Performance Analysis of a Collaborative DSA-Based Network with Malicious Nodes

Augustine Takyi[1(✉)], Melissa Densmore[1], Senka Hadzic[1], and David Johnson[1,2]

[1] Department of Computer Science, University of Cape Town, Rondebosch 7701, South Africa
{atakyi,mdensmore,shadzic}@cs.uct.ac.za

[2] Center for Scientific and Industrial Research, Meiring Naudé Road Brummeria, Pretoria, South Africa
djohnson@csir.co.za

Abstract. This work analyses the performance of a Dynamic Spectrum Access (DSA) network with secondary nodes to provide Internet services, and studies the impact of malicious nodes and cooperative secondary nodes on the performance of the network and spectrum utilization. The work mathematically models the throughput, latency, and spectrum utilization with varying numbers of malicious nodes, secondary nodes, miss probabilities, and false alarm probabilities, and studies their effect on performance of the network. The results point to rapid spectrum starvation as the number of malicious nodes increase, as well as the negative impact of too many secondary nodes crowding out available spectrum with resultant degradation of throughput and latency.

Keywords: Spectrum utilization · Secondary node · Backhaul
Malicious node · Throughput · Latency · Primary user

1 Introduction

Estimates have confirmed availability of white spaces (unused licensed bands) and similar observation of under-utilization of the allocated spectrum have been reported by Spectrum Policy Task Force appointed by Federal Communication Commission in the United States and others [1,4]. Spectrum efficiency can be increased significantly by giving opportunistic access of these frequency bands to a group of potential users (unlicensed users) for whom the band has not officially been allocated to use [4]. The users in these networks are expected to be opportunistic. The users refer to the nodes on the network. Therefore granting access to such users in the spectrum may create room for malicious nodes (secondary nodes which do not follow spectrum etiquette and cause harm to other spectrum users). There is the need for all the opportunistic nodes within a specified location to collaborate or cooperate to ensure fairness in the spectrum. Recently, there has been much research in the areas of nodes collaboration or cooperation

V. Odumuyiwa et al. (Eds.): AFRICOMM 2017, LNICST 250, pp. 72–82, 2018.
https://doi.org/10.1007/978-3-319-98827-6_6

and the effects of malicious nodes presence in the DSA-based (dynamic spectrum access based) networks [1–3,5–10]. The rationale for the collaboration is to help detect secondary nodes present in the network or to help report system abuse to the decision centers to identify malicious nodes in the network.

Neighbour collaborative monitoring was demonstrated in [5] where nodes monitor neighbours by measuring their RSSI (received signal strength indicator) values to estimate the distance of the neighbour nodes, which effectively help to detect sybil nodes. Sybil (replicated nodes produced by a secondary node) Nodes Detection is a neighbour monitoring approach used to detect sybil attacks on a network. It uses localization verification technique based on received signal strength, which allows a node to verify the authenticity of another node by estimating its future geographic location and comparing them to its evaluated position. However, the sybil detection failed to prove the validity of the RSS (received signal strength) in estimating the distance to determine the future distance. It was observed in [5] that communication cost was too high which will have a severe negative effect on the performance metrics (throughput and delay) of the network.

Again, neighbour nodes discovery was proposed in [6]. This approach considers a single seed node (with all the parameters known) to locate other nodes by broadcasting a message to all neighbour nodes within its range. The most distant node from the seed node becomes the next seed node, using the above process, all the nodes coordinates are estimated [6]. The proposed protocol seems promising, but it may unnecessarily increase network communication overhead when implemented in the real world: which can be a major problem for opportunistic networks that have limited channels to use for communication.

Moreover, the presence of malicious nodes in a DSA-based network was proposed by Jin et al. [8]. In their work, it was observed that the closer the malicious nodes to the secondary node, the higher the values of miss and false alarm probabilities obtained. The higher probabilities also affected the detection of the presence of the primary user by the honest secondary node (the unlicensed user in the spectrum that does not work against the spectrum etiquette).

Furthermore, Pinifolo et al. [11] considered interference of neighbour nodes in the secondary devices that operate on UHF (Ultra high frequency) band. It discovered that neighbour nodes within a distance range of 7 km apart could have neighbour nodes interference in the UHF band. However, it failed to consider neighbour monitoring in the cooperative network to know the impact on the performance of the density of the secondary nodes in the network.

The main contribution of this paper is three folds. Firstly, we model dynamic spectrum access network that uses neighbour monitoring in cooperative secondary nodes and analyses how malicious nodes present in the network may downgrade performance indicators such as throughput and delay and also affect spectrum utilization. Secondly, It also assesses the impact on performance by increasing the number of collaborative secondary nodes in backhaul nodes of a DSA-based network. Thirdly, The study developed mathematical models to measure throughput, latency and spectrum utilization taking into consideration all

possible interferences. We demonstrate this work through simulations. The paper is organized as follows; Sect. 1 considers introduction, Sect. 2 considers general system model and the performance metrics, Sect. 3 results and discussion and finally Sect. 4 conclusion and future work.

2 System Model

In our model, we positioned fixed secondary nodes (the unlicensed users within the spectrum) connected to the fusion center. The secondary nodes are positioned within a square area of $(d * d)\, km$. The i^{th} device, with position coordinates $P_i = (x_i, y_j)$ where, $i = 1, 2, 3, ..., N$ and $j = 1, 2, 3, ..., N$ the positions of n nodes are assumed to be independent of each other. Each of the secondary nodes has a transmission range R within the area. Primary user (license user within the spectrum) is located at a minimum distance of $\sqrt{(x_i^2 + y_i^2)}$, from the secondary node. The fusion center is empowered with the responsibility of making spectrum decisions for the secondary nodes. Secondary and malicious nodes sensed the spectrum using energy detection, as shown in Fig. 1. Secondary nodes are also embedded with spectrum analyzers to capture the received signal strength from the neighbours, which is forwarded to the fusion center. We make the following assumptions to perform the analysis.

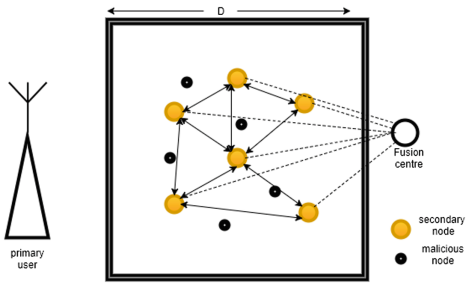

Fig. 1. Network with TV white space devices as back haul controlled by FC

2.1 Assumptions

I. There are N secondary nodes and M malicious nodes in the system.
II. Each secondary node, shall communicate to the fusion center using control channel.
III. Secondary nodes are static and do not change position.
IV. Secondary nodes are used as backhaul nodes to provide access network to rural communities
V. The primary user (transmitter) is at a minimum distance of $\sqrt{(x_q^2 + y_q^2)}$, where $q = 1, 2, 3, ..., \infty$, Such that x_q and y_q are position coordinates of a secondary node.

VI. The primary user transmits at the power of P_t, the secondary node at P_s and the malicious node at a P_m.
VII. The positions of the secondary nodes and the malicious nodes are uniformly distributed in the square of a side length of $(d)km$. They are statistically independent of each other.
VIII. Malicious nodes are randomly distributed.
IX. The received signal strength indicator values received by the fusion center are normally distributed random variables with mean μ and variance σ^2.
X. There is cooperation between the secondary nodes. Therefore a malicious node attack is analyzed collaboratively.
XI. Two access networks are connected to the backhaul network via access point device.
XII. The fusion center has Internet connectivity through a gateway node and therefore provides access to broadband internet through the backhaul secondary nodes to the users.
XIII. Each secondary node has an adaptive modulation scheme which offers the capability to increase the radio's receiver sensitivity.

2.2 Performance Metrics

We shall consider how malicious nodes affect throughput, latency and spectrum utilization of the network shown in Fig. 1. In computing the latency and the Throughput we assume that the transmitter is fully able to utilize the entire channel capacity. Also channel coefficient values are dependent on the transmission environment parameters such as, distance, antenna height, etc. But, The channel coefficients are independent on the Bandwidth. Coefficients were derived from the Hata propagation model.

Throughput is defined as the amount of data that can be transmitted through a given channel or link per second. It is measured in bits per second (bps) Given the bandwidth of the channel in the backhaul network as B. We arbitrary considered a bandwidth value of 100 MHz, this is because of the scenario of the backhaul nodes we considered. We assume that there are m secondary nodes in the network. The throughput can therefore be estimated as follows,

$$Throughput(TP) = Blog_2\left(\frac{|h_t|P_t}{|h_{int}|P_{int}+p_{miss}\sum_{m=0}^{M}|h_m|P_m+\sigma^2}\right), \quad (1)$$

where
h_t = transmitter coefficient
P_t = transmitter power
h_{int} = interference coefficient
P_{int} = interference power
h_m = malicious node interference coefficient
P_m = malicious node power

p_{miss} = miss detection probability
σ = additive white Gaussian noise.

Also, including the factor of the secondary nodes collaborating in the network, throughput will be given by:

$$Throughput(TP) = Blog_2\left(\frac{|h_t|P_t}{|h_{int}|P_{int}+p_{miss}\sum_{m=0}^{M}|h_m|P_m+\sum_{S=0}^{S}|h_s|P_s+\sigma^2}\right), \quad (2)$$

where
h_s = secondary node coefficient
P_s = secondary node power
σ = .additive white Gaussian noise

Latency is the time it takes for data transmitted by a sender to reach the intended receiver (destination). Considering Fig. 1, when user 1 sends message to user 4 on the other network with data size of (D)Mbps.

$$Latency = D\left[\frac{1}{TP_1}+\frac{1}{TP_2}+\frac{1}{TP_3}+...+\frac{1}{TP_q}\right], \quad (3)$$

where,
TP_q = Throughput for the link between the transmitter and the receiver, $\forall q$, $q = 1, 2, 3, 4, ..., n$. The latency is the sum of all the individual links delay because, the backhual nodes operate mesh routing protocol which may route packet through any of the links available and optimal at all times. We therefore assumed that packets travel through all the q links.

Spectrum utilization in simple terms is the usage of the spectrum. Both the secondary and malicious nodes sense the spectrum with a given probability of detection, miss-detection (Miss detection probability is when the transmission is made by the primary transmitter, but the secondary node assumes the transmission is made by the malicious node [8]) or false alarm (is when the actual transmission is made by the malicious node but the secondary node assumes the transmission is from the primary transmitter [8]) probabilities.

Let N be the set of secondary nodes that provide backhaul to the access point.

$$N = \{n_1, n_2, n_1, ..., n_\alpha\} \quad (4)$$

In addition, let C be the set of channels that can be used by the backhaul secondary nodes:

$$C = \begin{bmatrix} c_{n_1}^1 & c_{n_1}^2, ..., & c_{n_1}^\beta \\ c_{n_2}^1 & c_{n_2}^2, ..., & c_{n_2}^\beta \\ . & . & . \\ . & . & . \\ . & . & . \\ c_{n_\alpha}^1 & c_{n_\alpha}^2, ..., & c_{n_\alpha}^\beta \end{bmatrix}, \quad (5)$$

where $c^y_{n_x}$; $n_x \in N, y \in \beta$ is the y^{th} channel of secondary backhaul node n_x. Furthermore, let $p_{fa}(c^y_{n_x})$ be the false alarm probability of y in n_x. The spectrum utilization, S_1 derived as,

$$S_1 = \frac{\sum_{x=1}^{\alpha}\sum_{y=1}^{\beta}(1 - p_{fa}(c^y_{n_x}))B(c^y_{n_x})}{\sum_{x=1}^{\alpha}\sum_{y=1}^{\beta}B(c^y_{n_x})} \tag{6}$$

Considering presence of malicious node in spectrum utilization, let γ_{n_x} be the set of malicious nodes around secondary node in the backhaul n_x

$$\gamma_{n_x} = \{\gamma^1_{n_x}, \gamma^2_{n_x}, ..., \gamma^{\Phi}_{n_x}\} \tag{7}$$

Hence, with the malicious nodes present, spectrum utilization S_2 is given by (8)

$$S_2 = \frac{\sum_{x=1}^{\alpha}\sum_{y=1}^{\beta}(1-p_{fa}(c^y_{n_x}))B(c^y_{n_x}) - |\gamma_{nx}|p_{fa}(c^y_{n_x})B(\gamma_{nx})}{\sum_{x=1}^{\alpha}\sum_{y=1}^{\beta}B(c^y_{n_x})} \tag{8}$$

3 Results and Discussions

The values of the numerical parameters we considered for our simulation test are listed in Table 1. Also, miss detection and false alarm probability values were adopted from Jin et al. [8]. Statistically, we validated our simulation results by running about thirty different simulations tests by randomly varying various parameters within fixed ranges. The results presented by all the tests did not show any significant variation.

In Fig. 2, the throughput was obtained by varying miss probability values. Again, in Fig. 3 throughput depended on the variation in the number of malicious nodes present in the network. Also, In both Figs. 4 and 5, latency and spectrum utilization depended on the number of malicious nodes found in the network. Figure 6 we varied the number of secondary node nodes and kept some malicious nodes constant and plotted against the simulated throughput values obtained. And, in Fig. 7 we simulated the latency as we kept fixed the number of malicious nodes and varied the number of secondary nodes in the backhaul and lastly, Fig. 8 presents throughput against number of malicious nodes present in the network. We again simulated the network throughput by varying the number of secondary nodes with fixed number of secondary nodes in the backhaul nodes.

Figure 2 measures channel throughput against miss detection probabilities. Looking closely at the simulation results it shows that when miss detection rate was zero, two things were considered, that is, the malicious nodes may be present but do not cause any miss detection attacks, or there may be no malicious node found in the network. The throughput obtained by the simulation at zero miss detection rate was 0.136 Mbps. Also, at miss detection probability rate of 0.01, the throughput dropped to 0.082 Mbps which represents a percentage decrease of about 39% from when there was zero recording of miss detection, which shows

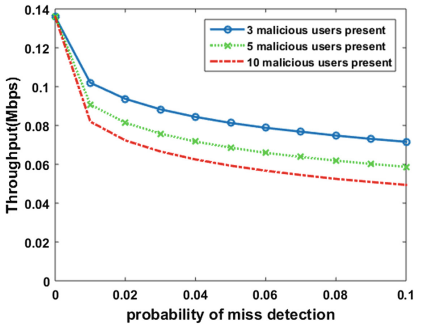

Fig. 2. Throughput versus miss detection rate

Table 1. Simulation parameters

Parameter	Value
Secondary power	(35–41) dBm
Malicious power	(33–38) dBm
Frequency	(470–790) MHz
Nodes density	1 to 10
Interference power	(4–11) dBm
Coefficient values	0.1 t0 2
Bandwidth	100 MHz
Data Size	100 MB

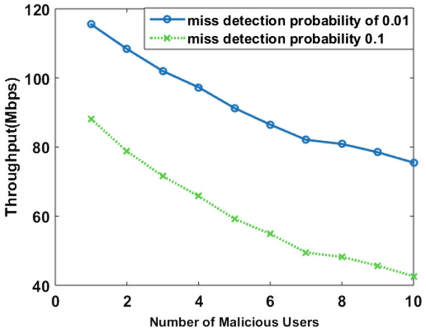

Fig. 3. Throughput versus number of malicious nodes present around the backhaul secondary nodes

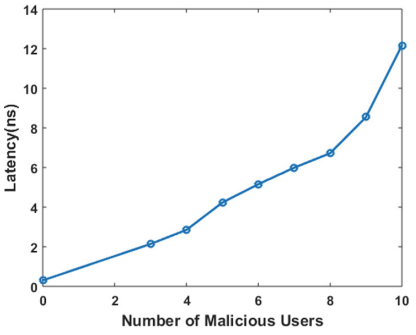

Fig. 4. Latency versus number of malicious nodes present around the backhaul secondary nodes

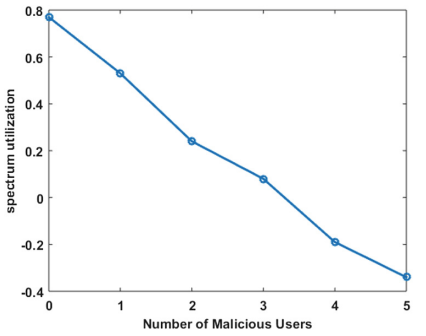

Fig. 5. Utilization versus number of malicious nodes around the backhaul secondary nodes

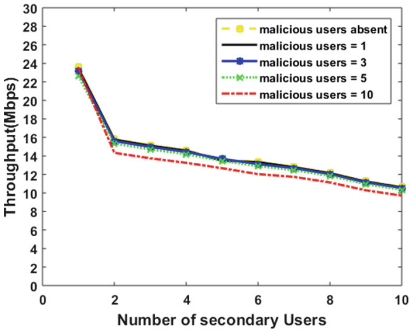

Fig. 6. Throughput versus density of secondary nodes around the backhaul secondary nodes

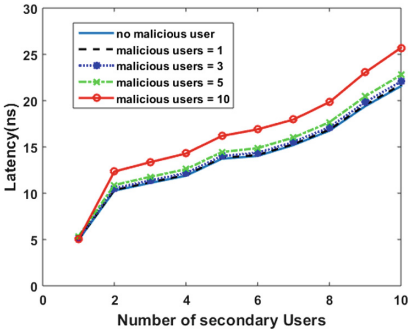

Fig. 7. Latency versus density of secondary nodes around the backhaul secondary nodes

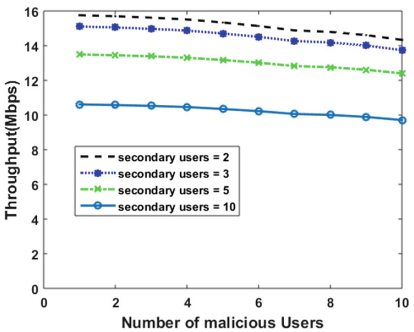

Fig. 8. Throughput versus number of malicious nodes present around the backhaul nodes

that at 99% detection the maximum quality of service can not be guaranteed. The same decrease trend was observed in the throughput with the number of malicious nodes of 3, 5 and 10 with varying miss detection rates. But there was a significant difference in the drop in throughput when the number of malicious nodes increases as shown in Fig. 2. Inversely, from Fig. 2 the result indicates that increased in miss detection probability directly decreased the value of the throughput.

In Fig. 3 throughput was also found to decrease with the increase in the number of malicious nodes in the network with constant miss detection rate. But the higher the miss detection probability value, the greater the drop in throughput as shown in Fig. 3. The miss detection probability of 0.1 recorded much decrease in throughput as compared to miss probability value of 0.01 as shown in Fig. 3.

We also considered an end-to-end effect of latency by the presence of malicious nodes on the network. End-to-end here refers to a user on a different network connected to our backhaul network, which is supposed to serve one community and another user on a different network connected to our backhaul network serving another community. We assume that user 1 on the network connected to secondary node say D sends a message to user 4 on the network connected to secondary node say C. The simulation result shows that when there was no malicious node present in the network, the delay recorded was 0.30 ns but once malicious nodes were introduced into the network, the latency increased as the number of malicious nodes also increased as shown in Fig. 4.

We further modeled and simulated spectrum utilization using different false alarm probability rate on various channels and using four fixed secondary nodes as backhaul nodes. We kept the false alarm probabilities constant for each channel and varied the number of malicious nodes. It was observed that it is not possible for the spectrum to hold more than three malicious nodes at a time

if the quality of service is to be guaranteed for the users on the network, as indicated in Fig. 5.

Moreover, we also varied the density of the secondary nodes in the network and kept the malicious nodes and the miss probability of 0.1 constant at all cases. We observed variations in throughput and latency, as shown in Figs. 6 and 7 respectfully. Considering Fig. 6 it could be deduced that increased in the number of cooperative secondary nodes reduced the throughput significantly from one secondary node present to two secondary nodes present. But, as the number of cooperative secondary nodes increased the variation in the throughput as against fixed number of malicious nodes present did not significantly affect the throughput (from two to ten cooperative secondary node). However, there was a significant increase in the latency as data traveled from one network to another network. For fixed ten malicious nodes as against no malicious node present among the backhaul nodes (the cooperative secondary nodes) recorded high increase. We also inferred that as the cooperative sensing nodes increase, malicious nodes combined effect on latency also reduced, as demonstrated in Fig. 7.

Again, Fig. 8 shows that when cooperative nodes of a size of 2, 3 *or* 5 secondary nodes considerably work better than 10 cooperative nodes, which indicates when the cooperative or collaborative nodes increase it affects the throughput of the network. We inferred that when the number of cooperative nodes increased, it introduced a lot of interference signals to the network. So, therefore, the lower the cooperative nodes, the lesser the network interference. Also, the lower the number of cooperative nodes are, the greater the performance (throughput) of the network. But the performance deteriorated when the number of cooperative nodes grew up to a size of 10 as shown in Fig. 8.

Our system model above is closest to the model adopted by Jin et al. [8], however, it failed to measure the performance metrics and utilization of the network. Again, their model considered only one secondary node with multiple malicious nodes. Also, their model was used to detect primary user emulation attack. However, In our model, we considered various numbers of secondary nodes as against multiple numbers of malicious nodes. Also, we varied the distances from all the secondary nodes to the primary transmitter based on their coordinate points (X and Y). Again, our work confirmed the research findings of Pinifolo et al. [11], that neighbour nodes within a distance range of 7 km produces interference to the neighbour nodes. However, we further showed that secondary nodes might be able to collaborate well by monitoring each node if malicious nodes are not existing in the network.

4 Conclusion

In conclusion, we have demonstrated through simulations that, the presence of malicious nodes in dynamic spectrum access networks downgrades the performance of the network. We further showed that densely collaborated nodes in DSA network might affect the performance of the network, as interferences are

introduced into the spectrum. Again, we demonstrated that, if malicious users are absent in the DSA network, neighbour monitoring collaborative network may be feasible to implement with fewer legitimate secondary nodes at a time. The malicious nodes present can significantly affect the authorized users, as the spectrum may occasionally appear to be fully utilized. The major limitation of this study is that, the interference factors used in the performance and the utilization models may not be realistic in real world application. In future, we shall undertake real world measurements to get actual impact of the malicious nodes on the performance of a DSA-based network. Again, we shall consider developing detection algorithm to identify the malicious nodes to reduce their impact on the performance of DSA-based collaborative networks.

References

1. Kaligineedi, P., Khabbazian, M., Bhargava, V.K.: Secure cooperative sensing techniques for cognitive radio systems. In: 2008 IEEE International Conference on Communications, pp. 3406–3410 (2008)
2. Yu, F.R., et al.: Defense against spectrum sensing data falsification attacks in mobile ad hoc networks with cognitive radios. In: 2009 Military Communications Conference, MILCOM 2009. IEEE (2009)
3. Chen, R., Park, J.-M., Bian, K.: Robust distributed spectrum sensing in cognitive radio networks. In: INFOCOM 2008, The 27th Conference on Computer Communications. IEEE (2008)
4. Mfupe, L., Mekuria, F., Montsi, L., Mzyece, M.: Geo-location white space spectrum databases: review of models and design of a dynamic spectrum access coexistence planner and manager. In: Mishra, A., Johnson, D. (eds.) White Space Communication, pp. 153–194. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-08747-4_6
5. Bouassida, M.S., et al.: Sybil nodes detection based on received signal strength variations within VANET. Int. J. Netw. Secur. **9**(1), 22–33 (2009)
6. Othman, A.K., Adams, A.E., Tsimenidis, C.C.: Node discovery protocol and localization for distributed underwater acoustic networks. In: 2006 International Conference on Internet and Web Applications and Services/Advanced International Conference on Telecommunications, AICT-ICIW 2006. IEEE (2006)
7. Takyi, A., Densmore, M., Johnson, D.: Collaborative neighbour monitoring in TV white space network. In: Proceedings Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2016), George, South Africa (2016)
8. Jin, Z., Anand, S., Subbalakshmi, K.P.: Detecting primary user emulation attacks in dynamic spectrum access networks. In: 2009 IEEE International Conference on Communications, ICC 2009. IEEE (2009)
9. Sharma, S.K., Chatzinotas, S., Ottersten, B.: Cooperative spectrum sensing for heterogeneous sensor networks using multiple decision statistics. In: Weichold, M., Hamdi, M., Shakir, M.Z., Abdallah, M., Karagiannidis, G.K., Ismail, M. (eds.) CrownCom 2015. LNICST, vol. 156, pp. 321–333. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24540-9_26
10. Jain, M., Kumar, V., Gangopadhyay, R., Debnath, S.: Cooperative spectrum sensing using improved p-norm detector in generalized κ-μ fading channel. In: Weichold, M., Hamdi, M., Shakir, M., Abdallah, M., Karagiannidis, G., Ismail, M.

(eds.) CrownCom 2015. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 156, pp. 225–234. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24540-9_18
11. Pinifolo, J., et al.: Successful deployment and key applications of television white space networks (TVWS) in Malawi. In: Proceedings and Report of the 7th UbuntuNet Alliance Annual Conference, pp. 347–354 (2014)