A Hardware Add-On for IoT Secure Communications: Polarization Shift Keying Smart Antenna System

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

A Hardware Add-On for IoT Secure Communications: Polarization Shift Keying Smart Antenna System

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*—Internet of Things security still remains a major concern. In the literature, the security approaches are subject to various limitations. For example, fingerprinting based on intrinsic properties is hampered by physical environmental phenomena and wireless channel's dynamic. In this paper, a new security technique for message authentication in IoT is proposed. This proposed 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. In this work, Polarization Shift Keying using two polarizations (Binary-PoSK) is experimented, along with different primary modulations. The results show that this technique could be a way of achieving secure communications in Internet of Things where devices are resource-constrained.**

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

I. INTRODUCTION

Internet of Things (IoT) devices are increasingly present in all areas of our society, while their resource-constrained nature continues to make their security challenging. Indeed, the targeted 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. Although the literature is becoming more and more rich, with a significant number of papers on authentication and intrusion detection, it is still difficult to find a solution that meets aforementioned requirements. For instance, in [1], Bouazzati et al. present a lightweight Intrusion Detection System (IDS) against IoT memory corruption attacks. They achieved very interesting results with a detection accuracy of 99.98%, but their solution is not protocol-independent.

When it comes to device authentication, the most explored approach is fingerprinting, which aims to associate a unique and constant signature with a given device, based on inherent imperfections of that device. Also, this approach is limited by several challenges, such as: (1)- the advances in manufacturing processes, which reduce more and more device imperfections; (2)- the electronic devices non-stability regarding environment and (3)- the dynamic nature of the transmission channel, as illustrated in [2] where Sanogo et al. show that different devices can produce same Power Spectral Density (PSD) and a same device can produce different PSDs. Also, in [3], Chatterjee et al. illustrated electronic devices instability regarding environmental parameters. Indeed, changing the temperature of their experimental closed environment in discrete steps of 5 °C in the range of 0 °C – 25 °C modified the transmitter properties, and the receiver (or "fingerprinter") considered every 5 °C change in the temperature as a different transmitter.

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 radio-communications is more recent. In December 2004, Sibecas et al. published the patent "US 2004/0264592 A1" entitled "Polarization state

techniques for wireless communications" [7]. More recent papers about PoSK can be found in the literature. In [8], Arend et al. deal with the use of PoSK in satellite communications. In [9], Wu et al. investigated fundamental properties of PoSK in wireless channels subject to fading, with a particular interest in Rayleigh and Rician fading channels. To the best of our knowledge, this work is the first proposition of PoSK for radiocommunications security. The principle consists in dynamically controlling the polarization of the radio-frequency (RF) wave during its emission. The polarization change pattern is based on a cryptographic algorithm. Then, the receiver needs to retrieve this cryptographic code to authenticate the received message.

II. PoSK-based Security

A. Presentation and Experimental Setup

Fig. 1 shows the architecture for PoSK-based security. In this architecture, the "Wireless Sensor Node" standard antenna is replaced by an Active Antenna System (AAS), a set of antennas providing multiple polarizations controlled by a "Cryptographic Polarization Selector" through a "Router", which is a switch in this work. In this way, polarization shift keying can be performed. The "Cryptographic Polarization Selector" dynamically controls the polarization of the outgoing RF signal following a cryptographic algorithm, *e.g.*, AES. This control is triggered by the detection of a RF power indicating the beginning of a transmission. The two terminals share a primitive secret cryptographic key. The ultimate goal would be to have all the elements within a dashed rectangle (see Fig. 1) on a single compact integrated circuit, which is definitely possible nowadays.

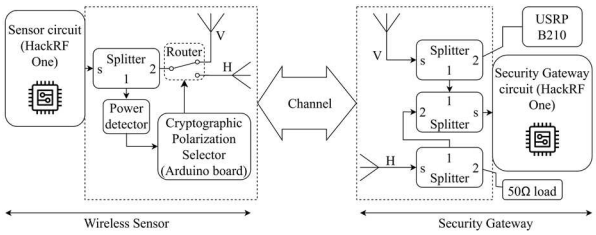


Fig. 1. A PoSK-based security architecture.

Fig. 2 shows the experimental setup. In this work, HackRF Ones [10] are used as "Sensor circuit" and "Security Gateway circuit". An Arduino board is used as "Cryptographic Polarization Selector" and the "Router" is a custom-made switch based on the Analog Device's AD8137 Low Power Differential ADC Driver. The power detector, also custom-made, is based on the Linear Technology's LTC5536 Precision RF Detector. For the recovery of the cryptographic authentication code, another Software-Defined Radio (SDR) device, the B210 Universal Software Radio Peripheral (USRP), is used. Actually, this device fulfills the role of the security gateway's second port. If the "Security Gateway circuit", the HackRF One, had at least two ports, the USRP B210 would not be necessary.

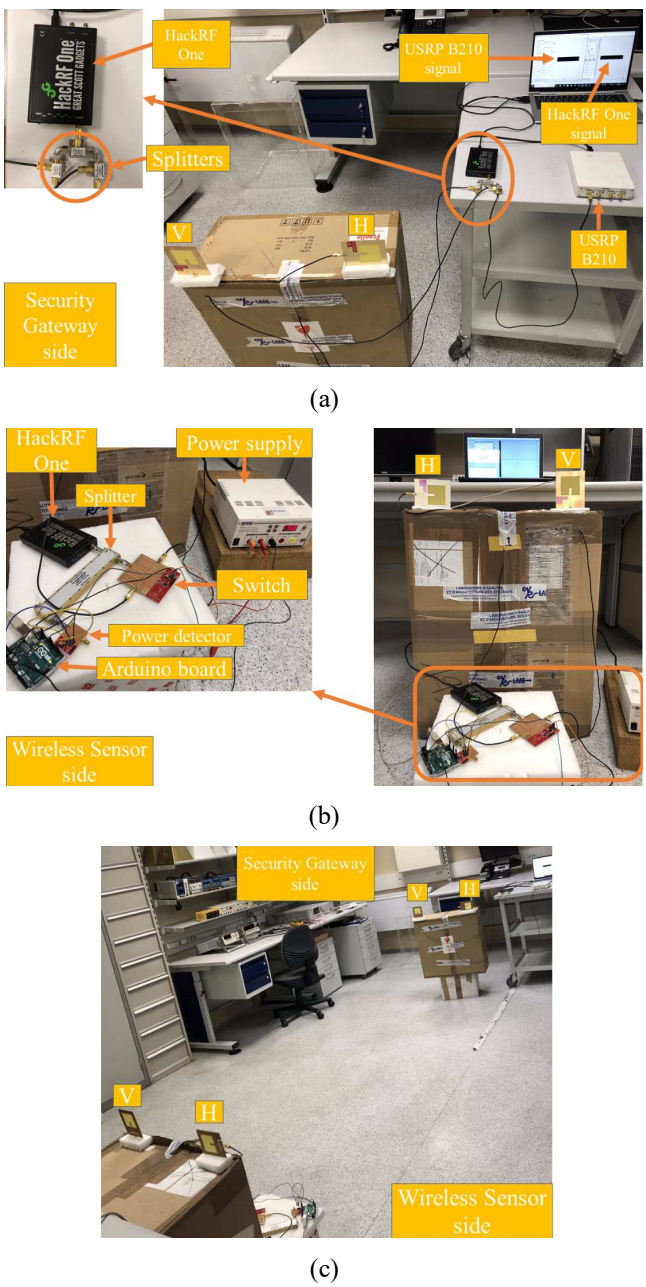


Fig. 2. PoSK-based security experimental setup. (a): the 'Security Gateway' side; (b): the 'Wireless Sensor' side'; (c): the whole setup.

The polarizations used in PoSK represent the symbols of this modulation. With the right "Router", it is possible to use either linear or circular polarizations. For example, a switch-type router can be used for linear polarizations, as in this work. For circular polarizations, a router made of power divider and phase shifters could be used.

For transmissions, Universal Radio Hacker (URH) is used [11]; the received signal is then recorded in complex IQ format in a binary file.

For demodulation, a GNU Radio [12] flowgraph is developed, as URH has limited demodulation performances.

B. *Authentication Process*

The authentication is based on instantaneous power. Let X and Y be the polarizations used in the PoSK. The "Security Gateway" port dedicated to authentication, the USRP B210 in this work, is receiving on only one of the polarizations, assume that it is polarization X. Therefore, the power received on the authentication port is then higher when the transmitter transmits on this polarization X than when the transmitter transmits on polarization Y. 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:

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

It is recommended that polarizations X and Y be as similar as possible.

So, the profile of the instantaneous power received on the authentication port reveals the PoSK authentication code used by the transmitter when it sent the message. The "Security Gateway" knows the expected code because it is running the same cryptographic algorithm as the transmitter, 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. Thus, a dynamic authentication system for messages is provided.

III. Experimental Results And Discussion

A. *Main Message recovering*

In the experimental setup, the main message with its primary modulation is the signal received on the HackRF One, which is the "Security Gateway" port dedicated to the main message. The possibility of recovering this main message despite the PoSK mechanism is therefore investigated. In order to make accurate measurements and do precise interpretations, the PoSK has been experimented at a very low frequency first. So, $F_S = 4$ baud is chosen as the main message symbol rate, that is 4 bits per second for our 2-symbol modulations; $F_{PoSK} = 16$ Hz is the "Cryptographic Polarization Selector" output rate, *i.e.*, the bit rate of the authentication code. The 50% / 100% Amplitude Shift Keying (ASK), 64 kHz / 128 kHz Frequency Shift Keying (FSK) and -90° / +90° Phase Shift Keying (PSK) are experienced, as shown in Fig. 3. In the three cases, (a), (b) and (c) of Fig. 3, the top graph is the modulated signal and the bottom graph is its demodulation. To reduce the risk of bit errors, the demodulated signals have been filtered with a low-pass filter with a cut-off frequency (32 Hz) at least twice the symbol rate (F_S). This filtering mitigates the impact of PoSK on the signal. Indeed, the PoSK mechanism introduces some brief sharp drops in the signal, the cause of these drops is explained in more detail later in the paper.

From the demodulated and filtered signals, one can easily recover the message by a simple binary slicing. In this case, the message is the hexadecimal sequence 0xa12345. So, in this experiment, the PoSK did not degrade the RF signal enough to cause bit errors and do not impede error-free recovery of

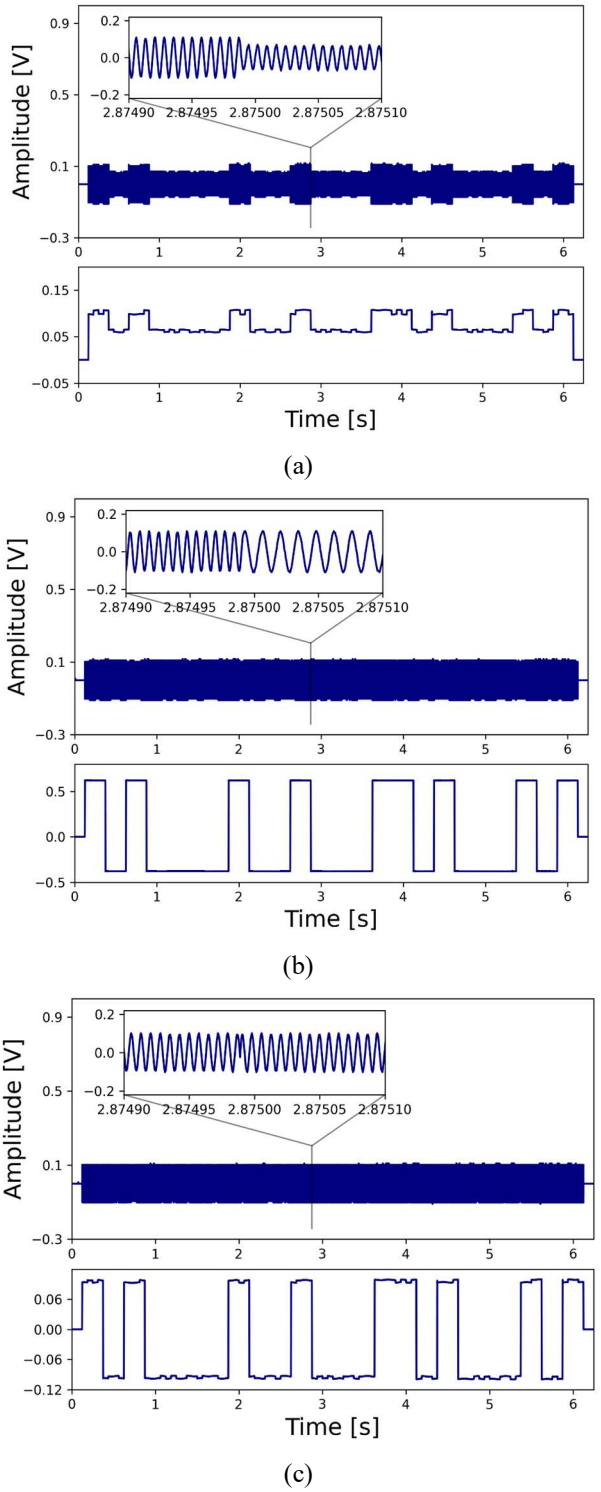


Fig. 3. Messages received by the 'Security Gateway' coming from the 'Wireless Sensor Node'. (a): 50% / 100% ASK; (b): 64 kHz / 128 kHz FSK; (c): -90° / 90° PSK.

the main message. After this experiment where a very low PoSK frequency and bit rate were used, experiment with higher PoSK frequencies and a more realistic bit rate has been carried out. So, F_S = 100 kbaud is chosen for the main message symbol rate and F_{PoSK}(kHz) = {1, 10} for different

values of the "Cryptographic Polarization Selector" output rate. A 49164-bits frame (aaa001…fff555) has been transmitted 6 times, that is, 1 time in each modulation (50% / 100% ASK, 500 kHz / 1 MHz FSK and -90° / 90° PSK) in each F_{PoSK} value, that is a total of 294984 bits. With the GNU Radio demodulators, all the 6 transmissions have been successfully demodulated and the entirety of the bits has been recovered without error.

B. Authentication Code recovering

As previously mentioned, the profile of the instantaneous power received by the USRP B210 corresponds to the authentication code. Let's try to recover the authentication code of the previous subsection message.

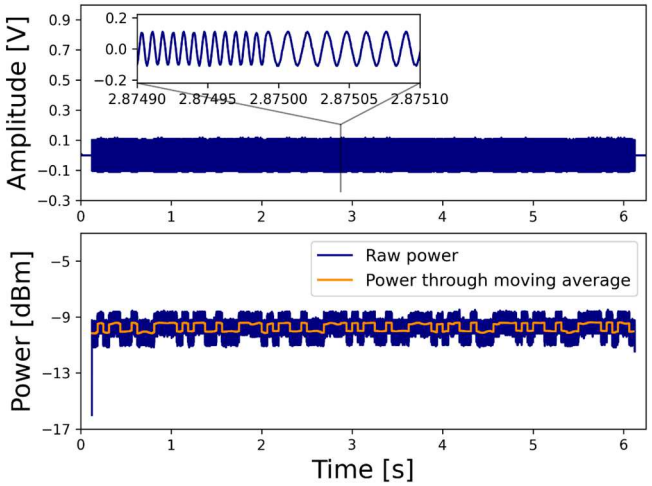
On Fig. 4 (b), the instantaneous power of the authentication signal clearly reveals the PoSK code used by the transmitter when sending the message. In this experimental context, a simple Linear Feedback Shift Register (LFSR) is used as a preliminary cryptographic algorithm for its ease of implementation. Fig. 5 shows the architecture of the used LFSR algorithm.

The LFSR output, shown in Fig. 5, is indeed the one repeating in the authentication signal power profile shown in Fig. 4 (b). The code is inverted on the authentication signal and this is normal, this depends on the polarization used for authentication and the connection on the switch with regard to its normally close side (switch initial state).

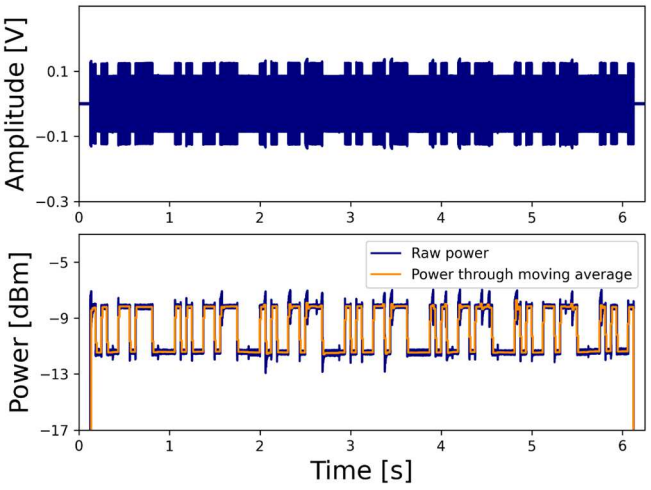
On Fig. 4 (a), the power profile of the main message also shows the authentication code but with a much smaller gap between 1 and 0 than that of the signal dedicated to authentication. This phenomenon, which is actually undesirable, is caused by the switch losses, which are lower on one of its outputs than on the other. Following condition is required to eliminate this phenomenon.

$$|P_{XX}(t) - P_{YY}(t)| = 0 \quad (2)$$

Where X and Y are used polarizations, $P_{XX}(t)$ and $P_{YY}(t)$ are received power in a co-polarization X to X and Y to Y transmissions respectively.



(a)



(b)

Fig. 4. (a): Instantaneous power of the main message, received on the dedicated port, that is the HackRF One's port. (b): instantaneous power corresponding to the authentication code, received on the port dedicated to authentication, that is the USRP B210's port.

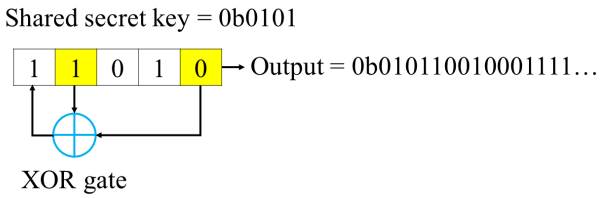


Fig. 5. Architecture of the LFSR used in this experimentation.

It is important that the router has the same loss when connected to the vertical antenna as when connected to the horizontal antenna. The two antennas must present the same polarization properties. It is highly likely that circular polarizations will be more robust than linear polarizations from a wave propagation point of view. Environment and relative positioning of antennas could also be partly responsible for this phenomenon.

C. Assessment of the PoSK robustness

To assess the robustness of the PoSK and highlight its impact on the transmitted RF signal, the following experiment has been carried out, which is the worst-case experiment for PoSK. So, F_S = 100 kbaud is chosen for the main message symbol rate and F_{PoSK}(kHz) = {1, 10, 100, 500, 1000} for different values of the "Cryptographic Polarization Selector" output rate. To make this experiment the worst case possible for PoSK, a square-wave signal is generated by a waveform generator as F_{PoSK} signal instead of Arduino board running LFSR script, as shown in Fig. 6.

A 49164-bits frame (aaa001…fff555) modulated in 500 kHz / 1 MHz FSK is transmitted at all of the F_{PoSK} frequencies. With the GNU Radio demodulators, all the transmissions have been successfully demodulated and the entirety of the bits has been recovered without error.

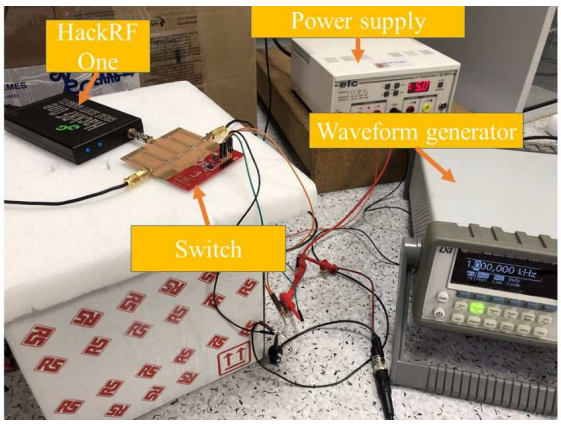


Fig. 6. Experimental setup using a waveform generator.

Again, PoSK did not alter the RF signal enough to introduce bit errors in these standard modulations, but it still has some influence on it, as shown in Fig. 7.

Fig. 7 (a) shows that the higher the polarization change frequency, the greater its impact on the signal. For example, at F_{PoSK} = 1 MHz square-wave signal, we end up with 10 polarization changes in every bit, remember that bit rate BR = 100 kbps is equal to symbol rate F_S = 100 kbaud in 2-symbol modulations.

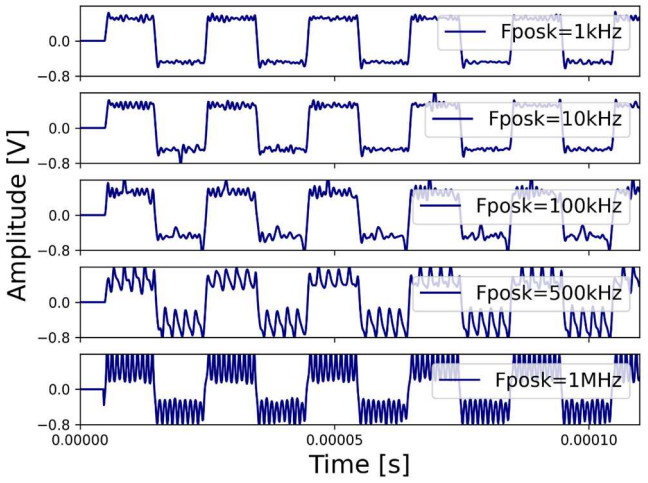
The impact of the PoSK can be seen as fluctuations in the demodulated signals in Fig. 7 (a). These fluctuations are caused by the switching time. Indeed, a switch is used as "Router" to perform PoSK by switching from one antenna to the other, and so on.

As it happens, a switch has a non-zero switching time. During this switching time, the RF signal is connected to neither of the two antennas, which leads to a power break at the receiver, thus causing these fluctuations. Fortunately, these fluctuations can be minimized by filtering as shown in Fig. 7 (b) where a low-pass filter with a cut-off frequency at least twice the symbol rate (F_S) was used. The more the duration of the modulation symbol is higher than the duration of the switching time (which is actually the duration of a power drop), the more efficient the filtering.

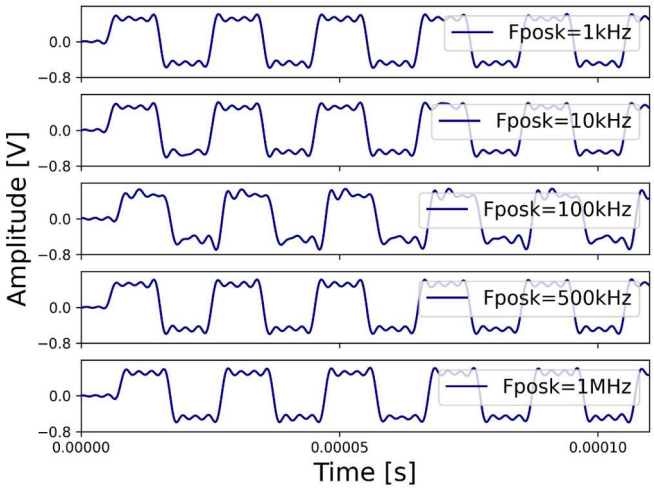
In PoSK, the duration of the switching time is very important: the shorter this duration, the lower the risk of bit error due to PoSK.

Nevertheless, in this experiment, bits can even be recovered from the raw signals (see Fig. 7 (a)) by a simple binary slicing, without even need for filtering. However, in the case of amplitude modulations, the closer the amplitudes the greater the risk of bit errors if the signal is not filtered before binary slicing. 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 MHz range are not only unnecessary, but also increase power consumption in an environment where energy is already scarce.



(a)



(b)

Fig. 7. First bits of the message demodulation at different F_{PoSK} frequencies. (a): Raw signals. (b): Signals after a low-pass filter with 400 kHz of cut-off frequency has been apply to them. The bit rate is 100 kbps.

IV. Conclusion

This work represents a proof of concept for the use of PoSK to secure wireless communications without need for major modifications on the device. We are able to demodulate signals from a PoSK transmitter for standard modulations (ASK, FSK, PSK). We have demonstrated that transmitter authentication is possible *via* the instantaneous power. We have also outlined the impact that PoSK could have on the signal, and we propose filtering as one of the techniques for overcoming the undesirable effects introduced by the PoSK.

Nevertheless, there is still a lot of work to be carried out on PoSK. We must carry out more in-depth investigations on the impact of the PoSK on the bit error rate (BER) in different environments and at different noise levels. Eventually, we have to find and experiment with advanced filtering techniques and error correction algorithms specifically tailored to mitigate any unwanted degradation introduced by the PoSK. Also, the PoSK has to be experimented in the

presence of multipath propagation and with the use of more than two polarizations. Next, we will be working on the miniaturization and integration of all the components used to perform PoSK: the power divider, the power detector, the cryptographic polarization selector and the antennas. Finally, advanced studies on the PoSK's energy consumption must be carried out.

The integration of the PoSK into existing IoT devices is easier than the integration of most of the solutions proposed in the literature, because PoSK only affects the antenna part: the standard antenna is simply replaced by a more sophisticated one. It is a minor modification, accessible to the designers of devices, since it does not affect protocols.

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

Future works will deal with the use of circular polarizations and the AES cryptographic algorithm.

REFERENCES

[1] M. E. Bouazzati, R. Tessier, P. Tanguy and G. Gogniat, “A Lightweight Intrusion Detection System against IoT Memory Corruption Attacks,” 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," in 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 March 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," 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 IEEE International Conference on Communications (ICC) (2016): 1-6.

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

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

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