Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems

Yulong Zou, Senior Member, IEEE, Benoit Champagne, Senior Member, IEEE, Wei-Ping Zhu, Senior Member, IEEE, and Lajos Hanzo, Fellow, IEEE

Abstract—We consider a cognitive radio (CR) network consisting of a secondary transmitter (ST), a secondary destination (SD) and multiple secondary relays (SRs) in the presence of an eavesdropper, where the ST transmits to the SD with the assistance of SRs, while the eavesdropper attempts to intercept the secondary transmission. We rely on careful relay selection for protecting the ST-SD transmission against the eavesdropper with the aid of both single-relay and multi-relay selection. To be specific, only the “best” SR is chosen in the single-relay selection for assisting the secondary transmission, whereas the multi-relay selection invokes multiple SRs for simultaneously forwarding the ST’s transmission to the SD. We analyze both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing. We also evaluate the performance of classic direct transmission and artificial noise based methods for the purpose of comparison with the proposed relay selection schemes. It is shown that as the intercept probability requirement is relaxed, the outage performance of the direct transmission, the artificial noise based and the relay selection schemes improves, and vice versa. This implies a trade-off between the security and reliability of the secondary transmission in the presence of eavesdropping attacks, which is referred to as the security-reliability trade-off (SRT). Furthermore, we demonstrate that the SRTs of the single-relay and multi-relay selection schemes are generally better than that of classic direct transmission, explicitly demonstrating the advantage of the proposed relay selection in terms of protecting the secondary transmissions against eavesdropping attacks. Moreover, as the number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve. Finally, our numerical results show that as expected, the multi-relay selection scheme achieves a better SRT performance than the single-relay selection.

Index Terms—Security-reliability trade-off, relay selection, intercept probability, outage probability, eavesdropping attack, cognitive radio.

I. INTRODUCTION

The security aspects of cognitive radio (CR) systems [1]–[3] have attracted increasing attention from the research community. Indeed, due to the highly dynamic nature of the CR network architecture, legitimate CR devices become exposed to both internal as well as to external attackers and hence they are extremely vulnerable to malicious behavior. For example, an illegitimate user may intentionally impose interference (i.e., jamming) for the sake of artificially contaminating the CR environment [4]. Hence, the CR users fail to accurately characterize their surrounding radio environment and may become misled or compromised, which leads to a malfunction. Alternatively, an illegitimate user may attempt to tap the communications of authorized CR users by eavesdropping, to intercept confidential information.

Clearly, CR networks face diverse security threats during both spectrum sensing [5], [6] as well as spectrum sharing [7], [6] spectrum mobility [8] and spectrum management [9]. Extensive 57 studies have been carried out for protecting CR networks both against primary user emulation (PUE) [10] and against denial-of-service (DoS) attacks [11]. In addition to PUE and DoS attacks, eavesdropping is another main concern in protecting the data confidentiality [12], although it has received less attention in literature on CR network security. Traditionally, cryptographic techniques are employed for guaranteeing transmission confidentiality against an eavesdropping attack. However, this introduces a significant computational overhead [13] as well as 66 imposing additional system complexity in terms of the secret key management [14]. Furthermore, the existing cryptographic approaches are not perfectly secure and can still be decrypted by an eavesdropper (E) provided that it has the capacity to carry out exhaustive key search with the aid of brute-force attack [15].

Physical-layer security [16], [17] is emerging as an efficient approach for defending authorized users against eavesdropping attacks by exploiting the physical characteristics of wireless 73 channels. In [17], Leung-Yan-Cheong and Hellman demonstrated that perfectly secure and reliable transmission can be achieved, when the wiretap channel spanning from the source to the eavesdropper is a further degraded version of the main 78
channel between the source and destination. They also showed that the maximal secrecy rate achieved at the legitimate destination, which is termed the secrecy capacity, is the difference between the capacity of the main channel and that of the wiretap channel. In [18]–[20], the secrecy capacity limits of wireless fading channels were further developed and characterized from an information-theoretic perspective, demonstrating the detrimental impact of wireless fading on the physical-layer security. To combat the fading effects, both multiple-input multiple-output (MIMO) schemes [21], [22] as well as cooperative relaying [23]–[25] and beamforming techniques [26], [27] were investigated for the sake of enhancing the achievable wireless secrecy capacity. Although extensive research efforts were devoted to improving the security of traditional wireless networks [16]–[27], less attention has been dedicated to CR networks. In [28] and [29], the achievable secrecy rate of the secondary transmission was investigated under a specific quality-of-service (QoS) constraint imposed on the primary transmission. Additionally, an overview of the physical-layer security aspects of CR networks was provided in [30], where several security attacks as well as the related countermeasures are discussed. In contrast to conventional non-cognitive wireless networks, the physical-layer security of CR networks has to consider diverse additional challenges, including the protection of the primary user’s QoS and the mitigation of the mutual interference between the primary and secondary transmissions.

Motivated by the above considerations, we explore the physical-layer security of a CR network comprised of a secondary transmitter (ST) communicating with a secondary destination (SD) with the aid of multiple secondary relays (SRs) in the presence of an unauthorized attacker. Our main focus is on investigating the security-reliability trade-off (SRT) of the cognitive relay transmission in the presence of realistic physical-layer security. The notion of the SRT in wireless physical-layer security was introduced and examined in [31], where the security and reliability was characterized in terms of the intercept probability and outage probability, respectively. In contrast to the conventional non-cognitive wireless networks studied in [31], the SRT analysis of CR networks presented in this work additionally takes into account the mutual interference between the primary user (PU) and secondary user (SU).

The main contributions of this paper are summarized as follows.

- We propose two relay selection schemes, namely both single-relay and multi-relay selection, for protecting the secondary transmissions against eavesdropping attacks. More specifically, in the single-relay selection (SRS) scheme, only a single relay is chosen from the set of multiple SRs for forwarding the secondary transmissions from the ST to the SD. By contrast, the multi-relay selection (MRS) scheme employs multiple SRs for simultaneously assisting the ST-SD transmissions.
- We present the mathematical SRT analysis of the proposed SRS and MRS schemes in the presence of realistic spectrum sensing. Closed-form expressions are derived for the intercept probability (IP) and outage probability (OP) of both schemes for transmission over Rayleigh fading channels. The numerical SRT results of conventional direct transmission and artificial noise based schemes are also provided for comparison purposes.
- It is shown that as the spectrum sensing reliability is increased and/or the false alarm probability is reduced, the SRTs of both the SRS and MRS schemes are improved. Numerical results demonstrate that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRTs.

The remainder of this paper is organized as follows. Section II presents the system model of physical-layer security in CR networks in the context of both the direct transmission as well as the SRS and MRS schemes. In Section III, we analyze the SRTs of these schemes in the presence of realistic spectrum sensing over Rayleigh fading channels. Next, numerical SRT results of the direct transmission, SRS and MRS schemes are given in Section IV, where the SRT performance of the artificial noise based scheme is also numerically evaluated for comparison purposes. Finally, Section V provides our concluding remarks.

II. RELAY SELECTION AIDED PROTECTION AGAINST EAVESDROPPING IN CR NETWORKS

We first introduce the overall system model of physical-layer security in CR networks. We then present the signal model of the conventional direct transmission approach, which will serve as our benchmarker, as well as of the SRS and MRS schemes for improving the CR system’s security against eavesdropping attacks.

A. System Model

As shown in Fig. 1, we consider a primary network in coexistence with a secondary network (also referred to as a CR network). The primary network includes a primary base station (PBS) and multiple primary users (PUs), which communicate with the PBS over the licensed spectrum. By contrast, the secondary network consisting of one or more STs and SDs exploits the licensed spectrum in an opportunistic way. To
be specific, a particular ST should first detect with the aid of spectrum sensing whether or not the licensed spectrum is occupied by the PBS. If so, the ST is not at liberty to transmit to avoid interfering with the PUs. If alternatively, the licensed spectrum is deemed to be unoccupied (i.e. a spectrum hole is detected), then the ST may transmit to the SD over the detected spectrum hole. Meanwhile, E attempts to intercept the secondary transmission from the ST to the SD. For notational convenience, let \( H_0 \) and \( H_1 \) represent the event that the licensed spectrum is deemed to be occupied. \( \hat{H} = H_0 \) represents the case that the licensed spectrum is deemed to be unoccupied, while \( \hat{H} = H_1 \) indicates that the licensed spectrum is deemed to be occupied.

The probability \( P_d \) of correct detection of the presence of PBS and the associated false alarm probability \( P_f \) are defined as \( P_d = \Pr(\hat{H} = H_1|H_1) \) and \( P_f = \Pr(\hat{H} = H_0|H_0) \), respectively. Due to the background noise and fading effects, it is impossible to achieve perfectly reliable spectrum sensing without missing the detection of an active PU and without false alarm, which suggests that a spectral band is occupied by a PU, when it is actually unoccupied. Moreover, the missed detection of the presence of PBS will result in interference between the PU and SU. To guarantee that the interference imposed on the PUs is below a tolerable level, both the successful detection probability (SDP) \( P_d \) and false alarm probability (FAP) \( P_f \) should be within a meaningful target range. For example, the IEEE 802.22 standard requires \( P_d > 0.9 \) and \( P_f < 0.1 \) [2]. For better protection of PUs, we consider \( P_d = 0.99 \) and \( P_f = 0.01 \), unless otherwise stated. Additionally, we consider a Rayleigh fading model for characterizing all the channels between any two nodes of Fig. 1. Finally, all the received signals are assumed to be corrupted by additive white Gaussian noise (AWGN) having a zero mean and a variance of \( N_0 \).

### B. Direct Transmission

Let us first consider the conventional direct transmission as a benchmark scheme. Let \( x_p \) and \( x_s \) denote the random symbols transmitted by the PBS and the ST at a particular time instance. Without loss of generality, we assume \( E[|x_p|^2] = 213 \) where \( E[\cdot] \) represents the expected value operator. The transmit powers of the PBS and ST are denoted by \( P_p \) and \( P_s \), respectively. Given that the licensed spectrum is deemed to be unoccupied by the PBS (i.e. \( \hat{H} = H_0 \)), ST transmits its signal \( x_s \) at a power of \( P_s \). Then, the signal received at the SD can be written as

\[
y_d = h_{sd}\sqrt{P_s}x_s + n_d,
\]

where \( h_{sd} \) and \( n_d \) represent the fading coefficients of the channel spanning from ST to SD and that from PBS to SD, respectively. Furthermore, \( n_d \) represents the AWGN received at the SD and the random variable (RV) \( \alpha \) is defined as

\[
\alpha = \begin{cases} 
0, & H_0 \\
1, & H_1,
\end{cases}
\]

where \( H_0 \) represents that the licensed spectrum is unoccupied by PBS and no primary signal is transmitted, leading to \( \alpha = 0 \). By contrast, \( H_1 \) represents that PBS is transmitting its signal \( x_p \) over the licensed spectrum, thus \( \alpha = 1 \). Meanwhile, due to the broadcast nature of the wireless medium, the ST’s signal will be overhead by E and the overhead signal can be expressed as

\[
y_e = h_{se}\sqrt{P_s}x_s + h_{pe}\sqrt{\alpha P_p}x_p + n_e,
\]

where \( h_{se} \) and \( h_{pe} \) represent the fading coefficients of the channel spanning from ST to E and that from PBS to E, respectively, while \( n_e \) represents the AWGN received at E.

Upon combining Shannon’s capacity formula [31] with (1), we obtain the capacity of the ST-SD channel as

\[
C_{sd} = \log_2 \left( 1 + \frac{|h_{sd}|^2 \gamma_s}{\alpha |h_{pe}|^2 \gamma_p + 1} \right),
\]

where \( \gamma_s = P_s/N_0 \) and \( \gamma_p = P_p/N_0 \). Similarly, the capacity of the ST-E channel is obtained from (3) as

\[
C_{se} = \log_2 \left( 1 + \frac{|h_{se}|^2 \gamma_s}{\alpha |h_{pe}|^2 \gamma_p + 1} \right).
\]

### C. Single-Relay Selection

In this subsection, we consider the cognitive relay network of Fig. 2, where both SD and E are assumed to be beyond the coverage area of the ST [24], [25], and \( N \) secondary relays (SRs) are employed for assisting the cognitive ST-SD transmission. We assume that a common control channel (CCC) [6] is available for coordinating the actions of the different network nodes and the decode-and-forward (DF) relaying using two adjacent time slots is employed. More specifically, once the licensed spectrum is deemed to be unoccupied, the ST first broadcasts its signal \( x_s \) to the \( N \) SRs, which attempt to decode \( x_s \) from their received signals. For notational convenience, let \( D \) represent the set of SRs that succeed in decoding \( x_s \). Given \( N \) SRs, there are \( 2^N \) possible subsets \( D \), thus the sample space of \( D \) is formulated as

\[
\Omega = \{ \emptyset, D_1, D_2, \ldots, D_n, \ldots, D_{2^N-1} \},
\]

where \( \emptyset \) represents the empty set and \( D_n \) represents the \( n \)-th non-empty subset of the \( N \) SRs. If the set \( D \) is empty, implying that no SR decodes \( x_s \) successfully, then all the SRs remain silent and thus both SD and E are unable to decode \( x_s \) in this case. If the set \( D \) is non-empty, a specific SR is chosen from \( D \) to forward its decoded signal \( x_d \) to SD. Therefore, given \( \hat{H} = H_0 \) (i.e. the licensed spectrum is deemed unoccupied), ST broadcasts its signal \( x_s \) to \( N \) SRs at a power of \( P_p \) and a rate of \( R \). Hence, the signal received at a specific SR is given by

\[
y_i = h_{si}\sqrt{P_s}x_s + h_{pi}\sqrt{\alpha P_p}x_p + n_i,
\]

where \( h_{si} \) and \( h_{pi} \) represent the fading coefficients of the ST-SR and PBS-SR, channel, respectively, with
n \text{ representing the AWGN at SR}_i. From (7), we obtain the capacity of the ST-SR channel as
\[ C_{sl} = \frac{1}{2} \log_2 \left( 1 + \frac{|h_{sid}|^2 \gamma_S}{\alpha |h_{pid}|^2 |p| + 1} \right) , \] (8)
where the factor \( \frac{1}{2} \) arises from the fact that two orthogonal time slots are required for completing the message transmission from \( ST \) to \( SD \) via \( SR_i \). According to Shannon’s coding theorem, 296 if the data rate is higher than the channel capacity, the receiver becomes unable to successfully decode the source signal, regardless of the decoding algorithm adopted. Otherwise, the receiver can succeed in decoding the source signal. Thus, using (8), we can describe the event of \( D = 0 \) as
\[ C_{sl} < R, \quad i \in \{1, 2, \ldots, N\} . \] (9)
272 Meanwhile, the event of \( D = D_n \) is described as
\[ C_{sl} > R, \quad i \in D_n \]
273 where \( D_n \) represents the complementary set of \( D \). Without loss of generality, we assume that SR, is chosen within \( D_n \) to transmit its decoded result \( x_t \) at a power of \( P_t \), thus the signal received at SD can be written as
\[ y_d = h_{id} \sqrt{P_t} x_t + h_{pd} \sqrt{\alpha P} x_p + n_d , \] (11)
where \( h_{id} \) represents the fading coefficient of the \( SR_i \) - SD channel. From (11), the capacity of the \( SR_i \) - SD channel is given by
\[ C_{id} = \frac{1}{2} \log_2 \left( 1 + \frac{|h_{id}|^2 \gamma_S}{\alpha |h_{pd}|^2 |p| + 1} \right) , \] (12)
where \( i \in D_n \). In general, the specific \( SR_i \) having the highest instantaneous capacity to SD is chosen as the “best” \( SR \) for assiting the \( ST \)’s transmission. Therefore, the best relay selection criterion is expressed from (12) as
\[ \text{Best SR} = \arg \max_{i \in D_n} C_{id} = \arg \max_{i \in D_n} |h_{id}|^2 , \] (13)
284 which shows that only the channel state information (CSI) \( |h_{id}|^2 \) is required for performing the relay selection without the need for the eavesdropper’s CSI knowledge. Upon combining (12) and (13), we obtain the capacity of the channel spanning from the “best” \( SR \) to SD as
\[ C_{bd} = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_S}{\alpha |h_{pd}|^2 |p| + 1} \max_{i \in D_n} |h_{id}|^2 \right) , \] (14)
where the subscript ‘\( b \)’ in \( C_{bd} \) denotes the best \( SR \). It is observed from (14) that the legitimate transmission capacity of the SRS scheme is determined by the maximum of independent random variables (RVs) \( |h_{id}|^2 \) for different \( SR_i \)s. By contrast, one can see from (4) that the capacity of classic direct transmission is affected by the single RV \( |h_{sd}|^2 \). If all RVs \( |h_{id}|^2 \) and \( |h_{sd}|^2 \) are independent and identically distributed (i.i.d), it would be most likely that \( \max_{i \in D_n} |h_{id}|^2 \) is much higher than \( |h_{sd}|^2 \) for a sufficiently large number of \( SR \)s, resulting in a performance improvement over the SRS scheme over the classic direct transmission. However, even if the RVs \( |h_{id}|^2 \) and \( |h_{sd}|^2 \) are non-identically distributed and the mean value of \( |h_{id}|^2 \) is much higher than that of \( |h_{sd}|^2 \), then it may be more likely that \( \max_{i \in D_n} |h_{id}|^2 \) is smaller than \( |h_{sd}|^2 \) for a given number of \( SR \)s. In this extreme case, the classic direct transmission may perform better than the SRS scheme. It is worth mentioning that in practice, the average fading gain of the \( ST \) – SD channel, \( |h_{sd}|^2 \), should not be less than that of the ST-SD channel \( |h_{sd}|^2 \), since \( SR \)s are typically placed in the middle between the \( ST \) and SD. Hence, a performance improvement for the SRS scheme over classic direct transmission would be achieved in practical wireless systems. Note that although a factor \( 1/2 \) in (14) is imposed on the capacity of the main channel, it would not affect the performance of the SRS scheme from a SRT perspective, since the capacity of the wiretap channel is also multiplied by \( 1/2 \) as will be shown in (16).
285 Additionally, given that the selected \( SR \) transmits its decoded result \( x_t \) at a power of \( P_t \), the signal received at E is 316 expressed as
\[ y_e = h_{be} \sqrt{P_t} x_t + h_{pe} \sqrt{\alpha P} x_p + n_e , \] (15)
where \( h_{be} \) and \( h_{pe} \) represent the fading coefficients of the channel from “best” \( SR \) to E and that from PBS to E, respectively. From (15), the capacity of the channel spanning from the “best” \( SR \) to E is given by
\[ C_{be} = \frac{1}{2} \log_2 \left( 1 + \frac{|h_{be}|^2 \gamma_S}{\alpha |h_{pe}|^2 |p| + 1} \right) , \] (16)
where \( b \in D_n \) is determined by the relay selection criterion given in (13). As shown in (16), the eavesdropper’s channel 323 capacity is affected by the channel state information (CSI) of \( |h_{be}|^2 \) of the wiretap channel spanning from the “best” relay to E by 325 the eavesdropper. However, one can see from (13) that the best \( SR \) is selected from the decoding set \( D_n \) solely based on the main channel’s CSI \( |h_{id}|^2 \) i.e. without taking into account the 328 eavesdropper’s CSI knowledge of \( |h_{ie}|^2 \). This means that the 329 selection of the best relay aiming for maximizing the legitimate 330 transmission capacity of (14) would not lead to significantly 331
332 beneficial or adverse impact on the eavesdropper's channel
333 capacity, since the main channel and the wiretap channel are
334 independent of each other.
335 For example, if the random variables (RVs) \(|h_{ie}|^2\) related to
336 the different relays are i.i.d, we can readily infer by the law
337 of total probability that \(|h_{ie}|^2\) has the same probability den-
338 sity function (PDF) as \(|h_{ie}|^2\), implying that the eavesdropper’s
339 channel capacity of (16) is not affected by the selection of the
340 best relay given by (13). Therefore, the SRS scheme has no
341 obvious advantage over the classic direct transmission in terms
342 of minimizing the capacity of the wiretap channel. To elaborate
343 a little further, according to the SRT trade-off, a reduction of
344 the outage probability (OP) due to the capacity enhancement
345 of the main channel achieved by using the selection of the
346 best relay would be converted into an intercept probability
347 (IP) improvement, which will be numerically illustrated in
348 Section IV.

349 D. Multi-Relay Selection
350 This subsection presents a MRS scheme, where multiple SRs
351 are employed for simultaneously forwarding the source signal
352 to SD. To be specific, ST first transmits \(x_s\) to \(N\) SRs over a
353 detected spectrum hole. As mentioned in Subsection II-C, we
354 denote by \(D\) the set of SRs that successfully decode \(x_s\). If \(D\)
355 is empty, all SRs fail to decode \(x_s\) and will not forward the
356 source signal, thus both SD and E are unable to decode \(x_s\). If \(D\)
357 is non-empty (i.e. \(D = D_h\)), all SRs within \(D_h\) are utilized
358 for simultaneously transmitting \(x_s\) to SD. This differs from the
359 SRS scheme, where only a single SR is chosen from \(D_h\) for
360 forwarding \(x_s\) to SD. To make effective use of multiple SRs, a
361 weight vector denoted by \(w = [w_1, w_2, \ldots, w_{|D_h|}]^T\) is employed
362 at the SRs for transmitting \(x_s\), where \(|D_h|\) is the cardinality of
363 the set \(D_h\). For the sake of a fair comparison with the SRS
364 scheme in terms of power consumption, the total transmit power
365 across all SRs within \(D_h\) shall be constrained to \(P\), and thus the
366 weight vector \(w\) should be normalized according to \(\|w\| = 1\).
367 Thus, given \(D = D_h\) and considering that all SRs within \(D_h\) are
368 selected for simultaneously transmitting \(x_s\) with a weight vector
369 \(w\), the signal received at SD is expressed as

\[
 y_d^{\text{multi}} = \sqrt{P_s}w^T H_d x_s + \sqrt{\alpha P_d} h_{pd} x_p + n_d, \quad (17)
\]

370 where \(H_d = [h_{1d}, h_{2d}, \ldots, h_{|D_h|d}]^T\). Similarly, the signal received
371 at E can be written as

\[
 y_e^{\text{multi}} = \sqrt{P_s}w^T H_e x_s + \sqrt{\alpha P_e} h_{pe} x_p + n_e, \quad (18)
\]

372 where \(H_e = [h_{1e}, h_{2e}, \ldots, h_{|D_h|e}]^T\). From (17) and (18), the
373 signal-to-interference-plus-noise ratios (SINRs) at SD and E
374 are, respectively, given by

\[
 \text{SINR}_d^{\text{multi}} = \frac{\gamma_s}{\alpha|h_{pd}|^2 |y_p|^2 + 1} |w^T H_d|^2, \quad (19)
\]

375 and

\[
 \text{SINR}_e^{\text{multi}} = \frac{\gamma_s}{\alpha|h_{pe}|^2 |y_p|^2 + 1} |w^T H_e|^2. \quad (20)
\]

In this work, the weight vector \(w\) is optimized by maximizing
376 the SINR at SD, yielding

\[
 \max_w \text{SINR}_d^{\text{multi}}, \quad \text{s.t.} \ ||w|| = 1, \quad (21)
\]

377 where the constraint is used for normalization purposes. Using
378 the Cauchy-Schwarz inequality [32], we can readily obtain the
379 optimal weight vector \(w_{\text{opt}}\) from (21) as

\[
 w_{\text{opt}} = \frac{H_d^*}{|H_d|^2}, \quad (22)
\]

380 which indicates that the optimal vector design only requires the
381 SR-SD CSI \(H_d\), whilst dispensing with the eavesdropper’s CSI
382 \(H_e\). Substituting the optimal vector \(w_{\text{opt}}\) from (22) into (19) and (23)
383 and using Shannon’s capacity formula, we can obtain the
384 channel capacities achieved at both SD and E as

\[
 C_d^{\text{multi}} = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_s}{\alpha \gamma_s |h_{pd}|^2 + 1} \sum_{i \in D_h} |h_{id}|^2 \right), \quad (23)
\]

386 and

\[
 C_e^{\text{multi}} = \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_s}{\alpha \gamma_s |h_{pe}|^2 + 1} \frac{|H_d^H H_e|}{|H_d|^2} \right), \quad (24)
\]

385 for \(D = D_h\), where \(H^*\) represents the Hermitian transpose. One
387 can observe from (14) and (23) that the difference between the
388 capacity expressions \(C_d\) and \(C_d^{\text{multi}}\) only lies in the fact that 389
390 the maximum of RVs \(|h_{id}|^2\) for different SRs (i.e., \(\max_{i \in D_h} |h_{id}|^2\))
391 is used for the SRS scheme, while the sum of RVs \(|h_{id}|^2\) (i.e., \(\sum_{i \in D_h} |h_{id}|^2\))
392 is employed for the MRS scheme. Clearly, if we have \(\sum_{i \in D_h} |h_{id}|^2 > \max_{i \in D_h} |h_{id}|^2\), resulting in a performance
393 gain for MRS over SRS in terms of maximizing the legitimate 394
395 transmission capacity. Moreover, since the main channel \(H_d\)
396 and the wiretap channel \(H_e\) are independent of each other, the 397
398 optimal weights assigned for the multiple relays based on \(H_d\)
399 will only slightly affect the eavesdropper’s channel capacity. 399
400 This means that the MRS and SRS schemes achieve more or 401
402 less the same performance in terms of the capacity of the wire- 403
404 tap channel. Nevertheless, given a fixed outage requirement, the 405
406 MRS scheme can achieve a better intercept performance than 407
408 the SRS scheme, because according to the SRT, an outage 409
410 reduction achieved by the capacity enhancement of the legiti- 411
412 mate transmission relying on the MRS would be converted into an 413
414 intercept improvement. To be specific, given an enhanced 415
416 capacity of the legitimate transmission, we may increase the 417
418 data rate \(R\) based on the OP definition of (25) for maintaining 419
420 a fixed OP, which, in turn leads to a reduction of the IP, since a 421
422 higher data rate would result in a lower IP, according to the IP 423
424 definition of (26).

425 It needs to be pointed out that in the MRS scheme, a 426
427 high-complexity symbol-level synchronization is required for 428
429 multiple distributed SRs, when simultaneously transmitting to 430
431 SD, whereas the SRS does not require such a complex synchro- 432
433 nization process. Thus, the performance improvement of MRS 434
435 over SRS is achieved at the cost of a higher implementation 436
complexity. Additionally, the synchronization imperfections of the MRS scheme will impose a performance degradation, which may even lead to a performance for the MRS scheme becoming worse than that of the SRS scheme.

Throughout this paper, the Rayleigh model is used for characterizing the fading amplitudes (e.g., $|h|_{\text{sd}}$, $|h|_{\text{si}}$, $|h|_{\text{sd}}$, etc.) of wireless channels, which, in turn, implies that the fading square magnitudes $|h|_{\text{sd}}^2$, $|h|_{\text{si}}^2$ and $|h|_{\text{sd}}^2$ are exponentially distributed random variables (RVs). So far, we have completed the presentation of the signal model of the direct transmission, of the SRS, and of the MRS schemes for CR networks applications in the presence of eavesdropping attacks.

III. SRT ANALYSIS OVER RAYLEIGH FADING CHANNELS

This section presents the SRT analysis of the direct transmission, SRS and MRS schemes over Rayleigh fading channels. As discussed in [31], the security and reliability are quantified in terms of the IP and OP experienced by the eavesdropper and destination, respectively. It is pointed out that in CR networks, as discussed in [31], the security and reliability are quantified in terms of the IP and OP experienced by the eavesdropper and destination, respectively. It is pointed out that in CR networks, ST starts to transmit its signal only when an available spectrum hole is detected. Similarly to [34], the OP and IP are thus calculated under the condition that the licensed spectrum is detected to be unoccupied by the PBS. The following gives the definition of OP and IP.

Definition 1: Let $C_d$ and $C_e$ represent the channel capacities achieved at the destination and eavesdropper, respectively. The OP and IP are, respectively, defined as

$$P_{\text{out}} = \Pr(C_d < R|\hat{H} = H_0),$$

and

$$P_{\text{int}} = \Pr(C_e > R|\hat{H} = H_0),$$

where $R$ is the data rate.

A. Direct Transmission

Let us first analyze the SRT performance of the conventional direct transmission. Given that a spectrum hole has been detected, the OP of direct transmission is obtained from (25) as

$$P_{\text{out}}^{\text{direct}} = \Pr(C_{\text{sd}} < R|\hat{H} = H_0),$$

where $C_{\text{sd}}$ is given by (4). Using the law of total probability, we can rewrite (27) as

$$P_{\text{out}}^{\text{direct}} = \Pr(C_{\text{sd}} < R|H_0, \hat{H} = H_0) + \Pr(C_{\text{sd}} < R, H_1|\hat{H} = H_0),$$

which can be further expressed as

$$P_{\text{out}}^{\text{direct}} = \Pr(C_{\text{sd}} < R|H_0, \hat{H} = H_0) \Pr(H_0|\hat{H} = H_0) + \Pr(C_{\text{sd}} < R|H_1, \hat{H} = H_0) \Pr(H_1|\hat{H} = H_0).$$

It is shown from (2) that given $H_0$ and $H_1$, the parameter $\alpha$ is obtained as $\alpha = 0$ and $\alpha = 1$, respectively. Thus, combining (2) and (4), we have $C_{\text{sd}} = \log_2(1 + |h_{\text{sd}}|^2)$ given $H_0$ and $C_{\text{sd}} = 4 \log_2(1 + \frac{|h_{\text{sd}}|^2}{|h_{\text{sd}}|^2 + 1})$ given $H_1$. Substituting this result into (29) yields

$$P_{\text{out}}^{\text{direct}} = \Pr(|h_{\text{sd}}|^2 < 2R - 1) \Pr(H_0|\hat{H} = H_0) + \Pr \left(\frac{|h_{\text{sd}}|^2}{|h_{\text{sd}}|^2 + 1} < 2^R - 1 \right) \Pr(H_1|\hat{H} = H_0).$$

Moreover, the terms $\Pr(H_0|\hat{H} = H_0)$ and $\Pr(H_1|\hat{H} = H_0)$ can be obtained by using Bayes’ theorem as

$$P_{\text{out}}^{\text{direct}} = \frac{\Pr(H_0) \Pr(H_0|\hat{H} = H_0)}{\sum_{\theta \in \{0, 1\}} \Pr(H_\theta) \Pr(H_\theta|\hat{H} = H_0)} \Delta \pi_0,$$

and

$$P_{\text{out}}^{\text{direct}} = \frac{\Pr(H_1) \Pr(H_1|\hat{H} = H_0)}{\sum_{\theta \in \{0, 1\}} \Pr(H_\theta) \Pr(H_\theta|\hat{H} = H_0)} \Delta \pi_1,$$

where $\Pr(H_0) = \Pr(H_0)$ is the probability that the licensed spectrum is unoccupied by PBS, while $\Pr(H_1) = \Pr(H_1|H_1)$ are the SDP and FAP, respectively.

For notational convenience, we introduce the shorthand $\pi_0 = 464 \Pr(H_0|\hat{H} = H_0), \pi_1 = \Pr(H_1|\hat{H} = H_0)$ and $\Delta = 2^R - 1$. Then, 465 using (31) and (32), we rewrite (30) as

$$P_{\text{out}}^{\text{direct}} = \pi_0 \Pr(|h_{\text{sd}}|^2 < \Delta) + \pi_1 \Pr(|h_{\text{sd}}|^2 - |h_{\text{sd}}|^2 \gamma_{\text{sd}} \Delta < \Delta).$$

Noting that $|h_{\text{sd}}|^2$ and $|h_{\text{sd}}|^2$ are independently and exponentially distributed RVs with respective means of $\sigma_{\text{sd}}^2$ and $\sigma_{\text{sd}}^2$, we obtain

$$\Pr(|h_{\text{sd}}|^2 < \Delta) = 1 - \exp \left(\frac{\Delta}{\sigma_{\text{sd}}^2}\right),$$

and

$$\Pr(|h_{\text{sd}}|^2 - |h_{\text{sd}}|^2 \gamma_{\text{sd}} \Delta < \Delta) = 1 - \frac{\sigma_{\text{sd}}^2}{\sigma_{\text{sd}}^2} \exp \left(\frac{\Delta}{\sigma_{\text{sd}}^2}\right).$$

Additionally, we observe from (26) that an intercept event 471 occurs, when the capacity of the ST-E channel becomes higher than the data rate. Thus, given that a spectrum hole has been detected (i.e. $\hat{H} = H_0$), ST starts transmitting its signal to SD and 474 E may overhear the ST-SD transmission. The corresponding IP 475 is given by

$$P_{\text{int}}^{\text{direct}} = \Pr(C_{\text{se}} > R|\hat{H} = H_0),$$

which can be further expressed as

$$P_{\text{int}}^{\text{direct}} = \Pr(C_{\text{se}} > R|\hat{H} = H_0, H_0) \Pr(H_0|\hat{H} = H_0) + \Pr(C_{\text{se}} > R|\hat{H} = H_0, H_1) \Pr(H_1|\hat{H} = H_0)$$

$$= \pi_0 \Pr(|h_{\text{se}}|^2 > \Delta) + \pi_1 \Pr(|h_{\text{se}}|^2 - |h_{\text{se}}|^2 \gamma_{\text{se}} \Delta > \Delta).$$
where the second equality is obtained by using $C_{se}$ from (5).

Noting that RVs $|h_{se}|^2$ and $|h_{pe}|^2$ are exponentially distributed and independent of each other, we can express the terms $\Pr(|h_{se}|^2 > \Delta)$ and $\Pr(|h_{pe}|^2 - |h_{pe}|^2 \gamma_p \Delta > \Delta)$ as

$$\Pr(|h_{se}|^2 > \Delta) = \exp\left(-\frac{\Delta}{\sigma_{se}^2}\right),$$

(38)

and

$$\Pr(|h_{se}|^2 - |h_{pe}|^2 \gamma_p \Delta > \Delta) = \frac{\sigma_{se}^2}{\sigma_{pe}^2 \gamma_p \Delta + \sigma_{se}^2} \exp\left(-\frac{\Delta}{\sigma_{se}^2}\right),$$

(39)

where $\sigma_{se}^2$ and $\sigma_{pe}^2$ are the expected values of RVs $|h_{se}|^2$ and $|h_{pe}|^2$, respectively.

**B. Single-Relay Selection**

In this subsection, we present the SRT analysis of the proposed SRS scheme. Given $\hat{H} = H_0$, the OP of the cognitive transmission relying on SRS is given by

$$p_{out}^{\text{single}} = \Pr(C_{bd} < R, D = \emptyset | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N} \Pr(C_{bd} < R, D = D_n | \hat{H} = H_0),$$

(40)

where $C_{bd}$ represents the capacity of the channel from the “best” SR to SD. In the case of $D = \emptyset$, no SR is chosen to forward the source signal, which leads to $C_{bd} = 0$ for $D = \emptyset$.

Substituting this result into (40) gives

$$p_{out}^{\text{single}} = \Pr(D = \emptyset | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N} \Pr(C_{bd} < R, D = D_n | \hat{H} = H_0),$$

(41)

Using (2), (9), (10), and (14), we can rewrite (41) as (42), shown at the bottom of the page, where $\Lambda = \frac{\sigma_{se}^2}{\gamma_p \sigma_{pe}^2}$. Noting that $|h_{sd}|^2$ and $|h_{ps}|^2$ are independent exponentially distributed random variables with respective means of $\sigma_{sd}^2$ and $\sigma_{ps}^2$, we have

$$\Pr(|h_{sd}|^2 < \Lambda) = 1 - \exp\left(-\frac{\Lambda}{\sigma_{sd}^2}\right),$$

(43)

and

$$\Pr(|h_{ps}|^2 < \Lambda | h_{sd}|^2 \gamma_p + \Lambda) = 1 - \frac{\sigma_{sd}^2}{\sigma_{ps}^2 \gamma_p \Lambda + \sigma_{sd}^2} \exp\left(-\frac{\Lambda}{\sigma_{sd}^2}\right),$$

(44)

where the terms $\Pr(|h_{sd}|^2 > \Lambda)$, $\Pr(|h_{sd}|^2 < \Lambda)$, and $\Pr(|h_{ps}|^2 < \Lambda | h_{sd}|^2 \gamma_p + \Lambda)$ can be similarly determined in closed-form.

Moreover, based on Appendix A, we obtain $\Pr(\max_{i \in D_n} |h_{id}|^2 < \Lambda)$

and

$$\Pr(\max_{i \in D_n} |h_{id}|^2 < \Lambda | h_{pd}|^2 \gamma_p + \Lambda)$$

as

$$\Pr(\max_{i \in D_n} |h_{id}|^2 < \Lambda) = \prod_{i \in D_n} \left[1 - \exp\left(-\frac{\Lambda}{\sigma_{id}^2}\right)\right],$$

(45)

and

$$\Pr(\max_{i \in D_n} |h_{id}|^2 < \Lambda | h_{pd}|^2 \gamma_p + \Lambda)$$

as

$$\Pr(\max_{i \in D_n} |h_{id}|^2 < \Lambda) = \prod_{i \in D_n} \left[1 - \exp\left(-\frac{\Lambda}{\sigma_{id}^2}\right)\right],$$

(46)

where $D_n(m)$ represents the $m$-th non-empty subset of $D_n$. Additionally, the OP of the SRS scheme can be expressed as

$$p_{out}^{\text{single}} = \Pr(C_{bd} > R, D = \emptyset | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N} \Pr(C_{bd} > R, D = D_n | \hat{H} = H_0),$$

(47)

where $C_{bd}$ represents the capacity of the channel spanning from the “best” SR to E. Given $D = \emptyset$, we have $C_{bd} = 0$, since no relay is chosen for forwarding the source signal. Thus,
508 substituting this result into (47) and using (2), (9), (10), and 509 (16), we arrive at

\[ P_{\text{int}}^{\text{single}} = \pi_0 \sum_{n=1}^{2^{N-1}} \prod_{i \in \mathcal{D}_h} \text{Pr}(|h_{si}|^2 > \Lambda) \prod_{j \in \mathcal{D}_h} \text{Pr}(|h_{sj}|^2 < \Lambda) \times \text{Pr}(|h_{be}|^2 > \Lambda) + \pi_1 \sum_{n=1}^{2^{N-1}} \prod_{i \in \mathcal{D}_h} \text{Pr}(|h_{si}|^2 > \Lambda|h_{pi}|^2\gamma_p + \Lambda) \times \prod_{j \in \mathcal{D}_h} \text{Pr}(|h_{sj}|^2 < \Lambda|h_{pj}|^2\gamma_p + \Lambda) \times \text{Pr}(|h_{be}|^2 > \Lambda|h_{pe}|^2\gamma_p + \Lambda), \]  

510 where the closed-form expressions of \( \text{Pr}(|h_{si}|^2 > \Lambda) \) and 511 \( \text{Pr}(|h_{si}|^2 > \Lambda|h_{pi}|^2\gamma_p + \Lambda) \) can be readily obtained by using 512 (43) and (44). Using the results in Appendix B, we can express 513 \( \text{Pr}(|h_{be}|^2 > \Lambda) \) and \( \text{Pr}(|h_{be}|^2 > \Lambda|h_{pe}|^2\gamma_p + \Lambda) \) as

\[ \text{Pr}(|h_{be}|^2 > \Lambda) = \sum_{i \in \mathcal{D}_b} \exp\left(-\frac{\Lambda}{\sigma^2_e}\right) \times \left[ 1 + \sum_{m=1}^{2^{N-1}} (-1)^{C_m(i)} \left( 1 + \sum_{j \in C_n(m)} \frac{\sigma^2_d}{\sigma^2_{id}} \right)^{-1} \right], \]  

514 and

\[ \text{Pr}(|h_{be}|^2 > \Lambda|h_{pe}|^2\gamma_p + \Lambda) = \sum_{i \in \mathcal{D}_b} \frac{\sigma^2_e}{\sigma^2_{pe}\gamma_p\Lambda + \sigma^2_e} \exp\left(-\frac{\Lambda}{\sigma^2_e}\right) \times \left[ 1 + \sum_{m=1}^{2^{N-1}} (-1)^{C_m(m)} \left( 1 + \sum_{j \in C_n(m)} \frac{\sigma^2_d}{\sigma^2_{id}} \right)^{-1} \right], \]  

515 where \( C_m(m) \) represents the \( m \)-th non-empty subset of \( \mathcal{D}_b \) \( \{-i\} \) and ‘\(-\’ represents the set difference.

517 C. Multi-Relay Selection

518 This subsection analyzes the SRT of our MRS scheme for 519 transmission over Rayleigh fading channels. Similarly to (41), 520 the OP in this case is given by

\[ P_{\text{out}}^{\text{multi}} = \text{Pr}(\mathcal{D} = \emptyset|\hat{H} = H_0) + \sum_{n=1}^{2^{N-1}} \text{Pr}(\sum_{i \in \mathcal{D}_h} |h_{si}|^2 < \gamma_p\Lambda|h_{pe}|^2 + \Lambda). \]  

Using (2), (9), (10) and (23), we can rewrite (51) as (52), shown 551 at the bottom of the page, where the closed-form expressions 552 of \( \text{Pr}(|h_{si}|^2 < \Lambda) \), \( \text{Pr}(|h_{si}|^2 < \Lambda|h_{pi}|^2\gamma_p + \Lambda) \), \( \text{Pr}(|h_{si}|^2 < \Lambda) \), 553 \( \text{Pr}(|h_{si}|^2 < \Lambda|h_{pi}|^2\gamma_p + \Lambda) \), \( \text{Pr}(|h_{si}|^2 < \Lambda|h_{pi}|^2\gamma_p + \Lambda) \) can be readily 554 derived, as shown in (43) and (44). However, it is challenging 555 to obtain the closed-form expressions of \( \text{Pr}(\sum_{i \in \mathcal{D}_h} |h_{si}|^2 < \Lambda) \) and 556 \( \text{Pr}(\sum_{i \in \mathcal{D}_h} |h_{si}|^2 < \gamma_p\Lambda|h_{pe}|^2 + \Lambda) \). For simplicity, we assume that 557 the fading coefficients of all SRs-SD channels, i.e. \( |h_{id}|^2 \) for 558 \( i \in \{1, 2, \ldots, N\} \), are i.i.d. RVs having the same mean (average channel gain) denoted by \( \sigma^2_d \). This assumption is 559 widely used in the cooperative relaying literature and it is 560 valid in a statistical sense, provided that all SRs are uniformly 561 distributed over a certain geographical area. Assuming that 552 RVs of \( |h_{id}|^2 \) for \( i \in \mathcal{D}_b \) are i.i.d., based on Appendix C, we 562 arrive at

\[ \text{Pr}\left(\sum_{i \in \mathcal{D}_b} |h_{id}|^2 < \gamma_p\Lambda|h_{pe}|^2 + \Lambda\right) = \Gamma\left(\frac{\Lambda}{\sigma^2_d}, |\mathcal{D}_b|\right), \]  

and

\[ \text{Pr}\left(\sum_{i \in \mathcal{D}_b} |h_{id}|^2 < \gamma_p\Lambda|h_{pe}|^2 + \Lambda\right) = \Gamma\left(\frac{\Lambda}{\sigma^2_d}, |\mathcal{D}_b|\right) \times \left[ 1 - \Gamma\left(\frac{\Lambda\sigma^2_d + \sigma^2_{pe}\gamma_p\Lambda}{\sigma^2_{pe}\gamma_p\Lambda - \sigma^2_d}, |\mathcal{D}_b|\right) \right] e^{-\frac{1}{\sigma^2_{pe}\gamma_p\Lambda} |\mathcal{D}_b| \sum_{i \in \mathcal{D}_b} |h_{id}|^2}, \]  

where \( \Gamma(x,k) = \int_0^k e^{-t} \frac{1}{\Gamma(x)} \, dt \) is known as the incomplete 553 Gamma function [32]. Substituting (53) and (54) into (52) yields 554 a closed-form OP expression for the proposed MRS scheme.
Next, we present the IP analysis of the MRS scheme. Similarly to (48), the IP of the MRS can be obtained from (24) as

\[
P_{\text{IP, MRS}} = \tau_0 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \Pr(h_{si}^2 > \Lambda) \prod_{j \in D_n} \Pr(h_{sj}^2 < \Lambda) \\
\times \Pr \left( \frac{|H_d^H H_e|^2}{|H_d|^2} > \Lambda \right) \\
+ \tau_1 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \Pr(h_{si}^2 > \Lambda | h_{pi}^2 > \gamma_p + \Lambda) \\
\times \prod_{j \in D_n} \Pr(h_{sj}^2 < \Lambda | h_{pj}^2 > \gamma_p + \Lambda) \\
\times \Pr \left( \frac{|H_d^H H_e|^2}{|H_d|^2} > \gamma_p \Lambda | h_{pe}^2 > \Lambda \right), \quad (55)
\]

where the closed-form expressions of \( \Pr(h_{si}^2 > \Lambda) \), \( \Pr(h_{sj}^2 < \Lambda) \), \( \Pr(h_{si}^2 > \Lambda | h_{pi}^2 > \gamma_p + \Lambda) \) and \( \Pr(h_{sj}^2 < \Lambda | h_{pj}^2 > \gamma_p + \Lambda) \) may be readily derived by using (43) and (44).

However, it is challenging to obtain the closed-form solutions for \( \Pr \left( \frac{|H_d^H H_e|^2}{|H_d|^2} > \Lambda \right) \) and \( \Pr \left( \frac{|H_d^H H_e|^2}{|H_d|^2} > \gamma_p \Lambda | h_{pe}^2 > \Lambda \right) \).

Although finding a general closed-form IP expression for the MRS scheme is challenging, we can obtain the numerical IP results with the aid of computer simulations.

### IV. Numerical Results and Discussions

In this section, we present our performance comparisons among the direct transmission, the SRS and MRS schemes in terms of their SRT. To be specific, the analytic IP versus OP of the three schemes are obtained by plotting (33), (37), (46), (48), (52), and (55). The simulated IP and OP results of the three schemes are also given to verify the correctness of the theoretical SRT analysis. In our computer simulations, the fading amplitudes (e.g., \( |h_{ui}|, |h_{sj}|, |h_{sj}|, \text{etc.} \)) are first generated based on the Rayleigh distribution having different variances for different channels. Then, the randomly generated fading amplitudes are substituted into the definition of an outage (or intercept) event, which would determine whether an outage (or intercept) event occurs or not. By repeatedly achieving this process, we can calculate the relative frequency of occurrence for an outage (intercept) event, which is the simulated OP (or IP).

Additionally, the SDP, and FAP are set to \( P_d = 0.99 \) and \( P_f = 0.01 \), unless otherwise stated. The primary signal-to-noise ratio (SNR) of \( \gamma_p = 10 \text{ dB} \) and the data rate of \( R = 1 \text{ bit/s/Hz} \) are used in our numerical evaluations.

The artificial noise based method [35], [36] is also considered for the purpose of numerical comparison with the relay selection schemes. To be specific, in the artificial noise based scheme, ST directly transmits its signal \( x_s \) to SD, while both SRS and MRS attempt to confuse the eavesdropper by sending an interfering signal (referred to as artificial noise) that is approximately designed to lie in the null-space of the legitimate main channel. In this way, the artificial noise will impose interference on the 79 eavesdropper without affecting the SD. For a fair comparison, the total transmit power of the desired signal \( x_s \) and the artificial noise are constrained to \( P_s \). Moreover, the equal power allocation method [35] is used in the numerical evaluation.
Fig. 4. IP versus OP of the SRS and MRS schemes for different $P_t$ with $\gamma_i \in [0, 30 \text{ dB}]$, $N = 6$, $\sigma_{sd} = \sigma_{si} = \sigma_{sd} = 1$, $\sigma_{se} = \sigma_{se} = 0.1$, and $\sigma_{pd} = \sigma_{pd} = \sigma_{pd} = 0.2$.

Fig. 5. IP versus OP of the SRS and the MRS schemes for different $(P_d, P_f)$ with $P_t = 0.8$, $\gamma_i \in [0, 30 \text{ dB}]$, $N = 6$, $\sigma_{sd}^2 = \sigma_{si}^2 = \sigma_{sd}^2 = 1$, $\sigma_{se}^2 = \sigma_{se}^2 = 0.1$, and $\sigma_{pd}^2 = \sigma_{pd}^2 = \sigma_{pd}^2 = 0.2$.

In Fig. 5, we depict the IP versus OP of the SRS and MRS schemes for different spectrum sensing reliabilities, where $(P_d, P_f) = (0.9, 0.1)$ and $(P_d, P_f) = (0.99, 0.01)$ are considered. It is observed that as the spectrum sensing reliability is improved from $(P_d, P_f) = (0.9, 0.1)$ to $(P_d, P_f) = (0.99, 0.01)$, the SRTs of the SRS and MRS schemes improve accordingly. This is due to the fact that for an improved sensing reliability, an unoccupied licensed band would be detected more accurately and hence less mutual interference occurs between the PUs and SUs, which results in a better SRT for the secondary transmissions. Fig. 5 also shows that for $(P_d, P_f) = (0.9, 0.1)$ and $(P_d, P_f) = (0.99, 0.01)$, the MRS approach outperforms the SRS scheme in terms of the SRT, which further confirms the advantage of the MRS for protecting the secondary transmissions against eavesdropping attacks.

Fig. 6 shows the IP versus OP of the conventional direct transmission as well as of the proposed SRS and MRS schemes for $N = 2$, $N = 4$, and $N = 8$. It is seen from Fig. 6 that the SRTs of the proposed SRS and MRS schemes are generally better than that of the conventional direct transmission for $N = 2$, $N = 4$ and $N = 8$. Moreover, as the number of SRs increases from $N = 2$ to $8$, the SRT of the SRS and MRS schemes significantly improves, explicitly demonstrating the security and reliability benefits of exploiting multiple SRs for assisting the secondary transmissions. In other words, the security and reliability of the secondary transmissions can be concurrently improved by increasing the number of SRs. Additionally, as shown in Fig. 6, upon increasing the number of SRs from $N = 2$ to $8$, the SRT improvement of MRS over SRS becomes more notable. Again, the SRT advantage of the MRS over the SRS comes at the expense of requiring elaborate symbol-level synchronization among the multiple SRs for simultaneously transmitting to the SD.

V. CONCLUSION

In this paper, we proposed relay selection schemes for a CR network consisting of a ST, a SD and multiple SRs communicating in the presence of an eavesdropper. We examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and reliability of secondary transmissions are characterized in terms of their IP and OP, respectively. We also analyzed the SRT of the conventional direct transmission as a benchmark. It was illustrated that as the spectrum sensing reliability increases, the SRTs of both the SRS and MRS schemes improve. We also showed that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRT. Moreover, the SRT performance of MRS is better than that of SRS. Additionally, as the number of SRs increases, the SRTs of both the SRS and of the MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and reliability of secondary transmissions.
APPENDIX A

DERIVATION OF (45) AND (46)

Letting \(|h_{id}|^2 = x_i\) and \(|h_{pd}|^2 = y\), the left hand side of (45) and (46) can be rewritten as \(\Pr \left(\max_{i \in D_h} x_i < \Lambda \right)\) and \(\Pr \left(\max_{i \in D_h} x_i < \Lambda, \left|h_{pd}\right|^2\right)\), respectively. Noting that random variables \(|h_{id}|^2\) and \(|h_{pd}|^2\) are exponentially distributed with respective means \(\sigma_{id}^2\) and \(\sigma_{pd}^2\), and independent of each other, we obtain

\[
\Pr \left(\max_{i \in D_h} x_i < \Lambda \right) = \prod_{i \in D_h} \Pr \left(\left|h_{id}\right|^2 < \Lambda \right)
\]

\[
= \prod_{i \in D_h} \left[1 - \exp \left(\frac{-\Lambda}{\sigma_{id}^2} \right)\right], \quad (A.1)
\]

which is (45). Similarly, the term \(\Pr \left(\max_{i \in D_h} x_i < \Lambda, \left|h_{pd}\right|^2\right)\) can be computed as

\[
\Pr \left(\max_{i \in D_h} x_i < \Lambda, \left|h_{pd}\right|^2\right) = \int_0^\infty \frac{1}{\sigma_{pd}^2} \exp \left(\frac{-y}{\sigma_{pd}^2} \right) \prod_{i \in D_h} \left(1 - \exp \left(\frac{-\Lambda y + \Lambda}{\sigma_{id}^2} \right)\right) dy,
\]

(A.2)

wherein

\[
\prod_{i \in D_h} \left(1 - \exp \left(\frac{-\Lambda y + \Lambda}{\sigma_{id}^2} \right)\right) = 1 + \sum_{m=1}^{2^{|D_h|-1}} \left(-1\right)^m \left|h_{pd}(m)\right| \exp \left(-\sum_{i \in D_h(m)} \frac{\Lambda y + \Lambda}{\sigma_{id}^2}\right),
\]

(A.3)

where \(|D_h|\) is the cardinality of set \(D_h\), \(\tilde{D}_h(m)\) represents the \(m\)-th non-empty subset of \(D_h\), and \(|\tilde{D}_h(m)|\) is the cardinality of set \(\tilde{D}_h(m)\). Substituting \(\prod_{i \in D_h} \left(1 - \exp \left(\frac{-\Lambda y + \Lambda}{\sigma_{id}^2} \right)\right)\) from (A.3) into (A.2) yields

\[
\Pr \left(\max_{i \in D_h} x_i < \Lambda, \left|h_{pd}\right|^2\right) = \int_0^\infty \frac{1}{\sigma_{pd}^2} \exp \left(\frac{-y}{\sigma_{pd}^2} \right) dy
\]

\[
+ \sum_{m=1}^{2^{|D_h|-1}} \left(-1\right)^m \left|h_{pd}(m)\right| \frac{1}{\sigma_{pd}^2}
\]

\[
\times \int_0^\infty \exp \left(-\frac{y}{\sigma_{pd}^2} - \sum_{i \in D_h(m)} \frac{\Lambda y + \Lambda}{\sigma_{id}^2}\right) dy.
\]

(A.4)

Finally, performing the integration of (A.4) yields

\[
\Pr \left(\max_{i \in D_h} x_i < \Lambda, \left|h_{pd}\right|^2\right) = 1
\]

\[
+ \sum_{m=1}^{2^{|D_h|-1}} \left(-1\right)^m \left|h_{pd}(m)\right| \frac{1}{\sigma_{pd}^2}
\]

\[
\times \left(1 + \sum_{i \in \tilde{D}_h(m)} \frac{\Lambda y + \Lambda}{\sigma_{id}^2}\right)^{-1}.
\]

(A.5)

This completes the proof of (45) and (46).

APPENDIX B

PROOF OF (49) AND (50)

Given \(D = D_h\), any SR within \(D_h\) can be selected as the best relay for forwarding the source signal. Thus, using the 695 law of total probability, we have

\[
\Pr \left(|h_{se}|^2 > \Lambda\right) = \sum_{i \in D_h} \Pr \left(|h_{se}|^2 > \Lambda, b = i\right)
\]

\[
= \sum_{i \in D_h} \Pr \left(|h_{se}|^2 > \Lambda, |h_{pd}|^2 > \max_{j \in D_h-i} \left|h_{pd}(j)\right|^2\right)
\]

\[
= \sum_{i \in D_h} \Pr \left(|h_{se}|^2 > \Lambda\right) \Pr \left(\max_{j \in D_h-i} \left|h_{pd}(j)\right|^2 < |h_{pd}|^2\right),
\]

(B.1)

where in the first line, variable \(b\) stands for the best SR and the second equality is obtained from (13) and \(\cdot\cdot\cdot\) represents the set difference. Noting that \(|h_{se}|^2\) is an exponentially distributed random variable with a mean of \(\sigma_{se}^2\), we obtain

\[
\Pr \left(|h_{se}|^2 > \Lambda\right) = \exp \left(-\frac{\Lambda}{\sigma_{se}^2}\right).
\]

(B.2)

Letting \(|h_{pd}|^2 = x_j\) and \(|h_{id}|^2 = y\), we have

\[
\Pr \left(\max_{j \in D_h-i} \left|h_{pd}\right|^2 < |h_{id}|^2\right) = \int_0^\infty \frac{1}{\sigma_{id}^2} \exp \left(-\frac{y}{\sigma_{id}^2} \right) \prod_{j \in D_h-i} \left(1 - \exp \left(-\frac{y}{\sigma_{jd}}\right)\right) dy,
\]

(B.3)

wherein

\[
\prod_{j \in D_h-i} \left(1 - \exp \left(-\frac{y}{\sigma_{jd}}\right)\right) = 1
\]

\[
+ \sum_{m=1}^{2^{|D_h|-1}} \left(-1\right)^m \left|C_n(m)\right| \exp \left(-\sum_{j \in C_n(m)} \frac{y}{\sigma_{jd}}\right),
\]

(B.4)

where \(|D_h|\) denotes the cardinality of the set \(D_h\) and \(C_n(m)\) represents the \(m\)-th non-empty subset of \(\{D_h - \{i\}\}\)). Combining (B.3) and (B.4), we obtain

\[
\Pr \left(\max_{j \in D_h-i} \left|h_{pd}\right|^2 < |h_{id}|^2\right) = 1
\]

\[
+ \sum_{m=1}^{2^{|D_h|-1}} \left(-1\right)^m \left|C_n(m)\right| \left(1 + \sum_{j \in C_n(m)} \frac{\sigma_{jd}^2}{\sigma_{jd}^2}\right)^{-1}.
\]

(B.5)
Substituting (B.2) and (B.5) into (B.1) gives (B.6), shown at the bottom of the page, which is (49). Similarly to (B.1), we can rewrite \( \Pr(|h_{pe}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) \) as

\[
\Pr(|h_{pe}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \sum_{i \in \mathcal{D}_h} \Pr(|h_{ie}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) 
\times \Pr \left( \max_{j \in \{2k-i\}} |h_{jd}|^2 < |h_{id}|^2 \right), \tag{B.7}
\]

Since the random variables \(|h_{ic}|^2\) and \(|h_{pe}|^2\) are independently and exponentially distributed with respective means of \(\sigma_{ie}^2\) and \(\sigma_{pe}^2\), we readily arrive at

\[
\Pr(|h_{ie}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \frac{\sigma_{ie}^2}{\sigma_{pe}^2 \gamma_p \Lambda + \sigma_{ie}^2} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right). \tag{B.8}
\]

Substituting (B.5) and (B.8) into (B.7) gives (B.9), shown at the bottom of the page, which is (50).

**APPENDIX C**

**PROOF OF (53) AND (54)**

Upon introducing the notation of \( X = \sum_{i \in \mathcal{D}_h} |h_{id}|^2 \) and \( Y = \sum_{i \in \mathcal{D}_h} |h_{pe}|^2 \), we can rewrite the terms \( \Pr \left( \sum_{i \in \mathcal{D}_h} |h_{id}|^2 < \Lambda \right) \) and

\[
\Pr \left( \sum_{i \in \mathcal{D}_h} |h_{id}|^2 < \gamma_p \Lambda |h_{pe}|^2 + \Lambda \right) \text{ as } \Pr(X < \Lambda) \text{ and } \Pr(X < \gamma_p \Lambda + \Lambda), \tag{C.1}
\]

respectively. Noting that the fading coefficients of all SR-SD channels, i.e. \(|h_{id}|^2\) for \( i \in \{1,2,\cdots,N\} \), are assumed to be i.i.d., we obtain the probability density function (PDF) of

\[
X = \sum_{i \in \mathcal{D}_h} |h_{id}|^2 \text{ as } f_X(x) = \frac{1}{\Gamma(|\mathcal{D}_h|) \sigma_d^{2|\mathcal{D}_h|}} x^{\frac{2|\mathcal{D}_h| - 1}{2}} e^{-\frac{x}{\sigma_d^2}}, \tag{C.1}
\]

where \( \sigma_d^2 = E(|h_{id}|^2) \). Meanwhile, the random variable \( Y = \sum_{i \in \mathcal{D}_h} |h_{pe}|^2 \) is exponentially distributed and its PDF is given by

\[
f_Y(y) = \frac{1}{\sigma_{pd}^2} \exp \left( -\frac{y}{\sigma_{pd}^2} \right). \tag{C.2}
\]

Substituting (C.1) and (C.2) into (C.3) yields

\[
\Pr(X < \gamma_p \Lambda + \Lambda) = \int_0^\Lambda f_X(x)dx 
+ \int_\Lambda^\infty \int_{-\frac{a}{\gamma_p \Lambda}}^{\frac{y}{\gamma_p \Lambda}} f_X(x)f_Y(y)dxdy. \tag{C.4}
\]

where the second equality is obtained by substituting \( \frac{a}{\gamma_p \Lambda} = t \) and

\[
\Gamma(a,k) = \int_0^t \frac{1}{t^{-1}} \exp(-t)dt \text{ is known as the incomplete Gamma function. Additionally, considering that the random variables } X \text{ and } Y \text{ are independent of each other, we obtain } \Pr(X < \gamma_p \Lambda + \Lambda) \text{ as }
\]

\[
\Pr(X < \gamma_p \Lambda + \Lambda) = \int_0^\Lambda f_X(x)dx 
+ \int_\Lambda^\infty \int_{-\frac{a}{\gamma_p \Lambda}}^{\frac{y}{\gamma_p \Lambda}} f_X(x)f_Y(y)dxdy. \tag{C.4}
\]

Substituting (C.1) and (C.2) into (C.4) yields

\[
\Pr(X < \gamma_p \Lambda + \Lambda)
= \int_0^\Lambda \frac{1}{\Gamma(|\mathcal{D}_h|) \sigma_d^{2|\mathcal{D}_h|}} x^{\frac{2|\mathcal{D}_h| - 1}{2}} e^{-\frac{x}{\sigma_d^2}} - \frac{x}{\sigma_d^2} \gamma_p \Lambda d \frac{x}{\sigma_d^2} \gamma_p \Lambda \tag{C.5}
\]

where the second equality is obtained by using \( \frac{a}{\gamma_p \Lambda} + \frac{x}{\sigma_{pd}^2} = t \). Hence, we have completed the proof of (53) and (54) as (C.3) and (C.5), respectively.

\[
\Pr(|h_{be}|^2 > \Lambda) = \sum_{i \in \mathcal{D}_h} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right) \left[ 1 + \sum_{m=1}^{|\mathcal{D}_h| - 1} (-1)^{|G_{m}(n)|} \left( 1 + \sum_{j \in G_{m}(n)} \frac{\sigma_{id}^2}{\sigma_{jd}^2} \right)^{-1} \right] \tag{B.6}
\]

\[
\Pr(|h_{be}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \sum_{i \in \mathcal{D}_h} \frac{\sigma_{ie}^2}{\sigma_{pe}^2 \gamma_p + \sigma_{ie}^2} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right) \left[ 1 + \sum_{m=1}^{|\mathcal{D}_h| - 1} (-1)^{|G_{m}(n)|} \left( 1 + \sum_{j \in G_{m}(n)} \frac{\sigma_{id}^2}{\sigma_{jd}^2} \right)^{-1} \right] \tag{B.9}
\]
ZOU et al.: RELAY SELECTION IMPROVES THE SECURITY-RELIABILITY TRADE-OFF IN CR SYSTEMS

REFERENCES


Benoit Champagne (S’87–M’89–SM’03) was born in Joliette (PQ), Canada, in 1961. He received the B.Eng. degree in engineering physics and the M.Sc. degree in physics from the University of Montreal in 1983 and 1985, respectively, and the Ph.D. degree in electrical engineering from the University of Toronto in 1990. From 1990 to 1999, he was with INRS, University of Quebec, where he held the positions of Assistant and then Associate Professor. In 1999, he joined McGill University, Montreal, as an Associate Professor with the Department of Electrical and Computer Engineering. He served as Associate Chairman of Graduate Studies in the Department from 2004 to 2007 and is now a Full Professor. His research interests focus on the investigation of new computational algorithms for the digital processing of information bearing signals and overlap many sub-areas of statistical signal processing, including: detection and estimation, sensor array processing, adaptive filtering, multirate systems, and applications thereof to broadband voice and data communications. Over the years, he has supervised many graduate students in these areas and co-authored several papers, including key works on subspace tracking, speech enhancement, time delay estimation and spread sources localization.

Wei-Ping Zhu (SM’97) received the B.E. and M.E. degrees from Nanjing University of Posts and Telecommunications, and the Ph.D. degree from Southeast University, Nanjing, China, in 1982, 1985, and 1991, respectively, all in electrical engineering. He was a Postdoctoral Fellow from 1991 to 1992 and a Research Associate from 1996 to 1998 with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. During 1993–1996, he was an Associate Professor with the Department of Information Engineering, Nanjing University of Posts and Telecommunications. From 1998 to 2001, he worked with hi-tech companies in Ottawa, Canada, including Nortel Networks and SR Telecom Inc. Since July 2001, he has been with Concordia’s Electrical and Computer Engineering Department as a full-time faculty member, where he is presently a Full Professor. His research interests include digital signal processing fundamentals, speech and audio processing, and signal processing for wireless communication with a particular focus on MIMO systems and cooperative relay networks.

Dr. Zhu was an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART I: Fundamental Theory and Applications from 2001 to 2003, and an Associate Editor of Circuits, Systems and Signal Processing from 2006 to 2009. He was also a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue of “Broadband Wireless Communications for High Speed Vehicles, and Virtual MIMO” in 2011–2013. Since 2011, he has served as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART II: Express Briefs. Dr. Zhu was the Secretary of Digital Signal Processing Technical Committee (DSPTC) of the IEEE Circuits and System Society during 2012–2014, where he is presently the Chair of the DSPTC.

Lajos Hanzo received the degree in electronics in 1976 and the doctorate in 1983. In 2009 he was awarded “Doctor Honoris Causa” by the Technical University of Budapest. During his 37-year career in telecommunications he has held various research and academic posts in Hungary, Germany, and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised 80+ Ph.D. students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10,000 pages, published 1,400+ research entries at IEEE Xplore, acted both as TPC and General Chair of 939 IEEE conferences, presented keynote lectures and has been awarded a number 940 of distinctions. Currently he is directing a 100-strong academic research team, working on a range of research projects in the field of wireless multimedia 942 communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Council’s Advanced 944 Fellow Grant and the Royal Society’s Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of 946 industrial courses. He is also a Governor of the IEEE VTS. During 2008–2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also 948 at Tsinghua University, Beijing. His research is funded by the European 949 Research Council’s Senior Research Fellow Grant. For further information on 950 research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk Lajos has 20,000+ citations.
AUTHOR QUERY

NO QUERY.
Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems

Yulong Zou, Senior Member, IEEE, Benoit Champagne, Senior Member, IEEE, Wei-Ping Zhu, Senior Member, IEEE, and Lajos Hanzo, Fellow, IEEE

Abstract—We consider a cognitive radio (CR) network consisting of a secondary transmitter (ST), a secondary destination (SD) and multiple secondary relays (SRs) in the presence of an eavesdropper, where the ST transmits to the SD with the assistance of SRs, while the eavesdropper attempts to intercept the secondary transmission. We rely on careful relay selection for protecting the ST-SD transmission against the eavesdropper with the aid of both single-relay and multi-relay selection. To be specific, only the “best” SR is chosen in the single-relay selection for assisting the secondary transmission, whereas the multi-relay selection invokes multiple SRs for simultaneously forwarding the ST’s transmission to the SD. We analyze both the intercept probability and outage probability of the proposed single-relay and multi-relay selection schemes for the secondary transmission relying on realistic spectrum sensing. We also evaluate the performance of classic direct transmission and artificial noise based methods for the purpose of comparison with the proposed relay selection schemes. It is shown that as the intercept probability requirement is relaxed, the outage performance of the direct transmission, the artificial noise based and the relay selection schemes improves, and vice versa. This implies a trade-off between the security and reliability of the secondary transmission in the presence of eavesdropping attacks, which is referred to as the security-reliability trade-off (SRT). Furthermore, we demonstrate that the SRTs of the single-relay and multi-relay selection schemes are generally better than that of classic direct transmission, explicitly demonstrating the advantage of the proposed relay selection in terms of protecting the secondary transmissions against eavesdropping attacks. Moreover, as the number of SRs increases, the SRTs of the proposed single-relay and multi-relay selection approaches significantly improve. Finally, our numerical results show that as expected, the multi-relay selection scheme achieves a better SRT performance than the single-relay selection.

Index Terms—Security-reliability trade-off, relay selection, intercept probability, outage probability, eavesdropping attack, cognitive radio.

I. INTRODUCTION

THE security aspects of cognitive radio (CR) systems [1]–[3] have attracted increasing attention from the research community. Indeed, due to the highly dynamic nature of the CR network architecture, legitimate CR devices become exposed to both internal as well as to external attackers and hence they are extremely vulnerable to malicious behavior. For example, an illegitimate user may intentionally impose interference (i.e., jamming) for the sake of artificially contaminating the CR environment [4]. Hence, the CR users fail to accurately characterize their surrounding radio environment and may become misled or compromised, which leads to a malfunction. Alternatively, an illegitimate user may attempt to tap the communications of authorized CR users by eavesdropping, to intercept confidential information.

Clearly, CR networks face diverse security threats during both spectrum sensing [5], [6] as well as spectrum sharing [7], spectrum mobility [8] and spectrum management [9]. Extensive studies have been carried out for protecting CR networks against primary user emulation (PUE) [10] and against denial-of-service (DoS) attacks [11]. In addition to PUE and DoS attacks, eavesdropping is another major concern in protecting the data confidentiality [12]; although it has received less attention in the literature on CR network security. Traditionally, cryptographic techniques are employed for guaranteeing transmission confidentiality against an eavesdropping attack. However, this introduces a significant computational overhead [13] as well as imposing additional system complexity in terms of the secret key management [14]. Furthermore, the existing cryptographic approaches are not perfectly secure and can still be decrypted by an eavesdropper (E), provided that it has the capacity to carry out exhaustive key search with the aid of brute-force attack [15].

Physical-layer security [16], [17] is emerging as an efficient approach for defending authorized users against eavesdropping attacks by exploiting the physical characteristics of wireless channels. In [17], Leung-Yan-Cheong and Hellman demonstrated that perfectly secure and reliable transmission can be achieved, when the wiretap channel spanning from the source to the eavesdropper is a further degraded version of the main channel.
channel between the source and destination. They also showed that the maximal secrecy rate achieved at the legitimate destination, which is termed the secrecy capacity, is the difference between the capacity of the main channel and that of the wiretap channel. In [18]–[20], the secrecy capacity limits of wireless fading channels were further developed and characterized from an information-theoretic perspective, demonstrating the detrimental impact of wireless fading on the physical-layer security. To combat the fading effects, both multiple-input multiple-output (MIMO) schemes [21], [22] as well as cooperative relaying [23]–[25] and beamforming techniques [26], [27] were investigated for the sake of enhancing the achievable wireless secrecy capacity. Although extensive research efforts were devoted to improving the security of traditional wireless networks [16]–[27], less attention has been dedicated to CR networks. In [28] and [29], the achievable secrecy rate of the secondary transmission was investigated under a specific quality-of-service (QoS) constraint imposed on the primary transmission. Additionally, an overview of the physical-layer security aspects of CR networks was provided in [30], where several security attacks as well as the related countermeasures are discussed. In contrast to conventional non-cognitive wireless networks, the physical-layer security of CR networks has to consider diverse additional challenges, including the protection of the primary user’s QoS and the mitigation of the mutual interference between the primary and secondary transmissions.

Motivated by the above considerations, we explore the physical-layer security of a CR network comprised of a secondary transmitter (ST) communicating with a secondary destination (SD) with the aid of multiple secondary relays (SRs) in the presence of an unauthorized attacker. Our main focus is on investigating the security-reliability trade-off (SRT) of the cognitive relay transmission in the presence of realistic spectrum sensing. The notion of the SRT in wireless physical-layer security was introduced and examined in [31], where the security and reliability was characterized in terms of the intercept probability and outage probability, respectively. In contrast to the conventional non-cognitive wireless networks studied in [31], the SRT analysis of CR networks presented in this work additionally takes into account the mutual interference between the primary user (PU) and secondary user (SU).

The main contributions of this paper are summarized as follows.

- We propose two relay selection schemes, namely both single-relay and multi-relay selection, for protecting the secondary transmissions against eavesdropping attacks. More specifically, in the single-relay selection (SRS) scheme, only a single relay is chosen from the set of multiple SRs for forwarding the secondary transmissions from the ST to the SD. By contrast, the multi-relay selection (MRS) scheme employs multiple SRs for simultaneously assisting the ST-SD transmissions.
- We present the mathematical SRT analysis of the proposed SRS and MRS schemes in the presence of realistic spectrum sensing. Closed-form expressions are derived for the intercept probability (IP) and outage probability (OP) of both schemes for transmission over Rayleigh fading channels. The numerical SRT results of conventional direct transmission and artificial noise based schemes are also provided for comparison purposes.
- It is shown that as the spectrum sensing reliability is increased and/or the false alarm probability is reduced, the SRTs of both the SRS and MRS schemes are improved. Numerical results demonstrate that the proposed SRS and MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRTs.

The remainder of this paper is organized as follows. Section II presents the system model of physical-layer security in CR networks in the context of both the direct transmission as well as the SRS and MRS schemes. In Section III, we analyze the SRTs of these schemes in the presence of realistic spectrum sensing over Rayleigh fading channels. Next, numerical SRT results of the direct transmission, SRS and MRS schemes are given in Section IV, where the SRT performance of the artificial noise based scheme is also numerically evaluated for comparison purposes. Finally, Section V provides our concluding remarks.

II. RELAY SELECTION AIDED PROTECTION AGAINST EAVESDROPPING IN CR NETWORKS

We first introduce the overall system model of physical-layer security in CR networks. We then present the signal model of the conventional direct transmission approach, which will serve as our benchmarker, as well as of the SRS and MRS schemes for improving the CR system’s security against eavesdropping attacks.

A. System Model

As shown in Fig. 1, we consider a primary network in coexistence with a secondary network (also referred to as a CR network). The primary network includes a primary base station (PBS) and multiple primary users (PUs), which communicate with the PBS over the licensed spectrum. By contrast, the secondary network consisting of one or more STs and SDs exploits the licensed spectrum in an opportunistic way. To investigate the security-reliability trade-off (SRT) of the secondary wireless transmission, the PBS and multiple PUs, which communicate with the PBS over the licensed spectrum. By contrast, the secondary network consisting of one or more STs and SDs exploits the licensed spectrum in an opportunistic way.
be specific, a particular ST should first detect with the aid of spectrum sensing whether or not the licensed spectrum is occupied by the PBS. If so, the ST is not at liberty to transmit to avoid interfering with the PUs. If alternatively, the licensed spectrum is deemed to be unoccupied (i.e. a spectrum hole is detected), then the ST may transmit to the SD over the detected spectrum hole. Meanwhile, E attempts to intercept the secondary transmission from the ST to the SD. For notational convenience, let $H_0$ and $H_1$ represent the event that the licensed spectrum is deemed to be occupied and that the licensed spectrum is deemed to be unoccupied, respectively. Specifically, $H = H_0$ represents the case that the licensed spectrum is deemed to be unoccupied, while $H = H_1$ indicates that the licensed spectrum is deemed to be occupied.

The probability $P_d$ of correct detection of the presence of PBS and the associated false alarm probability $P_f$ are defined as

$$P_d = \Pr(H = H_1 | H_1)$$

and

$$P_f = \Pr(H = H_1 | H_0),$$

respectively. Due to the background noise and fading effects, it is impossible to achieve perfectly reliable spectrum sensing without missing the detection of an active PU and without false alarm, which suggests that a spectral band is occupied by a PU, when it is actually unoccupied. Moreover, the missed detection of the presence of PBS will result in interference between the PU and SU. To guarantee that the interference imposed on the PUs is below a tolerable level, both the successful detection probability (SDP) $P_d$ and the false alarm probability (FAP) $P_f$ should be within a meaningful target range. For example, the IEEE 802.22 standard requires $P_d > 0.9$ and $P_f < 0.1$ [2]. For better protection of PUs, we consider $P_d = 0.99$ and $P_f = 0.01$, unless otherwise stated. Additionally, we consider a Rayleigh fading model for characterizing all the channels between any two nodes of Fig. 1. Finally, all the received signals are assumed to be corrupted by additive white Gaussian noise (AWGN) having a zero mean and a variance of $N_0$.

### B. Direct Transmission

Let us first consider the conventional direct transmission as a benchmark scheme. Let $x_p$ and $x_s$ denote the random symbols transmitted by the PBS and the ST at a particular time instance. Without loss of generality, we assume $E[|x_p|^2] = 1$. $E[.]$ represents the expected value operator. The transmit powers of the PBS and ST are denoted by $P_p$ and $P_s$, respectively. Given that the licensed spectrum is deemed to be unoccupied by the PBS (i.e. $H = H_0$), ST transmits its signal $x_s$ at a power of $P_s$. Then, the signal received at the SD can be written as

$$y_d = h_{sd}\sqrt{P_s}x_s + h_{pd}\sqrt{\alpha P_p}x_p + n_d,$$

where $H_0$ represents that the licensed spectrum is unoccupied by PBS and no primary signal is transmitted, leading to $\alpha = 0$. By contrast, $H_1$ represents that PBS is transmitting its signal $x_p$ over the licensed spectrum, thus $\alpha = 1$. Meanwhile, due to the broadcast nature of the wireless medium, the ST’s signal will be overheard by E and the overheard signal can be expressed as

$$y_e = h_{se}\sqrt{P_s}x_s + h_{pe}\sqrt{\alpha P_p}x_p + n_e,$$

where $h_{se}$ and $h_{pe}$ represent the fading coefficients of the channel spanning from ST to E and that from PBS to E, respectively, while $n_e$ represents the AWGN received at E. Upon combining Shannon’s capacity formula [31] with (1), we obtain the capacity of the ST-SD channel as

$$C_{sd} = \log_2 \left(1 + \frac{|h_{sd}|^2}{\alpha|h_{pd}|^2} \left(\gamma_s + 1\right)\right),$$

where $\gamma_s = P_s/N_0$, and $\gamma_p = P_p/N_0$. Similarly, the capacity of the ST-E channel is obtained from (3) as

$$C_{se} = \log_2 \left(1 + \frac{|h_{se}|^2}{\alpha|h_{pe}|^2} \left(\gamma_p + 1\right)\right).$$

### C. Single-Relay Selection

In this subsection, we consider the cognitive relay network of Fig. 2, where both SD and E are assumed to be beyond the coverage area of the ST [24], [25], and N secondary relays (SRs) are employed for assisting the cognitive ST-SD transmission. We assume that a common control channel (CCC) [4], [6] is available for coordinating the actions of the different network nodes and the decode-and-forward (DF) relaying using two adjacent time slots is employed. More specifically, once 244 the licensed spectrum is deemed to be unoccupied, the ST first broadcasts its signal $x_s$ to the N SRs, which attempt to decode $x_s$ from their received signals. For notational convenience, let $\mathcal{D}$ represent the set of SRs that succeed in decoding $x_s$. Given 248 $N$ SRs, there are $2^N$ possible subsets $\mathcal{D}$, thus the sample space of $\mathcal{D}$ is formulated as

$$\Omega = \{\emptyset, \mathcal{D}_1, \mathcal{D}_2, \ldots, \mathcal{D}_n, \ldots, \mathcal{D}_{2^N-1}\},$$

where $\emptyset$ represents the empty set and $\mathcal{D}_n$ represents the $n$-th non-empty subset of the $N$ SRs. If the set $\mathcal{D}$ is empty, implying 252 that no SR decodes $x_s$ successfully, then all the SRs remain silent and thus SD and E are unable to decode $x_s$ in this case. If the set $\mathcal{D}$ is non-empty, a specific SR is chosen from 255 $\mathcal{D}$ to forward its decoded signal $x_d$ to SD. Therefore, given 256 $\mathcal{D}$, ST broadcasts its signal $x_d$ to $N$ SRs at a power of $P_s$ and a rate of $R$. Hence, the signal received at a specific SR is given by

$$y_i = h_{si}\sqrt{P_s}x_s + h_{pi}\sqrt{\alpha P_p}x_p + n_i,$$

where $h_{si}$ and $h_{pi}$ represent the fading coefficients of the ST-SR, channel and that of the PBS-SR, channel, respectively, with 261
likely that max

affected by the single RV

see from (4) that the capacity of classic direct transmission is

variables (RVs)

scheme is determined by the maximum of independent random

otherwise, the receiver becomes unable to successfully decode the source signal, regardless of the decoding algorithm adopted. Otherwise, the receiver can succeed in decoding the source signal. Thus, using (8), we can describe the event of $D = 0$ as

$$C_{si} < R, \quad i \in \{1, 2, \ldots, N\}.$$  (9)

Meanwhile, the event of $D = D_n$ is described as

$$C_{si} > R, \quad i \in D_n$$

$$C_{sj} < R, \quad j \in \bar{D}_n,$$  (10)

where $\bar{D}_n$ represents the complementary set of $D_n$. Without loss of generality, we assume that SR is chosen within $D_n$ to transmit its decoded result $x_i$ at a power of $P_s$, thus the signal received at SD can be written as

$$y_d = h_{id} \sqrt{P_s x_i} + h_{pd} \sqrt{\alpha P_p x_p} + n_d, \quad (11)$$

where $h_{id}$ represents the fading coefficient of the SR $i$ to SD channel. From (11), the capacity of the SR $i$ to SD channel is given by

$$C_{id} = \frac{1}{2} \log_2 \left(1 + \frac{|h_{id}|^2 \gamma_s}{\alpha|h_{pd}|^2 P_p + 1}\right), \quad (12)$$

where $i \in D_n$. In general, the specific SR $i$ having the highest instantaneous capacity to SD is chosen as the “best” SR for assisting the ST’s transmission. Therefore, the best relay selection criterion is expressed from (12) as

$$\text{Best SR} = \arg \max_{i \in D_n} C_{id} = \arg \max_{i \in D_n} |h_{id}|^2, \quad (13)$$

which shows that only the channel state information (CSI) $|h_{id}|^2$ is required for performing the relay selection without the need for the eavesdropper’s CSI knowledge. Upon combining (12) and (13), we obtain the capacity of the channel spanning from the “best” SR to SD as

$$C_{bd} = \frac{1}{2} \log_2 \left(1 + \frac{\gamma_s}{\alpha|h_{pd}|^2 P_p + 1} \max_{i \in D_n} |h_{id}|^2\right), \quad (14)$$

where the subscript ‘b’ in $C_{bd}$ denotes the best SR. It is observed from (14) that the legitimate transmission capacity of the SRS scheme is determined by the maximum of independent random variables (RVs) $|h_{id}|^2$ for different SRs. By contrast, one can see from (4) that the capacity of classic direct transmission is affected by the single RV $|h_{id}|^2$. If all RVs $|h_{id}|^2$ and $|h_{ad}|^2$ are independent and identically distributed (i.i.d), it would be most likely that $\max_{i \in D_n} |h_{id}|^2$ is much higher than $|h_{ad}|^2$ for a sufficiently large number of SRs, resulting in a performance improvement for the SRS scheme over the classic direct transmission. However, if the RVs $|h_{id}|^2$ and $|h_{ad}|^2$ are non-identically distributed and the mean value of $|h_{ad}|^2$ is much higher than that of $|h_{id}|^2$, then it may be more likely that $\max_{i \in D_n} |h_{id}|^2$ is smaller than $|h_{ad}|^2$ for a given number of SRs. In this extreme case, the classic direct transmission may perform better than the SRS scheme.

It is worth mentioning that in practice, the average fading gain of the ST-SD channel, $|h_{id}|^2$, should not be less than that of the ST-SR channel $|h_{ad}|^2$, since SRs are typically placed in the middle between the ST and SD. Hence, a performance improvement for the SRS scheme over classic direct transmission would be achieved in practical wireless systems. Note that although a factor 1/2 in (14) is imposed on the capacity of the main channel, it would not affect the performance of the SRS scheme from a SRT perspective, since the capacity of the wiretap channel is also multiplied by 1/2 as will be shown in (16).

Additionally, given that the selected SR transmits its decoded result $x_i$ at a power of $P_s$, the signal received at E is 316 expressed as

$$y_e = h_{be} \sqrt{P_s x_i} + h_{pe} \sqrt{\alpha P_p x_p} + n_e, \quad (15)$$

where $h_{be}$ and $h_{pe}$ represent the fading coefficients of the channel from “best” SR to E and that from PBS to E, respectively. From (15), the capacity of the channel spanning from the “best” SR to E is given by

$$C_{be} = \frac{1}{2} \log_2 \left(1 + \frac{|h_{be}|^2 \gamma_s}{\alpha|h_{pe}|^2 P_p + 1}\right), \quad (16)$$

where $b \in D_n$ is determined by the relay selection criterion given in (13). As shown in (16), the eavesdropper’s channel 325 capacity is affected by the channel state information (CSI) $|h_{be}|^2$ of the wiretap channel spanning from the “best” relay to 325 the eavesdropper. However, one can see from (13) that the best parcel selected from the decoding set $D_b$ is the main channel’s CSI $|h_{ad}|^2$ i.e. without taking into account the eavesdropper’s CSI knowledge of $|h_{pe}|^2$. This means that the 329 selection of the best relay aiming for maximizing the legitimate 330 transmission capacity of (14) would not lead to significantly
beneficial or adverse impact on the eavesdropper’s channel capacity, since the main channel and the wiretap channel are independent of each other. For example, if the random variables (RVs) \(|h_{ie}|^2\) related to the different relays are i.i.d, we can readily infer by the law of total probability that \(|h_{ie}|^2\) has the same probability density function (PDF) as \(|h_{ie}|^2\), implying that the eavesdropper’s channel capacity of (16) is not affected by the selection of the best relay given by (13). Therefore, the SRS scheme has no obvious advantage over the classic direct transmission in terms of minimizing the capacity of the wiretap channel. To elaborate a little further, according to the SRT trade-off, a reduction of the outage probability (OP) due to the capacity enhancement of the main channel achieved by using the selection of the best relay would be converted into an intercept probability (IP) improvement, which will be numerically illustrated in Section IV.

### 3.49 D. Multi-Relay Selection

This subsection presents a MRS scheme, where multiple SRs are employed for simultaneously forwarding the source signal to SD. To be specific, ST first transmits \(x_s\) to \(N\) SRs over a detected spectrum hole. As mentioned in Subsection II-C, we denote by \(\mathcal{D}\) the set of SRs that successfully decode \(x_s\). If \(\mathcal{D}\) is empty, all SRs fail to decode \(x_s\) and will not forward the source signal, thus both SD and E are unable to decode \(x_s\). If \(\mathcal{D}\) is non-empty (i.e., \(\mathcal{D} = \mathcal{D}_n\)), all SRs within \(\mathcal{D}_n\) are utilized for simultaneously transmitting \(x_s\) to SD. This differs from the SRS scheme, where only a single SR is chosen from \(\mathcal{D}_n\) for forwarding \(x_s\) to SD. To make effective use of multiple SRs, a weight vector denoted by \(w = [w_1, w_2, \ldots, w|\mathcal{D}_n|]^T\) is employed at the SRs for transmitting \(x_s\), where \(|\mathcal{D}_n|\) is the cardinality of the set \(\mathcal{D}_n\), For the sake of a fair comparison with the SRS scheme in terms of power consumption, the total transmit power across all SRs within \(\mathcal{D}\) shall be constrained to \(P_t\), and thus the weight vector \(w\) should be normalized according to \(\|w\| = 1\).

Thus, given \(\mathcal{D} = \mathcal{D}_n\) and considering that all SRs within \(\mathcal{D}_n\) are selected for simultaneously transmitting \(x_s\) with a weight vector \(w\), the signal received at SD is expressed as

\[
y_d^\text{multi} = \sqrt{P_t}w^T H_d x_s + \sqrt{\alpha P_t} h_{pd} x_p + n_d, \tag{17}
\]

where \(H_d = [h_{1d}, h_{2d}, \ldots, h_{|\mathcal{D}_n|}]^T\). Similarly, the signal received at E can be written as

\[
y_e^\text{multi} = \sqrt{P_t}w^T H_e x_s + \sqrt{\alpha P_t} h_{pe} x_p + n_e, \tag{18}
\]

where \(H_e = [h_{1e}, h_{2e}, \ldots, h_{|\mathcal{D}_n|}]^T\). From (17) and (18), the signal-to-interference-plus-noise ratios (SINRs) at SD and E are, respectively, given by

\[
\text{SINR}_d^\text{multi} = \frac{\gamma_s}{\alpha|h_{pd}|^2|\gamma_p| + 1} |w^T H_d|^2, \tag{19}
\]

and

\[
\text{SINR}_e^\text{multi} = \frac{\gamma_s}{\alpha|h_{pe}|^2|\gamma_p| + 1} |w^T H_e|^2. \tag{20}
\]

In this work, the weight vector \(w\) is optimized by maximizing the SINR at SD, yielding

\[
\max_w \text{SINR}_d^\text{multi}, \quad \text{s.t. } \|w\| = 1, \tag{21}
\]

where the constraint is used for normalization purposes. Using the Cauchy-Schwarz inequality [32], we can readily obtain the optimal weight vector \(w^\text{opt}\) from (21) as

\[
w^\text{opt} = \frac{H_d^*}{|H_d|^2}, \tag{22}
\]

which indicates that the optimal vector design only requires the SR-SD CSI \(H_d\), whilst dispensing with the eavesdropper’s CSI \(H_e\). Substituting the optimal vector \(w^\text{opt}\) from (22) into (19) and (20) and using Shannon’s capacity formula, we can obtain the channel capacities achieved at both SD and E as

\[
C_d = \frac{1}{2} \log_2 \left(1 + \frac{\gamma_s}{\alpha|\gamma_p|h_{pd}|^2 + 1} \sum_{i \in \mathcal{D}_n} |h_{id}|^2 \right), \tag{23}
\]

and

\[
C_e = \frac{1}{2} \log_2 \left(1 + \frac{\gamma_s}{\alpha|\gamma_p|h_{pe}|^2 + 1} \frac{H_d^* H_e}{|H_d|^2} \right), \tag{24}
\]

for \(\mathcal{D} = \mathcal{D}_n\), where \(H\) represents the Hermitian transpose. One can observe from (14) and (23) that the difference between the capacity expressions \(C_d\) and \(C_e^\text{multi}\) only lies in the fact that 389 the maximum of RVs \(|h_{id}|^2\) for different SRs (i.e., max \(|h_{id}|^2\)) is used for the SRS scheme, while the sum of RVs \(|h_{id}|^2\) (i.e., \(\sum_{i \in \mathcal{D}_n} |h_{id}|^2\)) is employed for the MRS scheme. Clearly, we have \(\sum_{i \in \mathcal{D}_n} |h_{id}|^2 > \max_{i \in \mathcal{D}_n} |h_{id}|^2\), resulting in a performance gain for MRS over SRS in terms of maximizing the legitimate transmission capacity. Moreover, since the main channel \(H_d\) and the wiretap channel \(H_e\) are independent of each other, the optimal weights assigned for the multiple relays based on \(H_d\) will only slightly affect the eavesdropper’s channel capacity. This means that the MRS and SRS schemes achieve more or less the same performance in terms of the capacity of the wiretap channel. Nevertheless, given a fixed outage requirement, the MRS scheme can achieve a better intercept performance than the SRS scheme, because according to the SRT, an outage reduction achieved by the capacity enhancement of the legitimate transmission relying on the MRS would be converted into an intercept improvement. To be specific, given an enhanced capacity of the legitimate transmission, we may increase the data rate \(R\) based on the OP definition of (25) for maintaining a fixed OP, which, in turn leads to a reduction of the IP, since a higher data rate would result in a lower IP, according to the IP 410 definition of (26).

It needs to be pointed out that in the MRS scheme, a high-complexity symbol-level synchronization is required for multiple distributed SRs, when simultaneously transmitting to SD, whereas the SRS does not require such a complex synchronization process. Thus, the performance improvement of MRS over SRS is achieved at the cost of a higher implementation.
complexity. Additionally, the synchronization imperfections of the MRS scheme will impose a performance degradation, which may even lead to a performance for the MRS scheme becoming worse than that of the SRS scheme.

Throughout this paper, the Rayleigh model is used for characterizing the fading amplitudes (e.g., $|h_{sd}|$, $|h_{d}^{}|$, $|h_{sd}|^2$, etc.) of wireless channels, which, in turn, implies that the fading square magnitudes $|h_{sd}|^2$, $|h_{d}^{}|^2$ and $|h_{sd}|^2$ are exponentially distributed random variables (RVs). So far, we have completed the presentation of the signal model of the direct transmission, of the SRS, and of the MRS schemes for CR networks applications in the presence of eavesdropping attacks.

### III. SRT Analysis over Rayleigh Fading Channels

This section presents the SRT analysis of the direct transmission, SRS and MRS schemes over Rayleigh fading channels. As discussed in [31], the security and reliability are quantified in terms of the IP and OP experienced by the eavesdropper and destination, respectively. It is pointed out that in CR networks, ST starts to transmit its signal only when an available spectrum hole is detected. Similarly to [34], the OP and IP are thus calculated under the condition that the licensed spectrum is detected to be unoccupied by the PBS. The following gives the definition of OP and IP.

**Definition 1:** Let $C_d$ and $C_e$ represent the channel capacities achieved at the destination and eavesdropper, respectively. The OP and IP are, respectively, defined as

$$P_{\text{out}} = \Pr (C_d < R|\hat{H} = H_0),$$

(25)

and

$$P_{\text{int}} = \Pr (C_e > R|\hat{H} = H_0),$$

(26)

where $R$ is the data rate.

#### A. Direct Transmission

Let us first analyze the SRT performance of the conventional direct transmission. Given that a spectrum hole has been detected, the OP of direct transmission is obtained from (25) as

$$P_{\text{out}}^{\text{direct}} = \Pr (C_d < R|\hat{H} = H_0),$$

(27)

where $C_d$ is given by (4). Using the law of total probability, we can rewrite (27) as

$$P_{\text{out}}^{\text{direct}} = \Pr (C_d < R|H_0, \hat{H} = H_0) + \Pr (C_d < R|H_1, \hat{H} = H_0),$$

(28)

which can be further expressed as

$$P_{\text{out}}^{\text{direct}} = \Pr (C_d < R|H_0, \hat{H} = H_0) \Pr (H_0|\hat{H} = H_0)$$

$$+ \Pr (C_d < R|H_1, \hat{H} = H_0) \Pr (H_1|\hat{H} = H_0).$$

(29)

It is shown from (2) that given $H_0$ and $H_1$, the parameter $\alpha$ is obtained as $\alpha = 0$ and $\alpha = 1$, respectively. Thus, combining (2) and (4), we have $C_{sd} = \log_2(1 + |h_{sd}|^2\gamma_s)$ given $H_0$ and $C_{sd} = \log_2(1 + \frac{|h_{sd}|^2\gamma_s}{|h_{sd}|^2\gamma_p + 1})$ given $H_1$. Substituting this result into (29) yields

$$P_{\text{out}}^{\text{direct}} = \Pr \left( |h_{sd}|^2 \gamma_s < 2^R - 1 \right) \Pr (H_0|\hat{H} = H_0)$$

$$+ \Pr \left( \frac{|h_{sd}|^2 \gamma_s}{|h_{sd}|^2 \gamma_p + 1} < 2^R - 1 \right) \Pr (H_1|\hat{H} = H_0).$$

(30)

Moreover, the terms $\Pr (H_0|\hat{H} = H_0)$ and $\Pr (H_1|\hat{H} = H_0)$ can be obtained by using Bayes’ theorem as

$$\Pr (H_0|\hat{H} = H_0) = \frac{\sum_{\gamma \in \{0,1\}} \Pr (\hat{H} = H_0|H_0) \Pr (H_0)}{\Pr (\hat{H} = H_0)}$$

$$= \frac{P_0(1 - P_f)}{P_0(1 - P_f) + (1 - P_0)(1 - P_d)} \Delta \pi_0,$$

(31)

and

$$\Pr (H_1|\hat{H} = H_0) = \frac{(1 - P_0)(1 - P_d)}{P_0(1 - P_f) + (1 - P_0)(1 - P_d)} \Delta \pi_1,$$

(32)

where $P_0 = \Pr (H_0)$ is the probability that the licensed spectrum is not occupied by PBS, while $P_2 = \Pr (\hat{H} = H_1|H_1)$ are the SDP and FAP, respectively. For notational convenience, we introduce the shorthand $\pi_0 = 0.46$ and $\pi_1 = \Pr (H_1|\hat{H} = H_0)$ and $\Delta = \frac{2^R - 1}{\gamma_s}$. Then, we rewrite (30) as

$$P_{\text{out}}^{\text{direct}} = \pi_0 \Pr (|h_{sd}|^2 < \Delta) + \pi_1 \Pr \left( |h_{sd}|^2 - |h_{sd}|^2 \gamma_p \Delta < \Delta \right).$$

(33)

Noting that $|h_{sd}|^2$ and $|h_{sd}|^2$ are independently and exponentially distributed RVs with respective means of $\sigma_{sd}^2$ and $\sigma_{sd}^2$, we obtain

$$\Pr \left( |h_{sd}|^2 < \Delta \right) = 1 - \exp \left( -\frac{\Delta}{\sigma_{sd}^2} \right),$$

(34)

and

$$\Pr \left( |h_{sd}|^2 - |h_{sd}|^2 \gamma_p \Delta < \Delta \right) = 1 - \frac{\sigma_{sd}^2}{\sigma_{sd}^2 + \sigma_{sd}^2} \exp \left( -\frac{\Delta}{\sigma_{sd}^2} \right).$$

(35)

Additionally, we observe from (26) that an intercept event occurs, when the capacity of the ST-E channel becomes higher than the data rate. Thus, given that a spectrum hole has been detected (i.e., $\hat{H} = H_0$), ST starts transmitting its signal to SD and E may overhear the ST-SD transmission. The corresponding IP is given by

$$P_{\text{int}}^{\text{direct}} = \Pr (C_e > R|\hat{H} = H_0),$$

(36)

which can be further expressed as

$$P_{\text{int}}^{\text{direct}} = \Pr (C_e > R|\hat{H} = H_0, H_0) \Pr (H_0|\hat{H} = H_0)$$

$$+ \Pr (C_e > R|\hat{H} = H_0, H_1) \Pr (H_1|\hat{H} = H_0)$$

$$= \pi_0 \Pr \left( |h_{se}|^2 > \Delta \right) + \pi_1 \Pr \left( |h_{se}|^2 - |h_{pe}|^2 \gamma_p \Delta > \Delta \right),$$

(37)
478 where the second equality is obtained by using $C_{se}$ from (5). Noting that RVs $|h_{se}|^2$ and $|h_{pe}|^2$ are exponentially distributed and independent of each other, we can express the terms $\Pr(|h_{se}|^2 > \Delta)$ and $\Pr(|h_{se}|^2 - |h_{pe}|^2 \gamma_p \Delta > \Delta)$ as

$$\Pr(|h_{se}|^2 > \Delta) = \exp \left( - \frac{\Delta}{\sigma_{se}^2} \right),$$  

(38)

and

$$\Pr(|h_{se}|^2 - |h_{pe}|^2 \gamma_p \Delta > \Delta) = \frac{\sigma_{se}^2}{\sigma_{pe}^2 \gamma_p \Delta + \sigma_{se}^2} \exp \left( - \frac{\Delta}{\sigma_{se}^2} \right).$$  

(39)

where $\sigma_{se}^2$ and $\sigma_{pe}^2$ are the expected values of RVs $|h_{se}|^2$ and $|h_{pe}|^2$, respectively.

485 B. Single-Relay Selection

In this subsection, we present the SRT analysis of the proposed SRS scheme. Given $\hat{H} = H_0$, the OP of the cognitive transmission relying on SRS is given by

$$P_{\text{out}}^{\text{single}} = \Pr(C_{bd} < R, D = 0 | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N-1} \Pr(C_{bd} < R, D = D_n | \hat{H} = H_0),$$  

(40)

where $C_{bd}$ represents the capacity of the channel from the “best” SR to SD. In the case of $D = 0$, no SR is chosen to forward the source signal, which leads to $C_{bd} = 0$ for $D = 0$.

492 Substituting this result into (40) gives

$$P_{\text{out}}^{\text{single}} = \Pr(D = 0 | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N-1} \Pr(C_{bd} < R, D = D_n | \hat{H} = H_0).$$  

(41)

Using (2), (9), (10), and (14), we can rewrite (41) as (42), shown at the bottom of the page, where $\Lambda = \frac{p_k^i}{N_p-1}$. Noting that $|h_{si}|^2$ and $|h_{pi}|^2$ are independent exponentially distributed random variables with respective means of $\sigma_{si}^2$ and $\sigma_{pi}^2$, we have

$$\Pr(|h_{si}|^2 < \Lambda) = 1 - \exp \left( - \frac{\Lambda}{\sigma_{si}^2} \right),$$  

(43)

and

$$\Pr(|h_{si}|^2 < \Lambda| |h_{pi}|^2 \gamma_p + \Lambda) = 1 - \frac{\sigma_{si}^2}{\sigma_{pi}^2 \gamma_p + \sigma_{si}^2} \exp \left( - \frac{\Lambda}{\sigma_{si}^2} \right),$$  

(44)

where the terms $\Pr(|h_{si}|^2 > \Lambda)$, $\Pr(|h_{si}|^2 < \Lambda)$, and $\Pr(|h_{si}|^2 > 2\Lambda| |h_{pi}|^2 \gamma_p + \Lambda)$ can be similarly determined in closed-form. Moreover, based on Appendix A, we obtain $\Pr(\max_{i \in \mathbb{D}_h} |h_{id}|^2 < \Lambda)$ and

$$\Pr(\max_{i \in \mathbb{D}_h} |h_{id}|^2 < \Lambda| |h_{pd}|^2 \gamma_p + \Lambda)$$

$$= \prod_{i \in \mathbb{D}_h} \left[ 1 - \exp \left( - \frac{\Lambda}{\sigma_{id}^2} \right) \right],$$  

(45)

and

$$\Pr(\max_{i \in \mathbb{D}_h} |h_{id}|^2 < \Lambda| |h_{pd}|^2 \gamma_p + \Lambda)$$

$$= \prod_{i \in \mathbb{D}_h} \left[ 1 - \exp \left( - \frac{\Lambda}{\sigma_{id}^2} \right) \right],$$  

(46)

where $\mathbb{D}_h(m)$ represents the $m$-th non-empty subset of $\mathbb{D}_h$. Additionally, the IP of the SRS scheme can be expressed as

$$P_{\text{int}}^{\text{single}} = \Pr(C_{be} > R, D = 0 | \hat{H} = H_0)$$

$$+ \sum_{n=1}^{N-1} \Pr(C_{be} > R, D = D_n | \hat{H} = H_0),$$  

(47)

where $C_{be}$ represents the capacity of the channel spanning from the “best” SR to E. Given $D = 0$, we have $C_{bd} = 0$, since no relay is chosen for forwarding the source signal. Thus, 507
where the closed-form expressions of $\text{Pr}$ transmission over Rayleigh fading channels. Similarly to (41), we arrive at

\[ P_{\text{int}}^{\text{single}} = \pi_0 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \text{Pr}(|h_{zi}|^2 > \Lambda) \prod_{j \in D_n} \text{Pr}(|h_{sj}|^2 < \Lambda) \times \text{Pr}(|h_{be}|^2 > \Lambda) + \pi_1 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \text{Pr}(|h_{zi}|^2 > \Lambda|p_{zi}^2 \gamma_p + \Lambda) \times \prod_{j \in D_n} \text{Pr}(|h_{sj}|^2 < \Lambda|p_{sj}^2 \gamma_p + \Lambda) \times \text{Pr}(|h_{be}|^2 > \Lambda|p_{be}^2 \gamma_p + \Lambda), \]  

(48)

where the closed-form expressions of $\text{Pr}(|h_{zi}|^2 > \Lambda)$ and $\text{Pr}(|h_{zi}|^2 > \Lambda|p_{zi}^2 \gamma_p + \Lambda)$ can be readily obtained by using (43) and (44). Using the results in Appendix B, we can express $\text{Pr}(|h_{be}|^2 > \Lambda)$ and $\text{Pr}(|h_{be}|^2 > \Lambda|p_{be}^2 \gamma_p + \Lambda)$ as

\[ \text{Pr}(|h_{be}|^2 > \Lambda) = \sum_{i \in D_{\Lambda}} \exp \left( -\Lambda \sigma_{ie}^2 \right) \times \left[ 1 + \sum_{m=1}^{2^{D_n} - 1} (-1)^m C_m \left( \left( 1 + \sum_{j \in C_m(m)} \sigma_{je}^2 \right)^{-1} \right) \right], \]  

(49)

and

\[ \text{Pr}(|h_{be}|^2 > \Lambda|p_{be}^2 \gamma_p + \Lambda) = \sum_{i \in D_{\Lambda}} \sigma_{pe}^2 \gamma_p \Lambda + \sigma_{ie}^2 \exp \left( -\Lambda \sigma_{ie}^2 \right) \times \left[ 1 + \sum_{m=1}^{2^{D_n} - 1} (-1)^m C_m \left( \left( 1 + \sum_{j \in C_m(m)} \sigma_{je}^2 \right)^{-1} \right) \right], \]  

(50)

where $C_m(m)$ represents the $m$-th non-empty subset of $D_n \setminus \{i\}$ and ‘$-$’ represents the set difference.

\[ P_{\text{out}}^{\text{multi}} = \pi_0 \prod_{i=1}^{N} \text{Pr}(|h_{zi}|^2 < \Lambda) + \pi_1 \prod_{i=1}^{N} \text{Pr}(|h_{zi}|^2 < \Lambda|p_{zi}^2 \gamma_p + \Lambda) \]

\[ + \pi_0 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \text{Pr}(|h_{zi}|^2 > \Lambda) \prod_{j \in D_n} \text{Pr}(|h_{sj}|^2 < \Lambda) \text{Pr} \left( \sum_{i \in D_n} |h_{id}|^2 < \Lambda \right) \]

\[ + \pi_1 \sum_{n=1}^{2N-1} \prod_{i \in D_n} \text{Pr}(|h_{zi}|^2 > \Lambda|p_{zi}^2 \gamma_p + \Lambda) \prod_{j \in D_n} \text{Pr}(|h_{sj}|^2 < \Lambda) \text{Pr} \left( \sum_{i \in D_n} |h_{id}|^2 < \Lambda \right) \]

\[ \times \text{Pr} \left( \sum_{i \in D_n} |h_{id}|^2 < \gamma_p \Lambda |p_{id}^2 + \Lambda \right), \]  

(52)

Using (2), (9), (10) and (23), we can rewrite (51) as (52), shown at the bottom of the page, where the closed-form expressions of $\text{Pr}(|h_{zi}|^2 < \Lambda), \text{Pr}(|h_{zi}|^2 < \Lambda|p_{zi}^2 \gamma_p + \Lambda), \text{Pr}(|h_{zi}|^2 > \Lambda)$, and $\text{Pr}(|h_{zi}|^2 > \Lambda|p_{zi}^2 \gamma_p + \Lambda)$ can be readily derived, as shown in (43) and (44). However, it is challenging to obtain the closed-form expressions of $\text{Pr}(\sum |h_{id}|^2 < \Lambda)$ and $\text{Pr}(\sum |h_{id}|^2 < \gamma_p \Lambda |p_{id}^2 + \Lambda)$. For simplicity, we assume that the fading coefficients of all SRs-SD channels, i.e. $|h_{id}|^2$ for $i \in \{1, 2, \ldots, N\}$, are i.i.d. RVs having the same mean (average channel gain) denoted by $\sigma_d^2 = E(|h_{id}|^2)$. This assumption is widely used in the cooperative relaying literature and it is valid in a statistical sense, provided that all SRs are uniformly distributed over a certain geographical area. Assuming that $\text{MRS}$ RVs of $|h_{id}|^2$ for $i \in D_n$ are i.i.d., based on Appendix C, we arrive at

\[ \text{Pr} \left( \sum_{i \in D_n} |h_{id}|^2 < \Lambda \right) = \Gamma \left( \frac{\Lambda \sigma_d^2}{\sigma_p^2}, |D_n| \right), \]  

(53)

and

\[ \text{Pr} \left( \sum_{i \in D_n} |h_{id}|^2 < \gamma_p \Lambda |p_{id}^2 + \Lambda \right) = \Gamma \left( \frac{\Lambda \sigma_d^2 + \sigma_p^2 \gamma_p \Lambda}{\sigma_p^2}, |D_n| \right) \times \left( 1 + \sigma_p^2 \sigma_d^2 \gamma_p \Lambda - 1 \right)^{|D_n|} e^{-1/(\sigma_p^2 \gamma_p \Lambda)}, \]  

(54)

where $\Gamma(x, k) = \int_0^x e^{-t} t^{k-1} dt$ is known as the incomplete Gamma function [32]. Substituting (53) and (54) into (52) 538 yields a closed-form OP expression for the proposed MRS scheme.

\[ 539 \]

507 C. Multi-Relay Selection

This subsection analyzes the SRT of our MRS scheme for transmission over Rayleigh fading channels. Similarly to (41), the OP in this case is given by

\[ P_{\text{out}}^{\text{multi}} = \text{Pr}(D = \emptyset | \hat{H} = H_0) \]

\[ + \sum_{n=1}^{2N-1} \text{Pr}(C_n^{\text{multi}} < R, D = D_n | \hat{H} = H_0), \]  

(51)

510 where $\text{Pr}$ the OP in this case is given by 520

509 substituting this result into (47) and using (2), (9), (10), and 508

507

507

507

507

507

507

507

507

507

507

507

507

507
Next, we present the IP analysis of the MRS scheme. Similarly to (48), the IP of the MRS can be obtained from (24) as
\[
P^\text{multi}_{\text{int}} = \rho_0 \sum_{n=1}^{2N-1} \prod_{i \in \mathcal{D}_n} \Pr(|h_{si}|^2 > \Lambda) \prod_{j \in \mathcal{D}_n} \Pr(|h_{sj}|^2 < \Lambda)
\times \Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \Lambda\right)
+ \rho_1 \sum_{n=1}^{2N-1} \prod_{i \in \mathcal{D}_n} \Pr(|h_{si}|^2 > \Lambda|p_i|^2 \gamma_p + \Lambda)
\times \prod_{j \in \mathcal{D}_n} \Pr(|h_{sj}|^2 < \Lambda|p_j|^2 \gamma_p + \Lambda)
\times \Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \gamma_p \Lambda|p_e|^2 + \Lambda\right),
\] (55)
where the closed-form expressions for \(\Pr(|h_{si}|^2 > \Lambda), \Pr(|h_{sj}|^2 < \Lambda), \Pr(|h_{si}|^2 > \Lambda|p_i|^2 \gamma_p + \Lambda)\) and \(\Pr(|h_{sj}|^2 < \Lambda|p_j|^2 \gamma_p + \Lambda)\) may be readily derived by using (43) and (44).

However, it is challenging to obtain the closed-form solutions for \(\Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \Lambda\right)\) and \(\Pr\left(\frac{|H_d^H H_e|^2}{|H_d|^2} > \gamma_p \Lambda|p_e|^2 + \Lambda\right)\).

Although finding a general closed-form IP expression for the MRS scheme is challenging, we can obtain the numerical IP results with the aid of computer simulations.

IV. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we present our performance comparisons among the direct transmission, the SRS and MRS schemes in terms of their SRT. To be specific, the analytic IP versus OP of the three schemes are obtained by plotting (33), (37), (46), (48), (52), and (55). The simulated IP and OP results of the three schemes are also given to verify the correctness of the theoretical SRT analysis. In our computer simulations, the fading amplitudes (e.g., \(|h_{sid}|, |h_{sij}|, |h_{sid}|, \ldots\) ) are first generated based on the Rayleigh distribution having different variances for different channels. Then, the randomly generated fading amplitudes are substituted into the definition of an outage (or intercept) event, which would determine whether an outage (or intercept) event occurs or not. By repeatedly achieving this process, we can calculate the relative frequency of occurrence for an outage (intercept) event, which is the simulated OP (or IP).

Additionally, the SDP \(P_d\) and FAP \(P_f\) are set to \(P_d = 0.99\) and \(P_f = 0.01\), unless otherwise stated. The primary signal-noise ratio (SNR) of \(\gamma_p = 10\) dB and the data rate of \(R = 1\) bit/s/Hz are used in our numerical evaluations.

The artificial noise based method [35], [36] is also considered for the purpose of numerical comparison with the relay selection schemes. To be specific, in the artificial noise based scheme, ST directly transmits its signal \(x_s\) to SD, while N SRs attempt to confuse the eavesdropper by sending an interfering signal (referred to as artificial noise) that is approximately designed to lie in the null-space of the legitimate main channel.

In this way, the artificial noise will impose interference on the eavesdropper without affecting the SD. For a fair comparison, the total transmit power of the desired signal \(x_s\) and the artificial noise are constrained to \(P_s\). Moreover, the equal power allocation method [35] is used in the numerical evaluation.

Fig. 3 shows the IP versus OP of the direct transmission, SRS, and MRS schemes for \(P_0 = 0.8\), where 584 the solid lines and discrete marker symbols represent the analytic and simulated results, respectively. It can be seen from Fig. 3 that the IP of the direct transmission, the artificial noise based SRS, and MRS schemes outperform the direct transmission and the 590 artificial noise based approaches in terms of their SRT, showing 591 the advantage of exploiting relay selection against the eaves- 592 dropped attack. Moreover, the SRT performance of the MRS is 593 better than that of the SRS. Although the MRS achieves a better SRT performance than its SRS-aided counterpart, this result is obtained at the cost of a higher implementation complexity, since multiple SRs require high-complexity symbol-level synchronanomaly for simultaneously transmitting to the SD, whereas the SRS does not require such elaborate synchronization.

Fig. 4 illustrates our numerical SRT comparison between the SRS and MRS schemes for \(P_0 = 0.2\) and \(P_0 = 0.8\). Observe from Fig. 4 that the MRS scheme performs better than the SRS in terms of its SRT performance for both \(P_0 = 0.2\) and \(P_0 = 0.8\). It is also seen from Fig. 4 that as \(P_0\) increases from 0.2 to 0.6 0.8, the SRT of both the SRS and MRS schemes improves. This is because upon increasing \(P_0\), the licensed band becomes unoccupied by the PUs with a higher probability and hence the 609 secondary users (SUs) have more opportunities for accessing the licensed band for their data transmissions, which leads to a reduction of the OP for CR transmissions. Meanwhile, 612 increasing \(P_0\) may simultaneously result in an increase of the IP, since the eavesdropper also has more opportunities for tapping the cognitive transmissions. However, in both the SRS and MRS schemes, the relay selection is performed for the sake of maximizing the legitimate transmission capacity without affecting the eavesdropper’s channel capacity. Hence, upon increasing \(P_0\), it becomes more likely that the reduction of OP is more significant than the increase of IP, hence leading to an overall SRT improvement for the SRS and MRS schemes.
the proposed SRS and MRS schemes are generally better than that of the conventional direct transmission for \(N = 2, 4, 8\) and \(N = 8\). Moreover, as the number of SRs increases from 2 to 8, the SRT of the SRS and MRS schemes significantly improves, explicitly demonstrating the security and reliability benefits of exploiting multiple SRs for assisting the secondary transmissions. In other words, the security and reliability of the secondary transmissions can be concurrently improved by increasing the number of SRs. Additionally, as shown in Fig. 6, upon increasing the number of SRs from 2 to 8, the SRT improvement of MRS over SRS becomes more notable. Again, the SRT advantage of the MRS over the SRS comes at the expense of requiring elaborate symbol-level synchronization among the multiple SRs for simultaneously transmitting to the SD.

In this paper, we proposed relay selection schemes for a CR network consisting of a ST, a SD and multiple SRs communicating in the presence of an eavesdropper. We examined the SRT performance of the SRS and MRS assisted secondary transmissions in the presence of realistic spectrum sensing, where both the security and reliability of secondary transmissions are characterized in terms of their IP and OP. We also analyzed the SRT of the conventional direct transmission as a benchmark. It was illustrated that as the spectrum sensing reliability increases, the SRTs of both the SRS and MRS schemes improve. We also showed that the proposed MRS schemes generally outperform the conventional direct transmission and artificial noise based approaches in terms of their SRT. Moreover, the SRT performance of MRS is better than that of SRS. Additionally, as the number of SRs increases, the SRTs of both the SRS and of the MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and reliability of secondary transmissions.

V. CONCLUSION

In Fig. 5, we depict the IP versus OP of the SRS and MRS schemes for different spectrum sensing reliabilities, where \(P_d, P_f\) are considered. It is observed that as the spectrum sensing reliability is improved from \(P_d, P_f = (0.9, 0.1)\) to \(P_d, P_f = (0.99, 0.01)\), the SRTs of the SRS and MRS schemes improve accordingly. This is due to the fact that for an improved sensing reliability, an unoccupied licensed band would be detected more accurately and hence less mutual interference occurs between the PUs and SUs, which results in a better SRT for the secondary transmissions. Fig. 5 also shows that for \(P_d, P_f = (0.9, 0.1)\) and \(P_d, P_f = (0.99, 0.01)\), the MRS approach outperforms the SRS scheme in terms of the SRT, which further confirms the advantage of the MRS for protecting the secondary transmissions against eavesdropping attacks.

Fig. 6 shows the IP versus OP of the conventional direct transmission as well as of the proposed SRS and MRS schemes for \(N = 2, 4, 8\). It is seen from Fig. 6 that the SRTs of the SRS and MRS schemes improve significantly, demonstrating their benefits in terms of enhancing both the security and reliability of secondary transmissions.

In Fig. 4, Fig. 5, and Fig. 6, the SRTs of the SRS and MRS schemes are compared for different spectrum sensing reliabilities, where \(P_d, P_f\) are considered. It is observed that as the spectrum sensing reliability is improved from \(P_d, P_f = (0.9, 0.1)\) to \(P_d, P_f = (0.99, 0.01)\), the SRTs of the SRS and MRS schemes improve accordingly. This is due to the fact that for an improved sensing reliability, an unoccupied licensed band would be detected more accurately and hence less mutual interference occurs between the PUs and SUs, which results in a better SRT for the secondary transmissions. Fig. 5 also shows that for \(P_d, P_f = (0.9, 0.1)\) and \(P_d, P_f = (0.99, 0.01)\), the MRS approach outperforms the SRS scheme in terms of the SRT, which further confirms the advantage of the MRS for protecting the secondary transmissions against eavesdropping attacks.
APPENDIX A

DERIVATION OF (45) AND (46)

Letting $| h_{id} |^2 = x_i$ and $| h_{pd} |^2 = y$, the left hand side of (45) and (46) can be rewritten as $\Pr(\max x_i < \Lambda)$ and $\Pr(\max x_i < \Lambda \gamma p + \Lambda)$, respectively. Noting that random variables $| h_{id} |^2$ and $| h_{pd} |^2$ are exponentially distributed with respective means $\sigma_{id}^2$ and $\sigma_{pd}^2$, and independent of each other, we obtain

$$\Pr(\max x_i < \Lambda) = \prod_{i \in D_h} \Pr(| h_{id} |^2 < \Lambda)$$

$$= \prod_{i \in D_h} \left[ 1 - \exp\left( -\frac{\Lambda}{\sigma_{id}^2} \right) \right], \quad (A.1)$$

which is (45). Similarly, the term $\Pr(\max x_i < \Lambda \gamma p + \Lambda)$ can be computed as

$$\Pr\left( \max_{i \in D_h} x_i < \Lambda \gamma p + \Lambda \right) = \int_0^\infty \frac{1}{\sigma_{pd}^2} \exp\left( -\frac{y}{\sigma_{pd}^2} \right) \prod_{i \in D_h} \left( 1 - \exp\left( -\frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) \right) dy,$$

(A.2)

wherein

$$\prod_{i \in D_h} \left( 1 - \exp\left( -\frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) \right) \text{ can be further expanded as}$$

$$\prod_{i \in D_h} \left( 1 - \exp\left( -\frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) \right) = 1$$

$$+ \sum_{m = 1}^{2^{| D_h |} - 1} (-1)^{| D_h(m) |} \exp\left( -\sum_{i \in D_h(m)} \frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right), \quad (A.3)$$

864 where $| D_h |$ is the cardinality of set $D_h$, $D_h(m)$ represents the $m$-th non-empty subset of $D_h$, and $| D_h(m) |$ is the cardinality of set $D_h(m)$. Substituting $\prod_{i \in D_h} \left( 1 - \exp\left( -\frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) \right)$ from (A.3) into (A.2) yields

$$\Pr\left( \max_{i \in D_h} x_i < \Lambda \gamma p + \Lambda \right) = \int_0^\infty \frac{1}{\sigma_{pd}^2} \exp\left( -\frac{y}{\sigma_{pd}^2} \right) \prod_{i \in D_h(m)} \left( 1 - \exp\left( -\frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) \right) dy$$

$$\times \sum_{m = 1}^{2^{| D_h |} - 1} (-1)^{| D_h(m) |} \exp\left( -\sum_{i \in D_h(m)} \frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right) dy. \quad (A.4)$$

Finally, performing the integration of (A.4) yields

$$\Pr(\max x_i < \Lambda \gamma p + \Lambda) = 1$$

$$+ \sum_{m = 1}^{2^{| D_h |} - 1} (-1)^{| D_h(m) |} \exp\left( -\sum_{i \in D_h(m)} \frac{\Lambda}{\sigma_{id}^2} \right) \exp\left( -\sum_{i \in D_h(m)} \frac{\Lambda \gamma p + \Lambda}{\sigma_{id}^2} \right), \quad (A.5)$$

This completes the proof of (45) and (46).

APPENDIX B

PROOF OF (49) AND (50)

Given $D = D_h$, any SR within $D_h$ can be selected as the “best” relay for forwarding the source signal. Thus, using the 695 law of total probability, we have

$$\Pr\left( | h_{ie} |^2 > \Lambda \right) = \sum_{i \in D_h} \Pr\left( | h_{ie} |^2 > \Lambda, b = i \right)$$

$$= \sum_{i \in D_h} \Pr\left( | h_{ie} |^2 > \Lambda \right) \Pr(\max_{j \in D_h(i)} | h_{jd} |^2), \quad (B.1)$$

where in the first line, variable “$b$” stands for the best SR and the second equality is obtained from (13) and “$|$” represents the set difference. Noting that $| h_{ie} |^2$ is an exponentially distributed random variable with a mean of $\sigma_{ie}^2$, we obtain

$$\Pr\left( | h_{ie} |^2 > \Lambda \right) = \exp\left( -\frac{\Lambda}{\sigma_{ie}^2} \right). \quad (B.2)$$

Letting $| h_{jd} |^2 = x_j$ and $| h_{id} |^2 = y$, we have

$$\Pr\left( \max_{j \in D_h(i)} | h_{jd} |^2 < y \right)$$

$$= \int_0^y \frac{1}{\sigma_{jd}^2} \prod_{j \in D_h(i)} \left( 1 - \exp\left( -\frac{y}{\sigma_{jd}} \right) \right) dy.$$

(B.3)

wherein

$$\prod_{j \in D_h(i)} \left( 1 - \exp\left( -\frac{y}{\sigma_{jd}} \right) \right) = 1$$

$$+ \sum_{m = 1}^{2^{| D_h(i) |} - 1} (-1)^{| C_n(m) |} \exp\left( -\sum_{j \in C_n(m)} \frac{y}{\sigma_{jd}} \right), \quad (B.4)$$

where $| D_h(i) |$ denotes the cardinality of the set $D_h$ and $C_n(m)$ represents the $m$-th non-empty subset of “$D_h - \{i\}$”. Combining (B.3) and (B.4), we obtain

$$\Pr\left( \max_{j \in D_h(i)} | h_{jd} |^2 < y \right) = 1$$

$$+ \sum_{m = 1}^{2^{| D_h(i) |} - 1} (-1)^{| C_n(m) |} \left( 1 + \sum_{j \in C_n(m)} \frac{\sigma_{jd}^2}{\sigma_{jd}^2} \right)^{-1}. \quad (B.5)$$
Substituting (B.2) and (B.5) into (B.1) gives (B.6), shown at 707 the bottom of the page, which is (49). Similarly to (B.1), we 708 can rewrite \( \text{Pr}( |h_{he}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) \) as

\[
\text{Pr}( |h_{ie}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \sum_{i \in \mathcal{D}_h} \text{Pr}( |h_{ie}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) \\
\times \text{Pr}( \max_{j \in \{\mathcal{D}_h \setminus i\}} |h_{jd}|^2 < |h_{id}|^2 ), \quad (B.7)
\]

709 Since the random variables \( |h_{id}|^2 \) and \( |h_{pe}|^2 \) are independently 710 and exponentially distributed with respective means of \( \sigma_{ie}^2 \) and \( \sigma_{pe}^2 \), we readily arrive at

\[
\text{Pr}( |h_{ie}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \frac{\sigma_{ie}^2}{\sigma_{pe}^2 \gamma_p \Lambda + \sigma_{ie}^2} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right). \quad (B.8)
\]

712 Substituting (B.5) and (B.8) into (B.7) gives (B.9), shown at the 713 bottom of the page, which is (50).

**APPENDIX C**

**PROOF OF (53) AND (54)**

714 Upon introducing the notation of \( X = \sum_{i \in \mathcal{D}_h} |h_{id}|^2 \) and \( Y = \sum_{i \in \mathcal{D}_h} |h_{pe}|^2 \), we can rewrite the terms \( \text{Pr}( \sum_{i \in \mathcal{D}_h} |h_{id}|^2 < \Lambda) \) and \( \text{Pr}( \sum_{i \in \mathcal{D}_h} |h_{id}|^2 < \gamma_p \Lambda |h_{pe}|^2 + \Lambda) \) as \( \text{Pr}(X < \Lambda) \) and \( \text{Pr}(X < \gamma_p \Lambda + \Lambda) \), respectively. Noting that the fading coefficients of 720 all SR-SD channels, i.e. \( |h_{id}|^2 \) for \( i \in \{1, 2, \ldots, N\} \), are assumed 721 to be i.i.d., we obtain the probability density function (PDF) of 722 \( X = \sum_{i \in \mathcal{D}_h} |h_{id}|^2 \) as

\[
f_X(x) = \frac{1}{\Gamma(|\mathcal{D}_h|) \sigma_d^{2|\mathcal{D}_h|}} x^{(2|\mathcal{D}_h|)-1} \exp \left( -\frac{x}{\sigma_d^2} \right), \quad (C.1)
\]

723 where \( \sigma_d^2 = E(|h_{pd}|^2) \). Meanwhile, the random variable \( Y = \sum_{i \in \mathcal{D}_h} |h_{pe}|^2 \) is exponentially distributed and its PDF is given by

\[
f_Y(y) = \frac{1}{\sigma_{pd}^2} \exp \left( -\frac{y}{\sigma_{pd}^2} \right), \quad (C.2)
\]

where \( \sigma_{pd}^2 = E(|h_{pd}|^2) \). Using (C.1), we arrive at

\[
\text{Pr}(X < \Lambda) = \int_0^\Lambda \frac{1}{\Gamma(|\mathcal{D}_h|) \sigma_d^{2|\mathcal{D}_h|}} x^{(2|\mathcal{D}_h|)-1} \exp \left( -\frac{x}{\sigma_d^2} \right) dx
\]

\[
= \frac{\Lambda^{2|\mathcal{D}_h|-1}}{\Gamma(|\mathcal{D}_h|) \sigma_d^{2|\mathcal{D}_h|}} \exp(-\Lambda)\int_0^\Lambda dt (C.3)
\]

where the second equality is obtained by substituting \( \frac{x}{\sigma_d^2} = t \) and 726 \( \Gamma(a, b) = \int_0^1 t^{a-1} e^{-bt} \exp(-t)dt \) is known as the incomplete Gamma 727 function. Additionally, considering that the random variables \( X \) and \( Y \) are independent of each other, we obtain \( \text{Pr}(X < \gamma_p \Lambda + \Lambda) \) as

\[
\text{Pr}(X < \gamma_p \Lambda + \Lambda) = \int_0^\Lambda f_X(x)dx
\]

\[
+ \int_\Lambda^\infty \int_{\gamma_p x}^\infty f_X(x) f_Y(y) dy dx. \quad (C.4)
\]

Substituting \( f_X(x) \) and \( f_Y(y) \) from (C.1) and (C.2) into (C.4) 731 yields

\[
\text{Pr}(X < \gamma_p \Lambda + \Lambda) = \int_0^\Lambda \frac{\Lambda}{\sigma_d^2 |\mathcal{D}_h|} \exp \left( -\frac{x}{\sigma_d^2} \right) dx
\]

\[
+ \int_\Lambda^\infty e^{1/2(\sigma_{pd}^2 \gamma_p A)^2/2|\mathcal{D}_h|} \exp \left( -\frac{x}{\sigma_{pd}^2} \right) \left(1 + \frac{x}{\sigma_{pd}^2 \gamma_p A}\right)^{-1/2(\sigma_{pd}^2 \gamma_p A)} dx
\]

\[
= \int_\Lambda^\infty \left[1 - \Gamma \left( \frac{\Lambda}{\sigma_d^2 |\mathcal{D}_h|} \right) \left(1 + \frac{\Lambda}{\sigma_d^2 \gamma_p A} \right)^{-1/2(\sigma_{pd}^2 \gamma_p A)} \right] dx \quad (C.5)
\]

where the second equality is obtained by using \( \frac{x}{\sigma_d^2} + \frac{x}{\sigma_{pd}^2 \gamma_p A} = t \). Hence, we have completed the proof of (53) and (54) as (C.3) 734 and (C.5), respectively.

\[
\text{Pr}( |h_{he}|^2 > \Lambda) = \sum_{i \in \mathcal{D}_h} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right) \left[1 + \sum_{m=1}^{2|\mathcal{D}_h|-1} (-1)^{G_m(\Lambda)(m)} \left(1 + \sum_{j \in G_m(\Lambda)} \frac{\sigma_{id}^2}{\sigma_{jd}^2} \right)^{-1}\right] \quad (B.6)
\]

\[
\text{Pr}( |h_{he}|^2 > \Lambda |h_{pe}|^2 \gamma_p + \Lambda) = \sum_{i \in \mathcal{D}_h} \frac{\sigma_{ie}^2}{\sigma_{pe}^2 \gamma_p \Lambda + \sigma_{ie}^2} \exp \left( -\frac{\Lambda}{\sigma_{ie}^2} \right) \left[1 + \sum_{m=1}^{2|\mathcal{D}_h|-1} (-1)^{G_m(\Lambda)(m)} \left(1 + \sum_{j \in G_m(\Lambda)} \frac{\sigma_{id}^2}{\sigma_{jd}^2} \right)^{-1}\right] \quad (B.9)
\]
REFERENCES


Benoit Champagne (S’87–M’89–SM’03) was born in Joliette (PQ), Canada, in 1961. He received the B.Ing. degree in engineering physics and the M.Sc. degree in physics from the University of Montreal in 1983 and 1985, respectively, and the Ph.D. degree in electrical engineering from the University of Toronto in 1990. From 1990 to 1999, he was with INRS, University of Quebec, where he held the positions of Assistant and then Associate Professor. In 1999, he joined McGill University, Montreal, as an Associate Professor with the Department of Electrical and Computer Engineering. He served as Associate Chairman of Graduate Studies in the Department from 2004 to 2007 and is now a Full Professor. His research interests focus on the investigation of new computational algorithms for the digital processing of information bearing signals and overlap many sub-areas of statistical signal processing, including: detection and estimation, sensor array processing, adaptive filtering, multirate systems, and applications thereof to broadband voice and data communications. Over the years, he has supervised many graduate students in these areas and co-authored several papers, including key works on subspace tracking, speech enhancement, time delay estimation and spread sources localization.

Wei-Ping Zhu (SM’97) received the B.E. and M.E. degrees from Nanjing University of Posts and Telecommunications, and the Ph.D. degree from Southeast University, Nanjing, China, in 1982, 1985, and 1991, respectively, all in electrical engineering. He was a Postdoctoral Fellow from 1991 to 1992 and a Research Associate from 1996 to 1998 with the Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada. During 1993–1996, he was an Associate Professor with the Department of Information Engineering, Nanjing University of Posts and Telecommunications. From 1998 to 2001, he worked with hi-tech companies in Ottawa, Canada, including Nortel Networks and SR Telecom Inc. Since July 2001, he has been with Concordia’s Electrical and Computer Engineering Department as a full-time faculty member, where he is presently a Full Professor. His research interests include digital signal processing fundamentals, speech and audio processing, and signal processing for wireless communication with a particular focus on MIMO systems and cooperative relay networks.

Dr. Zhu was an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART I: Fundamental Theory and Applications from 2001 to 2003, and an Associate Editor of Circuits, Systems and Signal Processing from 2006 to 2009. He was also a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issues of: Broadband Wireless Communications for High Speed Vehicles, and Virtual MIMO during 2011–2013. Since 2011, he has served as an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS PART II: Express Briefs. Dr. Zhu was the Secretary of Digital Signal Processing Technical Committee (DSPTC) of the IEEE Circuits and System Society during 2012–2014, where he is presently the Chair of the DSPTC.

Lajos Hanzo received the degree in electronics in 1976 and the doctorate in 1983. In 2009 he was awarded “Doctor Honoris Causa” by the Technical University of Budapest. During his 37-year career in telecommunication he has held various research and academic posts in Hungary, Germany, and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised 80+ Ph.D. students, co-authored 20 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10,000 pages, published 1,400+ research entries at IEEE Xplore, acted both as TPC and General Chair of 90+ IEEE conferences, presented keynote lectures and has been awarded a number of 940 distinctions. Currently he is directing a 100-strong academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Council’s Advanced Fellow Grant and the Royal Society’s Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of 946 industrial courses. He is also a Governor of the IEEE VTS. During 2008–2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also at Tsinghua University, Beijing. His research is funded by the European Research Council’s Senior Research Fellow Grant. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk Lajos has 20,000+ citations.
AUTHOR QUERY

NO QUERY.