User Provided and Community Networks as *μ*-Operators in Cognitive Dynamic Spectrum Access

George C. Polyzos

Mobile Multimedia Laboratory
Department of Informatics/Computer Science
Athens University of Economics and Business
Athens 113 62, Greece

Tel.: +30 210 8203 650, Fax: +30 210 8203 325, Email: polyzos@aueb.gr, http://mm.aueb.gr/

Abstract

Low cost wireless network access equipment operating in unlicensed bands has revolutionized local area communications and has permitted, perhaps for the first time in history, to the general public to provide communications services and run *User Provided Networks*. Coupled with the ease of deployment of these wireless technologies, it has made such networks ubiquitous in densely populated urban areas, introducing the potential for alternative spectrum access and new business models. The issue is not anymore coverage, but interference. The mushrooming of such networks, which was seen as bliss in the early years, it is now becoming a curse. Their unplanned deployments and very dynamic topologies demand highly autonomic operation for survival.

Access Points (APs), and transmitters in general, belonging to a heterogeneous crowd of Wireless Internet Service Providers, non-profit organizations, municipalities and residential users, among others, contend for spectrum. In addition, many different technologies such as Bluetooth, Wi-Fi, WiMax and others compete among themselves. The lack of coordination among them, coupled with the scarcity of spectrum and the density of these deployments usually cause severe interference conditions, which necessitate advanced interference mitigation strategies, which however, in our view cannot be limited to the physical layer.

These APs belong in general to different entities that play the role of *μ-Operators*. With high AP power, they cover a wide area in the neighborhood and have the potential to provide high utility to their owners, either in the form of (possibly virtual) payments, or just because of the pride in providing extended coverage. However, this leads to increased interference to other *μ-Operators* and can be considered antisocial behavior. Decreasing transmitter power can lead to increased utility if other transmitters (*μ-Operators)* cooperate. In the past we have proposed and investigated distributed techniques for "opening up" wireless access and providing incentives for cooperation among *μ-Operators* based on Peer-to-Peer techniques.

Cognitive radio techniques come to the rescue. Feedback from user devices and out-of band communication can be utilized to generate dynamic coverage and interference maps. Roaming user devices can measure and report spectrum use. For Wi-Fi systems, technology for reporting spectrum sensing results has been standardized (IEEE 802.11k) and will hopefully become widely available. Specialized sensors, strategically positioned, can also be assigned to this task, but client mobility is invaluable. Dealing with "random" user devices as sources of network status information, however, raises incentives and security concerns. Trusted devices cannot always be assumed; devices polluting system information with invalid reports may lead to suboptimal configuration and spectrum access decisions, which can in turn cause more interference.

We are studying the robustness and security of the reporting process. We consider various attacker strategies and devise mechanisms for effectively tackling them. Our simpler mechanisms for securing the process of interference reporting and increasing its robustness in the presence of adversaries are based on applying simple majority rules. For colluding attackers, our strategy changes; since this scenario involves relationships between users and service providers, it is reasonable to assume a level of trust among them. Reports submitted by users affiliated with a network are valued more, while reports by "foreign" users are discounted, considering each user's trust value.

Finally, User Provided Networks are not limited to the Access Networks. *Wireless Community Networks* have emerged throughout the world. Using inexpensive wireless technology, autonomous wireless backbones and internetworks have been built and are operating, offering a variety of broadband services to their members and other users. Together with smaller or larger Wireless Services Providers, Wireless Service Aggregators and other network providers, they provide a wide range of service providers. Relationships among all these are not straightforward anymore and are becoming very dynamic. Automated Trust management is becoming a key issue for their interconnection and successful interoperation.