Nested QPSK Encoding for Information Theoretic Security

Gregory T. Rendon*, Willie K. Harrison†, Marco A. C. Gomes‡, and João P. Vilela§
*Department of Electrical and Computer Engineering, University of Colorado Colorado Springs, CO, USA
†Department of Electrical and Computer Engineering, Brigham Young University, UT, USA
‡Instituto de Telecomunicações, Department of Electrical and Computer Engineering, University of Coimbra, Portugal
§CISUC and Department of Informatics Engineering, University of Coimbra, Portugal
Emails: grendon@uccs.edu, willie.harrison@byu.edu, marco@co.it.pt, jpvilela@dei.uc.pt

***Abstract*—This paper proposes a method to provide secrecy for digital communications with arbitrarily large quadrature amplitude modulation (QAM) constellations for transmission over a Gaussian fading wiretap channel. This is accomplished by breaking the constellation down into nested quadrature phase-shift keying (QPSK) symbols and randomizing the assignment between message bits and modulated symbols using channel state information (CSI). If enough random bits can be generated from CSI it becomes possible to uniquely map an arbitrary message to any symbol in the large QAM constellation. The proposed method can thereby provide perfect secrecy while maintaining high reliability by exclusively assigning minimum-distance-mapped constellations through the randomization for use by the legitimate decoder.**

I. Introduction

Development of the 5G standard and the phenomenon of the Internet of things (IoT) have received a great deal of interest among many, including those who study physical-layer security. Both of these topics demonstrate an underlying technological trend toward massively distributed, networked computing. Under this emerging computational model, securing communications at the physical-layer can enhance traditional cryptographic security. Physical-layer security is information theoretically secure rather than computationally secure, i.e., security is measured with regard to the mutual information between signals in a Markov chain rather than the resources required to defeat a system. Also, physical-layer security schemes are generally less computationally demanding, which is particularly advantageous for the low-power devices expected in IoT applications.

The seminal work by Shannon [1] presents the notion of perfect secrecy wherein an encrypted message $\mathbf{E}$ alone provides no information about the unencrypted message $\mathbf{M}$, i.e., $\mathbb{I}(\mathbf{M};\mathbf{E}) = 0$. He showed that the only way to achieve perfect secrecy is to use an encryption key that has entropy at least as high as the unencrypted message. Given the impracticality of key distribution for such a system, focus was shifted for many years into securing communications using shorter keys. In exploring this, it was noticed that the state of a fading wireless channel is randomly distributed and uncorrelated from itself beyond half a wavelength, and that this could be used to generate short random sequences for cryptographic keys [2]. Later work focused on improving the key generation rate by more efficiently extracting randomness from the channel state, specifically by optimizing the process of agreement upon random bits and the hashing of those bits into a smaller set that is completely unknown to an eavesdropper [3]–[5]. The advent of widespread multiple antenna wireless systems and particularly massive multiple-input, multiple-output (MIMO) has allowed progress due to the presence of a larger pool of channel states from which secret key bits can be drawn [6], [7]. Nonetheless, the key generation rate remains a significant hurdle impeding practical implementation.

Other research has focused on the notion, first shown by Wyner for the physically degraded wiretap channel [8], that secrecy can be achieved when the legitimate channel is better than the eavesdropper channel. Toward this end, beamforming techniques have been proposed both to maximize the signal power for a legitimate receiver and to actively degrade the signal for eavesdroppers by transmitting interference that sits in the nullspace of the legitimate receiver [9], [10]. Alternately, a degenerate constellation can be created for eavesdroppers by transmitting a QAM constellation as a sum of beamformed binary phase-shift keying (BPSK) signals [11], [12]. This approach has the added advantage that it requires less power for a given constellation since non-linear amplifiers can be used.

The above techniques depend on the assumption that there are more antennas available for transmission and jamming than for eavesdropping. If this is not so, then the eavesdropper is able to resolve the signal from each antenna [13], [14] and remove the jamming signals or properly reconstruct the constellation.

One way for a legitimate receiver to gain an advantage over an unknown eavesdropper is to create greater uncertainty on the assignment from message to broadcast symbol at the eavesdropper's receiver. Schemes such as original symbol phase rotation (OSPR) have been proposed that use CSI to drive randomization of this assignment through choices on antenna and/or phase assignments [15]. However, for each of these there

This work was partially funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1460085), the FLAD project INCISE (Interference and Coding for Secrecy), project SWING2 (PTDC/EEI-TEL/3684/2014), funded by Fundos Europeus Estruturais e de Investimento (FEEI) through Programa Operacional Competitividade e Internacionalização - COMPETE 2020 and by National Funds from FCT - Fundação para a Ciência e a Tecnologia, through projects POCI-01-0145-FEDER-016753 and UID/EEA/50008/2013.

is a trade-off. For the former, there is a reduction in the maximum constellation size that can be transmitted as antennas are reassigned as jamming transmitters. For the latter, the reliability between legitimate users is reduced because minimum distance assignments cannot be maintained as individual QPSK sub-constellations are rotated. One instance of this is illustrated in Fig. 1 where a rotation of $\pi/2$ in each quadrant of the constellation mapping causes a third of all adjacencies to have a Hamming distance of three.

In this paper, a novel scheme called mirror-mapped encoding is proposed that uses CSI to randomize the assignment of message bits to sets of contemporaneously transmitted QPSK symbols in such a way that assignments into the generated QAM constellation are minimum distance and distributed according to the CSI. As such, a party with the relevant CSI is able to work within a minimum-distance-mapped QAM constellation and one without it can only guess among all minimum distance mappings of a given size. It will be shown that this prevents the eavesdropper from gaining any information about the transmitted message.

The remainder of the paper is organized as follows. In Section II, a system model, variable definitions, and metrics are discussed, while Section III presents the mirror-encoded mapping scheme. Section IV consists of analysis to verify the validity of the scheme, and Section V concludes the paper.

II. Model and Metrics

Throughout this work, random variables are denoted as capital letters, while their alphabets are denoted with calligraphic capital letters. Vectors of random variables are represented as boldface capital letters, and the ith element of $\mathbf{X}$ is given as $\mathbf{X}[i]$, with indexing beginning at $i = 1$. Finally, an estimate of a random variable X is denoted $\hat{X}$. Alice wants to transmit an n-bit message $\mathbf{M} \in \mathbb{F}_2^n = \mathcal{M}$ to Bob. She broadcasts a symbol X to Bob over a Gaussian fading channel and Eve intercepts the transmission as in Fig. 2. The mutual channel between Alice and Bob has parameters H_b and N_b, with H_b being the zero-mean, normally distributed complex channel state that describes the gain and phase shift applied to the symbol through the channel, and N_b being the zero-mean, normally distributed complex noise present at Bob. Thus, Bob receives $Y = H_b X + N_b$. Eve's mutual channel with Alice has parameters H_e and N_e so she receives $Z = H_e X + N_e$. For convenience, it is assumed that over each mutual channel, both Alice and the receiving party have perfect knowledge of the channel state. It is additionally assumed that the parameters for Bob's and Eve's mutual channels with Alice are not correlated, so Bob does not know Eve's channel state and vice versa.

Bob makes a maximum likelihood (ML) estimation

$$\hat{X} = X \in \mathcal{X} \;\Big|\; |X - Y| = \min_{x \in \mathcal{X}} |x - Y|, \tag{1}$$

from which he maps to $\hat{\mathbf{M}} \in \mathcal{M}$, forming an estimation of the original message. Since Eve's presence and capabilities are unknown it must be assumed that she can perfectly estimate X from Z and extract all mutual information between X and $\mathbf{M}$. This assumption may seem problematic, but it will be shown that the proposed scheme guarantees that $\mathbb{I}(\mathbf{M}; X) = 0$.

A. Metrics

In discussing the reliability provided over the model in Fig. 2 for communications between Alice and Bob, it is necessary to have some metric for the similarity between elements in $\mathcal{M}$ as well as a metric for the distance between constellation symbols of $\mathcal{X}$ in the complex plane.

For an arbitrary pair of binary vectors $\mathbf{M}_a$ and $\mathbf{M}_b$, the Hamming distance $|\mathbf{M}_a - \mathbf{M}_b|$ is the number of bit positions where the two vectors differ in value.

A Gaussian integer, e.g. X, is a complex valued number for which the real and imaginary components are integers. The Euclidean distance between Gaussian integers X_a and X_b is defined as

$$|X_a - X_b| = \sqrt{\Re\mathrm{e}\{X_a - X_b\}^2 + \Im\mathrm{m}\{X_a - X_b\}^2}. \tag{2}$$

The mapping from a binary vector to an element from a set of Gaussian integers, e.g. a QAM constellation, maintains minimum distance if an arbitrary pair of binary vectors $\mathbf{M}_a$, $\mathbf{M}_b$ with $|\mathbf{M}_a - \mathbf{M}_b| = 1$ map to some pair of Gaussian integers X_a, X_b with minimum Euclidean distance for the set if and only if their Hamming distance is 1. That is, for a minimum distance mapping,

$$|\mathbf{M}_a - \mathbf{M}_b| = 1 \Leftrightarrow |X_a - X_b| = \min_{a \neq c} |X_a - X_c|. \tag{3}$$

The mutual information between a binary vector $\mathbf{M}$ and a Gaussian integer X is calculated as

$$\begin{aligned} \mathbb{I}(\mathbf{M}, X) &= \mathbb{H}(\mathbf{M}) - \mathbb{H}(\mathbf{M}|X) \\ &= \sum_{m \in \mathcal{M}} \Pr(m) \sum_{x \in \mathcal{X}} \Pr(x|m) \log_2 \frac{\Pr(x|m)}{\Pr(x)}. \end{aligned} \tag{4}$$

The reliability of the proposed scheme will be verified through simulation and quantified using the probability of bit error P_b. For n_t transmissions of n-bit messages P_b can be calculated by averaging the Hamming distances between each message and the estimate of that message

$$P_b = \frac{1}{n_t} \sum_{i=1}^{n_t} \left| \mathbf{M}_{n_i} - \hat{\mathbf{M}}_{n_i} \right|. \tag{5}$$

III. Mirror-Mapped Encoding

The goal of the proposed scheme is to simultaneously achieve both perfect secrecy and minimize P_b across all possible mappings from $\mathcal{M}$ to $\mathcal{X}$. Given a minimum distance mapped constellation built up from QPSK symbols, CSI is used to permute the constellation while maintaining minimum distance mapping. The set of unique permutations available is as large as the set of symbols in the constellation, resulting in a permutation space as large as the message space and, thus, allowing us to achieve both reliability and perfect secrecy.

To begin, a method of assigning binary vectors into a Gray coded constellation using QPSK symbols is developed by exploring the case of a 16-QAM constellation. Subsequently, a means of altering this method using CSI to provide the requisite permutations for perfect secrecy is presented.

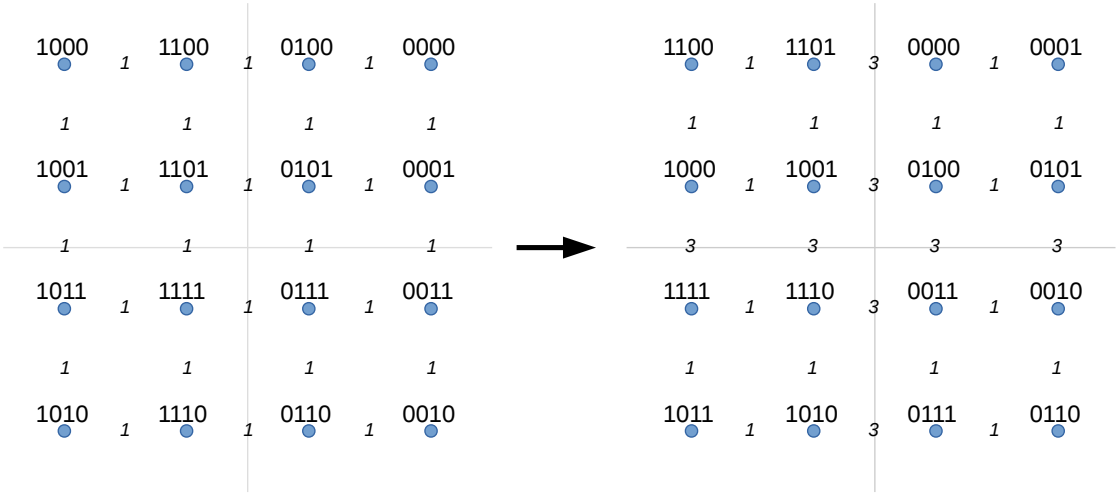

Fig. 1. A Gray coded 16-QAM constellation generated from two QPSK signals (left). Rotating the smaller QPSK constellation by $\pi/2$, the message assignments in each quadrant are shifted counter-clockwise by one symbol (right). This assigns messages of Hamming distance three adjacently across axis boundaries.

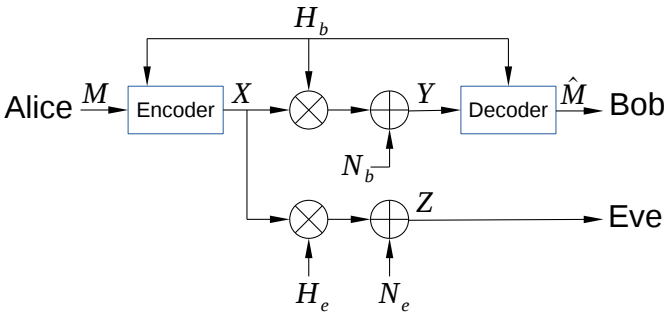

Fig. 2. Gaussian fading broadcast channel with known CSI.

A. Mapping Messages into the Default Symbol Space

Consider the left constellation in Fig. 1 and assume the scale is such that 0000 sits at $3+j3$ and 1111 sits at $-1-j$. By superposition, any symbol X in the constellation can be represented by two QPSK symbols as $X = 2^1(\pm 1 \pm j) + 2^0(\pm 1 \pm j)$. For example, the QAM symbol for 0000 can be created as $X_{0000} = 3+j3 = 2^1(1+j)+2^0(1+j)$ where the larger QPSK symbol pushes 0000 into the first quadrant at $2+j2$, and the smaller symbol increases the magnitude to $3+j3$. In general, the larger QPSK constellation describes the quadrant where the QAM symbol resides and the smaller QPSK constellation describes the position of the QAM symbol within that quadrant.

Again observing the left constellation in Fig. 1, define that each message vector is indexed from left to right. Given this, there are three important patterns to notice regarding the Gray mapping.

- The values of $\mathbf{M}[1]$ and $\mathbf{M}[2]$ are consistent for a given location on the real axis, and the values of $\mathbf{M}[3]$ and $\mathbf{M}[4]$ are consistent for a given location on the imaginary axis. From this we propose that $\mathbf{M}[1]$ and $\mathbf{M}[2]$ describe the real value of the symbol, $\mathbf{M}[3]$ and $\mathbf{M}[4]$ describe the imaginary value of the symbol.
- A 1 in $\mathbf{M}[1]$ or $\mathbf{M}[3]$ accompanies symbols with a negative value on the real or imaginary axis, respectively, and a 0 accompanies positive values. Thus, $\mathbf{M}[1]$ and $\mathbf{M}[3]$ describe the quadrant where the symbol resides.
- A 1 in $\mathbf{M}[2]$ or $\mathbf{M}[4]$ accompanies symbols with a magnitude of 1 in the real or imaginary axis, respectively, and a 0 accompanies a magnitude of 3. Thus, $\mathbf{M}[2]$ and $\mathbf{M}[4]$ describe the magnitude of the symbol.

Clearly, $\mathbf{M}[1]$ and $\mathbf{M}[3]$ describe the larger QPSK symbol. For a 16-QAM symbol composed of two QPSK symbols $X = X^{(1)} + X^{(2)}$, the larger symbol can be directly described as

$$X^{(1)} = 2^1 \left[(-1)^{\mathbf{M}[1]} + j(-1)^{\mathbf{M}[3]}\right]; \tag{6}$$

however, $\mathbf{M}[2]$ and $\mathbf{M}[4]$ do not directly describe the smaller symbol $X^{(2)}$. Instead $X^{(2)}$ is described by the sum of $\mathbf{M}[2]$ and $\mathbf{M}[4]$ with $\mathbf{M}[1]$ and $\mathbf{M}[3]$, respectively,

$$X^{(2)} = 2^0 \left[(-1)^{\mathbf{M}[1]+\mathbf{M}[2]} + j(-1)^{\mathbf{M}[3]+\mathbf{M}[4]}\right]. \tag{7}$$

Extending this analysis, it is possible to describe the mapping for any n-bit vector $\mathbf{M}$ to a symbol X in a square 2^n-QAM Gray mapped constellation (i.e. n is even) as a sum of $n/2$ QPSK symbols

$$X = \sum_{i=1}^{n/2} X^{(i)}, \tag{8}$$

where the value of the ith QPSK symbol is a function of all the preceding symbol values and consequently

$$X^{(i)} = 2^{n/2-i}\left[(-1)^{p_1} + j(-1)^{p_2}\right] \tag{9}$$
$$p_1 := \sum_{k=1}^{i} \mathbf{M}[k], \quad p_2 := \sum_{k=1}^{i} \mathbf{M}\left[\frac{n}{2}+k\right].$$

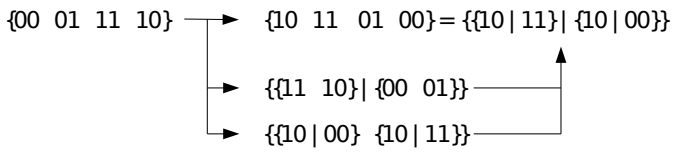

Fig. 3. Rearranging the elements of a Gray-code sequence by mirroring the arrangement of subsequences. The bars denote the axis around which a subsequence has been mirrored.

B. Mapping Messages into the Symbol Space Using CSI

The above framework will now be extended to utilize CSI to permute the mapping from message to symbol, while maintaining minimum distance.

Consider a two bit Gray coded sequence. Clearly, minimum distance will be maintained between adjacent elements if the sequence is reversed. Additionally, as can be seen in Fig. 3, if the sequence is divided in half and the order of the halves is reversed or the order of the elements in each half is reversed, minimum distance is maintained in the resulting sequence. If the order of the halves, and the order of the elements in each half are reversed, the result is the reverse of the original sequence.

For any n-bit Gray coded sequence that is recursively divided evenly into two subsets, any element order reversal that is consistently applied to all subsets of a given size results in a sequence that maintains minimum distance between adjacent elements. If the order of all subsets are reversed, the result is the same as reversing the order of the original set.

Notice from Fig. 1 that in a 16-QAM constellation, the first two message bits reproduce the reversed sequence moving from left to right in the constellation and the last two message bits reproduce this sequence moving from top to bottom in the constellation. With a short intuitive leap it can be observed that reversing the order of the halves in the two bit sequence corresponds to reversing the sign of the real or imaginary part of the larger QPSK symbol and reversing the order of the elements in each half corresponds to reversing the sign of the smaller QPSK symbol.

Recall that it is assumed the two parties, Alice and Bob, with a mutual channel have perfect knowledge of the CSI for that channel, i.e., H_b, and all other parties have no knowledge of that CSI, but rather the CSI of their own mutual channel with Alice. Since the CSI is assumed zero-mean, normally distributed, its phase is a continuous, uniformly distributed random variable. Thus an arbitrarily long binary vector $\mathbf{C}$ can be used to describe the phase of the CSI by assigning values of $\mathbf{C}$ evenly into the range $[0, 2\pi)$ and each bit in this vector will be independent and uniformly distributed. For convenience it is defined that $\mathbf{C}$ contains n-bits, the same as the message $\mathbf{M}$.

The assignments for each QPSK constellation can then be mirrored using one bit of channel state information for each axis, where each bit determines whether the corresponding axis is mirrored. To do this (9) is modified to

$$X^{(i)} = 2^{n/2-i}\left[(-1)^{p_1+\mathbf{C}[i]} + j(-1)^{p_2+\mathbf{C}[n/2+i]}\right]. \quad (10)$$

IV. Analysis

The scheme for mapping has been described but it remains to be proven that the scheme provides minimum distance mapping for all permutations of the mapping into a 2^n-QAM constellation that would result from $\mathbf{C}$. Once this is proven it will be shown through simulation that this scheme provides better reliability than a method that does not ensure minimum distance mappings. We will then proceed to prove that the mutual information through the mapping from binary message to QAM symbol is zero and thus the scheme provides perfect secrecy. Finally, we will verify through simulation-based estimates of $\mathbb{I}(\mathbf{M}, \hat{\mathbf{M}})$ that the mutual information through a Gaussian fading channel between message $\mathbf{M}$ and estimate $\hat{\mathbf{M}}$ is zero for an eavesdropping party.

A. Minimum Distance

The minimum Euclidean distance of a 2^n-QAM constellation is found between symbols that are horizontally or vertically adjacent, i.e. their values differ in only the real or only the imaginary component. Thus, to ensure all adjacent symbols have minimum distance messages mapped to them it is sufficient to show equivalent vectors will be mapped to the same value along a given axis and that it is impossible for binary vectors with Hamming distance greater than 1 to have minimum Euclidean distance mapping along a given axis.

Define $\mathbf{A}$, $\mathbf{B}$ as n-bit vectors mapped to symbols X_a, X_b using n-bit CSI vector $\mathbf{C}$. For convenience, define $m = n/2$. The change in Euclidean distance of the mappings on the real axis contributed by the ith bits can be determined from (10) as

$$(X_a - X_b)_i = 2^{m-i}(-1)^{\mathbf{C}[i]} \times \left[(-1)^{\sum_{k=1}^{i}\mathbf{A}[k]} - (-1)^{\sum_{k=1}^{i}\mathbf{B}[k]}\right]. \quad (11)$$

Note that the summations can be thought of as parity checks on the first i bits of each message, and the subtraction as a comparison of parity between the two messages over those bits. The channel state bit $\mathbf{C}[i]$ does not affect the magnitude of the change in distance, only whether the change to the distance is positive or negative.

Begin by considering the case $\mathbf{A} = \mathbf{B}$. For each i, the first i bits in $\mathbf{A}$ and $\mathbf{B}$ are identical and have the same parity. The result is a zero inside the brackets in (11) and the distance in symbol assignment is zero as expected. Summing the results for all i yields the Hamming distance, $|X_a - X_b| = 2^{m-1}(-1)^{\mathbf{C}[1]}[\mathbf{0}] + \cdots + 2(-1)^{\mathbf{C}[n-1]}[\mathbf{0}] + 1(-1)^{\mathbf{C}[n]}[\mathbf{0}] = 0$, i.e., the vectors are mapped to the same symbol.

Now take the case $\mathbf{A} \neq \mathbf{B}$. Examine the first i for which the ith bit in $\mathbf{A}$ and $\mathbf{B}$ differ. The first i bits in $\mathbf{A}$ and $\mathbf{B}$ have opposite parity and the value inside the bracket becomes either +2 or -2. This results in a change in distance (from zero) of 2^{n-i+1}. At this point we remind ourselves that given a positive common ratio, a geometric series is less than the next element in the sequence, i.e., $2^m > \sum_{k=1}^{m-1} 2^k$ for $m > 1$. Thus, once the distance between X_a and X_b leaves a value it cannot return to or cross that value. The only way to acquire minimum distance

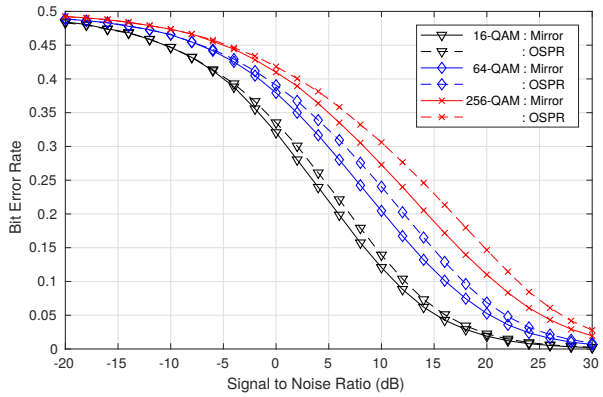

Fig. 4. Comparison of the bit error rate as a function of SNR over a Gaussian fading channel for 16, 64, and 256 QAM transmissions using mirror-mapped encoding and using OSPR encoding.

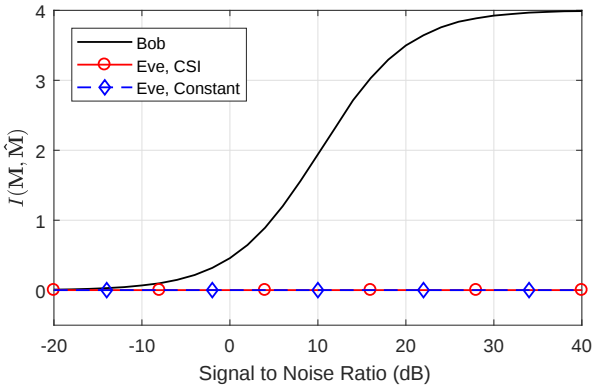

Fig. 5. Mutual information between $\mathbf{M}$ and $\hat{\mathbf{M}}$ of a 16-QAM broadcast over a Gaussian fading channel for Bob using the same CSI as Alice, Eve using uncorrelated CSI, and Eve using a static constellation

is for all further parity comparisons to push the distance back toward zero,

$$|X_a - X_b| = 2^{m-1}(0) + \cdots + 2^{m-i}(\pm 2) + 2^{m-(i+1)}(\mp 2) + \cdots + 2^0(\mp 2) = 2.$$

This requires all further parity checks to be unequal. For subsequent i, $\mathbf{A}[i] \neq \mathbf{B}[i]$ causes the first i bits in either $\mathbf{A}$ or $\mathbf{B}$ to switch parity, resulting in an equivalent parity check. The remaining bits in $\mathbf{A}$ and $\mathbf{B}$ must be equivalent. Thus, to have minimum distance assignments, $\mathbf{A}$ and $\mathbf{B}$ can only differ by one bit.

Further, after $\mathbf{A}$ and $\mathbf{B}$ have diverged, all subsequent parity checks must have the opposite result so, ignoring $\mathbf{C}$, both $\mathbf{A}$ and $\mathbf{B}$ must flip parity and then keep that parity. The next bit of both $\mathbf{A}$ and $\mathbf{B}$ must have value 1 and all further bits must have value 0. However, $\mathbf{C}$ can flip the result of each parity comparison, so the remaining bits of $\mathbf{A}$ and $\mathbf{B}$ must be $(10\cdots0) \oplus \mathbf{C}$, yielding

$$\mathbf{A} = \{A_1, \cdots, A_i, \bar{C}_{i+1}, C_{i+2}, \cdots, C_n\},$$
$$\mathbf{B} = \{A_1, \cdots, \bar{A}_i, \bar{C}_{i+1}, C_{i+2}, \cdots, C_n\}.$$

B. Reliability

To evaluate the reliability of our scheme, we simulate a Gaussian fading channel and calculate the bit error rate (BER) using (5) over ten-thousand transmissions. Each bit is randomly generated since it is assumed that the message has been encrypted and encoded. This is done for message lengths of four, six and eight bits. The results are presented in Fig. 4 for our scheme (mirror-mapped encoding) as well as for OSPR. Both schemes have BER that approaches zero as signal-to-noise ratio (SNR) increases, but mirror-mapped encoding has lower BER for all SNR. For small constellations such as 16-QAM the advantage is minimal; however, as the constellation size increases so does the reliability gain of our scheme over OSPR.

C. Perfect Secrecy

To prove that this scheme provides perfect secrecy what is shown is that given $\mathbf{M}$, each value X in the QAM constellation $\mathcal{X}$ is assigned using (10) with a unique CSI value $\mathbf{C}$. If this is true and $\mathbf{C}$ is uniformly distributed then $\mathbf{M}$ is mapped to each symbol in the constellation with equal probability. Consequently, $\mathbb{H}(X) = \mathbb{H}(X|\mathbf{M})$ and by (4) the mutual information between $\mathbf{M}$ and X is zero.

Define $\mathbf{C_x}$ as the binary vector that is used to map $\mathbf{M}$ to X using (8). Define $\mathbf{M}_{sum}$ as a vector containing the p_1 for each k followed by the p_2 for each k, i.e., the cumulative sums of each half of $\mathbf{M}$. For example, $\mathbf{M} = 1111 \Leftrightarrow \mathbf{M}_{sum} = 1212$. Then clearly, each constellation element X can result from (10) by defining $\mathbf{C} = \mathbf{C_x} \oplus (\mathbf{M}_{sum} \bmod 2)$. Since the sets $\mathcal{X}$ and $\mathcal{C}$ are the same size, and each X can be mapped from any $\mathbf{M}$ using some C, there must be a one-to-one correspondence between $\mathcal{C}$ and $\mathcal{X}$ through the mapping, and $\mathbf{C}$ uniquely maps $\mathbf{M}$ to X.

D. Mutual Information over Gaussian Fading Channel

To supply some evidence of perfect secrecy through simulation of mirror-mapped 16-QAM broadcasts over a Gaussian fading channel, the mutual information between $\mathbf{M}$ and $\hat{\mathbf{M}}$ is experimentally estimated. The distribution on $\hat{\mathbf{M}}$ is determined through Monte Carlo simulation for each message M. The mutual information is then calculated using (4). The results can be seen in Fig. 5 for the legitimate receiver Bob, for eavesdropper Eve using the CSI from her mutual channel with Alice, and for Eve using the default Gray coded constellation.

The mutual information through the channel for Bob is a function of the SNR of the channel. As SNR becomes large, the mutual information asymptotically approaches the information in the message. Conversely, for Eve the mutual information through the channel is near zero regardless of the SNR. The experiment corroborates the analytical result that perfect secrecy is achieved using mirror mapping.

V. Conclusion

In this paper the technique of mirror-mapped encoding is presented that assigns binary messages to locations in a QAM constellation using CSI and that provides optimal reliability and perfect secrecy. It is shown through simulation that the proposed scheme provides better reliability than a similar scheme (OSPR) that can provide perfect secrecy but does not guarantee minimum distance mapping. The gains in reliability increase with QAM constellation size. It is additionally shown through simulation that the amount of information received per broadcast symbol for a legitimate receiver is a function of the SNR of the channel and zero for eavesdroppers.

Given a sufficiently large set of QPSK transmitters it is possible to transmit any symbol from an arbitrarily large QAM constellation. It is also possible to assign binary message vectors into a QAM constellation in such a way that minimum distance mapping holds for all symbols. In this paper it is proven that using a random binary vector, generated in this case from the state of Alice and Bob's mutual channel, of equal length to a binary message vector, it is possible, using (8) and (10), to uniquely assign an arbitrary message to any symbol in the constellation while maintaining minimum distance mapping for all assignments into the constellation. As such, it is possible to broadcast a message over a Gaussian fading channel with optimal reliability and perfect secrecy.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[3] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[4] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, 2011.

[5] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2011, pp. 1422–1430.

[6] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. IEEE 3rd Eur. Conf. Antennas Propagation (EuCAP)*, 2009, pp. 1499–1503.

[7] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2010, pp. 1–9.

[8] A. D. Wyner, "The wire-tap channel," *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[9] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[10] G. Anjos, D. Castanheira, A. Silva, and A. Gameiro, "Exploiting reciprocal channel estimations for jamming to secure wireless communications," in *Proc. IEEE Wireless Days*, 2017, pp. 136–142.

[11] P. Montezuma, V. Astucia, R. Dinis, and M. Beko, "On the use of multiple amplifiers and antennas for efficient directive transmission with large constellations," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, 2013, pp. 1597–1603.

[12] P. Montezuma and R. Dinis, "Implementing physical layer security using transmitters with constellation shaping," in *Proc. IEEE 24th Int. Conf. Comput. Commun. Networks (ICCCN)*, 2015, pp. 1–4.

[13] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 186–195, 2014.

[14] T.-Y. Liu, P. Mukherjee, S. Ulukus, S.-C. Lin, and Y.-W. P. Hong, "Secure degrees of freedom of MIMO Rayleigh block fading wiretap channels with no CSI anywhere," *IEEE Trans. Wireless Commun,*, vol. 14, no. 5, pp. 2655–2669, 2015.

[15] B. Chen, C. Zhu, W. Li, J. Wei, V. C. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.