Increasing the Information-Theoretic Secrecy by Cooperative Relaying and Jamming

Ninoslav Marina, Member, IEEE, Toni Draganov Stojanovski, Member, IEEE and H. Vincent Poor, Fellow, IEEE

Abstract—The use of cooperation to increase the information-theoretic secrecy in a decentralized ad-hoc wireless network is investigated. In particular, four cases of cooperative relaying are analyzed and compared. These cases include the no-cooperation case, the case with single-hop cooperation with multiple relays, the case with single-hop cooperation with the strongest relay, and finally the case of multi-hop cooperation with the strongest relay. From the results, it is seen that cooperation increases the probability of a positive secrecy rate between two nodes in a network with friendly (cooperative) nodes and eavesdropping nodes. The improved information-theoretic secrecy increases the probability that two nodes can share a secret message with perfect secrecy using a multi-hop route of trusted nodes. Cooperative jamming is also studied, and it is observed that very often it is more beneficial to use friendly nodes for cooperative jamming than cooperative relaying. Finally, a combination of cooperative relaying and jamming is considered.

I. INTRODUCTION

It is envisioned that future wireless networks will be decentralized, ad-hoc in nature and will have the capability for self organization. Because of these properties and the broadcast nature of the wireless medium they will be very sensitive to passive and active attacks from unwanted parties, since any node close enough to a transmitter can potentially receive sensitive information. Classical cryptographic methods, although offering a high level of protection, might be either impossible or quite challenging to implement in a network without infrastructure due to the difficulty of key management. Information-theoretic security is a framework that guarantees secrecy at the physical layer, such that adversaries get practically zero information about the transmitted message, while it can be still decoded at the legitimate receiver with a small probability of error. The concept was initially introduced by Shannon [1]. In 1975, Wyner defined the wiretap channel and established the possibility of creating almost perfectly secure communication links without relying on exchange of secret keys [2]. In that case, we say that the secrecy capacity is positive, and a maximal level of secrecy towards the eavesdropper is obtained. In other words, the eavesdropper is kept in a total ignorance of the transmitted message to the legitimate receiver, hence it may not decode any confidential information from its observations. Leung-Yan-Cheong and Hellman characterized the secrecy capacity of the additive white Gaussian noise wiretap channel [3], and Csiszár and Körner generalized Wyner’s approach by considering the transmission of confidential messages over broadcast channels [4]. In recent years, information-theoretic security has re-gained popularity since it is a powerful tool to study security of wireless networks.

In [5] and [6] Haenggi and Sarkar introduced the concept of a secrecy graph. Nodes in a wireless network are represented as vertices, and edges between vertices exist only if the secrecy capacity between the corresponding nodes in the wireless network is positive. Assuming Poisson point processes for nodes and eavesdroppers, Haenggi and Sarkar provide analytical results on mean node degrees and percolation thresholds. Pinto et al. [7] analyze the secrecy capacity when the positions of eavesdroppers follow an arbitrary spatial process. For colluding eavesdroppers and a Poisson spatial process, the cumulative distribution function of the secrecy capacity, as well as the outage of the secrecy capacity are derived. Both lines of work conclude that even a modest presence (density) of eavesdroppers has a detrimental impact on the percolation threshold and graph connectivity, hence, on the secrecy capacity. Zhou et al. [8] study the impact of physical layer security requirements on the network throughput. Tekin and Yener [9] introduce a cooperation scheme called cooperative jamming in which "bad" friendly nodes, which are close to the eavesdropper, jam the eavesdropper to help increase the achievable secrecy rates for the transmitter.

In this paper we are interested in providing positive secrecy rates between as many as possible pairs of nodes in a wireless network with multiple eavesdroppers via user cooperation. The idea is to ensure that as many as possible pairs will be able to communicate their secret cryptographic keys under perfect secrecy, after which it will be possible to send the main data encrypted thus keeping all information in perfect secrecy. In particular, the exchanged secret can be used as a master key between the two parties. The master key is typically used to encrypt and exchanges session keys, which are then used to encrypt the data transmitted between the two parties. The master key between two parties is usually not changed very frequently. The amount of secrecy capacity determines how quickly the master key will be
exchanged between the two parties. Since it changes very rarely, transmitting it with even very small rates is sufficient. Once the master key is exchanged, the legitimate parties can start communicating at the maximum data rate since their communication channel is cryptographically protected and thus achieving computational secrecy [1].

In Section II we present the system model. The main result of this work, that such cooperation improves information-theoretic secrecy is presented in Section III. In that section we describe the non-cooperative scenario and three different cooperative scenarios: single-hop cooperation with multiple relays, single-hop cooperation with the strongest relay, and multi-hop cooperation with the strongest relay. Section IV first analyzes the case of cooperative jamming, and then considers the use of both cooperative relaying and jamming: a bad relay is turned into a good jammer and cooperates together with the best relay. Section V concludes the paper.

II. SYSTEM MODEL

We analyze a wireless ad-hoc network of $N_f$ legitimate or friendly nodes and $N_e$ passive eavesdroppers that try to intercept the information that is transmitted between the pairs of legitimate nodes, hence reducing the secrecy capability of the network. Passive eavesdroppers are adversary nodes that intend only to receive but not transmit any signal.

An example of such a network with $N_f = 6$ friendly and $N_e = 2$ eavesdropper nodes is shown in Figure 1. In the sequel, we use the following notation when node $i$ is communicating to node $j$: the transmitted signal from the legitimate node $i$ will be denoted by $X_i$; the received signal at legitimate node $j$ when node $i$ is transmitting (and all the other nodes, except $i$ and $j$ are helping) is denoted by $Y_{j,i}$; the received signal at helping node $k$ is denoted by $Y_{k,i}$; the received signal at eavesdropper $m$ when there is a communication from node $i$ to node $j$ is denoted by $Z_m(i,j)$, the additive noise at receiver $j$ by $V_j$ and at eavesdropper $m$ by $W_m$. The set of all positive integers smaller than or equal to $N$ is denoted by $[N]$. There is a transmit power constraint at each friendly node $i$, that is, $E[|X_i|^2] \leq P_i$ for $i \in [N_f]$. Then, for a communication between the transmitting node $i$ and the receiving node $j$, we use the following additive white Gaussian model:

$$Y_{j,i} = d_{j,i}^{-\beta/2} X_i + \sum_{k \in M_{i,j}} d_{j,k}^{-\beta/2} X_k + V_j$$

$$\hat{Y}_{k,i} = d_{k,i}^{-\beta/2} X_i + V_k, \quad k \in M_{i,j},$$

where $V_j, j \in [N_f]$ are assumed to be independent zero mean Gaussian random variables with variance $\sigma^2$, $d_{i,j}$ is the distance between nodes $i$ and $j$, $\beta$ is the path-loss coefficient [10] and $M_{i,j} \equiv [N_f] \setminus \{i, j\}$. The received signal at eavesdropper $m$ when there is a communication between nodes $i$ and $j$ equals

$$Z_m(i,j) = r_{m,i}^{-\beta/2} X_i + \sum_{k \in M_{i,j}} r_{m,k}^{-\beta/2} X_k + W_m,$$  

for all $m \in [N_e]$. In (2) $r_{m,i}$ is the distance between the eavesdropper $m$ and the node $i$, and $W_m$ represents white Gaussian noise.

The natural non-cooperative communication between any pair of friendly nodes in the network will be point to point, and as we shall show later, in that case the network will be very vulnerable, since the eavesdroppers can arbitrarily move and approach each of the sources. The point to point capacity (without any relaying) between node $i$ and $j$ is given by

$$C_{pp}(i,j) = \log_2 \left( 1 + \frac{P_i d_{j,i}^{-\beta}}{\sigma^2} \right).$$

Here, for simplicity we omit the factor $1/2$ in front of all capacity expressions. Obviously, $C_{pp}(i,j) = C_{pp}(j,i)$, since $d_{i,j} = d_{j,i}$.

In order to improve the secrecy we observe what happens when all legitimate relays help the communication between $i$ and $j$. All relays can operate in full duplex mode, that is, they can receive and transmit at the same time. There are a total of $M = N_f - 2$ relays that help any communication pair. Since the capacity of the relay channel is not known, we use the following upper bound:

$$C(i,j) \leq \log_2 \frac{\sigma^2 + \min\{A_{i,j} P_i, (P_t + P_{i,j}^+) D_{i,j}\}}{\sigma^2 + \sum_{c=1}^{d_{i,j}} \frac{B_{i,j} (d_{i,j}^{-\beta} P_{c} + \sigma^2)}{(A_{i,j} - d_{i,j}^{-\beta})^c}} P_i,$$

and lower bound:

$$C(i,j) \geq \log_2 \left( 1 + \frac{(A_{i,j} - d_{i,j}^{-\beta}) + 2 \sqrt{B_{i,j} (d_{i,j}^{-\beta} P_{c} + \sigma^2)}}{\sigma^2 + \sum_{c=1}^{d_{i,j}} (A_{i,j} - d_{i,j}^{-\beta})^c P_{i,j}^+} P_i \right)$$

as in [11]. In the above equations

$$P_{i,j}^+ = \sum_{k \in M_{i,j}} P_k, \quad A_{i,j} = d_{i,j}^{-\beta} + \sum_{k \in M_{i,j}} d_{i,k}^{-\beta},$$

$$B_{i,j} = \sum_{k \in M_{i,j}} \frac{d_{i,k}^{-\beta} P_k + \sigma^2}{d_{i,k}^{-\beta} d_{i,j}^{-\beta}}, \quad D_{i,j} = d_{i,j}^{-\beta} + \sum_{k \in M_{i,j}} d_{i,k}^{-\beta}.$$

The above expressions are valid for all $i, j \in [N_f]$. The capacity of the $m$-th eavesdropper channel is modeled as that of the multiple-access channel, since that is the best any of the eavesdroppers can receive from $N_f - 1$ nodes (the transmitting node $i$ plus the helping $N_f - 2$ nodes); that is

$$C_m^E(i,j) = \log_2 \left( 1 + \frac{1}{\sigma^2} \left( \frac{P_i}{r_{m,i}^{-\beta}} + \sum_{t=1}^{M} \frac{P_t}{r_{m,t}^{-\beta}} \right) \right), m \in [N_e].$$

We simplify the analysis by studying the following achievable secrecy rate when $i$ communicates to $j$

$$C_s(i,j) = \min_{m \in [N_e]} \left[ C(i,j) - C_m^E(i,j) \right]^+, \quad m \in [N_e]$$

where $x^+ = \max(x, 0)$. Note that (7) is determined by the eavesdropper with the strongest channel. In the sequel of the paper, for simplicity we refer to the expression above as the secrecy capacity.
III. IMPACT OF COOPERATION ON SECRECY CAPACITY

In this section we examine the impact of cooperation on the secrecy capacity between two communicating nodes. In a network with \( N_f \) friendly nodes, any two communicating nodes can use the remaining \( M = N_f - 2 \) nodes as relays. The secrecy capacity between the nodes \( i \) and \( j \) is denoted as \( C_s(i,j) \), for any pair \((i,j), \ i,j = 1, 2, \ldots, N_f\).

We use directed weighted graphs to represent the existence of positive secrecy capacity between any pair of communicating nodes. Such graphs are called directed secrecy graphs in [5] and [6]. Each communicating node is represented as a vertex. The existence of an edge from vertex \( i \) to vertex \( j \) signifies that the secrecy capacity \( C_s(i,j) \) from node \( i \) to node \( j \) is positive. The weight of an edge between \( i \) and \( j \) is \( C_s(i,j) \).

As in graph theory, we use an adjacency matrix to represent which of the nodes are connected in our network (graph) of \( N_f \) nodes. The adjacency matrix of a directed weighted graph with \( n \) vertices is an \( n \times n \) matrix \( A = \{a_{i,j}\} \) such that \( a_{i,j} \) is equal to the weight of the edge between vertices \( i \) and \( j \) when there is an edge. Otherwise \( a_{i,j} = 0 \). In our case, by convention we take \( a_{i,i} = Q \), where \( Q \) is some large number.

Throughout the paper we use a sample network with \( N_f = 6 \) friendly nodes and \( N_e = 2 \) eavesdroppers. We calculate the secrecy capacity between any pair of friendly nodes under the following assumptions: (i) the transmission power of all nodes is equal and is denoted by \( P \); (ii) the ratio \( P/\sigma^2 = 10 \) where \( \sigma^2 \) is the noise power. Figure 1 shows a particular network with six friendly nodes and two eavesdroppers. The number beside each directed edge is the corresponding secrecy capacity between the two nodes. There is an edge only if the secrecy capacity is positive. Note that in general the adjacency matrix is non-symmetric. The symmetry between nodes 3 and 4 in Figure 1 comes from the fact that the closest eavesdropper is at the same distance to both nodes 3 and 4.

For this example, we have the following adjacency matrix:

\[
A = \begin{pmatrix}
Q & 0.031 & 0 & 0 & 0 & 0 \\
0 & Q & 0.018 & 0 & 0 & 0 \\
0 & 0.053 & Q & 0.573 & 0 & 0 \\
0 & 0 & 0.573 & Q & 0.048 & 0 \\
0 & 0 & 0 & 0 & Q & 0.368 \\
0 & 0 & 0 & 0 & 0.432 & Q \\
\end{pmatrix}.
\]

The impact of cooperation depends heavily on the relative location of relay nodes with respect to the communicating nodes and eavesdroppers [12]. Therefore, rather than analyzing individual cases we observe what happens on average. We employ Monte Carlo simulations [13] to numerically estimate these average values. The positions of all nodes (communicating nodes, relays and eavesdroppers) are chosen to be mutually independent and uniformly distributed random variables over the region \([0,10] \times [0,10]\). In our simulations we calculate the probability that the secrecy capacity between the two communicating nodes \( i \) and \( j \) is positive, i.e., \( \Pr\{C_s(i,j) > 0\} \). As explained earlier, the existence of positive secrecy capacity is sufficient to allow two communicating parties to share secrets e.g. a master key. We analyze four cases, which are explained in the remainder of this section.

A. No cooperation

First we analyze the case without relay nodes, i.e., the non-cooperative scenario. If the capacity of the communication channel between the transmitter and any of the eavesdroppers is larger than the capacity of the channel between the two communicating nodes, then \( C_s = 0 \), otherwise, \( C_s > 0 \). The line denoted with \( M = 0 \) in Figure 2 gives the probability that the secrecy capacity \( C_s > 0 \) between the two communicating nodes as a function of the number of eavesdroppers \( N_e \). It is not difficult to conclude that \( \Pr\{C_s > 0, N_e\} = 1/(1 + N_e) \). \( C_s > 0 \) if the receiving node is closer to the transmitting node than any of the eavesdroppers. In other words, \( C_s > 0 \) if the receiving node is the closest node to the transmitting node amongst the set of 1 + \( N_e \) nodes: 1 receiving node and \( N_e \) eavesdroppers. If \( d(n_t,n_r) \) is used to denote the distance between the transmitting and the receiving node, and \( d(n_t,n_e) \) is the distance between the transmitting node and an eavesdropper, then \( \Pr\{C_s > 0, N_e\} = \Pr\{d(n_t,n_r) < d(n_t,n_e) \text{ for all } N_e \text{ eavesdroppers}\} \). Because of our assumption that the positions of all nodes are i.i.d. random variables with uniform distribution in the region \([0,10] \times [0,10]\), the probability of this event is \( 1/(1 + N_e) \).

B. Single hop cooperation with multiple parallel relays

Next we analyze the case with multiple parallel relays. As expected, the presence of multiple relays increases the channel capacity of the legitimate receiver. However, the capacity of the channels to the eavesdroppers increases at the same time. Upper and lower bounds for the capacity
of the main channel are given by (4) and (5), respectively. The capacity of each eavesdropper is given by (6). In this paper we assume that the eavesdroppers do not cooperate. Thus, the secrecy capacity of the main channel is determined by the strongest eavesdropper and is given by (7). Figure 3 gives the probability that the secrecy capacity $C_s$ between two communicating nodes is positive as a function of the number of relay nodes $M$. The number of eavesdroppers $N_e$ is the parameter. In Figure 3 the non-cooperative case corresponds to $M = 0$ in the upper-bound curve. One can note that the existence of one relay $M = 1$ has negative impact on the secrecy capacity compared to the non-cooperative case. Adding more relays increases the upper bound on the probability $\Pr\{C_s > 0\}$, but the upper bound is still smaller than the probability $\Pr\{C_s > 0\}$ for the non-cooperative case. This observation becomes more obvious from Figure 2, which gives the probability that the secrecy capacity $C_s$ between the two communicating nodes is positive as a function of the number of eavesdroppers $N_e$, where the number of relay nodes $M$ is the parameter.

For both upper bound and lower bound on the probability $\Pr\{C_s > 0\}$, it is valid that $\Pr\{C_s > 0, N_e, M | M > 0\} < \Pr\{C_s > 0, N_e, M | M = 0\}$.

We conclude that the presence of randomly positioned relay node(s) on average has a negative impact on the secrecy capacity and secrecy region. In order to benefit from the presence of relay nodes, they have to be carefully positioned taking into account the relative positions of the communicating nodes and the eavesdroppers. This is examined in the next subsection.

C. Single hop cooperation with the best relay

In this subsection we consider a case in which the strongest relay is selected from a set of randomly positioned relays. It is assumed that each pair of communicating nodes can choose only one relay node, and it is the relay node which most improves the secrecy capacity. If there exists no relay node that improves the secrecy capacity of the main channel, then no relay will be used. Clearly, the secrecy capacity in this case is lower bounded by the non-cooperative case. We call this type of cooperation “single hop cooperation with the best relay.”

The positive impact of the single hop cooperation with the best relay is depicted in Figure 4. Both the lower-bound and the upper-bound curves are monotonically increasing with $M$, which means that using only the best relay improves the probability that there is positive secrecy capacity between two communicating nodes. In other words, as the number of friendly nodes $M$ increases, the probability that there is at least one relay that improves the secrecy capacity of the main channel also increases. Note from Figure 4 that although probability $\Pr\{C_s > 0\}$ increases when single hop cooperation with the best relay is used, the probability is still far from 1. For $M = 10$ and $N_e = 1$, $\Pr\{C_s > 0\}$ increases from 0.5 for the non-cooperative case to 0.693 for the single hop cooperation with the best relay. This means that in a network with $N_f = 12$ cooperating nodes and only 1 eavesdropper, as much as 30.7% of the pairs of friendly nodes will be unable to communicate secretly. The following adjacency matrix gives the upper bound on the secrecy capacity between any pair of nodes from the network given in Figure 1 when single hop cooperation with the best relay is used.
relay is used:

\[
A = \begin{pmatrix}
Q & 0.031 & 0 & 0 & 0 & 0 \\
0 & Q & 0.018 & 0 & 0 & 0 \\
0 & 0.053 & Q & 0.573 & 0 & 0 \\
0 & 0 & 0.573 & Q & 0.048 & 0 \\
0 & 0 & 0 & 0.023 & Q & 0.368 \\
0 & 0 & 0 & 0.023 & 0.432 & Q
\end{pmatrix}.
\]

Due to the cooperation with the best relay, the secrecy capacity from nodes 5 and 6 to node 4 now becomes positive.

A question naturally arises: Is there another type of cooperation that can increase the number of pairs of communicating nodes that can communicate secretly? We describe one improvement to cooperative relaying in the next subsection.

**D. Cooperation with multiple hops**

We consider the case in which a secret needs to be transferred between two nodes. If the secrecy capacity is positive, then the two nodes can exchange the secret between them. If there is no secrecy capacity between the two nodes, then they can try to use other friendly nodes to help them share a secret. For example, in the network shown in Figure 1, there is zero secrecy capacity between nodes 1 and 6. However, node 1 can send a secret to node 6 via the following route: 1-2-3-4-5-6. In this section we assume that none of the friendly nodes is compromised, i.e., all of them are trustful. We are again interested in the probability that a secret can be transferred between two nodes via multiple hops.

As explained earlier, the existence of secrecy channels between pairs of friendly nodes in a network of friendly and eavesdropping nodes can be represented using a directed weighted graph and its corresponding adjacency matrix. Then, transferring a secret between two nodes via multiple hops is equivalent to the “reachability” question from graph theory. It is a well-known result from graph theory (e.g., see [14]) that the existence of a path between any two vertices is determined by the graph’s transitive closure. The adjacency matrix determines only which nodes are adjacent to each other. On the other hand, the transitive closure answers the reachability question: is there a path between any two vertices? Usually, transitive closure is stored as a Boolean matrix:

\[
G = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

Above \( \land \) and \( \lor \) denote “boolean and” and “boolean or” operators, respectively. The transitive closure for the sample network from Figure 1 is given by:

\[
G^+ = \sum_{k=1}^{n} \left( G \cdot \left( G^+ \right)^{k+1} \right).
\]

A new unweighted graph can be formed in which nodes of the original graph belonging to the same cycle are merged together to form a single new node. After doing the following grouping \{1\}, \{2,3,4\}, \{5,6\}, the new graph has the following adjacency matrix:

\[
B = \begin{pmatrix}
1 & 1 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.
\]

Figures 5, 6, and 7 give the probability that a node can reach another node in the network via a route consisting of communication links with \( C_s > 0 \). In Figures 5 and 6 the secrecy capacity between two nodes is calculated using the no-cooperation case. It is obvious that the “cooperation with multiple hops” has significant impact on the probability that two nodes secretly communicate via a route consisting of communication links with \( C_s > 0 \). For example, for \( N_e = 1 \), \( \Pr(C_s > 0) = 0.5 \) without cooperation. If \( M = 10 \) friendly nodes are used, the probability that two nodes can share a secret, increases to 0.775, and further to 0.917 for \( M = 28 \). It is clear then, that this probability increases with the number of friendly nodes in the network. Figure 7 shows the results from combining the “cooperation with the best relay” and the “cooperation with multiple hops.”
The secrecy capacity between two nodes is improved using the cooperation with the best relay. Then we calculate the probability that two nodes can share a secret via a route consisting of communication links with $C_s > 0$. For the non-cooperative case, $\Pr\{C_s > 0\} = 0.5$ for $N_c = 1$. For the “cooperation with the best relay,” lower and upper bounds on $\Pr\{C_s > 0\}$ for $N_c = 1$ and $M = 18$ are 0.579 and 0.721, respectively. Finally, for the “cooperation with multiple hops and the best relay,” lower and upper bounds on $\Pr\{C_s > 0\}$ for $N_c = 1$ and $M = 18$ increase to 0.875 and 0.91, respectively.

**IV. COOPERATIVE JAMMING**

Friendly nodes that are close to the eavesdropper, or closer to the eavesdropper than to the legitimate receiver, are unlikely to be useful as relays. They can be more useful if turned into jammers, since in that case they can flood the eavesdropper with interference, which we hope to be much weaker at the legitimate receiver. In this section we study two cases: cooperation with the best jammer and cooperative relaying and jamming.

**A. Cooperation with the best jammer**

In this section we analyze the case in which a single node is used as a jammer. When node $m$ is jamming with power $P_m$, then the point to point capacity between nodes $i$ and $j$ is given by

$$C_{pp}(i, j, m) = \log_2 \left( 1 + \frac{P_d d_{i,m}^{-\beta}}{\sigma^2 + P_m d_{j,m}^{-\beta}} \right). \quad(10)$$

For a given jammer, secrecy capacity is again determined by the strongest eavesdropper as given by Eq. (7)

$$C_s(i, j, m) = \min_{e \in [N_c]} \left[ \log_2 \left( 1 + \frac{P_d d_{i,e}^{-\beta}}{\sigma^2 + P_m d_{j,m}^{-\beta}} \right) \right]. \quad(11)$$

Hence, the strongest eavesdropper is the node $e \in [N_c]$ that maximizes the following SNR:

$$\frac{P_d d_{i,e}^{-\beta}}{\sigma^2 + P_m d_{j,m}^{-\beta}}. \quad(12)$$

There is no trivial way to determine the jammer that maximally improves the secrecy capacity. Thus, we exhaustively analyze all friendly nodes and check whether there is a jammer which gives $C_s > 0$. The best jammer is the node $m \in [N_f]$ that maximizes Eq. (11).

We have conducted numerical simulations to compare the cooperation with the best jammer to the cooperation with the best relay. For the sake of simplicity, we assume that $P_m = P_1$. Improvements to the possibility for secure communication at the physical layer when cooperating with the best jammer are depicted in Figure 8, and Figure 9.

We observe that cooperation with the best jammer can significantly improve the probability for secure communication between two nodes. The probability $\Pr\{C_s > 0\}$ monotonically increases with the number of possible jammers $M$, where $M = 0$ corresponds to the no-cooperation
We expect that the probability $\Pr\{C_s > 0\}$ can be further increased with cooperative jamming if (i) $P_{m}$ is modified/optimized, and (ii) more than one friendly node is used as a jammer. We plan to consider these issues in further research.

Figures 10 and 11 show that it is better to use the friendly nodes as jammers than as relays.

### B. Cooperative relaying and jamming

In the single hop cooperation with the best relay scheme (see Section III-C) only the best relay cooperates with the transmitter. The other relays are idle. Here we choose to use some of the other relays too. We speculate that a relay close to an eavesdropper could be more helpful by jamming the eavesdropper rather than staying idle or trying to relay a message.

The secrecy rate is increased by means of widening the gap between the SNR at the legitimate receiver and the SNR at the eavesdroppers. Cooperating relays tend to increase secrecy rate by increasing SNR at the legitimate receiver more than they increase SNR at the eavesdroppers. Cooperative jamming aims to reduce the SNR at the eavesdroppers more than it is reduced at the legitimate receiver.

In this section, in addition to the best relay used for single hop cooperation, we also use a single node for jamming purposes. A relay and a jammer are used only if they increase the secrecy capacity. Exhaustive searching through all possible (relay, jammer) pair is done to identify the pair that mostly increases the secrecy capacity. Figures 10 and 11 illustrate the improvement in the probability of existence of a secrecy channel between two nodes when cooperation with the best relay and the best jammer is used.

Figure 12 shows that “cooperation with the best relay and the best jammer” is the superior cooperation strategy.

### V. Conclusion

In this work we have seen that cooperation can significantly improve information-theoretic secrecy in wireless networks. The type of cooperation is quite important for the resulting secrecy capacity. Randomly chosen relay nodes can have a negative impact on the secrecy capacity as shown in Section III-B. However, Section III-C shows that appropriately choosing the helping relay with the strongest channel can improve the secrecy capacity a great deal. Section III-D shows how information-theoretic secrecy can be used to establish a secure channel to distribute a master key between two communicating parties in a multi-hop manner. In Section IV, we have studied how both cooperative
jamming and a combination of jamming and relaying improves information-theoretic secrecy. If done appropriately, jamming is more useful than relaying.

**References**


