Secure Network Coding for Wiretap Networks of Type II

Salim El Rouayheb, Emina Soljanin, Alex Sprintson

Abstract

We consider the problem of securing a multicast network against a wiretapper that can intercept the packets on a limited number of arbitrary network edges of its choice. We assume that the network employs the network coding technique to simultaneously deliver the packets available at the source to all the receivers. We show that this problem can be looked at as a network generalization of the wiretap channel of type II introduced in a seminal paper by Ozarow and Wyner. In particular, we show that the transmitted information can be secured by using the Ozarow-Wyner approach of coset coding at the source on top of the existing network code. This way, we quickly and transparently recover some of the results available in the literature on secure network coding for wiretap networks. Moreover, we derive new bounds on the required alphabet size that are independent of the network size and devise an algorithm for the construction of secure network codes. We also look at the dual problem and analyze the amount of information that can be gained by the wiretapper as a function of the number of wiretapped edges.

I. Introduction

Consider a communication network represented as a directed graph $G = (V, E)$ with unit capacity edges and an information source S that multicasts information to t receivers $R_1, \ldots, R_t$ located at distinct nodes. Assume that the minimum size of a cut that separates the source and each receiver node is n. It is known that a multicast rate of n is achievable by using a linear

S. El Rouayheb and A. Sprintson are with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, 77845 USA emails: {rouayheb@tamu.edu, spalex@ece.tamu.edu}.

E. Soljanin is with the Mathematics of Networking and Communication Deptartment, Enabling Computing Technologies, Bell Laboratories, Alcatel-Lucent, Murray Hill, NJ 07974, email: emina@alcatel-lucent.com.

A preliminary version of this paper appeared in the Proceedings of the IEEE International Symposium on Information Theory (ISIT), Nice, France, 2007 [1].

network coding scheme [2], [3]. In this paper, we focus on secure multicast connections in the presence of a wiretapper that can access data on a limited number of edges of its choice. Our primary goal is to design a network coding scheme that delivers data at maximum rate to all the destinations and does not reveal any information about the transmitted message to the wiretapper.

The problem of making a linear network code information-theoretically secure in the presence of a wiretaper that can look at a bounded number, say μ, of network edges was first studied by Cai and Yeung in [4]. They considered directed graphs and constructed codes over an alphabet with at least $\binom{|E|}{\mu}$ elements which can support a secure multicast rate of up to $n-\mu$. In [5], they proved that these codes use the minimum amount of randomness required to achieve the security constraint. However, the algorithm due to [4] has high computational complexity and requires a very large field size (exponential in the number of wiretapped edges). Feldman *et al.* derived trade-offs between security, code alphabet size, and multicast rate of secure linear network coding schemes in [6], by using ideas from secret sharing and abstracting the network topology. Another approach was taken by Jain in [7] who obtained security by merely exploiting the topology of the underlying network. Weakly secure network codes that insure that no meaningful information is revealed to the adversary were studied by Bhattad and Narayanan in [8].

A related line of work considers a more powerful *Byzantine* adversary that can also modify the packets on the edges it controls. Such an adversary can be potentially more harmful in networks that employ the network coding technique because a modification in one packet can propagate throughout the network and affect other packets as well. Secure network coding in the presence of a Byzantine adversary has been studied by Ho *et al.* in [9] and Jaggi *et al.* in [10], [11], [12]. In [11], [12], the authors devise distributed polynomial-time algorithms that are rate-optimal and achieve information theoretical security against several scenarios of adversarial attacks.

The problem of error correction in networks was also studied by Cai and Yeung in [13], [14] where they generalized classical error-correction coding techniques to network settings. A different model for error correction was introduced by Koetter and Kschischang in [15] where communication is established by transmitting subspaces instead of vectors through the network. The use of rank-metric codes for error control under this model was investigated in [16]. The common approach in these works is to encode packets at the source, prior to sending them over the network, using an error correcting code so that the packets carry not only data but also some redundant information derived from the data which will help to reduce the probability of incorrect decoding.

We also consider the coding at the source technique to be a natural approach for addressing the information-theoretic security of wiretap networks. In a network where the min-cut value between the source and each receiver node is n and an adversary can access up to μ edges of his choice, we introduce a coding at source scheme that ensures information-theoretic security based on the Ozarow-Wyner wiretap channel of type II, introduced in [17] and [18], where the source transmits n symbols to the receiver and an adversary can access any μ of those symbols.

Ozarow and Wyner showed that the maximum number of symbols (say k) that the source can communicate to the receiver securely in the information-theoretic sense is equal to $n - \mu$. They also showed how to encode the k source symbols into the n channel symbols for secure transmission. Clearly, if the n channel symbols are multicast over a network using a routing scheme, the k source symbols remain secure in the presence of an adversary with access to any μ edges. We will illustrate later that this is not necessarily the case when network coding is used. However, we will show that a network code based on the Ozarow-Wyner scheme that preserves security of the k source symbols, which are coded into the n multicast symbols, can be designed over a sufficiently large field.

Using the observations made by Feldman *et al.* in [6], we show that our scheme is equivalent to the one proposed in the pioneering work of Cai and Yeung in [4]. However, with our approach, we can quickly and transparently recover some of the results available in the literature on secure network coding for wiretapped networks. The algorithm due to [4] is based on the code construction proposed by Li *et al.* in [3], however more efficient network coding algorithms have been proposed recently (see, e.g., [19] and [20]). We use the results on the encoding complexity of the network coding presented in [20], [21], [22] to derive new bounds on the required field size of a secure network code that are independent of the number of edges in the network and that depend only on the number k of source symbols and the number t of destinations. We also propose an algorithm for construction of a secure network code that achieves these bounds. Furthermore, we look at the dual problem and analyze the security of a given Ozarow-Wyner code by studying the amount of information that can be gained by the wiretapper as a function of the number of wiretapped edges.

Parts of the results presented in this paper were published in [1] and were later extended in [23], [24] by Silva and Kschischang to construct universal secure network codes based on maximum rank-distance (MRD) codes, and by Mills *et al.* in [25] to achieve secrecy for wireless erasure networks.

This paper is organized as follows: In Section II, we briefly review the Ozarow-Wyner wiretap channel of type II problem. In Section III, we introduce the network generalization of this problem. In Section IV, we present an algorithm for secure network code design and establish new bounds on the required code alphabet size. In Section V, we study the security of Ozarow-Wyner codes. In Section VI, we highlight some connections of this work with other works on secure network coding and network error correction. Finally, we conclude in Section VII with a summary of our results and open problems.

II. Wiretap Channel II

We first consider a point-to-point scenario in which the source can transmit n symbols to the receiver and an adversary can access any μ of those symbols [17], [18]. For this case, we know that the maximum number of symbols that the source can communicate to the receiver securely in the information-theoretic sense is equal to $n - \mu$.

The problem is mathematically formulated as follows. Let $S = (s_1, s_2, \ldots, s_k)^T$ be the random variable associated with the k information symbols that the source wishes to send securely, $Y = (y_1, y_2, \ldots, y_n)^T$ the random variable associated with the symbols that are transmitted through the noiseless channel between the source and the receiver, and $Z = (z_1, z_2, \ldots, z_\mu)^T$ the random variable associated with the wiretapped symbolsof Y. When $k \leq n - \mu$, there exists an encoding scheme that maps S into Y such that:

1) The uncertainty about S is not reduced by the knowledge of Z (perfect secrecy condition), *i.e.*,

$$H(S|Z) = H(S), \tag{1}$$

and,

2) The information S is completely determined (decodable) by the complete knowledge of Y, that is,

$$H(S|Y) = 0. \tag{2}$$

For $n = 2$, $k = 1$, $\mu = 1$, such a coding scheme can be constructed as follows. If the source bit equals 0, then either 00 or 11 is transmitted through the channel with equal probability. Similarly, if the source bit equals 1, then either 01 or 10 is transmitted through the channel with equal probability:

source bit s_1	0	1
codeword $y_1 y_2$ chosen at random from	$\{00, 11\}$	$\{01, 10\}$

It is easy to see that knowledge of either y_1 or y_2 does not reduce the uncertainty about s_1, whereas the knowledge of both y_1 and y_2 is sufficient to completely determine s_1, namely, $s_1 = y_1 + y_2$.

In general, $k = n - \mu$ symbols can be transmitted securely by a coding scheme based on an $[n, n - k]$ linear maximal distance separable (MDS) code $\mathcal{C} \subset \mathbb{F}_q^n$. In this scheme, the encoder is a probabilistic device which operates on the space $\mathbb{F}_q^n$ partitioned into q^k cosets of $\mathcal{C}$, where q is a large enough prime power. The k information symbols are taken as the syndrome which specifies a coset, and the transmitted word is chosen uniformly at random from the specified coset. The decoder recovers the information symbols by simply computing the syndrome of the received word. Because of the properties of MDS codes, knowledge of any $\mu = n - k$ or fewer symbols will leave the uncertainty of the k information symbols unchanged. The code used in the above example is the $[2, 1]$ repetition code with the parity check matrix

$$\mathcal{H} = \begin{bmatrix} 1 & 1 \end{bmatrix}. \tag{3}$$

III. Wiretap Network II

We now consider an acyclic multicast network $G = (V, E)$ with unit capacity edges, an information source, t receivers, and the value of the min-cut to each receiver is equal to n. The goal is to maximize the multicast rate with the constraint of revealing no information about the multicast data to the adversary that can access data on any μ edges. We assume that the adversary knows the implemented network code, *i.e.* all the coefficients of the linear combinations that determine the packets on each edge. Moreover, we assume that there is no shared randomness between the source and the receivers. The latter assumption rules out the use of traditional “key” cryptography to achieve security.

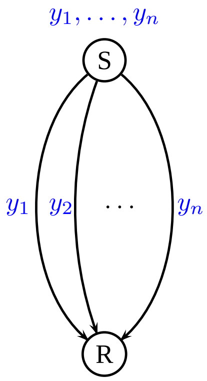

Fig. 1. Network equivalent to the wiretap channel of type II.

It can be seen that the wiretap channel of type II is equivalent to the simple unicast network of Figure 1 formed by n disjoint edges between the source and the destination, each carrying a different symbol. For this network, the source can multicast $k \leq n - \mu$ symbols securely if it first applies a secure wiretap channel code (as described above) mapping k information symbols into n transmitted symbols $(y_1, \ldots, y_n)$.

For general networks, when security is not an issue, we know that a multicast rate n is possible with linear network coding [2], [3]. It is interesting to ask whether, using the same network code, the source can always multicast $k \leq n - \mu$ symbols securely using a wiretap channel code at the source. Naturally, this would be a solution if a multicast rate of n can be achieved just by routing.

Example 1 (Butterfly Network): Consider this approach for the butterfly network shown in Figure 2 where we have $n = 2$, $k = 1$, $\mu = 1$. If the source applies the coding scheme described in the previous section and the usual network code as in Figure 2(a), the wiretapper will be able to learn the source symbol if it taps into any of the edges BE, EF or ED. Therefore, a network code can break down a secure wiretap channel code. However, if the network code is changed so that node B combines its inputs over, *e.g.*, $\mathbb{F}_3$ and the coding vector of edge BE is $\begin{bmatrix} 1 & \alpha \end{bmatrix}$ where α is a primitive element of $\mathbb{F}_3$ (*i.e.*, the message sent on edge BE is $x_1 + \alpha x_2$ as in Figure 2(b)), the wiretap channel code remains secure, that is, the adversary cannot gain any information by accessing any single edge in the network. Note that the wiretap channel code based on the MDS code with $\mathcal{H} = \begin{bmatrix} 1 & 1 \end{bmatrix}$ remains secure with any network code whose BE

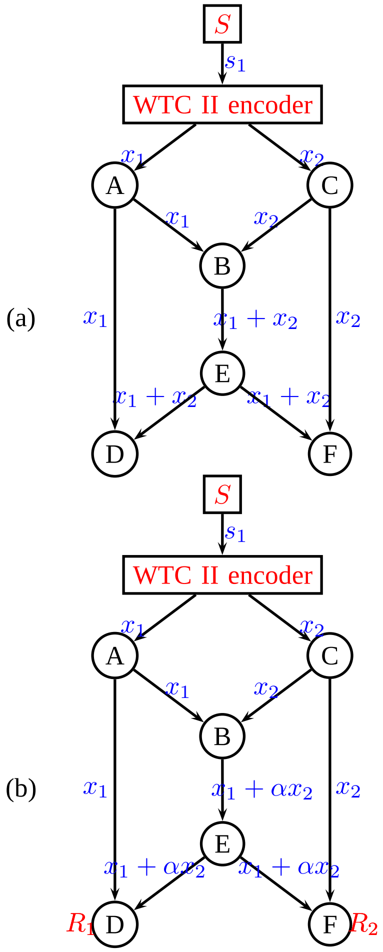

Fig. 2. Single-edge wiretap butterfly network with a) insecure network code and b) secure network code.

coding vector is linearly independent of $\begin{bmatrix}1 & 1\end{bmatrix}$.

We will next show that the source can multicast $k \leq n - \mu$ symbols securely if it first applies a secure wiretap channel code based on an MDS code with a $k \times n$ parity check matrix $\mathcal{H}$ if the network code is such that no linear combination of $\mu = n - k$ or fewer coding vectors belongs to the space spanned by the rows of $\mathcal{H}$. Let $W \subset E$ denote the set of $|W| = \mu$ edges the wiretapper chooses to observe, and $Z_W = (z_1, z_2, \ldots, z_\mu)^T$ the random variable associated with the packets carried by the edges in W. Let C_W denote the matrix whose rows are the coding vectors associated with the observed edges in W. As in the case of the wiretap channel, $S = (s_1, s_2, \ldots, s_k)^T$ denotes the random variable associated with the k information symbols that the source wishes to send securely, and $Y = (y_1, y_2, \ldots, y_n)^T$ the random variable associated with the n wiretap channel code symbols. The n symbols of Y will be multicast through the network by using linear network coding. Writing $H(S, Y, Z_W)$ in two different forms, and taking into account the decodability condition of Equation (2), we get

$$H(S|Z_W) + H(Y|SZ_W) = H(Y|Z_W) + \underbrace{H(S|YZ_W)}_{=0}. \tag{4}$$

Our objective is to conceal all the information data from the wiretapper. The perfect secrecy condition implies

$$H(S|Z_W) = H(S), \forall W \subset E \text{ s.t. } |W| = \mu.$$

Thus we obtain,

$$H(Y|SZ_W) = H(Y|Z_W) - H(S). \tag{5}$$

This implies, in turn that

$$n - \text{rank}(C_W) - k \geq 0. \tag{6}$$

Since there is a choice of edges such that rank$(C_W) = \mu$, the maximum rate for secure transmission is bounded as

$$k \leq n - \mu.$$

If the bound is achieved with equality, we have $H(Y|SZ_W) = 0$ and consequently, the system of equations

$$\begin{bmatrix} S \\ Z_w \end{bmatrix} = \begin{bmatrix} \mathcal{H} \\ C_W \end{bmatrix} \cdot Y$$

has to have a unique solution for all W for which rank$(C_W) = \mu$. That is,

$$\text{rank} \begin{bmatrix} \mathcal{H} \\ C_W \end{bmatrix} = n \quad \text{for all } C_W \text{ s.t. rank}(C_W) = \mu. \tag{7}$$

This analysis proves the following result:

Theorem 1: Let $G = (V, E)$ be an acyclic multicast network with unit capacity edges and an information source such that the size of a minimum cut between the source and each receiver is equal to n. Then, a wiretap code at the source based on an MDS code with a $k \times n$ parity check matrix $\mathcal{H}$ and a network code such that no linear combination of $\mu = n-k$ or fewer coding vectors belongs to the space spanned by the rows of $\mathcal{H}$ make the network information-theoretically secure against a wiretap adversary who can observe at most $\mu \leq n-k$ edges. Any adversary able to observe more than $n-k$ edges will have uncertainty about the source smaller than k.

Next, we give an application of the previous theorem to the family of *combination* networks illustrated in Figure 3.

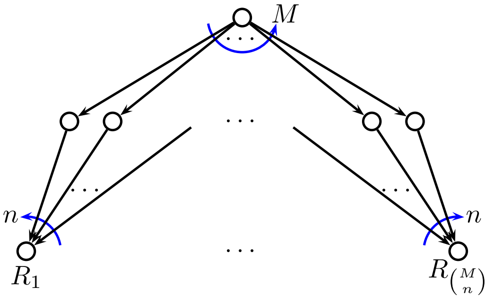

Fig. 3. Combination $B(n,M)$ network.

Example 2 (Combination Networks): A combination network $B(n,M)$ is defined over a 3-partite graph comprising three layers. The first layer contains a single source node, the second layer M intermediate nodes and the last layer is formed by $\binom{M}{n}$ receiver nodes such that every set of n nodes of the second layer is observed by a receiver.

The result of Theorem 1 can be used to construct a secure network code for $B(n,M)$ from an $[M+k, M+k-n]$ MDS code which would achieve perfect secrecy against a wiretapper that can observe any $\mu = n-k$ edges in the network. Let $\mathcal{H}$ be an $n \times (M+k)$ parity check matrix of such MDS code over $\mathbb{F}_q$. A secure network code can be obtained by taking the first k rows of $\mathcal{H}^T$ to form the matrix of the coset code at the source, and the rest of the rows of $\mathcal{H}^T$ to be the coding vectors of the M edges going out of the source. Equation (7) is satisfied since the considered code is MDS and, therefore, any n columns of $\mathcal{H}$ form a basis of $\mathbb{F}_q^n$. For instance if $M+k+1$ is equal to a prime power q, a secure network code can be derived based on an $[M+k, M+k-n]$ Reed-Solomon code with the following Vandermonde parity check matrix

$$\mathcal{H} = \begin{bmatrix} 1 & \alpha & \dots & \alpha^{M+k-1} \\ 1 & \alpha^2 & \dots & \alpha^{2(M+k-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^n & \dots & \alpha^{n(M+k-1)} \end{bmatrix}, \tag{8}$$

where α is a primitive element of $\mathbb{F}_q$. Figure 4 depicts a secure network code for the network $B(3,4)$ and $k = 2$ using a [6,3] Reed-Solomon code over $\mathbb{F}_7$ whose parity check matrix is given by Equation (8) for $\alpha = 3$.

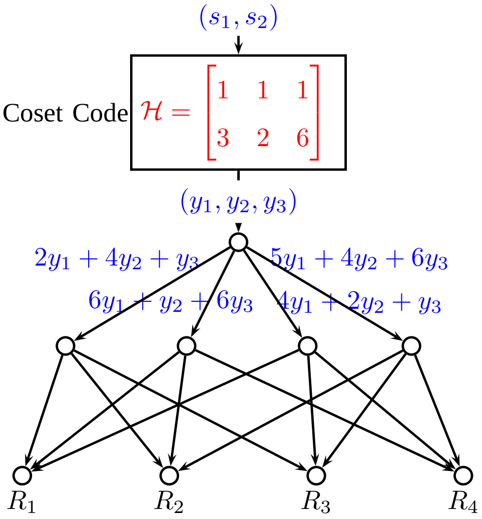

Fig. 4. A secure network code for the $B(3,4)$ combination network based on a [6,3] Reed-Solomon code over $\mathbb{F}_7$.

The above analysis shows that the maximum throughput can be achieved by applying a wiretap channel code at the source and then designing the network code while respecting certain constraints. The decoding of secure source symbols S is then merely a matrix multiplication of the decoded multicast symbols Y since $\mathcal{H}Y = S$. The method gives us a better insight of how much information the adversary gets if he can access more edges than the code is designed for. It also enables us to design secure network coding schemes over smaller alphabets. These two issues are discussed in detail in the next two sections.

IV. Network Code Design Alphabet Size

The approach described previously in the literature for finding a secure multicast network code consisted of decoupling the problem of designing a multicast network code and making it secure by using some code on top of it. Feldman *et al.* showed in [6] that there exist networks where the above construction might require a quite large field size. In this section, we present a different construction that exploits the topology of the network. This is accomplished by adding the security constraints to the *Linear Information Flow* (LIF) algorithm of [19] that constructs linear multicast network codes in polynomial time in the number of edges in the graph. The result is a better lower bound on the sufficient field size. However, the modified LIF algorithm does not have a polynomial time complexity.

We start by giving a brief high level overview of the LIF algorithm of [19]. The inputs of the algorithm are the network, the source node, the t receivers and the number n of packets that need to be multicast to all receivers. Assuming the min-cut between the source and any receiver is at least n, the algorithm outputs a linear network code that guaranties the delivery of the n packets to all the receivers.

The algorithm starts by 1) finding t flows $F_1, F_2, \dots, F_t$ of value n each, from the source to to each receiver and 2) defining t $n \times n$ matrices B_{F_j} (one for each receiver) formed by the global encoding vectors of the n last visited edges in the flow F_j. Initially, each matrix B_{F_j} is equal to the identity matrix I_n. Then, the algorithm goes over the network edges, visiting each one in a topological order. In each iteration, the algorithm finds a suitable local encoding vector for the visited edge, and updates all of the t matrices B_{F_j}. The algorithm maintains the invariant that the matrices B_{F_j} remain invertible after each iteration. Thus, when it terminates, each receiver will get n linear combinations of the original packets that form a full rank system. Thus each destination can solve for these packets by inverting the corresponding matrix.

The analysis of the algorithm due to [19] implies that a field of size at least t (the number of destinations) is sufficient for finding the desired network code. In particular, as shown in [19, Lemma 8], a field of size larger or equal to t is sufficient for satisfying the condition that the t matrices B_{F_j} are always invertible.

To construct a secure network code, we modify the LIF algorithm in the following way. We select a $k \times n$ parity check matrix $\mathcal{H}$. Without loss of generality, we assume that the μ packets observed by the wiretapper are linearly independent, *i.e.*, rank $C_W = \mu$. We denote by e_i the edge visited at the i-th iteration of the LIF algorithm, and by P_i the set of the edges that have been processed by the end of it. Then, we extend the set of invariants to guaranty that the encoding vectors are chosen so that the matrices $M_W = \begin{bmatrix} \mathcal{H} \\ C_W \end{bmatrix}$ are also invertible; which, by Theorem 1, achieves the security condition. More precisely, using the same techniques as the original LIF algorithm, we make sure that by the end of the i-th iteration, the matrices B_{F_j} and the matrices M_{W_i} are invertible; where $W_i = \{e_i\} \cup W'$ and W' is a subset of P_i containing $\mu - 1 = n - k - 1$ edges. The total number of matrices that need to be kept invertible in this modified version of the LIF algorithm is at most $\binom{|E|-1}{\mu-1} + t$. Thus, similarly as in [19, Lemma 8], we obtain the following improved bound on the alphabet size for secure multicast:

Theorem 2: Let $G = (V, E)$ be an acyclic network with unit capacity edges and an information source such that the min-cut value to each of the t receivers is equal to n. A secure multicast at rate $k \leq n - \mu$ in the presence of a wiretapper who can observe at most $\mu \leq n$ edges is possible over the alphabet $\mathbb{F}_q$ of size

$$q \geq \binom{|E| - 1}{\mu - 1} + t. \tag{9}$$

The bound given by Equation (9) can be further improved by realizing as was first done in [20] that not all edges in the network carry different linear combination of the source symbols. Langberg *et al.* showed in [21] that the number of *encoding edges* in a *minimal* acyclic multicast network is bounded by $2n^3t^2$. Encoding edges create new packets by combining the packets received over the incoming edges of their tail nodes. A minimal multicast network does not contain redundant edges, *i.e.*, edges that can be removed from the network without violating its optimality. Reference [22] presents an efficient algorithm for construction of a minimal acyclic network $\widehat{G}$ from the original network G. This work also shows that a feasible network code for a minimal network can be used for the original network as well with only slight modifications.

The main idea of our scheme is to find a secure network code for the minimal network $\widehat{G}$, and then use the procedure described in [22] to construct a network code for original network G which will also be secure. Now consider the problem of finding secure network codes for $\widehat{G}$. This problem will not change if the wiretapper is not allowed to wiretap the *forwarding edges*, *i.e.*, the edges that just forward packets received by their tail nodes. Therefore, the set of edges that the wiretapper might have access to consists of the encoding edges and the edges outgoing from the source. The number of such edges is bounded by $2n^3t^2$. Now, applying Theorem 2 on $\widehat{G}$ and taking into consideration the restriction on the edges that can be potentially wiretapped, we obtain the following bound on the sufficient field size which is independent of the size of the network.

Corollary 1: For the transmission scenario of Theorem 2, a secure mulitcast network code always exists over the alphabet $\mathbb{F}_q$ of size

$$q \geq \binom{2k^3t^2}{\mu - 1} + t. \tag{10}$$

For networks with two sources, we can completely settle the question on the required alphabet size for a secure network code. Note that the adversary has to be limited to observing at most one edge of his choice. Based on the work of Fragouli and Soljanin in [20], the coding problem for these networks is equivalent to a vertex coloring problem of some specially designed graphs, where the colors correspond to the points on the projective line $\mathbb{PG}(1, q)$:

$$[0\,1],\ [1\,0],\ \text{and}\ [1\,\alpha^i]\ \text{for}\ 0 \leq i \leq q-2, \tag{11}$$

where α is a primitive element of $\mathbb{F}_q$. Clearly, any network with two sources and arbitrary number of receives can be securely coded by reducing the set of available colors in (11) by removing point (color) $[1\,1]$ and applying a wiretap code based on the matrix $\mathcal{H} = [1\,1]$ as in the example above. Alphabet size sufficient to securely code all network with two sources also follows from [20]:

Theorem 3: For any configuration with two sources t receivers, the code alphabet $\mathbb{F}_q$ of size

$$\lfloor \sqrt{2t - 7/4} + 1/2 \rfloor + 1$$

is sufficient for a secure network code. There exist configurations for which it is necessary.

V. Wiretapper Equivocation

In this section, we analyze the performance of coset codes in the case of a wiretapper with variable strength, *i.e.*, the number μ of edges he can observe is not fixed. For a given coset code, we seek to quantify the amount of information that is leaked to the wiretapper as a function of μ.

Assume that at the source s of a multicast network a coset code defined by a $k \times n$ parity check matrix $\mathcal{H}$ is used as described in the previous section. The equivocation $\Delta(\mu)$ of the wiretapper, *i.e.*, the uncertainty it has about the information source vector $S=(s_1,\dots,s_k)^T$, is defined, as in [18], based on the worst case scenario, by

$$\Delta(\mu) := \min_{W\subset E; |W|=\mu} H(S|Z_W), \tag{12}$$

where $Z_W=(z_1,\dots,z_\mu)^T$ is the random variable representing the observed packets on the set $W\subseteq E$ of wiretapped edges. We have $Z_W=C_WY$ where C_W is an $\mu\times n$ matrix, and $Y=(y_1,\dots,y_n)^T$ is the output of the coset code at the source. It can be seen that $\Delta(\mu)$ can be written as:

$$\Delta(\mu) = \min_{\substack{W\subset E; |W|=\mu\\ \text{rank}(C_W)=\mu}} H(S|Z_W). \tag{13}$$

Therefore, we will assume from now on without loss of generality that W is such that rank$(C_W)=\mu$. For a given choice of such W, let $C_W^\perp$ be the parity check matrix of the $[n,\mu]$ code generated by C_W. Let I_n be the $n\times n$ identity matrix. Define $J_{n,\mu}$ to be the $n\times(n-\mu)$ matrix where the first μ rows are all zeros and the last $n-\mu$ rows form $I_{n-\mu}$. Theorem 4 below gives the expression of $\Delta(\mu)$ which depends on the network code and the coset code used.

Theorem 4:

$$\Delta(\mu) = \min_{\substack{W\subset E; |W|=\mu\\ \text{rank}(C_W)=\mu}} \text{rank}(\mathcal{H}\begin{bmatrix} C_W \\ C_W^\perp \end{bmatrix}^{-1} J_{n,\mu}). \tag{14}$$

Proof:

First let $A_W=\begin{bmatrix} C_W \\ C_W^\perp \end{bmatrix}$. By Equation (4), we have

$$
\begin{aligned}
H(S|Z_W) &= H(Y|Z_W) - H(Y|SZ_W) \\
&= n - \text{rank}(C_W) - (n - \text{rank}\begin{bmatrix}\mathcal{H}\\ C_W\end{bmatrix}) \\
&= \text{rank}(\begin{bmatrix}\mathcal{H}\\ C_W\end{bmatrix} A_W^{-1}) - \text{rank}(C_W) \\
&= \text{rank}(\begin{bmatrix}\mathcal{H}A_W^{-1}\\ C_WA_W^{-1}\end{bmatrix}) - \text{rank}(C_W) \\
&= \dim(\langle \mathcal{H}A_W^{-1}\rangle) + \dim(\langle C_WA_W^{-1}\rangle) \\
&- \dim(\langle \mathcal{H}A_W^{-1}\rangle \cap \langle C_WA_W^{-1}\rangle) - \text{rank}(C_W) \\
&= k - \dim(\langle \mathcal{H}A_W^{-1}\rangle \cap \langle J'_{n,\mu}\rangle),
\end{aligned}
\tag{15}
$$

where $\langle\cdot\rangle$ denotes the row space of a matrix and $J'_{n,\mu}$ is the $\mu \times n$ matrix where the first μ columns form I_μ and the last $n-\mu$ columns are all zeros. Note that $\dim(\langle \mathcal{H}A_W^{-1}\rangle \cap \langle J'_{n,\mu}\rangle)$ is exactly k minus the rank of the last $n-\mu$ column vectors of $\mathcal{H}A_W^{-1}$. ■

A relevant concept to our work here is that of the generalized Hamming weights $d_1(\mathcal{C}), \dots, d_k(\mathcal{C})$ of a linear code $\mathcal{C}$ which was introduced by Wei in [26] and that characterize the performance of coset codes over the classical wiretap channel of type II. The generalized Hamming weights were extended to the wiretap networks setting in [27]. Given a certain network with an associated network and coset codes, Theorem 4 provides an equivalent expression of the network formulation of the r-th generalized Hamming weight d_r as the minimum number of edges that should be wiretapped to leak r symbols to the wiretapper. Then, we can write

$$
\begin{aligned}
d_r &:= \min\{\mu; \Delta(\mu) = k - r\} \\
&:= \min\{\mu; \min_{\substack{W\subset E; |W|=\mu \\ \text{rank}(C_W)=\mu}} \text{rank}(\mathcal{H}\begin{bmatrix}C_W\\ C_W^{\perp}\end{bmatrix}^{-1} J_{n,\mu}) = k - r\}.
\end{aligned}
\tag{16}
$$

Next, we focus on three special cases. First, we revisit the model of the wiretap channel of type II of [17]. Second, we consider the case where the wiretapper may gain access to more edges than what the secure code is designed to combat. Third, we study the scenario where only a part of the network edges are vulnerable to wiretapping.

A. Wiretap Channel of Type II

Consider again the wiretap channel of type II studied in [17]. Theorem 4 can be used to easily recover the following classical result for this channel.

Corollary 2: The equivocation rate of the wiretapper in the wiretap channel of type II is given by

$$\Delta(\mu) = \min_{\substack{U \subseteq \{1,2,\ldots,n\} \\ |U|=n-\mu}} \text{rank}\{\mathcal{H}_i ; i \in U\}, \tag{17}$$

where $\mathcal{H}_i$ denote the ith column of the parity check matrix $\mathcal{H}$.

Proof: The wiretap channel of type II is equivalent to the network depicted in Figure 1. Assume that the edges between the source and the destination are indexed from 1 to n, so that $E = \{1, \ldots, n\}$. For any $W \subseteq \{1, \ldots, n\}$, define I_W to be the matrix formed by the rows of the $n \times n$ identity matrix indexed by the elements of W in an increasing order. Since edge i carries the packet y_i, for a given set $W \subseteq E$ of wiretapped edges, $C_W = I_W$ and $C_W^{\perp} = I_U$, where $U = \{1, \ldots, n\} \setminus W$. Therefore, $A_W^{-1} = \begin{bmatrix} I_W \\ I_U \end{bmatrix}^{-1} = A_W^T$, and the last $n - \mu$ columns of $\mathcal{H}A_W^T$ are exactly the columns of $\mathcal{H}$ indexed by U. ■

B. Underestimated Wiretapper

Suppose the coset code defined by the $k \times n$ parity check matrix $\mathcal{H}$ satisfies Theorem 1 and achieves perfect secrecy against a wiretapper that can observe λ edges. If, however, the wiretapper can access μ edges, where $\mu > \lambda$, then the amount of information leaked to the wiretapper can be shown to be equal to $\mu - \lambda$, *i.e.*, the number of additional wiretapped edges.

Corollary 3: For the case of an underestimated wiretapper, the equivocation of the wiretapper is given by:

$$\Delta(\mu) = k - (\mu - \lambda).$$

Proof: Since the coset code achieves perfect secrecy for λ wiretapped edges, by Theorem 1, we have $k = n - \lambda$ and $H(S|YZ_W) = 0$. Thus, Equation (4) gives

$$H(S|Z_W) = H(Y|Z_W) = n - \text{rank}(C_W) = k + \lambda - \text{rank}(C_W).$$

The minimum value of $H(S|Z_W)$ is obtained when C_W has maximal rank, i.e, when $\text{rank}(C_W) = \mu$.

■

C. Restricted Wiretapper

In practice, for instance in large networks, the wiretapper may not have access to all the network edges, and his choice of μ edges is limited to a certain edge subset $E' \subset E$. For this model, the equivocation rate of the wiretapper is determined by Equation 14 where E is replaced by E'. An interesting case arises, however, when the edges in E' belong to a cut of n edges between the source and one of the receivers. In this case, the performance of the coset code is the same as when it is used for a wiretap channel of type II.

Corollary 4: In the case of a restricted wiretapper that can observe any μ edges in a cut between the source and one of the destinations, the equivocation rate of the wiretapper is given by Equation (17).

Proof: Assume the edges that are vulnerable to wiretapping are indexed from 1 to n, so that $E' = \{1, \dots, n\}$. Let $Z_{E'} = (z_1, \dots, z_n)^T$ denote the packets carried by those edges, such that edge i carries packet z_i. We can write $Z_{E'} = C_{E'}Y$, where $C_{E'}$ is an $n \times n$ matrix. Since the cut comprises n edges, the matrix $C_{E'}$ is invertible; otherwise, by the properties of linear network codes, the destination corresponding to the considered cut cannot decode Y. For a choice $W \subseteq E'$ of wiretapped edges, we have $Z_W = C_W Y$, where $C_W = I_W C_{E'}$. Moreover, $C_W^{\perp} = I_{\overline{W}} C_{E'}$, where $\overline{W} = E' \setminus W$. Therefore,

$$\mathcal{H} \begin{bmatrix} C_W \\ C_W^{\perp} \end{bmatrix}^{-1} = \mathcal{H}(C_{E'} \begin{bmatrix} I_W \\ I_{\overline{W}} \end{bmatrix})^{-1} = \mathcal{H} C_{E'}^{-1} \begin{bmatrix} I_W \\ I_{\overline{W}} \end{bmatrix}^T .$$

Similar to the proof of Corollary 2, the last $n - \mu$ columns of $\mathcal{H} A^{-1} \begin{bmatrix} I_W \\ I_{\overline{W}} \end{bmatrix}^T$ are exactly the columns of $\mathcal{H} A^{-1}$ indexed by U. So, by Theorem 4, we have

$$\begin{aligned} \Delta(\mu) &= \min_{\substack{U \subseteq \{1,2,\dots,n\} \\ |U| = n-\mu}} \text{rank}\{(\mathcal{H}A^{-1})_i; i \in U\} \\ &= \min_{\substack{U \subseteq \{1,2,\dots,n\} \\ |U| = n-\mu}} \text{rank}\{\mathcal{H}_i; i \in U\}. \end{aligned}$$

■

Note that the previous result still holds for any subset E' of possible wiretapped edges such that $C_{E'}$ is invertible. For this scenario, the equivocation rate of the wiretapper can be alternatively

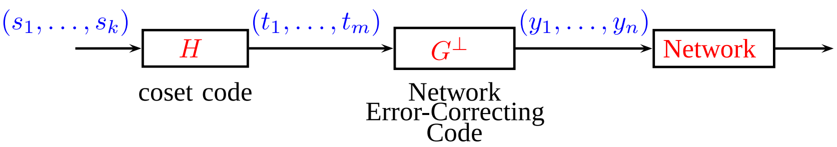

Fig. 5. A coding scheme achieving perfect secrecy against a limited Byzantine wiretapper.

given by the generalized Hamming weights [26] $d_1(\mathcal{C}),\dots,d_k(\mathcal{C})$ of the linear code $\mathcal{C}$ generated by $\mathcal{H}$. In this case, for a given μ, $\Delta(\mu)$ is the unique solution to the following inequalities [26, Cor. A]:

$$d_{n-\mu-\Delta(\mu)}(\mathcal{C})) \leq n-\mu < d_{n-\mu-\Delta(\mu)+1}(\mathcal{C}).$$

VI. Connections with Other Schemes

In this section, we explore the relationship between the proposed scheme and previously known constructions [4], [28], [29], [23].

A. *Secure Network Coding and Filtered Secret Sharing*

Cai and Yeung were first to study the design of secure network codes for multicast demands [4]. They showed that, in the setting described above, a secure network code can be found for any $k \leq n-\mu$. Their construction is equivalent to the following scheme:

1) Generate a vector $R = (r_1, r_2, \dots, r_\mu)^T$ choosing its components uniformly at random over $\mathbb{F}_q$,
2) Form vector X by concatenating the μ random symbols R to the k source symbols S:
$$X = \begin{bmatrix} S \\ R \end{bmatrix} = (s_1,\dots,s_k,r_1,\dots,r_\mu)^T$$
3) Chose an *invertible* $n \times n$ matrix T over $\mathbb{F}_q$ and a feasible multicast network code [3] to ensure the security condition (1). (It is shown in [4, Thm. 1] that such code and matrix T can be found provided that $q > \binom{|E|}{\mu}$.)
4) Compute $Y = TX$ and multicast Y to all the destinations by using the constructed code.

Feldman *et al.* considered also the same problem in [6]. Adopting the same approach of [4], they showed that in order for the code to be secure, the matrix T should satisfy certain conditions ([6, Thm. 6]). In particular, they showed that in the above transmission scheme, the security condition (1) holds if and only if any set of vectors consisting of

1) at most μ linearly independent edge coding vectors and/or
2) any number of vectors from the first k rows of T^{-1}

is linearly independent. They also showed that if one sacrifices in the number of information packets, that is, take $k < n - \mu$, then it is possible to find secure network codes over fields of size much smaller than the very large bound $q > \binom{|E|}{\mu}$.

We will now show that our approach based on coding for the wiretap channel at the source is equivalent to the above stated scheme [4] with the conditions of [6].

Proposition 1: For any $n \times n$ matrix T satisfying the security conditions defined above, the $k \times n$ matrix $\mathcal{H} = T^*$ formed by taking the first k rows of T^{-1} satisfy the condition of Theorem 1.

Proof: Consider the secure multicast scheme of [4] as presented above. For a given information vector $S \in \mathbb{F}_q^k$, let $B(S)$ be the set of all possible vectors $Y \in \mathbb{F}_q^n$ that could be multicast through the network under this scheme. More precisely,

$$B(S) = \left\{ Y \in \mathbb{F}_q^n | Y = TX, X = \begin{bmatrix} S \\ R \end{bmatrix}, R \in \mathbb{F}_q^{n-k} \right\}.$$

Then, for all $Y \in B(S)$, we have $T^*Y = T^*T \begin{bmatrix} S \\ T \end{bmatrix} = S$. Therefore, any $Y \in B(S)$ also belongs to the coset of the space spanned by the rows of T^* whose syndrome is equal to S. Moreover, since T is invertible, $|B(S)| = 2^{n-k}$ implying that set $B(S)$ is exactly that coset. The conditions of [6] as stated above directly translate into (18), the remaining condition of Theorem 1. ■

B. Universal Secure Network Codes

For practical implementations of linear multicast network codes over $\mathbb{F}_q$, the information sources are typically packets of a certain length m, *i.e.*, $s_1, \ldots, s_k$ are vectors in $\mathbb{F}_q^m$. Applying the approach presented in the preliminary version of this paper [1], Silva and Kschischang devised in [23] a scheme that achieves a complete decoupling between the secure code and the network code design. Their scheme is universal in the sense that it achieves secrecy by applying a coset code at source with no knowledge of the network code used. The main idea is to use a special class of MDS codes called maximal rank-distance codes (MRD) which are non-linear over $\mathbb{F}_q$ but linear over the extension field $\mathbb{F}_{q^m}$. The parity check matrix of an MRD code over $\mathbb{F}_{q^m}$, has the interesting property that it always satisfies the condition of Theorem 1 when the edge coding vectors are over $\mathbb{F}_q$, as stated in the theorem below.

Lemma 1: [23, Lemma 3] Let $\mathcal{H}$ be the parity check matrix of an $[n, n-k]$ linear MRD code over $\mathbb{F}_{q^m}$. For any full rank $(n-k) \times n$ matrix B over $\mathbb{F}_q$, the $n \times n$ matrix $\begin{bmatrix} \mathcal{H} \\ B \end{bmatrix}$ is invertible.

Therefore, MRD codes will always achieve perfect secrecy irrespective of the network code used. The choice of the MRD code will only depend on the underlying field $\mathbb{F}_q$ of the network code.

C. Byzantine Adversaries

The malicious activity of the wiretapper in the model considered in this paper was restricted to eavesdropping. A more powerful wiretapper, with jamming capabilities, may not only listen to the data in the network but also alter it. This may lead to flooding the whole network with erroneous packets. Schemes to combat such wiretappers, known in literature as Byzantine adversaries, were studied in [12], [15], [16] and the references within.

Consider a scenario where the wiretapper can not only observe μ edges but also jam α edges of his choice that are unknown to the destinations. In this case, we will describe a coding scheme that achieves a multicast rate of $k = n - 2\alpha - \mu$ and guaranties that the information will remain hidden from the wiretapper. This can be achieved by using a coset code as described in Section III followed by a powerful network error-correcting code [13], [14]. First, we recall an important result in [14, Theorem 4]

Theorem 5: For an acyclic network $G(V, E)$ with min-cut n, there exists a linear α-error-correcting code of dimension $(n - 2\alpha)$ over a sufficiently large field.

Let $\mathcal{G}$ be the generator matrix of a linear α-error-correcting code of dimension $(n-2\alpha)$ whose existence is guaranteed by the previous theorem, and Let $\mathcal{G}^{\perp}$ be its parity check matrix. A block diagram of the coding scheme that achieves secrecy against a Byzantine wiretapper at a rate $k = n - 2\alpha - \mu$ is depicted in Figure 5. First, the information $S = (s_1, \ldots, s_k)^T$ is encoded using a coset code of parity check matrix $\mathcal{H}$ into the vector $T = (t_1, \ldots, t_m)^T$, with $m = k + \mu$.

The vector T is then encoded into $Y = (y_1, \ldots, y_n)^T = \mathcal{G}T$ using the network error-correcting code. To achieve perfect secrecy, $\mathcal{H}$ should satisfy the condition of Theorem 1, which can be expressed here as:

$$\text{rank} \begin{bmatrix} \mathcal{H} \\ C_W \mathcal{G} \end{bmatrix} = k + \mu \quad \text{for all } C_W \text{ s.t. } \text{rank}(C_W) = \mu. \tag{18}$$

We assume that the code is over a field large enough to guaranty the existence of the network error-correcting code and the matrix $\mathcal{H}$ satisfying the above condition as well. At each destination, a decoder corrects the errors introduced by the wiretapper and recovers T. The information S is then obtained as the unique solution of the system $\mathcal{H}S = T$. It was recently shown in [30] that the rate $k = n - 2\alpha - \mu$ is optimal and another construction for codes with the same properties was presented there.

VII. Conclusion

We considered the problem of securing a multicast network implementing network coding against a wiretapper capable of observing a limited number of edges of his choice, as defined initially by Cai and Yeung. We showed that the problem can be formulated as a generalization of the wiretap channel of type II which was introduced and studied by Ozarow and Wyner, and decomposed into two sub-problems: the first one consists of designing a secure wiretap channel code, or a coset code, and the second consists of designing a network code satisfying some additional constraints. We proved there is no penalty to pay by adopting this separation, which we find in many ways illuminative. Moreover, this approach allowed us to derive new bounds on the required alphabet size for secure codes. These new bounds differ from those in the literature in that they are independent from the network size and are functions of only the number of information symbols and that of destinations. We also analyzed the performance of the proposed coset codes under various wiretapper scenarios.

A number of interesting questions related to this problem remain open. For instance, the bounds presented here on the code alphabet size can be large in certain cases and it is worthy to investigate whether tighter bounds exist. Another issue which was not addressed in this paper is that of designing efficient decoding algorithms at the destinations which can be very important in practical implementations. Also, the work of [23] hinted at some advantages of non-linear codes. The benefits of nonlinearity in security applications, whether at the source code or at the network code level, are still to be better understood.

Acknowledgments

The authors would like to thank C. N. Georghiades for his continued support.

References

[1] S. El Rouayheb and E. Soljanin, “On wiretap networks II,” in *2007 IEEE International Symposium on Information Theory (ISIT 2007)*, Nice, France, Jun 2007.

[2] R. Ahlswede, N. Cai, S-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inform. Theory*, pp. 1204–1216, July 2000.

[3] S-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 371–381, Feb. 2003.

[4] N. Cai and R. W. Yeung, “Secure network coding,” in *Proc. 2002 IEEE International Symposium on Information Theory (ISIT’02)*, June 2002.

[5] S. W. Yeung and N. Cai, “On the optimality of a construction of secure network codes,” in *Proc. IEEE International Symposium on Information Theory (ISIT’08)*, 2008.

[6] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, “On the capacity of secure network coding,” in *Proc. 42nd Annual Allerton Conference on Commun., Control, and Comput.*, 2004.

[7] K. Jain, “Security based on network topology against the wiretapping attack,” *IEEE Wireless Communications*, pp. 68–71, Feb. 2004.

[8] K. Bhattad and K. R. Narayanan, “Weakly secure network coding,” in *Proc. First Workshop on Network Coding, Theory, and Applications (NetCod’05)*, Apr. 2005.

[9] T. Ho, B. Leong, R. Koetter, M. Medard, M. Effros, and D. Karger, “Byzantine modification detection in multicast networks using randomized network coding,” in *Proc. 2004 IEEE International Symposium on Information Theory (ISIT’04)*, June 2004.

[10] S. Jaggi, M. Langberg, T. Ho, and M. Effros, “Correction of adversarial errors in networks,” in *Proc. IEEE International Symposium on Information Theory (ISIT’07)*, 2007.

[11] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Medard, “Resilient network coding in the presence of byzantine adversaries,” in *Proc. 26th IEEE International Conference on Computer Communications (INFOCOM’05)*, 2005.

[12] S. Jaggi, M. Langberg, S. Katti, T.Ho, D. Katabi, M. Medard, and M. Effros, “Resilient network coding in the presence of byzantine adversaries,” *IEEE Trans. Inform. Theory*, pp. 2596–2603, June 2008.

[13] N. Cai and R. W. Yeung, “Network error correction, part I: Basic concepts and upper bounds,” *Communications in Information and Systems*, no. 1, pp. 19–36, 2006.

[14] ——, “Network error correction, part II: Lower bounds,” *Communications in Information and Systems*, no. 1, pp. 37–53, 2006.

[15] R. Koetter and F. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. Inform. Theory*, pp. 3579–3591, Aug. 2008.

[16] D. Silva, R. Koetter, and F. Kschischang, “A rank-metric approach to error control in random network coding,” *IEEE Trans. Inform. Theory*, pp. 3951–3967, Aug. 2008.

[17] L. H. Ozarow and A. D. Wyner, “The wire-tap channel II,” *Bell Syst. Tech. Journ.*, vol. 63, pp. 2135–2157, 1984.

[18] ——, “Wire-tap channel II,” in *Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 33–51.

[19] S. Jaggi, P. Sanders, P. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Trans. Inform. Theory*, pp. 1973–1982, June 2005.

[20] C. Fragouli and E. Soljanin, “Information flow decomposition for network coding,” *IEEE Trans. Inform. Theory*, pp. 829–848, Mar. 2006.

[21] M. Langberg, A. Sprintson, and J. Bruck, “The encoding complexity of network coding,” *Information Theory, IEEE Transactions on*, vol. 52, no. 6, pp. 2386–2397, June 2006.

[22] ——, “Network coding: A computational perspective,” *IEEE Transactions on Information Theory*, vol. 55, no. 1, pp. 147–157, Jan. 2009.

[23] D. Silva and F. R. Kschischang, “Security for wiretap networks via rank-metric codes,” in *2008 IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Canada, Jul 2008.

[24] ——, “Universal secure network coding via rank-metric codes,” *arXiv:0809.3546v1*, 2008.

[25] A. Mills, B. Smith, T. C. Clancy, E. Soljanin, and S. Vishwanath, “On secure communication over wireless erasure networks,” in *2008 IEEE International Symposium on Information Theory (ISIT 2008)*, Toronto, Canada, Jul 2008.

[26] V. K. Wei, “Generalized Hamming weights for linear codes,” *IEEE Trans. Inform. Theory*, pp. 1412–1518, Sept. 1991.

[27] C.-K. Ngai, R. W. Yeung, and Z. Zhang, “Network generalized hamming weight,” in *2009 Workshop on Network Coding, Theory and Applications (NetCod 2009)*, Lausanne, Switzerland, June 2009.

[28] Z. Zhang, “Network error correction coding in packetized networks,” in *Proc. 2006 IEEE Int. Inform. Theory Workshop (ITW’06)*, Chengdu, China, Oct. 2006.

[29] S. Yang and R. W. Yeung, “Characterizations of network error correction/detection and erasure correction,” in *Proc. Third Workshop on Network Coding, Theory, and Applications (NetCod’07)*, San Diego, CA, Jan. 2007.

[30] C.-K. Ngai and R. W. Yeung, “Secure error-correcting (sec) network codes,” in *2009 Workshop on Network Coding, Theory and Applications (NetCod 2009)*, Lausanne, Switzerland, June 2009.