Future Internet **2010**, *2*, 212-237; doi:10.3390/fi2030212

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Review

Misbehavior Scenarios in Cognitive Radio Networks

Stamatios Arkoulis [1], Giannis F. Marias [1], Pantelis A. Frangoudis [1], Jens Oberender [2], Alexandru Popescu [3], Markus Fiedler [3], Hermann de Meer [2] and George C. Polyzos [1,*]

[1] Mobile Multimedia Laboratory, Athens University of Economics and Business, Athens 11362, Greece; E-Mails: arkoulistam@aueb.gr (S.A.); marias@aueb.gr (G.F.M.); pfrag@aueb.gr (P.A.F.)

[2] Faculty of Computer Science and Mathematics, University of Passau, Innstraße 43, 94032 Passau, Germany; E-Mails: jens.oberender@uni-passau.de (J.O.); demeer@fmi.uni-passau.de (H.M.)

[3] Department of Communications and Computer Systems, School of Computing, Blekinge Institute of Technology, 371 79 Karlskrona, Sweden; E-Mails: app@bth.se (A.P.); markus.fiedler@bth.se (M.F.)

* Author to whom correspondence should be addressed: E-Mail: polyzos@aueb.gr; Tel.: +30-210-820-3650; Fax: +30-210-820-3325.

Received: 21 June 2010; in revised form: 20 July 2010 / Accepted: 23 July 2010 / Published: 29 July 2010

Abstract: Recent advances in the fields of Cognitive Radio and the proliferation of open spectrum access promise that spectrum-agile wireless communication will be widespread in the near future, and will bring significant flexibility and potential utility improvements for end users. With spectrum efficiency being a key objective, most relevant research focuses on smart coexistence mechanisms. However, wireless nodes may behave selfishly and should be considered as *rational* autonomous entities. Selfishness, pure malice or even faulty equipment can lead to behavior that does not conform to sharing protocols and etiquette. Thus, there is a need to secure spectrum sharing mechanisms against attacks in the various phases of the sharing process. Identifying these attacks and possible countermeasures is the focus of this work.

Keywords: spectrum sharing; dynamic spectrum access; security; wireless network access

---

1. Introduction

Wireless communications, and especially 4G Mobile systems, will be a critically important component of the future Internet [1] for a number of reasons. Most importantly they will fully support user mobility with personal devices (e.g., today's smartphones accessing the Internet) [2]. Offering

multimode protocol stacks, the new generation smart-phones will support fast wireless system discovery and selection, and functions that determine and update the location of the terminals in various systems. This will provide the necessary flexibility to perform horizontal, as well as vertical, handoffs, with minimum handover latency and packet loss. Thus, network heterogeneity will enable the ubiquitous network paradigm [3]. Additionally, they enable the self-organization of personal area networks where many, different personal devices, handsets, as well as sensors and actuators, in the environment will be discovered, associated, and interact easily within dynamically assembled sets of surroundings. Today's Bluetooth-based paradigm of personal area networking will be extended to a more dynamic environment where, for example, as a user changes context and surroundings, different audio-video devices will be selected for rendering, enabling personal mobility [2]. Moreover, wireless solutions are more easily introduced or updated in everyday life, including increasing data rates and performance (even though the technical problems are typically much harder for wireless communications). Furthermore, a plethora of devices of small form factor, equipped with wireless communications capabilities, will also be the building blocks of the *Internet of Things* [4,5]. This new ubiquitous (mostly machine-to-machine) communications environment will challenge all current networking layers. Focusing on the wireless communications layer, one of the most significant challenges is how to cope with the increased demand for spectrum that the vast amount of wireless devices will bring about. Also, with sensor networks being an integral part of a future wireless Internet, specific challenges emerge [6]. Crowded spectrum may lead to excessive packet loss for traffic that is inherently bursty (due to the event-driven traffic patterns in wireless sensor networks), and retransmissions will faster exhaust the limited power resources of sensor nodes. Also, in many cases, reliably communicating sensor readings is critical (e.g., for healthcare applications). Cognitive Radio networks are part of the answer.

Recent advances in the area of wireless communications promise a breakthrough both from the user and the service provider point of view. There is a clear trend towards open (or at least more open) wireless access, mainly driven by the low cost and the ease of deployment of equipment that operates in unlicensed (more accurately, "license exempt") spectrum bands. On the other hand, there is the realization that spectrum is often scarce (e.g., in the case of unlicensed bands in dense urban environments), or underutilized (e.g., in the case of analog TV bands). On the other hand, acquiring a license to operate in a contention-free fashion is very costly (see, for instance, the 3G spectrum auctions).

The above observations have, to a significant extent, motivated research in the areas of self-organized wireless systems and Cognitive Radio (CR) networks [7]. Typical CR networking scenarios involve a number of secondary (unlicensed) users sharing spectrum determined not in use at the time by the primary (licensed) users. The exact meaning of this sentence and many of its terms continues to be the subject of intense research and various proposals. This research is also backed up by the emergence of Software-Defined Radio (SDR) technologies and the fact that, with the advent of open-source device drivers for Wi-Fi cards, many additional configuration options are now available. Moreover, tweaking protocol operation to achieve performance optimization is now sometimes possible.

With the goal of efficient coexistence in a shared spectrum, a significant number of approaches promise to increase the overall wireless network efficiency, expressed in terms of limiting interference, optimizing resource utilization, ensuring fair spectrum sharing and, eventually, increasing Quality of

Service (QoS) or user quality of experience and the "social welfare" factor. However, the viability of such mechanisms is based to a large extent on the cooperation among autonomous network entities and their conformance to protocol-specified spectrum sharing rules. A critical question that naturally emerges is how such behavior can be checked and/or enforced.

The vast majority of the body of research in this area, implicitly or explicitly, assumes that all participating entities demonstrate full cooperation [8]. However, there exist approaches focusing on studying selfish behavior, often using tools from game theory. A common approach is to offer competing nodes the proper incentives for fair spectrum use and conformance to agreed-upon rules. At the same time, efforts have been made to limit the benefits of non-conformant behavior. The proposed mechanisms are based on reputation schemes [9], tit-for-tat models [10], punish/reward schemes or transfer models [11], where some kind of compensation is offered in return for using a spectrum portion. Still, an important assumption is the existence of a mechanism for effective detection of non-conformant operation and identification of misbehaving nodes (and even malicious intent).

We believe that in future spectrum sharing systems, it is necessary to put significant effort into the direction of modeling and quantifying the effects of uncooperative or anomalous behavior and preventing it, or making the system robust against it. As a first step, in this work we identify such misbehavior scenarios and relevant attacks to various phases of the spectrum sharing process. The remainder of this article is structured as follows. In Section 2 we consider the building blocks of the spectrum sharing process, namely negotiation among interested parties, dissemination of the derived spectrum sharing rules and their implementation, as well as sensing the environment for data collection or to monitor rule conformance. Before we delve into the identification of cases of misbehavior for each of the above processes, in Section 4, we briefly describe the profiles of potential attackers in Section 3. We conclude the article in Section 5 with a brief summary and outlook.

2. Spectrum Sharing Processes

Dynamic spectrum sharing can be considered (at least conceptually) a three-phase process. First, there is the negotiation phase, where nodes coordinate to come to a spectrum sharing plan. Then, the outcome of the negotiation process, *i.e.* spectrum access policies/rules, is disseminated to all interested parties. Finally, the aforementioned access rules need to be implemented by nodes themselves. It should be noted that there is a *monitoring* process that spans the above phases and provides the necessary information. *Sensing* the environment, either to receive information about spectrum usage and availability, or to monitor conformance to spectrum access rules, as well as receiving *feedback* on the quality of prior spectrum allocations from nodes, is tackled in this process. The interplay among these phases is shown in Figure 1.

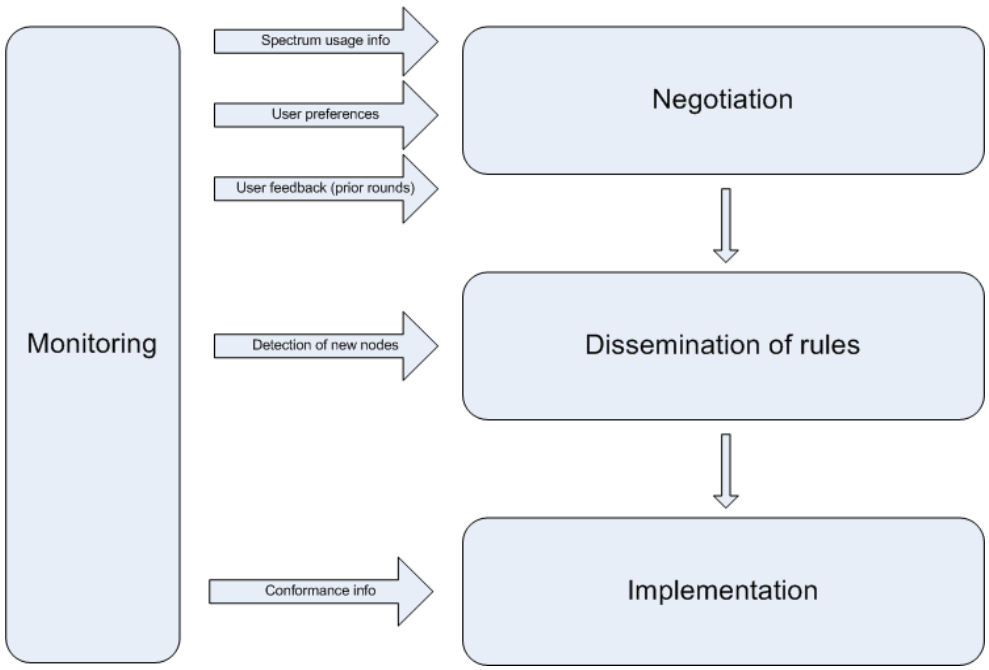
2.1. Sensing and Monitoring

Spectrum sensing refers to the ability of a CR entity to observe the characteristics of its radio environment. In other words, every CR entity has to be able to sense, measure, learn and be aware of a number of parameters related to radio channel characteristics, operating environment, spectrum and power availability, network infrastructure, existent radio entities, local policies and other operating

restrictions. In short, it is a multi-dimensional process used to identify occupancy in an *n*-dimensional space, particularly aiming at identifying "free spaces" in the CR domains.

As seen in Figure 1, spectrum monitoring plays a key role during the spectrum sharing process. Monitoring spectrum means discovering to what extent a frequency band or a channel of interest is occupied by other users. Such occupancy can typically be detected through power densities measured significantly above the noise level, which might interfere with other transmissions.

Figure 1. Spectrum sharing phases.



The methods of spectrum sensing [12] are typically based on the so-called transmitter detection technique (detecting the presence of a signal transmission), cooperative spectrum sensing (in case of noise uncertainty presence, fading and shadowing), interference-based detection (interference assessment) or using prediction. *Passive* monitoring [13,14] means that no signals that might interfere with the monitored transmissions are used by the monitoring station(s). It can thus be executed continuously. On the other hand, *active* monitoring [15] means to produce (possibly interfering) beacon signals and analyze their outcome. Thus, it is preferably used during "guard" times, when there is no data traffic that might be affected. Depending on what type of monitoring takes place, it may confirm the existence of other users [16], or even show their identities [17]. Monitoring can be initiated both by a user, as well as by a central entity in order to check for spectrum availability and entity compliance.

Ahead of the negotiation phase, the targeted spectrum needs to be sensed for availability. For instance, potential primary users must be discovered in order to be considered in the spectrum negotiation between secondary users. Furthermore, newly arriving nodes need also to be identified and integrated into the negotiations to share the same spectrum.

Once the use of spectrum has been (re-)agreed upon, the role of monitoring becomes evaluative, with compliance to the negotiated sharing rules as the key issue. Once the spectrum sharing plan is in

place, correct use of the spectrum needs to be monitored and communicated. A user wanting to take over a channel would typically check whether the channel has been vacated before starting to use it. Failure to access it would eventually be reported. Such failure can, for instance, be triggered by time synchronization issues: a potential guard time is exceeded once the vacating user's clock is lagging behind the waiting user's clock. Another possibility is that the vacating user keeps the channels deliberately, leading to a form of misuse. The control of channel availability is typically performed at regular intervals until the channel is free. The number of subsequent failures might indicate the degree of suspicion of misuse.

Monitoring has user-related and application-related interfaces. While the requirements of applications and specifications of the generated traffic might provide criteria for the actual division of the spectrum, users may directly express their preferences and in particular their degree of satisfaction with the outcomes of prior spectrum allocation rounds. It is important to note that, apart from user preferences, spectrum sharing mechanisms also consider user equipment capabilities, such as frequencies on which the radio transceivers can operate, transmission power limits or battery availability, among others.

2.2. Negotiation

Spectrum access is subject to negotiations among competing groups. Negotiations can be carried out in a fully distributed and localized manner (e.g., among neighbor groups [18]), at regular intervals, or when the need to reallocate spectrum emerges. This is the case, e.g., when a new wireless Access Point (AP) is set up in an area where existing entities have already come to an agreed upon spectrum allocation scheme. Different forms of negotiations are possible. Simple mechanisms rely on the broadcast of fixed policies, while interactive mechanisms require bi-directional communication, but enrich possible features.

Negotiation can take place in a centralized or decentralized fashion. Centralized mechanisms [19,20] require significant bandwidth around the point of decision to bring in the information. Challenges arise in dealing with incomplete or outdated information. In decentralized approaches [21,22], local and up-to-date information is usually available, but delays can defer global synchronization.

Another issue pertains to the control channel [23]. In order to be robust against malicious behavior, the control channel must be out-of-band. In order to ensure the availability of such a channel, it can be exclusively assigned to a channel owner, who is in charge of the resource. A single control channel must be shared by multiple parties and can therefore be subject to attacks.

Many frameworks for negotiation protocols have been proposed, also in other contexts (e.g., Web services). Such a protocol must also consider the trust relationships between the participants. Imported information from untrusted sources can enable an attacker to alter resource allocation.

The resource allocation must cope with the physical limitations of the stations. Allocating resources is an optimization process which takes into account, among other things, parameters such as the capacity demands of the senders, the transmission distance and noise based on local knowledge about sources of interference. The signal-to-noise ratio at the receiver should be included in the decision making for resource allocations.

2.3. Distribution of Rules

The output of the negotiation process, *i.e.*, the rules and policies that control spectrum access, needs to be distributed to all interested nodes. In this *update* phase, competing nodes are informed of their usage rights for each spectrum portion under negotiation, the duration of the particular spectrum allocation, and, importantly, the node configuration necessitated by these rules, putting constraints to node operation (e.g., maximum transmission power, operating frequency, timeslot size and timeslot allocation map, *etc.*).

There are also cases when new nodes emerge and are not aware of current spectrum allocation status in their vicinity. This phase thus also aims at informing newcomers of current access rules. Also, new nodes may lead to spectrum re-allocation or modification of current access rules, which existing nodes need to become aware of.

Potential attackers may be tempted to tamper with the rule distribution process [24], thus giving their victims a false view of current spectrum allocations in an attempt to increase their spectrum access opportunities or to deliberately reduce the performance of the underlying network and the QoS attained by other nodes.

2.4. Implementation

A spectrum sharing scheme can be implemented along the dimensions of *space* (e.g., use of directional antennas and MIMO—Multiple Input Multiple Output—technologies, power control), *frequency* (proper channel selection), *code* (with Code Division Multiple Access—CDMA), *time* (application of TDMA), *power*, and combinations of those. Next, we briefly discuss how such a scheme can be built using these dimensions.

Space: Coexistence in the same spectrum can be achieved by means of smart sharing in the space domain. This can be implemented by using directional antennas so as to minimize coverage overlaps, in particular with smart antenna technologies, such as MIMO, as well as by applying transmission power control schemes, where the transmission range is dynamically adjusted for the purpose of maximizing the number and quality of wireless links by minimizing interference. The power dimension is further discussed below.

Power: Depending on the employed coding technology for the available spectrum, different CR users can exploit the same frequencies simultaneously. CDMA makes it possible to maximize utilization in the available spectrum, though only if the proper power window is maintained, *i.e.*, it is mandatory to define, assign and enforce the channel power assignment. Too much power in a band interferes with other users and might push them out.

Time: If a specific channel (defined by frequency, coding and modulation) in a particular coverage area is to be shared amongst different users, time slot allocation is natural, yielding the Time Division Multiple Access (TDMA) scheme. Guard intervals should be employed between time slots to compensate for a possible lack of time synchronization with the subsequent risk of unintended collisions.

Channel: In a specific coverage area, several channels can be used at the same time. In this case, each user is assigned a specific channel, which can actually be composed of other (sub-)channels. Thus, we arrive at Frequency Division Multiple Access (FDMA). From a single user's point of view,

isolating the different channels from each other is of the utmost importance. This helps in maintaining the throughput which otherwise is reduced by interference. A typical example is the use of channels in the unlicensed 2.4 GHz band by Wi-Fi technology: There are 11 (in the US) available 22 MHz channels (13 in the EU and 14 in Japan), but there are only three non-interfering channels (e.g., 1, 6, 11 in the US). This limitation demonstrates the need for careful frequency assignment.

Furthermore, all the above-described methods can be combined to achieve a seamless functionality while being aware of all CR dimensions [25]. No matter which method is applied, the user needs to be sure that it can use the spectrum according to the negotiated sharing plan without (un-)intentional disturbance.

3. Attacker Profiles

There are various schemes for radio spectrum sharing and all assume explicitly or implicitly that wireless terminals and base stations (henceforth called "nodes") conform to the various rules (being dictated either by protocols, e.g., IEEE 802.22, or by regulators, such as the FCC in the USA, or by other third party entities, e.g., ISP consortia, *etc.*). Unfortunately, the above statement (that all nodes act legitimately, abiding by each network's rules and etiquette) is not always true.

While the system designer specifies protocols with the maximization of a system-wide metric in mind (e.g., high aggregate throughput, fairness and low delay), *rational* (or *selfish*) nodes seek to maximize their own utility, irrespective of the performance of their peers and the overall community welfare. Nodes, or groups of nodes, then may exhibit various kinds of non-conformant or anomalous behavior. It should be noted that non-compliance with the specified rules is not always a result of node rationality; equipment failures or pure malice, *i.e.* irrational misbehavior not guided towards increasing one's payoff, may account for that. Efstathiou [26] defines selfishness as a rational practice and malice as an irrational one, while Buttyán and Hubaux [27] make the distinction between rational and malicious misbehavior in wireless networks, but propose that they should be jointly tackled.

In this spirit, we distinguish between *conformant* and *non-conformant* entities and, in particular, consider only those that misbehave deliberately and not due to limited functionality or faulty equipment. A first attempt to identify and categorize non-conformant nodes in the Cognitive Radio Networking context is made by Arkoulis *et al.* [28]. Their classification is slightly modified and briefly summarized below:

- *Malicious nodes* are nodes violating the rules on purpose, without even necessarily attempting to obtain direct (short-term) benefit. Their goal is to cause disturbance either to the underlying network as a whole, or to selected (victim) nodes.
- *Rational nodes* are those whose aim is to increase their utility (gained by using the underlying network), mainly by using more spectrum resources (bands, or larger time frames, or codes *etc.*) than those assigned to them or agreed to by them (possibly implicitly). Rational nodes may attempt to determine unused resources and use them against explicit or implicit allocations, with no negative effect to others, *or cheat*, *i.e.*, attempt to maximize their payoff by degrading the performance of others (which are cheated out of their allocated resources).

Rational (strategic) entities are the most interesting category to consider because they are the ones responding to incentives, which need to be carefully designed to lead the system into good operating practices.

4. Security Threats

Following the discussion on spectrum sharing phases, we present a list of relevant attacks. For each phase, we provide a comprehensive description of the attacks that we have identified and potential countermeasures. It should be noted that some attacks may appear in more than one phase, albeit expressed differently.

4.1. Sensing and Monitoring

The traditional main goal of spectrum sensing in CR networks is for secondary users to detect the presence of primary user signals to avoid transmitting and interfering with them. However, more generally, sensing is needed to detect and possibly identify other users and the transmission technologies and protocols they use (for the sensing node, or group, to develop a communication strategy). Intense research is being carried out focusing on optimizing the spectrum sensing process both to reduce its performance overhead and to increase its accuracy (and even standardization activities of some aspects are ongoing). Also, a sensing process would be necessary to monitor conformance to agreed-upon access protocols and policies.

Misbehavior in the sensing process may emerge with users executing some of the following attacks:

- *Primary user masking*: A (malicious) node may transmit signals able to mask the primary user's ones towards misleading the spectrum sensing procedure. Thus, a legitimate node would not be able to detect the primary user's transmissions and falsely assume it found a spectrum hole [24].
- *Primary user emulation (PUE) attacks*: A node may transmit elaborately created signals which seem exactly the same as a primary user's ones. A sensing node may be unable to distinguish the real from the fake signals and falsely mark a spectrum portion as occupied by a primary user and defer its transmission, thus leaving more spectrum for the attacker. Mechanisms to counter PUE attacks are presented in [17,29,30].
- *Non-standards-compliant sensing techniques*: Standards as to how sensing should be implemented or requirements so that the desired sensing performance is achieved may be in place. Here we refer to cases when, either due to malice or selfishness, or even due to software or hardware failures, nodes do not follow the stipulated sensing behavior and we elaborate with some examples. First, nodes may use sensing intervals that are too long in order to allow for a timely reaction, e.g., to the appearance of a licensed user. Second, a node may not release a channel for sensing purposes in due time (given that sensing is to be performed at specified intervals, time during which secondary users need to remain "silent"). Other examples of misbehavior would be deliberately introducing de-synchronization between nodes, in order to blur the boundary between deliberate and accidental misuse or sensing with insufficient

sensitivity. Finally, there is the case for tampering with spectrum sensor software and hardware to affect their normal and stable operation [31].

It should be noted that, if we consider that nodes may be heterogeneous as to their sensing capabilities, an attacker with knowledge of their characteristics could target the "weaker" ones, as explained by Brown and Sethi [24]. To elaborate, there are nodes which, by design, have a single front-end used both as their transceiver and their spectrum sensor. In this case, the effective time for transmissions is limited by sensing intervals. In contrast with nodes that have separate interfaces for sensing and exchanging data, such a node would suffer more if an attacker jammed his transmissions.

The above discussion focuses on the sensing process. However, in the case of distributed spectrum sensing, equally important is the data fusion step, where information on spectrum usage conditions (e.g., primary user presence) from various sources (e.g., user devices, dedicated spectrum sensors, *etc.*) are collectively evaluated. Misbehaving nodes with the proper incentives or malfunctioning ones may submit invalid measurements and mislead the entity responsible for data fusion. Methods to increase the robustness of the distributed sensing process against data falsification attacks are studied in [30,32].

4.2. Negotiation

4.2.1. Negotiation Obstruction

The vast majority of the approaches found in the literature use a common control channel on which to base their negotiation procedure ([33–35]). Either centralized [36], or distributed [33,35,37], such spectrum sharing schemes require communication between network entities to operate successfully. In case this sharing is done in a centralized manner, nodes (competitors) use this channel to send their spectrum requests to the central node assigned with this task. Similarly, when allocations are determined in a distributed way, nodes use the common channel to exchange requests and other operational details. Obviously, this common channel must be accessible by all nodes of a Dynamic Spectrum Access (DSA) network and it is best if it is interference-free and characterized by high availability. If any of these requirements are not satisfied, a DSA network's normal operation could be jeopardized or be under significant threat.

To begin with, an attacker may attempt to occupy or even destroy this common control channel, which is the backbone of a spectrum sharing mechanism, with the goal of disrupting a DSA network's normal and optimal operation [38]. Among his alternatives would be to *jam* [39] the channel by simply transmitting a strong signal over that channel. As a consequence, no spectrum requests (or other operational details) could successfully reach their destination and the respective sharing mechanism would remain without input. Although switching to a new common control channel to continue the negotiation process could give a temporal solution to the problem, this approach cannot be characterized as the most efficient. In such a case, all the negotiating parties should get in touch with each other to agree upon a new channel to move to; as this is also a type of negotiation and, in any case, it requires a control channel to be achieved, we get into a loop, or we need to have predetermined a set of "new" channels to move to when the current one is rendered unavailable. Unfortunately, a number of issues arise here that make the implementation of such a technique extremely difficult. Namely, efficiently detecting jamming attacks with minimum ambiguity is not trivial, while both

resynchronization and common channel reassignment is costly, especially if such attacks are too frequent for this cost to be amortized over time. Exactly the same problem could occur and identical statements would hold if, instead of jamming, a malicious node chose to realize a *flooding attack* against the common control channel [40]. According to that attack, (dummy) packets are continuously transmitted over a channel with the goal of heavily congesting it and, as a result, significantly increasing packet transmission delays and packet loss rates (to the point of making the control channel useless).

However, there are also sharing mechanisms that avoid basing their operation solely on a common control channel. The negotiating parties here have to exchange both requests and other information regarding their operation over the channel currently assigned to them [41]. In such cases, it is more difficult for an attacker to obstruct the negotiation process, but it is still possible. For instance, by carefully monitoring the flowing traffic and predicting when the next desirable "control" packet will be transmitted, an adversary could obstruct the negotiation process by simply colliding with the latter.

Note that more discriminating and sophisticated attacks may be more difficult to undertake, and may even have lower success rate, or take longer to achieve results, but they are much harder to detect or prove as non-conformant and therefore may go undetected for long periods of time, or more generally be effective longer. Instead, continuous jamming and similar non-refined techniques cannot be overcome with communication techniques, but are more obvious and the jammer can more easily be identified and stopped by external intervention.

Concluding, negotiation obstruction may introduce significant problems in the normal operation of a DSA network. Firstly, it could affect competition between its nodes since a malicious one may choose to realize this attack exactly after his spectrum requests are received by the sharing mechanism. His competitors' requests may never reach their destination, leaving the decision mechanism with incomplete input. Unavoidably, the resulting decision may be much different now than the "fair" one, offering extra profits to the attacker. Moving one step forward, resource starvation, spectrum under-utilization, as well as sub-optimal network operation would sooner or later emerge as side effects of such misbehavior.

4.2.2. Fake Spectrum Requests Injection

All entities taking part in the negotiation process have to send their requests, as well as other details concerning their operation, to the spectrum sharing mechanism of a DSA network [42]. Obviously, each single node may send one or no such requests, depending on its current needs. One problem that arises here is that an attacker could inject fake requests (and information) [28] into the DSA network aiming at either confusing the sharing mechanism, or misleading it to assign the available opportunities to the wrong nodes. In the latter case, the fake requests might seem to be sent from an existing and valid entity of the network (a victim in this case), while in the former case this is not a requirement. In any case, since the input of the sharing mechanisms would not be representative of the nodes' needs, the output would be—with high probability—suboptimal, unfair and possibly highly disturbing. Efficient authentication techniques, as well as detailed lists of all valid participants in the negotiation processes, could prove beneficial and act as a countermeasure to such an attack.

4.2.3. Spectrum Requests Falsification

One more problem, which arises when exchanging requests and other operational details between nodes and the spectrum sharing mechanism, is that an attacker may try to falsify the requests sent by its competitors [28]. Such an attack belongs to the class of *man-in-the-middle* ones, where an attacking node captures the packets in question (carrying negotiation-related information) and injects them back after manipulating their contents in a way advantageous to itself. The most appropriate way to cope with this attack would be to apply techniques able to assure the integrity of the exchanged messages.

4.2.4. Client Feedback Falsification

Almost any approach being proposed in the literature exploits information pertaining to operational parameters of the nodes, as well as information about the environment they operate in. Such details are taken into account during the decision making phase of the (optimal) spectrum sharing procedure and are carefully combined with the received spectrum requests. All nodes should feed the sharing mechanism with their real data and measurements. Unfortunately, this might not always be the case. An attacker may either deny submitting the required information to the sharing mechanism, or may send information not representing the reality [28,29]. Such behavior is based on the fact that both collecting the required details, as well as sending them back to the respective collector, is not only time, but also resource, consuming (e.g., energy to be consumed may be critical for small mobile devices).

In addition, an attacker may also attempt to modify the packets carrying the required information being sent by his legitimate competitors, or inject fake ones in the network. In a more extreme scenario, an attacker may even try to influence the environment his competitors operate in (temporarily, but at critical points in time), in order to mislead them towards reporting unrepresentative details regarding their operating conditions.

If any of the aforementioned attacks is carried out successfully, the sharing mechanisms operating in a DSA network might be rendered unable to get a real view, which will unavoidably lead to suboptimal and inappropriate transmission opportunities allocation. Additionally, in the case of the last attack described (temporarily influencing the environment), any instantaneous cross-checking mechanism would also fail to detect a different ("correct") view, extending the validity of the attack. To make matters worse, two or more misbehaving nodes could collude to make their attacks more credible and, consequently, even more difficult to detect. These observations are sufficient to reveal the need for applying novel techniques in DSA networks for efficiently cross-checking received information, filtering out incorrect and misleading information and blacklisting offending (or possibly, even suspicious) nodes.

4.2.5. Spectrum Needs Over-reporting

Each node participating in a DSA network should compute its spectrum needs by itself (in terms of channel, time, bandwidth, *etc.*), taking into account both its node characteristics and traffic demand (*i.e.*, traffic type, maximum acceptable delay, jitter, *etc.*). However, a selfish node could choose not to conform to this rule and request more resources than it really needs [11]. Motivated either by greed or

fear of problems in case of sudden QoS degradation, a node may choose to lie (over-claim), particularly if no cost is associated with resource requests (/reservations). Techniques to provide the right incentives for nodes to always report their true needs are required.

4.2.6. False Claims of Continuous Changing Demands or Environmental Conditions

Spectrum sharing mechanisms are responsible for maintaining appropriate resource allocations, independently of the state of the network. Each time the state of a network is significantly changed, the mechanisms have to carefully reassign the available resources. This should take place whenever either the underlying topology changes (e.g., new nodes are attached, move considerably, or are disconnected), or the operational and environmental parameters are altered (e.g., propagation conditions, interference from foreign networks or devices—not controlled by this mechanism—*etc.*). Although various approaches for resource reallocation triggering exist, including at regular time intervals (which are probably the more robust), the specific proposals are out of scope for this paper.

Dynamic reallocation triggering raises an important problem in the spectrum sharing procedure. A non-conformant node may falsely claim that either its environment or its resource demands are constantly changing, in order to cause frequent spectrum reallocations. Given the cost in terms of signaling traffic, computation load on the network node(s) computing the allocations, handover delays for nodes possibly reassigned, *etc.*, this could be a significant attack, with denial of service characteristics (considering the computation load on the re-allocator), but also introducing major disturbances to all nodes since their transmissions could be constantly interrupted and their transmission schedules changing.

4.2.7. Auction Cheating

A significant number of methods in the literature borrow ideas from auction theory to provide optimal spectrum allocation results. The intrinsic fairness, as well as the efficiency, characterizing such techniques makes them ideal for use in the CR paradigm. Multi-unit Sealed-Bid [43], Vickrey [44], Second Price [45] and Double Auctions [46] are some representative examples. Not surprisingly, since many such approaches depend on the truthfulness of the requests and information they receive from the negotiating entities, they are also vulnerable to the aforementioned attacks. However, some additional problems could arise, in particular in relation to auction implementation in automated, fast and underpowered environments, a brief description of which is provided below:

- *Bid Shielding* [47]: An attacking node may announce an extremely high bid to a sharing mechanism with the view to discourage its competitors from making any more offers. Since each node maintains its own affordable upper bid limit, in such a case it would be obliged to retire early from the whole process. To make things worse, if a node has the right to retract its last bid, allowing the second biggest one to be accepted, a number of colluding nodes may exploit such a vulnerability to successfully mislead the underlying mechanism and gain access to the auctioned spectrum at a really low price.
- *Shilling*: One or more attacking nodes may announce sequential bids to a sharing mechanism with aiming to increase the winning price of a special spectrum portion. In fact, these nodes

may even have no intention to win the auction, but their sole objective would be to press nodes in real need of the available spectrum to offer more and more money.

- *Sniping*: An attacking node may choose to announce a high (or higher than the current) bid, just before an auction closes. As a consequence, none of its opponents would have the time to respond with a higher one, losing automatically the chance to gain access to the spectrum. Since nodes could stop offering higher bids even before reaching the highest price they can afford (for example when they know that there has been no higher bid offered by their competitors until then), a legitimate node could fail to win the auction, even if it had not reached its price limit.
- *Bidding ring and loser collusion* [48]: These types of attacks are closely related to those already described in Section 4.2.5.
- *Sub-leasing* [48]: One or more cheating nodes may do their best to win an auction at the lowest possible price and, in turn, sublease the spectrum to others (and losers of the original auction may be included). The primary objective of such an attacker would be to earn extra profit at zero cost by gaining benefits which should be credited to the original spectrum auctioneer.

All these attacks are problems related to auction design and implementation, studied in the field of auctions and addressed in various ways. What may be different here is that some of these may be neglected to be addressed for various reasons, e.g. from simple oversight, to considerations of the value of the resource to be auctioned *vs.* the cost of addressing some of these problems (and enforcement of the rules).

Finally, there are approaches found in the literature that correlate a spectrum opportunity's value with the number of nodes competing for its usage [49]. Unfortunately, such an assumption can allow an important vulnerability to arise. A set of colluding attackers may simultaneously start competing for occupancy of a specific transmission opportunity whose quality is not the highest in the underlying network. Fraudulently increasing an opportunity's "reputation" will unavoidably mislead all other network nodes, making them falsely believe that there is a more valuable candidate. Given that the number of "good" opportunities will rise (even if a part of them are fake) and, consequently, the competition for each one of them will decrease, it will be easier for an attacker to gain access to a genuinely valuable one.

4.2.8. Fake Complaints Regarding the Received QoS

Spectrum sharing mechanisms operating in DSA networks usually allow nodes to send back either positive or negative feedback messages [50]. Such messages enable evaluating the success and quality of prior resource allocations. Obviously, all users must be honest regarding their achieved satisfaction levels to assist the respective mechanism gain a full and real view of the managed network. Unfortunately, this may not always be the case. A node may on purpose report lower satisfaction levels, or falsely claim that it suffers from significant QoS degradation [28]. Consequently, the misled sharing mechanism might choose to allocate more resources to the complaining nodes aiming at compensating them for their (fake) losses. Lying nodes would gain extra profits in terms of spectrum resources at zero cost, while the overall spectrum allocation would suffer from unfairness. The

currently described attack can be effectively eliminated by applying novel cross-checking and validating mechanisms on such feedback-based evaluation methods.

4.2.9. Identity Theft and the Use of Multiple Identities

During the negotiation phase, each participant must carry a unique, "permanent" identity [51]. This should unambiguously identify not only the nodes, but also the mechanisms assigned with the task of sharing the available spectrum in a DSA network. These identities should under no circumstances be modified. If the latter requirement is not satisfied, an attacking node can realize attacks such as identity theft or using multiple identities against either its legitimate competitors, or the sharing mechanism itself, posing a significant threat to the underlying network [29,52].

Identity theft is one of the most dangerous attacks. The main reason is that spoofing the identity of an unsuspecting victim could result in numerous unpredictable consequences. To begin with, an adversarial node may realize such an attack to successfully hide its non-conformant behavior. In this capacity, it can not only avoid being caught or punished because of acting in a non-conformant way, but also to accuse someone else for its own improper actions. Obviously, accusing innocent nodes for rule infringements they have never undertaken will cause strong user dissatisfaction, as well as high instability in the underlying DSA network. Additionally, an adversary having successfully spoofed the identity of another node could send spectrum requests to the sharing mechanism on behalf of its unaware victim. Such an attack could leave the respective spectrum portions unused, or oblige a victim node to pay the price for resources it never requested and, thus, never used. Unsurprisingly, such victim nodes could quickly stop trusting not only this DSA network, but also the CR paradigm as a whole.

Moreover, identity theft may enable an attacker to successfully mislead a spectrum sharing mechanism by simply sending fake feedback. The reader should recall that special reports carrying operational details or information regarding the environment each node operates in are required by some allocation mechanisms proposed in the literature. A misbehaving node could thus start such an attack to manipulate the view a sharing mechanism maintains of the managed network, either for gaining personal profits (selfish behavior) or for affecting the optimality or the resource allocation results (potentially malicious behavior).

An equally important threat can arise if an adversary is able to spoof more than one identity simultaneously. Such an action can enable him to achieve most of the malicious goals described above in a more efficient manner. In other words, an attacking node using multiple identities can provide more credible reports to the sharing mechanisms and, consequently, manipulate more successfully the view of the managing network of the latter. Also, he can better hide his actions and/or accuse innocent parties of them.

In a worst case scenario, a malicious node can even continuously change the identities it spoofs. In such a way, it can equally divide its maliciousness to all its competitors, causing the least possible disturbance to each one of them and, as a consequence, avoid triggering any punishment mechanism. Even in the case a victim node is suspected of being non-conformant and punishment measures are enforced against it, the real attacker can easily avoid being punished by simply changing again its identity. Any active monitoring and/or punishment mechanism would then fail to effectively counter

such an attack, posing a significant threat to both the stability as well as the efficiency of the operation of the underlying network.

4.3. Distribution of Sharing Rules

4.3.1. Rules Never Received Claim

As mentioned above, every spectrum sharing protocol utilizes its own preferred techniques for keeping its clients up-to-date with the current spectrum allocation rules. The DSA network, in turn, must provide its nodes with uninterrupted access to such rules towards assuring both their normal and stable operation. However, an adversarial node may deny that he ever received either the whole, or a special part of the aforementioned rules, aiming at hiding his maliciousness behind this "unawareness" claim [28]. For instance, in case a previous allocation is more favorable than the current one, a node may choose not to update its configuration, and thus not to adapt its operation to the new conditions, so as to continue gaining the same profits as before. If such behavior is detected by an existing security mechanism of the DSA network, the only way for the adversary to escape any potentially induced punishment would be to pretend to be the victim of a "fictitious" attack which prevented him from accessing the respective rules.

Obviously, each DSA network must be equipped with techniques ensuring that all nodes can gain access to the latest fresh rules and, additionally, that none of them can repudiate their reception [53]. Otherwise, an adversary could easily invert his position and pretend to be the victim, even if he is the offender.

4.3.2. Altered/Distorted Rules Received Claim

According to this attack, an adversarial node caught violating the rules in a DSA network may attempt to escape punishment using a slightly different claim. He may falsely claim that the rules or assignments he received were purposefully modified, or distorted. In other words, such a malicious node may claim that he always abides by the rules of the DSA network, but this time someone else infused specially modified rules to victimize him and lead him to act improperly. Obviously, each network should be able to protect against such situations by ensuring that no maliciously infused rules may be considered as valid by its nodes and, additionally, that no node can repudiate the receipt of the original ones [53]. Otherwise, an adversary could easily invert his position and pretend to be the victim, even if he is the offender.

4.3.3. Unreachable Rules

A common and important security vulnerability, posing a significant threat to a DSA network's operation, is that of preventing nodes from accessing the rules enforced on them [24]. As already mentioned, there are two discrete types of rules in such networks, those derived by a negotiation process and those predefined by either an administrative authority (e.g., the FCC), or the network administrator itself (which usually remain unchanged for long periods of time). Independent of the category, the managing network must assure that all its clients can access the rules in an uninterrupted manner. Since this access is usually supported by either a common control channel, or the data

channels themselves, a number of related security issues can arise and, thus, affect the overall network's stability. Following is a brief description of the most important such vulnerabilities. A careful reader will notice that some of them are closely related to threats already mentioned in previous sections, particularly in Section 4.2.1.

To begin with, an attacker may attempt to occupy the common control channel [38], if such exists, or else the backbone of the sharing mechanism of the DSA network. An attacker's alternatives include either jamming [38] or flooding [40] the control channel [63]. In the former case, the attacker has to simply transmit a high-power signal over the required channel to obstruct packet transmissions over it. Consequently, the number of packet collisions will significantly increase and large delays will unavoidably be instigated. In the latter case, an attacker has to inject fake traffic in the control channel with a view to increase the competition for its usage and make it operate under significant congestion. In both cases, packets containing the desired sharing rules can never reach their destination, causing strong disturbance and chaotic conditions. Network nodes are always able to switch to a new control channel to avoid any possible abnormal operating conditions. However, such an alternative does not come at zero cost. All communicating parties have to either communicate with each other to agree on which new channel to move to, or be informed in advance regarding which new channel they should move to each time a problem arises. The high handover costs, additionally, are not easy to be amortized over time.

On the other hand, when the rules distribution is carried out over the existing data channels of a DSA network, an attacker can follow a slightly different approach. An adversary may first determine the time periods during which the required control information is transmitted and the respective channel number and then cause significant targeted interference. The unavoidable increase in packet collisions will prevent any new or existing rule from reaching its destination, letting the underlying DSA network operate far from optimally. While such an attack is harder to execute and requires more resources to be spent from the attacker's side, it should not be ignored.

A very interesting categorization regarding the enforceable rules in a DSA network is presented in [24]. According to this, there are the positive, as well as the negative ones, a brief description of which is provided below.

- *Positive* rules: This category contains rules defining the conditions under which a node is allowed to use the available resources.
- *Negative* rules: These rules define the requirements to be satisfied to prevent a node from using the aforementioned resources.

Surprisingly, this categorization is enough to differentiate the way a DSA network is influenced by such an attack. In the first case, a lost positive rule may result in spectrum under-utilization and users' resource starvation, since no (new) rules to dictate when nodes are allowed to gain access to the spectrum exist. As a consequence, no node will be able to transmit any packet for satisfying its operational needs, leaving the spectrum unexploited. On the other hand, in case some (or even all) negative rules become inaccessible, the interference levels in the network can significantly increase, resulting in sub-optimal operation and strongly annoyed end-users. Since no rule (or fewer rules) preventing nodes from accessing the spectrum are present, more nodes than expected will simultaneously exploit the available resources.

4.3.4. Fake Rules Injection

One other vulnerability, which can be considered complementary to the previous one, threatens the normal operation of DSA networks. According to this one, an attacker may attempt to inject fake rules in such networks, motivated by various facts. To begin with, such an attack seems ideal for someone who aims at causing chaos in a target network, driven by pure malice. If new rules are infused, which are neither defined nor previously approved by the manager or the entities themselves through negotiation (in case of distributed spectrum sharing schemes), network operation will be affected. Additionally, such an attack seems also ideal for rational adversaries who aim at increasing their personal profit through improper use of a network's available resources. In other words, a node may create and inject fake rules to prevent, either carefully or randomly selected, legitimate nodes from exploiting special transmission opportunities. Since these opportunities will remain unused, a selfish node may attempt to occupy them at zero cost and without running the risk of disturbing any of his competitors (and thus to be detected) [28]. Obviously, to what extent the introduced sub-optimality and unfairness can affect the nodes composing a DSA network is absolutely dependent on each attacker's greed.

The outcome of this attack is also highly dependent on the type of the injected fake rules. To elaborate, in case some fake positive rules are infused in a DSA network, the interference levels suffered by its nodes will be unavoidably increased, since more nodes than expected will be allowed to have simultaneous access to the available spectrum resources. On the other hand, in case a number of fake negative rules are infused in the network, spectrum access will become more restrictive than before, less transmission opportunities will be efficiently exploited, and consequently, the spectrum utilization as well as node satisfaction levels will be significantly decreased.

To prevent potential attackers from exploiting such vulnerability, each single rule should be signed with its creator's unique signature [54]. Rules not signed by a trusted authority should be immediately filtered out, while their respective sender can be black-listed. This simple solution cannot be considered efficient since the rules enforced in a DSA network may constantly change. Most of the methods proposed in the literature for providing secure communication between nodes are not only resource-intensive in terms of computation power and memory needs, but also introduce significant delays in the overall communication procedure.

4.3.5. Rules Altering

One last attack, closely related to the previous one, is that of unauthorized rules modification. More specifically, an attacker may successfully modify packets containing information regarding the rules enforced in a DSA network to mislead some, or even all, competitors. One point to emphasize here is that such vulnerability can be eliminated by applying special techniques in the network to assure the integrity of packets encapsulating rules-related information.

To summarize, any attacker attempting to modify the valid set of rules of a DSA network may cause quite similar problems to the latter, irrespective of the nature of the realized attack. To make this statement clearer, it is enough to point out all possible motivations the attacker may have for misbehaving, instead of abiding by the enforced rules. To begin with, the most common such incentive

for the adversary is to increase his utility without having to pay the respective price. If such a target is accomplished, phenomena like unfair resource usage, competitors' satisfaction level degradation, annoyance and complaints from the victims' side, spectrum under-utilization, as well as negative effects on network efficiency, stability, flexibility and adaptation to changes, are highly probable to arise. Either when new fake rules are appended to the set of the existing ones, or some of the existing ones are deleted or modified, or even when a part of them (or even all) are not accessible by network nodes, it will become impossible to fully apply the required spectrum sharing model.

4.4. Implementation

4.4.1. Timeslots Usage Violation

A large number of approaches found in the literature adopt methods for sharing the available spectrum in the time domain [55,56]. The procedure followed is more or less the same for most of them, with the very first task to be carried out being that of time division into periods of fixed, or of dynamic length. Afterwards, a cognitive mechanism is assigned the task of optimally allocating these slots to the competing nodes in order not only to satisfy their needs, but also to increase the overall spectrum utilization and maximize social welfare. Each and every node of a DSA network must abide by these allocations and more generally its rules. Unfortunately, nodes may misbehave, causing a number of irregular conditions to arise.

To make things clearer, a non-conformant node may carry out transmissions during timeslots not allocated to him (or which he is not allowed to use) [57]. Such timeslots may be already assigned to one of his competitors, or be unavailable due to Primary User appearance. Illegally transmitted packets may collide with legal ones, resulting in (unexpectedly) increased packet loss rate (for the latter). QoS degradation would unavoidably be suffered by legitimate nodes, while the profits gained by attackers would increase steeply (since such nodes will gain access to the spectrum during periods they should otherwise refrain from using). Social fairness as well as welfare would also be affected.

Moreover, a misbehaving node may carry out such an attack in order to lower the value—and consequently the price—of particular timeslots and, especially, those considered highly profitable by his competitors [49]. Attacks against such high-quality transmission opportunities can render them automatically less attractive and, thus, effectively mislead more and more nodes to falsely turn their interest to alternative (more expensive or of lower quality) opportunities. Since the really valuable ones will remain unexploited, or characterized by lower competition, the attacker will be able to gain the right of accessing them much easier and at a much lower price than before, thus increasing his profit.

The reason why this attack can cause such negative results in a DSA network is twofold. Firstly, there is no technique for alleviating—at least to some extent—the aftermath of such a misbehavior, given that in such strictly scheduled environments there is no need for applying collision avoidance mechanisms (under normal conditions). Then, there are no mechanisms proposed to date for detecting and identifying these simultaneous transmissions carried out by misbehaving nodes (and at least in their simplest form, they are undetectable).

4.4.2 Transmission Power Thresholds Violation

A large number of approaches found in the literature carry out the required spectrum sharing process in the dimension of space [58]. To be more specific, in case a network has fewer channels available than the number of nodes requesting their usage, a common approach is to adjust the transmission power of the latter in a clever way so as to increase the reuse factor and the network's capacity and eliminate the interference caused due to simultaneous packet transmissions over the same channel in the same area. The first step in this direction is to divide the nodes of a network into carefully selected sets. Although each such set must be assigned with a different channel, this requirement is not always sufficient to mitigate the interference problems which can arise. So, a complementary technique often used is that of adjusting the transmission power of each network node so that no two simultaneous transmissions by neighboring nodes can interfere with each other.

The obvious strategy for nodes, without considering possible reprisals and long term results, is to transmit at the highest energy level supported by their hardware (if energy and life-time considerations for battery powered devices are not taken into account). In this way, each node will attempt to overcome any potential noise-related packet loss, as well as achieve the highest possible QoS level. But, if all (or many, or other strategically placed) nodes decide to behave in a similar way, the consequences for the underlying network will be destructive. In the ideal case, each node should continue lowering its transmission power until the lower bound of his satisfaction level is reached, and sometimes even lower, in order to achieve fairness and maximize the social welfare. However, since most of the time there is no direct incentive for a node to behave in such a possibly unfavorable way to its short-term interests, approaches relying on such expected, suggested, or dictated power adjustment techniques may fail to fulfill their aims.

Network nodes may have strong incentives to violate the transmission power-related rules, letting numerous irregular conditions to arise. A node decreasing his transmission power may probably suffer from increased packet loss rates and insufficient QoS, compared to when he transmits at full power. A greedy or conservative node may thus choose not to abide by such power-related rules for gaining extra profits, or avoid operating in unfavorable conditions, respectively. Such adversarial behavior will unavoidably result in increased interference levels inside a DSA network, while significant QoS degradation will also be suffered by other conformant nodes. In a similar way, a malicious node may purposefully push its transmission power to its limits causing strong disturbance in such a network, decreasing his competitors' profits or even affecting Primary Users' transmissions. Such an attack may also be realized to decrease the "reputation" of special channels available, and especially those which are considered highly profitable by his competitors [49].

4.4.3 Channel Usage Violation

There are numerous approaches proposed to date for sharing the available spectrum in a DSA network in the frequency domain [59]. They usually model spectrum sharing as a single (or joint, in case of complex cross-layer approach) problem of optimal assignment of channels to nodes. This channel allocation should be done in a way that no nodes with overlapping coverage are assigned to the same channel, or in case such a requirement cannot be totally satisfied, this allocation should

minimize as much as possible the interference caused by simultaneous packet transmissions. Among the main aims of these approaches are to preserve the optimal—in terms of efficiency and spectrum utilization—operation of the managed DSA network, as well as to satisfy each node's needs. Obviously, all nodes in a DSA network must obey the rules related to such allocations for enabling them to achieve their goals. But, as stated before, this may not be always the case and a malicious node may choose to violate these rules.

An adversary may attempt to transmit packets over a channel, even if he has no right to do so [57]. Such a channel may never have been assigned to him or could have been assigned to him at a previous time and since retracted. Additionally, this may already be occupied by one of his competitors, or even by a Primary User. Such unanticipated packet transmissions may result in significant interference problems, degrading each "attacked" channel's quality. This attack can also be instigated with the aim of lowering the reputation, as well as the price, of special, high-quality "expensive" channels [49].

4.4.4. Control and Management Time Period Violations

Despite their differences, the majority of spectrum sharing approaches, either centralized or distributed, have a common important requirement. They impose specific time periods during which no node is allowed to exploit the spectrum for transmitting data packets.

To begin with, no node should ever access a special spectrum portion while a negotiation procedure is being carried out over it. Similarly, often no packet transmission is allowed while an activity like sensing or monitoring is in progress. To clarify the latter statement, we should point out that many modern protocols, including IEEE 802.22 [56], define special time periods during which a subset, or even all, wireless nodes have to sense the available spectrum and report their findings back to either a central entity (when a centralized mechanism is used for spectrum assignment), or the other neighbor nodes (in case of distributed mechanisms). Obviously, any "illegal" transmission during such a procedure will not allow it to capture the real view of the underlying network, in terms of channel occupancy, interference, and noise conditions, and consequently it will affect the overall spectrum sharing procedure [60].

Another misbehavior scenario which could arise here is that of a malicious node transmitting during the so called guard-bands [61]. Perfect synchronization as well as the implementation of global clocks cannot be easily achieved. All methods proposed in the time division domain allow for the existence of a (small) synchronization error. A way to deal with such synchronization errors is the definition of special idle periods between consecutive slot allocations (preventing packets sent by the previous and current slot owners to overlap and destroy each other). For instance, each time a sharing mechanism re-allocates the available channels to nodes, it introduces idle periods between these two successive allocation instances for allowing all in-flight packets to reach their destination, as well as providing enough time to the loosely synchronized network nodes to adapt their operation to any possible rule changes. What is obvious here is that each node of such networks should abide by the rules and avoid transmitting anything during these periods. Again, an adversary may ignore the defined guard-bands and attempt transmissions over them aiming at maximizing his own profit and/or degrading both the spectrum utilization level characterizing the DSA network and the QoS received by other legitimate nodes.

4.4.5. Common Control Channel Jamming

Many approaches base the proposed overall spectrum sharing procedure on (one or more) common control channel usage. The consequences of jamming or flooding such channels are already described in previous sections, focusing either on the negotiation, or the rules distribution phase of such approaches. However, the list of possible problems includes further attacks, which may also affect the phase of node conformance to the DSA network rules.

There are protocols proposed to date that base the implementation of DSA-oriented collision avoidance mechanisms on common control channels. For instance, there are methods based on the exchange of modified RTS/CTS messages for CSMA/CA networks, whose headers enclose extra spectrum information [23]. Other approaches require the use of as many common sub-channels as the available channels of a DSA network. Whenever a node occupies a data channel, he must inform any potential user about this channel's state by transmitting a special signal (or else, a busy tone) over the respective common sub-channel [37].

In case a control channel is jammed, the network could be disrupted and some nodes could become isolated [38]. The resulting unawareness regarding the condition and the state of the available channels in a DSA network would lead them lacking in resources while the spectrum would remain underutilized. Moreover, a malicious node may transmit fake busy tone signals over selected sub-channels in order to mislead its competitors and prevent them from accessing particular spectrum portions. To make matters worse, an attacker could transmit the aforementioned signals over all the available sub-channels aiming at preventing all his competitors from transmitting any data packets and affecting their received QoS. A more rational attacker may try to also benefit from such behavior by occupying the vacant spectrum portions and, consequently, increasing his gained profits. Finally, a more far-fetched and difficult to realize technique would be for an adversary to transmit "inverse" signals over these sub-channels fading the currently transmitted one. The respective channels would falsely seem vacant, possibly letting more than one user occupy them, which can, in turn, increase interference.

4.4.6. Identity Theft/Multiple Identities

Unique, unambiguous and tamper-proof identities are required for securing not only the negotiation phase of a spectrum sharing protocol, but also that of rule conformance [51]. Otherwise, an identity theft and/or spoofing attack may pose a significant threat to the operation of most modern DSA networks.

A misbehaving node has strong motivation to steal or then mimic an unsuspecting competitor's identity. To begin with, this attack can enable an adversary to hide his malicious behavior behind someone else. As a result, not only the former will avoid being detected and punished, but also the latter will be accused for rule violations he never committed. Additionally, the attacker may perform identity spoofing to increase his own benefit without cost and degrade the performance of his competitors. As outlined above, spectrum can be shared in more than one dimension. After that, the resulting spectrum slices are assigned to network nodes in an optimal manner. If a selfish node achieves to successfully spoof someone else's identity, he will automatically be enabled to exploit his

victim's spectrum opportunities. Sooner or later, the nodes composing such a DSA will stop trusting the sharing mechanism and start searching for new alternatives.

Additionally, an attacker may attempt to simultaneously spoof more than one identity at a time for exactly the same reasons as above. In this case, however, not only would the possible adversary's benefits be increased, since access opportunities of more victims would be illegally exploited cumulatively, but also their malicious behavior would be masked in a more efficient manner. The impact of such a combined spoofing attack would be greater than before, causing bigger problems inside an underlying DSA network.

Even worse, an attacker can continuously change the spoofed identity equally dividing the caused disturbance to his competitors, making it harder to be detected.

4.4.7. NEPA, CEPA and LORA Parasite Attacks

Recently, three new misbehavior scenarios have appeared in the literature, namely the NEPA (Network Endo-Parasite Attack), CEPA (Channel Ecto-Parasite Attack) and LORA (Low-cost Ripple-effect Attack) attacks [62]. They pose a threat to the operation of modern mesh networks, but can also be executed against DSA schemes.

In brief, in the NEPA and CEPA parasite attacks, an attacker may illegally occupy the spectrum portions considered most valuable in a DSA network in order to increase his profit, degrade the received QoS and the satisfaction levels of his competitors, or even lower the reputation of special transmission opportunities [49].

In the case of LORA, an attacker may on purpose falsely announce to his competitors, or even to the spectrum sharing mechanism, that he will occupy a special spectrum portion, even if he has no right in doing so. As a consequence, any potential user will either avoid competing for them, or hasten to switch to a new one to preserve normal operation.

5. Conclusions

In this article, we focused on possibilities of misbehavior in future Cognitive Radio networking scenarios. We identified the attacker profiles from which such behaviors derive and classified attacks regarding the spectrum sharing phase each one pertains to. We believe that research in the area of securing spectrum sharing schemes is fully justified and, to this end, we wish to provide a spherical view of the threats such a system would face. Now that research and standardization efforts in the area of Cognitive Radio are in progress and many novel, efficient spectrum management schemes are proposed, exploring their potential security vulnerabilities is timely and incorporating appropriate security mechanisms into their design is critical.

Acknowledgement

This work was supported in part by the FP7 ICT Network of Excellence *Euro-NF (Anticipating the Network of the Future—From Theory to Design)* through the Specific Joint Research Project *ASPECTS (Agile SPECTrum Security).*

References

1. Polyzos, G.C.; Jerman-Blažič, B.; Trossen, D.; Kennedy, D.; Hailes, S.; Mähönen, P.; Papadimitriou, D. The EIFFEL approach towards Visions for a Future Networked Society. In Proceedings of the ICT Mobile Summit Conference & Exhibition, Santander, Spain, June 2009.
2. Hui, S.Y. Challenges in the Migration to 4G Mobile Systems. *IEEE Commun. Mag.* **2003**, *41*, 54–59.
3. Frattasi, S.; Fathi, H.; Fitzek, F.H.P; Prasad, R. Defining 4G Technology from the User's Perspective. *IEEE Network* **2006**, *6*, 35–41.
4. ITU Internet Reports 2005: The Internet of Things. Available online: http://www.itu.int/osg/spu/publications/internetofthings/index.html/ (accessed on 9 July 2010).
5. Botterman, M. *Internet of Things: An early reality of the Future Internet*; Workshop Report for European Commission, Information Society and Media Directorate General; Networked Enterprise & RFID Unit (D4): Prague, Czech Republic, 10 May 2009.
6. Akan, O.B.; Karli, O.B; Ergul, O. Cognitive Radio Sensor Networks. *IEEE Network* **2009**, *23*, 34–40.
7. Akyildiz, I.F.; Lee, W.Y; Vuran, M.C.; Mohanty, S. Next generation/dynamic spectrum access/cognitive radio wireless networks: A Survey. *Comput. Netw.* **2006**, *50*, 2127–2159.
8. Akyildiz, I.F.; Lee, W.Y.; Vuran, M.C.; Mohanty, S. A Survey on Spectrum Management in Cognitive Radio Networks. *IEEE Commun. Mag.* **2008**, *46*, 40–48.
9. McCoy, D.; Sicker, D.; Grunwald, D. A Mechanism for Detecting and Responding to Misbehaving Nodes in Wireless Networks. In Proceedings of the 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07), San Diego, CA, USA, June 2007.
10. Berlemann, L.; Hiertz, G.R.; Walke, B.; Mangold, S. Strategies for distributed QoS support in radio spectrum sharing. In Proceedings of the IEEE International Conference on Communications (ICC'05), Seoul, Korea, May 2005.
11. Fattahi, A.R.; Fangwen F.; van der Schaar, M.; Paganini, F. Mechanism-based resource allocation for multimedia transmission over spectrum agile wireless networks. *IEEE J. Sel. Area. Commun.* **2007**, *25*, 601–612.
12. Ycek, T.; Arslan, H. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutorial.* **2009**, *11*, 116–160.
13. Zhang, R.; Liang, Y.C. Exploiting hidden power-feedback loops for cognitive radio. In Proceedings of IEEE DySPAN 2008, Chicago, IL, USA, October 2008.
14. Zhao, G.; Li, Y.G.; Yang, C. Proactive detection of spectrum holes in cognitive radio. In Proceedings of the IEEE International Conference on Communications (ICC'09), Dresden, Germany, June 2009.
15. Cabric, D; Mishra, S.M.; Brodersen, R.W. Implementation Issues in Spectrum Sensing. In Proceedings of the Asilomar Conference on Signal, Systems and Computers, Pacific Grove, CA, USA, November 2004.

16. Isaksson, L.; Fiedler, M.; Rakus-Andersson, E. A Fuzzy Set Theory Based Method to Discover Transmissions in Wireless Personal Area Networks. In Proceedings of ICWMC'06, Bucuresti, Romania, July 2006.
17. Chen, R; Park, J.-M.; Reed, J.H. Defense against primary user emulation attacks in cognitive radio networks. *IEEE J. Sel. Area. Commun.* **2008**, *26*, 25–37.
18. Cao, L.; Zheng, H. Distributed Spectrum Allocation via Local Bargaining. In Proceedings of IEEE SECON'05, Santa Clara, CA, USA, September 2005.
19. Peng, C.; Zheng, H.; Zhao, B.Y. Utilization and fairness in spectrum assignment for opportunistic spectrum access. *Mobile Netw. Appl.* **2006**, *11*, 555–576.
20. Steenstrup, M. Opportunistic use of radio-frequency spectrum: a network perspective. In Proceedings of IEEE DySPAN 2005, Baltimore, MD, USA, November 2005.
21. Neel, J.; Reed, J. Performance of distributed dynamic frequency selection schemes for interference reducing networks. In Proceedings of IEEE MILCOM 2006, Washington, DC, USA, October 2006.
22. Nie, N.; Comaniciu, C. Adaptive channel allocation spectrum etiquette for cognitive radio networks. In Proceedings of IEEE DySPAN 2005, Baltimore, MD, USA, November 2005.
23. Vamsi Krishna, T; Das, A. A survey on MAC protocols in OSA networks. *Comput. Netw.* **2009**, *53*, 1377–1394.
24. Brown, T.X.; Sethi, A. Potential cognitive radio denial-of-service vulnerabilities and protection countermeasures: a multidimensional analysis and assessment. In Proceedings of the 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2007), Orlando, FL, USA, 9 August 2007.
25. Popescu, A; Erman, D.; Fiedler, M; Kouvatsos, D. A Multi-Dimensional CAN Approach to CRN Routing. In Proceedings of the 6th International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks (HET-NETs), Zakopane, Poland, 14–16 January 2010.
26. Efstathiou, E. A Peer-to-Peer Approach to Sharing Wireless Local Area Networks. Ph.D. Thesis, Athens University of Economics and Business, Athens, Greece, June 2006.
27. Buttyán, L.; Hubaux, J.P. *Security and Cooperation in Wireless Networks*; Cambridge University Press: Cambridge, UK, 2008.
28. Arkoulis, S.; Kazatzopoulos, L.; Delakouridis, C.; Marias, G.F. Cognitive Spectrum and its Security Issues. In Proceedings of the 2nd IEEE International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST), Cardiff, Wales, UK, September 2008.
29. Chen R.; Park, J. Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. In Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Reston, VA, USA, September 2006.
30. Chen, R; Park, J.-M.; Hou, Y.T.; Reed J.H. Toward secure distributed spectrum sensing in cognitive radio networks. *IEEE Commun. Mag.* **2008**, *46*, 50–55.
31. Xiao, S.; Park, J.; Ye, Y. Tamper Resistance for Software Defined Radio Software. In Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, Seattle, Washington, DC, USA, July 2009.

32. Frangoudis, P.A.; Zografos, D.I.; Polyzos, G.C. Secure Interference Reporting for Dense Wi-Fi Deployments. In Proceedings of the ACM CoNEXT '09 Student Workshop, Rome, Italy, December 2009.
33. Jia, J.; Zhang, Q.; Shen, X. HC-MAC: A hardware-constrained cognitive MAC for efficient spectrum management. *IEEE J. Sel. Area. Commun.* **2008**, *26*, 106-117.
34. So, J.; Vaidya, N. Channelization: multi-channel MAC for ad hoc networks: handling multi-channel hidden terminals using a single transceiver. In Proceedings of ACM MobiHoc, Florence, Italy, May 2004.
35. Thoppian, M.; Venkatesan, S.; Prakash, R.; Chandrasekaran, R. MAC layer scheduling in multi-hop wireless networks. In Proceedings of IEEE WoWMoM 2006, Niagara-Falls, Buffalo, NY, USA, June 2006.
36. Romero, J.-P.; Sallent, O.; Agusti, R.; Giupponi, L. A novel on-demand cognitive pilot channel enabling dynamic spectrum allocation. In Proceedings of IEEE DySPAN 2007, Dublin, Ireland, April 2007.
37. Ma, L.; Han, X.; Shen, C.-C. Dynamic open spectrum sharing MAC protocol for wireless ad hoc networks. In Proceedings of IEEE DySPAN 2005, Baltimore, MD, USA, November 2005.
38. Lazos, L.; Liu, S.; Krunz, M. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the Second ACM Conference on Wireless Network Security (WiSec'09), Zurich, Switzerland, March 2009.
39. Brown, T.X.; James, J.E.; Sethi, A. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of the 7th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Florence, Italy, May 2006.
40. Bian, K.; Park, J.M. MAC-layer misbehaviors in multi-hop cognitive radio networks. In Proceedings of the 2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006), Teaneck, NJ, USA, August 2006.
41. Ma, L.; Shen, C.-C.; Ryu, B. Single-radio adaptive channel algorithm for spectrum agile wireless ad hoc networks. In Proceedings of IEEE DySPAN 2007, Dublin, Ireland, April 2007.
42. Brik, V.; Rozner, E.; Banarjee, S.; Bahl, P. DSAP: A protocol for coordinated spectrum access. In Proceedings of IEEE DySPAN 2005, Baltimore, MD, USA, November 2005.
43. Kloeck, C.; Jaekel, H.; Jondral, F. K. Dynamic and local combined pricing, allocation and billing system with coginitive radios. In Proceedings of IEEE DySPAN 2005, Baltimore, MD, USA, November 2005.
44. Cramton, P.; Shoham, Y.; Steinberg R. *Combinatorial Auctions*; MIT Press: Cambridge, MA, USA, 2006.
45. Krishna, V. *Auction Theory*; Academic Press: San Diego, CA, USA, 2002.
46. Ji, Z.; Liu, K.J.R. Multi-stage pricing game for collusion resistant dynamic spectrum allocation. *IEEE J. Sel. Area. Commun.* **2008**, *26*, 182-191.
47. Benyoucef, M.; Alj, H.; Levy, K.; Keller, R.K. A Rule-Driven Approach for Defining the Behaviour of Negotiating Software Agents. In Proceedings of the 4th International Workshop on Distributed Communities on the Web, Sydney, Australia, April 2002.

48. Wu, Y.; Wang, B.; Liu, K.; Clancy T. Collusion-resistant multi-winner spectrum auction for cognitive radio networks. In Proceedings of IEEE Globecom, New Orleans, LA, USA, December 2008.
49. Cao, L.; Zheng, H. Distributed Rule-Regulated Spectrum Sharing. *IEEE J. Sel. Area. Commun.* **2008**, *26*, 130–145.
50. Rondeau, T.; Rieser, C.; Le, B.; Bostian, C. Cognitive radios with genetic algorithms: Intelligent control of software defined radios. In Proceedings of the SDR Forum Conference, Phoenix, AZ, USA, November 2004.
51. Atia, G.; Saligrama, V.; Sahai, A. Codes to unmask spectrum violators. In Proceedings of the Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, USA, October 2008.
52. Xu, W.; Kamat, P.; Trappe W. TRIESTE: A Trusted Radio Infrastructure for Enforcing SpecTrum Etiquettes. In Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Reston, VA, USA, September 2006.
53. Stallings, W. *Network Security Essentials: Applications and Standards*, 3rd ed.; Prentice Hall: Upper Saddle River, NJ, USA; p. 432.
54. Chapin, J.M.; Lehr, W.H.. The path to market success for dynamic spectrum access technology. *IEEE Commun. Mag.* **2007**, *45*, 96–103.
55. Cordeiro, C.; Challapali, K. C-MAC: A cognitive MAC protocol for multi-channel wireless networks. In Proceedings of IEEE DySPAN 2007, Dublin, Ireland, April 2007.
56. IEEE 802.22 Working Group on Wireless Regional Area Networks. Available online: http://www.ieee802.org/22/ (accessed on 9 July 2010).
57. Atia, G.; Sahai, A.; Saligrama, V. Spectrum enforcement and liability assignment in cognitive radio systems. In Proceedings of IEEE DySPAN 2008, Chicago, IL, USA, October 2008.
58. Haykin, S. Cognitive radio: brain-empowered wireless communications. *IEEE J. Sel. Area. Commun.* **2005**, *23*, 201–220.
59. Narayanan, L. Channel assignment and graph multicoloring. In *Handbook of Wireless Networks and Mobile Computing*; John Wiley and Sons, Inc.: New York, NY, USA, 2002; pp. 71–94.
60. Mody, A.N.; Reddy, R.; Sherman, M.J.; Kiernan, T.; Shyy, D.J. *Security and the Protocol Reference Model Enhancements in IEEE 802.22*; IEEE Document No. 802.22-08-0083r04; IEEE Standards Association: Piscataway, NJ, USA, June 2008.
61. Sahai, A.; Tandra, R.; Mishra, S.M.; Hoven, N. Fundamental design tradeoffs in cognitive radio systems. In Proceedings of the 1st International Workshop on Technology and Policy For Accessing Spectrum (TAPAS'06), Boston, MA, USA, August 2006.
62. Naveed A.; Kanhere, S. Security vulnerabilities in channel assignment of multi-radio multi-channel wireless mesh networks. In Proceedings of IEEE GLOBECOM 2006, San Francisco, CA, USA, November 2006.
63. All these apply independently of the category of the control channel. Note that according to [23], there are three types of control channels: global, local, and the dynamically selected ones.