Opportunistic relay selection for cooperative networks with secrecy constraints

I. Krikidis

Institute for Digital Communications, School of Engineering and Electronics, University of Edinburgh, Mayfield Road, Edinburgh EH9 3JL, Scotland, UK
E-mail: i.krikidis@ed.ac.uk

Abstract: This study deals with opportunistic relay selection in cooperative networks with secrecy constraints, where an eavesdropper node tries to overhear the source message. Previously reported relay selection techniques are optimised for non-eavesdropper environments and cannot ensure security. Two new opportunistic relay selection techniques, which incorporate the quality of the relay-eavesdropper links and take into account secrecy rate issues, are investigated. The first scheme assumes an instantaneous knowledge of the eavesdropper channels and maximises the achievable secrecy rate. The second one assumes an average knowledge of the eavesdropper channels and is a suboptimal selection solution appropriate for practical applications. Both schemes are analysed in terms of secrecy outage probability and their enhancements against conventional opportunistic selection policies are validated via numerical and theoretical results.

1 Introduction

Cooperation between nodes appears as one of the most interesting paradigms for the deployment of future wireless systems [1]. It is an efficient way to provide spatial diversity benefits to single-antenna systems and to extend the transmission coverage. However, outwith these conventional applications, it has recently been used to ensure secrecy in wireless systems, where malicious nodes – the eavesdroppers – try to overhear the source transmission. A relay that is closer to destination than the eavesdropper node maximises the secrecy rate (maximum transmission rate at which the eavesdropper is unable to decode any information) and can offer a positive secrecy also for scenarios where the direct transmission secrecy is zero [2–6].

In this paper, we deal with the relay selection in cooperative networks with eavesdropper nodes. Although relay selection has been well studied in the literature for non-eavesdropper configurations and for different contexts [7–11], relay selection for secrecy purposes has not been studied yet. A new selection strategy which is motivated by the secrecy capacity expression and takes into account the eavesdropper channels is investigated. In its optimal version, it requires the estimation of the quality of the instantaneous relay-eavesdropper links and corresponds to a maximisation of the instantaneous secrecy capacity. However, in practice, an instantaneous knowledge of the eavesdropper channel is not available and only an estimation of the average channel gains can be performed. The suboptimal version of the proposed scheme incorporates the average quality of the relay-eavesdropper links and gives an efficient solution without complicated modifications to the conventional relay selection.

The remainder of this paper is organised as follows. The system model as well as the proposed selection techniques are given in Section 2. Numerical results are shown and discussed in Section 3, followed by concluding remarks in Section 4.
source has no direct link with the nodes D, E (i.e. direct links are in deep shadowing) and the communication is performed through a reactive DF protocol. It is worth noting that this assumption is well known in the cooperative literature for systems with [4, 5] and without [7] secrecy constraints and simplifies our analysis. More specifically, this assumption refers to cooperative systems with a secure broadcast phase [5] or clustered relay configurations where the source node communicates with the relays via a local connection with small transmission power [8]. In the first phase of this protocol, the source broadcasts the signal to the relay nodes and during the second phase one relay node, which is selected among the relays that successfully decoded the source transmission \((k^* \in S_{relay} \subseteq S_{relay})\), forwards the signal towards the nodes D and E. Fig. 1 schematically presents the system model and the two phases of the considered cooperative scheme. 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 \(\sigma_{ij}^2 = d_{ij}^{-\beta}\), where \(d_{ij}\) is the Euclidean distance between terminals \(i\) and \(j\) and \(\beta\) is the path loss exponent. Furthermore, additive white Gaussian noise is assumed with a unit variance. If \(k^* \in S_{relay}\) denotes the selected relay, the instantaneous secrecy rate (secrecy capacity) is defined as [3]

\[
C(k^*) = \left[ \frac{1}{2} \log_2 \left( 1 + \gamma_{k^*,D} \right) \right]_+ - \left[ \frac{1}{2} \log_2 \left( 1 + \gamma_{k^*,E} \right) \right]_+ \tag{1}
\]

where \(\gamma_{ij} = |f_{ij}|^2 P\) denotes the instantaneous signal-to-noise ratio (SNR) for the link \(i \rightarrow j\), \(f_{ij}\) is the instantaneous channel coefficient for the link \(i \rightarrow j\), \(P\) is the transmitted power, \([x]^+ = \max\{x, 0\}\) and the above approximation holds for high SNRs. The selection of the relay depends on the relay selection technique and its optimisation is the main objective of this paper. It is worth noting that each relay selection technique assumes a perfect knowledge of the required channel-based parameters and channel estimation issues are beyond the scope of this paper.

### 2.2 Conventional selection

The conventional selection does not take into account the relay-eavesdropper links and is suitable for reactive DF schemes without secrecy constraints. According to [7], the conventional selection decides on the relay node with the best instantaneous relay-destination link and is expressed as

\[
k^* = \arg \max_{k \in S_{relay}} \{ \gamma_{k,D} \} \tag{2}
\]

In order to simplify the analysis and the related presentation, we focus on the high SNR regime where all the relay nodes successfully decode the source transmission \((S_{relay} = S_{relay})\). We note that this asymptotic assumption does not limit the benefits of the proposed schemes and is similar to [4]. The performance of the system is characterised by the secrecy outage probability which is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate \(R_s > 0\) [3]. The secrecy outage probability converges to

\[
P_{out} = \sum_{k=1}^{K} \Pr[k = k^*] \Pr[C(k) < R_s] = \sum_{k=1}^{K} \rho_k P_r (2^{2R_s}) \tag{3}
\]

with (by using order statistics (maximum among \(K\) i.i.d. random variables) [12])

\[
\rho_k = \Pr[k = k^*] = \prod_{i=1}^{K} \Pr[\gamma_{k,D} < \gamma_{i,D}] = \prod_{i=1}^{K} \lambda_{i,D} / (\lambda_{i,D} + \lambda_{k,D}) \tag{4}
\]

![Figure 1](image-url)  
**Figure 1** The system model and the two phases of transmission (the relay communicates with the destination via orthogonal relaying)

S: source, D: destination, E: eavesdropper, k: selected relay
where $\lambda_{i, j} \triangleq 1/\sigma_{i, j}^2$, $L_k$ is a subset with a cardinality equal to $k$ and $\sum_{i=1}^K L_i$ denotes the addition of the elements of $L_k$. The conventional approach does not take into account the eavesdropper node and motivates the investigation of more efficient relay selection techniques. However, it is worth noting that the asymptotic performance of the conventional approach for secure communications is also a part of the contribution of this work.

### 2.3 Optimal selection

The proposed selection technique incorporates the quality of the relay-eavesdropper links in the selection decision metric. In its optimal version, we assume that the instantaneous quality of the relay-eavesdropper links is available during the decision process. Based on the expression of the instantaneous secrecy capacity, which is given in (1), the proposed selection technique is written as

$$k^* = \arg \max_{k \in S_{\text{relay}}} \left\{ \frac{\gamma_{i, D}}{\gamma_{i, E}} \right\}$$

and the corresponding secrecy outage probability converges to

$$P_{\text{out}} = \Pr[C(k^*) < R_s] = P(2^{2R_s})$$

where

$$P(x) = \Pr(\gamma_{x, D}/\gamma_{x, E} < x) = \prod_{i=1}^{K} x/(\psi_i + x)$$

(by using basic order statistics theory [12]) and $\psi_i \triangleq \sigma_{i, D}^2/\sigma_{i, E}^2$. The new selection metric is related to the maximisation of the secrecy capacity and therefore is the optimal solution for reactive DF protocols with secrecy constraints. However, its application requires the knowledge of the relay-eavesdropper links and therefore its practical interest is limited.

### 2.4 Suboptimal selection

Although the tracking of the instantaneous relay-eavesdropper links seems to be impossible for practical applications, knowledge of the average channels can be provided by a long-term estimation process [13]. The proposed suboptimal selection technique follows the same structure with the optimal selection but incorporates the average relay-eavesdropper channels instead of their instantaneous quality. More specifically, the proposed suboptimal selection technique is written as

$$k^* = \arg \max_{k \in S_{\text{relay}}} \left\{ \frac{\gamma_{i, D}}{\sigma_{i, E}^2} \right\}$$

and the related secrecy outage probability is given as

$$P_{\text{out}} = \Pr[C(k^*) < R_s] = P(2^{2R_s})$$

with

$$P(x) = \Pr\left( \gamma_{x, D}/\gamma_{x, E} = \gamma_{x, D}/\sigma_{x, E}^2 = \frac{Z}{\Delta} < x \right)$$

$$= 1 - \sum_{i=1}^{K} (-1)^i \sum_{L_i \subseteq \{1, \ldots, K\}} \frac{1}{\sum_{i} L_i + 1}$$

where $\xi_i \triangleq \sigma_{i, D}^2/\sigma_{i, E}^2$, $\Delta$ is an exponential random variable with unit variance (resulting from the division of the variance) and $Z \triangleq \gamma_{x, D}/\sigma_{x, E}^2$ is an exponential random variable with a cumulative distribution function (CDF) equal to $P_x(x) = \Pr[Z < x] = \prod_{i=1}^{K} [1 - \exp(-\xi_i x)]$ (by using order statistics [12]). The proposed suboptimal relay selection technique takes into account the eavesdropper nature of the considered system without requiring the estimation of the instantaneous relay-eavesdropper channels. It has a complexity similar to the conventional selection technique (it does not require structural or protocol modifications) and thus seems to be suitable for applications that switch between eavesdropper and non-eavesdropper environments.

**Channel estimation error:** The suboptimal relay selection technique is independent of the instantaneous relay-eavesdropper links but it requires the knowledge of their average statistic. In practical systems, the average channels (which depend on the path loss and shadowing) remain constant for a long period of time and therefore the estimation of the average links at the relay nodes can be performed reliably (a perfect knowledge of the relay-eavesdropper links is a reasonable assumption). However, in order to take into account imperfect channel estimation as well as scenarios where the eavesdropper node is active for short periods of time, the estimated average relay-eavesdropper link can be modelled as

$$\sigma_{i, E}^2 = \sigma_{i, E}^2(1 \pm \delta)$$

where $\delta \in [0, 1]$ denotes the estimation error factor (The average channel estimation is based on a long observation of the relay-eavesdropper links and therefore the corresponding estimation error can be modelled as a constant parameter; the polarity of the channel estimation error is random (probability 1/2)). This simple model captures the effects of the channel estimation error and gives an idea about the related performance degradation via simulation results in the
A further analysis of the channel estimation error is beyond the scope of this paper.

3 Numerical results

The simulation environment follows the model of Section 2 and consists of a 2D square topology where the nodes S, D and E are located as \(\{x_S, y_S\} = \{0, 0\}\), \(\{x_D, y_D\} = \{1, 0\}\) and \(\{x_E, y_E\} = \{0, 1\}\), respectively. This node topology (symmetric source-destination and source-eavesdropper links) corresponds to a zero secrecy capacity and emphasises the importance of the relay selection (relaying can support a positive secrecy capacity and is the main concern of this work). A similar network topology, where the direct links cannot ensure a positive secrecy capacity, has been used in [2]. The relay nodes are randomly located according to a uniform distribution and their locations (for a specific simulation case) are shown in Fig. 2. We note that the selected topology is used for the sake of presentation and the enhancements of the proposed selection schemes hold for all the possible configurations. The path loss exponent is set to \(\beta = 3\) and the dimension of the network is normalised to \(1 \times 1\) unit lengths. The required spectral efficiency is \(R_0 = 2\) bits per channel use (BPCU) and the target secrecy rate is equal to \(R_s = 0.1\) BPCU. In addition to the network topology, Fig. 2 also shows how often a relay node is used in each relay selection strategy. More specifically, each relay node is related to three numerical values that represent the selection rate for the three proposed relay selection strategies at high SNRs (e.g. \(P = 50\) dB); the first value corresponds to the conventional selection, the second value corresponds to the optimal selection and the third value corresponds to the suboptimal selection.

Fig. 3 compares the outage secrecy probability of the conventional selection with the proposed optimal and suboptimal selection schemes. As can be seen, the conventional selection is not efficient for configurations with eavesdropper nodes and converges to the highest outage probability. On the other hand, the optimal proposed scheme minimises the secrecy outage probability and thus is the optimal selection policy for cooperative networks with secrecy constraints. However, owing to the required estimation of the eavesdropper channels, the optimal selection is suitable for extreme applications (i.e. military) and therefore in most of cases is a useful lower bound. As far as the suboptimal selection scheme is concerned, we can see that it outperforms the conventional selection and converges to a lower outage probability. The suboptimal scheme has a complexity overhead similar to the conventional selection as it does not require the estimation of the instantaneous eavesdropper channels and thus seems to be an efficient solution with practical interest. As for the imperfect channel estimation, Fig. 3 plots the outage performance of the suboptimal selection technique for \(\delta = 0.3\) and \(\delta = 0.5\) (Section 2.4). As can be seen an imperfect average channel estimation degrades the system performance and the outage probability is increased as the channel estimation factor increases. However, for moderate error factor values (i.e. \(\delta < 0.3\)) the performance degradation is small and therefore the suboptimal relay selection is robust to channel estimation ambiguities. In the same figure, we present the accuracy of the proposed simplified expressions. More specifically, Fig. 3 shows the outage probability, which results by using the approximation in (1) as well as the decoding assumption (all the relay nodes decode the source signal). As can be seen from the corresponding curves, the simplified approximation of (1) matches to the true performance and thus is an efficient approximation for intermediate and high SNRs. Furthermore, the proposed asymptotic analysis efficiently approximates the convergence of the true outage.
probability and this observation validates our analysis for the high SNR regime.

In order to confirm the above observations, Fig. 4 compares the average secrecy capacity $E[C(k^*)]$ of the different selection schemes against the transmitted power. It is worth noting that the average secrecy capacity is the main performance metric in the secrecy literature [2]. As can be seen, the plotted curves follow the above behaviour and therefore validate our conclusions.

4 Conclusion

Previously reported relay selection schemes select the best single relay without taking into account confidentiality issues. In this paper, we introduced relay selection as an efficient way in order to ensure secrecy and protect the source message against eavesdroppers. Two new selection techniques for a reactive DF cooperative network, which take into account the relay-eavesdropper links in their decision metrics, were investigated. The first scheme requires the estimation of the instantaneous eavesdropper channels and achieves the best possible secrecy performance. The second scheme assumes an average knowledge of the eavesdropper channel gains and seems to be an efficient solution for practical applications. Both schemes significantly outperform conventional relay selection techniques and their performance enhancements were validated by theoretical and numerical results.

5 References


