Cryptographically Secure Radios Based on Directional Modulation
– a real-world, hands-on demonstration –

V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, R. Cioni
IDS, Ingegneria Dei Sistemi S.p.A.
Via Enrica Calabresi, 24
56121 Pisa – Italy

Abstract

Directional modulation (DM) can be regarded as a new frontier in physical layer communication security. This new technique uses an antenna array as a spatial encryption system which partitions the surrounding space into regions where the transmission is either perfectly intelligible or intentionally obfuscated. Still, energy and spectral efficiency of current DM systems as well as their cryptographic robustness lag behind the modern performance standards in both cryptography and radio-communication. This contribution and the related demonstration propose a generalization of the DM concept which overcomes the limitations of its initial formulation by making it both compatible with state-of-art digital modulations and cryptographically secure. A live, high bit-rate demonstration of a DM-enabled ETSI DVB-T standard is presented in support of the proposed approach.

1. Introduction and Motivations

The security of communications has been a hot topic involving both civil and military applications since the very early days of radio science. In more recent years physical layer cryptography gained attention as an effective way of providing information security by exploiting physical properties of propagation media. In such a context, recent studies (see [2–4, 7]) have proved that an antenna array can operate as a *"spatial filter"* able to encrypt the communication and make the signal intelligible only within certain regions of the space. As a consequence, the transmission is voluntarily disrupted in the remaining part of the space, where the possible presence of eavesdroppers must be taken into account.

This very attractive technique is commonly referred to in literature as *Directional Modulation* (DM) [3,4,7] and holds a huge potential for providing information confidentiality in all communication scenarios where one or more of the following apply: (i) standard cryptography keys might have been compromised, (ii) key distribution is difficult or no key distribution infrastructure is available, and (iii) limited device computing power restrains the application of traditional cryptography methods.

Solutions proposed in literature are based on the use of: (i) *switched parasitic elements* [2], (ii) *switched array* [3, 5], (iii) *phased array* [4, 6], and (iv) *dual-beam* [7] techniques. Nevertheless, the above approaches are not able to provide a sufficiently secure transmission, due to the decision zones still being quite evident in constellation plots that are received even in undesired zones (see the discussion in [9]). Also, application of all such techniques to modern, bandwidth efficient and highly error protected transmission standards (e.g. ETSI Digital Video Broadcasting - Terrestrial (DVB-T), [1] or other OFDM systems) can be very complicated. This demonstration showcases the communication and cryptography performances of a new DM approach developed in [9] by presenting a fully functional, DM-enabled COFDM transmitter.

2. Scientific and Technical Description

Fig. 1 shows the functional block scheme of the presented DM transmitter. The picture distinguishes two main stages: (i) a traditional transmitter (baseband unit and radio-frequency section) generating the signal of the chosen radio standard, which we call the *base modulation*, and (ii) a phased antenna array that operates as the *spatial encryption system* by applying suitable dynamic phase shifts according to the planned *phase control strategy*.

This effect is well shown by the coloured curves in Fig. 2, each of which identifies the amplitude and phase response of a single phase-set when applied on linear arrays of different dimensions. Switching among all possible phase sets, according to a given *phase control strategy*, applies a multiplicative distortion process $D(t)$ to the base modula-

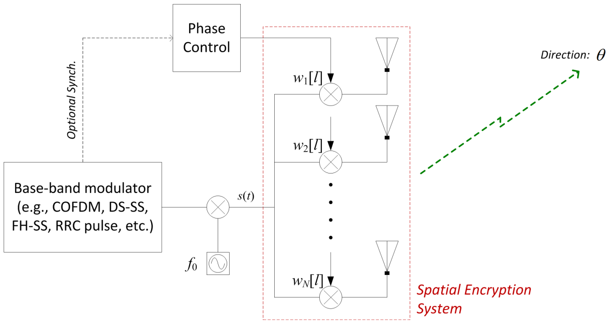
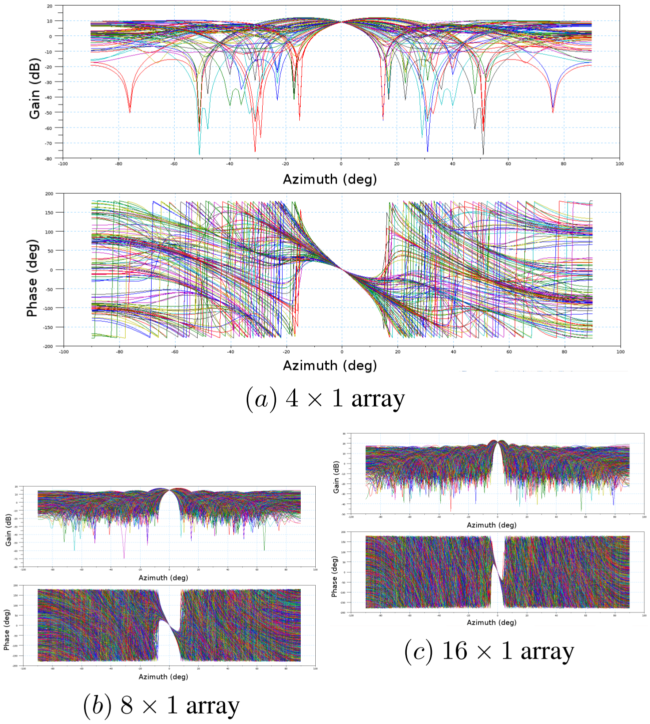

Phase Control
Optional Synch.
Base-band modulator (e.g., COFDM, DS-SS, FH-SS, RRC pulse, etc.)
$s(t)$
f_0
$w_1[l]$
$w_2[l]$
$w_N[l]$
Direction: θ
Spatial Encryption System

Figure 1. A DM transmitter, according to the generalized approach.

tion signal $s(t)$.

By observing the responses in Fig. 2, two regions can be identified: (i) one, within a certain angular interval of the central anchor point, where the signal is affected by a practically negligible distortion, which is called the *intelligible zone*, and (ii) the remainder of the space, where, depending on the chosen *phase control strategy*, the multiplicative distortion can be made arbitrarily severe. The latter is called the *interdicted zone*. By comparing the different plots in Fig. 2, it is clear how a larger array dimension results in finer geometrical control of the interdicted and intelligible zones.



(a) 4 × 1 array

(b) 8 × 1 array

(c) 16 × 1 array

Figure 2. Phased array (with isotropic radiating elements) responses at 0 deg. of elevation as a function of the phase-sets.

The main rationale behind this approach consists of using a typical antenna array as a *radio spatial encryption device* while partially giving up on its classic function as a directive antenna.

With respect to typical DM systems, the use of an independent antenna array for spatial encryption of the transmitted signal allows to decouple the complexity of signal generation from that of antenna management. Such advantage is, in turn, the ideal asset for achieving a finer control of the space, a much more robust information security as well as greater flexibility in choosing the base modulation.

3. Implementation and Use

A real-world, fully functional, DM-enabled COFDM transmitter is presented within this demo which was implemented by using [8] as the *real-time software radio* providing the *base modulation* signal $s(t)$. The very simple 4×1 antenna array, shown in Fig. 3 along with its control electronics, is used to radiate the DM-enabled signal within the demo area, see Fig. 4. A DVB-T transmission mode featuring 2048 subcarriers, $1/4$ guard interval, 16-QAM constellation and $2/3$ coding rate is used. Useful bit-rate during the tests is set at 11.612 Mbps. Several transmitter configurations are presented using different phase-set ensembles which set the intelligible zone at various angles between -90° and 90°. The received signal is probed throughout the demo area by means of a test receiver providing constellation plots as well as BER measures at various points along

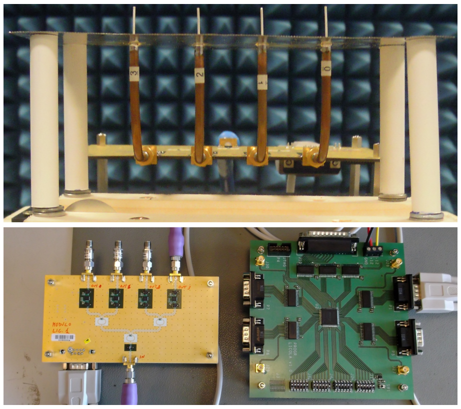


Figure 3. Prototype of DM-based phased array. Radiating element stub (above), control electronics (below).

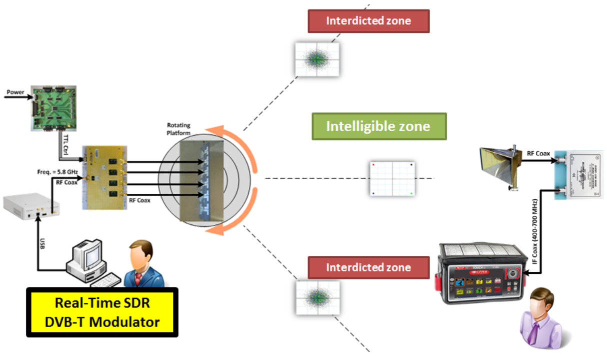
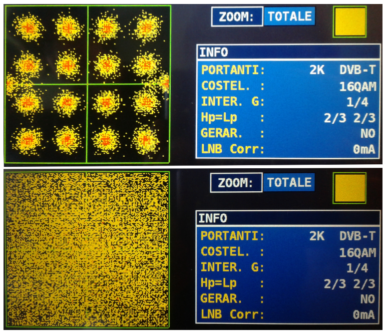


Figure 4. Pictorial representation of the proposed demonstration.



```
ZOOM: TOTALE
INFO
PORTANTI:      2K  DVB-T
COSTEL. :          16QAM
INTER. G:            1/4
Hp=Lp   :        2/3 2/3
GERAR.  :             NO
LNB Corr:            0mA
```

```
ZOOM: TOTALE
INFO
PORTANTI:      2K  DVB-T
COSTEL. :          16QAM
INTER. G:            1/4
Hp=Lp   :        2/3 2/3
GERAR.  :             NO
LNB Corr:            0mA
```

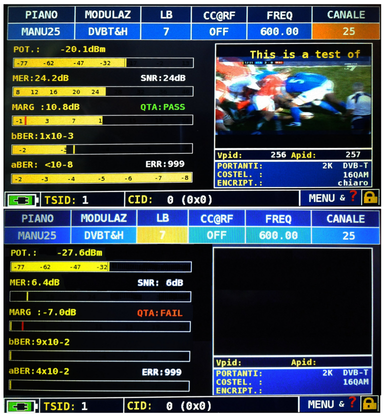
Figure 6. Constellations received in intelligible zone (above) and interdicted zone (below).

the demodulation chain. Demodulation is *quasi-error-free*, as required by the DVB-T standard, within the intelligible zones and impossible elsewhere. Signal quality parameters as well as symbol constellations experienced by the test receiver within such two reception conditions are observed and shown to the audience. An example of such parameters is shown in Fig. 5, constellation plots are instead visible in Fig. 6.

4. Conclusions and Future Developments

This presentation demonstrates the communication and cryptographic capabilities achieved by a generalization of the DM concept which is capable to overcome the main limits that restrain previously conceived techniques. It thus proves the compatibility of the proposed DM approach with *state-of-art* radio transmission systems and confirms the theoretical behaviour expected in [9].

Further developments of the proposed technology will aim at both: (i) increasing the *technology readiness level* (TRL) of the current *proof-of-concept* prototype and (ii) validating the robustness of this new technique to possible high-complexity cryptanalytic attacks.



```
PIANO    MODULAZ  LB  CC@RF  FREQ    CANALE
MANU25   DVBT&H   7   OFF    600.00  25
POT.:    -20.1dBm
MER:24.2dB            SNR:24dB
MARG :10.8dB          QTA:PASS
bBER:1x10-3
aBER: <10-8           ERR:999
This is a test of
Vpid:      256 Apid:      257
PORTANTI:           2K  DVB-T
COSTEL. :               16QAM
ENCRIPT.:              chiaro
TSID: 1   CID:  0 (0x0)   MENU &
```

```
PIANO    MODULAZ  LB  CC@RF  FREQ    CANALE
MANU25   DVBT&H   7   OFF    600.00  25
POT.:    -27.6dBm
MER:6.4dB             SNR: 6dB
MARG :-7.0dB          QTA:FAIL
bBER:9x10-2
aBER:4x10-2           ERR:999
Vpid:          Apid:
PORTANTI:           2K  DVB-T
COSTEL. :               16QAM
ENCRIPT.:
TSID: 1   CID:  0 (0x0)   MENU &
```

Figure 5. Measured signal parameters as received in intelligible zone (above) and interdicted zone (below).

References

[1] Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television. Technical Report EN 300 744 V1.5.1, ETSI, Sophia Antipolis, France, November 2004.

[2] A. Babakhani, D. B. Rutledge, and A. Hajimiri. Trasmitter architectures based on near-field direct antenna modulation. *IEEE J. Solid-State Circuits*, 2008.

[3] E. J. Baghdady. Directional signal modulation by means of switched spaced antennas. *IEEE Trans. Commun.*, 1990.

[4] M. P. Daly and J. T. Bernhard. Directional modulation technique for phased array. *IEEE Trans. Antennas Propag.*, 2009.

[5] M. P. Daly and J. T. Bernhard. Beamsteering in pattern reconfigurable arrays using directional modulation. *IEEE Trans. Antennas Propag.*, 2010.

[6] M. P. Daly, E. L. Daly, and J. T. Bernhard. Demonstration of directional modulation using a phased array. *IEEE Trans. Antennas Propag.*, 2010.

[7] T. Hong, M. Z. Song, and Y. Liu. Dual-beam directional modulation technique for physical-layer secure communication. *IEEE Antennas Wireless Propag. Lett.*, 2011.

[8] V. Pellegrini, G. Bacci, and M. Luise. Soft-dvb: a fully software, gnuradio based etsi dvb-t modulator. In *Proc. International Workshop on Software defined Radio (WSR'08)*, Karlsruhe, Germany, March 2008.

[9] V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, and R. Cioni. Cryptographically secure radios based on directional modulation. In *Proc. ICASSP 2014*, Firenze, Italy, May 2014.