Characterization of the Secrecy Region of a Single Relay Cooperative System

Ninoslav Marina
School of Engineering and Applied Science
Princeton University
Princeton, NJ 08544

Are Hjørungnes
UNIK – University Graduate Center
University of Oslo
Norway

Abstract—Security is an important aspect for the future wireless networks. Since the number of network nodes increases constantly, and, in addition, the networks are decentralized and ad-hoc in nature, it becomes more challenging to apply the current cryptographic methods that require exchange of keys between the communicating parties. Information-theoretic secrecy is an emerging security field that explores the possibility of achieving perfect secrecy data transmission between the intended network nodes, while possible malicious nodes (also called eavesdroppers) are kept ignorant of the transmitted information. In other words, that is the ability of the physical layer to provide security (beside the reliability) of the transmitted (broadcasted) data. For that reason, it is often called physical layer security. In this paper we observe how a simple cooperative network with one relay node can improve the physical layer security by decreasing the area in which the eavesdropper can reside and listen to the information transmitted to the destination. This region is called vulnerability region and we provide its characterization. Under certain conditions, the vulnerability region vanishes, which makes our wireless system perfectly secure for any position of the eavesdropper within the wireless network.

I. INTRODUCTION

Information-theoretic secrecy is a concept initially introduced by Shannon [1]. Wyner defined the wiretap channel and established the possibility to create almost perfect secure communication links without relying on exchange of private keys [2]. He showed that when the channel between the source and the eavesdropper, called *eavesdropper channel* is weaker than the channel between the source and the destination, called *main channel*, the source and the destination can exchange perfectly secure messages at a positive rate. At the same time the eavesdropper is not able to receive any information. In that case, we say that the *secrecy capacity* is positive. 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 [3] characterized the secrecy capacity of the additive white Gaussian noise (AWGN) wiretap channel. In their landmark paper, Csiszár and Körner [4] generalized Wyner's approach by considering the transmission of confidential messages over broadcast channels. Recently, there have been considerable efforts on generalizing these studies to the wireless channel and multi-user scenarios

(see [5]–[12] and references therein).

A model for the relay channel was introduced and studied in the pioneering works by van der Meulen [13]–[15]. Substantial advances in the theory were made by Cover and El Gamal [16], who developed two fundamental coding strategies for the relay channel. 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. Usually, the research related to relay channels is aimed at the increase of the transmission data rate. Lai and El Gamal [17] studied the relay-eavesdropper channel, and they proposed a new method called noise-forwarding strategy. In [18], we study how cooperation with multiple relays can improve the information theoretic security. There, we introduce the *vulnerability region* and its surface as a measure of how secret a given cooperative network is. In addition, we study the bounds of the surface as a function of the number of cooperating relays.

In this paper, we characterize the vulnerability region in a single relay cooperative wireless network. Cooperation improves the physical layer security in the network by minimizing the area in which the secrecy capacity is zero. We realize that under certain conditions, this area, called vulnerability region, vanishes. In other words, in this case, we have a perfectly secure system and no matter where the eavesdroppers reside, they will not be able to receive any information intended to the desired destination. This will be possible by carefully designed codes that achieve the secrecy capacity and *without* any key exchange. The improvement in the security is achieved by increasing the capacity of the direct channel by the help of the relay, as well as decreasing the capacity of the eavesdropper channel by introducing interference (jamming) from the relay and the source. The cooperation by jamming was previously studied in [17] and [19].

The rest of the paper is organized as follows: In Section II, the system model is described, while in Section III, the characterization of the vulnerability region is provided. The conditions for which a perfect secrecy system can be obtained are discussed in Section IV, and the paper is concluded in Section V.

II. SYSTEM MODEL

Observe the four node relay-eavesdropper network in Fig. 1. There is a source node that transmits data to a destination node, while there is a malicious node (eavesdropper) that “listens” to the transmitted information. In the following, we will use the words eavesdropper and malicious node interchangeably. There is a single relay in the network that cooperates with the source by relaying the transmitted data and, hence, increasing the information-theoretic secrecy. We consider the standard

Fig. 1. Cooperative network with a source, a destination, a single cooperative relay, and a malicious node (eavesdropper).

Gaussian channel in which the channel coefficients are determined by the distance between the corresponding nodes raised to the negative power of the path loss coefficient β . The direct channel is represented by the standard relay channel

$$\begin{aligned} Y_d &= d_{d,s}^{-\beta/2} X_s + d_{d,r}^{-\beta/2} X_r + Z_d, \\ Y_r &= d_{r,s}^{-\beta/2} X_s + Z_r. \end{aligned} \quad (1)$$

Here, Y_d and Y_r are the received signals at the destination and the relay nodes, respectively, while, X_s and X_r are the transmitted signals from the source and the relay nodes, respectively. There is a power constraint on the transmitted signals from the source node

$$E[|X_s|^2] \leq P_s,$$

and from the relay node

$$E[|X_r|^2] \leq P_r.$$

The fading coefficients are determined only by the distance between the transmitting and the receiving nodes, such that the ratio of the received power at node B and the transmitted power from node A is given by $d_{B,A}^{-\beta}$ and β is the *path loss coefficient*. A more realistic model should include the random fading, however, in that case the whole analysis is getting more demanding. Here, we decided to consider only the simple attenuation due to the path loss, in order to get some initial ideas about the structure of the secrecy region. Both channels

in (1) have complex additive Gaussian noise, represented by Z_d and Z_r , having zero mean and unit variances.

The malicious node observes signals from both, the source and the relay and can receive part of their signals. Similarly as in [18], we assume that the source and the relay are smart enough to use part of their available power to introduce Gaussian interference at the malicious node. Hence, the received signal at the malicious node is represented by

$$Y_m = d_{m,s}^{-\beta/2} \sqrt{q} X_s + d_{m,r}^{-\beta/2} \sqrt{k} X_r + Z_m, \quad (2)$$

where by the coefficients q and k we model how perfectly the malicious node can listen to the source and the relay. We call q a *source synchronization coefficient* and k a *relay synchronization coefficient*. Note that $q, k \in [0, 1]$, $q = 1$ ($k = 1$) means that the malicious node is perfectly synchronized with the source (relay) and $q = 0$ ($k = 0$) means that the malicious node cannot receive anything from the source (relay). The additive Gaussian noise at the malicious node Z_m has zero mean and variance

$$\text{Var}(Z_m) = aP_s d_{m,s}^{-\beta} + bP_r d_{m,r}^{-\beta} + 1. \quad (3)$$

That means, beside the thermal noise with unit variance the source and the relay introduce some interference using part of their powers. The interference introduced by the source is generated by some portion of its power, that is aP_s . Here, $a \in [0, 1]$ is called *source interference coefficient* and naturally, $a + q \leq 1$. Similarly, bP_r is the portion of the relay power that is used to “disturb” the malicious node, where $b \in [0, 1]$ is called *relay interference coefficient* and $b + k \leq 1$.

We assume that the positions of the source, the relay, and the destination are fixed. In that case the secrecy capacity will depend on the location of the malicious node. The secrecy capacity of this cooperative system with a single relay is given by

$$C_s = \max(C - C_m, 0), \quad (4)$$

where C is the capacity of the main channel between the source and the destination, and C_m is the capacity of the eavesdropper channel. Note that in this paper, the secrecy capacity is used in a weak manner defined by (4). In this case, the capacity of the main channel C will be the capacity of the relay channel. The capacity of the relay channel is not known, but here we do not need to use a particular expression for it, since we will analyze the vulnerability regions as a function of C . Since the secrecy capacity depends on the location of the malicious node, we may consider it as a function in the two dimensional plane, if without loss of generality we put the source at the origin and the destination node at the point (x_d, y_d) , with $d_{d,s} = \sqrt{x_d^2 + y_d^2}$. Without loss of generality, the location of the relay node is $(x_r, 0)$, $x_r \in \mathbb{R}$, meaning $d_{r,s} = |x_r|$. Also, without loss of generality, we may assume that the relay node and the destination node are always to the right of the source node, or in other words, $x_r > 0$ and $x_d > 0$. In that case, the secrecy capacity will be a function of the location of the malicious node (x_m, y_m) .

In order to proceed to the analysis, we use the following definitions, introduced in [18].

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

Therefore, the secrecy region is

$$\mathcal{R}_S = \{(x_m, y_m) : C_m(x_m, y_m) < C\}. \quad (5)$$

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

Hence, the vulnerability region is

$$\mathcal{R}_V = \{(x_m, y_m) : C_m(x_m, y_m) \geq C\}. \quad (6)$$

The goal is to minimize the vulnerability region which is equivalent to maximizing the secrecy region. In the rest of the paper, we characterize the vulnerability region. It is in our interest to determine under which conditions it is minimal.

III. CHARACTERIZATION OF THE VULNERABILITY REGION

In this section, we analyze the shape of the vulnerability region, which is the region in which if any malicious node resides, the communication between the source and the destination is not secret.

To start the analysis, note that by definition the secrecy capacity if a malicious node resides in the vulnerability region. In that case, within the vulnerability region, since $C_s = 0$, we have

$$C_m(x_m, y_m) \geq C. \quad (7)$$

From our assumptions, the malicious node receives information from both, the source and the relay, while at the same time the interference is coming from both of them as well. In that case, from (2) and (3) we have

$$C_m = \log_2 \left(1 + \frac{qd_{m,s}^{-\beta} P_s + kd_{m,r}^{-\beta} P_r}{ad_{m,s}^{-\beta} P_s + bd_{m,r}^{-\beta} P_r + 1} \right). \quad (8)$$

Hence, an alternative representation of the vulnerability region would be

$$\mathcal{R}_V = \left\{ (x_m, y_m) : \frac{qd_{m,s}^{-\beta} P_s + kd_{m,r}^{-\beta} P_r}{ad_{m,s}^{-\beta} P_s + bd_{m,r}^{-\beta} P_r + 1} \geq 2^C - 1 \right\},$$

where

$$\begin{aligned} d_{m,s} &= \sqrt{x_m^2 + y_m^2}, \\ d_{m,r} &= \sqrt{(x_m - x_r)^2 + y_m^2}. \end{aligned}$$

For convenience we can also express it as

$$\mathcal{R}_V = \{(r, \varphi) : c_1 d_{m,s}^{-\beta} + c_2 d_{m,r}^{-\beta} \geq 1\},$$

where

$$\begin{aligned} c_1 &= \left(\frac{q}{2^C - 1} - a \right) P_s, \\ c_2 &= \left(\frac{k}{2^C - 1} - b \right) P_r, \end{aligned} \quad (9)$$

and we switch to polar coordinates (r, φ) for the location of the malicious node. Moreover, since $x_m = r \cos \varphi$ and $y_m = r \sin \varphi$ we have

$$\begin{aligned} d_{m,s} &= r, \\ d_{m,r} &= \sqrt{r^2 + x_r^2 - 2x_r r \cos \varphi}. \end{aligned}$$

That means the vulnerability region is given by the polar coordinates

$$c_1 r^{-\beta} + c_2 (r^2 + x_r^2 - 2x_r r \cos \varphi)^{-\beta/2} \geq 1. \quad (10)$$

Depending on the sign of c_1 and c_2 , we observe four different cases.

Case 1: $c_1 \leq 0$ and $c_2 \leq 0$. In this case, since $r^{-\beta}$ and $(r^2 + x_r^2 - 2x_r r \cos \varphi)^{-\beta/2}$ are positive, it is straightforward that the vulnerability region vanishes. We shall see later that this is the only case for which the vulnerability region vanishes for any r and φ . Hence, this is the preferred case.

Case 2: $c_1 \leq 0$ and $c_2 > 0$. From (10) we have

$$\cos \varphi \geq \frac{r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{2/\beta}}{2x_r r}. \quad (11)$$

Hence, the vulnerability region is obtained as the union of the following two regions

$$\begin{aligned} \mathcal{R}_{2,1} &= \left\{ (r, \varphi) : \left| r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{2/\beta} \right| \leq 2x_r r, \right. \\ &\quad \left. |\varphi| \leq \arccos \left(\frac{r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{2/\beta}}{2x_r r} \right) \right\}, \end{aligned}$$

and

$$\mathcal{R}_{2,2} = \{(r, \varphi) : (r + x_r)^\beta (r^\beta - c_1) < c_2 r^\beta, \forall \varphi\}.$$

That gives

$$\mathcal{R}_V = \mathcal{R}_{2,1} \cup \mathcal{R}_{2,2}.$$

Case 3: $c_1 > 0$ and $c_2 \leq 0$. Note that if c_1 is positive, $r^\beta > c_1$ gives $c_1 r^{-\beta} < 1$ and since $c_2 \leq 0$, (10) will be an empty set. That means $\mathcal{R}_V$ is non-empty only if $r^\beta \leq c_1$. Then, from (10) we have, we have

$$\cos \varphi \leq \frac{r^2 + x_r^2 - \left(\frac{|c_2| r^\beta}{c_1 - r^\beta} \right)^{2/\beta}}{2x_r r}. \quad (12)$$

Therefore, the vulnerability region is obtained as the union of the following two regions

$$\begin{aligned} \mathcal{R}_{3,1} &= \left\{ (r, \varphi) : \left| r^2 + x_r^2 - \left(\frac{|c_2| r^\beta}{c_1 - r^\beta} \right)^{2/\beta} \right| \leq 2x_r r, \right. \\ &\quad \left. r \leq c_1^{1/\beta}, |\varphi| \geq \arccos \left(\frac{r^2 + x_r^2 - \left(\frac{|c_2| r^\beta}{c_1 - r^\beta} \right)^{2/\beta}}{2x_r r} \right) \right\}, \end{aligned}$$

Fig. 2. Shapes of the vulnerability region for $c_1 > 0$ and $c_2 \leq 0$ (Case 3). Here $c_1 = 0.05, 0.5, 1, 2, 3, 4$ and c_2 is fixed at -0.05 .

and

$$\mathcal{R}_{3,2} = \left\{ (r, \varphi) : r \leq c_1^{\frac{1}{\beta}}, \frac{|1 - \frac{x_r}{r}|^\beta (c_1 - r^\beta)}{|c_2|} < 1, \forall \varphi \right\}.$$

That gives

$$\mathcal{R}_V = \mathcal{R}_{3,1} \cup \mathcal{R}_{3,2}.$$

Note that Case 3 is equivalent to Case 2. We describe it here just for completeness with respect to (10). It is obvious that if we change the coordinate system and place the origin where the relay is, we shall get exactly the same results as in Case 2.

Different shapes of the vulnerability region for $c_1 > 0$ and $c_2 \leq 0$ (Case 3) are shown in Fig. 2. Here, $\beta = 3$ and $x_r = 0.8$. The source node is represented by a square at the origin, the relay node by a star and the shaded region around the source node is the vulnerability region. If the malicious node stays in this region the secrecy capacity is zero, i.e., secret communication at non-zero rate between the source and the destination is not possible. The shapes for Case 2 are exactly the same if the source and the relay change their places. We notice different shapes for different values of c_1 and c_2 .

Case 4: $c_1 > 0$ and $c_2 > 0$. Note that if $c_1 r^{-\beta} \geq 1$, (10) is true for all φ . In the case $r > c_1^{1/\beta}$, from (10), we have

$$\cos \varphi \geq \frac{r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{2/\beta}}{2x_r r}. \quad (13)$$

Then, the vulnerability region is obtained as a union of the following three sets

$$\begin{aligned} \mathcal{R}_{4,1} &= \left\{ (r, \varphi) : r \leq c_1^{\frac{1}{\beta}}, \forall \varphi \right\}, \\ \mathcal{R}_{4,2} &= \left\{ (r, \varphi) : \left| r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{\frac{2}{\beta}} \right| \leq 2x_r r, \right. \\ &\quad \left. r > c_1^{\frac{1}{\beta}}, |\varphi| \leq \arccos \left(\frac{r^2 + x_r^2 - \left(\frac{c_2 r^\beta}{r^\beta - c_1} \right)^{\frac{2}{\beta}}}{2x_r r} \right) \right\}, \end{aligned}$$

and

$$\mathcal{R}_{4,3} = \left\{ (r, \varphi) : r > c_1^{\frac{1}{\beta}}, \frac{(1 + \frac{x_r}{r})^\beta (r^\beta - c_1)}{c_2} < 1, \forall \varphi \right\}.$$

That gives

$$\mathcal{R}_V = \mathcal{R}_{4,1} \cup \mathcal{R}_{4,2} \cup \mathcal{R}_{4,3}.$$

Different shapes of the vulnerability region for $c_1 > 0$ and $c_2 > 0$ (Case 4) are observed in Fig. 3 for $\beta = 3$ and $x_r = 0.8$. The geometry of the vulnerability region is completely described for all possible values of c_1 and c_2 . In the following section we discuss most interesting case where the vulnerability region is zero, i.e., we have a perfect information-theoretic secrecy system.

IV. PERFECT SECRECY SYSTEM

From the previous analysis, we observe that if the coefficients c_1 and c_2 are negative, the system will be perfectly secure for any position of the eavesdropper. The values of

Fig. 3. Shapes of the vulnerability region for $c_1 > 0$ and $c_2 > 0$ (Case 4). Here $c_1 = 0.01, 0.03, 0.05, 0.5, 2, 4$ and c_2 is fixed at 0.05.

c_1 and c_2 depend on the transmit powers of the source and the relay, the capacity of the direct channel and the synchronization and interference coefficients of the source and the relay. In order to determine in which case both c_1 and c_2 are negative, we observe (9) and we find

$$C > \max \left\{ \log_2 \left(1 + \frac{q}{a} \right), \log_2 \left(1 + \frac{k}{b} \right) \right\}. \quad (14)$$

Since $\log(\cdot)$ is a continuous and increasing function and all coefficients are positive we may rewrite (14) that

$$C > \log_2 \left(1 + \max \left\{ \frac{q}{a}, \frac{k}{b} \right\} \right). \quad (15)$$

This tells us that if the coefficients q, a, k , and b are given, a perfect information-theoretic secrecy is guaranteed if the capacity of the relay channel is larger than the right hand side of (15).

In the following text we consider the special cases $a = 1 - q$ and $b = 1 - k$. Then, we get

$$C > -\log_2(\min\{1 - q, 1 - k\}). \quad (16)$$

Note, however that in reality the synchronization coefficients will depend on the proximity of the malicious node to the source and the relay node. An appropriate model for that is needed. In [18], two models for the synchronization coefficients are discussed. In Model 1 or the exponential model,

$$\begin{aligned} q &= e^{-d_{m,s}}, \\ k &= e^{-d_{m,r}}. \end{aligned} \quad (17)$$

In Model 2 or the Gaussian model,

$$\begin{aligned} q &= e^{-d_{m,s}^2}, \\ k &= e^{-d_{m,r}^2}. \end{aligned} \quad (18)$$

If Model 1 is used, from (16), we get a perfectly secure system if the malicious node is located such that

$$\begin{aligned} d_{m,s} &> -\ln(1 - 2^{-C}), \\ d_{m,r} &> -\ln(1 - 2^{-C}). \end{aligned} \quad (19)$$

If Model 2 is used, a perfectly secure system is obtained if

$$\begin{aligned} d_{m,s} &> \sqrt{-\ln(1 - 2^{-C})}, \\ d_{m,r} &> \sqrt{-\ln(1 - 2^{-C})}. \end{aligned} \quad (20)$$

Geometrically, this is a region outside of the union of the two circles centered at the source and the relay locations. The radii R of these circles are

$$R^{(1)} = -\ln(1 - 2^{-C}),$$

for Model 1, and

$$R^{(2)} = \sqrt{-\ln(1 - 2^{-C})},$$

for Model 2. The circles intersect if $d_{r,s} < 2R$. In the worst case, $d_{r,s} \geq 2R$, and we have an upper bound on the surface of the vulnerability region as the surface of two circles. For Model 1, the bound is

$$V_U^{(1)}(C) = 2\pi \ln^2(1 - 2^{-C}), \quad (21)$$

and for Model 2, it is

$$V_U^{(2)}(C) = -2\pi \ln(1 - 2^{-C}). \quad (22)$$

Fig. 4. The upper bound of the vulnerability region surface for Model 1 and Model 2 as a function of C .

The corresponding upper bounds on the surface of the vulnerability region are shown in Fig. 4. Note that for small C , Model 2 behaves better, while Model 1 is better for larger C . For large C , using the Taylor series expansion [20], $\ln(1 - 2^{-C}) \approx -2^{-C}$, the bounds (21) and (22) can be approximated as

$$\begin{aligned} V_U^{(1)}(C) &\approx \pi 2^{1-2C}, \\ V_U^{(2)}(C) &\approx \pi 2^{1-C}. \end{aligned} \quad (23)$$

Note that Model 1 and Model 2, although not realistic models, help us to understand what happens to the vulnerability region if the proximity is important for the malicious node to synchronize with the transmitting source and relay nodes.

V. CONCLUSIONS

We characterized the vulnerability region for different parameters of the four node relay-eavesdropper channel. It is shown that the physical layer security of this wireless network can be increased by cooperation. Depending on the capabilities of the malicious node, one could improve the security considerably, by minimizing the vulnerability region. We observe that under certain conditions a perfect information-theoretic

secrecy can be achieved by cooperation. In other words, a network with no vulnerability region can be obtained. This depends heavily on the assumed model for the synchronization and interference coefficients. We present an example in which for the earlier proposed Models 1 and 2 we numerically find the upper bound on the surface of the vulnerability region. Although the proposed analysis is for simplified models, we believe it could serve as a solid starting point to study the locations of the cooperating nodes in more complex networks, such that the physical layer security of the entire system is improved.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656 – 715, Oct. 1949.
- [2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355 – 1387, Oct. 1975.
- [3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 24, no. 4, pp. 451 – 456, Jul. 1978.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339 – 348, May 1978.
- [5] A. O. Hero, "Secure space-time communication," *IEEE Trans. on Inf. Theory*, vol. 49, no. 12, pp. 3235 – 3249, Dec. 2003.
- [6] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. of 41st Conference on Information Sciences and Systems*, Baltimore, MD, USA, Mar. 2007.
- [7] R. Negi and S. Goelm, "Secret communication using artificial noise," in *Proc. of IEEE Vehicular Technology Conference - Fall*, vol. 3, Dallas, TX, USA, Sep. 2005, pp. 1906 – 1910.
- [8] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. of IEEE Int. Symp. on Inf. Theory*, Adelaide, Australia, Sep. 2005, pp. 2152 – 2155.
- [9] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. of IEEE Int. Symp. on Inf. Theory*, Nice, France, Jun. 2007, pp. 2466 – 2470.
- [10] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. on Inf. Theory*, vol. 54, no. 6, pp. 2470 – 2492, Jun. 2008.
- [11] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. on Inf. Theory*, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.
- [12] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Secure collaborative beamforming," in *Proc. of the Forty-Seventh Annual Allerton Conference on Communication, Control, and Computing*, Allerton, IL, USA, Oct. 2008.
- [13] E. C. van der Meulen, "Transmission of information in a t -terminal discrete memoryless channel," Ph.D. dissertation, Department of Statistics, Univ. of California, Berkeley, 1968.
- [14] —, "Three-terminal communication channels," *Advances in Applied Probability*, vol. 3, no. 1, pp. 120 – 154, Spring 1971.
- [15] —, "A survey of multiway channels in information theory: 1961 – 1976," *IEEE Trans. on Inf. Theory*, vol. 23, no. 1, pp. 1 – 37, Jan. 1977.
- [16] T. M. Cover and A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Trans. on Inf. Theory*, vol. 25, no. 5, pp. 572 – 584, Sep. 1979.
- [17] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005 – 4019, Sep. 2008.
- [18] N. Marina, R. Bose, and A. Hjørungnes, "Increasing the secrecy capacity by cooperation in wireless networks," in *IEEE Personal, Indoor and Mobile Radio Communications Symposium (PIMRC 2009)*, Tokyo, Japan, Sep. 2009.
- [19] Z. Han, N. Marina, M. Debbah, and A. Hjørungnes, "Physical layer security game: How to date a girl with her boyfriend on the same table," in *Game Theory for Networks (GameNets 2009)*, Istanbul, Turkey, Sep. 2009.
- [20] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 6th ed. New York: Academic, 2000.