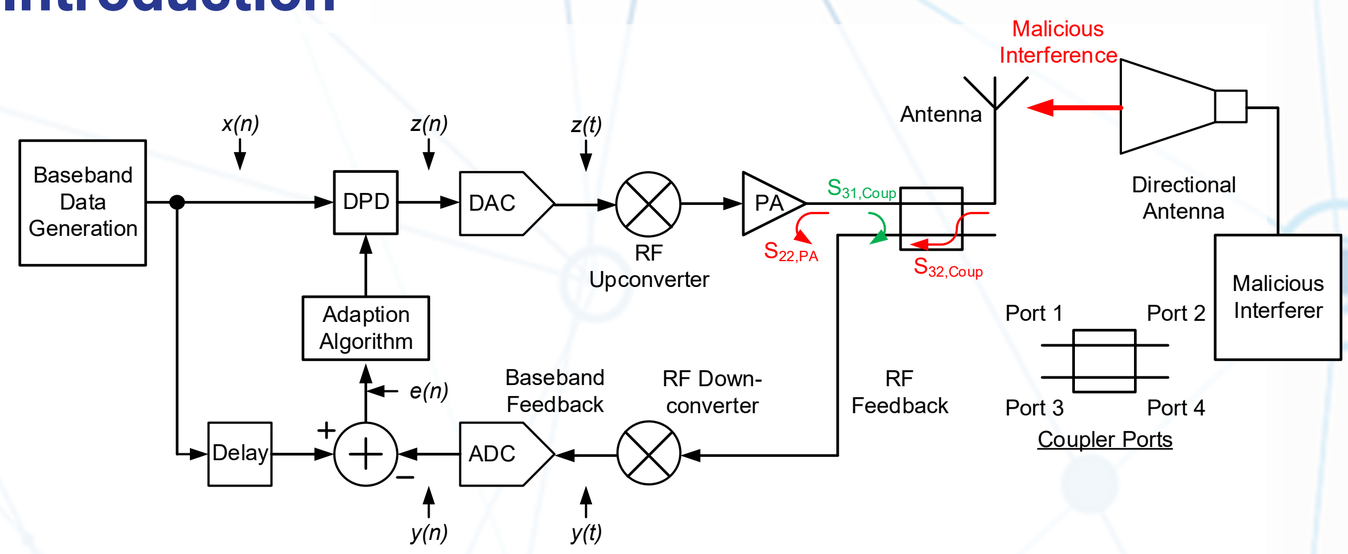
Detection of Cyber Attack on Transmitters Featuring Digital Predistortion

Gavin T. Watkins

Aim: To detect a malicious attack on the digital predistortion (DPD) feedback path of a 5G transmitter

Introduction

- Attack on receivers by jamming or spoofing is well documented, but can the transmitter be attacked?
- External signals received by the transmit antenna can generate intermodulation distortion (IMD) [1]
- This degrades transmitter linearity – adjacent channel power ratio (ACPR) and error vector magnitude (EVM)

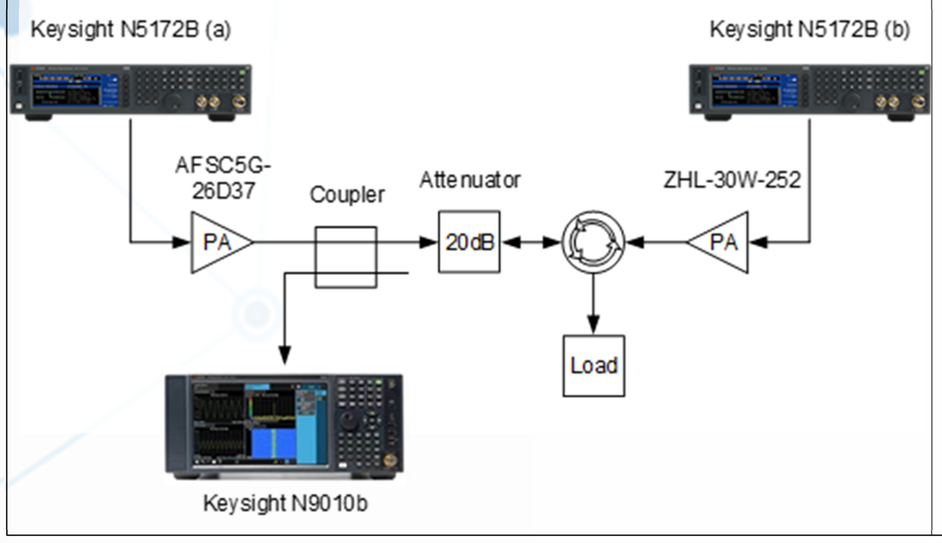


- Modern transmitters use DPD to linearise the power amplifier (PA)
- DPD requires a feedback path to the digital baseband
- A malicious interfere can enter the DPD feedback loop to “confuse” the DPD algorithm

PA Measurement Setup

Measurement setup

- AFSC5G-26D37 5G Doherty PA
- Narda 29820 with 13 dB coupler and 48 dB isolation
- ZML-30W “malicious” PA



PA Measurements

- AFSC5G produces 5W modulated output power (P_{OUT})
- 2.6 GHz operation
- 25 dBm CW malicious interferer
- Interferer measured as 7.9 dBm at coupler output
- AFSC5G $S_{22,PA}$ estimated at -1.1 dB
- 2 dB degradation in ACPR

Simulated Cyber Attack

- DPD simulation in Cadence’s virtual system simulator (VSS)
- Interference injected into DPD feedback loop during

Signal	Frequency (GHz)	Power (dBm)	ACPR (dBc)	EVM (%)
CW	2.60	-30	-36.9	2.9
CW	2.60	-20	-33.8	4.9
CW	2.60	-10	-15.7	21.0
CW	2.62	-30	-37.4	3.2
CW	2.62	-20	-27.5	3.9
CW	2.62	-10	-17.3	25.0
CW	2.64	-30	-36.9	3.1
CW	2.64	-20	-29.6	2.8
CW	2.64	-10	-17.1	21.5
OFDM	2.60	-30	-37.3	3.0
OFDM	2.60	-20	-35.5	3.3
OFDM	2.60	-10	-21.9	12.9

Detection of Attack

DPD Optimiser Cost Function

Given a known typical cost function behaviour, one that does not minimise or takes longer than usual could be an indication of attack.

Signal Features

Machine Learning could be trained to examine the feedback signal. Similar approaches have been demonstrated for receiver jamming and spoofing detection.

Time Division Duplex (TDD) Time Slots

Some 5G bands use TDD (i.e. n38, n41 and n90 at 2.6 GHz). A malicious signal could be detected during the uplink or unused downlink time slots.

Conclusions

Transmitters are susceptible to attack via the DPD feedback path

Three methods are identified for detecting an attack and will be investigated in the future

References

[1] D. Hand, “Reverse Intermodulation in a VHF RF Power Amplifier: a pragmatic approach”, Spring ARMMS Conference, 2016.

This research was supported through the UKRI/EPSRC Prosperity Partnership in Secure Wireless Agile Networks (EP/T005572/1).

Communication Systems & Networks Research Group
Merchant Venturers Building, Woodland Road, Bristol, BS8 1TR

@PartnershipSWAN
https://www.swan-partnership.ac.uk/
linkedin.com/company/swan-prosperity-partnership
swan-programme@bristol.ac.uk