Distributed Sensing for Spectrum Agility: Incentives and Security Considerations[⋆]

Stamatios Arkoulis[1], Markus Fiedler[2], Pantelis A. Frangoudis[1], Ralph Herkenhöner[3], Giannis F. Marias[1], Hermann de Meer[3], and George C. Polyzos[1]

[1] Athens University of Economics and Business
{pfrag,arkoulistam,marias,polyzos}@aueb.gr
[2] Blekinge Institute of Technology
markus.fiedler@bth.se
[3] University of Passau
rhk@fim.uni-passau.de, demeer@fmi.uni-passau.de

Abstract. In the last few years, we have witnessed a tremendous growth in the number of wireless devices operating in unlicensed spectrum. Wi-Fi equipment has become standard in laptops and handhelds, while Bluetooth prevails for short-range connectivity. The vision of the *Internet of Things*, where myriads of heterogeneous devices will interconnect over wireless sublayers, forming a huge network of networks is fast approaching its realization. In view of these advances, traditional Internet architectures at all layers will need to transform and adapt to accommodate for the increasing communication demands. Unlicensed wireless spectrum is scarce and we need agile sharing schemes to achieve its increased utilization. The cost for the lack of strict regulation is interference; for spectrum agility, thus, alternative interference mitigation strategies are necessary. A crucial step in this process is sensing the wireless environment to detect interference conditions. In this work, we focus on distributed unlicensed spectrum sensing, where information on spectrum usage conditions from multiple sources are fused to come to smart spectrum access decisions. In the heterogeneous open access environment that we envisage, multiple self-interested entities participate in the sensing and sharing processes. This poses security challenges, which we discuss in this paper.

1 Introduction

Wireless systems operating in unlicensed parts of the spectrum have grown in popularity and wealth of applications. The ubiquity of IEEE 802.11 and Bluetooth-enabled devices and the extensive wireless coverage, especially in modern densely-populated metropolitan areas, are clear indicators of the trend towards open spectrum access. This trend is largely attributable to the fact that the aforementioned wireless technologies operate in unlicensed spectrum and have low installation and operational cost.

[⋆] This work is supported by the Euro-NF (NoE) ASPECTS Specific Joint Research Project.

In this work, we focus on a communication paradigm where: (1) the use of unlicensed spectrum is assumed, (2) mobile users have open access to all public networks, without necessary prior contracts and subscriptions, and (3) everyone can become an operator simply by offering wireless coverage over an area. Lacking strict regulation, operation in unlicensed spectrum comes with the cost of interference. This situation is expected to be aggravated in the near future, in a pervasive environment where devices such as mobile terminals, wireless sensors and Access Points (APs) belonging to a heterogeneous crowd of users and operators will compete for spectrum access. The need for spectrum agitily is, thus, evident. Smart unlicensed spectrum access involves sophisticated spectrum sharing algorithms in three dimensions: frequency (channel assignment), space (power control and directionality of antennas) and time (TDM-like spectrum access).

Before such sharing schemes are in place, though, we need to be able to determine spectrum usage conditions efficiently and decide on which sources of information should be the input to these schemes. Spectrum sensing should be a basic property of the intelligent wireless access systems of the future. Such systems will use feedback from their wireless environment and reconfigure for optimized operation. Our approach is to delegate the role of spectrum sensing to mobile terminals, dedicated sensors and even the APs themselves. Thus, exploiting user mobility and fusing information from multiple sources, a more complete view of spectrum usage conditions can be built.

Since, by default, regulation is not assumed and everyone has equal spectrum access rights, and considering the fact that entities participating in this future networking environment are self-interested, important questions as to the security and robustness of proposed schemes are raised. Do users have incentives to participate in the distributed sensing process? How can the validity of reported information be verified? Is it straightforward to build up policies to control unlicensed spectrum access and detect cases when these policies are violated? In this paper, we show the timeliness of the above issues by presenting motivating cases in the Internet of the present and the future and study security issues in the process of achieving unlicensed spectrum agility. The focus of our work is on Open Spectrum Access systems, but many of our observations and findings may be equally applicable to the case of licensed spectrum.

2 Motivating cases

2.1 Anarchic Wi-Fi deployment

Deployment freedom, minimal necessary investments and ease of configuration of wireless technologies such as Wi-Fi come with a cost; current IEEE 802.11-based network deployments are usually unplanned, and, combined with the scarcity of unlicensed spectrum, lead to significant interference problems and suboptimal spectrum utilization. To make matters worse, it is typical for home WLANs to operate on default frequency and power settings. Thus, the need for interference mitigation is urgent and mandates intelligent self-organizing mechanisms for spectrum sensing and sharing.

2.2 Hidden interference

One of our basic premises is dependence on Distributed Spectrum Sensing (DSS). We deal with heterogeneous sources of information, such as wireless AP measurements, deployed dedicated sensors/monitors, and especially mobile user terminals. The reason for this choice is the fact AP-centric interference mitigation schemes, that is, schemes based on local observations by APs, fail to capture interference at client locations (hidden interference [1]).

2.3 Wireless coverage maps

Part of our motivation in developing a distributed sensing scheme for unlicensed spectrum stems from the need to build wireless coverage maps. Apart from discovering interference conditions, coverage maps can reveal "white spots", i.e. areas with limited wireless service presence, so that prospective providers can determine potential spots to deploy new infrastructure. Also, they can serve as input for power control schemes, and, as a side effect, they can help mobile users in handover planning. However, such a system needs to be secure against fake reporting, robust against invalid or outdated information and capable of handling large amounts of data.

2.4 The Internet of Things

Supported by technological advances in the fields of wireless communications, nanotechnology and sensor networking, the *Internet of Things* [2] is near its realization. We refer to an environment characterized by the omnipresence of smart wireless devices embedded into everyday objects, enabling new information and communication paradigms. The vastly increased communication needs that it will bring about create new challenges at all networking layers. In the spectrum access domain, contention is expected to increase and its dynamics will dramatically change, calling for more agile and spectrum efficient access schemes.

2.5 Virtualization in WLAN access

In our vision of the Internet of the future, a WLAN (micro-)operator may be a member of different *wireless communities* or operate several virtual networks on the same physical AP, each network having different configuration and pricing options. For instance, existing community-based WLAN access schemes, such as FON [3] or P2PWNC [4], involve residential Wi-Fi sharing (either on an altruistic or reciprocal or a for-profit basis) with community members. The challenge here is not only to separate the AP's virtual networks (e.g. community and home network) from each other to grant privacy and security on each one of them, but also to guarantee that spectrum is efficiently shared among them and that user-perceived interference is minimized.

Again, considering the Internet of Things, trust, security and privacy gain great importance, since a user may at the same time join a multitude of Virtual Private Networks (e.g. VPN of all *things* belonging to a user, the supermarket retailer network for his fridge, the government network where he can access government services, etc.) over untrusted shared WLANs. On the other hand, efficiently handling increased numbers of such virtual networks (with increased numbers of participants each) in a shared spectrum becomes harder to tackle.

2.6 Relevant technological advances

Technologies that can be applied for unlicensed spectrum sensing are readily available today; the IEEE 802.11k [5] standard for radio resource measurements has recently been finalized, while scanning for AP presence is a typical procedure in the operation of IEEE 802.11-capable devices.

As to the licensed parts of the spectrum, fixed allocation has proven inflexible and licensed spectrum is often underutilized [6]. This situation calls for *Dynamic Spectrum Access* (DSA) and this is where *Cognitive Radios (CRs)* come to play. According to the DSA model, non-licensed users will be able to sense the spectrum an access it on an opportunistic basis, whenever they detect absence of primary (licensed) users.

3 Incentives and security considerations

In this section we discuss agile spectrum access challenges, with a special focus on distributed spectrum sensing and relevant security issues. Since we heavily rely on user feedback on spectrum conditions, the very nature of the submitted information makes verifying their validity a non-trivial task.

3.1 The cost of spectrum sensing

Our prior experimental work [7] has shown that spectrum sensing with typical IEEE 802.11 equipment can have significant performance overhead, especially for delay-sensitive applications (e.g. VoIP), if requested very often. However, if a client monitors channel usage with reasonable frequency (e.g. once or twice per minute), this overhead is negligible. This provides insight on the incentives of clients to fake their reports or simply refuse to provide them.

Since spectrum sensing incurs cost, it is reasonable to assume that wireless network operators might wish to offer clients a reward for it. This reward might be in the form of improved QoS [7]; operators may allocate more Internet bandwidth for good reporters, prioritize some of their delay-sensitive traffic flows, or even offer them price discounts (in case they pay for wireless access).

3.2 Competition and misbehavior

Apart from the obvious cost of spectrum sensing, competition among wireless network operators may bring in misbehavior. Users affiliated with an operator, may report fake information to his neighbor competitors (e.g. false reports about the channels neighbor APs operate on) to pollute their view of channel usage at their spot and cause them to operate sub-optimally.

Besides such deliberate misbehavior, even accidental misbehavior has to be considered. For instance, equipment unconscious of policies, APs that do not have access to the latest policy information, or APs running out of time synchronisation might use wrong parts of the spectrum at wrong times. Any kind of potential misbehavior motivates the need for spectrum sensing and reporting in order to enable quick and efficient policy enforcement – if possible – or policy adaption.

3.3 Information filtering

To limit the effects of false information reporting, efficient filtering schemes should be present. The issue of spectrum sensing data falsification attacks has also been raised in the context of CR [8]. We believe that using information for multiple sources may help operators filter out false reports by applying simple majority rules; especially in the case where spatial (e.g. GPS coordinates) and temporal (timestamps) information is included in the reports, the entity where reports are collected can easily detect “odd” spectrum measurements.

Furthermore, given that a user identification scheme is in place, user reputations can be built. Then, each report will be weighted according to the reporting entity’s reputation. Users who are consistently suspected (using methods such as the one described above) to report fake information get lower reputation values and, eventually, are subject to *punishment*. Punishment mechanisms can be developed at a different layer. For example, bad reporters may find it hard to gain wireless access of acceptable QoS.

3.4 Trustworthy spectrum sensors

Alternative approaches can also be explored for more efficient spectrum sensing and reporting. For instance, tamperproof monitoring modules can be deployed, whose role is to sense the wireless medium and spectrum conditions. Indeed, Isaksson et al. have shown [9] that such monitors can be built using low-cost hardware. In their work, they make use of Zig-Bee radios at 2.4GHz to passively detect interference among various coexisting technologies (Wi-Fi, Bluetooth, Zig-Bee, microwave ovens) in a Personal Area Network space, applying a fuzzy set-theoretic model to decide which channels are less congested. New tradeoffs are, thus, introduced. Such monitors are inexpensive and trusted by default, so the reported information is considered valid and, in effect, can help detect fake reporters nearby. However, deciding on where to place monitors, how many of them should be deployed and who is responsible for installing, configuring and maintaining them are, still, thorny issues.

3.5 The role of identities

The discussion of Section 3.3 highlights the importance of persistent user identities, so that report "rating" can be achieved. To this end, trusted certification authorities may be needed to issue these IDs and potentially bind user identities with network-level entity identifiers (such as MAC addresses, since this information may be important for lower-layer sensing-reporting mechanisms such as IEEE 802.11k). Identity management schemes already in use may be exploited here. For instance, wireless community user identifiers may be used. Thus, the community can more easily extend its rules, offer community benefits and apply punishment for non-conforming behavior as to the sensing and reporting process.

3.6 Privacy issues

Reports about spectrum usage may reveal information that users might not wish to disclose. For instance, users may include their actual locations in their reports. Thus, the confidentiality of reports should be appropriately ensured and this can be achieved by means of traditional cryptography.

Yet, an other problem arises from the necessity of having several identities (one for every accessed network). Using different identities often includes sharing different personal data with the corresponding network operators. For instance, connecting to a charged network requires accounting information like a credit card number, but for accessing an open network only some contact information like name and email are sufficient. If operators of different networks are sharing data, the threat arises that data of different identities (of the same data subject) could be merged and thus reveal more information about a data subject than originally intended. Thus, accessing different networks requires a sophisticated identity management granting the expected privacy of the data subject.

4 Conclusion

We focus on agile spectrum access systems and, especially, the process of distributed spectrum sensing. Our target is open unlicensed spectrum access, but the issues we discuss and potential solutions are more generic, and can be applied to typical CR environments, where DSA to licensed bands is desired. We thoroughly present our motivation and draw attention to incentives and security considerations, relevant attacks, and how to effectively detect and combat them, in order to build robust spectrum-agile schemes.

References

1. Mishra, A., Brik, V., Banerjee, S., Srinivasan, A., Arbaugh, W.A.: A Client-Driven Approach for Channel Management in Wireless LANs. In: Proc. IEEE INFOCOM 2006, Barcelona, Spain (April 2006)
2. ITU: ITU Internet Reports 2005: The Internet of Things. (2005)

3. FON, http://en.fon.com
4. Elias C. Efstathiou and Pantelis A. Frangoudis and George C. Polyzos: Stimulating Participation in Wireless Community Networks. In: Proc. IEEE INFOCOM, Barcelona, Spain (April 2006)
5. IEEE 802.11 WG: IEEE Standard for information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Radio Resource Measurement of Wireless LANs, IEEE 802.11k-2008. The Institute of Electrical and Electronics Engineers, Inc., New York, USA. (June 2008)
6. McHenry, M.: Spectrum white space measurements. In: New America Foundation BroadBand Forum. (June 2003)
7. Frangoudis, P.A., Polyzos, G.C.: Coupling QoS Provision with Interference Reporting in WLAN Sharing Communities. In: Proc. IEEE PIMRC 2008 Social and Mesh Networking Workshop. (September 2008)
8. Chen, R., Park, J.M., Hou, Y.T., Reed, J.H.: Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Communications (April 2008)
9. Isaksson, L., Fiedler, M., Rakus-Andersson, E.: A Fuzzy Set Theory Based Method to Discover Transmissions in Wireless Personal Area Networks. In: Proc. ICWMC'06. (July 2006)