Hindawi
Security and Communication Networks
Volume 2017, Article ID 3261058, 16 pages
https://doi.org/10.1155/2017/3261058

Research Article

A Collaborative Approach for Monitoring Nodes Behavior during Spectrum Sensing to Mitigate Multiple Attacks in Cognitive Radio Networks

Mahmoud Khasawneh and Anjali Agarwal

Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada

Correspondence should be addressed to Mahmoud Khasawneh; m_khasaw@encs.concordia.ca

Received 19 June 2017; Revised 20 August 2017; Accepted 14 September 2017; Published 19 October 2017

Academic Editor: Angelos Antonopoulos

Spectrum sensing is the first step to overcome the spectrum scarcity problem in Cognitive Radio Networks (CRNs) wherein all unutilized subbands in the radio environment are explored for better spectrum utilization. Adversary nodes can threaten these spectrum sensing results by launching passive and active attacks that prevent legitimate nodes from using the spectrum efficiently. Securing the spectrum sensing process has become an important issue in CRNs in order to ensure reliable and secure spectrum sensing and fair management of resources. In this paper, a novel collaborative approach during spectrum sensing process is proposed. It monitors the behavior of sensing nodes and identifies the malicious and misbehaving sensing nodes. The proposed approach measures the node's sensing reliability using a value called belief level. All the sensing nodes are grouped into a specific number of clusters. In each cluster, a sensing node is selected as a cluster head that is responsible for collecting sensing-reputation reports from different cognitive nodes about each node in the same cluster. The cluster head analyzes information to monitor and judge the nodes' behavior. By simulating the proposed approach, we showed its importance and its efficiency for achieving better spectrum security by mitigating multiple passive and active attacks.

1. Introduction

In Cognitive Radio Networks (CRNs), as most of the spectrum is assigned to specific users known as licensed users (primary users (PUs)), the most important challenge is to share the licensed spectrum between the licensed users (PUs) and the unlicensed users (secondary users (SUs)) when the PUs are inactive [1].

Cognitive radio techniques provide the capability to use or share the spectrum in an opportunistic manner. The SUs have to detect the unused spectrum bands, which are known as spectrum holes, and this process is called spectrum sensing [2]. Spectrum sensing is recognized as the basic functionality provided by CR. In the spectrum sensing process, the SUs continue to monitor the channel(s) that are owned by the PU(s). Once a channel is available, the SUs can start to use it. Failing to sense the spectrum correctly might cause substantial interference for those that use the spectrum and therefore may lead to inefficient spectrum utilization. When the conditions of a CRN are more dynamic, collaborative sensing helps to detect spectrum holes faster [3]. The detection probability to obtain correct sensing results is increased when the cooperation concept is applied among the different secondary users. Additionally, cooperative spectrum sensing alleviates the negative impacts on performance caused by multipath fading and shadowing [2]. Every cognitive user that participates in the cooperative spectrum sensing first senses the spectrum using any spectrum sensing method such as matched filter, energy detection, or cyclostationary feature detection [4]. This is followed by the exchange of their initial detection decisions and making the final sensing decision based on all the nodes' sensing results.

As in any other type of wireless networks, CRNs are vulnerable to many security attacks (both passive and active) especially during the spectrum sensing phase. The radio technology itself is vulnerable to attacks, since any radio

frequency can be blocked or jammed if a transmitter sends a signal at the same frequency with enough power. There is no control over the behavior of these unlicensed users, which threatens the security of the licensed users. The most important behaviors of attackers can be categorized into the following: (i) misbehaving, (ii) selfish, (iii) cheating, or (iv) malicious [5]. A misbehaving user does not obey the rules set in the network by an authority entity. A selfish user wants to keep the network resources for its own use and it does not care about other network users if they benefit from the network or not. A cheating user does not give true information about the network resources on purpose to increase its quality of service (QoS). A malicious user intentionally targets the network on purpose to degrade the other nodes QoS and the network efficiency. If a node behaves in one of the previous categories, the node will be an adversary node and it might launch multiple attacks. An attacker that behaves in one of these ways during spectrum sensing can emulate PUs or send false sensing results. The attacker aims to prevent other nodes from using the spectrum efficiently, keep network resources for its own benefits, reduce the quality of service (QoS) of other nodes, and therefore degrade the network security and performance.

As security is an important issue in the context of any wireless network as well as in CRN, researchers have moved their interest towards it [6]. New attacks have been introduced, which are unique to CRNs especially during spectrum sensing process, whereas malicious nodes use the vulnerability of the CR reliability issues to attack a CRN. The attack is active as long as a network node is behaving in any of the attacker behaviors and is affecting the network security. Otherwise, the attack is passive and the network node is waiting for a chance to switch to an active attack. Addressing passive attacker behavior or attacks is important as it is considered a proactive solution to prevent such behavior or such attacks from switching to active attacks if they have the chance to do so. Primary User Emulation Attack (PUEA) in [7–10] and Spectrum Sensing Data Falsification Attack (SSDF) in [11–13] are two examples of attacks, which are unique to CRN. These attacks occur during the spectrum sensing phase. They are results of the different attacker behaviors and they both can be passive or active. PUEA is an active attack when a malicious node is emulating a PU, while other nodes are unable to detect it before making their own sensing decision. PUEA is a passive attack when other nodes can detect the malicious node before making their own sensing decision. SSDF is an active attack if a node sends false sensing results to the other nodes in the network, and they consider its false sensing results in making their own sensing decision. SSDF is a passive attack if its sensing results are not considered in making the final sensing decision. Unlike most researchers who have focused on addressing the active attacks individually, Althunibat et al. and Sucasas et al. have addressed mutable attacks simultaneously [14, 15]. They have analyzed PUEA and SSDF in their active state. To the best of our knowledge, the attacker behaviors that may lead to passive and active attacks, which may launch more than one attack at the same time, have not been studied.

Table 1: The relationship between attacks and adversary nodes behavior.

Attack name	Adversary node behavior
PUEA	Misbehaving, malicious, and cheating
SSDF	Misbehaving, cheating, and selfish
DoS	Misbehaving, malicious, selfish, and cheating
Collusion	Misbehaving, selfish, malicious, and cheating
Objective function	Misbehaving and malicious

There are other attacks addressed in other types of wireless networks such as DoS, collusion, and objective function attacks [6] that can be launched in CRNs as a result of PUEA and/or SSDF attacks. In the DoS attack, the adversary node acts normally in the network to gain the trust of the other nodes and then targets the network by behaving in one of the attacker behavior categories. The DoS attack is an active attack. Another form of the DoS attack is when the adversary node emulates a PU signal (i.e., launches PUEA) to force other nodes to vacate the spectrum. The DoS attack [16] results in degrading other nodes quality of service (QoS). In the collusion attack, multiple adversary nodes agree on targeting benign node(s) in order to eliminate normal behaving nodes. During this time, adversary nodes keep the network resources for their own use. In the objective function attack, one or multiple adversary nodes try to change the radio parameters (e.g., center frequency, bandwidth, or modulation). Addressing such attacks is important in CRNs especially during the spectrum sensing phase as it results in improving network performance, security, and spectrum utilization.

Any attack is a result of an attackers' behavior. Therefore, mitigating the attackers' behavior will lead to detect and mitigate fewer simultaneous attacks without addressing the attacks themselves.

In Table 1, we show the different attacks that might be launched as a result of one or multiple adversary nodes behaviors.

In this paper and in [17, 18], the attackers' behaviors rather than the attacks themselves are addressed for the first time in CRNs. It was not considered before in the literature of CRN security. In [17], we proposed an approach for monitoring nodes' behavior during the spectrum sensing process, and in [18], we used it to propose a novel and secure routing algorithm. By mitigating the attacker's behavior(s), we can mitigate multiple attacks while they are active or passive. The proposed approach is an interweave approach (i.e., it is an opportunistic spectrum access approach), wherein the different SUs keep monitoring the spectrum band to find the opportunity to access it when the PUs are absent. Meanwhile, the SUs have to leave the spectrum band upon the presence of PUs. We use the concept of reputation-based mitigation systems which have been recently addressed by researchers in CRN and wireless sensor networks (WSN) [19–21] and merge it with the cooperative spectrum sensing in order to monitor the behavior of the nodes participating in the spectrum sensing process.

We propose a collaborative approach that monitors nodes' behavior in order to identify and penalize malicious and misbehaving node(s) during the spectrum sensing phase. Each sensing node is assigned a value called belief level (BL), which is used to describe their reliability in making the final sensing decision. During the spectrum sensing phase, each network node senses the spectrum and then forwards its sensing decision to its neighbors and to a central point within the cluster namely cluster head (CH). The behavior of the sensing nodes is monitored by each other and it is reported to the CH that analyzes them in order to penalize the adversary node(s) and reward the normal behaving node(s). We secure the messages sent between the different network nodes by encrypting them using the symmetric key cryptography, which has many advantages such as its straightforwardness, its less memory occupation, its less memory use, and its less power utilization [22]. Permitting only normal behaving sensing nodes to participate in the spectrum sensing process and to access the network resources helps to fairly share and manage the network resources, hence improving the spectrum security and utilization.

The contributions of this paper can be summarized as follows:

(i) To the best of our knowledge, it is the first work in CRN security that focuses on addressing the adversary nodes' behaviors, instead of focusing on the attacks, themselves. By doing so,

  (a) multiple attacks other than just PUEA and SSDF attacks, such as DoS, collusion, and objective function attacks, are mitigated;

  (b) the proposed approach works as a reactive approach to active attacks and as a proactive approach to passive attacks;

  (c) the proposed approach increases the probability of detecting adversary nodes, which improves the spectrum utilization.

(ii) Two additional metrics, the false alarm and detection probability, used for showing the performance of the proposed approach have been added and compared with other state-of-the-art models.

(iii) The proposed approach increases the probability of detecting vacant spectrum channels and it also decreases the false alarm probability.

(iv) It secures the sensing-reputation reports exchanged between the different sensing nodes by encrypting the messages carrying them through the public and symmetric key cryptography.

(v) A new K-rule is proposed. It helps in making the sensing process faster and more secure.

The rest of this paper is organized as follows: a literature review is conducted in Section 2. The threat model is shown in Section 3. Section 4 shows the proposed approach in detail. Section 5 presents the complexity analysis of the proposed approach. In Section 6, the proposed approach is simulated and its performance is evaluated and compared to other models. We analyze the proposed approach from the security perspective and we show the different attacks that it can detect and mitigate in Section 7. We conclude the paper and show future directions in Section 8.

2. Related Work

During the spectrum sensing phase, PUEA and SSDF attacks are the main attacks that affect the accuracy of the spectrum sensing results. Both of these attacks can perform in an active or passive way. Detection and mitigation of these two attacks have received considerable attention from researchers in CRNs.

In PUEA, an attacker may modify their air interface as it emulates the primary user's signal characteristics [15]. In this attack, other secondary users SUs will falsely determine that the frequency is in use by a legitimate primary user while in real it is not. Therefore, if the other SUs vacate the frequency accordingly, PUEA is considered an active attack; otherwise it is a passive attack. The following research work addresses the active PUEA. In [23], a robust technique for spectrum sensing process is proposed based on the principal component analysis to find any attack targeting the network. A detection method of PUEA is proposed in [24]. A sequence of steps is followed by all secondary users in the network until the adversary nodes are eliminated from the spectrum sensing process. In [25], the different SUs in the network send the sensing information to a fusion center, which uses estimation algorithms to differentiate the primary user from the attacker. A new scheme, namely, INCA, for detecting PUEA in decentralized cognitive radio ad hoc networks is described in [26]. All SUs cooperate with each other to identify the node(s) that emulate PU as they broadcast the probability of PU's presence to each other. This probability is calculated based on some predetermined criteria such as the received signal strength, transmission power, distance, noise, and/or transmission rate. Despite the improvement of the detection probability that INCA showed the maximum value of the detection probability that can be reached is 0.5, which is relatively not enough to rely on this mechanism.

In SSDF attack, the attackers participate in the sensing process by sharing wrong sensing with the other nodes in the network. By doing so, the attackers aim to selfishly keep the network resources for themselves only or the attackers may aim to disrupt the network throughput for other reasons. The following research addresses the active SSDF. In [27], a mitigation method for SSDF attack is proposed. During the sensing process, all the network nodes including the malicious ones and the other SUs make their own decisions about the presence/absence of PUs in their bands, and then those decisions are forwarded to a central point called fusion center. The fusion center counts the number of times each node has the right decision about the PU, which is referred to as *measure*. The node's observations accuracy increases, as the *measure* value increases. The sensing results of the nodes that have a higher value of *measure* will be excluded from the following sensing iteration. In [28], the authors develop a malicious user detection algorithm that

calculates the suspicious level of secondary users and then utilizes the suspicious level to eliminate the malicious users' influence on the primary user detection results. An attack-tolerant distributed sensing protocol that selectively filters out abnormal sensor reports and maintains the accuracy of incumbent detection is explained in [29]. The key idea behind this mechanism is that the measured primary signal strength at nearby sensors should be correlated due to shadow fading. The authors in [30] analyze a challenging attack scenario, wherein multiple cooperative attackers can overhear the honest SU sensing reports and the honest SUs are unaware of the existence of attackers. In [12], the authors use similarity degree to measure the evidence reliability of different users. A low reliability indicates a malicious user and therefore, it will be excluded from the fusion center (FC)'s final decision about the spectrum. The authors in [31] use a bioinformatics algorithm to propose a cooperative spectrum sensing approach. The sensing nodes which sensed spectrum multiple times in one allocated sensing time slot forward their sensing results to a fusion center that compares them using the bioinformatics algorithm. Based on the comparison, a similarity index is computed for each CR user. CR users with similarity indices below a threshold are declared malicious, while in [32], a principal-agent-based joint spectrum sensing and access framework is proposed to thwart the malicious behaviors of malicious users in CR networks.

There are many limitations in previous work. First, the PUEA and SSDF attacks are addressed individually (i.e., no previous work has considered both the attacks happening at the same time except for PUEA and SSDF happening simultaneously in [14, 15]). It is important to address these attacks together to improve the network performance because their detrimental effects are greater when the attacks occur simultaneously. Second, researchers focused on addressing the PUEA and SSDF attacks in their active state and none of them have studied these two attacks in their passive state. Addressing active PUEA and SSDF attacks works as a reactive solution to attacks that are actually occurring and degrading the network performance. However, addressing the passive attacks, which works as a proactive solution, leads to eliminating attacks before they occur and affect the network performance. Third, the messages carrying the sensing results are exchanged between the different sensing nodes in an unencrypted way, which opens the doors widely and makes it easier for adversary nodes to overhear and capture the sensing results and consequently, launch multiple active attacks. Fourth, the previous reputation-based systems are not resilient to such attacks when the number of adversary nodes in the network is high. Moreover, in other reputation-based mechanisms, the sensing reports lack the identities of the senders; therefore, more work is needed by the node that analyzes those sensing report to distinguish whether the reports are sent from trusted sensing nodes or adversary nodes, which implies higher energy consumption levels and higher communication and computation overhead.

The authors in [14, 15] propose a model that takes in consideration simultaneous PUEA and SSDF active attacks. Their model is a lightweight cryptographic algorithm that provides authentication and integrity to SUs' reports. Each node sends its sensing results to an FC encrypted with a variable number of security bits, which depends on how certain the node is about its sensing result. Despite the importance of this work, it has disadvantages. This work focuses more on authenticating the sent sensing result and it does not consider the cases when a sensing node sends a wrong sensing result through a correct authenticated message. In other words, their main focus is on the reporting nodes not on the contents of the sensing reports. Moreover, they considered the adversary nodes from outside the network and not the nodes that are already part of the network waiting for the opportunity to target the other network nodes. In these cases, wrong sensing result will be considered correct. Moreover, it does not provide a solution for the case when collusive nodes agree on sending false sensing results, and therefore, the SSDF attack is not mitigated in this case.

In our work in [17, 18] and in this paper, we address the limitations of the previous work by proposing an approach that considers the attackers' behavior rather than the attacks themselves during spectrum sensing phase. In addition, the proposed approach works as a proactive solution to passive attacks and a reactive solution to active attacks. The simulation results show that the proposed approach outperforms other state-of-the-art approaches. The key elements added to this proposed work that were not mentioned in our work in [17, 18] can be summarized as follows:

(a) The process of analyzing the sensing-reputation reports by the CH has been explained and showed all possible cases.

(b) A novel algorithm for finding the final decision about the spectrum sensing result has been proposed.

(c) Two additional metrics used for showing the performance of the proposed approach have been added and compared with other state-of-the-art models. The analyses of these metrics, the false alarm and detection probability, have been explained step by step and showed its effect to the proposed approach.

(d) The complexity analysis of the proposed approach has been investigated, specifically the computation and the communication overhead.

(e) The attacks have been analyzed from the attacker behavior prospective, which is a new contribution. No previous works have addressed the attacker behavior. They focused on mitigating the attacks themselves. Moreover, the threat model in our system has been identified and described.

(f) The nodes' behavior has been categorized into four categories based on the nodes BL value, which eases the analysis process of the nodes behavior.

(g) A novel K-rule has been proposed. It helps in making the sensing process faster and more secure. The impact of this novel K-rule has been illustrated in the simulation results.

(h) The contents of the sensing-reputation report have been expanded to also include the sensing decision.

(i) The related work has been expanded to cover all state-of-the-art mechanisms used for detecting the attacks that might occur during the sensing process.

3. The Threat Model

In our system, an abnormal node might behave in one or more of the four different behavior categories (ways) to threaten the network in order to degrade the network security and performance. The threat model will be as follows:

(i) A node behaves in a malicious, misbehaving, cheating, and/or selfish way to launch PUE attack by emulating one PU through sending signals over the spectrum channels.

(ii) A node behaves in a malicious, misbehaving, cheating, and/or selfish way to launch SSDF attack by sending false sensing results to other nodes.

(iii) Multiple collusive nodes behave in a malicious, misbehaving, cheating, and/or selfish way to launch collusion attack by sending false reputation reports about benign nodes aiming at degrading their QoS and gaining exclusive access to the spectrum for themselves.

(iv) One or multiple nodes may behave in a malicious, misbehaving, cheating, and/or selfish way to launch DoS attack by sending any data over the spectrum channels in order to reduce the chance for other nodes from using the spectrum for their data transmission.

(v) One or multiple adversary nodes may behave in a malicious, misbehaving, cheating, and/or selfish way to launch objective function attack by trying to change the radio parameters such as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size in order to reduce the network performance and security. There are three goals that the radio wants to achieve: low power, high data rate, and secure communication. Depending on the application, each of these goals has a different weight. Therefore, the adversary nodes try different combinations of input parameters, measure the observed statistics such as bit error rate, and then evaluate the objective functions to see which inputs give the best results for their application.

4. The Proposed Approach

The proposed approach is specific to CRN due to many characteristics that it has. Firstly, any CR node can analyze and learn information from its surrounding communication environment about other users' preferences and demands. Secondly, it can reconfigure itself by adjusting system parameters conforming to certain policies and regulations. Last but not least, a CR node can also initiate a negotiation with other network nodes to enable more efficient spectrum and network utilization. These characteristics are implicitly implemented in the proposed mechanism.

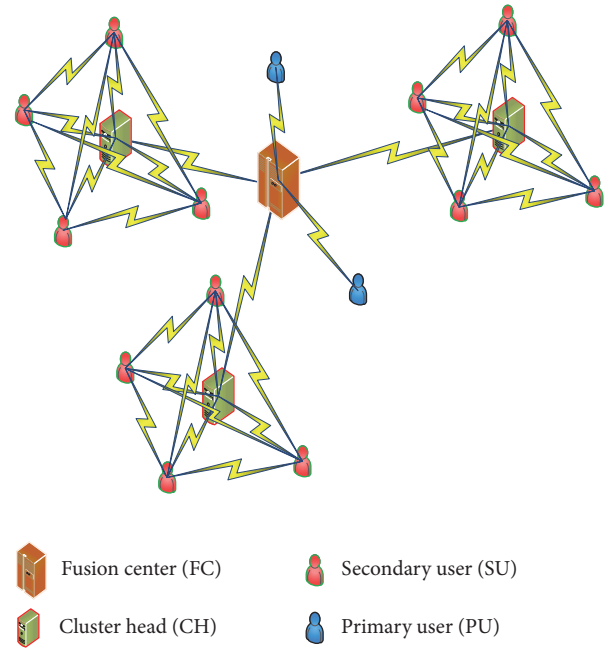

Figure 1: System model.

4.1. Preface. Our system, as shown in Figure 1, is a network that has M secondary users (SUs) divided into K clusters based on their geographical locations as in [33]. The details of the clustering method and its constraints are out of the scope of this paper. However, the authors in [33] summarized all clustering metrics that can be applied in CRNs such as channel availability, geographical location, signal strength and channel quality, and node degree. We assume the existence of a node called fusion center (FC) that controls the traffic over the network and manages the clusters. Each sensing node is assigned a value called belief level (BL), which describes the accuracy and reliability of the sensing nodes that participate in making the final sensing decision. The belief level of each node is the key element of the proposed approach as it will be used to correctly monitor the sensing nodes' behavior and detect the adversary nodes during the spectrum sensing phase. We assume four categories of trust and the BL has a range of [0-4] based on these categories of trust as follows:

$$\begin{aligned} &0 \leq \mathrm{BL} \leq 1\text{: Very\_Untrusted} \\ &1 < \mathrm{BL} < 2\text{: Untrusted} \\ &2 \leq \mathrm{BL} < 3\text{: Trusted} \\ &3 \leq \mathrm{BL} \leq 4\text{: Very\_Trusted.} \end{aligned} \tag{1}$$

Each node is assigned an initial moderate belief level (BL) of value equal to two; that is, it is in the "Trusted" category. In each cluster, one node is chosen by the FC as a cluster head (CH), which has the highest BL. At the time of cluster formation any node is randomly chosen as a CH as all the nodes have the same initial BL value. The cluster heads are not fixed all the time; whenever, a new node is added to a cluster and it has a higher BL than the current CH's BL, the new node

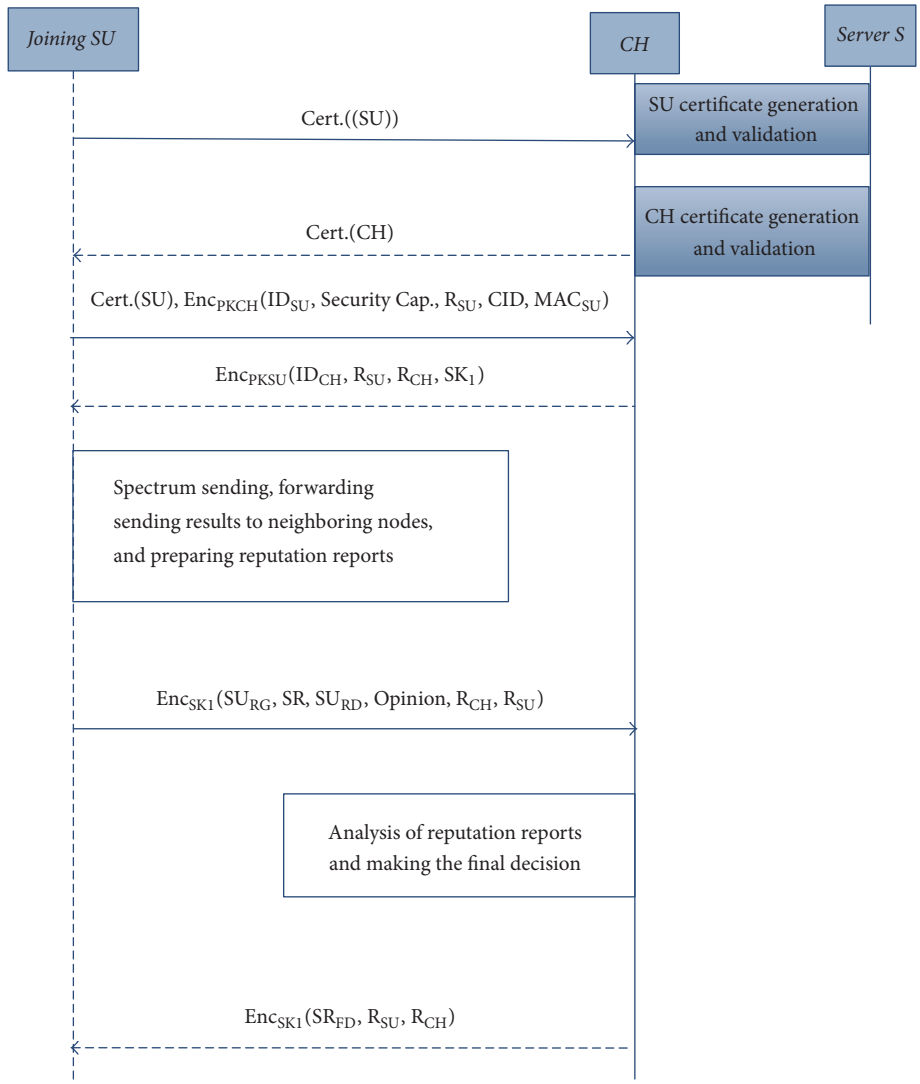

Figure 2: System sequence diagram.

will be selected as a CH. We assume that the energy detection method is used by all SUs to detect the presence or absence of the PU in its spectrum band. Note that the proposed approach focuses on the analysis of the sensing result and thus it is independent of the applied sensing method. The cooperative spectrum sensing is done as in [34], wherein all the cluster nodes sense the spectrum, make a decision about the PU presence/absence, and forward their decision to other nodes. To make the communication of the current nodes secure, we assume that the communication between the network nodes is completed with the public-key cryptography and the symmetric key cryptography. Public-key cryptography is used until a symmetric key is shared between the joining node, the FC, and the CH. The symmetric key will be assigned to each node during the node's authentication process. The details of the authentication process will not be discussed in this paper and are shown in [35]. Each node uses the same key for encrypting and decrypting the messages in the spectrum sensing phase. When a node sends a message to another node in the network, this message will be encoded with the symmetric key. Meanwhile, the receiver decodes this message by using the same key.

The sequence diagram of the proposed approach is shown in Figure 2 that starts with exchanging nodes certificates, nodes IDs, and their security capabilities in order to keep track of nodes IDs that participate in the sensing process, followed by assigning symmetric keys to the sensing nodes that will be used later for encrypting the sensing-reputation reports. Next, the sensing nodes perform the sensing, monitor other nodes' behavior, prepare the sensing-reputation reports, and forward them to the CH (Section 4.2). These sensing-reputation reports are analyzed in each cluster by its CH to make the final decision about the spectrum availability and the sensing nodes behavior. The CH then forwards the

final sensing decisions to its cluster nodes (Section 4.3). All cluster nodes are rewarded or penalized based on their behavior in the cluster during the sensing process (Section 4.4).

4.2. Monitoring Nodes Behavior. All the clusters nodes perform the spectrum sensing process to find the vacant spectrum channels by using any sensing method such as the energy detection technique wherein each sensing node measures the signal strengths in all PU's channels, and by using the energy detection method or any other sensing methods, SUs make the initial binary decision about the presence/absence of PU in its reserved channel(s). Each sensing SU uses the preknown information about PUs signal (such as signal power threshold and modulation type) and compares it with the sensing signal in order to avoid PUEA. If the received signal does not match the expected signal (i.e., a malicious node emulates PU), the sensing SU broadcasts a message to all cluster nodes notifying them and therefore PUEA is mitigated. However, if they match, it means a PU is present in its spectrum channels. If an SU does not receive any signal over the sensing channel, it decides that the spectrum is free and can be used. Each sensing node forwards its sensing decision(s) to its neighbors, compares their sensing results with its sensing results, prepares sensing-reputation reports about their neighboring node(s), and forwards these reports to the CH.

In case PUEA is avoided as mentioned earlier, each sensing SU senses the spectrum and saves its sensing results in a parameter called the *sensing result* (SR). It has two values, either 0 for a free spectrum or 1 for an occupied spectrum by a real PU. The sensing SU forwards its SR to its neighboring nodes, which have their own SRs. Each sensing node compares its own SR with the received SR from its neighboring node and if they match, with the received SR from its neighboring node and if they match, the sensing node decides that its neighboring node is a "GOOD" node G; otherwise it is a "BAD" node B. The sensing node does the same for all its neighboring nodes.

4.3. Analyzing Nodes Behavior. Each node will keep monitoring the behavior of its neighboring nodes and keep sending periodic sensing-reputation reports to its CH about their sensing results and their neighboring nodes' behavior. Sensing-reputation reports sent by each cluster node to its CH have the following format (Reporting Node ID (RG) ‖ SR_{RG} ‖ Reported Node ID (RD) ‖ Opinion) where SR_{RG} is the sensing result of the reporting node and it is either 0 (i.e., *"Free"* spectrum) or 1 (i.e., *"Occupied"* spectrum) and Opinion is about the reported node (RD) and it is either 0 (i.e., *"BAD"* node) or 1 (i.e., *"GOOD"* node). Note that a reporting node is a reported node in its neighboring nodes' sensing-reputation reports and a reported node is a reporting node in its own sensing-reputation report. CH is a trustworthy node and it is the only node that can check the correctness of the periodic sensing-reputation reports. Upon the reception of the different sensing-reputation reports from the different cluster nodes, CH analyzes these reports by extracting the sensing result of the reporting nodes and their opinion about the reliability of the reported nodes to make the final decision about the spectrum availability and about the nodes behavior.

The sensing-reputation reports analysis of making the final sensing decision, SR_{FD}, is described in Algorithm 1. CH forms two groups of nodes occupied group (OG) and free group (FG), where all the nodes in the same group have the same sensing decision "occupied" or "free," respectively. CH analyzes the sensing-reputation reports received from the trusted nodes in each group only. A trusted node is a node that has its BL greater than or equal to a value called $BL_{threshold}$, which describes the lower limit of a BL for a node to be considered trusted.

CH makes the final decision about the spectrum availability based on the reports sent by different nodes and their BL values and then forwards the final decision to its cluster nodes. A specific rule is applied to process these reports in order to make the final decision about the reported node. The general rule of *K-out-of-N* rule is where K users out of N users must have the same opinion in order to consider their opinion. In case 50% K-rule is used, K is equal to $N/2$. We propose a new K-rule, where K represents the number of votes and where we assign each user a different voting weight based on its BL value. We apply the following criteria in order to find the value of K:

(i) A node's decision with a BL value of $3 \leq BL \leq 4$ counts as three votes.

(ii) A node's decision with a BL value of $2.5 \leq BL < 3$ counts as two votes.

(iii) A node's decision with a BL value of $2 \leq BL < 2.5$ counts as one vote.

(iv) A node's decision with a BL value less than 2 does not count.

The total votes' number of the nodes, which have the same sensing decision, has to fulfill the 50% K-rule (i.e., it has to be greater than or equal to a value called $M_{threshold}$), which is equal to half the number of the cluster nodes.

CH analyzes the sensing-reputation reports to determine the malicious and misbehaving reporting and reported nodes as follows:

If the reporting node reports "GOOD" about the reported node, one has the following:

(i) If (SR_{FD} == SR_{RG} && SR_{FD} == SR_{RD}), then it is a true *"GOOD"* opinion → both the reporting and the reported node are trusted nodes.

(ii) If (SR_{FD}! = SR_{RG} && SR_{FD} == SR_{RD}), then it is a true *"GOOD"* opinion → the reporting node is an adversary node (SSDF attack).

(iii) If (SR_{FD} == SR_{RG} && SR_{FD}! = SR_{RD}), then it is a false *"GOOD"* opinion → both the reporting and the reported node are adversary nodes (SSDF and Collusion attacks).

(iv) If (SR_{FD}! = SR_{RG} && SR_{FD}! = SR_{RD}), then it is a false *"GOOD"* opinion → both the reporting and the reported node are adversary nodes (SSDF and Collusion attacks).

Initialization
OG: All reporting nodes including CH that have SR = 1
FG: All reporting nodes including CH that have SR = 0
C: Number of SUs in a cluster
$\mathrm{BL}_{\mathrm{threshold}}$: Threshold value of the reporting node's belief level
$M_{\mathrm{threshold}}$: Threshold value of the number of nodes that should have the same sensing decision and is equal to $\lceil C/2 \rceil$
OccupiedCount: Votes count of reporting nodes that have SR = 1 and initialized to zero
FreeCount: Votes count of reporting nodes that have SR = 0 and initialized to zero
$\mathrm{SR}_{\mathrm{FD}}$: Final sensing decision
$K\mathrm{Rule}(\mathrm{BL}_{\mathrm{RG}_m})$: Function to calculate the votes count for each node
K: Total votes for all nodes and initialized to zero
$\forall \mathrm{RG}_i \in \mathrm{OG}$
  IF $(\mathrm{BL}_{\mathrm{RG}_i} \geq \mathrm{BL}_{\mathrm{threshold}})$
    OccupiedCount += $K\mathrm{Rule}(\mathrm{BL}_{\mathrm{RG}_i})$
==========
$\forall \mathrm{RG}_j \in \mathrm{FG}$
  IF $(\mathrm{BL}_{\mathrm{RG}_j} \geq \mathrm{BL}_{\mathrm{threshold}})$
    FreeCount += $K\mathrm{Rule}(\mathrm{BL}_{\mathrm{RG}_j})$
==========
IF (*OccupiedCount* $\geq M_{\mathrm{threshold}}$ && *OccupiedCount* > *FreeCount*)
  $\mathrm{SR}_{\mathrm{FD}} = 1$
else IF (*FreeCount* $\geq M_{\mathrm{threshold}}$ && *FreeCount* > *OccupiedCount*)
  $\mathrm{SR}_{\mathrm{FD}} = 0$
else
  $\mathrm{SR}_{\mathrm{FD}} = \mathrm{SR}_{\mathrm{CH}}$
K = *OccupiedCount* + *FreeCount*
$K\mathrm{Rule}(\mathrm{BL}_{\mathrm{RG}_m})$
{
  count = 0;
  IF $3 \leq \mathrm{BL}_{\mathrm{RG}m} \leq 4$
    count = *count* + 3;
  else IF $2.5 \leq \mathrm{BL}_{\mathrm{RG}m} < 3$
    count = *count* + 2;
  else IF $2 \leq \mathrm{BL}_{\mathrm{RG}m} < 2.5$
    count = *count* + 1;
  else IF $\mathrm{BL}_{\mathrm{RG}m} < 2$
    count = *count* + 0;
  return count;
}

Algorithm 1: Final decision of spectrum sensing.

If the reporting node reports "BAD" about the reported node, one has the following:

(i) If ($\mathrm{SR}_{\mathrm{FD}}$ == $\mathrm{SR}_{\mathrm{RG}}$ && $\mathrm{SR}_{\mathrm{FD}}$ == $\mathrm{SR}_{\mathrm{RD}}$), then it is a false *"BAD"* opinion → the reporting node is an adversary node (Collusion attack).

(ii) If ($\mathrm{SR}_{\mathrm{FD}}$! = $\mathrm{SR}_{\mathrm{RG}}$ && $\mathrm{SR}_{\mathrm{FD}}$ == $\mathrm{SR}_{\mathrm{RD}}$), then it is a false *"BAD"* opinion → the reporting node is an adversary node (SSDF and Collusion attacks).

(iii) If ($\mathrm{SR}_{\mathrm{FD}}$ == $\mathrm{SR}_{\mathrm{RG}}$ && $\mathrm{SR}_{\mathrm{FD}}$! = $\mathrm{SR}_{\mathrm{RD}}$), then it is a true *"BAD"* opinion → the reported node is an adversary node (SSDF and Collusion attacks).

(iv) If ($\mathrm{SR}_{\mathrm{FD}}$! = $\mathrm{SR}_{\mathrm{RG}}$ && $\mathrm{SR}_{\mathrm{FD}}$! = $\mathrm{SR}_{\mathrm{RD}}$), then it is a true *"BAD"* opinion → both the reporting and the reported node are adversary nodes (SSDF and Collusion attacks).

In summary, each node is given a variable weight of votes based on its BL, and this variable votes' weight affects the final sensing results decision. The nodes behavior is analyzed based on the final sensing results decision. Note that we assume the channels carrying the sensing-reputation reports are error-free and each sensing-reputation report has a timestamp associated with it. If CH does not receive a sensing-reputation report from a node within its timestamp, CH considers the node as an adversary node. Moreover, if a node is erroneously reporting or CH erroneously does not consider one node's reporting in one reporting round, it will be considered in the following report round as the

sensing-reputation reports analysis is a continuous process. We assume that all the nodes can reach the CH and their reports will be received by the CH as long as they were sent within the timestamp.

4.4. Reward/Punishment Mechanism. CH adjusts the belief level of each node based on whether a node is to be rewarded or penalized. Each "GOOD" behaving node will be rewarded by increasing its BL. Each "BAD" behaving node will be penalized by decreasing its BL and applying a proper penalty action according to a value called Adjustment Factor (AF) that is calculated by CH as in (2) and then it is added to the latest value of BL as in (3). AF is calculated according to the number of "GOOD" and "BAD" reports sent by the reporting nodes about the reported node.

$$\begin{aligned} &\text{at } t = t_{\text{update}} \\ &\text{AF}_{\text{SU}_i} = \left(\sum_{g=1,\neq i}^{G} \propto^{*} \mathbb{N}\left(\text{BL}_{\text{SU}_g}\right) \right) \\ &\qquad - \left(\sum_{b=1,\neq i}^{B} \beta^{*} \mathbb{N}\left(\text{BL}_{\text{SU}_b}\right) \right) \\ &\text{s.t.} \quad -4 \le \text{AF} \le 4, \end{aligned} \tag{2}$$

where G and B are the number of nodes, which decide that SU_i is a good and bad node, respectively. $\propto$ represents the rewarding factor, β represents the penalizing factor, $\mathbb{N}(\text{BL}_{\text{SU}_b})$ represents the normalized belief level of the node, which reports that SU_i is a bad node, and $\mathbb{N}(\text{BL}_{\text{SU}_g})$ represents the normalized belief level of the node, which reports that SU_i is a good node. The rewarding factor and the penalizing factor are chosen as in real life where penalty has more weight than rewarding.

The range of AF value is $[-4, 4]$, i.e., if AF value is more than 4, it will be set to 4 and if it is less than -4 it will be set to -4. The BL of each reporting cluster node is important in the process of finding the AF; the higher the BL of a reporting cluster node is, the higher the effect on the AF value is.

Normal behaving sensing nodes will be rewarded for their normal behavior, which allows them to gain higher belief level in the cluster. On the other hand, an adversary node (attacker) is penalized by decrementing its BL and applying penalty action(s) for its abnormal activity in the network. The penalty mechanism affects the attacker throughput as that decreases its belief level and reduces the resources assigned to it, which therefore results in a low throughput. Consequently, the desire of other cluster nodes to communicate with the misbehaving node during data transmission phase is low; hence, no node will want to behave in an abnormal way.

CH penalizes the adversary node by applying the proper penalty actions according to the AF value. These penalty actions are shown in Table 2.

Table 2 shows the proposed penalty scheme, which depends on other cluster nodes' decision about each other.

Table 2: Penalty scheme.

Adjustment factor (AF)	Penalty action(s)
$-1 < \text{AF} \le 0$	No extra penalty
$-2 < \text{AF} \le -1$	P1
$-3 < \text{AF} \le -2$	P1 and P2
$-4 < \text{AF} \le -3$	P3
-4	P3 and P4

(i) P1: give a time out for three sensing rounds; (ii) P2: deallocate 50% of the assigned resources to the adversary node; (iii) P3: deallocate all resources and disconnect this adversary node; (iv) P4: mark the adversary node as an undesirable node.

Equation (3) finds the updated value of belief level of each cluster node at every reporting round, where $(\text{BL}_{\text{SU}_i})_{t_{\text{update}-1}}$ is the belief level in the previous updating round.

$$\left(\text{BL}_{\text{SU}_i}\right)_{t_{\text{update}}} = \left(\text{AF}_{\text{SU}_i}\right) + \left(\text{BL}_{\text{SU}_i}\right)_{t_{\text{update}-1}}. \tag{3}$$

4.5. Analysis of Detection and False Alarm Probability. We use the value of K (calculated as in Algorithm 1) to formulate the detection probability P_D^{BL}, which is the probability of identifying a malicious reported node as malicious or the probability of identifying a used spectrum as used, as shown in

$$P_D^{\text{BL}} = \begin{cases} \sum_{i=K}^{C} \binom{C}{i} {P_d}^i \left(1 - P_d\right)^{C-i}, & K < C, \\ 1, & K \ge C, \end{cases} \tag{4}$$

where P_d denotes the individual detection probability of the reporting node and C is the number of SUs in each cluster.

A malicious reporting node is a node that sends false reports to CH about the reported node or false sensing results. When CH receives the report from the reporting nodes, it analyzes if the reporting node acts in a misbehaving way either by sending false reputation report about the reported node or by sending false sensing result. The probability for CH to make a wrong decision about the reported node or about the spectrum availability is denoted as $P_F(C, K)$ as in (5) where P_f denotes the individual false alarm probability of the reporting node, (i.e., it is the probability that the reporting node erroneously transmits to the CH a false report about the reported node or a false sensing result).

$$P_F\left(C, K\right) = \begin{cases} \sum_{i=K}^{C} \binom{C}{i} {P_f}^i \left(1 - P_f\right)^{C-i}, & K < C, \\ 1, & K \ge C. \end{cases} \tag{5}$$

A malicious reporting node (SU_z) will try to send false reports to CH about the reported node or false sensing result with a probability of success $P_s^{\text{SU}_z}$ as in

$$P_s^{\text{SU}_z} = \frac{\text{BL}_{\text{SU}_z}}{\text{BL}_{\max}} * \frac{1}{2^{\text{BV}}}, \tag{6}$$

where BL_{SU_z} is the belief level of the malicious reporting node (SU_z) and BV is the number of bad votes about SU_z.

The probability of false alarm using our mechanism can be expressed as in (7) where $P_F(C, K)$ is obtained from (5).

$$P_F^{\mathrm{BL}} = \sum_{i=1}^{Y} \prod_{z\in(1,i)} \left[P_s^{\mathrm{SU}_z}\right] \prod_{z\in(1,i)} \left[1 - P_s^{\mathrm{SU}_z}\right] P_F(C, K), \quad (7)$$

where Y is the number of malicious reporting nodes and K represents the total number of votes of the malicious reporting node(s) about the same reported node. K is calculated in the same way as in the K-rule used for the spectrum sensing decision; however this time the node's decision with a BL value less than 2.5 counts as a one vote.

Collusive cluster nodes or compromised node(s) can send false sensing results or report a benign node as misbehaving node. In the case of targeting a benign node, the collusion attack occurs if multiple nodes report to CH about a benign node that this benign node is a *"BAD"* node while in real it is not. Our approach prevents any node from acting as a collusive node or compromised node by analyzing and comparing the different reports sent by different cluster nodes about the benign node. In other words, CH applies one of five different actions to the reported and the reporting nodes. These actions are A1 (Do nothing), A2 (Increment its BL), A3 (Decrement its BL), A4 (Decrement its BL after five nonconsecutive or three consecutive *"BAD"* reports about its neighboring reported node), and A5 (Penalize the adversary node by one of the penalty actions).

4.6. Energy Consumption Analysis. As the cognitive radio nodes are battery-powered and the sensing process is continuous, energy is consumed during the sensing process and it should be taken into consideration during the design process of counter-mechanisms for attacks. The main goal of attacks detection mechanisms should be maximizing the security level and minimizing the energy consumption in the network.

Energy consumption is high in the presence of an adversary node (s) that behave in an abnormal way to launch PUEA or/and SSDF attacks. In other words, each sensing node consumes more energy to broadcast its own sensing result, analyze the sensing results of other nodes, and identify the adversary node(s) in the network in addition to sense the spectrum correctly.

In the proposed approach, if attackers exist in the network, the false alarm probability increases and the detection probability decreases leading to higher energy consumption levels. However, applying the proposed K-rule and the penalty mechanism decreases the false alarm probability and therefore decreases the energy consumption levels as the adversary nodes do not have enough resources to launch such attacks.

5. Complexity Analysis

In this section, we discuss the complexity of the monitoring nodes behavior algorithm proposed, including the sensing phase, in terms of computation overhead and communication overhead. In our proposed algorithm, all SUs are divided into different clusters and the cluster nodes communicate with their CHs instead of communicating with a centralized point (i.e., FC). This reduces the amount of computation and resource management and, therefore, improves the security level of the network.

Firstly, we analyze the computation overhead in the proposed approach and in the centralized model with no clusters. In the centralized model with no clusters, a bidirectional way of messaging between all SUs and the FC is used. Therefore, the FC needs to manipulate $2 * |M|$ messages, where M represents the total number of SUs. In the proposed model using clusters, the FC manipulates $2 * |K|$, where K represents the number of cluster heads. The computation overhead at the FC in both approaches is $\approx O(M)$ and $\approx O(K)$, respectively. However, $|K| < |M|$; therefore, our approach reduces the computation overhead at the FC.

In our proposed approach, the number of messages that the CH has to manipulate is $|N|$ messages, where N represents the number of SUs in the cluster. Therefore, the computation overhead at the CH is $\approx O(N)$.

Secondly, we use the number of messages exchanged to also calculate the communication overhead. The number of messages is equal to that used in the computation overhead calculation; therefore, the communication overhead at the FC with no clustering is $\approx O(M)$, at the FC with clustering is $\approx O(K)$, and at the CH is $\approx O(N)$ where $|K| < |N| < |M|$.

6. Performance Evaluation

We simulate the proposed approach to identify the adversary sensing nodes during the spectrum sensing phase. Table 3 shows the network simulated with values used for the parameters required in our approach as in [14–18]. The simulation results are analyzed from two perspectives. First, the importance and the effects of the concepts used in the proposed approach such as (monitoring nodes behavior, BL, K-rule, and detection and false alarm probability) are analyzed as shown in Figures 3–6. Second, a comparison is made between the proposed approach and other approaches in the literature in terms of detection probability and false alarm probability as shown in Figures 7–9. The detection probability found in (4) in our approach is compared with that in INCA [26] and with two other approaches as we refer them as Model A and Model B proposed in [14] and [15], respectively. Moreover, we compare the false alarm probability found in (7) in our approach with that in Model A and Model B [14, 15].

The normal behavior of any cluster node in our proposed model is illustrated in Figure 3 as each node starts with a moderate belief level and keeps gaining more belief through the spectrum sensing phase until it reaches the maximum belief level of four. All nodes aim at increasing their BL in the network. On the other hand, the adversary node (even with a maximum belief level value of four) can have its belief level decreased to the minimum value of zero due to its abnormal behavior in the cluster.

The transmission rate in our proposed model is compared with and without monitoring nodes behavior as shown in Figure 4. We assume that all nodes initially achieve 70 percent of their desired transmission rate. The behavior of the trusted nodes, the semimisbehaving nodes, and the full-misbehaving

Table 3: Simulation parameters.

Parameter	Value
Number of SUs	[0–125]
Number of clusters	[0–15]
Number of malicious nodes	3
The rewarding factor α	0.3
The penalizing factor β	0.7
$BL_{threshold}$	2 (for the spectrum sensing final decision) 2.5 (for the adversary node detection)
BL_{CH}	[2–4]
P_d	0.8
P_f	0.2
Number of security bits B_{opt} used in [14, 15]	5

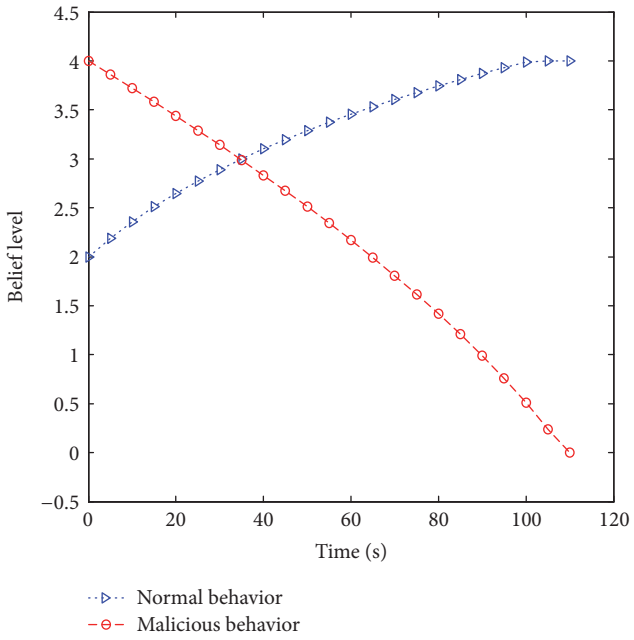

Figure 3: Belief level over time.

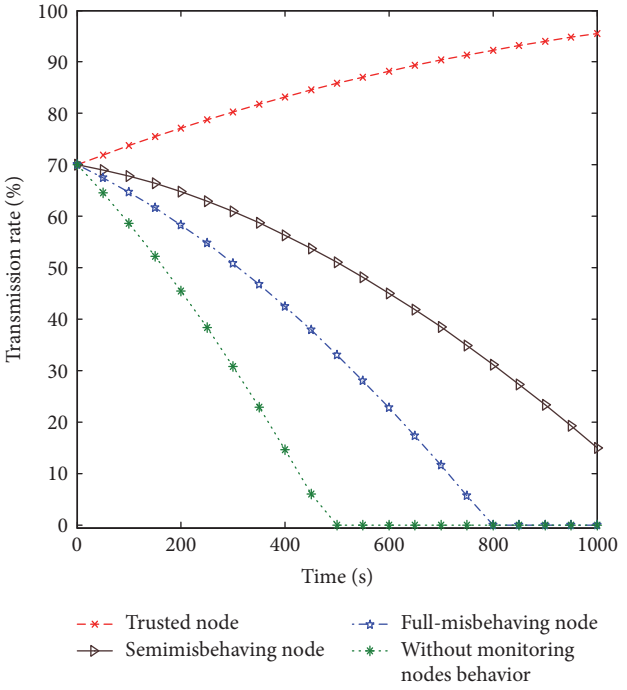

Figure 4: Transmission rate over time.

node is monitored. The normal behavior of the trusted node makes its BL increase and therefore, its transmission rate increases gradually. The semimisbehaving node lures some nodes in the cluster; therefore, those nodes vote "BAD" while other nodes vote "GOOD" about its behavior. Overall, its BL relatively decreases (i.e., |AF| is less than 3) and therefore its transmission rate decreases. The transmission rate of the full-misbehaving node that lures all nodes in the cluster decreases rapidly and its BL reaches zero in a shorter time, since all the cluster nodes vote "BAD" about its behavior (i.e., |AF| is greater than 3). The transmission rate of an adversary node without monitoring its behavior (i.e., no BL associated with the node's behavior) is also measured. It is found that its transmission rate decreases and reaches zero faster due to its malicious behavior.

Figure 5 illustrates the effects of the different number of nodes in a cluster with their BL on the detection probability. It is depicted that, with a higher BL, the detection probability increases (i.e., reaches the maximum value of one) due to the increase in the number of the cooperating SUs. Therefore, when more SUs that have high BL participate in the sensing phase, the detection is completed faster.

Figure 6 shows the effects of applying two different K rules on the detection probability in our proposed approach. We assume that the number of SUs in a cluster is 12. In the first K-rule (50%), the detection probability reaches the maximum value of one, when 50% of the users (i.e., six out of twelve SUs) successfully have the same decision, while

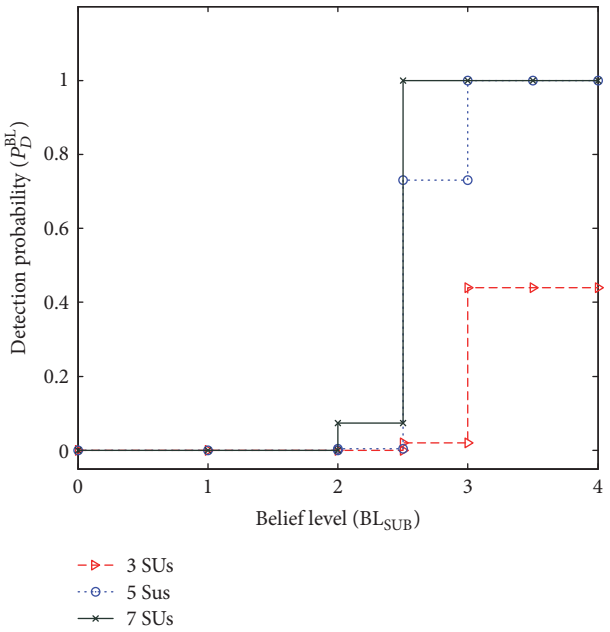

FIGURE 5: Effects of BL on detection probability in proposed approach.

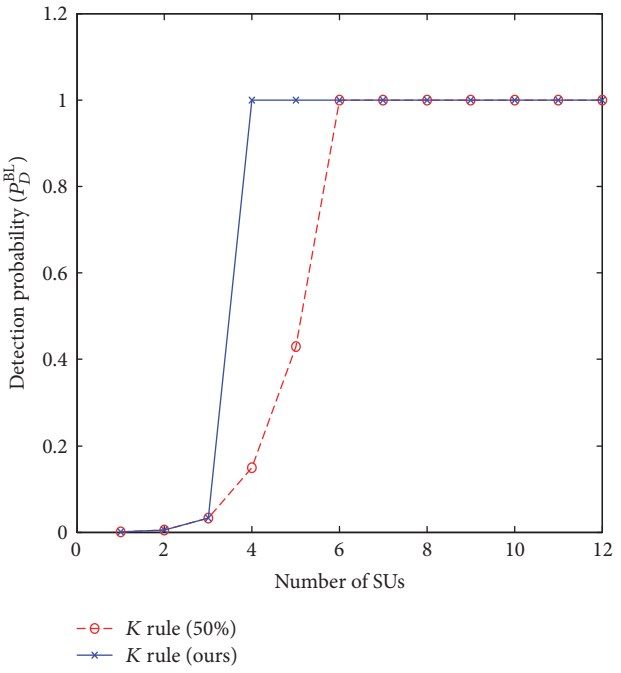

FIGURE 6: Effect of two K rules on detection probability in proposed approach.

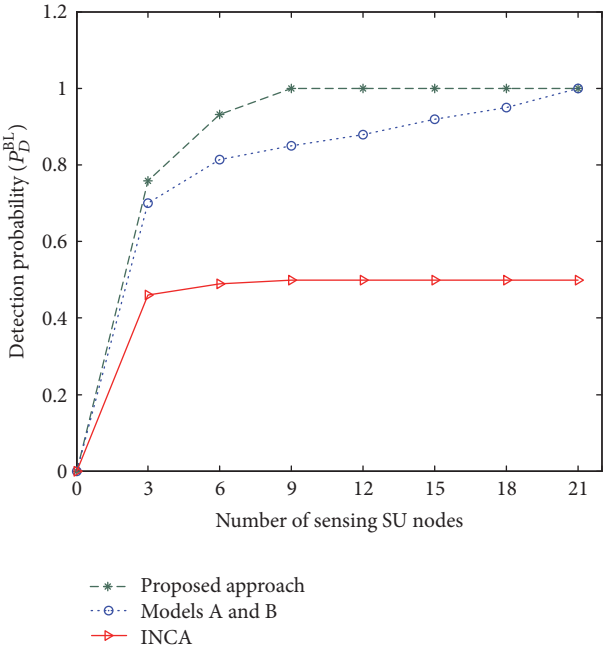

FIGURE 7: Detection probability (proposed approach versus other models).

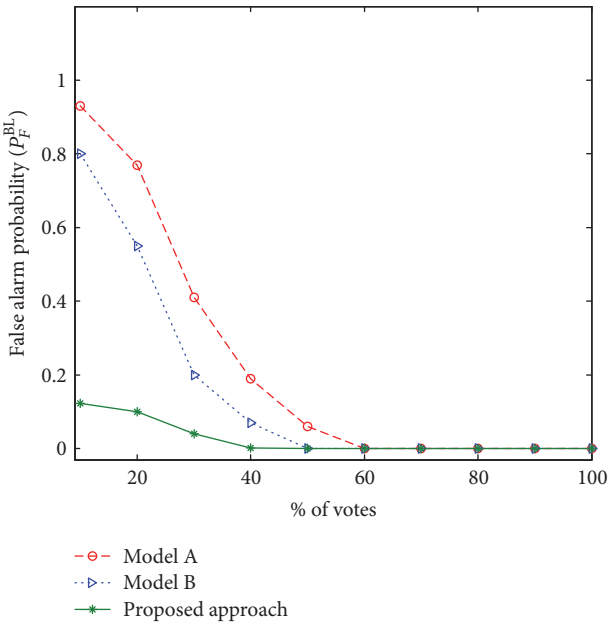

FIGURE 8: A comparison of false alarm probability versus percentage of votes.

in our proposed K-rule, the detection probability reaches the maximum value of one when fewer users (i.e., four out of twelve SUs), which have higher BL, make the same decision. In comparison with the 50% K-rule, the detection is completed faster by applying our proposed K-rule.

Figure 7 compares the detection probability in our proposed model, INCA [26], and Models A and B [14, 15]. The detection probability increases when the number of sensing SU nodes increases. In INCA, the maximum detection probability is 0.5. In our proposed approach using the proposed K-rule, the detection probability continues to increase to a maximum value of one, where at least nine out of twenty-one nodes in the cluster decide that a node is an adversary node (i.e., number of "*BAD*" reports B = 9 nodes). The detection probability in Models A and B keeps increasing; however, it

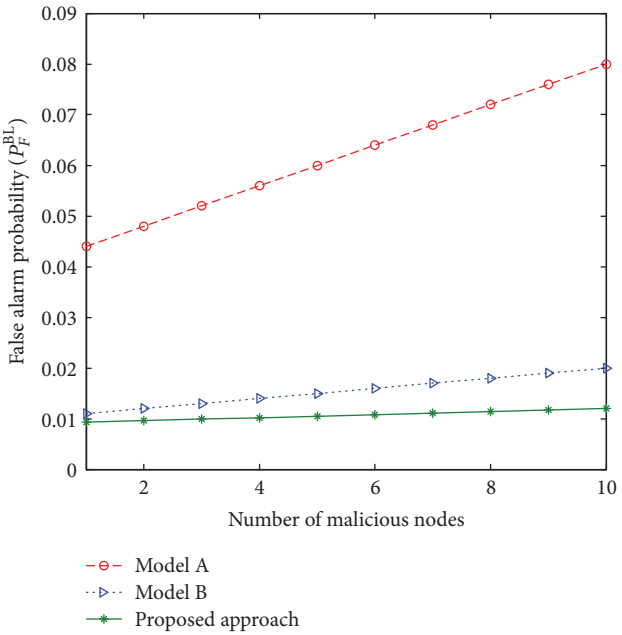

Figure 9: A comparison of false alarm probability versus malicious nodes.

reaches the maximum value of one when all the cluster nodes participate in the detection process. Therefore, our approach outperforms the INCA approach as well as Models A and B as it can reach the maximum value of the detection probability and in a shorter time.

Figure 8 compares the false alarm probability in our proposed approach with that in Model A [14] and Model B [15]. In Model A and Model B, the 50% K-rule is applied, while in our proposed model the proposed K-rule is used to calculate the percentage of votes. It is clear from the figure that the false alarm probability decreases as the percentage of votes (i.e., number of the nodes participating in the spectrum sensing process) increases. Our proposed model with the proposed K-rule lowers the false alarm probability compared to the other two models with a reduction of more than 60%. Therefore, our proposed approach outperforms Model A and Model B in terms of lowering the false alarm probability.

In Figure 9, the false alarm probability in our proposed model is again compared with that in Model A and Model B, but this time, with respect to the number of malicious (adversary) nodes in the network. It is depicted from the figure that our proposed model with the proposed K-rule outperforms the other two models when the number of malicious nodes increases. The punishment scheme applied by the CH against any malicious node is a possible reason for this advantage. Lowering the false alarm probability increases the security of the network.

7. Security Analysis

The proposed model prevents any node from acting in a misbehaving way. Different attacks that might occur because of the abnormal behavior of network nodes (adversary nodes) are eliminated by our proposed collaborative approach. We show here some attacks that can be detected and mitigated by our collaborative approach. Note that all the simulation results of the detection probability and false alarm probability in the previous section can represent the detection and false alarm probability of the following attacks separately.

7.1. PUE Attack Analysis. PUEA is launched when one node emulates the PU by sending signals over PUs channels. When SUs sense the PUs channels, they will receive signals over these channels stating that a PU is present in its channels, while in reality, it is a node that is emulating the real PU. We assume that there is one node emulating PU and sending signals over PUs channels and there is no real PU using the channels. When SUs sense the PUs channels and receive signals over these channels, each SU compares the received signals with the expected signals in order to check if the received signals belong to a real PU or an adversary node that emulates PU. Based on this comparison, if the sensing node decides that the spectrum is busy, the malicious node is performing as an active PUEA; otherwise it is a passive PUEA. We mitigate both the active and passive PUEA in our approach by applying the collaboration between the different sensing nodes, our belief level mechanism, and making the final sensing decision based on all the sensing nodes' decisions and not based on one node's decision only. More specifically, by applying our proposed K-out-of-N rule, the SU with the higher BL has a higher weight in making the final decision if the received signal is from a real PU or not. If a node, after analyzing the received signal, decides that this received signal belongs to an emulator, it will send a special sensing-reputation report to its neighbors and CH. CH will collect these special reputation reports and analyze them to make the final decision and based on that the passive PUEA is mitigated. The detection of a PUEA will be faster when the sensing nodes have higher BL, since the higher BL values give them higher number of votes.

In the case of M SUs sense the spectrum, which have the maximum BL, the detection of PUEA will be faster than that when at least one node does not have the maximum BL. In case all the nodes are new nodes, which are joining the cluster for the first time (i.e., their BL value is still moderate), the detection probability will not be high enough in the first sensing round. However, as the sensing is carried out over multiple rounds, the BL of the nodes will increase and the detection probability will continue to increase.

The active PUEA is mitigated by the symmetric cryptography, since, a node can emulate a PU if it has its shared symmetric key with other nodes, which is not the case in our proposed approach. If a node is an emulating PU, it has to have the PU's symmetric key to send messages over the PUs channels. We simulate a scenario with multiple SUs with different BLs and show the results in Figure 10. It is depicted that the detection probability increases as the time increases and as the BL of the normal behaving nodes increases. A higher BL of a normal behaving node indicates a faster PUEA detection.

7.2. SSDF Attack Analysis. The attacker might send false sensing results to its neighbors stating that the PU is present

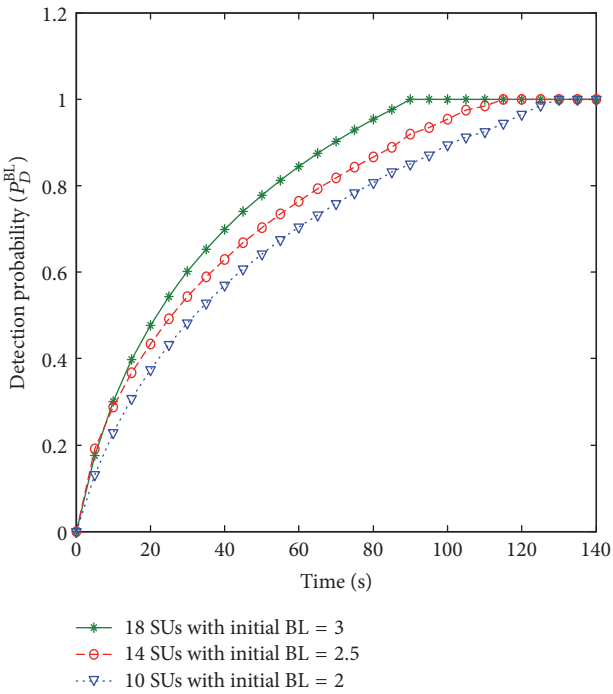

Figure 10: Detection probability of PUEA.

in its band, when in fact the PU is not present. The attacker's intention is to gain exclusive access to the spectrum and to prevent other nodes from using the spectrum efficiently. Another form of this attack is when the attacker falsely states that the PU is absent in its band. In this case, the attacker aims to cause interference with the PU and consequently, the PU's QoS is degraded. In both forms, the SSDF might be active or passive. If a malicious node sends its false sensing result to other nodes and the final sensing result was the same as the malicious node's sensing result, active SSDF is launched; otherwise SSDF is passive. Our approach will detect this malicious behavior that leads to active or passive SSDF by applying the collaboration, BL management, and monitoring nodes mechanisms (i.e., each node votes about its neighboring nodes behavior). The final spectrum sensing decision is made based on all the nodes sensing results and in different consecutive sensing rounds (i.e., if one node succeeded to launch SSDF in one sensing round, its chance for relaunching SSDF decreases in the next sensing rounds). With active SSDF attack, the malicious behavior of the node is detected by other nodes that have the opposite sensing decision. Therefore, the votes' weight of the malicious node will be decreased as the sensing time elapse. Moreover, the CH as a trustworthy node can decide if any node is sending false sensing results or false reports about other nodes. In the case of passive SSDF attack, monitoring nodes' behavior and analysis of their behavior, which is done by the CH, reduce the nodes' BL and their votes' weight; hence, passive SSDF is mitigated.

All the nodes will rely on CH's final decision about the spectrum availability. According to our analysis, a malicious node's chance to launch the SSDF attack is high when the node has a high BL or fewer nodes decide that a node is a malicious node. On the other hand, this chance decreases when the number of nodes that decide if a node is a malicious node increases (i.e., when the malicious node's BL decreases). During the reporting rounds, the number of nodes, which decide that a node is a malicious node, increases if the malicious node's sensing results oppose their sensing results, and therefore the malicious node's BL decreases with the reporting time elapse. When the malicious node sends false reports to the CH, the other cluster nodes will vote "BAD" for it and consequently, its BL is decreased.

7.3. DoS Attack Analysis. It might be launched at the CH, since a joining node might show a good behavior at the joining time to become a CH, and then it acts abnormally and cheats about the honesty of other nodes. This adversary joining node aims to reduce the other nodes' belief level value and reduce the network throughput. Such a behavior is prevented by our proposed approach as the clusters are being dynamically reformed whenever a new node is admitted to the network or when a node has a BL that is higher than the CH's BL. Therefore, the cluster heads are not fixed all the time. Moreover, each normal behaving cluster node that is penalized by its malicious CH contacts the FC, which takes appropriate actions against the malicious CH.

It might be launched at SU level as an SU might send any sensing result about the spectrum to its neighbors or send "BAD" reports about its neighboring nodes in order to degrade their QoS and prevent them from achieving their desired service. It is prevented by applying our proposed reports analysis and punishment mechanisms, as any node, which sends false sensing information or false opinion about other nodes, will be punished with proper penalty action depending on the severity of the launched DoS attack. Every node is monitored and its behavior is evaluated at the end of every reporting round. Therefore, for any node to stay in the network and keep using its resources, it has to act normally in the network.

7.4. Objective Function Attack Analysis. The attacker tries to change the radio parameters (such as center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type, and frame size) to reduce the network objective, which is always to have higher security and higher transmission rate. Any change in these parameters will lead to false sensing results of other nodes and might lead to launch PUE attack. However, by applying our proposed BL management scheme and penalty mechanism, a node will not have the opportunity to change any of these parameters. Our proposed approach reduces the resources assigned to the misbehaving node, which reduces the opportunity for the misbehaving node to change the radio parameters. If a node launches this attack, other nodes will notify CH about the abnormal behavior of this node. Therefore, CH applies appropriate penalty actions, such as deallocating part of the resources, which weakens its ability to perform such an attack.

7.5. Collusion Attack Analysis. As the collusive reporting node sends false reports about its neighboring node(s), CH

uses the reports sent by its next node(s) to determine the correctness of its reports. Incorrect reports are determined upon the comparison of the reports sent by the reporting node, other nodes' reports, and CH's sensing decision itself. Such a comparison leads to identify the compromised and collusive nodes in the network. No node will like to have its belief level reduced or be considered as compromised or collusive node. By the role of CH and applying the penalty scheme, a node will send true reports about its neighboring node(s) and will not send false reports to protect itself from being penalized or considered as a collusive or compromised node.

Another form of collusion attack is when multiple nodes agreed about reporting a benign node as a "BAD" node, when the node is not "BAD." When CH receives the reputation reports from the collusive nodes about the benign node, it analyzes the reports sent by the collusive nodes about the benign node and the reports sent by the benign node about the collusive. Based on that analysis, CH can tell if the "BAD" reports are true or false reports. Consequently, the CH takes the appropriate actions against the collusive nodes or the misbehaving node. Hence, detecting the collusive nodes will become easier and faster with time as the BL of the collusive nodes will be decreased. As a result, their reports will have no high effect on other benign nodes.

8. Conclusion and Future Work

Securing the spectrum sensing process in CRN is very important as adversary nodes might behave in different abnormal ways to launch different attacks that degrade the spectrum sensing reliability. Therefore, the network security and throughput will be reduced. Current mechanisms of attack detection focus on addressing the attacks independently or two kinds of attacks a time, which is not realistic, as multiple attacks can exist simultaneously.

Monitoring nodes behavior during the spectrum sensing process helps to identify and eliminate adversary nodes from the network, which improves the accuracy of the sensing results, the network security, and the performance.

In this paper, we propose a collaborative approach during the spectrum sensing process that focuses on monitoring the nodes' behavior rather than addressing the attacks themselves. It works as a proactive approach to passive attacks and as a reactive approach to active attacks. In the proposed approach, all sensing nodes monitor the behavior of each other to identify the adversary nodes.

The simulation results show the performance of our proposed approach compared to other models. This approach improves the detection probability and false alarm probability, which increases the network security and implicitly enhances the spectrum utilization and network throughput. Moreover, the security analysis shows the different kind of active and passive attacks that can be detected and mitigated through the proposed approach by monitoring the sensing nodes behavior.

As future directions to this work, the energy efficiency of the proposed approach will be addressed. Moreover, the trade-off between the required security level and the energy consumption in the network should be identified. As the proposed approach is a reputation-based technique, its performance will be compared to other reputation-based mechanisms in order to show its efficiency and its added value.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors would like to acknowledge the financial support provided by NSERC (Natural Sciences and Engineering Research Council of Canada), with Grant no. N00668.

References

[1] J. Mitola, "Cognitive radio for flexible multimedia communications," in *Proceedings of the IEEE International Workshop on Mobile Multimedia Communications (MoMuC '99)*, pp. 3–10, IEEE MoMuC, San Diego, CA, USA, USA, 1999.

[2] S. M. Mishra, D. Cabric, C. Chang et al., "A real time Cognitive Radio testbed for physical and link layer experiments," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 562–567, Baltimore, MD, USA, November 2005.

[3] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[4] M. Khasawneh, S. Alrabaee, A. Agarwal, N. Goel, and M. Zaman, "Power trading in cognitive radio networks," *Journal of Network and Computer Applications*, vol. 65, pp. 155–166, 2016.

[5] S. Alrabaee, M. Khasawneh, A. Agarwal, N. Goel, and M. Zaman, "Applications architectures and protocol design issues for cognitive radio networks: a survey," *International Journal of Wireless and Mobile Computing*, vol. 7, no. 5, pp. 415–427, 2014.

[6] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *Journal of Internet Technology*, vol. 12, no. 2, pp. 1–18, 2011.

[7] L. Lai, Y. Fan, and H. V. Poor, "Quickest detection in cognitive radio: a sequential change detection framework," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 1–5, New Orleans, La, USA, December 2008.

[8] D. Das and S. Das, "Primary user emulation attack in cognitive radio networks: a survey," *International Journal of Computer Networks and Wireless Communications*, vol. 3, no. 3, pp. 312–318, 2013.

[9] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, Dresden, Germany, June 2009.

[10] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 772–781, 2014.

[11] F. Richard Yu, H. Tang, M. Huang, Z. Li, and P. C. Mason, "Defense against spectrum sensing data falsification attacks in

mobile ad hoc networks with cognitive radios," in *Proceedings of the IEEE Military Communications Conference (MILCOM '09)*, pp. 1–7, October 2009.

[12] Y. Han, Q. Chen, and J.-X. Wang, "An enhanced D-S theory cooperative spectrum sensing algorithm against SSDF attack," in *Proceedings of the 75th Vehicular Technology Conference (VTC '12)*, Yokohama, Japan, June 2012.

[13] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[14] S. Althunibat, V. Sucasas, H. Marques, J. Rodriguez, R. Tafazolli, and F. Granelli, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1564–1567, 2013.

[15] V. Sucasas, S. Althunibat, A. Radwan et al., "Lightweight security against combined IE and SSDF attacks in cooperative spectrum sensing for cognitive radio networks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3978–3994, 2015.

[16] V. Zlomislić, K. Fertalj, and V. Sruk, "Denial of service attacks: an overview," in *Proceedings of the 9th Iberian Conference on Information Systems and Technologies (CISTI '14)*, Barcelona, Spain, June 2014.

[17] M. Khasawneh and A. Agarwal, "A collaborative approach towards securing spectrum sensing in cognitive radio networks," *Procedia Computer Science*, vol. 94, pp. 302–309, 2016.

[18] M. Khasawneh and A. Agarwal, "A secure routing algorithm based on nodes behavior during spectrum sensing in cognitive radio networks," in *Proceedings of the 35th IEEE International Performance Computing and Communications Conference (IPCCC '16)*, Las Vegas, NV, USA, December 2016.

[19] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, and Y. Song, "Group-based trust management scheme for clustered wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 11, pp. 1698–1712, 2009.

[20] C. Fu, X. Gao, M. Liu, X. Liu, L. Han, and J. Chen, "GRAP: Grey risk assessment based on projection in ad hoc networks," *Journal of Parallel and Distributed Computing*, vol. 71, no. 9, pp. 1249–1260, 2011.

[21] J. Li, R. Li, and K. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 108–114, 2008.

[22] H. H. Ngo, X. Wu, P. D. Le, C. Wilson, and B. Srinivasan, "Dynamic key cryptography and applications," *International Journal of Network Security*, vol. 10, no. 3, pp. 161–174, 2010.

[23] F. Lin, Z. Hu, S. Hou et al., "Cognitive radio network as wireless sensor network security consideration," in *Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON '11)*, pp. 324–328, Dayton, OH, USA, July 2011.

[24] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han, "Defeating primary user emulation attacks using belief propagation in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1850–1860, 2012.

[25] L. Li and C. Chigan, "Fuzzy C-Means clustering based secure fusion strategy in collaborative spectrum sensing," in *Proceedings of the 2014 1st IEEE International Conference on Communications, ICC 2014*, pp. 1355–1360, Sydney, Australia, June 2014.

[26] J. Soto, S. Queiroz, M. Gregori, and M. Nogueira, "A flexible multi-criteria scheme to detect primary user emulation attacks in CRAHNs," in *Proceedings of the 2013 IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, Madrid, Spain, June 2013.

[27] M. J. Saber and S. M. S. Sadough, "Optimal energy detection in cognitive radio networks in the presence of malicious users," in *Proceedings of the 3rd International Conference on Computer and Knowledge Engineering, ICCKE 2013*, pp. 173–177, Mashhad, Iran, November 2013.

[28] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS '09)*, pp. 130–134, Baltimore, MD, USA, March 2009.

[29] A. W. Min, K. G. Shin, and X. Hu, "Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434–1447, 2011.

[30] L. Duan, A. W. Min, J. Huang, and K. G. Shin, "Attack prevention for collaborative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1658–1665, 2012.

[31] H. A. Shah, M. Usman, and I. Koo, "Bioinformatics-inspired quantized hard combination-based abnormality detection for cooperative spectrum sensing in cognitive radio networks," *IEEE Sensors Journal*, vol. 15, no. 4, pp. 2324–2334, 2015.

[32] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2392–2405, 2015.

[33] K.-L. A. Yau, N. Ramli, W. Hashim, and H. Mohamad, "Clustering algorithms for Cognitive Radio networks: A survey," *Journal of Network and Computer Applications*, vol. 45, pp. 79–95, 2014.

[34] M. Khasawneh, A. Agarwal, N. Goel, M. Zaman, and S. Alrabaee, "Sureness efficient energy technique for cooperative spectrum sensing in cognitive radios," in *Proceedings of the International Conference on Telecommunications and Multimedia (TEMU '12)*, pp. 25–30, Chania, Greece, August 2012.

[35] M. Khasawneh and A. Agarwal, "A secure and efficient authentication mechanism applied to cognitive radio networks," *IEEE Access Journal*, vol. 5, pp. 15597–15608, 2017.