3-Receiver Broadcast Channels with Common and Confidential Messages

Yeow-Khiang Chia
Department of Electrical Engineering
Stanford University
Stanford, CA 94305, USA
Email: ykchia@stanford.edu

Abbas El Gamal
Department of Electrical Engineering
Stanford University
Stanford, CA 94305, USA
Email: abbas@ee.stanford.edu

***Abstract*—Achievable secrecy rate regions for the general 3-receiver broadcast channel with one common and one confidential message sets are established. We consider two setups: (i) when the confidential message is to be sent to two of the receivers and the third receiver is an eavesdropper; and (ii) when the confidential message is to be sent to one of the receivers and the other two receivers are eavesdroppers. We show that our secrecy rate regions are optimum for some special cases.**

I. Introduction

In a seminal paper, Wyner [1] introduced the wiretap channel, where a sender wishes to communicate a message to a receiver, while keeping the message secret from an eavesdropper. He established the secrecy capacity of the channel, which is the optimal trade-off between the rate for reliable communication to the legitimate receiver and the eavesdropper's message equivocation rate. This result was later extended by Csiszár and Körner [2] to establish the secrecy capacity of the 2-receiver broadcast channel with one confidential message and one common message. In their setup, a common message is to be sent to both receivers and a confidential message is to be sent only to the first receiver under a constraint on the second receiver's (eavesdropper) equivocation rate. More recent work following this direction includes the paper by Ruoheng et al. [3] in which inner and outer bounds on the secrecy capacity regions of both the broadcast and interference channels with independent confidential messages are established.

Extending the result of Csiszár and Körner to more than 2 receivers has remained open, since the capacity region (without secrecy constraints) of the 3-receiver broadcast channel with degraded message sets is not known in general. Recently, Nair and El Gamal [4] showed that the straightforward extension of the Körner and Marton capacity region for the 2-receiver broadcast channel with degraded message sets [5] to more than 3 receivers is not optimal. They established an achievable rate region for the general 3-receiver broadcast channel and showed that it can be strictly larger than the straightforward extension of the Körner and Marton region.

In this paper, we consider the 3-receivers broadcast channel with one common and one confidential message sets. This setup leads to two natural variations; a *2-receiver, 1-eavesdropper* scenario where the confidential message is to be reliably communicated to two receivers and kept secret from the third receiver, and a *1-receiver, 2-eavesdropper* scenario where the confidential message is to be communicated to only one receiver and kept secret from the other two receivers. We establish inner bounds on the secrecy capacity regions for both scenarios using the techniques of rate splitting, superposition coding, random binning, Marton binning, and indirect decoding [4]. We specialize the inner bound for the 2-receiver, 1-eavesdropper setup to obtain a lower bound on the secrecy capacity for the case where a message is to be sent to the two receivers but kept secret from the eavesdropper. We show that this lower bound is tight for the reversely degraded product broadcast channel. For the 1-receiver, 2-eavesdropper scenario, we establish inner and outer bounds on the secrecy capacity region for the class of 3-receiver multi-level broadcast channel [6]. We show that the bounds coincide when the receiver is more capable than the non-degraded eavesdropper.

II. Definitions and Problem Setup

We consider the 3-receiver discrete memoryless broadcast channel with input alphabet $\mathcal{X}$, output alphabets $\mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3$ and conditional probability mass functions $p(y_1, y_2, y_3|x)$ and investigate the following two scenarios.

A. 2-Receivers, 1-Eavesdropper

Here the confidential message is to be sent to receivers Y_1 and Y_2 and is to be kept secret from the eavesdropper Y_3. A $(2^{nR_0}, 2^{nR_1}, n)$ message set code for this scenario

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

consists of: (i) two messages (M_0, M_1) uniformly distributed over $[1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$; (ii) an encoder that randomly generates a codeword $X^n(m_0, m_1)$ according to the conditional pmf $p(x^n|m_0, m_1)$; and (iii) 3 decoders; the first decoder assigns to each received sequence y_1^n an estimate $(\hat{M}_{01}, \hat{M}_{11}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ or an error message, the second decoder assigns to each received sequence y_2^n an estimate $(\hat{M}_{02}, \hat{M}_{12}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ or an error message, and the third receiver assigns to each received sequence y_3^n an estimate $\hat{M}_{03} \in [1 : 2^{nR_0}]$ or an error message. The probability of error for this scenario is

$$P_{e1}^{(n)} = \mathrm{P}\left\{\hat{M}_{0j} \neq M_0 \text{ for } j = 1, 2, 3 \text{ or } \hat{M}_{1j} \neq M_1 \text{ for } j = 1, 2\right\}.$$

The equivocation rate at receiver Y_3, which measures the amount of uncertainty receiver Y_3 has about message M_1, is given by $H(M_1|Y_3^n)/n$.

A secrecy rate tuple (R_0, R_1, R_e) is said to be achievable if

$$\lim_{n\to\infty} P_{e1}^{(n)} = 0, \text{ and } \liminf_{n\to\infty} \frac{1}{n} H(M_1|Y_3^n) \geq R_e.$$

The *secrecy capacity region* is the closure of the set of achievable rate tuples (R_0, R_1, R_e).

B. 1-Receiver, 2-Eavesdroppers

In this scenario, the confidential message is to be sent only to receiver Y_1 and kept secret from the eavesdroppers Y_2 and Y_3. A $(2^{nR_0}, 2^{nR_1}, n)$ message set code for this scenario consists of the same message sets and encoding function as in the 2-receiver, 1-eavesdropper case. The first decoder assigns to each received sequence y_1^n an estimate $(\hat{M}_{01}, \hat{M}_1) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ or an error message, the second decoder assigns to each received sequence y_2^n an estimate $\hat{M}_{02} \in [1 : 2^{nR_0}]$ or an error message, and the third receiver assigns to each received sequence y_3^n an estimate $\hat{M}_{01} \in [1 : 2^{nR_0}]$ or an error message. The probability of error is

$$P_{e2}^{(n)} = \mathrm{P}\{\hat{M}_{0j} \neq M_0 \text{ for } j = 1, 2, 3 \text{ or } \hat{M}_1 \neq M_1\}.$$

The equivocation rates at the two eavesdroppers are $H(M_1|Y_2^n)/n$ and $H(M_1|Y_3^n)/n$.

A secrecy rate tuple $(R_0, R_1, R_{e2}, R_{e3})$ is said to be achievable if

$$\lim_{n\to\infty} P_{e2}^{(n)} = 0,$$
$$\liminf_{n\to\infty} \frac{1}{n} H(M_1|Y_j^n) \geq R_{ej}, \ j = 2, 3.$$

The *secrecy capacity region* is the closure of the set of achievable rate tuples $(R_0, R_1, R_{e2}, R_{e3})$.

In the following sections, we establish inner bounds on the secrecy capacity regions for the above two scenarios.

III. 2-RECEIVERS, 1-EAVESDROPPER

We establish an inner bound on the secrecy capacity for the 3-receiver broadcast channel with one common and one confidential message when the confidential message is to be sent to receivers Y_1 and Y_2 and kept secret from receiver Y_3. As motivation, first consider the case when $M_0 = \emptyset$ and $M_1 = M \in [1 : 2^{nR}]$ is to be kept asymptotically secret from Y_3, i.e., $\lim_{n\to\infty} I(M; Y_3^n)/n = 0$. For this case, a straightforward extension of the Csiszár and Körner [2] scheme to 3-receivers yields the achievable secrecy rate

$$R < \max_{p(v,x)} \min\{I(V;Y_1) - I(V;Y_3), I(V;Y_2) - I(V;Y_3)\}.$$

Now, suppose Y_3 is a degraded version of Y_1, then from the Wyner wiretap result, we know that $I(V;Y_1) - I(V;Y_3) \leq I(X;Y_1) - I(X;Y_3)$ for all $p(v,x)$. However, no such inequality holds in general for the second term. Using indirect decoding [4], we can replace V with X in the first term while keeping V in the second term, which can potentially increase the rate. To show the achievability of this potentially larger rate, we generate 2^{nS_0} sequences $v^n(l_0)$, $l_0 \in [1 : 2^{nS_0}]$ each according to $\prod_{i=1}^n p(v_i)$ and partition the set $[1 : 2^{nS_0}]$ into 2^{nR} equal size bins. For each $v^n(l_0)$, conditionally independently generate $2^{n(S_1)}$ sequences $x^n(l_0, l_1)$, $l_1 \in [1 : 2^{nS_1}]$ each according to $\prod_{i=1}^n p(x_i|v_i)$. To send a message $m \in [1 : 2^{nR}]$, randomly choose an index L_0 from bin m and and an index $L_1 \in [1 : 2^{nS_1}]$, and send $x^n(L_0, L_1)$. Y_2 finds m by directly decoding V and Y_1 finds m by indirect decoding through X. These steps succeed with high probability provided

$$S_0 < I(V;Y_2), \ S_0 + S_1 < I(X;Y_1).$$

It can be shown that M is hidden from Y_3 if

$$S_0 - R > I(V;Y_3), \ S_1 > I(X;Y_3|V).$$

Using Fourier-Motzkin shows the achievability of the rate

$$R < \max_{p(v,x)} \min\{I(X;Y_1) - I(X;Y_3), I(V;Y_2) - I(V;Y_3)\}.$$

The above argument can be generalized to obtain the following inner bound.

Theorem 1: An inner bound to the secrecy capacity region of the 2-receiver, 1-eavesdropper broadcast channel with one common and one confidential messages is

given by the set of non-negative rate tuples (R_0, R_1, R_e) such that

$$\begin{aligned}
R_0 &< I(U;Y_3),\\
R_1 &< \min\{I(V_1;Y_1|U) - I(V_1;Y_3|V_0),\\
&\qquad I(V_2;Y_2|U) - I(V_2;Y_3|V_0)\},\\
2R_1 &< I(V_2;Y_2|U) + I(V_1;Y_1|U) - I(V_1,V_2|V_0)\\
&\quad - I(V_1;Y_3|V_0) - I(V_2;Y_3|V_0),\\
R_0+R_1 &< \min\{I(V_1;Y_1) - I(V_1;Y_3|V_0),\\
&\qquad I(V_2;Y_2) - I(V_2;Y_3|V_0)\},\\
R_0+2R_1 &< I(V_1;Y_1) + I(V_2;Y_2|U) - I(V_1;V_2|V_0)\\
&\quad - I(V_1;Y_3|V_0) - I(V_2;Y_3|V_0),\\
R_0+2R_1 &< I(V_1;Y_1|U) + I(V_2;Y_2) - I(V_1,V_2|V_0)\\
&\quad - I(V_1;Y_3|V_0) - I(V_2;Y_3|V_0),\\
2R_0+2R_1 &< I(V_1;Y_1) + I(V_2;Y_2) - I(V_1;V_2|V_0)\\
&\quad - I(V_1;Y_3|V_0) - I(V_2;Y_3|V_0),\\
R_e &\le [R_1 - I(V_0;Y_3|U)]^+,
\end{aligned}$$

for some $p(u,v_0,v_1,v_2,x) = p(u)p(v_0|u)p(v_1|v_0)$ $\cdot\, p(x,v_2|v_0,v_1) = p(u)p(v_0|u)p(v_2|v_0)p(x,v_1|v_0,v_2)$ such that $I(V_1,V_2;Y_3|V_0) \le I(V_1;Y_3|V_0) + I(V_2;Y_3|V_0)$, where $[x]^+ := \max\{0,x\}$.

Note that if we discard the equivocation constraints and set $V_0 = V_1 = V_2 = X$, the inner bound reduces to the straightforward extension of the Körner-Marton degraded message set region to the 3-receiver case [4, Corollary 1]. We provide a proof outline.

Codebook generation: Randomly and independently generate 2^{nR_0} sequences $u^n(m_0)$ each according to $\prod_{i=1}^n p(u_i)$. For each $u^n(m_0)$, independently generate 2^{nR_1} sequences $v_0^n(m_1,m_0)$ each according to $\prod_{i=1}^n p(v_{0i}|u_i)$. For each $v_0^n(m_1,m_0)$, generate 2^{nT_1} sequences $v_1^n(t_1,m_1,m_0)$ each according to $\prod_{i=1}^n p(v_{1i}|v_{0i})$, and partition them into 2^{nS_1} equal size bins. Similarly, for each $v_0^n(m_1,m_0)$, randomly generate 2^{nT_2} sequences $v_2^n(t_2,m_1,m_0)$ each according to $\prod_{i=1}^n p(v_{2i}|v_{0i})$, and partition them into 2^{nS_2} bins. Finally, for each product bin $(l_1,l_2) \in [1 : 2^{nS_1}] \times [1 : 2^{nS_2}]$, find a jointly typical sequence pair $(v_1^n(t_1(l_1),m_1,m_0), v_2^n(t_2(l_2),m_1,m_0))$. This succeeds with high probability provided

$$S_1 + S_2 < T_1 + T_2 - I(V_1;V_2|V_0).$$

Encoding: To send a message pair (m_0,m_1), the encoder first chooses the sequence pair $(u^n(m_0), v_0^n(m_1,m_0))$. It then randomly chooses a product bin (L_1,L_2) and finds the jointly typical sequence pair $(v_1^n(t_1(L_1),m_1,m_0), v_2^n(t_2(L_2),m_1,m_0))$ in it. Finally, it generates a codeword X^n at random according to $\prod_{i=1}^n p(x_i|v_{1i},v_{2i})$.

Decoding and error analysis: Receiver Y_1 finds (m_0,m_1) indirectly by decoding V_1. Receiver Y_2 finds (m_0,m_1) by indirectly decoding V_2. Receiver Y_3 finds m_0 by decoding U. These steps succeed with high probability provided

$$\begin{aligned}
R_0+R_1+T_1 &< I(V_1;Y_1),\\
R_1+T_1 &< I(V_1;Y_1|U),\\
R_0+R_1+T_2 &< I(V_1;Y_2),\\
R_1+T_2 &< I(V_1;Y_2|U),\\
R_0 &< I(U;Y_3).
\end{aligned}$$

Equivocation analysis: We consider two cases. If $R_1 \le I(V_0;Y_3|U)$, then $R_e = 0$. If $R_1 > I(V_0;Y_3|U)$, we split message M_1 into 2 independent parts, $M_{1c} \in [1 : 2^{n(I(V_0;Y_3|U)+4\delta(\epsilon))}]$ and $M_{1p} \in [1 : 2^{n(R_1 - I(V_0;Y_3|U)-4\delta(\epsilon))}]$ and lower bound the equivocation as follows

$$\begin{aligned}
H(M_1|Y_3^n) &\ge H(M_{1p}|Y_3^n,U^n)\\
&= H(M_{1p}) - I(M_{1p};Y_3^n|U^n)\\
&\overset{(a)}{\ge} H(M_{1p}) - 3n\delta(\epsilon) - 3n\epsilon_n\\
&= n(R_1 - I(V_0;Y_3|U) - 7n\delta(\epsilon) - 3\epsilon_n),
\end{aligned}$$

where $\delta(\epsilon) \to 0$ as $\epsilon \to 0$ and $\epsilon_n \to 0$ as $n \to \infty$. This implies that

$$R_e \le R_1 - I(V_0;Y_3|U) - 7\delta(\epsilon) - 3\epsilon_n.$$

To prove step (a), consider

$$\begin{aligned}
&I(M_{1p};Y_3^n|U^n)\\
&= I(t_1(L_1),t_2(L_2),M_{1p},M_{1c};Y_3^n|U^n)\\
&\quad - I(t_1(L_1),t_2(L_2),M_{1c};Y_3^n|M_{1p},U^n)\\
&\overset{(b)}{\le} I(V_1^n,V_2^n;Y_3^n|U^n) - I(M_{1c};Y_3^n|M_{1p},U^n)\\
&\quad - I(t_1(L_1),t_2(L_2);Y_3^n|M_1,U^n)\\
&\overset{(c)}{\le} nI(V_1,V_2;Y_3|U) - H(M_{1c}|M_{1p},U^n)\\
&\quad + H(M_{1c}|M_{1p},U^n,Y_3^n)\\
&\quad - I(t_1(L_1),t_2(L_2);Y_3^n|M_1,U^n)\\
&\overset{(d)}{\le} nI(V_1,V_2;Y_3|U) - n(I(V_0;Y_3|U)+4\delta(\epsilon))\\
&\quad + 5n\delta(\epsilon) + n\epsilon_n - I(t_1(L_1),t_2(L_2);Y_3^n|M_1,U^n)\\
&= nI(V_1,V_2;Y_3|V_0) - H(t_1(L_1)|M_1,U^n)\\
&\quad - H(t_2(L_2)|M_1,U^n)\\
&\quad + H(t_1(L_1),t_2(L_2)|M_1,U^n,Y_3^n) + n\delta(\epsilon) + n\epsilon_n\\
&\overset{(e)}{\le} nI(V_1,V_2;Y_3|V_0) - n(S_1+S_2)
\end{aligned}$$

$$
\begin{aligned}
&+ H(t_1(L_1)|M_1, U^n, Y_3^n) \\
&+ H(t_2(L_2)|M_1, U^n, Y_3^n) + n\delta(\epsilon) + n\epsilon_n \\
&\overset{(f)}{\leq} nI(V_1, V_2; Y_3|V_0) - n(S_1 + S_2) + nS_1 + nS_2 \\
&- nI(V_1; Y_3|V_0) - nI(V_2; Y_3|V_0) + 3n(\delta(\epsilon) + \epsilon_n) \\
&\overset{(g)}{\leq} 3n(\delta(\epsilon) + \epsilon_n),
\end{aligned}
$$

where (b) follows by the data processing inequality, (c) follows by the concavity of mutual information (averaged over codewords), (d) holds from the rate definitions, (e) follows because conditioning reduces entropy, (g) follows from the constraint $I(V_1, V_2; Y_3|V_0) \leq I(V_1; Y_3|V_0) + I(V_2; Y_3|V_0)$, and (f) holds provided

$$S_j \geq I(V_j; Y_3|V_0) + 4\delta(\epsilon),\ j = 1, 2.$$

Using Fourier-Motzkin gives the achievable region stated in Theorem 1.

As a special case of Theorem 1, consider the asymptotically perfect secrecy setting. In the proof of Theorem 1, we showed that a sub-message M_{1p} with rate $R_{1p} = R_1 - I(V_0; Y_3|U) - 4\delta(\epsilon)$ can be hidden from the eavesdropper with asymptotically perfect secrecy. Using this observation and the fact that the region in Theorem 1 is convex, we set $R_0 = 0$ and $R = R_1 - I(V_0; Y_3|Q)$ in the characterization of Theorem 1 to obtain the following.

Corollary 1: A rate R is achievable for the setup of sending a confidential message to two receivers, with one eavesdropper if

$$
\begin{aligned}
R < \min\{&I(V_1; Y_1|Q) - I(V_1; Y_3|Q), \\
&I(V_2; Y_2|Q) - I(V_2; Y_3|Q), \\
&\frac{1}{2}(I(V_1; Y_1|Q) + I(V_2; Y_2|Q) - I(V_1; Y_3|Q) \\
&\quad - I(V_2; Y_3|Q) - I(V_1; V_2|V_0))\}
\end{aligned}
$$

for some $p(q, v_0, v_1, v_2, x) = p(q)p(v_0|q)p(v_1|v_0) \cdot p(x, v_2|v_0, v_1) = p(q)p(v_0|q)p(v_2|v_0)p(x, v_1|v_0, v_2)$ such that $I(V_1, V_2; Y_3|V_0) \leq I(V_1; Y_3|V_0) + I(V_2; Y_3|V_0)$.

As an example of Corollary 1, consider the reversely degraded product broadcast channel with sender $X = (X_1, X_2 \ldots, X_k)$, receivers $Y_j = (Y_{j1}, Y_{j2} \ldots, Y_{jk})$ for $j = 1, 2, 3$, and conditional probability mass functions $p(y_1, y_2, y_3|x) = \prod_{l=1}^{k} p(y_{1l}, y_{2l}, y_{3l}|x_l)$. In [7], it is shown that the secrecy rate R is achievable if

$$R < \min_{j \in \{1,2\}} \sum_{l=1}^{k} [I(U_l; Y_{jl}) - I(U_l; Y_{3l})]^+ \qquad (1)$$

for some $p(u_1, \ldots, u_k, x) = \prod_{l=1}^{k} p(u_l)p(x_l|u_l)$. Further, this rate is shown to be optimal when the channel is reversely degraded (with $U_l = X_l$), i.e., each subchannel is degraded but not necessarily in the same order. We can show that this result is a special case of Corollary 1. Define the sets of l indexes: $\mathcal{C} := \{l : I(U_l; Y_{1l}) - I(U_l; Y_{3l}) \geq 0, I(U_l; Y_{2l}) - I(U_l; Y_{3l}) \geq 0\}$, $\mathcal{A} := \{l : I(U_l; Y_{1l}) - I(U_l; Y_{3l}) \geq 0\}$ and $\mathcal{B} := \{l : I(U_l; Y_{2l}) - I(U_l; Y_{3l}) \geq 0\}$. Now, setting $V_0 = \{U_l : l \in \mathcal{C}\}$, $V_1 = \{U_l : l \in \mathcal{A}\}$, and $V_2 = \{U_l : l \in \mathcal{B}\}$ in the rate expression of Corollary 1 yields (1) Note that the constraint in the corollary is satisfied for this choice of auxiliary random variables.

IV. 1-RECEIVER, 2-EAVESDROPPERS

We now consider the case where the confidential message M_1 is to be sent only to Y_1 and kept hidden from the eavesdroppers Y_2 and Y_3. For simplicity, we only consider the special case of multi-level broadcast channel [6], where $p(y_1, y_2, y_3|x) = p(y_1, y_3|x)p(y_2|y_1)$.

Proposition 1: An inner bound to the secrecy capacity region of the 1-receiver, 2-eavesdropper multi-level broadcast channel with one common message and one confidential message is given by the set of non-negative rate tuples $(R_0, R_1, R_{e2}, R_{e3})$ such that

$$
\begin{aligned}
R_0 &< \min\{I(U; Y_2), I(U_3; Y_3)\}, \\
R_1 &< I(V; Y_1|U), \\
R_0 + R_1 &< I(U_3; Y_3) + I(V; Y_1|U_3), \\
R_{e2} &\leq \min\{R_1, I(V; Y_1|U) - I(V; Y_2|U)\}, \\
R_{e2} &\leq [I(U_3; Y_3) - R_0 - I(U_3; Y_2|U)]^+ \\
&\quad + I(V; Y_1|U_3) - I(V; Y_2|U_3), \\
R_{e3} &\leq \min\{R_1, [I(V; Y_1|U_3) - I(V; Y_3|U_3)]^+\}
\end{aligned}
$$

for some $p(u, u_3, v, x) = p(u)p(u_3|u)p(v|u_3)p(x|v)$. If we set $V = X$ and discard the terms involving R_e, we obtain the capacity region for the degraded message sets in [4]. Setting $U = U_3 = Y_3 = \emptyset$, $V = X$, $R_0 = 0$, and $R_{e2} = R_1$, we obtain the secrecy capacity of the Wyner wiretap channel. Further, setting $Y_2 = \emptyset$, $U_1 = U_2 = U$, we obtain the Csiszár-Körner secrecy region.

The proof of achievability follows that of [4, Section III], with V playing the role of X.

Codebook generation: Let $R_1 = S_1 + S_2$. Randomly and independently generate 2^{nR_0} sequences $u^n(m_0)$ each according to $\prod_{i=1}^{n} p(u_i)$. For each $u^n(m_0)$, independently generate 2^{nS_1} sequences $u_3^n(l_1, m_0)$ each according to $\prod_{i=1}^{n} p(u_{3i}|u_i)$. For each $u_3^n(l_1, m_0)$, generate 2^{nS_2} sequences $v^n(l_2, l_1, m_0)$ each according to $\prod_{i=1}^{n} p(v_i|u_{3i})$.

Encoding: To send a message (m_0, m_1), we consider the sequence $v^n(l_2, l_1, m_0)$ and send X^n generated according to $\prod_{i=1}^{n} p(x_i|v_i(l_2, l_1, m_0))$.

Decoding, error and equivocation: Receiver Y_1 finds (m_0, m_1) by decoding V, Y_2 finds m_0 by decoding U, and Y_3 finds m_0 indirectly through U_3. These decoding steps succeed with high probability provided

$$\begin{aligned} R_0 + R_1 &< I(V;Y_1), \\ R_1 &< I(V;Y_1|U), \\ S_2 &< I(V;Y_1|U_3), \\ R_0 &< I(U;Y_2), \\ R_0 + S_1 &< I(U_3;Y_3). \end{aligned}$$

The equivocations can be calculated in the same way as in the previous section, and we obtain the constraints

$$\begin{aligned} R_{e2} &\le [S_1 - I(U_3;Y_2|U)]^+ + [S_2 - I(V;Y_2|U_3)]^+, \\ R_{e3} &\le [S_2 - I(V;Y_3|U_3)]^+. \end{aligned}$$

Finally, we show that we can choose S_1 and S_2 to achieve any point in the region given by Theorem 2.

We now establish an outer bound and use it to show that the inner bound in Proposition 1 is tight for several special cases.

Proposition 2: An outer bound on the secrecy capacity of the multi-level 3-receiver broadcast channel with one common and one confidential messages is given by the set of rate tuples $(R_0, R_1, R_{e2}, R_{e3})$ such that

$$\begin{aligned} R_0 &\le \min\{I(U;Y_2), I(U_3;Y_3)\}, \\ R_1 &\le I(V;Y_1|U), \\ R_0 + R_1 &\le I(U_3;Y_3) + I(V;Y_1|U_3), \\ R_{e2} &\le I(X;Y_1|U) - I(X;Y_2|U), \\ R_{e2} &\le [I(U_3;Y_3) - R_0 - I(U_3;Y_2|U)]^+ \\ &\quad + I(X;Y_1|U_3) - I(X;Y_2|U_3), \\ R_{e3} &\le [I(V;Y_1|U_3) - I(V;Y_3|U_3)]^+ \end{aligned}$$

for some $p(u, u_3, v, x) = p(u)p(u_3|u)p(v|u_3)p(x|v)$.

The proof of this proposition uses a combination of standard converse techniques from [8], [9] and [2].

Using Propositions 1 and 2, we can establish the secrecy capacity region for the following special cases.

1) Y_1 *more capable than* Y_3*:* If Y_1 is more capable than Y_3, the capacity region is given by:

$$\begin{aligned} R_0 &\le \min\{I(U;Y_2), I(U_3;Y_3)\}, \\ R_1 &\le I(X;Y_1|U), \\ R_0 + R_1 &\le I(U_3;Y_3) + I(X;Y_1|U_3), \\ R_{e2} &\le I(X;Y_1|U) - I(X;Y_2|U), \\ R_{e2} &\le [I(U_3;Y_3) - R_0 - I(U_3;Y_2|U)]^+ \\ &\quad + I(X;Y_1|U_3) - I(X;Y_2|U_3), \\ R_{e3} &\le [I(X;Y_1|U_3) - I(X;Y_3|U_3)]^+ \end{aligned}$$

for some $p(u, u_3, x) = p(u)p(u_3|u)p(x|u_3)$.

2) *One eavesdropper:* Here, we consider the two scenarios where either Y_2 or Y_3 is an eavesdropper and the other receiver is neutral, i.e., there is no constraint on its equivocation. The secrecy capacity regions for these two scenarios are as follows.

Y_3 *is neutral*: The secrecy capacity region is the set of rate tuples (R_0, R_1, R_{e2}) such that

$$\begin{aligned} R_0 &\le \min\{I(U;Y_2), I(U_3;Y_3)\}, \\ R_1 &\le I(X;Y_1|U), \\ R_0 + R_1 &\le I(U_3;Y_3) + I(X;Y_1|U_3), \\ R_{e2} &\le I(X;Y_1|U) - I(X;Y_2|U), \\ R_{e2} &\le [I(U_3;Y_3) - R_0 - I(U_3;Y_2|U)]^+ \\ &\quad + I(X;Y_1|U_3) - I(X;Y_2|U_3) \end{aligned}$$

for some $p(u, u_3, x) = p(u)p(u_3|u)p(x|u_3)$.

Y_2 *is neutral*: The secrecy capacity region is the set of rate tuples (R_0, R_1, R_{e3}) such that

$$\begin{aligned} R_0 &\le \min\{I(U;Y_2), I(U_3;Y_3)\}, \\ R_1 &\le I(V;Y_1|U), \\ R_0 + R_1 &\le I(U_3;Y_3) + I(V;Y_1|U_3), \\ R_{e3} &\le [I(V;Y_1|U_3) - I(V;Y_3|U_3)]^+ \end{aligned}$$

for some $p(u, u_3, v, x) = p(u)p(u_3|u)p(v|u_3)p(x|v)$.

ACKNOWLEDGMENT

We thank Chandra Nair, Han-I Su and Bernd Bandemer for helpful comments.

REFERENCES

[1] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[2] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Info. Theory*, IT-24:339–348, May 1978.

[3] Ruoheng Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Info. Theory*, 54(6):2493–2507, June 2008.

[4] C. Nair and A. El Gamal. The capacity region of a class of 3-receiver broadcast channels with degraded message sets. *IEEE Trans. Info. Theory*, 2008. Submitted. Available online at http://arxiv.org/abs/0712.3327.

[5] J. Körner and K. Marton. General broadcast channels with degraded message sets. *IEEE Trans. Info. Theory*, IT-23:60–64, Jan 1977.

[6] S. Borade, L. Zheng, and M. Trott. Multilevel broadcast networks. In *International Symposium on Information Theory*, 2007.

[7] A. Khisti, A. Tchamkerten, and G.W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Info. Theory*, 54(6):2453–2469, June 2008.

[8] A. El Gamal. The capacity of a class of broadcast channels. *IEEE Trans. Info. Theory*, 25(2):166–169, Mar 1979.

[9] A. El Gamal. The feedback capacity of degraded broadcast channels (corresp.). *IEEE Transactions on Information Theory*, 24(3):379–381, May 1978.