Optimizing Primary User Privacy in Spectrum Sharing Systems

Matthew Clark, *Member, IEEE*, and Konstantinos Psounis, *Fellow, IEEE*

***Abstract*— Spectrum regulators are pursuing centralized, dynamic sharing systems that will enable spectrum access for new wireless technologies. These sharing systems will leverage cognitive radio concepts to automatically identify suitable spectrum for users. Collected user information may be considered sensitive, and some incumbents are hesitant about spectrum sharing, citing privacy concerns. Privacy preserving strategies are needed to promote widespread spectrum sharing. However, privacy preserving techniques typically come at the expense of spectrum efficiency, resulting in reduced utility for the users. In this work we study this privacy-performance tradeoff. We develop a generalized spectrum sharing system architecture and formulate the multi-utility, user privacy optimization problem, where privacy is measured by exposure to potential adversary inference attacks. We derive the optimal solution for this spectrum sharing privacy problem and then formulate an efficient heuristic strategy that exploits the problem structure. Via numerical analysis, we demonstrate substantial improvement over the prevailing obfuscation strategies applied in the literature, with up to a 50% increase in privacy and negligible impact on spectrum efficiency for a real-world use case. To our knowledge, this is the first work to formally derive the optimal solution to the user privacy problem in a generalized spectrum sharing framework.**

***Index Terms*— Spectrum Access Systems (SAS), spectrum sharing, location privacy, radio spectrum management, dynamic spectrum access.**

I. Introduction

BANDWIDTH hungry wireless networks such as cellular, Wi-Fi, and the internet of things demand access to radio frequency spectrum. Unfortunately, desirable frequency ranges are limited, and there is no unencumbered spectrum for new services. Replacing legacy technologies is time consuming and expensive, meaning that rapid introduction of a new technology requires improvements to how we share spectrum.

How to best employ spectrum sharing technologies remains an open question. With the introduction of cognitive radio, smart devices that sense their spectrum environment and dynamically adjust their operations to avoid interference were thought to offer the solution to the apparent spectrum crunch.[1] Decentralized cognitive radio solutions face challenges such as the "hidden node problem," and difficulty with remediation of misbehaving devices [1]. Centralized solutions have been introduced, e.g., to facilitate sharing in television white spaces (TVWS) [2]. In this setting users interface directly with Spectrum Access Systems (SAS) which maintain databases of spectrum policy and use information. Centralized sharing offers improved efficiency through resource optimization [3], simplified RF devices [4], and is increasingly seen as a key tool for spectrum sharing [5].

In the U.S., the Federal Communications Commission issued rulemakings to create a Citizens Broadband Radio Service (CBRS) managed by dynamic SAS in the 3550-3700 MHz band [6], [7]. SAS will enable new entrants access to the band, sharing with priority incumbent systems. The SAS will interface with spectrum users, and will employ an infrastructure of spectrum sensors, called the Environmental Sensing Capability (ESC). Based on user inputs and measurements, the SAS is expected to identify suitable protections to prevent harmful interference to priority/primary users (PUs). These protections must be enforced by the SAS when granting spectrum access to secondary users (SUs).

Many of the PUs in 3550-3700 MHz are government entities e.g., military radars. Considering the databases of information held by the proposed SAS, incumbent users have raised concerns about maintaining the privacy of their operations [8]. The SAS needs information on user locations, frequencies, time of use, and susceptibility to interference, where any of these may be considered sensitive by the incumbents and should be protected from exposure to a potential adversary. An adversary may make inference attacks on user information by passively observing the sharing system. A more powerful adversary may be able to hack into the SAS and observe stored information directly. User privacy may be preserved for PUs by obfuscating the information reported to the SAS, and by obfuscating the allocations made by the SAS to SUs. Typical cyber security approaches are not alone sufficient as the normal operation of the SAS may allow an adversary to deduce critical aspects of a PU operation. For example, an adversary may legitimately operate a number of cell phones within a secondary network and leverage assignments from the SAS to make inferences about the characteristics of a military radar. The accuracy of the data communicated between users and the SAS will impact both user privacy and spectrum use efficiency. Coarse precision will reveal less PU information,

Manuscript received October 24, 2018; revised August 6, 2019; accepted December 23, 2019; approved by IEEE/ACM TRANSACTIONS ON NETWORKING Editor W. Lou. Date of publication February 6, 2020; date of current version April 16, 2020. This work was supported in part by the Aerospace Corporation Study Assistance Fellowship Program, in part by the NSF under Grant CNS-1618450 and Grant ECCS-1444060, in part by CISCO Systems through the CRC Grant, and in part by the University of Southern California's Center for High-Performance Computing. *(Corresponding author: Matthew Clark.)*

Matthew Clark is with The Aerospace Corporation, Los Angeles, CA 90245 USA (e-mail: matthew.a.clark@aero.org).

Konstantinos Psounis is with the Joint Electrical and Computer Engineering and Computer Science Departments, The University of Southern California, Los Angeles, CA 90089 USA (e-mail: kpsounis@usc.edu).

Digital Object Identifier 10.1109/TNET.2020.2967776

[1] https://www.fcc.gov/general/spectrum-crunch