# Relay Selection for Secure Cooperative Networks with Jamming

Ioannis Krikidis, *Member, IEEE,* John S. Thompson, *Member, IEEE,*
and Steve McLaughlin, *Senior Member, IEEE*

***Abstract*—This paper deals with relay selection in cooperative networks with secrecy constraints. The proposed scheme enables an opportunistic selection of two relay nodes to increase security against eavesdroppers. The first relay operates as a conventional mode and assists a source to deliver its data to a destination via a Decode-and-Forward strategy. The second relay is used in order to create intentional interference at the eavesdropper nodes. The proposed selection technique jointly protects the primary destination against interference and eavesdropping and jams the reception of the eavesdropper. The new approach is analyzed for different complexity requirements based on instantaneous and average knowledge of the eavesdropper channels. In addition an investigation of an hybrid security scheme which switches between jamming and non-jamming protection is discussed in the paper. It is proven that an appropriate application of these two modes further improves security. The enhancements of the proposed selection techniques are demonstrated analytically and with simulation results.**

***Index Terms*—Cooperative diversity, secure communications, wire-tap channel, relay selection.**

## I. Introduction

DUE to the broadcast nature of the wireless medium, all users which are in the coverage area of a transmission can overhear the source message. The capability to communicate confidential messages and the related protection of a communication link against possible eavesdroppers is of increasing importance. Information privacy in wireless networks has traditionally been the domain of the higher layers of the protocol stack via the use of cryptographically secure schemes [1]. However, as the implementation of secrecy at higher layers becomes the subject of increasing potential attacks, there has been a growing of interest in implementing security at the physical (PHY) layer as well [2]-[6].

The main objective of these techniques is to boost the capacity of the primary (confidential) links by decreasing simultaneously the capacity of the eavesdropper links. To achieve this target, several PHY-based approaches have been proposed in the literature. In [7] a joint design of power control and channel-based scheduling was derived in order to protect the primary link against collaborative and non-collaborative eavesdropper configurations. In [8], [9] channel-based beamforming techniques ensure security by adapting transmission to the direction of the destination. The interaction of the cooperative diversity concept [10]-[12] with secret communications has also recently been reported as an interesting solution [13]-[15]. In these systems a relay node located closer to the main destination provides a higher capacity to the main link than the eavesdropper link [13]. With this in mind, relay selection for cooperative networks with secrecy constraints has emerged as an interesting research topic. In our previously reported work [16], some relay selection metrics have been proposed with different levels of feedback overhead. Alternatively, jamming techniques which produce an artificial interference at the eavesdropper node in order to reduce the capacity of the related link seem to be an interesting approach for practical applications [17]-[19]. In [20] the interaction between relay and jammer is introduced as a non-cooperative game where both nodes have conflicting objectives and the Nash equilibrium (NE) of the system is derived.

This paper offers an extension of the work presented in [16] for cooperative ad-hoc environments with jamming. In contrast to [16], where only one relay node is selected to ensure security, here, the problem considered involves the selection of a relay and a jammer node. The relay node uses a Decode-and-Forward (DF) strategy in order to assist the source to deliver data to its destination. On the other hand, the jammer node transmits simultaneously with the relaying link in order to create artificial interference in order to degrade the eavesdropper links. The principal question here is how to select the relay and the jammer node in order to increase *perfect security* and protect the source message against eavesdroppers. In contrast to [18] and [19], we assume that the destination cannot mitigate artificial interference and thus decoding is subject to interference. This assumption overcomes the risk for an eavesdropper to track the jamming signal (i.e. during an initialization period) and provides a higher degree of protection. An appropriate selection of the relay and jammer nodes by taking into account the corresponding secret capacity expression, is proposed. The selected relay increases the perfect secrecy of the relaying link and the selected jammer increases interference at the eavesdropper node while simultaneously protecting the primary destination from interference. The new approach is analyzed under two different complexity constraints which correspond to (i) global instantaneous knowledge of all links and (ii) average knowledge of the eavesdropper links. Theoretical and numerical results reveal that jamming techniques significantly outperform previously reported approaches for scenarios with strong eavesdropper channels. In addition to the investigation of these jamming-based selection techniques, we show that jamming is not always beneficial for security. Motivated by this observation, an intelligent method for switching between jamming and non-jamming relay selection is proposed. Such hybrid schemes overcome jamming limitations and seem to be efficient solutions for practical application with critical secrecy constraints.

The paper is organized as follows. Section II introduces the

Manuscript received March 5, 2009; revised May 13, 2009; accepted July 11, 2009. The associate editor coordinating the review of this paper and approving it for publication was W. Choi.

The authors are with the Institute for Digital Communications, University of Edinburgh, EH9 3JL, UK (e-mail: {i.krikidis, john.thompson, steve.mclaughlin}@ed.ac.uk).

Digital Object Identifier 10.1109/TWC.2009.090323

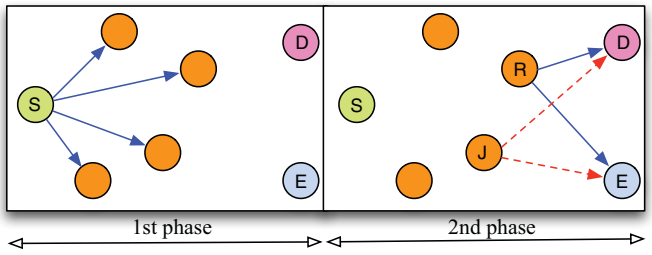


Fig. 1. The system model and the related communication scenario (the source-destination link is blocked and communication is performed via relays).

system model and presents the problem under consideration. Section III presents the proposed selection techniques and introduces their hybrid implementations. Numerical results are shown and discussed in Section IV, followed by concluding remarks in Section V.

## II. System Model and Problem Formulation

We assume a simple configuration consisting of one source $S$, one destination $D$, one eavesdropper $E$ and a relay set $S_{\text{relay}} = \{1, 2, \ldots, K\}$ with $K$ DF relays. Fig. 1 schematically presents the system model. Relays cannot transmit and receive simultaneously and therefore communication is performed in two orthogonal channels. During the broadcasting phase, the source transmits its data and the relays which can successfully decode the source signal form a decoding set $C_d \subseteq S_{\text{relay}}$ [1]. In the cooperative phase and according to the security protocol, two selected relays transmit towards the destination and the eavesdropper. The first relay $R$ operates a conventional relay mode, belongs to the subset $C_d$ and forwards the source message in order to assist the source to deliver its message to the destination. On the other hand, the second relay $J$ operates a "jammer mode", so does not need to decode the source signal, and is used in order to generate intentional interference to the relaying transmission. The main destination $D$ is not able to mitigate the artificial interference from the jammer node (interference is unknown at the destination) and refers to applications with critical secrecy constraints. In order to focus our study on the relaying link, which is the link of interest, we assume that the direct links ($S \to D$, $S \to E$) are not available and therefore security concerns only the cooperative channel. This assumption can be justified as follows:

- *Non-direct links:* The direct links $S \to D$ and $S \to E$ are not available (deep fading) and thus communication is performed via the relay nodes. This topology assumption follows the description in [11], [21] where the direct path between the source and destination (also source and eavesdropper in our case) is blocked by an obstruction, while relays are located at the periphery of the obstacle (around-the-corner).
- *Secure broadcast phase:* The cooperative protocol is performed in two separated orthogonal channels (i.e. frequencies or time slots), while the eavesdropper cannot overhear the broadcast channel but only the cooperative channel [15].
- *Clustered applications:* The source and the relays are located in the same cluster, while destination and eavesdropper are located outside the cluster. The source node broadcasts its message locally to the other nodes of the cluster with a small amount of power and therefore the information rate at the eavesdropper can be ignored [8].
- *Motivation:* The main objective of this paper is the investigation of relay/jammer selection criteria for cooperative systems with secrecy constraints. The considered set-up concentrates our study on the cooperative channel, where relay selection is performed, and clearly reveals its impact on the system secrecy [8]. The considered topology significantly simplifies the theoretical analysis and allows closed form solutions. However, the generalization of the proposed schemes to scenarios with direct links is straightforward (Section III.G highlights this generalization).

A slow, flat, block Rayleigh fading environment is assumed, where the channel remains static for one coherence interval (one slot) and changes independently in different coherence intervals with a variance $\sigma_{i,j}^2 = d_{i,j}^{-\beta}$, where $d_{i,j}$ is the Euclidean distance between terminals $i$ and $j$, and $\beta$ is the path-loss exponent. Furthermore, additive white Gaussian noise (AWGN) is assumed with zero mean and unit variance. The instantaneous secrecy capacity for a decoding set $C_d$ is written as [13]

$$C_S^{(|C_d|)}(R,J) = \begin{cases} 0 & \text{if } |C_d| = 0, \\ \left[\frac{1}{2}\log_2\left(1+\frac{\gamma_{R,D}}{1+\gamma_{J,D}}\right) \right. & \\ \left. -\frac{1}{2}\log_2\left(1+\frac{\gamma_{R,E}}{1+\gamma_{J,E}}\right)\right]^+ & \text{if } |C_d| > 0, \end{cases} \quad (1)$$

where $R \in C_d$ and $J \in S_{\text{relay}}$, $\gamma_{i,j} \triangleq P^{(i)}|f_{i,j}|^2$ is the instantaneous signal-to-noise ratio (SNR) for the link $i \to j$, $P^{(i)}$ denotes the transmitted power for $i$-th node, $f_{i,j}$ is the channel coefficient for the link $i \to j$ modeled as a zero-mean, independent, circularly-symmetric complex Gaussian random variable with variance $\sigma_{i,j}^2$, $[x]^+ \triangleq \max\{0, x\}$ and $|\mathcal{F}|$ denotes the cardinality of a set $\mathcal{F}$. In order to protect the destination from the artificial interference and maximize the benefits of the proposed scemes, the jammer node transmits with a lower power than the relay nodes and thus its transmitted power is defined as $P^{(J)} = P^{(R)}/L$ (with $P^{(S)} = P^{(R)}$), where $L \gg 1$ denotes the ratio of the relay power to the jammer power. Our objective is to select the nodes $R, J$ in order to maximize secrecy capacity for different types of channel feedback [22]. We note that although the node $R$ must belong to the decoding set $C_d$ due to the DF policy, the node $J$ can be any node of the set $S_{\text{relay}}$ as it does not require to decode the source message. If the secrecy performance of the system is characterized by the secrecy outage probability, which is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R_S > 0$ [6], the considered optimization problem

[1] $k \in C_d$ if $C_{S,k} > R_0$, where $C_{S,k}$ is the instantaneous capacity of the $S \to k$ link and $R_0$ is the transmission rate.

is formulated as

$$\mathbb{P}\{C_S < R_S\} = \sum_{k=0}^{K} \mathbb{P}\{|C_d| = k\}\mathbb{P}\{C_S^{(k)}(R,J) < R_S\}, \quad (2)$$

$$(R^*, J^*) = \arg \min_{\substack{R\in C_d,\\ J\in S_{\text{relay}},\\ R\neq J}} \mathbb{P}\{C_S < R_S\} \quad (3)$$

$$\text{s.t. } \Psi_i \quad (\text{for } i = 0, 1),$$

where $R^*$, $J^*$ denote the selected relay and jammer, respectively, $\mathbb{P}$ denotes probability, $\Psi_0 = \{\gamma_{k,D}, \gamma_{k,E}\}$, $\Psi_1 = \{\gamma_{k,D}, \mathbb{E}[\gamma_{k,E}]\}$ with $k \in S_{\text{relay}}$ are the feedback knowledge sets; $\mathbb{E}[\cdot]$ stands for the expectation operator, $\Psi_0$ denotes a global instantaneous knowledge for all the links and $\Psi_1$ denotes an average channel knowledge for the eavesdropper links. For high SNRs, all the relay nodes can decode the source message ($\mathbb{P}\{|C_d| = |S_{\text{relay}}| = K\} = 1$) and therefore the optimization problem is simplified by considering the outage probability $\mathbb{P}\{C_S < R_S\} = \mathbb{P}\{C_S^{(K)}(R,J) < R_S\}$. In this work, we deal with the high SNR regime, where the above simplified version of the considered optimization problem, is applied [8].

Regarding the adopted performance metric, the outage secrecy probability is a well-known criterion to evaluate secrecy protocols [6], [18], [23]. It is an appropriate design metric when a fixed (Wyner) code chosen in advance is used for all channel conditions. However, the practical suitability of this metric is beyond the scope of this paper and can be found in [23] (code construction based on secrecy outage probability).

### A. Selection techniques without jamming

The first category of solutions does not involve a jamming process and therefore only a conventional relay accesses the channel during the second phase of the protocol. The existing solutions are summarized as follows:

*1) Conventional selection (CS):* This solutions does not take into account the eavesdropper channels and the relay node is selected based on the instantaneous quality of the $S \to D$ links (reactive protocol in [11]). Although it is an effective solution for non-eavesdropper environments, it cannot support systems with secrecy constraints. The conventional selection is written as

$$R^* = \arg \max_{R\in C_d} \{\gamma_{R,D}\}. \quad (4)$$

*2) Optimal selection (OS):* The optimal selection scheme takes into account the relay-eavesdroppers links and decides the relay node based on the knowledge set $\Psi_0$. The optimal selection maximizes the perfect secrecy capacity and is given as [16]

$$R^* = \arg \max_{R\in C_d} \left\{\frac{\gamma_{R,D}}{\gamma_{R,E}}\right\}. \quad (5)$$

*3) Suboptimal selection (SS):* The suboptimal selection consists of a practical implementation of the optimal selection as it avoids the instantaneous estimate of the relay-eavesdropper links by deciding the appropriate relay based on the knowledge set $\Psi_1$. It is a solution which efficiently fills the gap between optimal and conventional selection with a low implementation/complexity overhead. The suboptimal selection is expressed as [16]

$$R^* = \arg \max_{R\in C_d} \left\{\frac{\gamma_{R,D}}{\mathbb{E}[\gamma_{R,E}]}\right\}. \quad (6)$$

## III. Selection Techniques for Jamming

In this Section, we present an extension to the above eavesdropper-based relay selection approaches for systems with jamming. We deal with the complete optimization problem given in Eq. (2) and we study the interaction between relay and jammer selection. A set of new selection schemes is investigated which are analyzed in the following subsections.

### A. Optimal selection with jamming (OSJ)

The optimal selection with jamming assumes a knowledge set $\Psi_0$ and ensures a maximization of the instantaneous secrecy capacity given in Eq. (1). The selection policy which maximizes Eq. (1) and therefore minimizes the secrecy outage probability is given as

$$\begin{aligned}(R^*, J^*) &= \arg \max_{\substack{R\in C_d,\\ J\in S_{\text{relay}},\\ R\neq J}} \left\{C_S^{(|C_d|)}(R,J)\right\} \\ &= \arg \max_{\substack{R\in C_d,\\ J\in S_{\text{relay}},\\ R\neq J}} \left\{\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{R,D}}{1+\gamma_{J,D}}}{1+\frac{1+\gamma_{R,E}}{\gamma_{J,E}}}\right)\right\} \\ &= \arg \max_{\substack{R\in C_d,\\ J\in S_{\text{relay}},\\ R\neq J}} \left\{\frac{1+\frac{\gamma_{R,D}}{1+\gamma_{J,D}}}{1+\frac{1+\gamma_{R,E}}{\gamma_{J,E}}}\right\}. \end{aligned} \quad (7)$$

The direct application of Eq. (7) for all the available relays solves the optimization problem. However, this solution requires a large number of comparisons (computations) which significantly increases with the number of the relays (complexity $\mathrm{O}(K^2)$). A simpler selection policy can be proposed based on the following secrecy capacity approximation. More specifically, Eq. (7) can be simplified as

$$\begin{aligned}(R^*, J^*) &\simeq \arg \max_{\substack{R\in C_d,\\ J\in S_{\text{relay}},\\ R\neq J}} \left\{\frac{\gamma_{R,D}}{\gamma_{J,D}}\frac{\gamma_{R,E}}{\gamma_{J,E}}\right\} \quad (\text{see Appendix A}) \\ &\Rightarrow \begin{cases} R^* = \arg\max_{R\in C_d}\left\{\frac{\gamma_{R,D}}{\gamma_{R,E}}\right\} \\ J^* = \arg\min_{J\in\{S_{\text{relay}}-R^*\}}\left\{\frac{\gamma_{J,D}}{\gamma_{J,E}}\right\} \end{cases} \\ &= \begin{cases} J^* = \arg\min_{J\in\{S_{\text{relay}}\}}\left\{\frac{\gamma_{J,D}}{\gamma_{J,E}}\right\} \\ R^* = \arg\max_{R\in\{C_d-J^*\}}\left\{\frac{\gamma_{R,D}}{\gamma_{R,E}}\right\} \end{cases} \end{aligned} \quad (8)$$

With regard to the relay and the eavesdropper nodes, the relay selection tries to maximize the ratio $\gamma_{k,D}/\gamma_{k,E}$, while the jammer tries to minimize the same function, consequently the selection policy is independent of the selection order and will alway select different relay terminals. As far as the complexity is concerned, the simplified OSJ policy has a complexity $\mathrm{O}(K)$ and does not require algebraic computations.

*Asymptotic performance for a symmetric configuration:* For high SNRs, all nodes can decode the source signal

and thus can be selected as either relay or jammer nodes ($|C_d| = |S_{\text{relay}}| = K$). In order to simplify the presentation for the asymptotic (high SNRs) analysis of OSJ, we assume a *symmetric clustered configuration* where the $K$ relays are clustered relatively closely together and have equivalent distances to the destination and the eavesdropper, respectively. This assumption provides average SNRs equal to $\mathbb{E}[\gamma_{R,D}] = \mathbb{E}[\gamma_{R,E}] = P^{(R)}\sigma^2$ for the relay-(destination, eavesdropper) links and $\mathbb{E}[\gamma_{J,D}] = \mathbb{E}[\gamma_{J,E}] = P^{(J)}\sigma^2$ for the jammer-(destination, eavesdropper) links, where $\sigma^2$ denotes the variance of the channel coefficients. We recall that the jammer and the relay nodes transmit with a different average power which results in different average SNRs. According to Appendix A, for high SNRs, the secrecy outage probability for this case converges to

$$P_{\text{OSJ}} = \frac{\rho^K}{2^K - (1+\rho)^K}\left(\frac{1}{\rho} - 1\right), \tag{9}$$

where $\rho = 2^{2R_S}$. The generalization of this result for an asymmetric configuration is straightforward and follows the same method presented in Appendix A.

### B. Optimal switching (OW)

From Eq. (1), the jammer node, in addition to the useful interference that it introduces on the relay-eavesdropper link, simultaneously degrades the relaying link. Based on the assumption that the destination cannot mitigate this artificial interference, continuous jamming is not always beneficial for the system. More specifically, for some operational scenarios, (i.e. jammer is close to the destination), the continuous use of jamming decreases secrecy and acts as a bottleneck for the system. In order to overcome this limitation, we propose intelligent switching between optimal selection with jamming and optimal selection without jamming. The proposed hybrid selection scheme overcomes problems of "negative jamming" which leads to excessive interference and is introduced as the optimal general solution for the problem under consideration. The required condition for the participation of the jammer node is

$$C_S^{(|C_d|)}(R,J) > \underbrace{\left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{R,D}}{1+\gamma_{R,E}}\right)\right]^+}_{\text{secrecy capacity without jamming-OS}}, \tag{10}$$

For high SNRs and based on an appropriate power allocation (see Appendix A), the secrecy capacity for the OSJ and OS schemes can be simplified and therefore Eq. (10) can be written as follows

$$\underbrace{\left[\frac{1}{2}\log_2\left(\frac{\gamma_{R,D}\gamma_{J,E}}{\gamma_{R,E}\gamma_{J,D}}\right)\right]^+}_{\text{secrecy capacity of OSJ (Appendix A)}} > \underbrace{\left[\frac{1}{2}\log_2\left(\frac{\gamma_{R,D}}{\gamma_{R,E}}\right)\right]^+}_{\text{secrecy capacity without jamming-OS}}$$
$$\Rightarrow \gamma_{J,E} > \gamma_{J,D} \Rightarrow \frac{\gamma_{J,D}}{\gamma_{J,E}} < 1. \tag{11}$$

The above condition shows that jamming is useful only when the "positive interference" (interference at $E$) is higher than "negative interference" (interference at $D$). As a knowledge set $\Psi_0$ is assumed for the decision, the implementation of the hybrid scheme corresponds to a direct application of the above channel-based condition. In the case of a symmetric configuration (same average SNR for all $R \to D, E$ and $J \to D, E$ links), the probability of switching is written as

$$\overline{P}_{\text{OW}} = \mathbb{P}(\text{switching from OSJ to OS}) = \frac{1}{2^{K-1}}, \tag{12}$$

where the proof of the above expression can be found in Appendix B. The above expression shows that for a clustered relay configuration, the probability of switching is decreased as the number of relays is increased ($\overline{P}_{\text{OW}} \to 0$ as $K \to \infty$).

### C. Suboptimal selection with jamming (SSJ)

Although the assumption $\Psi_0$ provides some optimal selection metrics, its practical interest is limited to some special applications, (e.g. military applications), where appropriate protocols measure the instantaneous quality of the relay-eavesdropper links when eavesdroppers act as sources. However, in practice, only an average knowledge of these links would be available from long-term supervision of the eavesdropper transmission. This suboptimal technique is a translation of perfect selection with jamming when knowledge feedback set $\Psi_1$ is available. It corresponds to the selection metric

$$\begin{aligned} R^* &= \arg\max_{R\in C_d}\left\{\frac{\gamma_{R,D}}{\mathbb{E}[\gamma_{R,E}]}\right\}, \\ J^* &= \arg\min_{J\in\{S_{\text{relay}}-R^*\}}\left\{\frac{\gamma_{J,D}}{\mathbb{E}[\gamma_{J,E}]}\right\}. \end{aligned} \tag{13}$$

*Asymptotic performance for a symmetric configuration:* As with the perfect selection metric, in order to simplify the analysis of the proposed scheme, a symmetric configuration with equivalent average channels is assumed. According to Appendix C, for high SNRs, the outage probability for suboptimal jamming converges to

$$P_{\text{SSJ}} = 1 + (K-1)\sum_{k=1}^{K}\binom{K}{k}(-1)^k\frac{K-1-k\rho+k\rho\ln\left(\frac{k\rho}{K-1}\right)}{(K-1-k\rho)^2}, \tag{14}$$

where $\rho = 2^{2R_S}$.

### D. Suboptimal switching (SW)-bound

Motivated by the fact that jamming is not always a positive process for the secrecy of the system, we introduce an hybrid protocol which switches between suboptimal selection with jamming and suboptimal selection without jamming. Firstly, and for comparison reasons, we assume that although the relay and jammer nodes are selected based on the suboptimal selection with jamming criterion, the switching is performed based on Eq. (11). The corresponding protocol corresponds to the "best" suboptimal switching and is used as a reference scheme in our simulation results.

### E. Suboptimal switching (SW)

This scheme refers to the practical application of the above suboptimal switching. The basic idea is the same but the switching criterion uses also the available set $\Psi_1$. More

specifically, the required condition for switching from SSJ to SS mode, is written as

$$C_S'^{(|C_d|)}(R,J) > \left[\frac{1}{2}\log_2\left(\frac{1+\gamma_{R,D}}{1+\mathbb{E}[\gamma_{R,E}]}\right)\right]^+$$
$$\Rightarrow \left[\frac{1}{2}\log_2\left(\frac{\gamma_{R,D}}{\mathbb{E}[\gamma_{R,E}]}\frac{\mathbb{E}[\gamma_{J,E}]}{\gamma_{J,D}}\right)\right]^+ > \left[\frac{1}{2}\log_2\left(\frac{\gamma_{R,D}}{\mathbb{E}[\gamma_{R,E}]}\right)\right]^+$$
$$\Rightarrow \mathbb{E}[\gamma_{J,E}] > \gamma_{J,D} \Rightarrow \mathbb{E}[\gamma_{J,D}] > \gamma_{J,D}. \quad (15)$$

In a manner equivalent to the previous subsections, the probability of switching for a symmetric configuration simplifies to

$$\overline{P}_{\text{SW}} = \mathbb{P}(\text{switching from SSJ to SS}) = \mathbb{P}\{\gamma_{J,D} > \mathbb{E}[\gamma_{J,D}]\}$$
$$= \int_{\mathbb{E}[\gamma_{J,D}]}^{\infty}(K-1)\frac{1}{\mathbb{E}[\gamma_{J,D}]}\exp\left(-\frac{[K-1]y}{\mathbb{E}[\gamma_{J,D}]}\right)dy$$
$$= \exp(-[K-1]), \quad (16)$$

where for the above expression we have used order statistics theory, (select the minimum among $K-1$ independent and identically distributed (i.i.d.) exponential distributed random variables) [24]. The above expression shows that as the number of relays is increased, the probability of switching is decreased.

### F. Optimal selection with "controlled" jamming (OSCJ)

This paper deals with a noise-forwarding scheme where the jamming signal is unknown at both destination and eavesdropper nodes. This assumption avoids initialization time periods, where the source communicates with the destination in order to define a jamming sequence, and refers to systems with high secrecy constraints. For comparison reasons, in this subsection, we present a noise-forward scheme, where the jamming signal can be decoded at the destination but not at the eavesdropper node [19]. In this case, the secrecy capacity expression given in Eq. (1) is modified as follows

$$C_S^{(|C_d|)}(R,J) = \left[\frac{1}{2}\log_2(1+\gamma_{R,D}) - \frac{1}{2}\log_2\left(1+\frac{\gamma_{R,E}}{1+\gamma_{J,E}}\right)\right]^+ \quad (\text{for } |C_d|>0) \quad (17)$$

Accordingly, the selection policy which solves the considered optimization problem is simplified to

$$R^* = \arg\max_{R\in C_d}\left\{\frac{\gamma_{R,D}}{\gamma_{R,E}}\right\},$$
$$J^* = \arg\max_{J\in\{S_{\text{relay}}-R^*\}}\{\gamma_{J,E}\} \quad (18)$$

The OSCJ scheme is taken into account in the numerical results section as a reference strategy. However, further analysis of the OSCJ is beyond the scope of this paper.

### G. Selection with direct links

All the above algorithms can be extended in a straightforward maner to scenarios with direct links and unsecured broadcast phases. In this case, although the selection policy for the second phase remains the same, the broadcast phase is supported by a jammer selection. During the source transmission, an appropriate selection of the jammer node can protect the source message. If a maximum ratio combiner (MRC) is used in order to combine the two transmissions at the destinations, the secrecy capacity given in Eq (1) is modified to

$$C_S^{(|C_d|)}(R,J) = \left[\log_2\left(1+\frac{\gamma_{S,D}}{1+\beta^{(1)}\gamma_{J,D}^{(1)}}+\frac{\gamma_{R,D}}{1+\beta^{(2)}\gamma_{J,D}^{(2)}}\right) - \log_2\left(1+\frac{\gamma_{S,E}}{1+\beta^{(1)}\gamma_{J,E}^{(1)}}+\frac{\gamma_{R,E}}{1+\beta^{(2)}\gamma_{J,E}^{(2)}}\right)\right]^+, \quad (19)$$

where $|C_d|>0$, $\gamma_{i,j}^{(t)}$ denotes the $i\to j$ link for the $t$-th communication phase and $\beta^{(t)}\in\{0,1\}$ is a binary variable used in order to take into account scenarios where the jammer node is not activated during the $t$-th phase (hybrid selection). By generalizing the previous results, the OW selection for the first communication phase gives

$$J^* = \arg\min_{J\in S_{\text{relay}}}\left\{\frac{\gamma_{J,D}^{(1)}}{\gamma_{J,E}^{(1)}}\right\}, \quad \beta^{(t)} = \begin{cases} 1, & \text{if } \gamma_{J^*,E}^{(t)} > \gamma_{J^*,D}^{(t)} \\ 0, & \text{elsewhere} \end{cases} \quad (20)$$

with $t\in\{1,2\}$, while the selection policy for the second communication phase ($t=2$) is similar to Section III.B. The selection policy for the SW scheme can be extended accordingly, by considering the variance of the $J\to E$ links.

## IV. Numerical Results

Computer simulations were carried out in order to validate the performance enhancements of the proposed selection schemes. The simulation environment follows the model of Section II and consists of a 2D square topology where the nodes $S$, $D$ and $E$ are located as $\{X_S,Y_S\}=\{0,0\}$, $\{X_D,Y_D\}=\{1,0\}$, $\{X_E,Y_E\}=\{0,0\}$ and the direct paths $S\to D$, $S\to E$ are blocked by an obstruction. This symmetric configuration focuses our study on the relaying links and has been introduced in [13] in order to reveal the secrecy benefits of relaying when the secrecy capacity for the direct links is zero. In order to support the assumption given in Eq. (21) and therefore to enable the simplified expression given in Appendix A, the relay and the jammer nodes transmit with a relay-jammer power ratio equal to $L=100$. The number of the relays is equal to $K=4$ and the relays are located randomly in the 2D space considered; their exact location is given for each example considered. The path-loss exponent is set to $\beta=3$, the area of the network is a $1\times 1$ unit square, the transmission spectral efficiency is equal to $R_0=2$ bits per channel use (BPCU) and the target secrecy rate is equal to $R_S=0.1$ BPCU. The performance metric is the secrecy outage probability but some results are also given in terms of ergodic secrecy capacity ($\mathbb{E}[C_S]$) . We note that outage probability is the adopted metric for this work, but for some applications the secrecy ergodic capacity is a more appropriate metric.

The first simulation results assume a scenario in which $K=4$ relays are located in the middle of the space and thus have comparable links with $D$ and $E$. Fig. 2 shows the considered topology. In Fig. 3, we plot the secrecy outage

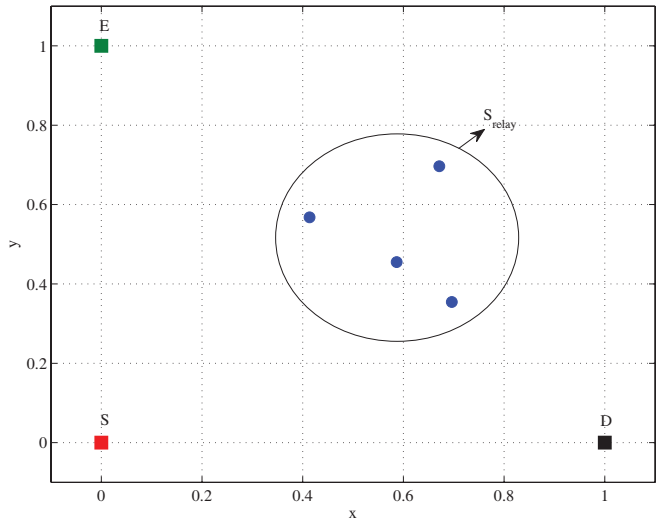


Fig. 2. The simulation environment with $K = 4$ relays, $\beta = 3$ and dimension $1 \times 1$ unit length.

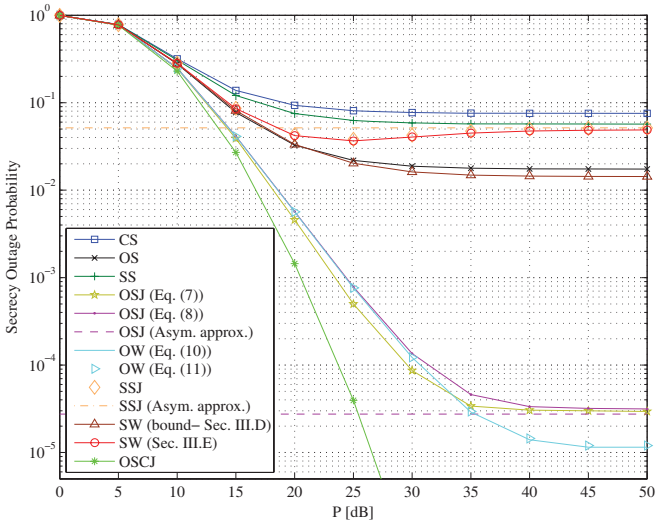


Fig. 3. Secrecy outage probability versus transmitted power $P$; $R_S = 0.1$ BPCU, $R_0 = 2$ BPCU

probability of the different selection techniques versus the transmitted power $P$ (where $P \triangleq P^{(R)} = P^{(S)}$). The considered selection schemes are: conventional selection (CS), optimal selection without jamming (OS), suboptimal selection without jamming (SS), optimal selection with jamming (OSJ), optimal switching (OW), suboptimal selection with jamming (SSJ), suboptimal switching (SW) and optimal selection with controlled jamming (OSCJ). The first important observation is that selection with jamming outperforms the corresponding non-jamming techniques. The integration of jamming in the optimal selection reduces the asymptotic secrecy outage probability to $3 \cdot 10^{-5}$ rather $2 \cdot 10^{-2}$ for the non-jamming case. This significant gain introduces jamming selection as an efficient technique to support secrecy constraints and it is a practical way to achieve lower secrecy outage probabilities (due to the convergence behavior of the OSJ scheme, letting the SNR$\rightarrow \infty$ does not decrease the secrecy outage probability). The integration of jamming also improves the suboptimal selection protocols (based on average channel knowledge); the

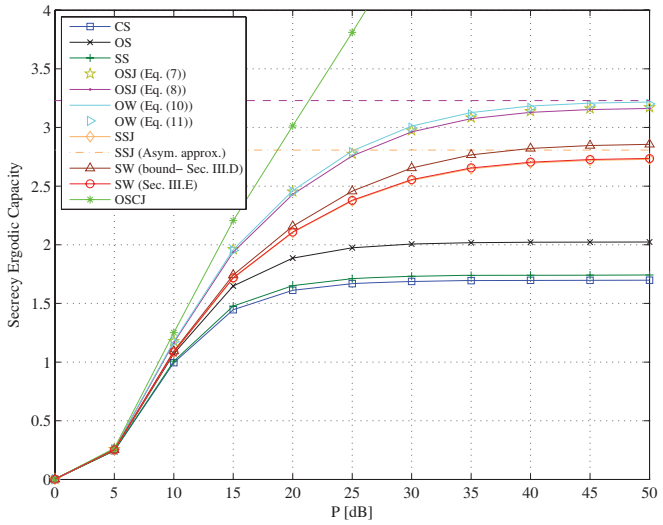


Fig. 4. Secrecy ergodic capacity versus $P$ for the different selection schemes.

outage probability for the SSJ scheme converges to $5 \cdot 10^{-2}$ rather $6 \cdot 10^{-2}$ for the SS scheme with a gain higher for the lower SNRs.

A comparison between the OSJ scheme which uses the true statistical expression (Eq. (7)) and the simplified OSJ which is based on Eq. (8) shows that the simplified OSJ protocol approximates the true performance for all the cases and converges to the same outage probability value at high SNRs. For scenarios where the simplified secrecy capacity expression (Appendix A) holds, the simplified version of OSJ gives a similar performance with the true OSJ scheme while requiring a lower computational complexity. Regarding the hybrid schemes, it can be seen that OW outperforms all the selection techniques and provides the best performance (it converges to outage probability $10^{-5}$). This result validates that an appropriate mechanism for switching between OS and OSJ overcomes cases where the interference decreases secrecy. For the suboptimal case, we can see that SW with optimal switching (bound) provides the best suboptimal performance. This gain becomes less for the practical implementation of SW, but still remains the suboptimal solution with the minimum outage probability (it is slightly better than SSJ). Furthermore, a comparison between the proposed asymptotic approximation and the true performance validates our analytical results. The proposed approximation exactly fits with the irreducible outage probability for both OSJ and SSJ schemes. Finally, Fig. 3 also plots the performance of the reference protocol OSCJ. As can be seen, the ability of the OSCJ scheme to decode the artificial interference at the main destination, provides the highest secrecy outage probability without a diversity loss and seems to be an interesting solution worth of further investigation. Fig. 4 compares the considered selection techniques for the above configuration by using as a metric the secrecy ergodic capacity. The presented results are in line with the above outage probability results and show that jamming significantly improves the secrecy capacity for both OS and SS schemes. Regarding the hybrid protocols, the OW outperforms all schemes and SW has a higher gain than SSJ in terms of secrecy capacity. It is worth noting that the

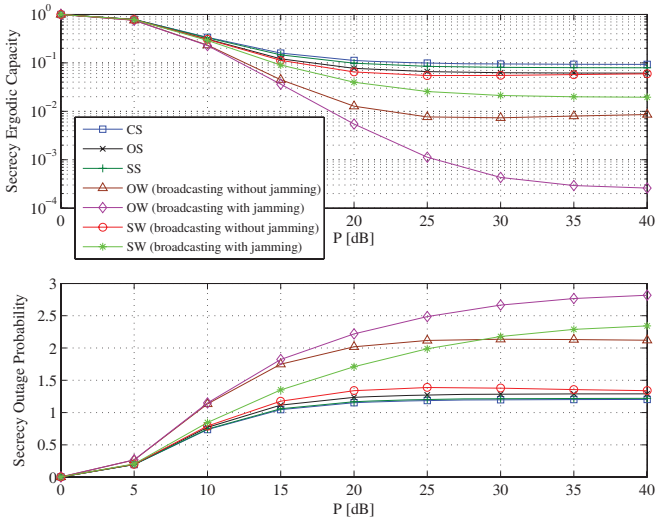


Fig. 5. Secrecy outage probability and secrecy ergodic capacity versus $P$ for the different selection schemes with direct links ($S \to D, S \to E$).

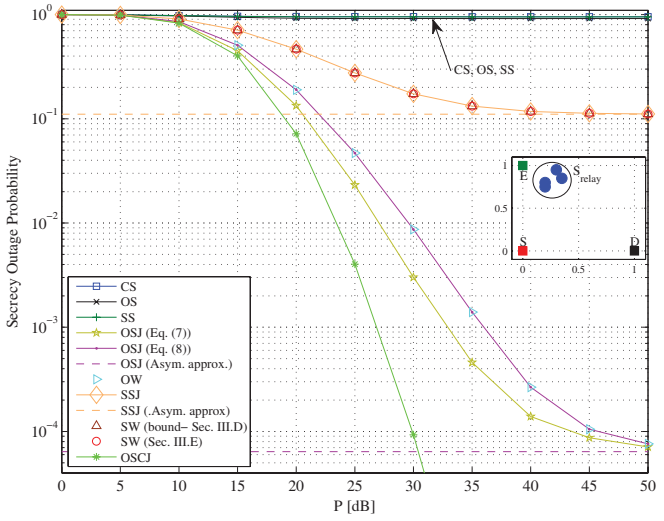


Fig. 6. Secrecy outage probability for a scenario where relays are located close to the eavesdropper; $K = 4$ relays, $R_S = 0.1$ BPCU, $R_0 = 2$ BPCU, $\beta = 3$.

practical implementation of SW approximates the SW-bound capacity.

In order to validate the efficiency of the proposed schemes for general network configurations, in the following simulation results, we relax the constraint of deep fading direct links and we assume that the source message can be received at both $D$ and $E$ during the broadcast phase of the cooperative protocol. Fig. 5 plots the secrecy outage probability and the secrecy ergodic capacity of the extended versions of the OW and SW schemes (Section III.G) versus the transmitted power ($P$) for the above considered configuration. For comparison reasons, the OW and SW schemes with an unprotected broadcast communication phase are also presented (jamming is activated only in the second phase). As can be seen, jamming is also beneficial for scenarios with direct links (unsecured broadcast phase) and significantly improves the secrecy performance. The integration of appropriate jamming in both phases of the communication outperforms the partial jamming application and provides the best performance for both OW and SW schemes in terms of outage probability and secrecy capacity. It worth noting that for the configuration considered, the direct links are symmetric and very strong, and thus the achieved secrecy performance is decreased in comparison with the non-direct link set-ups.

The next simulation results deal with two extreme configurations which reveal the potential of the proposed jamming techniques. The first simulation scenario assumes a topology in which $K = 4$ relays are located close by the eavesdropper $E$. Fig. 6 presents the considered topology, as well as the secrecy outage probability of the different selection schemes. It is clear that the non-jamming approaches are inefficient as the relays have a strong link with the eavesdropper. On the other hand, jamming techniques confuse the eavesdropper and increase significantly the secrecy outage probability. For this configuration, the proposed hybrid schemes (OW, SW) have a similar performance to their non-adaptive versions (OSJ, SSJ), as jamming is almost always beneficial. We note that as the eavesdropper channel becomes stronger, the difference

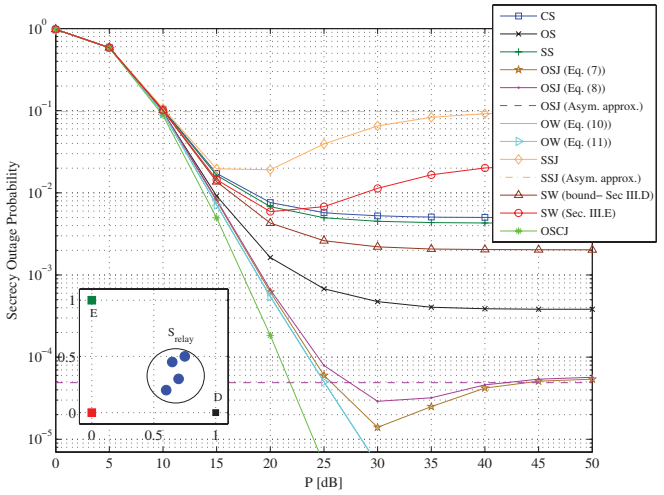


Fig. 7. Secrecy outage probability for a scenario where relays are located close to the destination; $K = 4$ relays, $R_S = 0.1$ BPCU, $R_0 = 2$ BPCU, $\beta = 3$.

between the true OSJ and the simplified OSJ is increased but both schemes converge to the same value at high SNRs.

Finally, Fig. 7 assumes a configuration where $K = 4$ relays are located close by the destination. As can be seen, for this scenario, continuous jamming techniques introduce high interference at the destination and become less efficient. Furthermore, we can observe that for the considered simulation parameters, the continuous jamming techniques have a U-shaped outage probability and thus their irreducible outage probability is higher than the minimum outage probability, (the reference optimal OSJ scheme validates this behavior). The main reason for this result is that for strong relay-destination links, jamming becomes stronger at high SNRs and can decrease the secrecy performance achieved. A comparison of the true OSJ and simplified OSJ shows that their difference is negligible as the relays approach the destination. As far as the hybrid techniques is concerned, appropriate switching improves significantly the performance compared with the

continuous jamming techniques. Both OW and SW schemes yield a higher gain than previous configurations and further can overcome the problem of U-shaped outage performance. These two extreme configurations reveal that jamming is an interesting solution for scenarios with strong relay-eavesdropper links. The hybrid protocols avoid strong interference at the destination and are thus promising solutions to maximize secrecy capacity.

## V. Conclusion

In this paper, we have dealt with relay and jammer selection in cooperative systems with secrecy limitations. The proposed selection schemes select two nodes which access the channel simultaneously. The first relay forwards the data of the source, (i.e. conventional relay) and the second one transmits an intentional interference signal in order to confuse the eavesdropper. The investigated techniques select the two nodes by achieving an optimization of the perfect secrecy capacity and have been analyzed based on both instantaneous and average knowledge of the eavesdropper channels. It is proven that jamming is an efficient solution for scenarios with strong eavesdropper links. In order to overcome jamming limitations for scenarios with weak eavesdropper links, an hybrid method for switching between jamming and non-jamming is also proposed. The hybrid selection is introduced as a general solution and optimizes the secrecy capacity for all cases.

## Acknowledgements

The work reported in this paper has formed part of the Wireless Enabling Techniques work area of the Core 4 Research Programme of the Virtual Centre of Excellence in Mobile and Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. We acknowledge the support of the Scottish Funding Council for the Joint Research Institute with the Heriot-Watt University which is a part of the Edinburgh Research Partnership. Furthermore, the authors would like to thank the anonymous reviewers for their insightful and constructive comments, which significantly improved the paper.

## Appendix A
## Asymptotic analysis of OSJ

The analysis of the proposed schemes focuses on a symmetric configuration and deals with high SNRs (i.e. asymptotic analysis). More specifically, in order to simplify the presentation, the analysis is derived for a symmetric clustered system model where all the relays are the same distance from the destination and the eavesdropper ($\sigma_{k,j} = \sigma^2 \ \forall \ k \in S_{\text{relay}}, j \in \{D, E\}$). Accordingly, the average SNRs for each link are assumed to be $\mathbb{E}[\gamma_{R,D}] = \mathbb{E}[\gamma_{R,E}] = P^{(R)}\sigma^2$ and $\mathbb{E}[\gamma_{J,D}] = \mathbb{E}[\gamma_{J,E}] = P^{(J)}\sigma^2$, respectively. Furthermore, for high SNRs, all the relay nodes can decode the source message and therefore the asymptotic analysis assumes a decoding set with $|C_d| = |S_{\text{relay}}| = K$.

If $(X_k, Y_k)$ with $k = 1, \ldots, K$ is an i.i.d. exponential distributed random variable set with parameter $\lambda$ (which represents the channel of the $k$-th relay with the destination and the eavesdropper, respectively), $\alpha_\mu, \alpha_\nu$ are deterministic variables, $Z_1 \triangleq \frac{X_\mu}{Y_\mu}$ and $Z_2 \triangleq \frac{X_\nu}{Y_\nu}$ denote random variables with $\mu = \arg\max_{k\in\{1,2,\ldots K\}}\{X_k/Y_k\}$ and $\nu = \arg\min_{k\in\{1,2,\ldots K\}-\mu}\{X_k/Y_k\}$, respectively, the outage probability under question is written as

$$\mathbb{P}\left\{\frac{1}{2}\log_2\left(\frac{1+\frac{\alpha_\mu X_\mu}{1+\alpha_\nu X_\nu}}{1+\frac{\alpha_\mu Y_\mu}{1+\alpha_\nu Y_\nu}}\right)\right\} \simeq$$
$$\simeq \mathbb{P}\left\{\frac{1}{2}\log_2\left(\frac{1+\frac{\alpha_\mu X_\mu}{\alpha_\nu X_\nu}}{1+\frac{\alpha_\mu Y_\mu}{\alpha_\nu Y_\nu}}\right)\right\}$$
$$\text{(for high SNRs } \ \alpha_\nu X_\nu \gg 1, \alpha_\mu X_\mu \gg 1)$$

$$\simeq \mathbb{P}\left\{\frac{1}{2}\log_2\left(\frac{\frac{\alpha_\mu X_\mu}{\alpha_\nu X_\nu}}{\frac{\alpha_\mu Y_\mu}{\alpha_\nu Y_\nu}}\right)\right\} \qquad (\text{If } \ \alpha_\mu/\alpha_\nu \gg 1) \quad (21)$$
$$= \mathbb{P}\left\{\frac{1}{2}\log_2\left(\frac{Z_1}{Z_2}\right) < R_S\right\}$$
$$= \mathbb{P}\left\{\frac{Z_1}{Z_2} < \rho\right\}$$
$$= P_{\mathcal{Z}}(\rho), \quad (22)$$

where $\rho = 2^{2R_S}$ and $P_{\mathcal{Z}}(\cdot)$ denotes the Cumulative Distribution Function (CDF) of $\mathcal{Z} \triangleq Z_1/Z_2$ which is given by

$$P_{\mathcal{Z}}(y) = \mathbb{P}\left\{\frac{Z_1}{Z_2} < y\right\} = \mathbb{P}\{Z_1 < Z_2 y\}$$
$$= \int_0^\infty P_{Z_1}(z_2 y) p_{Z_2}(z_2) dz_2$$
$$= \int_0^\infty \left[\frac{z_2 y}{1+z_2 y}\right]^K (K-1)\frac{1}{(1+z_2)^2}\left[1-\frac{z_2}{1+z_2}\right]^{K-2} dz_2$$
$$= (K-1)y^K \int_0^\infty \left[\frac{z_2}{(1+z_2 y)(1+z_2)}\right]^K dz_2$$
$$= \frac{y^K}{2^K-(1+y)^K}\left(\frac{1}{y}-1\right), \quad (23)$$

where for the above expressions we have used order statistics [24]. It is worth noting that the approximation given in Eq. (21) can be ensured either by the relay selection policy or by an appropriate transmitted power allocation (the jammer node transmits with a lower power than the relay node and thus $\alpha_\mu \gg \alpha_\nu$)[2]. This behavior is validated by simulation results in Section IV. In the case that this assumption does not hold, the above approximation provides a useful lower performance bound.

## Appendix B
## Probability of switching for OW

We define the random variable $Z_k = \frac{Y_k}{X_k}$ with $k = 1, \ldots, K-1$ where $X_k$, $Y_k$ are i.i.d. exponential random variables with parameter $\lambda$. The random variables $Z_k$ are i.i.d. with a CDF equal to $P_Z(z) = z/(1+z)$ and a probability density function (PDF) equal to $p_z(z) = 1/(1+z)^2$. The

[2]If $\zeta \triangleq \frac{X_\mu}{X_\nu}$, $\delta \triangleq \frac{\alpha_\mu}{\alpha_\nu}$ then $\mathbb{P}\{\delta\zeta > y\} = \frac{\delta}{\delta+y} \to 1$ when $\delta \gg y$. In our case, the proposed approximation holds when $\delta \gg y \gg 1$.

PDF of the random variable $\mathcal{Z} = \min\{Z_k\}$ is expressed by using order statistics as [24]

$$P_{\mathcal{Z}}(z) = (K-1)p_Z(z)[1-P_Z(z)]^{K-2} = (K-1)\frac{1}{(1+z)^K}. \tag{24}$$

Therefore the probability of switching is written as

$$\begin{aligned}\mathbb{P}(\text{switching}) = \mathbb{P}(\mathcal{Z}>1) &= \int_1^\infty (K-1)\frac{1}{(1+z)^K} \\ &= \frac{1}{2^{K-1}}.\end{aligned} \tag{25}$$

## APPENDIX C
## ASYMPTOTIC ANALYSIS OF SSJ

In a manner equivalent to Appendix A, we assume a symmetric configuration with an equivalent average SNR for each link. If $(X_k, Y_k)$ with $k = 1, \ldots, K$ is an i.i.d. exponential distributed random variable set with parameter $\lambda$, (which represents the channel of the $k$-th relay with the destination and the eavesdropper, respectively), the sub-optimal selection for the symmetric case corresponds to $\mu = \arg\max_{k\in\{1,2,\ldots K\}}\{X_k\}$ and $\nu = \arg\min_{k\in\{1,2,\ldots,K\}-\mu}\{X_k\}$. In this case the corresponding outage probability is expressed as

$$\mathbb{P}\{C_S < R_S\} \simeq \mathbb{P}\left\{\frac{1}{2}\log_2\left(\frac{\frac{X_\mu}{X_\nu}}{\frac{Y_\mu}{Y_\nu}}\right) < R_S\right\} \tag{26}$$

$$\begin{aligned}&= \mathbb{P}\left\{\frac{Z_1}{Z_2} < \rho\right\} = \mathbb{P}\Big\{Z_1 < Z_2\rho\Big\} \\ &= \int_0^\infty P_{Z_1}(z_2\rho)p_{Z_2}(z_2)dz_2 \\ &= 1 + (K-1)\sum_{k=1}^{K}\binom{K}{k}(-1)^k\frac{K-1-k\rho+k\rho\ln\left(\frac{k\rho}{K-1}\right)}{(K-1-k\rho)^2},\end{aligned} \tag{27}$$

with

$$\begin{aligned}P_{Z_1}(z) = \mathbb{P}\{X_\mu < zY_\nu\} &= \int_0^\infty P_{X_\mu}(zy)p_{Y_\nu}(y)dy \\ &= \int_0^\infty [1-\exp(-\lambda zy)]^K(K-1) \\ &\qquad \times \lambda\exp(-\lambda y)[\exp(-\lambda y)]^{K-2}dy \\ &= (K-1)\sum_{k=0}^{K}\binom{K}{k}(-1)^k\frac{1}{K-1+kz},\end{aligned} \tag{28}$$

$$p_{Z_2}(z) = \frac{1}{(1+z)^2}, \tag{29}$$

where $Z_1 \triangleq X_\mu/X_\nu$, $Z_2 \triangleq Y_\mu/Y_\nu$, $\rho = 2^{2R_S}$ and for the above expressions we have used order statistics [24] and the binomial theorem $(x+y)^n = \sum_{m=0}^{n}\binom{n}{m}x^{n-m}y^m$.

## REFERENCES


[1] E. D. Silva, A. L. D. Santos, L. C. P. Albini, and M. Lima, "Identity-based key management in mobile ad hoc networks: techniques and applications," *IEEE Wireless Commun.*, vol. 15, pp. 46-52, Oct. 2008.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355-1387, Jan. 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, pp. 451-456, July 1978.

[4] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2493-2507, June 2008.

[5] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2515-2534, June 2008.

[6] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Seattle, USA, pp. 356-360, July 2006.

[7] Y. Liang, H. V. Poor, and L. Ying, "Wireless broadcast networks: reliability, security, and stability," in *Proc. IEEE Inf. Theory Appl. Work.*, San Diego, CA, USA, pp. 249-255, Feb. 2008.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure wireless communications via cooperation," in *Proc. Allerton Conf. Commun. Cont. Comp.*, Urbana-Champaign, IL, USA, Sept. 2008.

[9] I. Krikidis, J. Thompson, and S. McLaughlin, "On the diversity order and secrecy rate of non-orthogonal amplify-and-forward relay protocols," *IEEE Trans. Wireless Commun.*, submitted for publication Nov. 2008. [Available online: www.see.ed.ac.uk/∼ikrikidi/paper_TWC.pdf]

[10] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative divesrity in wireless networks: efficient protocols and outage behavior," *IEEE Trans. Inform. Theory*, vol. 50, pp. 3062-3080, Dec. 2004.

[11] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, pp. 3450-3460, Sept. 2007.

[12] S. Yang and J.-C. Belfiore, "Towards the optimal amplify-and-forward cooperative diversity scheme," *IEEE Trans. Inform. Theory*, vol. 53, pp. 3114-3126, Sept. 2007.

[13] L. Lai and H. El Gamal, "The relay-eavesdropper channel: cooperation for secrecy," *IEEE Trans. Inform. Theory*, vol. 54, pp. 4005-4019, Sept. 2008.

[14] Y. Oohama, "Relay channels with confidential messages," *IEEE Trans. Inform. Theory*, submitted for publication Mar. 2007. [Available online: http://arxiv.org/pdf/cs/0611125v7].

[15] V. Aggarwal, L. Sankar, A. R. Calderbank, and H. V. Poor, "Secrecy capacity of a class of orthogonal relay eavesdropper channels," *EURASIP J. Wireless Commun. Net.*, accepted for publication, June 2009.

[16] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IEEE Signal Processing Lett.*, submitted for publication, July 2009.

[17] O. Simeone and P. Popovski, "Secure communications via cooperating base stations," *IEEE Commun. Lett.*, vol. 12, pp. 188-190, Mar. 2008.

[18] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inform. Foren. Sec.*, vol. 4, pp. 242-256, June 2009.

[19] E. Tekin and A. Yener, "The general Gaussian multiple access and two-way wire-tap channels: achievable rates and cooperative jamming," *IEEE Trans. Inform. Theory*, vol. 54, pp. 2735-2751, June 2008.

[20] T. Wang and G. B. Giannakis, "Mutual information jammer-relay games," *IEEE Trans. Inform. Foren. Sec.*, vol. 3, pp. 290-303, June 2008.

[21] S. Lee, M. Han, and D. Hong, "Average SNR and ergodic capacity analysis for opportunistic DF relaying over Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, pp. 2807-2812, June 2009.

[22] F. A. Onat, A. Adinoyi, Y. Fan, H. Yanikomeroglu, J. S. Thompson, and I. D. Marsland, "Threshold selection for SNR-based selective digital relaying in cooperative wireless networks," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 4226-4237, Nov. 2008.

[23] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inform. Theory*, vol. 55, pp. 1575-1591, Apr. 2009.

[24] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*, 4th ed. New York: McGraw-Hill, 2002.