On Intercept Probability Minimization under Sparse Random Linear Network Coding

Andrea Tassi, Robert J. Piechocki, and Andrew Nix

***Abstract*—This paper considers a network where a node wishes to transmit a source message to a legitimate receiver in the presence of an eavesdropper. The transmitter secures its transmissions employing a sparse implementation of Random Linear Network Coding (RLNC). A tight approximation to the probability of the eavesdropper recovering the source message is provided. The proposed approximation applies to both the cases where transmissions occur without feedback or where the reliability of the feedback channel is impaired by an eavesdropper jamming the feedback channel. An optimization framework for minimizing the intercept probability by optimizing the sparsity of the RLNC is also presented. Results validate the proposed approximation and quantify the gain provided by our optimization over solutions where non-sparse RLNC is used.**

***Index Terms*—Sparse random network coding, intercept probability, physical layer security, secrecy outage probability.**

I. Introduction

Due to the broadcast nature of the medium, wireless communications can be vulnerable to eavesdropping. Physical layer security strategies, operating at the lower protocol stack layers, aim to achieve the secrecy of transmitted messages. In partibular, an eavesdropper is prevented from recovering any of the packets broadcast by a source node (*per-packet secrecy*) by optimizing the transmission rate [1].

In this paper, we advance and compare against the framework for physical layer security presented in [2], and more recently in [3]. In particular, we refer to a system model where achieving per-packet secrecy is not necessary if the transmitted packets are a function of a source message intended to be delivered to a legitimate receiver, and if, in order to recover the source message, a receiver has to collect at least a target number of packets [4]. As observed in [2] and [3], this assumption is met by Random Linear Network Coding (RLNC) [5], where a source node generates a stream of coded packets by linearly combining the source packets forming a source message. The legitimate receiver or an eavesdropper can recover the source message only if they successfully receive a number of linearly independent coded packets equal to the number of source packets defining the source message.

We secure communications by minimizing the intercept probability – defined as the probability of an eavesdropper recovering the source message intended for a legitimate receiver. Unlike [2], [3], the devised proposal applies to both the case when the legitimate receiver does and does not acknowledge the source the successful reception of a message. This is achieved, by establishing our theoretical framework under the conditions where the transmission of acknowledgment messages takes place over a feedback channel that is not assumed fully reliable. In particular, our performance investigation will focus on attacks where an eavesdropper attempts to increase its intercept probability by jamming the feedback channel – thus, increasing the probability of the acknowledgment message not being successfully received and forcing the source node to keep transmitting coded packets even after the legitimate receiver successfully recovered a source message. To avoid that, we will show how the intercept probability can be significantly reduced by adopting a sparse implementation of the RLNC approach where the number of non-zero elements in the encoding matrix is smaller than in the case of classic RLNC [6].

In this paper, we provide the following key contributions:

- Existing expressions of the intercept probability are only applicable to extreme cases where the legitimate receiver either does not acknowledge to the source the successful reception of a source message or when an acknowledgment message is transmitted over a fully reliable feedback channel. By resorting to a novel Markov chain-based model, we propose a generic approximation of the intercept probability that is also applicable when the feedback channel is impaired by an arbitrary erasure probability.
- By employing a sparse implementation of RLNC, we devise a novel optimization strategy for optimizing the sparsity of the code and then minimizing the intercept probability when the feedback channel is jammed.

The rest of the paper is organized as follows. Section II describes the considered system model. Section III presents our novel approximation of the intercept probability and Section IV shows how the sparsity of the code can be optimized to minimize the intercept probability. The accuracy of the proposed approximation and the effectiveness of our optimization model are presented in Section V. Finally, in Section VI, we draw our conclusions.

II. System Model

We consider a system model where a node (Alice) wishes to transmit to a legitimate receiving node (Bob) a source message in the presence of an eavesdropper (Eve), over a broadcast channel. Bob and Eve experience a packet error probability equal to ϵ_{B} and ϵ_{E}, respectively.

We assume that the packet erasures experienced by Bob and Eve occur as statistically independent events and, based on a general condition for physical layer security over a Wyner's wiretap channel model [7, Chapter 1], $\epsilon_{\mathrm{B}} \leq \epsilon_{\mathrm{E}}$ [8].

Remark 2.1: It directly follows from [2], [3] that, for $\epsilon_{\mathrm{B}} > \epsilon_{\mathrm{E}}$, the average number of coded packet successfully

Copyright (c) 2015 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

A. Tassi, R. J. Piechocki and A. Nix are with the Department of Electrical and Electronic Engineering, University of Bristol, UK (e-mail: {A.Tassi,R.J.Piechocki,Andy.Nix}@bristol.ac.uk).

received by Bob is smaller than that received by Eve – thus, the average number of coded packet transmissions that Eve needs to recover a source message is inevitably smaller than the number of coded packets Bob needs to recover a source message. That is, for $\epsilon_{\mathrm{B}} > \epsilon_{\mathrm{E}}$, the secrecy capacity of a multicast or broadcast communication system cannot be improved by only employing strategies based on rateless codes. Thus, alternative physical layer security techniques achieving per-packet secrecy have to be used. The investigation of scenarios where $\epsilon_{\mathrm{B}} > \epsilon_{\mathrm{E}}$ are beyond the scope of this paper.

Alice segments the source message into K source packets and linearly combines at random the source packets to obtain $\hat{N}$ coded packets for transmission according to the sparse RLNC principle defined as follows.

Definition 2.1: Each coded packet $\mathbf{c}_j$ is obtained as $\mathbf{c}_j = \sum_{i=1}^{K} g_{i,j} \cdot \mathbf{s}_i$, where $g_{i,j}$ follows the following probability law [6]:

$$\mathbb{P}\left(g_{i,j} = v\right) = \begin{cases} p & \text{if } v = 0 \\ \dfrac{1-p}{q-1} & \text{otherwise,} \end{cases} \tag{1}$$

where $\frac{1}{q} < p < 1$ and q is the size of the finite field $\mathbb{F}_q$ over which network coding operations are performed. The bigger p, the more likely that $g_{i,j}$ is equal to 0. Thus, the average number of source packets concurring in the generation of a coded packet is a function of p. Classic RLNC assumes $p = \frac{1}{q}$ [9].

Let n_{B} and n_{E} be the number of coded packets successfully received by Bob and Eve, for $0 \leq n_{\mathrm{B}} \leq \hat{N}$ and $0 \leq n_{\mathrm{E}} \leq \hat{N}$, respectively. Column by column, Bob and Eve populate a $K \times n_{\mathrm{B}}$ and a $K \times n_{\mathrm{E}}$ decoding matrix $\mathbf{M}_{\mathrm{B}}$ and $\mathbf{M}_{\mathrm{E}}$, respectively, with the coding vectors associated with the coded packets they successfully received. Bob and Eve recover the source message as soon as the defect of the decoding matrix, defined as $\mathrm{def}(\mathbf{M}_{\mathrm{X}}) = K - \mathrm{rank}(\mathbf{M}_{\mathrm{X}})$ is equal to zero, for $X = \mathrm{B}$ and $X = \mathrm{E}$, respectively [5].

As soon as the source message has been successfully recovered, Bob transmits an acknowledgment message to Alice over a feedback channel. Alice stops broadcasting coded packets as soon as the feedback is successfully received or when $\hat{N} > K$ coded packets have been broadcast. The acknowledgment message is re-transmitted when Bob detects a new coded packet transmission pertaining to a source message that Bob has already recovered. The detection of new packet transmissions is assumed to be fully reliable. The feedback channel is assumed independent and separated from the broadcast channel used to transmit coded packets. The erasures of acknowledgement messages occur with probability ϵ_{K}, for $0 < \epsilon_{\mathrm{K}} \leq 1$.

III. Performance Analysis

We derive the probability of Eve recovering the source message, i.e., the intercept probability, by means of the Markov chain $\mathcal{M}$ (shown in Fig. 1) where its states are defined as follows.

Definition 3.1: We say that $\mathcal{M}$ is in state $(d_{\mathrm{B}}, d_{\mathrm{E}}, \delta)$ if $\mathrm{def}(\mathbf{M}_{\mathrm{B}}) = d_{\mathrm{B}}$, $\mathrm{def}(\mathbf{M}_{\mathrm{E}}) = d_{\mathrm{E}}$, and the ACK has not ($\delta = 0$) or has been ($\delta = 1$) successfully received by Alice.

From Definition 3.1, we observe that the total number of states defining $\mathcal{M}$ is $2(K+1)^2$, which directly follows from

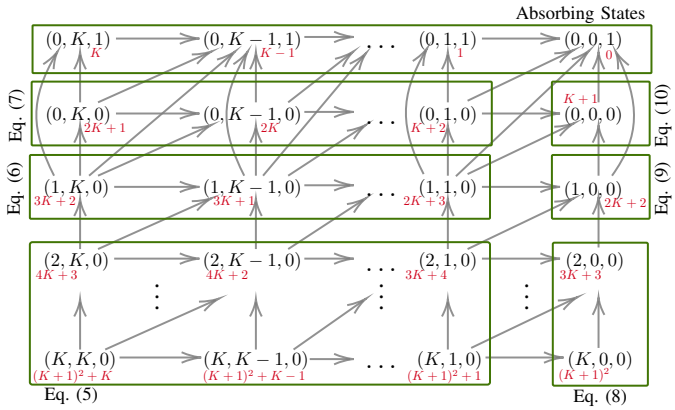


Fig. 1. State transition diagram for $\mathcal{M}$ (self-transition loops have been omitted and only the states that can be reached with a non-zero probability are represented). Each state has been tagged with its numeric label.

the fact that: (i) the maximum value of defect d_{B} and d_{E} is equal to K (corresponding to the cases when Bob and Alice have not successfully received any coded packet), and (ii) a ACK can either be received ($\delta = 1$) or not ($\delta = 0$).

After a coded packet transmission, assuming $d_{\mathrm{B}} \geq 1$, the rank of $\mathbf{M}_{\mathrm{B}}$ will increase by one if and only if Bob receives a coded packet that is linearly independent with the previously received. Equivalently, the rank of $\mathbf{M}_{\mathrm{B}}$ can at most be increased by one after a single coded packet transmission, i.e., the defect of $\mathbf{M}_{\mathrm{B}}$ can at most be reduced by one after a coded packet transmission. The same holds true from Eve. As for the value of δ, Bob will attempt to acknowledge the successful recovery of a source message as soon as d_{B} becomes equal to 0. For these reasons, all the $K(K+1)$ states where $d_{\mathrm{B}} \geq 1$ and $\delta = 1$ cannot be reached and can be disregarded. Thus, we will only consider the remaining $2(K+1)^2 - K(K+1) = (K+1) \cdot (K+2)$ states.

Example 3.1: Assume the system is in state $(K, K, 0)$ and ignore self-transition loops, Fig. 1 shows that $\mathcal{M}$ is expected to exhibits non-null transition probabilities for states $(K-1, K, 0)$, $(K-1, K-1, 0)$ and $(K, K-1, 0)$ corresponding to the cases when Bob, Bob and Alice or just Alice successfully receive a linearly independent coded packet, respectively. Since Bob cannot transmit an ACK message before a source message has been recovered, the transition probability toward any state where $\delta = 1$ is zero.

We then label the remaining $(K+1) \cdot (K+2)$ states.

Definition 3.2: Each state takes a numeric label ranging from 0 to $(K+1) \cdot (K+2) - 1$. If $\delta = 1$, the label of a state is equal to d_{E}, otherwise it is equal to $(d_{\mathrm{B}} + 1)(K+1) + d_{\mathrm{E}}$. Furthermore, in order to derive the probability transition matrix of $\mathcal{M}$, we prove the following lemma.

Lemma 3.1: Assume that matrix $\mathbf{M}_{\mathrm{X}}$ consists of $K \times (t+1)$ elements and assume that the first t columns are linearly independent, for $X \in \{\mathrm{B}, \mathrm{E}\}$ and $1 \leq t \leq (K-1)$. If $p > \frac{1}{q}$, the probability W_t of $\mathbf{M}_{\mathrm{X}}$ having rank $t+1$ can be approximated as follows:

$$\mathrm{W}_t \cong (1 - p^K) \exp\left(- \sum_{\ell=2}^{t+1} \binom{t}{\ell - 1} \frac{\pi_{\ell,K}}{(1-p^K)^{\ell}} \right), \tag{2}$$

where $\pi_{1,r} = \rho_{1,r}$, $\pi_{\ell,r} = \rho_{c,r} - \sum_{s=1}^{\ell-1} \binom{\ell-1}{s} \rho_{s,\ell} \pi_{\ell-s,r}$ and $\rho_{c,r} = \left[\frac{1}{q} \left(1 + (q-1) \left(1 - \frac{q(1-p)}{q-1} \right) \right) \right]^{c}_{r}$. If $p = \frac{1}{q}$, W_t is $\mathrm{W}_t = 1 - \frac{1}{q^{K-t}}$.

Proof: Let $\mathrm{R}_{K,t+1} = \mathbb{P}\left[\mathrm{rank}(\mathbf{M}_\mathrm{X})\right]$ be the probability of matrix $\mathbf{M}_\mathrm{X}$ having rank $t+1$. That is, let $\mathbf{M}_{\mathrm{X},t}$ be the $K \times t$ matrix defined by the first t columns of $\mathbf{M}_\mathrm{X}$. The relation

$$\mathrm{W}_t = \frac{\mathbb{P}\left[\mathrm{rank}(\mathbf{M}_\mathrm{X}) = t+1\right]}{\mathbb{P}\left[\mathrm{rank}(\mathbf{M}_{\mathrm{X},t}) = t\right]} \tag{3}$$

holds true due to the fact that if $\mathbf{M}_\mathrm{X}$ has rank $t+1$ then the first t columns are linearly independent. From [9, Theorem 3.1], in the case of a $r \times c$ sparse random matrix over $\mathbb{F}_q$, it follows that

$$\mathrm{R}_{r,c} \cong (1-p^r)^c \exp\left(-\sum_{\ell=2}^{c} \binom{c}{\ell} \frac{\pi_{\ell,r}}{(1-p^r)^\ell}\right), \tag{4}$$

for $r \geq c$. Thus, by substituting (4) in (3) and by noting that $\binom{t}{\ell-1} = \binom{t+1}{\ell} - \binom{t}{\ell}$, (2) holds. Finally, the case when $p = 1/q$ directly follows form [9, Eq. (2)]. ■

From (2), the probability transition matrix $\mathbf{P}$ of $\mathcal{M}$ can be approximated by means of the following lemma.

Lemma 3.2: The probability $\mathrm{P}_{i,j}$ of moving from state i to state j can be approximated as follows (only non-zero probabilities are listed):

- If $(K+1)(K-\tau+2)-K \leq i \leq (K+1)(K-\tau+2)-1$, for $\tau = 0, \ldots, (K-2)$,

$$\mathrm{P}_{i,j} \cong \begin{cases} \epsilon_\mathrm{B}(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}} & \text{if } j = i-1 \wedge d_\mathrm{B} \geq d_\mathrm{E} \\ (1-\epsilon_\mathrm{E})[\mathrm{W}_{K-d_\mathrm{E}} - (1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{B}}] & \text{if } j = i-1 \wedge d_\mathrm{B} < d_\mathrm{E} \\ \epsilon_\mathrm{E}(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-K-1 \wedge d_\mathrm{E} \geq d_\mathrm{B} \\ (1-\epsilon_\mathrm{B})[\mathrm{W}_{K-d_\mathrm{B}} - (1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{E}}] & \text{if } j = i-K-1 \wedge d_\mathrm{E} < d_\mathrm{B} \\ (1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})\mathrm{W}_{K-\min(d_\mathrm{B},d_\mathrm{E})} & \text{if } j = i-K-2 \\ 1 - \sum_{j=\{i-1,i-K-1,i-K-2\}} \mathrm{P}_{i,j} & \text{if } j = i \end{cases} \tag{5}$$

- If $2K+3 \leq i \leq 3K+2$,

$$\mathrm{P}_{i,j} \cong \begin{cases} \epsilon_\mathrm{B}(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}} & \text{if } j = i-1 \wedge d_\mathrm{B} \geq d_\mathrm{E} \\ (1-\epsilon_\mathrm{E})[\mathrm{W}_{K-d_\mathrm{E}} - (1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{B}}] & \text{if } j = i-1 \wedge d_\mathrm{B} < d_\mathrm{E} \\ \epsilon_\mathrm{K}\epsilon_\mathrm{E}(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-K-1 \wedge d_\mathrm{E} \geq d_\mathrm{B} \\ \epsilon_\mathrm{K}(1-\epsilon_\mathrm{B})[\mathrm{W}_{K-d_\mathrm{B}} - (1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{E}}] & \text{if } j = i-K-1 \wedge d_\mathrm{E} < d_\mathrm{B} \\ \epsilon_\mathrm{K}(1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})\mathrm{W}_{K-\min(d_\mathrm{B},d_\mathrm{E})} & \text{if } j = i-K-2 \\ (1-\epsilon_\mathrm{K})\epsilon_\mathrm{E}(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-2K-2 \wedge d_\mathrm{E} \geq d_\mathrm{B} \\ (1-\epsilon_\mathrm{K})(1-\epsilon_\mathrm{B})[\mathrm{W}_{K-d_\mathrm{B}} - (1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{E}}] & \text{if } j = i-2K-2 \wedge d_\mathrm{E} < d_\mathrm{B} \\ (1-\epsilon_\mathrm{K})(1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})\mathrm{W}_{K-\min(d_\mathrm{B},d_\mathrm{E})} & \text{if } j = i-2K-3 \\ 1 - \sum_{j=\{i-1,i-K-1,i-K-2,i-2K-2,i-2K-3\}} \mathrm{P}_{i,j} & \text{if } j = i \end{cases} \tag{6}$$

- If $K+2 \leq i \leq 2K+1$,

$$\mathrm{P}_{i,j} \cong \begin{cases} \epsilon_\mathrm{K}(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}} & \text{if } j = i-1 \\ (1-\epsilon_\mathrm{K})(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}} & \text{if } j = i-K-1 \\ (1-\epsilon_\mathrm{K})[1-(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}}] & \text{if } j = i-K-2 \\ \epsilon_\mathrm{K}[1-(1-\epsilon_\mathrm{E})\mathrm{W}_{K-d_\mathrm{E}}] & \text{if } j = i \end{cases} \tag{7}$$

- If $i = (K+1)(K-\tau+1)$, for $\tau = 0, \ldots, (K-2)$,

$$\mathrm{P}_{i,j} \cong \begin{cases} (1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-K-1 \\ 1-(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i \end{cases} \tag{8}$$

- If $i = 2(K+1)$,

$$\mathrm{P}_{i,j} \cong \begin{cases} (1-\epsilon_\mathrm{K})(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-2K-2 \\ \epsilon_\mathrm{K}(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i-K-1 \\ 1-(1-\epsilon_\mathrm{B})\mathrm{W}_{K-d_\mathrm{B}} & \text{if } j = i \end{cases} \tag{9}$$

- For $i = K+1$,

$$\mathrm{P}_{i,j} = \begin{cases} (1-\epsilon_\mathrm{K}) & \text{if } j = i-K-1 \\ \epsilon_\mathrm{K} & \text{if } j = i \end{cases} \tag{10}$$

- If $0 \leq i \leq K$, the state is and absorbing state and, hence, $\mathrm{P}_{i,j} = 1$.

Proof: We consider the case as per (5). In particular, we consider the case where $j = i-1$, which we can informally regard as the case where a state transition occurs *horizontally*, from left to right (see Fig. 1). As such, Bob will either not correctly receive a coded packet with probability ϵ_B or he will receive a coded packet without reducing the defect of $\mathbf{M}_\mathrm{B}$. Conversely, Eve successfully receives a coded packet that reduces the defect of $\mathbf{M}_\mathrm{E}$. That is,

$$\begin{aligned} \mathrm{P}_{i,j} = {} & \epsilon_\mathrm{B}(1-\epsilon_\mathrm{E})\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E}] \\ & + (1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E}) \\ & \cdot \mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{B}) = K - d_\mathrm{B} \wedge \mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E} + 1], \end{aligned} \tag{11}$$

since $\mathbf{M}_\mathrm{B}$ and $\mathbf{M}_\mathrm{E}$ are statistically correlated. Thus, we have the following cases. If $d_\mathrm{B} \geq d_\mathrm{E}$, the probability of M_B not reducing its defect while M_E does is expect to be small. Thus, the term $\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{B}) = K - d_\mathrm{B} \wedge \mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E} + 1]$ can be disregarded, and relation $\mathrm{P}_{i,j} \geq \epsilon_\mathrm{B}(1-\epsilon_\mathrm{E})\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E}]$ holds. If $d_\mathrm{B} < d_\mathrm{E}$, the term $\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{B}) = K - d_\mathrm{B} \wedge \mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E} + 1]$ can be approximated by subtracting the probability of $\mathbf{M}_\mathrm{B}$ reducing its defect from the probability of d_E being reduced as a result of a successfully received coded packet. From [5, Lemma 3.2], it follows that $\mathrm{P}_{i,j} \geq \epsilon_\mathrm{B}(1-\epsilon_\mathrm{E})\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E}] + (1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})\Big(\mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{E}) = K - d_\mathrm{E} + 1] - \mathbb{P}[\mathrm{rank}(\mathrm{M}_\mathrm{B}) = K - d_\mathrm{B} + 1]\Big)$. The same reasoning holds true when $j = i-K-1$ and we informally say that the transition occurs *vertically*, from top to bottom. In that case, the third and fourth cases of (5) follows by simply substituting E with B in the first and second cases of the same relation. Let us now consider the situation where $j = i-K-2$, which corresponds to the case where both M_B and M_E reduce their defect as a result of a successfully received coded packet. In this case, we informally say that the transition occurs *diagonally*. That is, both Bob and Eve successfully receive a coded packet with probability $(1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})$. Since $\mathbf{M}_\mathrm{B}$ and $\mathbf{M}_\mathrm{E}$ are statistically correlated, from [5, Lemma 3.2], it follows that $\mathrm{P}_{i,j}$ is upper-bounded by the product of $(1-\epsilon_\mathrm{B})(1-\epsilon_\mathrm{E})$ and the probability of M_t reducing its defect, where the index $\mathrm{t} \in \{\mathrm{B}, \mathrm{E}\}$ signifies the matrix with the smallest defect between M_B and M_E. We then approximate $\mathrm{P}_{i,j}$ with the aforementioned upper-bound.

As for the cases when i fulfills the conditions for (6), from Fig. 1, we observe that the probability of having a horizontal transition ($j = i-1$) can be approximated as per the first and second case of (5). Once again, the probability of having a vertical transition can be approximated according to the third and fourth case of (5) multiplied for $(1-\epsilon_\mathrm{K})$ or ϵ_K if the transition leads to a state where the ACK message has ($\delta = 1$) or has not been successfully delivered ($\delta = 0$), respectively. The same reasoning holds true for the diagonal transitions.

When i fulfil the conditions for (7), transition probability can be seen as a special case of (5) where $\mathrm{W}_{K-d_\mathrm{B}}$ is 0 as the defect of $\mathbf{M}_\mathrm{B}$ is 0. Relations (8) and (9) are special cases of (5) and (6), respectively, where only vertical transitions are considered and $\mathrm{W}_{K-d_\mathrm{E}}$ is 0, as d_E is equal to 0. When i fulfills the condition for (10), both d_B and d_E are equal to 0 – thus, the system remains in the state $(K+1)$ for as long as the ACK message cannot be successfully delivered. Finally, the first $K+1$ states are absorbing as Bob can successfully

acknowledge to Alice the recovery of the source message and the transmission of coded packets is subsequently halted. ■

From Lemma 3.2, it follows that $\mathcal{M}$ does not contain any cycles other than loops. For these reasons, $\mathbf{P}$ is a $(K+2)\times(K+1)$ lower-triangular matrix with non-zero diagonal elements, which makes $\mathbf{P}$ invertible in the real field. Finally, The intercept probability can be obtained as follows.

Theorem 3.1: For a given probability p and a maximum number of coded packet transmissions $\hat{N}$, the intercept probability $\mathrm{I}_{\hat{N}}(p)$ can be approximated as

$$\mathrm{I}_{\hat{N}}(p) \cong \sum_{\substack{j\in\{\tau(K+1),\\ \text{for } \tau=0,\dots,(K+1)\}}} \mathbf{P}^{\hat{N}}\left((K+1)^2+K,j\right), \tag{12}$$

where $\mathbf{P}^{\hat{N}}(s,t)$ signifies the (s,t)-th element of the matrix $\mathbf{P}$ after it has been elevated to the power of $\hat{N}$, for s and $t=0,\dots,(K+1)^2+K$.

Proof: The system starts with probability 1 from the state with label $(K+1)^2+K$, i.e., the system starts from state $(K,K,0)$ with probability 1. The term $\mathrm{I}_{\hat{N}}(p)$ is equal to the probability of the system being in any of the states having d_{E} equal to 0, for a given $\hat{N}$. From Definition 3.2, we observe that states with labels $\tau(K+1)$, for $\tau=0,\dots,(K+1)$ are associated with those cases where Eve successfully recovered the information message. That is, (12) holds. ■

IV. Optimization Model

We define the Intercept Minimization (IM) problem as follows:

$$\text{IM} \quad \min_{p} \ \mathrm{I}_{\hat{N}}(p) \tag{13}$$

$$\text{s.t.} \quad \mathrm{D}_{\hat{N}}(p) \geq \hat{D} \tag{14}$$

where $\mathrm{D}_{\hat{N}}(p)$ signifies the probability of Bob recovering the source message. For a given value of p and $\hat{N}$, constraint (14) ensures that Bob recovers the source message with at least probability $\hat{D}$. Form [6], [9], it follows that the average number of coded packet transmissions needed to recover a source messages increases as p increases. Thus, not only Eve but also Bob is expected to require more coded packet transmissions to recover a source message. To prevent the IM problem to minimize the intercept probability by increasing the value of p at the expense of the number of coded packet transmissions, constraint (14) not only imposes a minimum threshold for the probability of Bob recovering a source message but also it ensures that a source message has to be recovered by $\hat{N}$ coded packets transmissions. As such, if we consider the case where one coded packet transmission takes place in one-time slot, the proposed optimization framework ensures the delivery of a source message with a probability greater than or equal to $\hat{D}$ in $\hat{N}$ time slots or less.

Remark 4.1: By following the same reasoning as in Theorem 3.1, term $\mathrm{D}_{\hat{N}}(p)$ can be approximated as $\sum_{j=0}^{K+1}\mathbf{P}^{\hat{N}}\left((K+1)^2+K,j\right)$. However, as discussed in the proof of Lemma 3.2, the proposed approximation of $\mathbf{P}_{i,j}$ is likely to over-estimate both $\mathrm{I}_{\hat{N}}(p)$ and $\mathrm{D}_{\hat{N}}(p)$ – thus making approximation (12) an empirical upper-bound of the system intercept probability but leading to potentially overestimating the probability of Bob recovering the source message. For the sake of solving the IM problem, $\mathrm{D}_{\hat{N}}(p)$ is approximated by directly employing (4), as per [9, Eq. (2), Theorem 3.1]:

$$\mathrm{D}_{\hat{N}}(p) \cong \sum_{n=K}^{\hat{N}} \binom{\hat{N}}{n}(1-\epsilon_{\mathrm{B}})^n \epsilon^{\hat{N}-n}\mathrm{R}_{n,K}. \tag{15}$$

The the IM problem can be solved as follows.

Remark 4.2: From (2), it follows that term $\sum_{\ell=2}^{t+1}\binom{t}{\ell-1}\frac{\pi_{\ell,K}}{(1-p^K)^\ell}$ is a non-decreasing function of p, which makes W_t a non-increasing function of p. That is, for a given $\hat{N}$, the higher p, the more unlikely it gets for the system to be in any of the states with label $\tau(K+1)$, for $\tau=0,\dots,(K+1)$, i.e., the more unlikely it gets for Eve to recover the source message. In the following section, we will show how the proposed approximation for the intercept probability $\mathrm{I}_{\hat{N}}(p)$ is largely a non-increasing function of p, for $q^{-1}\leq p<1$ and $\epsilon_{\mathrm{K}}\geq 0.85$. Similarly, (4) is a non-increasing function of p, which makes (15) a non-increasing function as well. For these reasons, the solution of the IM problem is given by the real root of $\mathrm{D}_{\hat{N}}(p)-\hat{D}=0$, which can be derided by employing the bisection method.

V. Numerical Results

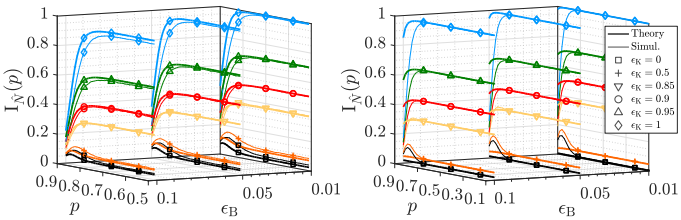
This section compares the derived expression of the intercept probability with Monte Carlo simulations, and solves the IM problem for different configurations. The code needed to reproduce our results is available online[1].

Fig. 2 compares the expression of the intercept probability as per (12) with Monte Carlo simulations, for $K=20$, $q=\{2,2^4\}$ and $\hat{N}=2K$. We also set Bob's and Eve's packet error probability equal to $\epsilon_{\mathrm{B}}=\{0.01,0.05,0.1\}$ and $\epsilon_{\mathrm{E}}=\epsilon_{\mathrm{B}}+0.25$, respectively. In particular, Fig. 2a shows that, for $q=2$, (12) is a tight empirical approximation of the intercept probability – the maximum Mean Squared Error (MSE) between simulations and our proposed approximation (12) is equal to $0.933\cdot 10^{-3}$, for $\epsilon_{\mathrm{B}}=0.01$, $\epsilon_{\mathrm{E}}=0.26$ and $\epsilon_{\mathrm{K}}=1$.

For $q=2^4$, Fig. 2b shows that the intercept probability are almost constant for $2^{-4}\leq p\leq 0.73$, which follows from the fact that both $\rho_{c,r}$ and $\pi_{\ell,K}$ approach 0 as q grows (see Lemma 3.1), and hence, W_t can be approximated with $(1-p^K)$. The proposed approximation becomes looser only when the probability p of a source packet not taking part in the generation of coding vector is very large ($p\geq 0.8$).

From Fig. 2, we also observe that the proposed (12) is also an empirical upper-bound of the intercept probability both in the case of $q=2$ and 2^4, for $\epsilon_{\mathrm{K}}\geq 0.85$ and $\epsilon_{\mathrm{K}}\geq 0.9$, respectively. In addition, for $p\geq 0.8$ and $\epsilon_{\mathrm{K}}\geq 0.85$, the simulated $\mathrm{I}_{\hat{\mathrm{N}}}(p)$ sharply decreases as the value of p approaches 0.9 and hence, the probability of having all-zero coding vectors sharply increases thus, making for both Eve and Bob more unlikely to recover a source message – for instance, if the value of p increases from 0.8 to 0.9, the probability of having an all-zero coded packet increases from 0.012 to 0.12, for $K=20$. For $\epsilon_{\mathrm{K}}\leq 0.5$ or $\epsilon_{\mathrm{K}}\leq 0.85$, for $q=2$ and 2^4, respectively, the intercept probability increases with p, for $0.75\leq p\leq 0.85$. That is, as ϵ_{K} decreases, the number of coded packets transmitted after Bob has already recovered

[1] https://github.com/andreatassi/SparseRLNC.



(a) $q = 2$ (b) $q = 2^4$

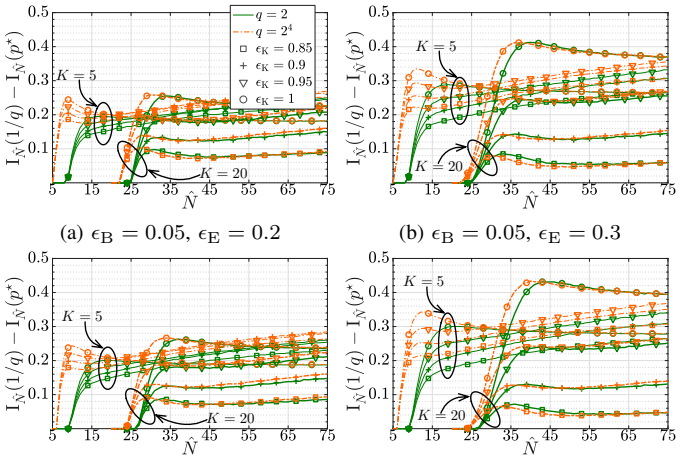
Fig. 2. Comparison of $\mathrm{I}_{\hat{\mathrm{N}}}(p)$ as a function of p obtained through simulations (Simul.) and approximated (Theory) as in (12), for $\epsilon_{\mathrm{B}} = \{0.01, 0.05, 0.1\}$, $\epsilon_{\mathrm{E}} = \epsilon_{\mathrm{B}} + 0.25$, $\epsilon_{\mathrm{K}} = \{0, 0.5, 0.85, 0.9, 0.95, 1\}$, $K = 20$, $\hat{N} = 2K$ and $q = \{2, 2^4\}$. Legend of both figures is reported in Fig. 2b.

the source message decreases as well. This impacts on the probability of Eve recovering the source message, and hence, the overall value of $\mathrm{I}_{\hat{\mathrm{N}}}(p)$ reduces up to 0.05. In these cases, from Lemma 3.1, we note that some composite transition probabilities are non-decreasing functions with p and in this case they can be appreciated in the overall expression of $\mathrm{I}_{\hat{\mathrm{N}}}(p)$. Assuming $\epsilon_{\mathrm{E}} = \epsilon_{\mathrm{B}} = 0$, $K = 20$ and that $\mathcal{M}$ transitions from $(4, 5, 0)$ to $(3, 4, 0)$ and then to $(3, 3, 0)$, the overall probability of this transitions to happen is $\mathrm{W}_{K-4}(\mathrm{W}_{K-4} - \mathrm{W}_{K-3})$ which is a non-decreasing function of p when $0.7 \leq p \leq 0.87$ and $0.7 \leq p \leq 0.9$, for $q = 2$ and 2^4, respectively.

Fig. 3 compares the intercept probability obtained by employing the proposed IM problem with the state-of-the-art performance of a system model as per [2], [3] where $p = 1/q$ and hence, the classic RLNC is used. In particular, Fig. 3 shows the *intercept probability gain* defined as the difference between the intercept probability values obtained by using the classic RLNC and the intercept probability that we get by setting p equal to the solution of the IM problem $p^\star$ – namely, $\mathrm{I}_{\hat{\mathrm{N}}}(1/q) - \mathrm{I}_{\hat{\mathrm{N}}}(p^\star)$. In order to show the intercept probability gain effectively achieved, both $\mathrm{I}_{\hat{\mathrm{N}}}(1/q)$ and $\mathrm{I}_{\hat{\mathrm{N}}}(p^\star)$ are obtained by employing Monte Carlo simulations.

Let us consider Fig. 3a, for $\epsilon_{\mathrm{B}} = 0.05$, $\epsilon_{\mathrm{E}} = 0.2$, $K = 5$ and $q = 2$. In the case of $\epsilon_{\mathrm{K}} = 1$, the intercept probability gain sharply increases and reaches its maximum of 0.196 for $\hat{N} = 17$. As ϵ_{K} decreases, the intercept probability gain decreases as well. In particular, for $\hat{N} = 17$ and $\epsilon_{\mathrm{K}} = 0.85$, the intercept probability gain reduces to 0.15. For $q = 2^4$, the intercept probability gain is generally larger. That is, for $\epsilon_{\mathrm{K}} = 1$ and $\epsilon_{\mathrm{K}} = 0.85$, the intercept probability gain reaches its maximum of 0.25 and 0.27, for $\hat{N} = 75$. With regard to Fig. 3b, as ϵ_{E} increases to 0.3, the intercept probability gain reaches the value of 0.33 and 0.36, for $q = 2$ and $q = 2^4$, respectively. As K is set equal to 20, the intercept probability gain associated to $q = 2$ and $q = 2^4$ are comparable. We also note that, as ϵ_{K} decreases, we expect the intercept probability gain to decrease the chances of Eve successfully receiving enough coded packets to recover the source message are impaired by the reduced probability of Alice having to unnecessarily broadcast coded packets due to the loss of acknowledge messages from Bob.

In Figs. 3c and 3d, Bob's packet error probability is doubled ($\epsilon_{\mathrm{B}} = 0.1$). Yet, the intercept probability gains are comparable to those in the cases where ϵ_{B} was equal to 0.05. Since in Fig. 3 the difference $\epsilon_{\mathrm{E}} - \epsilon_{\mathrm{B}}$ is fixed and set equal to 0.15 or 0.25, we can conclude that the value of the intercept probability gain is determined by the difference in the packet



(a) $\epsilon_{\mathrm{B}} = 0.05$, $\epsilon_{\mathrm{E}} = 0.2$ (b) $\epsilon_{\mathrm{B}} = 0.05$, $\epsilon_{\mathrm{E}} = 0.3$

(c) $\epsilon_{\mathrm{B}} = 0.1$, $\epsilon_{\mathrm{E}} = 0.25$ (d) $\epsilon_{\mathrm{B}} = 0.1$, $\epsilon_{\mathrm{E}} = 0.35$

Fig. 3. Intercept probability gain as a function of $\hat{N}$, for $\epsilon_{\mathrm{B}} = \{0.05, 0.1\}$, $\epsilon_{\mathrm{E}} - \epsilon_{\mathrm{B}} = \{0.15, 0.25\}$, $\epsilon_{\mathrm{K}} = \{0.85, 0.9, 0.95, 1\}$, $K = \{5, 20\}$ and $q = \{2, 2^4\}$. Legend of all figures is reported in Fig. 3a.

error probability between Eve and Bob, for a given p and $\hat{N}$.

VI. Conclusions

We present a novel strategy for approximating the intercept probability for networks where secrecy is achieved by employing a sparse implementation of RLNC. The proposed approximation is general and applies to the cases where transmissions are not acknowledged or when they are and the eavesdropper jams the feedback channel. We also propose an optimization framework for minimizing the intercept probability by increasing the sparsity of RLNC in use. Analytic results empirically establish that the proposed approximation for the intercept probability is tight, for practical network and transmission parameters. Our optimization framework ensures a reduction of the intercept probability of up to 82% compared to the case where classic RLNC is used.

VII. Acknowledgments

The authors would like to thank Oliver Johnson (University of Bristol, Bristol, UK) for the insightful discussions and precious feedback.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless Information-Theoretic Security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[2] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. Du, "Exploiting Fountain Codes for Secure Wireless Delivery," *IEEE Commun. Lett.*, vol. 18, no. 5, May 2014.

[3] A. S. Khan, A. Tassi, and I. Chatzigeorgiou, "Rethinking the Intercept Probability of Random Linear Network Coding," *IEEE Commun. Lett.*, vol. 19, no. 10, Oct. 2015.

[4] N. Cai and R. W. Yeung, "Secure Network Coding," in *Proc. of IEEE ISIT*, Lausanne, CH, Jun. 2002.

[5] E. Tsimbalo, A. Tassi, and R. J. Piechocki, "Reliability of Multicast Under Random Linear Network Coding," *IEEE Trans. Commun.*, vol. 66, no. 6, Jun. 2018.

[6] A. Tassi, I. Chatzigeorgiou, and D. E. Lucani, "Analysis and Optimization of Sparse Random Linear Network Coding for Reliable Multicast Services," *IEEE Trans. Commun.*, vol. 64, no. 1, pp. 285–299, Jan. 2016.

[7] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[8] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[9] S. Brown, O. Johnson, and A. Tassi, "Reliability of Broadcast Communications Under Sparse Random Linear Network Coding," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, May 2018.