

On Secure Communication over Wireless Erasure Networks

Andrew Mills	Brian Smith	T. Charles Clancy	Emina Soljanin	Sriram Vishwanath
Department of CS	ECE Department	ECE Department	Alcatel-Lucent Bell Labs	ECE Department
U. Texas at Austin	U. Texas at Austin	University of Maryland	600 Mountain Avenue	U. Texas at Austin
Austin, TX 78712	Austin, TX 78712	College Park, MD 20472	New Providence, NJ	Austin, TX 78712
amills@cs.utexas.edu	bsmith@ece.utexas.edu	tcc@umd.edu	emina@alcatel-lucent.com	sriram@ece.utexas.edu

Abstract—This paper studies the secrecy capacity of unicast communication in a wireless erasure network setting in the presence of a wire-tapper. From an information-theoretic setting of perfect secrecy, both upper bounds and achievable secrecy rates are presented. Secrecy capacity is determined in closed form for a class of broadcast constrained erasure networks.¹

I. INTRODUCTION

A special network model which incorporates the broadcast nature of wireless transmission and models each link as a memoryless erasure channel has proven to be a useful abstraction to study wireless networks. While it captures the physical nature of the medium to a large extent and provides key insights into viable network protocols, this *wireless erasure network model* is much more tractable than the more general network information-theoretic setting that also includes interference. The capacity of wireless erasure networks has been studied in significant depth, and for multiple settings it has been characterized in closed form [1], [2], [3], [4]. In this paper, we are concerned with the secrecy capacity of unicast communications over these networks in the presence of a wiretapper that has access to a certain number of network links of his choice.

Just as the capacity of networks has been analyzed in different domains using different assumptions and notions of network throughput, secure communication over networks has been studied using multiple distinct assumptions and notions of secrecy. In particular, perfect secrecy capacity for the general class of information-theoretic channels has seen a resurgence of interest in recent years [5], [6], [7]. For a single source multicast networks implementing network coding, the problem of making a linear network code information-theoretically secure in the presence of a wiretap adversary that can look at a bounded number, say k , of network edges was first studied by Cai and Yeung in [8]. They considered directed (V, E) graphs and demonstrated the existence of a code over an alphabet with at least $\binom{|E|}{k}$ elements which can support a secure multicast rate of up to $n-k$. They also showed that such codes can be designed in $\mathcal{O}(\binom{|E|}{k})$ steps. The required edge bandwidth and the secure code design complexity are main

drawbacks of this pioneering work. Feldman *et al.* derived trade-offs between security, code alphabet size, and multicast rate of secure linear network coding schemes in [9], by using ideas from secret sharing and abstracting network topology. El Rouayheb and Soljanin showed that network security can be achieved by using the Ozarow-Wyner approach of coset coding at the source on top of the implemented network code [10]. Weakly secure network coding (which insures that only useless information rather than none is revealed to the adversary) was studied by Bhattad and Narayanan in [11], and practical schemes are missing in this case as well. Another approach was taken by Jain in [12] who obtained security by merely exploiting the topology of the network in question.

In this paper, we deal wireless erasure networks in an attempt to find a network generalization of the information-theoretic perfect secrecy analysis for the Wyner wiretap channel model [6] to the capacitated network secrecy capacity for unicast networks. In particular, we determine achievable strategies and upper bounds on secrecy capacity, which match for a class of broadcast-constrained erasure networks.

The paper is organized as follows. In the next section, we detail our system model. In Section 3, we present the main upper bound on secrecy capacity. In Section 4, we obtain an achievable scheme for a particular placement of wire-tappers in a broadcast-constrained erasure network. Finally, we conclude with Section 5.

II. SYSTEM MODEL

The network under investigation is a single-source, single-destination, lossy, wireless packet network, modeled as a directed acyclic graph (V, E) with nodes V and communication links E . An example is illustrated in Figure II. The “wireless” component of the network is manifested in a broadcast constraint; that is, each transmitter must send a single, identical packet on every communication link exiting that node in any given time-slot. These broadcasted packets are all taken to be symbols of a finite field transmit alphabet $GF(q)$ for some (large) q . The network is “lossy” because each edge in the graph experiences packet drops, or equivalently, symbol erasures. These erasures are independent across both time and space, and associated with each directed edge (i, j) between nodes i and j is the value of that erasure probability, denoted

¹This work was supported in part by the DARPA IAMANET program and a grant from the Department of Defense

by ϵ_{ij} . We assume that each receiver obtains all of the symbols along its incoming edges without interference. The capacity of this non wire-tapped network model was first given in [1] (and its achievability alternatively demonstrated by a random linear network coding scheme in [3]), and is given by the expression:

$$C = \min_S \lg q \sum_{i \in S} \left(1 - \prod_{j \in S^c} \epsilon_{ij} \right) \quad (1)$$

where S is a vertex-cut. Specifically, S is any subset of the nodes which contains the source and not the destination. This paper extends the work on this notion of lossy wireless networks to demonstrate its secrecy capacity.

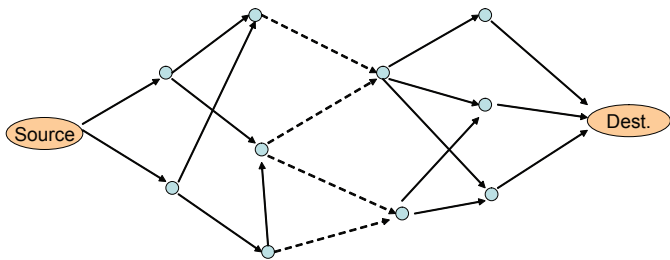


Fig. 1. System Model - Dotted Edges Represent an Example Edge Cut-set.

Along the lines of the model in [8], the eavesdropper has access to *any* k edges of this network, in the sense that it can observe the outputs of each edge in the network. Specifically, if the packet transmitted along any wire-tapped edge is erased (or dropped), the wire-tapper as well the receiving node fail to receive it. Our objective is to ensure perfect secrecy of the message in the network from the wire-tapper, defined in the sense of [6]. Specifically, we wish to determine the highest rate possible such that the wire-tapper gains no information about the message being communicated, and that the mutual information between the wire-tapper's information and the source's intended message is zero.

Let $s \in V$ denote the source and $d \in V$ the destination. This paper defines an edge cut as any set $T \subset E$ such that there does not exist a path from s to d in $E \setminus T$. We assume a path from s to d exists in E , so a cut must be nonempty. Also, note that E itself defines a cut in this network. The definition of a cut in this paper is distinct from that used in [1], which is a vertex-based definition of a "cut" in the network.

Letting $A \subseteq E$ be a set of edges of the graph, we define a size $m \times n$ incidence matrix. The number of columns n will be equal to the number of distinct parent vertexes of the edges in A . That is, $n = |I_A|$, where $I_A = \{i | (i, j) \in A\}$. The number of rows m in a network with no interference will be equal to the number of edges in A , that is $m = |A|$. For each time slot t , the incidence matrix $G_A(t)$ will contain a 1 in each row corresponding to an edge whose symbol was not dropped, in the column corresponding to the corresponding parent vertex. Let X_i denote the symbol transmitted from node i , $Y_{j,i}$ denote the symbol received at node j which had been transmitted from

node i , and γ_{ij} be independent Bernoulli random variables with $P[\gamma_{ij} = 0] = \epsilon_{ij}$. Then, for the network displayed in Figure 2, the matrix

$$\begin{bmatrix} Y_{2,s} \\ Y_{2,1} \\ Y_{d,1} \end{bmatrix} = \begin{bmatrix} \gamma_{s2} & 0 \\ 0 & \gamma_{12} \\ 0 & \gamma_{1d} \end{bmatrix} \begin{bmatrix} X_s \\ X_1 \end{bmatrix}$$

defines G_A for the cut $A = \{(s, 2), (1, 2), (1, d)\}$. Note that when A is chosen to be the set of edges crossed by the vertex min-cut, then the expected value of G_A corresponds precisely to the value of the min-cut capacity given in Equation (1).

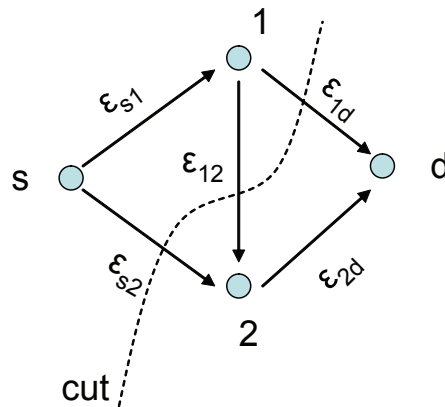


Fig. 2. Example Network and Edge Cut Set

III. UPPER BOUND ON SECRECY CAPACITY

Example 1: Consider for a moment a simple unicast scenario shown in Fig. 3. Assume that the source is directly

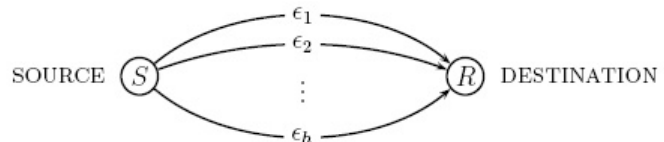


Fig. 3. At the source node, k information symbols are encoded into h coded symbols, which are then simultaneously transmitted to the destination.

connected to the destination through n network links where link i , $1 \leq i \leq n$ has erasure rate ϵ_i , and that any k of these edges can be accessed by a wiretapper. If we assume that all erasure rates are equal, that is $\epsilon \triangleq \epsilon_1 = \dots \epsilon_n$, then this network unicast is equivalent to the Wyner wiretap channel model in which the intended user observes the output of an erasure channel with the erasure rate ϵ^n , and the wiretapper observes the output of a degraded channel with the erasure rate ϵ^k .

Outer Bound: Let S be any set of k edges in the network. Let $T : S \subseteq T \subseteq E$ be a cut in the network. Then, the secrecy capacity of the network is bounded by:

$$C \leq \lg q (\mathbb{E}[\text{rank}(H_T)] - \mathbb{E}[\text{rank}(G_S)]) \quad (2)$$

where H_T is the incidence matrix of the cut T and G_S the incidence matrix of S .

Specifically, secrecy capacity for the network is upper bounded by:

$$C \leq \lg q \min_{T: T \text{ is a cut}} \left[\mathbb{E}[\text{rank}(H_T)] - \max_S \mathbb{E}[\text{rank}(G_S)] \right]$$

In the notation of [1], this expression is equivalent to

$$C \leq \min_A \lg q \sum_{i \in A} \prod_{j: j \in S^C, (i,j) \in S} \left(1 - \prod_{j: j \in A^C, (i,j) \notin S} \epsilon_{ij} \right) \quad (3)$$

where, to be clear, A refers to a vertex cut and S refers to the set of edges to which the wire-tapper has access.

Proof: Wire-tappers are placed on any k edges of the graph (V, E) , forming the subset $S \subseteq E$. Consider any edge cut, and if necessary, supplement it with the edges in S to form the edge cut $T \supseteq S$ with inputs $X^n(T)$ and outputs $Y^n(T)$.

Intuitively, in this setting, our goal is to upper bound the secrecy capacity of the network by a cutset bound: The amount of information that the receiver can get while the wire-tapper still has no information about the source should be no more than the rate that the network can get across any cut, minus the amount that the wire-tapper can see on that same cut.

$$\begin{aligned} nR_e &\stackrel{(a)}{\leq} H(W|Y(S)^n) \\ &\stackrel{(b)}{\leq} H(W|Y(S)^n) - H(W|Y(T)^n) + n\epsilon_n \\ &= I(W; Y(T)^n) - I(W; Y(S)^n) + n\epsilon_n \\ &= H(Y(T)^n) - H(Y(T)^n|W) - H(Y(S)^n) \\ &\quad + H(Y(S)^n|W) + n\epsilon_n \\ &\stackrel{(c)}{\leq} H(Y(R)^n|Y(S)^n) - H(Y(R)^n|W, Y(S)^n) + n\epsilon_n \\ &\leq H(Y(R)^n|Y(S)^n) \\ &\quad - H(Y(R)^n|X(T)^n, W, Y(S)^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n (H(Y(R)_i|Y(S)_i) \\ &\quad - H(Y(R)_i|X(T)^n, W, Y(S)^n, Y(R)^{i-1})) \\ &\stackrel{(d)}{=} \sum_{i=1}^n (H(Y(R)_i|Y(S)_i) - H(Y(R)_i|X(T)_i, Y(S)_i)) \\ &= \sum_{i=1}^n (I(X(T)_i; Y(T)_i) - I(X(T)_i; Y(S)_i)) \\ &\stackrel{(e)}{\leq} \sum_{i=1}^n (I(X(T)_i; Y(T)_i) - I(X(S)_i; Y(S)_i)) \\ &\leq \sum_{i=1}^n \max_{p(X(T)_i)} (I(X(T)_i; Y(T)_i) - I(X(S)_i; Y(S)_i)) \\ &= n \max_{p(X(T))} (I(X(T); Y(T)) - I(X(S); Y(S))) \end{aligned}$$

where

(a) follows from the definition of secrecy rate

(b) follows from Fano's inequality [16]. All the information must be retrieved from the final destination node with high probability, and the Data Processing Inequality applies since $W \rightarrow T \rightarrow Y_d$ is a Markov Chain.

In (c), R is defined as $T \setminus S$ so that $X(T) = (X(R), X(S))$ (d) follows from the fact that, given $X(T)_i$, $Y(S)_i$ is conditionally independent of W and $Y(S)_{i-1}$.

(e) follows because $X(S)_i$ is a degraded version of $X(T)_i$.

Intuitively, for every cut $T \supseteq S$, The network behaves as an information-theoretic wiretap channel with a (physically) degraded wire-tapper. Note that in the (symmetric) erasure network setting, it is easy to show that the optimum input distribution is uniform (straightforward extension of result in [1]), and thus the upper bound reduces to the difference between the max-rate across the cut T and the max-rate across the subset of nodes S . From [13], the rate across any subset of nodes is given by the expected rank of its incidence matrix. This gives us the result. This converse is general, and hold for some additional models of erasure networks. Specifically, in a network with additive finite-field interference at the receivers (for example, [14] or [13], or an extension of [15]) then the cut-capacity still evaluates to the expected rank of the incidence matrix.

IV. ACHIEVABILITY

In this section, we show that the outer bound given by (2) can be achieved under certain conditions. Specifically, let T^* be the cut that minimizes $\lg q \mathbb{E}(\text{rank}(H_{T^*}))$, i.e, T^* is the cut that minimizes the (non-wiretap) capacity of the network. Let S^* be a k -edge subset of T^* such that the upper bound given by (2) is minimized for T^* .² Define

$$C^* \triangleq \lg q \mathbb{E}(\text{rank}(H_{T^*})) - \mathbb{E}(\text{rank}(G_{S^*}))$$

Our goal in this section is to show that in a broadcast-constrained erasure network, if T^{**} is the minimizing cut for (2) and $T^{**} = T^*$, then C^* is the secrecy capacity of the network.

Achievability: Given that the system has k wire-tappers placed arbitrarily on the cut T^* as defined above, a (linear) encoding scheme exists such that C^* is achievable with a perfect secrecy constraint.

Proof: The key idea, similar to that in [9] and [18], is to send information packets and “noise” packets such that the legitimate receiver can decode both the information and noise packets, while the wire-tapper can only decode the “noise” packets. The noise packets are independent of information packets thus guaranteeing perfect secrecy.

Note that two coding schemes exist that achieve the cut-set upper bound on capacity of broadcast-constrained erasure networks (in a non-wiretap setting). The first is based on random coding arguments in [1], while the second is based on random linear network coding in [1], [3], [14]. Note that, in each case, it is assumed that the exact erasure locations at

²Note that T^* may not be the minimizing cut for (2) of this graph.

the intermediate nodes is known to the receiver. In the rest of this document, we will utilize the linear network coding framework for coding at the intermediate nodes in [1]. Note that our proof for secrecy capacity can be modified to the case when random network coding is used [1].

Let n be a positive integer. Define $m \triangleq n\mathbb{E}(\text{rank}(H_{T^*}))$ and $l \triangleq n\mathbb{E}(\text{rank}(G_{S^*}))$. Then $C^* = \frac{m-l}{n} \lg q$. Intuitively, we show that if m un-erased packets reach the legitimate destination and l un-erased packets reach the wire-tapper, then there exists a coding scheme that achieves C^* .

The encoding scheme is as follows: A transmit vector of length m packets for some $\epsilon > 0$ is constructed consisting of $(m-l-n\epsilon)$ information (or data) packets and $(l+n\epsilon)$ noise packets that are independent of the data source and chosen uniformly from $GF(q)$. We refer to this as the vector x^m , with $a^{(m-l-n\epsilon)}$ denoting data packets, $b^{l+n\epsilon}$ denoting “noise” packets, and $x^m = [a^{(m-l-n\epsilon)} \ b^{l+n\epsilon}]$.

A linear encoding scheme is used at each node, which results in $n \times m$ transfer matrices M_n and F_n for the legitimate destination and the wire-tapper respectively. By the weak law of large numbers (which results in the notion of strong typicality as in [16]), the received vector at the legitimate destination is at least an $(m-n\epsilon)$ -sized subset of the n -length vector $M_n x^m$ with probability greater than $1 - \delta$. Similarly, the wire-tapper observes at most an $(l+n\epsilon)$ -ary subset of the vector $F_n x^m$ with high probability.

In [1, Section 7-A], the authors show that averaging over all matrices, the average probability of error in decoding can be made less than ϵ . Therefore, the information vector $a^{m-l-n\epsilon}$ is received successfully with high probability at the destination allowing for a rate arbitrarily close to $C^* - \epsilon$.

Let the $(l+n\epsilon)$ -ary subset of the vector $F_n x^m$ received at the wire-tapper with high probability be denoted as:

$$z^{l+n\epsilon} \triangleq F_{l+n\epsilon} x^m$$

Define

$$\hat{z}^{(l+n\epsilon)} \triangleq \hat{F}_{(l+n\epsilon)} b^{(l+n\epsilon)}$$

where $\hat{F}_{(l+n\epsilon)}$ is a $(l+n\epsilon) \times (l+n\epsilon)$ matrix of the last $(l+n\epsilon)$ columns from $F_{l+n\epsilon}$.

A key step is for us to choose coefficients for the network (i.e., one particular M_n and F_n) such that:

- $a^{(m-l-n\epsilon)}$ is decodable at the legitimate destination with probability of error arbitrarily small, and
- $\hat{F}_{l+n\epsilon}$ is invertible.

Note that a random choice in coefficients ensures both of these simultaneously with high probability [1], [17], and therefore a particular set of M_n and F_n exist that satisfy these requirements.

By Fano’s inequality [16], the information recovered by the wire-tapper is upper bounded by:

$$\begin{aligned} I(a^{m-l-n\epsilon}; z^{l+n\epsilon}) &= H(z^{l+n\epsilon}) - H(z^{l+n\epsilon} | a^{m-l-n\epsilon}) \\ &\stackrel{(a)}{=} H(z^{l+n\epsilon}) - H(\hat{z}^{l+n\epsilon} | a^{m-l-n\epsilon}) \\ &\stackrel{(b)}{=} H(z^{l+n\epsilon}) - H(\hat{z}^{l+n\epsilon}) \\ &\stackrel{(c)}{=} H(z^{l+n\epsilon}) - (l+n\epsilon) \lg q \\ &\stackrel{(d)}{\leq} (l+n\epsilon) \lg q - (l+n\epsilon) \lg q \\ &= 0 \end{aligned}$$

where:

(a) follows from the definition of $\hat{z}^{(l+n\epsilon)}$ and the property of entropy.

(b) follows from the independence between $a^{(m-l-n\epsilon)}$ and $b^{(l+n\epsilon)}$.

(c) follows from the invertibility of $\hat{F}_{(l+n\epsilon)}$, and that $b^{(l+n\epsilon)}$ are i.i.d. and uniform.

Or in essence, no information is recovered by the wire-tapper. This concludes the achievability proof.

V. UPPER BOUND COUNTER EXAMPLE

Counter to the authors’ intuitive expectations, the upper bound of Section III is not tight in general. This section provides a counter example demonstrating this fact.

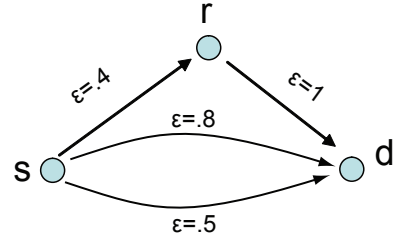


Fig. 4. Upper Bound Counter Example

Consider the three node network shown in Figure 4. This network has two independent edges which connect the source to the destination. The wiretapper may choose any one edge to wiretap, but it is clear that the set consisting of the edge $S = \{sr\}$ is the most favorable. Note that this set S does not lie in the minimum cut edge set of the original network $T_{min} = \{rd, sd_1, sd_2\}$, whose cut value is $1 - (.8)(.5) = .6$.

We evaluate along the cut $T = \{sr, sd_1, sd_2\}$,

$$(\mathbb{E}[\text{rank}(H_T)] - \mathbb{E}[\text{rank}(G_S)]) = (1 - (.4)(.5)(.8)) - .6 = .24$$

to find the minimum of the outerbounds on capacity from Equation 2. However, the actual secrecy capacity of this network is equal to zero.

The wiretapper receives the data transmitted by the source, with a loss of 40% of all the symbols. The destination will also receive the data transmitter by the source, again with a loss of 40% of the symbols. Therefore, whatever the destination d can decode, the wiretapper will also be able to decode, and there is no secrecy capacity.

VI. CONCLUSIONS

This work investigates the secrecy capacity, or specifically the equivocation rate, of a wire-tapped wireless erasure network. Secrecy capacity for this network takes the same intuitive form as it does in many other network models: we desire to maximize the difference in the amount of data that the receiver can interpret and the amount of information from the source the wire-tapper could receive. In a simple, error and interference-free network, this result has the straightforward interpretation of subtracting the number of wire-tapped edges from the number of edges in the minimum cut. For the wireless erasure network, the subtraction is equivalent, given the modified cut-set bound.

This paper shows that the upper-bound is achievable when the wire-tappers are chosen from a specific subset of the nodes, that is, along the minimum cut of the original network. The strategy is interesting because of its history in the secrecy context, and its application to a non-traditional secrecy model. When the wiretappers do not lie along the minimum-cut of the original network, we have shown that our upper-bound may not, in general, be tight.

REFERENCES

- [1] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. on Inform. Theory*, Vol. 52, pp. 789 - 804, March 2006.
- [2] D. Julian, "Erasure Networks," *Proc. IEEE ISIT*, pp. 138, 2002.
- [3] D. S. Lun, M. Médard, and M. Effros, "On coding for reliable communication over packet network," *Proc. 42nd Annual Allerton Conf. on Commun. Control, and Computing*, September 2004.
- [4] M. Xiao, M. Médard, and T. Aulin, "A Binary Coding Approach for Combination Networks and General Erasure Networks," *Proc. IEEE ISIT*, 2007.
- [5] I. Csiszár and J. Körner, "Broadcast channels with confidential messages", *IEEE Trans. Inform. Theory*, 24(3):339-348, May 1978.
- [6] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, 54(8):1355-1387, October 1975.
- [7] Y. Liang and H. V. Poor, "Generalized multiple access channels with confidential messages", *IEEE Trans. Inform. Theory*, 2006.
- [8] N. Cai and R. W. Yeung, "Secure Network Coding," ISIT 2002.
- [9] J. Feldman, T. Malkin, C. Stein, R. A. Servedio "On the Capacity of Secure Network Coding", *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing*, September 2004.
- [10] S. E. Rouayheb and E. Soljanin, "On wiretap networks II," in *Proc. 2007 International Symposium on Information Theory (ISIT'07)*, Nice, France, June 2007.
- [11] K. Bhattad and K. R. Narayanan, "Weakly secure network coding", *Netcod 2005*, Italy, April 2005.
- [12] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Communications*, pp. 68-71, Feb. 2004.
- [13] B. Smith and S. Vishwanath, "Unicast transmission over multiple access erasure networks: capacity and duality", *IEEE Information Theory Workshop*, Lake Tahoe, CA, Sep 2007.
- [14] S. Bhadra, P. Gupta, and S. Shakkottai, "On network coding for interference networks," in *Proc. IEEE ISIT 2006*, Seattle, WA, Jul 2006.
- [15] A. Avestimehr, S. Diggavi, D. Tse, "Wireless network information flow", *Proc. 45th Annual Allerton Conference on Communication, Control, and Computing*, September 2007.
- [16] R. W. Yeung, "A First Course in Information Theory," Kluwer Academic Press.
- [17] T. Ho, R. Koetter, M. Médard, D. R. Karger and M. Effros, "The benefits of coding over routing in a randomized setting," *IEEE International Symposium on Information Theory (ISIT)*, 2003.
- [18] A. Shamir, "How to Share a Secret", *Communications*, 1979.