Embedding security metadata into wireless communication signals using Polarization Shift Keying

Angelo Monti, Eric Alata, Daniela Dragomirescu

Embedding security metadata into wireless communication signals using Polarization Shift Keying

A. Monti✉, E. Alata and D. Dragomirescu

This Letter proposes a technique for embedding additional information into wireless communication signals by employing a secondary modulation, as a mean of conveying security data. We utilize polarized antennas coupled to an RF switch as a way of embedding data in a wireless frame, minimizing the impact on the received signal with a polarization-insensitive antenna, while an external receiver can retrieve both informations from the signal. We analyze the impact of the secondary modulation with respect to the Bit Error Rate (BER) for the original receiver, as a function of the relative rates of the two orthogonal modulations.

Introduction: Conventional communication systems use wireless channels between devices to transfer information, by employing a variety of modulation techniques and networking protocols. Security mechanisms are usually introduced by modifying the aforementioned protocols, while Physical Layer Security is an emerging research topic. Besides encryption techniques aiming to ensure the privacy of wireless exchanges, a critical aspect of Physical Layer Security is message authentication, allowing a receiver to associate a received message with a trusted identity [1].

To our knowledge, mainstream physical authentication solutions are implemented either by modifying modulation schemes or lower layers of the communication protocols, such as the Medium Access Control (MAC) layer, or by gathering features of a received signal and combining them to obtain a unique signature [2]. The first approach leads to solutions that are difficult to deploy on existing systems, expensive and specific to a wireless standard or application, while the second method also requires expensive components in order for capturing fine details of received signals. Moreover, the latter assumes such unique features are not erased by the noisy communication channel.

We propose, as a basis for implementing physical message authentication, to modify existing wireless systems in a reasonable way, minimizing software and hardware alterations. Further reduction of the complexity of our solution is achieved by moving the authentication intelligence from each receiving devices of the network to a single new dedicated device denoted thereafter as the *monitor*. Such extrinsic approach to Physical Layer Security provides greater adaptability to a wide range of wireless communication protocols and hardware, thus minimizing integration complexity and increasing the cost-effectiveness of the overall system.

Additional information, which we denote further as *metadata*, is embedded into messages using the polarization state of electromagnetic waves. Exploiting unused properties of the communication channel such as the polarization state of waves allows to transmit metadata without occupying supplementary time or bandwidth, therefore no modification of the MAC layer is needed. Polarization Shift Keying has been used in optical fields and recently theorized for wireless communication [3], where bits are mapped to different polarization states that can be retrieved using multiple polarized antennas. To our knowledge, it has only been used on Continuous Wave (CW) signals carrying no information in the frequency domain. This Letter proposes to apply Polarization Shift Keying on the conventionally modulated signals produced by emitting devices to be authenticated.

First, we shall present the operating principle of the proposed architecture, in which we then identify impairment sources and their origin. We subsequently present evaluation results and conclude on further work.

Principle of operation: The proposed system architecture is depicted on Fig. 1. Dashed boxes represents elements from the original wireless system (Fig. 1.*a*) which are not altered. The modified system is represented on Fig. 1.*b*, where the antenna of the emitter is replaced with an active antenna system performing Polarization Shift Keying in order to embed additional metadata into the emitted electromagnetic wave. As the emitted wave is modulated twice, we shall thereafter denote the modulation performed by the emitter as the *primary modulation* and the Polarization Shift Keying as the *secondary modulation*.

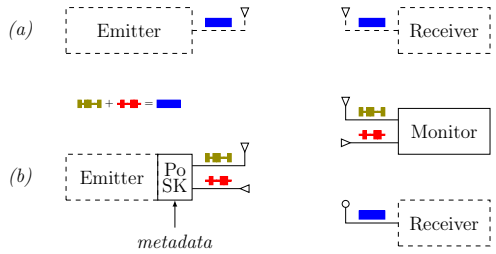

Fig. 1 *(a) Original wireless system. (b) Wireless system with additional metadata encoded using Polarization Shift Keying (PoSK).*

As a first prototype, we propose to use a dual linearly polarized antenna [4] providing two discrete polarization states (denoted as horizontal and vertical), and represented on Fig. 1 as orthogonal antenna pairs. Polarization Shift Keying is implemented using an RF switch swappig the output port of the emitter between the two ports of the polarized antenna.

In order to minimize the impact of the secondary modulation on the receiver, its antenna is changed for a circularly polarized antenna providing insensitivity to the direction of polarization of the received electromagnetic wave. To illustrate the working principle, each antenna on Fig. 1 is labelled with a simple signal depiction. The blue bar represents the primarily modulated signal, while the red and green items symbolize the components obtained after applying the secondary modulation. Using a second dual linearly polarized antenna, the monitor device is able to decode the metadata encoded into the incident wave, provided the mutual orientation of the emitting and receiving antennas is not 45 degrees.

Software Defined Radio (SDR) equipments were used to implement the original emitter and receiver, facilitating instrumentation and modification of the primary modulation scheme. Experiments were all run with a carrier frequency of 2.45 GHz, as it lies in the free Industrial, Scientific and Medical (ISM) band and broadly used among the wireless ecosystem.

Received signal impairments: The proposed technique should minimize impairments incured to the signal seen by the original receiver, in order for the system to be integrated transparently. Two different types of signal distortions can be introduced by the secondary modulation. First, the switching time of the RF switch always being nonzero, transient-related distortions are applied to the primarily modulated signal, leading to additional noise and synchronization difficulties on the receiver side. The switch transient can be observed in Fig. 2, depicting the Root Mean Square (RMS) envelopes of a Continuous Wave (CW) signal whose polarization is switched, as seen by the original receiver equipped with a circularly polarized antenna. At each polarization state change, the received signal is strongly impaired during the switch transient, whose duration is determined by hardware characteristics of the RF switch.

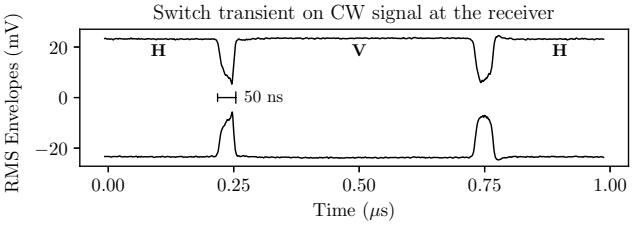

Fig. 2 *The switch transient as seen by the original receiver for a continuous wave, switched from horizontal (**H**) to vertical (**V**) polarization and back*

A second type of distortion is introduced due to antenna imperfections, leading to unequal gains in the polarized channel. Such gain variations can be explained either by uneven transmission coefficients of the ports of the keying antenna or by the receiving antenna being slighly elliptically polarized. Such effect can be observed on Fig. 3, featuring both transient impairments and exaggerated polarization sensitivity. In complex environments, electromagnetic effects such as reflexions or

multipath may either be polarization-dependent or alter the polarization state of waves, and thus would also induce improper balancing of the received signal.

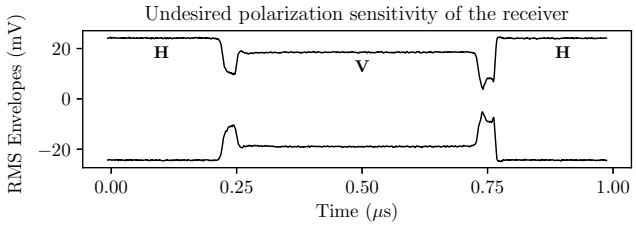

Fig. 3 *An exaggerated depiction of the distortion introduced by an improperly balanced polarized channel*

Performance study: We have studied the effect of such distortions through the Bit Error Rate (BER) at the original receiver for different symbol rates of Binary Phase Shift Keying (BPSK) and Quadrature Phase Shift Keying (QPSK) as primary modulation schemes. The BER of the modified wireless system was estimated by sending 4096 -bytes frames consisting of a maximum length Pseudo Random Binary Sequence (PRBS). Synchronization is achieved at the receiver side using a portion of the frame as a preamble, while the number of bit errors is continuously counted. Averaging the proportion of bit errors per frame provides us with an estimate of the BER introduced by the Polarization Shift Keying.

As to obtain a worst-case evaluation, the polarization of the transmitted wave is continuously switched at a rate denoted thereafter as the *keying frequency* (F_k), maximizing the number of distortions applied to the received signal. Indeed, when using a proper secondary modulation scheme encoding metadata, distortions would be applied to the signal less often. The study of the BER with respect to this parameter appears to us of utter interest as it determines the allowable rates for the secondary modulation. The obtained measurements for a differential BPSK primary modulation scheme are represented on Fig. 4, where we clearly observe two distinct behaviors separated by a sharp discontinuity, located at the *critical keying frequency*, which we denote as F_c.

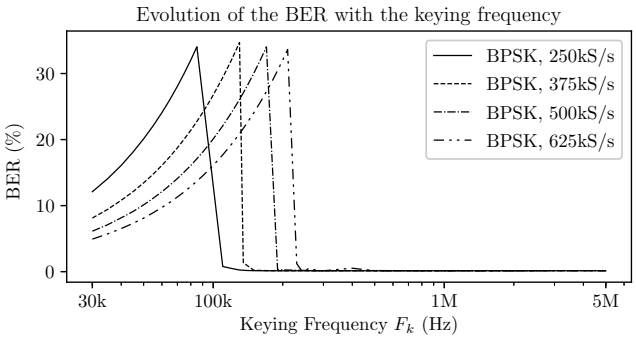

Fig. 4 *The BER as a function of keying frequency, for several rates of BPSK (rates in symbols per second)*

When $F_k < F_c$, the BER displays a linear evolution with respect to the keying frequency, furthermore its absolute value scores several percents. On the other hand, when F_k exceeds the critical keying frequency, the BER estimate suddenly drops to values less than 200 ppm and does not show any further dependence on the keying frequency. It has been determined empirically that the critical keying frequency is of the same order of magnitude as half of the primary symbol rate, corresponding to the case where a single distortion is applied at every symbol. Optimal operation of the system can then be achieved by choosing a secondary keying frequency much greater than the primary modulation rate. This result demonstrates the validity of our proposition, but also leads us to its key limitation. Indeed, the maximum keying frequency is determined by the RF switch itself, thus limiting the range of applicable systems to those whose symbol rate is small enough.

It should be noted that keying frequencies greater than the primary symbol rate allows us to encode large amounts of metadata, that is a quantity comparable to the authenticated message, providing sufficient room to implement cryptographic authentication methods. We shall also mention that the obtained results vary depending on the receiver's architecture as, given a primary modulation scheme, more advanced receivers will obviously be more resilient to signal impairments. As we used a trivial receiver architecture in our experiments, we expect results to improve for commercial or state-of-the-art communication systems.

Conclusion and future work: We proposed a generic architecture allowing additional metadata to be transmitted alongside an already modulated wireless communication signal, as a basis for implementing physical message authentication following an extrinsic approach, that is with reasonable modifications of the system to be secured. Using an RF switch followed by a dual linearly polarized antenna, a secondary modulation is introduced and used to transmit security-related signals, leaving the intended receiver nearly unaffected owing to its circularly polarized receiving antenna. The effect of the secondary modulation has been studied in the light of the introduced Bit Error Rate, and constraints on the secondary modulation has been empirically found to ensure proper functionning of the system.

While offering sufficient bit rates to implement cryptographic authentication algorithms, the main advantage of the proposed technique lies in the fact that it does not require any software-level modification of the devices. Indeed, no spurious transmissions are introduced, neither on other frequency bands nor outside message boundaries managed by the MAC layer.

Future work shall cover effects on frequency-based modulations and go toward the reduction of transient-related distortions. Moreover, efforts will be put into devising a proper secondary modulation scheme allowing further minimization of the Bit Error Rate, as well as on miniaturization of the overall system.

Acknowledgment: This work has been supported by Continental ITS France

A. Monti (*Continental ITS France and LAAS-CNRS, University of Toulouse, CNRS, Toulouse, France*), E. Alata and D. Dragomirescu (*LAAS-CNRS, University of Toulouse, CNRS, INSA, Toulouse, France*)

E-mail: amonti@laas.fr

References

1 Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L.: 'Principles of physical layer security in multiuser wireless networks: A survey', *IEEE Communications Surveys & Tutorials*, 2014, **16(3)**, pp. 1550-1573

2 Liu, Y., Chen, H. H., & Wang, L.: 'Physical layer security for next generation wireless networks: Theories, technologies, and challenges', *IEEE Communications Surveys & Tutorials*, 2017, **19(1)**, pp. 347-376

3 Zhang, J., Wang, Y., Zhang, J., & Ding, L.: 'Polarization Shift Keying (PolarSK): System Scheme and Performance Analysis', *IEEE Transactions on Vehicular Technology*, 2017, **66(11)**, pp. 10139-10155

4 Li, Y., Zhang, Z., Chen, W., Feng, Z., & Iskander, M. F.: 'A dual-polarization slot antenna using a compact CPW feeding structure', 2010, *IEEE Antennas and Wireless Propagation Letters*, **9**, pp. 191-194.