

# Achievable Error Exponents for Two-Way AWGN Channels

Kenneth Palacio-Baus<sup>\*†</sup>, Natasha Devroye<sup>\*</sup>

<sup>\*</sup>University of Illinois at Chicago, {kpalac2, devroye}@uic.edu

<sup>†</sup>University of Cuenca, Ecuador

**Abstract**—We present achievable error exponent regions for the Two-Way AWGN channel under an expected block power constraint and variable-length coding (VLC). We propose an achievability scheme that allows terminals to cooperate via interaction to detect decoding errors and request re-transmissions. Under this scheme, in certain rate-pair regimes both directions are able to simultaneously attain error exponent pairs larger than the feedback-free point-to-point random coding error exponents.

A full version of this paper is accessible at: [1].

## I. INTRODUCTION

Shannon [2] introduced the two-way channel, consisting of two terminals,  $T_i$  for  $i \in \{1, 2\}$ , that exchange messages. For the Two-way AWGN memoryless channel, the capacity region corresponds to a rectangular region [3], [4] determined by the interference-free AWGN capacities at signal-to-noise ratio SNR,  $C = \frac{1}{2} \log(1 + \text{SNR})$  of each direction (denoted by  $C_{12}$  and  $C_{21}$ ).

The reliability function (or error exponent)  $E(R) = \limsup_{N \rightarrow \infty} \frac{-\ln P_e}{N}$  provides a more refined yet still asymptotic characterization of the communication limits, where  $P_e$  is the probability of error of a blocklength- $N$  code. For one-way channels,  $E(R)$  has been studied with and without feedback. In memoryless channels, while feedback cannot increase capacity, it may simplify coding schemes and enlarge error exponent [5].

In the presence of noiseless feedback in one-way AWGN channels, error exponents can be greatly improved as shown in [6]–[10]. When noisy feedback is used, error exponent improvements over non-feedback channels are still possible, in particular when the feedback channel is stronger (less noisy) than the forward channel. A generalization of the Yamamoto-Itoh coding scheme under VLC with perfect feedback [10] to noisy feedback was presented by Sato-Yamamoto [11], and this scheme’s reliability tends to Schalkwijk-Barron’s [9] as the feedback noise approaches zero.

For two-way parallel memoryless channels (such as the Two-way AWGN channel), terminals send messages and (noisy) feedback over the same channels. This interaction (noisy feedback) does not increase the capacity region of the Two-way AWGN channel. Whether interaction in the Two-way AWGN channel can increase error exponents is addressed in [12] at zero-rate; here we focus on positive rate-pairs.

Apart from the authors’ prior work on two-way channels [12], the most related prior work is that for error exponents

for one-way channels with noisy feedback in the positive rate regime [11], [13]. In the one-way noisy feedback setting, error exponent gains have mainly been attained when the feedback channel is much stronger than the direct channel, as in [14] where the sphere packing bound is exceeded for a wide rate regime. This work considers an expected block power constraint, as that used in [15] for the zero-rate regime (transmission of two messages). Interestingly, in the two-way setting for positive rate, we are able to attain error exponent gains even when the channels in the two directions are symmetric – one direction need not be much stronger than the other. In fact, the scheme presented here exploits this symmetry, and is hence useful in a wider range of settings, including for example full duplex two-way communications with channel reciprocity. This scheme does rely on the flexibility provided by an expected power constraint.

## II. PROBLEM STATEMENT AND MAIN RESULT

Consider a two-way AWGN channel as in Figure 1, for the transmission of  $|\mathcal{W}_1| = 2^{\{nR_{12}\}}$  and  $|\mathcal{W}_2| = 2^{\{nR_{21}\}}$  equally likely messages in the  $1 \rightarrow 2$  and  $1 \leftarrow 2$  directions respectively. The output of this channel at the  $i$ -th terminal at the  $k$ -th channel use is modeled as in (1):

$$Y_{i,k} = X_{i,k} + a_{i,k}X_{3-i,k} + N_{i,k}, \quad \text{for } k = 1, 2, \dots \quad (1)$$

where,  $a_{i,k}$  is a constant,  $X_{i,k} \in \mathbb{R}$  the channel input satisfying a block power constraint,  $Y_{i,k} \in \mathbb{R}$  the output, and  $N_{i,k} \sim \mathcal{N}(0, \sigma_i^2)$  zero-mean AWGN, each independent and identically distributed across channel uses. Since each terminal may subtract its own input, and setting  $a_{i,k} = 1$ , (1) simplifies to:  $Y_{i,k} = X_{3-i,k} + N_{i,k}$ .

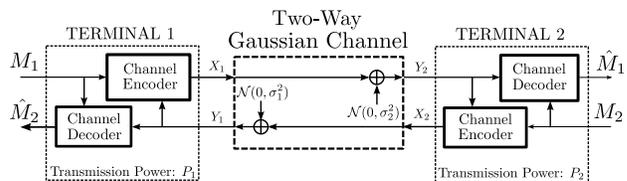


Fig. 1. Two-way AWGN channel.

Let  $\mathcal{X}_1, \mathcal{Y}_1, \mathcal{X}_2, \mathcal{Y}_2$  be the set of reals. A *variable-length two-way code*  $\mathcal{C}_{v1}(|\mathcal{W}_1|, |\mathcal{W}_2|, P_1, P_2, \sigma_1^2, \sigma_2^2, N)$  for the transmission of messages  $M_i$  uniformly selected from  $\mathcal{W}_i$  in the  $i \rightarrow (3 - i)$  directions for  $i = 1, 2$  over a two-way AWGN

channel with average transmitter power  $P_i$ , and noise variances  $\sigma_i^2$  respectively, consists of:

1. Two encoding functions:  $f_{i,k} : \mathcal{W}_i \times \mathcal{Y}_i^{k-1} \rightarrow \mathcal{X}_i$  for  $i = 1, 2$  and  $k = 1, 2, \dots$  leading to channel inputs  $X_{i,k} = f_{i,k}(M_i, Y_i^{k-1})$  satisfying an expected block power constraint for each block of length  $N$  (where  $\mathbb{E}[\cdot]$  denotes expectation):

$$\mathbb{E} \left[ \sum_{k=1}^N X_{i,k}^2 \right] \leq NP_i. \quad (2)$$

2. Two decoding functions:  $\phi_{i,k} : \mathcal{Y}_i^k \rightarrow \mathcal{W}_{3-i}$ .

3. A non-negative transmission time  $\Delta$  (a random variable) satisfying  $\mathbb{E}[\Delta] \leq N$ , defined as the slot at which both messages are decoded (and transmitters can move on to the next message).

Let the average rate in the  $i \rightarrow (3-i)$  direction be:  $\bar{R}_{i,(3-i)} = \frac{\log |\mathcal{W}_i|}{\mathbb{E}[\Delta]}$ . Next, let the signal-to-noise ratio for each direction be  $\text{SNR}_{i,(3-i)} = P_i/\sigma_{3-i}^2$ , and the maximum error probability attained in each direction by a two-way  $C_{\text{vl}}(|\mathcal{W}_1|, |\mathcal{W}_2|, P_1, P_2, \sigma_1^2, \sigma_2^2, N)$  variable length code at an average rate-pair  $(\bar{R}_{12}, \bar{R}_{21})$  under power constraint (2) be:

$$\begin{aligned} & P_{\text{error}}^{i \rightarrow (3-i)}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, \Delta) \\ & := \max_{m_i \in \mathcal{W}_i} \mathbb{P} \left( \phi_i^\Delta \neq m_{3-i} \mid M_i = m_i, M_{3-i} = m_{3-i} \right) \end{aligned}$$

The two way capacity region is known [16] to equal all rate-pairs  $(R_1, R_2)$  inside the rectangle bounded by  $R_1 \leq C_{12} = \frac{1}{2} \log(1 + \frac{P_1}{\sigma_2^2})$  and  $R_2 \leq C_{21} = \frac{1}{2} \log(1 + \frac{P_2}{\sigma_1^2})$ .

*Definition 1:* An error exponent pair,  $(E_{12}, E_{21})$ , is achievable if simultaneously, for  $\mathbb{E}[\Delta] \leq N$ :

$$\begin{aligned} E_{12}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}) & \geq \\ & \frac{-\ln P_{\text{error}}^{1 \rightarrow 2}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N)}{\mathbb{E}[\Delta]} \\ E_{21}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}) & \geq \\ & \frac{-\ln P_{\text{error}}^{1 \leftarrow 2}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N)}{\mathbb{E}[\Delta]} \end{aligned}$$

*Definition 2:* The error exponent region (EER) of a two-way AWGN channel transmitting at an average rate-pair  $(\bar{R}_{12}, \bar{R}_{21})$  under an expected block power constraint corresponds to the union of all achievable error exponent pairs  $E_{12}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21})$  and  $E_{21}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21})$ .

We first present a proposition that involves the use of block codes under an average power constraint  $\sum_{k=1}^N X_{i,k} \leq NP$  in the absence of terminal interaction / feedback (i.e. the encoding functions are functions of the messages alone):

*Proposition 1:* An achievable error exponent pair for the two-way AWGN channel for the rate pair  $(R_{12}, R_{21})$  under an average power constraint is:

$$\begin{aligned} E_{12}(R_{12}, R_{21}, \text{SNR}_{12}, \text{SNR}_{21}) & \geq E_{\text{AWGN}}^{\text{rc}}(R_{12}, \text{SNR}_{12}), \\ E_{21}(R_{12}, R_{21}, \text{SNR}_{12}, \text{SNR}_{21}) & \geq E_{\text{AWGN}}^{\text{rc}}(R_{21}, \text{SNR}_{21}), \end{aligned}$$

where  $E_{\text{AWGN}}^{\text{rc}}(R, \text{SNR})$  corresponds to the random coding error exponent lower bound for a one-way AWGN channel of signal to noise ratio SNR at rate  $R$ , see [17, Section 7.4].

Our main results correspond to two achievable EERs defined for any average rate-pair in the capacity region. One uses compression to send the feedback signals and the other does not. The former is useful for rates close to capacity, whereas the latter for lower rates. Our results are both based on a variable length coding scheme under power constraint (2) that exploits interaction to facilitate error detection and correction. We will show how the scheme operates for the case with compression (the one without compression can be easily obtained from the one with compression). Let  $R := \max\{\bar{R}_{12}, \bar{R}_{21}\}$  and  $C := \min\{C_{12}, C_{21}\}$ .

*Theorem 1: Uncompressed feedback:* An achievable error exponent pair for the two-way AWGN channel under variable-length coding and an expected block power constraint at an average rate-pair  $(\bar{R}_{12}, \bar{R}_{21})$ , for  $0 < R < 0.5C$  is determined as the union over all  $0 \leq \lambda \leq 1$ ,  $R_{\text{FB}} = R$ , and satisfying  $\bar{R}_{12}/\lambda \leq C_{12}$ ,  $\bar{R}_{21}/\lambda \leq C_{21}$  and  $R_{\text{FB}}/(1-\lambda) \leq C$ , of

$$E_{12}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \geq (3)$$

$$E_{21}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \geq (4).$$

*Theorem 2: Compressed feedback:* An achievable error exponent pair for the two-way AWGN channel under variable-length coding and an expected block power constraint at an average rate-pair  $(\bar{R}_{12}, \bar{R}_{21})$ , is determined as the union over all  $\lambda$  and  $R_{\text{FB}}$  in  $0 \leq \lambda \leq 1$ ,  $\bar{R}_{12}/\lambda \leq C_{12}$ ,  $\bar{R}_{21}/\lambda \leq C_{21}$ ,  $0 \leq \bar{R}_{\text{FB}} < \min\{(1-\lambda)C, R\}$  of

$$\begin{aligned} & E_{12}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \\ & \geq \min \left\{ (3), R_{\text{FB}} \ln(2) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{12}}{\lambda}, \text{SNR}_{12} \right) \right\} \\ & E_{21}(\bar{R}_{12}, \bar{R}_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \\ & \geq \min \left\{ (4), R_{\text{FB}} \ln(2) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{21}}{\lambda}, \text{SNR}_{21} \right) \right\}. \end{aligned}$$

Note that we have excluded the zero-rate regime, since this scheme is outperformed by the one derived in [18], which results from a generalization of a one-way scheme with noisy feedback [15] to the two-way AWGN channel under the same power constraint.

The following section presents a coding scheme that achieves Theorems 1 and 2.

### III. TWO-WAY INTERACTIVE CODING SCHEME

Both Theorems employ a coding scheme in which terminals first exchange their messages, and then initiate a cooperative feedback stage aiming to detect errors at both receivers. The only difference between the two coding schemes is that one sends feedback uncompressed, which can only be done for small enough rates, and the other uses hashing to compress the feedback signal, which allows transmission at higher rates. If an error is detected at any terminal, an alarm signal is triggered during the final stage, otherwise both transmitters remain silent. The occurrence of an alarm forces both terminals to retransmit their messages using a new block of length  $N$ . Since alarm events occur with exponentially small probability, retransmissions are very rare and thus the power constraint (2)

$$E_{12}(R_{12}, R_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \geq \min \left\{ (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{\text{FB}}}{1 - \lambda}, \text{SNR}_{12} \right) \right. \\ \left. + (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{\text{FB}}}{1 - \lambda}, \text{SNR}_{21} \right) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{12}}{\lambda}, \text{SNR}_{12} \right), \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{12}}{\lambda}, \text{SNR}_{12} \right) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{21}}{\lambda}, \text{SNR}_{21} \right) \right\}. \quad (3)$$

$$E_{21}(R_{12}, R_{21}, \text{SNR}_{12}, \text{SNR}_{21}, N) \geq \min \left\{ (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{\text{FB}}}{1 - \lambda}, \text{SNR}_{21} \right) \right. \\ \left. + (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{\text{FB}}}{1 - \lambda}, \text{SNR}_{12} \right) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{21}}{\lambda}, \text{SNR}_{21} \right), \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{21}}{\lambda}, \text{SNR}_{21} \right) + \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R_{12}}{\lambda}, \text{SNR}_{12} \right) \right\}. \quad (4)$$

is satisfied. If no alarm is triggered, both transmitters move to the transmission of a new message.

During the feedback stage terminals exchange a special message that is a function of the true message sent out in the first stage and the one received from the other terminal. This message should be the same for both directions. Once this message is exchanged, both terminals can compare the decoded special message and trigger an alarm if they are not equal. By means of this cooperation each terminal may become aware of decoding errors made locally or at the other end during the first stage. As we will see, we may still have decoding errors in which no alarm is triggered.

### A. Scheme operation

We present the coding scheme which employs compression (Theorem 2), but note that the no compression Theorem 1 may be easily obtained from this scheme by simply omitting the hashing function used to reduce the feedback rate. We first introduce some notation that will be useful in the upcoming sections. Let  $\mathcal{C}^{\text{RC}}(2^{NR}, P, N)$  denote a randomly generated code for the transmission for  $2^{NR}$  messages using a block of length  $N$  under average power  $P$ . An achievable error exponent for this code is determined by the random coding error exponent lower bound  $E_{\text{AWGN}}^{\text{RC}}(R, \text{SNR})$  as shown in [17].

Figure 2 shows a block diagram of our scheme comprising three stages whose durations are parameterized by  $\lambda \in [0, 1]$ :

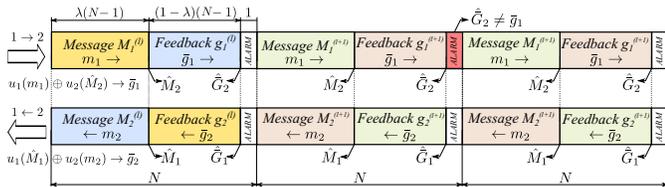


Fig. 2. Block diagram for the two-way coding scheme under a expected block power constraint. Note that the special message  $g_i$  or its corresponding hash  $\bar{g}_i$  is fed back depending on whether compression is used or not.

**1. Transmission:** This stage lasts for  $\lambda(N-1)$  channel uses, where terminal  $T_i$  transmits message  $M_i = m_i$ , uniformly selected from  $\mathcal{W}_i$  utilizing a random code in each direction, which are respectively denoted by  $\mathcal{C}^{\text{RC}}(2^{N\bar{R}_{12}}, P_1, \lambda N)$  and  $\mathcal{C}^{\text{RC}}(2^{N\bar{R}_{21}}, P_2, \lambda N)$ . By the end of this stage, each terminal has a preliminary estimate of the received message  $\hat{M}_{3-i}$ .

**2. Feedback:** This stage lasts for  $(1 - \lambda)(N - 1)$  channel uses. Here, each terminal  $T_i$  generates a special feedback message we denote by  $g_i$  that are exchanged during this stage and used later to detect errors. To generate  $g_i$ , the  $i$ -th encoder combines the true known message  $m_i$  and the estimate  $\hat{M}_{3-i}$  as follows: Let  $\mathbb{F}_q^N$  be a finite field of size  $q^N$ , where  $q$  is chosen as the smallest prime for which  $q^n > \max \{ \lceil 2^{N\bar{R}_{12}} \rceil, \lceil 2^{N\bar{R}_{21}} \rceil \}$ , where  $\lceil x \rceil$  denotes to the smallest integer larger than  $x$ . Next, let  $u_i(m_i)$  be an injective mapping  $m_i \mapsto \mathbb{F}_q^N$  where  $m_i \in \mathcal{W}_i$ . Then, for terminal  $T_1$ ,  $g_1 = u_1(m_1) \oplus u_2(\hat{M}_2)$ , whereas for  $T_2$ ,  $g_2 = u_1(\hat{M}_1) \oplus u_2(m_2)$ , where  $\oplus$  denotes modulo addition over the finite field  $\mathbb{F}_q^N$ . Message  $g_i$  is an element of the set  $\mathcal{G} = \{1, \dots, \max\{2^{N\bar{R}_{12}}, 2^{N\bar{R}_{21}}\}\}$ , whose cardinality is determined by the direction transmitting at a higher rate. Note that in the absence of errors during the first stage, the messages decoded at each terminal  $T_{3-i}$  are  $\hat{M}_i = m_i$  for  $i = 1, 2$ , and we must have  $g_1 = g_2$ .

Note also that in this stage, both directions transmit at the same rate, which may exceed the rate available at one or both directions because of their capacities and since only  $(1 - \lambda)(N - 1)$  channel uses remain from the first stage. Therefore, we consider the compression method introduced in [19] in which the  $|\mathcal{G}| = \max\{2^{N\bar{R}_{12}}, 2^{N\bar{R}_{21}}\}$  messages are randomly assigned to  $2^{N\bar{R}_{\text{FB}}}$  bins, where  $\bar{R}_{\text{FB}}$  is a design parameter. Thus, the feedback message becomes the bin number (or hash) that contains  $g_i$ , which we denote by  $\bar{g}_i \in \{1, \dots, 2^{N\bar{R}_{\text{FB}}}\}$ . It follows that  $\bar{R}_{\text{FB}} \leq (1 - \lambda) \min\{C_{12}, C_{21}\}$ . If  $\bar{R}_{\text{FB}} = \max\{2^{N\bar{R}_{12}}, 2^{N\bar{R}_{21}}\}$  then each bin contains exactly one message, and  $\bar{g}_i = g_i$ . Messages  $\bar{g}_i$  are exchanged using a  $\mathcal{C}^{\text{RC}}(2^{N\bar{R}_{\text{FB}}}, P_i, (1 - \lambda)N)$  code in each direction and respectively decoded as  $\hat{G}_{3-i}$ .

Observe as well that the compression following the generation of messages  $g_i$ , may cause binning (or hash) collisions in which a  $g_i$  containing an error may result in the same bin as the  $g_i$  of an error free transmission. We consider this and other possibilities when we analyze the probability of error of the scheme in Section IV.

**3. Alarm:** For this stage, each terminal compares the locally generated message bin index  $\bar{g}_i$  with the estimate  $\hat{G}_{3-i}$  obtained in the second stage. An alarm event is declared in

case of a mismatch. The result of this operation is sent to the other terminal using the single channel use signaling (5):

$$X_{i,N} = \begin{cases} 0, & \text{if } \bar{g}_i = \hat{G}_{3-i}, \\ \sqrt{\frac{P_i}{P(\text{Alarm})}}, & \text{otherwise.} \end{cases} \quad (5)$$

Thus, an alarm corresponds to a very high amplitude transmission since, as we show later in the Appendix of [1],  $P(\text{Alarm})$  is exponentially small (and also corresponds to the probability of a retransmission  $P(\text{Rtx})$ ). This transmission is decoded at the  $(3-i)$ -th terminal by comparing the received signal  $Y_{3-i,N}$  with a threshold  $\Upsilon = N$ , as in [15], where this signaling is introduced for the AWGN channel with active noisy feedback and the transmission of two messages. Moreover, it can be shown that the probability of error in decoding  $Y_{3-i,N}$  decays to zero faster than any exponential, hence without error.

When an alarm occurs, both terminals discard their preliminary estimates and initiate a retransmission, which means a repetition of the three stages using a new block of length  $N$  for the same message. Figure 2 illustrates three of these consecutive blocks. Stages have been colored to identify what message they are associated with and for which direction. We have depicted the transmission of a stream of messages indexed by  $(l)$ . The first block corresponds to the  $l$ -th messages being sent from both terminals and successfully decoded since no alarms are triggered. The second block corresponds to the transmission of the  $(l+1)$ -th messages. Note that terminal  $T_1$  triggers an alarm (colored in red), therefore, a retransmission is necessary for both directions, and occurs in the next block, where the three stages are repeated for messages  $(l+1)$ . This time, transmission is successful since no alarms are triggered, and both terminals can move to message  $(l+2)$  in the next block (not shown).

**Decoding rule:** Once the three stages have concluded, the  $i$ -th receiver declares that the message sent by the other terminal corresponds to the preliminary decision  $\hat{M}_{3-i}$  if no alarm is detected, otherwise, it awaits until the end of a new block of length  $N$  that conveys a retransmission. The final decoding decision occurs only in the absence of alarms, hence, multiple retransmissions may happen until both terminals can move to a new message.

#### IV. PROOF OF THEOREM 2

This section presents a short version of the proof of Theorem 2. We refer the reader to the Appendix A for the complete analysis. The proof consists of three parts: the analysis of the probability of error, the expected transmission time, and the error exponents. Here, we consider compressed feedback, since as we show in the Appendix of the extended version [1], this is related to the uncompressed one by the inclusion of an extra term in the overall probability of error.

##### A. Probability of error analysis

In the following, the feedback stage uses compression. We analyze the  $1 \rightarrow 2$  direction only, since the other follows by symmetry. Let the probability of error of the first and second

stages, meaning that a message sent (without feedback) is incorrectly decoded, be denoted as  $\overrightarrow{P}_{e_1}$  for the first stage, and  $\overrightarrow{P}_{e_2}$  for the second stage, where arrows indicate the communication direction. Then,

$$\begin{aligned} P_{\text{error}}^{1 \rightarrow 2} &= P(\hat{M}_1 \neq m_1, \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2) \\ &= P(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2) \\ &\quad + P(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2) \end{aligned} \quad (6)$$

The event  $\{\text{No-Alarm}\} \equiv \{(\hat{G}_1 = \bar{g}_2) \cap (\hat{G}_2 = \bar{g}_1)\}$ , means that no alarm occurs if both terminals declare that their *feedback message*  $\bar{g}_i$  matches the one received from the other terminal. As shown in the Appendix of [1], this probability can be upper bounded as:

$$P_{\text{err}}^{1 \rightarrow 2} \leq \max \left\{ \overrightarrow{P}_{e_2} \overleftarrow{P}_{e_2} \overrightarrow{P}_{e_1}, p_h \overrightarrow{P}_{e_1}, \overrightarrow{P}_{e_1} \overleftarrow{P}_{e_1} \right\} \quad (7)$$

$$P_{\text{err}}^{1 \leftarrow 2} \leq \max \left\{ \overleftarrow{P}_{e_2} \overrightarrow{P}_{e_2} \overleftarrow{P}_{e_1}, p_h \overleftarrow{P}_{e_1}, \overleftarrow{P}_{e_1} \overrightarrow{P}_{e_1} \right\} \quad (8)$$

##### B. Expected transmission time:

Recalling that a retransmission occurs when an alarm is declared at either terminal, the alarm event corresponds to:  $\{\text{Alarm}\} = \{(\hat{G}_2 \neq \bar{g}_1) \cup (\hat{G}_1 \neq \bar{g}_2)\}$ . Hence, a retransmission happens with probability  $P(\text{Rtx}) = P(\text{Alarm})$ :

$$\begin{aligned} P(\text{Rtx}) &= P\left(\left(\hat{G}_2 \neq \bar{g}_1\right) \cup \left(\hat{G}_1 \neq \bar{g}_2\right) \mid M_1 = m_1, M_2 = m_2\right) \\ &\leq P\left(\hat{G}_2 \neq \bar{g}_1 \mid M_1 = m_1, M_2 = m_2\right) \\ &\quad + P\left(\hat{G}_1 \neq \bar{g}_2 \mid M_1 = m_1, M_2 = m_2\right) \end{aligned}$$

As we show in the Appendix of [1],  $P(\text{Rtx}) \rightarrow 0$  as the block length  $N \rightarrow \infty$ . It follows that the expected transmission time is determined by the probability of retransmission, given as:

$$E[\Delta] = N \cdot \sum_{k=0}^{\infty} P(\text{Rtx})^k = N \cdot \frac{1}{1 - P(\text{Rtx})}$$

Thus,  $E[\Delta] \approx N$  when  $P(\text{Rtx}) \rightarrow 0$ .

##### C. Error exponents

Equations (7) and (8) describe the probability of error in terms of the following probabilities.

$$\begin{aligned} \overrightarrow{P}_{e_1} &\leq \exp \left\{ -N \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R}{\lambda}, \text{SNR}_{12} \right) \right\}, \\ \overrightarrow{P}_{e_2} &\leq \exp \left\{ -N (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R}{1 - \lambda}, \text{SNR}_{12} \right) \right\}, \\ \overleftarrow{P}_{e_1} &\leq \exp \left\{ -N \lambda E_{\text{AWGN}}^{\text{rc}} \left( \frac{R}{\lambda}, \text{SNR}_{21} \right) \right\}, \\ \overleftarrow{P}_{e_2} &\leq \exp \left\{ -N (1 - \lambda) E_{\text{AWGN}}^{\text{rc}} \left( \frac{R}{1 - \lambda}, \text{SNR}_{21} \right) \right\}. \end{aligned}$$

Note that in each of the probability of error terms shown above, the error exponent is scaled down by either  $\lambda$  or  $(1 - \lambda)$  depending on whether the term corresponds to the first or second stage of the scheme. Moreover, the instantaneous transmission rate is scaled up in order to compensate for the shorter block length (determined by duration of each stage) and to guarantee that the target operating rate-pair is achieved. Finally, it follows that from (7), an expected transmission time  $E[\Delta] \approx N$ , we have that for very large  $N$ :

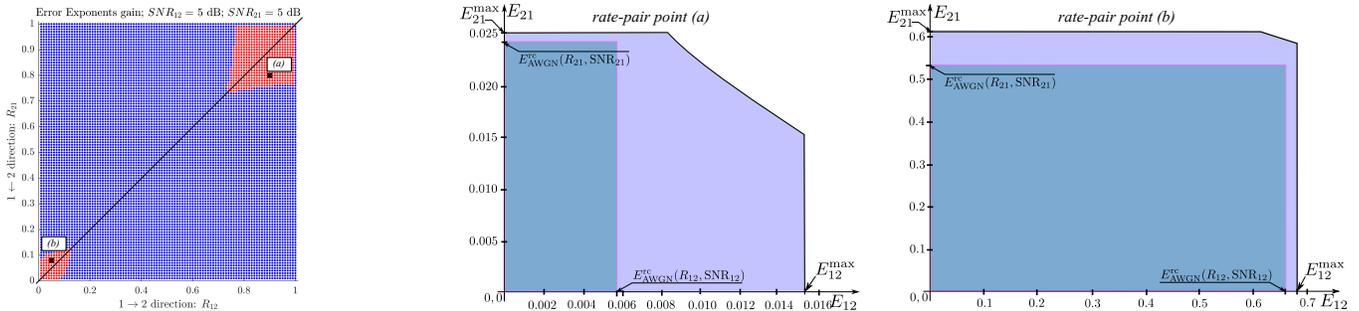


Fig. 3. Consider a two-way channel with  $\text{SNR}_{12} = \text{SNR}_{21} = 5\text{dB}$ . Left: Capacity region, where blue dots represent rate-pairs for which the random coding error exponent can be achieved. The red dots represent rate-pair for which the random coding error exponent can be exceeded for both directions. Center-Right: EER for the rate-pair point (a) ( $0.9C_{12}, 0.8C_{21}$ ), and rate-pair point (b) ( $0.02C_{12}, 0.08C_{21}$ ).

$$\frac{-1}{E[\Delta]} \ln P_{\text{error}}^{1 \rightarrow 2} \geq \frac{-1}{E[\Delta]} \min \left\{ \ln \left( \overrightarrow{P}_{e_2} \overleftarrow{P}_{e_2} \overrightarrow{P}_{e_1} \right), \ln \left( p_h \overleftarrow{P}_{e_1} \right), \ln \left( \overrightarrow{P}_{e_1} \overleftarrow{P}_{e_1} \right) \right\},$$

from which (3) is obtained. The result for the other direction follows by symmetry.

## V. NUMERICAL SIMULATIONS

This section presents numerical evaluations of our results. Figure 3-left presents the capacity region of a two-way AWGN channel where red color denotes the rate-pair regimes in which our schemes outperform the random coding error exponent simultaneously in both directions. In the center/right plots, we present the achievable error exponent regions for the rate-pair points marked as (a) and (b) in the capacity region. As a comparison reference, these plots also show the achievable EER by means of point-to-point transmissions and no cooperation, corresponding to the darker rectangle resulting from Proposition 1. Observe an interesting trade off between the error exponents of both directions. This is more dramatic for point (a), which is in the higher rate-pair regime. Also, note that for both points (a) and (b) it is possible to attain error exponents larger than Proposition 1 in both directions simultaneously.

Next, we evaluate Theorems 1 and 2 for the rate-pairs along the line that connects the points  $(0,0)$  and  $(C_{12}, C_{21})$  of the capacity region of the two-way AWGN channel (as shown in Figure 3-left with a solid black line). We considered a symmetric two-way channel in which both directions are of similar SNR. Figure 4 shows the largest error exponent achieved by the scheme in the  $1 \rightarrow 2$  direction. A similar plot would result for the opposite direction. The solid blue line presents the random coding error exponent lower bound, achievable when terminals do not interact. The dashed red line results by evaluating both Theorems and choosing the largest achievable error exponent. Note that there exists important error exponent gains in two regimes: lower (close to zero) and higher (close to capacity) rate regimes. In the remaining rate-pairs the scheme achieves the random coding error exponent.

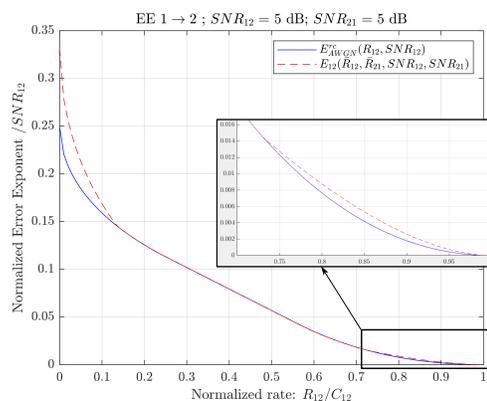


Fig. 4. Achievable error exponents for the  $1 \rightarrow 2$  direction for rates  $0 < \bar{R}_{12} \leq C_{12}$  for a Two-Way AWGN channel with  $\text{SNR}_{12} = \text{SNR}_{21} = 5\text{dB}$ . Error exponents are normalized over the SNR and evaluated for rate-pairs along the line connecting points  $(0,0)$  and  $(C_{12}, C_{21})$ , see Figure 3 (left).

## VI. CONCLUSION

The coding scheme we presented suggests that in a two-way AWGN channel, interaction may be exploited to improve (over non-feedback one-way error exponents under block coding) error exponents in both directions simultaneously – even when both directions have similar channel strength. Our feedback strategy correlates the errors in the two directions, and any terminal may trigger an alarm when the received feedback message does not match the one sent. This cooperation increases the error detection capabilities in both terminals. Moreover since we use variable length coding, a detected error can be corrected by the message retransmission that follows the occurrence of an alarm.

The expressions presented in Theorems 1 and 2 are mathematically involved. We have left analytically optimizing the parameters  $\lambda$  and  $R_{\text{FB}}$  for future work.

## REFERENCES

- [1] K. Palacio-Baus and N. Devroye, “Achievable error exponents for the two-way AWGN channel,” <https://devroye.lab.uic.edu/research-2/publications/>, 2020, [Extended version].
- [2] C. E. Shannon, “Two-way communications channels,” in *4th Berkeley Symp. Math. Stat. Prob.*, Chicago, IL, Jun. 1961, pp. 611–644.
- [3] H. Sato, “Two-user communication channels,” *IEEE Trans. Inf. Theory*, vol. 23, 1977.

- [4] T. Han, "A general coding scheme for the two-way channel," *IEEE Trans. Inf. Theory*, vol. IT-30, pp. 35–44, Jan. 1984.
- [5] C. Shannon, "The zero error capacity of a noisy channel," *IRE Transactions on Information Theory*, vol. 2, no. 3, pp. 8–19, Sept. 1956.
- [6] J. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback—I: No bandwidth constraint," *IEEE Transactions on Information Theory*, vol. 12, no. 2, pp. 172–182, Apr 1966.
- [7] A. Wyner, "On the Schalkwijk-Kailath coding scheme with a peak energy constraint," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 129–134, 1968.
- [8] A. Kramer, "Improving communication reliability by use of an intermittent feedback channel," *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 52–60, 1969.
- [9] J. Schalkwijk and M. Barron, "Sequential signaling under a peak power constraint," *IEEE Transactions on Information Theory*, vol. 17, no. 3, pp. 278–282, May 1971.
- [10] H. Yamamoto and K. Itoh, "Asymptotic performance of a modified Schalkwijk-Barron scheme for channels with noiseless feedback (Corresp.)," *IEEE Transactions on Information Theory*, vol. 25, no. 6, pp. 729–733, November 1979.
- [11] A. Sato and H. Yamamoto, "Error exponents of discrete memoryless channels and AWGN channels with noisy feedback," in *Proc. IEEE Int. Symp. Inf. Theory*, Oct 2010, pp. 452–457.
- [12] K. Palacio-Baus and N. Devroye, "Two-Way AWGN channel error exponents at zero-rate," in *Proc. IEEE Int. Symp. Inf. Theory*, 2018.
- [13] Z. Chance and D. J. Love, "Concatenated Coding for the AWGN Channel With Noisy Feedback," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6633–6649, 2011.
- [14] A. Ben-Yishai and O. Shayevitz, "Interactive Schemes for the AWGN Channel with Noisy Feedback," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2409–2427, April 2017.
- [15] Y. H. Kim, A. Lapidoth, and T. Weissman, "Error exponents for the Gaussian channel with active noisy feedback," *IEEE Transactions on Information Theory*, vol. 57, no. 3, pp. 1223–1236, March 2011.
- [16] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York:Wiley, 2006.
- [17] R. Gallager, *Information Theory and Reliable Communication*. New York, NY: Wiley, 1968.
- [18] K. Palacio-Baus and N. Devroye, "Achievable Error Exponents of the One-Way and Two-Way AWGN Channels," *Submitted to: IEEE Transactions on Information Theory*, December 2018.
- [19] S. C. Draper, K. Ramchandran, B. Rimoldi, A. Sahai, and D. Tse, "Attaining maximal reliability with minimal feedback via joint channel-code and hash-function design," *43th Annual Allerton conference on communication, control and computing*, 2005.

APPENDIX A  
PROOF OF THEOREM 1

This appendix presents the detailed derivation of our results. First we present the analysis for our scheme in which the feedback stage does not use compression, which implies some limitations on the rates for which error exponent improvements are possible. The use of compression is presented later in a different subsection.

1) **Probability of error analysis:** The probability of error in the  $1 \rightarrow 2$  direction is determined by the decoding rule of the scheme and given by:

$$\begin{aligned} P_{\text{error}}^{1 \rightarrow 2} &= P\left(\hat{M}_1 \neq m_1, \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2\right) + P\left(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2\right) \end{aligned}$$

For the feedback stage, each terminal generates and transmits message  $g_i$ , whereas it decodes the one sent from the other end as  $\hat{G}_{3-i}$ . Note that the event  $\{\text{No-Alarm}\} \equiv \{(\hat{G}_1 = g_2) \cap (\hat{G}_2 = g_1)\}$ . Meaning that no alarm would be detected at the system if both terminals declare that their *feedback message* match the one received from the other terminal. We analyze each term of the summation above as follows:

$$\begin{aligned} &P\left(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2\right) \cdot P\left(\hat{M}_1 \neq m_1 \mid \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \\ &\quad \underbrace{= 1 - \overleftarrow{P}_{e_1} \leq 1}_{\leq \overleftarrow{P}_{e_1}} \cdot \underbrace{P\left(\hat{M}_1 \neq m_1 \mid \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right)}_{\leq \overrightarrow{P}_{e_1}} \\ &\quad \cdot P\left(\text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \\ &\leq P\left(\text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \cdot \overrightarrow{P}_{e_1} \\ &= P\left(\underbrace{(\hat{G}_1 = g_2); (\hat{G}_2 = g_1)}_{\text{No-Alarm}} \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \cdot \overrightarrow{P}_{e_1} \\ &= P\left(\hat{G}_1 = g_2 \mid \hat{G}_2 = g_1, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \\ &\quad \cdot P\left(\hat{G}_2 = g_1 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2\right) \cdot \overrightarrow{P}_{e_1} \end{aligned} \tag{9}$$

In the following we let  $g_c$  to be the feedback message generated by the true messages  $m_1$  and  $m_2$ . The events given in the probability terms above imply:

$$\begin{aligned} \hat{M}_1 \neq m_1 &\implies g_2 \neq g_c \\ \hat{M}_2 = m_2 &\implies g_1 = g_c \end{aligned}$$

Then, (9) can be rewritten as:

$$\begin{aligned} &P\left(\text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2\right) \\ &\leq P\left(\hat{G}_1 = g_2 \mid \hat{G}_2 = g_1, \left(\hat{M}_1 \neq m_1 \implies g_2 \neq g_c\right), \left(\hat{M}_2 = m_2 \implies g_1 = g_c\right), M_1 = m_1, M_2 = m_2\right) \\ &\quad \cdot P\left(\hat{G}_2 = g_1 \mid \left(\hat{M}_1 \neq m_1 \implies g_2 \neq g_c\right), \left(\hat{M}_2 = m_2 \implies g_1 = g_c\right), M_1 = m_1, M_2 = m_2\right) \cdot \overrightarrow{P}_{e_1} \\ &= P\left(\underbrace{\hat{G}_1 = g_2 \mid \hat{G}_2 = g_1, \left(\hat{M}_1 \neq m_1 \implies g_2 \neq g_c\right), \left(\hat{M}_2 = m_2 \implies g_1 = g_c\right), M_1 = m_1, M_2 = m_2}_{\leq \overrightarrow{P}_{e_2}}\right) \\ &\quad \cdot \underbrace{P\left(\hat{G}_2 = g_1 \mid \left(\hat{M}_1 \neq m_1 \implies g_2 \neq g_c\right), \left(\hat{M}_2 = m_2 \implies g_1 = g_c\right), M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{P}_{e_2}} \cdot \overrightarrow{P}_{e_1} \end{aligned} \tag{10}$$

$$\leq \overrightarrow{P}_{e_2} \cdot \overleftarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_1} \tag{11}$$

Equation (11) results from the facts that for the first term in (10) we have that  $g_1 = g_c$  is sent, and we evaluate the probability that  $\hat{G}_1 = g_2$  (being  $g_2 \neq g_c$ ), so it is clearly upper bounded by the probability of error in the second stage. Similarly, when

$g_2 \neq g_c$  is being sent, we need the probability that  $\hat{G}_2 = g_1$ , (being  $g_1 = g_c$ ) which again, is upper bounded by the probability of error in the second stage of the scheme. Next, we proceed similarly with the second term of the sum in (9):

$$\begin{aligned}
& \text{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid \hat{M}_1 = m_1; \hat{M}_2 = m_2 \right) \\
&= \underbrace{\text{P} \left( \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2 \right)}_{\leq \overleftarrow{P}_{e_1}} \cdot \underbrace{\text{P} \left( \hat{M}_1 \neq m_1 \mid \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overrightarrow{P}_{e_1}} \\
&\quad \cdot \text{P} \left( \text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
&\leq \text{P} \left( \text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \\
&\leq \text{P} \left( \underbrace{(\hat{G}_1 = g_2); (\hat{G}_2 = g_1)}_{\text{No-Alarm}} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \\
&\leq \text{P} \left( \hat{G}_1 = g_2 \mid \hat{G}_2 = g_1, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
&\quad \cdot \text{P} \left( \hat{G}_2 = g_1 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \tag{12}
\end{aligned}$$

Since the events given in the probability terms above imply:

$$\begin{aligned}
\hat{M}_1 \neq m_1 &\implies g_2 \neq g_c \\
\hat{M}_2 \neq m_2 &\implies g_1 \neq g_c,
\end{aligned}$$

We can rewrite (12) as:

$$\begin{aligned}
& \text{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid \hat{M}_1 = m_1, \hat{M}_2 = m_2 \right) \\
&\leq \underbrace{\text{P} \left( \hat{G}_1 = g_2 \mid \hat{G}_2 = g_1, \left( \hat{M}_1 \neq m_1 \implies g_2 \neq g_c \right), \left( \hat{M}_2 \neq m_2 \implies g_1 \neq g_c \right), M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \\
&\quad \cdot \underbrace{\text{P} \left( \hat{G}_2 = g_1 \mid \left( \hat{M}_1 \neq m_1 \implies g_2 \neq g_c \right), \left( \hat{M}_2 \neq m_2 \implies g_1 \neq g_c \right), M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \cdot \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \\
&\leq \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \tag{13}
\end{aligned}$$

Above, we upper bound the two first factors by 1 since given an error in both transmissions of the first stage, we have that  $g_1 \neq g_c$  and  $g_2 \neq g_c$  (which does not mean that  $g_1 = g_2$  since both decoders may have reach distinct decoding errors). When these messages are fed back in the second stage, they may be decoded correctly or incorrectly, and since we cannot identify the exact error occurred in the first stage, we simply (and may loosely) decided to upper bound these probabilities by one. Note that any further analysis that may lead to tighter bounds can only improve the error exponent we derive here but upper bounding this factors by one.

Next, considering the overall probability of error upper bound shown in (6), and the upper bound of both summing terms (11) and (13), it follows that:

$$\overrightarrow{P}_{\text{err}} \leq \overrightarrow{P}_{e_2} \cdot \overleftarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_1} + \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1}.$$

An equivalent result can be obtained for the other direction:

$$\begin{aligned}
P_{\text{error}}^{1 \leftarrow 2} &= \text{P} \left( \hat{M}_2 \neq m_2; \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2 \right) \\
&= \text{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2 \right) + \text{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2 \right) \tag{14}
\end{aligned}$$

Similarly, analyzing each term in the sum above separately, we have:

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2 \right) \\
&= \underbrace{\mathbb{P} \left( \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2 \right)}_{=1 - \overrightarrow{\mathbb{P}}_{e_1} \leq 1} \cdot \underbrace{\mathbb{P} \left( \hat{M}_2 \neq m_2 \mid \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overleftarrow{\mathbb{P}}_{e_1}} \\
&\quad \cdot \mathbb{P} \left( \text{No-Alarm} \mid \hat{M}_2 \neq m_2, \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2 \right) \\
&\leq \mathbb{P} \left( \underbrace{(\hat{G}_1 = g_2); (\hat{G}_2 = g_1)}_{\text{No-Alarm}} \mid \hat{M}_2 \neq m_2, \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2 \right) \cdot \overleftarrow{\mathbb{P}}_{e_1} \\
&= \mathbb{P} \left( \hat{G}_2 = g_1 \mid \hat{G}_1 = g_2, \hat{M}_2 \neq m_2, \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2 \right) \\
&\quad \cdot \mathbb{P} \left( \hat{G}_1 = g_2 \mid \hat{M}_2 \neq m_2, \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2 \right) \cdot \overleftarrow{\mathbb{P}}_{e_1} \tag{15}
\end{aligned}$$

Then, recalling that:

$$\begin{aligned}
\hat{M}_2 \neq m_2 &\implies g_1 \neq g_c \\
\hat{M}_1 = m_1 &\implies g_2 = g_c
\end{aligned}$$

It follows that (15):

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2 \right) \\
&\leq \underbrace{\mathbb{P} \left( \hat{G}_2 = g_1 \mid \hat{G}_1 = g_2, \left( \hat{M}_2 \neq m_2 \implies g_1 \neq g_c \right), \left( \hat{M}_1 = m_1 \implies g_2 = g_c \right), M_1 = m_1, M_2 = m_2 \right)}_{\leq \overleftarrow{\mathbb{P}}_{e_2}} \\
&\quad \cdot \underbrace{\mathbb{P} \left( \hat{G}_1 = g_2 \mid \left( \hat{M}_2 \neq m_2 \implies g_1 \neq g_c \right), \left( \hat{M}_1 = m_1 \implies g_2 = g_c \right), M_1 = m_1, M_2 = m_2 \right)}_{\overrightarrow{\mathbb{P}}_{e_2}} \cdot \overleftarrow{\mathbb{P}}_{e_1} \\
&\leq \overleftarrow{\mathbb{P}}_{e_2} \cdot \overrightarrow{\mathbb{P}}_{e_2} \cdot \overleftarrow{\mathbb{P}}_{e_1} \tag{16}
\end{aligned}$$

Similarly, proceeding with the second term in the sum of (14):

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2 \right) \\
&= \underbrace{\mathbb{P} \left( \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2 \right)}_{\leq \overrightarrow{\mathbb{P}}_{e_1}} \cdot \underbrace{\mathbb{P} \left( \hat{M}_2 \neq m_2 \mid \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overleftarrow{\mathbb{P}}_{e_1}} \\
&\quad \cdot \mathbb{P} \left( \text{No-Alarm} \mid \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right) \\
&\leq \mathbb{P} \left( \underbrace{(\hat{G}_1 = g_2); (\hat{G}_2 = g_1)}_{\text{No-Alarm}} \mid \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{\mathbb{P}}_{e_1} \cdot \overleftarrow{\mathbb{P}}_{e_1} \\
&= \mathbb{P} \left( \hat{G}_2 = g_1 \mid \hat{G}_1 = g_2, \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right) \\
&\quad \cdot \mathbb{P} \left( \hat{G}_1 = g_2 \mid \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{\mathbb{P}}_{e_1} \cdot \overleftarrow{\mathbb{P}}_{e_1} \tag{17}
\end{aligned}$$

It follows that (17) can be written as:

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \hat{M}_2 \neq m_2; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2 \right) \\
&\leq \underbrace{\mathbb{P} \left( \hat{G}_2 = g_1 \mid \hat{G}_1 = g_2, \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \\
&\quad \cdot \underbrace{\mathbb{P} \left( \hat{G}_1 = g_2 \mid \hat{M}_2 \neq m_2, \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \cdot \overrightarrow{\mathbb{P}}_{e_1} \cdot \overleftarrow{\mathbb{P}}_{e_1} \\
&\leq \overrightarrow{\mathbb{P}}_{e_1} \cdot \overleftarrow{\mathbb{P}}_{e_1} \tag{18}
\end{aligned}$$

Finally, taking (14), and replacing the corresponding upper bound for its two terms from (16) and (18), we have that an upper bound on the overall probability of error in the  $1 \leftarrow 2$  direction is:

$$P_{\text{error}}^{1 \leftarrow 2} \leq \overleftarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_2} \cdot \overleftarrow{P}_{e_1} + \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_1}$$

We have obtained that under a per block expected block power constraint  $E \left[ \frac{1}{N} \sum_{i=1}^N X_i^2 \right] \leq P$ , the probabilities of error for both directions is:

$$P_{\text{error}}^{1 \rightarrow 2} \leq \max \left\{ \overrightarrow{P}_{e_2} \overleftarrow{P}_{e_2} \overrightarrow{P}_{e_1}, \overrightarrow{P}_{e_1} \overleftarrow{P}_{e_1} \right\} \quad (19)$$

$$P_{\text{error}}^{1 \leftarrow 2} \leq \max \left\{ \overleftarrow{P}_{e_2} \overrightarrow{P}_{e_2} \overleftarrow{P}_{e_1}, \overleftarrow{P}_{e_1} \overrightarrow{P}_{e_1} \right\} \quad (20)$$

2) **Expected transmission time:** A retransmission occurs when an alarm is declared at any terminal, that is, when the feedback message generated locally does not match that received from the other end. Thus the event alarm corresponds to:  $\{\text{Alarm}\} = \{(\hat{G}_2 \neq g_1) \cup (\hat{G}_1 \neq g_2)\}$ . This means that a retransmission happens with the probability of occurrence of this event, which we denote by  $P(\text{Rtx})$ :

$$\begin{aligned} P(\text{Rtx}) &= P(\text{Alarm} \mid M_1 = m_1, M_2 = m_2) \\ &= P\left((\hat{G}_2 \neq g_1) \cup (\hat{G}_1 \neq g_2) \mid M_1 = m_1, M_2 = m_2\right) \\ &\leq P\left(\hat{G}_2 \neq g_1 \mid M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_1 \neq g_2 \mid M_1 = m_1, M_2 = m_2\right) \end{aligned} \quad (21)$$

Next we upper bound each of the two terms above as follows. For the left hand side term of (21):

$$P\left(\hat{G}_2 \neq g_1 \mid M_1 = m_1, M_2 = m_2\right) = P\left(\hat{G}_2 \neq g_1, g_1 = g_c \mid M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_2 \neq g_1, g_1 \neq g_c \mid M_1 = m_1, M_2 = m_2\right) \quad (22)$$

We analyze each of the two terms of (22) separately, thus for the left term:

$$\begin{aligned} &P\left(\hat{G}_2 \neq g_1, g_1 = g_c \mid M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_2 \neq g_1 \mid g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \underbrace{P(g_1 = g_c \mid M_1 = m_1, M_2 = m_2)}_{=1 - \overleftarrow{P}_{e_1} \leq 1} \\ &\leq P\left(\hat{G}_2 \neq g_1 \mid g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_2 \neq g_c; g_2 = g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_2 \neq g_c; g_2 \neq g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_2 \neq g_c \mid g_2 = g_c, g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot P(g_2 = g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2) \\ &\quad + P\left(\hat{G}_2 \neq g_c \mid g_2 \neq g_c, g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot P(g_2 \neq g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2) \\ &= P\left(\hat{G}_2 \neq g_c \mid g_2 = g_c, g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \underbrace{P(g_2 = g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2)}_{=1 - \overrightarrow{P}_{e_1} \leq 1} \\ &\quad + P\left(\hat{G}_2 \neq g_c \mid g_2 \neq g_c, g_1 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \underbrace{P(g_2 \neq g_c \mid g_1 = g_c, M_1 = m_1, M_2 = m_2)}_{\leq \overrightarrow{P}_{e_1}} \\ &\leq \overleftarrow{P}_{e_2} + \overrightarrow{P}_{e_1} \end{aligned} \quad (23)$$

Now, we proceed with the right hand side term of (22):

$$\begin{aligned}
& \mathbb{P}\left(\hat{G}_2 \neq g_1, g_1 \neq g_c \mid M_1 = m_1, M_2 = m_2\right) \\
&= \mathbb{P}\left(\hat{G}_2 \neq g_1 \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right) \cdot \underbrace{\mathbb{P}\left(g_1 \neq g_c \mid M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{P}_{e_1}} \\
&\leq \mathbb{P}\left(\hat{G}_2 \neq g_1 \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right) \cdot \overleftarrow{P}_{e_1} \\
&= \left[ \mathbb{P}\left(\hat{G}_2 \neq g_1; g_2 = g_c \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right) + \mathbb{P}\left(\hat{G}_2 \neq g_1; g_2 \neq g_c \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right) \right] \cdot \overleftarrow{P}_{e_1} \\
&= \underbrace{\mathbb{P}\left(\hat{G}_2 \neq g_1 \mid g_2 = g_c, g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq 1} \cdot \underbrace{\mathbb{P}\left(g_2 = g_c \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - \overrightarrow{P}_{e_1} \leq 1} \cdot \overleftarrow{P}_{e_1} \\
&\quad + \underbrace{\mathbb{P}\left(\hat{G}_2 \neq g_1 \mid g_2 \neq g_c, g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq 1} \cdot \underbrace{\mathbb{P}\left(g_2 \neq g_c \mid g_1 \neq g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overrightarrow{P}_{e_1}} \cdot \overleftarrow{P}_{e_1} \\
&\leq \overleftarrow{P}_{e_1} + \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_1}
\end{aligned} \tag{24}$$

Thus, we have from (22), (23) and (24):

$$\mathbb{P}\left(\hat{G}_2 \neq g_1 \mid M_1 = m_1, M_2 = m_2\right) \leq \left(\overleftarrow{P}_{e_2} + \overrightarrow{P}_{e_1}\right) + \left(\overleftarrow{P}_{e_1} + \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_1}\right)$$

We now proceed in a similar way for the right hand side term of (21):

$$\begin{aligned}
& \mathbb{P}\left(\hat{G}_1 \neq g_2 \mid M_1 = m_1, M_2 = m_2\right) \\
&= \mathbb{P}\left(\hat{G}_1 \neq g_2; g_2 = g_c \mid M_1 = m_1, M_2 = m_2\right) + \mathbb{P}\left(\hat{G}_1 \neq g_2; g_2 \neq g_c \mid M_1 = m_1, M_2 = m_2\right)
\end{aligned} \tag{25}$$

We analyze each of the terms summing up in (25) separately, thus for the left hand side term:

$$\begin{aligned}
& \mathbb{P}\left(\hat{G}_1 \neq g_2; g_2 = g_c \mid M_1 = m_1, M_2 = m_2\right) \\
&= \mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \underbrace{\mathbb{P}\left(g_2 = g_c \mid M_1 = m_1, M_2 = m_2\right)}_{=1 - \overrightarrow{P}_{e_1} \leq 1} \\
&\leq \mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \\
&= \mathbb{P}\left(\hat{G}_1 \neq g_2; g_1 = g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) + \mathbb{P}\left(\hat{G}_1 \neq g_2; g_1 \neq g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \\
&= \mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_1 = g_c, g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \mathbb{P}\left(g_1 = g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \\
&\quad + \mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_1 \neq g_c, g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \cdot \mathbb{P}\left(g_1 \neq g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_1 = g_c, g_2 = g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overrightarrow{P}_{e_2}} \cdot \underbrace{\mathbb{P}\left(g_1 = g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - \overleftarrow{P}_{e_1} \leq 1} \\
&\quad + \underbrace{\mathbb{P}\left(\hat{G}_1 \neq g_2 \mid g_1 \neq g_c, g_2 = g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq 1} \cdot \underbrace{\mathbb{P}\left(g_1 \neq g_c \mid g_2 = g_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{P}_{e_1}} \\
&\leq \overrightarrow{P}_{e_2} + \overleftarrow{P}_{e_1}
\end{aligned} \tag{26}$$

Similarly for the right hand side term of (25):

$$\begin{aligned}
& \mathbb{P} \left( \hat{G}_1 \neq g_2; g_2 \neq g_c \mid M_1 = m_1, M_2 = m_2 \right) \\
&= \mathbb{P} \left( \hat{G}_1 \neq g_2 \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right) \cdot \underbrace{\mathbb{P} (g_2 \neq g_c \mid M_1 = m_1, M_2 = m_2)}_{\leq \bar{P}_{e_1}} \\
&\leq \mathbb{P} \left( \hat{G}_1 \neq g_2 \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \\
&= \left[ \mathbb{P} \left( \hat{G}_1 \neq g_2; g_1 = g_c \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right) + \mathbb{P} \left( \hat{G}_1 \neq g_2; g_1 \neq g_c \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right) \right] \cdot \bar{P}_{e_1} \\
&= \underbrace{\mathbb{P} \left( \hat{G}_1 \neq g_2 \mid g_1 = g_c, g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \cdot \underbrace{\mathbb{P} (g_1 = g_c \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2)}_{=1 - \bar{P}_{e_1} \leq 1} \cdot \bar{P}_{e_1} \\
&\quad + \underbrace{\mathbb{P} \left( \hat{G}_1 \neq g_2 \mid g_1 \neq g_c, g_2 \neq g_c, M_1 = m_1, M_2 = m_2 \right)}_{\leq 1} \cdot \underbrace{\mathbb{P} (g_1 \neq g_c \mid g_2 \neq g_c, M_1 = m_1, M_2 = m_2)}_{\leq \bar{P}_{e_1}} \cdot \bar{P}_{e_1} \\
&\leq \bar{P}_{e_1} + \bar{P}_{e_1} \cdot \bar{P}_{e_1}
\end{aligned} \tag{27}$$

Finally, taking (25), (26) and (27), we obtain:

$$\mathbb{P} \left( \hat{G}_1 \neq g_2 \mid M_1 = m_1, M_2 = m_2 \right) \leq \left( \bar{P}_{e_2} + \bar{P}_{e_1} \right) + \left( \bar{P}_{e_1} + \bar{P}_{e_1} \cdot \bar{P}_{e_1} \right)$$

Thus, from (21) we see that the probability of alarm is given by:

$$\begin{aligned}
\mathbb{P}(\text{Rtx}) &\leq \mathbb{P} \left( \hat{G}_2 \neq g_1 \mid M_1 = m_1, M_2 = m_2 \right) + \mathbb{P} \left( \hat{G}_1 \neq g_2 \mid M_1 = m_1, M_2 = m_2 \right) \\
&\leq \left( \bar{P}_{e_2} + \bar{P}_{e_1} \right) + \left( \bar{P}_{e_1} + \bar{P}_{e_1} \cdot \bar{P}_{e_1} \right) + \left( \bar{P}_{e_2} + \bar{P}_{e_1} \right) + \left( \bar{P}_{e_1} + \bar{P}_{e_1} \cdot \bar{P}_{e_1} \right) \\
&= \bar{P}_{e_2} + 2 \cdot \bar{P}_{e_1} + 2 \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1} + 2 \cdot \bar{P}_{e_1} + \bar{P}_{e_2}
\end{aligned} \tag{28}$$

Note from (28) that  $\mathbb{P}(\text{Rtx}) \rightarrow 0$  as the block length  $N \rightarrow \infty$ . This occurs since each of the summing terms in (28) decays exponentially as  $N \rightarrow \infty$ . It follows that the expected transmission time is determined by the probability of retransmission, given as:

$$\begin{aligned}
\mathbb{E}[\Delta] &= N \cdot [\mathbb{P}(\text{Rtx})]^0 + N \cdot [\mathbb{P}(\text{Rtx})]^1 + \dots + N \cdot [\mathbb{P}(\text{Rtx})]^\infty \\
&= N \cdot \sum_{k=0}^{\infty} \cdot \mathbb{P}(\text{Rtx})^k = N \cdot \frac{1}{1 - \mathbb{P}(\text{Rtx})}
\end{aligned}$$

Thus,  $\mathbb{E}[\Delta] \approx N$  when  $\mathbb{P}(\text{Rtx}) \rightarrow 0$ .

3) **Error exponents:** Finally, the error exponent in Theorem 1 can be obtained using (19) and (20), and the expected transmission time derived above.

APPENDIX B  
PROOF OF THEOREM 2

This section consider the case in which the feedback message transmission utilizes a hashing compression method.

1) *Probability of error analysis*:

$$\begin{aligned} P_{\text{err}}^{1 \rightarrow 2} &= \mathbb{P} \left( \hat{M}_1 \neq m_1; \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2 \right) \\ &= \mathbb{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2 \right) + \mathbb{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2 \right) \end{aligned} \quad (29)$$

Note that when compression is used, the event  $\{\text{No-Alarm}\} \equiv \{(\hat{G}_1 = \bar{g}_2) \cap (\hat{G}_2 = \bar{g}_1)\}$ , where we have used the bin indexes (or hashing). The notation using a bar on top of a variable, such as in  $\bar{g}_i$ , refers to index of the bin that contains message  $g_i$ . When this is sent to the other terminal ( $3 - i$ ), it is estimated as  $\hat{G}_i$ . We analyze each term of the summation above as follows.

For the left hand side of (29), the following holds:

- $(\hat{M}_2 = m_2) \implies g_1 = g_c$ : Since  $g_1$  corresponds to the correct feedback message, it is assigned to the correct bin, whose index is transmitted to terminal 2 in the feedback stage over the  $1 \rightarrow 2$  noisy channel.
- $(\hat{M}_1 \neq m_1) \implies g_2 \neq g_c$ : The transmission error in the first stage causes that  $g_2$  is not the correct feedback message. When this message is assigned to a bin, it may either be: wrongly assigned to the same bin as the correct message  $g_c$  which we denote as a **hash-collision**; or, assigned to a bin different from the one holding the correct feedback message  $g_c$ . The probability of a hash-collision is  $p_h = \frac{1}{2^{N_{\text{FB}}}}$ .

$$\begin{aligned} &\mathbb{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2 \right) \\ &= \underbrace{\mathbb{P} \left( \hat{M}_2 = m_2 \mid M_1 = m_1, M_2 = m_2 \right)}_{=1 - \overrightarrow{P}_{e_1} \leq 1} \cdot \underbrace{\mathbb{P} \left( \hat{M}_1 \neq m_1 \mid \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overrightarrow{P}_{e_1}} \\ &\quad \cdot \mathbb{P} \left( \text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \\ &\leq \mathbb{P} \left( \text{No-Alarm; No Hash-Collision } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{P}_{e_1} \\ &\quad + \mathbb{P} \left( \text{No-Alarm; Hash-Collision } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{P}_{e_1} \\ &= \mathbb{P} \left( \text{No-Alarm} \mid \text{No Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \\ &\quad \cdot \underbrace{\mathbb{P} \left( \text{No Hash-Collision } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{=1 - p_h \leq 1} \cdot \overrightarrow{P}_{e_1} \\ &\quad + \mathbb{P} \left( \text{No-Alarm} \mid \text{Hash-Collision } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \\ &\quad \cdot \underbrace{\mathbb{P} \left( \text{Hash-Collision } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{=p_h} \cdot \overrightarrow{P}_{e_1} \\ &= \mathbb{P} \left( \text{No-Alarm} \mid \text{No Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{P}_{e_1} \\ &\quad + \mathbb{P} \left( \text{No-Alarm} \mid \text{Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \cdot \overrightarrow{P}_{e_1} \\ &= \mathbb{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{No Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \overrightarrow{P}_{e_1} \\ &\quad + \mathbb{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \cdot \overrightarrow{P}_{e_1} \\ &= \underbrace{\mathbb{P} \left( \hat{G}_1 = \bar{g}_2 \mid \hat{G}_2 = \bar{g}_1, \text{No Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overrightarrow{P}_{e_2}} \cdot \overrightarrow{P}_{e_1} \end{aligned}$$

$$\begin{aligned}
& \cdot \underbrace{\left( \hat{G}_2 = \bar{g}_1 \mid \text{No Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \bar{P}_{e_2}} \\
& + \underbrace{\left( \hat{G}_1 = \bar{g}_2 \mid \hat{g}_2 = \bar{g}_1, \text{Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{=1 - \bar{P}_{e_2} \leq 1} \cdot p_h \cdot \bar{P}_{e_1} \\
& \cdot \underbrace{\left( \hat{G}_2 = \bar{g}_1 \mid \text{Hash-Collision } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 = m_2, M_1 = m_1, M_2 = m_2 \right)}_{=1 - \bar{P}_{e_2} \leq 1} \\
& \leq \bar{P}_{e_2} \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_2} + p_h \cdot \bar{P}_{e_1}
\end{aligned} \tag{30}$$

$$\leq \bar{P}_{e_2} \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_2} + p_h \cdot \bar{P}_{e_1} \tag{31}$$

For the first line of (30), we have that given  $g_2 \neq g_c$  and since there is no hash-collision, thus  $\bar{g}_2 \neq \bar{g}_c$ . Then, since  $g_1 = g_c$ , we also have that  $\bar{g}_1 = \bar{g}_c$  is sent as the feedback message, and this term is upper bounded by the probability of error in the feedback stage. This upper bound results since this term indicates the error of decoding the feedback message as  $\bar{g}_c$ . For the second line, similarly,  $\bar{g}_2 \neq \bar{g}_c$  is sent, and since  $\bar{g}_1 = \bar{g}_c$ , then the probability of this event is upper bounded by the probability of error in the feedback stage. The third line, the hash collision causes that  $\bar{g}_2 = \bar{g}_c$ , thus, since  $\bar{g}_1 = \bar{g}_c$  is sent, then the probability of this event is can be upper bounded by one. Finally, in the fourth line, the hash-collision causes  $\bar{g}_2 = \bar{g}_c$  is sent. Then, since  $\bar{g}_1 = \bar{g}_c$ , this probability is upper bounded also by one.

Observe that (31) corresponds to the term (11) plus an additional term that results from a hashing error.

Next, for the right hand side of (29), the following holds:

- $(\hat{M}_2 \neq m_2) \implies g_1 \neq g_c$ : The transmission error in the first stage causes that  $g_1$  is not the correct feedback message. When this message is assigned to a bin, it may either be: wrongly assigned to the same bin as the correct message  $g_c$  which we denoted as a hash-collision; or, assigned to a bin different from the one holding the correct feedback message  $g_c$ . The probability of a hash-collision is  $p_h = \frac{1}{2^{N_{\text{FB}}}}$ .
- $(\hat{M}_1 \neq m_1) \implies g_2 \neq g_c$ : The transmission error in the first stage causes that  $g_2$  is not the correct feedback message. When this message is assigned to a bin, it may either be: wrongly assigned to the same bin as the correct message  $g_c$  which we denoted as a hash-collision; or, assigned to a bin different from the one holding the correct feedback message  $g_c$ . The probability of a hash-collision is  $p_h = \frac{1}{2^{N_{\text{FB}}}}$ .

$$\begin{aligned}
& \text{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2 \right) \\
& = \underbrace{\text{P} \left( \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2 \right)}_{\leq \bar{P}_{e_1}} \cdot \underbrace{\text{P} \left( \hat{M}_1 \neq m_1 \mid \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \bar{P}_{e_1}} \\
& \cdot \text{P} \left( \text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \leq \text{P} \left( \text{No-Alarm} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1} \\
& = \text{P} \left( \text{No-Alarm}; \text{No Hash-Col } T_1; \text{No Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1} \\
& + \text{P} \left( \text{No-Alarm}; \text{No Hash-Col } T_1; \text{Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1} \\
& + \text{P} \left( \text{No-Alarm}; \text{Hash-Col } T_1; \text{No Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1} \\
& + \text{P} \left( \text{No-Alarm}; \text{Hash-Col } T_1; \text{Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot \bar{P}_{e_1} \cdot \bar{P}_{e_1}
\end{aligned} \tag{32}$$

We analyze each of the four terms with events described in parenthesis from (32) as follows. Then, for the first term:

$$\begin{aligned}
& \text{P} \left( \text{No-Alarm}; \text{No Hash-Col } T_1; \text{No Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& = \text{P} \left( \underbrace{\text{No Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2}_{=1 - p_h \leq 1} \right) \\
& \cdot \text{P} \left( \underbrace{\text{No Hash-Col } T_1 \mid \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2}_{=1 - p_h \leq 1} \right)
\end{aligned}$$

$$\begin{aligned}
& \cdot \mathbb{P} \left( \text{No-Alarm} \mid \text{No Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \leq \mathbb{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{No Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& = \mathbb{P} \left( \hat{G}_1 = \bar{g}_2 \mid \hat{G}_2 = \bar{g}_1, \text{No Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \quad \leq 1 \\
& \cdot \mathbb{P} \left( \hat{G}_2 = \bar{g}_1 \mid \text{No Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \leq 1 \tag{33} \\
& \quad \leq 1
\end{aligned}$$

The upper bounds in (33) result since  $\bar{g}_1 \neq \bar{g}_c$  and  $\bar{g}_2 \neq \bar{g}_c$  are sent as the corresponding feedback messages, and they could be either decoded correctly or incorrectly, so we opted by simply upper bound them by one. Note that a more precise analysis that could be performed in these terms can only improve our results.

For the second term in (32) we have:

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \text{No Hash-Col } T_1; \text{Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& = \mathbb{P} \left( \underbrace{\text{Hash-Col } T_2}_{=p_h} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \cdot \mathbb{P} \left( \underbrace{\text{No Hash-Col } T_1}_{=1-p_h \leq 1} \mid \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \cdot \mathbb{P} \left( \text{No-Alarm} \mid \text{No Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \leq \mathbb{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{No Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \\
& = \mathbb{P} \left( \hat{G}_1 = \bar{g}_2 \mid \hat{G}_2 = \bar{g}_1, \text{No Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \quad \leq \overrightarrow{P_{e_2}} \\
& \cdot \mathbb{P} \left( \hat{G}_2 = \bar{g}_1 \mid \text{No Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \\
& \quad \leq \overleftarrow{P_{e_2}} \\
& \leq \overrightarrow{P_{e_2}} \cdot \overleftarrow{P_{e_2}} \cdot p_h
\end{aligned}$$

Note that since  $g_1 \neq g_c$ , the event ‘‘No Hash-Col’’  $T_1$  implies that  $\bar{g}_1 \neq \bar{g}_c$ . Moreover, since  $g_2 \neq g_c$  the event ‘‘Hash-Col’’  $T_2$  implies that  $\bar{g}_2 = \bar{g}_c$ .

For the third term in (32) we have:

$$\begin{aligned}
& \mathbb{P} \left( \text{No-Alarm}; \text{Hash-Col } T_1; \text{No Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& = \mathbb{P} \left( \underbrace{\text{No Hash-Col } T_2}_{=1-p_h \leq 1} \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \cdot \mathbb{P} \left( \underbrace{\text{Hash-Col } T_1}_{=p_h} \mid \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \cdot \mathbb{P} \left( \text{No-Alarm} \mid \text{Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \leq \mathbb{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \\
& = \mathbb{P} \left( \hat{G}_2 = \bar{g}_1 \mid \text{Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\
& \quad \leq \overleftarrow{P_{e_2}}
\end{aligned}$$

$$\begin{aligned} & \cdot \underbrace{\left( \hat{G}_1 = \bar{g}_2 \mid \hat{G}_2 = \bar{g}_1, \text{Hash-Col } T_1, \text{No Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{\leq \overrightarrow{P}_{e_2}} \cdot p_h \\ & \leq \overleftarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_2} \cdot p_h \end{aligned}$$

Since  $g_1 \neq g_c$ , the event ‘‘Hash-Col’’  $T_1$  implies that  $\bar{g}_1 = \bar{g}_c$ . Moreover, since  $g_2 \neq g_c$  the event ‘‘No Hash-Col’’  $T_2$  implies that  $\bar{g}_2 \neq \bar{g}_c$ .

Finally, for the last term in (32) we have:

$$\begin{aligned} & \text{P} \left( \text{No-Alarm}; \text{Hash-Col } T_1; \text{Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\ & = \underbrace{\text{P} \left( \text{Hash-Col } T_2 \mid \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{=p_h} \\ & \cdot \underbrace{\left( \text{Hash-Col } T_1 \mid \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{=p_h} \\ & \cdot \text{P} \left( \text{No-Alarm} \mid \text{Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \\ & \leq \text{P} \left( \underbrace{(\hat{G}_1 = \bar{g}_2); (\hat{G}_2 = \bar{g}_1)}_{\text{No-Alarm}} \mid \text{Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right) \cdot p_h \cdot p_h \\ & = \underbrace{\text{P} \left( \hat{G}_1 = \bar{g}_2 \mid \hat{G}_2 = \bar{g}_1, \text{Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{=1-\overrightarrow{P}_{e_2} \leq 1} \\ & \cdot \underbrace{\left( \hat{G}_2 = \bar{g}_1 \mid \text{Hash-Col } T_1, \text{Hash-Col } T_2, \hat{M}_1 \neq m_1, \hat{M}_2 \neq m_2, M_1 = m_1, M_2 = m_2 \right)}_{=1-\overleftarrow{P}_{e_2} \leq 1} \cdot p_h \cdot p_h \\ & \leq p_h \cdot p_h \end{aligned}$$

Since there are hash-collisions at both terminals: we have that  $g_1 \neq g_c$  and the event ‘‘Hash-Col’’  $T_1$  implies that  $\bar{g}_1 = \bar{g}_c$ . Moreover, since  $g_2 \neq g_c$  the event ‘‘Hash-Col’’  $T_2$  implies that  $\bar{g}_2 = \bar{g}_c$ .

It follows from (32) that:

$$\begin{aligned} & \text{P} \left( \text{No-Alarm}; \hat{M}_1 \neq m_1; \hat{M}_2 \neq m_2 \mid M_1 = m_1, M_2 = m_2 \right) \\ & \leq \underbrace{\overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1}}_{\text{Dominant term}} + \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_2} \cdot \overleftarrow{P}_{e_2} \cdot p_h + \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_2} \cdot h + \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \cdot p_h \cdot p_h \\ & \doteq \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \end{aligned} \tag{34}$$

Hence, from (29), (31) and (34) we obtain:

$$\begin{aligned} \text{P}_{\text{error}}^{1 \rightarrow 2} & = \text{P} \left( \hat{M}_1 \neq m_1, \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2 \right) \\ & \leq \overrightarrow{P}_{e_2} \cdot \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_2} + p_h \cdot \overrightarrow{P}_{e_1} + \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_1} \\ \text{P}_{\text{error}}^{1 \leftarrow 2} & = \text{P} \left( \hat{M}_1 \neq m_1, \text{No-Alarm} \mid M_1 = m_1, M_2 = m_2 \right) \\ & \leq \overleftarrow{P}_{e_2} \cdot \overleftarrow{P}_{e_1} \cdot \overrightarrow{P}_{e_2} + p_h \cdot \overleftarrow{P}_{e_1} + \overrightarrow{P}_{e_1} \cdot \overleftarrow{P}_{e_1}, \end{aligned}$$

where results for the other direction follow by symmetry.

2) *Transmission time under compressed feedback*: A retransmission occurs when an alarm is declared at any of both terminals, that is, when the feedback stage result does not match the result of the first stage. Thus the event alarm corresponds to:  $\{\text{Alarm}\} = \{(\hat{G}_2 \neq \bar{g}_1) \cup (\hat{G}_1 \neq \bar{g}_2)\}$ . This means that a retransmission happens with the probability of occurrence of this event, which we denote by  $P(\text{Rtx})$ :

$$\begin{aligned} P(\text{Rtx}) &= P(\text{Alarm} \mid M_1 = m_1, M_2 = m_2) \\ &= P\left(\left(\hat{G}_2 \neq \bar{g}_1\right) \cup \left(\hat{G}_1 \neq \bar{g}_2\right) \mid M_1 = m_1, M_2 = m_2\right) \\ &\leq P\left(\hat{G}_2 \neq \bar{g}_1 \mid M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_1 \neq \bar{g}_2 \mid M_1 = m_1, M_2 = m_2\right) \end{aligned} \quad (35)$$

In the following, we denote the bin index corresponding to the correct message as  $\bar{g}_c$ . We consider each term of (35) as follows, for the right hand side term:

$$\begin{aligned} &P\left(\hat{G}_1 \neq \bar{g}_2 \mid M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_2 = \bar{g}_c \mid M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_2 \neq \bar{g}_c \mid M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \cdot P\left(\bar{g}_2 = \bar{g}_c \mid M_1 = m_1, M_2 = m_2\right) \\ &\quad + P\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \cdot P\left(\bar{g}_2 \neq \bar{g}_c \mid M_1 = m_1, M_2 = m_2\right) \\ &= \left[ P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 = \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \right] \\ &\quad \cdot \left[ P\left(\bar{g}_2 = \bar{g}_c; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2\right) + P\left(\bar{g}_2 = \bar{g}_c; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2\right) \right] \\ &\quad + \left[ P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 = \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \right] \\ &\quad \cdot \left[ P\left(\bar{g}_2 \neq \bar{g}_c; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2\right) + P\left(\bar{g}_2 \neq \bar{g}_c; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2\right) \right] \end{aligned} \quad (36)$$

Each of terms in (36) can be upper bounded as:

$$\begin{aligned} &P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 = \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_1 = \bar{g}_c, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \cdot P\left(\bar{g}_1 = \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\ &\leq \overrightarrow{P}_{e_2} \cdot \left[ P\left(\bar{g}_1 = \bar{g}_c; \hat{M}_2 = m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + P\left(\bar{g}_1 = \bar{g}_c; \hat{M}_2 \neq m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \right] \\ &= \overrightarrow{P}_{e_2} \cdot \left[ \underbrace{P\left(\bar{g}_1 = \bar{g}_c \mid \hat{M}_2 = m_2, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1-p_h \leq 1} \cdot \underbrace{P\left(\hat{M}_2 = m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1-\overleftarrow{P}_{e_1} \leq 1} \right. \\ &\quad \left. + \underbrace{P\left(\bar{g}_1 = \bar{g}_c \mid \hat{M}_2 \neq m_2, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=p_h} \cdot \underbrace{P\left(\hat{M}_2 \neq m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{P}_{e_1}} \right] \\ &\leq \overrightarrow{P}_{e_2} \left(1 + p_h \overleftarrow{P}_{e_1}\right) \end{aligned} \quad (37)$$

$$\begin{aligned} &P\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\ &= P\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_1 \neq \bar{g}_c, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \cdot P\left(\bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\ &\leq 1 \\ &\leq P\left(\bar{g}_1 \neq \bar{g}_c; \hat{M}_2 = m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + P\left(\bar{g}_1 \neq \bar{g}_c; \hat{M}_2 \neq m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \end{aligned}$$

$$\begin{aligned}
&= \underbrace{\text{P}\left(\bar{g}_1 \neq \bar{g}_c \mid \hat{M}_2 = m_2, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=0} \cdot \underbrace{\text{P}\left(\hat{M}_2 = m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - \overleftarrow{\text{P}}_{e_1} \leq 1} \\
&+ \underbrace{\text{P}\left(\bar{g}_1 \neq \bar{g}_c \mid \hat{M}_2 \neq m_2, \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - p_h \leq 1} \cdot \underbrace{\text{P}\left(\hat{M}_2 \neq m_2 \mid \bar{g}_2 = \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{\text{P}}_{e_1}} \\
&\leq \overleftarrow{\text{P}}_{e_1}
\end{aligned}$$

$$\begin{aligned}
&\text{P}\left(\bar{g}_2 = \bar{g}_c; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\bar{g}_2 = \bar{g}_c \mid \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2\right)}_{=1 - p_h \leq 1} \cdot \underbrace{\text{P}\left(\hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2\right)}_{=1 - \overrightarrow{\text{P}}_{e_1} \leq 1} \leq 1
\end{aligned}$$

$$\begin{aligned}
&\text{P}\left(\bar{g}_2 = \bar{g}_c; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\bar{g}_2 = \bar{g}_c \mid \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2\right)}_{=p_h} \cdot \underbrace{\text{P}\left(\hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2\right)}_{\leq \overrightarrow{\text{P}}_{e_1}} \leq p_h \overrightarrow{\text{P}}_{e_1}
\end{aligned}$$

$$\begin{aligned}
&\text{P}\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 = \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_1 = \bar{g}_c, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq 1} \cdot \text{P}\left(\bar{g}_1 = \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&\leq \text{P}\left(\bar{g}_1 = \bar{g}_c; \hat{M}_2 = m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + \text{P}\left(\bar{g}_1 = \bar{g}_c; \hat{M}_2 \neq m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\bar{g}_1 = \bar{g}_c \mid \hat{M}_2 = m_2, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1} \cdot \underbrace{\text{P}\left(\hat{M}_2 = m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - \overleftarrow{\text{P}}_{e_1} \leq 1} \\
&+ \underbrace{\text{P}\left(\bar{g}_1 = \bar{g}_c \mid \hat{M}_2 \neq m_2, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=p_h} \cdot \underbrace{\text{P}\left(\hat{M}_2 \neq m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{\text{P}}_{e_1}} \\
&\leq 1 + p_h \overleftarrow{\text{P}}_{e_1}
\end{aligned}$$

$$\begin{aligned}
&\text{P}\left(\hat{G}_1 \neq \bar{g}_2; \bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\hat{G}_1 \neq \bar{g}_2 \mid \bar{g}_1 \neq \bar{g}_c, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq 1} \cdot \text{P}\left(\bar{g}_1 \neq \bar{g}_c \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&\leq \text{P}\left(\bar{g}_1 \neq \bar{g}_c; \hat{M}_2 = m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) + \text{P}\left(\bar{g}_1 \neq \bar{g}_c; \hat{M}_2 \neq m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right) \\
&= \underbrace{\text{P}\left(\bar{g}_1 \neq \bar{g}_c \mid \hat{M}_2 = m_2, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=0} \cdot \underbrace{\text{P}\left(\hat{M}_2 = m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - \overleftarrow{\text{P}}_{e_1} \leq 1} \\
&+ \underbrace{\text{P}\left(\bar{g}_1 \neq \bar{g}_c \mid \hat{M}_2 \neq m_2, \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{=1 - p_h \leq 1} \cdot \underbrace{\text{P}\left(\hat{M}_2 \neq m_2 \mid \bar{g}_2 \neq \bar{g}_c, M_1 = m_1, M_2 = m_2\right)}_{\leq \overleftarrow{\text{P}}_{e_1}} \\
&\leq \overleftarrow{\text{P}}_{e_1}
\end{aligned}$$

$$\begin{aligned}
& \mathbb{P}(\bar{g}_2 \neq \bar{g}_c; \hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2) \\
&= \underbrace{\mathbb{P}(\bar{g}_2 \neq \bar{g}_c \mid \hat{M}_1 = m_1, M_1 = m_1, M_2 = m_2)}_{=0} \cdot \underbrace{\mathbb{P}(\hat{M}_1 = m_1 \mid M_1 = m_1, M_2 = m_2)}_{=1 - \overrightarrow{\mathbb{P}}_{e_1} \leq 1} = 0 \\
& \mathbb{P}(\bar{g}_2 \neq \bar{g}_c; \hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2) \\
&= \underbrace{\mathbb{P}(\bar{g}_2 \neq \bar{g}_c \mid \hat{M}_1 \neq m_1, M_1 = m_1, M_2 = m_2)}_{=1 - p_h \leq 1} \cdot \underbrace{\mathbb{P}(\hat{M}_1 \neq m_1 \mid M_1 = m_1, M_2 = m_2)}_{\leq \overrightarrow{\mathbb{P}}_{e_1}} \leq \overrightarrow{\mathbb{P}}_{e_1} \quad (38)
\end{aligned}$$

Next, plugging the upper bounds from (37)-(38) into (35), we obtain:

$$\mathbb{P}(\hat{G}_1 \neq \bar{g}_2 \mid M_1 = m_1, M_2 = m_2) = \left[ \overrightarrow{\mathbb{P}}_{e_2} (1 + p_h \overleftarrow{\mathbb{P}}_{e_1}) + \overleftarrow{\mathbb{P}}_{e_1} \right] \cdot \left[ 1 + p_h \overrightarrow{\mathbb{P}}_{e_1} \right] + \left[ 1 + p_h \overleftarrow{\mathbb{P}}_{e_1} + \overleftarrow{\mathbb{P}}_{e_1} \right] \cdot \overrightarrow{\mathbb{P}}_{e_1} \quad (39)$$

Next for the left hand side of (35), we have equivalently:

$$\mathbb{P}(\hat{G}_1 \neq \bar{g}_2 \mid M_1 = m_1, M_2 = m_2) = \left[ \overleftarrow{\mathbb{P}}_{e_2} (1 + p_h \overrightarrow{\mathbb{P}}_{e_1}) + \overrightarrow{\mathbb{P}}_{e_1} \right] \cdot \left[ 1 + p_h \overleftarrow{\mathbb{P}}_{e_1} \right] + \left[ 1 + p_h \overrightarrow{\mathbb{P}}_{e_1} + \overrightarrow{\mathbb{P}}_{e_1} \right] \cdot \overleftarrow{\mathbb{P}}_{e_1} \quad (40)$$

Note that since each term in (39) and (40) decay exponentially as  $N \rightarrow \infty$ . Hence, we have from (35) that  $\mathbb{P}(\text{Rtx}) \rightarrow 0$  as  $N \rightarrow \infty$ .