

Link Adaptation with Untrusted Relay

Assignment: Design and Performance Analysis

Hamid Khodakarami, Farshad Lahouti

Center for Wireless Multimedia Communications

School of Electrical and Computer Engineering, University of Tehran

Email: khodakarami@ut.ac.ir, lahouti@ut.ac.ir

Abstract

In this paper, a link adaptation and untrusted relay assignment (LAURA) framework for efficient and reliable wireless cooperative communications with physical layer security is proposed. Using sharp channel codes in different transmission modes, reliability for the destination and security in the presence of untrusted relays (low probability of interception) are provided through rate and power allocation. Within this framework, several schemes are designed for highly spectrally efficient link adaptation and relay selection, which involve different levels of complexity and channel state information requirement. Analytical and simulation performance evaluation of the proposed LAURA schemes are provided, which demonstrates the effectiveness of the presented designs. The results indicate that power adaptation at the source plays a critical role in spectral efficiency performance. Also, it is shown that relay selection based on the signal to noise ratio of the source to relays channels provides an interesting balance of performance and complexity within the proposed LAURA framework.

Index Terms

Amplify-and-forward relaying, cooperative communications, link adaptation, physical layer security, relay selection, untrusted relay.

I. INTRODUCTION

Diversity and link adaptation are two enabling techniques to facilitate high performance communications over wireless fading channels. In cooperation for diversity, the relays are to assist a reliable data transmission from the

A preliminary report on this work has been presented at the IEEE International Conference on Telecommunications, Cyprus, May 2011 [1].

source to the destination. One major challenge hindering the practical adoption of cooperative wireless communications is the security as the relaying nodes may in fact be able to eavesdrop on the source destination communications. In this paper, wireless link adaptation solutions are proposed to facilitate both reliability and physical layer security for cooperative communications in presence of untrusted relays.

The cooperation of the source with a relay node may include a so-called *service level* trust, i.e., the relay node indeed performs its expected function as a relay in the network. However, this cooperation may not necessarily include a *data level* trust, i.e., the relay may not be supposed to extract (decode) useful information from the source destination communication. The information theoretic aspect of this problem is investigated in [2], [3]. Specifically, an upper bound for the achievable secrecy rate in this setting is presented in [2].

Link adaptation by rate and power control could highly improve the performance of cooperative communications over time-varying channels. In [4], the capacity of adaptive transmission over cooperative fading channel is considered for amplify-and-forward relaying, where three different adaptive techniques are investigated. In [5], the performance of cooperative communications with relay selection and un-coded adaptive modulation is investigated. An scheme for joint power and bandwidth allocation and relay selection in a user cooperative network is proposed in [6], which considers optimizing a utility function of user traffic demands in a slow but frequency selective fading channel. In [7], single and multiple relay cooperation with amplify-and-forward (AF) relaying is considered. For reduced complexity, suboptimal multiple relay selection schemes are proposed and shown to achieve full diversity. In [8], a cross-layer approach to optimize the spectral efficiency of the relay channel employing adaptive modulation and coding in conjunction with cooperative automatic repeat request is proposed.

A practical code design approach to physical layer security based on capacity achieving low density parity check (LDPC) codes is introduced in [9]. The setting is a wiretap binary erasure channel involving a source, a destination and an eavesdropper. In fact, constructive approaches for (imperfect) physical layer security may be set up to ensure a reliable source destination communication, while maintaining a high probability of error for the eavesdropper. To this end, design of sharp punctured LDPC codes for which the bit error rate (BER) curve falls sharply from high BERs to very low BERs (steep waterfall region), is considered in [10]. Yet, adaptive transmission may be exploited to enhance the system performance over time-varying channels both in terms of security and reliability [11].

In this paper, a framework for cooperative communications through link adaptation with untrusted relay assignment (LAURA) is proposed. The purpose is to utilize the cooperation of arbitrary number of relays for reliable communi-

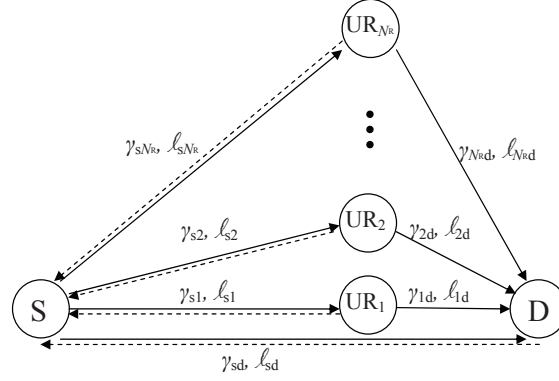


Fig. 1. Network topology; γ and ℓ indicate the channel SNR and the distance.

cations, while ensuring they cannot decode useful information from their relayed signal. Different LAURA schemes are set up based on network CSI that is already necessary for quality of service (QoS) provisioning over wireless fading channels. The resource degrees of freedom, i.e., transmission power, transmission rate, and cooperating relays, are exploited in an optimized manner to address the QoS reliability and security requirements of the cooperative communication networks dealing with untrusted relays. Specifically, several power adaptation and relay selection strategies are proposed for LAURA that are designed for high spectral efficiency communication based on discrete rate adaptation with sharp channel codes and different levels of complexity and CSI requirements. Analytical and simulation performance evaluation of the proposed LAURA schemes are provided, which demonstrates the effectiveness of the presented designs. The results indicate that the LAURA design with source (only) power adaptation and relay selection based on (only) source relay channels CSI provide an interesting balance of performance and complexity within the proposed LAURA framework.

The paper is organized as follows. Section II presents the system model and describes the problem under consideration. In Section III, the link adaptation and relay selection problem is introduced and its exact solution is presented. Section IV explores the scenarios where source and relays transmit with constant power. In Section V, suboptimal relay selection strategies are investigated. Section VI presents the simulation and theoretical results for the proposed LAURA schemes. Section VII concludes the paper.

II. SYSTEM MODEL AND PROBLEM STATEMENT

A wireless communication system with one source node (S), one destination node (D) and a set of N_R available relay nodes, $\{UR_i | i \in \mathcal{M}_R = \{1, 2, \dots, N_R\}\}$, is considered (Fig. 1). There are N_C cooperating relays, denoted by the set \mathcal{M}_C , that are selected from the set of available relays \mathcal{M}_R . The cooperation protocol is AF. The rest of the relays in the set $\mathcal{M}_R - \mathcal{M}_C$ are referred to as non-cooperating relays. The relays are assumed trusted at the service level and untrusted at the data level. Service level trust entails following the AF protocol as expected. This involves for relays to feedback true CSI, remain inactive if not selected for cooperation, and upon selection for cooperation, adapting their power according to source schedule, and forwarding the amplified version of received signal without modification. Since the relays are data level untrusted, the source imposes security constraints on relays. This is to prevent all relay nodes from extracting useful information from their received signal.

Total network security calls for an array of technologies and steps involving different layers of communications protocol stack, and including hardware, process and physical security. For instance, service level security could be facilitated in part by hardware and physical security to avoid hardware tampering. In this work, we focus on data level security that can be provided by link adaptation and relay assignment in wireless AF relay networks. Needless to say, this will serve as one (added) layer of security and in general does not make other security mechanisms evadable.

In the first phase of the transmission, the S node transmits signal x to the D node and relays. The received signal at the D node and at the UR_i node are respectively

$$y_{sd} = h_{sd} x + w_d \quad (1)$$

$$y_{si} = h_{si} x + w_{si}, \quad (2)$$

where h_{sd} , and h_{si} denote the Rayleigh fading coefficients between S and D nodes, and S and UR_i nodes, respectively. The noise is denoted at the UR_i node as w_{si} and at the D node as w_d . The N_C cooperating relays amplify the received signal and transmit it to the D node in the second phase of cooperation. The received signal at the D node from the UR_i node is

$$y_{id} = G_i h_{id} y_{si} + w'_d, \quad (3)$$

where G_i is the UR_i node amplifier gain and h_{id} and w'_d are Rayleigh fading coefficients from UR_i node to the D node and noise at the D node, respectively.

The S-D, S-UR_i and UR_i-D channels, for $1 \leq i \leq N_R$, are independent Rayleigh fading channels with SNRs of γ_{sd} , γ_{si} and γ_{id} , respectively. The SNRs are exponentially distributed with parameters $\frac{1}{\gamma_{sd}}$, $\frac{1}{\gamma_{si}}$ and $\frac{1}{\gamma_{id}}$ and, probability density functions of $f_{sd}(\gamma_{sd})$, $f_{si}(\gamma_{si})$ and $f_{id}(\gamma_{id})$, respectively. With full CSI assumption, the instantaneous SNRs of the three channels are assumed known at the onset of each frame interval at the S node. Assuming maximum ratio combining (MRC) of signals received from S node and N_C cooperating relay nodes at the D node, the equivalent SNR of AF relaying protocol at the D node is [12]

$$\gamma_{eq} = \frac{S_s}{S} \gamma_{sd} + \sum_{i \in \mathcal{M}_C} \gamma_i, \quad (4)$$

where

$$\gamma_i = \frac{\frac{S_s}{S} \gamma_{si} \frac{S_i}{S} \gamma_{id}}{\frac{S_s}{S} \gamma_{si} + \frac{S_i}{S} \gamma_{id} + 1}, \quad (5)$$

where S_s and $S = \{S_i | i \in \mathcal{M}_C\}$ are transmission power of source and the set of transmission powers of relays, respectively. Here, S normalizes the transmission power to the case where no power adaptation is employed. For the sake of tractability of theoretical performance analyses in some cases, we may use an upper bound on γ_i as follows [4]-[5]

$$\gamma_{i,u} = \min\left(\frac{S_s}{S} \gamma_{si}, \frac{S_i}{S} \gamma_{id}\right). \quad (6)$$

This yields the following upper bound on the equivalent SNR at the destination $\gamma_{eq,u} = \frac{S_s}{S} \gamma_{sd} + \sum_{i \in \mathcal{M}_C} \gamma_{i,u}$.

We use a set of N transmission modes (TM) each corresponding to a combination of modulation and coding. These TMs provide transmission rates of R_1, R_2, \dots, R_N bits per symbol and we assume $R_n > R_{n-1}$. The LAURA schemes proposed in the sequel may be set up based on any given set of coding and modulation pairs, as for their design we assume closed-form expressions for the performance of TMs. Indeed, we can express the instantaneous BER of TM n as an approximated function of received SNR, γ , through curve fitting by

$$\text{IBER}_n(\gamma) = \begin{cases} 0.5 e^{-p_n \gamma^{q_n}} & \text{if } \gamma < \gamma_{lh}^n \\ \frac{a_n}{(1 + e^{c_n(\gamma - b_n)})^{k_n}} & \text{if } \gamma \geq \gamma_{lh}^n \end{cases}$$

where p_n , q_n , a_n , b_n , c_n and k_n are the approximation fitting parameters for a given modulation and coding pair. The value of γ_{lh}^n is determined by the intersection of the two parts of the approximation. The expression for the second part is a modification of what is proposed in [13], and the first part is devised here for better performance modeling of TMs in the low SNR regime. The inverse of $\text{IBER}_n(\gamma)$ describing received SNR as a function of BER

is given by

$$\Gamma_n(P_e) = \begin{cases} \left(\ln\left(\frac{0.5}{P_e}\right) / p_n \right)^{\frac{1}{q_n}} & \text{if } P_e > \text{IBER}_n(\gamma_{lh}^n) \\ \frac{1}{c_n} \ln \left[\left(\frac{a_n}{P_e} \right)^{1/k_n} - 1 \right] + b_n & \text{if } P_e \leq \text{IBER}_n(\gamma_{lh}^n). \end{cases} \quad (7)$$

The objective is to maximize the spectral efficiency of the system while providing both security against eavesdropping of data level untrusted relays and reliable communications for the destination. These two requirements are expressed as follows

$$\begin{aligned} \text{C1. } & \text{BER}_i \geq \text{BER}_{\text{tgt}}^r \text{ for } 1 \leq i \leq N_R \\ \text{C2. } & \text{BER}_d \leq \text{BER}_{\text{tgt}}^d, \end{aligned} \quad (8)$$

where BER_i is the BER at the UR_i node and BER_d is the BER at the D node applying MRC. In (8), $\text{BER}_{\text{tgt}}^r$ is a target lower limit for BER_i to ensure security against eavesdropping of relays, and $\text{BER}_{\text{tgt}}^d$ is a target upper limit for BER at the destination to ensure reliable communications. The average spectral efficiency is expressed as

$$\eta = \sum_{n=1}^N \frac{R_n}{2} \Pr(\text{TM} = n), \quad (9)$$

where $\Pr(\text{TM} = n) = P_n$ is the probability of selecting TM number n for transmission. The factor $1/2$ multiplied by R_n is due to the half-duplex cooperative transmission. The equation (9) indicates that to compute the average spectral efficiency of the system, we only need to derive an expression for P_n .

III. LINK ADAPTATION AND UNTRUSTED RELAY ASSIGNMENT FOR COOPERATIVE COMMUNICATIONS

The general optimization problem for LAURA with power adaptation is expressed as follows

$$\begin{aligned} & \max_{\mathcal{M}_c} \max_{n \in \{1, 2, \dots, N\}} \max_{S_s, S} R \\ \text{s.t. } & \text{C1. } \text{BER}_j \geq \text{BER}_{\text{tgt}}^r \text{ for } 1 \leq j \leq N_R \\ & \text{C2. } \text{BER}_d \leq \text{BER}_{\text{tgt}}^d \\ & \text{C3. } S_s + \sum_{i \in \mathcal{M}_c} S_i \leq S_{\text{tot}}, \end{aligned} \quad (10)$$

where R is the transmission rate in a given frame in bits per symbol or equivalently the spectral efficiency. Note that the solution to this problem provides the instantaneous (per frame) power allocation scheme in the two transmission phases. The constraint C3 in (10) expresses a network sum power constraint, where the total transmission of source and cooperating relays are limited. This is of course justified given that the relays are service level trusted (Section

TABLE I

CSI AND POWER OPTIMIZATION REQUIREMENTS OF DIFFERENT PROPOSED SCHEMES. AAR, ACR AND ASR DENOTE ALL AVAILABLE RELAYS, ALL COOPERATING RELAYS AND ALL N_C MEMBER SUBSETS OF RELAYS, RESPECTIVELY.

Scheme	Relay Selection	CSI requirements	Power Optimization
LAURA1	Optimal	γ_{si} (for AAR), γ_{id} (for AAR), γ_{sd}	Source & ASR
LAURA2	Based on S-UR _i CSI	γ_{si} (for AAR), γ_{id} (for ACR), γ_{sd}	Source & ACR
LAURA1-CPR	Optimal	γ_{si} (for AAR), [γ_{eq} (for ASR)] or [γ_{sd} and γ_{id} (for AAR)]	Source
LAURA2-CPR	Based on S-UR _i CSI	γ_{si} (for AAR), [γ_{eq} (for ACR)] or [γ_{sd} and γ_{id} (for ACR)]	Source
LAURA3-CPR	Based on Average S-UR _i SNR	γ_{si} (for AAR), [γ_{eq} (for ACR)] or [γ_{sd} and γ_{id} (for ACR)]	Source
LAURA1-CP	Optimal	γ_{si} (for AAR), [γ_{eq} (for ASR)] or [γ_{sd} and γ_{id} (for AAR)]	N/A

II), and in line with many articles in literature, e.g., [14], [15], allows us to better understand the potential benefit of (additional) relays given a certain network power budget. As we shall discuss in Remark 1, the case with separate power constraints for the source and each of the relays will simply be a special case. An instance of the problem with $N_C = 1$ is considered in [1], where a single relay is selected for cooperation out of the N_R available relays. In the following, the exact solution to the problem (10) is presented and in the next section we explore some other possible solutions. A list of the proposed LAURA schemes and a summary of their characteristics are provided in Table I.

A. Exact Solution

The problem (10) can be solved exactly and the resulting solution which serves as an upper-bound on performance is referred to as LAURA1 in the sequel. In this case, the CSI of S-D, S-UR_i and UR_i-D are required at the S node at the beginning of each transmission interval. The following proposition enables the proposed solution.

Proposition 1: While C2 is to be satisfied in (10), maximizing R_n is equivalent to maximizing γ_{eq} .

Proof: Consider γ_{eq}^* as the optimized γ_{eq} constrained to C2. Suppose that $\gamma'_{eq} < \gamma_{eq}^*$. Now, if $n' = \arg \max_n \{ \text{IBER}_n(\gamma'_{eq}) \leq \text{BER}_{\text{tgt}}^d \}$, i.e., the maximum value of n given that $\text{IBER}_n(\gamma'_{eq})$ is less than or equal to $\text{BER}_{\text{tgt}}^d$, and $n^* = \arg \max_n \{ \text{IBER}_n(\gamma_{eq}^*) \leq \text{BER}_{\text{tgt}}^d \}$, then $R_{n^*} \geq R_{n'}$. ■

Using Proposition 1, for a given set \mathcal{M}_C and a given TM n , the following design subproblem is considered.

$$\begin{aligned} & \max_{S_s, \mathbf{S}} \quad \gamma_{\text{eq}} \\ \text{s.t.} \quad & \text{C1. } S_s \leq S \frac{\Gamma_n^r}{\gamma_{s\tilde{i}}} \\ & \text{C3. } S_s + \sum_{i \in \mathcal{M}_C} S_i \leq S_{\text{tot}}, \end{aligned} \tag{11}$$

where $\tilde{i} = \arg \max_i \gamma_{si}$ and based on (7), $\Gamma_n^r \triangleq \Gamma_n(\text{BER}_{\text{tgt}}^r)$. Setting \tilde{i} as such ensures security against eavesdropping of any of the relays. As presented below, the solution to this problem provides optimized instantaneous power allocation at the source and the set of cooperating relays under consideration. Next, we use the results within Algorithm 1, which yields the optimum TM n and choice of cooperating relays \mathcal{M}_C in presence of the constraint C2 in (10). In fact, Algorithm 1 identifies the largest TM n (rate) for which the set of cooperating relays leading to maximum γ_{eq} in subproblem (11) satisfies C2 in (10).

It can be easily shown that γ_{eq} is a concave function of (S_s, \mathbf{S}) . In other words, the next three conditions for γ_{eq} hold [16, Appendix 1]: $\partial^2 \gamma_{\text{eq}} / \partial S_i^2 \leq 0$, $\partial^2 \gamma_{\text{eq}} / \partial S_s^2 \leq 0$ and $(\partial^2 \gamma_{\text{eq}} / \partial S_i^2)(\partial^2 \gamma_{\text{eq}} / \partial S_s^2) - [(\partial^2 \gamma_{\text{eq}} / \partial S_s \partial S_i)]^2 \leq 0$, for $i \in \mathcal{M}_R$. Thus, the KKT condition gives the optimal solution to problem (11). In order to simplify the solution, we first solve (11) without C1. The governing Lagrangian for this problem temporarily ignoring C1 is

$$\mathcal{L} = \gamma_{\text{eq}} + \lambda_1 \left(S_s + \sum_{i \in \mathcal{M}_C} S_i - S_{\text{tot}} \right). \tag{12}$$

The optimal S_s and S_i should satisfy

$$\frac{\partial \mathcal{L}}{\partial S_s} = 0 \text{ and } \frac{\partial \mathcal{L}}{\partial S_i} = 0 \text{ for } i \in \mathcal{M}_C. \tag{13}$$

Then,

$$\frac{\partial \mathcal{L}}{\partial S_i} = \frac{\frac{\gamma_{si}^2 \gamma_{id}}{S^3} S_i^2 + \frac{\gamma_{si} \gamma_{id}}{S^2} S_i}{\left(\frac{S_s}{S} \gamma_{si} + \frac{S_i}{S} \gamma_{id} + 1 \right)^2} + \lambda_1 = 0, \tag{14}$$

that yields

$$S_i = \frac{S}{\gamma_{id}} \left[\frac{1}{\nu} \left(\frac{S_s^2}{S^3} \gamma_{si}^2 \gamma_{id} + \frac{S_s}{S^2} \gamma_{si} \gamma_{id} \right)^{1/2} - \frac{S_s}{S} \gamma_{si} - 1 \right]^+, \tag{15}$$

where $\nu = \sqrt{-\lambda_1}$ and $[x]^+$ denotes $\max(x, 0)$. Also,

$$\frac{\partial \mathcal{L}}{\partial S_s} = \frac{\gamma_{sd}}{S} + \sum_{i \in \mathcal{M}_C} \frac{\frac{\gamma_{si} \gamma_{id}^2}{S^3} S_s^2 + \frac{\gamma_{si} \gamma_{id}}{S^2} S_s}{\left(\frac{S_s}{S} \gamma_{si} + \frac{S_i}{S} \gamma_{id} + 1 \right)^2} + \lambda_1 = 0. \tag{16}$$

Substitution of (15) in C3 of (11) and (16) gives a set of two equations. Numerically solving this set of equations yields the optimal S_i for $i \in \mathcal{M}_C$ and also S_s for (11) considering only C3. Now we check whether the solution satisfies C1 in (11). If the condition is satisfied, then the solution is the optimal one, else according to C1 we set $S_s = S \frac{\Gamma_n}{\gamma_{si}^r}$ in (15). Next, using the result in C3 of (11) yields the optimum S by quantifying the new value of ν . Using the presented solution to (11), as described, the Algorithm 1 formulates the LAURA1 scheme or the exact solution to design problem (10). In this algorithm, we use the optimal power allocation for source and relays for every N_C member subset of the available relays as possible cooperating ones, and choose the best subset according to the equivalent SNR it provides. Based on this, we find the highest possible transmission rate such that both security and reliability constraints are satisfied.

Algorithm 1: Exact Solution for LAURA

- 1) Select $n = N$.
 - 2) If $n = 0$ then go to outage mode and exit.
 - 3) Build the set \mathcal{M}_A comprised of all N_C member subsets of \mathcal{M}_R and index its members as $\mathcal{M}_{C,l}$, $l \in \{1, 2, \dots, \frac{N_R!}{(N_R - N_C)!N_C!}\}$.
 - 4) For $l = 1$ to $\frac{N_R!}{(N_R - N_C)!N_C!}$
 - 4-1) Set $\mathcal{M}_C = \mathcal{M}_{C,l}$
 - 4-2) Solve (11) and obtain $S_s^{(l)}$ and $S_i^{(l)}$, $i \in \mathcal{M}_C$
 - 4-3) Calculate $\gamma_{eq}^{(l)}$.
 - 5) Select the set of cooperating relays by $l^* = \arg \max_l \gamma_{eq}^{(l)}$ and set $\gamma_{eq} = \gamma_{eq}^{(l^*)}$.
 - 6) If C2 in (10) is satisfied, set $TM = n$ and exit; else $n = n - 1$ and go to step 2.
-

B. Analytical Results for $N_C = 1$

In case only one relay is to be selected for cooperation, i.e., $N_C = 1$, closed form solutions for transmission powers of source and relay can be obtained. This in turn allows for an analytical performance evaluation in this case. For $N_C > 1$, we resort to numerical results for performance evaluation in Section VI.

Considering the design subproblem in (11) for $N_C = 1$ and using UR_i node for cooperation, we have $S_i = S_{tot} - S_s$

and (16) yields $S_{s,n,i}^* = \frac{-\theta_i - \sqrt{\theta_i^2 - 4\mu_i\rho_i}}{2\mu_i}$, where

$$\begin{aligned}\mu_i &= \gamma_{id}^2(\gamma_{si} + \gamma_{sd}) + \gamma_{si}^2(\gamma_{sd} - \gamma_{id}) - 2\gamma_{sd}\gamma_{id}\gamma_{si} \\ \theta_i &= 2[\gamma_{si}(\gamma_{sd} - \gamma_{id} + \gamma_{id}\gamma_{sd}S_{\text{tot}}) - \gamma_{id}^2S_{\text{tot}}(\gamma_{si} + \gamma_{sd}) - \gamma_{id}\gamma_{sd}] \\ \rho_i &= \gamma_{sd} + \gamma_{id}^2(\gamma_{si} + \gamma_{sd})S_{\text{tot}}^2 + (2\gamma_{id}\gamma_{sd} + \gamma_{id}\gamma_{si})S_{\text{tot}}.\end{aligned}$$

Then, the optimal transmission power of S node cooperating with UR_i node is

$$S_{s,n,i}^{\text{opt}} = \min(S_{s,n,i}^*, S_{\text{tot}}, S \frac{\Gamma_n^r}{\gamma_{si}}). \quad (17)$$

We next use this result in Algorithm 1. Noting the constraint C2 in (10) for $N_C = 1$, we consider the following event, which describes the case when relay UR_i is selected and TM n satisfies both the reliability and the network security constraints,

$$A_n^i : \gamma_{\text{eq}}^{(i)} = \left[\frac{S_s}{S} \gamma_{sd} + \frac{\frac{S_s}{S} \gamma_{si} \frac{S_{\text{tot}} - S_s}{S} \gamma_{id}}{\frac{S_s}{S} \gamma_{si} + \frac{S_{\text{tot}} - S_s}{S} \gamma_{id} + 1} \right]_{S_s = S_{s,n,i}^{\text{opt}}} \geq \Gamma_n^d, \quad (18)$$

where $\Gamma_n^d \triangleq \Gamma_n(\text{BER}_{\text{tgt}}^d)$. For the presented transmission strategy in Algorithm 1, the event that TM number n satisfies both security and reliability requirements is denoted by A_n and its probability is

$$\begin{aligned}\Pr(A_n) &= \Pr\left(\bigcup_{i=1}^{N_R} A_n^i\right) = 1 - \Pr\left(\bigcap_{i=1}^{N_R} (A_n^i)^c\right) = 1 - \mathbf{E}_{\gamma_{sd}, \gamma_{si}} \left\{ \Pr\left(\bigcap_{i=1}^{N_R} (A_n^i)^c \mid \gamma_{sd}, \gamma_{si}\right) \right\}, \\ &= 1 - \mathbf{E}_{\gamma_{sd}, \gamma_{si}} \left\{ \prod_{i=1}^{N_R} \left[1 - \Pr\left(\gamma_{\text{eq}}^{(i)} \geq \Gamma_n^d \mid \gamma_{sd}, \gamma_{si}\right) \right] \right\},\end{aligned} \quad (19)$$

where $\mathbf{E}_{\gamma_{sd}, \gamma_{si}}$ denotes the expectation with respect to independent variables γ_{sd} and γ_{si} . The last equality in (19) results from the independence of A_n^i and A_n^j for $i \neq j$ and given γ_{sd} and γ_{si} . The transmission mode m is selected when it is the TM with the largest rate (here equivalently the largest TM) that with optimal power allocation and relay selection can provide both the security and reliability constraints. The probability of selecting TM m may then be computed as follows

$$P_m = \Pr\left(\bigcup_{n=m}^N A_n\right) - \Pr\left(\bigcup_{n=m+1}^N A_n\right) = \mathbf{E}\left\{\mathbf{I}(A_{\tilde{n}_m}) - \mathbf{I}(A_{\tilde{n}_{m+1}})\right\}, \quad (20)$$

where $\mathbf{I}(\cdot)$ is the indicator function that is $\mathbf{I}(E) = 1$ if E is true and $\mathbf{I}(E) = 0$ if E is false, and

$$\tilde{n}_m(\gamma_{\text{eq}}^{(i)}, \gamma_{si}) = \arg \min_{n \in \{m, \dots, N\}} \left(\gamma_{\text{eq}}^{(i)} \geq \Gamma_n^d \mid S_s = S_{s,n,i}^{\text{opt}} \right). \quad (21)$$

In fact, using UR_i relay node with optimum power allocations described, $\tilde{n}_m(\gamma_{\text{eq}}^{(i)}, \gamma_{si})$ denotes the minimum TM number from the set $\{m, \dots, N\}$ for which the reliability and security constraints in given realizations of the fading

channels are satisfied. Here, in order to facilitate the analysis we introduce an approximation whose effectiveness is shown in Section VI. We consider

$$\tilde{n}_m(\gamma_{\text{eq}}^{(i)}, \gamma_{\bar{s}i}) \approx m. \quad (22)$$

Then, the probability of TM m is

$$P_m = \Pr(A_m) - \Pr(A_{m+1}). \quad (23)$$

It can be easily verified that in case there is no security constraint, (23) holds without any approximation. Appendix A presents the joint PDF of $\gamma_{\bar{s}i}$ and γ_{si} that is required to compute P_m in (23) and hence the average spectral efficiency. The authors also presented the above analysis in [1].

IV. LAURA: CONSTANT POWER STRATEGIES

The exact solution for (10) or the LAURA1 scheme is optimal and provides a benchmark for comparison to other possible simpler schemes. In the following, two suboptimal power allocation strategies with reduced complexity are introduced. In Section IV-A, a LAURA scheme with constant power source and relays is presented. In Section IV-B, a LAURA scheme with adaptive power source transmission and constant power relays is presented.

A. Constant Power Transmission (LAURA1-CP)

A constant power solution to (10) is obtained by considering constant power transmission for the relays, i.e., $S_i^{(l)} = S$ and constant power transmission for the source, i.e., $S_s = S$ and removing step 4-2 in Algorithm 1. In this case, the SNR of S-UR $_i$ and γ_{eq} are required at the S node as CSI to enforce the security and reliability constraints, respectively. The equivalent SNR, γ_{eq} , is estimated at the destination and fed back to the S node, or it can be calculated by S node knowing CSI of S-D, S-UR $_i$ and UR $_i$ -D.

The performance of LAURA1-CP is evaluated in Section VI. As elaborated below, for the case with one cooperating relay ($N_C = 1$), the theoretical performance analysis is possible. Consider $i^* = \arg \max_i \gamma_{\text{eq}}^{(i)}$ obtained from step 5 of Algorithm 1. The event that relay i^* satisfies the reliability constraint corresponds to the event that there is at least one relay that can satisfy this constraint. For LAURA1-CP with single cooperating relay, we have

$$A_n : \bigcap_{i=1}^{N_R} \gamma_{si} \leq \Gamma_n^r \cap \bigcup_{i=1}^{N_R} \gamma_{\text{eq}}^{(i)} \geq \Gamma_n^d. \quad (24)$$

Then, the probability of selecting TM m is

$$\begin{aligned}
P_m^{\text{CP}} &= \Pr \left(A_m \cap \bigcap_{n=m+1}^N A_n^c \right) = \Pr \left(\left\{ \bigcap_{i=1}^{N_R} \gamma_{si} \leq \Gamma_m^r \cap \bigcup_{i=1}^{N_R} \gamma_{eq}^{(i)} \geq \Gamma_m^d \right\} \cap \bigcap_{i=1}^{N_R} \gamma_{eq}^{(i)} < \Gamma_{m+1}^d \right) \\
&= \Pr \left(\left\{ \bigcap_{i=1}^{N_R} \gamma_{si} \leq \Gamma_m^r \cap \gamma_{eq}^{(i)} < \Gamma_{m+1}^d \right\} \cap \bigcup_{i=1}^{N_R} \gamma_{eq}^{(i)} \geq \Gamma_m^d \right) \\
&= \Pr \left(\bigcap_{i=1}^{N_R} \gamma_{si} \leq \Gamma_m^r \cap \gamma_{eq}^{(i)} < \Gamma_{m+1}^d \right) - \Pr \left(\bigcap_{i=1}^{N_R} \gamma_{si} \leq \Gamma_m^r \cap \gamma_{eq}^{(i)} < \Gamma_m^d \right). \tag{25}
\end{aligned}$$

Since different relay channels are independent, given γ_{sd} , $\gamma_{eq}^{(i)}$ is independent of $\gamma_{eq}^{(j)}$ for $i \neq j$. Then

$$P_m^{\text{CP}} = \mathbf{E}_{\gamma_{sd}} \left\{ \prod_{i=1}^{N_R} \Pr \left(\gamma_{si} \leq \Gamma_m^r \cap \gamma_{eq}^{(i)} < \Gamma_{m+1}^d | \gamma_{sd} \right) - \prod_{i=1}^{N_R} \Pr \left(\gamma_{si} \leq \Gamma_m^r \cap \gamma_{eq}^{(i)} < \Gamma_m^d | \gamma_{sd} \right) \right\}. \tag{26}$$

Using the upper bound for equivalent SNR in (6), a closed form expression for the TM probability is obtained as follows

$$\begin{aligned}
P_m^{\text{CP}} &= \mathbf{E}_{\gamma_{sd}} \left\{ \prod_{i=1}^{N_R} \left(1 - e^{-\frac{\Gamma_m^r}{\gamma_{si}}} - \left[e^{-\frac{[\Gamma_m^d - \gamma_{sd}]^+}{\gamma_{si}}} - e^{-\frac{\Gamma_m^r}{\gamma_{si}}} \right]^+ \cdot e^{-\frac{[\Gamma_m^d - \gamma_{sd}]^+}{\gamma_{id}}} \right) \right. \\
&\quad \left. - \prod_{i=1}^{N_R} \left(1 - e^{-\frac{\Gamma_m^r}{\gamma_{si}}} - \left[e^{-\frac{[\Gamma_{m+1}^d - \gamma_{sd}]^+}{\gamma_{si}}} - e^{-\frac{\Gamma_m^r}{\gamma_{si}}} \right]^+ \cdot e^{-\frac{[\Gamma_{m+1}^d - \gamma_{sd}]^+}{\gamma_{id}}} \right) \right\}. \tag{27}
\end{aligned}$$

Then, the average spectral efficiency is computed by substitution of (27) in (9). The authors also reported the above analysis in [1].

B. Constant Power Relay Transmission (LAURA1-CPR)

The LAURA1-CPR scheme involves adaptive power transmission for the source and constant power relay transmission. In this case, we set $S_i = S$ for $i \in \mathcal{M}_C$. The required CSI are S-UR_{*i*} and γ_{eq} . For γ_{eq} , we need to transmit from S node with the power S_s , and wait for the estimation of γ_{eq} at the destination or it can be calculated by S node knowing CSI of S-D, S-UR_{*i*} and UR_{*i*}-D. A modification of the Algorithm 1 yields the solution for constant power relay transmission, where, step 4-2 is replaced as follows

$$\text{Set } S_i^{(l)} = S \text{ and } S_s^{(l)} = \min(S_{\text{tot}} - N_C S, S \frac{\Gamma_n^r}{\gamma_{si}^r}). \tag{28}$$

This substitutes solving the power allocation problem (11) with a simple power allocation that assumes power constraint for source and each relay separately.

Remark 1: In LAURA problem described in (10), if we consider separate power constraints S for source and each of the relays the total power constraint will still be $S_{\text{tot}} = (N_C + 1)S$, the optimized solution will be LAURA1-CPR.

This is due to the fact that the cooperating relays will need to transmit with their maximum allocated power to ensure maximized reliable transmission rate, and the source will be transmitting with its optimized adaptive power based on security and power constraints.

V. LAURA: RELAY SELECTION STRATEGIES

The solution presented for LAURA (problem (10)) in Algorithm 1 provides high performance but involves an exhaustive search over all N_C member subsets of \mathcal{M}_R . Specifically, it examines optimized $\gamma_{eq}^{(l)}$ for the said relay subsets, which of course only a single one is finally used. In addition, the source requires γ_{id} for non-cooperating relays as CSI as well. Suboptimal solutions may have some advantages in practice, as their CSI requirements and complexity could be far less than the optimal one. In this section, we propose two efficient relay selection strategies for LAURA.

A. Relay Selection Based on Source Relay CSI (LAURA2)

An efficient solution with manageable CSI requirement may be constructed by taking a suboptimal relay selection approach that relies on γ_{si} , $i \in \mathcal{M}_R$ and γ_{eq} resulting from \mathcal{M}_C . Hence, there is no need to UR_i-D CSI feedback ($i \in \mathcal{M}_R$). To limit the complexity, we wish to avoid solving (11) to obtain γ_{eq} (4) for all subsets of \mathcal{M}_R . To this end, the instantaneous source to relay SNR can be used as the relay selection criterion. Due to the security constraint, γ_i is limited to $\frac{\Gamma_n^r \gamma_{si}}{\gamma_{si}^-}$. As a result, the subset of relays that provide a high γ_{eq} may also be identified by selecting the relays with the highest γ_{si} 's. Indeed, as we shall see in Section VI, this suboptimal and yet efficient relay selection strategy does not significantly degrade the performance of the optimal solution. Algorithm 2, gives this solution that is labeled as LAURA2.

B. Constant Power Relay Transmission with Relay Selection Based on Source Relay CSI (LAURA2-CPR)

The relay selection criterion according to SNR of source to relays can also be applied to the LAURA1 scheme with adaptive power source and constant power relays (Section IV-B). This will further reduce the computational complexity and CSI requirements. A modification of the Algorithm 2 yields the solution with adaptive power source and constant power relay transmission, where the step 4 is replaced with the following

$$\text{Set } S_i = S \text{ and } S_s = \min(S_{\text{tot}} - N_C S, S \frac{\Gamma_n^r}{\gamma_{si}^-}).$$

Algorithm 2: LAURA with Modified Relay Selection

- 1) Select $n = N$.
 - 2) If $n = 0$ then go to outage mode and exit.
 - 3) Sort the set of available relays \mathcal{M}_R according to their γ_{si} in descending order and select \mathcal{M}_C as the first N_C in the set.
 - 4) Solve (11) and obtain S_s and S_i for $i \in \mathcal{M}_C$.
 - 5) Calculate γ_{eq} .
 - 6) If C2 in (10) is satisfied, set $TM = n$ and exit; else $n = n - 1$ and go to step 2.
-

C. Constant Power Relay Transmission with Relay Selection Based on Source Relay Channel Statistics (LAURA3-CPR)

The instantaneous relay selection criterion according to SNR of source to relays involves high speed (per frame) switching of relays and hence a rather sizable network control overhead. A relay selection criterion according to the statistics of source to relay channels can help mitigate this problem. This will further reduce the computational complexity and CSI requirements since the selected relays are fixed as long as the average SNRs of source to relays remain unchanged. A modification of the Algorithm 2 yields the solution for adaptive power source transmission and constant power relay transmission in which the step 3 is replaced as follows

Sort the set of available relays \mathcal{M}_R according to their $\bar{\gamma}_{si}$ in descending order and select \mathcal{M}_C as the first N_C in the set.

The selection of relays according to the average channel conditions also makes the theoretical performance analysis of the system possible. In the following, we present a performance analysis of LAURA3-CPR. The event A_n in this case using the upper bound for equivalent SNR is expressed by

$$\Pr(A_n) = \Pr\left(\gamma_{eq,u} \geq \Gamma_n^d \mid S_s = \tilde{S}_{s,n}(\gamma_{si}^{\tilde{}})\right), \quad (29)$$

where $\tilde{S}_{s,n}(\gamma_{si}^{\tilde{}}) = \min(S_{tot} - N_C S, S \frac{\Gamma_n^d}{\gamma_{si}^{\tilde{}}})$. In order to calculate the probability of event A_n , we first derive the moment generating function (MGF) of $\gamma_{eq,u}$ given $\gamma_{si}^{\tilde{}}$ and $S_s = \tilde{S}_{s,n}(\gamma_{si}^{\tilde{}})$. Since $\frac{S_s}{S} \gamma_{sd}$ and $\{\gamma_{i,u}\}$ are all independent

of each other given $\gamma_{s\tilde{i}}$, the desired MGF knowing $S_s = \tilde{S}_{s,n}(\gamma_{s\tilde{i}})$ is given by

$$M_{\gamma_{\text{eq},u}|\gamma_{s\tilde{i}}}(s|x) = M_{\frac{\tilde{S}_s}{S}\gamma_{sd}|\gamma_{s\tilde{i}}}(s|x) \prod_{i \in \mathcal{M}_C} M_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(s|x), \quad (30)$$

where $M_{\frac{\tilde{S}_s}{S}\gamma_{sd}|\gamma_{s\tilde{i}}}(s|x)$ and $M_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(s|x)$ are respectively the MGF of $\frac{\tilde{S}_s}{S}\gamma_{sd}$ and $\gamma_{i,u}$ given $\gamma_{s\tilde{i}}$ and $S_s = \tilde{S}_{s,n}(\gamma_{s\tilde{i}})$.

Using the definition of the MGF as $M_X(s) = \mathbf{E}(e^{-sX})$, it can be easily shown that

$$M_{\frac{\tilde{S}_s}{S}\gamma_{sd}|\gamma_{s\tilde{i}}}(s|x) = \frac{1}{1 + s \cdot \frac{\tilde{S}_{s,n}(x)}{S}}. \quad (31)$$

In order to calculate $M_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(s|x)$ we first calculate cumulative distribution function (CDF) of $\gamma_{i,u}$ as follows

$$F_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(z) = \Pr(\gamma_{i,u} \leq z|\gamma_{s\tilde{i}} = x) = 1 - \Pr\left(\frac{S_s}{S}\gamma_{si} \geq z|\gamma_{s\tilde{i}} = x\right)\Pr(\gamma_{id} \geq z), \quad (32)$$

where $\Pr(\gamma_{id} > z) = e^{-\frac{z}{\gamma_{id}}}$. Using the conditional PDF of $f_{\gamma_{si}|\gamma_{s\tilde{i}}}(y|x)$ according to Appendix A, we have

$$\begin{aligned} \Pr\left(\frac{S_s}{S}\gamma_{si} > z|\gamma_{s\tilde{i}} = x\right) &= \int_{\frac{z}{\tilde{S}_{s,n}(x)/S}}^{\infty} f_{\gamma_{si}|\gamma_{s\tilde{i}}}(y|x) dy \\ &= \int_{\frac{z}{\tilde{S}_{s,n}(x)/S}}^{\infty} \left[\frac{B_i(x)}{C(x)} \frac{1}{\gamma_{si}} e^{-\frac{y}{\gamma_{si}}} \mathcal{U}(x-y) + \frac{D_i(x)}{C(x)} \delta(y-x) \right] dy \\ &= \left[\frac{B_i(x)}{C(x)} \left(e^{-\frac{S z}{\tilde{S}_{s,n}(x)\gamma_{si}}} - e^{-\frac{x}{\gamma_{si}}} \right) + \frac{D_i(x)}{C(x)} \right] \mathcal{U}\left(x - \frac{S z}{\tilde{S}_{s,n}(x)}\right), \end{aligned} \quad (33)$$

where $\mathcal{U}(\cdot)$ and $\delta(\cdot)$ are unit step and unit impulse functions, respectively, and $B_i(x)$, $C(x)$ and $D_i(x)$ are defined in Appendix A. Then,

$$\begin{aligned} M_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(s|x) &= s \int_0^{\infty} F_{\gamma_{i,u}|\gamma_{s\tilde{i}}}(z|x) e^{-sz} dz \\ &= 1 - \frac{B_i(x)}{C(x)} \frac{s}{\frac{S}{\tilde{S}_{s,n}(x)\gamma_{si}} + \frac{1}{\gamma_{id}} + s} \cdot \left(1 - e^{-x \frac{\tilde{S}_{s,n}(x)}{S} \left(\frac{S}{\tilde{S}_{s,n}(x)\gamma_{si}} + \frac{1}{\gamma_{id}} + s \right)} \right) \\ &\quad + \left(\frac{B_i(x)}{C(x)} e^{-\frac{x}{\gamma_{si}}} - \frac{D_i(x)}{C(x)} \right) \cdot \frac{s}{\frac{1}{\gamma_{id}} + s} \left(1 - e^{-x \frac{\tilde{S}_{s,n}(x)}{S} \left(\frac{1}{\gamma_{id}} + s \right)} \right). \end{aligned} \quad (34)$$

Finally,

$$\Pr(A_n) = \Pr(\gamma_{\text{eq}} \geq \Gamma_n^d) = 1 - \mathbf{E}_x \left\{ \Pr(\gamma_{\text{eq}} \leq \Gamma_n^d | \gamma_{s\tilde{i}} = x) \right\} = 1 - \mathbf{E}_x \left\{ \mathfrak{L}^{-1} \left\{ \frac{M_{\gamma_{\text{eq}}|\gamma_{s\tilde{i}}}(s|x)}{s} \right\}_{\gamma_{\text{eq}} = \Gamma_n^d} \right\}, \quad (35)$$

where \mathfrak{L}^{-1} denotes inverse Laplace transform with respect to $\gamma_{\text{eq},u}$ that is simply computed through symbolic evaluation with MATLAB for every \mathcal{M}_R and \mathcal{M}_C . Then, the expectation with respect to $\gamma_{s\tilde{i}}$ is computed through numerical integration.

Following (20), the probability of TM m for LAURA3-CPR is expressed as

$$P_m^{\text{LAURA3-CPR}} = \Pr\left(\bigcup_{n=m}^N A_n\right) - \Pr\left(\bigcup_{n=m+1}^N A_n\right) = \mathbf{E} \left\{ \mathbf{I}(A_{\tilde{n}_m}) - \mathbf{I}(A_{\tilde{n}_{m+1}}) \right\}, \quad (36)$$

where

$$\tilde{n}_m(\gamma_{\text{eq,u}}, \gamma_{\tilde{s}i}) = \arg \min_{n \in \{m, \dots, N\}} \left(\gamma_{\text{eq,u}} \geq \Gamma_n^{\text{d}} \mid S_s = \tilde{S}_{s,n}(\gamma_{\tilde{s}i}) \right). \quad (37)$$

In order to facilitate the analysis we consider an approximation like the one in (22) as

$$\tilde{n}_m(\gamma_{\text{eq,u}}, \gamma_{\tilde{s}i}) \approx m. \quad (38)$$

And finally, the probability of TM m is

$$P_m^{\text{LAURA3-CPR}} = \Pr(A_m) - \Pr(A_{m+1}). \quad (39)$$

Calculating the probability of TM based on (39) and (35), enables the computation of average spectral efficiency according to (9).

Remark 2: Since for $N_C = N_R$ no relay selection is employed, the LAURA performance is independent of the relay selection strategy. Hence, the presented performance evaluation of LAURA3-CPR in (39) (and (35)) also applies to LAURA1-CPR and LAURA2-CPR schemes.

VI. PERFORMANCE EVALUATION

In this section, the performance of the proposed LAURA1, LAURA2 and LAURA3 schemes of different relay selection strategies in conjunction with different power control mechanisms of adaptive power, CP and CPR are evaluated. Both analytical and numerical results are presented and the effects of different parameters on the performance are investigated.

A. Experiment Setup

Figure 1 illustrates the topology of the network under consideration with N_R available relays. We consider average SNR of each channel proportional to $\frac{1}{\ell^\alpha}$, due to path loss, where ℓ denotes the distance between the two parties (α is set to 4 in this paper). Without loss of generality we consider the distance between S and D nodes normalized to 1. Relays are all located on a line perpendicular to the line connecting S and D nodes each distanced 0.1 apart as depicted in Figure 1. As shown in Fig. 1, UR_1 node is fixed at the distance ℓ_{s1} on the line connecting S and D nodes. In all figures, $\text{BER}_{\text{tgt}}^{\text{r}}$ and $\text{BER}_{\text{tgt}}^{\text{d}}$ are set to 0.1 and 10^{-6} , respectively. The sum power constraint S_{tot} is set to $(N_R + 1)S$ in all cases.

The TMs used with the proposed LAURA schemes could be in fact any set of possible channel coding and modulation pairs. The suggestion is to use sharp channel codes to obtain sharp BER curves for TMs, which provide

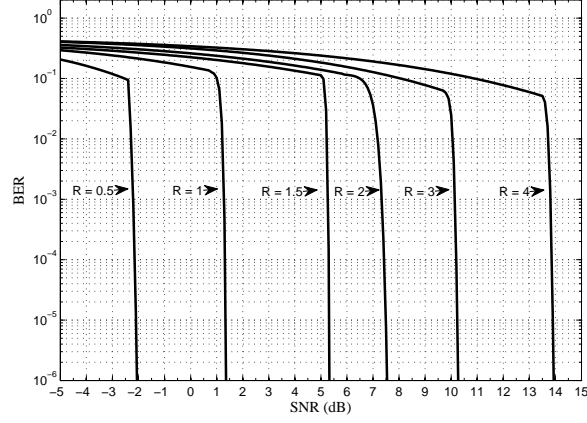


Fig. 2. BER curves for six transmission modes and their corresponding rates

TABLE II
TRANSMISSION MODES FOR AMC SCHEME AND THEIR CORRESPONDING FITTING PARAMETERS

Mode	1	2	3	4	5	6
modulation	BPSK	4-QAM	8-QAM	8-QAM	16-QAM	32-QAM
coding rate	1/2	1/2	1/2	2/3	3/4	4/5
rate: R_n	1/2	1	3/2	2	3	4
p_n	2.97	1.17	0.80	0.65	0.46	0.38
q_n	1.05	0.68	0.54	0.59	0.67	0.58
a_n	1.55	0.13	0.14	0.12	0.06	0.07
b_n	0.62	1.43	3.48	6.19	10.37	24.09
c_n	41.9	34.90	20.03	3.52	5.13	2.21
k_n	16.81	104.70	48.83	75.99	6.77	6.50

a low security gap and an acceptable reliability performance (for the design parameter ranges of interest). The set of LDPC codes in DVB-S2 standard [17] offer this characteristic. These channel codes in conjunction with different modulation schemes yield the BER curves depicted in Fig. 2. The TMs specifications and fitting parameters used for numerical results are presented in Table II.

B. Numerical Results

Figure 3 depicts the end to end average spectral efficiency of LAURA1, LAURA1-CPR and LAURA1-CP schemes illustrating the effect of type of power control. The horizontal axis indicates $\bar{\gamma}_{sd}$. It is observed that for LAURA1-CP, increasing average SNR of S-D link beyond a specific value leads to a reduced average spectral efficiency. This is

due to the limitation in number of TMs. If there is a TM that could still satisfy the security constraint in high SNRs, then the declination occurs later at a higher average SNR of S-D channel. Comparing the performance of LAURA1 and LAURA1-CP highlights the advantage of source power adaptation that significantly reduces the outage events for enforcing the security constraint.

The performance comparison of LAURA1 and LAURA1-CPR suggests that for low to medium SNR regimes relay power adaptation improves the performance of the system. This is more significant with larger N_C 's. One sees from the performance of LAURA1 and LAURA1-CP that the larger the number of cooperating relays, the better the performance we achieve through cooperation. However, there is no significant advantage in using more than four relays for $N_R = 5$. This observation is in contrast to the understanding in traditional (non-secure) amplify and forward relaying that the best relay selection ($N_C = 1$) achieves almost all of the spectral efficiency performance gain [18].

Comparing LAURA1-CPR for $N_C = 4$ and 5 in low SNR regimes reveals that with constant power relays and sum power constraint, increasing the number of cooperating relays beyond a limit may decrease the performance. The reason is that in this case, the available power to the S-node (and hence the SNRs of source to relays) becomes limited.

Figure 4 illustrates the effect of relay selection strategies on the average spectral efficiency performance of LAURA schemes. The main observation is that the performance of relay selection according to source-relay channel SNRs coincides with that of optimal relay selection. This is evident both by performance comparison of LAURA1 with LAURA2 and LAURA1-CPR with LAURA2-CPR. It is also observed that the performance of LAURA3-CPR with relay selection according to average source-channel SNRs approaches that of LAURA2-CPR utilizing instantaneous channel SNRs only when the number of relays increases to $N_C = 5$. Nevertheless, the relay selection according to average channel statistics requires slower relay switching.

Figure 5 depicts and compares the simulation and approximate analytical results for certain LAURA schemes. As discussed in Remark 2, for $N_C = N_R$, since no relay selection is employed, the theoretical calculation of spectral efficiency proposed for V-C applies to all the schemes with constant power relay transmission. The results verify the accuracy of the proposed analytical performance evaluations.

Figure 6 demonstrates the effect of relays positions on the performance of the proposed LAURA scheme. It is evident that when the relays are positioned closer to the D node, LAURA provides a better average spectral efficiency

performance. In fact, in this setting the security constraint is satisfied more easily. Our experiments reveal that in an amplify and forward cooperative communication system, in the SNR ranges of interest for cooperation (low S-D SNR regimes), when a sufficiently large number of available relays are utilized, provisioning the security constraint in LAURA only imposes a negligible spectral efficiency performance penalty. In fact, for larger number of cooperating relays, the performance penalty is small even for high SNR regime, e.g., less than 7% for $N_C = N_R = 5$.

VII. CONCLUSIONS

In this paper, a link adaptation and untrusted relay assignment framework for cooperative communications with physical layer security is proposed. The design problem is set up for highly spectrally efficient communications with reliability for the destination and security in the presence of untrusted relays. The security constraint is imposed by ensuring that the relays cannot decode useful information from the signal they relay. The optimal solution to the design optimization problem is presented while strategies for mitigating practical challenges are also proposed. This involves several relay selection strategies and power adaptation solutions. Performance of these approaches is analyzed theoretically, in certain cases, and rigorously through simulations. The effect of different design strategies and parameters, including relay selection, power control at source and/or relays, relays positions, and number of cooperating relays are investigated.

The future research of interest in this direction includes tackling potential eavesdroppers in the network or considering the malicious behavior of relays without a service level trust. Another orientation of research interest is to design particular channel codes with low security gap and reliability performance within this framework and in line with the works reported in [10].

APPENDIX A

In this section we derive the joint and conditional PDF of $\gamma_{\tilde{s}i}$ and γ_{si} . The joint cumulative distribution function of these two variables is given by

$$F_{\gamma_{\tilde{s}i}, \gamma_{si}}(x, y) = \Pr(\max_j \gamma_{sj} < x, \gamma_{si} < y) = \prod_{\substack{j=1 \\ j \neq i}}^{N_R} \left(1 - e^{-\frac{x}{\gamma_{sj}}}\right) \left[\left(1 - e^{-\frac{x}{\gamma_{si}}}\right) \mathcal{U}(y - x) + \left(1 - e^{-\frac{y}{\gamma_{si}}}\right) \mathcal{U}(x - y) \right].$$

Then, the joint probability density function of $\gamma_{s\bar{i}}$ and γ_{si} is

$$\begin{aligned}
 f_{\gamma_{s\bar{i}}, \gamma_{si}}(x, y) &= \frac{\partial^2 F_{\gamma_{s\bar{i}}, \gamma_{si}}(x, y)}{\partial x \partial y} \\
 &= \sum_{\substack{l \neq i \\ l=1}}^{N_R} \frac{1}{\bar{\gamma}_{sl}} e^{-\frac{x}{\bar{\gamma}_{sl}}} \prod_{\substack{j \neq l \\ j \neq i}} \left(1 - e^{-\frac{x}{\bar{\gamma}_{sj}}}\right) \left[\frac{1}{\bar{\gamma}_{si}} e^{-\frac{y}{\bar{\gamma}_{si}}} \mathcal{U}(x - y) \right] + \prod_{\substack{j \neq i \\ j=1}}^{N_R} \left(1 - e^{-\frac{x}{\bar{\gamma}_{sj}}}\right) \frac{1}{\bar{\gamma}_{si}} e^{-\frac{x}{\bar{\gamma}_{si}}} \delta(y - x) \\
 &\triangleq B_i(x) \left[\frac{1}{\bar{\gamma}_{si}} e^{-\frac{y}{\bar{\gamma}_{si}}} \mathcal{U}(x - y) \right] + D_i(x) \delta(y - x),
 \end{aligned} \tag{40}$$

and the PDF of $\gamma_{s\bar{i}}$ is simply

$$f_{\gamma_{s\bar{i}}}(x) = \sum_{l=1}^{N_R} \frac{1}{\bar{\gamma}_{sl}} e^{-\frac{x}{\bar{\gamma}_{sl}}} \prod_{j \neq l} \left(1 - e^{-\frac{x}{\bar{\gamma}_{sj}}}\right) \triangleq C(x). \tag{41}$$

The PDF of γ_{si} given $\gamma_{s\bar{i}}$ is then

$$f_{\gamma_{si}|\gamma_{s\bar{i}}}(y|x) = \frac{f_{\gamma_{s\bar{i}}, \gamma_{si}}(x, y)}{f_{\gamma_{s\bar{i}}}(x)} = \frac{B_i(x)}{C(x)} \left[\frac{1}{\bar{\gamma}_{si}} e^{-\frac{y}{\bar{\gamma}_{si}}} \mathcal{U}(x - y) \right] + \frac{D_i(x)}{C(x)} \delta(y - x). \tag{42}$$

REFERENCES

- [1] H. Khodakarami and F. Lahouti, "Link adaptation for fixed relaying with untrusted relays: Transmission strategy design and performance analysis," in *Proc. International Conference on Telecommunications (ICT)*, Cyprus, 2011, pp. 309–314.
- [2] Y. Oohama, "Coding for relay channels with confidential messages," *Information Theory Workshop*, 2001.
- [3] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *submitted to IEEE Trans. Inform. Theory*, 2007.
- [4] T. Nechiporenko, K. T. Phan, C. Tellambura, and H. H. Nguyen, "On the capacity of rayleigh fading cooperative systems under adaptive transmission," *IEEE Trans. Wireless Commun.*, vol. 9, no. 4, pp. 1626–1631, Apr 2009.
- [5] K. S. Hwang, Y. C. Ko, and M. Alouini, "Performance analysis of incremental opportunistic relaying over identically and non-identically distributed cooperative paths," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 1953–1961, Apr 2009.
- [6] T. C.-Y. Ng and W. Yu, "Joint optimization of relay strategies and resource allocations in cooperative cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 328–339, Feb 2007.
- [7] Y. Jing and H. Jafarkhani, "Single and multiple relay selection schemes and their achievable diversity orders," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1414–1423, Mar. 2009.
- [8] M. Mardani, J. S. Harsini, F. Lahouti, and B. Eliasi, "Joint adaptive modulation coding and cooperative arq for wireless relay networks," in *Proc. IEEE international Symposium on Wireless Communication Systems (ISWCS)*, Rykevick, Island, Oct. 2008.
- [9] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Application of LDPC codes to the wiretap channel," *IEEE Trans. Inform. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug 2007.
- [10] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for physical layer security," in *Proc. IEEE GLOBECOM, USA*, 2009, pp. 1–6.
- [11] H. Khodakarami and F. Lahouti, "Link adaptation for physical layer security over wireless fading channels," *Communications, IET*, vol. 6, no. 3, pp. 353–362, 2012.
- [12] K. J. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative communications and networking*. Cambridge University Press, 2009.

- [13] D. J. C. MacKay and C. P. Hesketh, "Performance of low density parity check codes as a function of actual and assumed noise levels," *Electr. Notes Theor. Comput. Sci.*, vol. 74, pp. 89–96, 2003.
- [14] J. Luo, R. Blum, L. Cimini, L. Greenstein, and A. Haimovich, "Decode-and-forward cooperative diversity with power allocation in wireless networks," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 3, pp. 793–799, 2007.
- [15] I. Maric and R. Yates, "Bandwidth and power allocation for cooperative strategies in gaussian relay networks," *Information Theory, IEEE Transactions on*, vol. 56, no. 4, pp. 1880–1889, 2010.
- [16] F. S. Hillier and G. J. Lieberman, *Introduction to Operations Research*. Oakland, CA: Holden-Day, Inc., 1986.
- [17] *DVB-S.2 Standard Specification*, ETSI EN 302 307 V1.1.1, Mar. 2005.
- [18] A. Bletsas, A. K. D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas in Commun.*, vol. 24, no. 3, p. 659672, May 2006.

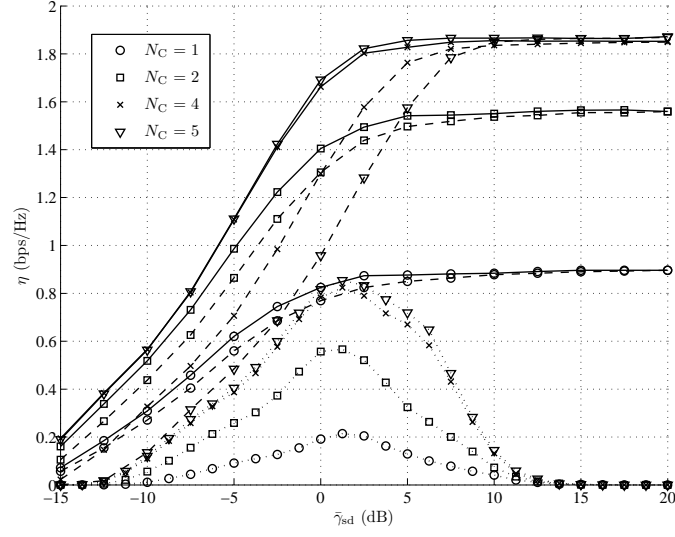


Fig. 3. Average spectral efficiency of different transmission power strategies with optimal relay selection for $N_R = 5$ and $\ell_{s1} = 0.9$. Solid, dashed and dotted lines are for LAURA1, LAURA1-CPR and LAURA1-CP, respectively.

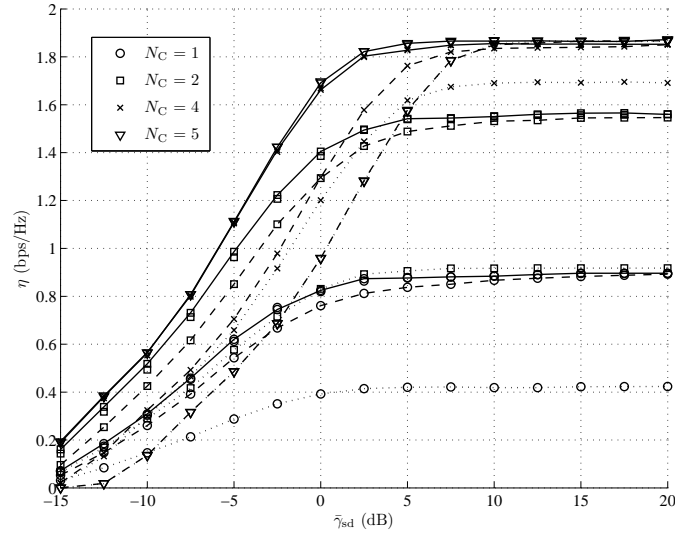


Fig. 4. Average spectral efficiency of different relay selection schemes for $N_R = 5$ and $\ell_{s1} = 0.9$. Solid, dashed and dotted lines are for LAURA1, LAURA2-CPR and LAURA3-CPR, respectively. No line is used to connect the markers associated with LAURA2, but they closely follow those of LAURA1. Note that the performance of LAURA2-CPR and LAURA3-CPR for $N_C = 5$ coincide.

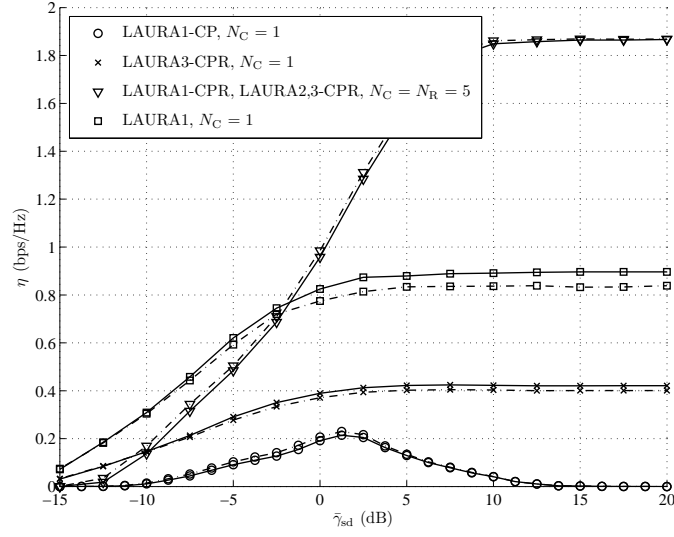


Fig. 5. Comparison of analytical and simulation results for average spectral efficiency of different LAURA schemes for $N_R = 5$, $\ell_{s1} = 0.9$. Solid and dashed lines depict the simulation and analytical results, respectively.

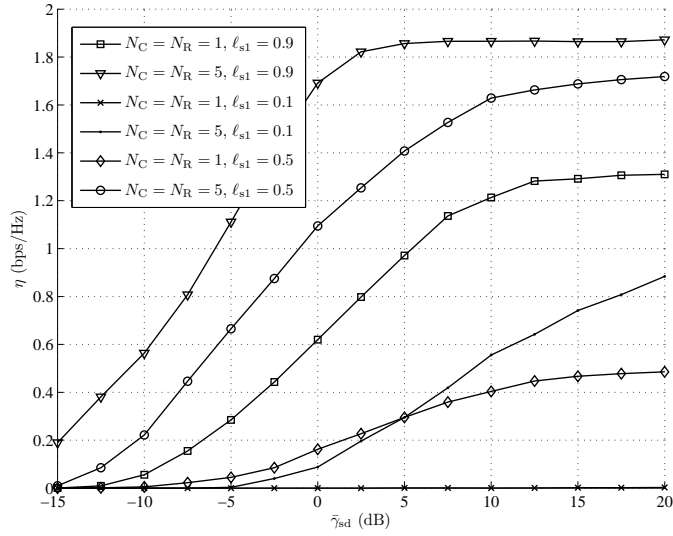


Fig. 6. Average spectral efficiency of LAURA1 scheme for different relay placements.