SDR Testbed of Full-Duplex Jamming for Secrecy

André Silva[†‡], Marco A. C. Gomes[‡] João P. Vilela[*], Willie K. Harrison[§]
[†]University of Coimbra, CISUC, Department of Informatics Engineering, Portugal.
[‡]University of Coimbra, Instituto de Telecomunicações, Department of Electrical and Computer Engineering, Portugal.
[*]CRACS/INESCTEC, Departamento de Ciência de Computadores, Faculdade de Ciências, Universidade do Porto,
Rua do Campo Alegre s/n, 4169–007 Porto, Portugal.
[§]Department of Electrical and Computer Engineering, Brigham Young University, UT, USA.
Emails: uc2015228086@student.uc.pt, marco@co.it.pt, jvilela@fc.up.pt, willie.harrison@byu.edu

***Abstract*—In order to secure wireless communications, we consider the usage of physical-layer security (PLS) mechanisms (i.e. coding for secrecy mechanisms) combined with self-interference generation. We present a prototype implementation of a scrambled coding for secrecy mechanism with interference generation by the legitimate receiver and the cancellation of the effect of self-interference (SI). Regarding the SI cancellation, two algorithms were evaluated: least mean square and recursive least squares. The prototype implementation is performed in real-world software-defined radio (SDR) devices using GNU-Radio.**

***Index Terms*—Software-defined radio, GNU-Radio, Physical-layer security, Jamming, Full-duplex, Self-interference cancellation**

I. Introduction

Wireless communications are broadcast in nature. It is therefore difficult to restrict the communication to an intended receiver (Bob) while granting secrecy against an illegitimate one (Eve). Although modern cryptography helps to ensure secrecy in communication, it settles on the premise of the computational infeasibility of breaking cryptographic schemes. Information theoretically secure coding schemes, unfortunately, are currently unknown for real-wold channels.

That said, in the past few years there have been efforts for PLS to act as a complement of the modern cryptographic schemes. Wyner's wiretap channel [1] considers a three-party communication setup (Alice, Bob and Eve) where the wiretap channel (Alice and Eve channel) is degraded relative to the main channel (Alice and Bob channel). Also, Wyner showed that it is possible to build wiretap codes to achieve reliable communication to Bob and secrecy against Eve. More practical coding schemes have been proposed, for instance, Klinc [2] took advantage of the low-density parity-check (LDPC) code characteristics along with puncturing to create a coding scheme to transmit a coded message with punctured bits. In order to not directly expose the transmitted information, Baldi [3] proposed the use of scrambling/interleaving techniques [3], [4]. Following these works, a coding for secrecy scheme was recently proposed called interleaved/scrambled coding for secrecy with a hidden key (ICS-HK / SCS-HK) [5], [6].

This work was funded by the European Regional Development Fund (FEDER), through the Regional Operational Programme of Lisbon under Grant POR LISBOA 2020, by the Competitiveness and Internationalization Operational Programme (COMPETE 2020) of the Portugal 2020 framework [Project 5G with Nr. 024539 under Grant POCI-01-0247-FEDER-024539], and by FCT/MCTES through national funds and when applicable co-funded EU funds under the projects UIDB/EEA/50008/2020, and PES3N (SAICT-45-2017-POCI-01-0145-FEDER-030629).

Eve's channel disadvantage with respect to Bob is difficult to assure at all times, thus leading to the development of cooperative jamming schemes where there is one helper transmitting and degrading Eve's channel. However, this type of scheme has some drawbacks like synchronization, willingness of cooperation by the helper and the need of a trusted relationship. This work addresses these drawbacks through a solution in which Bob (other than a third party) acts himself as a jammer, while transmitting in the same frequency in which he is receiving (i.e. full-duplex), therefore suffering from self-interference (SI) upon reception [7]. A SDR testbed implementation, using Ettus Universal Software Radio Peripheral (USRP) B210 devices, is presented as a proof of concept where the adapted SCS-HK coding scheme is combined with full-duplex jamming. Furthermore, two algorithms of SI cancellation will be evaluated.

The remainder of the paper is organized as follows. In Section II, concepts of PLS are introduced along with the mechanisms used on the prototype implementation. In Section III the setup is explained and results presented, and Section IV concludes the paper.

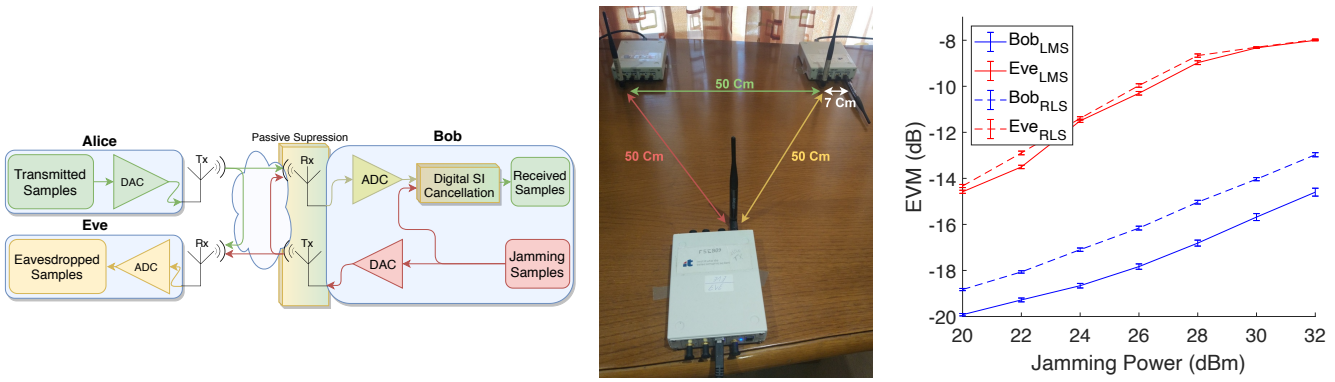
II. Physical Layer Security

A. SCS-HK Adapted Scheme

The ICS-HK and SCS-HK coding schemes [5], [6] rely on scrambling/interleaving the information with a random key, followed by encoding them together with an LDPC code. Some of the bits of the resultant codeword are punctured before the transmission to guarantee that only the legitimate receiver having a better channel can correctly recover the message. The SCS-HK scheme [5] was adapted to use in this prototype. The modifications were mainly in the type of scrambler used (additive rather than multiplicative) and how a packet is found (a simple verification after the header being decoded through a Reed-Solomon code).

B. Jamming and Cooperative Jamming

In the coding for secrecy schemes it is necessary for Bob to have some advantage over Eve, often an uncontrollable factor. Cooperative jamming [8] was considered to overcome this challenge to help lower the signal to noise ratio (SNR) of the wiretap channel. It consists in having an external jammer to help Alice to communicate with Bob using several known schemes, namely cooperative jamming by Gaussian noise, by structured codes and by alignment.



(a) (b) (c)

Fig. 1. (a) Conceptual Scheme of SI Cancellation of this work; (b) SDR setup; (c) Jamming Power and EVM comparison of Bob and Eve on LMS and RLS with 95% confidence intervals.

All these schemes have some disadvantages, for instance: 1) the synchronization, that is, the helper needs to be in sync with Alice to correctly help Bob to have the necessary advantage; 2) the willingness of the helper to spend his own energy in order to emit the jamming signal to make other communications secure; and 3) there has to be a trusted relationship between the helper and Bob, because if it stops jamming, then Eve can retrieve the signal. Using Bob as a jammer can overcome most of these issues since it helps to solve the synchronization problem, the issue of the need for cooperation and it facilitates the removal of interference (the receiving device knows the characteristics of the interference being generated).

C. Full-Duplex and Self-Interference

Full-duplex (FD) enables simultaneous uplink and downlink communication in the same frequency at the same time [9] which is useful in this context: Bob receives the transmitted signal and at the same time emits the jamming signal. The main drawback in FD is the self-interference that is generated due to the signal created on the transmitter antenna being fed back into the receiver antenna of the same device. On top of that, the SI signal has higher gain than the intended one. Thus, Bob will not only receive the information signal but also receive the jamming signal (with higher gain) that is generated resulting in a lower signal to interference and noise ratio (SINR) of the channel [10].

Furthermore, to successfully retrieve the signal of interest it is required to reduce the SI signal to decode it correctly, so the goal of SI cancellation is to predict and model the distortions and compensate for them at the receiver antennas.

D. Self-Interference Cancellation

There are three different categories of SI cancellation [9], namely passive suppression, analog cancellation and finally digital cancellation. *Passive suppression* is based on attenuating the SI signal by physically separating somehow the transmitter antenna and the receiver antenna of the device. The *analog SI cancellation* is performed before the signal goes into the analog-digital converter (ADC) (e.g. by using a noise canceling integrated circuit, which is not possible in our prototype). The *digital SI cancellation* mechanism works after the signal goes into the ADC and takes advantage of the knowledge of the interfering signal for the purpose of canceling it. There are adaptive algorithms like the least mean square (LMS) and recursive least squares (RLS) which iteratively adjust the coefficients of the signal in a way to predict the desired one. This will be the focus of this work: explore the usage of the adapted SCS-HK scheme (Section II-A) along with interference generation (Section II-B) by the receiver and its cancellation using methods of Section II-C (using either LMS or RLS). The conceptual scheme of the implemented prototype is represented in Fig. 1(a).

III. Setup and Results

To assess reception quality we will measure the error vector magnitude (EVM), i.e. the distance between the received constellation symbols and the ideal ones. A smaller EVM value, means better approximation to the constellation points, thus, better possibilities to correctly retrieve the information.

In this work, the usage of both LMS and RLS algorithms will be evaluated in order to cancel the SI signal. To be as fair as possible, the SDRs are evenly separated by 50 centimeters, as indicated in Fig. 1(b). It is important to note that Bob's transmit antenna is laying down for better SI cancellation (i.e. using passive suppression as mentioned in Section II-C). For better final results, 30 tests for each jamming power were performed and the mean and 95% confidence interval were calculated on the EVM data. In all these tests, Alice's power is fixed at 20 dBm and Bob's jamming power is varying between 20 dBm to 32 dBm (with a 2 dBm step).

All the corresponding EVM (of Bob and Eve with both algorithms) and jamming power values are presented in Fig. 1(c). As it is possible to analyze, the LMS algorithm has lower EVM values than the RLS, thus, the first outperforms the latter on the SI cancellation enabling better recovering of Alice's signal. Furthermore, with better recovery it is possible to increase the jamming power for the purpose of degrading as much as possible Eve's channel with minimal effect on Bob.

IV. Conclusion

In this paper, we presented an SDR prototype implementation in GNU Radio of the SCS-HK coding for secrecy scheme with interference generation by the receiver and its cancellation using full-duplex mechanisms. The results show a clear advantage for Bob with respect to an eavesdropper due to the ability to execute self interference cancellation. Also, it was shown that the LMS outperforms the RLS algorithm for the same environment.

References

[1] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.

[2] D. Klinc, J. Ha, S. W. McLaughlin, J. Barros, and B. Kwak. LDPC codes for the gaussian wiretap channel. *IEEE Trans. on Inform. Forensics and Security*, 6(3):532–540, 2011.

[3] M. Baldi, M. Bianchi, and F. Chiaraluce. Coding with scrambling, concatenation, and HARQ for the AWGN wire-tap channel: A security gap analysis. *IEEE Trans. on Inf. Forens. and Secur.*, 7:883–894, 2012.

[4] J. 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*, 23(3):356–360, 2016.

[5] D. Sarmento, J. Vilela, W. K. Harrison, and M. Gomes. Interleaved coding for secrecy with a hidden key. In *2015 IEEE Globecom Workshops*, pages 1–6, 2015.

[6] C. Martins, T. Fernandes, M. Gomes, and J. Vilela. Testbed implementation and evaluation of interleaved and scrambled coding for physical-layer security. In *2018 IEEE 87th VTC - Spring*, pages 1–6, June 2018.

[7] Z. Dryer, A. Nickerl, M. Gomes, J. Vilela, and W. K. Harrison. Full-duplex jamming for enhanced hidden-key secrecy. In *IEEE ICC*, pages 1–7, May 2019.

[8] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener. Cooperative security at the physical layer: A summary of recent advances. *IEEE Signal Processing Magazine*, 30(5):16–28, 2013.

[9] Z. Zhang, K. Long, A. V. Vasilakos, and L. Hanzo. Full-duplex wireless communications: Challenges, solutions, and future research directions. *Proceedings of the IEEE*, 104(7):1369–1409, July 2016.

[10] J. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin. Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security*, 6(2):256–266, 2011.