Physically unclonable function based security for wireless sensor networks

Brisbane Ovilla Martínez

CINVESTAV Tamaulipas - Information Technology Laboratory

Thesis Advisor: Arturo Díaz Pérez

September 20, 2011
1. Background
2. Motivation
3. Problem Definition
4. Methodology
5. Schedule of Activities
6. Conclusions
WSN Applications

WSN often:
- Operate in hostile environments
- Collect sensitive data
Background

Wireless sensor network

The research areas are:
- Applications
- Communications
- Energy consumption
- Data acquisition
- Security
Some security issues are:
- Unauthorized access
- Manipulation access
- Denial of service
Obstacles of Sensor Security

- Modest computational power
- Small memory/storage
- Low-bandwidth network connectivity
- Limited energy supply
Physically unclonable function based security for wireless sensor networks

Problems Encountered in Providing Security in WSN

- Resistance to frequent attacks [Walters et. al, 2007].
- Key establishment and management [Eschenauer et. al, 2002, Huang et. al, 2003].
- Energy consumption [Wander et. al, 2005].

What is needed?

Secure Channel
Layer Model for Information Security Applications

Applications

Authentication Protocols: SSL/TLC, etc

Security Services: Confidentiality, Integrity, Authentication, Non-repudiation

Cryptography Primitives: Encryption/Decryption, Signature/Verification, Hash, PUFs, etc

Public-Key Cryptography: RSA, DSA, ECC, etc.
Private-Key Cryptography: AES, DES, RC4, etc.

Computer Arithmetic: +, -, *, /, ^2, ^n, etc.
Concept of PUF was introduced by [Pappu, 2001]

- Variation is inherent in fabrication process
- Can be used as a secret key
- Easy to evaluate and cheap to integrable on an IC
Principles of generation

- **Delay**
  - Input: \(...\)
  - Output: 0/1
  - Arbiter

- **Glitch**
  - Input: \(...\)
  - Output: 0/1
  - Arbiter

- **Memory**
  - SRAM cell
  -Mismatch
  - Output: 0/1
Motivation

Why use PUFs?

- No changes are needed in the manufacturing process of IC.
- It is possible to generate unique identifiers and secret keys.
- No need to use memory to store the keys.
- In a scheme of key management and establishment, it could reduce the size and number of messages exchanged.
- They are structures that consume very little area of hardware.
### Summary of the PUF’s

<table>
<thead>
<tr>
<th>Construction</th>
<th>Type</th>
<th>Principle</th>
<th>Author</th>
<th>Year</th>
<th>Challenge</th>
<th>Response</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optical</td>
<td>Explicitly randomness</td>
<td>Distribute particles</td>
<td>R. Pappu</td>
<td>2001</td>
<td>Laser beam</td>
<td>Arising speckle pattern</td>
<td>Anti Counterfeiting</td>
</tr>
<tr>
<td>Coating</td>
<td>Explicitly randomness</td>
<td>Coating particles</td>
<td>Tuyls et. al.</td>
<td>2006</td>
<td>Selected sensors</td>
<td>Capacitance</td>
<td>Identification</td>
</tr>
<tr>
<td>LC PUF</td>
<td>Explicitly randomness</td>
<td>Distribute particles</td>
<td>Guajardo et. al.</td>
<td>2009</td>
<td>Radio frequency electromagnetic field The curve response</td>
<td>Identification</td>
<td></td>
</tr>
<tr>
<td>Arbiter PUF</td>
<td>Intrinsic randomness</td>
<td>Delays</td>
<td>Lim et. al.</td>
<td>2005</td>
<td>Vector of ( n ) bits</td>
<td>One bit per arbiter</td>
<td>Authentication</td>
</tr>
<tr>
<td>Ring Oscillator PUF</td>
<td>Intrinsic randomness</td>
<td>Delays</td>
<td>Suh &amp; Devadas</td>
<td>2007</td>
<td>Vector selection</td>
<td>Vector of ( n(n-1)/2 ) bits</td>
<td>Authentication, key generation</td>
</tr>
<tr>
<td>SRAM PUF</td>
<td>Memory</td>
<td>The start-up values of SRAM</td>
<td>Guajardo et. al.</td>
<td>2007</td>
<td>A memory address</td>
<td>Power-up state</td>
<td>IP protection</td>
</tr>
<tr>
<td>Butterfly PUF</td>
<td>Memory</td>
<td>Unstable states</td>
<td>Kumar et. al.</td>
<td>2008</td>
<td>Stimulus</td>
<td>One bit</td>
<td>IP protection</td>
</tr>
</tbody>
</table>
Summary of the PUF’s

<table>
<thead>
<tr>
<th>Construction</th>
<th>Type</th>
<th>Principle</th>
<th>Author</th>
<th>Year</th>
<th>Challenge</th>
<th>Response</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flip-flop PUF</td>
<td>Memory</td>
<td>Unstable states</td>
<td>Maes et. al.</td>
<td>2008</td>
<td>Stimulus</td>
<td>One bit</td>
<td>IP protection</td>
</tr>
<tr>
<td>RE PUF</td>
<td>Explicitly randomness</td>
<td>Resistance variations</td>
<td>Helinski et. al.</td>
<td>2009</td>
<td>Stimulus</td>
<td>A set of voltage drops</td>
<td>Anti Counterfeiting</td>
</tr>
<tr>
<td>LUT PUF</td>
<td>Intrinsic randomness</td>
<td>Glitch</td>
<td>J. Anderson</td>
<td>2010</td>
<td>Vector selection</td>
<td>Vector of (n(n-1)/2)</td>
<td>IP protection</td>
</tr>
<tr>
<td>Sensor PUF</td>
<td>Hybrid</td>
<td>Sensed value</td>
<td>Rosenfeld et. al.</td>
<td>2010</td>
<td>Physical quantity, challenge bits</td>
<td>Vector of (n) bits</td>
<td>Sensor nodes</td>
</tr>
</tbody>
</table>
By using PUF in wireless sensor networks...

- How does the key can be set up under the exchange of challenges?
- What are the characteristics that a PUF should fulfill to be used in WSN?

- What type of cryptographic schemes is appropriate using PUF to generate a security key?
- How security processes impact energy-consumption in WSN?

- Have PUF-based security mechanisms similar strength than others or are they more vulnerable?
- Can theft and spoofing be avoided by providing each node with a PUF?
A secure scheme based on PUFs for establishing and managing keys in WSN is feasible and useful to reduce energy consumption without a negative impact in the attack resistance.
Design and implement new security mechanisms for wireless sensor networks based on physically unclonable functions with cost-effective energy consumption and resilient to frequent attacks.
Particular Objectives

- Design and implement a new PUF-based scheme for key distribution and management in secure communications for WSN.
- Design a new PUF-based cryptographic scheme with cost-effective energy consumption.
- Analyze the strength of the PUF-based cryptographic scheme in most frequent attacks founded in home automation WSNs.
Phase 1: Key Establishment and Management

Study of the PUFs

(Challenge) → PUF → Response

Select a PUF

Study the schemes of key establishment/management

Design a scheme of key establishment/management based in PUF
Phase 2: Energy Consumption

1. Select the most representative cryptographic algorithms used in WSN
2. Select the arithmetic to implement security algorithms in WSN
3. Implement the algorithms selected in the WSN
4. Study of the techniques for measuring energy consumption
5. Analysis of energy consumption
6. Propose algorithms with appropriated balance: Energy consumption/efficiency
Phase 3:

1. Study the resistance to frequent attacks of the selected mechanisms.
2. Study the common attacks in the home automation WSN’s.
3. Design a set of attacks.
4. Verification of the theoretical analysis by using the set of attacks.
5. Theoretical analysis of the main weakness of each one.
6. Propose a mechanism to reduce the weaknesses of the algorithms studied.
Expected contributions

1. Propose a novel PUF design for FPGAs and its application in key-management and distribution secure protocol.
2. Propose a scheme of establishment and management of keys for WSN using a PUF.
3. Get in-depth analysis on the PUF’s and their applications to mobile devices.
4. To extract secret keys from IC’s (motes) to be used in cryptographic algorithms to secure data within a WSN.
5. Propose cryptographic algorithms with lower power consumption in a WSN.
6. Identify WNS security schemes that are less vulnerable to frequent attacks.
7. Design an architecture for sensor nodes, providing PUF-based security services.
## Schedule of Activities

<table>
<thead>
<tr>
<th>ACTIVIDADES</th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>C5</th>
<th>C6</th>
<th>C7</th>
<th>C8</th>
<th>C9</th>
<th>C10</th>
<th>C11</th>
<th>C12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and implementation of a scheme of establishment and key management based on PUFs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Study of energy conservation among the different cryptographic algorithms used in the WSN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis of resistance to common attacks on security schemes and cryptographic algorithms used in the WSN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration of results</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PreDoctoral Exam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Writing thesis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Writing of Articles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Courses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjustments in thesis redaction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doctoral exam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Green**: Completed
- **Yellow**: In progress
- **Gray**: Uninitiated

Brisbane Ovilla Martínez

PUF based security for wireless sensor networks
Conclusions

- It is necessary to provide security services for WSN applications to protect their information.
- In a WSN is important to deal with limited resources and to preserve energy.
- Key management is one of the most important aspects in security WSN.
- A PUF can be efficiently used in security applications.
- Make efficient use of energy consumption is vital for wireless sensor networks.
- Thesis’ main contribution will be on PUF-based security mechanisms for WSN.
Bibliography I

Pappu Srinivasa Ravikanth.

Kumar et. al

Eschenauer et. al

Zhu et. al.

H. Chan.

Huang et. al.
D. Lim.  

Suh et. al  

Suh and Devadas.  

Guimaraes et. al.  

Wander et. al.  

Walters et. al.  
Additional Material
## Plataform boards

<table>
<thead>
<tr>
<th>Plataform</th>
<th>Microcontroller</th>
<th>Frequency</th>
<th>RAM</th>
<th>EEPROM</th>
<th>FLASH</th>
<th>Current draw</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waspmote</td>
<td>ATmega1281</td>
<td>8MHz</td>
<td>8KB</td>
<td>4KB</td>
<td>128KB</td>
<td>AM:8mA, SM:8uA</td>
</tr>
<tr>
<td>IRIS</td>
<td>ATmega1281</td>
<td>8 MHz</td>
<td>8KB</td>
<td>4KB</td>
<td>512KB</td>
<td>AM:9mA, SM:64uA</td>
</tr>
<tr>
<td>MICA2/MICAz</td>
<td>ATmega1281</td>
<td>8 MHz</td>
<td>8KB</td>
<td>4KB</td>
<td>512KB</td>
<td>AM:9mA, SM:15uA</td>
</tr>
<tr>
<td>TelosB*</td>
<td>TI MPS430-16bit</td>
<td>8MHz</td>
<td>10KB</td>
<td>16KB</td>
<td>1024KB</td>
<td>AM:1.8mA, SM:5.1uA</td>
</tr>
<tr>
<td>Imote2</td>
<td>Marvell PXA271</td>
<td>13MHz</td>
<td>256KB</td>
<td>–</td>
<td>32MB</td>
<td>AM:31mA, SM:390uA</td>
</tr>
</tbody>
</table>