Physical Layer Security in Frequency-DomainTime-Reversal SISO OFDM Communication

Sidney Golstein

May 18, 2020

Abstract

As networks flourish worldwide, data security is an important issue that must be implemented in a cost-effective manneer at all layers. The objective of secure communication is twofold and was expressed by Shannon in 1949,[1] . The intended receiver should recover the message without errors while nobody else should acquire any information.

Surpisingly, the physical layer has long been overlooked to secure the communications. Classical security techniques are the use of cryptography and encryption where the algorithms are based on mathematical operations assumed hard to compute. However, since the computing power increases at a fast pace, these mathematical operations, that were assumed to be unfeasible, are now within reach. Furthermore, a key element of secrecy systems is randomness which is abundantly available in the physical nature of communication channel.

In addition, due to their broadcast nature, wireless communications are naturally unsecured. With the deployment of 5G as an heterogeneous network possibly involving different radio access technologies, phyical layer security (PLS) has gained recent interests in order to secure wireless communications, [2],[3],[4]. PLS classically takes benefit of the characteristics of wireless channels, such as multipath fading, to improve security of communications against potential eavesdroppers. A secure communication can exist as soon as the eavesdropper channel is degraded with respect to the legitimate user one, [5]. This can be achieved by increasing the signal to interference plus noise ratio (SINR) at the intended position and decreasing the SINR at the unintended position if its channel state information (CSI) is known, and/or, by adding an artificial noise (AN) signal that lies in the null space of the legitimate receiver's channel. While many works implement these schemes using multiple antennas at the transmitter, only few ones intend to do so with single-input single-output

(SISO) systems [6],[7],[8],[9],[10].

In [6], a technique is proposed that combines a symbol waveform optimisation in time domain (TD) to reach a desired SINR at the legitimate receiver and an AN injection using the remaining available power at the transmitter when eavesdropper's CSI is not known. Another approach to increase the SINR in SISO systems is time reversal (TR). This has the advantage to be implemented with a simple precoder at the transmitter. TR achieves a gain at the intended receiver position only, thereby naturally offering a possibility of secure communication, [11]. TR is achieved by up/downsampling the signal in the TD. It as been shown in [7] that TR can be equivalently achieved in frequency domain (FD) by replicating and shifting the signal spectrum. FD implementation has the advantage to be easily performed using orthogonal frequency division multiplexing (OFDM). To further enhance the secrecy, few works combine TD TR precoding with AN injection [8],[9],[10]. In these works, the AN is added either on all the channel taps or on a set of selected taps. While the condition for AN generation is given, its derivation is however not detailed. Furthermore, the impact of back-off rate (BOR), defined as the up/downsampling rate [12], has not been yet studied in the literature.

An approach to establish secure communication using a FD TR precoder in SISO OFDM systems is proposed. An AN signal is designed to maximize the secrecy rate (SR) of the communication in presence of a passive eavesdropper whose CSI is supposed unknown. The proposed scheme uses only frequency diversity inherently present in multipath environments to achieve security. It can therefore be used in SISO systems and is then well-suited for resource-limited nodes such as encountered in IOT for instance. Indeed, MIMO capabilities require several antennas and as many transceivers and ADC/DAC, which might not fit into small-size sensors and could be too power-consuming for such IoT scenarios. Furthermore, the OFDM implementation makes this approach compatible with LTE and 5G systems.

References

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

[2] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

[3] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of tas/mrc with antenna correlation," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 254–259, 2012.

[4] D.-D. Tran, D.-B. Ha, V. Tran-Ha, and E.-K. Hong, "Secrecy analysis with mrc/sc-based eavesdropper over heterogeneous channels," *IETE Journal of Research*, vol. 61, no. 4, pp. 363–371, 2015.

[5] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] M. Li, S. Kundu, D. A. Pados, and S. N. Batalama, "Waveform design for secure siso transmissions and multicasting," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1864–1874, 2013.

[7] T.-H. Nguyen, J.-F. Determe, M. Van Eeckhaute, J. Louveaux, P. De Doncker, and F. Horlin, "Frequency-domain time-reversal precoding in wideband miso ofdm communication systems," *arXiv preprint arXiv:1904.10727*, 2019.

[8] Q. Xu, P. Ren, Q. Du, and L. Sun, "Security-aware waveform and artificial noise design for time-reversal-based transmission," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5486–5490, 2018.

[9] S. Li, N. Li, Z. Liu, H. Wang, J. Xu, and X. Tao, "Artificial noise aided path selection for secure tr communications," in *2017 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–6, IEEE, 2017.

[10] S. Li, N. Li, X. Tao, Z. Liu, H. Wang, and J. Xu, "Artificial noise inserted secure communication in time-reversal systems," in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, IEEE, 2018.

[11] C. Oestges, A. D. Kim, G. Papanicolaou, and A. J. Paulraj, "Characterization of space-time focusing in time-reversed random fields," *IEEE transactions on antennas and propagation*, vol. 53, no. 1, pp. 283–293, 2005.

[12] T. Dubois, M. Crussiere, and M. Helard, "On the use of time reversal for digital communications with non-impulsive waveforms," in *2010 4th International Conference on Signal Processing and Communication Systems*, pp. 1–6, IEEE, 2010.