Media-based modulation for secrecy communications

I. Yildirim, E. Basar and G. K. Kurt

Media-based modulation (MBM) concept is exploited to increase physical layer (PHY) security in the presence of an illegitimate listener. A precoding design is developed to increase the mutual secrecy rate of MBM, and the secrecy mutual information expressions are derived. 

The provided analyses and numerical results have also shown that MBM is a perfect candidate for PHY security by providing the maximum achievable secrecy mutual information, even in the presence of channel estimation errors.

Introduction: Spatial modulation (SM), which uses antenna indices as an additional source of information, has been proposed as a promising alternative to traditional MIMO systems [1]. Media-based modulation (MBM) is a new type of digital modulation technique that creates different channel fading realisations by exploiting the ON/OFF states of the available radio frequency (RF) mirrors. MBM provides attractive benefits in terms of spectral efficiency and error performance [2, 3]. 

In order to increase the spectral efficiency, the requirement of having a high number of transmit antennas has been effectively relaxed in MBM systems based on the use of RF mirrors [4]. SM systems are also based on randomness and matchlessness of the channel. If all channels in SM are indistinguishable, corresponding data symbols cannot be recovered correctly at the receiver. Hence, physical layer (PHY) security and index modulation (IM) are fed from the same input.

Alice and Eve are represented by $\mathcal{A} = \{x_1, x_2, \ldots, x_N\}$ and $\mathcal{E} = \{e_1, e_2, \ldots, e_N\}$, respectively. When the $m$th antenna state is selected for the transmission of the $i$th symbol $x_i$, the received signals at Bob and Eve are given as

$$y_n = h_{n,i}x_i + n_n, \quad y_E = g_{n,E}x_i + n_E,$$

(1) where $n_n$ and $n_E$ are the Gaussian noise samples at the corresponding receivers. In order to satisfy the transmit power constraint, we assume $E[x_n^2] = 1$ in the following. When the antenna state is selected as $m$, transmission is performed via $h_m$, and the received signal at Bob ($y_B$) follows the complex Gaussian distribution with the conditional probability density function (PDF) expressed as

$$p(y_B|h_m, x_i) = \frac{1}{\sigma^2} \exp\left(-\frac{|y_B - h_m x_i|^2}{\sigma^2}\right).$$

(2)

With some algebraic manipulations, the mutual information of Bob can be expressed as

$$I(y_B; h, x) = I(h; y_B|x) + I(x; y_B)$$

$$= \log_2 Q^{2N_d} - \frac{1}{Q^{2N_d}} \sum_{n=1}^{2N_d} \sum_{i=1}^{Q} E_n \left[ \log_2 \left( \sum_{m=1}^{2N_d} \sum_{i=1}^{Q} \exp(\Delta_n) \right) \right]$$

(4)

where $\Delta_n = -(|d_n + q_n|^2 - |r_n|^2)/\sigma^2$ and $d_n = h_n x_i - h_{n,E} x_i$. 

Signal-to-noise ratio (SNR) is defined as $\text{SNR} = 1/\sigma^2$. If SNR goes to infinity, the upper bound of the mutual information of the Bob is obtained as $I(x; h, y_B)^{\text{UP}} = N_d + \log_2 Q$. By following the steps above, the mutual information over the Eve’s channel is obtained as

$$I(y_E; g, x) = I(g; y_E|x) + I(x; y_E)$$

$$= \log_2 Q^{2N_d} - \frac{1}{Q^{2N_d}} \sum_{n=1}^{2N_d} \sum_{i=1}^{Q} E_n \left[ \log_2 \left( \sum_{m=1}^{2N_d} \sum_{i=1}^{Q} \exp(\Delta_n) \right) \right]$$

(5)

where $\Delta_n = -(|d_n + q_n|^2 - |r_n|^2)/\sigma^2$ and $d_n = g_{n,E} x_i - g_{n,E} x_i$. 

Consequently, the secrecy mutual information is written as

$$R_S = \left[I(y_B; h, x) - I(y_E; g, x)^{\text{UP}}\right]^+.$$ 

(6)

The above expectations in (4) and (5) are performed by Monte Carlo simulation due to the difficulty in analytical expression.

Secrecy mutual information of SM–MBM: The secrecy rate analyses of SM–MBM are similar to MBM owing to their similar working principles. For this case, the sets of the transmit symbol and the channel states are represented by $X = \{x_1, x_2, \ldots, x_N\}$ and $K = \{1, 2, \ldots, N/2N_d\}$, respectively. When $m$th state is selected for the transmission of the $i$th symbol $x_i$, the received signals at Bob and Eve can be represented as in (1). Each antenna state and data symbol are selected with the same probability of $1/N/2N_d$ and $1/Q$, respectively. If the similar steps in (2)–(5) are followed, the secrecy mutual information of the SM–MBM is obtained as (6).

Fig. 1: System model of MBM and SM–MBM with active listener (Eve)

a) MBM-based system model
b) SM–MBM-based system model

System model of media-based modulation: We consider a single-input single-output wireless communication system with a legitimate transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), as shown in Fig. 1a. It is assumed that Alice is equipped with $N_d$ RF mirrors, while Bob and Eve have a single antenna. Eve is assumed to operate as an active listener. This means that CSI of the Alice–Eve link is available at Alice. The Rayleigh fading channels between Alice and Bob, and Alice and Eve are represented by $h_m$ ($m = 1, 2, \ldots, 2N_d$) and $g_n$ ($n = 1, 2, \ldots, N_d$), respectively. The noise component present in all receiver nodes is assumed to be white complex Gaussian distributed with zero mean and $\sigma^2$ variance.

A total of $n = \log_2 (Q) + N_d$ bits enter the transmitter of the MBM scheme per channel use. The first $\log_2 (Q)$ bits of the incoming bit sequence are used for ordinary $Q$-QAM, while the subsequent $N_d$ bits select the active channel state.
Precoded MBM and SM–MBM. In MBM and SM–MBM, the selection of an antenna and antenna state determines the channel to be used. In other words, after forming the data symbol, the channel over which this symbol is transmitted is specified.

One of the most effective ways to increase the secrecy mutual information is to worsen Eve’s detection performance of the transmitted symbol. Decoding of IM bits is performed by separately detecting the received signals with the classical maximum likelihood detection as considered and it would not be affected. Eve and Bob can detect the received symbol. However, the precoding and CSI are known by the legitimate receiver and the precoding still prevents Eve to decode information. Even if Alice does not have perfect CSI of the transmitter, the BER performance of Eve in the presence of imperfect CSI (I-CSI), where we assume that \( g_m \) is estimated at Alice with a Gaussian distributed error that has \( \sigma^2 \) variance, which is fixed and equals to \( \sigma^2 \). We show that even if Alice does not have perfect CSI of the Alice–Eve link, the applied precoding still prevents Eve to decode information.

As a result, the maximum value of secrecy rate for MBM and SM–MBM, when precoding is performed, is written, respectively, as

\[
R_S = I(y; g, x)^{\text{UP}} - I(y; g, x)^{\text{UP}} = N_{rf}
\]

\[
R_S = I(y; g, x)^{\text{UP}} - I(y; g, x)^{\text{UP}} = N_{rf} + \log_2 N_t
\]

Numerical studies: In this section, we provide computer simulation results for the proposed MBM and SM–MBM schemes with respect to SNR. We consider natural mapping for channel states and transmit antenna indices, while we employ Gray mapping for Q-PSK/QAM symbols.

Fig. 2 Secrecy rate with various \( N_t \) and Q values

a Secrecy mutual information of MBM

b Secrecy mutual information of SM–MBM with two transmit antennas

Fig. 2 demonstrates the secrecy mutual information for MBM and SM–MBM schemes with precoding. Computer simulation results in Fig. 2a reveal that the maximum secrecy mutual information is equal to the number of RF mirrors, i.e. 3 bits/s/Hz at 30 dB for \( N_t = 3 \). While \( N_t = 8 \) transmit antennas are used for a 3 bits/s/Hz secrecy rate in SM, the same performance is achieved by MBM with one transmitter and three RF mirrors. Fig. 2b shows the secrecy mutual information of the SM–MBM scheme with precoding. We observe that the maximum secrecy mutual information is sum of the number of RF mirrors and the logarithm of the number of transmit antennas, i.e. it reaches 4 bits/s/Hz at 30 dB for \( N_t = 2 \) and \( N_d = 3 \). The BER curves of the proposed schemes for various number of RF mirrors are shown in Fig. 3. It is shown that the proposed MBM scheme leads to a considerably high BER at Eve, while Bob can operate as usual. In Fig. 3, we also investigate the BER performance of Eve in the presence of imperfect CSI (I-CSI), where we assume that \( g_m \) is estimated at Alice with a Gaussian distributed error that has \( \sigma^2 \) variance, which is fixed and equals to \( \sigma^2 \). We show that even if Alice does not have perfect CSI of the Alice–Eve link, the applied precoding still prevents Eve to decode information.

Conclusions: In this Letter, we have investigated the schemes of MBM and SM–MBM in terms of PHY security. Assuming that transmitter has the ideal CSI of Eve and Bob, we have minimised the mutual information of eavesdropper. Even in the presence of channel estimation errors, the Eve’s mutual information has been reduced by precoding.

Acknowledgment: The work of E. Basar was supported by the TUBA-GEBIP Award Programme.

References