# Collaborative neighbour monitoring in TV white space networks

Augustine Takyi[1#], MelissaDensmore[2#],David Johnson[3*]

[#]*Computer Science Department, Universityof Cape Town*

[1]tkyaug001@uct.ac.za

[2]mdensmore@cs.uct.ac.za

[*]*Meraka Institute, Council for Scientific and Industrial Research, South Africa*

[3]djohnson@csir.co.za

*Abstract*—**Collaborative sensing among secondary users in television white space (cognitive radio) networks can considerably increasethe 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.

The TV white spaces ecosystem will include the following parties: licensed users (primary users), unlicensed users (secondary users), and regulators and spectrum database service providers who ensure that primary users are protected through spectrum use policy and spectrum databases and/or spectrum sensing [6]. Each party interest should be addressed in the spectrum utilization. There is therefore the need to monitor the secondary users in order to maximize spectrum efficiency. An important challenge for all Dynamic Spectrum Access (DSA) methods is security. Most of the research on the operation of DSA systems assumes that the secondary users are honest, cooperative and that no malicious adversaries will attack or exploit the network [4]. This work focuses on secondary users within the spectrum and how each may serve as a watchdog for neighbouring spectrum usage.

## II. PROBLEMSTATEMENT

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 thatreports 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.

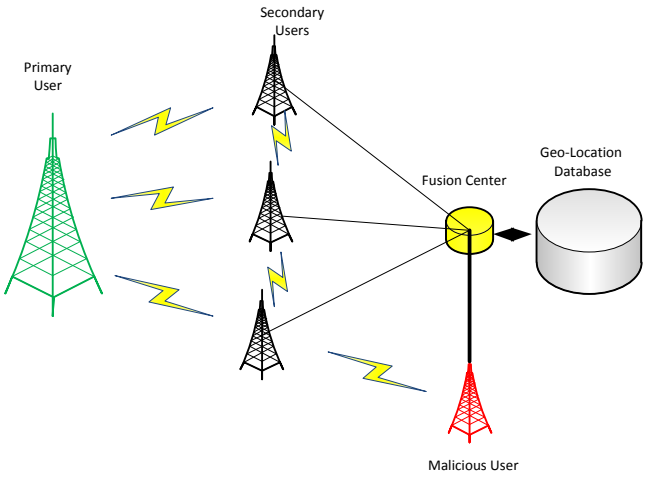


Figure 1: Illustration of Malicious attacks

## III. Motivation

This research is motivated by the problems associated with wireless transmission networks. It is challenging to secure a wireless network because the wireless medium makes it prone to attacks. TV white space networks are wide area networks and as such need to be secured to protect its users. Also the opportunistic nature of unlicensed users who access the unused spectrum band make it vulnerable to attacks. It is difficult to identify who a genuine user is in such network environment. In such networks, since the secondary users are expected to collaborate for optimal performance, some users may send false sensing results which may cause interference and inefficient spectrum usage. Primary users within the spectrum always have priority over the secondary users. Secondary users have to vacate the spectrum at any time a licensed or primary user wants to use the spectrum, and one type of attack involves malicious users masquerading as primary users, an attack known as a primary user emulation attack [8, 9]. This research proposes to resolve these and many more attacks in the use of dynamic spectrum access technology by secondary users.

## IV. Methodology

Energy detectors shall be installed in each secondary user device to enable it to detect the signal strength of its closest nodes immediately after it joins the network and compute its energy threshold. Athreshold needs to be specified when the user is not occupying any channel. This threshold shall be stored in the user's database. Subsequently, a hypothesis test will be employed to check whether the user is abusing the system or not [8]. The energy detected intermittently shall be compared with the threshold figure. If it is greater than or equal to the threshold, then the final sensing decision is "user occupied" otherwise it is set to "user not occupied". If the sensing decision is "user is occupied", the decision is sent to the base station or geo-location database for further analysis. Again, other cyclostationary data like usage patterns shall be used to check whether the user is abusing the spectrum usage or not. The position of the secondary user shall also be estimated by using triangulation or triliteration on received signal strength and antenna direction information from multiple secondary users This collaboratively determined position information is crucial to determine if secondary users are faking their position or to locate the position of a malicious user.

## V. Expectedoutcome

The ongoing research is expected to provide solutions to TVwhite spaces 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

[1] K. Praveen, M. Khabbazian, and V. K. Bhargava. "Secure cooperative sensing techniques for cognitive radio systems."Communications, 2008. ICC'08. IEEE International Conference on. IEEE, 2008.

[2] S.T. Zargar, Saman T., Martin BH Weiss, C. E. Caicedo, and J. BD Joshi. Security in dynamic spectrum access systems: A survey. 2009.

[3] Zhao, Qing, and Brian M. Sadler. "A survey of dynamic spectrum access."Signal Processing Magazine, IEEE 24.3, 2007: 79-89. 2007

[4] Liu, Song, et al. "Aldo: An anomaly detection framework for dynamic spectrum access networks." INFOCOM 2009, IEEE. IEEE, 2009.

[5] A. Lysko, M. T. Masonta and D. Lioyd Johnson, The Television White Space Opportunity in Southern Africa: From Field Measurements to Quantifying White Spaces, Springer international publishing switzaland, 2015

[6] L. Mfupe, F. Mekuria, L. Montsi and M. Mzyece, Geo-location White Space Spectrum Database: Review of Models and Design of a Dynamic Spectrum Access Coexistence Planner and Manager, Springer international publishing switzaland, 2015

[7] V. Pejovic, D. Lloyd Johnson, M. Zheleva, E. M. Belding, VillageLink: A channel Allocation Technique for Wide-Area White Space Networks, Springer international publishing switzaland, 2015

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

[9] Clancy, T. Charles, and Nathan Goergen. "Security in cognitive radio networks: Threats and mitigation." Cognitive Radio Oriented Wireless Networks and Communications, 2008. CrownCom 2008. 3rd International Conference on. IEEE, 2008.

**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 Communication 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.