**International Journal of Pure and Applied Mathematics**
**Volume 118 No. 24 2018**
ISSN: 1314-3395 (on-line version)
**url:** http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

# Performance Analysis of Secure Communication over a Cooperative Cognitive Radio Network

Namita Madhira, Dakshita Kumar, Raktim Dutta, T.Deepa
Dept. of Telecommunication Engineering,
SRM Institute of Science and Technology,
Kattankulathur, Chennai, India.

April 23, 2018

**Abstract**

In the existing model of a Cooperative Cognitive Radio Network (CCRN) based on Orthogonal Frequency Division Multiple Access (OFDMA), information is sent in 2 ensuing time slots, giving any existing passive hackers two opportunities to listen in. During slot one; the passive hackers can listen when information is transmitted to the secondary users from the Primary Base Station (PBS). In slot two, the eavesdroppers are given a chance when the SUs transmit to the secondary base station (SBS) and obscure Primary Users (PUs). It is presumed that the eavesdroppers use a diversity technique called the maximal ratio combining technique on the signals received. The SUs behave as relays to transmit information to PUs which are outside the transmitting range of the PBS. Hence, the SUs are given a part of the free spectrum from the legitimate PUs for its own transmission, as repayment. Also, the SUs are allotted and given the free spectrum only if they help the PUs satisfy the demand for secure communication.

Therefore, we propose to analyse the performance of secure communication over a cooperative cognitive radio network system, where multiple eavesdroppers are present in

the vicinity. The scheme will first be simulated in the form of a performance analysis, using the decode-and-forward (DF) relay. Subsequently, the more efficient, filter-and-forward (FF) relay, which not only avoids signal power leakage, but also reduces the noise power, will be adopted. Furthermore, the scheme will take a more practical approach by only assuming the channel distribution information of the eavesdroppers. Additionally, since it is assumed that eavesdroppers use the MRC technique to learn of the signals, non- MRC solutions will be looked into and an optimal solution will be adopted.

# 1 INTRODUCTION

There exists an overall dearth is available spectrum, making spectrum leasing via cognitive radio networks (CRNs) [1] the optimal solution. CRNs ensure an efficient use of bandwidth by allowing a set of unlicensed secondary users make use of any additional spectrum owned by licensed primary users [2]. The structure of the system is based on the concept of cooperative cognitive radio networks where the licensed primary users lease some of their additional spectrum to unlicensed secondary users in exchange for some services [3 - 11].

The data transmitted over a wireless channel is susceptible to attacks from illegal eavesdroppers. This is due to the fact that a wireless channel is a broadcast channel. Layer one (physical layer) security is the prime requirement of a system to ensure dynamic security during communication [14]. Profitable physical layer security approaches like cooperative jamming and cooperative communication are discussed by the authors of [15], [16] and [17]. Cooperative cognitive radio networks not only makes the most effective use of the spectrum, but can also be taken as the prime model to enhance secure communication [18] - [22]. The non-cooperative users are asked to send a friendly jamming signal to boost the privacy of the legitimate user. The non-cooperative users are then repaid with access to some of the network resources. The SUs are remunerated with entry into the network and its resources. In the second plan, a PU takes the assistance of two SUs. One SU works as a cooperative relay while the other works as a cooperative jammer. Together they work to increase the level of privacy the PU can get.

As remuneration, the SUs are given a time slot to send their own data.

We propose a system model in which a primary network (PN) has a primary base station (PBS) that needs to send information to several primary users securely. There exist a set of static hackers or eavesdroppers that can gain access to the information as well as the spectrum. Additionally, a secondary network (SN) consisting of secondary users (SU) wants to communicate with the secondary base station (SBS). The PN, which is the legal owner of the resources, enlists the cooperation of the SUs to transmit its information to distant PUs in exchange for some of its resources. The SUs behave as DF relays to relay the information from the PBS to the distant PNs. To achieve total secrecy of the information, the SUs need to be secured as well. The transmission takes place in two consecutive time slots.

It is assumed that the legal users have knowledge of the channel distribution information (CDI) of all the legal channels. Also, in this proposed scheme, the CDIs of the eavesdroppers are taken as known. This makes the system more practical as it is difficult to gain access to the channel state information (CSI) of the unknown eavesdroppers. CDI if the eavesdropper can simply be got from estimating the total path-loss. There exists some CDI imperfectness in the channel due to fading, large scale channel variations and fluctuations. The effect of this imperfectness is estimated using Kernel Density Estimation (KDE) and its robust counterpart, robust kernel density estimation (RKDE) [26], [27]. The proposed scheme is taken as an optimization problem and solved using Lagranges dual method. Here, the primal objective is to magnify the privacy of the secondary users and thereby achieving the dual objective, the minimum secrecy requirement of the primary users. It is assumed that the eavesdroppers use the maximal ratio combining (MRC) approach on the signals in the first and second time slots. Hence, a non- MRC approach is taken to ensure maximum efficiency. By using the Lagrange dual method, we are able to determine which SUs perform the relay function, which sub-carriers are to be allotted for transmission and how much transmitter power will provide optimal solutions.

Furthermore, while this proposed scheme uses DF relays, we also analyze the performance of the Filter and Forward relaying

scheme. The FF relaying scheme is an improved relaying technique that not only avoids signal power leakage, but also reduces noise power. It also achieves a higher SNR compared to both AF and DF relaying schemes. Hence, we also analyze the secrecy rate of the primary users where the secondary users work as filter and forward relays.

This paper is organized as follows: Section 2 depicts the system model and presents our resource allocation methods. Decode and forward relaying is defined in Section 3. Section 4 looks into the optimization problem and Lagrange dual solution. The effect of CDI imperfectness and the KDE solution is studied in Section 5. Section 6 examines the Filter- and Forward relaying scheme. The simulation results are presented in Section 7, and Section 8 is dedicated to our conclusion.

# 2 SYSTEM MODEL AND BASE FORMULAE

A. System Model

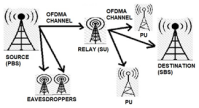


**Fig. 1: System Model of a CCRN using OFDMA as the channel**

We take into account a CRN which uses OFDMA as a channel to transmit its information. We suspect the presence of several passive hackers within the vicinity of the system, who are all eavesdropping on the data being transmitted within the network independently.

We denote the group of Primary Users (PUs) as $U_p = \{1, \ldots, U_p\}$, the group of Secondary Users (SUs) as $U_s = \{1, \ldots, U_s\}$, group of sub-carriers is denoted as, $N_s = \{1, \ldots, N_s\}$, and the group of eavesdroppers by Ev = $\{1, \ldots, \text{Ev}\}$. The SUs are segregated in two groups: first group is denoted by Ucs = 1. . . Ucs, that integrates cooperating secondary users (CSUs), which are earmarked as the PBS aids. The unused SUs, transfer their own data, designated by Us = Us  Ucs.

The proceeding of each network is ruled and operated by a central network controller (CNC) that has the entire knowledge of the system criterion of the legal receivers, e.g. their CSIs.

The CNC is presumed to allot sub-carriers in an orthogonal manner. We also presume that it has no knowledge of the CSI of the eavesdroppers.The free secondary sub-carriers amongst the SUs at an instant in the second time interval transmit their own data to the SBS . The notation: sub-carrier pair (SP) (m, n) is employed to imply that the sub-carrier m is employed by the PN within the 1ststst time slot and n is employed by the SN within the 2nd time slot for primary transmission. The passive listeners are presumed to use the MRC diversity technique over the carriers that are received in the 1st and 2nd intervals of time for every individual PU. Hence, we conform to non-MRC solutions in the system. The current system scheme is formulated as an optimization problem and solutions called energy conservation solutions are adopted to be the most optimal ones to solve the problem. As the relays (SUs) are widely dispersed, it is conjectured that the eavesdroppers in that vicinity can gain maximum knowledge of information when they overhear the PBS in the initial time interval. In order to make the system more practical, we only take the eavesdroppers Channel Distribution Information (CDI) into consideration as details of the Channel State Information (CSI) wouldnt be accessible to the legitimate users. Any persisting CDI imperfectness is estimated by Kernel Density Estimation (KDE) and Robust Kernel Density Estimation (RKDE).

Furthermore, in our proposed system model we will first be simulating and scrutinizing the Decode and Forward (DF) relay scheme, followed by an analysis of the Filter and Forward (FF) relay scheme.

The parameters that are taken into consideration are,

I The number of sub-carriers (Ns)

II The number of primary users (PUs)

III The number of secondary users (SUs).

IV The number of eavesdroppers (Ev)

V The channel gains

VI The transmission power

VII The rate of transmission

VIII The rate of secrecy.

B. Base Formulae
The normalized channel gains are given as,

$$g^m_{b_pU_{cs}} = \frac{|h^m_{b_pU_{cs}}|^2}{(\delta^m_{U_s})^2} \tag{1}$$

$$g^n_{U_{cs}U_p} = \frac{|h^m_{U_{cs}U_p}|^2}{(\delta^n_{U_p})^2} \tag{2}$$

$$g^k_{U_sb_s} = \frac{|h^k_{U_sb_s}|^2}{(\delta^k_{b_s})^2} \tag{3}$$

$$g^m_{b_pe} = \frac{|h^m_{b_pe}|^2}{(\delta^m_e)^2} \tag{4}$$

$$g^k_{U_sE} = \frac{|h^k_{U_sE}|^2}{(\delta^k_E)^2} \tag{5}$$

Where $h^a_b$ are the channel coefficients and $\delta^c_d$ represent the powers of the additive white Gaussian noise (AWGN) for the following cases respectively:

1. Between PBS (bp) & CSU (Ucs), over subcarrier m.
2. Between CSU & PU (Up), over subcarrier n.
3. Between SU (Us) & SBS (bs), over the subcarrier k.
4. Between PBS & the eavesdropper (Ev) over subcarrier m.
5. Between SU & the eavesdropper over subcarrier k.

The amount of power to be transmitted is assigned by the following for the respective cases:

• The PBS to CSU by subcarrier m during the initial time interval is denoted as: $p^m_{bpUcs}$

• The CSU to PU by subcarrier n during the 2nd time interval is denoted as:$p^n_{UcsUp}$

• The SU to SBS by subcarrier k during the 2nd time interval is denoted as:$p^k_{Usbs}$

The instantaneous rate of transmission between:

• PBS & CSU by the sub-carrier m during the initial time interval is denoted as:

$$R^m_{b_pU_{cs}} = \frac{1}{2}\log(1 + g^m_{b_pU_{cs}} p^m_{b_pU_{cs}}) \tag{6}$$

• CSU & PU y the sub-carrier n during the succeeding time interval is denoted as:

$$R^n_{U_{cs}U_p} = \frac{1}{2}\log(1 + g^n_{U_{cs}U_p} p^n_{U_{cs}U_p}) \tag{7}$$

The speed at which data is forwarded by the PBS to the PU in cooperation with the CSU, employing SP (m, n), is denoted as:

$$R^{mn}_{U_csU_p} = min(R^m_{b_pU_cs}, R^n_{U_csU_p}) \tag{8}$$

The level of secrecy achievable by the PBS while transmitting to the PU through the CSU employing SP(m,n) is denoted by:

$$S^{mn}_{U_{cs}U_p} = min_{e\varepsilon\epsilon}[R^{mn}_{U_{cs}U_p} - R^m_{bpe}]^+ = [min(R^m_{b_pU_{cs}}, R^n_{U_{cs}U_p}) - max_{e\varepsilon\epsilon}(R^m_{b_pe})] \tag{9}$$

# 3 DECODE AND FORWARD RELAY SCHEME

The DF relay scheme is employed over the Amplify and Forward (AF) relay scheme as it reduces the additive noise at the relay. In fig.2, it can be seen that the relays digitally transmit the information. The signal is sent from the source and received by the relay node, which decodes the received signal, re-encodes it and then forwards it to the destination. A DF relay can be referred to as a layer 2 relay as it provides a layer of security as compared to the AF relay. The speed at which secrecy is attained through DF relaying by the CSU and SP (m, n) is denoted by,

$$S^{mn}_{U_{cs}U_p} = [R^{mn}_{U_csU_p} - max_{e\varepsilon\epsilon}(R^m_{bpE})]^+ =$$

$$[\frac{1}{2}\log_2(1 + \frac{g^m_{bpUcs} g^n_{UcsUp}}{g^m_{bpUcs} + g^n_{UcsUp}} p^{mn}_{bpUcsUp}) - \frac{1}{2}\log_2(1 + max(g^m_{bpE}) p^m_{bpUcs})]^+ \tag{10}$$

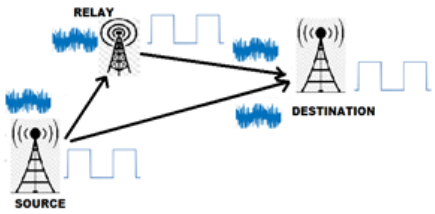


**Fig.2: Decode and Forward Relay Schematic**

# 4 OPTIMIZATION PROBLEM AND LAGRANGE SOLUTION

The entire scheme is examined as an optimization problem. The solutions are thus chosen based on their ability to appease the circumstances are referred to as energy conservative solutions.

The optimization problem of this scheme is solved using the Lagrange dual approach.

The dual solution can be looked at in two ways: through the primal problem or the dual problem.. Identical solutions to the primal and dual problems are not necessary. The dual scheme state that one of the solutions is to be maximized which is undoubtedly minimizes or ensures the minimum constraint of the other solution or vice-versa.

The objective of the proposed system is to achieve a higher total average level of secrecy for the SUs while undoubtedly achieving the required average level of secrecy for the PUs i.e. The need for secrecy of the SUs are maximized while ensuring that the PUs get the minimum level of secrecy.

Here, the non-MRC schemes for the system are proposed. The non-MRC solutions depend on the channel power gains. The channel gains are exponentially distributed as we consider the Rayleigh fading scenario. The average level of secrecy for the SUs while transmitting to the SBS using sub-carrier n, in the 2nd time interval is denoted by,

$E\{S^n_{Usbs}\} = E\{[\frac{1}{2}\log_2(1+g^n_{Usbs}p^n_{Usbs}) - \frac{1}{2}\log_2(1+\tilde{g^n_{Use}}p^n_{Usbs})]^+\} = \int_0^\infty \int_0^{g^n_{Usbs}} (\frac{1}{2}\log_2(1+g^n_{Usbs}p^n_{Usbs})$

$$-\frac{1}{2}\log_2(1+\tilde{g^n_{Use}}p^n_{Usbs}) \times f_{\tilde{g^n_{Use}}}(\tilde{g^n_{Use}}) f_{\tilde{g^n_{Use}}} f_{g^n_{Usbs}}(g^n_{Usbs}) d_{\tilde{g^n_{Use}}} d_{g^n_{Usbs}} \quad (11)$$

Where, $g_{Use}^{\sim n} = max_{e\varepsilon\epsilon} g_{Use}^{n}$ and $f_{g_{use}^{\sim n}}(g_{Use}^{\sim n})$ are the probability density functions (PDF) of the random variable, $g_{Use}^{\sim n}$.

The sub-carrier allocation is performed using the following formulae:

From the CSU (Ucs) and PUs (Up):

$$\varphi_{U_{cs}U_p}^{mn1} = \theta_{U_p} E\{S_{U_{cs}U_p}^{mn}\} - \lambda_0 E\{p_{b_p U_{cs}}^{m}\} - \lambda_{U_{cs}} E\{p_{U_{cs}U_p}^{n}\} \quad (12)$$

From SUs (Us):

$$\varphi_{U_{cs}}^{n} = E\{S_{U_s b_s}^{n}\} - \lambda_{U_{cs}} E\{p_{U_{cs}U_p}^{n}\} \quad (13)$$

# 5 CDI IMPERFECTNESS AND KDE SOLUTION

In order to simulate and compare the imperfect CDI effect, we consider an actual plot where we take actual noise samples received from the channel from which we assume the corresponding CDI which could be inexact. The performance of the obtained imperfect CDI is then assessed. CDI imperfectness can be evaluated in two ways: nonparametric and parametric.

In the parametric method, the equivalent parameters of an already assumed distribution are estimated [28]. However, we consider the nonparametric method in our model so as to not be restricted to a particular distribution. In the nonparametric method, the samples received from the channel are used to approximate the distribution, which is treated as completely unfamiliar. Kernel Density Estimation is adopted, as the basic Histogram Estimation provides non-discrete and open results. [29]. In a practical case, the measured samples contain some noisy and insignificant data. Therefore, a robust estimation method is taken in to obtain a satisfactory estimation despite the presence of corrupt samples.

A. Parametric:

Here, while it is presumed that the PDF has an already established distribution, the parameters are undiscovered. Maximum likelihood (ML) estimation [30] can be used to estimate the parameters. For our scheme, the exponential distribution is represented as,

$$f(x) = \frac{1}{x} exp(\bar{x}) \tag{14}$$

Where, $\bar{x}$ is the mean that can be evaluated using ML estimation. For ML estimation, is the mean is given by, $\hat{\bar{x}} = \frac{1}{Z}\sum_{i=1}^{\acute{z}} x_i$ , where $\hat{\bar{x}}$ is the estimated mean and $X = \{x_1, x_2 \cdots x_z\}$ are the samples using $\acute{z}$ samples.

B. Non-Parametric:

Kernel Density Estimation (KDE): The kernel density estimate of f(x) is denoted by $f_{KDE}(x) = \frac{1}{Z}\sum_{i=1}^{z} k_\delta(x, x_i)$, where $k_\delta(x, x_i)$ is the kernel function and $x_1, , x_Z x_i \varepsilon R^d$ is the set of samples that estimate a random vector, x having density f(x). Z illustrates the number of observation vectors.

The most familiar kernel function is,

$$k_\delta(x, x_i) = (\frac{1}{\sqrt{2\pi\delta}})^d exp(-\frac{(\|x - x_i\|)^2}{2\delta^2}) \tag{15}$$

The smoothing factor, , represents the bandwidth. Robust Kernel Density Estimation (RKDE): When data that consists of realizations from both minimal and coherent distribution as well as anomalous measurement, the data is said to be contaminated. In order to estimate this corrupted samples, a robust form of KDE needs to be employed. The form of RKDE [23], [24] is

$$\hat{f}_{KDE}(x) = \sum_{i=1}^{z} w_i k_\delta(x, x_i) \tag{16}$$

Where, $k_\delta(x, x_i)$ is the kernel function,$w_i$,$\bigtriangledown_i$ are non-negative weights whose sum is one i.e. $\sum_{i=1}^{z} w_i = 1$.

# 6 FILTER AND FORWARD RELAY SCHEME

An efficient improvement to the current schemes is the filter and - forward technique. FF relaying not only avoids signal power leakage, but also reduces the noise power. It also achieves a higher SNR in comparison with AF and DF relays.

The filter of the relay is designed to be similar to that of a FIR and IIR filter. In our design for filter and forward, we make use of

the hamming window. This ensures that the signal power doesnt leak while also reducing the noise power. The incoming signal is chipped off at the filter based on the constraints of the FIR or IIR filter. The rest of the signal is directly forwarded to the destination.

The filter and forward relay approach is given by,

$$f(w) = \sum_{l=0}^{L_f-1} f_l e^{-j\omega l} g(w) = \sum_{l=0}^{L_g-1} g_l e^{-j\omega l} \tag{17}$$

Where f(w) and g(w) are the filter coefficients similar to those of IIR and FIR filters.

# 7 SIMULATION RESULTS

Using simulations, we appraise the working of the designed system. The channels of the sub-carriers are independent and identically distributed and undergo Rayleigh fading. Assuming identical noise power at the eavesdropper nodes, the relay, and, the termination point, we achieve,$\sigma_p^2 = \sigma_s^2 = \sigma_e^2$

While evaluating the work of the designed system, we deal with imperfect CDI. Also, we calculate the number of observations required to approach an output resembling perfect CDI. The minimal data is achieved with exponential distribution and to obtain the eccentric data, we use Gaussian RV generation function nil mean and variance as unity, i.e. N (0, 1).

To obtain a random variable that doesnt have a definite formula for inverse CDF function, we use the acceptance/rejection method. For our case, in both interference and secondary channels, the actual density g(x) is studied to be exponential and having rate as 1.

The simulation specifications are listed in Table 1.

Table 1: Simulation Setup

| Parameters | Value |
|---|---|
| No. of Realizations | 1000 |
| Bandwidth | 10MHz |
| Average Path Loss | 35.3+37.6 log(d) |
| Fading Model | Rayleigh |
| Total no. of Subcarriers | 64 |
| Cell radius | 1Km |

A. Variation of Level of Secrecy of Primary and Secondary User Systems based on Number of Eavesdroppers.

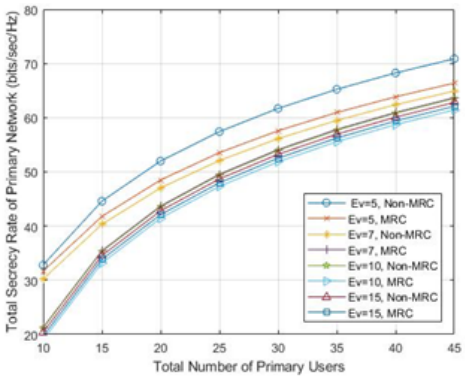


Fig. 3: Analysis of level of secrecy for PUs for both MRC and non-MRC methods for different number of eavesdroppers. Specifications: Ns= 64, Su= 11, Pp = 30dBm, PUs = 15dBm, RUp = 2 bits/sec.

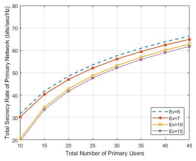

Fig. 4: Analysis of level of secrecy for PUs for different number of eavesdroppers Specifications: Ns= 64, Su= 11, Pp= 35 dBm, PUs = 20 dBm, RUp = 2 bits/sec

Fig.3 represents the total amount of privacy the primary users achieve against the number of PUs, for varying collection of eavesdroppers, Ev. As illustrated, raising the amount of PUs raises the

total level of secrecy of the users. It can be noted that the total level of secrecy of the PUs when the eavesdroppers adopt MRC is less than when MRC is not adopted. This is because, by using MRC, the eavesdroppers can gain more knowledge from genuine users as opposed to an instance when MRC is not used. Fig. 4 illustrates the total amount of privacy achievable by the SUs against the number of SUs; for varying number of eavesdroppers. As observed, the total rate of secrecy for the SUs increases, by raising the number of SUs. Raising the amount of eavesdroppers diminishes the overall privacy since a large number of eavesdroppers can use multiuser diversity to decipher the signals.

B. Variation of Level of Secrecy of Primary Network based on Number of Secondary Users

In Fig. 6, the total rate of secrecy of SN is depicted as functions of the entire group of PUs, for varying values of minimum enforced rate of secrecy of Pus, $bar R_{Up}^{SP}$=(2,4,6,8bit/sec)/Hz $\forall_{Up}\varepsilon p$,. It can be seen that the privacy of the secondary users is compromised when the number of primary users are increased.

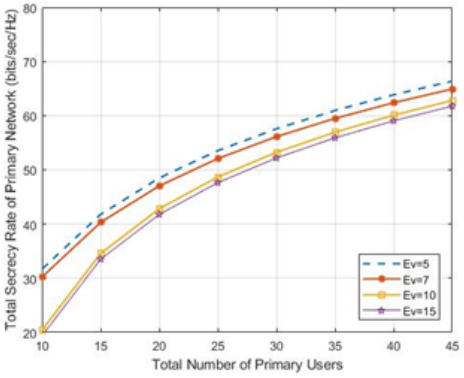


Fig. 5: Analysis of level of secrecy for PUs for varying values of minimum enforced rate of secrecy. Specifications: Ns= 64, Su= 11, Ev=7, Pp = 35 dBm, PUs = 20 dBm, RUp = 2 bits/sec

C. Comparison of Performance between the Planned Paradigm and Traditional Underlay Approach

In the traditional cognitive radio scheme, augmenting the overall achievable privacy for the SUs is pertinent to the interference threshold constraint. It is crucial to know if adopting other constraints would cause the overall secondary rate of secrecy to decline

in contrast to the existing scenario. To make an unbiased evaluation, we presume that the CSI value is analogous to any transmitter and receiver duo and can be compared for either situation. The CSI values are selected from a normalized Rayleigh distribution, in a random manner. For a particular group of CSI values, the threshold for interference is allocated and the conventional conundrum is resolved. From this, the maximum level of privacy is derived. Hence, we can also derive the resulting primary level of privacy.

In Fig. 7, we plotted the derived valued of the resulting primary privacy levels versus number of PUs for various values of thresholds for interference,

$\tau_{Up}^{n} = \tau, \bigtriangledown n\varepsilon N, \bigtriangledown_{Up}\varepsilon_{U}p$

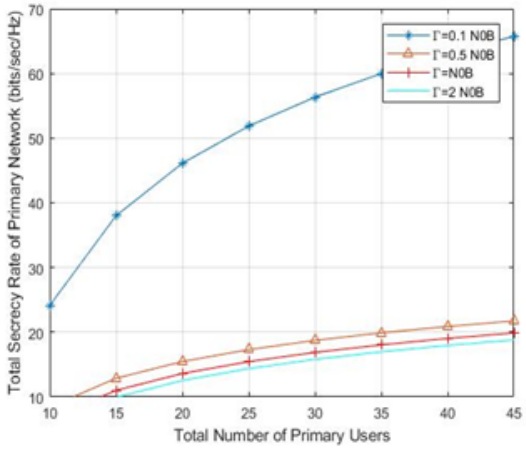


Fig. 7: Analysis of derived level of secrecy for PUs for various thresholds of interference. Specifications: Ns= 64, Su= 11, Ev=7, Pp= 35 dBm, PUs= 20 dBm, RUp = 2 bits/sec

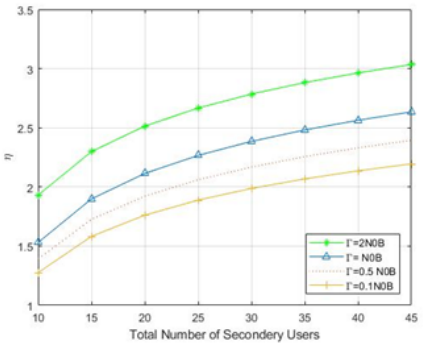


Fig. 8: Analysis of efficiency of derived level of secrecy for SUs for various thresholds of interference. Specifications: Ns= 64, Su= 11, Ev=7, Pp = 35 dBm, PUs= 20 dBm, RUp = 2 bits/sec.

For various values of primary privacy levels stated in Fig. 8, the proposed conundrum is resolved and the respective secondary level of secrecy is determined. Efficiency, $\eta$, is calculated as secondary privacy level of the proposed scheme by the privacy levels of the conventional scheme. We can see from Fig.8 that the new constraints invariably return better levels of privacy as the value of $\eta$ is always equal to or more than unity, without compromising the privacy of the secondary users.

D. Estimating the Effect of the Amount of Ostensible and Noisy Data on the Performance

We characterize$|\Delta RS|$ as the definite value of distinction between the total rates of secrecy of SUs attained based on the perfect and estimated CDI. The amount of ostensible data, L, is set to 200 for all situations.

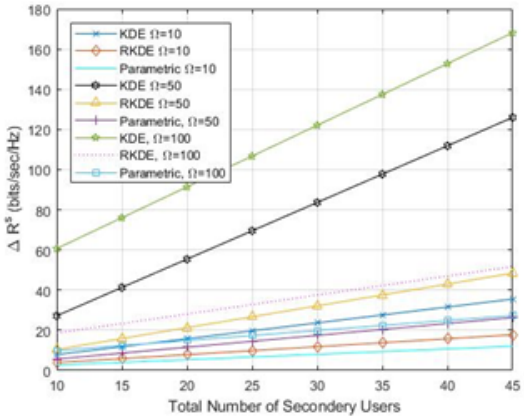


Fig. 9: Analysis of $|\Delta RS|$for total SUs for differing values of $\omega$ for both KDE and RKDE. Specifications Ns= 64, Su= 10, Ev=7, Pp = 35 dBm, PUs =20 dBm, , RUp = 2 bits/sec, $barR_{Up}^{SP}$= 3bits/sec,

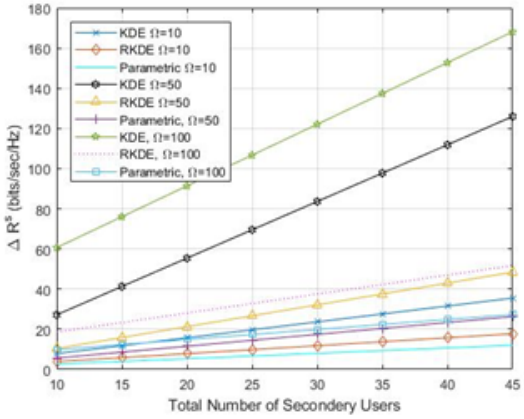


Fig. 10: Analysis of $|\Delta RS|$ for total SUs for differing values of L for both KDE and RKDE. Specifications: Ns= 64, Su= 10, Ev=7, Pp= 35 dBm, PUs = 20 dBm, RUp = 2

• Effect of the amount of outlier data: Fig. 9 depicts $|\Delta RS|$against the total amount of SUs for differing quantities of eccentric data. As shown in the figure, the value of $|\Delta RS|$ approaches zero for RKDE approach with = 10. As rises, $|\Delta RS|$ raises hinting at the difference from the current pdf. It is also seen that the value of

$|\Delta RS|$ for KDE is far from zero and the performance deteriorates quicker as compared to that of RKDE as $\omega$ rises.

• Impact of ostensible data: Fig. 10 shows the contrast among the overall levels privacy of SUs achieved due to perfect and estimated CDI, $|\Delta RS|$, as a function of total number of SUs for various amounts of the ostensible data for cognitive networks, correspondingly. $\omega = 20$ in fig.10. It can be seen that as L rises, the performance of both KDE and RKDE approaches gradually raises, and for L = 200, the overall secrecy derived due to RKDE is roughly close to that of perfect CDI for the traditional system.

E. Analysis of Filter and Forward Relay scheme on the level of Secrecy for Primary Users

Fig. 12 illustrates the improvement in secrecy rate that the filter and forward relaying scheme brings to the system in comparison with the decode and forward scheme. It can be observed from fig. 12 that the total secrecy rate of the primary network is higher than the DF relay scheme for all values of eavesdroppers whether a MRC or non-MRC scheme is used. Therefore for the same number of primary users, the FF relay scheme provides a much more efficient performance, hence a better secrecy rate.

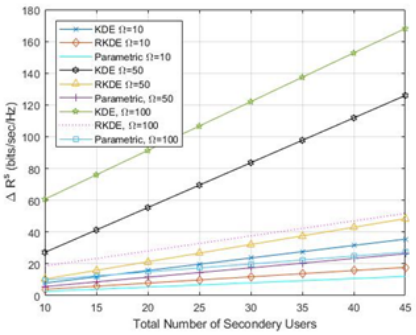


Fig. 11: Analysis of total level of secrecy for PUs when filter and forward relay is used. Specifications: Ns= 64, Su= 11, Ev=7, Pp= 35dBm, PUs= 20dBm, RUp = 2 bits/sec,$barR_{Up}^{Sp} = 3bits/sec, \forall_{Up}\varepsilon Us$

# 8 CONCLUSION

In conclusion, we proposed a model for secure communication over a cooperative communication system with better secrecy rates in the presence of eavesdroppers, who cannot intercept the transmitted data between the PBS and the SUs. Both MRC and non-MRC schemes are looked into. In our scheme, we first and mainly analyzed the behaviour of the SUs as DF relays to transmit information from the PBS to distant PUs in a secure manner. In exchange, the SUs are given some amount of the network to transmit their own messages, which are also secure. A more practical approach was involved as we only consider the CDI of the eavesdropper as the CSI is unavailable. The resulting CDI imperfectness is estimated using KDE and RKDE, for an optimal result. The entire scheme is considered to be an optimization problem and is solved using Lagranges dual approach, where, the primal problem is seen to be the security of information sent from the SUs and the dual problem is seen to be the information transmitted from the PUs. Finally, we also analyzed the performance of the scheme in terms of PU security, when the SUs behave as Filter and Forward relays, a much more efficient relaying scheme. In our forthcoming endeavours, we desire to extend the performance analysis to multiple input multiple output (MIMO) technology using FF relaying scheme.

**ACKNOWLEDGEMENT**

We, the authors would like to thank our guide, Dr.. T. Deepa (Associate prof., S.R.M. Institute of Science and Technology) for her invaluable and consistent encouragement throughout. This would have been impossible without her thorough guidance. Also, we would like to thank Dr. T. Rama Rao (HOD, Department of Telecommunication, S.R.M. Institute of Science and Technology) for his efforts to make this work possible.

# References

[1] Nader Mokari, Saeedeh Parsaeefard, Hamid Saeedi and Paeiz Azim, Cooperative Secure Resource Allocation in Cognitive Radio Networks with Guaranteed Secrecy Rate for Primary Users, IEEE Transactions on Wireless Communi-

cations, vol.: 13,no. 2, pp.1058 - 1073, February 2014, doi:10.1109/TWC.2013.010214.130929.

[2] Hyoungsuk Jeon, Steven W. McLaughlin, Il-Min Kim, Jeongseok Ha, Secure Communications with Untrusted Secondary Nodes in Cognitive Radio Networks, IEEE Transactions on Wireless Communications vol: 13, no.4,pp.1790 - 1805, April 2014,doi:10.1109/TWC.2013.021214.130089

[3] W. D. Lu, Y. Gong, S. H. Ting, X. L. Wu, and N. T. Zhang, Cooperative OFDM relaying for opportunistic spectrum sharing: Protocol design and resource allocation, IEEE Transactions on Wireless Communications, vol. 11, no. 6, pp. 21262135, June 2012.

[4] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, Spectrum leasing to cooperating secondary ad hoc networks, IEEE Journal on Selected Areas in Communications, vol. 26, no. 1, pp. 203213, January 2008.

[5] S. M. M. Toroujeni, S. M.-S. Sadough, and S. A. Ghorashi, Spectrum leasing for OFDM-based cognitive radio networks, IEEE Transactions on Vehicular Technology, vol. 62, no. 5, pp. 21312139, June 2013.

[6] W. Liang, S. X. Ng, and L. Hanzo, Cooperative communication between cognitive and primary users, IET Communications, vol. 7, no. 17, pp. 19821992, November 2013.

[7] A. Zarrebini-Esfahani and M. R. Nakhai, Secondary spectrum access and cell-edge coverage in cognitive cellular networks, IET Communications, vol. 6, no. 8, pp. 845851, May 2012.

[8] T. Jing, S. Zhu, H. Li2, X. Xing, X. Cheng, Y. Huo, R. Bie, and T. Znati, Cooperative relay selection in cognitive radio networks, IEEE Transactions on Vehicular Technology, vol. 64, no. 5, pp. 18721881, July 2015.

[9] M. Tao and Y. Liu, Spectrum leasing and cooperative resource allocation in cognitive OFDMA networks, Journal of Communications and Networks, vol. 15, no. 1, pp. 102110, February 2013.

[10] J. He, C. Xu, and L. Li, Power saving for cooperative spectrum sharing based cognitive radios under primary user short-term rate protection, IET Communications, vol. 6, no. 9, pp. 10971103, June 2012.

[11] W. Lu and J. Wang, Opportunistic spectrum sharing based on full duplex cooperative OFDM relaying, IEEE Communications Letters, vol. 18, no. 2, pp. 241244, February 2014.

[12] Yang li, Aria Nosratinia, Hybrid Opportunistic Scheduling in Cognitive Radio Networks Article in IEEE Transactions on Wireless Communications January 2012 DOI: 10.1109/TWC.2011.110811.110722

[13] S. Haykin, Cognitive radio: brain-empowered wireless communications, IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201220, February 2005.

[14] A. D. Wyner, The wire-tap channel, Bell System Technical Journal, vol. 54, pp. 13551387, 1975.

[15] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers, IEEE Transactions on Wireless Communications, vol. 12, no. 12, pp. 60766085, December 2013.

[16] B. Han, J. Li, and J. Su, Optimal relay assignment for secrecy capacity maximization in cooperative ad-hoc networks, in Proceedings IEEE International Conference on Communications (ICC), pp. 61286132, June 2013, Budapest, Hungary.

[17] H. Jeon, S. W. McLaughlin, I.-M. Kim, and J. Ha, Secure communications with untrusted secondary nodes in cognitive radio networks, IEEE Transactions on Wireless Communications, vol. 13, no. 4, pp. 17901805, April 2014.

[18] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users, IEEE Transactions on Wireless Communications, vol. 13, no. 2, pp. 10581073, February 2014.

[19] K. Lee, O. Simeone, C.-B. Chae, and J. Kang, Spectrum leasing via cooperation for enhanced physical-layer secrecy, IEEE Transactions on Vehicular Technology, vol. 62, no. 9, pp. 46724678, November 2013.

[20] I. Stanojev and A. Yener, Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users, IEEE Transactions on Wireless Communications, vol. 13, no. 2, pp. 10581073, February 2014.

[21] N. Zhang, N. Lu, N. Cheng, J. W. Mark, and X. Shen, Cooperative spectrum access towards secure information transfer for CRNs, IEEE Journal on Selected Areas in Communications, vol. 31, no. 11, pp. 2453 2464, November 2013.

[22] H. Zhang, H. Xing, X. Chu, A. Nallanathan, and a. X. W. W. Zheng, Secure resource allocation for OFDMA two-way relay networks, in Proceeding IEEE Global Communications Conference (GLOBECOM), pp. 36493654, December 2012, Anaheim, CA, 2012.

[23] Harshit Kumar Lohani,Vishal Jaiswal,N. Prabakaran, Performance Analysis of Wireless Networks using Filter and Forward Relay Technique, International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-4, Issue-5, May.-2016

[24] Donggun Kim, Junyeong Seo and Youngchul Sung, Filter-And-Forward Relay Design for OFDM Systems for Quality-of-Service Enhancement , Signal & Information Processing Association Annual Summit and Conference (APSIPA ASC), 2012 Asia-Pacific Date of Conference: 3-6 Dec. 2012

[25] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X.Wang, and T. Q. S. Quek, Resource allocation for cognitive small cell networks: A cooperative bargaining game theoretic approach, IEEE Transactions on Wireless Communications, vol. 14, no. 6, pp. 34813493, February 2015.

[26] H. Zhang, C. Jiang, X. Mao, and H.-H. Chen, Interference-limited resource optimization in cognitive femtocells with fair-

ness and imperfect spectrum sensing, IEEE Transactions on Vehicular Technology, vol. PP, no. 99, p. 1, February 2015.

[27] H. Zhang, C. Jiang, N. C. Beaulieu, X. Chu, X. Wen, and M. Tao, Resource allocation in spectrum-sharing OFDMA femtocells with heterogeneous services, IEEE TRANSACTIONS ON COMMUNICATIONS, vol. 62, no. 7, p. JULY, 2014.

[28] S. J. Sheather, Density estimation, Statistical Science, vol. 19, no. 4, pp. 588597, 2004.

[29] S. J. Sheather, Density estimation, Statistical Science, vol. 19, no. 4, pp. 588597, 2004.

[30] V. C. Raykar, Probability density function estimation by different methods, ENEE 739Q Spring 2002 Course Assignment 1 Report, 2002.