Increasing the Secrecy Capacity by Cooperation in Wireless Networks

Ninoslav Marina¹, Ranjan Bose², and Are Hjørungnes¹

¹UNIK - University Graduate Center, University of Oslo, Norway.
²Dep. of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi, India.

Abstract—Physical layer security is an emerging security field that explores the possibilities of achieving perfect secrecy data transmission between the intended network nodes, while possible malicious nodes that eavesdrop the communication obtain zero information. In this paper, we observe how node cooperation improves the physical layer security of a simple wireless network by reducing the surface of the geographical area in which the malicious nodes can listen to the transmitted data from the source to the destination. Our analysis and simulation results show a dramatic improvement even by cooperation with only one relay node. The improvement gets better by adding more cooperating nodes. We also observe that if cooperating nodes are closer to the line that connects the source and the destination node, the region in which the malicious node can profit from the eavesdropping gets smaller.

I. INTRODUCTION

In the future wireless networks that will be decentralized and ad-hoc in nature, various types of mobile terminals will join and leave at any moment. This aspect makes the network vulnerable and susceptible to attacks. Anyone within communication range can listen to the broadcasted information. Currently, different cryptographic methods with high level of security are employed, however, there is no system with perfect security on the physical layer. Hence, the physical layer security is regaining a new attention. The main goal of this paper is to show that cooperation among the “friendly” nodes can increase the physical layer security of the system. Since the system is wireless, we cannot guarantee perfect security. This comes from the fact that the malicious node (also called eavesdropper) can stay arbitrarily close to the transmitting node (also called source) and, hence, listen to the broadcasted information. Therefore, there is a region (area) around the source, in which it is not possible to have perfect secrecy. Here we show that the cooperation among the nodes can minimize this region. In approaches where physical layer security is applied, the main objective is to maximize the rate of reliable information from the source to the intended destination, while all malicious nodes are kept as ignorant of that information as possible. This maximum reliable rate is known as secrecy capacity. We will see later that the secrecy capacity in the abovementioned region vanishes. That means in order to have a perfect secrecy the malicious nodes must be kept outside this area.

The secrecy capacity was initially introduced by Aaron Wyner, who defined the wiretap channel and established the possibility to create almost perfect secure communication links without relying on private (secret) keys [1]. Wyner showed that when the eavesdropper channel is a degraded version of the main channel, the source and the destination can exchange perfectly secure messages at a non-zero rate. The main idea proposed by him is to exploit the additive noise impairing the eavesdropper by using a stochastic encoder that maps each message to many code-words according to an appropriate probability distribution. With this scheme, a maximal equivocation (conditional uncertainty) is induced at the eavesdropper. In other words, a maximal level of secrecy is obtained. By ensuring that the equivocation rate is arbitrarily close to the message rate, one can achieve perfect secrecy in the sense that the eavesdropper is now limited to learn almost nothing about the source-destination messages from its observations. Follow-up work by Leung-Yan-Cheong and Hellman characterized the secrecy capacity of the additive white Gaussian noise (AWGN) wiretap channel [2]. In their landmark paper, Csiszár and Körner generalized Wyner’s approach by considering the transmission of confidential messages over broadcast channels [3]. Recently, there have been considerable efforts on generalizing these studies to the wireless channel and multi-user scenarios (see [4–11] and references therein).

A model for the relay channel was introduced and studied in the pioneering work by van der Meulen [12–14]. Substantial advances in the theory were made by Cover and El Gamal, who developed two fundamental coding strategies for the relay channel [15]. A combination of these strategies achieves capacities for several classes of degraded memoryless relay channels. Most of the work done so far was related to memoryless relay channels with or without feedback. Most of the research related to relay channels is related to the increase of the transmission data rate. In this paper, we investigate how the cooperation can improve the security of a given wireless network. In other words, we see that the secrecy capacity can be improved by cooperation between the nodes. More precisely we analyze the so-called secrecy region, that is, the geographical area in which the secrecy capacity is zero. Obviously, one would like to design a system with a minimal secrecy region. Our results show that by a proper selection of the cooperating nodes the secrecy area could be minimized. Here, we analyze the Gaussian parallel multiple relay network. Although, the
capacity of this network is not known, we use its upper and lower bounds, with a hope that our results will initiate additional thinking in this interesting and important research area.

The rest of the paper is organized as follows: In Section II, the system model is described, while in Section III, the concept of secrecy capacity is explained and the main expressions are derived. The numerical results and simulations are presented in Section IV and the paper is concluded in Section V.

II. System Model

Observe the network in Fig. 1. There is a source node that transmits data to a destination node, while a malicious node “listens” to the transmitted information. There are several relay nodes that help the source by relaying the transmitted data.

The coefficients $h_i,s_i$, $i=1,2,\ldots,M$, are fixed and assumed to be known throughout the network. Moreover, that in order to get a full use of the signals transmitted from the source and the relay nodes, it must be fully synchronized with all of them. To capture the effect of synchronization, we model the received signal at the malicious node as follows

$$Y_m[j] = h_{m,s} \sqrt{q} X[j] + \sum_{i=1}^{M} h_{m,i} \sqrt{k_i} X[i] + Z_m[j],$$

where $Z_m[j]$ is a sequence of i.i.d.

(i.i.d.) circularly symmetric complex Gaussian random variables of zero mean and variance $\sigma^2$.

Similarly, $d_{m,i} = d_{m,s}^{-\beta/2}$ and $h_{m,i} = d_{m,i}^{-\beta/2}$, $i=1,2,\ldots,M$. That means the malicious node is perfectly synchronized with the source node, while $d_{m,i} = d_{m,s}^{-\beta/2}$, $i=1,2,\ldots,M$. More precisely, $q$ is the fraction of the source transmitting power that will be received by the malicious node as useful signal for itself, while $(1-q)$ is the fraction of the source power that makes interference at the malicious node. If $q=1$, that means the malicious node is perfectly synchronized with the source node, while if $q=0$ there is no synchronization and the malicious node receives only noise from the source. Similarly, $k_i$ is the fraction of the transmitting power of Relay Node $i$ that will be received by the malicious node as useful signal for itself, while $(1-k_i)$ is the fraction of the power of Relay Node $i$ that makes interference at the malicious node.

The same explanation is valid for the parameters $k_i$. That means, an almighty eavesdropper will have $q = k_i = 1$ for
all \(i = 1, 2, \ldots, M\) and a “dummy” eavesdropper will have \(q = k_i = 0\) for all \(i = 1, 2, \ldots, M\). In the former case, the vulnerability region will be maximal, while in the latter, it vanishes, i.e., we have a perfect secrecy system. In order to make the eavesdropper capabilities closer to reality, we introduce two models to describe the synchronization parameters as a function of the distance between the eavesdropper and the eavesdropped node. The first model is the exponential model, defined as

\[
q = e^{-d_{m,i}}, \\
k_i = e^{-d_{m,i}},
\]

and we call it Model 1. The second model is the Gaussian model, defined as

\[
q = e^{-a^2_{m,i}}, \\
k_i = e^{-a^2_{m,i}},
\]

and we call it Model 2.

For notational convenience, we use similar definitions as in [16], that is

\[
a_M = d_{d,s}^{-\beta} + \sum_{i=1}^{M} d_{i,s}^{-\beta}, \\
b_M = \sum_{i=1}^{M} d_{i,s}^{-\beta} P + \sigma^2, \\
d_M = d_{d,s}^{-\beta} + \sum_{i=1}^{M} d_{i,s}^{-\beta},
\]

With all these assumptions we will be able to determine the bounds on the secrecy capacity, since the capacity of a general non-degraded relay channel is not known in general.

Firstly, the capacity of the main channel (the parallel relay general non-degraded relay channel is not known in general. The bounds on the secrecy capacity, since the capacity of a Gaussian channel (7).)

In other words, the secrecy capacity is positive only if \(C > C_m\). In order to analyze how cooperation improves the secrecy, we introduce two definitions:

**Definition 1:** The geometrical area (region) in which the secrecy capacity is positive is called secrecy region.

**Definition 2:** The geometrical area (region) in which the secrecy capacity vanishes is called vulnerability region.

Obviously, we want to keep all malicious nodes away from the vulnerability region. In other words, the system is more secure if its vulnerability region is minimized, or, equivalently, if its secrecy region is maximized. Note that if there are no cooperating relay nodes \((M = 0)\), it is easy to show that the vulnerability region is a circle (disk) since it that case the capacity of the main channel is the capacity of the point to point Gaussian channel between the source and the destination. More precisely, the region is determined from

\[
C = \log_2 \left( 1 + \frac{P d_{d,s}^{-\beta}}{\sigma^2} \right) < \log_2 \left( 1 + \frac{q P d_{d,s}^{-\beta}}{(1-q)\sigma^2} \right) = C_m.
\]

Solving (10), we get that the vulnerability region is the disk centered at the source given by

\[
d_{s,m} \leq \left( q d_{d,s}^{-\beta} + \frac{1 - q}{\sigma^2} \right)^{1/\beta}, \tag{11}
\]

for \(q \in (0, 1]\). If \(q = 1\), the disk is given by \(d_{s,m} \leq d_{d,s}\), while in the case \(q = 0\), the vulnerability region vanishes.

**Definition 3:** The normalized vulnerability region is the ratio between the vulnerability region and the surface of the disk with radius \(d_{d,s}\).

The definition tells us that if the normalized vulnerability region of a cooperative system is less than one, we get a smaller vulnerability region than that a non-cooperative system, or in other words, cooperation increases the network security.

In a cooperative system, where \(M \geq 1\), we can determine numerically the lower and the upper bound of the normalized vulnerability region. It is natural that it depends heavily on the position of the cooperating relays, and that the lower bound of the vulnerability region is determined by the upper bound of the capacity of the main channel (6), while the upper bound of the vulnerability region is determined by the lower bound on the capacity of the main channel (8).
IV. Simulations Results

In this section, we show several examples of the shape of the secrecy region in a cooperative system. We also observe how the average surface depend on the number of relays.

We fix the parameters as follows: $\sigma^2 = 1$, $P = P_i = 1$, $i = 1, 2, \ldots, M$ and $\beta = 2$. For these parameters, typical vulnerability regions are described in Fig. 2 for $M = 1$, $M = 3$, and $M = 5$, using Model 2. There, the source node is represented by a centrally positioned star, the destination node by a square position to the right of the source, and the randomly placed relay nodes by diamonds. Dark area (dots) represent the positions of a malicious node for which the secrecy capacity is positive. In other words, when the malicious node is positioned within the dark area, a perfectly secure communication is possible. It is obvious then, that the white area (islands) represent the vulnerability region. It is easily noticeable that the increased number of cooperating relays reduces the vulnerability region, hence, increasing the system secrecy. In order to understand the importance of the cooperation in increasing the secrecy capacity or, equivalently, the secrecy region of a certain network, we characterize the surface of the vulnerability region. To that end, we analyze how the normalized vulnerability region depends on the number of cooperative relays. The dependance of the normalized vulnerability region lower and upper bounds on the number of relay nodes, $M$, for $\beta = 2$, for both correlation models is shown in Fig. 3. Our simulations indicate that choosing cooperation relays that are closer to the line that connects the source and the destination, minimizes the vulnerability region. In Fig. 4 we observe the dependence of the normalized vulnerability region bounds on the number of relay nodes, for $\beta = 2$, for both the correlation models when the relays are placed on the line connecting the source and the destination. Note that for both models the secrecy region is smaller in this case. That indicates, the source should choose relays that are closer to the line in order to minimize the secrecy region. This is not surprising since the relaying is the most efficient when the relay node lies on the line of sight between the source and the destination. For $M = 1$, we notice in Fig 5 a minimum of the lower and upper bounds on the normalized vulnerability region if the relay is placed between the source and the destination. The minimum depends on $\beta, P, P_M$ as well as the chosen model. It is very intuitive that by choosing larger transmit power for either the source or the relays, makes the system more vulnerable, and, hence, the secrecy region larger. Finally, we would like to comment that the correlation Model 2 is worse than the correlation Model 1. This comes from the properties of the exponential and the Gaussian function and how they affect the secrecy capacity.

![Fig. 2. Examples of the lower and upper bounds on the shape of a typical vulnerability region for $M = 1$ (upper), $M = 3$ (middle), and $M = 5$ (lower).](image1)

![Fig. 3. Lower bound (LB) and upper bound (UB) of the normalized vulnerability region for $\beta = 2$ and the correlation Model 1 (up) and Model 2 (down) as a function of the number of cooperating relays $M$.](image2)
Fig. 4. Lower (LB) and upper bound (UB) of the normalized vulnerability region for $\beta = 2$ and the correlation Model 1 (up) and Model 2 (down) as a function of the number of cooperating relays $M$ that are placed on the line between the source and the destination.

V. Conclusions

We demonstrated that the physical layer security of a network can be increased by cooperation. Depending on the capabilities of the malicious node, one could improve a lot the security, by minimizing the vulnerability region. As we include more and more relays, the increase in the improvement is less and less. The most dramatic improvement is obtained by cooperation with one relay and for each additional relay the improvement that is obtained is smaller and smaller. From the simulation results, we see that depending on the correlation model of the eavesdropper, we have different size of the vulnerability region. In addition to this, the source should choose relays that stay closer to the line that connects the source and the destination in order to minimize the secrecy region. Depending on the system parameters there is a distance between the source and the relay node that makes the region minimal. The main message of the paper is that by a simple analysis we have shown that cooperation can dramatically improve the physical layer security in a given wireless network. One has to be aware, however, that the security improvement is not simply because of the reduction of the transmission range between the hops in a multihop communication setting. It actually comes from the fact that the capacity of the main channel is much more increased by cooperation, than the capacity of the eavesdropper channel can profit from eavesdropping on multiple relay nodes in addition to the source.

REFERENCES