NETWORK-CODED COOPERATION FOR A TWO-USER WIRETAP CHANNEL

Rodrigo T. Kaido, Ohara K. Rayel, João Luiz Rebelatto and Richard Demo Souza

Department of Electronics
Federal University of Technology - Paraná
Curitiba, PR, 80230-901, Brazil
Email: rodrigokaido@gmail.com, ohara@eletrica.eng.br, {jlrebelatto, richard}@utfpr.edu.br

ABSTRACT

We evaluate the secrecy outage probability of a two-user network-coded cooperative network in the presence of an eavesdropper. We show through theoretic and numerical analyses that the secrecy can be increased through the use of network coding when compared to the direct transmission and traditional cooperative techniques.

***Index Terms*—** Cooperative communications, network coding, wiretap channel, secrecy outage probability.

1. INTRODUCTION

Information security has become a major concern in wireless communications, due to the broadcast nature of the wireless medium which allows eavesdroppers to potentially intercept any transmission. Information theoretic secrecy, introduced by Shannon in 1949 [1], is a promising approach towards increasing communication security. In [2], Wyner elaborated on the work of Shannon by introducing the so-called wiretap channel, which is composed of a pair of legitimate users communicating in the presence of an eavesdropper. Recent works have applied information theoretic secrecy ideas to wireless communications, showing that the randomness inherent to wireless channels can help in improving the secrecy of the network [3,4]. However, similarly to communication networks without secrecy constraints, the channel conditions dictate the network performance. It is necessary for the legitimate users to have some advantage over the eavesdropper in terms of instantaneous channel quality to guarantee the existence of secure communications.

Many techniques have been proposed to increase the secrecy in wireless networks. Some of them consider the use of multiple antennas [5, 6], or even adopt the concept of cooperative communications [7, 8], which is a technique that can increase the reliability of wireless communications [9, 10]. In cooperative networks, the nodes help each other by relaying their messages, and the transmission is usually divided in two phases: the so-called *broadcast phase* (BP), where the sources broadcast their own information frames (IFs), and the *cooperative phase* (CP), where the nodes transmit parity frames (PFs) to the destination, which are composed of redundant information related to their own IFs and/or to the IFs of their partners. One of the most well known cooperative protocols is the decode-and-forward (DF) [9], where the nodes just act as routers in the cooperative phase, relaying the IF from its partner, as illustrated in Fig. 2(a).

In [8], the authors presented a pioneering study on the secrecy of cooperative communications, by combining concepts of the relay [11] and wiretap [2] channels in the so-called relay-eavesdropper channel, as well as establishing the theoretical bounds for the rate-equivocation of the channel. More recently, the secrecy performance of a cooperative network under the DF protocol was carried out in [7], considering either a passive or an active eavesdropper. It was shown in [7] that cooperation is capable of increasing the network secrecy when compared to the direct transmission.

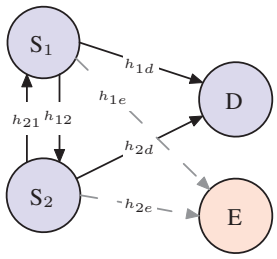


Fig. 1. System model. Two source nodes (S_1 and S_2) have independent information to transmit to a common destination (D) in the presence of an eavesdropper (E).

Another technique capable of increasing the reliability of cooperative networks is the network coding approach [12–14], where the users transmit linear combinations of different messages instead as just acting as routers, as illustrated in Fig 2(b). It was shown in [13, 14] that, if such linear combinations are performed over a large enough non-binary finite field GF(q), the system diversity order can be increased when compared to the traditional DF protocol, reducing the system outage probability.

Motivated by the promising performance of the network coding technique, in this work we evaluate the performance of such technique in a scenario subject to secrecy constraints, due to the presence of an eavesdropper. We present a closed-form equation for the secrecy outage probability (SOP) of the network, and validate the analysis through numerical results. Our work shows that the network coded cooperation achieves a higher diversity order and considerably outperforms the traditional DF protocol or the direct transmission when a low SOP is required.

The rest of this work is organized as follows. In Section 2 we introduce the system model, while Section 3 presents the SOP for the direct non-cooperative communication and for the traditional DF cooperative protocol. In Section 4 the outage probability of the network-coded cooperation for a two-user wiretap channel is introduced, and some numerical results are discussed in Section 5. Finally, Section 6 concludes the paper.

Notations: $\log(\cdot)$ denotes base-2 logarithm. $(x)^+$ means $\max\{0, x\}$. Lower-case boldface symbols represent vectors.

We acknowledge the support of CNPq, CAPES and Fundação Araucária.

2. SYSTEM MODEL

We consider a cooperative network composed of $M = 2$ sources having independent information to transmit to a common destination node. We assume the existence of a malicious eavesdropper, as illustrated in Fig. 1. Omitting the time index, the signal received by node j after a transmission performed by user i is given by

$$\mathbf{y}_j = \sqrt{P_i d_{ij}^{-m}} h_{ij} \mathbf{x}_i + \mathbf{n}_j, \tag{1}$$

where P_i corresponds to the transmission power, d_{ij} represents the distance between nodes i and j, m stands for the path-loss exponent, h_{ij} represents the block-fading coefficient, modeled as a Rayleigh independent identically distributed (i.i.d.) random variable. The additive white Gaussian noise is represented by $\mathbf{n}_j$.

We adopt the notation $i, j \in \{1, 2, d, e\}$ when referring to source 1 (S_1), source 2 (S_2), destination (D) and eavesdropper (E), respectively. The instantaneous signal-to-noise ratio (SNR) is defined as

$$\gamma_{ij} = \overline{\gamma}_{ij} |h_{ij}|^2, \tag{2}$$

where $\overline{\gamma}_{ij} = \frac{P_i}{d_{ij}^m \sigma_j^2}$ is the average SNR and σ_j^2 is the noise variance. As we assume a scenario in which S_1 and S_2 2 are at approximately the same distance from D, then $\overline{\gamma}_{1d} = \overline{\gamma}_{2d} = \overline{\gamma}_d$. Moreover, we also assume that both sources are at approximately the same distance from E, so that $\overline{\gamma}_{1e} = \overline{\gamma}_{2e} = \overline{\gamma}_e$.

Without secrecy constraints, assuming unitary bandwidth and Gaussian inputs, an outage event occurs when the mutual information $I_{ij} = \log(1 + \gamma_{ij})$ falls below a given target information rate R. The probability of such an event is called *outage probability*. For Rayleigh fading, it becomes

$$\begin{aligned} \mathcal{P}_{ij} &\triangleq \Pr\{I_{ij} < R\} \\ &= \Pr\left\{\gamma_{i,j} < 2^R - 1\right\} \\ &= 1 - \exp\left(-\frac{2^R - 1}{\overline{\gamma}_{ij}}\right). \end{aligned} \tag{3}$$

3. SECRECY OUTAGE PROBABILITY (SOP)

In the presence of an eavesdropper, taking S_1 as a reference, the instantaneous secrecy capacity is defined as [3, 4]

$$\mathcal{C}_s = (I_{1d} - I_{1e})^+. \tag{4}$$

Similarly to the case without secrecy constraints, the *secrecy outage probability* (SOP) is defined as the probability that $\mathcal{C}_s$ is less than a target secrecy rate R_s [4], so that

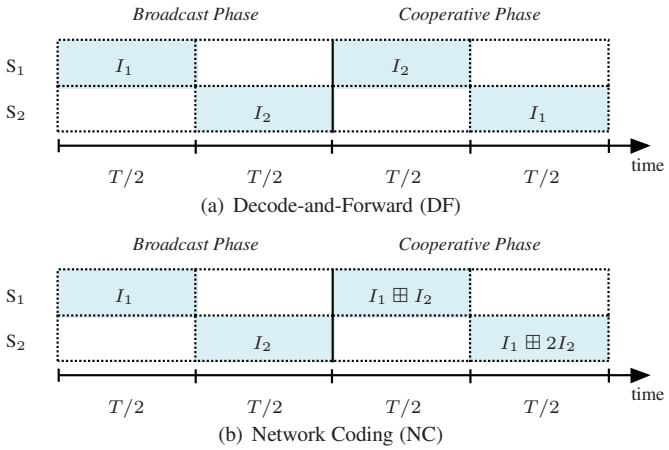
$$\mathcal{P}_s = \Pr\{\mathcal{C}_s < R_s\}. \tag{5}$$

The definition of SOP in (5) inherently handles two possibilities for the occurrence of an outage: *i)* The message is not recovered simultaneously by both D and E; *ii)* The message is correctly recovered by E, regardless of D.

3.1. Direct Transmission (DT)

For the non-cooperative direct transmission (DT) with secrecy constraints, considering that the transmission is subjected to Rayleigh fading and taking S_1 as a reference (the result is the same for S_2 due to symmetry), the SOP is [3]

$$\mathcal{P}_{s,\text{DT}} = 1 - \frac{\overline{\gamma}_{1d}}{\overline{\gamma}_{1d} + 2^{R_s}\overline{\gamma}_{1e}} \exp\left(-\frac{2^{R_s} - 1}{\overline{\gamma}_{1d}}\right). \tag{6}$$



(a) Decode-and-Forward (DF)

(b) Network Coding (NC)

Fig. 2. Time division channel allocation considering (a) Decode-and-Forward (DF) protocol; (b) Network Coding-based (NC) protocol. T represents the time-slot duration and the symbol $\boxplus$ in (b) stands for summation over a finite field.

3.2. Decode-and-Forward (DF)

In the DF protocol, after broadcasting their own IFs, nodes S_1 and S_2 retransmit their partner's IF in the cooperative phase, as illustrated in Fig. 2(a). Let us focus on the message from S_1 (the same result is valid to S_2 due the symmetry). The signal received at node $j \in \{2, d, e\}$ is given by

$$\mathbf{y}_j = \sqrt{P_1} h_{1j} \mathbf{x_1} + \mathbf{n}_j, \tag{7}$$

The outage probability at S_2 is then [9]

$$\begin{aligned} \mathcal{P}_{12} &= \Pr\left\{\gamma_{12} < 2^{2R} - 1\right\}, \\ &= 1 - \exp\left(-\frac{2^{2R} - 1}{\overline{\gamma}_{12}}\right). \end{aligned} \tag{8}$$

Note that in (8), when compared to (3), the rate is doubled in order to keep the same overall spectral efficiency as the direct transmission since in the DT scheme two IFs are transmitted in four time slots.

Let us consider a selective decode-and-forward (SDF) protocol [9] where S_2 only relays the message of S_1 in the cooperative phase when $\gamma_{12} > 2^{2R} - 1$ (the channel between S_1 and S_2 is not in outage). Upon receiving two copies of the same message, we consider that the destination performs maximal ratio combining (MRC). If S_2 could not recover the message from S_1, it retransmits its own message in the cooperative phase. The overall signal received at D containing the message from S_1 can then be written as [9]

$$\mathbf{y}_d = \begin{cases} \left(\sqrt{P_1} h_{1d} + \sqrt{P_2} h'_{2d}\right)\mathbf{x_1} + \mathbf{n}_d, & \text{if } \gamma_{12} \geq \gamma^{\text{th}}; \\ \left(\sqrt{P_1} h_{1d} + \sqrt{P_1} h'_{1d}\right)\mathbf{x_1} + \mathbf{n}_d, & \text{if } \gamma_{12} < \gamma^{\text{th}}; \end{cases} \tag{9}$$

where $\gamma^{\text{th}} \triangleq (2^{2R} - 1)$ and the superscript $'$ refers to the channel realization in the cooperative phase (h_{id} and h'_{id} are assumed to be independent). The signal received at E is also obtained from (9), through the replacement of D by E in the sub-indexes. The secrecy capacity of the DF scheme is then given by

$$\mathcal{C}_{s,\text{DF}} = \frac{1}{2}\Big(\log_2(1 + \gamma_d) - \log_2(1 + \gamma_e)\Big)^+, \tag{10}$$

where

$$\gamma_d = \begin{cases} \overline{\gamma}_{1d}|h_{1d}|^2 + \overline{\gamma}_{2d}|h'_{2d}|^2, & \text{if } \gamma_{12} \geq \gamma^{\text{th}} \\ \overline{\gamma}_{1d}\left(|h_{1d}|^2 + |h'_{1d}|^2\right), & \text{if } \gamma_{12} < \gamma^{\text{th}} \end{cases} \tag{11}$$

is the instantaneous SNR at D after combining the messages, obtained from (9), and γ_e is similarly defined. From the results in [3,9], it can be shown that the SOP of the DF scheme is given by:

$$\begin{aligned}\mathcal{P}_{s,\text{DF}} &= \Pr\{\mathcal{C}_{s,\text{DF}} < R_s\} \\ &= \Pr\{\mathcal{C}_{s,\text{DF}} < R_s | \gamma_{12} \geq \gamma^{\text{th}}\} \Pr\{\gamma_{12} \geq \gamma^{\text{th}}\} + \\ &\quad \Pr\{\mathcal{C}_{s,\text{DF}} < R_s | \gamma_{12} < \gamma^{\text{th}}\} \Pr\{\gamma_{12} < \gamma^{\text{th}}\} \\ &= 1 - \frac{\overline{\gamma}_{1d}}{\left(\overline{\gamma}_{1d} + \xi\,\overline{\gamma}_{1e}\right)^3} \exp\left(-\frac{\xi-1}{\overline{\gamma}_{1d}}\right) \times \\ &\quad \times \left[\overline{\gamma}_{1d}\left(\xi - 1 + \overline{\gamma}_{1d}\right) + \xi\,\overline{\gamma}_{1e}\left(\xi - 1 + 3\,\overline{\gamma}_{1d}\right)\right], \quad (12)\end{aligned}$$

where $\xi = 2^{2R_s}$.

4. NETWORK-CODED COOPERATION (NC)

In a non-binary network-coded (NC) based cooperative protocol, instead as just acting as routers, during the cooperative phase the nodes are able to transmit linear combinations of all the available IFs. If such linear combinations are performed over a high enough finite field, it is shown in [13] that gains in terms of diversity order can be achieved over the DF scheme.

Let us focus again on the message from S_1. If the inter-user channel is not in outage ($\gamma_{12} \geq \gamma^{\text{th}}$), we can see that D is able to recover S_1's message from any two out the following four received packets ($I_1,\ I_2,\ I_1 \boxplus I_2,\ I_1 \boxplus 2I_2$). The information packet from S_1 is not recovered by D when the direct transmission and at least two out of the three remaining packets cannot be decoded, which happens with probability [13]

$$\Pr\{\gamma_{1d} < \gamma^{\text{th}} | \gamma_{12} \geq \gamma^{\text{th}}\} \approx 3\mathcal{P}_o^3. \quad (13)$$

When the channel between S_1 and S_2 is in outage ($\gamma_{12} < \gamma^{\text{th}}$), S_1 and S_2 retransmit their own messages in the cooperative phase. Upon receiving two copies of the same message, we assume that D performs MRC, leading to the following outage probability [13]

$$\Pr\{\gamma_{1d} < \gamma^{\text{th}} | \gamma_{12} < \gamma^{\text{th}}\} \approx 0.5\mathcal{P}_o^2. \quad (14)$$

Similarly to the DF scheme, it was shown that the outage probability of the NC scheme is given by [13]

$$\begin{aligned}\mathcal{P}_{\text{NC}} &= \Pr\{\gamma_{1d} < \gamma^{\text{th}} | \gamma_{12} \geq \gamma^{\text{th}}\} \Pr\{\gamma_{12} \geq \gamma^{\text{th}}\} + \\ &\quad \Pr\{\gamma_{1d} < \gamma^{\text{th}} | \gamma_{12} < \gamma^{\text{th}}\} \Pr\{\gamma_{12} < \gamma^{\text{th}}\} \\ &\approx 3.5\left[1 - \exp\left(-\frac{2^{2R}-1}{\overline{\gamma}_{1d}}\right)\right]^3. \quad (15)\end{aligned}$$

We can see from (15) that diversity order of 3 is achieved, in contrast to the diversity order of 2 obtained by the DF scheme in (12).

4.1. Network Coding with Secrecy Constraints

The SOP for the NC scheme is obtained from (5) as follows:

$$\begin{aligned}\mathcal{P}_{s,\text{NC}} &= \Pr\left\{\mathcal{C}_{s,\text{NC}} < R_s\right\} \\ &= \Pr\left\{\gamma_{1d} < \gamma_U = 2^{2R_s}(1+\gamma_{1e}) - 1\right\} \\ &= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1d},\gamma_{1e}}(\gamma_{1d},\gamma_{1e}) d\gamma_{1d} d\gamma_{1e} \\ &= \int_0^\infty \int_0^{\gamma_U} p_{\gamma_{1d}}(\gamma_{1d}) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1d} d\gamma_{1e} \\ &= \int_0^\infty F_{\gamma_{1d}}(\gamma_U) p_{\gamma_{1e}}(\gamma_{1e}) d\gamma_{1e}. \quad (16)\end{aligned}$$

According to (16), in order to calculate the SOP, one must have the pdf and CDF of the SNRs γ_{1d} and γ_{1e}. The CDF corresponds to the outage probability in (15). The pdf, in turn, can be obtained by differentiating the CDF. For γ_{1d} (the same procedure holds for γ_{1e}), the CDF and pdf of the NC scheme are[1]

$$F_{\gamma_{1d}}(\gamma_{1d}) = 3.5\left[1 - e^{-\frac{\gamma_{1d}}{\overline{\gamma}_{1d}}}\right]^3 \quad (17a)$$

$$\begin{aligned}p_{\gamma_{1d}}(\gamma_{1d}) &= \frac{\partial\left[F_{\gamma_{1d}}(\gamma_{1d})\right]}{\partial\gamma_{1d}} \\ &= \frac{10.5}{\overline{\gamma}_{1d}}\left[1 - e^{-\frac{\gamma_{1d}}{\overline{\gamma}_{1d}}}\right]^2 e^{-\frac{\gamma_{1d}}{\overline{\gamma}_{1d}}} \quad (17b)\end{aligned}$$

By replacing (17a) and (17b) in (16), it turns out that the SOP of the NC scheme is

$$\begin{aligned}\mathcal{P}_{s,\text{NC}} &= \int_0^\infty 3.5\left[1 - e^{-\frac{\gamma_U}{\overline{\gamma}_{1d}}}\right]^3 \frac{10.5}{\overline{\gamma}_{1e}}\left[1 - e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}}\right]^2 e^{-\frac{\gamma_{1e}}{\overline{\gamma}_{1e}}} d\gamma_{1e} \\ &= \frac{147}{4}\sum_{i=0}^{3}\binom{3}{i}(-1)^i \exp\left(-\frac{\xi-1}{\overline{\gamma}_{1d}} i\right) \times \\ &\quad \times \ \text{B}\left(\frac{\xi\,\overline{\gamma}_{1e}}{\overline{\gamma}_{1d}} i + 1, 3\right), \quad (18)\end{aligned}$$

where $\xi = 2^{2R_s}$ and $\text{B}(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}dt$ corresponds to the Beta function (first order Euler function) [15].

Proof. Based on [15, eq. (3.312.1)] and the fact that $[1-x]^n = \sum_{i=0}^{n}\binom{n}{i}[-1]^i x^i$. □

5. NUMERICAL RESULTS

In this section, we present some numerical results in order to validate the results obtained analytically. For the NC scheme, the instantaneous SNR γ_{1d} and γ_{1e} were obtained according to the inverse transform sampling method [16].

Fig. 3 presents the SOP versus the average SNR at the destination $\overline{\gamma}_{1d}$ for the DT, DF and NC schemes, considering that R_s=0.5 bits per channel use (bpcu) and that $\overline{\gamma}_{1e}$= 10 dB. We can see that the NC scheme presents highest diversity order among all the three schemes, and that such higher diversity order makes the NC scheme outperform the other schemes when a low SOP is required. It can also be seen that the numerical results match the analytical ones with good precision.

The influence of $\overline{\gamma}_{1e}$ in the SOP performance of the NC scheme is evaluated in Fig. 4, considering that R_s=0.5 bpcu and $\overline{\gamma}_{1e}$= {5,10,15} dB. We can see that when $\overline{\gamma}_{1e}$ increases, the SOP performance is degraded in terms of code gain (the curve is moved to the right). However, the diversity order remains unchanged.

It is worth noting that Eve in the NC scheme is assumed to be capable of fully recovering the network coding coefficients, being in turn more powerful than the eavesdropper in the DF and DT schemes. In a situation where Eve does not know the network coding coefficients, the gain of the NC scheme over the DF and DT schemes in terms of code gain would be much larger.

[1] Note that the CDF and the pdf in (17a) and (17b) are not limited to the unity and to have unity area, respectively, because the expression in (15) is an approximation for the high SNR. However, also note that this does not invalidate our analysis, it only makes it accurate for the high SNR only.

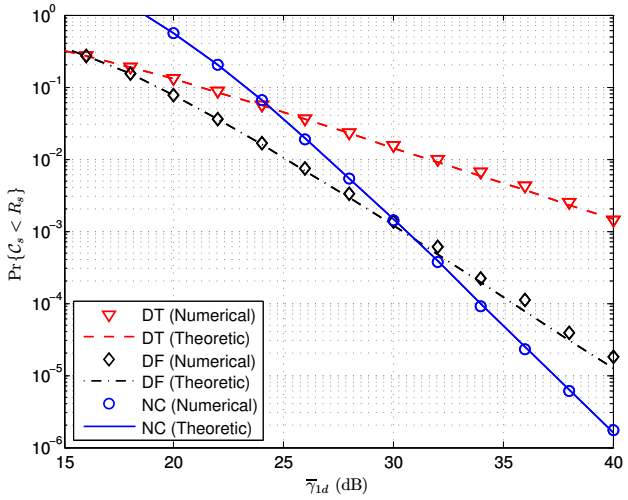


Fig. 3. Secrecy outage probability versus $\overline{\gamma}_{1d}$ for the DT, DF and NC schemes, considering $R_s = 0.5$ bpcu and Eve's average SNR $\overline{\gamma}_{1e} = 10$ dB.

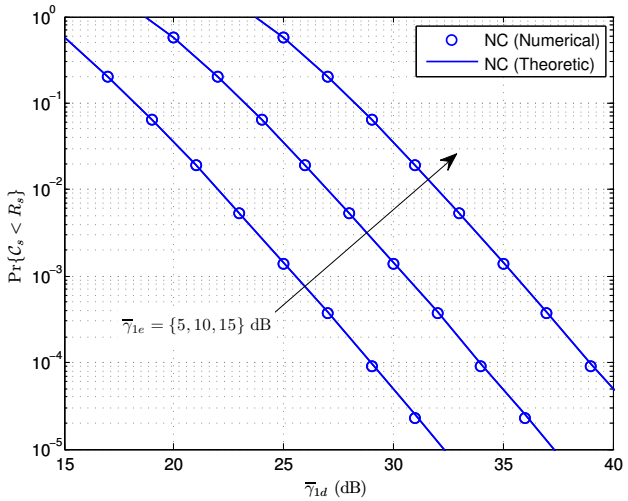


Fig. 4. Secrecy outage probability versus $\overline{\gamma}_{1d}$ for NC scheme, considering $R_s = 0.5$ bpcu and Eve's average SNR $\overline{\gamma}_{1e} = \{5, 10, 15\}$ dB.

6. FINAL COMMENTS

We evaluated the secrecy outage probability of a two-user network-coded cooperative network in the presence of an eavesdropper. We showed through theoretic and numerical analyses that the secrecy can be increased through the use of network coding when compared to the direct transmission and traditional cooperative techniques.

7. REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] João Barros and Miguel R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. of the IEEE Int. Symp. on Inform. Theory (ISIT'06)*, 2006.

[4] Matthieu Bloch and João Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, 2011.

[5] Hirley Alves, Richard Demo Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, June 2012.

[6] Nan Yang, Phee Lep Yeoh, Maged Elkashlan, Robert Schober, and Iain B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, January 2013.

[7] Frederic Gabry, *Cooperation for Secrecy in Wireless Networks*, Ph.D. thesis, KTH, School of Electrical Engineering, Communication Theory Laboratory, September 2012.

[8] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, September 2008.

[9] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage bahavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, December 2004.

[10] A. Sendonaris, E. Erkip, and B. Aazhang, "User cooperation diversity: Part I and Part II," *IEEE Trans. Commun.*, vol. 51, no. 11, pp. 1927–1948, November 2003.

[11] E. C. van der Meulen, "Three-terminal communication channels," *Advanced Applied Probability*, vol. 3, pp. 120–154, 1971.

[12] R. Ahlswede, Ning Cai, S.-Y.R. Li, and R.W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204 – 1216, 2000.

[13] Ming Xiao and Mikael Skoglund, "Multiple-user cooperative communications based on linear network coding," *IEEE Trans. Commun.*, vol. 58, no. 12, pp. 3345–3351, December 2010.

[14] João Luiz Rebelatto, Bartolomeu F. Uchôa-Filho, Yonghui Li, and Branka Vucetic, "Multi-user cooperative diversity through network coding based on classical coding theory," *IEEE Trans. Signal Process.*, vol. 60, no. 2, pp. 916–926, February 2012.

[15] I.S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic Press - Elsevier, 7h edition, 2007.

[16] Luc Devroye, *Non-Uniform Random Variate Generation*, New York: Springer-Verlag, 1986.