A Case for the use of PUFs in Indoor Localization Systems

Ana I. Gómez
Department of Computer Science
Universidad Rey Juan Carlos
Madrid, Spain
ana.gomez.perez@urjc.es

***Abstract*—Since the adoption of smartphones and other electronic devices, Global Positioning Systems (GPS) have become an essential tool in our lives. Unfortunately, GPS is not appropriate for inner spaces. Indoor positioning systems (IPS) are born with the recent development of Internet of Things (IOT), that have raised the interest of designing an equivalent technology for indoor environments. However, security is still an important issue for these systems, in which an attacker may inject malicious constructed packages for altering the distance measures performed. Ultra Wide Band (UWB) systems rely on the security of the physical layer, that mostly depends on the secrecy of the spreading codes employed. In this talk we share our practical experience to implement a public key infrastructure (PKI) which allows two different scenarios where anchor and tags communicate. For key generation and management we rely on a scheme based on the use of a Physical Unclonable Function (PUF) combined with Identity Based Encryption (IBE). We discussed the strength and weaknesses on this approach and the expected performance of the system along with the first results obtained from a prototype developed in a joint project with TST systems.**

I. Introduction

With the widespread use of smartphones, Global Positioning Systems (GPS) have become an essential tool in our lives. As a technological substitute for traditional paper maps, it can provide our location in a matter of seconds in a efficient manner. This could be very useful to extend to big closed spaces such as warehouses, airports, underground parking lots or supermarkets to locate people or objects. Unfortunately, GPS is not appropriate for inner spaces due to two main facts:

- High attenuation of the GPS signals in indoor locations because of walls or other obstacles in Non-Line of Sight conditions and fast changes in the environment.
- Precision requirements. GPS can reach at most $5m$-$10m$ accuracy, which is way less than what is needed for an indoor system.

Recent development of Internet of Things (IOT) have fostered the interest of designing an equivalent technology for indoor environments. This is how Indoor positioning systems (IPS) are born. Multiple technologies have been proposed to address this problem, just as an standalone product or as a combination of several solutions, that can be divided into three broad categories depending on the physical principle that supports them:

- Inertial navigation is a self contained technique based mostly on accelerometers and gyroscopes.
- Electromagnetic waves can use the visible, infrared, microwave or radio spectrum.
- Mechanical waves are mostly based in audible or ultrasound.

The most recent survey regarding the performance of commercial Indoor positioning systems (IPS), also known as Local positioning systems (LPS), appeared in 2017 [3]. The most accurate beacon-based IPS are based either in ultrasound [8], [9], [5], [6] or Ultra Wide Band (UWB) signals [10], [2], [11].

In this work, we focus on the following network architecture, which should allow actors within the system (mobile users and anchors) to communicate securely between three types of roles: anchors, passive mobile users and active mobile users. It should be noted that the IEEE 802.15.4 standard defines two types of nodes, "Full-Function Devices" (FFD) and "Reduced-Function Devices" (RFD) and the use of Pulse Position Modulation (PPM). This implies the use of families of Time Hopping Sequences. While anchors and active mobile users are allow to select different Time Hopping Sequences because they are classified as FFD using this terminology, passive mobile users are more limited in memory and computational resources (RFD).

As between FFD and RFD, the difference between active and passive mobile users is given by the way they behave within the network. Passive mobile users only emit a blink to broadcast their location, active mobile users can interact with the network, send control commands and initiate a protocol to calculate the position of the nearest users.

The presence of these roles raises concerns about security of the infrastructure, making necessary to implement different security level scenarios depending

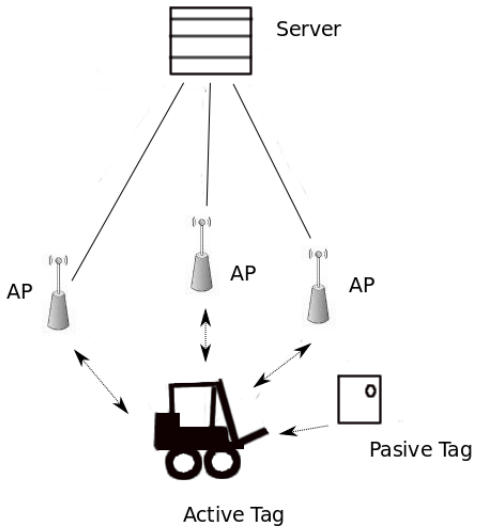

Figure 1. Communication links between the different actors of the system

on the mobile user:

- Using encryption for communication with passive mobile users. This allows changing Time Hopping sequences to protect communications against an intruder. This protocol ensures the confidentiality of a mobile user's location and prevents unauthorized tracking.
- Control of the active node's communication, the node can listen and send control commands to the anchors and tags. This allows an active node to calculate its own relative position by referring to other mobile users as well as access points. Such mobile users have access to FPGA (forklifts, heavy machinery, etc.) or active RFID (vests on humans).

In our case, the requirement for sharing information between two nodes in the system is that both share a pair of sequences for communication. The information has to be securely shared over a common channel or stored in memory before joining the network.

II. Practical Issues regarding Security

Most known security breaches in local positioning systems are active attacks, which inject malicious constructed packages for deceiving a receiver about the distance of a Mobile User, thus the need of an authentication and integrity mechanism for the messages.

Another threat are the jamming attacks which consist on a saboteur that deliberately generates collisions with the transmissions of the victim by emitting continuously. To successfully perform a jamming attack, this will require disruption of the signal and the knowledge of the time hopping sequences (THS). Again without this knowledge, the transmitter should generate a distortion pulse at each possible pulse position, thus requiring a costly transmission power in the GHz range.

However, we have to examine how likely is for an attacker to gain access to any of the hardware and what information can they get from trying to reverse engineer hardware information. Additionally to prevent spoofing of legitimate users, it is desirable to increase the security via Physical Unclonable Function (PUF) that is an option for high security systems. We consider two different complementary approaches: public key infrastructure at the medium access layer and the use of spread spectrum at the physical layer.

As it can be seen in figure 3, the authentication protocol implemented will vary depending on the type of entity (Mobile User/anchor). Two authentication mechanisms are proposed depending on the capabilities of the mobile user:

- PUF (mobile user to anchor)
- Signature-based (active mobile users to passive mobile user)

This is done to minimize the operations performed by a mobile device both for use of computational resources, channel usage, and battery size reasons.

Although the use of identifiers such as a serial number or a memory stored one was initially considered, this can be subject to duplication or modification. For this reason, the possibility of integrating a physically unclonable function (PUF) has been proposed for devices that require a higher level of physical security, for example because they are enabled for restricted access areas. These functions, which were mathematically modeled in [7], aim to provide a response given conditions and input (challenge) that uniquely identifies the device.

The architecture proposed in [4] provides an output with sufficient length for this application. The final purpose of this construction will be to generate an id identifier that will be used as the basis for message encryption within the device system. It also provides authentication for each device, therefore it can be used as an additional security measure against spoofing.

The final goal is to implement a public key infrastructure (PKI) which allows two different scenarios where anchor and Mobile Users share a communication channel.

The presence of these roles raises the need for two different security level scenarios depending on the Mobile User (MU):

- Using Identity Based Encryption (IBE) for securing the communication for a passive node. This allows to change the THS to protect com-

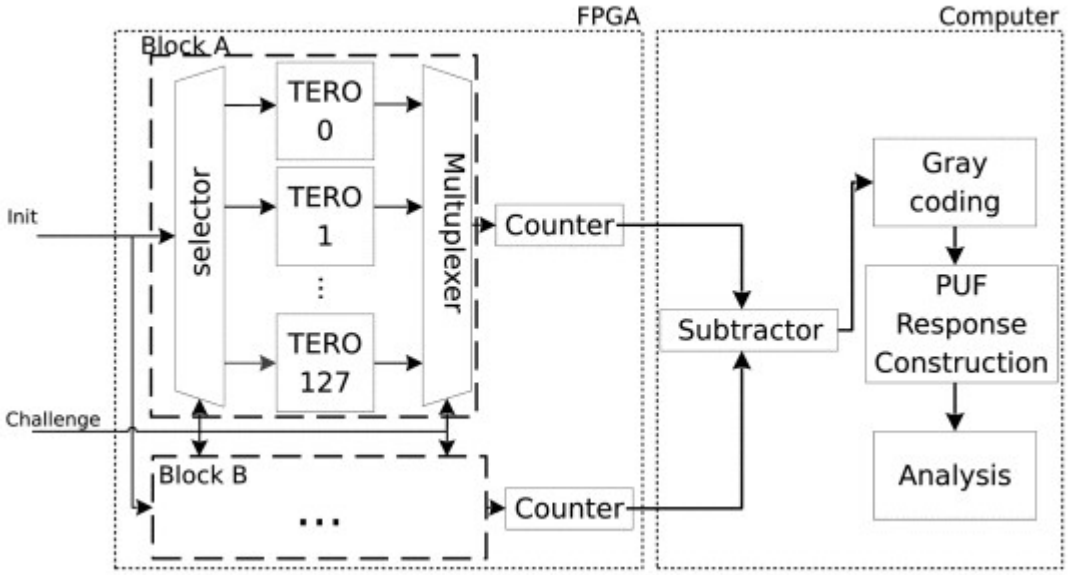

Figure 2. TERO-PUF. Source in [4]

munications against an eavesdropper. This protocol secures the localization of a node and prevents unauthorized tracking.

- Control of the active node communication, the node can listen and send control commands to the anchors and other MUs. This allows for an active node to calculate its own relative position referring to other MUs as well as anchors. This type of MUs have access to power sources like AC-batteries (forklifts, heavy machinery, etc) or DC-batteries (human vests).

In a location system, position information does not require confidentiality beyond a reasonable time. For example, this information can lose all its value to an attacker from one week to the next. This reduces the attack time and on the other hand influences the key refresh rate. This solves a well-known weakness of IBE systems, which is the "key scrow", which gives power to the central entity to decrypt all messages in the system, but in this case it is not relevant to the application.

Another weak point that IBE systems is the revocation of keys for each user. In this case, since a memory table is maintained with accepted THS for each MU, it is sufficient to delete the entry corresponding to that sequence so that the user cannot transmit in the system. This can be seen in Fig 3.

III. Proposed Public Key Infrastructure (PKI)

We describe the main operations of the system, which are represented and numbered in Fig. 3:

- **Mobile-to-Anchor authentication:**
  (1) Anchor send a PUF challenge to Mobile User.

$$\text{Send}(Encrypt(Challenge(a,b)), r_A))$$

  (2) Mobile User decrypt the message with ID_{Anchor} and send an encrypted answer.

$$\text{Send}(Encrypt(Response(a,b)), r_{user}))$$

- **THS-change:**
  (3) Anchor send new sequence using ID_{user}

$$\text{Send}(Encrypt((p1,p2), ID_{user}))$$

  (4) The user decrypt the message with its private key r_{user}
- **Passive-to-Active authentication:**
  (5) Active User send a random value C using the id of the passive user ID_{user}

$$\text{Send}(Encrypt(C, ID_{user}))$$

  (6) Pasive user sends C to the active user, after decrypting with r_{user}

$$\text{Send}(C)$$

The identities in the system are known by pairwise correspondence of sequences-to-identifiers that are maintained by the anchors. Steps 1-2 can be done in reverse guaranteeing authentication at both ends on-demand.

We propose to implement the Cocks system [1] because its simple implementation. The major disadvantage is in the cost of increased data to transmit due to two reasons:

- First, the sender cannot initially know whether the receiver has the private key r corresponding

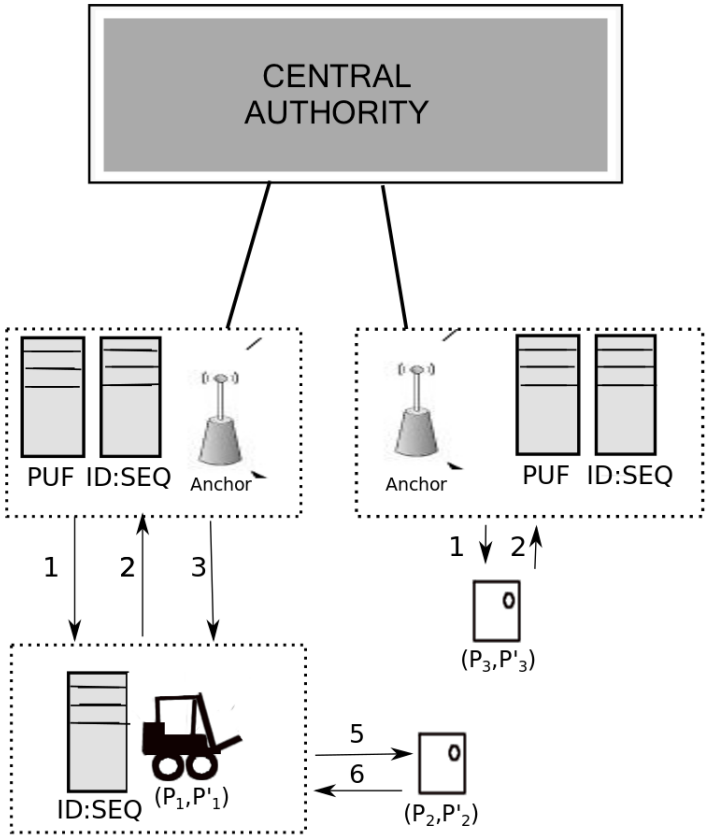

Figure 3. Message sending sequence. The memory tables that each type of node has to keep in memory, as well as the PUF responses for each identity (PUF) and the associations between identities and polynomial pairs (id-pair) are represented. The anchors (anchor) communicate to both active and passive devices

with the identifier a or $-a$ due to the design of Cocks systems. Therefore, the sender has to double the sending, transmitting for both identifiers.

- Each bit is encrypted with a number of bits as large as the key, this makes the ciphertext expand depending on the size of this key.

The resulting system has been designed with this in mind and simulations for the prototype parameters are shown in the following sections.

IV. Simulations

For an initial design, it is necessary to define the following parameters that have an impact on the performance of the system:

- **Key size**: For this prototype a key size of 1024 bits has been chosen, since it is not necessary to guarantee the confidentiality of the messages for more than eight years.
- **Size of UWB messages**. Following the Pulse Position Modulation, it is necessary to establish sequences with which each node will transmit. This prototype uses sequences of length 512 time slots.
- **Key renewal policy**: This can be freely chosen by the system administrator depending on the security level. In addition to the time period for changing the keys, it is possible to define a policy depending on the MU.
- **Size of the identifiers**: For this prototype, each node is identified by the THS, which is defined by three numbers between 0 and 22, occupying a total of 2 bytes. Additionally, for the public identity we will use for secure communication a 32-bit identifier, which will be generated with PUF, which can be adjusted to accommodate the number of nodes in the system.

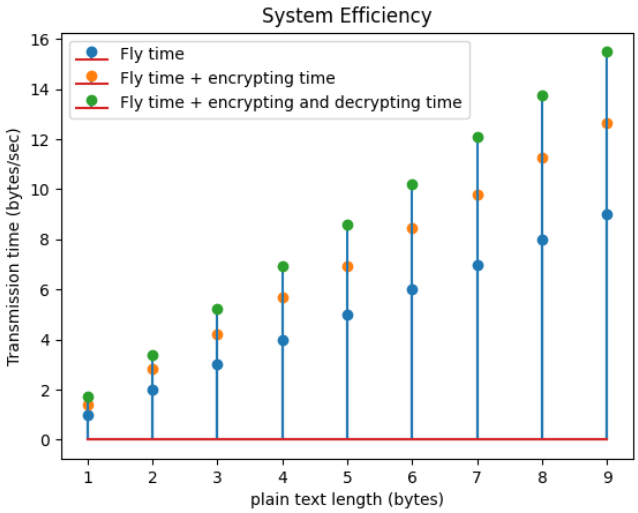

Figure 4. Simulation of transmission times in an UWB channel. Encryption and decryption times include the setting the PKI and generation of parameters.

The first two items will depend on the security to be achieved in the system. As in any system, it is designed taking into account a balance between efficiency and security, depending on the specific application. The second two items depend on the number of nodes that have to support the system, since it will influence the degree of the polynomials for the generation of the sequence and therefore the number of coefficients to send. Likewise, the number of bits dedicated to identify each node can be increased or reduced following the same idea.

The functional architecture of the system is represented in Fig 3. There is a central server that generates the private keys of the nodes and also performs the polynomial generation functions on demand, in our application they are loaded in memory in the form of a list. This could also imply that it contains the complete polynomial-user-id associations in the total system, which is replicated in the anchors. All anchors share the same ID_{Anchor} identity publicly known to all entities in the system and therefore share the same private key r_A.

As mentioned above, each anchor maintains a table with THS for the purpose of detecting the transmitted messages. Another table has been added to store the PUF responses to the challenges.

V. Conclusions

The times displayed in Fig. 4 would be valid to support a system with 23^3 total mobile users. With 2-byte identifiers, authenticating a mobile user into the system would take less than 4 seconds. On the other hand, if THS needs to be changed, this would take twice as long (approximately 8 seconds) counting the transmission time over the UWB communications channel.

The PUF allows to avoid generating identifiers and the identification is made possible using challenges. On the other hand, memory is not a problem for anchors, so they can pre-store a table with all or several responses for each mobile user, in this case the authentication is more reliable and allows more sophisticated functions such as the delimitation of access zones for active and passive nodes, with application in access control or alarm management.

Passive mobile users are assigned two sequences and a private key r from the IBE system to enable a secure communication channel to be established. Their functions are more restricted but, like the active nodes, they implement the PUF function for authentication and obtaining their identifier. Once they have assigned the sequences they will use to communicate, they can request others through their private key. The private key assignment stage is more laborious as it has to be done on a secure channel, for example by connecting them to the server. This means that key renewal policy has to be the least restrictive. We consider that the probability of spoofing is low because it requires the PUF to be successfully cloned. Active mobile user and anchors are able to listen to the blinks of passive mobile users, requiring up-to-date information on THS. The use of a backup communication network in active mobile users advisable in this case.

Future work will include total network performance measurements, including requirements on the noise levels of the channel, countermeasures against colluding MUs, full integration of the PUF in the system as well as its performance in different hardware

architectures.

REFERENCES

[1] Clifford Cocks. *An Identity Based Encryption Scheme Based on Quadratic Residues*, pages 360–363. Cryptography and Coding. Springer Berlin Heidelberg, 2001.

[2] I. Guvenc, C.C. Chong, and F. Watanabe. Nlos identification and mitigation for uwb localization systems. In *IEEE Wireless Communications and Networking Conference, WCNC*, pages 1573–1578, 2007.

[3] A.R. Jiménez and F. Seco. Comparing ubisense, bespoon, and decawave uwb location systems: Indoor performance analysis. *IEEE Transactions on Instrumentation and Measurement*, PP:1–12, 04 2017.

[4] Cédric Marchand, Lilian Bossuet, Ugo Mureddu, Nathalie Bochard, Abdelkarim Cherkaoui, and Viktor Fischer. Implementation and characterization of a physical unclonable function for iot: a case study with the tero-puf. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 37(1):97–109, 2017.

[5] J.C.. Prieto, C. Croux, and Jimenez. Ropeus: A new robust algorithm for static positioning in ultrasonic systems. *Sensors*, 9(6):4211–4229, 2009.

[6] J.C. Prieto, A.R. Jimenez, J. Guevara, J.L. Ealo, F. Seco, J.O. Roa, and F. Ramos. Performance evaluation of 3d-locus advanced acoustic lps. *IEEE Transactions on Instrumentation and Measurement*, 58(8):2385–2395, 2009.

[7] Ulrich Rührmair, Jan Sölter, and Frank Sehnke. On the foundations of physical unclonable functions. *IACR Cryptol. ePrint Arch.*, 2009:277, 2009.

[8] F. Seco, A.R. Jimenez, and F. Zampella. Fine-grained acoustic positioning with compensation of cdma interference. In *IEEE Int. Conf. on Industrial Technology (ICIT)*, pages 3418–3423, Seville, 2015.

[9] F. Seco, J.C.. Prieto, A.R. Jimenez, and J. Guevara. Compensation of multiple access interference effects in cdma-based acoustic positioning systems. *IEEE Transactions on Instrumentation and Measurement*, 63(10):2368–2378, 2014.

[10] J. Tiemann, F. Schweikowski, and C. Wietfeld. Design of an uw indoor-positioning system for uav navigation in gnss-denied environments. In *International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pages 1–7, 2015.

[11] L. Zwirello, T. Schipper, M. Jalilvand, and T. Zwick. Realization limits of impulse-based localization system for large-scale indoor applications. *IEEE Transactions on Instrumentation and Measurement*, 64(1):39–51, 2015.