Capacity of a Modulo-Sum Simple Relay Network

Youvaraj T. Sagar, Hyuck M. Kwon, and Yanwu Ding
Electrical Engineering and Computer Science, Wichita State University
Wichita, Kansas 67260, USA, {ytsagar; hyuck.kwon; yanwu.ding}@wichita.edu

Abstract — This paper presents the capacity of a modulo-sum simple relay network. In previous work related to this paper, capacity was characterized for the case where the noise was transmitted to the relay. And the closed-form capacity was derived only for the noise with a Bernoulli-(1/2) distribution. However, in this paper, the source is transmitted to the relay, and a more general case of noise with an arbitrary Bernoulli-(p) distribution, $p \in [0, 0.5]$, is considered. The relay observes a corrupted version of the source, uses a quantize-and-forward strategy, and transmits the encoded codeword through a separate dedicated channel to the destination. The destination receives both from the relay and source. This paper assumes that the channel is discrete and memoryless. After deriving the achievable capacity theorem (i.e., the forward theorem) for the binary symmetric simple relay network, this paper proves that the capacity is strictly below the cut-set bound. In addition, this paper presents the proof of the converse theorem. Finally, this paper extends the capacity of the binary symmetric simple relay network to that of an $m$-ary modulo-sum relay network.

Index Terms — Channel capacity; relay network; modulo-sum channel; quantize-and-forward; single-input single-output; cut-set bound.

I. INTRODUCTION

The relay network is a channel that has one sender and one receiver, with a number of intermediate nodes acting as relays to assist with the communications between sender and receiver. This paper exchanges the terminology of the relay channel in [1] with the relay network frequently because here a network is defined as a system consisting of more than two nodes [2], whereas a channel is for communication between two nodes. The simplest relay network or channel has one sender, one receiver, and one relay node. Fig. 1 shows this type of relay network, which is called a “simple” relay network.

The first original model of a relay network was introduced by van der Meulen in 1971 [3]. After that, extensive research was done to find the upper bounds, cut-set bounds, and exact capacity for this network. In 1979, Cover and El Gamal obtained the capacity for a special class of channels called physically degraded relay channels [4]. In that paper, they discussed the capacity of the relay channel with feedback and found an upper bound for a simple relay network, which is shown in Fig. 1. Later, El Gamal and Aref found the capacity for a special class of relay channels called “semideterministic relay channels” in [5]. Then, Kim found the capacity for a class of deterministic relay channels in [6], where he modeled the simple relay network as a noiseless channel between the relay and the destination. Also, van der Meulen corrected his previous upper bound on the capacity of the simple relay network with and without delay in a paper [7].

Using Kim’s results in [6], Aleksic et al. modeled the channel between the relay and the destination as a modular sum noise channel in [8]. Binary side information or channel state information is transmitted to the relay in [8]. He mentioned that the capacity of the simple relay network is not yet known. Recently, Tandon and Ulukus found a new upper bound for the simple relay network with general noise, obtained the capacity for symmetric binary erasure relay channel, and compared them with the cut-set bound in [9].

Aleksic et al. in [8] introduced a corrupting variable to the noiseless channel in [6], whereby the noise in the direct channel between the source and the destination is transmitted to the relay. The relay observes a corrupted version of the noise and has a separate dedicated channel to the destination. For this case, the capacity was characterized in [8]. However, the closed-form capacity was derived only for the noise with a Bernoulli-(p = 1/2) distribution.

The objective of this paper is to find the capacity of the simple modular sum relay network and show that its capacity is strictly below the cut-set bound [4]. This paper also presents a closed-form capacity for a general case, such as for any p where the source is transmitted to both the relay and the destination.

This paper considers all noisy channels, i.e., from the source to the destination, from the source to the relay, and from the relay to the destination, as shown in Fig. 1.
1, where all noisy channels are binary symmetric channels (BSCs) with a certain crossover probability, e.g., \( p \). This paper also derives the capacity for this class of relay channels. In other words, the capacity of a modulo-sum simple relay network is presented here. The capacity proof for the binary symmetric simple relay network and the proof for the converse depend crucially on the input distribution.

For the BSC, a uniform input distribution at the source is assumed because this distribution maximizes the entropy of the output (or the capacity) regardless of additive noise. Furthermore, because of the uniform input distribution, the output of a binary symmetric channel is independent of additive noise. After presenting the proof for the capacity of a binary symmetric simple relay network, this paper proves that the capacity obtained is strictly below the cut-set bound by using the results in [4]. Finally, this paper shows the converse theorem for this class of networks.

Section II describes the system model and presents the capacity of the binary symmetric simple relay network. Section III discusses the cut-set bound for the binary symmetric simple relay network and presents the numerical analysis results. Section IV extends the capacity to the \( m \)-ary modular additive case. Finally, Section V concludes the paper.

II. SYSTEM MODEL AND NETWORK CAPACITY

Fig. 2 shows a realistic binary phase-shift keying (BPSK) system under additive white Gaussian noise (AWGN), where \( X \) and \( Y \) are the binary input and output signal, respectively. Here, \( Y \) is obtained with a hard decision on the demodulated signal.

![Fig. 1. Simple relay network.](image)

![Fig. 2. Realistic BPSK communication system under AWGN.](image)

Fig. 3 shows a BSC with the crossover probability \( p \) equivalent to the realistic communication system in Fig. 2. Here, the crossover probability \( p \) is equal to
\[
\frac{Q\left(\sqrt{2E_b/\sigma^2}\right)}{2}, \quad Q(a) = \int_a^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt,
\]
and \( E_b \) and \( N_0 \) denote the bit energy and the one-side AWGN power spectral density, respectively.

This paper models a channel between any adjacent nodes in Fig. 1 as a BSC that has one sender, one receiver (or destination), and one relay node [1]. The random variable \( Y \) represents the received signal through the direct channel and is written as \( Y = X \oplus Z \), where \( X \) and \( Z \) denote the transmitted and noise random variable with distribution \( \text{Ber}(1/2) \) and \( \text{Ber}(p) \), respectively, and \( \oplus \) denotes the binary modulo-sum, i.e., \( Z = 1 \) with probability \( p \), and \( Z = 0 \) with probability \( (1 - p) \).

The simple relay network in Fig. 1 can be redrawn as Fig. 4. Here, the relay node has an input \( Y_1 \) and an output \( X_1 \). The relay node observes the corrupted version of \( X \), i.e., \( Y_1 = X \oplus N_1 \), encodes it using a codebook \( \mathcal{U}^n \) of jointly typical strong sequences [1], and transmits the code symbol \( X_1 \) through another separate BSC to the destination node, where \( \mathcal{U} \), \( n \), and \( N_1 \) denote the alphabet of code symbols, the codeword length, and the noise random variable at the relay with distribution \( \text{Ber}(\delta) \), respectively. The destination receives both \( Y \), through the direct channel, and \( S_0 = X_1 \oplus N_2 \), through the relay node, where \( N_2 \sim \text{Ber}(\varepsilon) \) represents the noise at the destination for the relay network.

Note that the binary modulo-sum and the BSC can be extended to an \( m \)-ary modulo-sum and an \( m \)-ary symmetric channel (MSC).
To the authors’ knowledge, there is no network capacity expression in the literature, even for the simple relay network shown in Fig. 4. Only the capacity of a deterministic relay channel, i.e., the case of $N_2 = 0$ in Fig. 4, is presented in [6]. The capacity of a relay network by replacing $X$ with $Z$, i.e., the case where the relay observes a corrupted version of the direct channel noise $Z$, is presented in [8]. This paper presents the capacity of the simple relay network shown in Fig. 4 in the following theorem.

**Theorem 1:** The capacity $C$ of the binary symmetric simple relay network shown in Fig. 4 is

$$C = p_{(y|y_1)} \max_{p(x_1)} \left\{1 + H(Y|U) - H(Z|U)\right\},$$

where the maximization is over the $U$’s conditional probability density function (p.d.f.) given $Y_1$; the cardinality of the alphabet $U$, is bounded by $|U| \leq |y_1| + 2$; and $R_0$ is the capacity for the channel between $X_1$ and $S_0$, which can be written as

$$R_0 = \max_{p(x_1)} I(X_1; S_0).$$

The cut-set bound for the capacity of the simple relay network shown in Fig. 4 can be written as

$$C = 1 + H(X|U) - H(Z|U).$$

Here, $H(X)$ and $I(X; Y)$ are the entropy of $X$ and the mutual information between $X$ and $Y$, respectively [1]; $\mathcal{H}(a)$ is the binary entropy function written as $\mathcal{H}(a) = -a \log_2 a - (1-a) \log_2 (1-a)$; and $a * \beta = a(1-\beta) + (1-a) \beta$ [10].

Proofs of the converse and achievability for this theorem are provided in appendices A and B of [12].

IV. CUTSET BOUND AND ANALYTICAL RESULTS

This section shows that the capacity of the binary symmetric simple relay network in Fig. 4 is strictly below the cut-set bound, except for the two trivial points at $R_0 = 0$ and $R_0 = 1$ when $p = 0.5$. The capacity in (1) can be upper-bounded by the cut-set bound as

$$C \leq \max_{p(x_1)} \min \{ I(X; X_1; Y, S_0), I(X; Y_1) \}$$

where the Ford-Fulkerson theorem [11], [4] is applied to the simple relay network in Fig. 4. Using (5), Theorem 2 can be established.

**Theorem 2:** The cut-set bound for the capacity of the binary simple relay network shown in Fig. 4 can be written as

$$C \leq \min \{1 - H(Z) + R_0, 1 - H(Z) + 1 - H(N_2)\} = \min \{1 - \mathcal{H}(p) + R_0, 1 - \mathcal{H}(p) + 1 - \mathcal{H}(\delta)\}.$$

Figs. 5(a) and 5(b) show the capacity in bits per transmission versus $R_0$ bits for $\delta = 0.1$, when $p = 0.1$ and $p = 0.5$, respectively. If $p = 0.5$, then the results are the same as those in [8]. Only the closed form of the capacity for the special case of $p = 0.5$ was analyzed and presented in [8], where the capacity $C$ of the binary simple relay network was obtained by replacing $X$ with $Z$ at the relay input shown in Fig. 4 and written as [8]

$$C = 1 - \mathcal{H}(\mathcal{H}^{-1}(1 - R_0) + \delta).$$

Here $\mathcal{H}^{-1}(\cdot)$ is the inverse of $\mathcal{H}(p)$ in the domain $p \in [0,0.5]$. Note that the capacity in (3) of this paper is valid for a general $p$ between 0 and 0.5, whereas the one in (34) of [8] or (7) is valid for only $p = 0.5$.

Note that the capacity in (3) is strictly below the cut-set bound in (6). Refer to Figure 5(b).

IV. CAPACITY FOR M-ARY MODULO-SUM RELAY NETWORK

This section extends the capacity derived for the binary symmetric simple relay network to the $m$-ary modular additive relay network. The received signal at the destination node can be written as $Y = X + Z \mod m$. The relay observes the corrupted version of $X$, i.e., $Y_1 = X + N_1 \mod m$, and the relay also has a separate channel to the destination: $S_0 = X_1 + N_2 \mod m$ with a capacity $R_0 = \max_{p(x_1)} I(X_1; S_0)$. Therefore, (1) becomes (8) in Theorem 3.

**Theorem 3:** The capacity $C$ of the symmetric $m$-ary modulo-sum simple relay network is

$$C = \max_{p(y|y_1), p(x_1)} \min \{ m + H(Y|U) - H(Z) - H(X|U) \}$$

where maximization is over the conditional $U$’s p.d.f. given $Y_1$ with $|U| \leq |y_1| + 2$, and $R_0$ is defined in (2).
Proof: The achievability for Theorem 3 follows the same steps as Theorem 1 by changing the binary to the \(m\)-ary case. Also, the uniform input distribution at the source maximizes the entropy of the output, regardless of the additive noise. Furthermore, because of the uniform input distribution, the output of an \(m\)-ary modulo-sum relay network is independent of the additive noise. Therefore, (8) holds true. The converse for Theorem 3 also holds true using the same steps of Theorem 1 by changing the binary modulo-sum to the \(m\)-ary modulo-sum.

Using these conditions, both proofs for the achievability and the converse of the capacity theorem were presented. Furthermore, this paper derived the cut-set bound and presented the numerical results for this network. Finally, this paper claimed that the capacity is strictly below the cut-set bound and achievable using a quantize-and-forward strategy at the relay.

**REFERENCES**