Polarization Shift Keying for Device Authentication in Wireless Sensor Network

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

Polarization Shift Keying for Device Authentication in Wireless Sensor Network

Lamoussa Sanogo[1], Eric Alata[12], Taki E. Djidjekh[1], Gael Loubet[12], Alexandru Takacs[13], Daniela Dragomirescu[12]

[1]LAAS-CNRS, CNRS, France.
[2]INSA Toulouse, Université de Toulouse, France.
[3]Université Toulouse III – Paul Sabatier, Université de Toulouse, France.
{lamousa.sanogo, eric.alata, taki-eddine.djidjekh, gael.loubet, alexandru.takacs, daniela.dragomirescu }@laas.fr

***Abstract* — This paper proposes a new security technique for device authentication in Internet of Things (IoT) Wireless Sensor Networks (WSN). This technique, based on Polarization Shift Keying (PoSK), 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 device or for the main message. Basically, this means cryptographically controlled modification of the polarization of the emitter outgoing wave. This is somehow a second modulation of the wave where the different used polarizations denote the symbols of this second modulation. Then, a security gateway synchronized with this emitter is able to retrieve these symbols. This creates a secure communication link between the two terminals at the physical layer. The PoSK mechanism should not alter the original waveform and its primary modulation enough to increase the bit error rate (BER). In this work, PoSK is experimented using two polarizations (Binary-PoSK), along with different primary modulations. The results show that this technique could be a way of achieving secure communications in IoT where devices are resource-constrained.**

***Keywords* — Active Antenna System (AAS), Authentication, Internet of Things (IoT), Polarization Shift Keying (PoSK), Security, Wireless Sensor Networks (WSN).**

I. Introduction

The resource-constrained nature of Internet of Things (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. 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, Bouazzati *et al.* present in [1] "A Lightweight Intrusion Detection System against IoT Memory Corruption Attacks". They achieved very interesting results with a detection accuracy of 99.98 %. However, their approach is not so protocol-independent.

When it comes to device authentication, the most explored approach may be 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 advances in manufacturing processes, thus reducing more and more device imperfections; electronic devices non-stability regarding environment and 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.

We propose Polarization Shift Keying (PoSK), a new lightweight, protocol-independent, non- invasive and dynamic authentication-enable solution. PoSK is a well-known technique in optical communications since a while [3,4]. Optical modulators capable of operating at tens of Gbps have been developed [5]. On the other hand, the use of PoSK in radio communications is more recent; in 2004 Sibecas *et al.* published the patent "US 2004/0264592 A1" entitled "Polarization state techniques for wireless communications" [6]. More recent papers in the literature include [7], where Arend *et al.* deal with PoSK in satellite communications and [8], where Wu *et al.* investigated fundamental properties of PoSK in wireless channels subject to fading. Wu *et al.* are particularly interested in Rayleigh and Rician fading channels. To the best of our knowledge, this paper is the first to propose PoSK for radiocommunications security.

II. PoSK-Based Security

A. Presentation and Experimental Setup

Fig. 1 shows the PoSK-based security architecture.

In the PoSK-based security architecture, the terminals standard antennas are replaced by an Active Antenna System (AAS). The expression "Active Antenna System" refers to a set of antennas providing multiple polarizations controlled by a 'Polarization Selector' through a 'Router'. In this way, polarization shift keying can be performed.

The 'Polarization Selector' dynamically controls the polarization of the RF signal following a cryptographic algorithm, *e.g.*, AES. This control is triggered by the detection of a RadioFrequency (RF) power indicating the beginning of a transmission / reception. 'Polarization Selectors' of the two

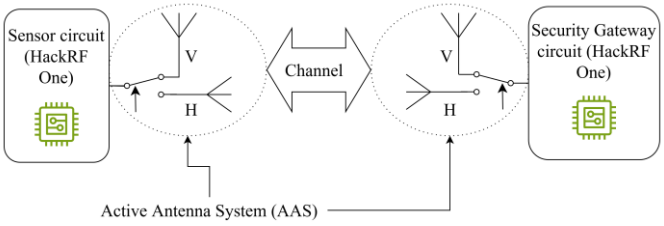


Fig. 1. PoSK-based security architecture.

terminals share a primitive secret cryptographic key and they are synchronized with the help of power detectors. The ultimate goal would be to have the whole AAS and power detector on a single compact integrated circuit, which is definitely possible nowadays.

Fig. 2 shows the experimental setup in the anechoic chamber. All the experiment in this work were carried out in anechoic chamber. In this work, HackRFs [9] are used as 'Sensor circuit' and 'Security Gateway circuit' blocks. Arduino boards are used as 'Polarization Selectors' and 'Routers' are own-made switches based on the Analog Device's AD8137 Low Power Differential ADC Driver. The power detectors are also own-made, they are based on the Linear Technology's LTC5536 Precision RF Detector.

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, we can use a router made of power divider and phase shifters.

B. *Authentication Process*

Authentication is performed through instantaneous power. Let X and Y be the polarizations used in the PoSK. 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. In this way, the 'Security Gateway' can detect any wireless node not synchronized with it at a given time t when the following relation is not true:

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

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

III. Experimental Results And Discussion

A. *Assessment of the PoSK's Impact on the RF signal*

To investigate the impact of the PoSK mechanism on the RF signal, we transformed the 'Security Gateway' into a standard receiver by replacing its AAS with a standard LHCP 2.45 GHz antenna as shown in Fig. 3. We used linear polarizations on the 'Wireless Sensor Node' that serves as the PoSK transmitter with a switch as a 'Router' and an Arduino board running a Linear Feedback Shift Register (LFSR) algorithm as a 'Polarization Selector'.

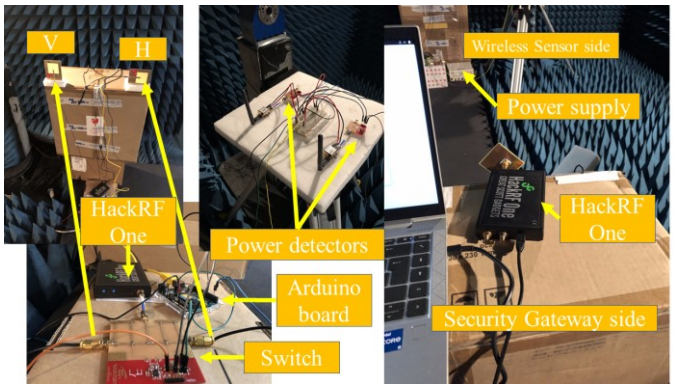


Fig. 2. PoSK-based security experimental setup in anechoic chamber. In this image, the 'Security Gateway' is used as a standard receiver, its AAS has been replaced by a standard circular-polarized antenna, it is as used in section III.A. experiments. It is noteworthy that not all these images come from the same experiment setup.

1) *Low-Frequency PoSK*

In order to make accurate measurements and do precise interpretations, we experiment PoSK at a very low frequency first. So, we choose: $F_S = 4\,baud$ as the main message symbol rate, that is 4 bits per second for our 2-symbol modulations (2-ASK, 2-FSK and 2-PSK); $F_{PoSK} = 16\,Hz$ is the 'Polarization Selector' output rate, *i.e.*, the bit rate of the authentication code. For transmissions, we use Universal Radio Hacker (URH) [10]; the received signal is then recorded in complex IQ format in a binary file. For demodulation, we use our own-build GNU Radio [11] flowgraphs, as we found that URH has limited demodulation performance. Fig. 4 shows some received signals.

We experimented: 0 % / 100 %, 25 % / 100 % and 50 % / 100 % amplitude modulations; 64 kHz / 128 kHz frequency modulation; and -90° / +90° and 180° / 0° phase modulations. For all these modulations, the signals have been easily and error-free demodulated, both with and without PoSK. In this experiment, the PoSK did not degrade the RF signal enough to cause bit errors, but actually it still has some influence on it, as shown in Fig. 5. On the raw demodulated signals (Fig. 5 top graph) we can see amplitude brief sharp drops introduced by

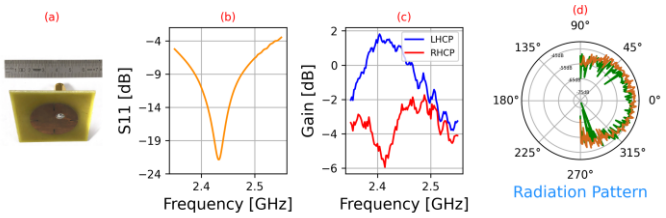


Fig. 3. LHCP antenna used by the 'Security Gateway'. For the green plot of the radiation pattern, the reference emitting antenna is at 0° angle relative to our circularly-polarized antenna, and 90° angle for the brown plot.

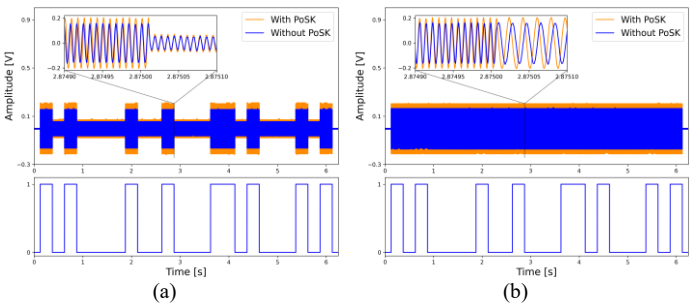


Fig. 4. Signals received by the standard receiver when they have been transmitted with/without PoSK. The top graphs show: (a) a 25%/100% analog amplitude-modulated signals; (b) a 64kHz/128kHz analog frequency-modulated signals. The bottom graphs show the bits after demodulation. The transmitted data was 0xa12345 and use carrier was 2.45GHz.

the PoSK in the orange signal; the zoom plot emphasizes one of these drops.

We are using a switch 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 brief sharp drops.

Nevertheless, one can still recovered bits from the raw signals even from the transmission with PoSK, but to reduce the risk of bit error, we can remove these unwanted drops before binary slicing. Indeed, these signals can be easily cleaned before decoding. To do so, we use a low-pass filter with a cut-off frequency higher than the modulation symbol rate F_S. More the duration of a modulation symbol is higher than the duration of the switching time which is actually the duration of a drop, the more efficient the filtering. Fig. 5 bottom graph shows the signals after 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.

2) *High-Frequency PoSK*

In this subsection, we are interested in high values for PoSK frequency. So, we choose: $F_S = 100\,kbaud$ for the main message symbol rate and $F_{PoSK}(kHz) = \{1,10,100,500,1000\}$ for different values of the 'Polarization Selector' output rate. To make this experiment the worst case possible for PoSK, we used a square-wave signal generated by a waveform generator as F_{PoSK} instead of Arduino board running LFSR script. We transmitted 25 times a 49164-bits (aaa001…fff555) frame for each of the following modulations: ASK 25 % / 100 %, ASK 50 % / 100 %, FSK 500 kHz / 1 MHz, PSK -90° / +90°, and PSK 180° / 0° (1 time for each F_{PoSK} value in each modulation), that is a total of 1229100 bits. With our GNU Radio demodulators, we have successfully demodulated all the 25 transmissions and recover the entirety of the bits, without error.

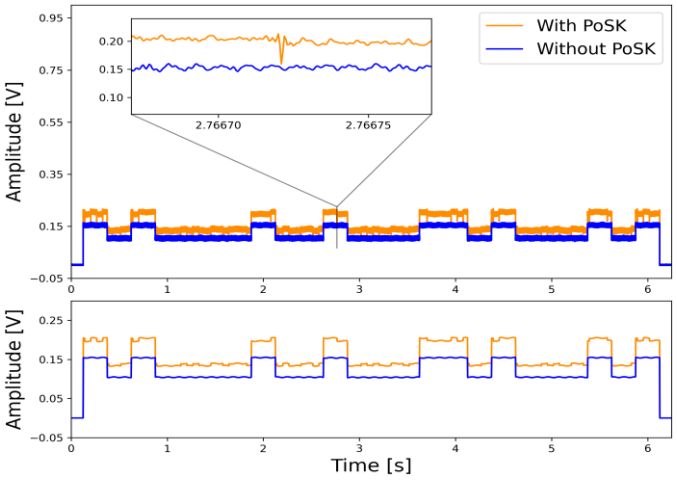


Fig. 5. Signals received (demodulated) by the standard receiver when they have been transmitted with/without PoSK. The top graph shows the raw demodulated signals and the bottom graph shows the same signals after filtering. Use modulation was ASK 50%/100%.

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. 6, 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 this case.

As explained in the previous subsection, the switching time introduced these fluctuations we can see in Fig. 6.

Nevertheless, once again bits can still be recovered 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 error if the signal is not filtered before binary slicing.

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, this can also make 'Polarization Selectors' synchronization challenging and less reliable.

B. *Authentication through PoSK*

Now, the 'Security Gateway' is no more a standard transceiver but a PoSK transceiver with the same configuration as the 'Wireless Sensor Node' (see Fig. 1). Both terminals are using linear polarizations. The 'Polarization Selectors' (Arduino boards) are synchronized with the help of power detectors and each of them is running the same LFSR algorithm.

For synchronization, we empirically propose relations (2) and (3) below, which allow not only synchronization, but also prevents the polarization change from occurring during the switching time, the objective being to avoid missing important events such as phase shifts in the PSK for example.

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

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

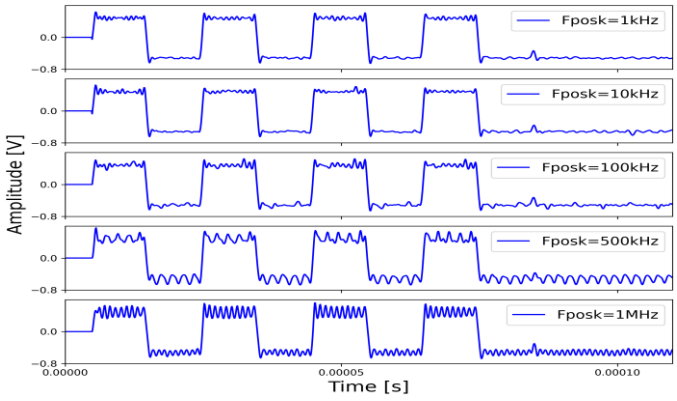


Fig. 6. Signals received (demodulated) by the standard receiver when they have been transmitted with PoSK for different PoSK frequencies. Use modulation was FSK 500 kHz / 1 MHz.

Where F_{PoSK} is the 'Polarization Selector' output rate, F_s the main message symbol rate, and φ the time shift of F_{PoSK} relative to F_s, *i.e.*, the beginning of the PoSK relative to the beginning of the transmission.

So, the 'Security Gateway' uses the instantaneous received power to determine dynamically the polarization used by the 'Wireless Sensor Node'. If the received power is below a given threshold, this means a cross-polarization transmission and the 'Security Gateway' deduces that the 'Wireless Sensor Node' is not the one to which it is synchronized. This is how an illegitimate emitter is detected, as summarized by relation (1) above. Let's take a look to Fig. 7 showing some frequency-modulated signals received by the 'Security Gateway'.

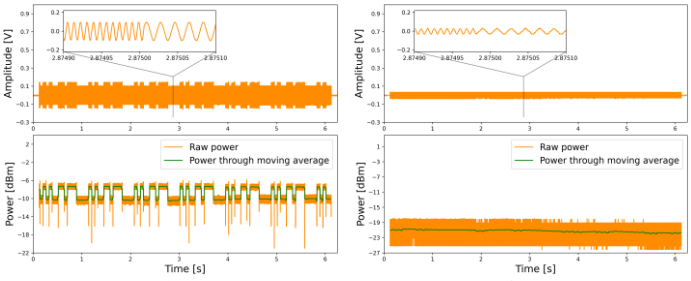
Once again, we can see the impact of the switching time on the power profile in Fig. 7 (a) bottom graph. As previously explained, we can get rid of these fluctuations by filtering. A moving average filter have been used here.

We can see that the power profile shows the authentication code generated by the LFSR algorithm. This phenomenon could be caused by 'Router' losses, which are lower on vertical polarization than on horizontal polarization, with a difference of about 3 dBm between the two polarizations. It's noteworthy that we are using our own-made switch as 'Router'. This phenomenon does obviously not compromise the detection process, since abnormalities correspond to cross-polarization transmissions where the power drop is much more important (about 10 dBm drop), as shown in Fig. 7 (b) bottom graph. However, it is important not to forget handling these power brief sharp drops before authenticate, otherwise one will end up with several false positives in authentication.

The aforementioned phenomenon caused by 'Router' losses is not actually a desired phenomenon, since it reveals cryptography, which fortunately is dynamic. Following condition is required to eliminate this phenomenon.

$$|P_{XX}(t) - P_{YY}(t)| = 0 \tag{4}$$

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



(a) (b)

Fig. 7. Signal received by the 'Security Gateway': (a) when it has been transmitted with PoSK; (b) without PoSK on vertical polarization and received on horizontal polarization (cross polarization transmission). In both (a) and (b): the top graphs show the 64 kHz / 128 kHz analog frequency-modulated signals, the bottom graphs show the instantaneous raw power and this same power after a moving average filter has been applied to it. In (b), the power is actually $P_{VH}(t)$ where V stands for vertical polarization and H stands for the horizontal polarization.

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 must be as similar as possible (gain, radiation pattern). It is highly likely that circular polarizations will be more robust to this phenomenon than linear polarizations. Environment could also be partly responsible for this phenomenon.

IV. Conclusion

This work represents a proof of concept for the use of PoSK to secure wireless communications. We were able to demodulate signals from a PoSK transmitter for standard modulations (ASK, FSK, PSK). We have demonstrated that transmitter authentication is indeed 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 PoSK. Still aiming to further mitigate the impact of PoSK on the transmitted signal, we also propose a synchronization technique that prevents the polarization change from occurring during the switching time, the objective being to avoid missing important events such as phase shifts in the PSK for example.

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

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, vol . 23, no. 2353, 2023, doi: 10.3390/s23042353.

[3] 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.

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

[5] [Online] https://www.versawave.ca/polarization-modulators/ (accessed on March 2024).

[6] 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.

[7] 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.

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

[9] [Online] https://greatscottgadgets.com/hackrf/one/ (accessed on March 2024).

[10] [Online] https://github.com/jopohl/urh (accessed on March 2024).

[11] [Online] https://www.gnuradio.org/ (accessed on March 2024).