Physical Unclonable Functions based on silicon micro-ring resonators for secure signature delegation in Wireless Sensor Networks

Borja Bordel[1]* and Ramón Alcarria[2]
[1]Department of Telematics Systems Engineering. Universidad Politécnica de Madrid, Spain
bbordel@dit.upm.es
[2]Department of Topographic Engineering and Cartography. Universidad Politécnica de Madrid, Spain
ramon.alcarria@upm.es

Abstract

With the arrival of the fourth industrial revolution and the era of Cyber-Physical Systems, Wireless Sensor Networks (WSN) are employed in a large catalogue of applications, many of them critical. At the beginning, encryption techniques were enough to protect WSN, but as more sophisticated applications are proposed, protection schemes turn also more complex. In particular, schemes based on digital signatures, hash functions and Public Key Infrastructures are extensively implemented. Nevertheless, all these solutions present a very important problem: nodes must store a secret key. As future systems will be unmanaged and be deployed in remote places without surveillance, the use of ROM memories where keys are stored in a permanent way is a critical risk. Therefore, in this paper we propose a new scheme for signature delegation in WSN, based on chaotic Physical Unclonable Functions (PUF). As the size of nodes is an essential parameter to be considered, the proposed technology is supported by micro-ring resonators. A simulation scenario is also defined to validate the usability and performance of the proposed framework.

Keywords: Wireless Sensor Networks, Physical Unclonable Functions, Chaotic resonators, Digital signature, Automatic key generators

1 Introduction

Wireless Sensor Networks (WSN) [26] have evolved from a theoretical and research paradigm to be a real and practical technology. Actually, several new applications are nowadays supported by WSN, many of them are even critical for society: traceability [5], ambient intelligence [28], biological signal control, etc. With the arrival of the fourth industrial revolution and the era of Cyber-Physical Systems [4], this evolution has been enhanced. In fact, Industry 4.0 systems [27] are based on pervasive sensing platforms, which feed intelligent systems being able to increase the global efficiency and productivity. These platforms are composed of a collection of heterogeneous hardware devices, with very different capabilities, but all of them managing private and critical information.

In order to really reduce costs and enable the creation of an intelligent and totally automated industry, future industrial systems will be unmanaged, including infrastructures deployed in remote places without surveillance (such as solutions for the Smart Farming) [32]. In this context, these systems turn vulnerable to unauthorized physical manipulations, the injection of malicious devices, Denial-of-Service attacks based on simple electromagnetic instruments, etc. This new paradigm of attacks against future

Journal of Internet Services and Information Security (JISIS), volume: 8, number: 3 (August 2018), pp. 40-53

*Corresponding author: E.T.S.I. Telecomunicación. Universidad Politécnica de Madrid. Avenida Complutense n^o 30. 28040 - Madrid (Spain), Tel. (+34) 91 549 57 00 ext. 3035 engineered systems is usually named as ”cyber-physical attacks” [2]. Although these cyber-physical attacks might seem like vandalism more than crimes with a specific objective, in truth is in Industry 4.0 solutions components are strongly related, and small changes in one element might have catastrophic consequences in other components. For example, changing the temperature value (even in a very small mount) acquired by sensors in charge of controlling the pasteurization process, can sink the production of a factory for several days. Thus, protecting WSN against these new cyber-physical attacks is a critical problem.

Regarding their physical architecture, nodes in a WSN include two subsystems: the sensing components and the communication elements [25]. Attacks to the sensing components must be addressed using physical technologies: new designs, new protection encapsulates, etc. On the other hand, attacks to the communication elements have to be solved using cybersecurity technologies and other new proposals (such as trust-based solutions) which even might be able to detect and react to attacks against the sensing components.

Initially, encryption techniques were enough to protect private and critical information being sent by senor nodes through their communication subsystems. Actually, stream or block cipher can actually perform a very important (and sometime essential) role in WSN, but as different attacks (not necessary based on unauthorized accesses to private information) are defined, protection schemes turns also more complex [33].

In particular, nowadays, most modern and recent applications supported by distributed networks of nodes employ schemes based on digital signatures, hash functions and Public Key Infrastructures (PKI) [18]. In these solutions the private information is not only secured, but also the data integrity is guaranteed, and the identity of the information source that create the message ensured. In order to be effective, these schemes must maintain a large secret key, which is used to encrypt and sign the private information. Nevertheless, this approach presents a very important problem in the proposed application scenario: a collection of unmanaged and unwatched nodes must store a secret key. In order to allow the permanent storage of secret keys, these nodes must include ROM memories where keys are maintained. However, this configuration open new and potential risks, as any could access to the context of this memory. Then, new security solutions where no secret keys should be maintained by devices are required.

Therefore, in this paper we propose a new security scheme for WSN. This proposal is based on the idea of signature delegation, instead of on enabling each physical devices to sign data with a different secret key. To support this new technology, chaotic Physical Unclonable Functions (PUF) [14] will be employed. PUF take advantage of any physical properties to build private keys which are inaccessible and impossible to replicable; what added to the intrinsic complexity of chaos will enable us to define an inviolable signature scheme. Many different PUF have being defined, nevertheless the size of nodes is a very critical parameter to be considered, so the physical element in charge of supporting the PUF must be very small and resource constraint. In that way, micro-ring resonators support the proposed technology.

The rest of the paper is organized as follows: Section 2 describes the state of the art on security provision technologies for WSN and Industry 4.0 solutions and PUF; Section 3 contains the main contribution; Section 4 presents a first experimental validation based on the proposed simulation scenario; and Section 5 concludes the paper.

2 State of the Art

Different proposals for security provision in WSN may be found. As in any other discipline related to security and cryptography, two main alternatives have been studied: asymmetric key schemes and symmetric key schemes.

In respect to symmetric key schemes, block ciphers [13] and cyclic redundancy codes (CRC) [11] are probably the most employed technologies nowadays, even in WSN and Industry 4.0. This kind of ciphers, furthermore, is very common in applications where transmitted packets are sparse and always present the same length. Moreover, hardware-supported algorithms [17] (based on registers and other sequential logic circuits) have been also described. Apart from block ciphers, stream ciphers are symmetric key schemes. Several proposals specifically designed to be applied in WSN scenarios have been reported, including some very efficient techniques supported by Pseudo-Random Number Generators (PRNG) [3].

On the other hand, asymmetric solutions require a higher computational power and employ mathematical techniques implicating an important calculation effort. For example, authentication protocols based on Elliptic Curves (EC) [20] or physical phenomena such as vibrations or temperature [24]. Using these Public Key Infrastructures (PKI), some works confirm that cryptography supported by EC may be implemented in WSN (with some modifications) [19, 21]. Besides, and using signature schemes based on the referred PKI, some proposals based on the transmission of signed information and data (for example, using JSON objects) may be also found [23].

However, this approach still requires all devices to store a private and secret key in a permanent manner in a kind of ROM memory.

In relation to new and innovative security policies for future engineered systems, different works may be found. First, the concept of cyber-physical attack has been investigated. Abstract taxonomies and description languages have been proposed [34]. On the other hand, works about security in new generation technological systems have been reported: enhanced control loops [30, 22], protection schemes for CPS applied to smart grids [35] and other systems under cyber-physical attacks [7], security solutions for networked control systems and industrial applications [22], etc.

Nevertheless, most of these technologies require a great computational power from devices, and the use of heavy intelligent solutions that do not meet the special characteristics of WSN.

A possible solution to this change is Physical Unclonable Functions [16]. PUF formalize the idea of random physical features employed to identify objects; which was firstly known as one-way functions, later as physical random functions and finally as PUF.

Basically three different types of PUF can be distinguished: non-electrical PUF, electronic PUF and delay-based intrinsic PUF.

Non-electrical PUF [6] refers the nature of components supporting the “random effects” in PUF, as the measurement and transmission techniques may be electronic. These PUF are de oldest and consists, in general, of optical systems. The random element to be evaluated is the speckle pattern generated by a helium-neon laser. It is a very complicate and heavy mechanical solution, as a very precise positioning system is needed.

Electronic PUF [1] consists of measuring an analog signal generated by an electronic system. Electronic systems, especially solid-state components such as transistors, present characteristic behaviors which are impossible to replicate in two elements. For example the threshold voltage in transistors. Then, analog signal passing through these elements also inherit this “personal” behavior and may be used as PUF. As main problem, an independent and maybe complex measuring circuit is necessary to do these PUF to work.

Finally, intrinsic PUF are functions that fulfill two requirements [16]: (i) the elements supporting the PUF integrate also the measuring components as an embedded device; and (ii) the construction of the PUF only must imply processes that are naturally involved in the manufacturing of such embedded device. Two different types of intrinsic PUF are defined: arbitrary PUF and ring oscillator PUF. Arbitrary PUF are based on the construction of a digital circuit with two paths, which require a slightly different time to be crossed, and the injection of an element that randomly decides at each moment what path must follow a certain signal. On the other hand, ring oscillators consist of an output randomly delayed line in a circuit that is employed to fee the input creating a ring whose oscillation frequency depends on the applied delay.

In relation to cryptographic systems based on PUF, two basic proposals may be found: key generators and device authentication algorithms. Key generators take advantage of the random PUF's behavior (supported by a real physical randomness) to create keys with a very high entropy [36, 15], Besides, different cryptographic schemes to protect circuits at hardware level have been also reported [9, 12]. Specific proposals to protect RFID devices can be also found [8]. On the other hand, device authentication algorithms are sparse and usually consist of comparing a set of preconfigured challenge-response pairs with the real-.time obtained results [31].

In this work we are using a second generation intrinsic PUF, where the main random effect to be employed to build the function is not a delay, but the non-linear effects in an optical fiber due to the intrinsic manufacturing impurities.

3 Signature delegation based on Physical Unclonable Functions

Digital signature schemes for nodes in WSNs are usually defined over Public Key Infrastructure (PKI), where two options are traditionally considered: (i) each device generates a key pair (including a secret and a public key), so each device may sign using a different digital identity; or (ii) the manager generates a unique key pair and all devices are provided with the same private key. Both options require from devices to store private keys in a ROM memory, but some additional circumstances must be considered. The first option implies the replication of the PKI and the signature scheme (see Figure 1) as many times as devices have to be communicated. The second options makes very vulnerable the secret key, reducing the global security. Thus, new schemes to enable nodes in WSN to sign messages but in an easier, safer and lighter way are required.

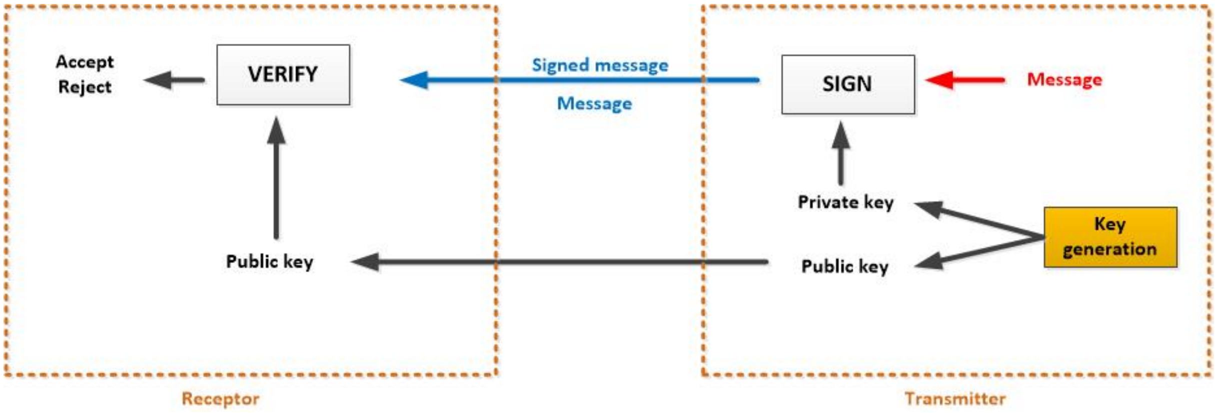

Figure 1: Traditional digital signature scheme

Traditionally, $\{_{asym}$ describes a PKI supporting the signature scheme (the certificate infrastructure is not referred here, although it is required, as it is independent from the proposed system). $\mathscr{F}_{asym}$ is a 3-tuple containing three different functions (1). G is the key generator, which produces key pairs $k = (p_k, s_k)$ being p_k the public key and s_k the private or secret key taken as input the parameter 1^η. These keys are calculated on the unary number 1^η being η a security parameter. A unary number 1^η is a number represented by repeating the unit η times (for example $4 \equiv 1111$).

$$\mathscr{F}_{asym} = (G, S, V) \tag{1}$$

S is the signature function, which for each message m and private key s_k, generates a tag t or signed message. Finally, V is the verifying function which takes as inputs the public key p_k, the message m and the tag t and produces an acceptance or reject output confirming the integrity of the received information and the identity of the transmitter. To really represent a correct PKI and signature scheme, this 3-tuple must fulfill a final condition (2).

$$Pr[(p_k, s_k) \leftarrow G(1^\eta), V(p_k, m, S(s_k, m)) = accept] = 1 \tag{2}$$

On the other hand, in order to be useful, a correct PKI must be, besides, secure. Imaging a non-uniform probabilistic polynomial time adversary A trying to impersonate the identity of a certain valid node D, the signature scheme is secure if the probability of reaching its goal is negligible.

$$Pr[(p_k, s_k) \leftarrow G(1^\eta), (m,t) \leftarrow A^{S(s_k,\cdot)}(p_k, 1^\eta), m \notin Q, V(p_k, m, t) = accept] < negl(\eta) \tag{3}$$

$A^{S(s_k,\cdot)}$ denotes an adversary with access to the oracle $S(s_k,\cdot)$ which has also intercepted the public key p_k and the unary number 1^η employed to calculate the key pair. In this context, an oracle is an entity capable of solving a problem such as a function problem. Q denotes the set of the queries on S made by A. $negl(\eta)$ is a negligible function $negl(\cdot) : \mathbb{N} \rightarrow \mathbb{R}$ such that for every positive integer p there exists an integer N_p that fulfills that for all real value $x, N_p > x$ (4).

$$|negl(p)| < \frac{1}{x^p} \tag{4}$$

This basic scheme, however, may be modified to authorize third-party entities to sign data in the name of the original device, which calculated the key pair. Using this new approach, only one PKI must be deployed. Nevertheless, this authorization is usually understood as a cession of keys, which (as said) reduces the security of the protection scheme as the secret key is stored in several unwatched ROM memories. As a solution, we propose to complement the traditional signature schemes with physical unclonable functions which enable a device or user to authorize third-party entities to sign data using its identity, but without reducing the global security of the deployed PKI.

3.1 Signature delegation architecture

The purpose of the described signature delegation architecture is to enable a collection of devices to sign information using the same identity (usually the identity of their owner), but without being necessary they to store the corresponding private key (the same for all devices) in a permanent way (usually, in a kind of ROM memory). Besides, as devices are usually deployed in unsecure places without surveillance, an identification technology that cannot be replicated, analyzed or modified is required. Physical Unclonable Functions (PUF) meet all these requirements.

The proposed solution for signature delegation must be small in size and resource constraint. The first requirement is met by implementing PUF through optical micro-rings. The second requirement is addressed by a low-cost design of the signature delegation architecture.

The PUF-based signature delegation presented in this work may be implemented in all kind of devices, including extremely resource constraint platforms (such as nodes based System-on-Chip solutions). The use of this technique the power consumption or complexity of the employed programming will decrease compared to traditional cryptography technologies.

Figure 2 shows the proposed architecture.

Although other solutions to delegate keys and identities have been proposed, only PUF guarantee that even if an unauthorized user gets a valid device, this cybercriminal is unable to replicate, analyze or modify the PUF-based identification system, as physical responses of these systems are, naturally, Unclonable and unrepeatable. It is important to remember that PUF output (usually named as "response") is unique and unpredictable for each input (usually named as "challenge"). Sometimes PUF responses to be "random" enough must be invoked using large or specific challenges; nevertheless, as we are seeing the use of chaotic signals allow the system to employ any available challenge. In any case, an unpredictable response is a good manner to identify an entity. In fact, in the simplest solutions, PUF responses are recorded and compared to some previously generated values to authenticate an entity.

However, using this configuration, an adversary could obtain the challenge being employed to authorize the third-party devices and create a new malicious element (containing this challenge in memory) [31]. Thus, the signature delegation mechanism must guaranteed that any adversary can access to the challenge being employed as authentication key.

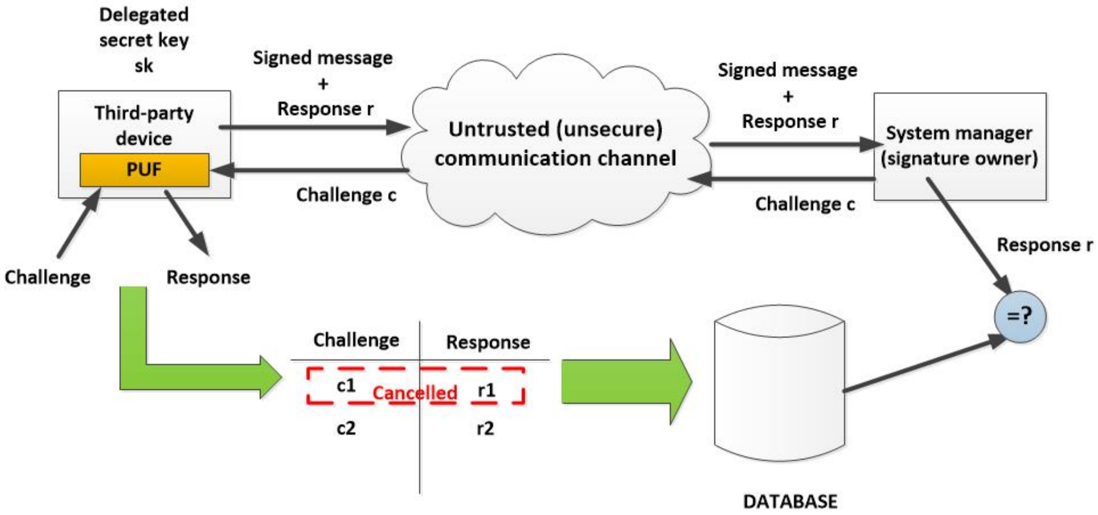

Figure 2: Signature delegation architecture

Proposed architecture (see Figure 2) takes advantage of the ability of PUF to generate an exponential number of different responses, considering only slightly different challenges. All this challenge-response pairs are randomly stored in a database. Then, to authenticate a device (or validate a signature, in this case) the receptor sends a random challenge to the authenticating device, and if it answers with the correct response, then its identity is validated. Once employed, this challenge-response pair is cancelled and removed from the database and is never employed again; so the system is resilient to man-in-the-middle attacks.

In that way, to authorize a delegated signature, the system manager generates a unique key pair through the PKI (p_k, s_k). Then, all authorized devices are provided with the corresponding secret key s_k, but a signature to be valid must be also complemented with the correct response to the corresponding challenge (which is sent in a second phase), identifying the remote device.

Mathematically, considering a PUF $\Pi : \mathscr{C} \rightarrow \mathscr{R}$, the condition to be met for the signature scheme considering the proposed delegation technology is a little more complex (5). U denotes the system manager, and c a challenge to the PUF in the device signing the message m.

$$Pr[(p_k, s_k) \leftarrow G(1^\eta), c \leftarrow U, V(p_k, m, S(s_k, m), \Pi(c)) = accept] = 1 \qquad (5)$$

Besides, to be secure this new delegation scheme, condition (3) must be adapted (6). Basically, this signature delegation scheme is secure if the probability of an adversary to create a valid signature is negligible, even knowing the secret key s_k and the architecture of the employed PUF.

$$Pr[(p_k,s_k) \leftarrow G(1^{\eta}),(m,t,r) \leftarrow A^{S(s_k,\cdot),\Pi}(p_k,1^{\eta},c,s_k),m \notin Q,V(p_k,m,t,r) = accept] < negl(\eta) \quad (6)$$

The proposed signature delegation architecture enables the fulfillment of these mathematical conditions, but the considered PUF must also meet these requirements.

3.2 PUF based on optical micro-rings resonators

Physical Unclonable Functions may be described at two different abstraction levels. Mathematically it is possible to define PUF using sets of abstract challenges and responses, but in engineering, these mathematical constructions are required to be binary vector to be able to be transmitted among remote entities.

The collection of all challenge-response pairs (CRP) in a PUF is usually named as CRP behavior and totally characterizes the PUF. To be equivalent the abstract PUF $\Pi : \mathscr{C} \rightarrow \mathscr{R}$ and its binary implementation $\Pi_b : \mathscr{C}_b \rightarrow \mathscr{R}_b$ must have the same CRP. Mathematically, both PUF are equivalent if it is possible to define two homeomorphisms $H_C : \mathscr{C} \rightarrow \mathscr{C}_b$ and $H_R : \mathscr{R} \rightarrow \mathscr{R}_b$ such that Π_b maintains the CRP behavior of Π (7).

$$\forall(c_b,r_b), c_b \in \mathscr{C}_b, r_b \in \mathscr{R}_b \ : \ c_b = H_c(c), r_b = H_R(r) \ then \ r_b = \Pi_b(c_b) \iff r = \Pi(c) \quad (7)$$

This mathematical model is usually known as "ideal PUFs" as secondary and practical effects are not considered. In particular, it has been proved that applying twice the same challenge to the same PUF does not generate exactly the same response [31]. Thus, it is necessary to design a certain detection solution as we are explaining later.

Considering a new security parameter $\eta_2 \in \mathbb{N}$, as in traditional PKI, and two new parameter $\alpha_1 \in \mathbb{N}$, and $\alpha_2 \in \mathbb{N}$ bounded in η_2 polynomially, then a binary ideal PUF may be easily implemented **??**eqno8).

$$\Pi_b : \ \{0,1\}^{\alpha_1} \rightarrow \{0,1\}^{\alpha_2} \quad (8)$$

Three conditions must be fulfilled by every ideal PUF. Namely [10]:

1. For all $c_b \in \mathscr{C}_b$ and $r_b^1 \in \mathscr{R}_b, r_b^2 \in \mathscr{R}_b$ being $r_b^1 = \Pi_b(c_b)$ and $r_b^2 = \Pi_b(c_b)$, then $Pr\left[r_b^1 = r_b^2\right] = 1$
2. Each probabilistic polynomial time adversary has a negligible advantage. In other words, no adversary can compute the output of the PUF, even if it can query the PUF for a polynomial number of times.
3. Any attempt to physically modify, see or replicate the PUF causes the destruction of the systems or its irreversible and complete modification.

Several different physical functions may fulfil these requirements, but in this work we are analyzing optical chaotic micro-ring resonators (also named as silicon micro-ring resonators due to the material used in optical fiber manufacturing). These micro-ring resonators (MRR) present two basic types: all-pass and add-drop rings (see Figure 3).

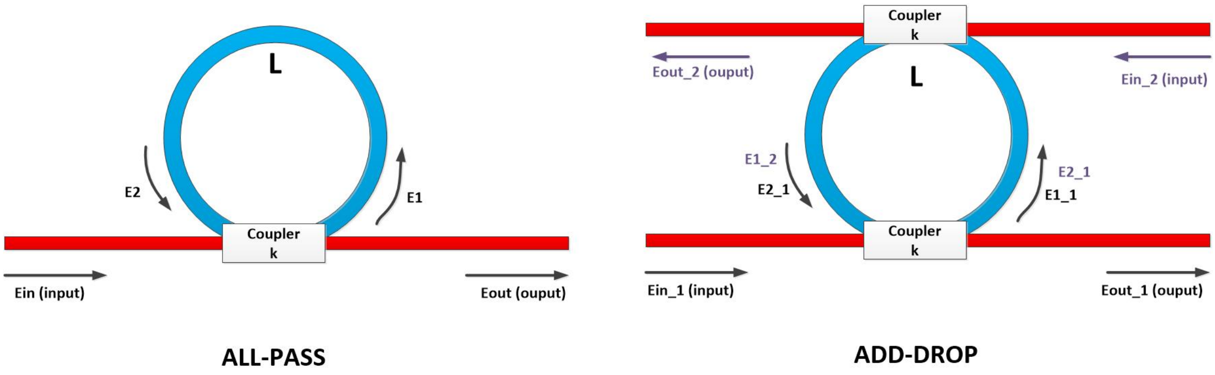

Figure 3: Basic silicon micro-ring resonators

In a simple analysis, the refractive index is considered to be invariant $n = n_0$. Thus, analysis equations turn linear and the output of the MRR very predictable. However, several nonlinearities affect silicon optical fibers. In particular, MRR are especially affected by Kerr-type nonlinearities (9).

$$n = n_0 + n_2 I = n_0 + \left(\frac{n_2}{A_{eff}}\right) P \tag{9}$$

n_0 is named ”linear refractive index”, n_2 is known as ”non-linear refractive index” and A_{eff} and P is the effective are in the optical fiber and the power of the optical field respectively. Considering the most simple MRR, the all-pass MRR, where a monochromatic Gaussian laser is employed as input, a coupler with coupling coefficient κ and loss coefficient γ is employed to introduce light in the ring, and the silicon material present a linear absorption coefficient α, it can be extracted the equations that govern the evolution of the optical field in the ring (10).

$$\begin{aligned} E_1^{w+1} = j\sqrt{(1-\gamma)\,\kappa}E_{in} + \sqrt{(1-\gamma)\,(1-\kappa)}\alpha_{att}E_1^w e^{-j(\phi_0+\phi_{nl})} \\ E_2^w = E_1^w \alpha_{att} e^{-j(\phi_0+\phi_{nl})} \\ E_{out} = \sqrt{(1-\gamma)}E_{in}\left[\sqrt{(1-\kappa)} + \frac{\sqrt{(1-\gamma)}\kappa\alpha_{att}e^{-j(\phi_0+\phi_{nl})}}{1-\sqrt{(1-\gamma)\,(1-\kappa)}\alpha_{att}e^{-j(\phi_0+\phi_{nl})}}\right] \end{aligned} \tag{10}$$

In these equations, ϕ_0 and ϕ_{nl} are the linear and non-linear phase shift (11). And α_{att} is total absorption in each half-round trip in the ring (12). λ denotes the wavelength of the Gaussian laser.

$$\begin{aligned} \phi_0 &= \frac{2\pi}{\lambda} L n_0 \\ \phi_{nl} &= \frac{2\pi}{\lambda} L n_2 \left|E_1^w\right|^2 \end{aligned} \tag{11}$$

$$\alpha_{att} = e^{-\frac{\alpha L}{2}} \tag{12}$$

These equations may be simplified if all constant parameters are grouped. Besides, to simplify the numerical analysis of these equations, important variables are written as a three-dimensional discrete chaotic map, whose variables may be also split into two two-dimensional independent maps (13).

$$\begin{bmatrix} E_1^w \\ E_2^w \\ E_{out}^w \end{bmatrix} = \begin{bmatrix} a_1 + a_2 E_1^{w-1} e^{a_3 \left| E_1^{w-1} \right|^2} \\ b_1 E_1^{w-1} e^{a_3 \left| E_1^{w-1} \right|^2} \\ c_1 + \frac{c_2 e^{a_3 \left| E_1^{w-1} \right|^2}}{1 - c_3 e^{a_3 \left| E_1^{w-1} \right|^2}} \end{bmatrix} \tag{13}$$

Using the same technique, and the superposition theorem, the add-drop MRR may be analyzed, together with other more advanced configurations such as sequences of coupled or independent rings (both all-pass and/or add-drop).

These discrete maps have been proved to be chaotic under certain circumstances [29]. Thus, a small change in E_{in} causes an unpredictable change in the study variables. Besides, the nonlinearities in optical fibers cannot be read or replicated; it would be necessary to extract a sample from the ring which would destroy the PUF.

Although these properties make from the proposed MRR a very good PUF, they introduce also an important problem: a PUF never generates the same response to the same challenge. Small variations in the environment, time, etc. cause this variability.

In this context, in order to successfully detect the ideal PUF response to which the received real response refers, two distances are calculated and considered:

- The inter-distance: It refers the distance between the responses generated by two PUF implementations for the same challenge.
- The intra-distance: It refers the distance between the responses generated by the same PUF implementation for two sequential applications of the same challenge.

If the maximum tolerated distance (of distance threshold for detection) is too high, then, different PUF implementations would be considered as the same (which is a very important vulnerability). On the contrary, if the distance threshold is selected to be too small, a PUF never would be authenticate as the algorithm understands the correct response has not been provided. The first problem is known as a false-acceptance (FA), and the second one as false-rejection (FR). A very sensible equilibrium (see Figure 4) must be reached to be successful in PUF response detection.

4 Experimental validation: simulation results

In order to validate the proposed solution as a valid technology for security provision in WSN, a simulation scenario was deployed and an experimental validation carried out.

Using advanced simulation techniques and the NS3 network simulator a real WSN was implemented including the proposed solutions. NS3 is a network simulator whose scenarios and behavior are controlled and described by means of C++ programs.

The proposed simulation scenario is an adaptation of a real Wireless Sensor Network. The WSN was designed to present one hundred and fifty (150) nodes, communicating with a central gateway in a trusted way. Although the performance of the proposed solution in a real environment may be different from the performance in a simulated scenario, the described simulation is enough close to a real deployment to be an acceptable first experimental validation. In particular, the most important and characteristic aspects of WSN are represented in the proposed simulation (their heterogeneity and the high density of resource-constraint devices).

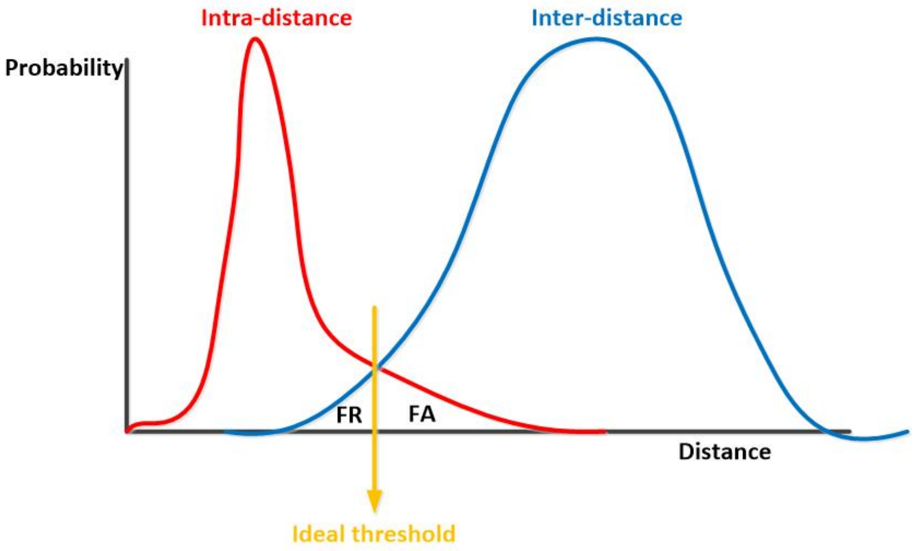

Figure 4: PUF detection problem

In the planned simulation, nodes in the WSN, and the gateway, were provided with the proposed algorithm and signature delegation system, configured in the same way as described in the previous sections. During the experiment, the number of considered nodes in the simulation scenario was increased. Twelve simulations were performed for each number of nodes in the WSN. With the acquired information, the success rate in communicating in a trusted way using the proposed signature delegation scheme was calculated. Figure 5 shows the obtained results.

In order to be able to perform the described simulation, node software must run in a virtual machine were the proposed mechanism might be deployed. These virtual machines must be embedded into the simulation scenario. In order to do that, different TAP bridges (or ghost nodes) connecting the virtual machines to the NS3 simulator were considered. Virtual machines were automatically generated and deployed through the Libvirt interface. All machines implemented the operating system Linux Ubuntu 16.0. The proposed simulation scheme employs the paravirtualization paradigm which allows a virtual machine (i.e. a NS3 node) to behave as an independent computer, providing all the configuration possibilities of a real machine. NS3 simulator provides support for the first three levels of this scheme. In that way, NS3 nodes can exchange messages with the real world and the host computer.

As can be seen, success rate is around 100% until the number of considered devices reaches a hundred. At this moment, the success rate is around 90%. From this point, the high number of devices using the signature delegation infrastructure causes problems to establish in an efficient and fast manner distance thresholds and to manage some many different CRP behaviors. If one hundred and fifty senor nodes are considered, the success rate descends to 75% (approximately). However, it is very complicated for WSN to maintain this number of trusted channels at the same time. The success rate goes below 50% for 180 nodes in the WSN (approximately). Therefore, the obtained results are a first evidence that the proposed technology is a valid solution for signature delegation and secure data transmission in future WSN.

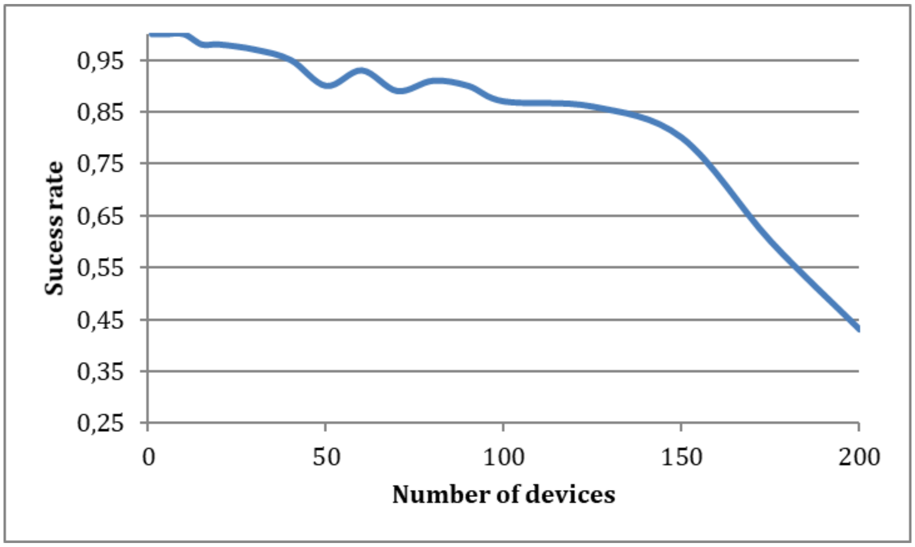

Figure 5: Success rate. Simulation results

5 Conclusions and future works

This paper describes a new scheme for signature delegation in WSN, based on chaotic Physical Unclonable Functions (PUF). We propose to complement the traditional signature schemes with physical unclonable functions which enable a device or user to authorize third-party entities to sign data using its identity, but without reducing the global security of the deployed PKI. As the size of nodes is an essential parameter to be considered, the proposed technology is supported by micro-ring resonators. In this work we are analyzing optical chaotic micro-ring resonators (also named as silicon micro-ring resonators due to the material used in optical fiber manufacturing), to define discrete maps have been proved to be chaotic under certain circumstances. Thus, a small change in the inputs causes an unpredictable change in the output variables. Besides, the nonlinearities in optical fibers cannot be read or replicated; it would be necessary to extract a sample from the ring, which would destroy the PUF.

In order to evaluate the performance of the proposed technology, a first simulation scenario was deployed and an experimental validation carried out to determine the scalability and the operation limits of the presented solution. Obtained results are a first evidence of the validity of the described solution.

Future works should consider physical prototypes (including, for example, the environmental effects on PUF performance) and address some practical problems not treated in this first work, such as the construction of the required laser to activate the MRR.

Acknowledgments

The research leading to these results has received funding from the Autonomous Region of Madrid through MOSI-AGIL-CM project (grant P2013/ICE-3019, co-funded by EU Structural Funds FSE and FEDER). Also from the Ministry of Economy and Competitiveness through INPAINK project (RTC-2016-4881-7), and from the Centre for the Development of Industrial Technology (CDTI) through Perimeter Security project (ITC-20161228). Borja Bordel has received funding from the Ministry of Education through the FPU program (grant number FPU15/03977).

References

[1] C. Bohm and M. Hofer. *Physical Unclonable Functions in Theory and Practice*. Springer, 2013.

[2] B. Bordel, R. Alcarria, D. Sánchez-de Rivera, and T. Robles. Protecting industry 4.0 systems against the malicious effects of cyber-physical attacks. In *Proc. of the International Conference on Ubiquitous Computing and Ambient Intelligence (UCAmI'17), Philadelphia, Pennsylvania, USA*, volume 10586, pages 161–171. Springer, Cham, October 2017.

[3] B. Bordel, A. B. Orue, R. Alcarria, and D. Sanchez-De-Rivera. An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators. *IEEE Access*, 6:16149–16164, March 2018.

[4] D. Bordel, B. and Alcarria, R. and Robles, T. and Martín. Cyber–physical systems: Extending pervasive sensing from control theory to the Internet of Things. *Pervasive and Mobile Computing*, 40:156–184, September 2017.

[5] B. Bordel Sánchez, R. Alcarria, D. Martín, and T. Robles. TF4SM: A Framework for Developing Traceability Solutions in Small Manufacturing Companies. *Sensors*, 15(11):29478–29510, November 2015.

[6] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair. The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions. In *Proc. of the 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'11), San Diego, California, USA*, pages 134–141. IEEE, June 2011.

[7] R. M. Clark and S. Hakim. *Cyber-physical security : protecting critical infrastructure at the state and local level*. Springer International Publishing, 2017.

[8] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal. Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. In *Proc. of the 2008 IEEE International Conference on RFID (IEEE RFID'08), Las Vegas, Nevada, USA*, pages 58–64. IEEE, April 2008.

[9] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection. In *Proc. of the 2007 International Conference on Field Programmable Logic and Applications (FPL'07), Amsterdam, Netherlands*, pages 189–195. IEEE, August 2007.

[10] S. Kardaş, S. Çelik, M. Yıldız, and A. Levi. PUF-enhanced offline RFID security and privacy. *Journal of Network and Computer Applications*, 35(6):2059–2067, November 2012.

[11] P. Koopman and T. Chakravarty. Cyclic redundancy code (CRC) polynomial selection for embedded networks. In *Proc. of the International Conference on Dependable Systems and Networks (DNS'04), Florence, Italy*, pages 145–154. IEEE, July 2004.

[12] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. In *Proc. of the 2008 IEEE International Workshop on Hardware-Oriented Security and Trust (HOST'08), Anaheim, CA, USA*, pages 67–70. IEEE, June 2008.

[13] X. Lai and Eidgenössische Technische Hochschule Zürich. *On the design and security of block ciphers*. Hartung-Gorre Verlag, 1992.

[14] R. Maes. *Physically Unclonable Functions: Properties*. Springer Berlin Heidelberg, 2013.

[15] R. Maes, A. Van Herrewege, and I. Verbauwhede. PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator. In *Proc. 2012 of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES'12), Leuven, Belgium*, volume 7428, pages 302–319. Springer, Berlin, Heidelberg, September 2012.

[16] R. Maes and I. Verbauwhede. *Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions*. Springer, Berlin, Heidelberg, 2010.

[17] H. Martin, P. Peris-Lopez, J. E. Tapiador, and E. San Millan. An Estimator for the ASIC Footprint Area of Lightweight Cryptographic Algorithms. *IEEE Transactions on Industrial Informatics*, 10(2):1216–1225, May 2014.

[18] U. M. Maurer. Modelling a public-key infrastructure. In *Proc. of the 4th European Symposium on Research in Computer Security: Computer Security (ESORICS'96), London, UK*, pages 325–350. ACM, September 1996.

[19] Microchip. Ecc-based devices. `http://www.microchip.com/` [Online; accessed on July 15, 2018].

[20] V. S. Miller. *Use of Elliptic Curves in Cryptography*, volume 218. Springer, Berlin, Heidelberg, December

1985.

[21] Openmote.org. Openmote cc2538. `http://www.openmote.com/` [Online; accessed on July 15, 2018].

[22] F. Pasqualetti, F. Dorfler, and F. Bullo. Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. In *Proc. of the 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC'11), Orlando, Florida, USA*, pages 2195–2201. IEEE, December 2011.

[23] H. C. Pohls. JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application. In *Proc. of the 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'15), Blumenau, Brazil*, pages 306–312. IEEE, July 2015.

[24] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila. Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. In *Proc. of the 2014 IEEE Wireless Communications and Networking Conference (WCNC'14), Istanbul, Turkey*, pages 2728–2733. IEEE, April 2014.

[25] C. S. Raghavendra, K. M. Sivalingam, and T. F. Znati. *Wireless sensor networks*. Springer-Verlag, 2004.

[26] T. Robles, B. Bordel, R. Alcarria, and D. Martin. Mobile wireless sensor networks: Modeling and analysis of three-dimensional scenarios and neighbor discovery in mobile data collection. *Ad Hoc & Sensor Wireless Networks (AHSWN)*, 35(1):67–104, January 2016.

[27] B. Sánchez, R. Alcarria, D. Sańchez-De-Rivera, and Á. Sańchez-Picot. Enhancing process control in industry 4.0 scenarios using Cyber-Physical systems. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 7:41–64, December 2016.

[28] A. Sanchez-Picot, D. Martin, D. S. de Rivera, B. Bordel, and T. Robles. Modeling and Simulation of Interactions Among People and Devices in Ambient Intelligence Environments. In *Proc. of the 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA'16), Crans-Montana, Switzerland*, pages 784–789. IEEE, March 2016.

[29] A. Shahidinejad, A. Nikoukar, I. S. Amiri, M. Ranjbar, A. A. Shojaei, J. Ali, and P. P. Yupapin. Network system engineering by controlling the chaotic signals using silicon micro ring resonator. In *Proc. of the 2012 International Conference on Computer and Communication Engineering (ICCCE'12), Kuala Lumpur, Malaysia*, pages 765–769. IEEE, July 2012.

[30] S. Sridhar, A. Hahn, and M. Govindarasu. Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, 100(1):210–224, January 2012.

[31] G. E. Suh and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In *Proc. of the 44th ACM/IEEE Design Automation Conference, San Diego, California, USA*, pages 9–14. IEEE, June 2007.

[32] P. Tripicchio, M. Satler, G. Dabisias, E. Ruffaldi, and C. A. Avizzano. Towards Smart Farming and Sustainable Agriculture with Drones. In *Proc. of the 2015 International Conference on Intelligent Environments (IE'15), Prague, Czech Republic*, pages 140–143. IEEE, July 2015.

[33] R. H. Weber. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1):23–30, January 2010.

[34] M. Yampolskiy, P. Horváth, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*, 8:40–52, January 2015.

[35] Yilin Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, and B. Sinopoli. Cyber–Physical Security of a Smart Grid Infrastructure. *Proceedings of the IEEE*, 100(1):195–209, January 2012.

[36] M.-D. Yu, R. Sowell, A. Singh, D. M'Raihi, and S. Devadas. Performance metrics and empirical results of a PUF cryptographic key generation ASIC. In *Proc. of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'12), San Francisco, California, USA*, pages 108–115. IEEE, June 2012.

Author Biography

Borja Bordel received the B.S. degree in telecommunication engineering in 2012 and the M.S. telecommunication engineering in 2014, both from Technical University of Madrid. He is currently pursuing the Ph.D. degree in telematics engineering at Telecommunication Engineering School, UPM. His research interests include Cyber-Physical Systems, Wireless Sensor Networks, Radio Access Technologies, Communication Protocols and Complex Systems.

Ramón Alcarria received his M.S. and Ph.D. degrees in Telecommunication Engineering from the Technical University of Madrid in 2008 and 2013 respectively. Currently, he is an assistant professor at the E.T.S.I Topography of the Technical University of Madrid. He has been involved in several R&D European and National projects related to Future Internet, Internet of Things and Service Composition. His research interests are Service Architectures, Sensor Networks, Human-computer interaction and Prosumer Environments.