Remote Detection of HPEM attacks on Wireless Front-Ends

Emmanuel Cottais and José Lopes Esteves
Wireless Security Lab
French Network & Information Security Agency (ANSSI)
Paris, France
emmanuel.cottais@ssi.gouv.fr
jose.lopes-esteves@ssi.gouv.fr

Chaouki Kasmi
TV Labs
Dark Matter LLC
Abu Dhabi, UAE
chaouki.kasmi@darkmatter.ae

Abstract**—**This study proposes a method intended to remotely detect and analyze the effect induced by a HPEM attack on a transmitter. Instead of analyzing the transmitter targeted by the attack, we propose to modify the receiver to monitor in real-time correction coefficients of compensation blocks, already present in most of the receivers.

Keywords-HPEM, RF coupling, detection, IQ modulation, polyglot signals.

I. INTRODUCTION

The effects of high power electromagnetic (HPEM) signals on radio frequency (RF) transmitters have been widely studied. Some of the effects observed on local oscillators could lead to small modifications of the carrier characteristics, resulting in a so-called polyglot signal [1]. In this study, we propose an approach allowing for the remote detection of HPEM attacks against RF emitters' front-ends by monitoring well-chosen observables at the reception level. The main outcome is the possibility of detecting an EM attack at the reception stage while the attack is made against the transmission equipment by analyzing the transmitted signal.

II. EFFECTS OF HPEM ON LOCAL OSCILLATORS OF RF TRANSMITTERS

RF mixers are a key part of a transmitter because they transpose baseband IQ signals around a carrier frequency. This reference carrier frequency is generated by one or two local oscillators, depending on the transmitter architecture. In [3, 4], it has been shown that, for some types of local oscillators, radiofrequency interferences could generate phase (Fig. 1) or frequency shifts of the output signal, which are limited to the exposure duration. Therefore, in some specific cases, the effects on the emitted signal can be viewed as polyglot signals.

III. PROPOSED DETECTION TECHNIQUE

In this paper, we propose to apply the methodology presented in [2], which has been shown as efficient to detect polyglot signals, to remotely detect the effect of an HPEM attack by monitoring the correction parameters at the reception level. All receivers have several correction blocks which are generally applied blindly, only the corrected output being of interest.

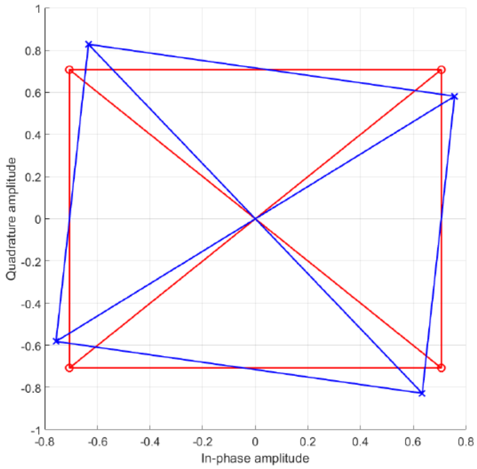

Figure 1: Expected emitted symbols (red) and during the perturbation of LOs (blue)

A specifically designed receiver could be able to detect abnormal behavior of the transmitter by the instrumentation of these well-known correction blocks. Interestingly, the method presented here could allow for detecting perturbations on transmitters by analyzing the signals at the receiver. Therefore, the detection can be performed without suffering from perturbations local to the attacked area. Besides, a set of transmitters can then be viewed as a sensor network, enabling the identification of the attacker's source position. During the presentation, the theoretical analysis and simulation results will be exposed and the benefits and limitations of the approach will be discussed.

REFERENCES

[1] T. Goodspeed and S. Bratus, "Polyglots and Chimeras in Digital Radio Modes," in REcon 2015, Montreal, Canada, 19–21 June 2015.

[2] J. Lopes Esteves, E. Cottais, C. Kasmi, "A ghost in your transmitter, analyzing polyglot signals for physical layer covert channels detection," in Hardwear.io, The Hague, The Netherlands, September 2017.

[3] T. Dubois et al, "Electromagnetic Susceptibility Studies of Op. Amp and a VCO for a PLL Application," Workshop International EMC Compo, 2009.

[4] L. Chien-Jung et al. , "A Rigorous Analysis of a Phase-Locked Oscillator Under Injection," Microwave Theory and Techniques IEEE Transactions on, volume 58, no. 5, pp. 1391 – 1400, ISSN 0018-9480, may 2010.