Trust Management in Cognitive Radio Networks : A Survey

Article *in* International Journal of Network Management · September 2017

DOI: 10.1002/nem.1999

Jihen Bennaceur
Ecole Nationale des Sciences de l'Informatique
5 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Hanen Idoudi
Université de la Manouba
51 PUBLICATIONS **100** CITATIONS
SEE PROFILE

Leila Azouz Saidane
Université de la Manouba
175 PUBLICATIONS **444** CITATIONS
SEE PROFILE

Received: 7 April 2017 | Revised: 19 July 2017 | Accepted: 12 August 2017

DOI: 10.1002/nem.1999

SPECIAL ISSUE PAPER

WILEY

Trust management in cognitive radio networks: A survey

Jihen Bennaceur | Hanen Idoudi | Leila Azouz Saidane

National School of Computer Science, University of Manouba, Campus of Manouba, 2010, Manouba, Tunisia

Correspondence
Jihen Bennaceur, National School of Computer Science, University of Manouba Campus of Manouba, 2010, Manouba, Tunisia.
Email: jihen.bennaceur@ensi-uma.tn

Summary

Cognitive radio is proposed to solve the interference and underutilized license problems. With the development of the cognitive functionalities, classical and new security threats become challenging. To make wireless cognitive radio networks more secure and more reliable, several approaches have been proposed in the literature. In recent years, trust and reputation management (TRM) techniques are more and more considered for cognitive radio networks to secure them against the malicious and misbehaving users that try to deprive others from using the white space. The scope of this survey is to give a comprehensive overview about the existing TRM-based mechanisms proposed for the cognitive radio networks. We expose the existing classifications of TRM techniques, then we introduce a new classification that takes into account, more exhaustively, different TRM properties and approaches.

1 | INTRODUCTION

Cognitive radio allows unlicensed users to access and use licensed channels. This is intended to reduce interference ad increase throughput, thus, improving the overall networks performances. In a cognitive radio network (CRN), an unlicensed or secondary user (SU) uses opportunistically the free spectrum, or the so-called the "white space," without interfering with the primary user (PU). If the spectrum is not used, the SU may use the spectrum for its transmissions. If the SU detects a PU activity, it leaves the channel to avoid interfering with the PU.[1]

Cognitive radio users usually perform in continuous or periodic manner, spectrum sensing and dynamic access. These operations are usually performed in a cooperative way. These new features introduce new vulnerabilities and security threats. In addition to being vulnerable to existing wireless networks attacks, such as jamming, sinkhole, and Sybyle attacks, CRNs face new types of threats that affect the cognitive features and lead to performance degradation. These attacks mainly aim either at affecting PUs functioning or depriving the SUs from accessing the underutilized channels. Thus, they grape selfishly the free channels by degrading perceptibly the network performance. To overcome this issue, the most used mechanisms in literature are the cryptography, malicious nodes location, and trust and reputation management (TRM) techniques. In CRNs, TRM is aimed at detecting malicious nodes collaboratively or individually. To sense the spectrum, each node will monitor its neighbor nodes and their actions over time. Depending on the actions performed by these neighboring nodes, one node will assign a trust index. Then, the computed trust values are used to secure a specific application in a CRN such as PU detection or data dissemination.

In this paper, we give an overview of TRM techniques in CRN. We begin with describing the existing and new threats affecting these networks. Then, we illustrate the TRM approaches in CRN using the existing classifications proposed in literature. We notice that the most used criteria for trust approaches classifications in CRN are trust proprieties, security purposes, and attack type. However, we identify other relevant criteria when applying TRM for securing CRNs. On the basis of this study, we define a novel and exhaustive taxonomy of TRM approaches proposed for CRNs.

https://doi.org/10.1002/nem.1999

The new classification aspects are the following:

1. The network topology: Every network topology may strongly affect the choice of the appropriate TRM mechanism.
2. The detection strategy: At the spectrum detection phase, the SU senses individually or cooperatively the PU activities in the channel. Each detection strategy, used to make the final decision, can be secured by different TRM mechanisms.
3. Trust computation: For each node, the trust value can be computed using intelligent or simple methods (Bayesian network, probability, etc) to distinguish between honest, suspicious, and malicious entities.
4. Spectrum management: To control the spectrum allocation and to manage the channel availability decisions, the CRN may use a centralized, distributed, or clustering spectrum sensing technique. For each spectrum management technique, different TRM approaches are proposed to secure the spectrum detection feature.

The remainder of this paper is organized as follows: In section 2, we will review the security attacks and vulnerabilities in CRNs. Then, we will define, in Section 3, the concepts of the TRM. Thus, we will illustrate the existing TRM approaches and classifications. In Section 4, we will present our new classification of TRM approaches in the CRNs.

2 | CRNS ATTACKS AND VULNERABILITIES

Wireless networks are vulnerable to several types of attacks and threats.[2] Indeed, attacks can be classified according to the target layer. Briefly, Table 1 illustrates a list of attacks that may affect all types of wireless networks.

Cognitive radio networks are vulnerable to conventional wireless networks attacks[3] but suffers further from specific attacks due to their intrinsic cognitive functionalities. In CRNs, the SUs, competing to exploit the white space, can be honest, selfish, faulty, or malicious. Faulty users may send incorrect sensing outcomes due to defective device, fading location, or shadowing zone. The erroneous spectrum detection affects the final decision and degrades the network performance. On the other hand, the selfish and malicious users aim at monopolizing the free spectrum and interfering with the other users (SU or PU) by launching several attacks. Attacks can be classified according to the targeted network layer.

2.1 | The physical layer

The physical layer is vulnerable to several attacks,[4] such as

- The PU Emulation Attack: It is caused by the malicious SU emulating the PU identity to use selfishly the spectrum without sharing it with the other users. The fake identity deprives the SUs to use the white space. Indeed, the SUs detect incorrectly the licensed PU presence. Contrariwise, the channel is idle and the malicious emulator exploits selfishly the resource.[5]

  The authors in Ta et al[6] proposed a game-based model to identify the illegal channel occupied by the selfish PUEA attackers.
- The Objective Function Attack: This attack is launched to modify the cognitive parameters. When the cognitive engine aims at adopting the current environment, the attacker can launch his attack by manipulating the parameters, such as transmission rate, to make the results biased and well-adapted to its interest and to its goals.
- Jamming Attack: The jammer attacker sends out its packets to prevent the legitimate user from communicating with the other users (sending or receiving information) by using the denial of service attack. The jammer tries to deprive other users from sensing the availability of a channel by sending packets continuously. When an attacker blocks the dedicated channel used to exchange the sensing data between users, the network will be considerably damaged.[7]

  To secure the physical layer from the previously defined threats, many approaches are proposed using different methods and techniques as the jammer selection algorithm in Oskoui et al[8] and Gao et al,[9] the trust protocol design using the location of eavesdroppers in Cai et al,[10] and the optimization of secrecy energy efficiency model in Ouyang et al,[11] which enhances significantly both the security and energy efficiency of CRN.

2.2 | The link layer

Many threats target the link layer functions in a CRN.[12] We expose here after some well-known attacks.

TABLE 1 Wireless networks attacks

Layer	Attacks	Definition
Transport	Flooding	A flooding attacker can make repeatedly a new connection request until destination are exhausted or until it reaches a maximum limit causing the ignorance of legitimate requests.
	De-synchronization	An attacker tries to disrupt an existing connection by spoofing repeatedly messages to an end host causing the request for re-transmission of missed frames.
Network	Information disclosure	A compromised node may leak confidential data to illegitimate nodes in the network. Such information may include important data concerning network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.
	Byzantine attack	A compromised node or a set ofcompromised nodes generates collision and conduct attacks, such as creating routing loops, forwarding packets in nonoptimal routes, and selectively dropping important packets. Yet these attacks are very difficult to detect.
	Wormhole	An attacker connects 2 distant malicious nodes through a powerful connection. This action will mislead the other nodes on actual distances between the 2 nodes. It forces the neighboring nodes to pass through malicious nodes to route their packets.
	Hello flood	The attacker aims at convincing the neighboring nodes and even those out of reach to reorient the information. In fact, the attack purpose is to force nodes to redirect their packets to the attacker, which leads to energy depletion of nodes.
	Sybil	A malicious node has several identities to attract as much traffic as possible and gain more influence over the ordinary nodes.
	Sinkhole	An attacker tries to pass the data into a false sink by being very attractive to the neighboring nodes. Then, it creates a faulty network topology. Consequently, to route their data, the neighboring nodes choose this node as the next hop.
	Selective packet forwarding	In a multihop network, all nodes must transmit messages to communicate. The attacker transfers some packets and deletes others, generating data loss.
	Spoofing	An attacker may spoof, alter, or replay routing information to disrupt traffic in the network. These disruptions include creation of routing loops, attracting or repelling network traffic from the selected nodes, extending or shortening source routes, generating fake error messages, and causing network partitioning.
Link	The collision	The attempting of 2 nodes to transmit on the same frequency simultaneously defines the collision. An attacker may cause the collisions in specific and strategic packets, such as ACK and control messages.
Physical	Jamming	A jamming attack can be harmful and powerful enough to disrupt the entire network when it interferes in radio frequencies that the nodes use in wireless network for the communication.

- Spectrum Sensing Data Falsification (SSDF): It may be caused by a malicious user sending faulty spectrum detections to its neighbors, the fusion center (FC), or the base station (BS). This attack generates a wrong spectrum-sensing decision in distributed and centralized cognitive networks. The SSDF attack leads to interferences and underutilization of the spectrum.
- Control Channel Saturation DoS Attack: This attack aims at decreasing the network performance using the collision concept. In fact, when many cognitive users want to communicate at the same time, the common control channel becomes saturated because it can only support a limited number of concurrent data channels.
- Selfish Channel Negotiation: This attack can degrade harmfully the performance of the whole cognitive network. A selfish node can refuse to forward other nodes packets to preserve its energy and increase its throughput, it can refuse to forward any data to others hosts.

2.3 | The network layer

The network layer in cognitive network is the most likely to be attacked by the adversaries launching the primary user emulation (PUE), objective function, or jamming attacks[13]:

- Network Endo-Parasite Attack (NEPA): In a NEPA, the affected links are along the routing path through the malicious nodes towards the wired gateway. By launching a NEPA attack, a compromised node assigns its packets to interfere the high priority channels in the network. However, it does not inform its neighbors about this change. Since the transmitted information is not verified by neighbors, the network remains unaware of this change.

- Channel Ecto-Parasite Attack (CEPA): This attack is a special case of NEPA with slight modification in the attack strategy. A malicious node launches CEPA attack by switching all its packets to interfere in the channel used by the highest priority link. However, the detection of this attack is relatively easy due to the severe CEPA effects on the cognitive network.
- Low cOst Ripple effect Attack: Faulty information about spectrum assignments pushes the network into a quasi-stable state. Indeed, this attack is launched by a compromised node that transmits faulty channel assignment information to its neighbors, forcing the other nodes to adjust their channel assignments. However, this attack is more harmful and severe than NEPA and CEPA due to the propagation effect to a large part of the network beyond the compromised node neighborhood.

2.4 | The transport layer

Several attacks affect this layer such as the lion attack where the attacker disrupts the TCP connection by launching the PUE attack. In fact, it can be considered as a cross-layer attack performed at the physical link layer and targeting the transport layer. Moreover, if the attacker knows or can guess some of the connection parameters, it launches even a DoS attack just by emulating a primary transmission at specific instants of time, which can be easily predicted. The licensed transmission emulation may cause severe interference with PUs or deprives the SUs from preforming their communications while the spectrum is available.

Several studies have dealt with securing the network using classical or innovative mechanisms. For instance, the cryptography mechanism is a security method that aims at protecting data by using a cryptographic key to verify if the transmitted signal belongs to the legitimate user or it is fake. Each user, that detects a signal, attempts to verify its integrated signatures. If verification fails, the signal will be considered to be fake. There are 4 key types used in the cryptography. Firstly, the global key, shared by the entire network, is used to encrypt the message to be sent and to decrypt the received data. Secondly, the shared key by peer nodes is defined when each node has a different key to communicate with a neighboring node sharing this key. So, if a node has n neighbors, it will have n keys to be stored to communicate with its neighbors. Thirdly, the shared key per nodes group is used when each group or cluster shares a common key that allows it to communicate within the group. In fact, the cluster heads (CHs) communicate with each other by using a common key to all CHs or a common key per peer of CHs. Fourthly, the individual key is designed when each node has a personal key to encrypt the information. Thus, a message, sent by this node, circulates in a hidden way in the network until it reaches the target.[14,15] However, this mechanism cannot be adopted by all the networks such as the cognitive wireless sensor network due to the low power, memory, and computation time constraints.

Besides, the authors in previous study[16] introduced the location approach, which is a mechanism used to detect the malicious nodes, particularly wormhole attacks. In fact, to apply the location mechanism, it needs geographical location techniques, such as GPS. Consequently, the network must be equipped with beacon nodes to know their location. With the location privilege, if a node requests to enter the network, the beacon nodes, receiving this demand, will be able to estimate its location relative to its range. Then, the beacon nodes will quadrille their respective listening area, and each node, receiving the inclusion request in the network, will vote for an area of the grid that is able to hear. The area receiving the highest number of votes will be considered as the new node host. In the case of wormhole attack, the 2 malicious nodes will be geo-located by the bacon nodes, which determines if the distance between these 2 nodes is greater than the real distance for the one-hop communication. However, the major weakness of this solution is the need to deploy beacons nodes equipped with a GPS device in the CRNs, which is very expensive.

As we have mentioned previously, security mechanisms face many problems when applied to CRNs (memory and computation costs, power consumption, etc). The TRM can be the solution for these problems, as it is an emerging technique to secure networks based on autonomous nodes. In the following section, we will define basic concepts of TRM and its use in different fields, especially in the CRN.

3 | TRM: DEFINITION AND CONCEPTS

Generally, the trust has several definitions according to the different disciplines in which it is used[17] such as sociology, economic, philosophy, psychology, and CRN. At the beginning, we should define the trust in each domain to understand the main idea and basic concept of trust management. We start with the trust in sociology. In this context, it represents an indicator for future actions based on the continuous interactions between entities to build good relationships between people as it is for network. However, trust in economics is based on the assumption that humans are rational, and a strict utility maximizes their own interests or incentives. Trust in philosophy is more like a thread relating people to maintain good relationships although it can be dangerous in a way that the trustee may be betrayed somehow since relying on others is not something that is forcibly given. Trust in psychology is an inborn attitude that may change according to the life conditions that the child has been risen in, and the experiences they have been through along their life. But once this trust is lost, it cannot be regained. Last but not least, the trust management concept becomes so attractive in the communication and the networking security. The design of many networks and protocols uses this mechanism to build trust relationships among participating nodes to create cooperative and collaborative environments to improve the network performance.

From the above discussions, we can conclude that generally the trust has the same main definition in different domains. Indeed, the differences appear only in the trust mechanisms and their sides (trustor, trustee). However, in the literature, the terms “trust,” “trustworthiness,” and “reputation” seem to be used interchangeably without clear distinction.[18]

- Trust: We define the trust as the subjective probability in which the aspect of belief plays an important role, and by which one (trustor) relies on another and expects that trustee would depend on its (trustor) own good. In fact, we define the trust level as the probability varying from 0 (complete distrust) to 1 (complete trust).
- Trustworthiness: The trustworthiness is an objective probability by which the trustee performs a given action on which the welfare of the trustor depends.
- Reputation: The reputation can be defined as the opinion of one person about the other, of one customer about a product, and by construct, of one node about another. In fact, trust is a derivation of the reputation of an entity. A trust level is computed for an entity by using the reputation. Indeed, the reputation itself has been built over time based on that entity behaviors history.

3.1 | TRM in CRNs

In CRNs, when some CR nodes aim to interact with each other, a level of trust must be required to establish a secured communication, a secured spectrum detection, a secured fusion decision, etc. Each trust value given to a node can be updated and computed by the directed interaction experience or recommendation from a third party (reputation value from other nodes). After computing trust values of nodes, it must be integrated into various security mechanisms to enforce the information confidentialities, data integrities, user privacy, and network performance. This trust value can be used to secure many applications in the network. For instance, we can mention secure routing, fusion, cluster, etc. Instead of routing the information using the shortest path, another route is calculated using the nodes with the highest trust value to protect the transmitted data. Furthermore, the trust values can be used to secure the fusion when the aggregation of the local detections considers only the sensing outcomes of honest nodes (with acceptable trust value). In addition, trust management mechanisms can be applied to secure the clustering in CRN by selecting the honest node to be a CH.

3.2 | TRM characteristics

Due to the unique characteristics of trust management in cognitive radio environments, the trust concept should be carefully defined. We will illustrate in the next section the various trust characteristics used to classify the trust mechanisms as they are presented in literature.[19]

“Trust is context-dependent.” Trust has a specific context in its scope. For example, for a given task, different types of trust (computational power trust, unselfishness trust, reporting trust, etc) are required. Zhang et al[20] introduced a new trust approach to guarantee the performance of cooperation between PU and SU by considering the energy efficiency. The authors considered the trust value to evaluate the SUs behaviors during the cooperation task. As a result, they proposed a cooperative SU selection scheme from the PU perspective. The interaction between the PU and the SU can be modeled as a Stachelberg game. The PU decides to cooperate or not by selecting the optimal SU, and it configures the cooperation parameters. Indeed, it can also choose the time of cooperation and with whom to cooperate and how to cooperate.

“Trust is composability.” The trust values of each neighbor and their recommendations about a particular node should be composed together and should lead to a single final trust level, which also belongs to the same set as the original trust information. Different composed functions can be used to aggregate the trust information depending on the situation and the kind of trust information. Feng et al[21] suggested a new weighted cooperative spectrum sensing approach to identify malicious SUs and mitigate their harmful effect on sensing performance. To make an accurate final decision, the authors gave a formula to calculate the weighted trust factor of each SU using their trust values and incorporate this factor in the process of sensing data fusion. So the final trust value is a result of trust fused values.

"Trust is slow." High trust and reputation need time to be build. In CRN, the trust values grow slowly with the good user behavior at a long period, depending on the historical values. Parvin et al[22] proposed a trust-based authentication mechanism to secure communication in CRNs, while authentication is a part of trust along with other technical or non-technical factors. In fact, when a node member sends a request to the BS, it sees the trust value of the requesting node. As a result, the requesting node is authenticated based on the trust value. Whenever, the new CR node wants to join the network, it should be authenticated by all the trusted nodes. At first, the new node broadcasts its certificate and random number to all members and the BS. The members and BS verify the node validity, and the BS computes the node signature. Then, the BS produces a random number RBS and calculates the signature for RN. The new node verifies the validity of BS certification and computes the numerical signature for RN. The BS and other members verify the numerical signature for RBS and broadcast the result that determines whether the new node can be passed or not. If the result obtained from the BS and the members is the same, the new node passes the authentication process, and the trust value of the node is incremented by one.

"Trust is Indirect." It is the second-hand information. When the trust level is based on the recommendations of neighbors about an entity that one does not know directly, it is considered as indirect trust. For example, to define a trust value, a node in the CRN can use the neighbor values about a specific node. Sagduyu et al[23] introduced a cooperative trust mechanism to protect the network against the SSDF. Each SU senses the spectrum to identify the channel state (idle, occupied). Then, the sensing outcomes are sent to the FC to be checked. After that, a probabilistic trust of each user is calculated or updated by the FC by using the Bayesian rules. The new recently calculated trust values define the decision rule taken by the FC.

"Trust is direct." We talk about the first-hand information that should always be the most reliable. In our context, a node uses its own information and observation to calculate the trust value node without external recommendations. Xu et al [24] proposed an energy detector with double-thresholds schemes in the cooperative network. This mechanism catches the malicious users with the "always occupied" or "always unoccupied" sensing outcomes. Indeed, the SUs set is divided into 3 groups N_1, N_2, and N_3. Thus, N_1 and N_2 groups present the number of users sending a detection result under and upper the bound thresholds. This scheme defines the SU as honest (trusted) or malicious (untrusted). However, group N_3 contains the number of SUs with sensing uncertain outcomes(when it falls between the 2 thresholds). These results are sent to the FC to make the final decision using the summation of $N_1 + N_2 + 1$.

"Trust is subjective." If Alice thinks that Bob's ideas are good, John may not think that Bob's ideas are good. In cognitive environment, the trust level given to the same trustee node can be different due to the various network topology changing dynamically, the attacks targeting the trust value, etc. Therefore, the trust value cannot be objective. To make the trust more objective, Parvin et al[25] suggested a trust mechanism based on authentication. The PU and the SU may not believe in each reputation value. As a solution, the certificate authority (CA) presents the third party that reserves 2 copies (protected and public copy) of reputation values of the SUs and the PUs. The 2 copies of each user are compared. Indeed, every mismatch indicates that the SU is attacked and the CA notices the PUs. If a SU requests the free spectrum, the PU BS checks the public copy from the CA. Thus, it allows the access if the public reputation value matches the PU threshold.

"Trust is not transitive." If John trusts Peter, and Peter trusts Carl, this does not mean that John trusts Carl. In our context, if a cognitive node X trusts a node Y and Y trusts node Z, this does not imply that X trusts Z. To use the trust transitivity between 2 entities to a third party, a trustor should trust a trustee as well as the trustee's recommendation of the third party.

"Trust is dynamic." The node in CRN can move periodically or can be broken due to many failures. So the information is always incomplete and not static. To capture the dynamicity of trust level, the latter should be expressed as a continuous rather than as a binary variable or even discrete-valued entity.

"Trust is asymmetric." The nodes with higher capability may not trust nodes with lower capability at the same level that nodes with lower capability trust nodes with higher capability. For example, in the studied framework, a supervisor tends to trust a student less than the student trusts the supervisor. Thus, we can conclude that their relationship cannot be symmetric due to the power, capacity, variation between nodes, etc.

"Trust is propagative." If Anna knows Bob who knows Clark, and Anna does not know Clark, then Anna can have some amount of trust on Clark based on how much she trusts Bob and how much Bob trusts Clark. In fact, the propagation is the most studied trust property.

"Trust is event sensitive." Trust takes long time to be build. However, a single high-impact event may erase it completely. This trust aspect is less interested in computer science.

"Trust is self-reinforcing." Members act positively with other members whom they trust. Similarly, if the trust between two members is below some threshold, it is highly unlikely that they will interact with each other, leading to even less trust on each other. This aspect of trust has received comparatively less attention in the literature.

3.3 | TRM challenges

Trust mechanisms have several goals and purposes. For instance, we can mention securing the routing and detecting the PU activities. We talk here about the final objective and what we want to accomplish. In fact, it represents the fundamental characteristic of trust management. This section summarizes trust management schemes based on the important design purposes developed for CRNs.

3.3.1 | Secure routing

Like any other networks, the task of routing in the CRN is fundamental. However, the routing suffers from classical as well as cognitive attacks. Indeed, securing the routing becomes indispensable need in the network concept. In fact, the security goals can be achieved by the trust management mechanisms.

Zhang et al[26] used the reputation as a mechanism to define the trust value. The main idea relies on the application of the trust mechanisms in the CRN to solve the security problem in the route. In some routing methods, the trusted paths are computed according to trusted nodes, which improves the reliability of data forwarding. This approach also adopts the reward and punishment mechanisms to encourage the nontrust node to collaborate in routing task. The reputation scheme uses beta probability density functions (PDFs) to combine the feedback and to derive reputation values. From node i, if neighboring node j successfully forwards data to the next hop, it is calculated as x_{ij}. Otherwise, it is calculated as $\bar{x}_{ij}$. The times of successful and failed transmissions are, respectively, noted by r_{ij} and s_{ij}. Trust T_{ij} of node i to neighboring node j is represented by formula 1 as the probability expectation that the neighboring node forwards data packet to the next hop.

$$T_{ij} = E(f(p|\alpha, \beta)) = \frac{\alpha}{\alpha + \beta} = \frac{r_{ij} + 1}{r_{ij} + s_{ij} + 2}. \tag{1}$$

The node i calculates the trust value of all neighboring nodes. Then, the latter are classified into trusted, common, and malicious nodes. Therefore, the malicious nodes are rejected from the routing tasks, which increases the network performance.

To secure routing, Fang et al[27] proposed another trust routing approach based on the game theory and resource allocation for the cooperative networks.

3.3.2 | PU detection

The detection of PU activities is a very important task in the cognitive process to avoid the interference or the underutilization of the free spectrum. Due to the importance of the PU detection in CRN, many trust approaches have been introduced to secure this task. Zhang et al[28] suggested a trust mechanism for the centralized and collaborative CRNs. At first, each SU host sends its detections to its SU BS, which aims to calculate the reputation value of each SU host to make accurately the final decision. Firstly, the SU BS calculates the local sensing difference f_i computed by Equation 2, which is defined as the difference between the sensing outcomes d_i from SU host i, and the mean value of sensing outcomes from N SU hosts of an SU BS.

$$f_i = |d_i - \frac{1}{N} \sum_{N} d_n| \tag{2}$$

Secondly, the SU BS computes the sensing location factor p_i, which is the factor of two types of distances from SU_i based on formula 3, where p_a^i is the distance between SU_i host and its SU BS and p_b^i is the distance between SU_i and a PU.

$$p_i = p_a^i \times p_b^i. \tag{3}$$

Thirdly, the SU BS computes the control channel condition, which is quite simply the signal-to-noise ratio of SU_i, which is equal to $c_i = SNR_i$. The SU BS uses a weighted function expressed by formula 4 to calculate SU_i reputation value by the following formula:

$$r_i = \alpha f_i' + \beta p_i' + \delta c_i', \tag{4}$$

where $f'i$, $p'i$, and $c'i$ are the normalized values of f_i, p_i, and c_i. Then, the SU BS makes the final decision, D, from all SUs illustrated by the following formula 5:

$$D = \sum N \times r_n \times d_n / \sum N \times r_n. \tag{5}$$

3.3.3 | Secure clustering

The cluster structure is an ideal topology to support collaborative tasks, such as channels sensing and routing that are indispensable to CRN. Therefore, secure clustering based on the trust management mechanisms becomes more demanding to maintain the network reliability. In this context, Afsana et al[29] proposed a trust energy aware cluster modeling for the cognitive ad hoc network. The algorithm begins with the network deployment and the formation of cluster. When an SU needs to transmit a packet, the CH belonging to this node manages the channel assignment. The monitoring of idle channels and spectrum availability detection become the responsibility of CHs. Indeed, the formation of cluster in the network is conducted by the control information exchange containing the channel details. However, the problem resides when a malicious user deprives the SU from accessing the white space by occupying all or part of multiple available channels leading to network performance degradation. To authenticate a reliable SU, a trust value denoted by T_{ij} is assigned to jth node of ith cluster. Trustworthiness is calculated using the following formula 6:

$$T_{ij} = \frac{1}{2} \times (\frac{PFR_{ij}}{PFR_{max}} + \frac{\Delta E_{ij}}{\Delta E_{max}}), \tag{6}$$

where PFR_{ij} presents the packet forward ratio of jth node of ith cluster, PFR_{max} is the maximum value packet forward ratio, E_{ij} is the energy of jth node of ith cluster, and E_{max} is defined as maximum value of energy of jth node of ith cluster. After the trust calculation for each node, the mechanism passes to selecting the CHs for the network. The election of the CH depends on 3 parameters: trust value, received signal strength indication, and the available channels number. All cognitive users within clusters are given separate priorities based on theses parameters. Then, cluster head election cost (CHEC) is estimated. Finally, the node, with minimum value of the CHEC, represents the most eligible node to be elected as CH from "n" nodes.

In this context, the authors in one study[30] are interested in securing the cluster from the harmful attacks by proposing a reinforcement learning–based trust and a reputation management approach to determine the credibility of a specific node as time goes by, and to select a honest node as CH in the cluster topology. In fact, due to the reinforcement learning, each SU can keep track and can learn about the neighbor behavior.

3.3.4 | Secure fusion

In CRN, the important task resides in the detection of the opportunistic spectrum to determine the activities of the PU to exploit the white space. Thus, the spectrum detection can be done in collaborative and individual manner. Collaborative spectrum sensing needs an FC to collect all the sensing reports from SUs and to make a final decision based on fusion rules (OR, AND, Majority). However, the cooperation spectrum sensing can be attacked by malicious SUs that send fake detections to mislead the final fusion decision. Securing the fusion becomes an indispensable task in such network. Li Fangwei et al[31] proposed a trust approach based on reputation scheme to secure the spectrum fusion in cooperative spectrum sensing network. After the detection of the PU energy, each node exchanges the values with its neighbors. Therefore, it makes a local decision based on the consistent result. After the information exchange, every honest node calculates the reputation value of neighbors based on the received values and its own value, which is computed as a combination of current and the historical trust value at time $n - 1$. This trust scheme uses reputation to help SU to detect correctly the state of channel(idle/unoccupied).

TABLE 2 Exiting approaches classification

Approach	Attacks	Propriety	Goal
Zhang et al[20]	Launch black, Gray hole attack	Context-dependent	SU selection
Feng et al[21]	General attack	Composability, context-dependent	Secure fusion
Parvin et al[22]	Data falsification attack	Slow, Context-dependent	PU detection
Sagduyu[23]	Data falsification attack	Indirect, Context-dependent	Secure fusion
Xu et al[24]	Data falsification attack	Direct,context-dependent	Secure fusion
Parvin et al[25]	Data falsification attack	Subjective, context-dependent	PU detection
Zhang et al[26]	Selective forwarding attack	Context-dependent, Indirect, Subjective, Composability	Secure routing
Fang et al[27]	Data falsification	Subjective, context-dependent	Secure routing
Zhang et al[28]	Random attack, Data falsification attack	Context-dependent, Indirect, Dynamic	PU detection
Afsana et al[29]	Data falsification attack	Context-dependent, Indirect, Propagative	Secure clustering
Koh et al[30]	Collusion attack, Aggressive attack, Selfish attack, Faulty attack	Direct and Indirect, Context-dependent, Asymmetric, Propagative	Secure clustering
Fangwei et al[31]	Data falsification attack	Indirect, Context-dependent, Propagative	Secure fusion
Wengui et al[32]	Data falsification attack	Indirect, Context-dependent	Secure fusion

Abbreviations: PU, primary user; SU, secondary user.

Many researchers, such as Wengui et al[32] tried to secure the fusion from the attacks by proposing many interested approaches and mechanisms. They have also introduced new concepts into the trust management in the CRN like the jury system.[32]

In short, we conclude with Table 2, which resumes the trust management classification of all the studied-previously approaches presented in the literature for the CRNs.

4 | TRM TECHNIQUES CLASSIFICATION

As we illustrated in the previous section, the trust management approaches can be classified according to the type of attacks to prevent, the trust propriety to concentrate, and the security goal to achieve. However, the trust classification of studied-previously approaches and mechanisms in the CRNs is incomplete and ineffective. The classification needs to be more exhaustive and to touch all the important issues generally in the network and specifically in the CRN to resolve this classification weakness. As a result, we propose our exhaustive classification, which focuses on 4 important criteria:

- The topology of the CRNs: Every CRN has a specific topology chosen in advance. We will present 3 types of topology that can be used to classify the trust management approaches: ad hoc, mobile and clustering topology.
- The strategy used to detect the channel availability by the SUs: The detection of the spectrum decides the presence or the absence of the PU in the channel. The SU senses the PU activities in individual or collaborative manner. Each adopted strategy can be an important criterion to classify the trust management mechanisms.
- The spectrum management adopted to sense the channel availability: The spectrum sensing and decision can be achieved using the disturbed, centralized, and cluster-based sensing manner. The researchers can use the sensing techniques diversity to classify the trust management approaches aiming at securing the spectrum sensing manner in the CRNs.
- The computation techniques used to calculate the trust value: To secure the CRNs from the intentional and unintentional attacks, a trust value is defined for each entity considered as honest, suspect, malicious, etc. Indeed, this value can be calculated using a predefined trust computation model. Each model has a particularity in the computation way that makes the trust computation another criterion for the approaches classification in CRN.

Figure 1 illustrates our contribution defined as the newest and the fullest trust management classification approach in CRNs. Thus, Table 3 summarizes the proposed trust management approaches classification.

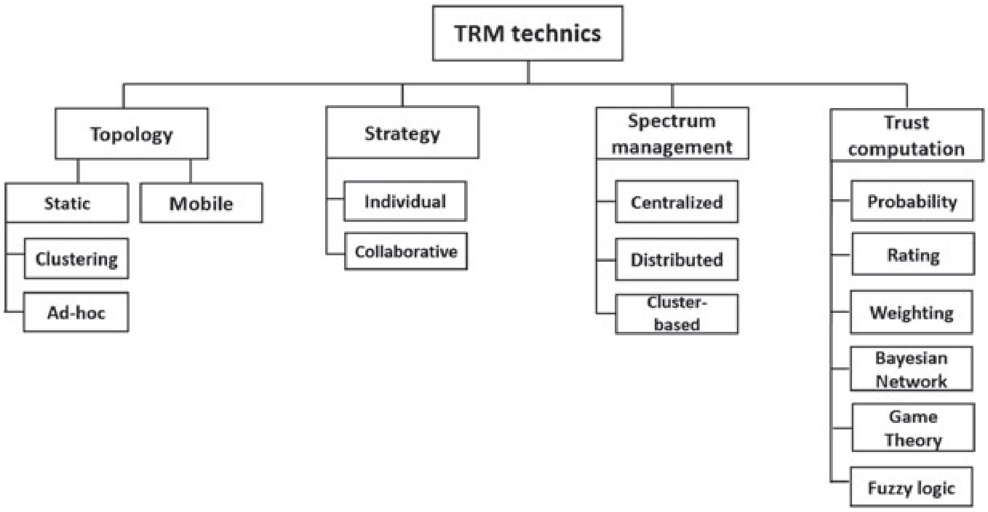

FIGURE 1 New trust approaches classification in cognitive radio network. TRM, trust and reputation management

4.1 | Trust computation

To compute the trust value, several important and intelligent methods have been proposed in the literature. Thus, the trust approaches in CRNs are classified using 6 models: the weighting, probability, rating, Bayesian network, game theory, and fuzzy logic. In this section, we will be interested in classifying of the existing approaches using the trust computation in the CRNs.

"Probability." In this case, the classical probability functions are used to calculate the trust value. To detect the PUE attack, the authors Jin et al in previous study[33] used analytical probability models for the received power using Fenton's approximation and Wald's sequential probability ratio test (WSPRT). In fact, the SUs compares the received power measurements on a spectrum band. When it is below a threshold, the spectrum is considered to be idle. Otherwise, the SU makes a decision that the detected signal was sent by the PU or an imitator attacker. Mathematical formulas are derived from the computation of the PDF of the received power to an SU due to a PU and the PDF of the received power to an SU due to malicious users. Then, the WSPRT is used to make a decision between 2 hypotheses: primary transmitter (H0) and malicious user (H1).

The authors in Feng et al[34] introduced a novel dynamic trust mechanism based on beta PDFs to secure cooperative spectrum sensing against the data falsification attacks.

"Weighting." In addition, the trust level can be computed basing on the weight functions, which are mathematical devices used to give some node more "weight" or influence than other nodes in the same cognitive network. To improve the network security, Li et al[35] proposed a new trust mechanism Security Management based on Trust Determination (SMTD). The main feature of this mechanism is defined by 6 functions: authentication, interactive, configuration, trust value collection, storage, update, and punishment. In fact, the DFC and the CHs have been put forward to manage trust value of cognitive users. Malicious users would be punished by FC by decreasing their trust value. The evaluation trust value from user SU_i to user SU_j is given by the following formula 7:

$$Tr_{ij} = \alpha \times DirTr_{ij} + \beta \times IndirTr_{ij} + \gamma \times HisTr_{ij} + Rew, \tag{7}$$

where α, β, and γ are the normalized weight factor, corresponding to direct trust DirTrij, indirect trust IndTrij, and historical trust HistTri values satisfying $\alpha+\beta+\gamma = 1$. The DirTr, IndirTr, and HistTri are designed, respectively, the direct, the indirect, and the historical trust values. Thus, the Rew represents the reward value.

Zhang et al[36] suggested another reputation-based scheme to increase the detection precision by using weighting functions. Indeed, the proposed mechanism gives a higher reputation value to the trusted node such as the SU BS, the SU CH, the access point, etc. Then, it calculates the final decision in 4 steps:

- Firstly, all the users reputation values are initialized. Each trusted SU_i is given a higher initial reputation value expressed by formula 8, which is equal to

$$r_i(t = 0) = \eta_b + (\eta_b - \eta_a)/2 \tag{8}$$

TABLE 3 Trust management approaches classification

	Trust computation							Spectrum management			Strategy		Topology		
Approach	Probability	Rating	Weighting	Bayesian Networks	Game Theory	Fuzzy Logic	Simple Computation	Centralized	Distributed	Cluster based	Individual	Collaborative	Ad hoc	Clustering	Mobile
Xu et al[24]	×							×				×	×		
Jana et al[56]	×		×					×				×			×
Jin et al[33]	×								×		×		×		
Feng et al[34]	×							×				×		×	
Arshad et al[37]		×						×				×	×		
Feng et al[21]			×					×				×	×		
Zhang et al[36]			×					×				×	×		
Du et al[47]			×					×				×	×		
Premarathne et al[48]			×					×				×	×		
Pei et al[58]			×					×				×	×		
Li et al[59]			×					×				×	×		
Pei et al[60]			×					×				×	×		
Li et al[35]			×					×		×	×			×	
Wang[57]			×					×				×			×
Zhang et al[28]			×						×			×	×		
Wengui et al[32]			×						×			×	×		
Vosoughi et al[52]			×						×			×	×		
Jeon et al[50]			×						×		×	×	×		
Lin et al[62]			×						×			×	×		
Koh et al[63]			×							×		×		×	
Sagduyu et al[23]				×				×				×	×		
Wang et al[38]				×				×				×	×		
Huo et al[39]				×				×				×	×		
Fangwei et al[40]				×				×				×	×		
Zhang et al[26]				×					×			×	×		
Ling et al[55]				×						×		×		×	
Zhang et al[20]					×				×			×	×		
Afghah et al[44]					×				×			×	×		
Zhendong et al[61]					×				×			×	×		
Fang et al[27]					×			×				×	×		
Wang et al[43]					×			×				×	×		
Houjeij et al[45]					×			×				×		×	
Taghavi et al[41]						×		×				×	×		
Wang et al[42]						×		×				×	×		
Parvin et al[22]							×	×			×		×		
Parvin et al[25]							×	×			×		×		
Koh et al[30]							×	×				×		×	
Fangwei et al[31]							×	×				×	×		
Kaligineedi et al[46]							×	×				×	×		
Dubey et al[49]							×		×		×		×		
Yu et al[51]							×		×		×		×		×
Afsana et al[29]							×			×		×		×	
Li et al[54]							×			×		×		×	

with $\eta a < \eta b$, where ηa and ηb are thresholds. When $r_i(t) < \eta a$, SU_i may be considered as malicious, but when $r_i(t) > \eta b$, SU_i may be considered as accepted, honest, etc.

- Secondly, the FC increments or decrements the reputation values of each SU_i using the comparison between the local detection $d_i(t)$ taken by the node SU_i and the local decision D of FC. The final decision is obtained by formula 9 as follows:

$$D(t) : r_i = r_i(t-1) + (-1)^{d_i(t)+D(t)}. \tag{9}$$

- Thirdly, the FC uses the reputation values for each SU_i to compute its weights based on Equation 10:

$$w_i(t) = w_i'(t) / \sum_i w_i'(t), \tag{10}$$

where $w_i'(t) = r_i(t-1)/max(r_i(t-1))$.

- Fourthly, the FC gathers the detections from SUs with a reputation value $r_i(t) \geq \eta b$ to make the final decision.

“Ratings.” Rating modeling tries to evaluate the trust of each node by giving a rating value. In fact, the reputation is factually a rating system that attempts to provide succinct summaries of a given node history in the CRN. In this context, Arshad et al[37] used a beta reputation system based on the rate process. The reputation is used to calculate the SU credibility score ς_i to define the reputation value for each user. The FC collects the local detections (binary digit 0 or 1) from all users to make a final decision based on the reputation system. Each SU models its respective local detection using only 2 rating parameters denoted by the positive rating α and the negative rating η. Therefore, the FC increases the positive rating $\alpha_i(t)$ or the negative rating $\eta_i(t)$ of an SU by 1 if its detection matches (or not) the final decision. The credibility score of the SU_i is calculated by the FC using the following formula 11:

$$\varsigma_i = \frac{(\alpha_{i+1})}{(\alpha_i + \eta_{i+1})}. \tag{11}$$

Using the credibility score, the FC calculates the reputation value according to Equation 12:

$$r_i = \frac{\varsigma_i}{\sum_i \varsigma_i}. \tag{12}$$

Hence, higher reputation value r_i of SU_i indicates higher precision of its detection.

“Bayesian Networks.” A Bayesian network is a relationship that uses statistic methods to represent the probability connections between different elements. Its theoretical foundation is the Bayes rule. Wang et al[38] used a Bayesian approach to develop a defense solution against the malicious SUs. At first, they analyzed the single malicious user case. The suspicious level of each node is estimated by their reporting histories. When the suspicious level goes beyond certain threshold, a node will be considered as malicious. Thus, it will be excluded from the decision-making task. This approach expresses the reputation value of SU_i calculated by the FC with $r_i(t) = 1 - \pi_i(t)$ at time slot t, where $\pi_i(t)$ is the suspicious value. The BS SU gathers the sensing outcomes from all the SUs in the CRN. Then, it calculates the final decision using the suspicious level of each user based on the Bayesian criterion, which is expressed by formula 13:

$$\pi_i = \frac{\prod_{\tau=1}^{t} \rho_i(\tau)}{\sum_{j=1}^{N} \prod_{\tau=1}^{t} \rho_j(\tau)}, \tag{13}$$

where $\rho_i(\tau)$ is the probability of the existence of PUs activities at $node_i$ from time slot $\tau = 1$ to t given that $node_i$ is malicious. Thus, an additional parameter, called trust consistency value $\Psi_i(t)$, is computed. In fact, it keeps track of the difference between the reputation value $r_i(t)$ and the mean of the reputation values. Therefore, a sensing detection of SU_i is accepted by the decision FC if $r_i(t) > rT(t)$ and $\Psi_i(t) > \Psi T(t)$, where rT(t) and $\Psi T(t)$ are both thresholds. In fact, several authors, such as in Huo et al[39] and Fangwei et al [40] aimed at securing the CRN using the trust management that is defined by the Bayesian network modeling.

“Fuzzy logic.” This method gives a way to get a definite and precise conclusion. The fuzzy logic process begins with receiving the input values representing the measures of the parameters to be analyzed. Then, it subjects the input values

TABLE 4 The payoff matrix for the DFC and a malicious SU

	SU_i **reports** S_i^t	SU_i **reports** $S_i^{\prime t}$
DFC checks	$L(S_i^t, R_i^t)$-C, -$L(S_i^t, R_i^t)$	$L(S_i^{\prime t}, R_i^t)$-C, -$L(S_i^{\prime t}, R_i^t)$
DFC does not check	-$G(S_i^t, O_i^t, R_i^t)$, $G(S_i^t, O_i^t, R_i^t)$	-$G(S_i^{\prime t}, O_i^t, R_i^t)$, $G(S_i^{\prime t}, O_i^t, R_i^t)$

Abbreviations: DFC, data fusion center; SU, secondary user.

to the fuzzy rules. The process passes to average and weights the results into one output decision. Taghavi et al[41] proposed a trust algorithm for CRNs by using the fuzzy logic that prefilters the sensing results of SUs. To detect the malicious users, the authors selected sensing outcomes as input parameters to the fuzzy controller. The input parameters are 3 membership functions designed by always no malicious, trusted, and always yes malicious. The output parameters are 2 fuzzy functions called fuzzy trust level (FTL) (when the sensing result is trusted user) and fuzzy suspicious level (when the sensing result is always no malicious user or the sensing result is always yes malicious user). To make the final decision by exempting the sensing of malicious users and combining each detection, the authors have considered only its FTL. Then, the final decision is calculated using the summation of FTLs of all users. Finally, the FC decides the PU presence if the obtained value is greater than a given threshold (eT). Similarly, in Wang et al,[42] the authors aimed at securing the cooperative spectrum sensing using a trust fuzzy scheme.

"Game Theory." It is a mathematical tool that illustrates the strategic collaborations and interactions among multiple decision makers. It provides a mathematical basis for the analysis of interactive decision-making process between a number of rational players. It also provides tools for predicting what might happen when players with conflicting interests interact. In this context, Wang et al[43] exploited the interest of game theory modeling to propose a new trust-based data aggregation scheme to encourage the malicious user to send a correct detection in the cooperative spectrum sensing in CRNs. To make the final decision, the data fusion center (DFC) gathers the detections O_i^t from the SU with a higher reputation value R_i^t and capacity of detection S_i^t using the aggregation function G. However, the malicious SU can generate a faulty capacity $S_i^{\prime t}$ higher than the ordinary capacity to be chosen in the detection spectrum task that may affect the final decision. Consequently, the DFC needs to check the spectrum to take a accurate decision and punishes the malicious SU with faulty capacity using the punishment function L with sensing cost C. The interaction between the DCF and the SU malicious is described by game theory, which is defined in Table 4.

To encourage the SU from reporting a fake capability sensing, the DFC checking probability p^t, aggregation function G, and punishment function L should satisfy the condition expressed by formula 14:

$$p^t > \frac{\Delta G}{\Delta G + \Delta L}. \tag{14}$$

Furthermore, many researchers become more interested in trust management based on game theory such as the authors in previous studies[44,45] who used this modeling to define the trust level between entities to secure the network from the misbehaving and malicious users.

4.2 | Strategy

In CRN, the SUs can cooperate and collaborate with each other by sharing its local sensing results to make an undoubted final decision. This strategy is called the collaborative sensing which is adopted very often in CNRs. However, the node can sense the spectrum and decides individually the presence of PU without cooperation with the other entities, which is called the individual strategy. The sensing strategy can be one of the classification criterion of the trust approaches in CNRs.

4.2.1 | Collaborative strategy (cooperative)

Through collaboration, SUs exchange messages, or share knowledge between themselves to achieve better CRN-wide performance enhancement compared with noncollaborative individual effort. Therefore, the collaborative strategy is widely used in CRNs to make a final and an undoubted decision. Thus, many trust management mechanisms are proposed secure the cooperation between entities. Kaligineedi et al[46] used the detection methods to evaluate reputation values in the centralized and the collaborative spectrum sensing scheme. This approach can identify and ignore sensing outcomes from malicious SUs with data falsification attacks and smart attacks. Once the local detections are filtered out, the SU BS calculates the final decision of SU_i at time slot t, by using historical sensing outcome values within time window L, according to the following formula 15:

$$D_i(t) = \sum_{(\alpha=t-L+1)}^{t} D(\alpha), \tag{15}$$

where $D_i(\alpha)$ is the sensing outcome of SU_i at time α. If the value of $D_i(t)$ deviates from the underlying distribution, SU_i is considered to be malicious. Otherwise, it is considered to be honest. Indeed, the final decision $D_i(t)$ is used to calculate the SU_i reputation value by setting the upper and the lower limit or by evaluating the $D_i(t)$ from the median $mD(t)$ in a decreasing exponential manner. The final decision at SU BS is calculated on the basis of N users reputation values and sensing outcomes, which is expressed by Equation 16:

$$D = \sum_{(i=1)}^{N} r_i(t) d_i(t). \tag{16}$$

Due to the importance of cooperation between the entities in CRN, many trust mechanisms such as Du et al[47] and Premarathnea et al[48] are proposed in literature to secure the collaborative exchange.

4.2.2 | Individual strategy (noncooperative)

In noncooperative detection, sensing is accomplished by a single CR node without collaborating with other SUs. Energy based detection is the most widespread mechanism to determine the spectrum availability. In energy detection, the node monitors the received energy over certain time periods. Comparing the observed value with a predefined energy threshold, the SU decides the spectrum availability. However, in literature, the trust approaches based on the individual detection are rarely used due to the cooperative detection privileges. Dubey et al[49] provided individual methods to determine if a PU emulator is present in the network when the PU location is known and fixed as coordinates. Indeed, this method uses a trust-based transmitter verification scheme to properly check the PU presence. It is assumed that all radios are aware of the location and the distance to the PUs in the area. The distance between the PU and the cognitive radio is calculated based on known coordinates. The distance between radio and the user sending the PU type signal is also computed based on the received power levels. The trustworthiness of the user is determined by comparing the resulting distances. In the literature,[50] Jeon et al introduced 2 trust methods for both noncooperative and cooperative strategies in the CRNs.

4.3 | Topology

As classical network, the design of the cognitive network can adopt one of the known topology based on the desired application and the final objective. The node can be organized in ad hoc, mobile and cluster-based manner. To apply the trust management in CRNs, we must take in consideration the topology adopted by the network. For this reason, many trust approaches are invented for each CRN type. It is one of new trust management classification approaches.

4.3.1 | Ad hoc topology

In ad hoc topology, the nodes send their spectrum detections to the sink in multiple hops. This topology imposes less communication overhead in terms of controlling data. However, due to the hidden terminal problem, spectrum sensing results may be inaccurate. The decision about the availability of the channel can be affected by many damaging attacks such as the SSDF. To defend the SSDF attacks in the distributed cognitive ad hoc network, Yu et al[51] proposed a trust scheme. The SUs exchange regularly information and take independently the decision upend the PU presence. Each SU applies the energy detection mechanism to detect the presence of PU activities in the channel. Then, the SU updates its measurements from similar information received by its neighbors, and it sends back the updated information. In fact, the information sent by the attackers is filtered out. Each SU calculates the maximum difference between the received information and the mean value. The users having the higher deviation are designed to be malicious and misbehaving. Their input is exempted later from the final decision. Each user decides that the band under test is occupied if the average result, after the exempting of the information provided by the attackers, is greater than a threshold. Therefore, the final decision for each user depends on the average result computed using its local detection along with that received by the neighboring nodes. Due to the extensive and significant use of ad hoc topology in CRN, the objective of many approaches as the literature[52,53] is to secure the ad hoc CRN from the newer and the classical threats.

4.3.2 | Clustering topology

The nodes can follow a cluster placement where each node chooses an adequate cluster for being a member and each cluster is controlled by a CH (the leader group). To select the CHs and cluster members, many algorithms and approaches are developed. This cluster-based topology is an appropriate choice for an effective and a dynamic spectrum management with a local common control channel approach in cognitive network. Li et al[54] proposed a TRM schemes called sub-spectrum sensing scheme (SSSS) for collaborative spectrum sensing schemes in clustered networks. In SSSS, each CH makes the final decision on the channel availability and sends it to the FC. The reputation value of an SU_i is computed on the basis of the matching results of its detection $d_i(t)$ with the final decision $D(t)$. If there is a match, the SU reputation value is increased and vice versa. Secondary users with higher reputation values are given higher priorities to access the channels, which encourages the SUs to provide accurate sensing outcomes. The reputation value is calculated based on formula 17 as follows:

$$r_i(t) = r_i(t-1) + (-1)^{d_i(t)+D(t)}. \tag{17}$$

The mechanism begins with the spectrum bands division. Indeed, each node is assigned to sense corresponding band to increase the sensing efficiency. Secondly, the consideration of reputation can prevent the attacks. The FC makes the final decision by gathering the data from cognitive nodes and updates the reputation of each user according to formula 17. Finally, after updating the reputation value, the malicious nodes are detected and removed from the spectrum sensing task to assure the security of the network. Protecting the clustering in the CRNs by using the trust management is treated widely in the literature and several mechanisms are proposed as in Ling and Yau.[55]

4.3.3 | Mobile topology

When the cognitive nodes are mobile and move frequently, the appropriate topology to be adopted is the mobile one. Moreover, cognitive radio communication protocols and security mechanisms for CRNs must consider the mobility as well. The need of security in CRN increases with introducing mobility in the network. Therefore, Jana et al[56] developed a new trust collaborative spectrum sensing model for mobile cognitive networks by using the location reliability (LR) and the malicious intention parameters. Location reliability captures the trust level over different positions as distributions of path loss, which are not identical although they are independent. Malicious intention defines the trustworthy degree of a user. The FC evaluates the reports received by analyzing the location LR and the source malicious intention of the report. Another introduced approach aims at securing the network considering the user mobility. For instance, the authors in one study[57] suggested a trust mechanism for the cooperative spectrum sensing for mobile SUs. The area is divided into several cells. The trust values allows the removing of malicious users independently in each cell.

4.4 | Spectrum management

In the CRN, the spectrum detection manner used differs from each other depending on the spectrum allocation, the application type, the functional entity placement, etc. In fact, we have 3 major organizations: the centralized, the distributed, and the clustering spectrum sensing manner presenting our next trust management classification for the CRNs.

4.4.1 | Centralized manner

The centralized CRN has a central entity that controls the spectrum allocation and takes the final decision about the presence or the absence of the PU. Furthermore, the central entity can lease spectrum to users in a limited geographical region for a specific amount of time. To make an accurate decision, each node communicates with the central entity which can be the BS, FC, etc. This architecture is vulnerable to many attacks affecting specifically the center entities and paralyzing the CRN. Many authors proposed trust management mechanisms to secure and to protect the centralized network such as Pei et al[58] who suggested a trust management model for the centralized network to detect the malicious SUs (faulty and selfish) and to protect the PUs from the interferences. Each SU BS entity is placed in the center surrounded by its SUs host. The SUs detect the spectrum band and send their sensing results to the SU BS to make the decision about the PU activities. Therefore, the SU BS is aware of the transmissions from its SU hosts through overhearing their packets. When a SU does not respect the presence of the PU and it transmits in the occupied channel, the SU BS is aware of it and punishes this malicious user by reducing the trust $r_i(t+1)$ by using its previous value $r_i(t-1)$ and the current value $r_i(t)$, which is expressed by formula 18:

$$r_i(t+1) = (1-\alpha) \times r_i(t-1) + \alpha \times r_i(t), \tag{18}$$

where $0 \leq \alpha \leq 1$ is a learning rate. The SU BS classifies the SUs as honest, malicious, or unknown based on the updated reputation value. Finally, SU BS grants the honest SUs channel access opportunity on the basis of their reputation values. In the same context, the authors in Li et al[59] and Pei et al[60] proposed 2 trust mechanisms to secure the centralized CRN from the attacks threatening mainly the final decision taken by the central entity to deprive the SUs from accessing the free channel.

4.4.2 | Distributed manner

The distributed CRN is characterized by the absence of the central entity in the network. Each node detects the spectrum band by using specific mechanisms. Then, it makes individually and independently its own decision. It can cooperate with the other nodes by sharing the trust and reputation value to make a precise decision about the PU activities. To secure the distributed architecture from the malicious and faulty nodes, Zhendong et al in the literature[61] proposed a trust game model to secure the cooperative detections by using game theory and reputation system. This approach encourages the SUs to choose the honest strategy. The authors began with 3 hypotheses:

- The SUs participate in the cooperative spectrum detection in distributed manner: The network does not have a centralized entity that makes a centralized decision. Each SU takes its local decision basing on the fusion rules (AND/OR).
- The SU honest participates in the spectrum detection task. Then, it sends its correct sensing results to the others SUs. The malicious SU obtains the spectrum information by listening to the sensing exchange. After that, it sends a faulty detection to other SUs.
- The behaviors of malicious SUs are independent and rational to maximize their gains during their lifetimes.

The authors computed the reputation value by using the following formula 19:

$$T_i^p = \frac{K}{\sum_{k=1}^{K}[\min_{SU_j \in \Omega_j, l \in k} GoTrust_{i,j}^l \times (\min_{l \in k} LCRTDS_i^l \times \min_{l \in k} DCR_i^l)^{-1}]}. \tag{19}$$

T^p presents the trust value, GoTrust is defined as the global reputation of SU_i by SU_j, LCRTDS denotes the times in which SU_i continues to send faulty information before sending correct sensing data. T^p parameter is used to judge whether the malicious behavior of SUs is occasional or intentional. DCR denotes the times in which SUs send false sensing information discontinuously in the most recent period. To secure the distributed CRN, many trust approaches as Lin et al[62] are proposed to improve the performance of network with the presence of faulty and malicious attackers .

4.4.3 | Cluster-based manner

As we have motioned before, securing cluster-based in the CRN becomes an indispensable task to ensure the centralized final decision making about the PU activities by the CH entities. Therefore, using trust management as a security mechanism for this architecture seems to be very efficient. Several approaches are proposed in literature such as the trust mechanism proposed in Koh et al[63] to secure the cluster-based architecture.

5 | CONCLUSION AND DISCUSSION

The Internet of Things (IoT) is a worldwide network of interconnected objects communication through standards protocols. However, the limited range problem of the wireless techniques, the interference problems due to the huge number of connected objects, the continuous connectivity to the objects that cannot be available at every place, and the necessity of spectrum sharing make the integration of the CR in the IoT increasingly considered.[64] Indeed, the adaptability of CRNs into IoT reveals new challenges as the security of cognitive added features. Securing the Internet of cognitive radio things by using the trust management techniques becomes an emergent issue in the literature. Moreover, the cognitive radio concept is recently added to the fifth generation mobile network (5G) to resolve the problem of massive data transfer from hundreds of thousands of simultaneous connections and users.[65,66] Securing the upcoming 5G mobile cognitive networks is considered to be one of the main challenges for the cognitive 5G concept. Therefore, the trust management and reputation can be one of the newest research field to propose emergent solutions and approaches to ensure the security of the 5G network with the cognitive radio technologies.

By way of conclusion, the CR concept becomes more and more popular by paving gradually its way into modern technologies as IoT, 5G, Vanet, etc. Thus, it becomes a more alluring and an attractive solution to the classical wireless problems. However, due to resources constraints, the open nature of the wireless medium, and the cognitive features, the CRNs face many security challenges. To make the network more reliable and more trustworthy, many approaches were proposed. In this paper, we focused on the use of TRM mechanisms to secure CRNs. Firstly, we identified the different attacks and threats that can affect the CRNs. Then, we detailed how the trust is defined in different disciplines and how the trust concepts can be applied to secure the CRNs. Secondly, we illustrated the trust management characteristics and challenges. At the end, we resumed the TRM approaches using the existing classifications (attack, propriety, and purpose) in the literature. Therefore, these classifications are incomplete since they do not consider all the important concepts in the CRNs. Consequently, we proposed an exhaustive and complete TRM classification for the CRNs that organizes the trust mechanisms based on 4 important criteria: the topology of the network (static, mobile), the trust value computation (probability, rating, weighting, Bayesian networks, fuzzy logic, and game theory), the strategy used by the SU to detect the spectrum band (cooperative and noncooperative), and the spectrum management (centralized, distributed, and clustering).

ORCID

Jihen Bennaceur http://orcid.org/0000-0001-8584-5253

REFERENCES

1. Mitola J. Cognitive Radio Architecture Evolution Systems. *Proceedings of the IEEE*. 2009;97(4):626-641.
2. Bawiskar A, Meshram BB. Survey of attacks on wireless network. *Int J Innovative Res Comput Commun Eng*. 2013;1(1):90-100.
3. Nanthini SB, Hemalatha M, Manivannan D, Devasena L. Attacks in cognitive radio networks (CRN)—a survey. *Indian J Sci Technol*. 2014;7(4):530-536.
4. Yu Y, Hu L, Li H, Zhang Y, Wu F, Chu J. The Security of Physical Layer in Cognitive Radio Networks. *J Commun*. 2014;9(12):28-33.
5. Sharifi AA, Sharifi M, Niya MJM. Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach. *AEU Int J Electron Commun*. 2015;70(1):95-104.
6. Ta DT, Nguyen-Thanh N, MaillÃl' P, Ciblat P. *Van-Tam Nguyen, Mitigating Primary Emulation Attacks in Multi-Channel Cognitive Radio Networks: A Surveillance Game*. USA: IEEE Globecom; 2016.
7. Mourougayane K, Srikanth S. Intelligent Jamming Threats to Cognitive Radio based Strategic Communication Networks - A Survey. In: 3rd International Conference on Signal Processing. Chennai, India: Communication and Networking (ICSCN); 2015.
8. Oskoui MG, Khorramshahi P, Salehi JA. Using game theory to battle jammer in control channels of cognitive radio ad hoc networks. In: International Conference on Communications ICC; Kuala Lumpur, Malaysia; 2016.
9. Gao Q, Huo Y, Ma L, et al. *Optimal Stopping Theory Based Jammer Selection for Securing Cooperative Cognitive Radio Networks*. USA: IEEE Globecom; 2016.
10. Cai Y, Xu X, He B, Yang W, Zhou X. Protecting cognitive radio networks against poisson distributed eavesdroppers. In: International Conference on Communications ICC; Kuala Lumpur, Malaysia; 2016.
11. Ouyang J, Zhu WP, Massicotte D, Lin M. Energy efficient optimization for physical layer security in cognitive relay networks. In: International Conference on Communications ICC; Kuala Lumpur, Malaysia; 2016.
12. Rajalakshmi S, Saravanan K. Survey on link layer attacks in cognitive radio networks. *Int J Comput Sci Eng Inf Technol (IJCSEIT)*. 2013;3(6):9-13.
13. Yu Y, Hu L, Li H, Zhang Y, Wu F, Chu J. The Security of physical layer in cognitive radio networks. *J Commun*. 2014;9(12):28-33.
14. Marinho J, Granjal J, Monteiro E. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP J Inf Secur*. 2015:1-14.
15. Fragkiadakis A, Angelakis V, Tragos EZ. Securing Cognitive Wireless Sensor Networks: A Survey. In: Int J Distrib Sens Netw; 2014:1-12.
16. Ibrahim Md, Rahman MM, Roy MC. Detecting sinkhole attacks in wireless sensor network using hop count. *I J Comput Netw Inf Secur*. 2015:50-56.

17. Cho JH, Swami A, Chen IR. A survey on trust management for mobile ad hoc networks. *IEEE Commun Surv Tutorials*. 2011;13(4):562-583.
18. Khalid O, Khan SU, Madani SA, Hayat K, Khan MI. Comparative study of trust and reputation systems for wireless sensor networks. *Secur Commun Netw*. 2013;6(6):669-688.
19. Sherchan W, Nepal S, Paris C. A survey of trust in social networks. *ACM Comput Surv*. 2013;45(4):1-33.
20. Zhang N, Lu N, Lu R, Mark JW, Shen X. Energy-efficient and trust-aware cooperation in cognitive radio networks. In: IEEE International Conference on Communications (ICC); Canada; 2012.
21. Feng J, Lu G, Bao Z. Weighted-Cooperative Spectrum Sensing Scheme using Trust in Cognitive Radio Networks. Vol. 3. China: Sig Process (ICSP); 2012.
22. Parvin S, Hussain FK. Trust-based security for community-based cognitive radio networks. In: IEEE International Conference on Advanced Information Networking and Applications; Japan; 2012.
23. Sagduyu YE. Securing cognitive radio networks with dynamic trust against spectrum sensing data falsification. In: IEEE Military Communications Conference; USA; 2014.
24. Xu S, Shang Y, Wang H. Double thresholds based cooperative spectrum sensing against untrusted secondary users in cognitive radio networks. In: IEEE Vehicular Technology Conference; Spain; 2009.
25. Parvin S, Han, Tian B, Hussain FK, Farque MA. Trust-based authentication for secure communication in cognitive radio networks. In: Embedded and Ubiquitous Computing; China; 2009.
26. Zhang G, Chen Z, Tian L, Zhang D. Using trust to establish a secure routing model in cognitive radio network. *Plos One J*. 2015;10(9): 1-15.
27. Fang H, Xu L, Xiao L. Secure routing and resource allocation based on Game theory in cooperative cognitive radio networks. *Concurrency and Computation: Pract Experience*. 2015;27(7):2958-2977.
28. Zhang K, Pawelczak P, Cabric D. Reputation-based cooperative spectrum sensing with trusted notes assistance. *IEEE Commun Lett*. 2010;14(3):1-10.
29. Afsana F, Jahan N, Sunny FA. Trust and energy aware cluster modeling and spectrum handoff for cognitive radio ad-hoc network. In: Electrical Engineering and Information and Communication Technology (lCEEICT); Bangladesh; 2015.
30. Koh CWK, Yau KLA. Trust and reputation scheme for clustering in cognitive radio networks. In: Frontiers of Communications, Networks and Applications; Malaysia; 2014.
31. Fangwei L, Fan L, Jiang Z, Yifang N. Reputation-based secure spectrum situation fusion in distributed cognitive radio networks. *Posts Telecommun*. 2015;22(3):110-117.
32. Wengui S, Yang L. A jury-based trust management mechanism in distributed cognitive radio networks. *IEEE, China Commun*. 2015;12(7):119-126.
33. Jin Z, Anand S, Subbalakshmi KP. Detecting primary user emulation attacks in dynamic spectrum access networks. In: IEEE International Conference on Communications; Germany; 2009.
34. Feng J, Zhang Y, Lu G, Zheng W. Securing cooperative spectrum sensing against ISSDF attack using dynamic trust evaluation in cognitive radio networks. *Secur Commun Netw*. 2015;8(17):3157-3166.
35. Li J, Feng Z, Wei Z, Feng Z, Zhang P. Security management based on trust determination in cognitive radio networks. *EURASIP J Adv Sig Process*. 2014;14(1):1-16.
36. Zhang G, Ding R, Huang L. Using trust to establish cooperative spectrum sensing framework. *Procedia Eng*. 2011;15(11):1361-1365.
37. Arshad K, Moessner K. Robust collaborative spectrum sensing based on beta Reputation system. In: Future Network and Mobile Summit; Poland; 2011.
38. Wang W, Li H, Sun Y, Han Z. Securing collaborative spectrum sensing against untrustworthy secondary users in cognitive radio networks. *EURASIP J Advances Sig Process*. 2010;10(4):1-15.
39. Huo Y, Wang Y, Lin W, Sun R. Three-layer Bayesian model based spectrum sensing to detect malicious attacks in cognitive radio networks. In: IEEE International Conference on Communication Workshop (ICCW); London, UK; 2015.
40. Fangwei L, Fan L, Jiang Z, Yifang N. Reputation-based secure spectrum situation fusion in distributed cognitive radio networks. *J China Univ Posts and Telecommun*. 2015;22(3):110-117.
41. Taghavi EM, Abolhassani B. A Two Step Secure Spectrum Sensing Algorithm Using Fuzzy Logic for Cognitive Radio Networks. *Int J Commun Netw Syst Sci*. 2011;4(8):507-513.
42. Wang Y, Li Y, Yuan F, Yang J. A Cooperative Spectrum Sensing Scheme Based on Trust and Fuzzy Logic for Cognitive Radio Sensor Networks. *IJCSI Int J Comput Sci Issues*. 2013;10(1):275-279.
43. Wang J, Chen IR. Trust-based data fusion mechanism design in cognitive radio networks. In: Cognitive Radio and Electromagnetic Spectrum Security; USA; 2014.
44. Afghah F, Costa M, Razi A, Abedi A, Ephremides A. A reputation-based Stackelberg game approach for spectrum sharing with cognitive cooperation. In: IEEE Conference on Decision and Control December; Italy; 2013.
45. Houjeij A, Saad W, Bascar T. A game-theoretic view on the physical layer security of cognitive radio networks. In: Communication and Information Systems Security Symposium; Budapest, Hungary; 2013.
46. Kaligineedi P, Khabbazian M, Bhargava VK. Secure cooperative sensing techniques for cognitive radio systems. In: IEEE International Conference on Communications; Beijing, China; 2008.
47. Du H, Fu S, Chu H. A credibility-based defense SSDF attacks scheme for the expulsion of malicious users in cognitive radio. *Int J Hybrid Inf Technol*. 2015;8(9):275-279.

48. Premarathnea US, Khalil I, Atiquzzaman M. Trust based reliable transmission strategies for smart home energy management in cognitive radio based smart grid. *Ad Hoc Netw*. 2016;41(4):15-29.

49. Dubey R, Sharma S, Chouhan L. Secure and trusted algorithm for cognitive radio network. In: Wireless and Optical Communications Networks (WOCN); India; 2012.

50. Jeon H, McLaughlin SW, Kim IM, Ha J. Secure communications with untrusted secondary nodes in cognitive radio networks. *IEEE Trans Wireless Commun*. 2014;13(4):1790-1805.

51. Yu F, Huang M, Li Z, Mason P. Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In: Military Communications Conference; USA; 2009.

52. Vosoughi A, Cavallaro JR, Marshall A. A cooperative spectrum sensing scheme for cognitive radio ad hoc networks based on gossip and trust. In: Signal and Information Processing (GlobalSIP); USA; 2014.

53. Amjad MF, Aslam B, Attiah A, Zou CC. Towards trustworthy collaboration in spectrum sensing for ad hoc cognitive radio networks. *Wireless Netw*. 2016;22(1):781-797.

54. Li H, Pei Q, Jiang X, Liang R, Geng P. A subspectrum sensing scheme based on reputation in cognitive radio networks. In: Computational Intelligence and Security; China; 2010.

55. Ling MH, Yau KLA. Reinforcement learning-based trust and reputation model for cluster head selection in cognitive radio networks. In: Internet Technology and Secured Transaction (ICITST); London, UK; 2014.

56. Jana S, Zeng K, Cheng W, Mohapatra P. Trusted collaborative spectrum sensing for mobile cognitive radio networks. *Inf Forensics Secur*. 2013;8(9).

57. Wang X, Jia M, Guo Q, Gu X. A Trust-value based Cooperative Spectrum Sensing Algorithm for Mobile Secondary Users. In: International Conference on Communication Workshop (ICCW); London, UK; 2015.

58. Pei Q, Liang R, Li H. A trust management model in centralized cognitive radio network. In: Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC); China; 2011.

59. Li H, Cheng X, Li K, Hu C, Zhang N, Xue W. Robust collaborative spectrum sensing schemes for cognitive radio networks. *IEEE Trans Parallel Distrib Syst*. 2014;25(8):2190-2200.

60. Pei Q, Yuan B, Li L, Li H. A sensing and etiquette reputation-based trust management for centralized cognitive radio network. *Neurocomputing*. 2013;101(15):129-138.

61. Zhendong W, Huiqiang W, Qiang Z. A trust game model and algorithm for cooperative spectrum sensing in cognitive radio networks. *Future Generation Communication and Networking*. 2015;8(3):1-14.

62. Lin H, Hu J, Huang C, Xu L, Wu B. Secure cooperative spectrum sensing and allocation in distributed cognitive radio networks. *Int J Distrib Sens Netw*. 2015;10.

63. Koh CWK, Yau KLA. Trust and reputation scheme for cognitive radio networks. In: Frontiers of Communications, Networks and Applications (ICFCNA); 2014.

64. Khanm AA, Rehman MH, Rached A. When cognitive radio meets the internet of things? In: Wireless Communications and Mobile Computing Conference (IWCMC); 2016.

65. Yang C, Li J, Guizani M, Anpalagan A, Elkashlan M. Advanced spectrum sharing in 5G cognitive heterogeneous networks. *IEEE Wireless Commun*. 2016;23(2):94-101.

66. Sexton C, Kaminski N, Marquez-Barja J, Marchetti N, Luiz A, Silva D. 5G: Adaptable networks enabled by versatile radio access technologies. *IEEE Commun Surv Tutorials*. 2017;99:688-720.

Jihen Bennaceur received her diploma in Computer Science from the Faculty of Science Gabes, Tunisia, in 2012. She received her Master's degree in Computer Networks from the Higher Institute of Computer Science and Communication Technologies, Sousse, Tunisia, in 2015. She received the Best Project Award from the Faculty of Science Gabes, in 2012. Since 2015, she is a PhD student at National School of Computer Science (ENSI), Tunisia. She is a member researcher in the CRISTAL laboratory, Tunisia. Her research interests are in the areas of wireless sensor networks, cognitive networks, security, with emphasis on mathematical modeling and performance analysis.

Hanen Idoudi earned her engineering and master degrees in computer science at the National School of Computer Science, University of Manouba, Tunisia in 2001 and 2002, respectively. She received her PhD joint degree from University of Rennes 1, France (where she was also member of IRISA, INRIA, Rennes), in 2008. Since 2009, she holds the position of assistant professor at the National School of Computer Science. Previously, she worked as lecturer at the National School of Computer Science and at the Higher Institute of Arts and Multimedia in Tunisia. She worked also for 3 years as a Networks engineer. Her research focuses on issues related to wireless networking (ad hoc, sensor, mesh, and cognitive networks): efficient MAC protocols design, networks modeling and performances, routing, quality of service (QoS), and energy conservation.

Leila Azouz Saïdane is a Professor at the National School of Computer Science (ENSI), at The University of Manouba, in Tunisia and the Chairperson of the PhD Commission at ENSI. She was the Director of this school and the supervisor of the Master's degree program in Networks and Multimedia Systems. She is the codirector of RAMSIS pole of CRISTAL Research Laboratory (Center of Research in Network and System Architecture, Multimedia and Image Processing) at ENSI. She collaborated on several international projects. She is author and coauthor of several papers in refereed journals, magazines, and international conferences.

How to cite this article: Bennaceur J, Idoudi H, Azouz Saidane L. Trust management in cognitive radio networks: A survey. *Int J Network Mgmt*. 2017;e1999. https://doi.org/10.1002/nem.1999