Abstract—This paper characterizes the secret message capacity of three networks where two unicast sessions share some of the communication resources. Each network consists of erasure channels with state feedback. A passive eavesdropper is assumed to wiretap any one of the links. The capacity achieving schemes as well as the outer bounds are formulated as linear programs. The proposed strategies are then numerically evaluated and shown to achieve higher rate performances (up to a double single- or sum-rate) with respect to alternative strategies, where the network resources are time-shared among the two sessions. These results represent a step towards the secure capacity characterization for general networks. They also show that, even in configurations for which network coding does not offer benefits in absence of security, it can become beneficial under security constraints.

I. INTRODUCTION

Secure network coding has well established the benefits of network coding for secure multicast transmission. We are here interested in a different type of traffic where we have two independent unicast sessions and we seek to answer the following question: what are the benefits that ‘network coding’ type operations offer?

We consider the three networks in Fig. 1 namely the Y-network, the Reverse Y (RY)-network and the X-network. In the Y-network two sources (able to generate randomness at infinite rate) wish to communicate two independent messages to a common destination, via an intermediate node (unable to generate randomness). In the RY-network one source (able to generate randomness at finite rate) aims to communicate two independent messages to two different receivers, through an intermediate node (unable to generate randomness). Finally, in the X-network two sources (able to generate randomness at infinite rate) seek to communicate two independent messages to two different receivers, via two intermediate nodes (unable to generate randomness). In our network model, the transmissions take place over orthogonal erasure channels; although this being a simplistic assumption, yet it captures some intrinsic properties of the wireless medium (such as its lossy nature). A passive eavesdropper wiretaps any one of the communication links, but the information about which one is not available. Public feedback, which in was shown to increase the secrecy capacity, is used, i.e., each of the legitimate nodes involved in the communication sends an acknowledgment after each transmission; this is received by all nodes in the network as well as by the eavesdropper.

We characterize the secret message capacity for the three networks in Fig. 1. The capacity-achieving schemes involve two phases: the key-sharing phase and the message-transmission phase. In particular, first a secret key is created between two consecutive legitimate nodes (link-by-link key generation); then, these keys are used to encrypt and transmit the message like in the one-time pad. For each of the analyzed networks, the capacity is given as the solution of a Linear Program (LP). We also show, through numerical simulations, the benefits of our schemes compared to two alternative strategies where (a) the two sessions are time-shared and (b) the shared link is time-shared among the two sessions. We prove that ‘network coding’ type operations are beneficial for the three networks in Fig. 1. This is because random packets transmitted by different sources can be mixed to create the key to be used on the shared link. Similarly, the same set of random packets can be used to generate secret keys for different destinations. This result is surprising since, in absence of security considerations, network coding is not beneficial for the networks in Fig. 1.

Related Work. The characterization of the secret capacity for wireless networks is a long-standing open problem. Relevant work includes, where the author derived the secret message capacity of the wiretap channel without feedback, and, where it was shown that secure network coding is optimal for wireless networks with error-free and unit capacity channels. The work presented in this paper follows a line of research which was pioneered by the authors in, where the secret capacity of the point-to-point channel was characterized and expressed as the solution of an LP. In particular, the capacity-
achieving scheme proposed by the authors consists of two phases, namely the key-sharing and the message-transmission phases. The same authors extended this approach to characterize the secret capacity of more complex networks, for example: (i) the parallel channel network where a source seeks to securely communicate a message to a destination through a number of independent parallel channels \[6\], and (ii) the V-network where two sources, which share a common randomness, aim to convey the same message to a common destination \[6\]. By using a similar approach, in \[7\] the authors derived the secret message capacity of the line network when the eavesdropper wiretaps one channel as well as all the channels. Recently, in \[8\] the authors considered a general network and designed two polynomial-time secure transmission schemes. Although the two schemes were not proven to be capacity-achieving, the work in \[8\] represents an attempt to characterize the secrecy capacity of an arbitrary network. Contrary to all these works, where a single unicast session was considered, here we study the case where two unicast sessions take place simultaneously and share part of the resources.

**Paper Organization.** Section \[II\] describes the three networks of interest, namely the Y-, the RY- and the X-network. Section \[III\] presents our main results, i.e., it characterizes the secret message capacity and it presents comparisons with alternative strategies. Finally, Section \[IV\] concludes the paper.

**II. System Model and Main Results**

**Notation.** With \([n_1 : n_2]\) we denote the set of integers from \(n_1\) to \(n_2\). For an index set \(\mathcal{A}\) we let \(Y_{\mathcal{A}} = \{Y_j : j \in \mathcal{A}\} ; \mathcal{A} \setminus B\) is the set of elements that belong to \(\mathcal{A}\) but not to \(B\). \(Y_i\) is a vector of length \(i\) with components \((Y_1, \ldots, Y_i)\).

We consider the three networks in Fig. \[I\] namely (i) the Y-network in Fig. \[I(a)\] where two sources \(S_1\) and \(S_2\) aim to communicate two independent messages \(W_1\) and \(W_2\) to a common destination \(D\); (ii) the RY-network in Fig. \[I(b)\] where one source \(S\) has a message \(W_1\) for destination \(D_1\) and a message \(W_2\) for destination \(D_2\); both in the Y- and in the RY-network the communication occurs through an intermediate/relay node \(M\); finally, we study (iii) the X-network in Fig. \[I(c)\] where two sources \(S_1\) and \(S_2\) seek to communicate two independent messages \(W_1\) and \(W_2\) to two different destinations \(D_1\) and \(D_2\) via two intermediate nodes \(M_1\) and \(M_2\).

Each communication link is an independent erasure channel with one legitimate receiver and one possible passive eavesdropper. In each network, the eavesdropper wiretaps one channel, which one exactly is not known. The erasure probabilities are denoted as \(\delta_j\) and \(\delta_E\), with \(j \in [1 : 3]\) for the Y- and the RY-network and \(j \in [1 : 5]\) for the X-network\[9\].

The \(j\)-th channel input at time instant \(i\), with \(i \in [1 : n]\) (where \(n\) is the total number of transmissions), is denoted as \(X_{ji} \in \mathbb{P}_q\) and referred to as a packet. Without loss of generality, in what follows we let \(L \log (q) = 1\), i.e., we express the rate in terms of packets. Similarly, \(Y_{ji}\) and \(Z_{ji}\) denote the outputs at the legitimate receiver and at the passive eavesdropper, respectively, on channel \(j\) at time \(i\).

For the three scenarios in Fig. \[I\] we assume public state feedback, i.e., each legitimate node sends an acknowledgment whether the packet transmission was successful, which is received by all other nodes as well as by the eavesdropper. We denote with \(F_{ji}\) the feedback of the transmission on channel \(j\) at time \(i\).

For the X-network in Fig. \[I(c)\] we have \[10\]

\[
\Pr \{Y_{[1:5]i}, Z_{[1:5]i} \mid X_{[1:5]i}\} = \prod_{j=1}^{5} \Pr \{Y_{ji} \mid X_{ji}\} \Pr \{Z_{ji} \mid X_{ji}\},
\]

\[
\Pr \{Y_{ji} \mid X_{ji}\} = \begin{cases} 1 - \delta_j, & Y_{ji} = X_{ji} \\ \delta_j, & Y_{ji} = \bot \end{cases},
\]

\[
\Pr \{Z_{ji} \mid X_{ji}\} = \begin{cases} 1 - \delta_E, & Z_{ji} = X_{ji} \\ \delta_E, & Z_{ji} = \bot \end{cases},
\]

where with \(\bot\) we denote the symbol of erasure.

We assume that the intermediate nodes are unable to generate private randomness. For the Y- and the X-network the sources \(S_1\) and \(S_2\) can generate private randomness \(\Theta_1\) and \(\Theta_2\) at infinite rate. Differently, for the RY-network the source \(S\) can generate private randomness at a finite rate \(D_0\). The messages \(W_1\) and \(W_2\) consist of \(N_1\) and \(N_2\) packets, respectively, and have to be reliably and securely decoded at the legitimate receiver.

**Definition 1.** For the X-network in Fig. \[I(c)\] a secure coding scheme with parameters \((N_1, N_2, n, \epsilon)\) consists of 5 encoding functions \(f_{ji}, j \in [1 : 5]\) for each \(i \in [1 : n]\) such that

\[X_{ji} = \begin{cases} f_{ji}(W_j, \Theta_j, F_{\mathcal{A}}^{j-1}) & \text{if } j \in [1 : 2] \\ f_{ji}(Y_j^{i-1}, Y_j^{i-1}, F_{\mathcal{A}}^{j-1}) & \text{if } j = 3 \\ f_{ji}(Y_j^{i-1}, F_{\mathcal{A}}^{j-1}) & \text{if } j \in [4 : 5] \end{cases},\]

where \(\mathcal{A} = [1 : 5]\), and of 2 decoding functions \(\phi_j\) such that \(D_j, j \in [1 : 2]\), can decode the message \(W_j\) with high probability, i.e., \(\Pr \{\phi_j(Y_j^{i+1}) \neq W_j\} < \epsilon\). Moreover, the messages \(W_1\) and \(W_2\) have to remain secret from the eavesdropper, i.e., \(I(W_1, W_2; Z_k) < \epsilon, \forall k \in [1 : 5]\). A non-negative rate pair \((R_1, R_2)\) is securely achievable if, for any \(\epsilon > 0\), there exists a secure coding scheme with parameters \((N_1, N_2, n, \epsilon)\) such that \(R_j < \frac{1}{n} N_j - \epsilon, \forall j \in [1 : 2]\).

The main contribution of this paper is the characterization of the secret message capacity region (the largest securely achievable rate pair \((R_1, R_2)\)) for the three networks in Fig. \[I\] as described in the next three theorems.

**Theorem 1.** The secret message capacity region of the Y-network in Fig. \[I(a)\] with unlimited private randomness at the sources \(S_1\) and \(S_2\) and no private randomness at the relay

\[3\]Although definitions are given only for the X-network, they straightforwardly extend to the Y- and the RY-network.

\[4\]The results here presented readily extend to the case when intermediate nodes can generate private randomness at finite rate. If intermediate nodes can generate randomness at infinite rate a naive link-by-link time sharing strategy would be capacity-achieving.
node \( M \) is the feasible region of the following LP:

\[
\begin{align*}
\text{max} & \quad g(R_1, R_2) \\
\text{s.t.} & \quad k_j \geq R_j \frac{1 - \delta_j}{1 - \delta_j}, \quad j \in [1 : 2] \\
& \quad k_3 \geq (R_1 + R_2) \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{R_1 + R_2} \frac{1 - \delta_3}{2 - \delta_3} \leq 1, \quad j \in [1 : 2] \\
& \quad R_1 + R_2 \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{k_3} \frac{1 - \delta_3}{2 - \delta_3} \leq 1 \\
& \quad k_3 \leq \left( \frac{k_3}{R_1 + R_2} + \frac{k_3}{k_3} \right) \frac{1 - \delta_3}{1 - \delta_3} \\
& \quad R_i, k_j \geq 0, \quad i \in [1 : 2], \quad j \in [1 : 3],
\end{align*}
\]

where \( g(R_1, R_2) \) can be any linear function of \((R_1, R_2)\).

**Theorem 2.** The secret message capacity region of the RY-network in Fig. 1(b) with limited private randomness of rate \( D_0 \) at the source \( S \) and no private randomness at the relay node \( M \), is the feasible region of the following LP:

\[
\begin{align*}
\text{max} & \quad g(R_1, R_2) \\
\text{s.t.} & \quad k_3 + (1 - \delta_3) = (R_1 + R_2) \frac{1 - \delta_3}{1 - \delta_3} \\
& \quad k_j \geq R_j \frac{1 - \delta_j}{1 - \delta_j}, \quad j \in [1 : 2] \\
& \quad k_3 \geq (R_1 + R_2) \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{R_1 + R_2} \frac{1 - \delta_3}{2 - \delta_3} \leq 1, \quad j \in [1 : 2] \\
& \quad R_1 + R_2 \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{k_3} \frac{1 - \delta_3}{2 - \delta_3} \leq 1 \\
& \quad k_3 \leq (D_0 - e) \frac{1 - \delta_3}{1 - \delta_3} \\
& \quad k_3 \leq (e + k_3) \frac{1 - \delta_3}{1 - \delta_3}, \quad j \in [1 : 2] \\
& \quad R_i, k_j \geq 0, \quad i \in [1 : 2], \quad j \in [1 : 3],
\end{align*}
\]

where \( g(R_1, R_2) \) can be any linear function of \((R_1, R_2)\).

**Theorem 3.** The secret message capacity region of the X-network in Fig. 1(c) with unlimited private randomness at the source \( S_1 \) and \( S_2 \) and no private randomness at the relay nodes \( M_1 \) and \( M_2 \), is the feasible region of the following LP:

\[
\begin{align*}
\text{max} & \quad g(R_1, R_2) \\
\text{s.t.} & \quad k_j \geq R_j \frac{1 - \delta_j}{1 - \delta_j}, \quad j \in [1 : 2] \\
& \quad k_3 + (1 - \delta_3) = (R_1 + R_2) \frac{1 - \delta_3}{1 - \delta_3} \\
& \quad k_j \geq R_j \frac{1 - \delta_j}{1 - \delta_j}, \quad j \in [4 : 5] \\
& \quad k_3 \geq (R_1 + R_2) \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{R_1 + R_2} \frac{1 - \delta_3}{2 - \delta_3} \leq 1, \quad j \in [1 : 2] \\
& \quad R_1 + R_2 \frac{1 - \delta_3}{1 - \delta_3} + \frac{k_3}{k_3} \frac{1 - \delta_3}{2 - \delta_3} \leq 1 \\
& \quad k_3 \leq (D_0 - e) \frac{1 - \delta_3}{1 - \delta_3} \\
& \quad k_3 \leq (e + k_3) \frac{1 - \delta_3}{1 - \delta_3}, \quad j \in [4 : 5] \\
& \quad R_i, k_j \geq 0, \quad i \in [1 : 2], \quad j \in [1 : 5],
\end{align*}
\]

where \( g(R_1, R_2) \) can be any linear function of \((R_1, R_2)\).

### III. Secure Capacity Characterization

We here describe the secure coding schemes\(^5\) and the outer bounds and formulate them as LPs. We then show through numerical evaluations the benefits (in terms of achievable secure rate) of our scheme with respect to two naive strategies: (i) **path sharing**, i.e., the whole communication resources are time-shared among the two sessions and (ii) **link sharing**, i.e., the shared link is time-shared among the two sessions.

**A. Achievability**

Our secure coding schemes for the networks in Fig. 1 consist of two phases, namely the key-sharing and the message-transmission. In what follows we describe these two phases and explain how these relate to the LPs in Theorems 2 and 3.

1) **The Y-network:** On channel \( j \in [1 : 2] \), source \( S_j \) sends \( \left( \frac{k_j}{R_j} \right) \) independent random packets generated from her private randomness (assumed to be infinite). Out of these, a total of \( k_j \) packets are received by the relay node \( M \), but not by the possible eavesdropper. We do not know exactly which packets, out of the \( \frac{k_j}{R_j} \) ones received by \( M \), are also received by the possible eavesdropper. However, out of the packets received by \( M \), we can always create \( k_j \) independent packets, which are also independent of the packets received by the possible eavesdropper. We do this by multiplying the \( k_j \) packets of \( M \) by an MDS code matrix of dimension \( \left[ \frac{k_j}{R_j} \right] \times [k_j] \). Thus, without loss of generality, we can assume that we always know which packets are received by the legitimate node and not by the possible eavesdropper, if we know their amount \( [k_j] \). All these packets are used to generate a secret key on channel \( j \in [1 : 2] \) between nodes \( S_j \) and \( M \) (key-sharing phase). These packets are then expanded by means of an MDS code matrix of size \( [k_j] \times [R_j] \) and used as in the one-time pad \( [2] \) to encrypt \( R_1 \) message packets, which are sent using the ARQ protocol (message-transmission phase). At the intermediate node \( M \) (assumed to be unable to generate any randomness) there are \( \left( \frac{k_j}{R_j} \right) \) available random packets (received from \( S_1 \) and \( S_2 \) on channels 1 and 2, respectively). By means of an MDS code these random packets are first expanded by a factor \( \frac{1}{1 - \delta_j} \), and then only \( \frac{k_j}{R_j} \) of them are sent to node \( D \). With this, the number of random packets received by \( D \), but not by the possible eavesdropper is \( k_3 \). These random packets are used to generate a secret key on channel 3 between nodes \( M \) and \( D \) (key-sharing phase). Similar to channels 1 and 2, also for channel 3 we expand these \( k_3 \) packets by means of an MDS code matrix of dimension \( [k_3] \times [R_1 + R_2] \) and then we use them to encrypt \( R_1 + R_2 \) message packets as in the one-time pad \( [2] \). These message packets are finally transmitted by using the ARQ protocol (message-transmission phase).

The scheme described above is equivalent to the LP in Theorem 1 where the variables \( R_1 \) and \( k_j \), with \( i \in [1 : 2] \) and \( j \in [1 : 3] \), represent the message rate for the pair \( S_i \) and the key created on channel \( j \), respectively. In particular: (i) the first and second inequalities are security constraints, i.e., they ensure that the key that is generated is greater than the key which is consumed, (ii) the third and fourth inequalities are time constraints, i.e., the length of the key generation phase

\(^5\) Since the encrypted packets are sent by using the ARQ protocol, the key consumed on channel \( j \in [1 : 3] \) (i.e., the number of packets received by the possible eavesdropper on that channel) is \( R_j \frac{1 - \delta_j}{1 - \delta_j} \), with \( R_3 = R_1 + R_2 \).
plus the length of the message sending phase cannot exceed the total available time; (iii) the fifth inequality follows since node $M$ has zero randomness and so the key that it can create is constrained by the randomness received from $S_1$ and $S_2$.

2) The RY-network: In [7], the authors showed that, in a line network where a node has limited randomness and the next node can generate randomness based on the one received from the previous node(s), a combination of ARQ and MDS coding is needed for optimally generating the key. Following this, on channel 3 of the RY-network, the source $S$ transmits $e$ independent random packets using the ARQ protocol. These packets are all received by the relay node $M$, while the possible eavesdropper receives a fraction $\frac{k_3}{1 - \delta_3}$ of them. By means of an MDS code, the remaining $(D_0 - e)$ random packets at the source $S$ are expanded by a factor $\frac{1}{1 - \delta_3}$ and then only $\frac{k_3}{1 - \delta_3}$ of them are sent to node $M$. Thus, the total number of packets received by the intermediate node $M$, but not by the possible eavesdropper is $k_3 + \frac{e}{1 - \delta_3}$. Similar to the Y-network, from the $e + \frac{k_3}{1 - \delta_3}$ independent random packets received by $M$, we generate $k_3 + \frac{e}{1 - \delta_3}$ packets. All these packets are used to generate a secret key on channel 3 between nodes $S$ and $M$ (key-sharing phase). They are then expanded by means of an MDS code matrix of size $[k_3 + 3e/1 - \delta_3] \times [R_1 + R_2]$ and used as the one-time pad [2] to encrypt $R_1 + R_2$ message packets, which are sent using the ARQ protocol (message-transmission phase).

At the relay node $M$ (assumed unable to generate any randomness) there are $(\frac{k_3}{1 - \delta_3} + e)$ available random packets (received from $S$ on channel 3). By means of an MDS code these random packets $\forall j \in [1 : 2]$ are first expanded by a factor $\frac{1}{1 - \delta_3}$ and then only $\frac{k_3}{1 - \delta_3}$ of them are sent to node $D_j$ on channel $j$. With this, the number of random packets received by $D_j$, but not by the possible eavesdropper is $k_j$. These packets are used to generate a secret key on channel $j$ between nodes $M$ and $D_j$ (key-sharing phase). These $k_j$ packets are then expanded by means of an MDS code matrix of dimension $[k_j] \times [R_j]$ and used to encrypt $R_j$ message packets as in the one-time pad [2]. These message packets are finally transmitted using ARQ (message-transmission phase).

Similar to the Y-network, also for the RY-network the secure transmission strategy above is equivalent to the LP in Theorem [2]. The variables $R_i$, $k_j$, and $e$, with $i \in [1 : 2]$ and $j \in [1 : 3]$, represent the message rate for the pair $S - D_i$, the key created on channel $j$, and the extra randomness (in addition to the one sent for generating the key $k_j$) sent from the source $S$, respectively. In particular: (i) the first and second inequalities are security constraints; (ii) the third and the fourth inequalities are time constraints; (iii) the fifth (respectively, sixth) inequality is due to the fact that the key that node $S$ (respectively, $M$) can create is constrained by its limited randomness (respectively, the randomness that it gets from $S$).

3) The X-network: The secure transmission strategy here proposed for the X-network in Fig. [1c] consists of a mix of the two schemes designed for the Y- and the RY-network. In particular, on channels 1 and 2 we use exactly the same operations used on channels 1 and 2 of the Y-network, while on channels 3-5 the same strategy proposed for the RY-network applies, with the small difference that the available finite randomness at node $S$ of the X-network (node $M_1$ in the X-network) is now replaced by $D_0 = \left( \frac{k_1}{\delta_1} + \frac{k_2}{\delta_2} \right)$.

B. Converse

We here highlight the main steps to derive an outer bound on the secure capacity for the networks in Fig. [1] and to formulate it as an LP; the complete proof can be found in the Appendix.

Step 1. We prove and make use of the following lemma (see Appendix A for the details), which is a generalization of those in [2] for the line network.

Lemma 4. For any $j \in A$, we have

\[
(1 - \delta_j) \sum_{i=1}^n \left( I(W_j; X_i | Y_{ji}^{-1}, Z_{ji}^{-1}, F_j^{-1}, W_B, F_{A,j}^n) - \right.
\]

\[
(1 - \delta_j) \sum_{i=1}^n \left( I(V_{ji}^{-1}, F_j^{-1}; X_i | Y_{ji}^{-1}, Z_{ji}^{-1}, F_j^{-1}, W_B, F_{A,j}^n) - \right.
\]

\[
= H(Y^n_j | W_B, F_{A,j}^n),
\]

\[
(1 - \delta_j) \sum_{i=1}^n \left( I(W_j; X_i | Y_{ji}^{-1}, Z_{ji}^{-1}, F_j^{-1}, W_B, F_{A,j}^n) - \right.
\]

\[
(1 - \delta_j) \sum_{i=1}^n \left( I(W_{ji}; X_i | Y_{ji}^{-1}, F_j^{-1}, W_B, F_{A,j}^n) - \right.
\]

\[
geq \frac{e}{1 - \delta_j},
\]

where: (i) for the Y-network $A = [1 : 3]$, $B = \{j\}$, $W_3 = W_{[1:2]}$ and $R_3 = R_1 + R_2$; (ii) for the RY-network $A = [1 : 3]$, $B = \{1 : 2\}$ and $R_3 = R_1 + R_2$; (iii) for the X-network $A = [1 : 5]$, $B = \{j\}$, $W_3 = W_4 = W_5 = W_{[1:2]}$, $R_3 = R_1 + R_2$, $R_4 = R_1$ and $R_5 = R_2$. Moreover, for node $D$ in the Y-network we have

\[
nR_3 \leq (1 - \delta_3) \sum_{i=1}^n I(W_1, W_2, X_{3i} | F_{A,j}^n, Y_{3i}^{-1}, F_{3i}^{-1}),
\]

for node $D_j$, $j \in [1 : 2]$ in the RY-network, we have

\[
nR_j \leq (1 - \delta_j) \sum_{i=1}^n I(W_j; X_i | F_{A,j}^n, Y_{ji}^{-1}, F_j^{-1}),
\]

and for node $D_j$, $j \in [1 : 2]$ in the X-network, we have

\[
nR_j \leq (1 - \delta_{j3}) \sum_{i=1}^n I(W_j; X_{j3i} | F_{A,j3}^n, Y_{j3i}^{-1}, F_{j3}^{-1}).
\]

Step 2. We use the correspondences between the terms in [2] at the top of the next page with: (i) $A = [1 : 3]$, $\kappa = 3$, $\lambda \in [1 : 2]$ and $W_3 = W_{[1:2]}$ for the Y-network; (ii) $A = [1 : 3]$, $j = 3$, $\kappa \in [1 : 2]$, $B = \{1 : 2\}$, $W_3 = W_{[1:2]}$ and $e_3 = e$ for the RY-network; (iii) $A = [1 : 5]$, $j = 3$, $\lambda \in [1 : 2]$, $\kappa \in [4 : 5]$, $B = \{j\}$, $W_3 = W_4 = W_5 = W_{[1:2]}$ and $e_3 = e$ for the X-network. All the
used only by one session; for example, for the X-network we
the whole communication resources, at each time instant, are

\[ \text{(1) } n k_j \leftrightarrow \frac{\delta_j (1 - \delta_j)}{\delta_j (1 - \delta_j)} \sum_{i=1}^{n} H \left( X_{ji} | Y_{ji}^{i-1}, Z_{ji}^{i-1}, F_j^{i-1}, W_B, F_{A\setminus j}^n \right) - H \left( Y_j^w | W_B, F_{A}^n \right), \]  \hspace{1cm} (2a)

\[ \text{(2) } n e_j \leftrightarrow \frac{1 - \delta_j \delta_B}{\delta_j (1 - \delta_j)} H \left( Y_j^w | W_B, F_{A}^n \right) - (1 - \delta_j) \sum_{i=1}^{n} H \left( X_{ji} | Y_{ji}^{i-1}, Z_{ji}^{i-1}, F_j^{i-1}, W_B \right), \]  \hspace{1cm} (2b)

\[ \text{(3) } n k_{\kappa} \leftrightarrow \delta_E (1 - \delta_E) \sum_{i=1}^{n} H \left( X_{\kappa i} | Y_{\kappa i}^{i-1}, Z_{\kappa i}^{i-1}, F_{\kappa}^{i-1}, W_1, W_2, F_{A\setminus \kappa}^n \right), \]  \hspace{1cm} (2c)

\[ \text{(4) } n k_{\lambda} \leftrightarrow \delta_E (1 - \delta_E) \sum_{i=1}^{n} H \left( X_{\lambda i} | Y_{\lambda i}^{i-1}, F_{\lambda}^{i-1}, W_\lambda, F_{A\setminus \lambda}^n \right). \]  \hspace{1cm} (2d)

quantities in \( \ref{2} \) are non-negative (see Appendix B-D for the
details).

**Step 3.** By using the correspondences in \( \ref{2} \), Lemma \( \ref{4} \) and
information theoretic properties we derive an outer bound on
the secure capacity (see Appendices B-D for the details). Each
constraint in the LPs in Theorems \( \ref{13} \) is proved to match an
outer bound.

**C. Numerical Evaluations**

We here compare the secrecy capacity performance of our
schemes in Theorems \( \ref{13} \) with respect to two naive strategies, i.e., the path sharing and the link sharing. In the path sharing
the whole communication resources, at each time instant, are
used only by one session; for example, for the X-network we
have a time-sharing between \( S_1 \cdot M_1 \cdot M_2 \cdot D_1 \) and \( S_2 \cdot M_1 \cdot M_2 \cdot D_2 \). Differently, in the link sharing strategy only the shared
communication link is time-shared among the two unicast
sessions; for example, in the X-network only the \( M_1 \cdot M_2 \) link
is time-shared. For both these strategies we do not allow
the source node that does not participate to act as a source
of randomness, e.g., for the X-network the random packets
sent by \( S_1 \) cannot be used to encrypt the message packets of
\( S_2 \). Fig. \( \ref{2} \) shows the performance (in terms of secrecy capacity
region) of these two time-sharing strategies and of our schemes
in Theorems \( \ref{13} \). From Fig. \( \ref{2} \) we observe that our schemes in
Theorems \( \ref{13} \) (solid line) achieve higher rates compared to the
two time-sharing strategies. Large rate gains are attained when,
for each channel, the eavesdropper receives almost everything
and the legitimate node receives almost no information. Under
these channel conditions, for the Y-network the individual rates
are double than those achieved by the link-sharing strategy; for
the RY- and X-network the sum-rate is twice than that of the
link-sharing scheme. In general, these gains follow since: (i)
in the Y-network \( S_1 \) and \( S_2 \) transmit random packets to \( M \)
and these can be mixed to create a key on the shared link;
(ii) in the RY-network the same set of random packets can
be used to generate keys for both the M-D1 and M-D2 links.
These factors decrease the number of random packets required
to be sent from the source(s) and implies that more message
packets can be carried. Finally, (iii) in the X-network we have
the benefits of both the Y- and RY-network.

**IV. Conclusions**

We characterized the secret capacity for networks where
two unicast sessions share one communication link. This was
attained by designing schemes and by deriving outer bounds
which were formulated as LPs. Through numerical evaluations
we showed that our transmission strategies achieve higher rates
compared to schemes where the communication resources are
time-shared among the two sessions. These results show that,
even in network configurations for which network coding
does not offer benefits in absence of security, it can become
beneficial under security constraints.

**APPENDIX A**
**PROOF OF LEMMA \( \ref{4} \)**

We here prove the result in Lemma \( \ref{4} \). We start by analyzing
the Y-network. We have, \( \forall j \in \mathcal{A} = [1 : 3] \) and with \( W_3 = \)
where: (i) the equality in (a) follows from the chain rule of the entropy; (ii) the equality in (b) is due to the definition of mutual information; (iii) finally, the equality in (c) is because $F_{ji}$ is independent of the rest of the random variables. By recursively proceeding in the same way for $H(Y_{j | A}^n | F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1})$, we get the result in (a). We now prove (b) which is similar to (a).

We have, $\forall j \in A = [1 : 3]$ and with $W_3 = W_{[1:2]}$, 

$$H(Y_j^n | W_j, F_{A}^n) = H(Y_j^n, F_j^n | W_j, F_{A}^n)$$

\[= (a) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A}^n) + H(Y_{jn} | W_j, F_{A}^n, Y_j^{n-1}) \]

\[= (b) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A \setminus j}^n, F_{j}^{n-1}) - I(Y_j^{n-1}, F_j^{n-1}; Y_{jn} | W_j, F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1}) + H(Y_{jn} | W_j, F_{A}^n, Y_j^{n-1}) \]

\[= (c) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A \setminus j}^n, F_{j}^{n-1}) - I(Y_j^{n-1}, F_j^{n-1}; Y_{jn} | W_j, F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1}) + H(Y_{jn} | W_j, F_{A}^n, X_j, F_{A \setminus j}^n, F_{j}^{n-1}) \]

\[= \sum_{i=1}^{n} (1 - \delta_{j,i}) I(W_j; X_{ji} | F_{A \setminus j}^n, F_{j}^{n-1}, Z_{j}^{n-1}) \]

By means of similar steps, it is not difficult to prove the result in (a) and (b) for the Y-network. We have, $\forall j \in A = [1 : 3]$ and with $W_3 = W_{[1:2]}$, 

$$H(Y_j^n | W_j, F_{A}^n) = H(Y_j^n, F_j^n | W_j, F_{A}^n)$$

\[= (a) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A}^n) + H(Y_{jn} | W_j, F_{A}^n, Y_j^{n-1}) \]

\[= (b) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A \setminus j}^n, F_{j}^{n-1}) - I(Y_j^{n-1}, F_j^{n-1}; Y_{jn} | W_j, F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1}) + H(Y_{jn} | W_j, F_{A}^n, Y_j^{n-1}) \]

\[= (c) H(Y_j^{n-1}, F_j^{n-1} | W_j, F_{A \setminus j}^n, F_{j}^{n-1}) - I(Y_j^{n-1}, F_j^{n-1}; Y_{jn} | W_j, F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1}) + H(Y_{jn} | W_j, F_{A}^n, X_j, F_{A \setminus j}^n, F_{j}^{n-1}) \]

\[= \sum_{i=1}^{n} (1 - \delta_{j,i}) I(W_j; X_{ji} | F_{A \setminus j}^n, F_{j}^{n-1}, Z_{j}^{n-1}) \]

where: (i) the inequality in (a) is due to the Fano’s inequality; (ii) the equality in (b) follows from the Markov chain $W_j \rightarrow Y_j^n, F_{A \setminus j}^n, Z_{j}^{n-1}, F_{j}^{n-1}$ for $j \in [1 : 2]$; (iii) the equality in (c) is due to the chain rule of the mutual information; (iv) the inequality in (d) is because the mutual information is a non-negative quantity; (v) the equality in (e) follows from the independence of $W_j$ and $F_{A \setminus j}^n$; (vi) the equality in (f) is due to the chain rule of the mutual information; (vii) finally, the equality in (g) follows from the independence of $W_j$ on $F_{A \setminus j}^n$. This proves (a) for the Y-network. By means of similar steps, it is not difficult to prove the result in (a) for the X-network.

Finally, for node D in the Y-network we have 

$$n(R_{1} + R_{2})$$
\[ (a) \quad I(W_1, W_2; Y_3, F_3^n) + n\epsilon \]
\[ = I(W_1, W_2; Y_3, F_3^n | F_{A\setminus 3}) + n\epsilon \]
\[ \geq \sum_{i=1}^{n} I(W_1, W_2; Y_3 | Y_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) + n\epsilon \]
\[ = (1 - \delta_3) \sum_{i=1}^{n} I(W_1, W_2; X_{3i} | Y_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) + n\epsilon, \]

where: (i) the inequality in (a) is due to the Fano’s inequality; (ii) the equality in (b) follows from the independence of the pair \((W_1, W_2)\) on \(F_{A\setminus 3}\); (iii) the equality in (c) is due to the chain rule of the mutual information; (iv) finally, the equality in (d) follows from the independence of the pair \((W_1, W_2)\) on \(F_{A\setminus 3}\). This proves (1b) for the Y-network. By means of similar steps, it is not difficult to prove the results in (1c) and (1g) for the RY- and X-network, respectively.

**APPENDIX B**

**PROOF OF THE CONVERSE OF THEOREM 1**

For the Y-network, in (2a) we set \( \mathcal{A} = [1 : 3], \lambda = 3 \) and \( \kappa = 3 \). We use (2a) and (2b) for proving the converse of Theorem 1. The RHS of these two expressions is positive as the entropy of a discrete random variable is positive.

**First constraint.** From (2a) we have

\[ nK_{\lambda} \]
\[ = \delta_{\lambda} (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Y_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ \geq \delta_{\lambda} (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ \geq \delta_{\lambda} (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ - H(Y_3^n | W_3, F_{A\setminus 3}^n, Z_3^n) \]
\[ \geq (1 - \delta_{\lambda}) \sum_{i=1}^{n} I(Y_3^{i-1}, F_3^{i-1}; X_{3i} | Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ \geq (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ - \sum_{i=1}^{n} H(X_{3i} | Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n, Y_3^{i-1}) \]
\[ \geq (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ - \sum_{i=1}^{n} H(X_{3i}; W_{3i} | Z_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) \]
\[ \geq (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Z_3^{i-1}, F_3^{i-1}, W_{3i}, F_{A\setminus 3}^n) \]
\[ - \sum_{i=1}^{n} H(X_{3i}; W_{3i} | Z_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) \]
\[ \geq (1 - \delta_{\lambda}) \sum_{i=1}^{n} H(X_{3i} | Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) \]
\[ - \sum_{i=1}^{n} I(X_{3i}; W_{3i} | Z_3^{i-1}, F_3^{i-1}, F_{A\setminus 3}^n) \]

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to (1a) in Lemma 4; (iii) the equality in (c) is due to the definition of mutual information; (iv) the equality in (d) follows from the definition of mutual information; (v) the inequality in (e) follows from the ‘conditioning reduces the entropy’ principle; (vi) the equality in (f) is due to the definition of mutual information; (vii) finally, the inequality in (g) follows by means of (1c) and (1d) in Lemma 4.
where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to (1a) in Lemma 3; (iii) the equality in (c) is due to the definition of mutual information; (iv) the inequality in (d) follows from the definition of mutual information; (v) the inequality in (e) follows from the ‘conditioning reduces the entropy’ principle; (vi) finally, the equality in (f) follows by means of (1c) and (1d) in Lemma 4 with $R_3 = R_1 + R_2$.

**Third constraint.** From (2d) we get

$$\frac{n k_3}{\delta_{3E}} = \left(1 - \delta_3 \right) \sum_{i=1}^{n} H \left( X_{3i} | Y_{3i}^{i-1}, F_{3i}^{i-1}, W_3, F_{A \setminus 3} \right) \leq \left(1 - \delta_3 \right) n - \frac{\epsilon}{1 - \delta_{3E}}$$

where the last equality follows from (1b) in Lemma 4.

Using this and Fano’s inequality with $\lambda \in [1 : 2]$ we have

$$n R_{\lambda} + \frac{n k_3}{\delta_{3E}} \leq I \left( W_1 ; Y_1^n , F_{A}^n \right) + H \left( Y_1^n | W_1 , F_{A} \right) + n \epsilon \quad (a)$$

$$\leq I \left( W_1 ; Y_1^n , F_{A}^n \right) + H \left( Y_1^n | W_1 , F_{A} \right) + n \epsilon \quad (b)$$

$$= I \left( W_1 ; Y_1^n , F_{A}^n \right) + H \left( Y_1^n | W_1 , F_{A} \right) + n \epsilon \quad (c)$$

$$\leq \left(1 - \delta_3 \right) n + \frac{\epsilon}{1 - \delta_{3E}} \quad (d)$$

where: (i) the inequality in (a) follows because of the Markov chain $W_1 \rightarrow Y_1^n , F_{A}^n \rightarrow Y_3^n \forall \lambda \in [1 : 2]$; (ii) the equality in (b) follows because of the independence between $F_{A}$ and $W_1$; (iii) the equality in (c) follows from the definition of mutual information; (iv) finally, the inequality in (d) follows since node M receives at most $n \left(1 - \delta_3 \right)$ packets on channel $\lambda \in [1 : 2]$.

**Fourth constraint.** From (1c) in Lemma 4 we have

$$n \left( R_1 + R_2 \right) \leq \left(1 - \delta_3 \right) \sum_{i=1}^{n} I \left( W_{1i} ; X_{3i} | F_{A \setminus 3} , Y_3^{i-1} , F_3^{i-1} \right)$$

$$\quad \leq \left(1 - \delta_3 \right) \sum_{i=1}^{n} H \left( X_{3i} | F_{A \setminus 3} , Y_3^{i-1} , F_3^{i-1} \right)$$

$$\quad - \frac{\sum_{i=1}^{n} H \left( X_{3i} | F_{A \setminus 3} , Y_3^{i-1} , F_3^{i-1} , W_{1i} \right)}{\delta_{3E}} \quad (a)$$

where: (i) the inequality in (a) follows from the definition of mutual information; (ii) the inequality in (b) follows since $H \left( X , Y \right) \leq H \left( X \right) + H \left( Y \right)$; (iii) the inequality in (c) follows since the entropy of a discrete random variable is a positive quantity; (iv) the equality in (d) is due to the chain rule of the mutual information; (v) the equality in (e) follows since node M does not have any randomness and so $X_{3i}$ is uniquely determined by knowing $(Y_1^n , Y_2^n , F_{A})$; (vi) the equality in (f) is due to the Markov chain $X_{3i}$ –
$W_1, W_2, F_{A\setminus 3}^n, Y_3^{i-1}, F_3^{i-1}, Z_3^{i-1} - F_3$, (vii) finally, the equality in (e) follows from (23).

APPENDIX C

PROOF OF THE CONVERSE OF THEOREM 2

For the RY-network, in (2) we set $A = [1 : 3], j = 3, \kappa \in [1 : 2], B = [1 : 2]$ and $e_3 = e$. We start by proving that the Right-Hand Side (RHS) of the quantities in (2) is positive. We use (23), (28) and (29) for proving the converse of Theorem 2. The RHS of (23) is positive as the entropy of a discrete random variable is positive. For the RHS of (28), we have

$$(1 - \delta_3 \delta_{3\epsilon}) \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, W_{[1:2]}, F_{A\setminus 3}^n\right)$$

$$- H\left(Y_3^n \mid W_{[1:2]}, F_{A\setminus 3}^n\right)$$

$$(a) \sum_{i=1}^n H\left(Y_{3i}, Z_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, W_{[1:2]}, F_{A\setminus 3}^n\right)$$

$$- H\left(Y_3^n \mid W_{[1:2]}, F_{A\setminus 3}^n\right)$$

$$(b) \left[ H\left(Y_3^n, Z_3^n \mid W_{[1:2]}, F_{A\setminus 3}^n\right) - H\left(Y_3^n \mid W_{[1:2]}, F_{A\setminus 3}^n\right) \right]$$

where: (i) the equality in (a) follows because given $F_{3i}$, the pair $(Y_{3i}, Z_{3i})$ is equal to $X_{3i}$, with probability $(1 - \delta_3 \delta_{3\epsilon})$ and null otherwise and because of the Markov chain $X_{3i} \rightarrow W_{[1:2]}, F_{A\setminus 3}^n, Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1} - F_3$; (ii) finally, the equality in (b) is due to the chain rule of entropy.

For the RHS of (28), we have

$H\left(Y_3^n \mid W_{[1:2]}, F_{A\setminus 3}^n\right)$

$$(1 - \delta_3) \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}^n, F_3^{i-1}, W_{[1:2]}\right)$$

$$(a) \sum_{i=1}^n H\left(Y_{3i} \mid W_{[1:2]}, F_{A\setminus 3}, Y_3^{i-1}\right)$$

$$- (1 - \delta_3) \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}, F_3^{i-1}, W_{[1:2]}\right)$$

$$(b) \sum_{i=1}^n H\left(Y_{3i} \mid W_{[1:2]}, F_{A\setminus 3}, Y_3^{i-1}, Z_3^{i-1}\right)$$

$$- (1 - \delta_3) \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}, F_3^{i-1}, W_{[1:2]}\right)$$

$$(c) \left[ \sum_{i=1}^n H\left(X_{3i} \mid W_{[1:2]}, F_{A\setminus 3}, Y_3^{i-1}, Z_3^{i-1}, F_3^{i-1}, F_{3i}\right) \right]$$

$$- \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}, F_3^{i-1}, W_{[1:2]}\right)$$

$$(d) \left[ \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}, F_3^{i-1}, W_{[1:2]}\right) \right]$$

$$- \sum_{i=1}^n H\left(X_{3i} \mid Y_3^{i-1}, Z_3^{i-1}, F_{A\setminus 3}, F_3^{i-1}, F_{A\setminus 3}\right)$$

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to (1a) in Lemma 4; (iii) the equality in (c) is due to the definition of mutual information; (iv) the equality in (d) follows from the definition of mutual information; (v) the inequality in (e) follows from the conditioning reduces
the entropy principle; (vi) the equality in (f) is due to the definition of mutual information; (vii) finally, the inequality in (g) follows by means of (1c) and (1d) in Lemma 4.

Second constraint. From (2c) we have

\[
nk \leq \delta_{E} \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | Y_{i}^{i-1}, z_{ki}^{i-1}, F_{nk}, W_{i}[1:2], F_{\lambda|\kappa}^{n} \right)
\]

(a) \[
\geq \delta_{E} \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | Y_{i}^{i-1}, z_{ki}^{i-1}, F_{nk}, W_{i}[1:2], F_{\lambda|\kappa}^{n} \right)
\]

(b) \[
\geq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} I \left( Y_{i}^{i-1}, F_{nk}^{i-1}, X_{ni} | z_{ki}^{i-1}, F_{nk}, W_{i}[1:2], F_{\lambda|\kappa}^{n} \right)
\]

(c) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | z_{ki}^{i-1}, F_{nk}^{i-1}, W_{i}[1:2], F_{\lambda|\kappa}^{n} \right)
\]

(d) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} I \left( X_{ni}, W_{[1:2]} | z_{ki}^{i-1}, F_{nk}^{i-1}, F_{\lambda|\kappa}^{n} \right)
\]

(e) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | Y_{i}^{i-1}, z_{ki}^{i-1}, F_{nk}, W_{i}[1:2], F_{\lambda|\kappa}^{n} \right)
\]

(f) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} I \left( X_{ni}, W_{[1:2]} | Y_{i}^{i-1}, z_{ki}^{i-1}, F_{nk}, F_{\lambda|\kappa}^{n} \right)
\]

(g) \[
\geq nR_{\lambda} \frac{1 - \delta_{E} \delta_{E | \kappa}}{1 - \delta_{E} \delta_{E | \kappa}} - \epsilon,
\]

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to (3a) in Lemma 4; (iii) the equality in (c) is due to the definition of mutual information; (iv) the equality in (d) follows from the definition of mutual information; (v) the inequality in (e) follows from the ‘conditioning reduces the entropy’ principle; (vi) the equality in (f) is due to the definition of mutual information; (vii) finally, the inequality in (g) follows by means of (1e) and (1d) in Lemma 4.

Third constraint. From (2a) and (2b) we get

\[
n \left( R_{1} + R_{2} \right) + ne + \frac{n \kappa}{\delta_{E}} = H \left( Y_{i}^{i+1}, W_{[1:2]}, F_{\lambda|\kappa}^{n} \right) \leq H \left( Y_{i}^{i+1}, W_{[1:2]}, F_{\lambda|\kappa}^{n} \right) + H \left( Y_{i}^{i+1}, W_{[1:2]}, F_{\lambda|\kappa}^{n} \right) + ne
\]

where: (i) the inequality in (a) follows because of the Markov chain \( W_{[1:2]} \rightarrow Y_{i}^{i+1} \rightarrow F_{\lambda|\kappa}^{n} \); (ii) the equality in (b) follows because of the independence between \( F_{\lambda|\kappa}^{n} \) and \( (W_{1}, W_{2}) \); (iii) the equality in (c) follows from the definition of mutual information; (iv) finally, the inequality in (d) follows since node M receives at most \( n \left( 1 - \delta_{E} \right) \) packets.

Fourth constraint. From (11) in Lemma 4 we have

\[
nR_{\lambda} \leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} I \left( W_{ni}; X_{ni} | F_{nk}^{ni}, y_{i}^{i-1}, f_{nk}^{i-1} \right)
\]

(a) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | F_{nk}^{ni}, y_{i}^{i-1}, f_{nk}^{i-1} \right)
\]

(b) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | F_{nk}^{ni}, y_{i}^{i-1}, f_{nk}^{i-1}, W_{i}[1:2] \right)
\]

(c) \[
\leq \left( 1 - \delta_{E} \right) \sum_{i=1}^{n} H \left( X_{ni} | F_{nk}^{ni}, y_{i}^{i-1}, f_{nk}^{i-1}, W_{i}[1:2], z_{ki}^{i-1} \right)
\]

(d) \[
\leq \left( 1 - \delta_{E} \right) n - \frac{\kappa}{\delta_{E}} n,
\]

where: (i) the inequality in (a) follows from the definition of mutual information; (ii) the inequality in (b) is due to the fact that \( H \left( X_{ni} \right) \leq 1 \); (iii) the inequality in (c) is due to the ‘conditioning reduces the entropy’ principle; (iv) finally, the equality in (d) follows from (2c).

Fifth constraint. The node S has a discrete source of randomness \( U_{0} \) such that

\[
nD_{0} = H \left( U_{0} \right)
\]

(a) \[
\leq H \left( U_{0} | W_{[1:2]}, F_{\lambda|\kappa}^{n} \right)
\]

(b) \[
\geq I \left( U_{0}; Y_{3}^{n}, z_{3}^{n}, f_{33}^{n} | W_{[1:2]}, F_{\lambda|\kappa}^{n} \right)
\]
follows from (2a) and (2b).

where: (i) the equality in (a) follows because of the independence between $(X_n, F, Y, W)$; (ii) the inequality in (b) follows since the entropy of a discrete random variable is positive; (iii) the equality in (c) is due to the chain rule of the mutual information; (iv) the equality in (d) follows because of the dependence between $X_n$ and $U_0$; (v) the equality in (e) follows because $X_n$ is uniquely determined given $(U_0, W, Z, F)$; (vi) finally, the equality in (f) follows from (2a) and (2b).

**Sixth constraint.** From (2a) and (2b) we have

\[
\begin{align*}
&\sum_{i=1}^{n} I \left( U_0; Y_{si}, Z_{si} | W_{[1:2]}, F_{A \setminus 3}^{n}, Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{-1} \right) \\
= &\sum_{i=1}^{n} I \left( U_0; Y_{si}, Z_{si} | W_{[1:2]}, F_{A \setminus 3}^{n}, Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{-1} \right) \\
= &\frac{(1 - \delta_3)\delta_3}{\delta_3} \cdot n k_3 + n e,
\end{align*}
\]

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to the chain rule of the mutual information; (iii) the equality in (c) follows since $X_{ni}$ (with $\kappa \in [1 : 2]$) is uniquely determined given $(Y_n, F^\kappa)$; (iv) the inequality in (d) follows because of the Markov chain $X_{ni} - W_{[1:2]}, F_{A \setminus 3}^{n}, Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{-1} - F_{ni}$; (v) finally, the equality in (e) follows from (2c).

**Appendix D**

**Proof of the converse of Theorem 3**

For the X-network, in (2) we set $A = [1 : 5]$, $\lambda \in [1 : 2]$, $j = 3, \kappa \in [4 : 5], B = \{j\}$, $W_3 = W_4 = W_5 = W_{[1:2]}$ and $e_3 = e$. We start by proving that the Right-Hand Side (RHS) of the quantities in (2) is positive. It is straightforward to see that the RHS of (2a) and (2b) is positive as the entropy of a discrete random variable is positive. For the RHS of (2a) we have

\[
\begin{align*}
(1 - \delta_3)\delta_3 \sum_{i=1}^{n} H \left( X_{ji} | Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{-1}, W_j, F_{A \setminus j}^{n} \right) \\
- H \left( Y_n | W_j, F_{A}^{n} \right) \\
\geq (a) \sum_{i=1}^{n} H \left( Y_{ji}, Z_{ji} | Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{n}, W_j, F_{A \setminus j}^{n} \right) \\
- H \left( Y_n | W_j, F_{A}^{n} \right) \\
\geq (b) \left( Y_n, Z_n | F_{j}^{n}, W_j, F_{A \setminus j}^{n} \right) - H \left( Y_n | W_j, F_{A}^{n} \right) \geq 0,
\end{align*}
\]

where: (i) the equality in (a) follows because given $F_{ji}$, $(Y_{ji}, Z_{ji})$ is equal to $X_{ji}$ with probability $(1 - \delta_3)\delta_3$ and null otherwise and because of the Markov chain $X_{ji} - W_j, F_{A \setminus j}^{n}, Y_{ji}^{-1}, Z_{ji}^{-1}, F_{ji}^{-1} - F_{ni}$; (ii) finally, the equality in (b) is due to the chain rule of entropy.

For the RHS of (2b) we have

\[
\begin{align*}
H \left( Y_n | W_j, F_{A}^{n} \right) \\
- (1 - \delta_3)\delta_3 \sum_{i=1}^{n} H \left( X_{ji} | Y_{j}^{-1}, Z_{j}^{-1}, F_{A \setminus j}^{n}, F_{j}^{-1}, W_j \right) \\
\geq (a) \sum_{i=1}^{n} H \left( Y_{ji}, Z_{ji} | Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{n}, W_j, F_{A \setminus j}^{n} \right) \\
- (1 - \delta_3)\delta_3 \sum_{i=1}^{n} H \left( X_{ji} | Y_{j}^{-1}, Z_{j}^{-1}, F_{A \setminus j}^{n}, F_{j}^{-1}, W_j \right) \\
\geq (b) \left( Y_n, Z_n | F_{j}^{n}, W_j, F_{A \setminus j}^{n} \right) - H \left( Y_n | W_j, F_{A}^{n} \right) \geq 0,
\end{align*}
\]

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to the chain rule of mutual information; (iii) the equality in (c) follows since $X_{ni}$ (with $\kappa \in [1 : 2]$) is uniquely determined given $(Y_n, F^\kappa)$; (iv) the equality in (d) follows because of the Markov chain $X_{ni} - W_{[1:2]}, F_{A \setminus 3}^{n}, Y_{j}^{-1}, Z_{j}^{-1}, F_{j}^{-1} - F_{ni}$; (v) finally, the equality in (e) follows from (2c).
\[-\sum_{i=1}^{n} H \left( X_{ji}, Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{A\lambda j}^{n}, F_{j-i}^{n}, W_{j} \right) = 0,\]

where: (i) the equality in (a) follows from the chain rule of the entropy; (ii) the inequality in (b) is due to the ‘conditioning reduces the entropy’ principle; (iii) finally, the equality in (c) follows because of the Markov chain $X_{ji} - W_j, F_{A\lambda j}^{n}, Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, F_{j-i}^{n}$.

**First to third constraints.** From (2d), $\forall j \in [1 : 2]$

$$nk_j = \delta_{JE} (1 - \delta_j) \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right)$$

$$\geq \delta_{JE} (1 - \delta_j) \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right),$$

where the inequality follows from the ‘conditioning reduces the entropy’ principle. From (2e), $\forall j \in [4 : 5]$

$$nk_j = \delta_{JE} (1 - \delta_j) \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right).$$

From (2a) and (2b) with $j = 3$

$$nk_j + c \left( 1 - \delta_j \right) \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right).$$

Thus, $\forall j \in [1 : 5]$ with $R_3 = R_1 + R_2, R_4 = R_1, R_5 = R_2$ and $c_1 = c_2 = c_4 = c_5 = 0$, we have

$$nk_j + nc \left( 1 - \delta_j \right) \delta_{JE} \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right)$$

$$\geq \delta_{JE} (1 - \delta_j) \sum_{i=1}^{n} H \left( X_{ji} \mid Y_{j-i}^{-1}, Z_{j-i}^{-1}, F_{j-i}^{n}, W_j, F_{A\lambda j}^{n} \right)$$

By means of (1g) in Lemma 4 we obtain

$$nR_{\lambda} + \frac{nk_{\lambda}}{\delta_{AE}} \leq I \left( W_{\lambda}; Y_{X-3}^{n}, F_{A\lambda}^{n} \right) + H \left( Y_{X-3}^{n} \mid W_{\lambda}, F_{A\lambda}^{n} \right)$$

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to (1a) in Lemma 4; (iii) the equality in (c) is due to the definition of mutual information; (iv) the equality in (d) follows from the definition of mutual information; (v) the inequality in (e) follows from the ‘conditioning reduces the entropy’ principle; (vi) the equality in (f) is due to the definition of mutual information; (vii) finally, the inequality in (g) follows by means of (1a) and (1b) in Lemma 4.

**Fourth constraint.** From (2d) and (1b), we have $\delta_{AE} = H \left( Y_{X-3}^{n} \mid W_{\lambda}, F_{A\lambda}^{n} \right)$. By using this and Fano’s inequality we have

$$nR_{\lambda} + \frac{nk_{\lambda}}{\delta_{AE}} \leq I \left( W_{\lambda}; Y_{X-3}^{n}, F_{A\lambda}^{n} \right) + H \left( Y_{X-3}^{n} \mid W_{\lambda}, F_{A\lambda}^{n} \right).$$

where: (i) the inequality in (a) follows because of the Markov chain $W_{\lambda} - Y_{X-3}^{n}, F_{A\lambda}^{n} - Y_{X-3}^{n}$; (ii) the inequality in (b) follows because of the Markov chain $W_{\lambda} - Y_{X-3}^{n}, F_{A\lambda}^{n} - Y_{X-3}^{n}$; (iii) the equality in (c) follows because of the independence between $F_{A\lambda}^{n}$ and $W_{\lambda}$; (iv) the equality in (d) follows from the definition of mutual information; (v) finally, the inequality in (e) follows since node $M_1$ receives at most $n (1 - \delta_{\lambda})$ packets on channel $\lambda \in [1 : 2]$.

**Fifth constraint.** By means of (1g) in Lemma 4 we obtain

$$nR_{\lambda} \leq (1 - \delta_{\lambda+3}) \sum_{i=1}^{n} I \left( W_{\lambda}; X_{\lambda+3i} \mid F_{A\lambda+3i}^{n}, Y_{\lambda+3i}^{n}, F_{\lambda+3i}^{n} \right)$$

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to the definition of mutual information; (iii) the equality in (c) follows because of the Markov chain $W_{\lambda} - Y_{X-3}^{n}, F_{A\lambda}^{n} - Y_{X-3}^{n}$; (iv) the inequality in (d) follows from the definition of mutual information; (v) finally, the inequality in (e) follows since node $M_1$ receives at most $n (1 - \delta_{\lambda})$ packets on channel $\lambda \in [1 : 2]$. 

**Fifth constraint.** By means of (1g) in Lemma 4 we obtain

$$nR_{\lambda} \leq (1 - \delta_{\lambda+3}) \sum_{i=1}^{n} I \left( W_{\lambda}; X_{\lambda+3i} \mid F_{A\lambda+3i}^{n}, Y_{\lambda+3i}^{n}, F_{\lambda+3i}^{n} \right)$$

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to the definition of mutual information; (iii) the equality in (c) follows because of the Markov chain $W_{\lambda} - Y_{X-3}^{n}, F_{A\lambda}^{n} - Y_{X-3}^{n}$; (iv) the inequality in (d) follows from the definition of mutual information; (v) finally, the inequality in (e) follows since node $M_1$ receives at most $n (1 - \delta_{\lambda})$ packets on channel $\lambda \in [1 : 2]$.
where: (i) the equality in (a) follows from the definition of mutual information; (ii) the inequality in (b) is because $H(X_{\lambda+3}) \leq 1$ and because of the `conditioning reduces the entropy’ principle; (iii) finally, the equality in (c) follows by using (2c).

Sixth constraint. From (2a) and (2b) we have $n c_3 + \frac{n k_3}{\delta_{HE}} = H(Y^n_3 | W_{[1:2]}, F^n_3)$. By using this and Fano’s inequality we have

$$n (R_1 + R_2) + n c_3 + \frac{n k_3}{\delta_{HE}} \leq I(W_{[1:2]}, Y^n_3, Z^n_3, F^n_3) + H(Y^n_3 | W_{[1:2]}, F^n_3) + n \epsilon$$

(a) $\leq I(W_{[1:2]}, Y^n_3, F^n_3) + H(Y^n_3 | W_{[1:2]}, F^n_3) + n \epsilon$

(b) $\leq I(W_{[1:2]}, Y^n_3 | F^n_3) + H(Y^n_3 | W_{[1:2]}, F^n_3) + n \epsilon$

(c) $= H(Y^n_3 | F^n_3) + n \epsilon$

(d) $\leq n (1 - \delta_3) + n \epsilon,$

where: (i) the inequality in (a) follows because of the Markov chain $W_1, W_2 - Y^n_3, F^n_3 - Y^n_3, Y^n_3$; (ii) the equality in (b) follows because of the independence between $F^n_3$ and $(W_1, W_2)$; (iii) the equality in (c) follows from the definition of mutual information; (iv) finally, the inequality in (d) follows since node $M_2$ receives at most $n (1 - \delta_3)$ packets.

Seventh constraint. From (2d) and (16) we have

$$n \left( \frac{k_1}{\delta_{HE}} + \frac{k_2}{\delta_{HE}} \right) \frac{(1 - \delta_3) \delta_{HE}}{1 - \delta_3 \delta_{HE}} \leq \frac{1 - \delta_3 \delta_{HE}}{1 - \delta_3 \delta_{HE}} \left[ H(Y^n_1 | W_1, F^n_3) + H(Y^n_2 | W_2, F^n_3) \right]$$

(a) $\geq I(Y^n_1 | W_1, F^n_3)$

(b) $\geq I(Y^n_2 | W_2, F^n_3)$

(c) $\geq \frac{(1 - \delta_3) \delta_{HE}}{1 - \delta_3 \delta_{HE}} I(Y^n_1, Y^n_2; Z^n_3, Y^n_3 | W_{[1:2]}, F^n_3)$

(d) $\geq \frac{(1 - \delta_3) \delta_{HE}}{1 - \delta_3 \delta_{HE}} I(Y^n_1, Y^n_2; Z^n_3, Y^n_3 | W_{[1:2]}, F^n_3)$

(e) $\geq \frac{(1 - \delta_3) \delta_{HE}}{1 - \delta_3 \delta_{HE}} (1 - \delta_3 \delta_{HE})$

$$\sum_{i=1}^{n} I(Y^n_1, Y^n_2; Z^n_3, Y^n_3 | W_{[1:2]}, F^n_3, Z^n_3, Y^n_3, F^n_3)$$

(e) $\geq \frac{(1 - \delta_3) \delta_{HE}}{1 - \delta_3 \delta_{HE}} (1 - \delta_3 \delta_{HE}).$

where: (i) the inequality in (a) follows since the entropy of a discrete random variable is positive; (ii) the equality in (b) is due to the chain rule of the mutual information; (iii) the equality in (c) follows since $X_{\lambda+3}$ is uniquely determined given $(Y^n_3, F^n_3)$; (iv) the equality in (d) follows because of the Markov chain $X_{\lambda+3} - W_{[1:2]}, F^n_3, Z^n_3, Y^n_3, F^n_3 - F^n_3$; (v) finally, the equality in (e) follows from (2c).
REFERENCES

[1] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
[2] C. Shannon, “Communication theory of secrecy systems,” *The Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.
[3] A. D. Wyner, “The wire-tap channel,” *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[4] N. Cai and R. W. Yeung, “Secure network coding on a wiretap network,” *IEEE Trans. Inf. Theory*, vol. 57, no. 1, pp. 424–435, 2011.
[5] L. Czap, V. Prabhakaran, C. Fragouli, and S. Diggavi, “Secret message capacity of erasure broadcast channels with feedback,” in *IEEE Inf. Theory Workshop (ITW)*, 2011, pp. 65–69.
[6] L. Czap, V. Prabhakaran, S. Diggavi, and C. Fragouli, “Exploiting common randomness: A resource for network secrecy,” in *IEEE Inf. Theory Workshop (ITW)*, 2013, pp. 1–5.
[7] A. Papadopoulos, L. Czap, and C. Fragouli, “Secret message capacity of a line network,” in *52nd Annual Allerton Conf. on Commun., Control, and Comput.*, 2014, pp. 1341–1348.
[8] ——, “LP formulations for secrecy over erasure networks with feedback,” in *IEEE Int. Symp. on Inf. Theory (ISIT)*, 2015, pp. 954–958.