Distributed Matching Algorithms for Spectrum Access: A Comparative Study and Further Enhancements

Bakhtiar Ali[1], Nida Zamir[1], Soon Xin Ng[2] and Muhammad Fasih Uddin Butt[1]
[1] Department of Electrical Engineering, COMSATS IIT,
Islamabad, Pakistan
[e-mail : {bakhtiar_ali, nida.zamir, fasih}@comsats.edu.pk]
[2] Department of Electronics and Computer Science, University of Southampton,
Southampton SO17 1BJ, UK
[e-mail: sxn@ecs.soton.ac.uk]
*Corresponding author: Muhammad Fasih Uddin Butt

Received March 28, 2017; revised August 18, 2017; revised October 12, 2017; accepted November 7, 2017; published April 30, 2018

Abstract

In this paper, we consider a spectrum access scenario which consists of two groups of users, namely Primary Users (PUs) and Secondary Users (SUs) in Cooperative Cognitive Radio Networks (CCRNs). SUs cooperatively relay PUs messages based on Amplify-and-Forward (AF) and Decode-and-Forward (DF) cooperative techniques, in exchange for accessing some of the spectrum for their secondary communications. From the literatures, we found that the Conventional Distributed Algorithm (CDA) and Pragmatic Distributed Algorithm (PDA) aim to maximize the PU sum-rate resulting in a lower sum-rate for the SU. In this contribution, we have investigated a suit of distributed matching algorithms. More specifically, we investigated SU-based CDA (CDA-SU) and SU-based PDA (PDA-SU) that maximize the SU sum-rate. We have also proposed the All User-based PDA (PDA-ALL), for maximizing the sum-rates of both PU and SU groups. A comparative study of CDA, PDA, CDA-SU, PDA-SU and PDA-ALL is conducted, and the strength of each scheme is highlighted. Different schemes may be suitable for different applications. All schemes are investigated under the idealistic scenario involving perfect coding and perfect modulation, as well as under practical scenario involving actual coding and actual modulation. Explicitly, our practical scenario considers the adaptive coded modulation based DF schemes for transmission flexibility and efficiency. More specifically, we have considered the Self-Concatenated Convolutional Code (SECCC), which exhibits low complexity, since it invokes only a single encoder and a single decoder. Furthermore, puncturing has been employed for enhancing the bandwidth efficiency of SECCC. As another enhancement, physical layer security has been applied to our system by introducing a unique Advanced Encryption Standard (AES) based puncturing to our SECCC scheme.

Keywords: Cognitive radio networks, cooperative communications, physical layer security, matching algorithm, SECCC, spectrum access strategy.

http://doi.org/10.3837/tiis.2018.04.011 **ISSN : 1976-7277**

1. Introduction

Cognitive radio (CR) is known to be a promising technology to improve spectral efficiency of a communication system by sharing the licensed spectrum of Primary User (PU) to the unlicensed Secondary User (SU) [1]. Conventionally, it does so by listening to the received signals and identifying the spectrum holes. These spectrum holes can then be used by the SUs for their transmission provided that they do not interfere or cause minimal interference to the PU. Two major challenges of Cognitive Radio Networks (CRNs) are the PU detection and the transmission opportunity exploration. CRs may operate in three different modes i.e., overlay, interweave and underlay modes [2]. In the interweave mode, the SU searches for spectrum holes and then obtain access to these spectrum holes opportunistically [3]. By contrast, simultaneous PU and SU transmissions are legitimized in underlay mode if the interference caused by the SU transmission does not worsen the performance of the PU. The overlay mode relates to a class of more sophisticated scenario, where the CR nodes are equipped with advanced signal processing capabilities are capable of decoding the PU messages. In addition, they are capable of maintaining or even improving the quality of PU transmission, while simultaneously obtaining spectrum opportunities to transmit their own SU messages [2].

Cognitive nodes can interact with their surrounding nodes and make decisions to improve their communications. These smart nodes will be employing their neighboring nodes to assist in their communications and in return will pay them back either in the form of monetary benefits or might trade with them their bandwidth, power or any other resource that their neighbors might need. These complex interactions provide new areas and challenges for the researchers to explore. One of the best tools for defining and modeling interactions between different participants or entities is game theory. Game theory found its roots in economics and now it is being widely used in different fields of social, behavioral and natural sciences [4–6]. Game theory is useful in situations where there is interaction between multiple decision makers. Game theoretic models are precise expressions of ideas which can be formulated mathematically. Matching game theory is a mathematical framework that allows analyzing the formation of mutually beneficial relationships over time [7].

Cooperative communications constitute a powerful technique that combats channel fading due to multipath propagation in a wireless environment. Cooperative communications technique was first conceived by Van der Meulen back in 1970s [8], where he constructed a three-terminal relay channel and derived both upper and lower bounds on its capacity. It gained ample interest 30 years later and has been seen as an essential technique for its significant capacity and multiplexing gain improvements. Many relaying protocols have been developed, including Amplify and Forward (AF), Decode and Forward (DF), Compress and Forward (CF), Selection and Dynamic Relaying (SDR) and Incremental Relaying (IR) [9].

Cooperation can naturally enhance the performance of a CRN where the transmissions of both PU and SU can be supported [10]. More explicitly CR relay networks were investigated in [11, 12]. Furthermore, Lin et al. [13] proposed a distributed spectrum sharing algorithm for multiple SUs and PUs, where PUs trade their spectrum with SUs in exchange for acquiring more revenue. A Conventional Distributed Algorithm (CDA) was presented in [14, 15] where the PU negotiates a specific time allocation for spectrum access with the SU. More specifically, SU helps in transmitting the PUs data in a fraction of the total allocated time slot and in return the SU gains access to the channel for the remaining time slot for its own data transmission. If SU receives a better offer from another PU then the previous match will be detached and the SU will be matched to the new PU. A Pragmatic Distributed Algorithm (PDA) was further proposed in [16] where each PU takes turn to match to its best available SU. It discourages

PUs to compete for the same SU, but allowing each PU to access its best available SU on around robin rotation basis [16].

PDA maximizes the sum-rate of PUs, but in some cases the traffic demand for the SUs can be higher than that of the PUs. Secondly in some situations, the SUs may have more privilege to gain access to the channel. For example, SUs might be giving a high monetary benefit to the PUs for acquiring the channel and hence can be given a higher priority. In disaster management scenarios, wireless communication techniques have been employed where emergency responders are used to prevent or respond to emergency situations [17,22]. Disaster management agencies use tools like sensors and surveillance cameras which may require higher bandwidth to support rescue operations [18]. However, the frequency spectrum allocated for public safety is getting congested [19]. Therefore, to overcome the congestion emergency responders with no access to the spectrum would act as SUs to look for additional spectrum. In addition, during tactical deployments, military personnel and devices will be dealing with various heterogeneous networks [20] and they as SUs will be requiring higher traffic demand so PDA-SU and CDA-SU can be used in these situations as well. Unmanned aerial vehicles (UAVs) or Drones are gaining popularity in military [21], public safety and commercial use which will require higher throughput. Furthermore, the Wireless Medical Telemetry Services (WMTS) band for medical applications is getting overcrowded [23-25]. Hence, there is a need for additional spectrum allocation for providing better healthcare facilities to the patients. Therefore, medical transceivers equipped with frequency-agile front-ends may opportunistically use portions of the WMTS band acting as SUs without adversely affecting the operation of the PUs as well as the legacy medical equipment in operation. In all these scenarios, the SUs will have higher demand so the SU based schemes will be more beneficial. PDA-SU and CDA-SU schemes will improve the SU sum-rate but will not affect PU's transmission quality and throughput.

In both PDA and CDA schemes, the offer is made by the PU. As a complement, we proposed SU-based CDA (CDA-SU) and SU-based PDA (PDA-SU) schemes, where SUs make the matching offer to PUs. Then, PUs would choose to match based on the achievable PU sum-rate. In return, SUs will gain access to the channel for the remaining amount of time. The PDA-SU scheme would provide higher sum-rate to the SUs while guaranteeing a PU sum-rate of at least similar to the direct-link based PU sum-rate i.e., the PU's minimum sum-rate is guaranteed. It is worth mentioning here that SU-based schemes are indeed legitimate if they do not violate the basic principle of cognitive radio networks as mentioned in [2] where it is mentioned that overlay schemes maintain or even improve the quality of PU transmission. While in the underlay case, the SUs maintain a minimum interference to the PU, which might slightly degrade the performance of the PU. Our SU-based overlay scheme would not degrade the PU transmission. More explicitly, the CDA-SU scheme would even provide a higher sum-rate for the PU, while the PDA-SU will maintain at least the minimum quality of the PU transmission. Nonetheless, PUs can also benefit from energy saving by transmitting in a cooperative scenario without degrading its own sum-rate due to the energy efficient nature of cooperation [26-29]. Furthermore, it would be interesting to look at the possible benefits of using SU-based schemes in comparison to the PU-based schemes for a matching algorithm. In situations where the PUs have higher traffic priority, we would invoke the PU-based schemes while in situations where SUs have higher traffic priority, we would switch to the SU-based schemes. In many situations where the demand is unknown or both have high traffic demands we can switch to PDA-ALL which gives optimized sum-rates for all PUs and SUs. The algorithm in [30] is the extension of the CDA algorithm given in [14], where [30] used variable power at the relay and proposed distributed algorithms to converge to equilibria under

different situations. Reference [30] only considered the large-scale fading. Both [30] and [14] are PU based algorithms where the aim is to maximize the PU sum-rate. On the contrary our CDA-SU algorithm is based on CDA of [14], where we aim to maximize the SU sum-rate. The algorithm in [31] is another matching based algorithm where the users strategies are influenced by historical behaviors of users. Therefore, preference will be given to a user which are cooperative as compared to selfish users. Secondly the objective of the matching algorithm in [31] is focused on improving the energy efficiency while in our algorithms the focus is on the sum-rate maximization and optimization.

Most of existing matching algorithms were investigated based on the Continuous input Continuous output Memoryless Channel (CCMC) [32] capacity, which assumed perfect channel coding and perfect modulation. In this contribution, we have also considered practical scenarios including the scenario where actual coding and modulation schemes are employed. More specifically, we have employed adaptive coded modulation schemes where both coding rate and modulation mode can be adapted according to the instantaneous channel conditions [33]. Practical Self-Concatenated Convolutional Codes (SECCCs) employing Iterative Decoding (SECCC-ID) [34, 35] are invoked, because they exhibit a low complexity by invoking only a single encoder and a single decoder. More explicitly, SECCC schemes have been proposed for BPSK modulation in [36, 37]. Iterative SECCC decoding works by exchanging extrinsic information between the current decoding and consecutive decoding using the same decoder. More advanced SECCC-ID schemes were proposed in [35], which invoke further iterations with the demapper. More details on SECCC principles may be found in [35].

In addition to reliability we also enhance the system's confidentiality by introducing Physical Layer Security (PLS). Due to the broadcast nature of wireless transmission the transmitted signal may be easily eavesdropped. Reliability and security are both important aspects of modern digital communication systems communicating over wireless medium [38-40]. Different cryptographic techniques (key-based enciphering) are used for securing the transmitted data [41] which are divided into two types on the basis of a shared key between both sender and receiver. More explicitly, symmetric algorithms use identical keys (private keys) while asymmetric algorithms use different keys (public and private keys) to encrypt and decrypt the transmitted data [42]. The strength of the algorithm depends on the length of key because more possible keys can be constructed if the key length is longer [42]. Data Encryption Standard (DES) used to be a highly influential block cipher [43], but was considered insecure for many applications due to short key length [44]. The U.S. National Institute of Standards and Technology (NIST) replaced DES with Rijndael algorithm which became the new Advanced Encryption Standard (AES) in 2001 [45]. Joint encryption and channel coding schemes have been studied in the literature [46-49]. In [50], a comprehensive review of physical layer security for wireless network is provided. Various secure channel coding schemes have been proposed for satellite communications [38, 39]. Furthermore, polar code for secret key generation was also proposed in [51-52]. Considering both security and reliability, we propose a secure SECCC-based channel coding scheme using an AES-encrypted puncturing. It efficiently provides both data secrecy and data reliability for the CR system.

In this contribution, we considered the following distributed matching algorithms which complement the PU-based algorithms in [14] and [16]:

1) SU-based CDA: In contrast to CDA of [14], we have implemented the SU-based CDA, where SUs compete among themselves and give offer to the PUs, in order to maximize the SU sum-rate.

2) SU-based PDA: The SUs cooperate among themselves and each SU offers a matching to its best PU in a round robin rotation manner, which maximizes the SU sum-rate. This is opposite to the PU-based PDA in [16].

3) All user-based PDA: All PUs and SUs cooperate among themselves by taking turns in a round robin manner to make offer to its best match. This provides an optimized sum-rate for both PUs and SUs.

The above study enables us to have a complete investigation on the performance of various distributed matching algorithms under the same family but with focus on different user groups. This comparative study is also conducted under idealistic CCMC-based scenario as well as under practical scenarios involving actual coding and modulation schemes. We have further enhanced the reliability and security of the system by invoking SECCC schemes that have unique puncturing patterns based on AES key.

The organization of the paper is as follows. Section 2 outlines the system model of our CCRN scheme, while the proposed spectral access strategies and coding schemes are presented in Section 3. Section 4 investigates the performance of all considered distributed matching algorithms under a range of idealistic and practical scenarios. Finally, our conclusion is offered in Section 5.

2. System Model

Similar to [14, 16] our model is based on the overlay cognitive radio system. Our system consists of M pairs of PU transmitter (Pt) and PU receiver (Pr) $(\{Pt_m, Pr_m\}_{m=1}^{M})$. The m^{th} pair has a rate requirement of $R_{PU_{m,req}}$, while each pair occupies a unique spectrum band of a constant size. Similarly, there are K pairs of SU transmitter (St) and SU receiver (Sr) $(\{St_k, Sr_k\}_{k=1}^{K})$, where the k^{th} pair has a rate requirement of $R_{SU_{k,req}}$, and each pair seeks to obtain access to a spectral-band occupied by a (Pt, Pr) pair. Each St offers to cooperate with the PU by relaying information between a unique (Pt, Pr) pair in exchange for permission to access the spectrum occupied by that unique (Pt, Pr) pair. **Fig. 1** shows the spectral access model, where T is the overall time period for the transmission between the (Pt_m, Pr_m) pair, while $\beta_{m,k}$ is the time allocation fraction having a value that is determined on the basis of the matching algorithm invoked, where $0 < \beta_{m,k} < 1$. During the time fraction T_0, Pt_m transmits its message to both the matched St_k and the destination Pr_m, During the time slot T_1, St_k forwards the message received from Pt_m towards Pr_m. Then, Pr_m applies maximal ratio combining technique for detecting the received signal. The freed spectrum is allocated to the (St_k, Sr_k) pair for its secondary transmission during the time slot $T_2 = (1-\beta_{m,k})T$.

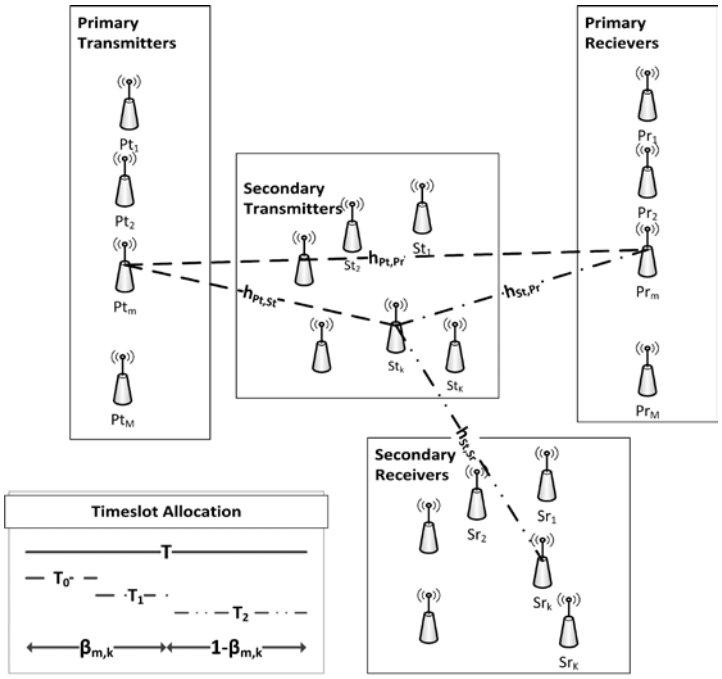

Fig. 1. Spectrum-access model for primary users and secondary users [16].

More specifically, the achievable sum-rate for the PU pair (Pt_m, Pr_m) based on the AF relaying protocol is given by [14] as:

$$R_{PU_{m,k}}(\beta_{m,k}) = \frac{\beta_{m,k}T}{2}\log_2\left(1+\frac{\gamma_{PU_m}|h_{Pt_m,Pr_m}|^2}{d^{\alpha}_{Pt_m,Pr_m}}+\frac{\gamma_{PU_m}\gamma_{SU_m}|h_{Pt_m,St_k}|^2|h_{St_k,Pr_m}|^2}{A+B+C}\right) \quad (1)$$

where, $A = d^{\alpha}_{St_k,Pr_m}\gamma_{PU_m}|h_{Pt_m,St_k}|^2$, $B = d^{\alpha}_{Pt_m,St_k}\gamma_{SU_k}|h_{St_k,Pr_m}|^2$, $C = d^{\alpha}_{Pt_m,St_k}d^{\alpha}_{St_k,Pr_m}$, and $\gamma_{PU_m} = \mathrm{P_S}/N_0$, $\gamma_{SU_k} = P_{St}/N_0$, while N_0 is the noise variance, P_S is the transmission power of Pt_m and P_{St} is the transmission power of St_k. Furthermore, h_{Pt_m,Pr_m}, h_{Pt_m,St_k} and h_{St_k,Pr_m} are the Rayleigh fading channel coefficients for the (Pt_m, Pr_m), (Pt_m, St_k) and (St_k, Pr_m) links, respectively, while d_{Pt_m,Pr_m}, d_{Pt_m,St_k} and d_{St_k,Pr_m} are the distances between the (Pt_m, Pr_m), (Pt_m, St_k) and (St_k, Pr_m) links, respectively. Finally, α is the pathloss exponent, which is given by and $\alpha = 4$ in our investigation.

The achievable sum-rate for the SU pair (St_k, Sr_k) is given by [14] as

$$R_{SU_{k,m}}(1-\beta_{m,k}) = (1-\beta_{m,k})T\log_2\left(1+\frac{\gamma_{SU_k}|h_{St_k,Sr_k}|^2}{d^{\alpha}_{St_k,Sr_k}}\right) \quad (2)$$

where h_{St_k,Sr_k} is the Rayleigh fading channel coefficient for the (St_k, Sr_k) link, while d_{St_k,Sr_k} is the distance between the (St_k, Sr_k) link. Note that Eq. (1) and Eq. (2) are based on the CCMC capacity, which implies that perfect channel coding and perfect modulation schemes are available for each communication link.

3. Proposed Matching Algorithm

The original PDA presented in [16] aims for obtaining the maximum data rate for the PU while SU gets a lower sum-rate, while CDA presented in [14] provides a slightly better SU sum-rate. Both these algorithms are PU initiated. We first present a SU-based CDA (CDA-SU) and a SU-based PDA (PDA-SU) which maximizes the SU rate while satisfying PU transmission requirement. Then, we make use of the PU-based algorithm of [16] and the SU-based algorithm proposed here for creating another algorithm, referred to as the ALL user-based PDA (PDA-ALL), which optimizes the sum-rate for both the PU and SU.

Our algorithm starts with the creation of a preference list named $SULIST_k$ by each St which has the list of all possible $Pt's$ that satisfies the minimum rate requirements of the specific St_k. The list is in descending order such that Pt which gives the highest sum-rate to the St is placed higher up. Similarly, each Pt has its own preference list named $PULIST_m$ of Sts that satisfy its sum-rate requirements.

3.1 CDA-SU

The main idea of our CDA-SU scheme is similar to the CDA scheme of [14], where an overlay cooperative paradigm is invoked. In contrast to the CDA, we present an SU-based algorithm where the (St_k, Sr_k) pair initiates the trade. The SU offers to relay the PU's message in exchange for a specific time allocation fraction denoted by $\beta_{m,k}$ for spectrum access to the (St_k, Sr_k) pair. Each St_k makes an offer to the first Pt_m in its preference list, to cooperatively relaying Pts message in return for a spectral access based on the time allocation factor $\beta_{m,k}$. If that St_k is also in the preference list of the intended Pt_m then they are matched. If that St_k is not in the $Pt_m's$ preference list $PULIST_m$ then St_k increases its relaying time offer $\beta_{m,k}$ by τ, where τ is the step size for time increment. If Pt_{curr} which is the already matched PU to St_{curr} which is the currently matched SU, receives a better offer from another St_k, then the current match will be rejected and Pt_{curr} will be matched to the new St_k. The algorithm continues until all of the Sts are matched to the Pts or until no more matchings are possible. The detailed algorithm is presented in Algorithm 1.

Algorithm 1 CDA-SU.

1) **Initialization**
   a) Set the initial *TS* allocation to $\beta_{init} = 0.01$, and set the step size of TS increment to $\tau = 0.05$.
   b) Construct $PULIST_m$ and $SULIST_k$, where *m* = {1, . . . , *M* } and *k* = {1, . . . , *K*}.
   c) Set k = 1 for the first transmission.
2) **Do the matching for the kth transmission.**
   a) SU_k offers $\beta_{m,k}$ to the first PU in its preference list Pt_m.
      i) If SU_k is not in the preference list of Pt_m then increase the TS allocation to $\beta_{m,k} = \beta_{m,k} + \tau$ and update both $PULIST_m$ and $SULIST_k$.

ii) If SU_k is in the preference list of Pt_m, then Pt_m and St_k are matched.

iii) If Pt_m is already matched to St_{curr}

A) If the St_k is higher up in the $PULIST_m$ than St_{curr}, then rematch Pt_m to St_k.

B) Else increase the *TS* allocation to $\beta_{m,k} = \beta_{m,k} + \tau$ and update $PULIST_m$ and $SULIST_k$.

b) If no more matchings are possible, set k=k+1 and goto step 2)-a).

3) If k=K, then the algorithm will stop.

The CDA-SU is a scheme where the SUs do not cooperate among themselves. Rather, they compete to find a better match for themselves for maximizing their own rate. The average rate of SU_k can be calculated based on [16] as:

$$r_k^S = E[R_k^S] \tag{3}$$

where $E[R_k^S]$ is the expected value of R_k^S, while R_k^S is the instantaneous achievable rate by the k^{th} SU and the superscript *S* denotes the selfish nature of the CDA-SU which is given by Eq. (2) i.e., $R_k^S = R_{SU_{k,m}}(1-\beta_{m,k})$. In line with [14] the proposed algorithm converge to a stable matching. After many rounds of exhaustive competition among the SUs for the acquisition of its best Pt_m, the SUs will give up on competing for the same PU as any further time slot increase will result in violation of the minimum rate requirement for that SU. At that time the matching will be stable because no further matching can be blocked [14].

3.2 PDA-SU

The basic idea of this algorithm is similar to [16] with the exception that the (St_k, Sr_k) pair initiates the offer to the (Pt_m, Pr_m) pair for cooperatively relaying their messages. The main difference between the PDA and CDA is that in CDA there is a competition amongst the offerers (in our case SUs) for trying to get the best match for themselves. This competition results in a lot of $\beta_{m,k}$ adjustments which gives a lower sum-rate for the SUs. Therefore, CDA will take longer to converge to a stable equilibrium thus making it computationally extensive or complex. To overcome this competition among the Sts, we generate a priority access list known as *ALIST* for the Sts. Then SUs will take turns to select the best available PU according to a round-robin type priority access list. The *ALIST* will decide which St has the right to choose its best possible match while others will have access to the best possible matches in the order according to the $ALIST_i$. In the next round, the last St in the $ALIST_i$ will jump up to the top while others will move a step downwards i.e., ($ALIST_1 = \{St_1, St_2, ..., St_K\}$, $ALIST_2 = \{St_K, St_1, ..., St_{K-1}\}$ and so on). The first St_k in $ALIST_i$ will have access to the best possible Pt_m in its preference list provided that St_k is also in the $Pt_m s$ preference list $PULIST_m$. Then the second St_k in the list selects the best available Pt_m from the remaining set of PUs. The algorithm goes on for *K* rounds such that

each of the K pairs of (St_k, Sr_k) has appeared in the top of $ALIST$ once. The process is then repeated many times, which forms a repeated game [53, 54]. The maximum TS allocation representing the maximum transmission period for the SU is given by [16] as:

$$\beta_{m,k}^{\max} = 1 - \frac{R_{SU_{k,req}}}{\log_2\left[1+\gamma_{SU} \mid h_{St_k,Sr_k} \mid^2\right]} \tag{4}$$

where $R_{SU_{k,req}}$ is set to a fixed value, which becomes the minimum sum-rate requirement for the SU. The minimum TS allocation is given by [16] as:

$$\beta_{m,k}^{\min} = \beta_{m,k} \frac{R_{PU_{m,req}}}{R_{PU_{m,k}}(\beta_{m,k})} \tag{5}$$

where $R_{PU_{m,req}} = T\log_2\left[1+\frac{\gamma_{PU} \mid h_{Pt_m,Pr_m} \mid^2}{d_{Pt_m,Pr_m}^{\alpha}}\right]$ is the achievable PU rate without relaying and $R_{PU_{m,k}}(\beta_{m,k})$ is given by Eq. (1). The detailed algorithm for PDA-SU is presented in Algorithm 2.

The rate of SU_k for PDA-SU can be derived based on [16] as:

$$R_k^C = \frac{1}{N}\sum_{k=1}^{K} R_{k,m}^{SU}(1-\beta_{m,k}) \tag{6}$$

where the superscript C represents the cooperative nature of PDA-SU, while $N = \min\{M, K\}$. The average rate of SU_k after many repetitions can then be calculated from [16] as:

$$r_k^C = E[R_k^C] \tag{7}$$

where $E[R_k^C]$ is the expected value of R_k^C.

Algorithm 2 PDA-SU.

1) Initialization

a) Set up the first priority list $ALIST_1 = \{St_1, St_2, ..., St_K\}$.

b) Compute $\beta_{m,k}^{min}$ and $\beta_{m,k}^{max}$.

c) Set i = 1 for the first round.

2) Matching for the *i*th round

a) Set the initial TS allocation to $\beta_{init} = \beta_{m,k}^{min}$, and set the step size of TS increment to $\tau = 0.05$.

b) Construct $PULIST_m$ and $SULIST_k$, where $m = \{1, ..., M\}$ and $k = \{1, ..., K\}$. Set j = 1 for the first transmission.

c) Do the matching for j^{th} transmission.

i) Find the corresponding St_k for transmission, based on the $ALIST_i$ (i.e) j^{th} element of $ALIST_i$.

ii) St_k selects the best available Pt_m from its $SULIST$ and offer a time slot $\beta_{m,k}$

A) If SU_k is in the preference list of Pt_m then Pt_m and St_k are matched.

B) If SU_k is not in the preference list of Pt_m then increase the TS allocation to $\beta_{m,k} = \beta_{m,k} + \tau$ and update both $PULIST_m$ and $SULIST_k$.

C) If $SULIST_k$ is empty, then St_k is left unmatched.

iii) Set $j = j + 1$ and goto step 2)-c) until $j = K$.

3) Set $i = i + 1$ and goto step 2 for the next round, until $i = K$.

The CDA presented in [14] and the CDA-SU in Section 3.1 are best for a one-shot game where there is no cooperation among the PUs or SUs. The downside is that the PUs in CDA (or SUs in CDA-SU) compete among the PUs (or SUs), resulting in lower average achievable PU (or SU) sum-rate. Note that the spectrum sharing between the PUs and SUs may last for a longer time period which can be viewed as a repeated game of many rounds. PDA in [16] proposed another strategy, where PU players form a coalition where they cooperate based on their individual reputation and their mutual trust. To keep the players in the game, there is a punishment strategy as discussed in [16] which helps to maintain stability in the algorithm. If a player deviates from the PDA, then there will be a limited duration punishment for all the players, where all PUs will switch to the CDA-based game which gives lower rate to all PU players. It has been shown in [16] that the average rate of a PDA-based scheme is higher than the CDA-based scheme. The PDA-SU proposed here is based on the same idea, where all SUs will switch to the CDA-SU arrangement whenever an SU deviates from the game, for a limited period as a form of punishment. Based on [16] our punishment period was found to be:

$$T_p > \max_k \frac{R_k^D - R_{SU_{k,req}}}{r_k^C - r_k^S} \tag{8}$$

where $R_k^D = R_k^S - R_k^C > 0$ is the deviation gain for the SU at a particular time, while r_k^S and r_k^C are given in Eqs. (3) and (7), respectively. Hence as long as T_p satisfy Eq. (8), the one-time payoff under the non-cooperative CDA-SU strategy would be negated by punishment. CDA-SU and PDA-SU algorithms are designed to maximize the SU sum-rate. Therefore, application example for this scenario can be a situation where the PUs have low sum-rate requirements with higher link reliability as the SUs will be providing link reliability in the form of providing cooperative diversity. Furthermore, SUs are users with higher sum-rate requirements.

3.3 PDA-ALL

We see that the original PDA discussed in [16] maximizes the sum-rate for the PU making it less attractive for the SU, while the PDA-SU algorithm discussed in Section 3.2 maximizes the sum-rate for the SU, consequently making it less desirable for the PU. Here we propose another scheme namely the PDA-ALL scheme, which creates a balance between the achievable sum-rates for both PU and SU. Our algorithm banks on the idea of coalition-based games, where we divide the game into two stages. The algorithm as seen in Algorithm 3 starts by setting up both $ALIST_{PU_m}$ and $ALIST_{SU_k}$ which constitute the priority lists for PU and SU for their specific stages. During the first stage all the PUs form a coalition as in [16] to match the PUs to their corresponding SUs in a round robin rotation manner. The stage lasts for M rounds where during each round the $ALIST_{PU_m}$ is updated in a similar fashion as in the PDA algorithm of [16] and the PUs are matched to the SUs according to that specific list. After the

completion of the first stage, the game enters its second stage where all the SUs form a coalition as discussed in PDA-SU of Section 3.2 to match to the corresponding PUs. This stage will last for a total of K rounds. Hence, a single completed cycle of PDA-ALL lasts for $M+K$ rounds such that each of the *Pts* and *Sts* has at least a chance to select its best match.

Algorithm 3 PDA-ALL.

1) **Initialization**
   a) Set up the first priority lists $ALIST_{PU_m}=\{Pt_1, Pt_2, ..., Pt_M\}$ for PU and $ALIST_{SU_k}=\{St_1, St_2, ..., St_K\}$ for SU.
   b) Compute $\beta_{m,k}^{min}$ and $\beta_{m,k}^{max}$.
2) **Stage I:**
   a) PDA Matching.
      i) Set $i=1$ for the first round.
   b) Algorithm of [16], under Section III.B.3: steps 2 and 3, for M rounds.
3) **Stage II:**
   a) PDA-SU Matching.
      i) Set $i=1$ for the first round.
   b) Algorithm 2: steps 2 and 3, for K rounds.

The rate of PU_m for PDA-ALL can be derived as:

$$\bar{R}_m^C=\frac{1}{2}\left[\frac{1}{N}\sum_{m=1}^{M}R_{m,\mathrm{k}}^{PU}(\beta_{m,k}^{PU})+\frac{1}{N}\sum_{m=1}^{M}R_{m,\mathrm{k}}^{PU}(\beta_{m,k}^{SU})\right] \tag{9}$$

while the rate of SU_k for PDA-ALL was found to be:

$$\bar{R}_k^C=\frac{1}{2}\left[\frac{1}{N}\sum_{k=1}^{K}R_{k,m}^{SU}(1-\beta_{m,k}^{PU})+\frac{1}{N}\sum_{k=1}^{K}R_{k,m}^{SU}(1-\beta_{m,k}^{SU})\right] \tag{10}$$

We can see from Eqs. (9) and (10) that the average sum-rate will be the same irrespective of whether we begin the PDA-ALL with PDA first or PDA-SU first.

Similar to the PDA in [16] and PDA-SU in Section 3.2, PDA-ALL also does not converge to a stable equilibrium in a single-shot game, where players will be inclined to deviate from the game if they receive a better offer from another SU or PU. To avoid deviation, we employed the repeated game scenario and also invoked a punishment strategy to enforce the players to stay in the game. In PDA-ALL, the punishment will have to be imposed on both the PU and SU. Here, we consider a game in which if any PU opts out of cooperation then the game will immediately switch to the PDA-SU resulting in a lower sum-rate for the PU, which will discourage the PUs from deviating. On the contrary, if any SU opts out of cooperation then the game will switch to the PDA, which will result in lower sum-rate for the SU and hence would discourage SUs from deviating. More specifically, when a PU deviates during the PDA stage, the punishment period can be derived as:

$$T_{P,PU}>\max_m\frac{(R_k^S-R_k^C)-R_{PU_{m,req}}}{E[R_m^C]-E[\mathrm{R}_m^S]} \tag{11}$$

where $E[R_m^S]$ is the expected value of R_m^S, while R_m^S is the instantaneous achievable rate by the m^{th} PU in a selfish mode which is given by Eq. (1) and $E[R_m^C]$ is the expected value of R_m^C, while R_m^C is the instantaneous achievable rate by the m^{th} PU in cooperative mode which is given by $R_m^C = \frac{1}{N}\sum_{m=1}^{M} R_{m,\mathrm{k}}^{PU}(\beta_{m,k}^{SU})$. Furthermore, $R_{PU_{m,req}} = T\log_2\left[1+\frac{\gamma_{PU}\,|\,h_{Pt_m,Pr_m}\,|^2}{d_{Pt_m,Pr_m}^{\alpha}}\right]$ is the achievable PU rate without relaying. Similarly, when a SU deviates during the PDA stage, the punishment period can be derived as:

$$T_{P,\mathrm{SU}} > \max_k \frac{(R_k^S - R_k^C) - R_{SU_{\mathrm{k},req}}}{r_k^C - r_k^S} \tag{12}$$

where r_k^S and r_k^C are given in Eqs. (3) and (7), respectively.

Hence, both groups of PU and SU players will be discouraged to opt out of cooperation as long as punishment periods satisfy Eqs. (11) and (12). The game will be repeated many times in the same way and any deviation from the game will result in a lower overall sum-rate for the players. Therefore, the game will converge to an equilibrium in the repeated game enforced by the threat of a limited duration punishment. Hence, the players will learn to stay in the game for a better overall sum-rate. More specifically, PDA-ALL can be deployed in situations where the sum-rate requirements for both set of users is higher.

PDA is a pareto optimal algorithm which maximize the PU sum-rate, while PDA-SU is also a pareto optimal algorithm with the aim to maximize the SU sum-rate. An algorithm is in pareto optimal state when the profit of one party cannot be increased without reducing the profit of another. Therefore, PDA maximizes the PU sum-rate and hence gives a lower sum-rate to the SU, on the other hand PDA-SU maximizes the SU sum-rate giving lower sum-rate to the PU (PU sum-rate is still better than the case when no matching is done). Finally, PDA-ALL algorithm is another pareto optimal algorithm where the convergence point is between the two extremes i.e., PDA and PDA-SU.

3.4 CODING AND MODULATION DESIGN

To make our system more realistic, we employ real coding and modulation to compute the practically achievable rates for all users in addition to the idealistic shannon capacity. Having both idealistic and realistic systems would make the paper to be more appealing to both theorists and engineers. We considered both AF and DF cooperative relaying protocol for our system. For the DF, we provide the results based on the CCMC capacity, Discrete input Continuous output Memoryless Channel (DCMC) capacity and SECCC BER performance. We first considered the idealistic situation when the system will operate at the CCMC [32] capacity for each communication link where perfect coding and perfect modulation are assumed. Then we also considered the DCMC capacity, where perfect coding is assumed. Finally, for a more realistic scenario, the system will be investigated when practical SECCCs employing Iterative Decoding (SECCC-ID) [34, 35] are invoked in conjunction with the QAM modulation.

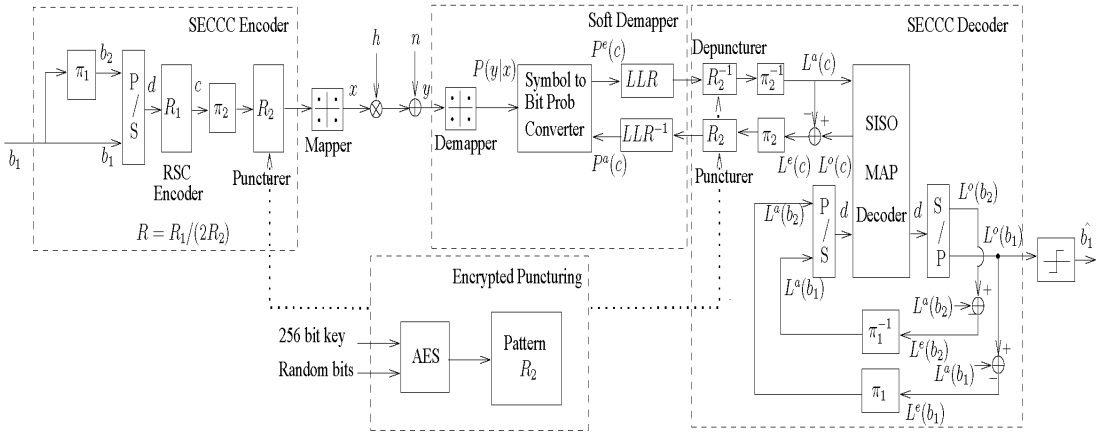

Fig. 2. Binary SECCC-ID system, with AES Encrypted Puncturing.

Our model makes use of the low complexity and bandwidth efficient SECCC-ID scheme as shown in **Fig. 2**. The bit-based SECCC design [55] employs a binary Recursive Systematic Convolutional (RSC) code as constituent code which eliminates the inherited mismatch caused by the symbol-based TCM design of [34] for creating flexible SECCC schemes which are capable to operate in both AWGN and uncorrelated Rayleigh fading enviornment [35]. We employ an Adaptive SECCC (ASECCC) scheme where a higher order modulation scheme is used when the link quality improves to enhance the throughput. The effective throughput range is given by $\eta = \{0,1,1.5,2,3,4,5\}$ bits per symbol (BPS) when there is no-transmission, 4QAM, 8QAM, 16QAM, 32QAM, 64QAM and 256QAM are considered, respectively. The SECCC based mode switching thresholds $\Gamma = [\gamma_0, \gamma_1, ..., \gamma_6]$ were found on the basis of BER performance curves of different code-rates and modulation schemes in multipath fading channels as shown in **Fig. 3**. The thresholds are considered at a BER of less than or equal to 10^{-5}, which are given by $\Gamma_{SECCC} = [5,8,11,17,21,24]$ dB. By contrast the CCMC capacity-based switching thresholds are given as $\Gamma_{CCMC} = [1,4,6.5,10.5,14,17]$ dB, while those of DCMC capacity are given by $\Gamma_{DCMC} = [2,5,8,12.5,16,20]$ dB based on the capacity versus SNR curves. Additionally, we introduce a physical layer security measure to our algorithms by incorporating SECCC with AES encryption scheme. The basic principle of the operation is the puncturing pattern which is determined by the AES encrypted secure key.

The notations *P*(.) and *L*(.) in **Fig. 2** represents the logarithmic symbol probabilities and Likelihood Ratio (LLR) of the bit probabilities, respectively, where *b* represents the information bit and *c* represents the coded bits. Similarly, *a*, *o* and *e* in **Fig. 2** represents the *a priori*, *a posteriori* and *extrinsic* information for various probabilities and LLRs. As shown in **Fig. 2**, information bit sequence $\{b_1\}$ is first interleaved with π_1 and then fed to RSC encoder after the parallel-to-serial (P/S) conversion. The RSC Encoder is systematic where the original information appears in its coded output. The code rate is represented by R_1 which is set to $R_1 = 1/2$. This means that each information bit would be encoded to four output bits. This can be explained by the fact that the sequence $\{b_2\}$ is a repeated but interleaved version of the original sequence $\{b_1\}$. These encoded bits are passed through

another interleaver π_2 (Channel Interleaver) which scrambles them and feeds them to the puncturer. It helps remove burst errors from occurring in the symbols during their transmission from an uncorrelated Rayleigh fading channels. The puncturer here is to remove bits, based on the AES encrypted random pattern with the puncturing rate R_2 as represented by (Encrypted Puncturing) block. This pattern is random and secure because it is generated by a private key that is only known to both the sender and receiver. For $R_2 = 1/2$ one bit out of two are punctured by the AES encrypted random pattern from the data stream. The AES block generates this pattern, as shown in **Fig. 2**, where a 256 bit key and random bits are used as its input. Different patterns for puncturing can be generated by changing the key length. More specifically, the AES block would produce a puncturing pattern having the same length as the SECCC encoded sequence $\{c\}$. The number of ones in the puncturing pattern equals to the desired number of unpunctured bits according to R_2. This puncturing pattern is then used to remove bits in $\{c\}$ whenever it has a value of zero in the pattern, and to retain the bit whenever it has a value of one in the pattern. The overall code rate of SECCC encoder is given by $R = R_1 / (2\,\mathrm{R}_2)$. The output of the SECCC encoder goes to the modulator block represented as (Mapper) in which *M*-ary QAM is implemented, where $M \in \{4,8,16,32,64,256\}$. The signal received from the channel can be written as;

$$y = hx + n,$$

where, h is the uncorrelated Rayleigh fading channel coefficient, n is the noise having a variance of $N_0/2$ per dimension and x is the transmitted *M*-ary QAM symbol. This received signal y will firstly pass through the soft demapper, which calculates the conditional PDF of the received symbol. The PDF values are then converted into extrinsic bit probabilities by the Symbol-to-Bit Probability Converter of **Fig. 2** [35]. These extrinsic bit probabilities are then transformed to the equivalent bit-based Log

Likelihood Ratios (LLRs), which are then passed through a soft depuncturer R_2^{-1} which inserts zero LLRs on the position of the bits which were punctured through the AES-encrypted random pattern. The LLRs are then deinterleaved π_2^{-1} and fed to the SISO MAP decoder [56]. The decoder in **Fig. 2** shows a self-concatenated decoder which makes iterations with itself. It computes the extrinsic LLRs, $L_e(\mathrm{b}_1)$ and $L_e(\mathrm{b}_2)$. The extrinsic LLRs are interleaved to get the a-priori LLRs $L_a(\mathrm{b}_1)$ and $L_a(\mathrm{b}_2)$ of the information bits, as shown in **Fig. 2**. The decoding continues for a fixed number of iterations, which in our case is fixed to 4.

The binary SECCC scheme shown in **Fig. 2** has the ability to exchange soft information with the demapper. In addition to having inner iterations in the outer SECCC decoder in **Fig. 2**, there are a fixed number of outer iterations that are invoked in order to exchange the extrinsic information between the SECCC Decoder and Soft Demapper. The extrinsic LLRs of the codeword $L_e(c)$ are fed back to the Soft Demapper by the SISO Decoder. These LLRs are interleaved and punctured through AES generated pattern according to R_2. Then they are converted to the *a-priori* bit probabilities $P_b^a(c)$ by the LLR^{-1} block in **Fig. 2**, which are then fed to the Soft Demapper. The Soft Demapper converts these bit probabilities to symbol

probabilities which provides the enhanced extrinsic LLR $L_e(c)$ of the codeword at its output. This completes the outer iteration between the SISO Decoder and the Soft Demapper. We found from our investigation that introducing the AES puncturing pattern does not degrade the error performance but makes our transmissions more secure as seen in **Fig. 4**. This is very beneficial because the AES-based puncturing would make our transmission in each link to be more secure, without compromising the performance.

4. Results and Discussion

Table 1 shows the simulation parameters for the proposed scheme.

Table 1. Simulation Parameters

Modulation	{4, 8, 16, 32, 64, 256}-QAM
Coding and Modulation type	CCMC, DCMC, SECCC-ID
Number of frames	10^5
Channel	Rayleigh fading channel
Total number of PUs	8
Total number of SUs	10
Step size	$\tau = 0.05$
Path loss exponent	$\alpha = 4$

4.1 Performance of the proposed schemes versus the PU-based schemes

Fig. 5, **Fig. 6** and **Fig. 7** show the average total sum-rate of the matched (Pt, Pr), (St, Sr) and $\{(Pt, Pr), (St, Sr)\}$ pairs versus the total number of SUs, $K = \{2, 3, ..., 10\}$ for the AF-based CCRN schemes, while the total number of PUs is fixed to $M = 8$. Note that these AF-based results assumed perfect coding and perfect modulation schemes are available for communicating at the CCMC capacity. In the figures, PDA is from [16] and CDA is from [14], CDA-SU and PDA-SU are the algorithms presented in Section 3.1 and Section 3.2, respectively. We assume that all the SUs have the same transmit SNRs of $\gamma_{SU} = 25$ dB or $\gamma_{SU} = 15$ dB, while the transmit SNR of all PUs is fixed to $\gamma_{PU} = 10$ dB. Other simulation parameters chosen are given in **Table 1**, which are similar to the parameters that were used in [16] so that we can have a fair comparison.

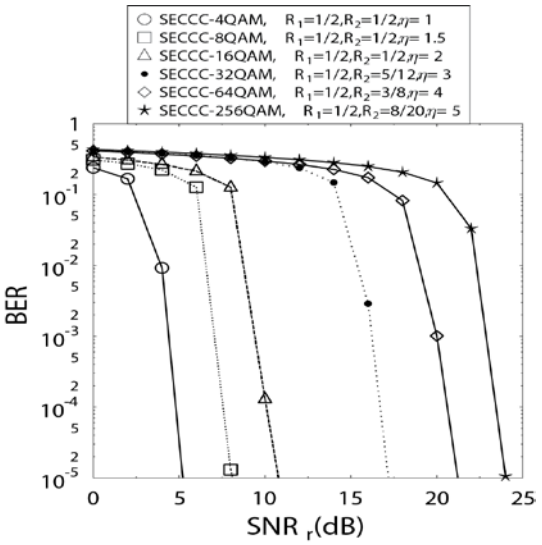

Fig. 3. The BER versus SNR performance of SECCC using frame length of 120,000 symbols, when communicating over Rayleigh channels.

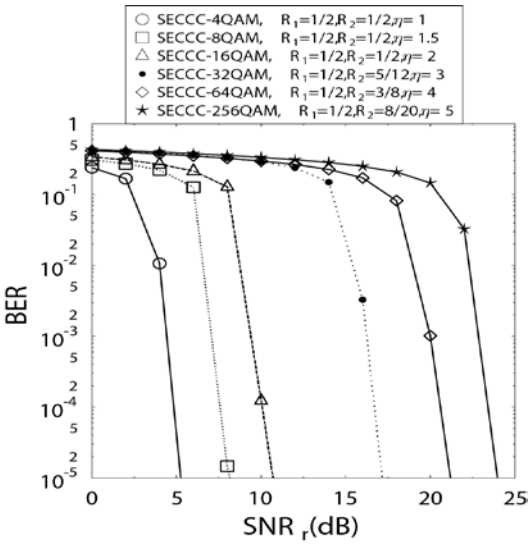

Fig. 4. The BER versus SNR performance of AES-based Secure SECCC using frame length of 120,000 symbols, when communicating over Rayleigh channels.

It is evident from **Fig. 5** that PDA achieves the best PU sum-rate of all, while CDA being the other PU-based scheme also performs better than PDA-SU and CDA-SU in terms of PU sum-rate. **Fig. 6** shows the SU sum-rate of these matching schemes.

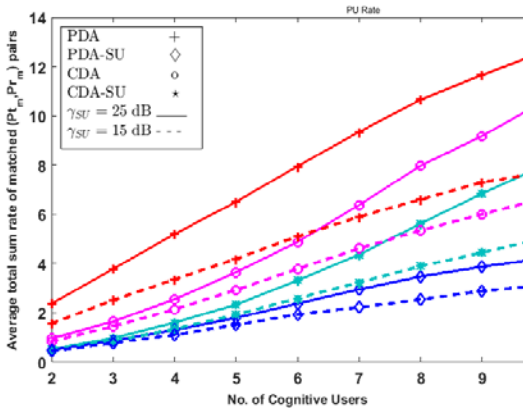

Fig. 5. PU sum-rate for matched (Pt, Pr) pair for CCRNs AF, where $\gamma_{PU} = 10$ dB.

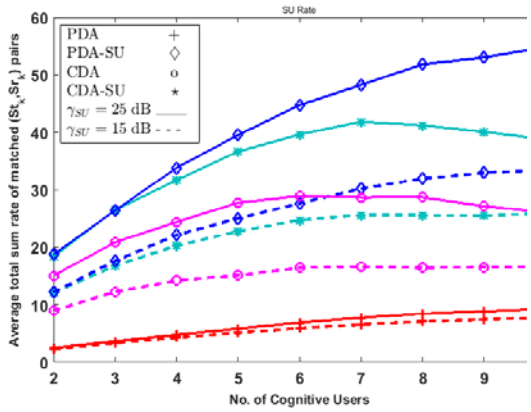

Fig. 6. SU sum-rate for matched (St, Sr) pair for CCRNs AF, where $\gamma_{PU} = 10$ dB.

We see that our SU-based schemes achieve a much higher SU sum-rate as compared to the PU-based PDA and CDA schemes. Even in the $\gamma_{SU} = 15$ dB case we see that our schemes are better in terms of SU sum-rate. We see that for cases of $K < 4$ both the PDA-SU and CDA-SU performs almost similarly while for $K > 3$ we see that PDA-SU outperforms CDA-SU. This is because for $K < 4$, there are less number of SUs competing for $M = 8$ PUs and almost all SUs end up getting the major share in the sum-rate because of minimal competition among the SUs to match with their desired PUs. As the number of SUs increases beyond 7 we see that the sum-rate of the CDA-SU schemes drop due to excessive competition

among the SUs for the acquisition of their best PUs. The PU-based CDA scheme also shows a similar trend in **Fig. 5**, where for a lower number of SUs, we see rising competition among the PUs resulting in a lower PU sum-rate, while SUs benefit from that and get a better share of sum-rate as shown in **Fig. 6**. As the number of SUs increases we see that the total SU sum-rate drops for both the CDA and CDA-SU because more SUs are competing for the limited resources offered by 8 PUs.

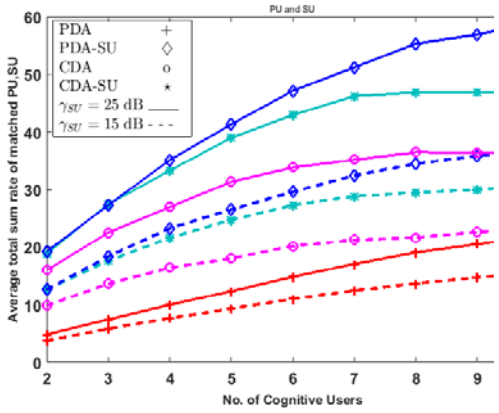

Fig. 7. Total sum-rate of matched PU+SU for CCRNs AF, Where $\gamma_{PU} = 10$ dB.

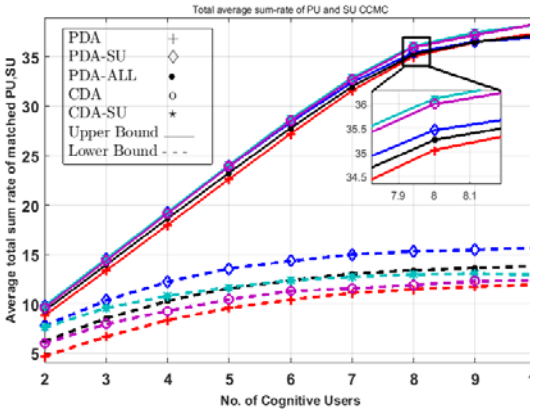

Fig. 8. Average total sum-rate of PU and SU for CCMC aided DF-based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

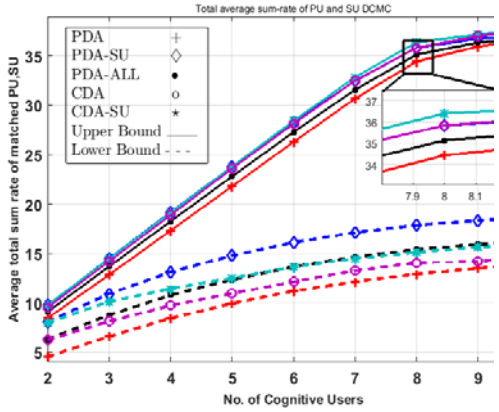

Fig. 9. Average total sum-rate of PU and SU for DCMC aided DF-based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

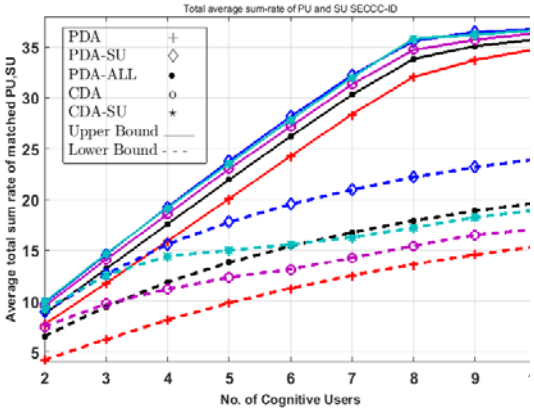

Fig. 10. Average total sum-rate of PU and SU for SECCC aided-DF based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

Fig. 7 shows the total sum-rate of the PUs and SUs which follows the trend in **Fig. 6**. Here we see that the SU-based schemes achieve the best overall sum-rate as compared to the PU-based PDA and CDA. We can see that for $K = 8$, PDA-SU,CDA-SU, CDA and PDA gives a total sum-rate of 56 BPS, 48 BPS, 38 BPS and 20 BPS, respectively. In our simulation setup shown in **Fig. 1**, the SU-based schemes are the ones which ensure high sum-rate as compared to the PU-based schemes. This trend can be explained as follows. In our simulation, the γ_{SU} is higher than γ_{PU} and the transmission distance between St and Sr is shorter than that between

Pt and Pr which results in a lower path loss for SUs compared to PUs. Hence, a higher achievable rate is available for SUs as compared to PUs. In this condition, it is reasonable to expect a higher overall sum-rate when SU-based schemes are employed, as compared to the PU-based schemes. This is practical because a Pt-Pr pair would prefer to cooperate with a group of SUs located between the Pt and Pr, which would provide a higher relaying gain as opposed to those SUs that are located far away from the PUs. In this scenario, the SUs are closer to each other resulting in a lower path loss.

Similar trends follow when we consider the DF-based CCRN schemes where CCMC, DCMC and SECCC are considered. We see from **Fig. 8**, **Fig. 9** and **Fig. 10** that the SU-based schemes give high sum-rate as compared to the PU-based schemes. The lower and upper bound represent the achievable sum-rate for the DF-based scheme. The lower bound is the most widely used method where the achievable capacity is considered to be limited by the weakest link and is given by [16]:

$$R_{m,k}^{lower} = \frac{1}{2}\min\{R_{Pt_m\_St_k}, R_{St_k\_Pr_m}\} \tag{1}$$

while the upper bound represents the achievable rate for the scenario where we assume that the St has enough storing capacity for the data arriving from the Pt, so that it always has enough data to be transmitted to the Pr and is given by [16]:

$$R_{m,k}^{upper} = \frac{1}{2}\{R_{Pt_m\_St_k} + R_{St_k\_Pr_m}\} \tag{2}$$

where $R_{Pt_m\_St_k}$ denotes the achievable rate between the PU transmitter Pt_m and the SU transmitter link St_k while $R_{St_k\_Pr_m}$ denotes the achievable rate between the SU transmitter St_k and the PU receiver Pr_m. From **Fig. 8**, **Fig. 9** and **Fig. 10**, we observe that the upper bound results are a bit compact where we see only slight improvement in the SU-based schemes. By contrast, we see a clear difference in the lower bound performance results. In terms of lower bound, we see that PDA-SU achieves the best sum-rate while CDA-SU comes second. Here we see a similar trend as was seen in the AF-based CCRN of **Fig. 7**, where the PDA-SU and the CDA-SU starts off with similar performance for upto $K = 3$, while the gap increases as we increase the number of SUs. It can be seen from **Fig. 7**, **Fig. 8**, **Fig. 9** and **Fig. 10**, that the proposed scheme achieves higher average total sum-rate for both PU and SU as compared to the PDA and CDA algorithms. On the other hand, **Fig. 5** shows that the PU average total sum-rate is lower for the proposed scheme as compared to its PU-based counterparts. Let us now look at the PDA-ALL scheme, which can provide a more balanced sum-rate for both PU and SU.

4.2 Performance of PDA-ALL versus PDA and PDA-SU

As evident from **Fig. 11**, **Fig. 12** and **Fig. 13**, we see that the PDA-ALL scheme minimizes the gap between the achievable sum-rate for PU and SU. We see that the PDA-ALL scheme is more favorable to both the PU and SU, unlike the PDA and PDA-SU which maximizes the sum-rate for one group of players only. We can see from **Fig. 11**, where perfect coding and perfect modulation schemes are assumed, that for the case when $K = 10$, the sum-rate of PU for PDA in [16] is 29 BPS, while for SU the sum-rate is 8 BPS therefore there is a sum-rate gap of 21 BPS for the achievable sum-rate for PU and SU. Similarly, for the PDA-SU the sum-rate for PU is 13 BPS while the sum-rate for SU is 23 BPS which gives a sum-rate gap of 10 BPS for the achievable sum-rate of PU and SU. Similar trend can be seen for the CDA algorithms.

From **Fig. 11** we can see that the sum-rate gap is the minimum when we consider the PDA-ALL scheme which gives a sum-rate gap of approximately 5 BPS. Similar trend can be seen in **Fig. 12**, where perfect coding is assumed. Explicitly, we see a sum-rate gap of approximately 4 BPS in **Fig. 12**. Finally, when employing actual coding, which in our system we have the AES assisted SECCC scheme, the sum-rate gap of approximately 3 BPS is observed for the PDA-ALL in **Fig. 13**, which is the minimum compared to other distributed matching algorithms.

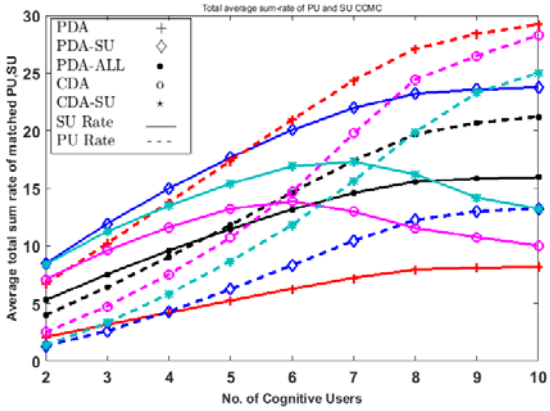

Fig. 11. Average total sum-rate of PU and SU for CCMC aided DF-based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

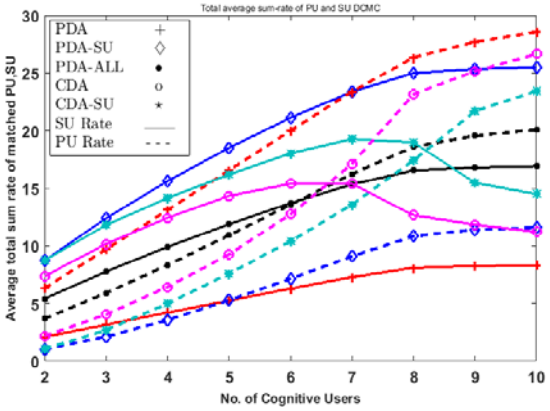

Fig. 12. Average total sum-rate of PU and SU for DCMC aided DF-based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

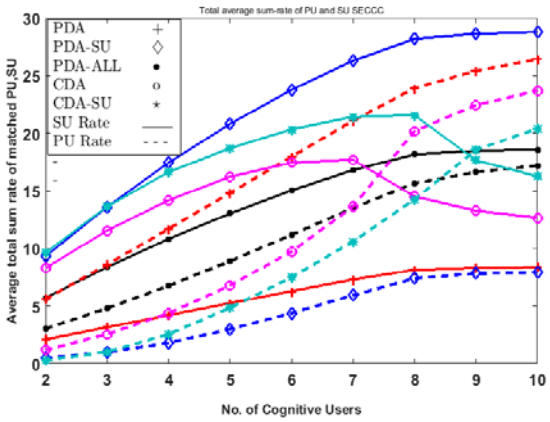

Fig. 13. Average total sum-rate of PU and SU for SECCC aided DF-based CCRNs, where $\gamma_{SU} = 35$ dB, and $\gamma_{PU} = 20$ dB.

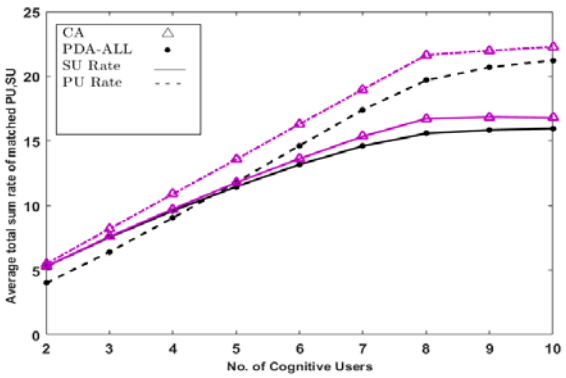

Fig. 14. PDA-ALL Vs CA for CCMC aided DF-based CCRNs.

Fig. 14 presents a comparison of the proposed PDA-ALL algorithm with the Centralized Algorithm (CA) for the CCMC aided DF-based CCRNs. Results shows that PDA-ALL algorithm performs very close to CA where a central controller performs all the matchings. CA can be assumed to be global optimal as no further enhancement is possible. The performance of PDA-ALL is very close to CA with considerably less complexity. CA will perform all possible permutations for matching for sum-rate maximization while PDA-ALL

on the other hand will make a priority list and do its matching based on that priority list. Hence, PDA-ALL is a less complex yet highly efficient matching algorithm.

5. Conclusion

In this paper, we investigated a range of distributed matching algorithms including CDA-SU and PDA-SU which maximize the SU sum-rate. Results confirm that our proposed SU-based algorithms provided a higher SU sum-rate. Secondly, we observed that the SU-based algorithms outperformed the PU-based algorithms in terms of the combined sum-rate for both the PU and SU. We also proposed an algorithm for maximizing the sum-rates of both PU and SU groups namely PDA-ALL. We showed that it would be beneficial to use different schemes for different applications i.e., PU-based, SU-based and All User-based schemes. We analyzed our schemes under the idealistic scenario involving perfect coding and perfect modulation, as well as under practical scenario involving actual coding and actual modulation. We considered adaptive coded modulation based DF schemes for our practical scenario for transmission flexibility and efficiency. More specifically, we employed secure SECCC scheme and showed that the added security feature does not degrade the performance as compared to standard SECCC.

References

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb 2005. Article (CrossRef Link)
[2] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, May 2009. Article (CrossRef Link)
[3] W. D. Horne, "Adaptive spectrum access: Using the full spectrum space," *The MITRE Corporation McLean*, VA, Tech. Rep., 2003.
[4] R. Gibbons, "Game Theory for Applied Economist," *Princeton University Press*, 1992.
[5] M. Shubik, "Game Theory in the Social Sciences," *MIT Press*, 1982.
[6] A. J. McKenzie, "Evolutionary Game Theory," *The Stanford Encyclopedia of Philosophy*, 2009.
[7] Z. Han,Y. Gu, and W. Saad, *Matching Theory for Wireless Networks*, Springer International Publishing, 2017. Article (CrossRef Link)
[8] E. C. van der Meulen, "Three-terminal communication channels," *Advances in Applied Probability*, vol. 3, no. 1, pp. 120–154, 1971. Article (CrossRef Link)
[9] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3062–3080, Dec 2004. Article (CrossRef Link)
[10] T. Luan, F. Gao, X. D. Zhang, J. C. F. Li, and M. Lei, "Rate maximization and beamforming design for relay-aided multiuser cognitive networks," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1940–1945, May 2012. Article (CrossRef Link)
[11] K. Lee and A. Yener, "CTH17-4: Outage performance of cognitive wireless relay networks," in *Proc. of IEEE Globecom 2006*, Nov 2006, pp. 1–5. Article (CrossRef Link)
[12] J. Jia, J. Zhang, and Q. Zhang, "Cooperative relay for cognitive radio networks," in *Proc. of INFOCOM 2009, IEEE*, April 2009, pp. 2304–2312. Article (CrossRef Link)
[13] P. Lin, J. Jia, Q. Zhang, and M. Hamdi, "Dynamic spectrum sharing with multiple primary and secondary users," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 4, pp. 1756–1765, May 2011. Article (CrossRef Link)

[14] S. Bayat, R. H. Y. Louie, Y. Li and B. Vucetic, "Cognitive radio relay networks with multiple primary and secondary users: distributed stable matching algorithms for spectrum access," in *Proc. of 2011 IEEE International Conference on Communications (ICC), Kyoto*, pp. 1-6, 2011. Article (CrossRef Link)
[15] S. Bayat, R. H. Y. Louie, B. Vucetic, and Y. Li, "Dynamic decentralised algorithms for cognitive radio relay networks with multiple primary and secondary users utilising matching theory," *Transactions on Emerging Telecommunications Technologies*, vol. 24, no. 5, pp. 486–502, 2013. Article (CrossRef Link)
[16] W. Liang, S. X. Ng, J. Feng, and L. Hanzo, "Pragmatic distributed algorithm for spectral access in cooperative cognitive radio networks," *IEEE Transactions on Communications*, vol. 62, no. 4, pp. 1188–1200, April 2014. Article (CrossRef Link)
[17] P. Rawat, M. Haddad, and E. Altman, "Towards Efficient Disaster Management: 5G and Device to Device Communication," in *Proc. of 2015 2nd International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, Rennes, pp. 79-87, 2015. Article (CrossRef Link)
[18] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of Wireless Communication Technologies for Public Safety," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 619-641, Second Quarter 2014. Article (CrossRef Link)
[19] A. Orsino, L. Militano, G. Araniti, A. Molinaro, and A. Iera, "Efficient Data Uploading Supported by D2D Communications in LTE-A Systems," in *Proc. of Proceedings of European Wireless 2015; 21th European Wireless Conference*, Budapest, Hungary, 2015, pp. 1-6. Article (CrossRef Link)
[20] H. Tang and S. Watson, "Cognitive Radio Networks for Tactical Wireless Communications," *Scientific Report*, No. DRDC-RDDC-2014-R185, Defence Research and Development Canada-Ottawa Research Centre Ottawa, Ontario Canada, 2014. Article (CrossRef Link)
[21] Y. Saleem, M. H. Rehmani, and S. Zeadally, "Integration of Cognitive Radio Technology with Unmanned Aerial Vehicles: Issues, Opportunities, and Future Research Challenges," *Journal of Network and Computer Applications*, vol. 50, pp. 15-31, 2015. Article (CrossRef Link)
[22] S. Ghafoor, P. D. Sutton, C. J. Sreenan, and K. N. Brown, "Cognitive Radio for Disaster Response Networks: Survey, Potential, and Challenges," *IEEE Wireless Communications*, vol. 21, no. 5, pp. 70-80, 2015. Article (CrossRef Link)
[23] A. Medeisis and O. Holland, "Cognitive Radio Policy and Regulation: Techno-Economic Studies to Facilitate Dynamic Spectrum Access," *Springer*, 2014. Article (CrossRef Link)
[24] R. Doost-Mohammady and K. R. Chowdhury, "Transforming Healthcare and Medical Telemetry through Cognitive Radio Networks," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 67-73, August 2012. Article (CrossRef Link)
[25] R. Chavez-Santiago et al., "Cognitive Radio for Medical Body Area Networks using Ultra Wideband," *IEEE Wireless Communications*, vol. 19, no. 4, pp. 74-81, August 2012. Article (CrossRef Link)
[26] A. K. Sadek, W. Yu, and K. J. R. Liu, "On the energy efficiency of cooperative communications in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 6, no. 1, pp. 5:1–5:21, Jan. 2010. Article (CrossRef Link)
[27] Z. Sheng and C. H. Liu, "Energy Efficient Cooperative Wireless Communication and Networks," *CRC Press*, 2014.
[28] W. Fang, F. Liu, F. Yang, L. Shu, and S. Nishio, "Energy-efficient cooperative communication for data transmission in wireless sensor networks," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 4, pp. 2185–2192, November 2010. Article (CrossRef Link)
[29] M. Nasim and S. Qaisar, "Cooperative Communication for Energy Efficiency in Mobile Wireless Sensor Networks," *Berlin, Heidelberg: Springer Berlin Heidelberg*, pp. 159–172, 2011. Article (CrossRef Link)
[30] X. Feng, G. Sun, X. Gan, F. Yang, X. Tian, X. Wang, and M. Guizani, "Cooperative Spectrum Sharing in Cognitive Radio Networks: A Distributed Matching Approach," *IEEE Transactions on Communications*, vol. 62, no. 8, pp. 2651-2664, Aug. 2014. Article (CrossRef Link)

[31] D. Liu, Y. Xu, L. Shen, and Y. Xu, "Self-Organizing Multiuser Matching in Cellular Networks: A Score-Based Mutually Beneficial Approach," *IET Communications*, vol. 10, no. 15, pp. 1928-1937, Oct. 2016. Article (CrossRef Link)
[32] S. X. Ng and L. Hanzo, "On the MIMO channel capacity of multidimensional signal sets," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 2, pp. 528–536, March 2006. Article (CrossRef Link)
[33] L. Hanzo, T. H. Liew, B. L. Yeap, R. Y. S. Tee, S. X. Ng, "Turbo Coding, Turbo Equalisation and Space-Time Coding: EXIT-Chart-Aided Near-Capacity Designs for Wireless Channels, 2nd Edition," *John Wiley and Sons*, Mar 1, 2011. Article (CrossRef Link)
[34] M. F. U. Butt, S. X. Ng, and L. Hanzo, "EXIT chart aided design of near-capacity self-concatenated trellis coded modulation using iterative decoding," in *Proc. of 67th IEEE Vehicular Technology Conference, Singapore*, pp.734–738, *May* 2008. Article (CrossRef Link)
[35] M. F. U. Butt, S. X. Ng, and L. Hanzo, "Self-concatenated code design and its application in power-efficient cooperative communications," *IEEE Communications Surveys Tutorials*, vol. 14, no. 3, pp. 858–883, Third 2012. Article (CrossRef Link)
[36] D. Divsalar and F. Pollara, "Serial and hybrid concatenated codes with applications," in *Proc. of Intl. Symp. Turbo Codes and Appls*, pp.80–87, 1997. Article (CrossRef Link)
[37] D. Divsalar and F. Pollara, "Hybrid concatenated codes and iterative decoding," in *Proc. of Proceedings of IEEE International Symposium on Information Theory*, Ulm, 1997. Article (CrossRef Link)
[38] A. Payandeh, M. Ahmadian, and M. R. Aref, "A secure channel coding scheme for efficient transmission of remote sensing data over the LEO satellite channels," in *Proc. of 2007 3rd International Conference on Recent Advances in Space Technologies*, June 2007, pp. 510–514. Article (CrossRef Link)
[39] A. Payandeh, M. Ahmadian, and M. R. Aref, "Adaptive secure channel coding based on punctured turbo codes," *IEE Proceedings - Communications*, vol. 153, no. 2, pp. 313–316, April 2006. Article (CrossRef Link)
[40] A. A. S. Afshar, T. Eghlidos, and M. R. Aref, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes," *IET Communications*, vol. 3, no. 2, pp. 279–292, February 2009. Article (CrossRef Link)
[41] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, May 1988. Article (CrossRef Link)
[42] A. Zaidan, B. Zaidan, M. Abdulrazzaq, R. Raji, and S. Mohammed, "Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography," *International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compendex*, vol. 20, 2009.
[43] FIPS Pub 46, "Data Encryption Standard (DES)," *National Institute of Standards and Technology (NIST)*, 15 January 1977.
[44] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Berlin, Heidelberg: Springer Berlin Heidelberg*, pp. 2–21, 1991. Article (CrossRef Link)
[45] FIPS 197, "Announcing the Advanced Encryption Standard (AES)," *National Institute of Standards and Technology (NIST)*, 26 November 2001.
[46] T. Li, J. Ren, Q. Ling, and A. Jain, "Physical layer built-in security analysis and enhancement of CDMA systems," in *Proc. of MILCOM 2005 - 2005 IEEE Military Communications Conference*, Oct 2005, pp. 956–962 Vol. 2. Article (CrossRef Link)
[47] T. Dean and A. Goldsmith, "Physical-layer cryptography through massive MIMO," in *Proc. of Information Theory Workshop (ITW), 2013 IEEE*, Sept 2013, pp. 1–5. Article (CrossRef Link)
[48] L. Mucchi, L. S. Ronga, and E. Del Re, "A novel approach for physical layer cryptography in wireless networks," *Wireless Personal Communications*, vol. 53, no. 3, pp. 329–347, 2010. Article (CrossRef Link)
[49] A. Zuquete and J. Barros, "Physical-layer encryption with stream ciphers," in *Proc. of 2008 IEEE International Symposium on Information Theory*, July 2008, pp. 106–110. Article (CrossRef Link)

[50] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014. Article (CrossRef Link)
[51] S. A. A. Fakoorian and A. L. Swindlehurst, "On the optimality of polar codes for the deterministic wiretap channel," in *Proc. of 2013 Asilomar Conference on Signals, Systems and Computers*, pp. 2089–2093, Nov 2013. Article (CrossRef Link)
[52] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *CoRR*, vol. abs/1305.4746, 2013. Article (CrossRef Link)
[53] R. J. Aumann and M. Maschler, "Repeated Games with Incomplete Information," *The MIT press*, 1995.
[54] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Repeated open spectrum sharing game with cheat-proof strategies," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1922–1933, April 2009. Article (CrossRef Link)
[55] M. F. U. Butt, R. A. Riaz, S. X. Ng, and L. Hanzo, "Near-capacity iteratively decoded binary self-concatenated code design using EXIT charts," in *Proc. of IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, Nov 2008, pp. 1–5. Article (CrossRef Link)
[56] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara, "A soft-input soft-output app module for iterative decoding of concatenated codes," *IEEE Communications Letters*, vol. 1, no. 1, pp. 22–24, Jan 1997. Article (CrossRef Link)

Bakhtiar Ali received his MS degree in Personal and Mobile Radio Communications from Lancaster University, UK in September 2008. He is currently pursuing a doctoral degree at COMSATS Institute of Information Technology, Islamabad, Pakistan. His research interests include the radio resource management in cooperative cognitive radio networks, space time block coding, cooperative communications, physical layer security, game theory and the study of future radio communications systems, i.e., 5G.

Nida Zamir received her Bachelor's degree in Electrical Engineering with specialization in Telecommunications from COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan in 2014. She is currently pursuing her MS in Electrical Engineering from the same institution. Her research interests include channel coding, physical layer security, game theory and quantum communications.

Soon Xin Ng received the B.Eng. degree (First class) in electronic engineering and the Ph.D. degree in telecommunications from the University of Southampton, Southampton, U.K., in 1999 and 2002, respectively. From 2003 to 2006, he was a postdoctoral research fellow working on collaborative European research projects known as SCOUT, NEWCOM and PHOENIX. Since August 2006, he has been a member of academic staff in the School of Electronics and Computer Science, University of Southampton. He was involved in the OPTIMIX and CONCERTO European projects as well as the IU-ATC and UC4G projects. He is currently an Associate Professor in telecommunications at the University of Southampton. His research interests include adaptive coded modulation, coded modulation, channel coding, space-time coding, joint source and channel coding, iterative detection, OFDM, MIMO, cooperative communications, distributed coding, quantum communications, quantum error correction codes and joint wireless-and-optical-fiber communications. He is currently working on an EPSRC project on Cooperative Classical and Quantum Communications Systems. He has published over 200 papers and co-authored two John Wiley/IEEE Press books in this field. He is a Senior Member of the IEEE, a Chartered Engineer and a Fellow of the Higher Education Academy in the UK.

Muhammad Fasih Uddin Butt received his B.E. degree from National University of Sciences & Technology (NUST), Pakistan in 1999. He received his M.E. degree from Center for Advanced Studies in Engineering, UET Taxila, Pakistan with specialization in Digital Communication/Computer Networks in 2003 and his Ph.D. degree from Communications Research Group, School of Electronics and Computer Science, University of Southampton, U.K in June 2010. Currently he is working as Assistant Professor in the Department of Electrical Engineering, COMSATS Institute of Information Technology (CIIT), Islamabad, Pakistan where he has been serving as an academic since 2002. His research interests include channel coding, iterative detection, cooperative cognitive radio networks, mm Wave radio-over-fiber technologies, energy harvesting and physical layer security. He has published over 30 research papers in various reputed journals and conference proceedings.