Secure Communication Through Nakagami-m Fading MISO Channel

Md. Zahurul I. Sarkar and Tharmalingam Ratnarajah
ECIT, Queen’s University Belfast
Queen’s Road, Queen’s Island
Belfast, BT9 9DT, UK
Email: msarkar01@qub.ac.uk

Abstract—We consider the problem of secret communication over Nakagami-m fading multiple-input single-output (MISO) broadcast channel, where transmitter sends messages to the destination users following two different transmission protocols. In the first transmission protocol, transmitter sends a confidential message to user 1, and user 2 acts as an eavesdropper. In this protocol, at first, we define the ergodic secrecy capacity for the full channel state information (CSI) case and then we consider the case of only main channel CSI at the transmitter. Finally, we define the secrecy capacity in case of open-loop spatial multiplexing transmission scheme and present the analytical expression for the lower bound of ergodic secrecy capacity. In the second transmission protocol, we consider the transmission of two independent messages to user 1 and user 2 with information-theoretic secrecy, where each user would like to obtain its own confidential message in a reliable and safe manner. Under this communication scenario, an achievable secrecy capacity region is developed using secret dirty-paper coding scheme.

Index Terms—Main channel, eavesdropper’s channel, ergodic secrecy capacity, secret dirty-paper coding.

I. INTRODUCTION

Security in wireless communication networks is an important issue, as these networks are used to transmit personal information. Recently, the secrecy capacity for both the transmitter and receiver equipped with single antenna (SISO) case [1], the transmitter with single antenna and the receiver with multiple antenna (SIMO) case [2], the transmitter with multiple antenna and the receiver with single antenna (MISO) case [3] were characterized for Rayleigh fading channels and the secrecy capacity for both the transmitter and receiver equipped with multiple antenna (MIMO) case for Gaussian channel was studied in [4]. On the other hand, Nakagami-m distribution provides more flexibility in matching experimental data than the Rayleigh, log-normal or Rician distributions. It has the advantages of including Rayleigh as a special case and it can model fading conditions which are more or less severe than that of Rayleigh [5]. Recently, the upper bound of secret key rate for Nakagami-m fading SISO channel in the presence of an eavesdropper was determined in [6]. In this paper, we consider two different transmission protocols through Nakagami-m fading MISO channel. In the first transmission protocol, we define ergodic secrecy capacity under different assumptions on the available transmitter CSI. In the second transmission protocol, we develop an achievable secrecy capacity region using secret dirty-paper coding scheme.

The rest of the paper is organized as follows. Section II describes the system model and transmission protocol. The formulation of secrecy capacity for transmission protocol 1 is discussed in Section III. Section IV describes the achievable secrecy capacity region for transmission protocol 2. Section V provides the numerical results of this paper. Finally, Section VI describes the concluding remarks of this work.

II. SYSTEM MODEL AND TRANSMISSION PROTOCOL

The system model is shown in Fig. 1. Two users called user 1 and user 2 communicate with the base station through channel 1 and channel 2, respectively. The transmitter is equipped with $n_T$ antennas while both the users are equipped with single antenna. Thus, each user experiences a superposition of different paths from the base station. The received signals at user 1 and user 2 are given by the following expressions;

$$y_{1,t} = h^Tx_t + w_{1,t}$$
$$y_{2,t} = g^Tx_t + w_{2,t}$$

where $x_t \in \mathbb{C}^{n_T \times 1}$ is the complex input vector at time $t$ with zero-mean and $n_T \times n_T$ covariance matrix $R_x \succeq 0$, i.e. $x_t \sim CN(0, R_x)$. $h, g \in \mathbb{C}^{n_T\times 1}$ are the subchannel gain vectors imposed on user 1 and user 2, respectively. The vectors $h$ and $g$ are the sum of magnitudes of complex Gaussian random variables, so the envelopes, $\|h_k\|$ and $\|g_k\|$, $k = 1, 2, ..., n_T$, for each subchannel are Nakagami-m with different integer values of $m$, and with $\Omega_1$ and $\Omega_2$ respectively, where $\Omega_1$ and $\Omega_2$ are the average signal to noise ratio (SNR) for different subchannels of channel 1 and channel 2, respectively. $w_{1,t} \sim CN(0, \sigma_1^2)$ and $w_{2,t} \sim CN(0, \sigma_2^2)$ are the noises at the receivers of user 1 and user 2, respectively.

Fig. 1. System Model.
TABLE I

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Transmitted Message</th>
<th>Intended User</th>
<th>Eavesdropper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol 1</td>
<td>S1 only</td>
<td>User 1</td>
<td>User 2</td>
</tr>
<tr>
<td>Protocol 2</td>
<td>Both S1 and S2</td>
<td>For S1: User 1</td>
<td>For S2: User 2</td>
</tr>
</tbody>
</table>

Table 1 shows the transmission protocols. In protocol 1, we assume that transmitter communicates only with user 1 and sends the confidential message S1 in n-channel with nR1 bits and user 2 acts as an eavesdropper. In protocol 2, the transmitter sends independent confidential messages S1 and S2 in n-channel with nR1 and nR2 bits respectively. The message S1 is destined for user 1 and eavesdropped upon by user 2, whereas the message S2 is destined for user 2 and eavesdropped upon by user 1. Each channel is power limited in the sense that \( \frac{1}{n} \sum_{i=1}^{n} |x_i|^2 \leq P_T \), where \( P_T \) corresponds to the average total power limitation at the transmitter.

### III. TRANSMISSION PROTOCOL 1: SECURITY CAPACITY

When transmitter communicates only with user 1, and user 2 acts as an eavesdropper, then channel 1 and channel 2 are referred as main channel and eavesdropper’s channel, respectively. The messages S1 is encoded into the codeword \( x^n \) which is suitable to be transmitted over the Nakagami-m fading channel.

#### A. Full CSI at the Transmitter

The instantaneous secrecy capacity of Nakagami-m fading MISO channel is given by,

\[
C^{(M)}_{S_{MISO}} = \max_{R_x: R_x \geq 0, tr(R_x) \leq P_T} E \left[ \log_e \left( 1 + \frac{P h^H R_x h}{\sigma^2} \right) \right]
\]

When the main channel and eavesdropper’s channel gains are known at the transmitter, then one would expect the optimal scheme to allow for the transmission, only when the main channel is better than eavesdropper’s channel. In this case, \( RX \) can be represented in terms of the power allocation policy \( P(h, g) \) that achieves the secrecy capacity and normalized signal covariance matrix \( Q \), so that \( RX = P(h, g) Q \) satisfying \( tr(R_X) \leq P_T \) and \( tr(Q) = 1 \). Under this assumption, the ergodic secrecy capacity is given by,

\[
(\langle C^{(M)}_{S_{MISO}} \rangle)^{(F full)} = \max_{R_x: R_x \geq 0, tr(R_x) \leq P_T} E \left[ \log_e \left( 1 + \frac{P h^H R_x h}{\sigma^2} \right) \right]
\]

#### B. Only main channel CSI at the Transmitter

When only the main channel gain of legitimate receiver is known at the transmitter, then \( RX \) is given by, \( RX = P(h, g) Q \) satisfying \( tr(R_X) \leq P_T \) and \( tr(Q) = 1 \). In this case, the ergodic secrecy capacity is given by,

\[
(\langle C^{(M)}_{S_{MISO}} \rangle)^{(F full)} = \max_{Q: Q \leq 0, tr(Q) \leq 1, E[P(h, g)] \leq P_T} E \left[ \log_e \left( 1 + \frac{P h^H Q h}{\sigma^2} \right) \right]
\]

#### C. Open-Loop Spatial Multiplexing Transmission Scheme

For this scheme, it is optimal for a multiple antenna transmitter to adapt an open-loop spatial multiplexing technique to send data equally in multiple orthogonal directions. This scheme is nearly identical to the case that is used in space-time coding and thus techniques. In this scheme, the performance curve might be a lower bound to the secrecy capacity and exists only when the SNR of main channel is greater than that of eavesdropper’s channel, otherwise the secrecy capacity is zero [1]. In this case, \( RX \) can be represented in terms of \( P_T \) and \( Q \), so that \( RX = P_T Q \) and \( tr(Q) = 1 \). When the open-loop spatial multiplexing technique is applied, then, \( Q = \left( \frac{1}{\sqrt{n_T}} F \right) \left( \frac{1}{\sqrt{n_T}} F \right)^H = \frac{1}{n_T} I_{n_T} \), where \( F \) is an arbitrary \( n_T \times n_T \) unitary matrix. So, the lower bound of secrecy capacity for Nakagami-m fading MISO channel is given by,

\[
C^{(M)}_{S_{MISO}} \geq \log_e \left( 1 + \frac{P_T}{n_T \Sigma_1^2} h^H g \right) - \log_e \left( 1 + \frac{P_T}{n_T \Sigma_2^2} g^H g \right)
\]

where \( \gamma_1 > \gamma_2 \) (7)
Case 1 (Non-identically independent (non-i.i.d.) Nakagami-m): In this case, the pdfs of $\psi_1$ and $\psi_2$ are approximated by [7, eq. 10],

$$f(\psi_{1\text{ non-i.i.d}}) = \frac{M_o \psi_1^{M_o-1} \exp\left(-\frac{M_o \psi_1}{\Omega_{T1}}\right)}{\Gamma(M_o)\Omega_{T1}^{M_o}}$$

and

$$f(\psi_{2\text{ non-i.i.d}}) = \frac{D_o \psi_2^{D_o-1} \exp\left(-\frac{D_o \psi_2}{\Omega_{T2}}\right)}{\Gamma(D_o)\Omega_{T2}^{D_o}}$$

where $M_o = \left(\sum_{k=1}^{n_T} \Omega_{1k}^2\right)^2 / \sum_{k=1}^{n_T} \left(\frac{\Omega_{1k}}{M_o}\right)^2$, $D_o = \left(\sum_{k=1}^{n_T} \Omega_{2k}^2\right)^2 / \sum_{k=1}^{n_T} \left(\frac{\Omega_{2k}}{D_o}\right)^2$, $\Omega_{T1} = \sum_{k=1}^{n_T} \Omega_{1k}$ and $\Omega_{T2} = \sum_{k=1}^{n_T} \Omega_{2k}$.

Case 2 (Identically independent (i.i.d.) Nakagami-m): In this case, the pdfs of $\psi_1$ and $\psi_2$ are given by [8],

$$f(\psi_{1\text{ i.i.d}}) = \frac{\psi_1^{m_{\text{MT}}-1} \exp\left(-\frac{\psi_1}{\beta_1}\right)}{\Gamma(m_{\text{MT}})\beta_1^{m_{\text{MT}}}}$$

and

$$f(\psi_{2\text{ i.i.d}}) = \frac{\psi_2^{m_{\text{MT}}-1} \exp\left(-\frac{\psi_2}{\beta_2}\right)}{\Gamma(m_{\text{MT}})\beta_2^{m_{\text{MT}}}}$$

where $\beta_1 = \frac{\Omega_{T1}}{m_{\text{MT}}}$ and $\beta_2 = \frac{\Omega_{T2}}{m_{\text{MT}}}$. Assume that $I_1 = \log e\left(1 + \frac{\psi_1}{\beta_1}\right) = \log e\left(1 + \theta_1\psi_1\right)$ and $I_2 = \log e\left(1 + \frac{\psi_2}{\beta_2}\right) = \log e\left(1 + \theta_2\psi_2\right)$, where $\theta_1 = \frac{\Omega_{T1}}{m_{\text{MT}}}$ and $\theta_2 = \frac{\Omega_{T2}}{m_{\text{MT}}}$. $\rho_1 = \frac{\Omega_{T1}}{\beta_1}$ and $\rho_2 = \frac{\Omega_{T2}}{\beta_2}$ are the transmit signal to noise ratios (SNRs) of main channel and eavesdropper’s channel, respectively. In order to find the pdf of mutual information, we use the following preliminary result.

**Proposition 1.** Let $v \sim \chi^2_{2n}$ and the probability density function of $v$ is denoted by $f(v)$. Then the probability density function of $I = \log e\left(1 + \theta v\right)$ is given by

$$q(I) = \frac{e^I}{\theta} f\left(\frac{e^I - 1}{\theta}\right)$$

By using proposition 1, the pdfs of $I_1$ and $I_2$ are given by,

$$q(I_1) = \frac{e^{I_1}}{\theta_1} f\left(\frac{e^{I_1} - 1}{\theta_1}\right)$$

and

$$q(I_2) = \frac{e^{I_2}}{\theta_2} f\left(\frac{e^{I_2} - 1}{\theta_2}\right)$$

respectively. For non-i.i.d. case, the pdf of $I_1$ obtained from (8) and (13) is approximated by,

$$q(I_{1\text{ non-i.i.d}}) = \frac{M_o \psi_1^{M_o-1} \exp\left(-\frac{M_o \psi_1}{\Omega_{T1}}\right)}{\Gamma(M_o)\Omega_{T1}^{M_o}}$$

and from (9) and (14), the pdf of $I_2$ is approximated by,

$$q(I_{2\text{ non-i.i.d}}) = \frac{D_o \psi_2^{D_o-1} \exp\left(-\frac{D_o \psi_2}{\Omega_{T2}}\right)}{\Gamma(D_o)\Omega_{T2}^{D_o}}$$

Similarly, for i.i.d. case, the pdf of $I_1$ obtained from (10) and (13) is given by,

$$q(I_{1\text{ i.i.d}}) = \frac{\psi_1^{m_{\text{MT}}-1} \exp\left(-\frac{\psi_1}{\beta_1}\right)}{\Gamma(m_{\text{MT}})\beta_1^{m_{\text{MT}}}}$$

and from (11) and (14), the pdf of $I_2$ is given by,

$$q(I_{2\text{ i.i.d}}) = \frac{\psi_2^{m_{\text{MT}}-1} \exp\left(-\frac{\psi_2}{\beta_2}\right)}{\Gamma(m_{\text{MT}})\beta_2^{m_{\text{MT}}}}$$

We find the lower bound of ergodic secrecy capacity for the following two cases.

**Case 1 (Non-i.i.d. Nakagami-m):** In this case, the lower bound of ergodic secrecy capacity is defined as,

$$\langle CS_{\text{SMISO}}\rangle_{\text{non-i.i.d}} \geq \int_0^\infty \int_0^\infty \left\{ (I_1 - I_2) q(I_1) \right\}_{\text{non-i.i.d}} dI_1 dI_2, \quad \text{if } \gamma_1 > \gamma_2$$

and the analytical expression obtained from equations (15), (16) and (19) is given in Theorem 1, where $\phi_1 = \theta_1 \Omega_{T1}$, $\phi_2 = \theta_2 \Omega_{T2}$, $\varphi_1 = M_o - \kappa_1 - 1$ and $\varphi_2 = D_o - b_1 - 1$.

**Theorem 1:** For a non-i.i.d. Nakagami-m fading MISO channel, the lower bound of ergodic secrecy capacity in nats per symbol is given by,

$$\langle CS_{\text{SMISO}}\rangle_{\text{non-i.i.d}} \geq \sum_{\kappa_1 = 0}^{M_o - 1} \sum_{b_1 = 0}^{D_o - 1} \left\{ \left(-1\right)^{\varphi_1 - 1} e^{\frac{M_o}{\phi_1}} \right\}_{\phi_1}$$

and the analytical expression obtained from equations (17), (18) and (21) is given in Theorem 2, where $\eta_1 = \theta_1 \beta_1$, $\eta_2 = \theta_2 \beta_2$ and $\xi_1 = m_{\text{MT}} - \nu_1 - 1$.

**Theorem 2:** For an i.i.d. Nakagami-m fading MISO channel, the lower bound of ergodic secrecy capacity in nats per symbol is given by,

$$\langle CS_{\text{SMISO}}\rangle_{\text{i.i.d}} \geq \sum_{\nu_1 = 0}^{m_{\text{MT}} - 1} \sum_{\nu_2 = 0}^{D_o - 1} \left\{ \left(-1\right)^{\xi_1 - 1} e^{\frac{1}{\eta_1}} \right\}_{\eta_1}$$

and

$$+ \sum_{\nu_1 = 0}^{m_{\text{MT}} - 1} \sum_{\nu_2 = 0}^{D_o - 1} \left\{ \left(-1\right)^{\xi_2 - 1} e^{\frac{1}{\eta_2}} \right\}_{\eta_2}$$

and

$$+ \sum_{\nu_1 = 0}^{m_{\text{MT}} - 1} \sum_{\nu_2 = 0}^{m_{\text{MT}} - 1} \left\{ \left(-1\right)^{\xi_1 + \xi_2 - 1} e^{\frac{1}{\eta_1}} \right\}_{\eta_1}$$

if $\eta_1 > \eta_2$. (22)
IV. TRANSMISSION PROTOCOL 2: ACHIEVABLE SECRECY CAPACITY REGION

We assume that the transmitted messages \((s_1, s_2)\) are jointly encoded as \(x^n\), where \(x^n = [x_1, \ldots, x_n] \in \mathbb{C}^{n \ell}, s \in S_\ell\) and \(\ell \in \{1, 2\}\). So the channel consists of a transmitter with an input alphabet \(x^n \rightarrow Y^n\) and two receivers with output alphabets \(y^n_1 \rightarrow Y^n_1\) and \(y^n_2 \rightarrow Y^n_2\). At the transmitter, the encoder is assumed to be stochastic to increase the randomness of transmitted messages. In other words, the encoder is specified by the conditional pdf \(f(x^n | s_1, s_2)\) that the messages \((s_1, s_2)\) are jointly encoded as the channel input sequence \(x^n\), where \(\int f(x^n | s_1, s_2) = 1\). The codebook \((2^{nR_1}, 2^{nR_2}, n)\) consists of two message sets, \(S_1 \in \{1, \ldots, 2^{nR_1}\}\) and \(S_2 \in \{1, \ldots, 2^{nR_2}\}\), an encoder \(f: S_1 \times S_2 \rightarrow X^n\) and two decoders, one at each receiver. The decoding function \(\omega_\ell\) at \(\ell\)th user is a deterministic mapping \(\omega_\ell: Y^n_\ell \rightarrow S_\ell\) i.e. \(\omega_1: Y^n_1 \rightarrow S_1 \in \{1, \ldots, 2^{nR_1}\}\) and \(\omega_2: Y^n_2 \rightarrow S_2 \in \{1, \ldots, 2^{nR_2}\}\). The reliability is measured by the maximum error probability. At the receiver ends, the error probability for user \(\ell\) is given by,

\[
P_{e,\ell}^{(n)} = 2^{-n(R_1+R_2)} \sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \Pr[\omega_\ell(y^n_\ell) \neq s_\ell | (s_1, s_2) \text{ sent}]
\]

and the maximum error probability is defined as \(P_e^{(n)} = \max\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\}\). The secrecy levels of confidential messages \(S_1\) and \(S_2\) are measured in terms of equivocation rates, which are defined as follows.

**Definition 1:** The equivocation rates \(R_{c1}\) and \(R_{c2}\) for secure broadcast MISO channel are given by, \(R_{c1} = \frac{1}{n} H(S_1 | y^n_2)\) and \(R_{c2} = \frac{1}{n} H(S_2 | y^n_2)\).

The perfect secrecy rates \(R_1\) and \(R_2\) are the amount of information that can be sent to the destined users both reliably and confidentially.

**Definition 2:** A secrecy rate pair \((R_1, R_2)\) is said to be achievable if for any \(\varepsilon > 0, \varepsilon_1 > 0\) and \(\varepsilon_2 > 0\), there exists a sequence of \((2^{nR_1}, 2^{nR_2}, n)\), such that for sufficiently large \(n\), \(P_e^{(n)} \leq \varepsilon, R_{c1} \geq R_1 - \varepsilon_1\) and \(R_{c2} \geq R_2 - \varepsilon_2\).

In the above definition, the first condition concerns the reliability, while the other conditions guarantee perfect secrecy for each individual messages. In this paper, ours achievable coding scheme enables both joint encoding at the transmitter by using Gelfand-Pinsker binning and preserving confidentiality by using random binning. The following corollary summarizes the encoding strategy.

**Corollary 1:** Let \(V_1\) and \(V_2\) be auxiliary random variables and \(\Xi\) be the class of joint probability densities \(f(v_1, v_2, x, y_1, y_2)\) which factor as \(f(v_1, v_2)f(x|v_1, v_2)f(y_1|v_1, y_2|x)\). Let \(R_\pi(\pi)\) denote the union of all non-negative rate pairs \((R_1, R_2)\) satisfying

\[
0 \leq R_1 \leq I(V_1; Y_1) - I(V_1; Y_2|V_2) - I(V_1, V_2)
\]

and

\[
0 \leq R_2 \leq I(V_2; Y_2) - I(V_2; Y_1|V_1) - I(V_1, V_2)
\]

for a given probability density \(\pi \in \Xi\). For the general broadcast channel with confidential messages, the following region is achievable

\[
(R_1, R_2) \in \text{co}\left\{ \bigcup_{\pi \in \Xi} R_\pi(\pi) \right\}
\]

where \(\text{co}\{A\}\) is the convex hull of set \(A\).

However, when we want to construct the rate region of (23), it is not clear how to choose the auxiliary random variables \(V_1\) and \(V_2\). Here, we employ the dirty-paper coding (DPC) technique with the double-binning code structure to develop secret dirty paper coding (SDPC) achievable secrecy capacity region. First, we separate the input \(x\) into two independent random vectors \(a_1\) and \(a_2\), so that \(a_1 + a_2 = x\). Here \(a_1, a_2, v_1, v_2\) are chosen as follows:

\[
a_1 \sim CN(0, A_1), a_2 \sim CN(0, A_2), v_1 = a_1 + Ba_2, \text{ and } v_2 = a_2
\]

such that \(tr(A_1 + A_2) = tr(R_x) \leq P_T\), where \(A_1\) and \(A_2\) are the covariances of \(a_1\) and \(a_2\), respectively, and are given by, \(A_1 = \mathbb{E}[a_1 a_1^H] \geq 0\) and \(A_2 = \mathbb{E}[a_2 a_2^H] \geq 0\). The optimal value of matrix \(B\) is given by, \(B = A_1 (\sigma_I^2 + A_1)^{-1}\). Based on corollary 1 and conditions (24), we obtain a SDPC rate region with \(w_1,t \sim CN(0, 1)\) and \(w_2,t \sim CN(0, 1)\) as follows.

**Corollary 2:** Let \(R_1^{SDPC}(A_1, A_2)\) denote the union of all \((R_1, R_2)\) satisfying

\[
0 \leq R_1 \leq \log_2 \left[ 1 + h^H A_1 h \right] + g^T A_1 g
\]

and

\[
0 \leq R_2 \leq \log_2 \left[ 1 + h^T (A_1 + A_2) h \right] + g^T (A_1 + A_2) g
\]

then any rate pair

\[
(R_1, R_2) \in \text{co}\left\{ \bigcup_{tr(A_1+A_2)=tr(S) \leq P_T} R_1^{SDPC}(A_1, A_2) \right\}
\]

is achievable.

Let \(D_1 = I + \vartheta P(h, g) h h^H, M_1 = I + (1-\vartheta) P(h, g) g g^H\), \(D_2 = I + \frac{1}{1-\vartheta} P(h, g) h h^H, M_2 = I + \frac{(1-\vartheta) P(h, g) g g^H}{1-\vartheta} h h^H\), and \(\lambda_{1\max}, \lambda_{2\max}\) are the largest generalized eigenvalues of the pencils \((D_1, M_1)\) and \((D_2, M_2)\), respectively, where \(0 \leq \vartheta \leq 1\) and \(\mathbb{E}[P(h, g)] \leq P_T\). Then the following theorem characterizes the SDPC secrecy capacity region.

**Theorem 3:** Let \(C_{m}^{MISO}\) denote the secrecy capacity region under an average total power constraint \(\mathbb{E}[P(h, g)] \leq P_T\), and \(\text{co}\) be the convex hull operator, then \(C_{m}^{MISO}\) is given by

\[
C_{m}^{MISO} = \text{co}\left\{ \bigcup_{0 \leq \vartheta \leq 1} R_1^{MISO}(\vartheta) \right\}
\]

where \(R_1^{MISO}(\vartheta)\) is the set of all \((R_1, R_2)\) satisfying

\[
R_1 \leq \log_2 \lambda_{\max}^{\vartheta}, \quad \vartheta = 1, 2.
\]
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.

In this paper, we focus to define the secrecy capacity under different assumption on the available transmitter CSI for Nakagami-\(m\) fading MISO broadcast channel. Some numerical results are shown to clear the insight of derived expressions. We also develop a secret dirty-paper coding scheme and use this scheme to develop an achievable secrecy capacity region. Our result has illustrated that both users can achieve positive rates with information-theoretic secrecy through a multiple antenna broadcast channel. Therefore, it is more practical and attractive to achieve information-theoretic secrecy in wireless networks by using multiple transmit antennas at the physical layer.

\section*{ACKNOWLEDGEMENT}

This work was supported by the UK Engineering and Physical Sciences Research Council under grant number EP/G026092/1.

\section*{REFERENCES}