

CHAPTER 7

Secure Network Coding: Bounds and Algorithms for Secret and Reliable Communications

Sidharth Jaggi and Michael Langberg

AQ

Contents

1. Introduction	186
1.1. Overview of Chapter	187
2. Model	188
2.1. Threat Model	188
2.2. Network and Code Model	188
3. Eavesdropping Security	190
3.1. The Coherent Case	190
3.2. The Non-Coherent Case	194
4. Jamming Security	196
4.1. The Coherent Case	196
4.2. The Non-Coherent Case	199
4.3. The Cryptographic Setting	204
5. Secret Transmission in Presence of Eavesdropping and Jamming Adversaries	208
5.1. The Coherent Case	208
5.2. The Non-Coherent Case	209
6. Some Other Variants	211
7. Discussion	212
Acknowledgments	212
References	212

Abstract

Network coding allows network routers to mix the information content in incoming packets before forwarding them. This mixing has been theoretically proven to be very beneficial in improving both throughput and robustness. But what if the network contains malicious nodes? Such nodes may “tap” the network in order to eavesdrop on ongoing communication, and/or may pretend to forward packets originating from the source, while in reality they inject corrupted packets into the information flow so as to disrupt communication.

Since network coding allows routers to mix packets' content, a single corrupted packet can end up corrupting all the information reaching a destination. Unless this problem is solved, network coding may perform much worse than pure forwarding in the presence of such malicious adversaries.

This chapter addresses the task of multicast communication using network coding in the presence of passive eavesdroppers and active jammers. Rather surprisingly, it is shown that high-rate private and reliable communication via schemes that are both computationally efficient and distributed is possible in the settings under study. This chapter summarizes almost a decade of study in the very dynamic and intriguing field of private and reliable network communication. The algorithmic techniques presented cover several paradigms and include tools from the study of combinatorics, linear algebra, cryptography, and coding theory.

Keywords: Network Coding, Network Communication, Error correction, Wiretap channel, Distributed protocols, Cryptography, Capacity

1. INTRODUCTION

Network coding allows the routers to mix the information content in packets before forwarding them. This mixing has been theoretically proven to maximize network throughput [1, 29, 40, 44]. For multicast communications it can be done in a distributed manner with low complexity, and is robust to packet losses and network failures [24, 46]. Furthermore, recent implementations of network coding for wired and wireless environments demonstrate its practical benefits [20, 32].

But what if the network contains malicious nodes? Nodes that *tap* the network aim to eavesdrop on ongoing communication. Further, some nodes may pretend to forward packets from source to destination, while in reality they *inject* corrupted packets into the information flow. Since network coding makes the routers mix packets' content, a single corrupted packet can end up corrupting *all* the information reaching a destination. Unless this problem is solved, network coding may perform much worse than pure forwarding in the presence of such malicious adversaries.

This chapter addresses the task of multicast communication using network coding in the presence of passive eavesdroppers and active jammers. Rather surprisingly, it will be shown that high-rate private and reliable communication via schemes that are both computationally efficient and distributed is possible in the settings under study. Despite the complexity introduced by distributed network coding, it turns out that many of the

classical results for private and reliable communication over point-to-point links have direct analogs in the network setting. This chapter summarizes almost a decade of study in the very dynamic and intriguing field of private and reliable network communication.

1.1. Overview of Chapter

The chapter consists of four sections. In Section 2 we set the notation, definitions, and model used throughout. In Section 3 we consider communication in the presence of *passive* adversaries who only have eavesdropping capability and wish to learn the information transmitted over the network. The objective in this case is the design of communication schemes that enable *secrecy*, *i.e.*, schemes which do not allow the adversary to learn the information transmitted by the source. In Section 4 we consider *active* adversaries, who have both eavesdropping and jamming capabilities whose objective is to cause a decoding error at the terminal nodes. Here, successful communication means *reliable* communication, *i.e.* correct decoding. In Section 5 we consider again communication in the presence of active adversaries with both eavesdropping and jamming capabilities, however in this case our objective is to design communication schemes that are both reliable and secret. Finally, in Section 6 we briefly note other models that do not fit into the above classifications. We conclude with a discussion in Section 7.

In each of the sections mentioned above, our overview includes between two to three refined models. We first address the *coherent* setting in which the terminal nodes are assumed to know the topology of the network alongside the (realization of the) communication scheme used. The second setting we address is the *non-coherent* setting. Here, no knowledge of the topology and/or code being used is assumed to be present at the terminal nodes. In both settings above, we follow an *information-theoretic* analysis assuming that the adversary has unlimited computational power and has full knowledge of the network topology and the communication scheme in use. We stress that any achievable rate R in the non-coherent setting is also achievable in the coherent one, and any upper bounds presented on R for the coherent setting also hold in the non-coherent one. Finally, we also consider the case in which the adversary is computationally limited, and discuss schemes with are conditioned on certain *cryptographic*

assumptions. We present an extended discussion in Section 4, while cryptographic schemes for Sections 3 and 5 can be reduced to our discussion in Section 4. Each of the refined models is presented in more detail in Section 2.

2. MODEL

We use a general model that encompasses both wired and wireless networks. To simplify notation, we consider only the problem of communicating from a single source to a single destination. But similarly to most network coding algorithms, our techniques generalize to multicast traffic.

2.1. Threat Model

There is a source, Alice, who communicates over a wired or wireless network to a receiver Bob. There is also an attacker Calvin, hidden somewhere in the network. Calvin aims to prevent the transfer of information from Alice to Bob, or at least to minimize it. He can observe some or all of the transmissions, and can inject his own. When he injects his own data, he pretends it is part of the information flow from Alice to Bob.

Calvin is quite strong. In both the coherent and non-coherent setting we assume that Calvin knows the encoding and decoding schemes of Alice and Bob, and the network code implemented by the interior nodes. He also knows the exact network realization. The computational power of Calvin is assumed to be unbounded unless specifically mentioned otherwise. In the latter case we will specify the exact computational problems limiting Calvin (e.g., the Discrete-Log problem).

2.2. Network and Code Model

Network Model

The network is modeled as a graph. Each transmission carries a packet of data over an edge directed from the transmitting node to the observer node. The graph model captures wired networks. For wireless networks, one may assume a model in which the network is a *hypergraph* in which each edge is determined by instantaneous channel realizations (packets may be lost due to fading or collisions) and connects the transmitter to all nodes that hear the transmission. In this survey we will focus on the wired setting, although several of the results extend naturally to the wireless setting as well.

Throughout, the graph is unknown to Alice and Bob prior to transmission in the non-coherent setting, but is assumed to be known in the coherent setting.

Source

Alice generates incompressible data that she wishes to deliver to Bob over the network. To do so, Alice encodes her data as dictated by the encoding algorithm (described in subsequent sections).

Adversary

Calvin is assumed to control certain links of the network. We assume that Calvin can corrupt the information transmitted on any subset of z_O links of the network and can observe the information on z_I links. The set of links controlled by Calvin is unknown to both Alice and Bob. Moreover, this set of links does not undergo any changes throughout the entire block-length of communication. In Section 3 we assume that z_I is unlimited but $z_O = 0$ (here, the objective is to design secret communication schemes). In Sections 4 and 5 we assume a positive value for z_O and discuss different settings of z_I (here, the objective is to respectively design reliable communication schemes, and schemes that are both reliable and secret).

In our model the error imposed by the Byzantine adversary Calvin is assumed to be *added* to the original information transmitted on the network. One can also consider a model in which these errors *overwrite* the existing information transmitted by Alice. We stress that if Calvin is aware of transmissions on links, these two models are equivalent. Overwriting a message x with z is equivalent to adding $-x + z$ over the field over which coding is performed. However, when Calvin is unaware of the information transmitted over the links, these models may differ.

Receiver

The receiver Bob decodes his incoming information using decoding procedures that are discussed in subsequent sections.

Network Transform

In many of the proposed schemes, the network performs classical distributed network coding [24]. Specifically, each packet transmitted by an internal node is a random linear combination of its incoming packets. Thus, the effect of the network at the destination can be summarized by

$Y = TX + T'Z$, where the matrix X represents the encoded source information, the matrix Z represents the error specified by the network, and the matrix Y corresponds to the incoming information at the terminal node, and both T and T' represent the linear transforms resulting from the network coding scheme. As is common in the network coding literature, one assumes that the coding is done over a certain finite field \mathbb{F} .

Definitions

We define the following concepts. The *network capacity*, denoted by C , is the time-average of the maximum number of packets that can be delivered from Alice to Bob, assuming no adversarial interference, *i.e.*, the max flow. It can be also expressed as *the min-cut from source to destination*. (For the corresponding multicast case, C is defined as the minimum of the min-cuts over all destinations.) The *error probability* is the probability that Bob's reconstruction of Alice's information is inaccurate. The rate R is the number of *information* symbols that can be delivered on average, per time step, from Alice to Bob. Rate R is said to be achievable if for any $\epsilon_1 > 0$ and $\epsilon_2 > 0$ there exists a coding scheme of block length n with rate $\geq R - \epsilon_2$ and error probability $\leq \epsilon_1$. The *capacity* of a certain adversarial setting, is the maximum achievable rate under this setting.

3. EAVESDROPPING SECURITY

We start by considering private communication in the context of multicast network coding.

3.1. The Coherent Case

We consider the rate of secret communication (also referred to as *secure* communication) in the coherent setting in the presence of a hidden eavesdropper that has access to z_I links of the network. Specifically, we denote the information transmitted by the source as the random variable X , that received by terminal t_i as Y_i and that observed by the adversarial eavesdropper as Z . Analogously to the conditions Shannon [64] used to define *perfectly secure* systems, we require that $H(X|Y_i) = 0$ (implying that the terminal is able to deduce the source information) and $I(X; Z) = 0$ (implying that the communication is secure). Letting C denote the maximum multicast communication rate (in the absence of an eavesdropper), we show

that one can securely communicate at *optimal* rate $R = C - z_I$. This rate is the best possible, as one cannot communicate securely at a higher rate even over the *one-hop* unicast network consisting of a single source s that wishes to communicate with a single terminal t over C multiple (s, t) links. This is implied by the following standard argument. Let \bar{Z} denote the random variable corresponding to the information on the links not observed by the eavesdropper (hence $Y_i = (Z, \bar{Z})$). Then

$$R = H(X) = H(X|Y_i) + I(X; Y_i) = H(X|Y_i) + I(X; Z, \bar{Z}) \quad (1)$$

$$= I(X; Z, \bar{Z}) = I(X; Z) + I(X; \bar{Z}|Z) \quad (2)$$

$$= I(X; \bar{Z}|Z) \leq H(\bar{Z}) \leq C - z_I. \quad (3)$$

Equalities (1) \Rightarrow (2) and (2) \Rightarrow (3) follow from our conditions for secure communications, and the remaining (in)equalities from standard information (in)equalities and the fact that \bar{Z} has at most $C - z_I$ links.

Secure communication in the context of coherent network coding has been addressed in several works over the last decade. This line of study was initiated by Cai and Yeung in [9] where they consider enhancing any linear network coding scheme which allows communication at rate C (in the absence of an eavesdropper) to one which is secure. Enhancing an existing linear network coding scheme (such as that of Jaggi *et al.* [29]) is done in an *end-to-end* manner. Namely, internal nodes of the network are oblivious to the fact that communication is done in the presence of an adversarial eavesdropper, and follow the original coding scheme. The presence of an adversarial eavesdropper is dealt with by an enhanced encoding at the source node and by specialized decoding at terminal nodes. To this end, the enhanced encoding of the source includes two steps. Primarily the source takes its $C - z_I$ characters of information X and appends to it a uniformly distributed random vector R of z_I characters to obtain (X, R) . Secondly, (X, R) over goes a certain invertible linear transform T resulting in the *message* M of length C . The message M is now transmitted over the network using the original (perhaps insecure) network coding scheme. On decoding, a terminal first recovers M and then via T recovers X .

We now address the security of the scheme suggested in [9]. Considering the original coding scheme as fixed, the code design of [9] involves specifying the matrix T which in turn defines the message $M = T(X, R)$ to be transmitted. Specifically, one needs to design the matrix T such that

any z_I linear combinations of M resulting from the linear encoding of the original network coding scheme do not reveal information on the value of X . This is a non-trivial task and the construction of T in [9] is done in a greedy iterative manner that resembles the Gilbert construction for error correcting codes [18]. The analysis of [9] uses a field \mathbb{F} of size $q \geq \binom{|E|}{z_I}$, which is exponential in network parameters. (This bound on q follows from the fact that there are at most $\binom{|E|}{z_I}$ different possible subsets of z_I links that the adversary may eavesdrop on, and the matrix T has to be resilient to each scenario.) An extension to *imperfect security* is also addressed in [9]. Using essentially the same construction and proof technique, it is shown that allowing $I(X; Z) \leq i$ (instead of $I(X; Z) = 0$) one can obtain rate $C + i - z_I$ (here one assumes $i \leq z_I$).

Theorem 1 ([9]). *Let G be an acyclic network with cut capacity C . Then, the coherent secure capacity in the presence of an adversary that may eavesdrop on up to z_I of the links of G is $C - z_I$.*

Following the paradigm of [9], Feldman *et al.* [14], study the achievable trade-off between rate and field size q . Namely, referring to the matrix T as a “filtered secret sharing scheme”, they show that finding T is equivalent to finding an error-correcting code with certain generalized distance properties. The latter is obtained via a random linear construction similar to that of Varshamov [79]. Using this connection, Feldman *et al.* [14] show that for any $\sigma > 1$ one can efficiently construct a matrix T that allows secure communication at rate $C - \sigma z_I$ and field size $q = |E|^{\Omega(\frac{1}{\sigma-1})}$. The intuition is that any scheme with the appropriate generalized distance has the property that projecting the linear transform onto z_I links results in a uniformly distributed random variable from the eavesdropper’s perspective.

In [61, 62], Rouayheb *et al.* study the two-step paradigm of [9] and take a different approach in which they concentrate on the design of the internal network coding scheme instead of the design of T . Namely, [61, 62] tie the task of coherent secure communication with that of the *wiretap channel of type II* introduced in the seminal work by Ozarow and Wyner [57, 58]. In the latter, coset coding is used to enable secure communication at rate $C - z_I$ over the simple one-hop network mentioned previously. The authors of [61, 62] observe that the naïve approach—one in which the source pre-encodes its information using the coset coding techniques of [57, 58] (via T) and then performs any feasible network

coding scheme—does not necessarily yield secure communication. However, [61, 62] show that if the network coding scheme satisfies certain requirements with respect to the specific coset coding used, then a secure rate of $C - z_I$ is indeed obtained. To obtain such network codes that have a good fit with a given pre-encoding scheme T , Rouayheb *et al.* modify the deterministic algorithm of [29] for the construction of network coding schemes (in the absence of an eavesdropper) and obtain efficiently constructible secure codes at optimal rate $C - z_I$ with field size roughly $|E|^{z_I}$. To reduce the field size to one which is independent of the size of the graph G and only depends on C , z_I and the number of terminals in the multicast connection t , [61, 62] use ideas from [42, 43] and obtain a field-size of $\binom{2^{(C-z_I)^3 t^2}}{z_I-1} + t$, which is independent of $|V|$ and $|E|$ but still exponential in other network parameters.

Pre-encoding using coset coding is further investigated by Ngai *et al.* in [53] in which a comprehensive study is performed. Motivated by the work of Wei on generalized Hamming weight for linear block codes [83], Ngai *et al.* define the notion of “Network Generalized Hamming Weight” and “Network MDS” codes. Roughly speaking, these notions tie block error-correcting codes with network coding schemes and suffice to characterize pre-encoding schemes T that allow secure communication when combined with a given network coding scheme (and *visa versa*).

Considering a *weak* notion of security Bhattad *et al.* [7] study the scenario in which the eavesdropper may indeed obtain partial information regarding the messages multicasted over the network, however this partial information does not suffice to deduce the exact value of any of the characters of the source information X . For example, on transmission of a message with two symbols a and b , eavesdropping on the sum $a + b$ reveals partial information about the message (a, b) but does not reveal the exact value of either a or b . Similarly to the paradigm of [9], the work of [7] shows that any network coding scheme of capacity C can be turned into a weakly secure one by multiplying the source information X with a certain matrix T . For this reduction to work, [7] requires a field roughly of size $|E|^{\frac{k}{C-k}}$, where $k \leq z_I$ is a parameter corresponding to the amount of information that the eavesdropper may obtain on the links under his control. Among other related questions, [7] also addresses the natural question of perfect/weak security of a random linear network code without any pre-encoding via T . Here, as in [26], a random linear network code is one

in which the linear coefficients governing the coding scheme are all chosen uniformly and independently at random from the underlying field \mathbb{F} . In addition one assumes that the actions of the eavesdropper (namely which links to control) are independent of these random choices. In this setting a trade-off between field size and probability of error is given (for both perfect and weak security). Roughly speaking, if one allows an ϵ probability of error in the design process, then the field size (when compared to the bounds of [9] for standard security and [7] for weak security) are to be multiplied by a factor of $1/\epsilon$.

The works mentioned above all focused on acyclic networks. Following the analytical techniques of [9], Jain [30] studies secure network coding in the general (not necessarily acyclic) setting. Namely, in [9] a general analysis of secure communication was conducted in the case where the eavesdropper may choose a set of links $A \subseteq E$ from a given set system \mathcal{A} . When the adversarial eavesdropper may control at most z_I links, then \mathcal{A} is just the set system consisting of all subsets of at most z_I links. This general analysis is strengthened in [30] for the cyclic case in which there is a single source node, a single terminal node and one wishes to communicate at unit rate. Namely, necessary and sufficient conditions for secure unit rate communication are presented in terms of the topology of G and the set system \mathcal{A} . In a nutshell, after preprocessing the graph G and removing from G nodes from which information can not reach the single terminal node, the necessary and sufficient condition for secure communication is the existence of a single *untapped* path, *i.e.*, a path not seen by the adversary, from sender to receiver when considering the preprocessed graph as undirected. A characterization for higher communication rate or more terminal nodes is an open problem.

3.2. The Non-Coherent Case

In this section we focus on communication in *non-coherent* settings. That is, the network topology and network coding operations are unknown in advance to the communicating parties. Despite this restriction, it can be shown that essentially the same performance as in the coherent setting can still be achieved. We focus on two lines of work – schemes with randomized source encoding functions, and those with deterministic source encoding functions.

The construction of Feldman *et al.* [14] mentioned in the previous section falls in the former case. In their construction, the linear filter that the source node passes its message through is obtained by randomly choosing a matrix of the appropriate dimension. Interior nodes in the network perform random linear combinations over sufficiently large finite fields, in the spirit of the distributed random linear network coding scheme of Ho *et al.* [26]—indeed, they can be unified to generate a distributed non-coherent random linear network code that is perfectly secure against a wiretapper that can eavesdrop on at most z_I links. They demonstrate that with high probability over these random choices, the generated linear code is perfectly secure against eavesdropping by any adversary that can wiretap at most z_I links. Further, if the min-cut of the network is denoted by C , the rate at which communication can be carried out in this scheme can be made arbitrarily close to $C - z_I$ as the field-size over which the scheme is designed grows without bound. They also show that the field-size required for such a scheme can be much smaller in general, than if one required secret communication at a rate exactly equaling $C - z_I$.

Theorem 2 ([14]). *For any $\sigma > 1$, for any field-size $q \geq \max\{|E|^{\Omega(1/(\sigma-1))}, |S|\}$, there exists a feasible linear network coding scheme with rate $C - \sigma z_I$ which is perfectly secure against a wiretapper eavesdropping on z_I -links. Further, a random choice of source filter achieves this performance with high probability.*

In contrast, they also show that if the desired rate of communication is exactly $C - z_I$, then the minimum field-size required is at least $|E|^{\Omega(\sqrt{z_I/\log z_I})}$. The reason that a small gap from the capacity results in a significant reduction of field-size is that the number of linear transforms that take a message at rate $C - \sigma z_I$ to a message of dimension C is significantly larger than the number of linear transforms that take a message at rate $C - z_I$ to a message of dimension C .

In contrast, Silva *et al.* [78] consider a deterministic source encoder that can be overlaid onto a non-coherent random linear network code (for instance, that of Ho *et al.* [26]). Their work is motivated by Rouayheb and Soljanin's formulation of a wiretap network and builds on their results. They propose a coset coding scheme based on “maximum rank-distance” (MRD) codes, that neither imposes any constraints on, nor requires any knowledge of, the underlying network code. In other words, for any linear network code that is feasible for multicast, secure communication at the

maximum possible rate is achieved with a fixed outer code. In particular, the field size can be chosen as the minimum required for multicasting. The essence of their approach is to use a vector linear outer code over a block-length n that is, in fact, also a linear code over the extension field \mathbb{F}_{q^n} .

Theorem 3 ([78]). *A perfectly secure communication scheme at rate $C - z_I$ can be achieved by using any feasible \mathbb{F}_q -linear network code in conjunction with a fixed end-to-end coset coding scheme based on any linear MRD (C, z_I) code over \mathbb{F}_{q^n} .*

4. JAMMING SECURITY

In this section we consider the design of network codes that enable reliable error-detection and communication in the presence of active jammers that have both eavesdropping and jamming capabilities. Our discussion follows the outline presented in the Introduction.

4.1. The Coherent Case

For the problem of error-correction we first study the rate of reliable communication in the coherent setting in the presence of an active jammer that can jam z_O links of the network and observe all links of the network. In a nutshell, we show that this rate is $C - 2z_O$ for $C \geq 2z_O$ and 0 otherwise. Namely, the rate is equal to $(C - 2z_O)^+$. We start by considering the class of one-hop unicast networks. In a one-hop unicast network there is a single source s that wishes to communicate with a single terminal t over C multiple (s, t) links. We assume that the links may carry a single character from a given alphabet Σ of size q , and that the source wishes to transmit R characters of Σ to t . It is not hard to verify that the task of designing a communication scheme with rate R that allows reliable communication over one-hop unicast networks in the presence of an adversary that may jam z_O of the links is equivalent to the design of $[C, R]$ error correcting codes that are resilient to z_O errors (i.e., have minimum distance $2z_O + 1$).¹

¹ By a similar argument it can also be observed that errors injected by an adversary who can jam z_O links may be detected if and only if the minimum distance of the code is at least $z_O + 1$, i.e., the maximum rate at which adversarial errors can still be detected is $C - z_O$. Here, it is crucial that we assume the coherent setting in which the (network) code is known to all parties. If, however, the adversary cannot observe everything in the network, the work of [25] demonstrates that errors can still be detected for any rate of communication strictly less than C .

Let q be the size of Σ . There are multiple bounds on the rate $R(C, z_O, q)$ of error correcting codes over alphabets of size q with block length C and minimum distance $2z_O + 1$. It is well-known that $R(C, z_O, q) \leq C - \Delta$ for $\Delta = \log_q \left(\sum_{i=0}^{z_O} \binom{C}{i} (q-1)^i \right)$, e.g. [48]. This bound is referred to as the *sphere packing* or *Hamming* bound, and follows from a simple volume argument. As q approaches infinity it can be verified that this bound approaches $C - z_O$. This bound holds for all types of errors—random or adversarial. Further, the *Singleton bound* (e.g. [48]), derived using the pigeonhole principle, shows that $R(C, z_O, q) \leq C - 2z_O$. Hence for sufficiently large alphabet sizes q , the Singleton bound is tighter than the sphere packing bound.

What about lower bounds on $R(C, z_O, q)$? Several coding techniques [48] (including for example Read-Solomon codes) imply C -block error correcting codes resilient to z_O errors whose rate equals $C - 2z_O$. Most relevant to this chapter are the works of Gilbert [18] and Varshamov [79] that show that $R(C, z_O, q) \geq C - \Delta$ where $\Delta = \log_q \left(\sum_{i=0}^{2z_O} \binom{C}{i} (q-1)^i \right)$. Notice that the summation in this case is from 0 to $2z_O$ (as apposed to z_O in the Hamming bound). The discussion above implies that as q tends to infinity, the Singleton bound is tight and corresponds to the capacity of one-hop unicast networks in the presence of jammers.

A natural and intriguing question is whether the above setting also holds in more complicated networks as well. This question was studied by Cai and Yeung in [10, 87] and was answered in the affirmative. Namely, [10, 87] show an analog to the Hamming bound, Singleton bound and Gilbert-Varshamov bound in the coherent network coding setting. Moreover, they show their Singleton-type bound for networks equals their Gilbert-Varshamov type bound for large values of q .² The crux of their analysis lies in understanding the combinatorial nature of information transmitted on minimum *cut-sets* of the network that separate source terminal pairs.³ In what follows we give an overview of the results in [10, 87].

²Tighter bounds on the field-size required were obtained by [2] and in [3] the authors demonstrated that the field-size requirement can be drastically reduced if one reduces the required rate slightly—the result is analogous to the one obtained by Feldman *et al.* [14] for eavesdropping security. High-complexity algorithms for adversarial network error-correction were also obtained in [88].

³The work of [74] translates this analysis (and further results in [10, 87] to be presented shortly) into the language of “matrix channels”, as discussed in Section 4.2.

Consider any given network $G = (V, E)$ with (error free) capacity C . Let A and B be a partition of V , and let $\text{cut}(A, B)$ denote the set of links directed from a node in A to a node in B . To obtain an analog to the Hamming bound for networks, [87] considers the information transmitted over cut sets $\text{cut}(A, B)$, or to be precise, the mapping between the source information X and the information $Z^m = Z_1, \dots, Z_m$ transmitted over the cut set. Here $m = |\text{cut}(A, B)|$. Roughly speaking, if there are no links directed from B to A in G , it must be the case that Z^m is an $[m, 2z_O + 1]$ error correcting code. This follows directly by the fact that decoding at terminal t is solely a function of Z^m . Indeed, if Z^m did not have minimum distance $2z_O + 1$ then a malicious jammer corrupting z_O links from $\text{cut}(A, B)$ may cause a decoding error at t . Note that the reduction above relies on the lack of edges from B to A , otherwise errors on certain links of $\text{cut}(A, B)$ may affect other links in $\text{cut}(A, B)$ (such effects do not occur in the standard model of error-correcting codes). Once the reduction between network communication and error correcting codes is established, the Hamming-type bound and Singleton-type bound follow.

Theorem 4 (Network Hamming Bound). *Let G an acyclic network with (error free) cut capacity C , in which each link can carry a single character of an alphabet Σ of size q . Then the coherent capacity when at most z_O of the links of G are jammed is at most $C - \Delta$ where*

$$\Delta = \log_q \left(\sum_{i=0}^{z_O} \binom{C}{i} (q-1)^i \right).$$

As the field-size q approaches ∞ with fixed C and z_O , this bound approaches $C - z_O$.

As for classical error-correcting codes, a stronger bound for the network adversarial error case for large q is the network analogue of the Singleton bound.

Theorem 5 (Network Singleton Bound). *Let G an acyclic network with (error-free) cut capacity C . Then, the coherent capacity in the presence of an adversary that may jam up to z_O of the links of G is at most $(C - 2z_O)^+$.*

We now turn to discuss lower bounds on the coherent capacity in the presence of an adversary that may jam up to z_O links. In [10] a Gilbert-Varshamov bound in the context of network communication is derived. It is well-known that in the error-free coherent setting, one can communicate the set Σ^C of distinct messages successfully over the network using, for example, linear network codes that are constructed at random. Using such network codes, the main idea in [10] is to carefully construct a subset of messages $W \subset \Sigma^C$ with the property that *no matter which error pattern* is chosen by the adversary, each terminal is able to correctly distinguish the message $w \in W$ transmitted. Namely, two words x and x' of Σ^C are said to be non-separable if there exist two error patterns e and e' such that the information reaching a terminal node when x is transmitted and the adversary applies the error pattern e is *identical* to that received when x' is transmitted and e' applied. The objective in [10] involves identifying a *large* subset W for which each $w \neq w' \in W$ are separable. The crux of their analysis lies in a careful study, for a given $x \in \Sigma^C$, of the subset V_x of possible words x' such that x and x' are non-separable. Bounding the size V of V_x and following the greedy technique of Gilbert [18] will yield sets W of size q^C/V . Moreover, using a Varshamov-type approach one is able to bound V by q^{2z_O} and obtain a linear W of size q^{C-2z_O} .

Theorem 6 (Network Gilbert-Varshamov Bound). *Let G an acyclic network with (error free) cut capacity C in which each link can carry a single character of an alphabet Σ of size q . If q is sufficiently large then, the coherent capacity in the presence of an adversary that may jam up to z_O of the links of G is at least $(C - 2z_O)^+$.*

Corollary 1 (Coherent Capacity). *Let G an acyclic network with (error free) cut capacity C . Then, the coherent capacity in the presence of an adversary that may jam up to z_O of the links of G is $(C - 2z_O)^+$.*

4.2. The Non-Coherent Case

We now consider the rate of reliable communication in the *non-coherent* setting in the presence of a hidden active jammer that can jam z_O links of the network. In this setting neither the network topology nor the network code are known in advance. We show that even then, the same rate of $(C - 2z_O)^+$ is achievable as in the coherent case. In fact, interior nodes in the network can be oblivious to the presence of adversaries, and may

just perform any “good” predesigned network coding operations (such as deterministic multicast network coding, or distributed random network coding). All the complexity is absorbed into the encoder and decoder, which nonetheless have computational complexity that is polynomial in network parameters.

The key to such performance lies in the following observations. As noted in Section 2, if the network performs linear network coding, the relationship between the source’s information X , the fake information Z injected by the adversary, and the information received by the receiver can be expressed as

$$Y = TX + T'Z. \quad (4)$$

This relationship between X and Y is denoted as the (linear) *operator channel*.

The work of [38, 39] contained the following insights. Let \mathcal{X} , \mathcal{Y} and \mathcal{Z} denote the row-spaces of the matrices X , Y , and Z . Then Equation (4) implies that the vector-space \mathcal{Y} is just the direct sum of the vector-spaces \mathcal{X} and \mathcal{Z} , *i.e.*, the smallest vector-space containing both \mathcal{X} and \mathcal{Z} . They then noted that a *subspace metric* $d_S(\cdot, \cdot)$ can be defined on the set of all subspaces of \mathbb{F}_q^n . This is as follows—for any subspaces \mathcal{U} and \mathcal{V} of \mathbb{F}_q^n ,

$$d_S(\mathcal{U}, \mathcal{V}) = \dim \mathcal{U} + \dim \mathcal{V} - 2 \dim(\mathcal{U} \cap \mathcal{V}).$$

It can be seen that this definition does induce a metric – in particular, the triangle inequality is satisfied by $d_S(\cdot, \cdot)$.

This then indicates a strategy for “good” code design for the operator channel, closely paralleling classical algebraic code designs (such as Reed-Solomon codes). The communicating parties choose in advance a codebook comprising of subspaces of \mathbb{F}_q^n , such that each pair of subspaces have a subspace distance of at least $4z_O + 1$ between them.⁴ In [38, 39] the authors demonstrate that it is possible to choose such a codebook with

⁴The reason that the appropriate choice is $4z_O + 1$ rather than the more “intuitive” $2z_O + 1$ one would expect from classical coding theory is as follows. Each packet injected by the adversary may, in the worst case, reduce the dimension of the row-space of TX by one, and simultaneously add a vector to it that is in the row-space of TX' for some $X' \neq X$. Hence each packet injected by the adversary can change the subspace distance by up to two. An alternative metric, the *injection metric* defined in [74] does not require this extra factor of two.

at least $q^{(C-2z_O)(n-C)}$ elements. For a sufficiently large field-size q and packet-length n , this approaches q^{C-2z_O} .

The decoder then does the following – it finds the codeword in the codebook that is closest in subspace distance to the observed space \mathcal{Y} . Since the adversary controls at most z_O links, the dimension of \mathcal{Z} is at most z_O , and hence this decoding algorithm is guaranteed to work correctly.

The authors of [38, 39] demonstrate computationally efficient encoding and decoding of such codes via codes based on *linearized polynomials*, which are analogues of Reed-Solomon codes from classical algebraic coding theory. They then demonstrate in [71, 73, 77] alternative decoding methods of such codes by using rank-metric decoding algorithms proposed by Gabidulin [17].

Taken together, these results imply the following elegant theorem.

Theorem 7 (Noncoherent Capacity for Adversarial Errors). *The noncoherent capacity in the presence of an adversary that may jam up to z_O of the links of G is $(C - 2z_O)^+$. This can be achieved by codes that have computational complexity $\mathcal{O}(C^2n)$.*

The problem of *detecting* (rather than correcting) adversarial network errors in a non-coherent setting is considerably more straightforward. In a scheme proposed in [25] the source appends a non-linear hash to each packet of the data contained within it. They then show that as long as there is even one uncorrupted path from the source to the destination, then arbitrary errors by the adversary can be detected with high probability, via a low-complexity scheme.

Related work also considers the case of random errors on links rather than adversarial errors. In this model the matrices Z are chosen uniformly at random from the set of $z_O \times n$ matrices, rather than deliberately chosen by an adversary so as to minimize the rate at which the sender and the receiver can communicate with each other. Hence one could in principle hope for a higher rate than with adversarial errors. The work in [50] and subsequently the work in [76] show that this is indeed the case. The proof in [76] is admirable in its succinctness, and we sketch the main ideas here.

By assumption (or with high probability under random network code design as in [26]), the transfer matrix T may be assumed to be invertible.

Hence (4) may be rewritten as

$$Y = T(X + T^{-1}T'Z). \tag{5}$$

Here $T^{-1}T'Z$ may also be assumed to be uniformly distributed over the set of all matrices of that dimension.⁵ The code construction is then very similar to the random code construction in [26], except that X is padded with rows and columns comprising entirely of zeroes. More precisely, the first z_0 rows and columns of X are all set to be zero, and the remaining $(C - z_0) \times (n - z_0)$ sub-matrix comprises of a $(C - z_0) \times (C - z_0)$ identity sub-matrix, and a $(C - z_0) \times (n - C)$ payload matrix U , as in

$$\begin{bmatrix} 0_{z_0 \times z_0} & 0_{C \times z_0} & 0_{n \times C} \\ 0_{(C-z_0) \times z_0} & I_{(C-z_0) \times (C-z_0)} & U \end{bmatrix} \tag{6}$$

Then it can be shown [76] that if the top left $z_0 \times z_0$ sub-matrix of W is full rank, then by Gauss-Jordan elimination the row-reduced form of the received matrix Y equals

$$\begin{bmatrix} Z_1 & 0_{C \times z_0} & Z_2 \\ 0_{(C-z_0) \times z_0} & TI_{(C-z_0) \times (C-z_0)} & TU \end{bmatrix} \tag{7}$$

But if this is the case, since T is assumed to be invertible, the information payload U can be reconstructed from the last $C - z_0$ rows of (7). The only remaining step is to demonstrate that W does indeed satisfy, with high probability over Z , the rank constraint assumed above. It is shown in [76] that for large q or n this probability is at least $1 - o(1/q^{n-2z_0})$.

This leads to the following theorem.⁶

Theorem 8 (Noncoherent Capacity for Random Errors). *Let G an acyclic network with (error free) cut capacity C . Then with probability at least $1 - o(1/q^{n-2z_0})$ the noncoherent capacity in the presence of random packets injected on at most z_0 of the links of G is $C - z_0$. This can be achieved by codes that have decoding complexity $\mathcal{O}(C^2n)$.*

⁵ This turns out to be the worst case – if $T^{-1}T'Z$ is not uniformly distributed due to rank deficiency in $T^{-1}T'$, the problem may be transformed linearly into another one with different parameters where in fact this is the case.

⁶ A similar result and algorithm for random errors was also independently proposed in [88].

Lastly, we touch upon an alternate schema for efficient noncoherent network error correction, proposed in [27, 28] in parallel to the work in [38, 39]. While the rates achievable are asymptotically equivalent in the limit of large field-size q and packet-length n , the parameters for [27, 28] are generally inferior, in that the required q and n are larger in [27, 28], and the computational complexity is $\Theta(n^3)$ rather than $\mathcal{O}(C^2n)$ as in [38, 39].

However, one advantage of the proof techniques in [27, 28] is that they allow for computationally efficient “linear list-decoding”. A code is said to be l -list decodable at rate $R(C, z_O, q)$ if, given the constraint z_O on the set of error patterns, the decoder can always output a list of size at most l which is guaranteed to contain the transmitted codeword. Further, it is said to be linear list decodable at that rate if the list can be represented in the form of an affine shift of a subspace of \mathbb{F}_q^n . That is, every vector in the list is of the form $\mathbf{v} + \mathcal{L}$, for some fixed vector \mathbf{v} and some fixed subspace \mathcal{L} with l elements. Then

Theorem 9 (Linear List Decoding). *There exist codes of rate $C - z_O$ that are linear q^{C^2} -list decodable in the presence of an adversary that may jam up to z_O of the links of G . The computational complexity of such codes is $\mathcal{O}(C^3n)$.*

The idea is as follows. The encoder chooses a codebook comprising of q^{C-z_O} matrices X , each of rank $C - z_O$. Since the rank of Z is at most z_O , therefore the rank of the matrix whose rows comprise of the rows respectively of X and Z is at most C – without loss of generality, we henceforth assume that it is in fact exactly C (if not, similar arguments hold for smaller values of the rank).

The decoder selects C linearly independent columns of Y , and denotes the corresponding matrix Y^s . The columns of X and Z corresponding to those in Y^s are denoted X^s and Z^s respectively. By (4), $Y^s = [T|T'] \begin{bmatrix} X^s \\ Z^s \end{bmatrix}$. Also, since Y^s acts as a basis for the columns of Y , we can write $Y = Y^s F$ for some matrix F . The decoder can compute F as $(Y^s)^{-1} Y$. Therefore Y can also be written as

$$Y = [T|T'] \begin{bmatrix} X^s F \\ Z^s F \end{bmatrix} \quad (8)$$

Comparing Equations (4) and (8), and again using the assumption that $[T|T']$ is invertible (with high probability) implies that

$$X = X^s F, \quad (9)$$

$$Z = Z^s F. \quad (10)$$

In particular, Equation (9) gives a linear relationship on X that can be leveraged into a list-decoding scheme for the decoder. The number of variables in X^s is C^2 . Therefore the entries of the matrix X^s span a vector space of dimension C^2 over \mathbb{F}_q . Bob's list is the corresponding C^2 -dimensional vector space \mathcal{L} spanned by $X^s F$.

Such a list-decoding result is useful in a variety of settings. For instance, in [27, 28] this result is used as the first stage of a noncoherent network error-correcting code—first this result is used by the decoder to generate an affine subspace containing the source's message X , and then the decoder refines this list using extra constraints imposed on the codebook as part of code design. Even though the size of this list is large (q^{C^2}) this refinement procedure can be done computationally efficiently, since the list is affine. Another use of this list decoding result is seen in the next section, on cryptographic protocols.

Note: A special class of errors is that of “packet erasures”. As has been observed by several authors (see, for instance [38]), z_O packet erasures, whether random or adversarial, correspond to a rate-loss of at most z_O , in contrast to a rate-loss of $2z_O$ in the presence of adversarial errors. Hence the best achievable rate in the presence of z_O erasures is $C - z_O$.

4.3. The Cryptographic Setting

In this section we address adversarial jammers that are computationally bounded. Namely, jammers against which one can apply certain cryptographic primitives. In this line of study, one assumes that certain computational tasks (such as Discrete Log or Factoring) are intractable, and based on these assumptions designs a feasible communication scheme. We show the ability to communicate at rate $C - z_O$ in the presence of a computationally bounded adversary that can corrupt up to z_O links of the network. Notice that this improves on the rate of $C - 2z_O$ presented in Sections 4.1 and 4.2 in which the jammer has no computational limitations. Also notice that this rate is the best possible. Since most of

the schemes described below proceed by first detecting adversarial attacks and then discarding erroneous packets, network error-detection is a direct by-product of the schemes.

Roughly speaking, the works we survey have one of two flavors: *in-network* authentication or *end-to-end* authentication. In the in-network setting, one designs certain authentication mechanisms that allow internal nodes of the network to identify information packets that have been corrupted by the jammer. Once such faulty packets are found, the internal nodes of the network may discard them. This reduces communication in the presence of a jammer to such in which the jammer is absent—but some links of the network are not able to transmit information. The latter scenario, for which standard random linear network coding schemes (e.g., [26]) allow reliable communication, is well understood. There are several challenges in this line of study. These include the design of efficient signature schemes that are on one hand closed under linear coding operations (such signature schemes are referred to as *homomorphic* [4–6, 12, 31, 49, 60]) and on the other do not need an elaborate infrastructure to support key distribution among internal nodes of the network. In-network authentication indeed guarantees communication at rate $C - z_O$, however, in many cases a higher rate is achievable (depending on the exact links controlled by the jammer).

In end-to-end authentication, internal nodes of the network are oblivious to the fact that communication is done in the presence of an adversarial jammer, and follow standard coding protocols used commonly when a jammer is absent. The presence of the jammer is dealt with by an enhanced encoding at the source node and by specialized decoding at terminal nodes. End-to-end schemes have obvious advantages in code management over in-network authentication, and as in-network schemes they promise rate $C - z_O$. However, when compared to in-network authentication on an “instance to instance” basis it may be true that end-to-end authentication obtains a lower rate (here the location of the jammer comes into play – end-to-end authentication schemes assume that the adversary locates itself in a worst-case manner in the network, and hence might be unduly pessimistic.).

In-Network Authentication

A hash function h is referred to as homomorphic if for $x = \sum_i x_i$ it holds that $h(x) = \sum_i h(x_i)$. Homomorphic hash functions lend themselves naturally to the random (non-coherent) network coding scheme of

Ho *et al.* [26]. A node receiving information y_e , and coefficients $\{\alpha_i\}$ (that in the error free scenario should satisfy $y_e = \sum \alpha_i x_i$ for source information x_i) may check if $h(y_e) = \sum \alpha_i h(x_i)$ and by so, authenticate the received information. Here local information $h(x_i)$ is assumed to be known at internal nodes of the network. Indeed, if h is homomorphic and it is computationally *hard* for a given y to compute x such that $h(x) = y$, then a corrupted y_e will, with high probability, fail the authentication check.

Given the outline above it is natural to study the requirements from the local information $h(x_i)$ specified above. In the works of Krohn *et al.* [41] and Gkantsidis and Rodriguez [21], the hashes of the source information $h(x_i)$ are assumed to be reliably communicated to internal nodes of the network (otherwise, an adversary able to forge this information may indeed inject fake messages that will pass the internal node authentication process). Hence, a centralized trusted authority is assumed to provide these hashes. The security of the communication scheme suggested in [21, 41] is based on the hardness of the Discrete-Log problem.

In the works of Charles *et al.* [11], Zhao *et al.* [13], and Boneh *et al.* [8] the need for a reliable channel to distribute the hash values used for authentication is obviated using the notion of public key cryptography. In [11], the communication scheme suggested is based on the hardness of Discrete-Log and the computational co-Diffie-Hellman problem on elliptic curves. Zhao *et al.* [13] present a scheme based on *linear subspace authentication* which prevents the adversarial jammer to inject a fake message v into the network given that v is not in the space V spanned by the source information. Their scheme relies solely on the hardness of Discrete Log. Finally, in [8], two schemes based on the linear subspace authentication paradigm of [13] are presented. Boneh *et al.* [8] show that both schemes have public key sizes that are essentially optimal for this authentication paradigm. The first scheme of [8] is a homomorphic one and is based on the computational Diffie-Hellman assumption, while the second scheme is a non-homomorphic variation to the schemes of [41] and [13] which is based on the Discrete-Log problem.

Theorem 10 (In-Network Authentication). *Let G an acyclic network with (error free) cut capacity C . Using in-network authentication, the capacity in the presence of a computationally bounded adversary that may jam up to z_O of the links of G is $C - z_O$.*

End-to-End Authentication

Similar to the works mentioned above, in [54] Nutman and Langberg also consider enhancing the (non-coherent) network coding scheme of Ho *et al.* [26]. However, in the communication scheme presented in [54] internal nodes of the network follow the exact same protocol as specified in [26]—and are thus oblivious to the presence of an adversarial jammer. The only changes made with respect to [26] are in the encoding and decoding procedures of the source and terminals.

To be more precise, the protocol of [54] builds on the non-coherent schemes of Jaggi *et al.* [27, 28] (which in turn builds on [26]) and has the following overall structure. In [27, 28], a non-coherent communication scheme of rate $C - z_O$ in the presence of an unconditional jammer (with unlimited computational power) that controls $C - z_O$ links is presented. The rate of $C - z_O$ is not possible in light of the discussion in Section 4.1 and can only be obtained under additional assumptions. Indeed in [27, 28], the rate $C - z_O$ is obtained under the additional assumption that the source and terminal nodes share a *low rate* side channel in which they may communicate a short secret (which is not known to the adversarial jammer). The analysis in [27, 28] is based on the observation that allowing *list decoding* (as opposed to *unique* decoding) at terminal nodes, rate $C - z_O$ is achievable in the presence of a jammer controlling z_O links (see Theorem 9). Once such a list is obtained, each terminal may pick the correct element from its list using the secret side information transmitted. The secrecy of the side information is crucial to avoid the jammer from imposing *taylor-made* errors that will imply certain lists at terminal nodes that cannot be disambiguated using the side information.

With the list decoding results of [27, 28] in mind (or any other list decodable scheme such as [47]), [54] considers the following natural modification. Instead of transmitting the side information of [27, 28] over a side channel (which is not present in the current model), [54] encrypts this information using any (not necessarily homomorphic) public key encryption scheme and transmit the encrypted side information over the network. Assuming the jammer cannot break the encryption scheme ensures that the side information remains secret, however the side information still needs to be transmitted to the terminals reliably. To attain this goal, [54] uses any one of the encoding schemes from Section 4.2 on the encrypted side information. Using the fact that the side information is of low rate, time

sharing between the encoded side information and the coded source information yields rate $C - z_O$. We note that to ensure reliable communication of the side information, [54] requires that $C > 2z_O$. This last condition is proven in [54] to be necessary (under certain assumptions).

Theorem 11 (End-to-End Authentication). *Let G be an acyclic network with (error free) cut capacity C . Using end-to-end authentication, the capacity in the presence of a computationally bounded adversary that may jam up to z_O of the links of G is $C - z_O$ for $C > 2z_O$.*

5. SECRET TRANSMISSION IN PRESENCE OF EAVESDROPPING AND JAMMING ADVERSARIES

5.1. The Coherent Case

In this final section we consider the interplay between eavesdropping and jamming. As we saw in Section 3, to protect a message against an eavesdropper that can listen to z_I links requires a rate-loss of at least z_I . We also saw that distributed low-complexity schemes with this rate-loss exist and achieve a secrecy rate of $C - z_I$. They do this essentially by linearly mixing a random message of rate z_I with the source message of rate $C - z_I$. Thus, these schemes can thus be thought of as a one-time pad ([64]) combined with network coding.

Next, in Section 4 we have seen that a network with a hidden adversarial jammer who observes all transmissions, and can jam z_O links, can effectively reduce the rate at which information can be transmitted from the source to the destination, down to $C - 2z_O$. Further, there are distributed low-complexity schemes that achieve this rate. These schemes can then be thought of as converting an error-prone operator channel of capacity C into an error-free operator channel of capacity $C - 2z_O$.

In scenarios where the adversary can only observe z_I transmissions in the network and jam z_O links, it is natural to ask what the best achievable rates of secret and reliable communication are. In the case with zero errors and single-letter coding, the work of [52] shows this to be the “natural” combination of the two above bounds, for an overall rate of $C - 2z_O - z_I$. They prove this by similar techniques as used to bound the rates in the previous two sections. This bound was extended by [72] and [75] to zero-error

block-length coding as well.⁷ Also, algorithms meeting these bounds are presented for the coherent case in [51] (for block coding) and [52] (for single-letter coding). These algorithms essentially work by merging the algorithms in the previous two sections—first they construct a coding scheme that converts the error-prone operator channel into an error-free operator channel of rate $C - 2z_O$, and on this channel they overlay a “one-time pad + network coding” scheme that ensures secrecy against a wiretapping adversary, which further reduces the rate to the overall rate of $C - 2z_O - z_I$. This leads to the following theorem.

Theorem 12 ([51, 52, 72, 75]). *The maximal rate at which secret information can be reliably communicated (with zero-error) over a network containing a hidden adversary who can eavesdrop on z_I links and jam z_O links is $C - 2z_O - z_I$.*

Interestingly, if one relaxes the requirement to zero-error to one of “small” error (asymptotically small in the field-size or block-length), then the upper bound of $C - 2z_O - z_I$ no longer holds – only a bound of $C - z_O - z_I$ can be shown. And in fact, as we shall see in the next subsection, this higher rate is in fact achievable with low-complexity code designs.

5.2. The Non-Coherent Case

The work of in [72, 75] extends the results of Section 5.1 to give *universal* code designs. That is, given an arbitrary linear network code such that the rank of the linear transform is C , [72, 75] present an end-to-end scheme that treats the network code as an operator channel, and achieves the secrecy rate of $C - 2z_O - z_I$ as in Section 5.1. These constructions are based on rank-metric codes – it is shown that such codes are good not just for error-correction as in Section 4.2, but also simultaneously for secrecy-preserving linear mappings at the source.

Further work in [86] demonstrated that as long as the sum of the adversary's jamming rate z_O and his eavesdropping rate z_I is less than

⁷ In fact [72] prove the more general lower bound of $C - 2z_O - z_I - \rho$, where ρ is the number of (possibly adversarially located) erasures.

the network capacity C , (i.e., $z_O + z_I < C$), there exist codes with low computational complexity that can communicate (with vanishingly small error probability) a single bit correctly and without leaking any information to the adversary. This is then combined with a “secret-sharing” result of [27, 28] to design codes that allow communication at the optimal source rate of $C - z_O + z_I$ while keeping the communicated message secret from the adversary. In particular, the secret-sharing result of [27, 28] implies:

Theorem 13 ([27, 28]). *If in a network containing a hidden adversary who can jam at most z_O links, ϵn bits (for any fixed $\epsilon > 0$) can be secretly and reliably transmitted from the source to the destination, then in fact $(C - z_O - z_I)n$ bits can be secretly and reliably transmitted from the source to the destination.*

The main idea behind Theorem 13 is as follows. If the source node generates a “small” secret linear hash of its information and sends it to the receiver over a secret and reliable channel, then, using the linear list decoding result of Theorem 9, with high probability the receiver is able to refine the list down to a single element.

It only remains to describe a protocol to secretly and reliably share a bit over the network (one that may emulate a secret and reliable channel). To do this [86] use the following straightforward “rank modulation” protocol. If the bit to be shared is a 0, then the source’s message is a matrix (over a short block-length, and hence asymptotically negligible in the true block-length corresponding to the packet-size) of rank $C - z_O - 1$. Else its message is a random matrix of rank C . The decoder decodes by estimating the rank of the received matrix. If it equals C , it decodes the secret bit as 1, else it decodes to 0.

To check that the above protocol succeeds with high probability one needs to check both its secrecy and the reliability. Secrecy is guaranteed since the adversary eavesdrops on at most z_I transmissions, which, due to the random linear mixing in the network and the constraint that $C - z_O - z_I > 0$, are not enough for it to be able to distinguish between a source message of rank $C - z_O - 1$, and a source message of rank C packets. Reliability is due to the following two arguments. First, since the adversary can inject at most z_O packets, if the source’s message was 0 and so it transmits a matrix of rank $C - z_O - 1$ the rank of the received matrix

must still be less than C . Conversely, if the source's message was 1 and hence it transmitted a truly random matrix of rank C , since the adversary does not know what this matrix is, the probability that it is able to reduce the rank of the received matrix is small.

6. SOME OTHER VARIANTS

We summarize here some of the other work on topics related to secure and reliable communication over networks, which do not fall neatly into previous sections.

- The work in refs [36, 37, 63] considers network error-correction problems in scenarios where links have unequal capacities—a complete characterization of achievable rates in this case is still open.
- Kosut *et al.* [55, 56] consider the problem where *nodes* rather than edges are adversarially controlled. Here, again, the rate-region is yet to be fully characterized. Reliable communication using network coding in the presence of untrusted nodes is also considered in [82].
- Multiple-access variants of network error-correction have been considered in refs [68–70, 81, 84].
- As an analog of the classical algorithms for point-to-point channels considered in [22], the work of [47] presents non-trivial list-decoding algorithms of network error-correcting codes.
- The work of [59] considers the problems of reliability and secrecy for distributed data storage.
- The problem of finding the actual location of errors in the network has been considered in, among other works refs [15, 16, 19, 23, 65–67, 85].
- In [45, 80], a **Secure Practical Network Coding** scheme (SPOC) is suggested that allows private communication against a computationally bounded adversary that may eavesdrop on all communication transmitted over the network. At its core, SPOC runs a modified variant of random linear coding [26] in which the *header* of each packet (containing the coding coefficients) is encrypted and unknown to the adversary while the body of the packet (containing the encoded information via network coding) is sent in the clear.
- The authors of refs [33–35] consider error detection in wireless networks in which adversarial nodes may behave maliciously. Using the

algebraic watchdog scheme, upstream nodes can detect malicious behaviors probabilistically by taking advantage of the broadcast nature of the wireless medium.

7. DISCUSSION

This chapter gives a brief summary of the coding schemes used in multicast network coding in the presence of passive and active jammers. We have seen that non-coherent secure communication at rate $C - z_I$ is possible in the presence of a passive eavesdropper that controls z_I links of the network. This rate is the best possible, even when considering coherent communication schemes. For active jammers, we have shown that non-coherent reliable communication at rate $C - 2z_I$ is possible in the presence of a jammer that controls z_O links of the network. If the jammer is computationally limited, a higher rate of $C - z_O$ is achievable. As before, these rates are the best possible, even when considering coherent communication schemes. Finally, when communicating in the presence of adversaries that may jam z_O links and eavesdrop on z_I links, communication which is both secure and reliable is possible at a tight rate of $C - 2z_O - z_I$ (or $C - z_O - z_I$ once one allows a small probability of error). The algorithmic techniques presented cover several paradigms and include tools from the study of combinatorics, linear algebra, and coding theory. The chapter at hand has addressed the task of multicast in acyclic networks. Understanding the power of network coding in a more general setting with or without adversaries remains an intriguing field of study that will surely evolve over the decades to come.

ACKNOWLEDGMENTS

The authors would like to thank Danilo Silva for many helpful discussions during the preparation of this chapter.

REFERENCES

- [1] R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung. Network information flow. *IEEE Transactions on Information Theory*, 46(5):1204–1216, July 2000.
- [2] H. Balli, X. Yan, and Z. Zhang. Error correction capability of random network error correction codes. In *Proc. International Symposium on Information Theory*, Sept. 2007.

- [3] H. Balli, X. Yan, and Z. Zhang. On Randomized Linear Network Codes and Their Error Correction Capabilities. *IEEE Transactions on Information Theory*, 55(7):3148–3160, 2009.
- [4] N. Baric and B. Pfitzmann. Collision-free accumulators and failstop signature schemes without trees. In *Advances in Cryptology EUROCRYPT*, 1997.
- [5] M. Bellare and D. Micciancio. A new paradigm for collision-free hashing: Incrementality at reduced cost. In *Advances in Cryptology EUROCRYPT*, 1997.
- [6] J. Benaloh and M. de Mare. One-way accumulators: A decentralized alternative to digital sinatures. In *Advances in Cryptology EUROCRYPT*, 1993.
- [7] K. Bhattad and K. R. Narayanan. Weakly secure network coding. In *proceedings of NetCod*, 2005.
- [8] D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *12th International Conference on Practice and Theory in Public Key Cryptography*, pages 68–87, 2009.
- [9] N. Cai and R. W. Yeung. Secure network coding. In *Proceedings of International Symposium in Information Theory*, Lausanne, Switzerland, June 2002.
- [10] N. Cai and R. W. Yeung. Network error correction, part II: Lower bounds. *Commun. Inf. Syst.*, 6(1):37–54, 2006.
- [11] D. Charles, K. Jain, and K. Lauter. Signatures for network coding. In *Proceedings of the fortieth annual Conference on Information Sciences and Systems*, Princeton, NJ, USA, 2006.
- [12] D. Chaum, E. van Heijst, and B. Pfitzmann. Cryptographically strong undeniable signatures, unconditionally secure for the signer. In *Advances in Cryptology CRYPTO*, 1991.
- [13] M. Médard, F. Zhao, T. Kalker, and K. J. Han. Signatures for content distribution with network coding. In *Proceedings of International Symposium on Information Theory (ISIT 2007)*, pages 556–560, 2007.
- [14] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio. On the capacity of secure network coding. In *Proceedings of 42nd Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2004.
- [15] C. Fragouli and A. Markopoulou. A network coding approach to network monitoring. In *Proc. of the 43rd Allerton Conference*, 2005.
- [16] C. Fragouli, A. Markopoulou, and S. Diggavi. Topology inference using network coding. In *Proc. of the 44th Allerton Conference*, 2006.
- [17] E. M. Gabidulin. Theory of codes with maximum rank distance. *Probl. Inform. Transm.*, 21(1):1–12, 1985.
- [18] E. N. Gilbert. A comparison of signalling alphabets. *Bell Systems Technical Journal*, 31:504–522, 1952.
- [19] M. Gjoka, C. Fragouli, P. Sattari, and A. Markopoulou. Loss tomography in general topologies with network coding. In *Proc. of IEEE Globecom*, 2005.
- [20] C. Gkantsidis and P. Rodriguez. Network coding for large scale content distribution. In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, Miami, March 2005.
- [21] C. Gkantsidis and P. Rodriguez. Cooperative security for network coding file distribution. In *Proceedings of IEEE Conference on Computer Communications (INFOCOM)*, pages 1–13, Barcelona, April 2006.
- [22] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45:1757–1767, September 1999.

- [23] L. Hailiang, H. Guangmin, Q. Feng, and Y. Zhihao. Network topology inference based on traceroute and tomography. In *Proc. of International Conference on Communications and Mobile Computing*, 2009.
- [24] T. Ho., R. Kötter, M. Médard, D. Karger, and M. Effros. The benefits of coding over routing in a randomized setting. In *IEEE International Symposium on Information Theory (ISIT)*, page 442, Yokohama, July 2003.
- [25] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. R. Karger. Byzantine modification detection in multicast networks using randomized network coding. *IEEE Transactions on Information Theory*, 54(6):2798–2803, 2008.
- [26] T. Ho, M. Médard, R. Kötter, D. R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE Transactions on Information Theory*, 52(10):4413–4430, 2006.
- [27] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard. Resilient network coding in the presence of Byzantine adversaries. In *Proc. 26th IEEE Int. Conf. on Computer Commun.*, pages 616–624, Anchorage, AK, May 2007.
- [28] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Médard, and M. Effros. Resilient network coding in the presence of Byzantine adversaries. *IEEE Transactions on Information Theory*, 54(6):2596–2603, June 2008.
- [29] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen. Polynomial time algorithms for multicast network code construction. *IEEE Transactions on Information Theory*, 51(6):1973–1982, June 2005.
- [30] K. Jain. Security based on network topology against the wiretapping attack. *IEEE Wireless Communications*, pages 68–71, Feb 2004.
- [31] R. Johnson, D. Molnar, D. Song, and D. Wagner. Homomorphic signature schemes. In *Progress in Cryptology CT RSA*, 2002.
- [32] S. Katti, H. Rahul, D. Katabi, W. Hu M. Médard, and J. Crowcroft. XORs in the Air: Practical Wireless Network Coding. In *ACM SIGCOMM*, Pisa, Italy, 2006.
- [33] M. Kim, M. Médard, and J. Barros. A multi-hop multi-source algebraic watchdog. In *IEEE Information Theory Workshop (ITW)*, Dublin, Ireland, August 2010.
- [34] M. Kim, M. Médard, and J. Barros. Algebraic watchdog: Mitigating misbehavior in wireless network coding. Submitted to *IEEE Journal on Selected Areas in Communications (JSAC)*, Advances in Military Networking and Communications, <http://arxiv.org/abs/1011.3879>, November 2010.
- [35] M. Kim, M. Médard, J. Barros, and R. Kötter. An algebraic watchdog for wireless network coding. In *IEEE International Symposium on Information Theory (ISIT)*, June 2009.
- [36] S. Kim, T. Ho, M. Effros, and S. Avestimehr. Network error correction with unequal link capacities: capacities and upper bound. In *preparation for submission to the IEEE Transactions on Information Theory*, 2009.
- [37] S. Kim, T. Ho, M. Effros, and S. Avestimehr. New results on network error correction: capacities and upper bound. In *Proceedings of Information Theory and Applications Workshop, UCSD*, San Diego, CA, 2010.
- [38] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. In *Proc. IEEE Int. Symp. Information Theory*, pages 791–795, Nice, France, June 24–29, 2007.
- [39] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.
- [40] R. Kötter and M. Médard. An algebraic approach to network coding. *IEEE/ACM Transactions on Networking*, 11(5):782–795, October 2003.

- [41] Maxwell N. Krohn, Michael J. Freedman, and David Mazires. On-the-fly verification of rateless erasure codes for efficient content distribution. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 226–240, Oakland, California, 2004.
- [42] M. Langberg, A. Sprintson, and J. Bruck. The encoding complexity of network coding. *IEEE Transactions on Information Theory (a joint special issue with IEEE/ACM Transactions on Networking on Networking and Information Theory)*, 52(6):2386–2397, 2006.
- [43] M. Langberg, A. Sprintson, and J. Bruck. Network Coding: A Computational Perspective. *IEEE Transactions on Information Theory*, 55(1):147–157, 2009.
- [44] S.-Y. R. Li, R. W. Yeung, and N. Cai. Linear network coding. *IEEE Transactions on Information Theory*, 49(2):371–381, 2003.
- [45] L. Lima, J. P. Vilela, J. Barros, and M. Médard. An information-theoretic cryptanalysis of network coding – is protecting the code enough? In *Proceeding of the International Symposium on Information Theory and its Applications (ISITA)*, 2008.
- [46] D. S. Lun, M. Médard, and R. Kötter. Efficient operation of wireless packet networks using network coding. In *International Workshop on Convergent Technologies (IWCT)*, Oulu, Finland, 2005.
- [47] H. Mahdaviifar and A. Vardy. Algebraic list-decoding on the operator channel. In *Proc. of International Symposium on Information Theory (ISIT)*, Austin, TX, USA, June 13–19 2010.
- [48] F. J. McWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [49] S. Micali and R. Rivest. Transitive signature schemes. In *Progress in Cryptology CT RSA*, 2002.
- [50] A. Montanari and R. Urbanke. Coding for network coding. *IEEE Transactions on Information Theory (submitted for publication)*, 2007. <http://arxiv.org/abs/0711.3935>.
- [51] C. K. Ngai and S. Yang. Deterministic secure error-correcting (SEC) network codes. In *Proc. IEEE. Information Theory Workshop*, pages 96–101, Bergen, Norway, June 24–29, 2007.
- [52] C.-K. Ngai and R. W. Yeung. Secure error-correcting (SEC) network codes. In *Workshop on Network Coding, Theory and Applications (NetCod)*, pages 791–795, Lausanne, Switzerland, June 2009.
- [53] C. K. Ngai, R. W. Yeung, and Z. Zhang. Network Generalized Hamming Weight. In *Proc. 2009 Workshop on Network Coding, Theory, and Applications*, 2009.
- [54] L. Nutman and M. Langberg. Adversarial models and resilient schemes for network coding. In *Proceedings of International Symposium on Information Theory*, pages 171–175, 2008.
- [55] L. Tong O. Kosut and D. Tse. Nonlinear network coding is necessary to combat general byzantine attacks. In *Proc. of 47th Annual Allerton Conference on Communication, Control, and Computing*, October 2009.
- [56] L. Tong O. Kosut and D. Tse. Polytope codes against adversaries in networks. In *Proc. of International Symposium on Information Theory (ISIT)*, Austin, TX, USA, June 13–19, 2010.
- [57] L. H. Ozarow and A. D. Wyner. The wire-tap channel II. *Bell Syst. Tech. Journ.*, 63:21352157, 1984.
- [58] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. In *Proceedings of the EURO-CRYPT 84 workshop on advances in cryptology: theory and application of cryptographic techniques*, pages 33–51, 1985.

AQ:1

- [59] S. Pawar, S. El-Rouayheb, and K. Ramchandran. On secure distributed data storage under repair dynamics. In *Proc. IEEE Int. Symp. Information Theory*, June 13–19 2010.
- [60] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Advances in Cryptology CRYPTO*, 1991.
- [61] S. E. Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. *Manuscript, available on arXiv.org*, 2009.
- [62] S. E. Rouayheb and E. Y. Soljanin. On Wiretap Networks II. In *proceedings of IEEE International Symposium on Information Theory*, pages 551–555, 2007.
- [63] M. Effros S. Kim, T. Ho and S. Avestimehr. Network error correction with unequal link capacities. In *Proceedings of 47th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, 2008.
- [64] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.
- [65] J. M. Siavoshani, C. Fragouli, and S. Diggavi. Subspace properties of randomized network coding. In *Proc. of IEEE ITW*, 2007.
- [66] M. Jafari Siavoshani, C. Fragouli, and S. Diggavi. On locating byzantine attackers. In *Network Coding Workshop: Theory and Applications*, 2008.
- [67] M. Jafari Siavoshani, C. Fragouli, S. Diggavi, and C. Gkantsidis. Bottleneck discovery and overlay management in network coded peer-to-peer system. In *Proc. of SIGCOMM workshop on Internet Network Management*, 2007.
- [68] M.J. Siavoshani, C. Fragouli, and S. Diggavi. Noncoherent multisource network coding. In *Proc. IEEE Int. Symp. Information Theory*, pages 817–821, Toronto, Canada, July 6–11, 2008.
- [69] M.J. Siavoshani, C. Fragouli, and S. Diggavi. Code construction for multiple sources network coding. In *Proc. of the MobiHoc*, 2009.
- [70] M.J. Siavoshani, S. Mohajer, C. Fragouli, and S. Diggavi. On the capacity of non-coherent network coding. In *Proc. of the IEEE International Symposium on Information Theory*, 2009.
- [71] D. Silva and F. R. Kschischang. Using rank-metric codes for error correction in random network coding. In *Proc. IEEE Int. Symp. Information Theory*, pages 796–800, Nice, France, June 24–29, 2007.
- AQ:1 [72] D. Silva and F. R. Kschischang. Universal secure network coding via rank-metric codes. *IEEE Transactions on Information Theory*, 2008. To appear in *IEEE Transactions on Information Theory*.
- [73] D. Silva and F. R. Kschischang. Fast encoding and decoding of Gabidulin codes. In *Proc. IEEE Int. Symp. Information Theory*, Seoul, Korea, June 2009.
- [74] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions on Information Theory*, 55(12):5479–5490, 2009.
- [75] D. Silva and F. R. Kschischang. Universal secure error control schemes for network coding. In *Proc. IEEE Int. Symp. Information Theory*, Austin, TX, USA, June 13–19, 2010.
- [76] D. Silva, F. R. Kschischang, and R. Kötter. Capacity of random network coding under a probabilistic error model. In *Proc. 24th Biennial Symposium on Communications*, Kingston, ON, Canada, June 2008.
- [77] D. Silva, F. R. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.

- [78] Danilo Silva and Frank R. Kschischang. Universal weakly secure network coding. In *Proc. Inform. Theory Workshop on Networking and Inform. Theory*, pages 281–285, Volos, Greece, June 10–12, 2009.
- [79] R. R. Varshamov. Estimate of the number of signals in error correcting codes. *Dokl. Acad. Nauk*, 117:739–741, 1957.
- [80] J. P. Vilela, L. Lima, and J. Barros. Lightweight security for network coding. In *Proc. of the IEEE International Conference on Communications (ICC 2008)*, Beijing, China, May 2008.
- [81] S. Vyetenko, T. Ho, M. Effros, J. Kliewer, and E. Erez. Rate regions for coherent and noncoherent multisource network error correction. In *Proc. of International Symposium on Information Theory (ISIT)*, Seoul, Korea, June 2009.
- [82] D. Wang, D. Silva, and F. R. Kschischang. Robust network coding in the presence of untrusted nodes. *To appear in IEEE Transactions on Information Theory*, 2010.
- [83] V. K. Wei. Generalized Hamming Weight for Linear Codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.
- [84] H. Yao, T. K. Dikaliotis, S. Jaggi, and T. Ho. Multiple access network information-flow and correction codes. In *Proc. IEEE Information Theory Workshop*, Dublin, Ireland, 2010.
- [85] H. Yao, S. Jaggi, and M. Chen. Passive network tomography for erroneous networks: A network coding approach. Under submission to the IEEE Transactions on Information Theory, 2010.
- [86] H. Yao, D. Silva, S. Jaggi, and M. Langberg. Network codes resilient to jamming and eavesdropping. In *Proc. Workshop on Network Coding Theory and Applications*, Toronto, Canada, June 9–11 2010.
- [87] R. W. Yeung and N. Cai. Network error correction, part I: Basic concepts and upper bounds. *Commun. Inf. Syst.*, 6(1):19–36, 2006.
- [88] Z. Zhang. Linear network error correction codes in packet networks. *IEEE Transactions on Information Theory*, 54(1):209–218, January 2008.

Author Queries

AQ Please provide the Affiliation.

AQ:1 Please provide publication details.