2024 IEEE Conference on Standards for Communications and Networking (CSCN) | 979-8-3315-0742-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSCN63874.2024.10849737

Keyless Secure Communication for 6G Wireless: Design and Implementation of Physical Layer Security with High-Order QAMs

Tetra Engdahl, Rafael Soler, Nuwan Janaranga Galabada Kankanamge, Nghi H. Tran
Department of Electrical & Computer Engineering, University of Akron, Akron, OH, USA

***Abstract*—Physical layer security (PLS) leverages physical characteristics of wireless channels to allow secure data transfer in wireless communications. While PLS has received considerable research, its practical implementation is still evolving. To address this gap, this work designs and implements a keyless PLS-based communication scheme using three USRP devices in an over-the-air environment in which a multi-antenna transmitter infuses an artificial Gaussian noise source to the nullspace of an intended receiver in order to obscure the received signal of an eavesdropper. The design is applicable to high-order quadrature amplitude modulation (QAM) constellations, which is suitable for high-spectral efficiency wireless communication systems. Our measurement results fully demonstrate the confidentiality achieved by the proposed PLS implementation.**

I. Introduction

Current security mechanisms use the virtue of cryptography, which are computationally intensive and inherently inflexible with physical wireless connections. Over the last two decades, physical layer security (PLS) has emerged as an attractive security solution that guarantees secrecy regardless of eavesdropper's computational power. While PLS has been heavily researched and is under consideration for 6G wireless networks [1], [2], its practical implementation is still evolving [3], [4]. Since PLS is achieved through the exploitation of physical-layer characteristics such as of noise and fading, the real-world PLS implementation must tackle practical challenges associated with channel estimation as well as phase and amplitude recovery.

In this work, we attempt to address the practical realization of PLS by implementing a keyless secure communication system on three USRP devices in which a multi-antenna transmitter Alice infuses artificial Gaussian noise to the nullspace of Bob, an intended receiver, in order to obscure the received signal of an eavesdropper Eve. Different from existing implementations [3], [4], our primary focus is on the design of channel estimation as well as phase recovery and demodulation at Bob and Eve for high-order quadrature amplitude modulation (QAM) schemes.

II. Design and Implementation

In our implementation, we use an NI USRP-2942R as Alice, an NI USRP-2922 as Bob, and an USRP N210 as Eve as shown in Fig. 1. With two transmit antennas, Alice divides their power between transmitting a message to Bob and transmitting Gaussian noise into Bob's nullspace. Assuming that Eve's channel doesn't align with Bob's, it results in Eve receiving a portion of that artificial noise while Bob's signal maintains its clarity. The core strength of this scheme is that signal distortion present at Eve scales well with an increase in signal-to-noise ratio. Additionally, this scheme relies on a channel state information (CSI) measurement of Bob's channel to be transmitted to Alice in order for it to function. Details of the design are further described in the following.

Fig. 1. Our setup with three USRP devices.

A. Transmitter Design

1) Header: For synchronization and channel estimation, the header is structured using unique words (UWs) as in [4].

2) Beamforming and Artificial Noise (AN) Injection: We consider 16- or higher-order QAMs. For beamforming, the modulated signal is pre-coded based on CSI of Alice-Bob channel such that the destructive interference from two transmit antennas is minimized and the phase shift is corrected. For artificial noise generation, the nullspace of CSI is first calculated, yielding a unit vector in the nullspace of the channel. This vector is then multiplied by a Gaussian noise source.

B. Receiver Design

1) Carrier and Timing Synchronization: An external clock is used for carrier frequency synchronization. This removes the need for blind recovery of the carrier and also aids in providing a more measurable signal at the receiving end. For timing recovery, the Polyphase Clock Sync block is adopted. This block also provides the second matched filter to cancel out inter symbol interference (ISI).

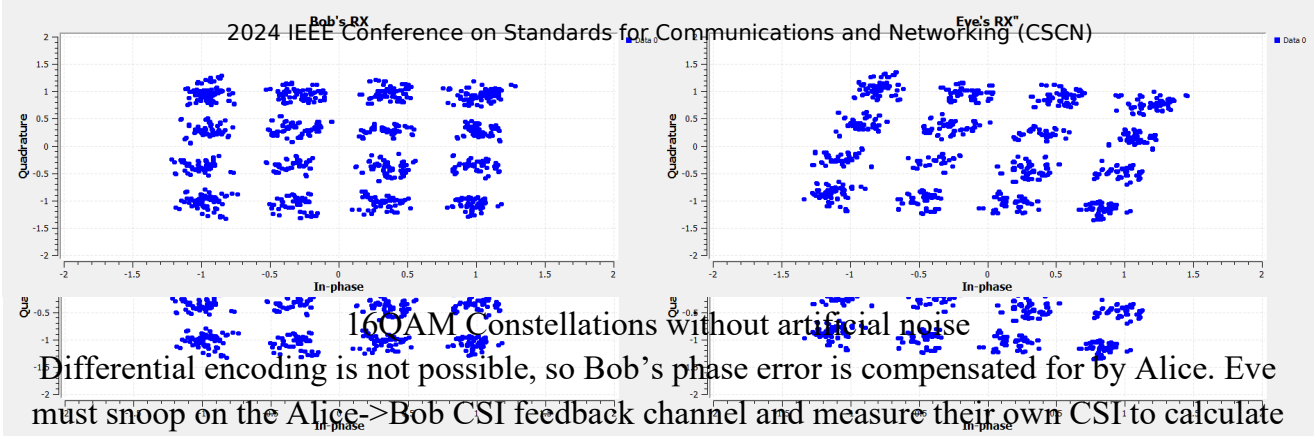

Fig. 2. Received signals at Bob and Eve with artificial noise disabled.

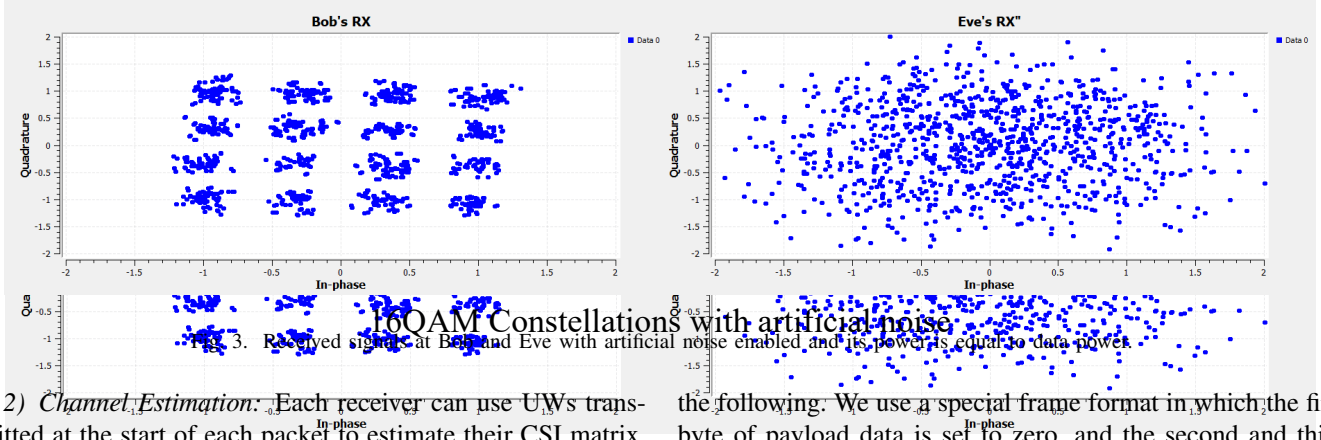

Fig. 3. Received signals at Bob and Eve with artificial noise enabled and its power is equal to data power.

2) Channel Estimation: Each receiver can use UWs transmitted at the start of each packet to estimate their CSI matrix. A GNU radio built-in FIR filter block is set up using the UW to calculate cross-correlations of UWs with signals. By the autocorrelation property of white noise, the cross-correlation will form a peak when the transmitted UW is matched. A custom peak detector block is developed, which uses the z-score algorithm with an adjustable z-score threshold.

3) Phase Recovery and Demodulation: For phase correction at Bob, the phase shift induced on their channel is accounted for by Alice. For Eve, because the use of QAM signals, instead of exploiting differential encoding as in [4], we consider the best case scenario such that Eve is able to snoop on Bob-Alice CSI feedback channel and measure their own CSI for phase recovery and demodulation. Specifically, using the knowledge of Eve's own CSI, they can undo their own phase shift. Using Bob's CSI, Eve can then undo the phase correction performed in the beamforming step.

III. Results and Future Work

Fig. 2 shows the signals measured at Bob and Eve when Alice-Bob and Alice-Eve distances are the same and 16-QAM is used over 2.4 GHz frequency range with AN disabled. Without AN, it can be seen that the received signals at Bob and Eve are 16-QAM constellations. On the other hand, Fig. 3 shows the results when AN is enabled, and its power is set equal to data power. It is clear that a standard 16-QAM is observed at Bob, while Eve's signal is completely distorted.

Note that our design also works with higher-order QAM schemes. In addition, with our setup, the bit error rate (BER) can be measured experimentally, which is briefly described in the following. We use a special frame format in which the first byte of payload data is set to zero, and the second and third bytes are set to a frame ID. The first few QAM symbols of the payload corresponding to these three bytes will not have artificial noise added to them. This way, once the signal was demodulated on the receiving end, the frame ID could be read and checked from bytes 2 and 3 and used to index a lookup table containing the test signal to be checked against. If a frame has mismatched frame ID bytes, it is rejected and not counted toward the BER measurement. By skipping a certain number of frames received, the system can reach a steady state before beginning BER measurement. The BER results, however, are omitted due to space limit.

Currently, we are exploring the possibility of extending the design to multi-user networks with multiple Eves over a more dynamic mmWave wireless channel.

Acknowledgment

This work was supported in part by the U.S. National Science Foundation (NSF) under award SaTC-1956110.

References

[1] M. Mitev, A. Chorti, H. V. Poor, and G. P. Fettweis, "What physical layer security can do for 6G security," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 375–388, 2023.

[2] Y. Yang and M. Guizani, "Metasource-based secret key: Physical layer security guarantee for future wireless networks," *IEEE Wireless Communications*, pp. 1–8, 2024.

[3] S. A. Hoseini, F. den Hartog, and F. Bouhafs, "Realizing physical layer security with common off-the-shelf WiFi equipment," in *Proc. IEEE 20th Consumer Communications and Networking Conference (CCNC)*, 2023, pp. 935–936.

[4] K. Ryland, M. Lichtman, and T. Clancy, "Implementation of two physical layer security techniques in an OTA system," *Proceedings of the GNU Radio Conference*, vol. 2, no. 1, p. 9, 2017.