Thesis Proposal

Working title: Adaptable ICSHK with Irregular QAM Constellations

Project Purpose: When sending messages wirelessly, we wish to keep the message secret from eavesdroppers. There is a method of securing the message if the intended recipient has a better signal than the eavesdropper, but this only works for specific levels of signal clarity. I will seek to make this method more adaptable so that it can ensure secrecy at a much wider range of signal levels.

Project Importance: Secrecy in wireless communication is one of the greatest problems facing technology today. This will become especially important as the internet of things continues to expand, leading to a multitude of devices wirelessly transmitting potentially sensitive information, such as health or financial data. There are methods that can guarantee secrecy, if the authorized user has a higher signal level than any eavesdroppers. However, there are no methods that can guarantee this secrecy at various levels of noise, meaning that they are only useful in very specific circumstances. My project will seek to fill this important gap by allowing methods that already guarantee secrecy to adapt to different noise levels without needing a larger advantage.
Here is a sample of papers showing the importance of this research:
Vilela, João P. et. al. "Interleaved Concatenated Coding for Secrecy in the Finite Blocklength Regime." IEEE Signal Processing Letters, Vol. 23, No. 3, March 2016.
Sarmento, Dinis et. al. "Interleaved Coding for Secrecy with a Hidden Key."
Maturo, Nicola et. al. "Security gap assessment for the fast fading wiretap channel." ICT 2013.
Harrison, Willie K. et. al. "Coding for Secrecy." IEEE Signal Processing Magazine. September 2013.

Project Overview:
Through this research, I will seek to find a way to achieve greater secrecy in wireless communications. My work will be focused on the model of communication presented in the article "Coding for Secrecy",[1] shown here as Figure 1.

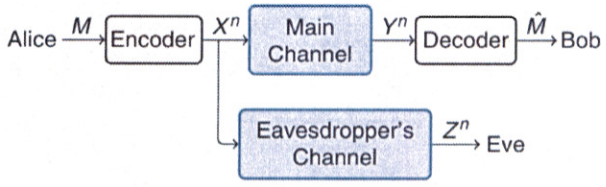

Figure 1. Wireless Communication Model

The model consists of three entities: Alice, who is trying to send a secure communication to Bob, who is trying to receive the communication, and Eve, who is trying to intercept and decode the secret message. In this model, Eve is a passive eavesdropper: she only receives and does not transmit anything. Before Alice transmits, she encodes the message, M, in order to protect it. The

[1] "Coding for Secrecy" Harrison, Willie K. et. al. IEEE Signal Processing Magazine. September 2013.

encoded message, X^n, is then sent through two separate channels. Each channel distorts the encoded message, so Bob receives the distorted signal Y^n and Eve receives the distorted signal Z^n. It is assumed that the channels are uncorrelated, meaning that the two signals are distorted in completely unrelated ways. The aim of all research using this model is twofold. First, we must ensure reliability for Bob. This means that, with very high probability, Bob will be able to recover the entirety of the message. Second, we must ensure security against Eve. This means that, with very high probability, Eve will not be able to recover any information from the transmission.

Much of the research on this model operates on the basis that Bob has a better channel than Eve.[2] My focus will be on the idea of a security gap. The security gap of a communication scheme is the difference between the minimum signal-to-noise ratio (SNR) at which Bob is guaranteed reliability and the maximum SNR at which secrecy against Eve is guaranteed. We would like to minimize this value, such that Bob only requires a slight channel advantage over Eve in order to attain the aims of communication.

My work on this project is heavily influenced by the paper "Interleaved Coding for Secrecy with a Hidden Key."[3] This essay, coauthored by my mentor, Professor Harrison, introduced a coding scheme to assist with secret communication. ICSHK, as it is abbreviated, is a multi-step process for encoding and modulating a message prior to wireless transmission. A random key is generated and then used to interleave the message. This entails swapping message bits in a predictable and reversible manner, as long as one has the key. The key is appended to the interleaved message, and the whole codeword is passed through a low-density parity check (LDPC) encoder. LDPC codes are powerful error correcting codes that utilize a large, mostly empty matrix to encode the data. Once the message and key are encoded, the codeword is punctured. This is done by erasing bits from the codeword. In the original paper, all the codeword bits relating to the key were punctured, thus leading to the idea of a hidden key; however, current research is looking into the optimum combination of key and message bits to be punctured. After puncturing, the remaining bits are modulated and transmitted. On the receiving end, the signal is softly demodulated, meaning that each bit is assigned a likelihood value instead of a bit value. This soft information is sent through an LDPC decoder, which iteratively converts the likelihoods into hard bit decisions. Once the codeword is recovered, the key is removed and used to deinterleave the message. In their paper, the authors found that the ICSHK scheme leads to a very small security gap, less than 3 dB. While this is a great result, there is still an issue; the security gap is a fixed value. This means that if the channels around Eve happen to be much better or worse than the values specified by the ICSHK scheme, then security and reliability won't be guaranteed. It would be better if we had the ability to move the security gap to a higher or lower value without changing the actual difference.

This is the area my research seeks to address. Specifically, I will be investigating the effects of changing the method of modulation used just before transmitting the signal. The default modulation that the authors used was binary phase-shift keying (BPSK) which encodes every bit as a ± 1. My project seeks to replace this with quadrature amplitude modulation (QAM), which assigns groups of bits to different symbols in the complex plane. I will focus first on 16 QAM, which sends groups of 4 bits as one of 16 possible symbols. QAM is most often used to increase the rate of transmission, as it can send 4 bits at once instead of 1, but that will not be my main objective. Instead, I will use an irregular QAM constellation to create an adaptable ICSHK

---

[3] "Interleaved Coding for Secrecy with a Hidden Key." Sarmento, Dinis et. al.

system. An irregular QAM constellation is a set of symbols in which the distance between adjacent symbols is not constant. For 16 QAM, this can be achieved by bringing the symbols in each quadrant closer together, while increasing the separation between quadrants. By altering the distance between points within a quadrant, I will seek to change the placement of the ICSHK security gap. If a higher SNR is available to Bob, the symbols could be brought closer together, raising the overall SNR required to successfully decode the message, and ensuring security against a wider range of possible eavesdroppers. After examining 16 QAM, I will also look into 64 QAM, which should have similar properties but at a higher rate of communication.
Should this prove successful, I would add an additional layer to hopefully add greater control. This would entail overlaying a coset code over the QAM modulation. A coset code involves breaking down all n-bit codewords into k groups. A $\log_2(k)$ bit message is used to select a group, and a random co-message is used to select a codeword from that group. With 16 QAM, there are 4 cosets, meaning that each transmission conveys 2 bits of information. While this would reduce the rate compared to the normal 16 QAM, it could help ensure greater secrecy. By strategically placing one codeword from each coset in every quadrant, the irregular QAM will lead to greater equivocation on the message than on the codewords, thus shrinking the security gap.
In order to conduct this research, I will split my work into two phases. The first phase involves reading academic papers written on the subject, particularly those explaining the ICSHK scheme. In order to alter the scheme for my own purposes, I first must thoroughly learn how it functions. The second phase is coding and simulation. Primarily using MATLAB, I will set up simulations and run through tens of thousands of tests in order to test the functionality of my additions. This is a common procedure throughout much of the research in wireless communication. After running simulations and collecting data, I'll compile the results and determine if the irregular QAM has had the desired effect on moving the security gap. If so, I will calculate an equation to represent the impact of constellation spacing on required SNR values. That equation, I believe, would be the heart of my research, as it would encapsulate all the simulations I'll run. At this point, assuming my simulations are successful, I would put my ideas into a paper and submit to the International Conference on Communication.

Qualifications of Thesis Committee:

Faculty advisor-Professor Willie Harrison

Professor Harrison graduated with his B.S. and M.S. degrees in Electrical Engineering from Utah State University, and his Ph.D. in Electrical and Computer Engineering from the Georgia Institute of Technology, with research focusing on physical-layer security, error-control coding, and cryptography. He has published papers on Coding for Cryptographic Security Enhancement Using Stopping Sets and Coset Codes in a Multi-hop Network. Because of his prior experience with coset codes and physical-layer security, Professor Harrison is well suited to be a mentor on this project. I met Professor Harrison while taking his class, ECEn 380, last semester.

Faculty reader- Michael Rice

Professor Michael Rice received his PhD from Georgie Tech in 1991, and has been a professor at BYU since 1991, where he is currently the Jim Abrams Professor in the Department of Electrical and Computer Engineering. His research focuses on digital and communication theory and error control coding with a special interest in aeronautical telemetry and software radio. Because of his familiarity with digital communications,

Professor Rice is well suited to be a faculty reader for this project. He was recommended for the position by Professor Harrison.

Department Honors Coordinator-Professor Karl Warnick

Project Timeline:

April 30, 2018-Fly to Portugal
May 1, 2018-Arrive at the University of Coimbra
July 16, 2018-Return to the US
End of July 2018-Finish simulations
September 2018-Finish edits to paper
October 14, 2018-Submit paper to conference

* missing some important dates
- Defense
- Draft
- etc.

why travel?

Funding: This project is fully funded through an International Research Experience for Students grant from the NSF.

Culminating Experience: After completion of this project, I will submit a paper for publication to the International Conference on Communication.