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, but they suffer from drawbacks such as poor performance and high complexity. More recent approaches, like the DM generalized concept proposed by IDS, offer improved performance.

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.

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.

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

Symbol Equivocation Metric

\[ \text{SEM} = \frac{\sum_{i} \sum_{j} e_{ij} \cdot s_{ij}}{(M-1)N} \]