Physical Layer Security of Generalized Selection Combining based Cognitive Radio Networks

Ajay Singh

Abstract—— **Security has become an important concern in the field of wireless communication, which is vulnerable to ruinous attacks due to open nature of wireless medium. For executing reliable transmission, physical layer security has been raised as an interesting approach with minimum complexity. Here we have considered a system having a secondary transmitter (Alice) and secondary receiver (Bob) and eavesdropper (Eve). In this model, we are assuming that the Eve wants to know about the communication between Alice and Bob in Rayleigh fading environment. This paper presents a new structure for scrutinizing intercept probability (IP). The aim is to measure the physical layer security of generalized selection combining based cognitive radio networks under Rayleigh fading using IP in the presence of primary user. We have derived new closed form expressions for IP and examined the effect of number of antennas on the secrecy of system.**

Keywords—***cognitive radio; generalized selection combining;intercept probability; physical layer security; wiretap channel.***

I. INTRODUCTION

These days wireless communication is experiencing a rapid growth and hence new security techniques are also being developed at the same increasing rate. Physical layer security has the ability to allow trustworthy authentication and secure transmission. Cognitive radio network (CRN) reduces spectral crowding problem by allowing the advantageous usage of idle licensed spectral frequency bands by the secondary users i.e. unlicensed users. In such complicated surroundings, because of diverse nature of upcoming high coverage heterogeneous systems and the distributed properties of the broadcasting medium, security has become a challenging issue. [1] presented new closed form expressions for the exact and asymptotic secrecy outage probability and revealed the impact of the primary network on the secondary network and [2] carried out a thorough analysis on the performance and power saving of minimum selection – generalized selection combining i.e. MS-GSC scheme.

The secrecy outage probability (SOP) performance over single input single output (SIMO) Nakagami-m fading channels in CRN considering physical layer security issue is analyzed in [3]. Recently, researchers show keen interest in the field of CRN because it is being seen as a radio spectrum scarcity solution [4], [5]. In CRN, there are 3 spectrum approaches namely underlay, overlay, and interweave approach through which all the secondary users i.e. unlicensed users can share the band with the primary users [6], [7]. Traditionally, in wireless communications, the security issues are mainly handled in the upper layer using public key and private key cryptographic authentication and identification. These cryptosystems required high computational power as their operation based on mathematical operations, security provided by these system is refer as computational security. Even computational techniques are very effective but it may become very difficult to execute these techniques in emerging network. Presently, extensive use of wireless communication networking and constant progress in wireless technology are making physical layer security as an interesting area for research [8].To comprehend secure communication using physical layer security techniques, the time-variable properties of wireless medium are utilized and no encryption keys are required in it [9], [10], [11].

In literature a lots of work is done which focuses on the security issues in physical layer in CRN [12]-[18] and also in [15]-[18], all the channels were undergo Rayleigh fading and at the receiving side authors only considered selection combining (SC) or maximal ratio combining (MRC) technique. In contrast to Rayleigh, Nakagami-m model provides a good match to various fact-based data [19] and it is broadly used for modeling wireless fading channels, which includes Rayleigh (m = 1) and one-sided Gaussian distribution (m = 0.5) as special cases[3].In [20], [21] detailed study has been done on Generalized selection combining (GSC) which is a hybrid combining scheme. GSC technique bridges the performance gap between MRC and SC and the performance is maximized at the cost of complexity [21].Ref. The effect of GSC and the channel state information (CSI) on the SOP in interference limited spectrum sharing network were analyzed in [22].Our main aim is to analyze the physical layer security of GSC based CRN over Rayleigh fading channels, and derive the closed-form expression for Intercept Probability (IP), and after derivation simulate the result using MATLAB and compare results with existing records.

The rest of the paper is organized as follows. In Section II, the system model considered in our work is described. In section III we have derived the mathematical expressions for intercept probability. Section IV includes numerical results and Section V concludes the paper.

II. SYSTEM MODEL

The system model consists of a cognitive wiretap radio network, which includes a primary user (PU) , secondary transmitter (Alice), secondary receiver as (Bob) and an eavesdropper as (Eve).The primary user and the secondary user are assumed to have single antenna whereas the secondary receiver and the eavesdropper are equipped with multiple antennas n_B and n_E respectively. Here we are

Ajay Singh is with the Department of Electrical Engineering,
Indian Institute of Technology Jammu,
Jammu & Kashmir, India. (Email: ajay.singh@iitjammu.ac.in)

considering the case where the confidential messages are being transmitted from a single antenna secondary transmitter to a multiple antenna secondary receiver in the presence of a multiple antenna eavesdropper and the eavesdropper wants to overhear their communication [1] as shown in the Fig1. We have taken an underlay spectrum sharing cognitive network in which concurrent transmissions are possible in the same spectrum band by the primary user and the secondary transmitter. In our system model, the licensed and unlicensed channels are experiencing independent identically distributed Rayleigh fading. The transmit power at the secondary transmitter should be such that the interference power at PU is less than a predefined threshold value. The channel gain and variance of primary user are $|h_0|^2$ and Ω_0 respectively.

Generalized Selection Combining(GSC)

In reducing fading problems, diversity techniques are advantageous in wireless communications. Optimal diversity techniques are chosen by examining and comparing various diversity techniques. Furthermore, a variety of diversity techniques can be merged and employed in wireless systems for reducing the effect of fading.

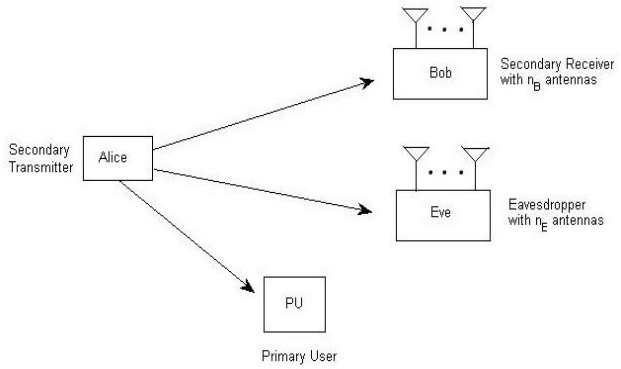

Fig.1.System model signifying cognitive wiretap radio network.

Diversity technique makes better the performance of wireless communication systems at the expense of increased processing power. In this paper we are considering receiver diversity combining. Diversity combining lessens multipath fading because the combined SNR is larger than the SNR of individual branch. In GSC during the data reception stage, all MRC branches are kept active by the receiver [2]. Here the main channel and the eavesdropper's channel do not depend on one another.

GSC is commonly known as hybrid selection/maximum ratio combining (H-S/MRC). In the GSC scheme, the most advantageous MRC scheme is applied to predetermined number of the best paths selected from existing ones. In GSC scheme, it is not necessary to execute each diversity path in the MRC manner due to this, its receiver hardware is less complicated as compared to receiver hardware in traditional MRC scheme.

By GSC we mean that the receivers combine L_c strongest antennas at both Bob and Eve such that ($1 \leq L_c \leq L$) gaining from best channel state information evaluation by means of pilot signals which are transmitted by Alice [3], [21]-[22].The receivers faultlessly evaluate CSI by using pilot signals information and organize the channel gains, denoted by $|h_i^k|^2$ $(i = 1, \dots, L)$, in decreasing order as $|h_1^k|^2 \geq |h_2^k|^2 \geq \cdots \geq |h_L^k|^2$[3]. The legitimate receiver and the eavesdropper consists of multiple antennas, therefore, the antenna selection at both of them are taken into account in such a way that they opt for their optimal receive antennas in accordance with best CSI estimation through pilot signals communicated by Alice [3]. Here the GSC scheme is applied both at the Bob and Eve.

The main channel's and eavesdropper's channel instantaneous signal to noise (SNR) are given by [3, Eq. 3]

$$\gamma_k = \sum_{i=0}^{L_c} \gamma_i^k = \frac{P_A}{N_0} Y_k \quad , k \in \{B, E\} \tag{1}$$

where P_A is the transmit power at A, and N_0 is the noise variance and

$Y_k = \sum_{i=1}^{L_c} |h_i^k|^2$,$k \in \{B, E\}$ are the channel gains of main channel and eavesdropper channel.

For ensuring reliable communication at PU, the interference power at PU should be smaller as compared to peak interference power threshold. According to underlay cognitive radio transmission, P_A is strongly confined by the maximum transmit power P_t at A and the peak interference power I_p at Primary user, [1] i.e.

$$P_A = \min(\frac{I_p}{X}, P_t) \tag{2}$$

When $X \leq \frac{\gamma_p}{\gamma_0}$, $\gamma_M = \gamma_0 Y_M$, $\gamma_E = \gamma_0 Y_E$

and when, $X > \frac{\gamma_p}{\gamma_0}$, $\gamma_M = \frac{\gamma_p}{X} Y_M$, $\gamma_E = \frac{\gamma_p}{X} Y_E$. (3)

where γ_p is the ratio of peak interference power I_p and noise variance, X is the channel gain of primary user and γ_0 is the ratio of maximum transmit power at A and noise variance and $\sigma = \frac{\gamma_p}{\gamma_0} = \frac{I_p}{P_t}$.

I. INTERCEPT PROBABILITY

The secrecy capacity analysis can help us to determine how secure a cognitive radio network is, and whether we need to further strengthen the security mechanisms to defend against the potential attacks in the cognitive radio networks. The secrecy rate is given by [1 Eq. 2]. The maximum achievable secrecy rate is named as secrecy capacity. In a CRN, considering single antenna at Alice and multiple antennas at Bob and Eve, the secrecy capacity can be defined as,

$$C_S = \begin{cases} C_M - C_E & \text{if } \gamma_M > \gamma_E \\ 0 & \text{if } \gamma_M \leq \gamma_E \end{cases} \tag{4}$$

where $C_M = \log_2(1+\gamma_M)$ is the capacity of the main channel and, $C_E = \log_2(1+\gamma_E)$is the capacity of the eavesdropper's channel.

The intercept probability is the outage probability when R_s=0. The outage probability is the probability that C_s falls below R_s [1 Eq. 3] is given below,

$$P_{out} = Pr(C_s < R_s) \quad (5)$$

$$P_{out} = \Pr(\gamma_M \le \gamma_E) + \Pr(\gamma_M > \gamma_E)\Pr(C_s < R_s | \gamma_M > \gamma_E) \quad (6)$$

Also $$C_S = log_2 \frac{(1+\gamma_M)}{(1+\gamma_E)} < R_s \quad (7)$$

which is equivalent to

$$\gamma_M < 2^{R_s}(1+\gamma_E) - 1 = \epsilon(\gamma_E) \quad (8)$$

Also, $R_s = 0$

We get, $$\gamma_M < \gamma_E = \epsilon(\gamma_E) \quad (9)$$

This means that the intercept probability is probability when signal to noise ratio of the main channel is less than or equal to signal to noise ratio of eavesdropper channel. The intercept probability given in [1, Eq 10] is

$$P_{out} = \int_0^\infty \int_0^\infty F_{\gamma_M|\{X=x\}}(\epsilon(\gamma_E)) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \quad (10)$$

where, $F_{\gamma M}(.)$ is the CDF of γ_M i.e. of main channel and which is also denoted by $P_{\Gamma_i}(.)$ and$f_{\gamma_E}(.)$is the PDF of eavesdroppers channel also denoted by $p_{\Gamma_i}(.)$

The CDF $P_{\Gamma_i}(.)$ is given by [2, Eq. 17] for Rayleigh fading special case. Putting $i = L_c$ in [2, Eq. 17], we get $P_{\Gamma_{L_c}}(x)$ as follows

$$P_{\Gamma_{L_c}}(x) = \frac{L!}{(L-L_c)!\,L_c!}\{1 - e^{-\frac{x}{\bar{\gamma}}}\sum_{k=0}^{L_c-1}\frac{1}{k!}\left(\frac{x}{\bar{\gamma}}\right)^k + \sum_{l=1}^{L-L_c}(-1)^{L_c+l-1}\frac{(L-L_c)!}{(L-L_c-l)!\,l!}\left(\frac{L_c}{l}\right)^{L_c-1} \times \left[\left(1+\frac{l}{L_c}\right)^{-1}\left[1 - e^{-\left(1+\frac{l}{i}\right)\left(\frac{x}{\bar{\gamma}}\right)}\right] - \sum_{m=0}^{L_c-2}\left(-\frac{l}{L_c}\right)^m (1 - e^{-\frac{x}{\bar{\gamma}}}\sum_{k=0}^{m}\frac{1}{k!}\left(\frac{x}{\bar{\gamma}}\right)^k)\right]\} \quad (11)$$

The PDF $f_{\gamma_E}(.)$ also denoted by $p_{\Gamma_i}(.)$ is given by [2, Eq. 33] for Rayleigh fading case. Putting $i = L_c$ in [2, Eq. 33], we get $p_{\Gamma_{L_c}}(x)$ as follows

$$p_{\Gamma_{L_c}}(x) = \frac{L!}{(L-L_c)!\,L_c!}e^{-\frac{x}{\bar{\gamma}}}\left[\frac{x^{L_c-1}}{(\bar{\gamma})^{L_c}(L_c-1)!} + \frac{1}{\bar{\gamma}}\sum_{l=1}^{L-L_c}(-1)^{L_c+l-1}\frac{(L-L_c)!}{(L-L_c-l)!\,l!}\left(\frac{L_c}{l}\right)^{L_c-1} \times (e^{-\left(\frac{lx}{L_c\bar{\gamma}}\right)} - \sum_{m=0}^{L_c-2}\frac{1}{m!}\left(-\frac{lx}{L_c\bar{\gamma}}\right)^m)\right] \quad (12)$$

The PDF of the primary user is denoted by $f_X(x)$.For The PDF of the primary user is denoted by $f_X(x)$.

For multiple primary users the mathematical expressions for PDF of primary users is given by [1, Eq. 22] where N is the number of primary user

$$f_X(x) = \sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n\frac{N}{\Omega_0}e^{-\frac{(n+1)x}{\Omega_0}} \quad (13)$$

For single primary user the mathematical expression for PDF of primary user can be deduced from above expression by putting N=1 and we get,

$$f_X(x) = \frac{1}{\Omega_0}e^{-\frac{x}{\Omega_0}}$$

The intercept probability can be calculated as,

$$P_{out} = \{\gamma_M \le \gamma_E\} \quad (14)$$

$$P_{out} = \int_0^{\frac{\gamma_p}{\gamma_0}}\int_0^\infty F_{\gamma_M|\{X=x\}}\left(\epsilon(\gamma_E)\right) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx + \int_{\frac{\gamma_p}{\gamma_0}}^{\infty}\int_0^\infty F_{\gamma_M|\{X=x\}}\left(\epsilon(\gamma_E)\right) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx = J1 + J2 \quad (15)$$

Where

$$J_1 = \int_0^{\frac{\gamma_p}{\gamma_0}}\int_0^\infty F_{\gamma_M|\{X=x\}}\left(\grave{o}(\gamma_E)\right) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \quad (16)$$

$$J_1 = \int_0^{\frac{\gamma_p}{\gamma_0}}\int_0^\infty F_{\gamma_M|\{X=x\}}\left(\grave{o}(\gamma_E)\right) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx$$

$$J_2 = \int_{\frac{\gamma_p}{\gamma_0}}^{\infty}\int_0^\infty F_{\gamma_M|\{X=x\}}\left(\grave{o}(\gamma_E)\right) f_{\gamma_E|\{X=x\}}(\gamma_E) f_X(x) d\gamma_E dx \quad (17)$$

After solving (16) for multiple primary users we getJ1 as follows

$$J1 = \frac{L!}{(L-L_c)!}\sum_{n=0}^{N-1}\binom{N-1}{n}(-1)^n \times \frac{1}{n+1}\left(1 - e^{-\frac{(n+1)\gamma_p}{\Omega_0\gamma_0}}\right) \times H \quad (18)$$

H is given by (19) where$\gamma_1$is the maximum possible average SNR of the channel between Alice and Bob, and $\gamma_2$is the

maximum possible average SNR of the channel between Alice and Eve.

$$H = \{1 - \sum_{k=0}^{\mathrm{L_c}-1} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \frac{1}{(\mathrm{L_c}-1)!}\left(\frac{1}{\gamma_2}\right)^{\mathrm{L_c}} \frac{\Gamma(\mathrm{k}+\mathrm{L_c})}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}\right)^{k+\mathrm{L_c}}} + \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} [\left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} - \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!}\left(-\frac{l}{\mathrm{L_c}}\right)^m \Gamma(\mathrm{m}+1) - \sum_{k=0}^{\mathrm{L_c}-1} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \frac{1}{\gamma_2} \times \frac{\Gamma(\mathrm{k}+1)}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}+\frac{l}{\mathrm{L_c}\gamma_2}\right)^{k+1}} + \sum_{k=0}^{\mathrm{L_c}-1} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!}\left(-\frac{l}{\mathrm{L_c}}\right)^m \times \left(\frac{1}{\gamma_2}\right)^m \frac{1}{\gamma_2} \frac{\Gamma(\mathrm{k}+\mathrm{m}+1)}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}\right)^{k+\mathrm{m}+1}} + \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} + \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} \times \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} - \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \times \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!}\left(-\frac{l}{\mathrm{L_c}}\right)^m \Gamma(\mathrm{m}+1) - \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} \left(\frac{1}{\gamma_2}\right)^{\mathrm{L_c}} \times \frac{1}{\left(\frac{1}{\gamma_1}+\frac{l}{\mathrm{L_c}\gamma_1}+\frac{1}{\gamma_2}\right)^{\mathrm{L_c}}} - \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \times \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \frac{1}{\gamma_2} \frac{1}{\left(\frac{1}{\gamma_1}+\frac{l}{\gamma_1\mathrm{L_c}}+\frac{1}{\gamma_2}+\frac{l}{\gamma_2\mathrm{L_c}}\right)} + \left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \times \frac{1}{\gamma_2} \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!}\left(-\frac{l}{\mathrm{L_c}}\right)^m \left(\frac{1}{\gamma_2}\right)^m \frac{\Gamma(\mathrm{m}+1)}{\left(\frac{1}{\gamma_1}+\frac{l}{\mathrm{L_c}\gamma_1}+\frac{1}{\gamma_2}\right)^{\mathrm{m}+1}} - \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m - \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \times \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(1+\frac{l}{\mathrm{L_c}}\right)^{-1} + \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m \times \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!}\left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!} \times \left(-\frac{l}{\mathrm{L_c}}\right)^m \Gamma(\mathrm{m}+1) + \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m \sum_{k=0}^{m} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \times \frac{1}{(\mathrm{L_c}-1)!}\left(\frac{1}{\gamma_2}\right)^{\mathrm{L_c}} \frac{\Gamma(\mathrm{k}+\mathrm{L_c})}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}\right)^{k+\mathrm{L_c}}} + \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m \times \sum_{k=0}^{m} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{1}{\gamma_2} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!} \times \left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \frac{\Gamma(\mathrm{k}+1)}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}+\frac{l}{\mathrm{L_c}\gamma_2}\right)^{k+1}} - \sum_{m=0}^{\mathrm{L_c}-2} \left(-\frac{l}{\mathrm{L_c}}\right)^m \times \sum_{k=0}^{m} \frac{1}{k!}\left(\frac{1}{\gamma_1}\right)^k \sum_{l=1}^{L-\mathrm{L_c}} (-1)^{\mathrm{L_c}+l-1} \frac{1}{\gamma_2} \frac{(L-\mathrm{L_c})!}{(L-\mathrm{L_c}-l)!\,l!} \times \left(\frac{\mathrm{L_c}}{l}\right)^{\mathrm{L_c}-1} \sum_{m=0}^{\mathrm{L_c}-2} \frac{1}{m!}\left(-\frac{l}{\mathrm{L_c}}\right)^m \left(\frac{1}{\gamma_2}\right)^m \frac{\Gamma(\mathrm{k}+\mathrm{m}+1)}{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}\right)^{k+\mathrm{m}+1}}]\} \quad (19)$$

Similarly J2 for multiple primary users is calculated and obtained as

$$\mathrm{J2} = \frac{\mathrm{L}!}{(\mathrm{L}-\mathrm{L_c})!} \sum_{n=0}^{\mathrm{N}-1} \binom{\mathrm{N}-1}{n} (-1)^n \times \frac{1}{n+1}\left(\mathrm{e}^{-\frac{(n+1)\sigma}{\Omega_0}}\right) \times H \quad (20)$$

Adding (18) and (20) we get the closed form expression for the intercept probability for multiple primary users.

IV. NUMERICAL RESULT

In this section, the numerical results are given for the verification of the proposed analytical model. Using (15), (18) and (19) the exact curves are obtained for the given model. The parameters used for analysis are assumed to be unity variance $\Omega_0 = 1$. After executing the program we got the following graphs which show that on increasing signal to noise ratio of legitimate receiver, the intercept prob. decreases. Fig. 2 shows the plot of intercept probability versus γ_1 for different values of $\mathrm{L_c}$ for multiple primary users (N). Here we have taken 4 primary users with parameters set as $\sigma = 0.5$, $n_A = 1$, $\mathrm{L}=n_B = n_E = 4$ and $\gamma_2 = 10$ dB and $\mathrm{L_c}$ ranges from 1 to 4 and γ_1 ranges from 0 dB to 25 dB. We see that as we increase γ_1, the intercept probability decreases. For $\mathrm{L_c} = 1$, the curve is higher than the curve for $\mathrm{L_c} = 2$. Similarly for $\mathrm{L_c} = 2$, the curve is higher than the curve for $\mathrm{L_c} = 3$. Similarly for $\mathrm{L_c} = 3$, the curve is higher than the curve for $\mathrm{L_c} = 4$. This means that as we increase the number of $\mathrm{L_c}$, the intercept probability decreases and the network becomes more secure. By increasing $\mathrm{L_c}$, the network becomes optimum. For MRC case i.e $\mathrm{L_c}$=L, the system is the most optimum and for SC case i.e $L_c = 1$ the system is least optimum.

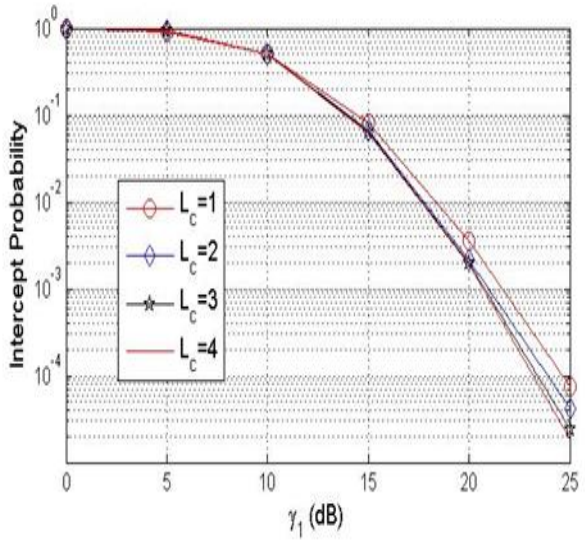

Fig. 2. Intercept probability versus γ_1 with σ = 0.5, n_A = 1, L= n_B= n_E = 4 , N=4, γ_2 = 10 dB and L_c=1 to 4.

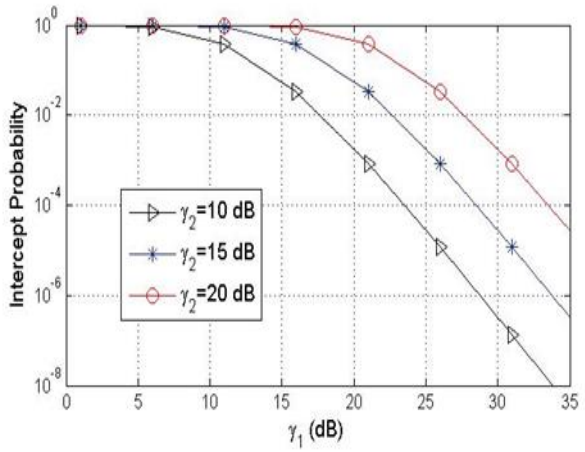

Fig. 3. Intercept probability versus γ_1 for different γ_2 with σ = 0.5, n_A = 1, L= n_B= n_E = 4 , N=4.

Fig. 3 shows the plot of intercept probability versus γ_1 for different γ_2, with parameters set as n_A = 1, L= n_B = n_E =4 and N = 4. It is shown that on increasing γ_2, the intercept probability increases and the system become more unsecure.

V. CONCLUSION

Higher layer cryptographic authentication and identification are expensive, power consuming and vulnerable to attacks. Hence physical layer security is used to secure data transmission as a solution to support and supplement existing cryptographic protocols. Using GSC scheme we derived closed loop expressions for the intercept probability which gives the measure of security of the system. This model is very efficient, and can be used reliably by utilities and industries in order to determine the measure of security of their network.

REFERENCES

[1] M. Elkashlan, L. Wang, T. Duong, G. Karagiannidis, and A. Nallanathan,"On the security of cognitive radio networks," IEEE Trans. Veh. Technol.,vol. 64, no. 8, pp. 3790-3795, Aug. 2015.

[2] Hong-Chuan Yang, "New Results on Ordered Statistics and Analysis of Minimum-SelectionGeneralized Selection Combining (GSC)", IEEE Trans. Wireless Commun., vol. 5, no. 7, July 2006.

[3] Hongjiang Lei, Huan Zhang, Imran Shafique Ansari, Chao Gao, Yongcai Guo, Gaofeng Pan, and Khalid A. Qaraqe, "Secrecy Outage Performance for SIMO Underlay Cognitive Radio Systems with Generalized Selection Combining over Nakagami-m Channels,"IEEE Trans. Veh. Technol., DOI 10.1109/TVT.2016.2536801.

[4] I. F. Akyildiz, L. Won-Yeol, M. C. Vuran, and S. Mohanty, "A surveyon spectrum management in cognitive radio networks," IEEE Commun.Mag., vol. 46, no. 4, pp. 40-48, Apr. 2008.

[5] S. Haykin, "Cognitive radio: Brain-empowered wireless communications,"IEEE J. Sel. Areas Commun., vol. 23, no. 2, pp. 201–220, Feb. 2005.

[6] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probabilityof cognitive relay networks with interference constraints," IEEE Trans.Wireless Commun., vol. 10, no. 2, pp. 390-395, Feb. 2011.

[7] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrumgridlock with cognitive radios: An information theoretic perspective,"Proc. IEEE, vol. 97, no. 5, pp. 894-914, May 2009.

[8] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo,Safeguarding 5G wireless communication networks using physical layersecurity," IEEE Commun. Mag. , vol. 53, no. 4, pp. 20-27, Apr. 2015.

[9] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physicallayer security over non-small scale fading channels," IEEE Trans. Veh.Technol., DOI: 10.1109/TVT.2015.2412140.

[10] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wirelessinformation-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6,pp. 2515-2534, Jun. 2008.

[11] G. Pan, C. Tang, T. Li, and Y. Chen, "Secrecy performance analysis forSIMO simultaneous wireless information and power transfer systems,"IEEE. Trans. Commun., vol. 63, no. 9, pp. 3423-3433, Sep. 2015.

[12] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radionetworks," IEEE Network, vol. 27, no. 3, pp. 28-33, May 2013.

[13] Y. Zou, J. Zhu, L. Yang, Y.-C. Liang, and Y.-D. Yao, "Securing physicallayercommunications for cognitive radio networks," IEEE Commun.Mag., vol. 53, no. 9, pp. 48-54, Sep. 2015.

[14] L. Zhang, R. Zhang, Y.-C. Liang, Y. Xin, and S. Cui, "On the relationshipbetween the multi-antenna secrecy communications and cognitive radiocommunications," IEEE Trans. Commun., vol. 58, no. 6, pp. 1877-1886,Jun. 2010.

[15] Y. Pei, Y.-C. Liang, L. Zhang, K. C. Teh, and K. H. Li, "Secure communicationover MISO cognitive radio channels," IEEE Trans. WirelessCommun., vol. 9, no. 4, pp. 1494-1502, Apr. 2010.

[16] H. Liu, H. Zhao, H. Jiang, C. Tang, G. Pan, T. Li, et al., "Physical-layersecrecy outage of spectrum sharing CR systems over fading channels,"Science China Information Sciences, DOI: 10.1007/s11432-015-5451-2.

[17] H. Zhao, D. Wang, C. Tang, Y. Liu, G. Pan, T. Li, and Y. Chen, "Physicallayer security of underlay cognitive radio using maximal ratio combining,"Frontiers of Information Technology & Electronic Engineering, to bepublished.

[18] H. Zhao, Y. Tan, G. Pan, Y. Chen, and N. Yang, "Secrecy outageon transmit antenna selection/maximal ratio combining in MIMOcognitive radio networks," IEEE Trans. Veh. Technol., DOI10.1109/TVT.2016.2529704.

[19] Z. Kang, K. Yao, and F. Lorenzelli, "Nakagami-m fading modeling inthe frequency domain for OFDM system analysis," IEEE Commun. Lett.,vol. 7, no. 10, pp. 484-486, Oct. 2003.

[20] X. Cai and G. B. Giannakis, "Performance analysis of combinedtransmit selection diversity and receive generalized selection combiningin Rayleigh fading channels," IEEE Trans. Wireless Commun., vol. 3, no.6, pp. 1980-1983, Nov. 2004.

[21] A. Annamalai, G. Deora, and C. Tellambura, "Analysis of generalizedselection diversity systems in wireless channels," IEEE Trans. Veh.Technol., vol. 55, no. 6, pp. 1765-1775, Nov. 2006.

[22] Y. Deng, M. Elkashlan, N. Yang, P. Yeoh, and R. Mallik, "Impactof primary network on secondary network with generalized selection combining," IEEE Trans. Veh. Technol., vol. 64, no. 7, pp. 3280-3285,Jul. 2015.