Circular Polarization Shift Keying for IoT Communications Security: A Proof of Concept

Lamoussa Sanogo, Eric Alata, Gaël Loubet, Taki E Djidjekh, Alexandru Takacs, Daniela Dragomirescu

Circular Polarization Shift Keying for IoT Communications Security: A Proof of Concept

Lamoussa SANOGO
LAAS-CNRS
Université de Toulouse, CNRS
Toulouse, France
lamoussa.sanogo@laas.fr

Eric ALATA
LAAS-CNRS
Université de Toulouse, CNRS, INSA
Toulouse, France
eric.alata@laas.fr

Gaël LOUBET
LAAS-CNRS
Université de Toulouse, CNRS, INSA
Toulouse, France
gael.loubet@laas.fr

Taki E. DJIDJEKH
LAAS-CNRS
Université de Toulouse, CNRS
Toulouse, France
taki-eddine.djidjekh@laas.fr

Alexandru TAKACS
LAAS-CNRS
Université de Toulouse, CNRS, UPS
Toulouse, France
alexandru.takacs@laas.fr

Daniela DRAGOMIRESCU
LAAS-CNRS
Université de Toulouse, CNRS, INSA
Toulouse, France
daniela.dragomirescu@laas.fr

***Abstract*—Considering the limitations of the IoT security solutions proposed in the literature, *e.g.*, fingerprinting based on intrinsic properties is hampered by physical environmental phenomena and wireless channel's dynamic, a new security technique for message authentication in IoT is proposed in this paper. This technique, based on Polarization Shift Keying, consists in using the polarization of the radio wave emitted by a device as a means of transmitting, in parallel with the main message, authentication data for this main message. Basically, this means cryptographically controlled modification of the polarization of the emitter outgoing wave. This is a kind of second modulation of the wave where the different used polarizations denote the symbols of this second modulation. Then, a security gateway is able to retrieve these symbols and recover the authentication code. This creates a secure communication link between the two terminals at the physical layer. The Polarization Shift Keying mechanism should not alter the original waveform and its primary modulation enough to increase the Bit Error Rate. After promising results with linear polarizations, this paper presents a proof-of-concept on the use of circular polarizations to perform Polarization Shift Keying.**

Keywords—Active Antenna System (AAS), Authentication, Circular Polarization, Internet of Things (IoT), Polarization Shift Keying (PoSK), Security.

I. INTRODUCTION

The resource-constrained nature of IoT devices makes their security challenging, as security solutions need to be not only efficient, but also lightweight in terms of memory footprint, low computational complexity and protocol-independent to be able to offer an authentication solution to many protocols in IoT. It is still difficult to find a solution in the literature that meets aforementioned requirements. For instance, in [1], a lightweight Intrusion Detection System (IDS) against IoT memory corruption attacks is presented. Very interesting results are achieved with a detection accuracy of 99.98%, but this approach is not protocol-independent.

Authentication by fingerprinting, based on device inherent properties, is also very popular in the literature. Also, this approach is limited by the electronic devices non-stability regarding environment and by the dynamic nature of the transmission channel, as illustrated in [2] where it is demonstrated that different devices can produce same Power Spectral Density (PSD) and a same device can produce different PSDs. In [3], electronic devices instability regarding environmental parameters is illustrated; multiple transmitters are emulated with the same physical device by changing the temperature of the experimental closed environment.

In this paper, a new lightweight, protocol-independent, non- invasive and dynamic authentication solution based on Polarization Shift Keying (PoSK) is proposed. Polarization Shift Keying is a well-known technique in optical communications [4;5], where optical modulators capable of operating at tens of Gbps have been developed [6]. On the other hand, the use of PoSK in radiocommunications is more recent. In December 2004, a patent entitled "Polarization state techniques for wireless communications" has been published [7]. In the literature, there are more recent paper about PoSK. In [8], the PoSK is employed for satellite communications. In [9], fundamental properties of PoSK are investigated in wireless channels subject to fading, with a particular interest in Rayleigh and Rician fading channels. To the best of our knowledge, this is the first time PoSK is proposed for radiocommunications security purposes.

II. CIRCULAR POSK-BASED SECURITY

A. Presentation

Fig. 1 shows an architecture for circular PoSK-based security. In Fig. 2, two other possible configurations for the security gateway are proposed; the main difference between these three configurations of the security gateway lies in the way authentication is performed.

In the PoSK-based security architecture, the standard antenna of a wireless sensor node is replaced by an Active Antenna System (AAS). An AAS refers to a set of antennas providing multiple polarizations controlled by a polarization selector through a router. Here, it is a single antenna with two ports, instead of a set of antennas, that is used to perform the circular Polarization Shift Keying.

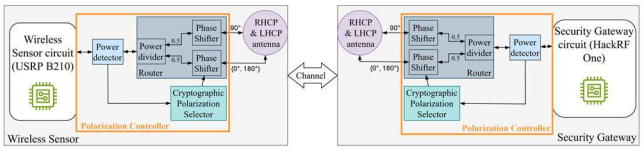
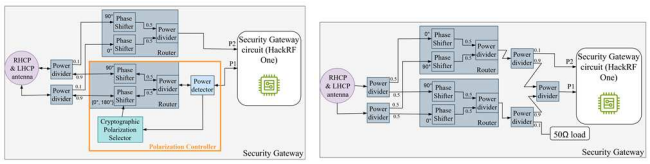


Fig. 1. Circular PoSK-based security architecture.



(a) (b)

Fig. 2. Two other possible configurations for the security gateway.

By introducing a 90° phase shift on one of its two ports, this antenna radiates in Right-Hand Circular Polarization (RHCP) mode; by introducing the phase shift on the other port, it radiates in Left-Hand Circular Polarization (LHCP) mode. Therefore, the router is made up of phase shifters.

Thus, polarization shift keying can be performed. The cryptographic polarization selector dynamically controls the phase shift between the two ports of the antenna following a cryptographic algorithm, e.g., AES. This control is triggered by the detection of a radio-frequency power indicating the beginning of a transmission.

The two terminals share a primitive secret cryptographic key. The ultimate goal would be to have the whole polarization controller and the antenna on a single compact integrated circuit, which is definitely possible nowadays.

B. Authentication Process

The security gateway can be configured in three different ways depending on how authentication is carried out. In all cases, the authentication is based on the instantaneous power. Let X and Y be the polarizations used in the PoSK. Generally speaking, at a time t, the received power $P_{XX}(t)$ or $P_{YY}(t)$ in a co-polarization X to X or Y to Y transmission will be higher than the received power $P_{XY}(t)$ or $P_{YX}(t)$ in a cross-polarization X to Y or Y to X transmission, as summarized by the following relation:

$$P_{XX}(t) \approx P_{YY}(t) \gg P_{XY}(t) \approx P_{YX}(t) \qquad (1)$$

It is recommended that polarizations X and Y corresponding antennas be as similar as possible (gain, radiation pattern).

In this work, the polarizations used are RHCP and LHCP, both performed with the same antenna. Relation (1) is very theoretical, but authentication process can be as simple as that for the time being because, in our experiments, the channel between the wireless sensor and the security gateway was Line-Of-Sight (LOS) and the experiments were carried out in an uncluttered environment to reduce multipath. In future work, this authentication approach will be studied more in-depth in order to establish a generalized relation based on solid mathematical foundations.

So, in the configuration shown in Fig. 1, the security gateway and the wireless sensor must be on the same polarization at each time t, this requires a synchronization between the two cryptographic polarization selectors. This approach allows the security gateway to guarantee that the received signal really does come from the expected wireless sensor, since both terminals have been synchronized with the same secret key and are following the same cryptographic algorithm, consequently the received power is theoretically constant. This solution requires a very precise synchronization, which is challenging in the IoT context.

The security gateway configuration shown in Fig. 2 (a) uses a second port (P2) to retrieve the authentication code by listening on only one of the two polarizations. In this configuration, synchronization can be omitted when the security gateway is a receiver. The main message is received on port P1 and the authentication code on port P2.

Finally, in the configuration shown in Fig. 2 (b), the security gateway is designed to be used for reception only. The authentication code is retrieved by listening on only one of the two polarizations; in this configuration, it is obtained through port P2. The main message is received on port P1. Synchronization is no longer necessary in this configuration.

In the two configurations shown in Fig. 2, authentication code recovery is based on the following assumption: when listening on only one of the two polarizations, let's assume it is polarization X, the power received on the authentication port is then higher when the wireless sensor transmits on this polarization X than when it transmits on polarization Y.

So, the profile of the instantaneous power received on the authentication port reveals the PoSK authentication code used by the wireless sensor when it was sending the message. The security gateway knows the expected code because it is running the same cryptographic algorithm as the wireless sensor, with the same shared secret key. The security gateway then compares the received code with the expected one, and the message is validated as authentic if the two codes are the same. A dynamic authentication system for messages is made.

C. Synchronization

When synchronization is required, empiric relations (2) and (3) are proposed, which allow not only synchronization, but also prevent some important events, *e.g.*, phase shifts in the Phase Shift Keying (PSK) modulation, from occurring during the polarization switching time, the objective is to avoid missing such important events, and thus avoid a significant increase of the Bit Error Rate (BER) due to PoSK.

$$F_{PoSK}(n) = 2^n F_s \, , n \in \mathbb{Z} \qquad (2)$$

$$\varphi(k) = \frac{1}{4 * F_{PoSK}} + \frac{k}{2 * F_{PoSK}} = \left(\frac{1 + 2k}{4 * F_{PoSK}}\right), k \in \mathbb{N} \qquad (3)$$

Where F_{PoSK} is the cryptographic polarization selector output rate, F_s is the main message symbol rate, and φ is a time offset between F_{PoSK} and F_s, *i.e.*, the beginning of the PoSK relative to the beginning of the transmission.

III. EXPERIMENTATION

To prove that the authentication method can work under our experimental conditions, relation (1) has to be verified experimentally. Fig. 3 shows the experimental setup. In this work, an USRP B210 was used as sensor circuit and two HackRFs One [10] were used as security gateway circuit. An Arduino board was used as cryptographic polarization selector and the router is made up of a power divider and the evaluation boards of Analog Devices HMC647ALP6E phase shifter. The power detector is custom-made, based on the Linear Technology's LTC5536 Precision RF Detector. For transmissions, Universal Radio Hacker (URH) [11] was used; the received signal is then recorded in complex IQ format in a binary file. For demodulation, GNU Radio [12] flowgraphs were developed, as URH has limited demodulation performance.

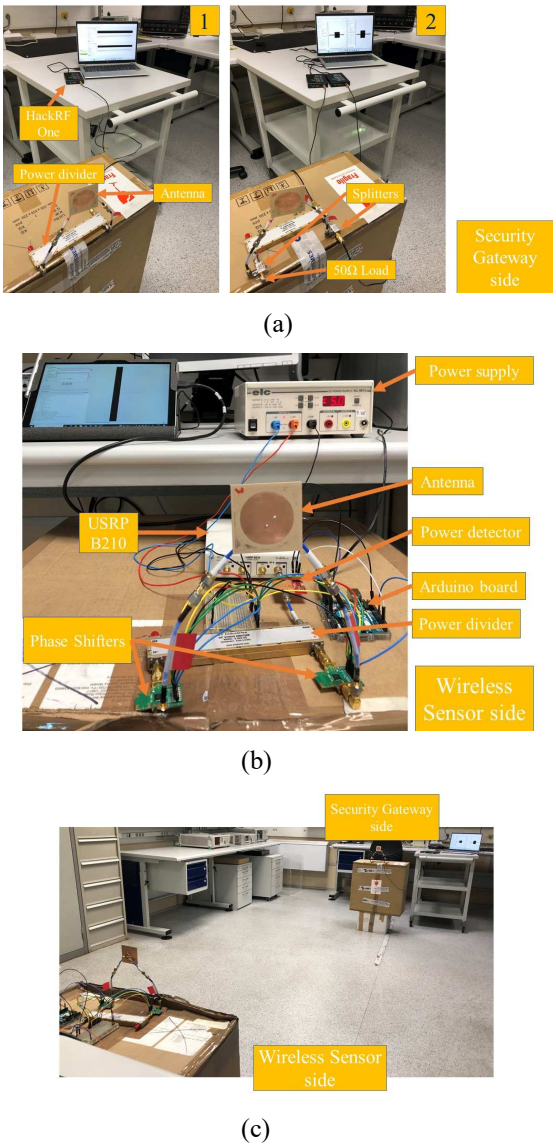


Fig. 3. Circular PoSK-based security experimental setup. (a): the security gateway side, the authentication signal is taken after the power divider in image labelled 1 and before the power divider in image labelled 2; (b): the wireless sensor side; (c): a view of the whole setup.

IV. RESULTS AND DISCUSSION

Co-polarization, cross-polarization and PoSK transmissions were carried out. Some received signals and their powers are shown in Fig. 4. In the case of Fig. 4 (c), the authentication signal was taken after the divider (see Fig. 3 (a) image labelled 1); it can be seen that the power gap between RHCP and LHCP is small. This may be due to the phase shifters used, which are not designed for use at 2.45 GHz but have acceptable characteristics at this frequency. Future work will investigate the phase shifters as well as the antenna in order to improve this power gap. Nevertheless, when the authentication signal is taken on only one of the antenna ports before the divider (see Fig. 3 (a) image labelled 2), a much larger gap is obtained, as shown in Fig. 4 (d). It can be seen on Fig. 4 (c) and Fig. 4 (d) that the instantaneous power of the authentication signal clearly reveals the PoSK code used by the wireless sensor when it was sending this message. In this experimental context, a simple Linear Feedback Shift Register (LFSR) was used as a preliminary cryptographic algorithm for its ease of implementation.

Fig. 5 shows the architecture of the used LFSR algorithm. This algorithm is implemented on the Arduino board that serves as cryptographic polarization selector, *i.e.*, while the wireless sensor is transmitting, the Arduino board dynamically changes the transmission mode (polarization), switching between LHCP and RHCP according to the LFSR algorithm output: the transmission is performed in LHCP polarization at 0 and in RHCP polarization at 1, or vice versa. The Arduino board performs this task by controlling the output phase of one of the phase shifters in such a way as to create -90° or +90° phase shift between the two ports of the antenna, -90° for LHCP and +90° for RHCP. By listening on one of the two polarizations, LHCP or RHCP, the security gateway can retrieve the authentication code (the LFSR output shown in Fig. 5) from the instantaneous power, as relation (1) forecasts this possibility.

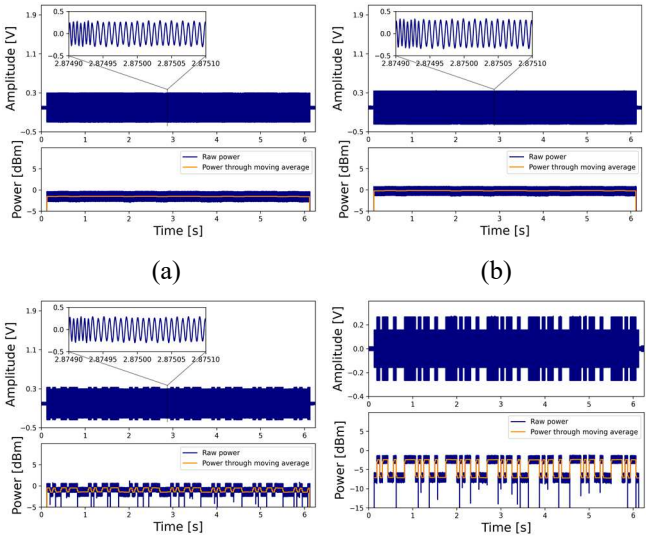


Fig. 4. Some received signals and their instantaneous powers. (a): cross-polarization transmission; (b): co-polarization transmission; (c) (d): PoSK transmissions.

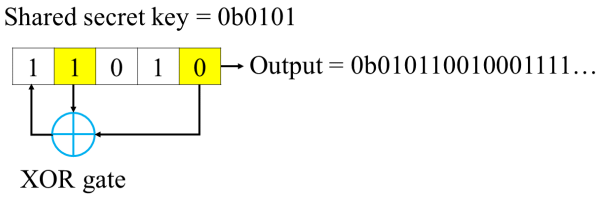


Fig. 5. Architecture of the LFSR used in this experimentation.

It can be seen that the LFSR output shown in Fig. 5 is indeed the one repeating in the authentication signal power profile shown in Fig. 4 (d). The code is inverted in Fig. 4 (c) and this is normal, it just depends on the polarization used for authentication. Differential coding allows to avoid the need for a shared reference.

In order to make accurate measurements and do precise interpretations, PoSK was experimented at very low frequency first. So, F_S=*4 baud* was chosen as the main message symbol rate, that is 4 bits per second for our 2-symbol modulations; F_{PoSK}=*16 Hz* was chosen as the cryptographic polarization selector output rate, *i.e.*, the bit rate of the authentication code. The primary modulation was 64 kHz / 128 kHz Frequency Shift Keying (FSK). Using GNU Radio, the main message can be successfully demodulated and bits can be error-free recovered easily by a simple binary slicing.

It can be seen on Fig. 4 (c) and Fig. 4 (d) that the PoSK mechanism introduces some brief sharp drops in the signal. These drops are due to the time it takes a phase shifter to update its output when switching from one state to another. During this switching time, the polarization controller of the wireless sensor is in an undefined state and there is no transmission, which leads to a power break at the security gateway, thus causing these fluctuations. The higher the polarization change frequency, the greater its impact on the signal. Fortunately, one can get rid of these fluctuations by filtering using a low-pass filter with a cut-off frequency at least twice the symbol rate (F_S). More the duration of a modulation symbol is higher than the duration of the phase switching time, *i.e.*, the duration of a power drop, the more efficient the filtering. This filtering mitigates the impact of PoSK on the signal and reduces the risk of bit errors.

It is important not to forget handling these power brief sharp drops in the authentication, otherwise one will end up with several false positives.

On the other hand, for F_{PoSK}, very high values in the megahertz range are not only unnecessary, but also increase power consumption in an environment where energy is already scarce.

V. Conclusion

This work represents a proof-of-concept for the use of circular polarizations in PoSK to secure radiocommunications without need for major modifications on the device. PoSK did not degrade the radio-frequency signal enough to cause bit errors and do not impede error-free recovery of the main message in these standard modulations.

It was demonstrated that the wireless sensor authentication is possible *via* the instantaneous power. The impact PoSK could have on the signal was also outlined and filtering is proposed as one of the techniques for overcoming the undesirable effects introduced by the PoSK.

Just as the frequency hopping mechanism has enhanced the security of some protocols such as Bluetooth, PoSK, which is a kind of polarization hopping mechanism, could enhance the security of radiocommunications regardless of protocols. Moreover, as PoSK is low energy mechanism it is suitable for Internet of Things resource-constrained devices.

Nevertheless, there is still a lot of work to be carried out on this approach, such as the assessment of its resilience to noise and multipath; more in-depth investigations on its potential impact on the Bit Error Rate (BER) have to be carried out; also, it has to be experimented with more powerful cryptographic algorithm, *e.g.*, AES.

References

[1] M. E. Bouazzati, R. Tessier, P. Tanguy and G. Gogniat, "A Lightweight Intrusion Detection System against IoT Memory Corruption Attacks," 2023 *26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, Tallinn, Estonia, 2023, pp. 118-123, doi: 10.1109/DDECS57882.2023.10139718.

[2] L. Sanogo, E. Alata, A. Takacs, and D. Dragomirescu, "Intrusion Detection System for IoT: Analysis of PSD Robustness," *Sensors* 2023, vol. 23, p. 2353, doi: 10.3390/s23042353.

[3] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," *IEEE Internet Things Journal* 2019, vol. 6, pp. 388–398, doi: 10.1109/JIOT.2018.2849324.

[4] S. Benedetto, and P. Poggiolini, "Theory of polarization shift keying modulation," *IEEE Transactions on Communications*, vol. 40, no. 4, pp. 708-721, April 1992, doi: 10.1109/26.141426.

[5] S. Benedetto, and P. T. Poggiolini, "Multilevel polarization shift keying: optimum receiver structure and performance evaluation," *IEEE Transactions on Communications*, vol. 42, no. 234, pp. 1174-1186, February-April 1994, doi: 10.1109/TCOMM.1994.580226.

[6] Available online: https://www.versawave.ca/polarization-modulators/ (accessed on June 2024).

[7] S. Sibecas, C. A. Corral, S. Emami, G. Stratis, and G. Rasor, "Polarization state techniques for wireless communications," *U.S. patent 2004 0 264 592 A1*, Dec. 30, 2004.

[8] L. Arend, R. Sperber, M. Marso and J. Krause, "Polarization shift keying over satellite - Implementation and demonstration in Ku-band," 2014 *7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASMS/SPSC)*, Livorno, Italy, 2014, pp. 165-169, doi: 10.1109/ASMS-SPSC.2014.6934539.

[9] X. Wu, T. G. Pratt, and T. E. Fuja, "Polarization signaling for wireless Communication." 2016 I*EEE International Conference on Communications (ICC)*, pp. 1-6.

[10] Available online: https://greatscottgadgets.com/hackrf/one/ (accessed on June 2024).

[11] Available online: https://github.com/jopohl/urh (accessed on June 2024).

[12] Available online: https://www.gnuradio.org/ (accessed on June 2024).