Trust Model-based Secure Cooperative Sensing Techniques for Cognitive Radio Networks

Deming Pang, Gang Hu, Ming Xu
School of Computer, National University of Defense Technology
Changsha, China
e-mail: pang3724@nudt.edu.cn, golfhg@vip.sohu.net, xuming-64@hotmail.com

***Abstract*—Cooperative spectrum sensing has been shown to enable Cognitive Radio (CR) networks to reliably detect licensed users and avoid causing interference to licensed communications. However, the performance of the scheme can be severely degraded due to presence of malicious users sending false sensing data. In this paper, we propose trust model-based cooperative sensing techniques to reduce the harmful effect of malicious users in cooperative sensing process. First of all, analysis model of anomalous behavior is devised to identify the malicious users. Then we employ PID (Proportional-Integral-Derivative) like controller to calculate the credit value of nodes, which is used as the weight of WBD (Weighted Bayesian Detection) to make spectrum decision. Simulation results demonstrate that, comparing with the existing methods, the proposed scheme performs better especially in the case that there exist a large number of malicious nodes.**

Keywords- Cognitive Radio Networks; Cooperative Spectrum Sensing; Trust Model; Weighted Bayesian Detection.

I. INTRODUCTION

Cognitive radio (CR) techniques provide the capability to use or share the spectrum in an opportunistic manner, which is proposed to solve current spectrum inefficiency problem [1]. In CR networks unlicensed users (secondary users, SUs) detect spectrum environment and utilize the idle spectrum while tolerable interference is guaranteed to the licensed users (primary users, PUs).

For CR networks, reliable spectrum sensing is an important step for any practical deployment. SUs should identify the presence of PUs over wide range of spectrum accurately without significant delay. This process is very difficult as we need to identify various PUs adopting different modulation schemes, data rates and transmission powers in presence of variable propagation losses, interference generated by other secondary users and thermal noise. Traditionally there are three spectrum sensing techniques, viz., energy detection, matched filter detection and cyclostationary feature detection [2]. If SUs are lack of knowledge about the characteristics of PU signal, energy detection is the optimal choice with the least complexity and generally adopted in recent research work. However, the performance of energy detection is always degraded because of signal-to-noise ratio wall or channel fading/shadowing [3].

Cooperation among SUs follows almost as a necessary consequence of the above constraints. Cooperative spectrum sensing has been shown to greatly increase the probability of detecting the PUs [4-6]. Each SU executes spectrum sensing by itself and sends the "local" spectrum sensing information to a DC (Data Collector) which uses an appropriate data fusion technique to make final spectrum sensing decision.

Since a DC utilises not only its own observations as a basis for decision making but also the observations of others, it is the obviously need to authenticate the shared observations. The DC needs to judge whether the observations from others are real or falsified. This is critical to prevent degradation of the network performance because of malicious behavior and to protect against the Byzantine attack. The Byzantine attack represents the case where a friend or acquaintance has, unbeknownst to the CR, become an adversary and represents the most difficult subset of this problem space. The Byzantine failure problem can be caused by malfunctioning sensing terminals or MUs (Malicious Users). They transmit false information instead of real detection results, which adversely affects the global decision.

This problem has been discussed in [7-9], and several methods were proposed to reduce the impact of false information. But these proposals failed when the proportion of MUs increased. In this paper, we investigate techniques to identify the nodes which provide false sensing information, and nullify their effect on the cooperative spectrum sensing system. By analyzing the behaviors of SUs in cooperative sensing, DC can establish trust model with PID (Proportional-Integral-Derivative) like controller [10], which can acquire relatively high speed to track the behaviors of neighbors. At last, we use a fusion technique called WBD (Weighted Bayesian Detection) derived from Bayesian detection to make spectrum decision. Simulation results show that this method improves the robustness of data fusion against attacks even when a large proportion of malicious users exist.

In Section II, we define the system model. In Section III, the proposed cooperative detection scheme is described in detail. Simulation results and analysis are illustrated in Section IV, and finally, a conclusion is given in Section V.

II. SYSTEM MODEL

In an ad hoc CR network, we consider a group of N second users in the presence of a primary user working on K different channels. The channels of PU and SUs use the HATA model for rural environments as the path loss model [11]. We assume perfect channel conditions for the control channel. Each of the SUs acts as a sensing terminal that is responsible for local spectrum sensing. The local detection results are reported to a DC that executes data fusion and makes the final spectrum decision. SUs use energy detector,

 ISBN:978-1-61208-113-7

and the sensing report is local sensing decision which is a binary variable— "1" denotes the presence of PU signal, and "0" denotes its absence. The data fusion problem therefore can be regarded as a binary hypothesis testing problem with two hypotheses represented by H1 and H0 (H1 means there exists primary user, and H1 means the channel is free). We consider three types of spectrum spoofing attacks: always-false, always-busy and always-free. An always-false attacker always sends spectrum reports that are opposite to its real local sensing results, and an always-busy attacker always notifies spectrum to be busy while an always-free attacker always reports contrary results.

III. TRUST MODEL-BASED SECURE COOPERATIVE SENSING

This Section will detail a reactive protection mechanism, a trust model-based cooperation enforcement mechanism to improve robustness of data fusion technique. First of all, the anomalous behaviors of malicious users should be identified. We design two kinds of behavior analysis models to track the behaviors of SUs. Based on that observation, a sensing terminal's reputation can be calculated with a PID-like trust model. Since the data fusion is a binary hypothesis testing problem, we propose a new technique called WBD to overcome the weakness of existing fusion techniques.

A. Analysis of Anomalous Behaviors

After receiving local reports of neighbors, DC should judge which one is believable, and make spectrum decision with appropriate reports. DC will get the ultimate sensing result *U* at the end of sensing period, which derives from *i* neighbors sensing *k* channels.

$$U=\begin{pmatrix} c_{11} & \cdots & c_{1k} \\ \vdots & \ddots & \vdots \\ c_{i1} & \cdots & c_{ik} \end{pmatrix}$$

where *U* is a $i\times k$ matrix which consists of 0 and 1, and c_{ik} is the sensing result of channel *k* detected by node *i*. $c_{ik}=1$ means there exists PU in channel *k*, and $c_{ik}=0$ means that channel *k* is free.

First of all, we focus on the analysis of abnormal sensing behaviors in single channel. $(c_{1j},\cdots,c_{mj},\cdots,c_{ij})$ is the sensing result of channel *j*. Without loss of generality, we assume the first *m* items are same, If $m>i/2$, *m* nodes correspond to these items are judged to be normal while the others are malicious. Different kinds of users will be assigned corresponding credit values with the following algorithm in Section B.

This is a kind of majority rule, which is feasible when the proportion of MUs is small. We consider CR networks with *N* SUs, among which *M* SUs are malicious. The false detection ratio with energy detection is α. The analysis of anomalous behaviors is effective under the condition

$$\begin{aligned} &\frac{(N-M)\cdot\alpha+M\cdot(1-\alpha)}{N}<50\% \\ &M<N/2 \end{aligned} \tag{1}$$

Since the correct detection ratio of energy detection is not ideal, the credit values of SUs calculated in single channel may not be assigned rightly (normal SU is regard as malicious node, whose credit value is decreased. v.v.). But in a sensing period multiple channels would be detected in the same way, and the credit value of each node will be updated in each channel. So the probability of miscalculation of credit value P_f could be shown as

$$\begin{aligned} P_f &= \sum_{i=\frac{k}{2}+1}^{k} P(a=i) \\ &= \sum_{i=\frac{k}{2}+1}^{k} C_k^i\cdot Q^i\cdot(1-Q)^{k-i} \end{aligned} \tag{2}$$

where *a* is the number of channels on which there exist trust misjudgment, and $P(a=i)$ means the probability that there exist *i* channels on which misjudgment is present. *Q* is the probability of misjudgment in single channel.

$$Q=P[H_1]\cdot P[0\,|\,H_1]+P[H_0]\cdot P[1\,|\,H_0] \tag{3}$$

Based on (2) (3), P_f would be very small when the regulation of evaluating sensing nodes' behavior is available, viz. the number of MUs is not more than SUs. (e.g., $k=20$, $Q=0.3$, we can deduce $P_f\approx 0.016$). So we can make a conclusion that the majority rule at multi-channel environment is effective in identifying malicious users.

When SUs have detected *k* channels in distributed manner in a sensing period, DC can deduce the numbers of available channels $M=(n_1,n_2,\cdots,n_i)$ from *i* different SUs where n_i is the number of available channels from the sensing report of node *i*. These numbers should be identical in theory, while difference always exists because of malfunction or intention of sensing nodes. For example, the number of available channels from the report of an always-busy attacker would be zero. In order to identify malicious behaviors by analyzing the numbers of available channels, *M* should be amended using prior probability to eliminate the infection of malfunction. We can make use of a proposal devised in paper [7] to get the prior probability in different channels.

$$\begin{aligned} P_{11} &= \begin{pmatrix} p_{1,1}^1 & \cdots & p_{i,1}^1 \\ \vdots & \ddots & \vdots \\ p_{1,k}^1 & \cdots & p_{i,k}^1 \end{pmatrix} = \left(P_1^1,P_2^1,\cdots,P_i^1\right) \\ P_{01} &= \begin{pmatrix} p_{1,1}^0 & \cdots & p_{i,1}^0 \\ \vdots & \ddots & \vdots \\ p_{1,k}^0 & \cdots & p_{i,k}^0 \end{pmatrix} = \left(P_1^0,P_2^0,\cdots,P_i^0\right) \end{aligned} \tag{4}$$

 ISBN:978-1-61208-113-7

where $p_{i,k}^1$, $p_{i,k}^0$ means the prior probability $P[1|H_1]$ and $P[0|H_1]$ of node *i* in channel *k* respectively. Thus DC can revise the number of available channels from each SU as follows

$$\begin{aligned} U &= (C_1,\cdots,C_i)' \\ E-U &= (D_1,\cdots,D_i)' \\ M &= (n_1,n_2,\cdots n_i) \end{aligned} \quad (5)$$

$$= \left(C_1\cdot P_1^1 + D_1\cdot P_1^0,\cdots,C_i\cdot P_i^1 + D_i\cdot P_i^0\right) \quad (6)$$

where E is a $i\times k$ matrix which consists of 1. Through comparing the number of available channels from any node *i* with DC *j*, we can distinguish malicious nodes among SUs as follows

$$\Delta n = \left|n_j - n_i\right|/k$$

$$\begin{cases} \Delta n > \beta, & \textit{node i behaviors anormally} \\ \Delta n < \beta, & \textit{node i behaviors normally} \end{cases} \quad (7)$$

where β is a threshold to distinguish the status of nodes.

B. PID-Like Trust Model

Considering that the sensing reports influence the allocation and accessing of spectrum resource directly, the credit values should track the behaviors of SUs rapidly in order to reduce the negative influence. On the other hand, energy detection is not ideal. Mistaken sensing reports may be send to DC by normal SUs which would be seen as malicious users. So the credit values should be modified in a smooth manner in order to avoid random mistake of normal SUs. We use a tuned PID controller in control systems to calculate the trust values of nodes [10]:

$$\begin{aligned} f(t) &= B(t) - V(t) \\ V(t) &= \alpha * \int_0^t f(t)dt \end{aligned} \quad (8)$$

Under the conditions:

$$B(t)\in\{0,1\}$$
$$V(t)\in[0,1],\ V(0)=1$$

In equation (8) $B(t)$ is an input which is the detected result of the neighbor's behavior, and $V(t)$ is the corresponding output. The right of the lower equation refers to the record of history about difference. According to the control theory, the input is zero order signal, and the controller can track the input in time and get no static difference. So this model can trace the behaviors of the neighbors at a higher speed and attain a smooth change of trust value. Based on (8) we can deduce

$$V(t) = e^{-\alpha\cdot t}, \quad t\ge 0 \quad (9)$$

Equation (9) can be used to calculate the parameter α .

In order to utilize this trust model, equation (8) is discretized as a discrete equation which is shown in Equation (10).

$$\begin{aligned} f_i^j(k+1) &= B_i^j(k+1) - V_i^j(k) \\ V_i^j(k+1) &= \alpha * \sum_{n=0}^{k+1} f_i^j(n) \\ \alpha * f_i^j(0) &= 1 \end{aligned} \quad (10)$$

where $V_i^j(k+1)$ denotes the trust value of node *i* in sensing period $k+1$ recorded in DC *j*. The others have the similar meanings corresponding to those in equation (8).

$$B_i^j(k) = \begin{cases} 0, & \textit{If node i behaviors anormally at period k} \\ 1, & \textit{If node i behaviors normally at period k} \end{cases}$$

In addition, we define a threshold of trust value V_T to indicate whether DC should believe its neighbors. Using V_T and *N* to substitute *V*(*t*) and *t* in equation (9) respectively, we can deduce the parameter α as

$$\alpha = -\frac{\ln V_T}{N} \quad (11)$$

where *N* is the number of steps in which the trust value changes from 1 to V_T when the input is always 0 after certain time point, defined as the speed to trace the behaviors of neighbors. *N* can be figured out approximately as

$$P^N < P_{toler} \quad (12)$$

where *P* is the incorrect detection probability performing energy detection, P_{toler} is the tolerated misidentify probability.

C. Weighted Bayesian Detection

When DC has received sensing reports, it needs to employ an appropriate fusion technique to make an accurate spectrum sensing decision. We apply a likelihood ratio test named WBD on data fusion. WBD is based on Bayesian detection [12], which is a hypothesis test for sequential analysis.

It requires the knowledge of prior probabilities of r_i 's when *r* is 0 or 1, i.e., $P[r_i|H_0]$ and $P[r_i|H_1]$. It also requires the knowledge of a prior probabilities of *r* , i.e., $P_0 = P[r=0]$ and $P_1 = P[r=1]$, which can be acquired with the method proposed in [7].

WBD can be represented by the following test, which inputs the sensing reports r_i of neighbors i and outputs a final spectrum sensing decision Γ.

$$\Gamma = \prod_{i=0}^{m} \left(\frac{P[r_i \mid H_1]}{P[r_i \mid H_0]} \right)^{V_i}$$
$$\begin{cases} \Gamma \geq \lambda \Rightarrow & accept\ H_1 \\ \Gamma < \lambda \Rightarrow & accept\ H_0 \end{cases} \quad (13)$$

where λ is a threshold calculated from

$$\lambda = \frac{P_0(C_{10} - C_{00})}{P_1(C_{01} - C_{11})} \quad (14)$$

where $C_{jk}(j = 0,1; k = 0,1)$ is the cost of declaring H_j true when H_k is present.

IV. SIMULATION

A. Simulation Environments

The simulation was run in MATLAB, and the same system environment with [7] was deployed to obtain comparable simulation results. The only difference was that we realized the simulation with multi-channel model. We compared three kinds of data fusion schemes, i.e., Bayesian detection, WBD and WSPRT [7]. We consider an ad hoc CR network with one PU as well as *N* SUs, among which *M* SUs are malicious. The primary user, a TV tower has twenty 6MHz channels in TV band, and the duty cycle of all the channels is fixed at 0.2. It locates D meters away from the center of the CR network. *N* SUs locate in a 2000m×2000m square area randomly, and follow a random waypoint movement model with a maximum speed of 10m/s and a maximum idle time of 120s. The transmission range of SUs is 250m. Three types of malicious nodes (always-busy, always-false and always-free) are same with normal SUs except reporting forged sensing reports. The layout of the simulated network is shown in Figure 1.

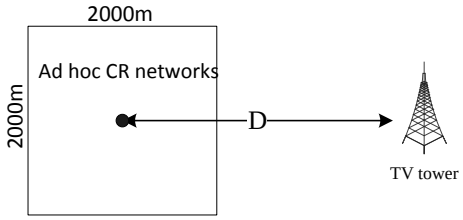

Figure 1. Simulation layout.

We use the HATA model for rural environments to calculate the path loss [11]. The values of the system parameters are listed in Table 1.

TABLE I. VALUES OF PARAMETERS USED IN THE SIMULATION

Parameter	Value
D	3000m
N	300
M	10,20,…,100
β	0.25
V_T	0.4
P_{toler}	0.01
P	0.3
PU antenna height	100m
SU antenna height	1m
transmitter power	100kW
receiver sensitivity	-94dbm
noise power	-106dbm

B. Simulation Results and Analysis

The threshold λ of Bayesian detection and WBD is calculated from (14), we first assume the perfect knowledge of P_0 and P_1, i.e., $P_0 = 0.8$ and $P_1 = 0.2$. The costs are assigned as: $C_{00} = C_{11} = 0$, $C_{10} = 1$, and $C_{01} = 10$. With these values, we can get $\lambda = 0.4$. Because the accurate knowledge on P_0 or P_1 may not be available, we simulated other threshold $\lambda' = 4\lambda = 1.6$. Another simulated fusion technique is WSPRT, the values of the parameters are the same with [7] except we deploy larger proportion of MUs.

We compare the performance of the three data fusion techniques. The metrics are correct sensing ratio, miss detection ratio and false alarm ratio, which add up to one. So we just focus on the first two metrics.

The number of malicious nodes increased from 0 to 100 at an interval of 10 in the three different attacks. Figures 2-4 show the simulation results when we consider always-busy, always-false and always-free attacks respectively. In all case, the correct sensing ratios of three types of data fusion techniques are more than 90% when the number of attackers is less than 30, which is acceptable based on the regulation of IEEE 802.22. But the performances diverge severely for the Bayesian detection with the number of MUs increasing, while the WBD is the most robust against attacks. The correct sensing ratios are above 80% with our proposed WBD under three types of attacks even the proportion of MUs is close to 1/3, while the miss detect ratios are acceptable at the same time. This shows that the trust model-based weight scheme has taken effect. WSPRT [7] employs similar weighted scheme with different trust evaluation strategy. It can reduce false information to a certain extent. But the increasing of malicious proportion would disturb the weight assignation in WSPRT, and finally, it largely increases the false alarm ratio.

It can be observed in Figure 4(a) that all the data fusion techniques perform stable under always-free attack, which increase miss detection ratio and decrease false alarm ratio. Figure 4(b) shows that the miss detection ratio is larger than other attacks.

 ISBN:978-1-61208-113-7

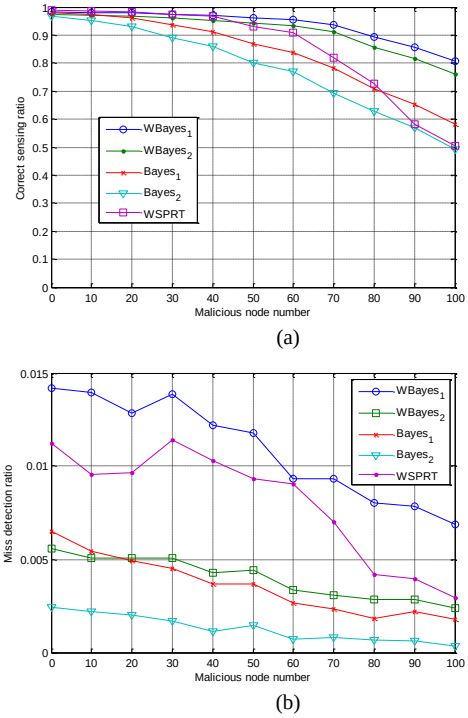

Figure 2. The performance of three fusion techniques with different number of always-busy attackers: (a) correct sensing ratio, (b) miss detection ratio. $\lambda = 0.4$: WBayes1, Bayes1; $\lambda' = 1.6$: WBayes2, Bayes2

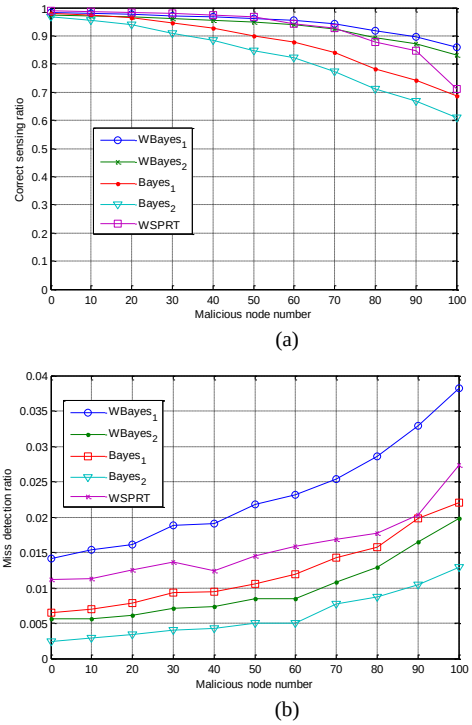

Figure 3. The performance of three fusion techniques with different number of always-false attackers: (a) correct sensing ratio, (b) miss detection ratio.

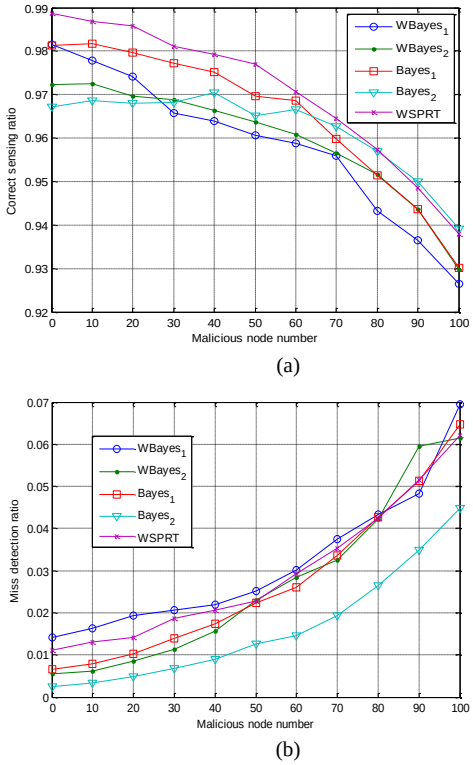

Figure 4. The performance of three fusion techniques with different number of always-free attackers: (a) correct sensing ratio, (b) miss detection ratio.

V. CONCLUSION

In this paper, we design two analysis models to identify anomaly behaviors in cooperative sensing process, and a PID trust model is employed to assign the credit value of SUs which can trace and nullify the malicious nodes rapidly. Simulation results demonstrate that comparing with the existing method the proposed scheme performs better especially in the case that there exist a large number of malicious nodes. In the behavior analysis model and data fusion technique the prior probability values play a key role, but the calculation of that needs many priori messages about the CR networks which may limit the deployment of the secure cooperative sensing techniques.

ACKNOWLEDGMENT

This work is supported by China NSF project No.61070211.

REFERENCES

[1] J. Mitola, "*Software Radio Architecture,*" John Wiley & Sons, 2000.

[2] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks : A survey," Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 50, Issue 13, September 2006, pp. 2127-2159.

[3] J. Unnikrishnan and V. Veeravalli, "Cooperative spectrum sensing and detection for cognitive radio, " in *IEEE Global*

Telecommunications Conference, GLOBECOM, Nov. 2007, pp. 2972 −2976.

[4] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN'05)*, Baltimore, USA, Nov. 2005, pp. 131−136.

[5] S. M. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE Int. Conf. Commun.*, Turkey, June 2006, vol. 4, pp. 1658−1663.

[6] G. Ganesan and Y. G. Li, "Cooperative spectrum sensing in cognitive radio−part I: two user networks," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 2204−2213, June 2007.

[7] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proceedings, INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, Apr. 2008. 1876-1884.

[8] P. Kaligineedi, M. Khabbazian, and V. K. Bharava, "Secure Cooperative Sensing Techniques for Cognitive Radio Systems," IEEE International Conference on Communications, May 2008, pp.3406-3410.

[9] T. Zhao and Y. Zhao, "A New Cooperative Detection Technique with Malicious User Suppression", IEEE International Conference on Communications, June 2009, pp,1–5.

[10] Z. Zhang, W. Jiang, and Y. Xue, "A Trust Model Based Cooperation Enforcement Mechanism in Mesh Networks", Proc. of the 6th International Conference on Networking (ICN), 2007, pp, 28-33.

[11] T. S. Rappaport, Wireless communications: principles and practice, vol.201. Prentice Hall PRT New Jersey, 1996.

[12] L. Lu, S.-Y. Chang, J. Zhang, L. Qian, J. Wen, V. K. N. Lau, R. S. Cheng, R. D. Murch, W. H. Mow, and K. B. Letaief, Technology Proposal Clarifications for IEEE 802.22 WRAN Systems, Mar. 2006. available at: http://www.ieee802.org/22/. [retrieved: September 14, 2010].

 ISBN:978-1-61208-113-7