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 features of wireless channels. In [5, 6], it is shown that SM can also improve PHY security by carefully designing the transmission signal.

In this Letter, our motivation is to reduce the amount of information in the eavesdropper by using precoding at the transmitter side, thereby increasing the secrecy mutual information rate for MBM [2] and SM–MBM [4] schemes. Furthermore, the average bit error rate (BER) of the legitimate receiver and the eavesdropper is obtained for MBM and SM–MBM in the presence of Rayleigh fading channels. According to the obtained results, it has been shown that the maximum secrecy mutual information of SM–MBM is the sum of the logarithms of the numbers of transmit antennas and RF mirrors, while the maximum secrecy mutual information of MBM equals to the number of RF mirrors.

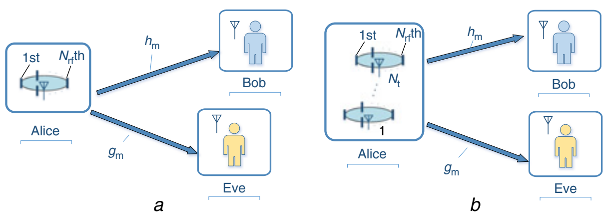

Fig. 1 *System model of MBM and SM–MBM with active listener (Eve)*
a MBM-based system model
b SM–MBM-based system model

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. 1*a*. It is assumed that Alice is equipped with a single transmit unit that has N_{rf} 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 $(m = 1, 2, \ldots, 2^{N_{\text{rf}}})$ and g_m $(m = 1, 2, \ldots, 2^{N_{\text{rf}}})$, respectively. The noise component present in all receiver nodes is assumed to be white complex Gaussian distributed with zero mean and σ^2 variance.

A total of $\eta = \log_2(Q) + N_{\text{rf}}$ 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_{rf} bits select the active channel state.

System model of SM–MBM: SM–MBM scheme is inspired from the SM and MBM schemes. We consider the wireless configuration that is shown in Fig. 1*b*. It is assumed that Alice is equipped with N_t transmit antennas that has N_{rf} RF mirrors each, while Bob and Eve have a single antenna. Fading channels between the activated antenna of Alice and Bob (Eve) are represented by h_m (g_m).

The spectral efficiency of SM–MBM is $\eta = \log_2(Q) + \log_2(N_t) + N_{\text{rf}}$ bpcu. The first $\log_2(Q)$ bits of the incoming bit sequence are used for ordinary Q-QAM, while the subsequent $\log_2(N_t)$ bits select the indices of the active transmit antennas for the transmission of the selected Q-QAM symbol. However, the last N_{rf} bits are reserved for the selection of the active channel state, which is the same for all possible activated transmit antennas of the SM–MBM scheme.

Secrecy mutual information of MBM: The sets of data symbols and the channel states are represented by $X = \{x_1, x_2, \ldots, x_Q\}$ and $K = \{1, 2, \ldots, 2^{N_{\text{rf}}}\}$, respectively. When the mth antenna state is selected for the transmission of the ith symbol x_i, the received signals at Bob and Eve are given as

$$\begin{aligned} y_{\text{B}} &= h_m x_i + n_{\text{B}}, \\ y_{\text{E}} &= g_m x_i + n_{\text{E}}, \end{aligned} \tag{1}$$

where n_{B} and n_{E} are the Gaussian noise samples at the corresponding receivers. In order to satisfy the transmit power constraint, we assume $E[|x|^2] = 1$ 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

$$p(y_{\text{B}}|h_m, x_i) = \frac{1}{\pi\sigma^2}\exp\left(-\frac{|y - h_m x_i|^2}{\sigma^2}\right), \tag{2}$$

where h_m and x_i represent possible channel realisations and data symbols, respectively. Each antenna state and data symbol are selected with the same probability of $1/2^{N_{\text{rf}}}$ and $1/Q$. Therefore, the PDF of the received signal at Bob is obtained as

$$p(y_{\text{B}}) = \frac{1}{Q2^{N_{\text{rf}}}}\sum_{m=1}^{2^{N_{\text{rf}}}}\sum_{i=1}^{Q}\frac{1}{\pi\sigma^2}\exp\left(-\frac{|y - h_m x_i|^2}{\sigma^2}\right). \tag{3}$$

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

$$\begin{aligned} I(y_{\text{B}}; h, x) &= I(h; y_{\text{B}}|x) + I(x; y_{\text{B}}) \\ &= \log_2 Q2^{N_{\text{rf}}} - \frac{1}{Q2^{N_{\text{rf}}}}\sum_{m=1}^{2^{N_{\text{rf}}}}\sum_{i=1}^{Q} E_{n_{\text{B}}}\left[\log_2 \sum_{m_2=1}^{2^{N_{\text{rf}}}}\sum_{i_2=1}^{Q}\exp(\Delta_{\text{B}})\right] \end{aligned} \tag{4}$$

where $\Delta_{\text{B}} = -(|d_{\text{B}} + n_{\text{B}}|^2 - |n_{\text{B}}|^2)/\sigma^2$ and $d_{\text{B}} = h_m x_i - h_{m_2} x_{i_2}$. 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 $I(x, h; y_{\text{B}})^{\text{UP}} = N_{\text{rf}} + \log_2 Q$. By following the steps above, the mutual information over the Eve's channel is obtained as

$$\begin{aligned} I(y_{\text{E}}; g, x) &= I(g; y_{\text{E}}|x) + I(x; y_{\text{E}}) \\ &= \log_2 Q2^{N_{\text{rf}}} - \frac{1}{Q2^{N_{\text{rf}}}}\sum_{m=1}^{2^{N_{\text{rf}}}}\sum_{i=1}^{Q} E_{n_{\text{E}}}\left[\log_2 \sum_{m_2=1}^{2^{N_{\text{rf}}}}\sum_{i_2=1}^{Q}\exp(\Delta_{\text{E}})\right] \end{aligned} \tag{5}$$

where $\Delta_{\text{E}} = -(|d_{\text{E}} + n_{\text{E}}|^2 - |n_{\text{E}}|^2)/\sigma^2$ and $d_{\text{E}} = g_m x_i - g_{m_2} x_{i_2}$. Consequently, the secrecy mutual information is written as

$$R_{\text{S}} = \left[I(y_{\text{B}}; h, x) - I(y_{\text{E}}; g, x)\right]^+. \tag{6}$$

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 $X = \{x_1, x_2, \ldots, x_Q\}$ and $K = \{1, 2, \ldots, N_t 2^{N_{rf}}\}$, respectively. When mth state is selected for the transmission of the ith 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 $1/N_t 2^{N_{rf}}$ 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).

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 used channel and the symbol. Due to this feature of IM, if the channels are not resolved correctly, the error performance at the receiver deteriorates. Since we assume that Eve is an active listener, Eve's channel state information (CSI) is available at Alice. In this case, a precoding to reduce the Euclidean distance of Eve ($|d_E|$) in Alice will diminish the mutual information of the eavesdropper. Similar to SM [5], IM systems are also based on randomness and matchlessness of the channel. If all channels in IM are indistinguishable, symbols cannot be solved correctly in the receiver. As a result, the channels for Eve can be indistinguishable with a proper precoding that will cause identical channels to Eve. When the symbol, sent over the selected mth channel realisation, is multiplied by the precoding constant ρ_m, this ensures that all wireless channels for Eve will satisfy

$$\rho_m g_m x_i = \delta x_i, \tag{7}$$

where $\rho_m = \delta / g_m$. With corresponding signal processing techniques, the transmitted symbol becomes always δx_i. Thus, the Euclidean distance of Eve is obtained as

$$d_E = \rho_m g_m x_i - \rho_m g_{m_2} x_{i_2} = 0, \tag{8}$$

where Eve cannot resolve the information carried by the index bits. However, the precoding and CSI are known by the legitimate receiver and it would not be affected. Eve and Bob can detect the received signals with the classical maximum likelihood detection as considered in [3]. It can be seen from (6), at high SNR values, the maximum value of Eve's mutual information for both MBM and SM–MBM is obtained as

$$I(y_E; g, x)^{UP} = \log_2 Q. \tag{9}$$

As a result, the maximum value of secrecy rate for MBM and SM–MBM, when precoding is performed, is written, respectively, as 1.0

$$\begin{aligned} R_S &= I(y_B; h, x)^{UP} - I(y_E; g, x)^{UP} = N_{rf} \\ R_S &= I(y_B; h, x)^{UP} - I(y_E; g, x)^{UP} = N_{rf} + \log_2 N_t. \end{aligned} \tag{10}$$

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.

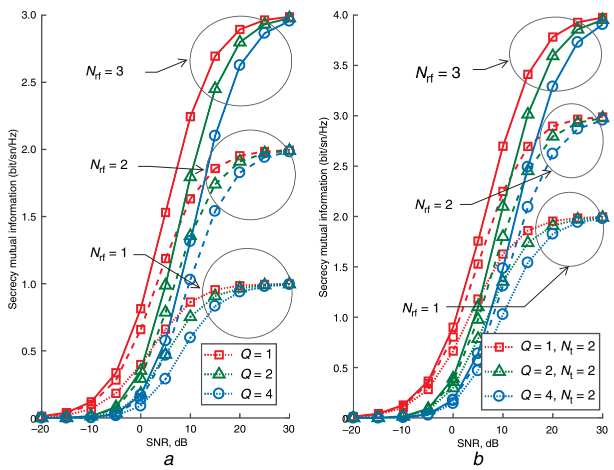

Fig. 2 *Secrecy rate with various N_{rf} and Q values*

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. 2*a* 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 $N_{rf} = 3$. 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. 2*b* 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 $N_{rf} = 3$. 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 σ_ε^2 variance, which is fixed and equals to σ^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.

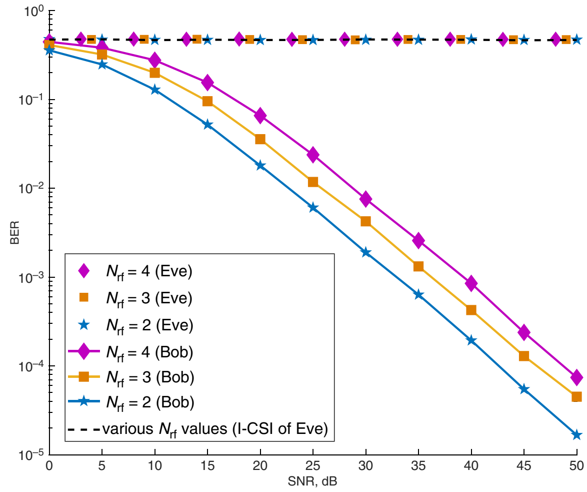

Fig. 3 *BER performance of precoded MBM employing 8-QAM with various N_{rf} values at the Bob and Eve*

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.

Submitted: *6 March 2018* E-first: *4 May 2018*
doi: 10.1049/el.2018.0764
One or more of the Figures in this Letter are available in colour online.

I. Yildirim, E. Basar and G. K. Kurt (*Faculty of Electrical and Electronics Engineering, Istanbul Technical University, 34469, Istanbul, Turkey*)

✉ E-mail: basarer@itu.edu.tr

References

1 Mesleh, R., Haas, H., Sinanovic, S., *et al.*: 'Spatial modulation', 2008, **57**, (4), pp. 2228–2241
2 Seifi, E., Atamanesh, M., and Khandani, A.K.: 'Media-based MIMO: A new frontier in wireless communication', October 2015. Available at arxiv.org/abs/1507.07556
3 Basar, E., and Altunbas, I.: 'Space-time channel modulation', *Trans. Veh. Technol.*, 2017, **66**, (8), pp. 7609–7614.
4 Naresh, Y., and Chockalingam, A.: 'On media-based modulation using RF mirrors', *Trans. Veh. Technol.*, 2017, **66**, (6), pp. 4967–4983
5 Guan, X., Cai, Y., and Yang, W.: 'On the secrecy mutual information of spatial modulation with finite alphabet'. Proc. IEEE Int. Conf. Wireless Commun. Signal Process., Huangshan, China, October 2012, pp. 1–4
6 Huang, Z., Gao, Z., and Sun, L.: 'Anti-eavesdropping scheme based on quadrature spatial modulation', *IEEE Commun. Lett.*, 2017, **21**, (3), pp. 532–535