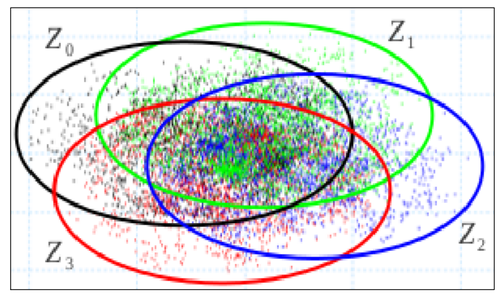
Cryptographically Secure Radios Based on Directional Modulation

– The new frontier in physical layer communication security –

V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, R. Cioni



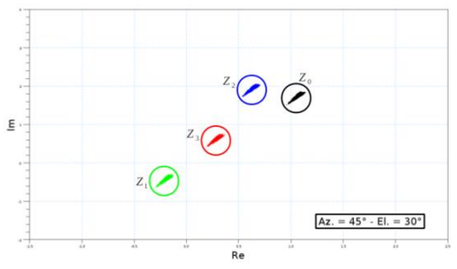
Directional modulation (DM) uses an antenna array as a ***spatial encryption system*** which partitions the surrounding space into regions where the transmission is either ***perfectly intelligible*** or ***intentionally obfuscated***

Traditional DM approaches exploit an antenna array to produce all constellation symbols

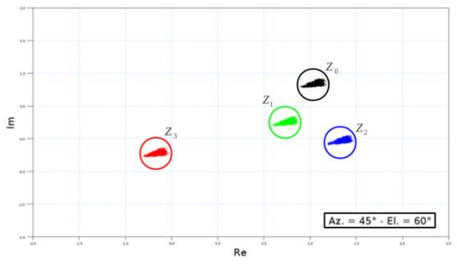
Solution available in literature:
(*i*) *switched parasitic elements*
(*ii*) *swicthed* or *phased arrays*
(*iii*) *dual-beam* techniques

DRAWBACKS

Poor performance & high complexity

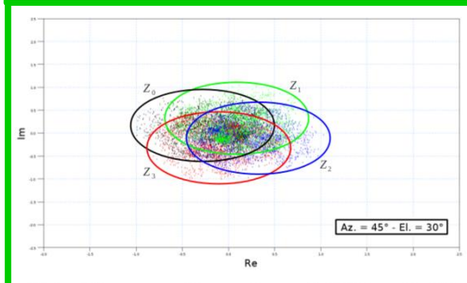


(a) Classic at $(45°, 60°)$

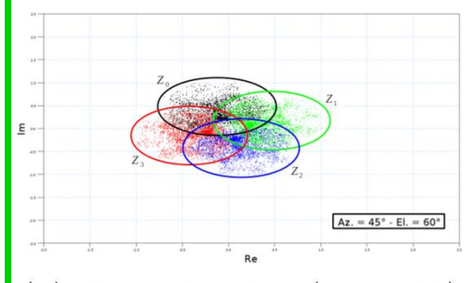


(c) Classic at $(45°, 30°)$

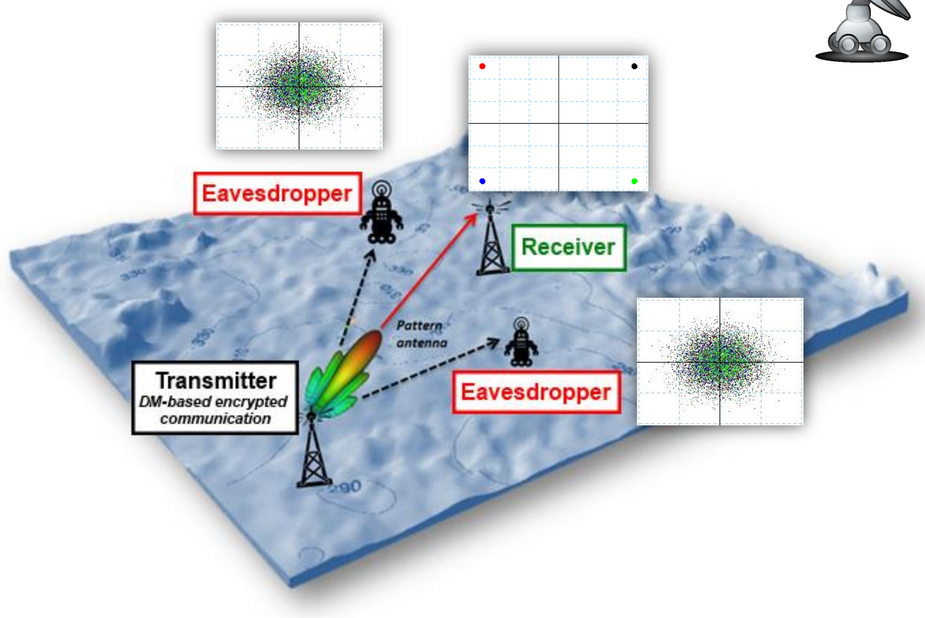
DM generalized concept
proposed by IDS



(b) Generalized at $(45°, 60°)$



(d) Generalized at $(45°, 30°)$



Communication scenarios

(*i*) Cryptography keys might have been compromised
(*ii*) Key distribution is difficult or its infrastructure is not available
(*iii*) Limited device computing power for using traditional cryptographic methods

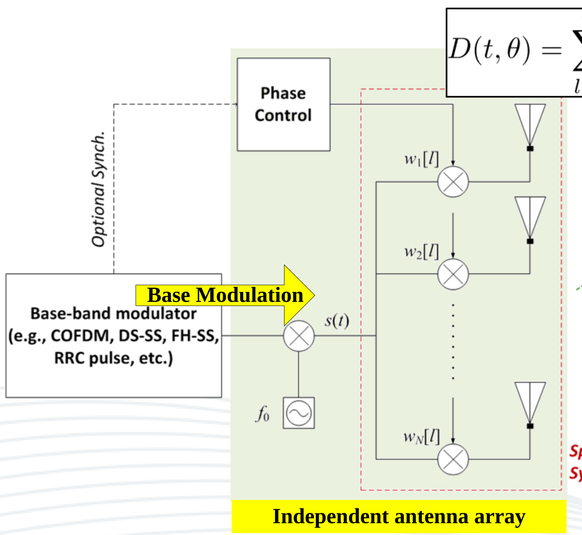
Generalized Approach to Directional Modulation (DM)

Asynchrony between BB modulator and phased array

The picture distinguishes two main stages: (i) a traditional transmitter (BB unit and RF 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.

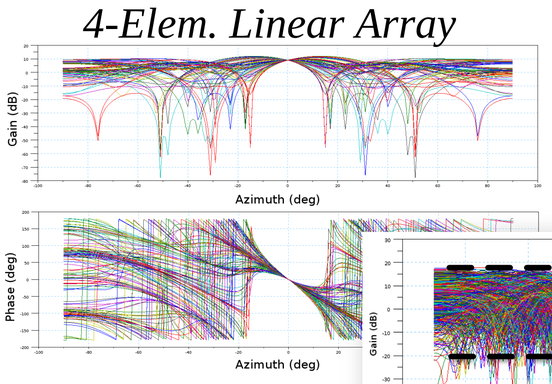
$$D(t,\theta) = \sum_{l=0}^{\infty} A[l,\theta] e^{i\omega[l,\theta]} rect\left(\frac{t - lT[l]}{T[l]}\right)$$

Phase Control Strategy

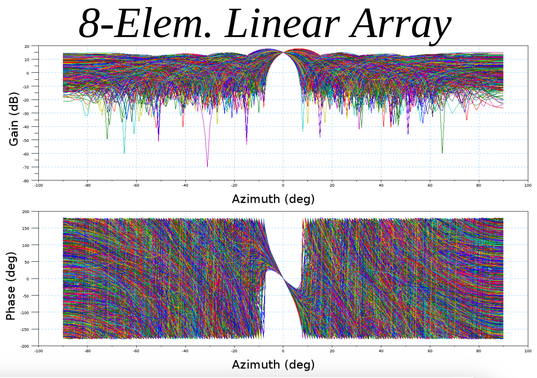


The **asynchrony** between the BB modulator and the phased array ,which becomes a viable option if the proposed approach is adopted ,allows application of DM security properties to mostly all current state-of-art digital modulations(e.g .coded OFDM ,spread spectrum ,classic pulse-shaped signals .)Indeed ,the generalized approach was named after the freedom and flexibility it provides in selecting the base modulation.

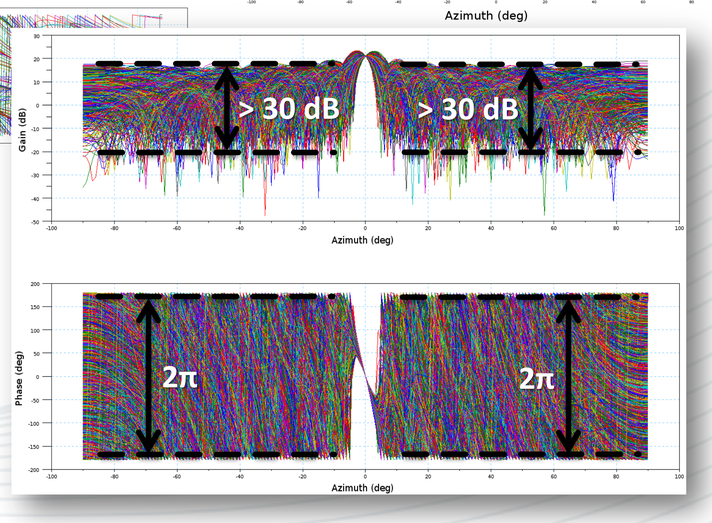
4-Elem. Linear Array



8-Elem. Linear Array

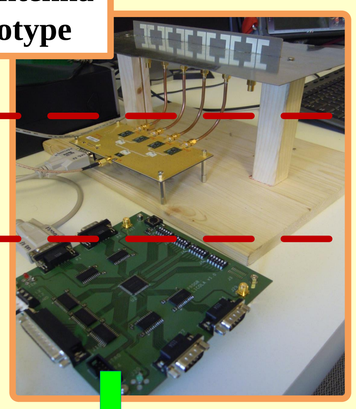


16-Element Linear Array



Experimental results

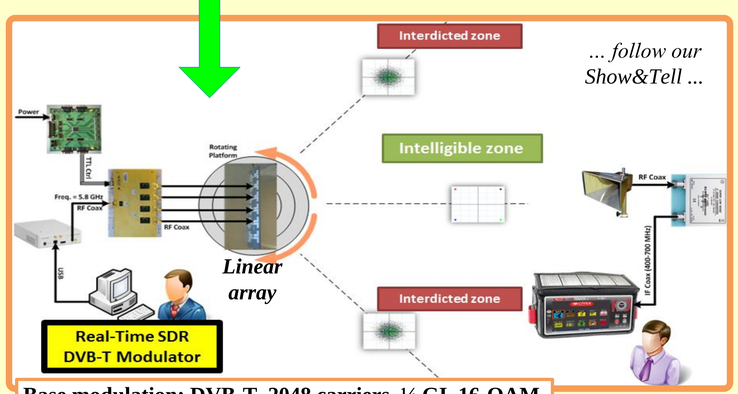
DM Antenna Prototype



Linear Antenna Array

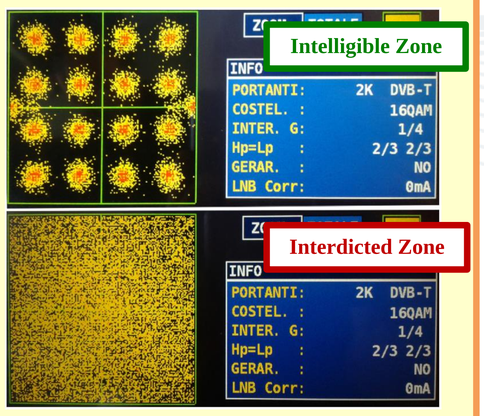
Phase shifter

Phase shifter control



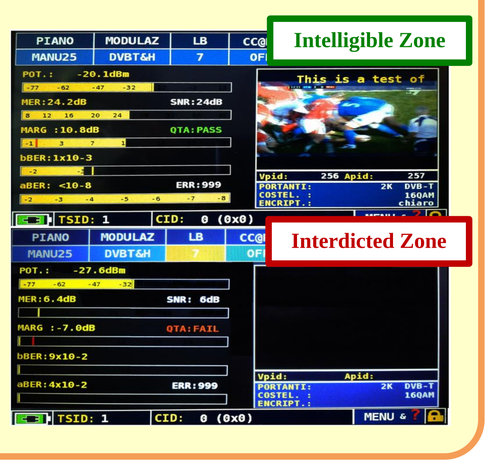
... follow our Show&Tell ...

Base modulation: DVB-T, 2048 carriers, ¼ GI, 16-QAM, 2/3 FEC, 11.612 Mbps useful bit-rate



Intelligible Zone

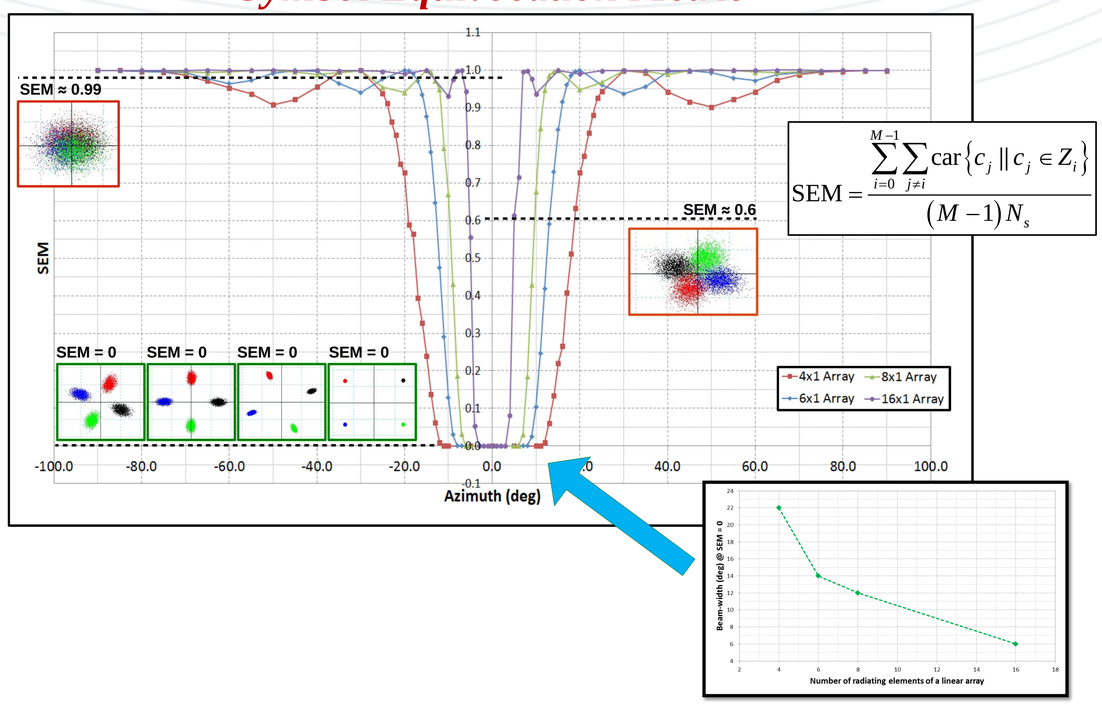
Interdicted Zone



Intelligible Zone

Interdicted Zone

Symbol Equivocation Metric



$$\mathrm{SEM} = \frac{\sum_{i=0}^{M-1}\sum_{j\neq i} \mathrm{car}\left\{c_j \,\|\, c_j \in Z_i\right\}}{(M-1)N_s}$$