CRYPTOGRAPHICALLY SECURE RADIOS BASED ON DIRECTIONAL MODULATION

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

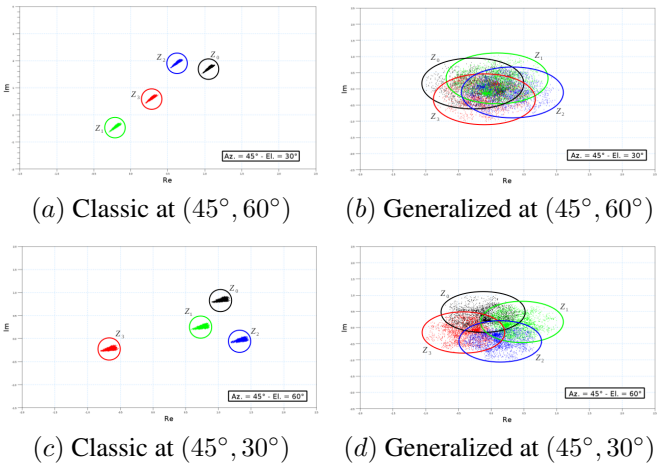
Directional modulation (DM) can be regarded as a new frontier in physical layer communication security. This new technique uses an antenna array as a *spatial encryption system* which partitions the surrounding space into regions where the transmission is either perfectly intelligible or intentionally obfuscated. Still, energy and spectral efficiencies of current DM systems as well as their cryptographic robustness lag behind the modern performance standards in cryptography and radiocommunication. This contribution proposes 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. Numerical analyses as well as *real-world, high bit-rate* implementation results are presented in support of the proposed approach.

Index Terms— Physical layer cryptography, OFDM.

1. INTRODUCTION

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 [1–4]) 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) [1,3,4] 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 cryptograpic methods.



(a) Classic at $(45°, 60°)$ (b) Generalized at $(45°, 60°)$

(c) Classic at $(45°, 30°)$ (d) Generalized at $(45°, 30°)$

Fig. 1. Constellations received within the interdicted zone. Conventional DM vs generalized DM approach at two angles (azimuth, elevation) from the intelligible zone.

In all such cases, without DM, one would be left with the choice of either transmitting information unprotected or giving the transmission up altogether. Provided that the location of the legitimate destination is known (and eavesdropper-free), DM will instead allow secure communication. Also, the application of directional modulation is not mutually exclusive with traditional cryptography techniques and can thus be employed along with such systems, in case this is advisable for the specific scenario.

Solutions proposed in literature are based on the use of: (i) *switched parasitic elements* [2], (ii) *switched array* [1, 5], (iii) *phased array* [3, 6], and (iv) *dual-beam* [4] 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 Fig. 1 and discussion in Sect. 2.2). Also, application of all such techniques to modern, bandwidth efficient and highly error protected transmission standards (e.g. European Telecommunication Standards Institute, ETSI, Digital Video Broadcasting - Terrestrial, DVB-T [7], or other OFDM systems) can be very complicated.

The authors wish to thank the Italian Department of Defense, *Segretariato Generale della Difesa* (SEGREDIFESA), for co-funding the LICOLA (*low interceptable communication link antennas*) project which led to the results described within this work. Furthermore, the authors would also thank Prof. Marco Luise, Prof. Agostino Monorchio (University of Pisa) and their staff for the precious support provided during each phase of this project.

Our analysis revises the DM concept, proposing a generalized approach that has a twofold advantage: it recovers such performance limitations while also simplifying the implementation.

2. A GENERALIZED APPROACH TO DM

2.1. Phased Arrays for Spatial Encryption

Fig. 2 proposes a pictorial representation of a DM transmitter, according to the generalized approach. 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. 3, 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 the multiplicative distortion process $D(t)$ to the base modulation signal $s(t)$.

$$D(t,\theta) = \sum_{l=0}^{\infty} A[l,\theta] e^{i\omega[l,\theta]} rect\left(\frac{t - lT[l]}{T[l]}\right) \qquad (1)$$

where $A[l,\theta]$ and $\omega[l,\theta]$ are respectively the amplitude and phase responses of the l-th set at angle θ and $T[l]$ is the time in use for the l-th set.

By observing the responses in Fig. 3, 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. 3, it is clear how a larger array dimension results in finer

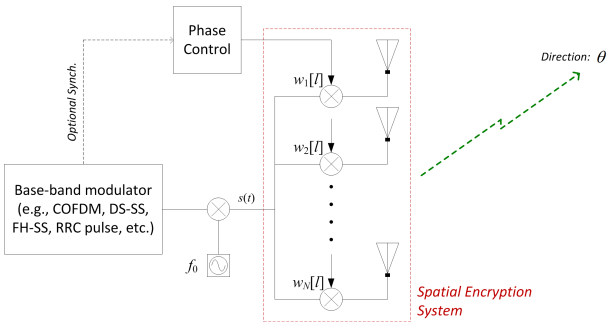
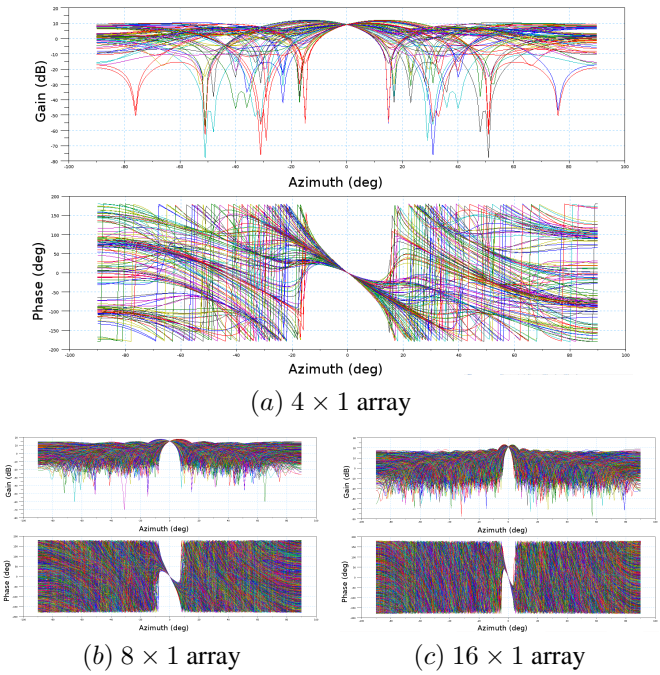


Fig. 2. A DM transmitter, according to the generalized approach.



(a) 4×1 array

(b) 8×1 array (c) 16×1 array

Fig. 3. Phased array (with isotropic radiating elements) responses at $0°$ of elevation as a function of the phase-sets.

geometrical control of the interdicted and intelligible zones. *Spectral occupancy* of the transmitted signal is practically unchanged within the intelligible zone and, being yielded by the frequency-domain convolution of $s(t)$ and $D(t)$, can be made very stable (by means of suitable phase control strategies, worst case spectral broadening $< 5\%$) even within the interdicted zone while still retaining substantial security performance.

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. Still, although a significant back-off (typically 3 to 4 dB with 4 array elements and 6-bits digital phase shifters) on the maximum achievable antenna gain is needed in order to implement DM via the generalized approach, a definitely useful directivity gain of the phased array can however be retained.

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, thus making up room for more sophisticated processing at the antenna stage. Such advantage is, in turn, the ideal asset for achieving both a finer control of the space and a much more robust information security. Furthermore, the asynchrony between the baseband 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 digi-

tal 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*. Obviously, in order to achieve good communication and security performance, structural features of the chosen radio standard must still be taken into account when designing the whole *phase control strategy* at the antenna stage. Actually, a good *phase control strategy* solves the critical trade-off among all the involved goals: cryptographic security, signal integrity in intelligible zones, spectral broadening in interdicted zones and overall system complexity. Directivity back-off and array dimension provide sufficient degrees of freedom to solve the problem by means of numerical simulation. A classic argument against DM-based systems is that space-based security can also easily be implemented by restricting power radiation to only the desired directions via conventional beamforming techniques. Still, such an argument neglects the following three outstanding facts: (i) if we imagine to restrict radiation with even a very good directive antenna (having a a side lobe level of, say, -30 dB), a 30 dB directivity gain will be sufficient, for an opponent aiming his antenna system at one of the side lobes, to access the full transmission. (ii) Given the same number of array elements, via a proper phase control strategy, the intelligible zone can be made narrower than the -10 dB beam-width of the equivalent classic phased array. (iii) If conventional beamforming is adopted, avoiding information leakage yielded by uncontrolled radiation in undesired directions requires artificial noise injection [8] which comes at the price of increased system complexity and reduced power efficiency.

2.2. Notes on Cryptographic Security

As anticipated in Sect. 1, current state-of-art DM systems yield a relatively small signal degradation within the intelligible zone, as well as major constellation transformations and distortions within the interdicted zone. Still, as visible in Fig. 1.*a* & 1.*c*, the obtained constellation maintains a very significant concentration of the – yet distorted and altered – symbol zones throughout the interdicted zone. In other words, different instances of the same constellation symbol do concentrate on the very same areas of the received constellation map, although such areas are transformed and relocated wrt standard decision zones. Such signals, in spite of having been received right at the heart of the interdicted zone, still contain a lot of information on the transmitted *plaintext*, to the extent that reconstruction of the transmitted message is within reach even by means of rather plain and uncomplicated SIGINT (SIGnal INTelligence) approaches.

Actually, after synchronization has been recovered by the standard means usually employed with traditional pulse-shaping modulations, the received distorted constellation map can be searched for the areas where symbol instances happen to concentrate. This will lead to the definition of new decision zones corresponding to the original undistorted ones. Subsequently, mapping each of the newly defined zones onto the original ones is a task that can be carried out according to several rather well-known attack strategies. For example, a rather simple brute force attack which uses the statistical recurrence of – even unknown – bit-level frame alignment preambles as its exit condition can suffice. Other exit conditions can comprise identification of known pilot symbols or sequences as well as of possibly known *plaintext* segments.

Table 1. Simulated SEM results.

DM Approach	*(Az,El) From Intelligible Zone*	*SEM*
Classic	$(45°, 30°)$	0
Classic	$(45°, 60°)$	0
Generalized	$(45°, 60°)$	0.96
Generalized	$(45°, 30°)$	0.55

Obviously, a received constellation map where all instances of each symbol were uniformly scattered throughout the complex plane (or within a certain given part of it) would be the ideal condition in order to prevent these attacks. This is true because, in this case, the only decision zone to be associated to each symbol, based on concentration measures, would be the whole complex plane (or its aforementioned sub-part) and equivocation among symbols would be maximized (see Fig. 1.*b*). In order to provide a quantitative measure of the effectiveness of each DM technique in approximating this ideal situation when its signal is received within interdicted zones, a descriptive parameter, called Symbol Equivocation Metric (SEM), was defined. SEM *equals zero* when zones relative to each constellation symbol are fully separated and don't intersect, it *equals one* instead when the ideal, full equivocation situation is reached. It is defined as follows:

$$SEM = \frac{\sum_{i=0}^{M-1} \sum_{j \neq i} car\{c_j \| c_j \in Z_i\}}{(M-1)N_s} \qquad (2)$$

where M is the cardinality of the used constellation, N_s is the number of transmitted independent, equally distributed constellation symbols, c_i is every received occurrence of the i-th constellation symbol, and Z_i is the region of the complex plane (at the receive side) associated with c_i (see Fig. 1).

Fig. 1 shows the typical interdicted zone performance of classic DM techniques as well as of the generalized approach when receiving, at two different angles from the intelligible zone, a standard 4-QAM constellation that was transmitted via a 2x2 array. SEM values for both techniques, and both angles are provided by Tab. 1.

Along with supporting high capacity, highly error protected, modern radio modulation stacks, a major goal for the generalized approach to DM is indeed to achieve cryptographic robustness by jointly designing the base modulation and the spatial encryption at the antenna stage. Indeed, using a standard phased antenna array based on hw phase-shifters

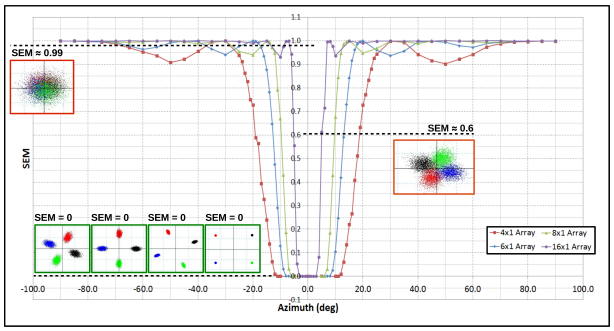


Fig. 4. SEM values vs azimuth for some linear arrays. Data is obtained using the generalized DM approach and a QPSK constellation. The small plots provide an insight of the received constellation aspect for a few significant SEM levels.

and accepting a small directivity back-off, as described in Sect. 2.1, provides several degrees of freedom. Minimizing signal distortion where the signal is intended to be received while resisting SIGINT attacks in interdicted zones is the aim such degrees of freedom are meant to be spent upon. Given Eq. (1), knowledge of the multiplicative distortion process $D(t)$ is equivalent to the knowledge of the following three items: (i) $\{w_l\}$ ensemble of all the available phase coefficient sets, (ii) w_l usage order of such sets, (iii) $T[l]$ usage time for each set, which all can be managed either in a truly random or pseudorandom mode. The former being suitable for a key-less, merely space-based encryption system, the latter instead capable of supporting both *key-less*, space based and *keyed* operation within the interdicted zone. Actually, when operating in pseudorandom mode, a receiver provided with knowledge of the distortion process, after having obtained proper synchronization, can use such knowledge to locally generate $D(t)$ and remove it from the received signal. The three base parameters mentioned above actually constitute a *triple key* made of three soft-valued independent items which, if determined by means of a suitable co-design of $D(t)$ and $s(t)$, can render a brute force attack by far impractical. When

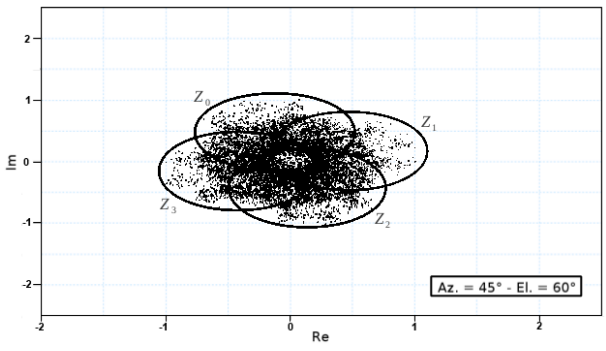


Fig. 5. Received constellation plot at SEM = 0.55 (same data as in Fig. 1, but without the color code).

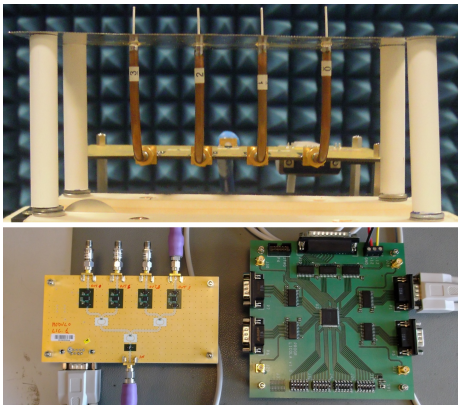


Fig. 6. Prototype of DM-based phased array. Radiating element stub (above), control electronics (below).

such a situation is reached, the vulnerability to a brute force attack is as low as it would be for a *direct sequence spread spectrum system* and is yielded by the statistical properties of $D(t)$.

3. IMPLEMENTATION RESULTS

In order to verify the cryptographic robustness of the proposed system, numerical simulations were run that explored the spatial distribution (within the interdicted and the intelligible zones) of the SEM parameter. Data presented in Fig. 4 provides a synthetic view of the obtained results by presenting the values of the SEM parameter for several azimuth angles. By using for example a 16×1 linear array (see Fig. 4), symbol equivocation equals zero within a $10°$ wide intelligible zone centered on $0°$, symmetrically grows from zero to one between $\pm 2.5°$ and $\pm 10°$ ($15°$ wide angular interval) and is constantly equal to one elsewhere. Other linear arrays featuring a smaller number of elements exhibit the same behaviour, though with reduced spatial resolution (i.e. with a coarser control in defining the boundaries of interdicted and intelligible zones). In order to evaluate the physical meaning of the SEM parameter, it is now worth to consider Fig. 5 which contains the same received constellation points as Fig. 1.*d*, the only difference being that the a-priori information on the actual transmitted symbol (carried in Fig. 1.*d* through the usage of different colors) was removed. Particularly Fig. 5 shows how, already with a SEM value of 0.55 (and without the color-coded a-priori information provided in Fig. 1.*d*), the identification of the equivalent decision zones corresponding to the original undistorted ones (as detailed in Sect. 2.2) becomes impossible.

Right after having earned a sufficient confidence through numerical analyses, a real-world, fully functional, DM-enabled DVB-T transmitter was implemented by using [9] as the *real-time software radio* providing the *base modulation* signal $s(t)$. The very simple 4×1 antenna array, shown

Fig. 7. Measured signal parameters as received in intelligible zone (above) and interdicted zone (below).

in Fig. 6 along with its control electronics, was instead used to radiate the DM-enabled signal into the surrounding space. A transmission mode featuring 2048 subcarriers, $1/4$ guard interval, 16-QAM constellation and $2/3$ coding rate was chosen. Useful bitrate during the tests was set at 11.612 Mbps. The reason for adopting a more protected mode wrt typical DVB-T transmissions to homes was dictated by the need to test security performance even in the presence of a modern, OFDM-based standard being well protected against channel distortions. Tests were run with different phase-set ensembles setting the intelligible zone at various angles between $-90°$ and $90°$. The received signal was probed throughout the surrounding space by means of a test receiver providing constellation plots as well as BER measures at various points along the demodulation chain. Demodulation was *quasi-error-free*, as required by the DVB-T standard, within the intelligible zones and totally impossible elsewhere. Signal quality parameters experienced within such two reception conditions are presented in Fig. 7. Instead, Fig. 8 shows a comparison between the received constellation plots from within both the intelligible zone and the interdicted zone.

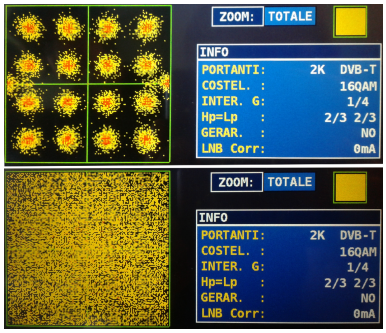


Fig. 8. Constellations received in intelligible zone (above) and interdicted zone (below).

4. CONCLUSIONS

This work proposes a generalization of the directional modulation concept being capable to overcome the main communication and security performance limits that restrain traditional DM techniques. Performance of the proposed approach was validated both by means of extensive numerical simulations, which show the high level of symbol equivocation in interdicted zones, and through a *fully functional*, *proof-of-concept*, *real-world* implementation of a DM-enabled DVB-T [7] transmitter. Such implementation demonstrates compatibility of the proposal with *state-of-art* radio transmission systems while also confirming theoretical analyses.

5. REFERENCES

[1] E. J. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Commun.*, vol. 38, no. 4, Apr. 1990.

[2] A. Babakhani, D. B. Rutledge, and A. Hajimiri, "Trasmitter architectures based on near-field direct antenna modulation," *IEEE J. Solid-State Circuits*, vol. 43, no. 12, Dec. 2008.

[3] M. P. Daly and J. T. Bernhard, "Directional modulation technique for phased array," *IEEE Trans. Antennas Propag.*, vol. 57, no. 9, May 2009.

[4] T. Hong, M. Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, 2011.

[5] M. P. Daly and J. T. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, July 2010.

[6] M. P. Daly, E. L. Daly, and J. T. Bernhard, "Demonstration of directional modulation using a phased array," *IEEE Trans. Antennas Propag.*, vol. 58, no. 5, Sept. 2010.

[7] ETSI, Sophia Antipolis, France, *Digital Video Broadcasting (DVB); Framing Structure, channel coding and modulation for digital terrestrial television*, Nov. 2004, EN 300 744 V1.5.1.

[8] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, Oct. 2010.

[9] 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, Mar. 2008.