Byzantine Modification Detection in Multicast Networks With Random Network Coding

Tracey Ho, *Member, IEEE*, Ben Leong,
Ralf Koetter, *Senior Member, IEEE*, Muriel Médard, *Fellow, IEEE*,
Michelle Effros, *Senior Member, IEEE*, and
David R. Karger, *Associate Member, IEEE*

***Abstract*—An information-theoretic approach for detecting Byzantine or adversarial modifications in networks employing random linear network coding is described. Each exogenous source packet is augmented with a flexible number of hash symbols that are obtained as a polynomial function of the data symbols. This approach depends only on the adversary not knowing the random coding coefficients of all other packets received by the sink nodes when designing its adversarial packets. We show how the detection probability varies with the overhead (ratio of hash to data symbols), coding field size, and the amount of information unknown to the adversary about the random code.**

***Index Terms*—Byzantine adversary, multicast, network coding, network error detection.**

I. Introduction

We consider the problem of information-theoretic detection of Byzantine, i.e., arbitrary, modifications of transmitted data in a network coding setting.

Interest in network coding has grown following demonstrations of its various advantages: in network capacity [1], robustness to nonergodic network failures [2] and ergodic packet erasures [3], [4], and distributed network operation [5]. Multicast in overlay and *ad hoc* networks is a promising application. Since packets are forwarded by end hosts to other end hosts, such networks are susceptible to Byzantine errors introduced by compromised end hosts.

We show that Byzantine modification detection capability can be added to a multicast scheme based on random linear block network coding [5], [6], with modest additional computational and communication overhead, by incorporating a simple polynomial hash/check value in each packet. With this approach, a sink node can detect Byzantine modifications with high probability, as long as these modifications have not been designed with knowledge of the random coding combinations present in all other packets obtained at the sink: the only essential condition is the adversary's incomplete knowledge of the random network code seen by the sink. No other assumptions are made regarding the topology of the network or the adversary's power to corrupt or inject packets. The adversary can know the entire message as well as portions of the random network code, and can have the same (or greater) transmission capacity compared to the source. This approach works even in the extreme case where every packet received by a sink has been corrupted by being coded together with an independent adversarial packet. This new adversarial model may be useful for application scenarios in which conventional assumptions of an upper bound on adversarial transmission capacity are less appropriate. For instance, in some peer-to-peer or wireless *ad hoc* settings we may not know how many adversarial nodes might join the network, while it may be more likely that there will be some transmissions that are not received by the adversarial nodes. In such cases, our approach can provide a useful alternative to existing methods.

Our approach provides much flexibility in trading off between the detection probability, the proportion of redundancy, the coding field size, and the amount of information about the random code that is not observed by the adversary. This approach can be used for low overhead monitoring during normal conditions when no adversary is known to be present, in conjunction with more complex, higher overhead techniques which are activated upon detection of a Byzantine error, such as adding more redundancy for error correction.

A preliminary version of this work with less general assumptions appeared in [7]. The security model is substantially generalized and strengthened in this work.

A. Background and Related Work

The problem of secure network communications in the presence of Byzantine adversaries has been studied extensively, e.g., [8]–[11]. A survey of information-theoretic research in this area is given in [12]. Two important issues are secrecy and authenticity;[1] this work concerns the latter. Like one-time pads [13], our approach relies on the generation of random values unknown to the adversary, though the one-time pad provides secrecy and not authenticity.

In the network coding context, the problem of ensuring secrecy in the presence of a wiretap adversary has been considered in [14]–[16]. The problem of correcting adversarial errors, which is complementary to our work, has been studied in [17]–[21].

Adversarial models in existing works on information-theoretic authenticity techniques commonly assume some upper bound on the number of adversarial transmissions, which leads to a requirement on the amount of redundant network capacity. For the problem of adversarial error correction or resilient communication, the number of links/transmissions controlled by the adversary must necessarily be limited with respect to the number of links/transmissions in a minimum source–sink cut or the amount of redundancy transmitted by the source. For instance, in the resilient communication problem of Dolev *et al.* [9], the source and sink are connected by n wires, and their model requires that no more than $(n-1)/2$ wires are disrupted by an adversary for resilient communication to be possible. In the network coding error correction problems of [17], [20], [21], the rate of redundant information that the source needs to transmit is between one and two times the maximum rate of information that can be injected by the adversary, depending on the specific adversarial model.

The above techniques can also be considered in the context of error detection. For example, in one phase of the secret sharing based algorithm in [9], the source communicates a degree τ polynomial $f(x) \in \mathbb{F}_q(x)$ by sending $f(i)$ on the ith wire. If the adversary controls at most $n-\tau$ wires, any errors it introduces can be detected. In general, for approaches based on error-correcting codes such as in [17], the number

[1]These are independent attributes of a cryptographic system [13].

Manuscript received November 24, 2006; revised February 16, 2008. This work was supported in part by AFOSR under Grant 5710001972, the Caltech Lee Center for Networking, and a gift from Microsoft Research. The material in this correspondence was presented in part at the IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004.

T. Ho and M. Effros are with the California Institute of Technology, Pasadena, CA 91125 USA (e-mail: tho@caltech.edu; effros@caltech.edu).

B. Leong is with the National University of Singapore, Singapore, 119260 Republic of Singapore (e-mail: benleong@comp.nus.edu.sg).

R. Koetter is with the Institute for Communications Engineering, Technische Universität München, D-80290 München, Germany (e-mail: ralf.koetter@tum.de).

M. Médard is with the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA (e-mail: medard@mit.edu).

D. R. Karger is with the Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139 USA (e-mail: karger@csail.mit.edu).

Communicated by U. Maurer, Guest Editor for Special Issue on Infromation Theoretic Security.

Digital Object Identifier 10.1109/TIT.2008.921894

of adversarial errors that can be detected is given by the difference between the source–sink minimum cut and the source information rate.

Such approaches have a threshold nature in that they do not offer graceful performance degradation when the number of adversarial transmissions exceeds the assumed upper bound. Their efficiency is also sensitive to overestimates of adversarial transmission capacity, which determines the amount of redundancy required.

The adversarial model considered in this work is slightly different. Instead of assuming a limit on the number of adversarial errors, our only assumption is on the incompleteness of the adversary's knowledge of the random code (the adversary can know the entire source message). In this case, the overhead (proportion of redundant information transmitted by the source) is no longer a function of the estimated upper bound on the number of adversarial errors. Instead, it is a design parameter which, as we will show, can be flexibly traded off against detection probability and coding field size. Unlike approaches based on secret sharing and its variants, where the required proportional overhead is a function of the adversarial strength, in our approach, for any nonzero proportional overhead and any adversarial strength short of full knowledge or control of network transmissions, the detection probability can be made arbitrarily high by increasing the field size. The former has the advantage of deterministic guarantees, while our approach has the advantage of greater flexibility with additional performance parameters that can be traded off against one another.

The use of our error detection technique for low-overhead monitoring under normal conditions when no adversary is known to be present, in conjunction with a more complex technique activated upon detection of an adversary, has a parallel in works such as [22] and [23]. These works optimize for normal conditions by using less complex message authentication codes and signed digests, respectively, during normal operation, resorting to more complex recovery mechanisms only upon detection of a fault.

B. Notation

In this work, we denote matrices with bold uppercase letters and vectors with bold lowercase letters. All vectors are row vectors unless indicated otherwise with a subscript T. We denote by $[\boldsymbol{x}, \boldsymbol{y}]$ the concatenation of two row vectors $\boldsymbol{x}$ and $\boldsymbol{y}$.

II. Model and Problem Formulation

Consider random linear block network coding [5], [6], [24] of a block of r exogenous packets which originate at a source node and are multicast to one or more sink nodes. We assume that the network coding subgraph is given by some separate mechanism, the details of which we are not concerned with.[2] An adversary observes some subset of packets transmitted in the network, and can corrupt, insert or delete one or more packets, or corrupt some subset of nodes. The only assumption we make is that the adversary's observations are limited such that when designing the adversarial packets, the adversary does not know the random coding combinations present in all other packets obtained at the sinks. This assumption is made precise using the notion of secret packets which we define below. The source and sinks do not share any keys or common information.

Each packet p in the network is represented by a row vector $\boldsymbol{w}_p$ of $d + c + r$ symbols from a finite field $\mathbb{F}_q$, where the first d entries are data symbols, the next c are redundant hash symbols, and the last r form the packet's (global) coefficient vector $\boldsymbol{t}_p$. The field size is 2 to the power of the symbol length in bits. The hash symbols in each exogenous packet are given by a function $\psi_d : \mathbb{F}_q^d \to \mathbb{F}_q^c$ of the data symbols. The coefficient vector of the ith exogenous packet is the unit vector with a single nonzero entry in the ith position. The coefficient vectors are used for decoding at the sinks as explained below.

Each packet transmitted by the source node is an independent random linear combination of the r exogenous packets, and each packet transmitted by a nonsource node is an independent random linear combination of packets received at that node. The coefficients of these linear combinations are chosen with the uniform distribution from the finite field $\mathbb{F}_q$, and the same linear operation is applied to each symbol in a packet. For instance, if packet p_3 is formed as a random linear combination of packets p_1 and p_2, then $\boldsymbol{w}_{p3} = \gamma_{1,3}\boldsymbol{w}_{p1} + \gamma_{2,3}\boldsymbol{w}_{p2}$ where $\gamma_{1,3}$ and $\gamma_{2,3}$ are random scalar coding coefficients distributed uniformly over $\mathbb{F}_q$.

Let row vector $\boldsymbol{m}_i \in \mathbb{F}_q^{(c+d)}$ represent the concatenation of the data and hash symbols for the ith exogenous packet, and let $\boldsymbol{M}$ be the matrix whose ith row is $\boldsymbol{m}_i$. A packet p is *genuine* if its data/hash symbols are consistent with its coefficient vector, i.e., $\boldsymbol{w}_p = [\boldsymbol{t}_p\boldsymbol{M}, \boldsymbol{t}_p]$. The exogenous packets are genuine, and any packet formed as a linear combination of genuine packets is also genuine. *Adversarial packets*, i.e., packets transmitted by the adversary, may contain arbitrary coefficient vector and data/hash values. An adversarial packet p can be represented in general by $[\boldsymbol{t}_p\boldsymbol{M} + \boldsymbol{v}_p, \boldsymbol{t}_p]$, where $\boldsymbol{v}_p$ is an arbitrary vector $\mathbb{F}_q^{c+d}$. If $\boldsymbol{v}_p$ is nonzero, p (and linear combinations of p with genuine packets) are nongenuine.

A set $\mathcal{S}$ of packets can be represented as a block matrix $[\boldsymbol{T}_\mathcal{S}\boldsymbol{M} + \boldsymbol{V}_\mathcal{S}|\boldsymbol{T}_\mathcal{S}]$ whose ith row is $\boldsymbol{w}_{p_i}$ where p_i is the ith packet of the set. A sink node t attempts to decode when it has collected a *decoding set* consisting of r linearly independent packets (i.e., packets whose coefficient vectors are linearly independent). For a decoding set $\mathcal{D}$, the decoding process is equivalent to premultiplying the matrix $[\boldsymbol{T}_\mathcal{D}\boldsymbol{M} + \boldsymbol{V}_\mathcal{D}|\boldsymbol{T}_\mathcal{D}]$ with $\boldsymbol{T}_\mathcal{D}^{-1}$. This gives $\left[\boldsymbol{M} + \boldsymbol{T}_\mathcal{D}^{-1}\boldsymbol{V}_\mathcal{D}|\boldsymbol{I}\right]$, i.e., the receiver decodes to $\boldsymbol{M} + \tilde{\boldsymbol{M}}$, where

$$\tilde{\boldsymbol{M}} = \boldsymbol{T}_\mathcal{D}^{-1}\boldsymbol{V}_\mathcal{D} \tag{1}$$

gives the disparity between the decoded packets and the original packets. If at least one packet in a decoding set is nongenuine, $\boldsymbol{V}_\mathcal{D} \neq \boldsymbol{0}$, and the decoded packets will differ from the original packets. A decoded packet is *inconsistent* if its data and hash values do not match, i.e., applying the function ψ_d to its data values does not yield its hash values. If one or more decoded packets are inconsistent, the sink declares an error.

The coefficient vector of a packet transmitted by the source is uniformly distributed over $\mathbb{F}_q^r$; if a packet whose coefficient vector has this uniform distribution is linearly combined with other packets, the resulting packet's coefficient vector has the same uniform distribution. We are concerned with the distribution of decoding outcomes conditioned on the adversary's information, i.e., the adversary's observed and transmitted packets, and its information on independencies/dependencies among packets. Note that in this setup, scaling a packet by some scalar element of $\mathbb{F}_q$ does not change the distribution of decoding outcomes.

For given $\boldsymbol{M}$, the value of a packet p is specified by the row vector $\boldsymbol{u}_p = [\boldsymbol{t}_p, \boldsymbol{v}_p]$. We call a packet p *secret* if, conditioned on the value of $\boldsymbol{v}_p$ and the adversary's information, its coefficient vector $\boldsymbol{t}_p$ is uniformly distributed over $\mathbb{F}_q^r \backslash W$ for some (possibly empty) subspace or affine space $W \subset \mathbb{F}_q^r$.[3] Intuitively, secret packets include genuine packets whose coefficient vectors are unknown (in the above sense)

[2]The network coding subgraph defines the times at which packets are or can be transmitted on each network link (see, e.g., [25]).

[3]This definition of a secret packet is conservative as it does not distinguish between packets with a nonuniform conditional distribution and packets that are fully known to the adversary. Taking this distinction into account would make the analysis more complicated but would in some cases give a better bound on detection probability.

to the adversary, as well as packets formed as linear combinations involving at least one secret packet. A set $\mathcal{S}$ of secret packets is *secrecy-independent* if each of the packets remains secret when the adversary is allowed to observe the other packets in the set; otherwise it is *secrecy-dependent*. Secrecy-dependencies arise from the network transmission topology, for instance, if a packet p is formed as a linear combination of a set $\mathcal{S}$ of secret packets (possibly with other nonsecret packets), then $\mathcal{S} \cup \{p\}$ is secrecy-dependent.

To illustrate these definitions, suppose that the adversary knows that a sink's decoding set contains an adversarial packet p_1 as well as a packet p_4 formed as some linear combination $k_2\boldsymbol{w}_{p_2} + k_3\boldsymbol{w}_{p_3}$ of an adversarial packet p_2 with a genuine packet p_3, so the adversary knows $\boldsymbol{t}_{p_1}, \boldsymbol{t}_{p_2}, \boldsymbol{v}_{p_1}, \boldsymbol{v}_{p_2}$ and $\boldsymbol{v}_{p_3} = \boldsymbol{0}$. Since a decoding set consists of packets with linearly independent coefficient vectors, the adversary knows that $\boldsymbol{t}_{p_1}$ and $\boldsymbol{t}_{p_3}$ are linearly independent. Suppose also that the adversary does not observe the contents of any packets dependent on p_3. Thus, the distribution of $\boldsymbol{t}_{p_4}$, conditioned on the adversary's information and any potential value $k_2\boldsymbol{v}_{p_2}$ for $\boldsymbol{v}_{p_4}$, is uniform over $\mathbb{F}_q^r \backslash \{k\boldsymbol{t}_{p_1} : k \in \mathbb{F}_q\}$. Also, packets p_3 and p_4 are secrecy-dependent.

Consider a decoding set $\mathcal{D}$ containing one or more secret packets. Choosing an appropriate packet ordering, we can express $[\boldsymbol{T}_{\mathcal{D}}|\boldsymbol{V}_{\mathcal{D}}]$ in the form

$$[\boldsymbol{T}_{\mathcal{D}}|\boldsymbol{V}_{\mathcal{D}}] = \left[\begin{array}{c|c} \boldsymbol{A}+\boldsymbol{B}_1 & \boldsymbol{V}_1 \\ \hline \boldsymbol{C}\boldsymbol{A}+\boldsymbol{B}_2 & \boldsymbol{V}_2 \\ \hline \boldsymbol{B}_3 & \boldsymbol{V}_3 \end{array}\right] \tag{2}$$

where for any given values of $\boldsymbol{B}_i \in \mathbb{F}_q^{s_i \times r}$, $\boldsymbol{V}_i \in \mathbb{F}_q^{s_i \times (d+c)}$, $i = 1, 2, 3$, and $\boldsymbol{C} \in \mathbb{F}_q^{s_2 \times s_1}$, the matrix $\boldsymbol{A} \in \mathbb{F}_q^{s_1 \times r}$ has a conditional distribution that is uniform over all values for which $\boldsymbol{T}_{\mathcal{D}}$ is nonsingular. The first $s_1 + s_2$ rows correspond to secret packets, and the first s_1 rows correspond to a set of secrecy-independent packets. $s_2 = 0$ if there are no secrecy-dependencies among the secret packets in $\mathcal{D}$.

This notion of secret packets provides the most general characterization of the conditions under which the scheme succeeds. For a given network topology, a requirement on the number of secrecy-independent secret packets received at the sink can be translated into constraints on the subsets of links/packets the adversary can observe and/or modify. For instance, if information is sent on n parallel paths from a source to a sink node, then the number of secrecy-independent secret packets is the number of linearly independent packets received on paths that are not observed or controlled by the adversary.

Note that we allow each packet of the decoding set to be corrupted with an independent adversarial packet, as long as at least one of the packets has been formed as a linear combination with some secret packet.

III. Main Results

In the following theorem, we consider decoding from a set of packets that contains some nongenuine packet, which causes the decoded packets to differ from the original exogenous packets. The first part of the theorem gives a lower bound on the number of equally likely potential values of the decoded packets—the adversary cannot narrow down the set of possible outcomes beyond this regardless of how it designs its adversarial packets. The second part provides, for a simple polynomial hash function, an upper bound on the proportion of potential decoding outcomes that can have consistent data and hash values, in terms of $k = \left\lceil \frac{d}{c} \right\rceil$, the ceiling of the ratio of the number of data symbols to hash symbols. Larger values for k correspond to lower overheads but lower probability of detecting an adversarial modification. This tradeoff is a design parameter for the network.

Theorem 1: Consider a decoding set $\mathcal{D}$ containing a secrecy-independent subset of s_1 secret (possibly nongenuine) packets, and suppose the decoding set contains at least one nongenuine packet.

a) The adversary cannot determine which of a set of at least $(q-1)^{s_1}$ equally likely values of the decoded packets will be obtained at the sink. In particular, there will be at least s_1 packets such that, for each of these, the adversary cannot determine which of a set of at least $q-1$ equally likely values will be obtained.

b) Let $\psi : \mathbb{F}_q^k \to \mathbb{F}_q$ be the function mapping $(x_1, \ldots, x_k)$, $x_i \in \mathbb{F}_q$, to

$$\psi(x_1, \ldots, x_k) = x_1^2 + \cdots + x_k^{k+1} \tag{3}$$

where $k = \left\lceil \frac{d}{c} \right\rceil$. Suppose the function ψ_d mapping the data symbols $x_1, \ldots, x_d$ to the hash symbols $y_1, \ldots, y_c$ in an exogenous packet is defined by

$$y_i = \psi(x_{(i-1)k+1}, \ldots, x_{ik}), \quad \forall\, i = 1, \ldots, c-1$$
$$y_c = \psi(x_{(c-1)k+1}, \ldots, x_d).$$

Then the probability of not detecting an error is at most $\left(\frac{k+1}{q}\right)^{s_1}$.

Corollary 1: Let the hash function ψ_d be defined as in Theorem 1b. Suppose a sink obtains more than r packets, including a secrecy-independent set of s secret packets, and at least one nongenuine packet. If the sink decodes using two or more decoding sets whose union includes all its received packets, then the probability of not detecting an error is at most $\left(\frac{k+1}{q}\right)^{s}$.

Example: With 2% overhead ($k = 50$), symbol length $= 7$ bits, $s = 5$, the detection probability is at least 98.9%; with 1% overhead ($k = 100$), symbol length $= 8$ bits, $s = 5$, the detection probability is at least 99.0%.

IV. Development, Proofs, and Ancillary Results

A. Vulnerable Scenarios

Before analyzing the scenario described in the previous sections, we first point out when this approach fails to detect adversarial modifications.

First, the sink needs some way of knowing if the source stops transmitting, otherwise, the assumption of no shared secret information results in the adversary being indistinguishable from the source. One possibility is that the source either transmits at a known rate or is inactive, and that the sink knows at what rates it should be receiving information on various subsets of incoming links when the source is active. If the adversary is unable to reproduce those information rates, e.g., because it does not control the same part of the network as the source, then the sink knows when the source is inactive.

Second, if the adversary knows that the genuine packets received at a sink have coefficient vectors that lie in some w-dimensional subspace $W \subset \mathbb{F}_q^r$, the following strategy allows it to control the decoding outcome and so ensure that the decoded packets have consistent data and hash values.

The adversary ensures that the sink receives w genuine packets with linearly independent coefficient vectors in W, by supplying additional such packets if necessary. The adversary also supplies the sink with $r - w$ nongenuine packets whose coefficient vectors $\boldsymbol{t}_1, \ldots, \boldsymbol{t}_{r-w}$ are not in W. Let $\boldsymbol{t}_{r-w+1}, \ldots, \boldsymbol{t}_r$ be a set of basis vectors for W, and let $\boldsymbol{T}$ be the matrix whose ith row is $\boldsymbol{t}_i$. Then the coefficient vectors of the r packets can be represented by the rows of the matrix

$$\left[\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{K} \end{array}\right] \boldsymbol{T}$$

where $\boldsymbol{K}$ is a nonsingular matrix in $\mathbb{F}_q^{w \times w}$. From (5), we have

$$\left[\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{K} \end{array}\right] \boldsymbol{T}\tilde{\boldsymbol{M}} = \left[\begin{array}{c} \tilde{\boldsymbol{V}} \\ \hline \boldsymbol{0} \end{array}\right]$$

$$\tilde{\boldsymbol{M}} = \boldsymbol{T}^{-1}\left[\begin{array}{c|c} \boldsymbol{I} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{K}^{-1} \end{array}\right]\left[\begin{array}{c} \tilde{\boldsymbol{V}} \\ \hline \boldsymbol{0} \end{array}\right] = \boldsymbol{T}^{-1}\left[\begin{array}{c} \tilde{\boldsymbol{V}} \\ \hline \boldsymbol{0} \end{array}\right].$$

Since the adversary knows $\boldsymbol{T}$ and controls $\tilde{\boldsymbol{V}}$, it can determine $\tilde{\boldsymbol{M}}$.

B. Byzantine Modification Detection

We next consider the scenario described in Section II, where the adversary designs its packets without knowing the contents of one or more secret packets the receiver will use for decoding, and prove the results of Section III.

We first establish two results that are used in the proof of Theorem 1. Consider the hash function defined in (3). We call a vector $(x_1, \ldots, x_{k+1}) \in \mathbb{F}_q^{k+1}$ *consistent* if $x_{k+1} = \psi(x_1, \ldots, x_k)$.

Lemma 1: At most $k+1$ out of the q vectors in a set

$$\{\boldsymbol{u} + \gamma \boldsymbol{v} : \ \gamma \in \mathbb{F}_q\}$$

where $\boldsymbol{u} = (u_1, \ldots, u_{k+1})$ is a fixed vector in $\mathbb{F}_q^{k+1}$ and $\boldsymbol{v} = (v_1, \ldots, v_{k+1})$ is a fixed nonzero vector in $\mathbb{F}_q^{k+1}$, can be consistent.

Proof: Suppose some vector $\boldsymbol{u} + \gamma \boldsymbol{v}$ is consistent, i.e.,

$$u_{k+1} + \gamma v_{k+1} = (u_1 + \gamma v_1)^2 + \cdots + (u_k + \gamma v_k)^{k+1}. \quad (4)$$

Note that for any fixed value of $\boldsymbol{u}$ and any fixed nonzero value of $\boldsymbol{v}$, (4) is a polynomial equation in γ of degree equal to $1 + \tilde{k}$, where $\tilde{k} \in [1, k]$ is the highest index for which the corresponding $v_{k'}$ is nonzero, i.e., $v_{\tilde{k}} \neq 0, v_{k'} = 0 \ \forall \ k' > \tilde{k}$. By the fundamental theorem of algebra, this equation can have at most $1 + \tilde{k} \leq 1 + k$ roots. Thus, the property can be satisfied for at most $1 + k$ values of γ. □

Corollary 2: Let $\boldsymbol{u}$ be a fixed row vector in $\mathbb{F}_q^n$ and $\boldsymbol{Y}$ a fixed nonzero matrix in $\mathbb{F}_q^{n \times (k+1)}$. If row vector $\boldsymbol{g}$ is distributed uniformly over $\mathbb{F}_q^n$, then the vector $\boldsymbol{u} + \boldsymbol{g}\boldsymbol{Y}$ is consistent with probability at most $\frac{k+1}{q}$.

Proof: Suppose the ith row of $\boldsymbol{Y}$, denoted $\boldsymbol{y}_i$, is nonzero. We can partition the set of possible values for $\boldsymbol{g}$ such that each partition consists of all vectors that differ only in the ith entry g_i. For each partition, the corresponding set of values of $\boldsymbol{u} + \boldsymbol{g}\boldsymbol{Y}$ is of the form $\{\boldsymbol{u}' + g_i \boldsymbol{y}_i : \ g_i \in \mathbb{F}_q\}$. The result follows from Lemma 1 and the fact that g_i is uniformly distributed over $\mathbb{F}_q$. □

Proof of Theorem 1: We condition on any given values of $\boldsymbol{B}_i, \boldsymbol{V}_i, i = 1, 2, 3$, and $\boldsymbol{C}$ in (2). Writing $\boldsymbol{A}' = \boldsymbol{A} + \boldsymbol{B}_1, \boldsymbol{T}_{\mathcal{D}}$ becomes

$$\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{C}(\boldsymbol{A}' - \boldsymbol{B}_1) + \boldsymbol{B}_2 \\ \boldsymbol{B}_3 \end{bmatrix}.$$

From (1), we have

$$\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{C}(\boldsymbol{A}' - \boldsymbol{B}_1) + \boldsymbol{B}_2 \\ \boldsymbol{B}_3 \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 \\ \boldsymbol{V}_2 \\ \boldsymbol{V}_3 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{A}' \\ -\boldsymbol{C}\boldsymbol{B}_1 + \boldsymbol{B}_2 \\ \boldsymbol{B}_3 \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 \\ \boldsymbol{V}_2 - \boldsymbol{C}\boldsymbol{V}_1 \\ \boldsymbol{V}_3 \end{bmatrix}$$

which we can simplify to

$$\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{B}' \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 \\ \boldsymbol{V}_2' \end{bmatrix} \quad (5)$$

by writing

$$\boldsymbol{B}' = \begin{bmatrix} -\boldsymbol{C}\boldsymbol{B}_1 + \boldsymbol{B}_2 \\ \boldsymbol{B}_3 \end{bmatrix}, \quad \boldsymbol{V}_2' = \begin{bmatrix} \boldsymbol{V}_2 - \boldsymbol{C}\boldsymbol{V}_1 \\ \boldsymbol{V}_3 \end{bmatrix}.$$

Since the determinant of a matrix is not changed by adding a multiple of one row to another row, and $\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{B}' \end{bmatrix}$ is obtained from $\boldsymbol{T}_{\mathcal{D}}$ by a sequence of such operations, we have

$$\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{B}' \end{bmatrix} \text{ is nonsingular } \Leftrightarrow \boldsymbol{T}_{\mathcal{D}} \text{ is nonsingular.}$$

Thus, matrix $\boldsymbol{A}' \in \mathbb{F}_q^{s_1 \times r}$ has a conditional distribution that is uniform over the set $\mathcal{A}$ of values for which $\begin{bmatrix} \boldsymbol{A}' \\ \boldsymbol{B}' \end{bmatrix}$ is nonsingular.

The condition that the decoding set contains at least one nongenuine packet corresponds to the condition $\boldsymbol{V}_{\mathcal{D}} \neq \boldsymbol{0}$. We consider two cases. In each case, we show that we can partition the set $\mathcal{A}$ such that at most a fraction $\left(\frac{k+1}{q}\right)^{s_1}$ of values in each partition give decoding outcomes $\boldsymbol{M} + \tilde{\boldsymbol{M}}$ with consistent data and hash values. The result then follows since the conditional distribution of values within each partition is uniform.

Case 1: $\boldsymbol{V}_2' \neq \boldsymbol{0}$. Let $\boldsymbol{v}_i$ be some nonzero row of $\boldsymbol{V}_2'$, and $\boldsymbol{b}_i$ the corresponding row of $\boldsymbol{B}'$. Then $\boldsymbol{b}_i \tilde{\boldsymbol{M}} = \boldsymbol{v}_i$.

We first partition $\mathcal{A}$ into cosets

$$\mathcal{A}_n = \{\boldsymbol{A}_n + \boldsymbol{r}^T \boldsymbol{b}_i : \ \boldsymbol{r} \in \mathbb{F}_q^{s_1}\}, \quad n = 1, 2, \ldots, \chi$$

where

$$\chi = \frac{|\mathcal{A}|}{q^{s_1}}.$$

This can be done by the following procedure. Any element of $\mathcal{A}$ can be chosen as $\boldsymbol{A}_1$. Matrices $\boldsymbol{A}_2, \boldsymbol{A}_3, \ldots, \boldsymbol{A}_\chi$ are chosen sequentially; for each $m = 2, \ldots, \chi$, $\boldsymbol{A}_m$ is chosen to be any element of $\mathcal{A}$ not in the cosets $\mathcal{A}_n, n < m$. Note that this forms a partition of $\mathcal{A}$, since the presence of some element c in two sets $\mathcal{A}_n$ and $\mathcal{A}_m$, $n < m$, implies that $\boldsymbol{A}_m$ is also in $\mathcal{A}_n$, which is a contradiction. It is also clear that each coset has size $\left|\{\boldsymbol{r} : \ \boldsymbol{r} \in \mathbb{F}_q^{s_1}\}\right| = q^{s_1}$.

For each such coset $\mathcal{A}_n$, the corresponding values of $\tilde{\boldsymbol{M}}$ satisfy, from (5)

$$\begin{bmatrix} \boldsymbol{A}_n + \boldsymbol{r}^T \boldsymbol{b}_i \\ \boldsymbol{B}' \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 \\ \boldsymbol{V}_2' \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 - \boldsymbol{r}^T \boldsymbol{v}_i \\ \boldsymbol{V}_2' \end{bmatrix}$$

$$\tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix}^{-1} \begin{bmatrix} \boldsymbol{V}_1 - \boldsymbol{r}^T \boldsymbol{v}_i \\ \boldsymbol{V}_2' \end{bmatrix}$$

where $\boldsymbol{r} \in \mathbb{F}_q^{s_1}$. Let $\boldsymbol{U}$ be the submatrix consisting of the first s_1 columns of $\begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix}^{-1}$. Since $\boldsymbol{U}$ is full rank, we can find a set $\mathcal{J} \subset \{1, \ldots, r\}$ of s_1 indices that correspond to linearly independent rows of $\boldsymbol{U}$. Let $[\boldsymbol{U}_1 \mid \boldsymbol{U}_2]$ be the $s_1 \times r$ submatrix of $\begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix}^{-1}$ consisting of rows with indices in $\mathcal{J}$. Consider the corresponding rows of $\boldsymbol{M} + \tilde{\boldsymbol{M}}$, which can be expressed in the form

$$\boldsymbol{M}_{\mathcal{J}} + \boldsymbol{U}_1 \boldsymbol{V}_1 - \boldsymbol{U}_1 \boldsymbol{r}^T \boldsymbol{v}_i + \boldsymbol{U}_2 \boldsymbol{V}_2' \quad (6)$$

where $\boldsymbol{M}_{\mathcal{J}}$ is the submatrix of $\boldsymbol{M}$ consisting of rows corresponding to set $\mathcal{J}$. Since $\boldsymbol{U}_1$ is nonsingular by the choice of $\mathcal{J}$, $\boldsymbol{U}_1 \boldsymbol{r}^T$ takes potentially any value in $\mathbb{F}_q^{s_1}$. Thus, the set of potential values for each row of (6), for any given value of $\boldsymbol{M}_{\mathcal{J}}, \boldsymbol{A}_n, \boldsymbol{B}', \boldsymbol{V}_1, \boldsymbol{V}_2', \boldsymbol{v}_i$, and the other rows, is of the form $\{\boldsymbol{u} + \gamma \boldsymbol{v}_i : \ \gamma \in \mathbb{F}_q\}$ where $\boldsymbol{u}$ is a function of $\boldsymbol{M}_{\mathcal{J}}, \boldsymbol{A}_n, \boldsymbol{B}', \boldsymbol{V}_1, \boldsymbol{V}_2'$. Applying Lemma 1 yields the result for this case.

Case 2: $\boldsymbol{V}_2' = \boldsymbol{0}$, i.e., $\boldsymbol{V}_2 - \boldsymbol{C}\boldsymbol{V}_1 = \boldsymbol{V}_3 = \boldsymbol{0}$. Then $\boldsymbol{V}_1 \neq \boldsymbol{0}$, since otherwise $\boldsymbol{V}_1 = \boldsymbol{V}_2 = \boldsymbol{0}$ and $\boldsymbol{V}_{\mathcal{D}} = \boldsymbol{0}$ which would contradict the assumption that there is at least one nongenuine packet.

We partition $\mathcal{A}$ such that each partition consists of all matrices in $\mathcal{A}$ that have the same row space

$$\mathcal{A}_n = \left\{\boldsymbol{R}\boldsymbol{A}_n : \boldsymbol{R} \in \mathbb{F}_q^{s_1 \times s_1},\ \det(\boldsymbol{R}) \neq 0\right\}, \quad n = 1, 2, \ldots, \chi$$

where

$$|\mathcal{A}_n| = \prod_{i=0}^{s_1-1} \left(q^{s_1} - q^i\right), \quad \chi = \frac{|\mathcal{A}|}{|\mathcal{A}_n|}.$$

This can be done by choosing any element of $\mathcal{A}$ as $\boldsymbol{A}_1$, and choosing $\boldsymbol{A}_n, n = 2, \ldots, \chi$ sequentially such that $\boldsymbol{A}_n$ is any element of $\mathcal{A}$ not in $\mathcal{A}_m, m < n$.

For each $\mathcal{A}_n, n = 1, \ldots, \chi$, the corresponding values of $\tilde{\boldsymbol{M}}$ satisfy, from (5)

$$\begin{bmatrix} \boldsymbol{R}\boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{V}_1 \\ \boldsymbol{0} \end{bmatrix}$$
$$\begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix} \tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{R}^{-1}\boldsymbol{V}_1 \\ \boldsymbol{0} \end{bmatrix}$$
$$\tilde{\boldsymbol{M}} = \begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix}^{-1} \begin{bmatrix} \boldsymbol{R}^{-1}\boldsymbol{V}_1 \\ \boldsymbol{0} \end{bmatrix}.$$

Let $\boldsymbol{U}$ be the submatrix consisting of the first s_1 columns of $\begin{bmatrix} \boldsymbol{A}_n \\ \boldsymbol{B}' \end{bmatrix}^{-1}$. We can find an ordered set $\mathcal{J} = \{i_1, \ldots, i_{s_1} : i_1 < \cdots < i_{s_1}\} \subset \{1, \ldots, r\}$ of s_1 indices that correspond to linearly independent rows of $\boldsymbol{U}$. Let $\boldsymbol{U}_{\mathcal{J}}$ and $\boldsymbol{M}_{\mathcal{J}}$ be the submatrices of $\boldsymbol{U}$ and $\boldsymbol{M}$, respectively, consisting of the s_1 rows corresponding to $\mathcal{J}$. Then $\boldsymbol{U}_{\mathcal{J}}$ is nonsingular, and the value of the matrix representation of the corresponding decoded packets is uniformly distributed over the set

$$\left\{\boldsymbol{M}_{\mathcal{J}} + \boldsymbol{R}'\boldsymbol{V}_1 : \boldsymbol{R}' \in \mathbb{F}_q^{s_1 \times s_1},\ \det(\boldsymbol{R}') \neq 0\right\}. \tag{7}$$

Let ν be the rank of $\boldsymbol{V}_1$. Consider a set of ν linearly independent rows of $\boldsymbol{V}_1$. Denote by $\mathcal{I}$ the corresponding set of row indices, and denote by $\boldsymbol{V}_{\mathcal{I}}$ the submatrix of $\boldsymbol{V}_1$ consisting of those rows. We can write

$$\boldsymbol{V}_1 = \boldsymbol{L}\boldsymbol{V}_{\mathcal{I}}$$

where $\boldsymbol{L} \in \mathbb{F}_q^{s_1 \times \nu}$ has full rank ν. We define $\boldsymbol{R}_{\mathcal{I}} = \boldsymbol{R}'\boldsymbol{L}$, noting that

$$\boldsymbol{R}_{\mathcal{I}}\boldsymbol{V}_{\mathcal{I}} = \boldsymbol{R}'\boldsymbol{L}\boldsymbol{V}_{\mathcal{I}} = \boldsymbol{R}'\boldsymbol{V}_1$$

and that $\boldsymbol{R}_{\mathcal{I}}$ is uniformly distributed over all matrices in $\mathbb{F}_q^{s_1 \times \nu}$ that have full rank ν. Thus, (7) becomes

$$\left\{\boldsymbol{M}_{\mathcal{J}} + \boldsymbol{R}_{\mathcal{I}}\boldsymbol{V}_{\mathcal{I}} : \boldsymbol{R}_{\mathcal{I}} \in \mathbb{F}_q^{s_1 \times \nu},\ \operatorname{rank}(\boldsymbol{R}_{\mathcal{I}}) = \nu\right\}. \tag{8}$$

Denote by $\boldsymbol{r}_1, \ldots, \boldsymbol{r}_{s_1}$ the rows of $\boldsymbol{R}_{\mathcal{I}}$, and by $\boldsymbol{R}_n$ the submatrix of $\boldsymbol{R}_{\mathcal{I}}$ consisting of its first n rows. We consider the rows sequentially, starting with the first row $\boldsymbol{r}_1$. For $n = 1, \ldots, s_1$, we will show that conditioned on any given value of $\boldsymbol{R}_{n-1}$, the probability that the i_nth decoded packet $\boldsymbol{M}_{i_n} + \boldsymbol{r}_n\boldsymbol{V}_{\mathcal{I}}$ is consistent is at most $\frac{k+1}{q}$.

Case A: $\boldsymbol{R}_{n-1}$ has zero rank. This is the case if $n = 1$, or if $n > 1$ and $\boldsymbol{R}_{n-1} = \boldsymbol{0}$.

Suppose we remove the restriction $\operatorname{rank}(\boldsymbol{R}_{\mathcal{I}}) = \nu$, so that $\boldsymbol{r}_n$ is uniformly distributed over $\mathbb{F}_q^{\nu}$. By Corollary 2, $\boldsymbol{m}_{i_n} + \boldsymbol{r}_n\boldsymbol{V}_{\mathcal{I}}$ would have consistent data and hash values with probability at most $\frac{k+1}{q}$. With the restriction $\operatorname{rank}(\boldsymbol{R}_{\mathcal{I}}) = \nu$, the probability of $\boldsymbol{r}_n$ being equal to $\boldsymbol{0}$ is lowered. Since the corresponding decoded packet $\boldsymbol{m}_{i_n} + \boldsymbol{r}_n\boldsymbol{V}_{\mathcal{I}}$ is consistent for $\boldsymbol{r}_n = \boldsymbol{0}$, the probability that it is consistent is less than $\left(\frac{k+1}{q}\right)$.

Case B: $n > 1$ and $\boldsymbol{R}_{n-1}$ has nonzero rank.

Conditioned on $\boldsymbol{r}_n$ being in the row space of $\boldsymbol{R}_{n-1}$, $\boldsymbol{r}_n = \boldsymbol{g}\boldsymbol{R}_{n-1}$ where $\boldsymbol{g}$ is uniformly distributed over $\mathbb{F}_q^{n-1}$. Since $\boldsymbol{V}_{\mathcal{I}}$ has linearly independent rows, $\boldsymbol{R}_{n-1}\boldsymbol{V}_{\mathcal{I}} \neq \boldsymbol{0}$, and by Corollary 2, the corresponding decoded packet

$$\boldsymbol{m}_{i_n} + \boldsymbol{r}_n\boldsymbol{V}_{\mathcal{I}} = \boldsymbol{m}_{i_n} + \boldsymbol{g}\boldsymbol{R}_{n-1}\boldsymbol{V}_{\mathcal{I}}$$

is consistent with probability at most $\frac{k+1}{q}$.

Conditioned on $\boldsymbol{r}_n$ not being in the row space of $\boldsymbol{R}_{n-1}$, we can partition the set of possible values for $\boldsymbol{r}_n$ into cosets

$$\left\{\boldsymbol{r} + \boldsymbol{g}\boldsymbol{R}_{n-1} : \boldsymbol{g} \in \mathbb{F}_q^{n-1}\right\}$$

where $\boldsymbol{r}$ is not in the row space of $\boldsymbol{R}_{n-1}$; the corresponding values of the i_nth decoded packet are given by

$$\left\{\boldsymbol{m}_{i_n} + \boldsymbol{r}\boldsymbol{V}_{\mathcal{I}} + \boldsymbol{g}\boldsymbol{R}_{n-1}\boldsymbol{V}_{\mathcal{I}} : \boldsymbol{g} \in \mathbb{F}_q^{n-1}\right\}.$$

Noting as before that $\boldsymbol{R}_{n-1}\boldsymbol{V}_{\mathcal{I}} \neq \boldsymbol{0}$ and applying Corollary 2, the i_nth decoded packet is consistent with probability at most $\frac{k+1}{q}$. □

Proof of Corollary 1: Suppose two or more different sets of packets are used for decoding. If not all of them contain at least one nongenuine packet, the decoded values obtained from different decoding sets will differ: sets containing only genuine packets will be decoded to $\boldsymbol{M}$, while sets containing one or more nongenuine packets will not. This will indicate an error.

Otherwise, suppose all the decoding sets contain at least one nongenuine packet. Let $\mathcal{S}$ denote the set of s secrecy-independent packets. Consider the decoding sets in turn, denoting by s_i' the number of unmodified packets from $\mathcal{S}$ in the ith decoding set that are not in any set $j < i$. Conditioned on any fixed values of packets in sets $j < i$, there remain s_i' secrecy-independent packets in the ith decoding set, and we have from Theorem 1 that at most a fraction $\left(\frac{k+1}{q}\right)^{s_i'}$ of decoding outcomes for set i have consistent data and hash values. Thus, the overall fraction of consistent decoding outcomes is at most

$$\left(\frac{k+1}{q}\right)^{\sum_i s_i'} = \left(\frac{k+1}{q}\right)^{s}.$$ □

V. Conclusion

We have described an information-theoretic approach for detecting Byzantine modifications in networks employing random linear network coding. Byzantine modification detection capability is added by augmenting each packet with a small, flexible number of hash symbols; this overhead can be traded off against the detection probability and symbol length. The hash symbols can be obtained as a simple polynomial function of the data symbols. The only necessary condition is that the adversarial packets are not all designed with knowledge of the random coding coefficients of all other packets received by the sink nodes. This approach can be used in conjunction with higher overhead schemes that are activated only upon detection of a Byzantine node.

Acknowledgment

The authors would like to thank the Associate Editor and reviewers for their valuable comments and suggestions.

References

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

[2] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[3] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 789–804, Mar. 2006.
[4] D. S. Lun, M. Médard, and M. Effros, "On coding for reliable communication over packet networks," in *Proc. 42nd Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep./Oct. 2004.
[5] T. Ho, R. Koetter, M. Médard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, Jun./Jul. 2003, p. 442.
[6] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. 41st Annu. Allerton Conf. Communication, Control, and Computing*, 2003.
[7] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D. R. Karger, "Byzantine modification detection for multicast networks using randomized network coding," in *Proc. 2004 IEEE Int. Symp. Information Theory* , Chicago, IL, Jun./Jul. 2004, p. 144.
[8] R. Perlman, "Network Layer Protocols with Byzantine Robustness," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 1988.
[9] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *J. ACM*, vol. 40, no. 1, pp. 17–47, Jan. 1993.
[10] D. Malkhi and M. Reiter, "A high-throughput secure reliable multicast protocol," *J. Comp. Security*, vol. 5, pp. 113–127, 1997.
[11] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Communication Netwirks and Distributed Systems Modeling and Simulation Conf. (CNDS 2002)*, San Antonio, TX, Jan. 2002.
[12] Y. Desmedt, "Unconditionally private and reliable communication in an untrusted network," in *Proc. IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Awaji Island, Japan, Oct. 2005, pp. 38–41.
[13] J. L. Massey, "Contemporary cryptography: An introduction," in *Contemporary Cryptology: The Science of Information Integrity*, G. J. Simmons, Ed. New York: Wiley/IEEE, 1999.
[14] N. Cai and R. W. Yeung, "Secure network coding," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, Jun./Jul. 2002, p. 323.
[15] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the capacity of secure network coding," in *Proc. 42nd Annu. Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Sep./Oct. 2004.
[16] K. Bhattad and K. R. Nayayanan, "Weakly secure network coding," in *Proc. WINMEE, RAWNET, and NETCOD 2005 Workshops*, Riva del Garda, Italy, Apr. 2005.
[17] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 19–36, 2006.
[18] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inf. Syst.*, vol. 6, no. 1, pp. 37–54, 2006.
[19] K. K. Chi and X. M. Wang, "Analysis of network error correction based on network coding," *IEE Proc.—Communications*, vol. 152, no. 4, 2005.
[20] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc. IEEE INFOCOM 2007*, Anchorage, AK, May 2007, pp. 616–624.
[21] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, submitted for publication.
[22] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OSDI: Proc. Symp. Operating Systems Design and Implementation*, New Orleans, LA, 1999, pp. 173–186.
[23] K. P. Kihlstrom, L. E. Moser, and P. M. Melliar-Smith, "The SecureRing protocols for securing group communication," in *Proc. 31st Annu. Hawaii Int. Conf. System Sciences (HICSS)*, 1998, vol. 3, pp. 317–326.
[24] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.
[25] D. S. Lun, N. Ratnakar, M. Médard, R. Koetter, D. R. Karger, T. Ho, E. Ahmed, and F. Zhao, "Minimum-cost multicast over coded packet networks," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2608–2623, Jun. 2006.

Computational Complexity of Continuous Variable Quantum Key Distribution

Yi-Bo Zhao, You-Zhen Gui, Jin-Jian Chen, Zheng-Fu Han, and Guang-Can Guo

***Abstract*—The continuous variable quantum key distribution has been considered to have the potential to provide high secret key rate. However, in present experimental demonstrations, the secret key can be distilled only under very small loss rates. Here, by calculating explicitly the computational complexity with the channel transmission, we show that under high loss rate it is hard to distill the secret key in present continuous variable scheme and one of its advantages, the potential of providing high secret key rate, may therefore be limited.**

***Index Terms*—Computational complexity, continuous variable (CV), error correction, quantum key distribution (QKD), reconciliation.**

I. Introduction

Due to its potential for achieving high modulation and detection speed, continuous variable (CV) quantum key distribution (QKD) has recently attracted more and more attention. Compared to single photon counting schemes, CVQKD does not require single photon sources and detectors which are technically challenging now. The CVQKD schemes typically use the quadrature amplitude of light beams as information carrier, and homodyne detection rather than photon counting. Some of these schemes use nonclassical states, such as squeezed states [1] or entangled states [2], while others use coherent states [3]–[6]. Because the squeezed states and entangled states are sensitive to losses in the quantum channel, coherent states are much more attractive for long distance transmission. To improve the performance of the CVQKD against the channel loss, Grosshans *et al.* proposed a reverse reconciliation (RR) protocol [11]. In the traditional direct reconciliation protocol, Alice sends Bob the quantum state and also sends the reconciliation information later.[1] Finally, Bob obtains Alice's data without any error. However, in the reverse reconciliation protocol, the quantum state is sent by Alice to Bob, but the reconciliation information is sent by Bob to Alice. Finally, Alice gets Bob's received data with no error.

Tabletop experimental setups that encode information in the phase and amplitude of coherent states have been demonstrated [7], [8], and recent experiments have shown the feasibility of CVQKD in optical fibers up to a distance of 55 km [9], [10], but without obtaining the final secret keys.

Unlike the single photon QKD schemes, many CVQKD schemes utilize the inertial quantum noise to protect information from Eve's attack [7], [12]. However, at the same time the quantum noise also causes errors between two legitimate communicators, Alice and Bob. It is widely

Manuscript received January 14, 2007; revised November 25, 2007. This work was supported in part by the National Fundamental Research Program of China under Grant 2006CB921900, National Natural Science Foundation of China under Grants 60537020 and 60621064, the Innovation Fund of the University of Science and Technology of China under Grants KD2006005, and the Knowledge Innovation Project of the Chinese Academy of Sciences (CAS).

The authors are with the Key Lab of Quantum Information, University of Science and Technology of China (CAS), Hefei, Anhui 230026, China (e-mail: zfhan@ustc.edu.cn).

Communicated by H. Imai, Guest Editor for Special Issue on Information Theoretic Security.

Digital Object Identifier 10.1109/TIT.2008.921889

[1]In the following, we use the conventional appellation. Alice is the quantum state sender and Bob is the quantum state receiver.