Cognitive Spectrum and its Security Issues

S. Arkoulis L. Kazatzopoulos *C. Delakouridis* G.F. Marias
Dept. Of Informatics, Athens University of Economics & Business
arkoulistam@aueb.gr *lkazatzo @aueb.gr* kodelak@aueb.gr marias@aueb.gr

Abstract

The current trend for opportunistic use of the licensed or licensed-exempt wireless spectrum with limited rules, or even without rules, introduces significant scientific and technical challenges for the Networks of the Future. Until now, for the realization of the cognitive radio paradigm, several spectrum sharing schemes have been proposed, such as centralized and distributed schemes, and cooperative or non-cooperative spectrum sharing mechanisms. Unfortunately, some of the existing proposals for spectrum sharing and management introduce significant security leakages, putting into effect unfairness, unavailability, and selfishness, or even malicious behaviors. Additionally, the identification, recording and reporting of selfish, free-riders, malicious and anomalous actions by peers is still an open issue in the majority of the existing spectrum management schemes. This paper discusses and classifies the weak points and the vulnerabilities of the spectrum sharing mechanisms.

1. Introduction

Software defined and cognitive radios 0 [2] might be considered as the first step towards the realization of Noam's vision for "Open Spectrum Access" [3]. In Noam's vision, there is no license, and no up-front spectrum auction. Instead, spectrum bands are license-free, all users those bands pay an access fee that is dynamically determined by the demand/supply conditions at the time, for instance by the existing congestion in the frequency bands, at time. Actually, due to the dramatic increase for access to the spectrum in the recent years, traditional spectrum policies have been reconsidered. Currently, dynamic spectrum access is proposed as a solution for the spectrum inefficiency. In this direction, DARPAs proposes the so-called NeXt Generation (xG) program which aims to implement a spectrum management framework based on cognitive radios [4][5]. The cognitive framework takes into account spectrum that is licensed, whereas primary users, i.e., those having rights for exclusive use of spectrum bands, release temporally some unused spectrum frequencies. These spectrum white spaces [2] are then shared opportunistically to non-primary users, so called secondary users. The sharing rules and the resolved dynamic spectrum allocation mainly focus on the avoidance of the interference conditions, mainly to primary users.

On the other hand, other spectrum regulation bodies, such as FCC, ECC, and the ITU World Radio Conference (WRC) have defined several unlicensed spectrum bands. For instance, the 2,4GHz Industrial Scientific and Medical (ISM) band was initially used for the deployment of the Radio LANs. U-NII systems, as defined by the FCC or WRC, operate using several license-free bands in the 5GHz spectrum. These bands are exploitable by Wireless Internet Service Providers (WISPs), that offer high data rates with much cheaper equipment and installation costs for providing Internet (or VPN) access services, voice and value added services, security provision, accounting and mobility management using WiMAX/WiFi technologies and standards. On the other hand, WISPs deployment disadvantages include limited coverage areas, lack of handover between hotspots, proven security and intra-domain authentication, and primarily, bandwidth efficiency due to the inadequate regulation that applies for the unlicensed spectrum usage.

We anticipate that future WIPS's Access Points (APs), equipped with cognitive radios, will use and compete for multiple orthogonal channels concurrently to offer high-speed wireless access in the unlicensed bands. Relevant standards, such as the 802.22 standard for Wireless Regional Area Networks, indicate that this in not only a hypothesis. Such competition for orthogonal channels will softly involve the end-nodes that are connected with the APs, since they should employ fast channel discovery and AP association techniques; end-nodes should also report traffic demands and Quality of Service requirement to the APs. The overall objective of the employment of cognitive radios in the

978-0-7695-3333-9 /08 $25.00 © 2008 IEEE
DOI 10.1109/NGMAST.2008.102

licensed-free bands is to share or distribute the spectrum channels to APs whcih compete for short-term and ephemeral reservation, and at the same time achieve fairness and efficacy.

In this paper we will focus our research in the cooperative approach over the unlicensed spectrum; we assume that APs, irrespectively of whether the APs are operated by a single or multiple WISPs, are jointly performing cognitive actions. These actions include spectrum sensing, allocation, sharing, or release, and might be performed distributed [7] [10] [11] [12] [13] [14] [16] [17] [18] [19] or centralized [6] [8] [9]. The main challenge for any solution that aims to efficiently facilitate dynamicity and fairly distribute the unlicensed spectrum channels to cognitive APs is to include countermeasures that defeat unfairness and security leakages. Towards this direction, identification, recording and reporting of selfish, free-riders, malicious and anomalous behaviours by APs is still an open issue.

The majority of the centralized or distributed approaches assume that the participating nodes, i.e., APs, are altruistic and rational. Except the LocDef scheme in [20], TRIESTE [15] and the key-based principle that is used in [21], selfishness and malicious operation are not thoroughly discussed. The majority of the cognitive radio management mechanisms are unaware of the possible misbehaviors and attacks that might be present. To the best of our knowledge, it is not yet available in the literature a thorough study for the weaknesses that the centralized or distributed approaches experience due to selfish actions, misbehaviors of APs, and malicious attacks.

The scope of this paper is to identify, analyze and explain security weaknesses and vulnerabilities of cooperated dynamic and open spectrum access frameworks that could be exploited by offender APs to damage operation or affect the performance for their own motivation. The contributions of this paper are the reference security framework for the cognitive spectrum paradigm, and the impact to the enhancement of any future dynamic access spectrum policy or mechanism, when the security concerns are incorporated.

2. Motivation

According to the cognitive radio paradigm APs are installed in the same geographical areas. For this application scenario the use or share of the spectrum is opportunistic. Collocated and overlapping APs compete for allocating a number of spectrum channels, for the duration of the allocation, as well as for the power they permitted to use during transmission. The latter is relative to their position, since transmission power deals with the radius of the coverage area. Thus, spectrum is sensed, selected or shared with peer APs. If the portion of spectrum is licensed-free, then there is no need for un-licensed users to vacate the channel when a licensed user (or primary) is detected, or to detect in which sub-bands of the spectrum a licensed users is present during the sensing phase. This paradigm requires only rules for sensing and sharing the spectrum, and no AP is considered to have a predefined priority to use the spectrum (i.e., there are no primary users with extraordinary priority). A scenario where heterogeneous operators' APs might coexist in a geographical area is also feasible. Such APs might serve:

- Fixed or Wireless ISPs who profit from residential APs installations, providing a richer set of services to their subscribers
- Universities or municipalities hot-spot installations to provide free-of-charge wireless broadband services to students and people
- Individual and residential AP owners who share their bandwidth on an altruistic or on a for profit basis

Until now, several spectrum sharing schemes have been proposed, such as centralized and distributed schemes, and cooperative or non-cooperative spectrum sharing mechanisms using game theory results, or even incentives and auction approaches. Cognitive networks have received increased interest and relevant standards, such as the IEEE 802.22 standard, indicate that they are a fast maturing technology. Additionally, several international initiatives, such as the IST projects Drive[1], OverDRiVE[2] and OBAN[3], as well as Nautilus[4] and HD-MAC[5].

In the centralized approach, a centralized entity assembles network status information, and efficiently allocates frequency channels to the APs in order to maximize a welfare utility. This approach does not scale well, since the central broker will eventually become a bottleneck in the system. Additionally it is not-well self-adapted to conditions where new APs are installed, or when multiple WISPs are share common deployment areas. On the other hand, being aware of the overall network status, the central utility provides global efficient allocations. In many proposals, a centralize server conducts and supervise a bidding proce-

[1] DRiVE Project Website:. http://www.ist-drive.org
[2] OverDRiVE Project Website: http://www.ist-overdrive.org
[3] OBAN Project Website: http://www.ist-oban.org
[4] Nautilus Project Website http://www.cs.ucsb.edu/~htzheng/cognitive/nautilus.html
[5] HD-MAC Project Website http://www.cs.ucsb.edu/~htzheng/cognitive/HDMAC.html

dure. Centralized approaches are by default cooperative.

Distributed approaches are applicable for scenarios where APs are self-organized in small groups, probably isolated from other groups or fixed-infrastructures, and compete to maximize a utility objective. In the cooperative approach, this competition might be implemented via collaborative means, such as control channels, etiquette rules or explicit message exchange, etc (e.g., [11]). The goal is the accomplishment of the utility function of the group, agreed in advance through collaborative means. In the non-cooperative approach, APs compete with each other to maximize their own profit.

For the rest of our analysis it is crucial to identify what kind of anomalous behavior we might expect in cognitive radio scenarios.

- A ***misbehaving AP*** simply does not follows any common rule for sensing, sharing, and managing the spectrum
- A ***selfish AP*** aims to increase its utility function, mainly by allocating more spectrum bands, or larger time frames than the one it was assigned or agreed. The main objective is concentrated to the private income and not to the reduction of peer APs returns. APs follow rules that only work in their favor and ignore those rules that turn against them.
- A ***cheat AP*** aims to increase its utility function, and at the same time to decrease the profit of competitors. This strategy is followed in purpose, because there is no other way to increase private income other than to cheat others.
- A ***malicious AP*** violates on purpose the rules of the competition, without taking into account incomes and utility objectives

We classify the aforementioned classes as misbehaviors (the first one) and attacks (the last three). These abnormalities can only be realized if a threat exists; i.e., if one or more APs aim to exploit vulnerabilities and weakness of the rules and protocols.

3. Misbehaviors and Attacks

We present is this section our main results of weakness and threats in the cognitive paradigm. In the following analysis, we present the type of the misbehavior or attack, the class of the attack, the type of protocols it targets (i.e., distributed or centralized) and the architecture that it applies (if any).

1.	The AP claims that it did not receive spectrum coordination or allocation signals.	**Type:** Misbehaving or Selfish **Category:** Distributed or Centralized
2.	The AP claims that it received corrupted spectrum coordination or allocation signals	**Type:** Misbehaving or Selfish **Category:** Distributed or Centralized
3.	Assume that sharing rules are based on a rich and poor inference (e.g., high and low channel allocation of APs). APs exchange metrics information. Selfish APs might send false metrics claiming that they are poor. Thus, they will always claim higher priority during channel bidding.	**Type:** Selfish **Category:** Distributed or Centralized **Source**: [25]
4.	Assume that the rate of a channel is 'high' if a great number of APs bidding for its usage. APs and bid for 'high' rated channels. A group of M APs cooperate to cheat the overall system. In this scenario N APs (N is a subset of M) bid for low quality channels (channels with low bit rates). This will work as a honey-pot for the rest of the APs of the system. Thus, K=M-N APs will be able to bid for high quality channels without enough competition.	**Type:** Cheat **Category:** Distributed or Centralized **Source:** [25]
5.	Node A is aware of high quality channels. Whenever another node uses these channels, node A transmits at the same time to cause interference. Thus, it downsizes the quality of the channel. As a result, it will be unlikely that other APs to bid over this low quality channel giving to node A much higher to allocate it.	**Type:** Cheat **Category:** Distributed or Centralized **Source:** [25]
6.	Assume that a threshold for the maximum number of channels a node can use is enforced. This threshold is related to the number of APs and available channels. A	**Type:** Selfish **Category:** Distributed or Centralized **Source:** [25]

	group of M APs cooperate to cheat the overall system. Just before an AP A bids for a channel, the remaining M-1 APs send dummy requests for bidding pretending non existing users. Threshold will be decreased and APs have to bid for fewer channels. Therefore node A will have higher probability to use a channel	
7.	In the existence of a Centralized Server (CS), APs send requests to CS with their needs. CS allocates spectrum according to a policy and inform APs about the winning nodes. A spoofing attack might be launched. During the bidding phase, a node A alters packages sent from competing APs to the CS, by modifying their needs or offers. At the end of the bidding procedure, the AP A will be selected as the winner of the competition.	**Type:** Cheat **Category:** Centralized **Source:** [6]
8.	Same as previous, but here the AP A highjack the packet send from the CS about the winning node, and alters the winning node in its favor.	**Type:** Cheat **Category:** Centralized **Source:** [6]
9.	Same as previous, but here the AP A highjack the announcement packets send from the CS to the nodes for available bandwidth, and decrease this value. Therefore, the rest of the nodes will produce demand and offers based on false input. As a result, node A will increase its probability to gain access rights.	**Type:** Cheat **Category:** Centralized **Source:** [6]
10.	When a negotiation for spectrum usage or bidding starts, an AP A might send its offer and simultaneously flood the network with dummy traffic. The centralized server or the peers will receive only A's offer; due to the flooding some of the other offers will not be delivered. Therefore, node A increases the probability to be the winning node.	**Type:** Selfish **Category:** Centralized or distributed **Source:** [6]
11.	When a negotiation for spectrum usage or bidding starts, the AP A sends its offer and floods the network with dummy traffic. The centralized server will receive node's A demand or offer but due to flooding the rest of the offers could not be delivered. Therefore, node A increases his probability to be the winning node.	**Type:** Cheat **Category:** Centralized **Source:** [6]
12.	Malicious APs try to spoof the identity of an AP user with large allocations, of an AP that recently awarded access, or a winner of a biding or competition, in order to gain access to radio.	**Type:** Cheat **Category:** Centralized or distributed **Source:** [26]
13.	When a central authority or guard entity is in place, malicious APs might try to spoof the identity of this entity to mislead the central authority on judging their misbehavior or attack.	**Type:** Selfish **Category:** Centralized or distributed **Source:** [15]
14.	When localization is used as a proof of misbehavior, an AP may alter his signal patterns (change antenna, power, signal direction etc) in order to import errors in the position estimation of the system.	**Type:** Selfish **Category:** Centralized or distributed **Source:** [15]
15.	An AP might transmit noise (jamming) in order to downgrade the communication quality of the neighbors. Thus, some of them may leave the frequency/channel. This will free resources and the AP will gain more spectrum.	**Type:** Selfish **Category:** Centralized or distributed
16.	When spectrum sharing and scheduling is based on QoS needs, an AP might claim more demands than the actual current needs to allocate more spectrum	**Type:** Selfish **Category:** Centralized or distributed **Source:** [9]
17.	A malicious AP may inject fake control frames inside the network. So, there may exist frames with erroneous headers SSID), misleading info about neighbors or interfe-	**Type:** Malicious **Category:** Centralized or distributed **Source:** [9] [23] [24]

	rence levels or other useful metrics. The network will easily become unstable and unfair in terms or resource allocation.	
18.	An attacking AP may mimic another AP (it observes the radio transmission patterns and control information and then it transmits using the same patterns, in the same bands). So, the victim may become isolated, its bandwidth requests will be useless, and its spectrum usage will eventually become unfair. As a result, QoS agreements may be broken. In the worst case scenario, the attacking AP may isolate a legitimate AP or completely overtake it.	**Type:** Malicious **Category:** Centralized or distributed **Source:** [23]
19.	An AP may sniff control packets and the usage reports of any other AP for spectrum needs. Based on these information it can predict the future AP's spectrum needs and their preference to particular channels. After that it might participate in an auction for a particular spectrum. So, the attacker AP does bids in channels that will be needed in the future by particular APs in order to increase their price and/or reputation.	**Type:** Selfish **Category:** Centralized or distributed **Source:** [23] [24]
20.	An attacker may sniff control packets, observe which channels are in the verge of being allocated and transmit (jamming) over them illegally. The applicants may be obliged to bid for a new channel and lose the paid price. The network will soon become unstable and the APs will stop trusting the broker (centralized) or their neighbours (distributed).	**Type:** Malicious **Category:** Centralized or distributed **Source:** [23] [24]
21.	If an AP_1 uses a channel that an AP_2 wants, a malicious AP_2 will cause interference to AP_1 and make this AP to handoff in order to allocate a better channel. So, the channel will become available to AP_1 and will be low-priced for brokering and bidding. If AP_1 win the next auction and allocate the channel, it will stop interfering.	**Type:** Cheat **Category:** Centralized or distributed **Source:** [9] [23]
22.	Assume that the spectrum allocation is based on a number of predefined policies. These may be stored in a central database (single-point-of-failure, easy to hack) or in a more distributed way, for security or robustness issues. A malicious AP may alter the contents of this database (centralized case) or spread false policy packets inside our network (distributed case) in order to mislead its neighbors or everyone who asks him a defined policy.	**Type:** Cheat **Category:** Centralized or distributed **Source:** [23]

4. Existing solutions and relative work

To mitigate or avoid the aforementioned misbehaviors or attacks, countermeasures are essential. An interesting approach is presented in [20], where specialized wireless sensors are deployed to identify an attack where the adversary transmits signals whose characteristics emulate those of incumbent signals. The proposed LocDef scheme verifies whether a given signal is that of an incumbent transmitter by estimating its location and observing its signal characteristics. Even if this scheme assumes a reliable and secure sensor network, which is not always the case, LocDef can assist to avoid or mitigate some of the aforementioned drawbacks, but on the other hand APs might not cooperate fairly for location estimation (see item 14). On the other hand, trust relationships between entities have been proposed to avoid unauthorized nodes attacking the cognitive system. To build trust a key-based principle was used in [21].

In [22] several multi-channel jamming are reported and analyzed. The paper concentrates on how jamming attack amplifies their impact across multiple channels using a single radio and evaluates the efficacy of the jamming duration as well. Finally, the work in [23] is focused on the denial of service vulnerabilities and explores potential remedies that can be applied in the cognitive radio paradigm. To the best of our knowledge, in the literature there is no any other survey related with the weak points and the vulnerabilities of the cognitive spectrum sharing mechanisms.

5. Conclusions

When protocols, architectures and mechanisms are designed to efficiently distribute resources in the cognitive radio paradigm, misbehaving weaknesses and security vulnerabilities are not of primary concern. Thus, spectrum sensing, allocation, brokering, scheduling and management policies might be targets of potential malicious or selfish APs. The identification, mitigation or isolation of misbehaviors, threats and attacks in the cognitive radio paradigm is essential for guaranteeing fairness, achieving the agreed QoS metric and avoiding free-riding phenomena, whilst it guarantees channel resources availability to legitimate unlicensed users.

10. References

[1] J. Mitola, and G. Q. Maguire, "Cognitive radio: making software radios more personal", IEEE Pers. Commun. 6, 4 (Aug. 1999), 13–18.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications", IEEE J. Select. Areas Commun. 23, 2 (Feb. 2005), 201–220.

[3] E. Noam "Taking the Next Step Beyond Spectrum Auctions: Open Spectrum Access", IEEE Communications Magazine, Dec. 1995

[4] DARPA XG WG, "The XG Architectural Framework V1.0", 2003.

[5] DARPA XG Working Group, "The XG Vision Request for Comments", Version 2.0, 2004

[6] O. Ileri, D. Samardzija, and N.B. Mandayam, "Demand responsive pricing and competitive spectrum allocation via spectrum server", IEEE DySPAN 2005

[7] G. F. Marias, "Spectrum Scheduling and Brokering Based on QoS Demands of Competing WISPs", IEEE DySPAN 2005

[8] C. Raman, R. D. Yates, and N. B. Mandayam, "Scheduling variable rate links via a spectrum server", IEEE DySPAN 2005

[9] M. M. Buddhikot, P. Kolody, S. Miller, K. Ryan, and J. Evans, "DIMSUMNet: New directions in wireless networking using coordinated dynamic spectrum access", IEEE WoWMoM 2005

[10] V. Brik, E. Rozner, S. Banarjee, and P. Bahl , "DSAP: a protocol for coordinated spectrum access", IEEE DySPAN 2005

[11] X. Jing X. and D. Raychaudhuri, "Spectrum Coexistence of IEEE 802.11b and 802.16a Networks Using Reactive and Proactive Etiquette Policies," ACM Journal Mob. Netw. Appl., 11(4):539-554, 2006.

[12] Nautilus Project Website, available at: www.cs.ucsb.edu/~htzheng/cognitive/nautilus.html

[13] SWAN: Self-organized Wireless Access Networks, available at www.pittsburgh.intelresearch.net/ ~kpapagia/ /SWAN/index.php

[14] G. F. Marias, "A QoS-based auction protocol for coexisting WISPs", IEEE LANMAN 2005

[15] W. Xu, P. Kamat, and W. Trappe "TRIESTE: A Trusted Radio Infrastructure for Enforcing SpecTrum Etiquettes", 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, 2006

[16] L. Cao, and H. Zheng, "Spectrum allocation in ad hoc networks via local bargaining", IEEE SECON 2005

[17] A. Mishra, et al., "Distributed channel management in uncoordinated wireless environments" MobiCom 2006

[18] J. Neel, and J. Reed, "Performance of distributed dynamic frequency selection schemes for interference reducing networks", IEEE Milcom 2006

[19] J. Zhao, H. Zheng, and G. Yang, "Distributed coordination in dynamic spectrum allocation networks", IEEE DySPAN 2005

[20] R. Chen, J.-M. Park, and J. H. Reed, "Defence against Primary User Emulation Attacks in Cognitive Radio Networks", IEEE JOSAIC, Vol. 26, No. 1, Jan 2008

[21] P. Pawełczak, C. Guo, R. V. Prasad, and R. Hekmat, "Cluster-based spectrum sensing architecture for opportunistic spectrum access networks," IRCTR-S-004-07 Report, Feb. 2007

[22] A. Sampath, H. Dai, H. Zheng, and B.Y. Zhao, "Multi-channel Jamming Attacks using Cognitive Radios", IEEE ICCCN 2007.

[23] T. X. Brown, and A. Sethi "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: A Multi-dimensional Analysis and Assessment", 2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2007

[24] K. Bian and J.-M. Park, "MAC-Layer Misbehaviors in Multi-Hop Cognitive Radio Networks", 2006 Virginia Tech Symposium Posters

[25] L. Cao and H. Zheng, "Distributed Rule-Regulated Spectrum Sharing," IEEE JOSAIC, vol. 26, No. 1, January 2008.

[26] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks," 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, Sept., 2006