Published in IET Communications
Received on 7th January 2014
Revised on 23rd February 2014
Accepted on 12th March 2014
doi: 10.1049/iet-com.2014.0023

ISSN 1751-8628

Physical layer security for some classes of three-receiver broadcast channels

Sadaf Salehkalaibar , Mohammad Reza Aref

Department of Electrical Engineering, Information Systems and Security Lab (ISSL), Sharif University of Technology, Tehran, Iran
E-mail: s_saleh@ee.sharif.edu

Abstract: In this study, the authors consider the secrecy of a one-receiver, two-eavesdropper broadcast channel (BC) with three degraded message sets. Consider a three-receiver BC with three messages, where the first message is decoded by all the receivers. The second message is decoded by the first and the second receivers and is to be kept secret from the third receiver. The third message is decoded by the first receiver and is to be kept secret from the second and the third receivers. The authors consider the imperfect secrecy condition at the second receiver, that is, it is allowed to partially decode the third message. However, the perfect secrecy condition at the third receiver, does not allow it to decode the confidential messages. The coding scheme for this model requires decoding strategy for finding the messages at different destinations. The authors propose a coding scheme which uses indirect decoding. The authors also obtain an outer bound and use it to determine the secrecy capacity region of some classes of one-receiver, two-eavesdropper BCs with three degraded message sets. The authors extend our results to the Gaussian case and evaluate the achievable region.

1 Introduction

With the increase of users in a wireless network, the secrecy of a transmission becomes a challenging issue. An information theoretic model for a secure transmission is WireTap Channel (WTC), where a transmitter sends a message to a receiver and the message is kept secret from an eavesdropper. The WTC was introduced by Wyner [1] and its capacity was determined when the channel of the eavesdropper is a degraded version of the channel to the legitimate receiver. The secrecy capacity of the general WTC (not necessarily degraded) was established by Csiszar and Korner [2]. In the proof of achievability, the confidential message is randomised by a dummy message. This randomness keeps the confidential message secret from the eavesdropper. The receiver decodes the confidential message together with the dummy message.

There are several works which have considered secrecy constraints at different nodes in a broadcast channel (BC) [3–9]. A BC with two receivers, where the private messages are to be kept secret from the unintended receiver, has been studied in [3]. A BC with two confidential messages and a common message to both receivers has been considered in [4]. Secret communication of two private messages over a BC with an external eavesdropper has been investigated in [5]. A K-receiver BC with an eavesdropper has been considered in [6]. In [7], a multi-receiver WTC with public and confidential messages has been studied. There are no secrecy constraints on the public messages, however, the confidential messages are to be kept secret from the eavesdropper. The secrecy of a three-receiver BC with one common and one confidential messages has been studied in [8]. A two-receiver, one-eavesdropper BC with two degraded message sets has been considered in [9]. A one-receiver, two-eavesdropper BC with three degraded message sets has been introduced in [10, 11].

In this paper, we consider the one-receiver, two-eavesdropper BC with three degraded message sets (see Fig. 1) which was studied in [10, 11]. In this model, there are three messages M_0, M_1 and M_2. The message M_0 is decoded by all receivers. The message M_1 is to be sent to the first and the second receivers and is to be kept secret from the third receiver (the second eavesdropper). The message M_2 is to be decoded by the first receiver and is to be kept secret from the second and the third receivers (both eavesdroppers). Comparing with [8], we consider three message parts instead of two messages. We define the perfect secrecy conditions at the third receiver (the second eavesdropper), that is, the messages M_1 and M_2 are completely kept secret from the third receiver. However, at the second receiver (the first eavesdropper), the imperfect secrecy constraint is defined, that is, it is allowed to partially decode the message M_2. The motivation of our definition can be explained through an example. Consider a wireless network with multiple destinations and messages. A group of these destinations try to eavesdrop some of the messages which are not intended to them. This group is also divided into two parts. The first part is allowed to partially decode the messages which are not intended to them. However, the other group is not allowed

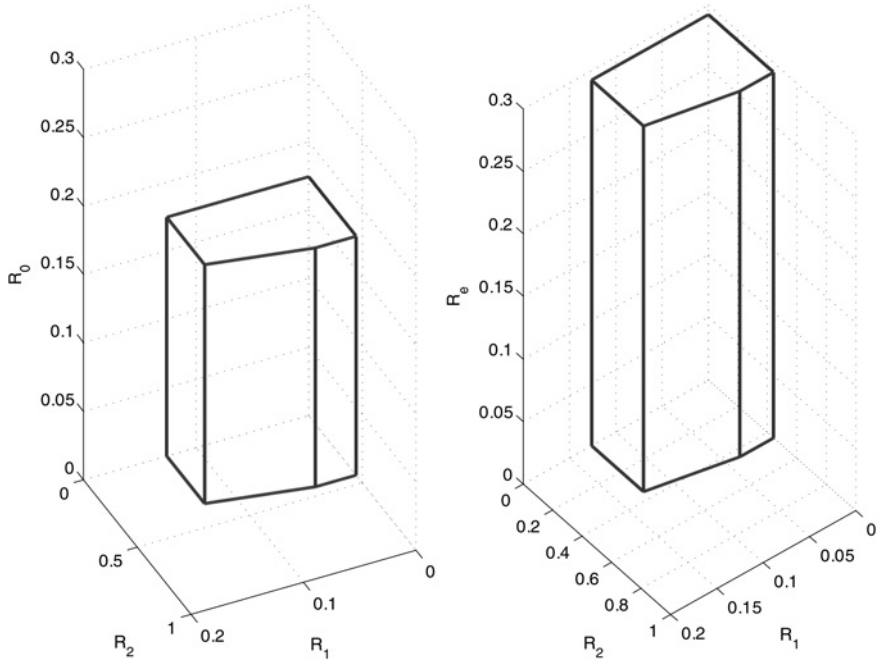

Fig. 1 *One-receiver, two-eavesdropper BC with three degraded message sets*

to decode the unintended messages. In [11], the perfect secrecy conditions are assumed at both eavesdroppers. The secrecy conditions which are defined in the current work, are relaxed comparing with the definition of [11]. Therefore the secrecy analysis in the current work is different from that of [11]. In the coding scheme of [11], the second receiver is not allowed to decode some part of the message M_2. This is because of the fact that the perfect secrecy condition has been defined at the second receiver. In this work, the imperfect secrecy condition at the second receiver allows it to decode some part of the message M_2. Therefore we propose a coding scheme using indirect decoding [12, 13]. In the indirect decoding strategy, the decoder finds the messages of interest, using the codebooks of all messages. However, it does not guarantee unique decoding of the messages not of interest. In our scheme, the message M_2 is splitted into two parts, where the first part is used in indirect decoding of the message M_1 at the second receiver. Another main part of the work is an outer bound which we propose to determine the secrecy capacity region of some classes of one-receiver, two-eavesdropper BCs with three degraded message sets. One of the classes, which we establish the secrecy capacity region, involves more capable channels which represents a more general class comparing with the class of degraded channels [12]. Finally, we extend our results to the Gaussian case and evaluate the achievable region. On the other side, finding a tight outer bound is more challenging in the current work, since this is a two-eavesdropper model with three messages and there are more secrecy constraints in the proposed model. This challenge also exists when we compare our work with [8], since we deal with three messages instead of two messages.

The paper is organised as follows: In Section 2, we present a mathematical framework for our work. In Section 3, we find an inner bound to the secrecy capacity region of the one-receiver, two-eavesdopper BC with three degraded message sets. In Section 4, an outer bound and secrecy capacity results are presented. Gaussian case is studied in Section 5. Conclusions are provided in Section 6.

2 Preliminaries and definitions

We denote discrete random variables with capital letters for example, X, Y, and their realisations with lower case letters x, y. X_i^j indicates a sequence of random variables (X_i, …, X_j). We use $H(.)$ to denote the entropy of a discrete random variable and $I(.;.)$ to denote the mutual information between two discrete random variables. We denote by $T_\varepsilon^n(X, Y)$, the set of ε-strongly jointly typical sequences of length n, on $p(x, y)$. A random variable X takes values in a set $\mathcal{X}$. Finally, we denote the probability mass function of X over $\mathcal{X}$ with $p(x)$ and the conditional probability mass function of X given Y by $p(x/y)$.

Consider a one-receiver, two-eavesdropper discrete memoryless BC with three degraded message sets, input alphabet $\mathcal{X}$, output alphabets $\mathcal{Y}_1$, $\mathcal{Z}_2$, $\mathcal{Z}_3$ and conditional probability mass function $p(y_1, z_2, z_3/x)$.

Definition 1: A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for the one-receiver, two-eavesdropper BC with three degraded message sets (Fig. 1) consists of: (i) three messages (M_0, M_1, M_2) uniformly distributed over $[1{:}2^{nR_0}] \times [1{:}2^{nR_1}] \times [1{:}2^{nR_2}]$; (ii) an encoder that randomly generates a codeword $X^n(m_0, m_1, m_2)$ according to the conditional distribution $p(x^n/m_0, m_1, m_2)$; and (iii) three decoders, the first decoder assigns to each received sequence y_1^n an estimate $(\hat{M}_{01}, \hat{M}_{11}, \hat{M}_{21}) \in [1{:}2^{nR_0}] \times [1{:}2^{nR_1}] \times [1{:}2^{nR_2}]$, the second assigns to each received sequence z_2^n an estimate $(\hat{M}_{02}, \hat{M}_{12}) \in [1{:}2^{nR_0}] \times [1{:}2^{nR_1}]$ and the third assigns to each received sequence z_3^n an estimate $\hat{M}_{03} \in [1{:}2^{nR_0}]$. The probability of error is defined as

$$P_e^n = Pr(\hat{M}_{0j} \neq M_0 \text{ for } j = 1{:}3 \text{ or } \hat{M}_{1j} \neq M_1 \text{ for } j = 1{:}2 \text{ or } \hat{M}_{21} \neq M_2)$$

doi: 10.1049/iet-com.2014.0023

The information leakage rate at the second eavesdropper is defined as $I(M_1, M_2; Z_3^n)/n$. The equivocation rate at the first eavesdropper is denoted by R_e. A rate tuple (R_0, R_1, R_2, R_e) is said to be achievable, if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes such that

$$\lim_{n\to\infty} P_e^n = 0 \tag{1}$$

$$\lim_{n\to\infty} \inf \frac{1}{n} H(M_2|Z_2^n) \geq R_e \tag{2}$$

$$\lim_{n\to\infty} \sup \frac{1}{n} I(M_1, M_2; Z_3^n) = 0 \tag{3}$$

We note that the secrecy requirement in (3) implies the following individual secrecy requirements

$$\lim_{n\to\infty} \sup \frac{1}{n} I(M_1; Z_3^n) = 0, \quad \lim_{n\to\infty} \sup \frac{1}{n} I(M_2; Z_3^n) = 0 \tag{4}$$

Note that the secrecy constraint in (2) represents the imperfect secrecy condition at receiver Z_2, that is, we have $R_e \leq R_2$. In the case of $R_e = R_2$, this constraint reduces to the perfect secrecy condition, which is more restricted comparing with the imperfect secrecy constraint. In a similar fashion, it is obvious that the constraint in (3) represents the perfect secrecy condition at receiver Z_3.

3 An inner bound

In this section, we find an achievable region for the one-receiver, two-eavesdropper BC with three degraded message sets. In the achievable scheme, we use indirect decoding at the second receiver. The proposed achievable region is given in the following theorem.

Theorem 1: An inner bound to the secrecy capacity region of the one-receiver, two-eavesdropper BC with three degraded message sets, is given by the set of rate tuples (R_0, R_1, R_2, R_e) such that

$$R_0 < \min\{I(W; Y_1), I(W; Z_2), I(W; Z_3)\} \tag{5}$$

$$R_1 < I(V; Z_2|W) - I(V; Z_3|W) \tag{6}$$

$$R_2 < I(X; Y_1|U) - I(X; Z_3|U) \tag{7}$$

$$R_1 + R_2 < I(X; Y_1|W) - I(X; Z_3|W) \tag{8}$$

$$R_1 + R_2 < I(X; Y_1|V) + I(V; Z_2|W) - I(X; Z_3|W) \tag{9}$$

$$R_e < I(X; Y_1|V) - I(X; Z_2|V) \tag{10}$$

for all $p(w)p(u/w)p(v/u)p(x/v)$.

Proof: The coding scheme uses superposition technique and Wyner's wiretap coding [1] as the secrecy achievability method. We also employ indirect decoding strategy [8]. The indirect decoding strategy was used in [8] to find new inner bounds for the three-receiver setups. The codebook is shown in Fig. 2. We represent the common message m_0 with the codeword w^n. This codeword is decoded by all receivers. The codeword u^n, which represents the message m_1, is superimposed on top of w^n and is decoded by Y_1. The message m_2 is splitted into two parts m_{21} and m_{22}. For each u^n, we generate the codeword v^n which represents the message m_{21}. Receiver Z_2 finds m_1 indirectly by decoding v^n. The codewords u^n and v^n are protected from Z_3 by Wyner's coding technique. The codeword x^n is generated according to u^n and v^n, and represents the message m_{22}. It is decoded by Y_1 and is protected from Z_3 by Wyner's code partitioning method. The receiver Y_1 jointly decodes m_1 with the messages m_{21} and m_{22} through the codewords u^n, v^n and x^n.

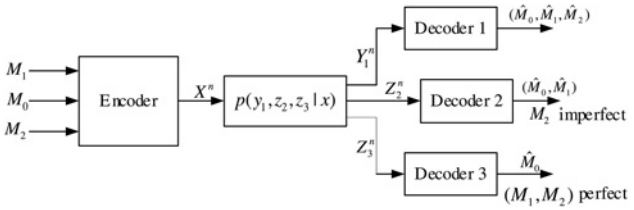

Fig. 2 *Coding for one-receiver, two-eavesdropper BC with three degraded message sets*

(a) *Code generation:* Split the message $M_2 \in \{1, \ldots, 2^{nR_2}\}$ into $M_{21} \in \{1, \ldots, 2^{nR_{21}}\}$ and $M_{22} \in \{1, \ldots, 2^{nR_{22}}\}$ where $R_2 = R_{21} + R_{22}$. Generate 2^{nR_0} i.i.d sequences $w^n(m_0)$, $m_0 \in [1{:}2^{nR_0}]$. For each $w^n(m_0)$, generate $2^{n(R_1+S_1)}$ i.i.d sequences $u^n(m_0, m_1, s_1)$, $m_1 \in [1{:}2^{nR_1}]$ and $s_1 \in [1{:}2^{nS_1}]$. For each $u^n(m_0, m_1, s_1)$, generate $2^{n(R_{21}+S_{21})}$ i.i.d sequences $v^n(m_0, m_1, s_1, m_{21}, s_{21})$, $m_{21} \in [1{:}2^{nR_{21}}]$ and $s_{21} \in [1{:}2^{nS_{21}}]$. For each $v^n(m_0, m_1, s_1, m_{21}, s_{21})$, generate $2^{n(R_{22}+S_{22})}$ i.i. dsequences $x^n(m_0, m_1, s_1, m_{21}, s_{21}, m_{22}, s_{22})$, $m_{22} \in [1{:}2^{nR_{22}}]$ and $s_{22} \in [1{:}2^{nS_{22}}]$.
(b) *Encoding:* To send the message triplet (m_0, m_1, m_2), the transmitter randomly chooses (s_1, s_{21}, s_{22}). It then transmits $x^n(m_0, m_1, s_1, m_{21}, s_{21}, m_{22}, s_{22})$.
(c) *Decoding and analysis of error:* Receiver Y_1 finds m_0 by decoding W, (m_1, m_2) by joint decoding of (U, V, X), Z_2 finds m_1 indirectly by decoding V and m_0 by decoding W, Z_3 finds m_0 by decoding W. The probability of error goes to zero as $n \to \infty$ if

$$R_0 < I(W; Y_1) \tag{11}$$

$$R_1 + S_1 + R_{21} + S_{21} + R_{22} + S_{22} < I(X; Y_1|W) \tag{12}$$

$$R_{21} + S_{21} + R_{22} + S_{22} < I(X; Y_1|U) \tag{13}$$

$$R_{22} + S_{22} < I(X; Y_1|V) \tag{14}$$

$$R_0 < I(W; Z_2) \tag{15}$$

$$R_1 + S_1 + R_{21} + S_{21} < I(V; Z_2|W) \tag{16}$$

$$R_0 < I(W; Z_3) \tag{17}$$

The conditions (12)–(14) are joint decoding constraints where receiver Y_1 jointly decodes m_1, m_{21} and m_{22}. The condition (16) shows that receiver Z_2 finds m_1 indirectly by decoding V.

(d) *Analysis of information leakage rate:* First, consider the mutual information between (M_1, M_2) and Z_3^n, averaged

over the random codebook $\mathcal{C}$. Thus, we have

$$
\begin{aligned}
&I(M_1, M_2; Z_3^n|\mathcal{C}) = H(M_1, M_2|\mathcal{C}) - H(M_1, M_2|Z_3^n, \mathcal{C})\\
&\overset{(a)}{=} H(M_1, M_2|M_0, \mathcal{C}) - H(M_1, M_2|Z_3^n, \mathcal{C})\\
&\overset{(b)}{\leq} H(M_1, M_2|M_0, \mathcal{C}) - H(M_1, M_2|Z_3^n, W^n, \mathcal{C})\\
&\overset{(c)}{\leq} H(M_1, M_2|W^n, \mathcal{C}) - H(M_1, M_2|Z_3^n, W^n, \mathcal{C})\\
&= I(M_1, M_2; Z_3^n|W^n, \mathcal{C})\\
&\overset{(d)}{=} I(X^n; Z_3^n|W^n, \mathcal{C}) - I(X^n; Z_3^n|W^n, M_1, M_2, \mathcal{C})\\
&\overset{(e)}{\leq} nI(X; Z_3|W) - I(X^n; Z_3^n|W^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&= nI(X; Z_3|W) - H(X^n|W^n, M_1, M_2, \mathcal{C})\\
&+ H(X^n|W^n, Z_3^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&\leq nI(X; Z_3|W) - n(S_1 + S_{21} + S_{22})\\
&+ H(X^n|W^n, Z_3^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&\overset{(f)}{=} nI(X; Z_3|W) - n(S_1 + S_{21} + S_{22})\\
&+ H(X^n, U^n, V^n|W^n, Z_3^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&= nI(X; Z_3|W) - n(S_1 + S_{21} + S_{22})\\
&+ H(U^n|W^n, Z_3^n, M_1, M_2, \mathcal{C})\\
&+ H(V^n|W^n, U^n, Z_3^n, M_1, M_2, \mathcal{C})\\
&+ H(X^n|W^n, U^n, V_1^n, Z_3^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&\leq nI(X; Z_3|W) - n(S_1 + S_{21} + S_{22})\\
&+ H(U^n|W^n, Z_3^n, M_1, \mathcal{C}) + H(V^n|W^n, U^n, Z_3^n, M_1, M_2, \mathcal{C})\\
&+ H(X^n|W^n, U^n, V^n, Z_3^n, M_1, M_2, \mathcal{C}) + 2n\delta\\
&\overset{(g)}{\leq} nI(X; Z_3|W) - n(S_1 + S_{21} + S_{22})\\
&+ n(S_1 + S_{21} + S_{22} - I(X; Z_3|W)) + 3n\delta + 2n\delta = 5n\delta
\end{aligned}
$$

where (a) follows because (M_1, M_2) is independent of M_0, (b) follows because conditioning does not increase entropy, (c) follows because $(M_0, \mathcal{C}) \to (W^n, \mathcal{C}) \to (M_1, M_2)$ forms a Markov chain, (d) follows from the Marko chain $(M_1, M_2, W^n, \mathcal{C}) \to X^n \to Z_3^n$, (e) follows from the following

$$H(Z_3^n|W^n, \mathcal{C}) \leq nH(Z_3|W) + n\delta \tag{18}$$

$$H(Z_3^n|W^n, X^n, \mathcal{C}) \geq nH(Z_3|W, X) - n\delta \tag{19}$$

where (18) and (19) follow from [14, Eq. (2.52)] and [14, Eq. (2.46)], respectively, (f) follows because U^n and V^n are deterministic functions of X^n, (g) follows because if (see [8, Lemma 1])

$$S_1 > I(U; Z_3|W) \tag{20}$$

$$S_{21} > I(V; Z_3|U) \tag{21}$$

$$S_{22} > I(X; Z_3|V) \tag{22}$$

then we have

$$
\begin{aligned}
&H(U^n|W^n, Z_3^n, M_1, \mathcal{C}) \leq n(S_1 - I(U; Z_3|W)) + n\delta\\
&H(V^n|W^n, U^n, Z_3^n, M_1, \mathcal{C}) \leq n(S_{21} - I(V; Z_3|U)) + n\delta\\
&H(X^n|W^n, U^n, V^n, Z_3^n, M_1, M_2, \mathcal{C}) \leq n(S_{22} - I(X; Z_3|V)) + n\delta
\end{aligned}
$$

Now, consider the entropy of M_2 given Z_2^n averaged over the random codebook $\mathcal{C}$. Thus, we have

$$
\begin{aligned}
&H(M_2|Z_2^n, \mathcal{C})\\
&= H(M_{21}, M_{22}|Z_2^n, \mathcal{C})\\
&\geq H(M_{22}|Z_2^n, \mathcal{C})\\
&\overset{(a)}{\geq} H(M_{22}|V^n, Z_2^n, \mathcal{C})\\
&= H(M_{22}|V^n, \mathcal{C}) - I(M_{22}; Z_2^n|V^n, \mathcal{C})\\
&\overset{(b)}{=} nR_{22} - I(M_{22}; Z_2^n|V^n, \mathcal{C})\\
&\overset{(c)}{=} nR_{22} - I(X^n; Z_2^n|V^n, \mathcal{C}) + I(X^n; Z_2^n|V^n, M_{22}, \mathcal{C})\\
&\overset{(d)}{\geq} nR_{22} - nI(X; Z_2|V) + I(X^n; Z_2^n|V^n, M_{22}, \mathcal{C}) - 2n\delta\\
&= nR_{22} - nI(X; Z_2|V) + H(X^n|V^n, M_{22}, \mathcal{C})\\
&- H(X^n|V^n, M_{22}, Z_2^n, \mathcal{C}) - 2n\delta\\
&= nR_{22} - nI(X; Z_2|V) + nS_{22} - H(X^n|V^n, M_{22}, Z_2^n, \mathcal{C}) - 2n\delta\\
&\overset{(e)}{\geq} nR_{22} - I(X; Z_2|V) + nS_{22} - (nS_{22} - nI(X; Z_2|V) + n\delta) - 2n\delta\\
&= nR_{22} - 3n\delta
\end{aligned}
$$

where (a) follows because conditioning does not increase entropy, (b) follows because M_{22} is independent of $(V^n, \mathcal{C})$ and also from the fact that M_{22} is chosen randomly from the set $\{1, \ldots, 2^{nR_{22}}\}$, (c) follows because $(M_{22}, V^n, \mathcal{C}) \to X^n \to Z_2^n$ forms a Markov chain, (d) follows from the following

$$H(Z_2^n|V^n, \mathcal{C}) \leq nH(Z_2|V) + n\delta \tag{23}$$

$$H(Z_2^n|V^n, X^n, \mathcal{C}) \geq nH(Z_2|V, X) - n\delta \tag{24}$$

where (23) and (24) follow from [14, Eq. (2.52)] and [14, Eq. (2.46)], respectively, (e) follows because if $S_{22} > I(X;Z_2/V)$, then we have (see [8, Lemma 1])

$$H(X^n|V^n, M_{22}, Z_2^n, \mathcal{C}) \leq nS_{22} - nI(X; Z_2|V) + n\delta$$

Therefore we have $R_e = R_{22}$ if

$$S_{22} > I(X; Z_2|V) \tag{25}$$

Collecting all terms and using Fourier–Motzkin elimination, we obtain the expressions in (5)–(10). □

Application of Theorem 1 yields the following results as special cases.

One-receiver, two-eavesdropper BC with three degraded message sets [11, *Theorem 3*]: Let $U = V$ and $R_e = R_2$ in Theorem 1. With the assumption $R_e = R_2$, the imperfect secrecy condition reduces to the perfect secrecy. Also, suppose that $Y_1 \to Z_2 \to Z_3$ forms a Markov chain. Thus, we

doi: 10.1049/iet-com.2014.0023

obtain

$$R_0 \le I(W; Z_3)$$
$$R_1 \le I(V; Z_2|W) - I(V; Z_3|W)$$
$$R_2 \le I(X; Y_1|V) - I(X; Z_2|V)$$

for some $p(w)p(v/w)p(x/v)$.

Two-receiver, one-eavesdropper BC with one confidential message [2]*:* Suppose that the first eavesdropper is neutral, that is, $R_e = 0$. Also, let $U = W = 0$, $V = X$, $R_0 = R_2 = 0$ in achievable rates of Theorem 1. Then, we have

$$R_1 \le \min\{I(X; Y_1) - I(X; Z_3), I(X; Z_2) - I(X; Z_3)\} \quad (26)$$

for all $p(x)$.

In the next section, we establish the secrecy capacity region of some classes of one-receiver, two-eavesdropper BCs with three degraded message sets.

4 Secrecy capacity results

In this section, we establish the secrecy capacity region of some classes of one-receiver, two-eavesdropper BCs with three degraded message sets. We show that the proposed inner bound is tight in some cases. In contrast to the case with no secrecy constraint, it is difficult to match our inner and outer bounds in general, when there are secrecy constraints. First, consider the case where Z_3 is a degraded version of Y_1 and Z_2, that is, $X \to Y_1 \to Z_3$ and $X \to Z_2 \to Z_3$ form a Markov chain. We find an outer bound to the secrecy capacity region of this class of one-receiver, two-eavesdropper BCs with three degraded message sets. We use this outer bound to determine the secrecy capacity region for a special case.

Theorem 2: An outer bound to the secrecy capacity region of the one-receiver, two-eavesdropper BC with three degraded message sets where Z_3 is a degraded version of Y_1 and Z_2 is given by the set of rate tuples (R_0, R_1, R_2, R_e) such that

$$R_0 \le I(W; Z_3) \quad (27)$$
$$R_1 \le I(V; Z_2|W) - I(V; Z_3|W) \quad (28)$$
$$R_2 \le I(X; Y_1|U) - I(X; Z_3|U) \quad (29)$$
$$R_1 + R_2 \le I(X; Y_1|W) - I(X; Z_3|W) \quad (30)$$
$$R_1 + R_2 \le I(X; Y_1|V) + I(V; Z_2|W) - I(X; Z_3|W) \quad (31)$$
$$R_e \le I(V_2; Y_1|V) - I(V_2; Z_2|V) \quad (32)$$

for some $p(w)p(u/w)p(v/u)p(v_2/v)p(x/v_2)$.

Proof: See Appendix 1. □

Remark 1: We note that the only difference between the inner and the outer bounds of Theorems 1 and 2 comes from the bound in (10). In other words, the constraints (10) and (32) do not match. We show that these constraints coincide when Y_1 is more capable than Z_2, that is, for all $p(x)$, we have $I(X;Y_1) \ge I(X;Z_2)$. It should be noted that the more capable condition is more general comparing with the degradedness condition and the less noisy condition [12].

In the following, we use Theorem 2 to determine the secrecy capacity region for a special case. Suppose that Z_3 is a degraded version of Y_1 and Z_2, and Y_1 is more capable than Z_2, that is, for all $p(x)$, we have $I(X;Y_1) \ge I(X;Z_2)$.

Theorem 3: The secrecy capacity region of the one-receiver, two-eavesdropper BC with three degraded message sets where Z_3 is a degraded version of Y_1 and Z_2, and Y_1 is more capable than Z_2 is given by the set of rate tuples (R_0, R_1, R_2, R_e) such that

$$R_0 \le I(W; Z_3) \quad (33)$$
$$R_1 \le I(V; Z_2|W) - I(V; Z_3|W) \quad (34)$$
$$R_2 \le I(X; Y_1|U) - I(X; Z_3|U) \quad (35)$$
$$R_1 + R_2 \le I(X; Y_1|W) - I(X; Z_3|W) \quad (36)$$
$$R_1 + R_2 \le I(X; Y_1|V) + I(V; Z_2|W) - I(X; Z_3|W) \quad (37)$$
$$R_e \le I(X; Y_1|V) - I(X; Z_2|V) \quad (38)$$

for some $p(w)p(u/w)p(v/u)p(x/v)$.

Proof: The achievability follows from Theorem 1. The converse follows from Theorem 2. Also, consider the condition (32), where we have

$$\begin{aligned} I(V_2; Y_1|V) - I(V_2; Z_2|V) &\le I(V_2; Y_1|V) - I(V_2; Z_2|V) \\ &\quad + I(X; Y_1|V_2) - I(X; Z_2|V_2) \\ &= I(X; Y_1|V) - I(X; Z_2|V) \end{aligned}$$

and the inequality follows because Y_1 is more capable than Z_2. □

Next, consider the case where Z_2 and Z_3 are degraded versions of Y_1, that is, $X \to Y_1 \to (Z_2, Z_3)$ forms a Markov chain. The capacity region of this case is given in the following.

Theorem 4: The secrecy capacity region of the one-receiver, two-eavesdropper BC with three degraded message sets when Z_2 and Z_3 are degraded versions of Y_1 is given by the set of rate tuples (R_0, R_1, R_2, R_e) such that

$$R_0 \le \min\{I(W; Z_3), I(W; Z_2)\} \quad (39)$$
$$R_1 \le I(U; Z_2|W) - I(U; Z_3|W) \quad (40)$$
$$R_2 \le I(X; Y_1|U) - I(X; Z_3|U) \quad (41)$$
$$R_e \le I(X; Y_1|U) - I(X; Z_2|U) \quad (42)$$

for some $p(w)p(u/w)p(x/u)$.

Proof: For the achievability, let $V = U$ in Theorem 1. The conditions (8) and (9) are redundant when Z_2 is a degraded version of Y_1. For the proof of converse, see Appendix 2. □

5 Gaussian case

In this section, we extend the results to the Gaussian case and evaluate the achievable region. Here, we consider the Gaussian one-receiver, two-eavesdropper BC which is defined by

$$Y_1 = X + N_1 \tag{43}$$

$$Z_2 = X + N_2 \tag{44}$$

$$Z_3 = X + N_3 \tag{45}$$

where the channel input X is subject to a constraint $\frac{1}{n}\sum_{i=1}^{n} x_i^2 \le P$ and N_1, N_2, N_3 are zero-mean Gaussian random variables with variances σ_1^2, σ_2^2, σ_3^2, respectively. We obtain an inner bound to the secrecy capacity region of the Gaussian one-receiver, two-eavesdropper BC with three degraded message sets as follows.

Theorem 5: An inner bound to the secrecy capacity region of the Gaussian one-receiver, two-eavesdropper BC with three degraded message sets is given by the set of rate tuples (R_0, R_1, R_2, R_e) such that

$$R_0 < \min\left\{\frac{1}{2}\log\frac{P+\sigma_1^2}{\alpha_1+\alpha_2+\alpha_3+\sigma_1^2}, \frac{1}{2}\log\frac{P+\sigma_2^2}{\alpha_1+\alpha_2+\alpha_3+\sigma_2^2}, \frac{1}{2}\log\frac{P+\sigma_3^2}{\alpha_1+\alpha_2+\alpha_3+\sigma_3^2}\right\} \tag{46}$$

$$R_1 < \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_2^2}{\alpha_3+\sigma_2^2} - \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_3^2}{\alpha_3+\sigma_3^2} \tag{47}$$

$$R_2 < \frac{1}{2}\log\frac{\alpha_2+\alpha_3+\sigma_1^2}{\sigma_1^2} - \frac{1}{2}\log\frac{\alpha_2+\alpha_3+\sigma_3^2}{\sigma_3^2} \tag{48}$$

$$R_1+R_2 < \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_1^2}{\sigma_1^2} - \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_3^2}{\sigma_3^2} \tag{49}$$

$$R_1+R_2 < \frac{1}{2}\log\frac{\alpha_3+\sigma_1^2}{\sigma_1^2} + \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_2^2}{\alpha_3+\sigma_2^2} - \frac{1}{2}\log\frac{\alpha_1+\alpha_2+\alpha_3+\sigma_3^2}{\sigma_3^2} \tag{50}$$

$$R_e < \frac{1}{2}\log\frac{\alpha_3+\sigma_1^2}{\sigma_1^2} - \frac{1}{2}\log\frac{\alpha_3+\sigma_2^2}{\sigma_2^2} \tag{51}$$

for $\alpha_1+\alpha_2+\alpha_3 \le P$.

Proof: Consider the following choices of random variables,

- W is selected as a zero-mean Gaussian random variable with variance $P-\alpha_1-\alpha_2-\alpha_3$ where $\alpha_1+\alpha_2+\alpha_3 \le P$.
- U is selected as $U = W + Q_1$, where Q_1 is a zero-mean Gaussian random variable with variance α_1, and is independent of W.

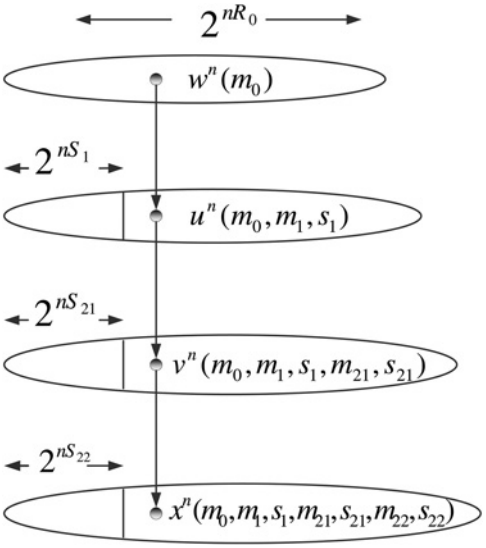

Fig. 3 *The regions (R_0, R_1, R_2) and (R_e, R_1, R_2) for $P = 12$, $\alpha_1 = 8$, $\alpha_2 = 0.1$, $\alpha_3 = 1$, $\sigma_1^2 = 0.5$, $\sigma_2^2 = 1$ and $\sigma_3^2 = 1.5$*

- V is selected as $V = U + Q_2$, where Q_2 is a zero-mean Gaussian random variable with variance α_2, and is independent of W, Q_1.
- X is selected as $X = V + Q_3$, where Q_3 is a zero-mean Gaussian random variable with variance α_3, and is independent of W, Q_1, Q_2. □

With these choices (5)–(10) reduce to (46)–(51). Here, we have some remarks about how the achievable region is affected with the change of the parameters α_1, α_2 and α_3.

Remark 2: When the value of the parameter α_3 increases, the common rate R_0 decreases. The secrecy rate R_e increases whenever $\sigma_1^2 \le \sigma_2^2$ and decreases when $\sigma_1^2 \ge \sigma_2^2$.

Remark 3: When the value of the parameter α_2 increases, the rates R_1 and R_2 increase whenever $\sigma_2^2 \le \sigma_3^2$ and $\sigma_1^2 \le \sigma_3^2$. However, the common rate R_0 decreases.

Remark 4: When the value of the parameter α_1 increases, the rate R_1 increases whenever $\sigma_2^2 \le \sigma_3^2$. Although the common rate R_0 decreases.

Remark 5: For some values of the parameters, the regions (R_0, R_1, R_2) and (R_e, R_1, R_2) are shown in Fig. 3.

6 Conclusion

In this paper, we considered the one-receiver, two-eavesdropper BC with three degraded message sets. Comparing with [8, 9], the proposed model includes three messages instead of two messages. Also, comparing with [11], we consider the imperfect secrecy conditions instead of the perfect case. We found an achievable secrecy region for the one-receiver, two-eavesdropper BC with three degraded message sets using indirect decoding. Our achievable scheme involves message splitting which is different from [11] with the perfect secrecy constraints. We

doi: 10.1049/iet-com.2014.0023

also obtained an outer bound and used it to establish the secrecy capacity of some classes of one-receiver, two-eavesdropper BCs with three degraded message sets. The procedure of finding the outer bound is more challenging comparing with [8], since we have three messages in our model. We extended our results to the Gaussian case. The results of this paper can be used in wireless networks with different secrecy constraints at the destinations.

7 Acknowledgments

The authors would like to thank Dr. Bahareh Akhbari for her comments that improved the paper.

This work was partially supported by Iranian NSF under contract no. 88114.46-2010 and by Iran Telecom Research Center (ITRC).

8 References

1 Wyner, A.D.: 'The wire-tap channel', *Bell Syst. Tech. J.*, 1975, **54**, (8), pp. 1355–1387
2 Csiszar, I., Korner, J.: 'Broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 1978, **24**, (3), pp. 339–348
3 Liu, R., Maric, I., Spasojevic, P., Yates, R.D.: 'Discrete memoryless interference and broadcast channels with confidential messages: secrecy rate regions', *IEEE Trans. Inf. Theory*, 2008, **54**, (6), pp. 2493–2507
4 Xu, J., Cao, Y., Chen, B.: 'Capacity bounds for broadcast channels with confidential messages', *IEEE Trans. Inf. Theory*, 2009, **55**, (10), pp. 4529–4542
5 Bagherikaram, G., Motahari, A.S., Khandani, A.K.: 'Secure broadcasting: the secrecy rate region'. 46th Annual Allerton Conf. on Communication and Computing, September 2008, pp. 834–841
6 Ekrem, E., Ulukus, S.: 'Secrecy capacity of a class of broadcast channels with an eavesdropper', *EURASIP J. Wirel. Commun. Netw.*, 2009, **2009**, pp. 1–20
7 Ekrem, E., Ulukus, S.: 'Multi-receiver wiretap channel with public and confidential messages', *IEEE Trans. Inf. Theory*, 2011, **56**, (6), pp. 2165–2177
8 Chia, Y.K., El Gamal, A.: 'Three-receiver broadcast channels with common and confidential messages', *IEEE Trans. Inf. Theory*, 2012, **58**, (5), pp. 2748–2765
9 Choo, L.C., Wong, K.K.: 'Physical layer security for a 3-receiver broadcast channel'. Int. Conf. on Wirel. Communication and Signal processing (WCSP), London, UK, November 2009, pp. 1–5
10 Salehkalaibar, S., Aref, M.R.: 'The capacity region of a class of 3-receiver broadcast channels with two eavesdroppers'. IEEE Int. Symp. on Information Theory (ISIT), St. Petersburg, Russia, July–August 2011, pp. 968–972
11 Salehkalaibar, S., Mirmohseni, M., Aref, M.R.: 'One-receiver, two-eavesdropper broadcast channel with degraded message sets', *IEEE Trans. Inf. Forensics Sec.*, 2013, **8**, (7), pp. 1162–1172
12 El Gamal, A., Kim, Y.H.: 'Network information theory' (Cambridge University Press, 2011)
13 Nair, C., El Gamal, A.: 'The capacity region of a class of three-receiver broadcast channels with degraded message sets', *IEEE Trans. Inf. Theory*, 2009, **55**, (10), pp. 4479–4493
14 Liang, Y., Poor, H.V., Shamai, S.: 'Information theoretic security', *Foundations Trends commun. Inf. Theory*, 2008, **5**, (4–5), pp. 355–580

9 Appendix

9.1 Appendix 1: Proof of Theorem 2

Define the following random variables

$$W_i = (M_0, Z_3^{i-1})$$
$$U_i = (M_0, M_1, Z_3^{i-1})$$
$$V_i = (M_0, M_1, Z_2^{i-1}, Y_{1,i+1}^n)$$
$$V_{2,i} = (M_0, M_1, M_2, Z_2^{i-1}, Y_{1,i+1}^n)$$

We also introduce the following lemmas which will be used frequently.

Lemma 1: ([2]):

$$\sum_{i=1}^{n} I(T_{2,i+1}^n; T_{1,i}|Q, T_1^{i-1}) = \sum_{i=1}^{n} I(T_1^{i-1}; T_{2,i}|Q, T_{2,i+1}^n)$$

Lemma 2:

$$I(M; T_1^n|Q) - I(M; T_2^n|Q) = \sum_{i=1}^{n} I(M; T_{1,i}|Q, T_1^{i-1}, T_{2,i+1}^n) - \sum_{i=1}^{n} I(M; T_{2,i}|Q, T_1^{i-1}, T_{2,i+1}^n)$$

The proof can be done using Lemma 1.

First, consider the rate R_1

$$\begin{aligned}
nR_1 &= H(M_1) \overset{(a)}{=} H(M_1|M_0) \\
&= I(M_1; Z_2^n|M_0) + H(M_1|Z_2^n, M_0) \\
&\overset{(b)}{\leq} I(M_1; Z_2^n|M_0) + n\delta \\
&\overset{(c)}{\leq} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n) + 2n\delta \\
&= I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n, M_0) \\
&\quad + I(M_1; M_0|Z_3^n) + 2n\delta \\
&\overset{(d)}{=} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) \\
&\quad + I(M_1; M_0|Z_3^n) + 2n\delta \\
&\leq I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) \\
&\quad + H(M_0|Z_3^n) + 2n\delta \\
&\overset{(e)}{\leq} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_1; Z_{2,i}|M_0, Z_2^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(M_1; Z_{3,i}|M_0, Z_{3,i+1}^n) + 3n\delta \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(M_1; Z_{2,i}|M_0, Z_2^{i-1}, Z_{3,i+1}^n) \\
&\quad - \sum_{i=1}^{n} I(M_1; Z_{3,i}|M_0, Z_2^{i-1}, Z_{3,i+1}^n) + 3n\delta \\
&\overset{(g)}{=} \sum_{i=1}^{n} I(M_1; Z_{2,i}|M_0, Z_2^{i-1}, Z_3^{i-1}, Z_{3,i+1}^n)
\end{aligned}$$

$$
\begin{aligned}
&- \sum_{i=1}^{n} I(M_1; Z_{3,i}|M_0, Z_2^{i-1}, Z_3^{i-1}, Z_{3,i+1}^n) + 3n\delta \\
&\overset{(h)}{\leq} \sum_{i=1}^{n} I(M_1; Z_{2,i}|M_0, Z_2^{i-1}, Z_3^{i-1}, Z_{3,i+1}^n) \\
&- \sum_{i=1}^{n} I(M_1; Z_{3,i}|M_0, Z_2^{i-1}, Z_3^{i-1}, Z_{3,i+1}^n) \\
&+ \sum_{i=1}^{n} I(Z_{3,i+1}^n, Z_2^{i-1}; Z_{2,i}|M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(Z_{3,i+1}^n, Z_2^{i-1}; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Z_{3,i+1}^n; Z_{2,i}|M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Z_{3,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&\overset{(i)}{\leq} \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Z_{3,i+1}^n; Z_{2,i}|M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Z_{3,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) \\
&+ \sum_{i=1}^{n} I(Y_{1,i+1}^n; Z_{2,i}|M_0, M_1, Z_{3,i+1}^n, Z_2^{i-1}, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_{3,i+1}^n, Z_2^{i-1}, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Y_{1,i+1}^n, Z_{3,i+1}^n; Z_{2,i}|M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Y_{1,i+1}^n, Z_{3,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&\overset{(j)}{=} \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Y_{1,i+1}^n; Z_{2,i}|M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_1, Z_2^{i-1}, Y_{1,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(V_i; Z_{2,i}|W_i) - \sum_{i=1}^{n} I(V_i; Z_{3,i}|W_i) + 3n\delta
\end{aligned}
$$

where (a) and (d) follow because M_1 is independent of M_0, (b) and (e) follow from Fano's inequality, (c) follows from the secrecy condition, (f) follows from Lemma 2, (g), (h) and (i) follow because Z_3 is a degraded version of Z_2, that is, $Z_3^{i-1} \to Z_2^{i-1} \to X_i \to Z_{2,i} \to Z_{3,i}$, $(M_0, Z_3^{i-1}, Z_{3,i+1}^n, Z_2^{i-1}) \to X_i \to Z_{2,i} \to Z_{3,i}$ and $(M_0, M_1, Z_{3,i+1}^n, Z_2^{i-1}, Z_3^{i-1}, Y_{1,i+1}^n) \to X_i \to Z_{2,i} \to Z_{3,i}$ form Markov chains, respectively, (j) follows because Z_3 is a degraded version of Y_1, that is, $Z_{3,i+1}^n \to Y_{1,i+1}^n \to X_i \to (Z_{2,i}, Z_{3,i})$ forms a Markov chain. Next, consider the rate R_2

$$
\begin{aligned}
nR_2 = H(M_2) &\overset{(a)}{=} H(M_2|M_1, M_0) \\
&= I(M_2; Y_1^n|M_1, M_0) + H(M_2|M_1, M_0, Y_1^n) \\
&\overset{(b)}{\leq} I(M_2; Y_1^n|M_1, M_0) + n\delta \\
&\overset{(c)}{\leq} I(M_2; Y_1^n|M_1, M_0) - I(M_2, M_1; Z_3^n) + 2n\delta \\
&\leq I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1) + 2n\delta \\
&= I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n, M_0|M_1) \\
&+ I(M_2; M_0|Z_3^n, M_1) + 2n\delta \\
&\overset{(d)}{=} I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) \\
&+ I(M_2; M_0|Z_3^n, M_1) + 2n\delta \\
&\leq I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) \\
&+ H(M_0|Z_3^n) + 2n\delta \\
&\overset{(e)}{\leq} I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_2; Y_{1,i}|M_1, M_0, Y_{1,i+1}^n) \\
&- \sum_{i=1}^{n} I(M_2; Z_{3,i}|M_0, M_1, Z_3^{i-1}) + 3n\delta \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(M_2; Y_{1,i}|M_1, M_0, Y_{1,i+1}^n, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_2; Z_{3,i}|M_0, M_1, Y_{1,i+1}^n, Z_3^{i-1}) + 3n\delta \\
&\overset{(g)}{\leq} \sum_{i=1}^{n} I(M_2; Y_{1,i}|M_1, M_0, Y_{1,i+1}^n, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_2; Z_{3,i}|M_0, M_1, Y_{1,i+1}^n, Z_3^{i-1}) \\
&+ \sum_{i=1}^{n} I(Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_2, Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}) + 3n\delta \\
&\overset{(h)}{\leq} \sum_{i=1}^{n} I(M_2, Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}) \\
&+ \sum_{i=1}^{n} I(X_i; Y_{1,i}|M_1, M_0, M_2, Y_{1,i+1}^n, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(X_i; Z_{3,i}|M_0, M_1, M_2, Y_{1,i+1}^n, Z_3^{i-1}) + 3n\delta \\
&\overset{(i)}{=} \sum_{i=1}^{n} I(X_i; Y_{1,i}|M_1, M_0, Z_3^{i-1})
\end{aligned}
$$

doi: 10.1049/iet-com.2014.0023

$$- \sum_{i=1}^{n} I(X_i; Z_{3,i}|M_0, M_1, Z_3^{i-1}) + 3n\delta$$

$$= \sum_{i=1}^{n} I(X_i; Y_{1,i}|U_i) - \sum_{i=1}^{n} I(X_i; Z_{3,i}|U_i) + 3n\delta$$

where (a) and (d) follow because M_2 is independent of (M_0, M_1), (b) and (e) follow from Fano's inequality, (c) follows from the secrecy condition, (f) follows from Lemma 2, (g) and (h) follow because Z_3 is a degraded version of Y_1, that is, $(M_1, M_0, Z_3^{i-1}, Y_{1,i+1}^n) \to X_i \to Y_{1,i} \to Z_{3,i}$ and $(M_1, M_0, M_2, Y_{1,i+1}^n, Z_3^{i-1}) \to X_i \to Y_{1,i} \to Z_{3,i}$ form Markov chains, respectively, (i) follows because given X_i, $Y_{1,\,i}$ and $Z_{3,\,i}$ are independent of other variables. Now, consider the rate $R_1 + R_2$

$$\begin{aligned}
n(R_1 + R_2) &= H(M_1, M_2) \overset{(a)}{=} H(M_1, M_2|M_0) \\
&= I(M_1, M_2; Y_1^n|M_0) + H(M_1, M_2|M_0, Y_1^n) \\
&\overset{(b)}{\le} I(M_1, M_2; Y_1^n|M_0) + n\delta \\
&\overset{(c)}{\le} I(M_1, M_2; Y_1^n|M_0) - I(M_1, M_2; Z_3^n) + 2n\delta \\
&= I(M_1, M_2; Y_1^n|M_0) - I(M_1, M_2; Z_3^n, M_0) \\
&\quad + I(M_1, M_2; M_0|Z_3^n) + 2n\delta \\
&\overset{(d)}{=} I(M_1, M_2; Y_1^n|M_0) - I(M_1, M_2; Z_3^n|M_0) \\
&\quad + I(M_1, M_2; M_0|Z_3^n) + 2n\delta \\
&\le I(M_1, M_2; Y_1^n|M_0) - I(M_1, M_2; Z_3^n|M_0) \\
&\quad + H(M_0|Z_3^n) + 2n\delta \\
&\overset{(e)}{\le} I(M_1, M_2; Y_1^n|M_0) - I(M_1, M_2; Z_3^n|M_0) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_1, M_2; Y_{1,i}|M_0, Y_{1,i+1}^n) \\
&\quad - \sum_{i=1}^{n} I(M_1, M_2; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&\overset{(f)}{=} \sum_{i=1}^{n} I(M_1, M_2; Y_{1,i}|M_0, Y_{1,i+1}^n, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(M_1, M_2; Z_{3,i}|M_0, Z_3^{i-1}, Y_{1,i+1}^n) + 3n\delta \\
&\overset{(g)}{\le} \sum_{i=1}^{n} I(M_1, M_2; Y_{1,i}|M_0, Y_{1,i+1}^n, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(M_1, M_2; Z_{3,i}|M_0, Z_3^{i-1}, Y_{1,i+1}^n) \\
&\quad + \sum_{i=1}^{n} I(Y_{1,i+1}^n; Y_{1,i}|M_0, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(Y_{1,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(M_1, M_2, Y_{1,i+1}^n; Y_{1,i}|M_0, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(M_1, M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&\overset{(h)}{\le} \sum_{i=1}^{n} I(M_1, M_2, Y_{1,i+1}^n; Y_{1,i}|M_0, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(M_1, M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, Z_3^{i-1}) \\
&\quad + \sum_{i=1}^{n} I(X_i; Y_{1,i}|M_0, M_1, M_2, Y_{1,i+1}^n, Z_3^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(X_i; Z_{3,i}|M_0, M_1, M_2, Y_{1,i+1}^n, Z_3^{i-1}) + 3n\delta \\
&\overset{(i)}{=} \sum_{i=1}^{n} I(X_i; Y_{1,i}|M_0, Z_3^{i-1}) - \sum_{i=1}^{n} I(X_i; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&= \sum_{i=1}^{n} I(X_i; Y_{1,i}|W_i) - \sum_{i=1}^{n} I(X_i; Z_{3,i}|W_i) + 3n\delta
\end{aligned}$$

where (a)–(i) follow from similar steps in bounding R_2 above. We have also the following bound on $R_1 + R_2$

$$\begin{aligned}
n(R_1 + R_2) &= H(M_1, M_2) \overset{(a)}{=} H(M_1, M_2|M_0) \\
&= H(M_2|M_1, M_0) + H(M_1|M_0) \\
&\overset{(b)}{\le} I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) + 2n\delta \\
&\overset{(c)}{\le} I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(M_1, M_2; Z_3^n) + 3n\delta \\
&= I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(M_1, M_2; Z_3^n, M_0) + I(M_1, M_2; M_0|Z_3^n) + 3n\delta \\
&\overset{(d)}{=} I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(M_1, M_2; Z_3^n|M_0) + I(M_1, M_2; M_0|Z_3^n) + 3n\delta \\
&\le I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(M_1, M_2; Z_3^n|M_0) + H(M_0|Z_3^n) + 3n\delta \\
&\overset{(e)}{\le} I(M_2; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(M_1, M_2; Z_3^n|M_0) + 4n\delta \\
&\overset{(f)}{=} I(X^n; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(X^n; Z_3^n|M_0) \\
&\quad + I(X^n; Z_3^n|M_0, M_1, M_2) \\
&\quad - I(X^n; Y_1^n|M_0, M_1, M_2) + 4n\delta \\
&\overset{(g)}{\le} I(X^n; Y_1^n|M_1, M_0) + I(M_1; Z_2^n|M_0) \\
&\quad - I(X^n; Z_3^n|M_0) + 4n\delta \\
&= \sum_{i=1}^{n} I(X^n; Y_{1,i}|M_1, M_0, Y_{1,i+1}^n) \\
&\quad + \sum_{i=1}^{n} I(M_1; Z_{2,i}|M_0, Z_2^{i-1}) \\
&\quad - \sum_{i=1}^{n} I(X^n; Z_{3,i}|M_0, Z_3^{i-1}) + 4n\delta
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} I(X^n;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, M_1,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(X^n;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&\overset{(h)}{=} \sum_{i=1}^{n} I(X^n;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&+ \sum_{i=1}^{n} I(Z_2^{i-1};\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, M_1,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(X^n;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&\overset{(i)}{=} \sum_{i=1}^{n} I(X^n;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(X^n;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&\overset{(j)}{=} \sum_{i=1}^{n} I(X^n;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n;\, Z_{2,i}|M_0,\, Z_2^{i-1},\, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(X^n;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&\leq \sum_{i=1}^{n} I(X^n;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n,\, Z_2^{i-1};\, Z_{2,i}|M_0,\, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(X^n;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&\overset{(k)}{=} \sum_{i=1}^{n} I(X_i;\, Y_{1,i}|M_1,\, M_0,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&+ \sum_{i=1}^{n} I(M_1,\, Y_{1,i+1}^n,\, Z_2^{i-1};\, Z_{2,i}|M_0,\, Z_3^{i-1}) \\
&- \sum_{i=1}^{n} I(X_i;\, Z_{3,i}|M_0,\, Z_3^{i-1}) + 4n\delta \\
&= \sum_{i=1}^{n} I(X_i;\, Y_{1,i}|V_i) + \sum_{i=1}^{n} I(V_i;\, Z_{2,i}|W_i) \\
&- \sum_{i=1}^{n} I(X_i;\, Z_{3,i}|W_i) + 4n\delta
\end{aligned}
$$

where (a) and (d) follow because (M_1, M_2) is independent of M_0, (b) and (e) follow from Fano's inequality, (c) follows from the secrecy condition, (f) follows because $(M_0, M_1, M_2) \to X^n \to (Y_1^n, Z_3^n)$ forms a Markov chain, (g) follows because Z_3 is a degraded version of Y_1, that is, $(M_0, M_1, M_2) \to X^n \to Y_1^n \to Z_3^n$ forms a Markov chain, (h) follows because $Z_2^{i-1} \to X_i \to Y_{1,i}$ forms a Markov chain from the memoryless property, (i) follows from Lemma 1, (j) follows because Z_3 is a degraded version of Z_2, that is, $Z_3^{i-1} \to Z_2^{i-1} \to X_i \to Z_{2,i} \to Z_{3,i}$ forms a Markov chain, (k) follows because $(X^{i-1}, X_{i+1}^n) \to X_i \to (Y_{1,i}, Z_{3,i})$ forms a Markov chain. Finally, consider the equivocation rate R_e

$$
\begin{aligned}
nR_e &\leq H(M_2|Z_2^n) \\
&= H(M_2) - I(M_2;\, Z_2^n) \\
&\overset{(a)}{=} H(M_2|M_0,\, M_1) - I(M_2;\, Z_2^n) \\
&\overset{(b)}{\leq} I(M_2;\, Y_1^n|M_0,\, M_1) - I(M_2;\, Z_2^n) + n\delta \\
&= I(M_2;\, Y_1^n|M_0,\, M_1) - I(M_2;\, Z_2^n,\, M_0,\, M_1) \\
&+ I(M_2;\, M_0,\, M_1|Z_2^n) + n\delta \\
&\overset{(c)}{=} I(M_2;\, Y_1^n|M_0,\, M_1) - I(M_2;\, Z_2^n|M_0,\, M_1) \\
&+ I(M_2;\, M_0,\, M_1|Z_2^n) + n\delta \\
&\leq I(M_2;\, Y_1^n|M_0,\, M_1) - I(M_2;\, Z_2^n|M_0,\, M_1) \\
&+ H(M_0,\, M_1|Z_2^n) + n\delta \\
&\overset{(d)}{\leq} I(M_2;\, Y_1^n|M_0,\, M_1) - I(M_2;\, Z_2^n|M_0,\, M_1) + 2n\delta \\
&= \sum_{i=1}^{n} I(M_2;\, Y_{1,i}|M_0,\, M_1,\, Y_{1,i+1}^n) \\
&- \sum_{i=1}^{n} I(M_2;\, Z_{2,i}|M_0,\, M_1,\, Z_2^{i-1}) + 2n\delta \\
&\overset{(e)}{=} \sum_{i=1}^{n} I(M_2;\, Y_{1,i}|M_0,\, M_1,\, Y_{1,i+1}^n,\, Z_2^{i-1}) \\
&- \sum_{i=1}^{n} I(M_2;\, Z_{2,i}|M_0,\, M_1,\, Y_{1,i+1}^n,\, Z_2^{i-1}) + 2n\delta \\
&= \sum_{i=1}^{n} I(V_{2,i};\, Y_{1,i}|V_i) - \sum_{i=1}^{n} I(V_{2,i};\, Z_{2,i}|V_i) + 2n\delta
\end{aligned}
$$

where (a) and (c) follow because M_2 is independent of (M_0, M_1), (b) and (d) follow from Fano's inequality, (e) follows from Lemma 2. Finally, by introducing a time-sharing random variable, we obtain the terms in the theorem.

IET Commun., 2014, Vol. 8, Iss. 11, pp. 1965–1976
doi: 10.1049/iet-com.2014.0023

9.2 Appendix 2: Proof of converse for Theorem 4

Define the following variables

$$W_i = (M_0, Z_3^{i-1}, Z_{2,i+1}^n)$$
$$U_i = (M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n)$$

First, consider the rate R_1

$$\begin{aligned}
nR_1 &= H(M_1) \overset{(a)}{=} H(M_1|M_0) \\
&\overset{(b)}{\leq} I(M_1; Z_2^n|M_0) + n\delta \\
&\overset{(c)}{\leq} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n) + 2n\delta \\
&= I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n, M_0) \\
&\quad + I(M_1; M_0|Z_3^n) + 2n\delta \\
&\overset{(d)}{=} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) \\
&\quad + I(M_1; M_0|Z_3^n) + 2n\delta \\
&\leq I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) \\
&\quad + H(M_0|Z_3^n) + 2n\delta \\
&\overset{(e)}{\leq} I(M_1; Z_2^n|M_0) - I(M_1; Z_3^n|M_0) + 3n\delta \\
&= \sum_{i=1}^n I(M_1; Z_{2,i}|M_0, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1}^n I(M_1; Z_{3,i}|M_0, Z_3^{i-1}) + 3n\delta \\
&\overset{(f)}{=} \sum_{i=1}^n I(M_1; Z_{2,i}|M_0, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1}^n I(M_1; Z_{3,i}|M_0, Z_3^{i-1}, Z_{2,i+1}^n) + 3n\delta \\
&= \sum_{i=1}^n I(U_i; Z_{2,i}|W_i) - \sum_{i=1}^n I(U_i; Z_{3,i}|W_i) + 3n\delta
\end{aligned}$$

where (a) and (d) follow because M_1 is independent of M_0, (b) and (e) follow from Fano's inequality, (c) follows from the secrecy condition, (f) follows from Lemma 2. Next, consider the rate R_2

$$\begin{aligned}
nR_2 &= H(M_2) \overset{(a)}{=} H(M_2|M_1, M_0) \\
&\overset{(b)}{\leq} I(M_2; Y_1^n|M_1, M_0) + n\delta \\
&\overset{(c)}{\leq} I(M_2; Y_1^n|M_1, M_0) - I(M_2, M_1; Z_3^n) + 2n\delta \\
&\leq I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1) + 2n\delta \\
&= I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n, M_0|M_1) \\
&\quad + I(M_2; M_0|M_1, Z_3^n) + 2n\delta \\
&\overset{(d)}{=} I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) \\
&\quad + I(M_2; M_0|M_1, Z_3^n) + 2n\delta \\
&\leq I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) \\
&\quad + H(M_0|M_1, Z_3^n) + 2n\delta \\
&\overset{(e)}{\leq} I(M_2; Y_1^n|M_1, M_0) - I(M_2; Z_3^n|M_1, M_0) + 3n\delta \\
&= \sum_{i=1}^n I(M_2; Y_{1,i}|M_1, M_0, Y_{1,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2; Z_{3,i}|M_0, M_1, Z_3^{i-1}) + 3n\delta \\
&\overset{(f)}{=} \sum_{i=1}^n I(M_2; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Y_{1,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Y_{1,i+1}^n) + 3n\delta \\
&\overset{(g)}{=} \sum_{i=1}^n I(M_2; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Y_{1,i+1}^n, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Y_{1,i+1}^n, Z_{2,i+1}^n) + 3n\delta \\
&\overset{(h)}{\leq} \sum_{i=1}^n I(M_2; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Y_{1,i+1}^n, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Y_{1,i+1}^n, Z_{2,i+1}^n) \\
&\quad + \sum_{i=1}^n I(Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 3n\delta \\
&= \sum_{i=1}^n I(M_2, Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 3n\delta \\
&\overset{(i)}{\leq} \sum_{i=1}^n I(M_2, Y_{1,i+1}^n; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(M_2, Y_{1,i+1}^n; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad + \sum_{i=1}^n I(X_i; Y_{1,i}|M_1, M_0, M_2, Y_{1,i+1}^n, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(X_i; Z_{3,i}|M_0, M_1, Z_3^{i-1}, M_2, Y_{1,i+1}^n, Z_{2,i+1}^n) + 3n\delta \\
&\overset{(j)}{=} \sum_{i=1}^n I(X_i; Y_{1,i}|M_1, M_0, Z_3^{i-1}, Z_{2,i+1}^n) \\
&\quad - \sum_{i=1} I(X_i; Z_{3,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 3n\delta \\
&= \sum_{i=1}^n I(X_i; Y_{1,i}|U_i) - \sum_{i=1} I(X_i; Z_{3,i}|U_i) + 3n\delta
\end{aligned}$$

where (a) and (d) follow because M_2 is independent of (M_0, M_1), (b) and (e) follow from Fano's inequality, (c) follows from the secrecy condition, (f) follows from Lemma 2, (g) follows because Z_2 is a degraded version of Y_1, that is,

$Z_{2,i+1}^n \to Y_{1,i+1}^n \to X_i \to (Y_{1,i}, Z_{3,i})$ forms a Markov chain, (h) and (i) follow because Z_3 is a degraded version of Y_1, that is, $(M_1, M_0, Z_3^{i-1}, Z_{2,i+1}^n, Y_{1,i+1}^n) \to X_i \to Y_{1,i} \to Z_{3,i}$ and $(M_1, M_0, M_2, Y_{1,i+1}^n, Z_3^{i-1}, Z_{2,i+1}^n) \to X_i \to Y_{1,i} \to Z_{3,i}$ form Markov chains, respectively, (j) follows because given X_i, $(Y_{1,\ i}, Z_{3,\ i})$ is independent of other variables. Now, consider the equivocation rate R_e

$$
\begin{aligned}
nR_e &\le H(M_2|Z_2^n) \\
&= H(M_2) - I(M_2; Z_2^n) \\
&\overset{(a)}{=} H(M_2|M_0, M_1) - I(M_2; Z_2^n) \\
&\overset{(b)}{\le} I(M_2; Y_1^n|M_0, M_1) - I(M_2; Z_2^n) + n\delta \\
&= I(M_2; Y_1^n|M_0, M_1) - I(M_2; Z_2^n, M_0, M_1) \\
&+ I(M_2; M_0, M_1|Z_2^n) + n\delta \\
&\overset{(c)}{=} I(M_2; Y_1^n|M_0, M_1) - I(M_2; Z_2^n|M_0, M_1) \\
&+ I(M_2; M_0, M_1|Z_2^n) + n\delta \\
&\le I(M_2; Y_1^n|M_0, M_1) - I(M_2; Z_2^n|M_0, M_1) \\
&+ H(M_0, M_1|Z_2^n) + n\delta \\
&\overset{(d)}{\le} I(M_2; Y_1^n|M_0, M_1) - I(M_2; Z_2^n|M_0, M_1) + 2n\delta \\
&= \sum_{i=1}^n I(M_2; Y_{1,i}|M_0, M_1, Y_1^{i-1}) \\
&- \sum_{i=1}^n I(M_2; Z_{2,i}|M_0, M_1, Z_{2,i+1}^n) + 2n\delta \\
&\overset{(e)}{=} \sum_{i=1}^n I(M_2; Y_{1,i}|M_0, M_1, Y_1^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(M_2; Z_{2,i}|M_0, M_1, Y_1^{i-1}, Z_{2,i+1}^n) + 2n\delta \\
&\overset{(f)}{=} \sum_{i=1}^n I(M_2; Y_{1,i}|M_0, M_1, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(M_2; Z_{2,i}|M_0, M_1, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) + 2n\delta \\
&\overset{(g)}{\le} \sum_{i=1}^n I(M_2; Y_{1,i}|M_0, M_1, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(M_2; Z_{2,i}|M_0, M_1, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) \\
&+ \sum_{i=1}^n I(Y_1^{i-1}; Y_{1,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(Y_1^{i-1}; Z_{2,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 2n\delta \\
&= \sum_{i=1}^n I(M_2, Y_1^{i-1}; Y_{1,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(M_2, Y_1^{i-1}; Z_{2,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 2n\delta
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(h)}{\le} \sum_{i=1}^n I(M_2, Y_1^{i-1}; Y_{1,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(M_2, Y_1^{i-1}; Z_{2,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&+ \sum_{i=1}^n I(X_i; Y_{1,i}|M_0, M_1, M_2, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(X_i; Z_{2,i}|M_0, M_1, M_2, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) + 2n\delta \\
&\overset{(i)}{=} \sum_{i=1}^n I(X_i; Y_{1,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) \\
&- \sum_{i=1}^n I(X_i; Z_{2,i}|M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n) + 2n\delta \\
&= \sum_{i=1}^n I(X_i; Y_{1,i}|U_i) - \sum_{i=1}^n I(X_i; Z_{2,i}|U_i) + 2n\delta
\end{aligned}
$$

where (a) and (c) follow because M_2 is independent of (M_0, M_1), (b) and (d) follow from Fano's inequality, (e) follows from Lemma 2, (f) follows because Z_3 is a degraded version of Y_1, that is, $Z_3^{i-1} \to Y_1^{i-1} \to X_i \to (Y_{1,i}, Z_{2,i})$ forms a Markov chain, (g) and (h) follow because Z_2 is a degraded version of Y_1, that is, $(M_0, M_1, Z_3^{i-1}, Z_{2,i+1}^n, Y_1^{i-1}) \to X_i \to Y_{1,i} \to Z_{2,i}$ and $(M_0, M_1, M_2, Y_1^{i-1}, Z_3^{i-1}, Z_{2,i+1}^n) \to X_i \to Y_{1,i} \to Z_{2,i}$ form Markov chains, respectively, (i) follows because given X_i, $(Y_{1,\ i}, Z_{2,\ i})$ is independent of other random variables. Finally, consider the rate R_0

$$
\begin{aligned}
nR_0 = H(M_0) &\le I(M_0; Z_3^n) + n\delta \\
&= \sum_{i=1}^n I(M_0; Z_{3,i}|Z_3^{i-1}) + n\delta \\
&\le \sum_{i=1}^n I(M_0, Z_3^{i-1}; Z_{3,i}) + n\delta \\
&\le \sum_{i=1}^n I(M_0, Z_3^{i-1}, Z_{2,i+1}^n; Z_{3,i}) + n\delta = \sum_{i=1}^n I(W_i; Z_{3,i}) + n\delta
\end{aligned}
$$

Also, we have

$$
\begin{aligned}
nR_0 &= H(M_0) \\
&\le I(M_0; Z_2^n) + n\delta \\
&= \sum_{i=1}^n I(M_0; Z_{2,i}|Z_{2,i+1}^n) + n\delta \\
&\le \sum_{i=1}^n I(M_0, Z_{2,i+1}^n; Z_{2,i}) + n\delta \\
&\le \sum_{i=1}^n I(M_0, Z_3^{i-1}, Z_{2,i+1}^n; Z_{2,i}) + n\delta \\
&= \sum_{i=1}^n I(W_i; Z_{2,i}) + n\delta
\end{aligned}
$$

By introducing a time-sharing random variable, we obtain the terms in the theorem.

doi: 10.1049/iet-com.2014.0023