Collaborative neighbour monitoring in TV white space networks
Augustine Takyi¹#, Melissa Densmore²#, David Johnson³#
¹Computer Science Department, University of Cape Town
tkyaug001@uct.ac.za
²mdensmore@cs.uct.ac.za
³Meraka Institute, Council for Scientific and Industrial Research, South Africa
djohnson@csir.co.za

Abstract—Collaborative sensing among secondary users in television white space (cognitive radio) networks can considerably increase the probability of detecting primary or secondary users. In current collaborative sensing schemes, all collaborative secondary users are assumed to be honest; however, the deployment of such networks is susceptible to attacks by malicious users, in which malicious secondary users either report false detection results or inject falsified data in order to unduly occupy a specific channel and deny other nodes from using it. This work seeks to allow each secondary user to monitor its neighbour to ensure there is no spectrum abuse by any secondary users so as to improve spectrum fairness in dynamic spectrum access (DSA) networks.

Keywords—White Space, Cognitive Radio, Collaborative, Malicious User, Dynamic spectrum access, sensing.

I. INTRODUCTION

White spaces are the portions of the licensed spectrum band that are not used or occasionally not used in a given geographical location. Measurement studies and the Federal Communications Commission (FCC) Spectrum Policy Task Force [1] confirmed availability of spectrum in licensed bands (white space) in the United States. Therefore, spectrum efficiency can be increased significantly by permitting opportunistic access of these frequency bands to a group of potential users for whom the band has not been officially allocated (unlicensed users) [2]. Although white spaces can be found in any allocated spectrum band, the focus of this work is on the use of television white spaces to provide Internet access to rural communities. In Africa, the television (TV) band is mostly unused in rural areas, which we expect will continue to be the case even after the digital migration and reallocation of the 700MHz and 800MHz bands to licensed International Mobile Telecommunications (IMT) operators [3]. Effective and efficient spectrum utilization of this available spectrum is an important step towards the realization of a successful national broadband policy [4].

It is estimated that Internet connectivity is available to about 39% of the world’s population [5]. The main reason for this low Internet connectivity is that greater numbers of the population live in rural areas. These rural areas are hard to reach given that most of the unlicensed operating bands with frequency of 2.4GHz or 5GHz have limited range. TV white space operates within the frequency range of 50-800MHz [5, 2]. It is known that the lower the frequency the wider the coverage area, therefore TV white spaces spectrum promises to deliver an affordable means to provide Internet access to rural communities.

II. PROBLEM STATEMENT

A rogue or malicious user can use an algorithm that can take control of the free channels unused by primary users and make it appear to other secondary users as though all the channels are busy [7]. Therefore a rogue or malicious user can force exclusive use of free channels or may overuse the available spectrum and deny access to other users. Spectrum-sensing data falsification attacks are also a serious threat created by malicious users within the spectrum and can impact the results of spectrum decisions, and lead to reduced system performance [2]. A typical example is depicted in Figure 1, where each secondary user acts as a sensing terminal that conducts local spectrum sensing. The local results are reported to a data collector (or “fusion center”) that executes data fusion and determines the final spectrum sensing result. The challenge is detecting a malicious user that reports false information to the spectrum database or pretends to be a primary user. A further challenge is a malicious user that appears to be a sensing terminal but in reality is transmitting false sensing results to the fusion center.
are faking their position or to locate the position of a malicious user.

V. EXPECTED OUTCOME

The ongoing research is expected to provide solutions to TV white space spectrum network inefficiencies created by malicious users emulating primary/licensed users or unfairly making use of secondary user spectrum. Neighbours collaborating in exchanging data is a crucial way to increase fairness within TV white space networks. Detection of neighbour usage and its position will also help reduce existence of malicious and greedy users within dynamic spectrum access (DSA) networks.

REFERENCES

[8] Internet Engineering Task Force (IETF) Request for Comments: 6953

Augustine Takyi is a PhD student at the Department of Computer, University of Cape Town, South Africa. He holds BSc Computer Science and Statistics (Combined Major) degree from University of Ghana 2004, Master of Engineering in Computer, and Information System from Huazhong University of Science and Technology, China 2010.

David Johnson is a Principal Researcher at the CSIR Meraka Institute and an adjunct Senior Lecturer in the Computer Science Department of the University of Cape Town. He received his PhD in Computer Science at the University of California, Santa Barbara in 2013 and he currently leads the UCT Net4D research group studying network solutions for developing regions.

Melissa Densmore is a Senior Lecturer in the Department of Computer Science at the University of Cape Town, and a member of the UCT Centre in Information and Communications and Technology for Development. She holds a PhD in Information, Management and Systems from the University of California Berkeley. Her research looks at the design, deployment, and uptake of new information technologies in the context of socio-economic development.