Security Threats in Military Cognitive Radio Networks

Feten Slimeni*†, Bart Scheers† and Zied Chtourou*
*VRIT Lab - Military Academy of Tunisia, Nabeul, Tunisia
Email: {feten.slimeni, ziedchtourou}@gmail.com
†CISS Departement - Royal Military Academy (RMA), Brussels, Belgium
Email: bart.scheers@rma.ac.be

***Abstract*—The emergence of new wireless services and the growing demand for wireless communications are creating a spectrum shortage problem. Moreover, the current technique of static frequency allocation leads to inefficiency utilization of the available spectrum. Cognitive radio (CR) and dynamic spectrum management (DSM) concepts, aim to solve this imbalance between scarcity and under utilization of the spectrum by dynamically using the free frequency bands. However, this technology introduces new vulnerabilities and opportunities for malicious users compared to traditional wireless networks due to its intrinsic characteristics. In this paper, we present a comprehensive review of common CR attacks and their potential countermeasures with projection on military radio networks. We classify the attacks based on the four main functions of the cognitive radio, not according to the layers of the OSI model as usually done. Through this classification, we tried to provide directions for related researches to discern which cognitive functionality has to be insured against each threat.**

I. Introduction

The electromagnetic radio spectrum is allocated as fixed frequency bands to legacy users to ensure secure and reliable wireless communication. Recently, because of the explosive growth of wireless services, this policy faces spectrum scarcity in particular spectrum bands. In contrast, a large portion of the assigned spectrum is inefficiently utilized in time and space. This leads to the interest in unlicensed and dynamic spectrum access (DSA) [1].

The cognitive radio (CR) technology enables the implementation of dynamic spectrum management (DSM) without interference between users. It can solve the imbalance between shortage and under utilization of the spectrum. The CRs are able to periodically scan and identify the vacant channels in the spectrum to opportunistically communicate without interfering the communications of legitimate non cognitive users. The CR concept was introduced by Joeseph Mitola in 1999-2000 [2] to describe a conscious, intelligent and flexible radio. It is able to make autonomous decisions and adapt its characteristics according to the variations of the environment. The CR is built on the software defined radio (SDR) technology, which is the result of an evolutionary process from purely hardware-based equipment to software-based equipment. In SDR, the transmitter operating parameters such as the frequency range, the modulation type and the maximum transmission power can be dynamically adjusted by software. The first application of CRN was introduced in [3] which provided the foundation of wireless regional area networks (WRAN) based on CRs.

The application of DSM enables spectrum sharing and aims to avoid interferences between CRs and legitimate transmitters, in one of these main three ways [4]:

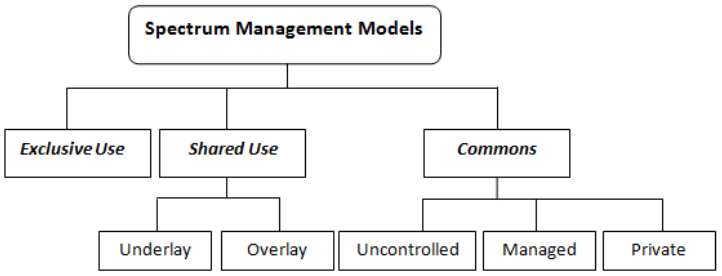

Figure 1: Dynamic Spectrum Management

1) Command&Control or Exclusive-Use:

In this spectrum access model, spectrum bands are licensed to serve for exclusive use and the rules of spectrum users are clearly governed by a central management body. This method solves the problem of interference between legitimate users. However, it can no longer respond to the increased demand of radio spectrum.

2) Shared-Use of Licensed Spectrum:

The spectrum is simultaneously shared between a primary licensed user (PU) of the spectrum band and multiple secondary users (SUs) who can opportunistically use the band. The SUs utilize underlay or overlay approaches to exploit the spectrum without interfering with the PUs.

a) Spectrum Underlay:

The SUs use ultra wideband (UWB) techniques to transmit simultaneously with the PUs over the same channels. A spectral mask is applied to secondary signal so that the interference is below the acceptable level of the PU's signal.

b) Spectrum Overlay:

The SU is allowed to utilize licensed bands in opportunistic way by identifying and exploiting spatial and temporal unused radio spectrum called white space. The spectrum overlay technique was first denoted by Mitola as spectrum pooling

technique and later called opportunistic spectrum access (OSA) in DARPA XG program.

3) Commons:

Under this spectrum access model, the spectrum bands are equitably and fairly accessible to every user and nobody can claim exclusive use. The commons model has three variants:

a) Uncontrolled Commons:

Each user has open spectrum access to a common band and can have many devices operating in it. But, the participating devices have to conform to a peak transmit power.

b) Managed Commons:

These commons are controlled jointly by a group of users with restrictions on who, when and how the resource is used, defined by the controller of the commons. The use of managed commons requires a good management protocol that encapsulates technology agnostic rules together with reliable and scalable mechanisms that quantify rule on performance of participating devices.

c) Private Commons:

The users access to licensed bands at the discretion of license holder. It is like managed commons but the ultimate ownership of the licensed spectrum is still centralized with the license holder who offers either private commons service or spectrum access.

Since countries have diverse spectrum access regulations and recently military operations are often conducted in coalitions, the application of DSM in future military networks will most probably be based on the shared use of licensed spectrum and commons dynamic spectrum access models. Therefore, we will not use the classical PU/SU denomination, but in a more general way classify the users as non-cognitive legacy users, having priority to access the spectrum and cognitive users, having to periodically scan and identify the vacant channels in the spectrum to communicate without interfering the non-cognitive user [5].

In addition to spectrum overcrowding, one of the major issues in military and commercial deployment of cognitive radio technology is security. As all wireless communication networks, cognitive radio networks (CRNs) are susceptible to common wireless security problems like eavesdropping and information tampering, but due to the following specific characteristics, the CRN introduce new classes of security threats [6]:

- High sensing sensitivity

It is an intrinsic characteristic of CR technology to detect even low signals to avoid interference with legacy users. However, it may lead to false detections resulting in inefficient use of the spectrum.

- Hidden terminal problem

This problem occurs when the CRN can't detect the communication of a non cognitive radio by sensing the medium. Therefore, a CR can start transmission and interfere with the legacy user.

- Synchronization requirement

The CRs involved in cooperative spectrum sensing have to sense the spectrum periodically and transfer sensing reports to a fusion center (FC), which takes the decision about the spectrum exploitation. This process requires the synchronization between the cooperative CRs.

- Lack of Common Control Channel (CCC)

In military communication system, a common control channel is often avoided because it is a signal point of failure. This means that the network needs to search for control signals across the entire spectral band.

An attack in CRNs can be defined as a use of these reliability issues resulting either in unacceptable interference to the non cognitive user or missed opportunities for cognitive users, which threats the radio spectrum sharing policy used to manage the spectrum access. Recent tactical military scenarios are based on SDR technology to enhance interoperability among different military services and allied forces, as well as among military and civil authorities. Therefore, these CR intrinsic threats emerge as a challenging issue for advanced defense applications, and have to be resolved to enhance the deployment of CRNs.

In table I, we review diverse classifications used in related surveys to describe the CRN attacks. Most of the papers opt the OSI model layer classification (physical, link, network, transport and cross-layer attacks). Some works use a classification according to the steps of the cognition cycle. However these papers sometimes misclassify certain attacks or do not detail the consequences of given attacks on the cognitive cycle. In this paper, we choose to rank specific cognitive attacks according to the four main functions of the CR and not according to the OSI model nor the cognitive cycle, to better evaluate its impact on CRNs.

In section II, we describe the four main functions of a CR. In the remainder of the paper, we give a more detailed review of common attacks and possible countermeasures for each function with a projection on tactical military context. Finally, we present the conclusions of the work.

Table I: Classifications of CR attacks

CRN attack classification	**Related paper**
Cognition cycle steps	[7], [8]
Inside/outside the CRN	[9]
Layer classification	[10], [11], [12]
Nature of manipulation (sensor, belief, control...)	[13]
Attacker type: malicious/greedy	[14]
CR components	[15]

II. COGNITIVE RADIO ARCHITECTURE

Fig. 2 presents a general architecture of a CR. We can distinguish several components. The application component represents the functionalities of the higher communication layers above the physical and link layers. The sensing component observes the radio atmosphere and transforms the

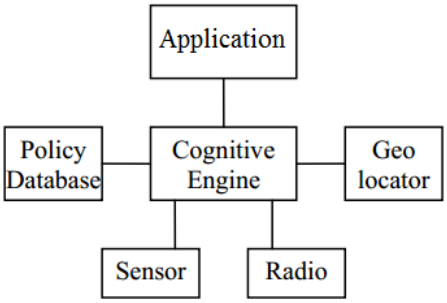

Figure 2: Cognitive Radio components

sensed parameters to the cognitive engine. This cognitive engine combines the received information with the policy information to make the decision about transmission, and the radio transmitter/receiver performs the transmission task. Some CRs also depend on the transmitter location information which is provided by a geo locater [16].

This architecture allows the CR to perform four major functions: spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility.

A. Spectrum Sensing

The CR first gathers (observe) information about its external electromagnetic environment to detect the unused spectrum bands called white spaces. Then, this information is evaluated (orient) to know its significance and to determine the features of each band. To improve the detection performance, cognitive nodes may collaborate to combat sensing issues such as the problem of hidden transmitting nodes. Cooperative spectrum sensing (SS) uses various data fusion schemes which can be classified mainly into hard fusion when the FC collects the local decisions of cognitive nodes, and soft fusion if it collects the local detected signal of each node.

B. Spectrum decision

Based on the evaluation of SS reports taken into account the information from policy database, the CR determines (plan) its alternatives to meet user communication requirements. Then, it chooses (decide) the most appropriate frequency band. In cooperative CRN, the FC makes the final decision about the availability of white spaces by combining either local decisions or local detected signals received from cognitive nodes.

C. Spectrum Sharing

Spectrum sharing techniques manage the allocation of available frequency bands to provide a fair spectrum scheduling among the users and to avoid the interference.

D. Spectrum Mobility known as spectrum handoff

It is defined as the process where the cognitive user changes its frequency of operation or vacate it to a non cognitive user.

According to these main functions, we will classify CR attacks as:

- Spectrum sensing attacks
- Spectrum decision attacks
- Spectrum sharing attacks
- Spectrum mobility attacks

III. Spectrum Sensing Attacks and Countermeasures

Spectrum sensing is the first functionality in the cognition cycle, it consists in detecting available portions of the spectrum. Then, CRs can temporarily transmit over these spectrum holes without creating interference to the legitimate users. It have to periodically sense the spectrum to detect the presence of incumbents and quit the band once detected. However, the sensing information can be falsified by malicious users. The most common attack threatening the functionality of SS is the primary user emulation (PUE) attack.

In this attack, a malicious user emulates the signal of the non cognitive user during the spectrum sensing period to get the priority, since other cognitive users will falsely sense that the frequency is in use by a legitimate user and vacate it. In commons DSM model, we don't have the concept of primary/secondary user, so we have better to call this attack as incumbent emulation (IE) attack to cover different DSM models mainly in military scenarios. This malicious action is easy to implement because the attacker doesn't need to be member of the existing network. The incumbent emulation attack has been studied over different classification criteria:

1) Selfish/Malicious attacker:

The goal of selfish IE attacker is to increase its share of the spectrum resource. A malicious attacker aims on top of being selfish also to interrupt the CRN current service.

2) Power-Fixed/Adaptive attacker:

A power-fixed attack has an invariable predefined power level regardless of the actual cognitive signal power and the surrounding radio environment. An adaptive attacker can employ estimation techniques and learning methods to adapt its transmitting power to the CR and channel parameters.

3) Static/Mobile attacker:

Static attacker has a fixed location, which can be revealed by using positioning techniques such as time of arrival (ToA) and angle of arrival (AoA). A mobile attacker constantly changes its location to escape from localization.

The IE attack can cause many troubles in military CRNs, not only for the spectrum sensing functionality, but also to the other steps of the cognition cycle. The potential consequences and impacts on each step are:

- Sensing step

By periodically sensing the spectrum, the CRs are able to dynamically use frequency white spaces. However, IE attackers may steal these resources.

- Decision step

It is not always possible to identify correctly the true legitimate user from the IE attacker which leads to wrong decision and so to interference with the non cognitive network.

- Sharing step

IE attackers can occupy many of the spectrum opportunities, so CRNs may find no radio resource even to set up a common control channel for delivering the control messages about the shared resources, which can lead to Denial of Service (DoS).

- Mobility step

IE attackers may force CRs to change their operating spectrum bands, which can lead to frequent spectrum handoff inducing QoS degradation and increasing connection unreliability.

A variety of IE attack solutions are presented in the review [17]. The author enlisted various methods but without details. The paper doesn't discern between techniques used just to detect an IE attacker and techniques used as countermeasure.

In the next paragraph, we present the common detection methods followed by some possible defensive techniques along with related references.

A. IE attack detection methods

It is indispensable to detect the IE attacker before thinking about a countermeasure to this attack. However, the CR has the challenge of distinction between the legacy incumbent node and the imitating attacker. To overcome this issue, the CR can localize the transmitting node and compare its position with known legacy users positions. It can also determine the characteristics of the detected signal and compare it with incumbent signals. We explain in table II common detection techniques and we refer to some papers.

Table II: Detection techniques of IE attacker

Detection method	**Technique description**	**Related paper**
Transmitter verification	-Distance difference test (DDT) or distance ratio test (DRT) to estimate the transmitter location -Received signal strength (RSS), time of arrival (ToA) or angle of arrival (AoA) to determine the characterizations of the detected signal -Localization defense (LocDef) combining location and characterization previous techniques	[18]
Analytical detection model	Fenton Approximation Method to determine the mean and the variance of the detected signal + Markov inequality or Wald Sequential Probability Ratio Test (WSPRT) to determine a threshold on the probability of a successful IEA	[19], [20]
Signal activity Pattern Acquisition and Reconstruction System	Reconstruction of the observed signal activity pattern (such as the ON/OFF periods) through spectrum sensing. + Examination of the reconstruction error to distinguish PU's signal activity pattern from attacker's one.	[21]

B. Defense schemes against IE attacker (IEA)

After identifying the IE attacker, the CR can either try to avoid or to countermeasure the attacker. The first approach consists in avoiding the channels used by the IE attacker. The CR can use game theory and learning algorithms, such as the Q-learning algorithm, to train until learning to choose good channels. For example, a defense scheme is proposed in [22] and called dogfight in spectrum. The scenario is modeled as a zero sum game between the IE attacker and defending CRs. It is based on randomly choosing a channel to sense and transmit at each time so as to avoid the IE attack statistically.

A countermeasure proposed in [23], assigns weights to the local detected energies to eliminate the malicious signal sent by the IE attacker. The problem is solved in [24] by using spatial correlation based user selection to choose the members taking part in cooperative spectrum sensing, and the maximum-minimum eigenvalue (MME) based detection mechanism to perform the cooperation. A technique of belief propagation of location information, presented in [25], enables not only detecting but also mitigating the IE attack. In this approach, each cognitive sensor calculates the location information based on RSS measurements and exchanges messages with the neighbors to detect the IE attacker according to the mean of the final beliefs based on a belief threshold. Then, a broadcast message informs all cognitive users about the characteristics of the malicious signal to avoid it in the future sensing period, thus the IE attacker will no longer falsify the sensing results.

IV. Spectrum Decision Attacks and Countermeasures

In the decision step, the CR decides which of the available bands is the appropriate according to the QoS requirements of its application. This decision is based on the local observations of the sensors and on the information from the policy database. In cooperative cognitive radio network, each CR senses the spectrum periodically and reports the measurement results to the FC node, which combines the data and makes the final decision of whether the non cognitive user is present or not. However, this result is based on the assumption that all users sending the sensing reports are honest and there is no malicious entity that can manipulate the spectrum decision process. This defect leads to several attacks by malicious nodes inside the CRN. The common threats to the spectrum decision functionality are the spectrum sensing data falsification (SSDF) and the objective function attacks.

A. Spectrum sensing data falsification (SSDF) attack

In cooperative spectrum sensing process, malicious user inside the CRN can mislead the final result by sending false information such as reporting the presence of legacy user to occupy the spectrum himself, or hiding the existence of legacy user to cause collision. This attack is known as SSDF attack or Byzantine attack.

Almost all related papers classify this issue as a sensing attack, but in this paper we consider it as a decision attack because it threatens the decision process after receiving the sensing reports. We present in the following paragraph the proposed solutions which can be classified into three categories, along with some related works:

1) Reputation based Approaches:

These approaches consist in assigning suspicion levels to the cognitive nodes. If the suspicion level of any node exceeds a certain threshold, it is marked as malicious and removed from decision process. However, this method assumes that the base station has prior knowledge about the activities of attackers which is not very common. Without such information, the thresholds are approximated, resulting in significant false detections of attackers. In table III, we present and discuss diverse proposed approaches to solve this problem.

Table III: SSDF reputation based countermeasures

Approach	**Description**	**Paper**
Onion peeling	Reputation values based on estimations or Bayesian statistics	[26], [27]
Weighted sequential probability ratio test (WSPRT)	-Combines reputation and SPRT to identify malicious nodes -Outperforms standard FC decision making strategies (e.g. OR, AND, and SPRT) in both minimizing missed detections and maximizing the correct sensing ratio.	[28]
Game theory	-Zero-sum game between attackers and the FC -Use of minimax approach to find optimal defense strategy -Kullback-Leibler divergence (KLD) and error probability at the FC considered as performance metrics to characterize detection performance. -Performance limits boundaries are established for independent and cooperative attackers	[29]
Dempster-Shafer	-The trust value is based on direct and indirect users observations -Degrade the impact of malicious entities during distributed cooperative spectrum sensing	[30]
Adaptative reputation based clustering algorithm	-Clustering the nodes according to the sensing history and initial reputations. -Then each node is assigned a positive or negative share based on its participation in the final decision to adjust its reputation. -The adjusted reputations are used to adjust the number of clusters for the next step.	[31]
Support vector data description (SVDD) algorithm	-SVDD is a kind of one-class classification method based on Support Vector Machine and described by a few target objects, known as support vectors. -It tries to construct the boundary around the target data enclosed within a minimum hyper-sphere. -Then the algorithm votes between trusted nodes to decide whether the spectrum is empty.	[32]

2) Data Mining Approaches:

Using these approaches, the fusion center have to intuitively interpret the received sensing report to decide to discard it if it is from a stealthy attacker.

An abnormality detection in the reported data mining is used in [33] as approach to detect independent attackers. This approach starts by representing the history of reports of each CR by a point in the space. Then, it calculates the Hamming distance between each pair of two CRs and declares the presence of attackers when the distance deviates from a normal level. However, when attackers collaborate, they can successfully evade this detection approach.

More robust approaches can analyze particular pieces of sensing reports using a biweight estimate and median absolute deviation to calculate magnitudes, which are then compared against thresholds to identify the attackers [34]. The proposed method increases missed detections when using incorrect static thresholds because inaccurately identified CRs could be excluded from the decision process. The correct setting of the detection thresholds can only be achieved with prior knowledge of attacker distribution which is unlikely to be available.

The detection of abnormal sensing reports can be combined with the verification of CRs locations, as proposed in [35]. In this reference, spatial correlation of the received signal strength among CRs is exploited to get the evidence whether the received signal strength is consistent with the location from where it is generated. Then, Dempster-Shafer theory is used to filter out abnormal reports by combining the evidence collected from the spatial correlation algorithm in each sensing period.

3) Artificial Intelligence Approaches:

The decision process is susceptible to long-term manipulations caused by the extension of malicious inaccurate information which become a historical fact. To avoid the propagation of corrupted reports, learned values should be updated automatically by certain level of common sense. The authors in [36] proposed the use of swarm behavior in determining a global decision on whether a sensed signal was actually generated by a malicious user, along with a trust-based scheme.

We suggest exploiting the learning and the reconfigurability abilities of the CR, to implement suitable learning algorithms (e.g. the Q-learning algorithm) in order to update the learned values and to get online defense strategy to the SSDF attack.

The SSDF attack requires sending a falsified sensing report to the FC leading to wrong decision, but an attacker can also maximize his own gain (in the transmission power or in the spectrum) by a simple manipulation of his utility function, as described in the following attack.

B. Biased utility function attack

The CR should adjust its transmission parameters according to the environment, such as its center frequency, bandwidth, power, modulation type, coding rate, channel access protocol, encryption type and frame size. According to [37], the radio might have three goals: low energy consumption, high data rate, and high security. Each of these goals has a different weight, which leads to a different objective function for each application.

The strategy of the biased utility function attack is the following: a malicious user can manipulate the transmission parameters to make the FC decision biased towards its benefit. For example, if a malicious user tweaks its utility function to transmit at higher power, it will result in other users getting less bandwidth. Some CRs may not even get to transmit. A scenario presented in [37] consists in an objective function composed of transmission rate (R) and security (S). An attacker may reduce the transmission rate by launching a jamming attack and hence reducing the overall objective function. Then, the CR will be forced to use a low security level and therefore it will be easily hacked. This attack is also known as objective function attack and belief-manipulation attack.

Game theory can be exploited to model utility function problems. For example, in [38], the authors propose an objective function to adjust CRs transmission power with the constraint that the interference temperature due to the CRN transmissions on the non cognitive receivers is below a given threshold. The problem is formulated as a public game and nash equilibrium solutions for a global optimum determines the transmit powers of the CRs.

There have been only few effective methods of mitigating objective function attacks. The paper [39] suggested defining thresholds for each of the adjustable parameters, so communications would be prevented when one or more of the parameters does not respect its predefined threshold. A secure spectrum decision protocol for a clustered infrastructure based network is proposed in [40]. In this solution, the spectrum decisions are made periodically and independently in each cluster. The suggested protocol consists of three steps:
(1) Each node should communicate with the cluster head (CH) to join the decision process. It generates a sequence of symmetric keys using iterative application of a hash function to some initial value. The CH checks the authenticity of the message using the public key related to each node, then it stores the identity of the node and the related information if the verification is successful. The CH sends back a signed message including information about communication parameters such as the time/frequency schedule for submitting sensing data and available channels for ordinary communication.
(2) The accepted nodes in each cluster send their spectrum sensing data to the CH using the key chain generated in the joining operation to protect the authenticity of the sensing information. The CH verifies the authenticity of the received messages to use it in the final decision.
(3) The CH makes the decision and sends back the final channel assignment to the nodes of its cluster.

In this section, we have reviewed the common attacks to the spectrum decision functionality in cooperative CRNs. These attacks are harmful to cooperative military CRNs, such as in a scenario with coalition forces. It can lead to interferences with incumbent transmitters and prevent the efficient and secure spectrum access because of wrong decisions.

V. Spectrum Sharing Attacks and Countermeasures

The spectrum sharing process manages the access of the CRs to the unused spectrum bands and governs the communication sessions. The spectrum sharing techniques can be applied inside a CRN (intra-network spectrum sharing) or among multiple coexisting CRNs (inter-network spectrum sharing) [41].

Generally, the management of the spectrum needs common control channels (CCC) to coordinate the DSA and to exchange control messages such as local sensing reports. However, in military applications CRNs may operate in dynamic spectrum-scarce and hostile environment. Therefore, CCCs could not be constantly available to CRs for control message exchange and could be susceptible to malicious behavior such the jamming and saturation attacks.

A. Common Control Channel jamming/saturation attack

Cooperative CRNs use a CCC to achieve spectrum sharing. However, this channel is susceptible to jamming and saturation attacks. Jamming this control channel can disrupt the communication among CRs, resulting in packet losses and sensing delays which may degrade the system performance. It can even lead to DoS, once the CCC is saturated by attackers. Common approaches to mitigate CCC jamming attack can be classified as follows:

1) Cross-channel control messages:

Using this defense approach, CRs continue to transmit on the jammed channel under interference to deceive the attacker and notify others about the new CCC for receiving control messages. As a result, the channels for transmitting and receiving control messages can be different to maintain the control message exchange with neighbors under jamming [42].

2) Random key distribution to hide CCC locations:

Each CR has a valid key to be able to locate the allocated CCCs by using keyed hash functions. Any compromised node having only partial keys in the key space will not be able to jam all the CCCs. The random CCC key assignment reduces the risks of learning the key assignment structure from the attackers [42].

3) Channel hopping:

The cluster heads are responsible of predetermining the hopping sequences for common control within the clusters. During the jamming attack, CRs hop on different sequences and communicate throw the predetermined CCC in the designated time slots without knowing the hopping sequences of others [43].

4) Intrusion defense strategies:

Diverse intrusion detection techniques are exploited to mitigate the CCC jamming attack [44]. Here some examples:

a) Action Strategy Coordination (ASC):

This technique is used to coordinate the action strategies among the CRs to establish a CCC by the exchange of a short control message including coordination parameters (current state, selected action and learning rate). The CRs update their action selection strategy with their own coordination parameters and those received from their neighbors. Such strategy increases the probability of selecting commonly available channels as control channels.

b) Best-Effort Cooperative Sensing (BCS):

This technique can combat jamming attacks and enhance jamming resilience by reducing sensing errors. BCS is a distributed cooperative sensing scheme that CRs make the best efforts to share local sensing data with neighbors by using control links established in the previous stage yet still valid in the current stage, and individually make sensing decisions based on any collected sensing data. Unlike conventional distributed sensing schemes, BCS does not require the participation of all neighbors or multiple iterations of message exchanges.

c) Deployment Density and Scalability:

It means the deployment of CRs in a given area. Increasing the deployment density in the jamming region leads to decrease of the average distance between the CRs while the average distance between the attacker and victims remains the same. This results in better SINR and less effective jamming perceived at the CRs.

5) Game theory exploitation:

The interaction between the CCC jammer and the CRs can be modeled as a game and an optimal anti-jamming approach when the game reaches the nash equilibrium. For example, the authors in [44] model the interactions of intelligent jammers and CRs as a stochastic general-sum game, called jamming-resilient control channel (JRCC) game. In this scenario, the CRN selects the optimal control channel allocation strategy by using an enhanced multiagent reinforcement learning (MARL) algorithm along with cooperative intrusion defense strategies.

Even, during a communication session, a jammer can intentionally and continuously transmit packets to prevent the CRs from exploiting the shared spectrum.This attack is known as intentional jamming attack.

B. Intentional Jamming attack

Malicious attackers may jam the current CR channel to make its signal-to-interference-plus-noise ratio (SINR) below the required threshold and to prevent it from efficient exploitation of the spectrum. This attack can be amplified by jamming with high power in several spectral bands. Furthermore, the jammer becomes difficult to caught if it performs the attack in one geographical area and moves to another one.

Intentional jamming is one of the most easy attacks to happen in CRNs and can hinder both cognitive and non cognitive network communications. It can be a dangerous attack to CR military networks because it presents many challenges, such as the time taken to detect the malicious user and to mitigate the attack which effects severely the network performance and reliability.

This attack can be carried out in several ways, and jammers can be classified according to the following criteria:

a) Spot/Sweep/Barrage jamming:

Spot jamming consists in attacking a specific frequency, while a sweep jammer will sweep across an available frequency band. A barrage jammer will jam a range of frequencies at once.

b) Single/Collaborative jamming:

The jamming attack can be done by a single jammer or in a coordinated way between several jammers to gain more knowledge about the network and to efficiently reduce the throughput of the cognitive users.

c) Constant/Random jamming:

The jammer can either send jamming signals continuously on a specific channel or alternate between jamming and sleeping.

d) Deceptive/Reactive jamming:

A deceptive jammer continuously transmits signals in order to imitate a legitimate or primary user. A reactive jammer transmits only when it detects busy channel to cause collisions.

The traditional anti-jamming solutions used in wireless networks consist in spread spectrum techniques by the use of either frequency hopping (FH) or direct-sequence spread spectrum (DS-SS) methods [45]. These solutions are enhanced to mitigate the jamming attack in CRNs.

1) Frequency hopping:

The CR is characterized by its ability of dynamic spectrum access to use the spectrum in opportunistic way. This ability can be exploited to overcome jamming attacks since the CR can change its operating frequency to avoid the jammers. However, the exploitation of frequency hopping in CRN anti-jamming approaches present a trade-off between the resource consumption every time to change the jammed frequency and the jamming impact if the CR still using the same frequency even jammed.

Recently, diverse CRN frequency hopping defense strategies, were analyzed in [46]. It presented proactive or impetuous hopping (selecting a new set of frequencies at every slot, irrespective of the jamming) and reactive or conservative hopping (unjammed users keep the same frequencies for the next slot, while the jammed users choose a set of new unused frequencies that exclude the jammed ones). The authors proposed a multi-tier proxy based cooperative defense strategy, in which users form tiers to exploit the temporal and spatial diversity to avoid jamming. The jammer's success was based on selecting a channel to jam, that is in use by a regular node. To increase its chances of success, it might use the approach of equal power partial band spoofing, by distributing its transmit power budget among multiple randomly selected channels. The authors started by computing the effect of a single jammer on a single receiver, then summed the jamming signal strengths to compute the total interference as the collaborative jammers distribute their transmit power budget over multiple channels.

The behaviors of the CR, doing transitions between available frequencies, and the jammer, trying to prevent it from efficiently utilizing the spectrum, can be modeled using game theory. In this context, several works have been using game models and learning algorithms to find optimal anti-jamming strategy for the CR. For example in [47], the authors model the CRN jamming scenario as zero-sum game because of the opposite CR and jammer objectives. Furthermore, they implement the minimax-Q learning algorithm to find the optimal defense policy. Recently, the problem is formulated as a non-zero-sum game in [48], by taking into account different hopping and transmission costs, as well as diverse reward factors for both the transmitter and the jammer side. Authors make use of fictitious play learning algorithm to learn optimal defense strategy.

2) Direct-sequence spread spectrum (DS-SS):

This spread spectrum technique consists in spreading the signal over several pieces of non-overlapping channels. It can be exploited as an anti-jamming technique because the jammer will have to choose either to jam a large number of

channels with negligible jamming effect in each one or to jam only few channels with important effect. The authors, in [49], proposed an uncoordinated spread spectrum technique that enables anti-jamming broadcast communication without predefinad shared secrets. They aimed to improve the common spread spectrum which depends on secret pairwise or group keys shared between the sender and the receivers before the communication, to adapt it for critical applications such as emergency alert broadcasts and military communications.

A random channel sharing was proposed, in [50], for broadcast CR communication to mitigate the insider jamming attack which resist to spread spectrum techniques. Spread spectrum has long been an effective technique to mitigate jamming attacks. However, in broadcast communication characterized by many receivers, once the attacker compromises a single receiver, he can discover which channels are in use and directly block those channels. The proposed idea is to organize receivers into multiple broadcast classified trusted/suspicious groups and use different channels for different groups. This ensures that a compromised receiver can only affect the members of the group it has been assigned to. A *'divide and conquer'* strategy is then used to isolate malicious receivers. The receivers are adaptively regrouped if the attacker launches a jamming attack so that the benign nodes are more likely to be merged into the trusted group, and the traitors are more likely to be included in a number of smaller suspicious groups. The random channel sharing improve the group-based approach by dynamically assign channels to groups such that different groups will randomly share their assigned channels. The data sent over the shared channel can reach more than one group, saving substantial communication cost. The receivers themselves do not know if their channels are shared with other receivers. Therefore, if a given channel is jammed and this channel is only assigned to one receiver, that receiver will be considered as one of the insiders. Thus, no matter when the insider chooses to jam the channel, there is a chance that he will be detected and removed from future channel assignments. This scheme requires each receiver to listen to one channel at a time, instead of multiple channels.

3) Other anti-jamming techniques:

In addition to approaches trying to evade the jammers, the CR can use coding techniques to mitigate the effect of the jamming attack on the transmitted signal. For example in [51], a hybrid jamming mitigating approach is proposed to better handle the effect of malicious jamming nodes in the context of fault model classifications (including transmissive and omissive value faults due to the jamming attack) and their respective fault handling. A transmissive fault results from delivery of erroneous value to one or more receivers, and omissive fault results from failure to deliver any value to one or more receiver. The presented approach is based on a hybrid forward error correction (FEC) code defined by the concatenation of Raptor codes (used to regain lost data due to Omissive faults through data redundancy) and SHA-2 hash function (used to handle transmissive faults). Furthermore, the concept of honeynode has been shown in [52] to be effective in deceiving jammers about the transmitting nodes. In this reference, a single honeynode is dynamically selected for each transmitting period, to act as a normal transmitting CR in order to attract the jammer to a specific channel.

Closed-form expressions to the jamming probabilities and the throughput of the CRN under various jamming attack models, was determined in [53] using the concept of Markov chain. Furthermore, the authors calculated the minimum and the maximum CRN throughput expressions under jamming, along with optimization of important anti-jamming parameters.

The jamming attack has been widely exploited as strategic maneuver in military wireless communications. This problem has been intensively researched for traditional wireless networks but it is still a challenging issue in CRNs.

VI. Spectrum Mobility Attacks and countermeasures

The CR have to vacate the current spectrum band whenever it detects an activity of a non cognitive user in that channel. In order to establish smooth communication as soon as possible, the CR needs to select a new appropriate spectrum band, and move immediately. This process is called spectrum mobility or hand-off.

An attack during spectrum mobility consists in forcing the CR to do handoff in wrong moment disturbing higher layers functionalities like routing protocols or security mechanisms. This problem is still less researched and most works are based on the assumption of successful handoffs. In this section, we enlist the common spectrum mobility attacks and we propose directions to future countermeasures.

A. Routing information Attack

A routing information attack is initiated when a malicious node causes spectrum handoff in the victim node just before it exchanges the routing information. During spectrum mobility, the victim node stops all ongoing communication, vacates the spectral band, opportunistically selects a new spectrum for transmission, scans the entire spectrum band to identify the neighboring nodes and informs it of the new frequency. Only, after all these operations, the CR can exchange the updated routing information with its neighbors. Until this period any path that goes through the victim node and its neighbors uses stale routing information.

One proposed solution to this attack is collision-free resident channel selection based solution (CF-RCS). It consists in selecting a resident channel by each node from the available channel set during network initialization. It then broadcasts this selection with its neighbors. Nodes are expected to receive any updates on the resident channel. However, this protocol requires that each cognitive node is equipped with two half duplex transceivers with one waiting on the resident channel for a request of control message exchange, and the other sitting on the data transmission channel [54].

B. Key Depletion Attack

Despite cryptographic measurements, the security of military CRNs could be degraded significantly with the important number of handoffs due to malicious issues. Frequent spectrum handoffs result in multiple sessions needed for any given application, and hence large number of cryptographic keys is used at the beginning of every transport layer session. Therefore, the probability of using the same key twice will

increase. Key repetitions can be exploited to break the cipher system.

For example, the wired equivalent privacy (WEP) and the temporal key integrity (TKIP) protocols used in IEEE 802.11 link layer are vulnerable to key repetition attacks [55]. The counter cipher mode with block chaining message authentication code protocol (CCMP) is designed to exponentially delay key repetitions. It offers enhanced security compared to TKIP by using 128-bit keys with a 48-bit initialization vector. It takes 128 bit key blocks of data through the AES encryption standard and uses WPA1 and WPA2 to allow for a quick handoff cipher block [56].

The security of the spectrum mobility functionality is still a challenging issue and an interesting road of research. Other security measurements should be added to the cryptographic algorithms to enhance the resistance counter the handoff process attacks. We can deduct from our enlisted references in previous sections about proposed solutions to CRN attacks, that game theory has emerged as a tool to model the IE, biased utility function and spectrum sharing attacks. Since there is a dynamics of pursuit and evasion between the CR and an attacker during the handoff process, game theory can be also a suitable tool to study the attacks of the spectrum mobility functionality.

VII. Conclusion

Recently, tactical military missions are characterized by the coexistence of multiple heterogeneous wireless networks in the same geographical area, which leads to the problems of interferences and malicious users. Furthermore, growing military wireless services are continuously increasing the spectrum requirements and reveal the problem of bandwidth shortage. The investment of CR technology may mitigate these tactical problems through using efficient DSM. However, CRNs are susceptible to specific security issues related to its dynamic spectrum access. Furthermore, the CR technology may be also exploited by the attackers to launch more intelligent and complicated threats. In this paper, we tried to give a broad comprehensive review of CRN attacks along with related works with the focus on tactical military applications. We have differently classified intrinsic CR threats according to the main functions of the CR (sensing, decision, sharing and mobility) to better understand the effect of each attack. We hope that this paper reveals directions for future CRN security researches especially in the context of military CRNs.

References

[1] K. Harrison, "Cognitive radios in the TV whitespaces: challenges and opportunities," Master's thesis, EECS Department, University of California, Berkeley, Dec 2011.

[2] J. Mitola, "Cognitive radio:an integrated agent architecture for software defined radio," PhD Thesis, Royal Institute of Technology (KTH), May 2000.

[3] C. Cordeiro, K. Challapali, D. Birru, and Sai Shankar N, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," in *Proc. IEEE Int. Symp. New Frontiers Dynamic Spectr. Access Networks*, 2005, pp. 328–337.

[4] S. Courtier and B. Scheers, "The state of the art of dynamic spectrum access," in *Military Communications and Information Systems Conference (MCC'2011), Prague, Czech Republic, September 2009*.

[5] B. Scheers, "Introduction of dynamic spectrum access technology in NATO europe tactical communications," in *IEEE Military Communications Conference (MILCOM'2013), pages 737-742, San Diego, CA, USA, November. (Invited Paper)*.

[6] Q. Mahmoud, *Cognitive Networks: Towards Self-Aware Networks*. John Wiley and Sons, 2007.

[7] W. Alhakami, A. Mansour, and G. A. Safdar, "Spectrum Sharing Security and Attacks in CRNs: a Review," *International Journal of Advanced Computer Science and Applications(IJACSA)*, vol. 5, no. 1, pp. 76–87, 2014.

[8] S. T. Zargar, M. B. Weiss, C. E. Caicedo, and J. B. Joshi, "Security in dynamic spectrum access systems: A survey," University of Pittsburgh, Working Paper, December 2009.

[9] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the phy-layer approach to defense against security threats in cognitive radio networks," *IEEE Network*, 2013.

[10] D. Hlavacek and J. M. Chang, "A layered approach to cognitive radio network security: A survey," *Computer Networks 2014*.

[11] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, 2013.

[12] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey," *J. Network and Computer Applications*, 2012.

[13] S. Bhattacharjee, S. Sengupta, and M. Chatterjee, "Vulnerabilities in cognitive radio networks: A survey." *Computer Communications*, 2013.

[14] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu, and V. C. M. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions," *Proceedings of the IEEE*, pp. 3172–3186, 2012.

[15] T. X. Brown and A. Sethi, "Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: A multi-dimensional analysis and assessment," *Mob. Netw. Appl.*, vol. 13, no. 5, Oct. 2008.

[16] M. A. Butt and M. Zaman, "Cognitive radio network: Security enhancements," *Journal of Global Research in Computer Science JGRCS*, 2013.

[17] A. Singh and A. Sharma, "A Survey of Various Defense Techniques to Detect Primary User Emulation Attacks," *International Journal of Current Engineering and Technology*, 2014.

[18] R. Chen, J.-M. P. 0001, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks." *IEEE Journal on Selected Areas in Communications*, no. 1, pp. 25–37, 2008.

[19] Z. J. S. Anand and K. P. Subbalakshmi, "An analytical model for puea in cognitive radio networks," *IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2008.

[20] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proceedings of IEEE International Conference on Communications, ICC, Dresden, Germany, 14-18 June 2009*, pp. 1–5.

[21] C. Xin and M. Song, "Detection of PUE attacks in cognitive radio networks based on signal activity pattern," *IEEE Trans. Mob. Comput.*, 2014.

[22] H. Li and Z. Han, "Dogfight in spectrum: Combating primary user emulation attacks in cognitive radio systems, part I: Known channel statistics," *IEEE Transactions on Wireless Communications*, 2010.

[23] C. Chen, "Investigation of primary user emulation attack in cognitive radio networks," thesis, Stevens Institute of technology, 2011.

[24] F. Liu, H. Chen, L. Xie, and K. Wang, "Maximum-minimum eigenvalue detection-based method to mitigate the effect of the PUEA in cognitive radio networks," *Wireless Communications and Signal Processing (WCSP), 2011 International Conference, pp.1,5, 9-11 Nov. 2011.*

[25] Z. Yuan, D. Niyato, H. Li, and Z. Han, "Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks," in *Proc. IEEE WCNC, Mar. 2011, pages 599 - 604*.

[26] K. Zeng, Q. Peng, and Y. Tang, "Mitigating spectrum sensing data falsification attacks in hard-decision combining cooperative spectrum sensing," *Science China Information Sciences*, 2014.

[27] W. Wang, H. Li, Y. Sun, and Z. Han, "CatchIt: Detect malicious nodes in collaborative spectrum sensing," in *Proceedings of the 28th*

IEEE Conference on Global Telecommunications (GLOBECOM'09), Honolulu, Hawaii, USA, 2009.

[28] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. 27th Conf. Comput. Commun., Phoenix, AZ, Apr. 13-18, 2008, pp. 1876-1884*.

[29] 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*, 2011.

[30] J. Wang, S. Feng, Q. Wu, X. Zheng, Y. Xu, and G. Ding, "A robust cooperative spectrum sensing scheme based on Dempster-Shafer theory and trustworthiness degree calculation in cognitive radio networks," *EURASIP J. Adv. Sig. Proc.*, 2014.

[31] C. S. Hyder, B. Grebur, and L. Xiao, "Defense against spectrum sensing data falsification attacks in cognitive radio networks," in *SecureComm*, 2011.

[32] F. Farmani, M. A. Jannat-Abad, and R. Berangi, "Detection of SSDF attack using SVDD algorithm in cognitive radio networks," in *CICSyN*, 2011.

[33] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: an abnormality detection approach," *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN)*, 2010.

[34] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system." *IEEE Transactions on Wireless Communications*, 2010.

[35] J. Du, D. Guo, B. Zhang, and L. Shang, "A secure cooperative spectrum sensing scheme in mobile cognitive radio networks," *IJDSN*, 2014.

[36] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," in *Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008). 3rd International Conference, Pages: 1-8, Singapore, 15-17 May 2008*.

[37] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," in *Journal of Internet Technology Vol. 12 No.2, 2011*.

[38] Y. Xing, C. N. Mathur, M. A. Haleem, R. Chandramouli, and K. P. Subbalakshmi, "Priority based dynamic spectrum access with QoS and interference temperature constraints," in *ICC*. IEEE, 2006.

[39] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing cognitive radio networks." *Int. J. Communication Systems*, 2010.

[40] G. Jakimoski and K. P. Subbalakshmi, "Towards secure spectrum decision," in *ICC*, 2009.

[41] A. Huseyin, *Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems*. Springer, 2007.

[42] B. F. Lo, "A survey of common control channel design in cognitive radio networks." *Physical Communication*, 2011.

[43] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," in *WISEC*. ACM, 2009.

[44] B. F. Lo, "Design and analysis of common control channels in cognitive radio ad hoc networks," thesis, Stevens Institute of technology, 2013.

[45] G. Ponuratinam, B. Patel, and S. S. R. K. M. Elleithy, "Improvement in the spread spectrum system in DSSS, FHSS, and CDMA," 2013.

[46] W. Wang, S. Bhattacharjee, M. Chatterjee, and K. Kwiat, "Collaborative jamming and collaborative defense in cognitive radio networks," *Pervasive and Mobile Computing*, vol. 9, no. 4, pp. 572–587, 2013.

[47] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An anti-jamming stochastic game for cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, 2011.

[48] K. Dabcevic, A. Betancourt, L. Marcenaro, and C. S. Regazzoni, "A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference*.

[49] C. Pöpper, M. Strasser, and S. Čapkun, "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques," *IEEE Journal on Selected Areas in Communications*, 2010.

[50] Q. Dong, D. Liu, and M. Wright, "Mitigating jamming attacks in wireless broadcast systems." *Wireless Networks*, 2013.

[51] V. Balogun and A. Krings, "On the impact of jamming attacks on cooperative spectrum sensing in cognitive radio networks," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop (CSIIRW '13), 2013*.

[52] S. Bhunia, X. Su, S. Sengupta, and F. J. Vázquez-Abad, "Stochastic model for cognitive radio networks under jamming attacks and honeypot-based prevention," in *Distributed Computing and Networking - 15th International Conference (ICDCN '14), pages 438-452, Coimbatore, India, January 4-7, 2014. Proceedings*.

[53] C. X. Wednel Cadeau, Xiaohua Li, "Markov model based jamming and anti-jamming performance analysis for cognitive radio networks." Communications and Network, 2014.

[54] Y. L. Xiangquan Zheng and H. Zhang, "A collision-free resident channel selection based solution for deafness problem in the cognitive radio networks," *IEEE International Conference, Wireless Information Technology and Systems (ICWITS), pp.1-4, 2010*.

[55] D. S. Vernekar, "An investigation of security challenges in cognitive radio networks," thesis, University of Nebraska - Lincoln, 2012.

[56] K. Z. Faith M. Heikkila and P. G. Ed Sale, "Securing telecommunications: Mission impossible?" *International Legal Technology Association (ILTA) White Papers and Surveys, Creating Omnipresence Through Telecommunications Technologies, Nov. 2005, p.3*.