Irregular Quadrature Amplitude Modulation for Adaptive Physical-Layer Security

Hunter Searle*, Marco A. C. Gomes†, João P. Vilela‡, and Willie K. Harrison*
*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: huntersearle@byu.edu, marco@co.it.pt, jpvilela@dei.uc.pt, willie.harrison@byu.edu

***Abstract*—We propose adding an irregular quadrature amplitude modulation (QAM) constellation to a wireless transmission scheme in order to obtain greater control over the signal-to-noise ratio (SNR) required to successfully decode the signal. By altering the separation between adjacent symbols, the minimum required SNR is raised without degradation in the performance of the scheme. This allows the system to adapt to preferable channel conditions for the authorized user, making it harder for eavesdroppers to intercept and decode the transmission, thus making the communication safer. In addition, we show that by overlaying a coset code onto the QAM constellation, a new, stronger security gap metric can be further improved. Results show the effectiveness of this strategy with an interleaved coding for secrecy with a hidden key (ICSHK) scheme.**

***Index Terms*—quadrature amplitude modulation, physical-layer security, security gap, coset coding**

I. Introduction

One of the greatest issues facing wireless communication in today's increasingly connected world is security. With the advent of the Internet of Things (IoT) [1], [2], more devices are communicating sensitive information, including health and financial data. Many of these devices are power constrained, rendering heavy encryption untenable. Instead, we must look to less power-intensive methods to secure this data [3], [4]. Physical-layer security techniques [5], [6], [7] form one potential solution, as they can guarantee security with less computation than typical encryption [8]. Current attempts to adapt practical schemes for physical-layer security include techniques rooted in cooperative jamming [9], [10], link scheduling [11], smart sub-carrier selection of an orthogonal frequency division multiplexing (OFDM) waveform [12], and smart selection from a bank of available codes and code rates [13].

One class of schemes has been designed to exploit differences in signal quality between authorized users and eavesdroppers to ensure secrecy. While effective, these schemes are based on fixed values for signal quality, and cannot adapt to changing conditions. In this paper, we propose an irregular quadrature amplitude modulation (QAM) digital modulation scheme as a way to introduce greater control over the minimum allowable signal-to-noise ratio (SNR) for an authorized user and the maximum allowable SNR for an eavesdropper. By dynamically changing the spacing on this irregular constellation in response to differing levels of signal quality, the system is able to maintain guarantees of reliability for an authorized user while also protecting against a wider range of possible eavesdroppers. We consider this adaptive modulation technique in connection with the interleaved coding for secrecy with a hidden key (ICSHK) practical physical-layer security coding scheme from [14] as a use case. Finally, we examine the value of overlaying a coset coding scheme onto the irregular QAM constellation for greater security at a reduced transmission rate. The rest of the paper is organized as follows. First, we describe our system model, our security metrics, and the ICSHK scheme in Section II. We then present the method of utilizing irregular QAM to increase the minimum required SNR for an authorized receiver in Section III. Section IV discusses how to overlay a coset code onto the QAM constellation and presents the results. Finally, Section V offers conclusions of the work.

This work was partially funded by the following entities and projects: the US National Science Foundation (Grant Award Number 1761280), 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, PES3N (2018-SAICT-45-2017-POCI-01- 0145-FEDER-030629), and UID/EEA/50008/2019.

II. Model

A. System Model

For this paper, we use the model presented in Fig. 1. The system consists of three entities, each with a different role: Alice, Bob, and Eve. Alice begins with the length k message M^k, which she wishes to transmit reliably to Bob without Eve being able to also receive the message. To achieve this, she processes the message using three blocks. The first is an encoder that outputs the length n codeword X^n. This is fed into a buffer that breaks X^n into coded segments, denoted as $M_e^{k'}$. These are individually sent through a block that encodes the coded segments and maps them to a modulation scheme. The modulated symbols, denoted $X_m^{n'}$, are sent through two independent additive white Gaussian noise (AWGN) channels, arriving at Bob's receiver as $Y_m^{n'}$ and at Eve's receiver as $Z_m^{n'}$. These signals are demodulated into $\hat{M}_e^{k'}$ and $\tilde{M}_e^{k'}$, buffered

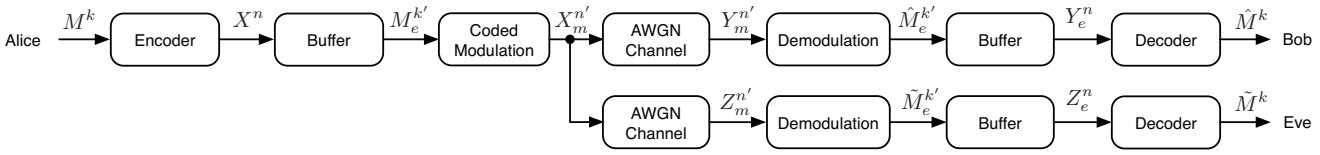

Fig. 1. Block diagram of wireless communication system model, showing the signal path between Alice and both Bob and Eve.

into Y_e^n and Z_e^n, then decoded into $\hat{M}^k$ and $\tilde{M}^k$, which represent Bob's and Eve's estimate of the message, respectively. The overall rate of the transmission R_t, is the product of the rates of the encoder R_e, and the coded modulation R_m, so that

$$\begin{aligned} R_t &= R_e \times R_m \\ &= \frac{k}{n} \times \frac{k'}{n'}. \end{aligned} \tag{1}$$

B. Metrics

Alice and Bob are successful if two conditions hold. The first is that Bob reliably receives the communication, meaning that there is very low probability of error in his received version of the message, $\hat{M}^k$. In this paper, we measure reliability using the bit-error rate (BER), $\hat{P}_b$ which is equal to

$$\hat{P}_b = \Pr(M \neq \hat{M}), \tag{2}$$

calculated at the bit level. In this paper, without loss of generality, we consider the system reliable of Bob's BER is less than 10^{-4}, or 1 error in 10,000 bits. The results hold for other thresholds.

The second condition that must hold is security against Eve, meaning that, with very high probability, Eve is unable to extract any information from $\tilde{M}^k$. We measure this using the bit error rate-cumulative distribution function (BER-CDF) first proposed in [15]. Instead of being a simple average, like the BER, the BER-CDF takes into account the full distribution of possible error values. For a given δ, the BER-CDF measures

$$\Pr(\hat{P}_b > 0.5 - \delta) \tag{3}$$

at a given SNR value. For the purpose of this paper, and without loss of generality, we will fix δ at 0.05 and consider a message secure if the BER-CDF is greater than 0.99.

The SNR above which the BER drops below 10^{-4} is called $\text{SNR}_{B,min}$, and the SNR below which the BER-CDF is above 0.99 is $\text{SNR}_{E,max}$. The difference between these two points in dB is called the security gap S_g. Note that this is different from the security gap in [16], which uses BER for both reliability and security. We would like to minimize the security gap, thus reducing the necessary advantage. However, we would also like the freedom to adjust $\text{SNR}_{B,min}$ to adapt to the instantaneous conditions of Bob's channel.

C. Transmission Scheme

The system model in Fig. 1 is a general model. Our analysis uses the ICSHK scheme presented in [15]. An overview of the scheme is illustrated in Fig. 2. The input is a length k message, M^k. The message is interleaved according to a random key K, producing the interleaved message M_i. K is then appended to M_i and this combination is encoded using a systematic inner code C_i. We use an low-density parity-check (LDPC) code [17]. This generates parity bits, P_b. After encoding, K is removed from the message, and only $X^n = \begin{bmatrix} M_i & P_b \end{bmatrix}$ is sent to the modulator. The modulated signal $X_m^{n'}$ is then transmitted through the channel. $Y_m^{n'}$ is received at the decoder. This is processed by a soft demodulator to output Y_e^n. A soft decoder for C_i extracts an estimate of the key $\dot{K}$, which is used to deinterleave the estimate of the interleaved message $\dot{M}_\text{i}$ to output the decoded message $\hat{M}^k$. It is assumed that Eve does something similar to produce her estimate, $\tilde{M}^k$.

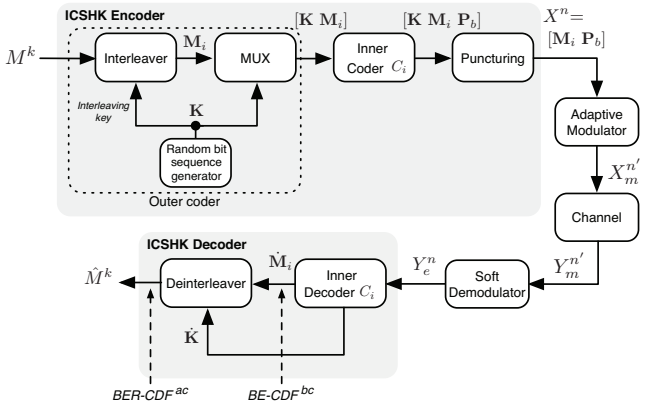

Fig. 2. Block diagram of interleaved coding for secrecy with a hidden key wireless transmission scheme.

III. Irregular QAM Constellation

While a transmission scheme might achieve a narrow security gap at its nominal level, as conditions improve, any security guarantees are lost. It is often impossible to measure Eve's SNR, and so we would like to adjust $\text{SNR}_{B,min}$ to the highest possible value to ensure security against the widest range of SNR values for Eve. We achieve this by adopting an adaptive modulation scheme called *irregular QAM*, which offers us greater control over the SNR required to decode the message. We refer to the constellations for this adaptive modulation scheme as *irregular* due to the fact that spacing between adjacent points is not constant.

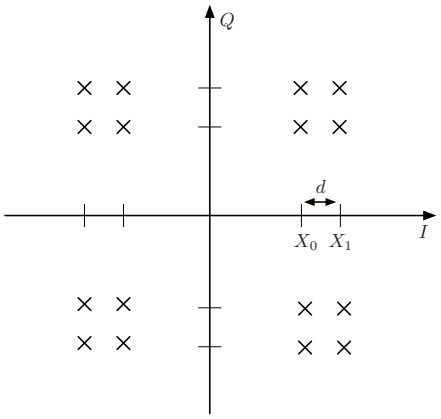

Fig. 3. Constellation of an arbitrary irregular 16-QAM constellation described by the ordered pair (X_0, X_1).

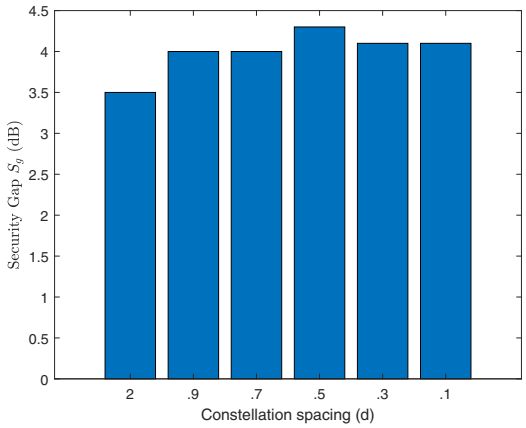

Fig. 4. Security gap (S_g) as a function of spacing (d) for various irregular 16-QAM constellations with the ICSHK scheme.

A. Irregular 16-QAM

For the case of 16-QAM, an irregular constellation can be described by the ordered pair (X_0, X_1), such that each point has a value of either $\pm X_0$ or $\pm X_1$ in both the I and Q axes. Fig. 3 shows an arbitrary irregular 16-QAM constellation, with the distance $d = X_1 - X_0$ marked. For our experiments, we fixed X_0 and altered X_1. This had the overall effect of compacting the points within each quadrant, while also increasing the relative distance between quadrants. This increases the BER for a given SNR. This can be seen by computing an error bound for each symbol. As described in [18], an upper bound on the average symbol error probability in an arbitrary constellation is given by

$$P(E) \leq \frac{1}{S} \sum_{m=0}^{S-1} \sum_{n=0, n\neq m}^{S-1} \Pr(\hat{s} = s_n | s_m), \tag{4}$$

where S is the modulation order and $\Pr(\hat{s} = s_n|s_m)$ is the probability that received symbol $\hat{s}$ is decoded as s_n given that s_m was sent. That probability is given by

$$\Pr(\hat{s} = s_n|s_m) = Q\left(\sqrt{\frac{d_{m,n}^2}{2N_0}}\right), \tag{5}$$

with $d_{m,n}$ being the Euclidean distance between points m and n in the I/Q plane, and N_0 the single-sided noise spectral density. Using the above equations, we can fine-tune the error rate of a constellation by adjusting the distances between adjacent symbols. For each symbol in the 16-QAM constellation, errors from the three adjacent symbols account for the majority of probable error. This makes sense as errors at high SNR are generally caused by the closest relative symbols [18]. At reliable SNR levels the contributions of the 12 smallest terms to the overall error rate is negligible, and so the error can be well approximated by only three terms. This simplified error equation is given by

$$P(E) = 2Q\left(\sqrt{\frac{d^2}{2N_0}}\right) + Q\left(\sqrt{\frac{2d^2}{2N_0}}\right). \tag{6}$$

Notice that these terms depend only on the difference between X_1 and X_0, but not the explicit values of these variables. The error performance of an irregular constellation depends almost exclusively on the spacing within each quadrant.

The above analysis focuses on the constellation, but it is important to see the effect when combined with the ICSHK scheme. Monte Carlo simulations show that changing the spacing d, has no significant effect on the security gap. It can be seen that the security gap S_g remains approximately equal for all spacings, as shown in Fig. 4. Although the security gap stays consistent, the values of $\text{SNR}_{B,min}$ and $\text{SNR}_{E,max}$ change exponentially as we decrease d. Fig. 5 shows the BER curves for various constellation spacings, which illustrate the consistent shape and exponential difference between successive values of d. The best fit line measuring $\text{SNR}_{B,min}$ as a function of d for our results is given by

$$\text{SNR}_{B,min} = 40.5e^{-.865d}. \tag{7}$$

While we used the spacing d as the independent variable in our simulations, it is more useful to calculate what spacing to use for a given $\text{SNR}_{B,min}$. Then, a measurement could be made of the current SNR between the transmitter and authorized receiver, and the optimal constellation spacing could be calculated. That relationship is the inverse of (7) which is

$$d = -.865 \ln(\text{SNR}_{B,min}/40.5). \tag{8}$$

We also include a graph showing the BER-CDF curve for each value of d as Fig. 6. As with the BER, it is evident from this graph that the slope is unaffected by the spacing, but the SNR values are increased exponentially with decreasing d.

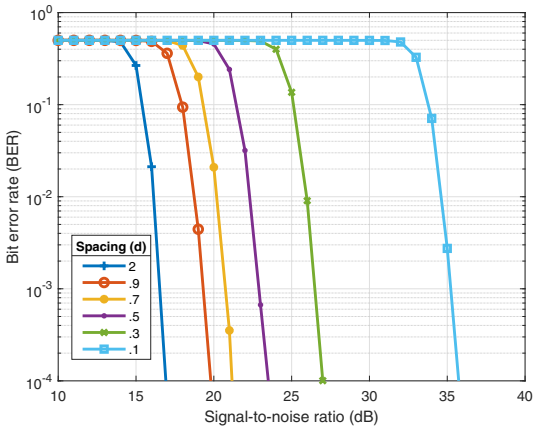

Fig. 5. Bit error rate (BER) curves for various spacings (d) of irregular 16-QAM constellations with ICSHK scheme.

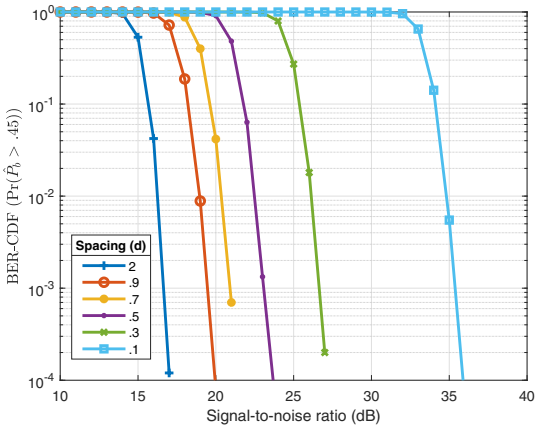

Fig. 6. BER-CDF with $\delta = .05$ for various spacings (d) of irregular 16-QAM constellations with ICSHK scheme.

B. Irregular 64-QAM

Although 16-QAM can be adjusted to any SNR value above its nominal value, it makes more sense to switch to 64-QAM once the SNR is high enough to support it. Due to the greater number of points, there are more options for how to alter the 64-QAM constellation. We denote a constellation as (X_0, X_1, X_2, X_3) and every point takes one of these four values in both the I and Q axis. While there are many ways to distort this constellation, we focused solely on two, which we name the *quadrant* and *box* methods. The quadrant method fixes X_3 and shifts all other values closer to it. This is analogous to the irregular 16-QAM constellation in that it groups together each quadrant, while increasing the separation between quadrants, as is shown in Fig. 7. The box method fixes x_0 and X_3, and moves the inner values out in opposite directions, x_1 towards X_0 and X_2 towards X_3. This is novel to the larger constellation and has the overall effect of grouping together every cluster of four points, while increasing the separation between these clusters or boxes, as shown in Fig. 8.

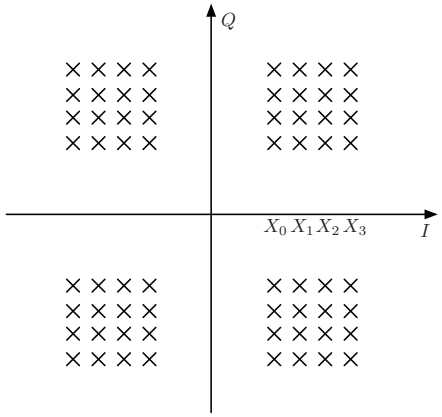

Fig. 7. Constellation diagram of irregular 64-QAM using quadrant method.

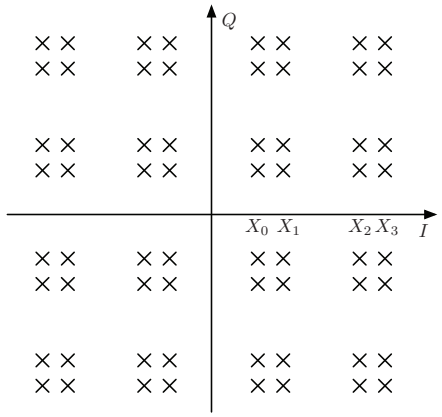

Fig. 8. Constellation diagram of irregular 64-QAM using box method.

Both methods allow for the same kind of control as with the 16-QAM constellation, although each method has a slightly different SNR to spacing relationship.

IV. Irregular QAM with Coset Coding

A. Encoding

The above analysis assumes straight-forward digital modulation, where four or eight bits from $M_e^{k'}$ map to a constellation symbol for 16-QAM or 64-QAM, respectively. The security gap can be further reduced by overlaying a coset code (often called a wiretap code [5], [19]) onto the QAM constellation. An (n', k') coset code splits all coded segments of length k' into $2^{k'}$ cosets. A length k' message selects one of the cosets, and a random co-message selects one of the $2^{k'-n'}$ codewords in that coset, which is then sent. Table I shows the coset code we used. This code was shown to have the best secrecy performance of any $(4, 2)$ code in [20]. The randomly generated co-message selects the column of the code table, while the message chooses the row. Since the co-message has nothing to do with the message, its only purpose is to provide confusion to eavesdroppers.

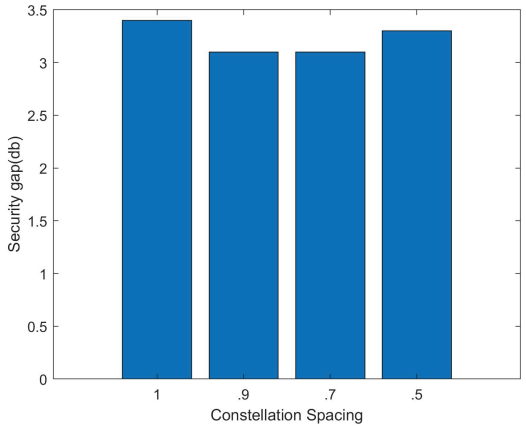

Fig. 9. Security gap S_g as a function of spacing d for various irregular 16-QAM constellations overlaid with a $(4, 2)$ coset code, with the ICSHK scheme.

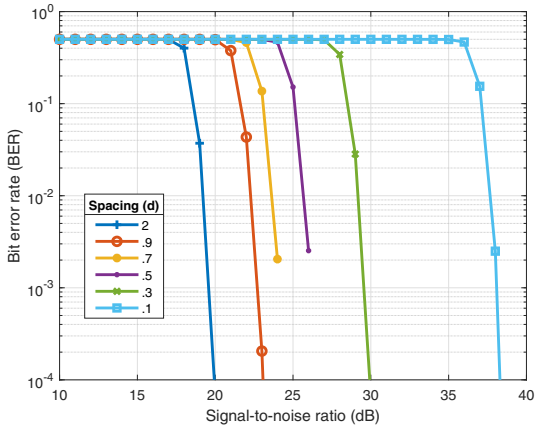

Fig. 10. BER for various spacings d for irregular 16-QAM constellations overlaid with a $(4, 2)$ coset code, with the ICSHK scheme.

TABLE I
CODEBOOK STRUCTURE FOR A COSET-BASED SECRECY CODE.

	$M_e^{k'}$	Symbol labels			
?	0	0000	1110	0111	1001
	1	0001	1111	0110	1000
	2	0010	1100	0101	1011
	3	0100	1010	0011	1101

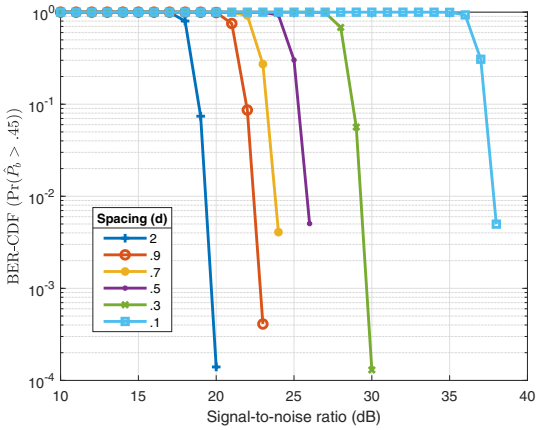

Fig. 11. BER-CDF for various spacings d for irregular 16-QAM constellations overlaid with a $(4, 2)$ coset code, with the ICSHK scheme.

B. Soft Decoding

Normally, decoding a coset code is a simple process that can be carried out by a matrix operation, a process which generates hard bit values. This will not work for the ICSHK scheme however, as the LDPC decoder requires log-likelihood ratio (LLR) values, which represent the likelihood of a single bit being either zero or one. The equation to calculate the LLR for bit i is

$$\mathrm{LLR}_i = \ln\left(\frac{\sum_{s_k \in \mathcal{S}_0} \exp(-|y - s_k|^2/\sigma_{N_z}^2)}{\sum_{s_k \in \mathcal{S}_1} \exp(-|y - s_k|^2/\sigma_{N_z}^2)}\right) \tag{9}$$

where s_k is a constellation symbol, $\mathcal{S}_0$ is the set of all constellation symbols with a zero in the ith position, $\mathcal{S}_1$ is the set of all constellation symbols with a one in the ith position, y is the received symbol, and $\sigma_{N_z}^2$ is the noise variance of the channel. In order to use this decoding method with coset coding, the decoder must know the symbol label to symbol mapping as well as the coset code. There are two important changes to the normal decoding process to adapt for coset codes. First, there should only be LLR values generated for coded segment bits, not for symbol label bits. This means that for the $(4, 2)$ code used previously, this equation would only output two LLR values, not four. The second change is the way in which $\mathcal{S}_0$ and $\mathcal{S}_1$ are chosen. $\mathcal{S}_0$ is the set of all constellation symbols which are decoded to have a zero in the ith coded segment bit and $\mathcal{S}_1$ is analogous. With these two changes, (9) will generate the proper LLR values to feed into the LDPC decoder and the scheme will benefit from the effects of the coset discussed in the previous section.

C. Combining Coset with ICSHK

To add a coset code to the ICSHK scheme, the output of the encoder in Fig. 1 is buffered, and then split into coded segments of length k'. These messages are each combined with a randomly generated co-message to produce a stream of length n' symbol labels, as in the example of Table I. Each symbol label is mapped onto an irregular QAM symbol and transmitted. In order to fully utilize the benefit of adding a coset code, this mapping must be carefully chosen so that, when the points in each quadrant are brought closer together, the confusion on the coset code increases faster than errors accumulate on the symbols. This means that small changes to the constellation lead to disproportionately large increases in the error rate, creating a sharper BER curve and a smaller security gap. The best way to achieve this is to map one symbol label from each coset onto a symbol in each quadrant. For 16-QAM, this is trivial. For 64-QAM, care must be taken

as there are various coset code options. A $(6, 4)$ code gives 16 cosets with 4 symbol labels each, so that the quadrant mapping can be preserved. This is ideal for the quadrant method of irregular 64-QAM. A $(6, 2)$ code has 4 cosets, and the box method may be preferred here so that one symbol from each 4-symbol box can be assigned to each coset. It should be noted that for both 16- and 64-QAM, the addition of the coset code reduces the rate. It is up to the designer whether it is preferable to have a higher rate or a smaller security gap.

Fig. 9 shows the security gap for 16-QAM with the $(4, 2)$ code in Table I. Comparison to Fig. 4 shows that the security gap has been reduced by the addition of the coset code. By comparing Fig. 10 to Fig. 5, and Fig. 11 to 6, it can be seen that adding the coset code also leads to a higher value for both $\text{SNR}_{B,min}$ and $\text{SNR}_{E,max}$ for the same constellation spacing.

V. Conclusions and Future Work

In order to adapt transmission schemes to a wider range of SNR, we propose an irregular QAM constellation be added to the process. Error bounding shows that decreasing the spacing within each quadrant of an irregular constellation increases the error rate, which leads to a higher required SNR to decode the message. Simulations show that changing the spacing has no significant impact on the security gap, meaning that security can be guaranteed at any noise level. This security gap can be further reduced by mapping a coset code onto the irregular constellation for a new type of coded modulation, although this comes at the expense of decreasing the rate of the code.

References

[1] M. Asghar, N. Mohammadzadeh, and A. Negi, "Principle application and vision in internet of things (iot)," in *Computing, Communication Automation (ICCCA), 2015 International Conference on*, May 2015, pp. 427–431.

[2] L. Tan and N. Wang, "Future internet: The internet of things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, vol. 5, Aug 2010, pp. V5–376–V5–380.

[3] G. Durisi, T. Koch, and P. Popovski, "Towards massive, ultra-reliable, and low-latency wireless: The art of sending short packets," *CoRR*, vol. abs/1504.06526, 2015. [Online]. Available: http://arxiv.org/abs/1504.06526

[4] ——, "Toward massive, ultrareliable, and low-latency wireless communication with short packets," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1711–1726, Sep. 2016.

[5] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] M. Bloch and J. Barros, *Physical Layer Security : From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[8] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct 2015.

[9] L. Hu, H. Wen, B. Wu, J. Tang, and F. Pan, "Adaptive secure transmission for physical layer security in cooperative wireless networks," *IEEE Communications Letters*, vol. 21, no. 3, pp. 524–527, Mar 2017.

[10] H. Song, H. Wen, L. Hu, Y. Chen, and R. Liao, "Optimal power allocation for secrecy rate maximization in broadcast wiretap channels," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 514–517, Aug 2018.

[11] K. T. Phan, Y. Hong, and E. Viterbo, "Adaptive resource allocation for secure two-hop communication," in *Proc. IEEE Wireless Communications and Networking Conference (WCNC)*, Apr 2018, pp. 1–6.

[12] M. Yusuf and H. Arslan, "On signal space diversity: An adaptive interleaver for enhancing physical layer security in frequency selective fading channels," *Physical Communication*, vol. 24, pp. 154 – 160, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1874490716302592

[13] Y. Zhang, A. Liu, C. Gong, G. Yang, and S. Yang, "Polar-LDPC concatenated coding for the AWGN wiretap channel," *IEEE Communications Letters*, vol. 18, no. 10, pp. 1683–1686, Oct 2014.

[14] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes, "Interleaved coding for secrecy with a hidden key," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[15] J. P. Vilela, M. Gomes, W. K. Harrison, D. Sarmento, and F. Dias, "Interleaved concatenated coding for secrecy in the finite blocklength regime," *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 356–360, Mar. 2016.

[16] M. Baldi, M. Bianchi, and F. Chiaraluce, "Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012.

[17] T. K. Moon, *Error Correction Coding : Mathematical Methods And Algorithms*. John Wiley & Sons, 2005.

[18] M. Rice, *Digital Communications: A Discrete-Time Approach*. Brigham Young University, 2009.

[19] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channels," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

[20] W. K. Harrison, D. Sarmento, J. P. Vilela, and M. Gomes, "Analysis of short blocklength codes for secrecy," *EURASIP Journal on Wireless Communications and Networking*, pp. 1–15, 2018.