cognitive radio network, nodes involved in data packet forwarding from source to destination must monitor PU activity and vacate the channel as soon as a PU is detected [39]. As a result, these new specifications open the door to new types of security threats. Furthermore, the classification of network layer attacks is linked to its responsibility, such as attacks on routing functions, host addressing attacks, and data packet forwarding attacks. Figure 3 shows the classification of each type of attack.

3.1 Attacks targeting the routing functions

Routing attacks occur during path determination from source to destination, packet forwarding, or route maintenance.

a. ***Path Selection Attacks***

During the path discovery process, the source must determine the best route to the destination. CRN's metric for this differs from that of other wireless networks in that it includes information about spectrum availability and route stability [38].

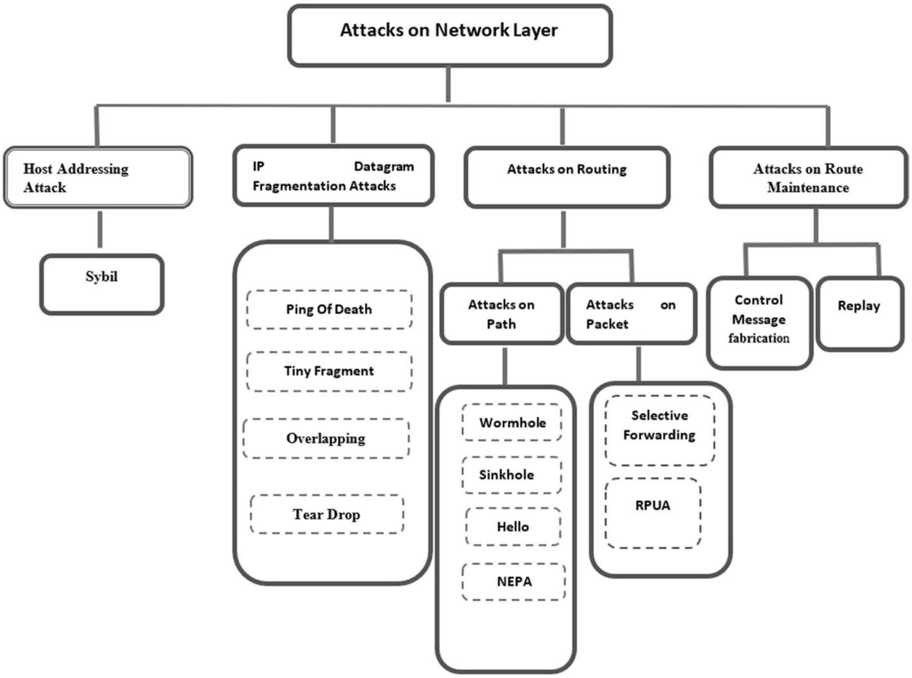

Fig. 3 Network layer attacks

In this attack, the attacker's goal is to modify the new metric so that it is more likely to be part of the route to the specific destination.

b. ***Wormhole***

The attacker records the RREQ packet at any point and sends it to another conspiring attacker at any point in the network in the wormhole attack. Furthermore, the attacker's modified RREQ packet should reach the destination first. As a result, the first receive RREQ packet is accepted and the remaining genuine packets are ignored. The primary goal of the wormhole attack is to have the RREQ packet arrive at the destination faster [40].

c. ***Sinkhole***

In this type of attack, the malicious user poses as the finest node to forward the packet to its intended destination. Furthermore, it manipulates the RREQ packet and convinces the source node that the compromised node is the best node to take to the destination [41].

d. ***Hello Flood Attack***

In this attack, the attacker broadcasts a high-powered hello packet, misguiding the Sus about the malicious node's position as a neighbor. As a result, nodes begin sending data packets to the attacker, resulting in packet loss [42].

e. ***Network Endo Parasite Attack (NEPA)& Low-Cost Ripple Effect Attack (LORA)***

This type of attack causes more interference on a busy high priority channel. Furthermore, in this type of attack, the malicious node misleads its neighbor by indicating that it has switched to a different channel when, in fact, its channel has not changed.

3.2 Data forwarding attacks

Data forwarding attacks, once's the attacker has gained access to the route to the destination, it can disturb the process of data forwarding by selectively dropping packets or increasing delay in packet transfer.

a. ***Routing towards Primary User Attack***

The routing protocol in CRN takes into account the availability of the channel that SU can use. As a result, the RPUA attacker deliberately forwards received packets to the SUs, which is closed to the PU potentially increasing packet transmission delay.

b. ***Selective Forwarding***

In this type of attack, the malicious user does not forward all received packets to their intended destination. Furthermore, this type of attack takes two forms: first, the attacker drops the packet coming from a specific node, resulting in denial of service (DOS) [43]. Second, the attacker discards packets from the arbitrary node. This type of selective forwarding attack is known as Neglect & Greed.

c. ***Route Maintenance Attack***

Nodes are used to keep track of the active path during route maintenance by sending HELLO and RERR messages. Furthermore, each node broadcasts the HELLO message on a regular basis to notify other nodes of its presence. When the destination is unreachable, RERR is displayed [44].

d. ***Control Message Fabrication Attack***

In this type of attack, malicious nodes fabricate the control message, Hello and RERR, to trick the source node into thinking the route to the destination is no longer accessible.

e. ***Replay Attack***

Control message fabrication, also known as a replay attack, entails using an old control packet, such as HELLO and RERR, that was previously received at a specific time [45].

f. ***Attack on host addressing function***

Each node in the network is given a unique IP address by the host addressing function. In CRN, SU's cooperate with each other to accomplish tasks, such as determine a path to a specific destination, evaluating trust through collective recommendation from neighboring nodes in cooperative sensing of spectrum [46, 47]. The most common attack is Sybil attack. The Sybil attack can launch some attacks such as Spectrum Sensing Data Falsification (SSDF).

g. ***IP datagram Fragmentation Attack***

The fragmentation process allows the IP datagram to be broken down into small fragments for transmission across different types of networks. Furthermore, the sender fragments the IP datagram into tiny fragments, which are gather again at the destination to obtain the original IP datagram. As a result, the attack takes advantage of IP datagram functionality, and CRN, like any other wireless network, is vulnerable to attacks such as denial of service (DOS), which can lead to attacks such as the death ping or teardrop attacks. Furthermore, an attacker can use the IP datagram function to circumvent some node's filtering rules. This is accomplished through the use of either tiny fragment attacks or overlapping fragment attacks [48–51].

1. Death Ping Attack
2. Teardrop
3. Minor Fragment
4. Overlapping Fragment Attack

4 Detection and counter measure

To counter attacks at various layers, several detection techniques and countermeasures have been proposed in the literature. Furthermore, solutions to various attacks such as dynamic spectrum sensing, belief manipulation, eavesdropping, and jamming attacks were mostly found in the Physical and LINK layers. In addition to this, the routing mechanisms in CRN encounter various attacks that are more specific to a cognitive radio network. Furthermore, in the network layer, solutions for attacks on host addressing and IP fragmentation are proposed in the context of a traditional wireless network. To the best of our knowledge, a solution to the attacks encountered in the physical, MAC, and network layers in the context of CRN has been proposed, but there is still work to be done. Detection and Countermeasures is shown in below Fig. 4.

a. **TOOLS AND METHODS FOR DETECTING POTENTIAL THREATS**

Due to the exponential increase in internet-connected devices, the search for reliable, effective, and powerful security protection mechanisms has risen to the top of the priority list in academia and industry. This section discusses various tools and methods for identifying and diagnosing potential threats. For example, intrusion detection systems, machine learning-based mechanisms, bio-inspired optimization algorithms, and software-defined radios are all capable of being utilized to improve the overall security of the wireless ecosystem [66]. Tools and methods for detection of potential threats in Wireless Ecosystem is shown in below Fig. 5.

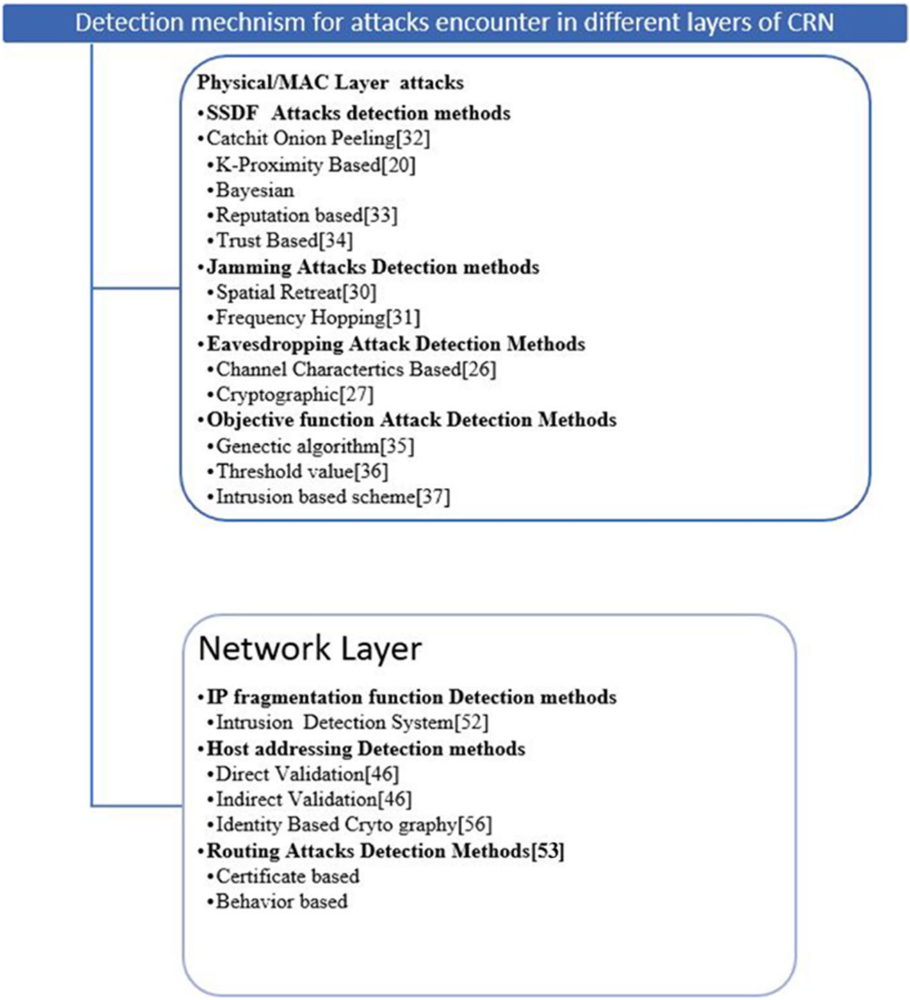

Fig. 4 Detection and Countermeasures

5 Comparison and discussion

Table 2 in the following section details various proposed work, the majority of which focuses on the security of CRN concerns to outside attacks. Outside attacks are primarily concerned with breaching data confidentiality and authentication. Data confidentiality ensures data protection and security from unauthorized access, and the data is transformed in such a way that it is inaccessible to unapproved malicious entities inside CRNs. Furthermore, authentication ensures that any communication between entities within the CRN architecture is authentic, ensuring that the data received from the assumed entity within CRNs is correct. The third and fourth columns provide a summary of the methodology and approach used to secure the network. The fifth column describes the attack that the proposed methodology protects against. The sixth column specifies whether the scheme is cooperative or non-cooperative. Furthermore, the last column specifies the additional

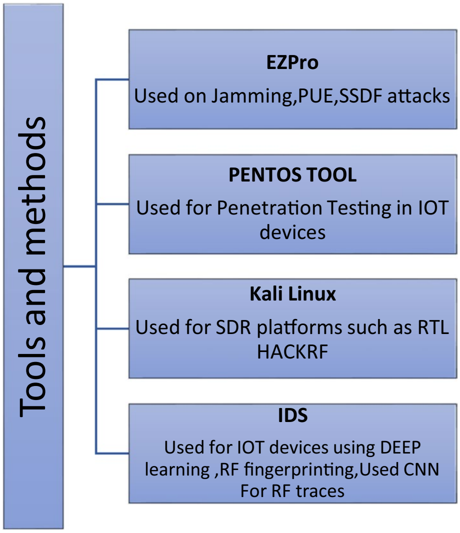

Fig. 5 Tools and methods for detection of potential threats in Wireless Ecosystem

security parameters such as energy consumption and QoS. Author [57] proposes using Random Secrecy Binning to secure communication with an untrusted SU. This technique aids in the defense against eavesdropping attacks. Researchers [58–65] proposed a framework for secure communication based on encryption techniques such as public key RSA, private key AES-128, AES-192, FH-DSA, and symmetric key.

Moreover, these framework helps to fight against attacks like Man in the Middle, DOS, SSDF, Byzantine attacks. Some researchers [66–68] uses the hybrid techniques based on Artificial Intelligence and Genetic Algorithm that helps to fight against the attacks such as Primary user Emulation, Spectrum sensing Data falsification.

6 Comparison of proposed research work preventing the inside attacks

Several authors proposed different mechanisms to protect against outside attacks in the previous section, including Eavesdropping, Man in the Middle, Primary User Emulation, False Alarming Rate, and many more [54–68]. Furthermore, this section focuses on attacks generated by malicious or selfish nodes within the cognitive radio network. Furthermore, cognitive radio networks are open and random-access networks in which unlicensed users can use channels not currently used by Pus. As a result, new security threats such as primary user emulation (PUE), SSDF, and a large number of unlicensed users have emerged, behaving maliciously and causing false alarms. Indeed, many researchers have proposed various methods for trusted communication in CRN, such as reputation-based methods for identifying malicious nodes and game-based methods for identifying malicious nodes. Stackelberg game theory, reinforcement learning trust model that intelligently detects attacks, omnipresent trust model based on recommendation and behavioral model, and other distributed models for evaluating trust by any peers without direct knowledge [59, 69–80]. Furthermore, Table 3 describes various proposed schemes for trusted communication, along with their advantages and disadvantages.

Table 2 Demonstrates various proposed work majorly focuses on the security related to Outside Attacks in CRN

Author Name	Proposed Work	Methodology Used	Encryption or other method used	Attack covered	Technique used	Parameter considered
Jeon 2014 [56]	Secured Communication with Untrusted Secondary Nodes In CRN	Using information-theoretic secrecy techniques, such as coding techniques for wiretap channels, the primary users can allow the secondary users to sense and relay the message while helping to keep the secondary users uninformed of the primary users' messages	Random secrecy binning	Eavesdropping	Cooperative and non-Cooperative	Secured and efficient
Hyun Sung Kim 2011 [57]	Location Based Authentication Protocol	This protocol uses location information as the secret credential and generates key by using public key cryptosystem and certificate for it	Public key encryption	Man in the middle attack	Cooperative	secured

Table 2 (continued)

Author Name	Proposed Work	Methodology Used	Encryption or other method used	Attack covered	Technique used	Parameter considered
Insoo Koo 2018 [58]	Transfer Learning Actor–Critic Algorithm	In this model SU itself interact with environment to learn the dynamics and accordingly decides to stay idle or transmit the data using suitable encryption methods. Encryption method is selected as per the energy level	Private key AES-128 AES-192	Eavesdropping, Reduction in sensing error and false alarming	Cooperative	Energy efficient and secure
Sazia Parvin 2012 [59]	Trust Oriented Digital Signature-Based Authentication Scheme	This framework ensures communication between trustworthy users in CRNs. Also possess features of public key encryption to detect various reply attacks	Public key cryptography RSA	Detection of malicious nodes, Avoid types of reply attacks	Cooperative	secured
S. Vimal 2018 [60]	Discrete-Time Partially Observed Markov Decision Process	This framework uses the private key encryption (AES) and ELCAT algorithm for energy detection and byzantine attack prediction	Private key encryption AES	Byzantine attack prediction	Cooperative	Energy efficient and secure

Table 2 (continued)

Author Name	Proposed Work	Methodology Used	Encryption or other method used	Attack covered	Technique used	Parameter considered
Xiaoyan Wang[2015] [61]	A Non-Monetary QOS-Aware Auction Framework for Secured CRN	This framework mutually formulates the optimal cooperator selection and the corresponding resource allocation problem by taking specific user's QOS into consideration. This is ensured by truthful bidding and auction is proposed by using dominant strategy equilibrium (DSE)		Eavesdropping	cooperative	Energy efficient, QOS and secured
Chao Zou [62]	Dynamic Spectrum Access-Based Cryptosystem For Cognitive Radio Networks	This framework proposes Group frequency hopping based key establishment dynamic spectrum access algorithm, a confidentiality-oriented DSA design based on FH-GKE	FH-DSA cryptosystem	Eavesdropping	Cooperative	Secured

Table 2 (continued)

Author Name	Proposed Work	Methodology Used	Encryption or other method used	Attack covered	Technique used	Parameter considered
Mahmoud Khasawneh2017 [63]	Secure and Efficient Authentication Mechanism Applied to Cognitive Radio Networks	This method uses 2 level authentication mechanism beforehand joining node gets access to network resources at different entities like in fusion center (FC) and Cluster Head (Ch) for making secure communication in CRN	Symmetric key cryptography	Denial of service, Man in the middle and reflection attack	cooperative	Secured and efficient
Sazia Parvin [2011] [64]	Digital Signature-Based Secure Communication in Cognitive Radio Networks	This framework proposed Markov chain-based trust-based model for analyzing trust value. They integrate trust and repudiation for threat of spectrum sensing data falsification (SSDF)	Digital signature possesses all features of public key encryption and trust evaluation also done	Eavesdropping, spectrum sensing data falsification	Cooperative	Secured
Do Vinh Quang [65]	Energy-Efficient Data Encryption Scheme For Cognitive Radio Networks	This framework uses partially observable Markov decision process which make decision at the beginning of slot to decide whether to stay silent or become active and encrypt data using opportune private key encryption	Private key encryption (AES)	Probability of false alarm detection is reduced, eavesdropping	cooperative	Secured and energy efficient

Table 2 (continued)

Author Name	Proposed Work	Methodology Used	Encryption or other method used	Attack covered	Technique used	Parameter considered
Sally M. Elghamrawy 2018 [66]	Defense Against Primary User Emulation Attacks Using Genetic Artificial Bee Colony (GABC) Algorithm	It proposes hybrid genetic artificial bee colony (GABC) to optimize the spectrum utilization by detecting PUE attacks and enhancing the probability of detection	Genetic artificial bee colony algorithm	Primary User emulation attack	Cooperative	Secured
K.B Shivakumar [67]	AI Based Algorithm & Framework for Efficient Pue Attack Detection Using Dual Classification Method in CRN	It uses deep learning convolution neural network, a rule-based classifier on FFT aggregated end signal at core	Core optimization method	Primary user emulation attack, reduction in false alarming	cooperative	Secured and efficient
Adnan Sajid [68]	Securing Cognitive Radio Networks Using Blockchains	It proposes block chain-based method for detection of malicious user (MU).MU are differentiated from reliable users through cryptographic keys	Blockchains and user verification is done by digital signature	Detection of malicious users, reduction in false alarming	Cooperative	Secured and energy efficient

Table 3 Demonstrates the proposed schemes for trusted communication

Available work	Principle of Proposed Work	Specialties (+) & Limitation (-)
Reputation-Based Cooperative Spectrum Sensing with Trusted Nodes Assistance [69]	Reputation based mechanism deals with Trust Node Assistance (TNA) and without TNA. This proposed work reveals that Cooperative spectrum sensing with TNA is more robust	(+) Identify misbehaving secondary nodes (+) Nullify their negative influences (-) Works well only when misbehaved CRs are small
A Robust Malicious User Detection Scheme in Cooperative Spectrum Sensing [70]	The proposed work uses spatial correlation of received signal strength among various secondary users which are close proximity. Moreover, it uses the robust outlier detection technique	(+) it uses the majority voting scheme among the various Secondary users for detection of malicious user (+) works well in large network size (-) performance is measured by considering the one PU with fixed location
ReDiSen: Reputation-based Secure Cooperative Sensing in Distributed Cognitive Radio Networks [71]	The proposed work uses the reputation-based method for identifying misbehaved nodes	(+) works well in large numbers of misbehavior nodes (+) uses proposed system with trusted node assistance (TNA) as well as without (TNA) (-) it only considered two types of misbehaving behavior Always busy (AB) and always free (AF)
An Adaptive Deviation-tolerant Secure Scheme for Distributed Cooperative Spectrum Sensing [72]	The proposed scheme lessens the misbehavior of inside malicious node and endures the large deviation presented by the honest node	(+) this scheme provides the mechanism to isolate the malicious node from network and allows the honest user with large deviation to be the part of overall decision making (-) unable to recognize the attack in random network topology
Trusted Collaborative Spectrum Sensing for Mobile Cognitive Radio Networks [73]	This scheme provides the location reliability information for path loss character tics and captures the Malicious intention of the secondary users	(+) in this scheme mobility plays important role in detection of malicious users and improve performance (-) how to detect a malicious node who changes its mobility and capable of hiding
Security management based on trust determination in cognitive radio networks [59]	In this scheme a centralized management is done by fusion center (FC). FC is responsible to authenticate the cognitive user and punish the defaulters	(+) It reduces computational load by incorporating a fusion center and a cluster head into a two-layer network hierarchical architecture (+) employs a centralized trust scheme (+) uses Grades of penalty mechanism (-) need to maintain the Nash equilibrium between cluster heads and network scale

Table 3 (continued)

Available work	Principle of Proposed Work	Specialties (+) & Limitation (-)
Energy-Efficient and Trust-aware Cooperation in Cognitive Radio Networks [74]	This scheme addresses the energy efficiency of PU and trustworthiness of SU. It uses the sequential decision procedure where PU acts as a leader and SU are followers, this is formulated through Stackelberg game theory	(+) maximize energy efficiency (+) facilitates secured transmission by assigning trust values (-) only works well in cooperative environment
A Reinforcement Learning-based Trust Model for Cluster Size Adjustment Scheme in Distributed Cognitive Radio Networks [75]	This scheme is based on reinforcement learning trust model and proposes single agent RL (SARL)based trust model for cluster size adjustment to recognize collaborative &intelligent attacks	(+) RL trust-based model adjusts the cluster size accordingly to increase the network scalability (-) In distributed network multi- cluster can be established and token can be shared among the cluster heads for optimal utilization of resources
Trust-based multi-hop cooperative spectrum sensing in cognitive radio networks [76]	This proposed scheme specifically deals with the spectrum sensing data falsification	(+) it uses the trust-based mechanism for the distributed cooperative spectrum sensing by considering the trust of the relay Sus (+) it seems that error rate of miss detection and false alarms have also been decreased (-) the proposed method imposes various overheads like memory overheads for maintaining the trust table and computational overheads for evaluation of overall trust value
Trust prediction and trust-based source routing in mobile ad hoc networks [77]	It uses the dynamic trust prediction model to evaluate trust worthiness of nodes by considering its historical behavior as well as its futuristic behavior via fuzzy logic rules	(+) proposed trust-based source routing protocol (TSR) ensures the flexible and feasible approach in finding the shortest route (+) TSR improves the PDR & reduces end to end latency (-) this routing protocol does not take QOS in to consideration while choosing route for real time applications
A Trust Game Model for the Cognitive Radio Networks [78]	This scheme proposes the trust-based game model for cooperative sensing spectrum to deal with malicious that launch the SSDF attacks	(+) trust-based mechanism used to detect the malicious node and penalty them (+) this model discourages the su from sending faulty sensing outcomes to the data fusion centers (-) this scheme only work well for recognizing the spectrum sensing attacks like SSDF

Table 3 (continued)

Available work	Principle of Proposed Work	Specialties (+) & Limitation (-)
An Omnipresent Formal Trust Model (FTM) for Pervasive Computing Environment [79]	it proposes the first omnipresent trust model for pervasive computing.it is based on recommendation and behavioral model to handle interactions	(+) it uses both direct trust protocol based on behavior and recommendation trust protocol which consider active and passive recommendations both (-) in this scheme detection of malicious recommendation is missing
Trust path: a distributed model of search paths of trust in a peer-to-peer system [80]	It helps in searching all trusted paths between any peers that have no direct knowledge	(+) it enables the distributed search algorithm of the path of trust by flooding the network by propagation to all known peers (-) it only helps in finding the trusted path from peer to peer and not deals with other outside attacks

7 Challenges and future direction

A variety of detection and protection mechanisms are proposed to improve security across the Physical, MAC, and Network layers of a cognitive radio Network. These methods rely on information available about the users involved, who can be primary, secondary, malicious, or selfish. Despite various efforts to address and mitigate attacker threats, the Physical, MAC, and NW layers continue to present unique challenges. For example, predicting the location of PU in real-time scenarios is difficult and heavily reliant on localization-based techniques. Anti-jamming techniques also necessitate higher energy consumption and design complexities. For example, using cryptographic techniques consumes resources such as power and bandwidth. Furthermore, the same protocol as SU and PU on the same layer authentication is required. As a result, cryptography must be a dependable and secure infrastructure. Furthermore, strategy-based intrusion detection systems require a significant amount of memory to process and analyses traffic, resulting in NW overhead. SS techniques that can differentiate between signals from legitimate PU and signals from malicious users must also be developed. Furthermore, detecting malicious devices is difficult, and software defined radio may be required (SDR). As a result, enforcing security at the PL is critical, as it focuses primarily on the SS phase. Furthermore, the Network layer considers spectrum availability. Indeed, cognitive radio routing should address all spectrum availability and security concerns. There are several protocols available, including the secure efficient Ad hoc distance vector protocol (SEAD) and the secure Ad hoc on demand distance protocol.

8 Conclusion

The Spectrum scarcity has arisen as a result of the exponential growth in mobile and wireless devices over the last decade. As a result, it is critical to address the future spectrum supply and demand imbalance. Hence, Cognitive radio technology is essential as it addresses spectrum scarcity problem by investigating spectrum sharing schemes in four key steps: spectrum sensing, spectrum allocation, spectrum access, and spectrum handoff. However, due to its dynamic nature, it also allows malicious users to launch new attacks by leveraging cognitive radio functionalities at different layers of TCP/IP protocol stacks. This paper focuses on physical, MAC, and network layer attacks. Furthermore, it showed attacks that can occur only in CRN due to their spectrum sharing and reconfigurability features. In addition, we have discussed the threats that the CRN cross layer encounters, as well as the detection mechanism and its countermeasures.

Still many intriguing questions remain to be addressed in future works. As a result, frameworks for detecting and responding to all potential attacks are required. Furthermore, cryptography techniques at different layers can provide this trustworthy information, allowing them to learn and think about their surroundings. Furthermore, to address the cybersecurity challenge in the wireless ecosystem, a combination of a robust intrusion detection system and a machine learning technique that can be applied to wireless technology analysis could be a step forward towards problem resolution.

Data availability All data generated or analyzed during this study are included in this article.

Declarations

Conflict of interest The authors declare no conflicts of interest.

References

1. Federal Communication Commission. (2002). Spectrum policy task force. Rep. ET Docket no 02.135.
2. Wang B, Liu KJR (2011) Advances in cognitive radio NWs: a survey. IEEE J Sel Top Signal Process 5(1):5–23
3. Mitola J, Maguire GQ (1999) Cognitive radio: making software radios more personal. IEEE Pers Commun 6(4):13–18
4. Haykin S (2005) Cognitive radio: brain-empowered wireless communications. IEEE J Sel Areas Commun 23(2):201–220
5. Liu, Y., & Zhou, Q. (2009, May). State of the art in cross-layer design for cognitive radio wireless networks. In 2009 International Symposium on Intelligent Ubiquitous Computing and Education (pp. 366-369). IEEE.
6. Raisinghani VT et al (2004) Cross-layer design optimizations in wireless protocol stacks. Comput Commun 27(8):720–724
7. Padmadas M, Krishnan N, Nayaki VN (2015) Analysis of attacks in cognitive radio NWs. Int J Adv Res Comput Commun Eng 4(8):170–174
8. Yilmaz MH, Arslan H (2015) A survey: spoofing attacks in PLsecurity. In: Proc. - Conf. Local Comput. NWs, LCN, vol 2015, pp 812–817
9. Parvin S, Hussain FK, Hussain OK, Han S, Tian B, Chang E (2012) Cognitive radio NW security: a survey. J Netw Comput Appl 35(6):1691–1708
10. Gupta I, Sahu OP (2018) An overview of PU emulation attack in cognitive radio NWs. In: IEEE International conference on computing methodologies and communication, pp 27–31
11. Yu R et al (2016) Securing CRN against PU emulation attacks. IEEE Network Mag 30(6):62–69
12. Wang Y, Xu X, Wu W, Bao J (2017) A PU emulation attack countermeasure strategy and energy-efficiency analysis in cognitive radio NWs. J Commun 12(1):1–7
13. Das D, Das S (2013) PU emulation attack in cognitive radio NWs: a survey. Int J Comput Network Wirel Commun 3(3):312–318
14. Chen R, Park J-M (2006) Ensuring trustworthy SS in cognitive radio NWs. In: Proc. IEEE Workshop NWing Technologies for Software Defined Radio NWs
15. Jin Z, Anand S, Subbalakshmi KP (2009) Detecting PU emulation attacks in dynamic spectrum access NWs. In: Proc. IEEE International Conference on Communications, pp 1–6
16. Hanen I, Daimi K, Saed M (2014) Security challenges in cognitive radio NWs. Proceedings of the world congress on engineering, vol 1, pp 1–7
17 Selvapriya T, Sharmila S, Sindhuja M, Sinthuja V, Jayasri C (2017) A database assisted detection against PU emulation in cognitive radio NW. Int J Innov Res Electric Electron Instrum Control Eng 5(3):1–6
18. Yuan Z, Han ZS, Li H, Song JB (2013) Routing-toward-primary-user attack and belief propagation-based defense in cognitive radio NWs. IEEE Trans Mob Comput 12(9):1750–1760
19. Zhou, X., Song, L., & Zhang, Y. (Eds.). (2013). Physical layer security in wireless communications. Crc Press.
20. Jin Z, Anand S, Subbalakshmi KP (2009) Detecting PU emulation attacks in dynamic spectrum access NWs. In: Proc. IEEE Int. Conf. Communications, pp 1–5
21. Tran H, Zepernick H (2016) Proactive attack: a strategy for legitimate eavesdropping. In: IEEE 6th international conference on communications and electronics, pp 457–461
22. Chorti A, Perlaza M, Han Z, Poor H (2012) PL security in wireless NWs with passive and active eavesdroppers. In: IEEE global communications conference, pp 4868–4873
23. Nguyen V, Duong T, Shin O, Nallanathan A, Karagiannidis G (2017) Enhancing PHY security of cooperative cognitive radio multicast communications. IEEE Trans Cogn Commun Netw 3(4):599–613

24. Hasnat M, Rurnee S, Razzaque M, Mamun-Or-Rashid M (2019) Security study of 5G heterogeneous NW: current solutions, limitations & future direction. In: IEEE international conference on electrical, computer and communication engineering, pp 1–4
25. Idoudi H, Daimi K, Saed M (2014) Security challenges in cognitive radio NWs. World Congr Eng 1:2–4
26. Holcomb S, Rawat D (2016) Recent security issues on cognitive radio NWs: a survey. In: Southeast conference, pp 1–6
27. Rathee G, Saini H (2016) Security concerns with open research issues of present computer NW. Int J Comput Sci Inf Secur 14(4):406
28. Kundu C, Ghose S, Bose R (2015) Secrecy outage of dual-hop regenerative multi-relay system with relay selection. IEEE Trans Wireless Commun 14(8):4614–4625
29. Lei H, Xu M, Ansari I, Pan G, Qaraqe K, Alouini M (2017) On secure underlay MIMO CRN with energy harvesting and transmit antenna selection. IEEE Trans Green Commun Netw 1(2):192–203
30. Balogun V, Krings A (2013) On the impact of jamming attacks on cooperative SSin cognitive radio NWs. In: Proceedings of the eighth annual cyber security and information intelligence research workshop, pp 1–6
31. Rizvi S, Showan N, Mitchell J (2015) Analyzing the integration of cognitive radio and cloud computing for secure NWing. Procedia Comput Sci 61:206–212
32. Wenkai W, Li H, Sun Y, Han Z (2009) Catch It: Detect malicious nodes in collaborative spectrum sensing. In: IEEE global telecommunications conference, pp 1–6
33. Rawat AS, Anand P, Chen H, Varshney PK (2010) Countering Byzantine attacks in cognitive radio NWs. In: IEEE international conference on acoustics, speech and signal processing, pp 3098–3101
34. Rawat A, Anand P, Hao C, Varshney K (2011) Collaborative SS in the presence of Byzantine attacks in cognitive radio NWs. IEEE Trans Signal Process 59(2):774–786
35. Chen R, Park J-M, Reed JH (2008) Defense against PU emulation attacks in cognitive radio NWs. IEEE J Sel Areas Commun 26(1):25–37
36. El-Hajj, W., Safa, H., & Guizani, M. (2011). Survey of security issues in cognitive radio networks. Journal of Internet Technology 12(2):181–198
37. Pei Q, Li H, Ma J et al (2011) Defense against objective function attacks in cognitive radio NWs. Chin J Electron 1:138–142
38. Salim S, Moh S (2013) On-demand routing protocols for cognitive radio ad hoc NWs. EURASIP J Wirel Commun Netw 2013(1):1–10
39. Zou Y, Zhu J, Yang L, Liang YC, Yao YD (2015) Securing physical-layer communications for cognitive radio NWs. IEEE Commun Mag 53(9):48–54
40. Thalor J, Monika M (2013) Wormhole attack detection and prevention technique in mobile ad hoc NWs: a review. Int J Adv Res Comput Sci Softw Eng 3(2):137–142
41. Khalil I, Bagchi S, Shroff NB (2005) LITEWORP: a lightweight countermeasure for the wormhole attack in multichip wireless NWs. In: 2005 International Conference on Dependable Systems and NWs (DSN'05). IEEE, pp 612–621
42. El Mouaatamid O, Lahmer M, Belkasmi M (2016) Internet of things security: layered classification of attacks and possible countermeasures. Electron J Inf Technol 9:24–37
43. Karlof C, Wagner D (2003) Secure routing in wireless sensor NWs: attacks and countermeasures. Ad Hoc Networks 1(2–3):293–315
44. Nafaa, M., & Ghanemi, S. (2014, April). Analysis of security attacks in AODV. In 2014 International Conference on Multimedia Computing and Systems (ICMCS) (pp. 752–756). IEEE
45. Newsome J, Shi E, Song D, Perrig A (2004) The Sybil attack in sensor NWs: analysis & defenses. In: Proc. 3rd
46 Elderini T, Kaabouch N, Reyes H (2017) Channel quality estimation metrics in cognitive radio NWs: a survey. IET Commun 11:1173–1179
47. Darwish M, Ouda A, Capretz L (2013) Cloud-based DDoS attacks and defenses. Information society (i-Society)
48. Atlasis, A. (2012). Attacking ipv6 implementation using fragmentation. Blackhat europe, 14-16.
49 Pathan ASK (ed) (2016) Security of self-organizing NWs: MANET, WSN, WMN, VANET. CRC Press, Boca Raton
50. Henze, M., Hiller, J., Hummen, R., Matzutt, R., Wehrle, K., & Ziegeldorf, J. H. (2017). Network Security and Privacy for Cyber-Physical Systems. Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications 25–56
51. Patel A, Mokbel MF, Zhao S (2007) Fragmentation attack on wireless NW. School of Computer Science, University of Windsor, Canada

52. Riahi Manesh M, Kaabouch N (2017) Analysis of attacks and vulnerabilities of automatic dependent surveillance-broadcast. Inter J Crit Infra Protect 19:16–31
53. Bouabdellah M, El Bouanani F, Ben-Azza H (2016) A secure cooperative transmission model in VANET using attribute-based encryption. In: Advanced Communication Systems and Information Security (ACOSIS), International Conference on. IEEE, pp 1–6
54. Kim M, Ning P (2011) SeCA: a framework for secure channel assignment in wireless mesh NWs. Comput Commun 34(4):567–576
55. Wang, W., Kwasinski, A., & Han, Z. (2014, April). A routing game in cognitive radio networks against routing-toward-primary-user attacks. In 2014 IEEE Wireless Communications and Networking Conference (WCNC) (pp. 2510–2515). IEEE
56. Zhang, Q., Wang, P., Reeves, D. S., & Ning, P. (2005, June). Defending against sybil attacks in sensor networks. In 25th ieee international conference on distributed computing systems workshops (pp. 185–191). IEEE
57. Clancy TC, Goergen N (2008) Security in cognitive radio NWs: threats and mitigation. In: 3rd International conference on cognitive radio oriented wireless NWs and communications, pp 1–8
58. Do QV, Vu VH, Koo I (2019) An efficient bandwidth allocation scheme for hierarchical cellular networks with energy harvesting: an actor-critic approach. Int J Electron 106(10):1543–1566
59. Parvin S (2013) Trust-based mechanisms for secure communication in cognitive radio networks (Doctoral dissertation, Curtin University)
60. Vimal S, Kalaivani L, Kaliappan M, Suresh A, Gao XZ, Varatharajan R (2020) Development of secured data transmission using machine learning-based discrete-time partially observed Markov model and energy optimization in cognitive radio networks. Neural Comput Appl 32(1):151–161
61. Wang X, Ji Y, Zhou H, Li J (2015) A nonmonetary QoS-aware auction framework toward secure communications for cognitive radio networks. IEEE Trans Veh Technol 65(7):5611–5623
62. Zou C, Chigan C (2016) Dynamic spectrum access-based cryptosystem for cognitive radio networks. Secur Commun Netw 9(17):4151–4165
63. Khasawneh M, Agarwal A (2017) A secure and efficient authentication mechanism applied to cognitive radio networks. IEEE Access 5:15597–15608
64. Parvin S, Hussain FK (2011) Digital signature-based secure communication in cognitive radio networks. In: 2011 international conference on broadband and wireless computing, communication and applications. IEEE, pp 230–235
65. Do-Vinh Q, Koo I (2018) Energy-efficient data encryption scheme for cognitive radio networks. IEEE Sens J 18(5):2050–2059
66. Elghamrawy SM (2020) Security in cognitive radio network: defense against primary user emulation attacks using genetic artificial bee colony (GABC) algorithm. Futur Gener Comput Syst 109:479–487
67. Srinivasan S, Shivakumar KB (2018) AI based algorithm & framework for efficient PUE attack detection using dual classification method in CRN. Int J Appl Eng Res 13(4):52–56
68. Sajid A, Khalid B, Ali M, Mumtaz S, Masud U, Qamar F (2020) Securing cognitive radio networks using blockchains. Futur Gener Comput Syst 108:816–826
69. Zakhary SR, Radenkovic M (2010) Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments. In: 2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS). IEEE, pp 161–167
70. Chen C, Song M, Xin C, Alam M (2012) A robust malicious user detection scheme in cooperative spectrum sensing. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp 4856–4861
71. Zhang T, Safavi-Naini R, Li Z (2013) ReDiSen: Reputation-based secure cooperative sensing in distributed cognitive radio networks. In: 2013 IEEE International Conference on Communications (ICC). IEEE, pp 2601–2605
72. Liu S, Zhu H, Li S, Li X, Chen C, Guan X (2012) An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing. In: 2012 IEEE Global Communications Conference (GLOBECOM). IEEE, pp 603–608
73. Ajayi OO, Badrudeen AA, Oyedeji AI (2021) Deep learning based spectrum sensing technique for smarter cognitive radio networks. J Invent Eng Technol 1(5):64–77
74. Zhang N, Lu N, Lu R, Mark JW, Shen X (2012) Energy-efficient and trust-aware cooperation in cognitive radio networks. In: 2012 IEEE international conference on communications (ICC). IEEE, pp 1763–1767
75. Ling MH, Yau KLA, Qadir J, Ni Q (2018) A reinforcement learning-based trust model for cluster size adjustment scheme in distributed cognitive radio networks. IEEE Trans Cogn Commun Netw 5(1):28–43
76. Sarkar S, Datta R (2012) A trust based protocol for energy-efficient routing in self-organized MANETs. In: 2012 Annual IEEE India Conference (INDICON). IEEE, pp 1084–1089
77. Xia H, Jia Z, Li X, Ju L, Sha EHM (2013) Trust prediction and trust-based source routing in mobile ad hoc networks. Ad Hoc Netw 11(7):2096–2114

78. Bennaceur J, Idoudi H, Saidane LA (2017) Game-based Secure Sensing for the CRN. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE, pp 2079–2084
79. Haque MM, Ahamed SI (2007) An omnipresent formal trust model (FTM) for pervasive computing environment. In: 31st annual international computer software and applications conference (COMPSAC 2007), vol 1. IEEE, pp 49–56
80. Moalla, S., & Rahmouni, M. (2015). Trust path: a distributed model of search paths of trust in a peer-to-peer system. Security and Communication Networks 8(3):360–367