Lightweight and Energy-Efficient Implementation of an Unclonable WSN Nodes on PSoC

Ke Xue1,2, Mengxian Chen3*, Rui Xu1,2, Ziqian Zhang1,2, Yiting Cai3 and Feng Ma1,2

1NARI Group Corporation / State Grid Electric Power Research Institute, City Nanjing 211106, China;
2NARI Information Communication Science and Technology Co. Ltd., City Nanjing 210003, China;
3State Grid Zhejiang Electric Power Co., Ltd. Wenzhou Power Supply Company, City Wenzhou 325000, China
Email: *monicaxian@126.com

Abstract. An adversary can easily capture a wireless sensor network (WSN) node and extract the security information stored in the node, including keys, shared secrets and so on. Due to the resources limitation, the traditional encryption and authentication protocols are impractical on WSN nodes. In this letter, we proposed a lightweight and energy-efficient anti-clone design for the WSN nodes, in which physical unclonable function (PUF) is adopted to enhance the security of the WSN nodes. The new structure aims at achieving a low cost and low energy method to prevent the node to be captured and cloned by the adversary. Unclonable WSN nodes are implemented on cypress PSOC 4, in which a configurable PUF structure is accomplished by use the universal digital block. Experimental results show that the proposed system can prevent the capture and clone attack in wireless sensor network, which is unavailable in previous WSN nodes.

1. Introduction
Wireless Sensor Network technology is wildly applied in various domains of daily life, including medical monitoring, environmental and military surveillance etc. Wireless sensor networks are consisted by hundreds or thousands of sensor nodes. Once the WSN nodes have been applied to the target area, seldom there will be an operator monitoring and intervention. This can become a problem because the WSN nodes are exposed to the adversary. Each node represents a potential point of attack, making it impractical to monitor and protect each individual sensor from either physical or logical attack. One of the famous physical attack is called cloning attack, in which cloned nodes are introduced into the network. If the WSN nodes only utilize commercial hardware and at the same time operating systems are applied, legitimate nodes are easily to be caught by an adversary, and then make copies by clone them, and then introduce these cloned WSN nodes into the original network. The clones may even be selectively reprogrammed to subvert the network [1].

Different from the wire or wireless device supply a power source, typical WSN nodes are powered by the battery, and usually cost effective, that means they have low capacity both in calculating and the memory. Due to these constraints, the general-purpose authentication protocols are not appropriate for WSNs. For example, the cost required to incorporate tamper-resistant hardware into sensor nodes is likely to be prohibitive. Public key cryptography approaches attempted to date are based on the RSA.
approach. Their energy consumption and computational latency makes them inappropriate for sensor network applications.

In this letter, we aim to find a resource efficient method to prevent cloning attack in sensor networks from hardware level in a lightweight and energy-efficient way. A novel structure based on physical unclonable function is presented, in which the WSN node employs a cortex M0 core and a unique and robust PUF encryption core. The proposed structure aims at achieving a low cost and low energy method to prevent the node to be cloned by the adversary.

The remainder of this paper is organized as follows. Section II discusses related work. Section III gives a detailed design of the unclonable wireless sensor network node, including the design of the PUF based on a WSN node. Section IV analyzes the proposed method and explains how we test our new design. Section V gives a conclusion of this paper.

2. Related Work

2.1. Clone Attack in Wireless Sensor Networks

As one of the urgent threats of the WSNs, clone attack has attracted researchers’ attention. Over the past few years, lots of algorithms and protocols for WSNs have been proposed to detect the clone attack, which can be classified into two different categories, centralized and distributed clone detection protocols. Centralized protocols utilize sink nodes to store the secure primitives of the sensors. When the source node send the private information to the sink nodes, the sink nodes will compare the information pre-stored inside it and then determine whether there is a clone attack. Different from the centralized detection protocol, distributed protocols have a set of witnesses, which are used to match the sensors in the network, consequently prevents the unauthorized transmission between the sink and sensors by malicious users [2].

To address the potential clone attacks, rather than detect it, there are two mainly method, one is solved from software level and another is based on the hardware level. At the software level, sensor networks need new capabilities to ensure secure operation even in the presence of a small number of malicious network nodes. Achieving these goals needs a very large resources. Another method is to build a temper-resistant hardware, which will prevent the adversary to extract the secret from the captured WSN nodes. Therefore the adversary cannot clone a same WSN node from the existed node. In this letter, a temper-resistant hardware based on PUF is proposed and discussed.

2.2. Physical Unclonable Function

A PUF can be viewed as a digital fingerprint of the electronic devices. Like the biometric fingerprint, the PUF is unique to the device it is implemented on and is, in theory, unclonable. This allows the same product to be utilized as a hardware trust anchor for a various range of potential use cases. The PUF is a function that takes in a challenge and returns a response. However as this function is based on the underlying hardware itself, this response is unique to both the challenge supplied and the device that it is implemented on.

![Configure Set for TCRO PUF](image)

PUFs exploit the fact that no two ICs are exactly the same, and that small differences exist at the microscopic level between seemingly identical chips. These differences are due to the random process variations during circuit manufacturing and exist even where ICs are fabricated on the same wafer.
Due to the random nature of these variations, they are essentially unclonable even to the device manufacturer themselves.

3. Concept and Circuit Design

In this letter, a lightweight and energy efficient unclonable WSN nodes is designed and implemented. As shown in Fig.1, the proposed unclonable WSN node mainly consists of MCU module, PUF encryption module, RF module, reconfigurable sensor interface module and battery module. The MCU module is implemented based on PSoC 4 and it has one ARM Cortex M0 core, in which a Contiki WSN operating system is integrated. The PUF module generates the challenge and response pairs (CRPs) to identify the WSN nodes and prevent illegal access to the wireless sensor networks. The radio module give the WSN node the ability to communicate with other WSN nodes or WSN gateways and the radio follows IEEE 802.15.4 standard. The reconfigurable sensor interface module enhance nodes the ability to integrate the common sensor without resign the circuits, include both digital interface sensors and analog interfaces.

![Figure 2. The structure of the proposed unclonable WSN node](image)

3.1. Unclone Design Based on PUF

Due to limited resources in WSN node, a lightweight PUF structure is adopted to extract wire and gate delay difference. A configurable ring oscillator PUF with improved uniqueness was adopted [3]. The structure of the configurable RO PUF is shown in Fig. 2. The CRO PUF is consisted of a chain of inverter delay units. Each inverter delay unit is composed by a multiplexer and an inverter, and the multiplexer is used to select the transmission paths for signals. To make the circuit oscillate, the number of the inverters in the CRO circuits must be odd.

![Figure 3. Typical CRO PUF scheme](image)
The CRO PUF adopted including three main modules: the mapping module, which transfer the challenge signal to configure signal for the CRO PUF; the PUF cell array, which compose the basic circuits for the PUF application; the control module, which controls both the mapping module and the PUF cells array. In the PUF cells array, a counter is utilized to count the output frequency of the oscillations; a register is used to store the output of the counter temporarily. As a sequence, a response bit can be generated by comparing the output frequency. Due to the unpredictable variations in fabrication, the delay of the multiplexer and the wires will cause difference in delays. In the design of a CRO PUF, every component is identically routed, the output frequency of any two picked up pairs will verify due to the variations in manufacture. Even the manufactory itself cannot clone the challenge and response pair, thus these challenge-response pairs can be used to authentication an access in the wireless sensor networks and prevent the clone attack and capture attack.

The CRO PUF is implemented based on the universal digital blocks (UDB) in PSoC4200. There are four individual UDBs in PSoC 4200, and each UDB is composed by two programmable “12C4” PLDs. The block diagram of a single UDB is illustrated in Figure 4.

In our design, we implement our novel secure PUF design in the UDB module, which we used to encrypt the WSN node.[reference] the function of the PUF is write in Verilog and synthesized and mapped to the PLD blocks by the PSoC Creator. In order to balance the routing, control files and directives are used to specify the designs.

![Figure 4. Single UDB Block Diagram](image)

3.2. WSN Functional Implementation

The main functional operation of a WSN node is accomplished in the ARM Cortex M0 processor inside PSoC 4200. The processor is an energy-efficient solutions for IoT applications, which is cost-competitive compared to traditional 8-bit or 16-bit processors while offers 32-bit performance. [5]. The maximum operating frequency of the CPU is 48MHz, which means with the CPU core, the WSN nodes can deal with various computing and communication easily.

Once the WSN nodes have been applied to the target area, seldom there will be an operator monitoring and intervention, include the battery. Sometime there will be Gateway WSN nodes powered by solar systems, however they also suffer a unstable supply voltage. PSoC 4200 support a wide supply voltage from 1.71V to 5.5V, which is extremely suit for WSN nodes powered by battery and small solar systems. Meanwhile the PSoC 4200 has a 20-nA stop mode with GPIO pin wakeup and hibernate and deep sleep modes allow wakeup-time versus power trade-offs.

To obtain the best performance of the WSN communications based on the constrained hardware, an operating system for the wireless communication is needed. Over the past years, different approaches to implement the operating system specifically for WSNs appeared, such as TinyOS, Contiki, MANTIS,Nano-RK, LiteOS and so on. In this letter, we adopt Contiki as the OS for the WSN node.

Contiki, as one the most popular operating system for wireless sensor networks, has been widely studied and researched recently, because it is lightweight open source operating system and it is friendly with C that means it is highly portable.
A typical Contiki configuration consumes 2 kilobytes of RAM and 40 kilobytes of ROM. A full Contiki installation includes features like: multitasking kernel, preemptive multithreading, proto-threads, TCP/IP networking, IPv6, a Graphical User Interface, a web browser, a personal web server, a simple telnet client, a screensaver, and virtual network computing.

![Contiki Architecture Diagram](image_url)

**Figure 5.** the block diagram of the Contiki architecture

The Contiki OS follows the modular architecture. At the kernel level it follows the event driven model, but it provides optional threading facilities to individual processes. The Contiki kernel comprises of a lightweight event scheduler that dispatches events to running processes. Process execution is triggered by events dispatched by the kernel to the processes or by a polling mechanism. The polling mechanism is used to avoid race conditions. Any scheduled event will run to completion. However, event handlers can use internal mechanisms for preemption.

### 3.3. Wireless Communication Module:

Previously, CC2420 and CC2430 from Texas Instruments are widely used in WSN nodes designs. The difference between two chips is that CC2430 has one MCU core while CC2420 doesn’t have it. In this letter, we choose CC2520, which is the upgrade vision of CC2420 as the communication radio. The radio module uses the SPI interface to connect with the ARM Cortex M0 core. This chip offers excellent link budget, operation up to 125°C and low voltage operation, while has a good selectivity and co-existence. Besides, the chip give a hardware solution for data buffering, data encryption, data authentication, clear channel assessment, link quality indication and so on. These can significantly reduce the load on the target MCU or embedded processor. In addition, compare with CC2420, CC2520 has a lower operating voltage and a smaller package size, which means it has a lower cost and lower power consumption during the same condition.

### 3.4. Reconfigurable Sensor Interface.

Sensors also play a very important role in WSN nodes. Only if they can work properly and collect information correctly, then the wireless sensor network can mean something. They are numerous different sensors designed to transfer the analog environmental parameters to digital, which the wireless sensor network can deal with. A reconfigurable intelligent sensor integrated interface is also implemented in this letter, the designed intelligent sensor interface integrates both analog interface sensors and digital interface sensors.
By using the programmable analog inside programmable analog, the reconfigurable sensor interface can easily integrated the analog interface sensors, including light intensity sensors, air pressure sensor and so on. The programmable analog unit contains one 12-bit 1-Msps SAR ADC, one integrated low-power opamps, two comparators and analog multiplexers, and all of this can work normally while the CPU and other system blocks are disabled during the low-power operating modes, which means the intelligent analog sensor interface will be cost effective and energy efficient.

The digital interface sensors are also been take into accounted. The Serial Communications Block of PSoC 4200 can be configured as a typical protocols, such as UART, I2C and SPI. However only one interface can be accessed at the same time. If the users need additional instances of the a UART or SPI interface, it can be implemented using the universal digital blocks. Also the GPIO can be programmed as a digital communication port, just like 1-wire communication protocol used in temperature sensors. Based on this, digital interface sensors, including temperature sensors, humidity sensors can be easily integrated through the intelligent digital interface.

4. Results and Discussions
In this letter, we aim to design an unclonable WSN nodes in a cost effective and energy efficient way. The proposed prototype has been designed and implemented base on PSoC 4200. Ten unclonable WSN nodes are deployed to test its performance. The picture of the implemented nodes is shown in Figure 7.

Hamming distance of PUF responses is an important metric in evaluating the quality of a PUF design. Consequently, we can also use this metric to evaluate the unclonable WSN nodes. The Hamming distances of the inter-chip responses $H_{\text{inter}}$ denotes the ability of an unclonable WSN node to be uniquely distinguished among a group of nodes. As shown in Fig. X, the distribution of $H_{\text{inter}}$ follows a normal distribution and the values of $H_{\text{inter}}$ are closely and nearly symmetrically placed around the mean value of 50%.
We also performed the our proposed scheme especially on the security front, our proposed scheme has been compared with five state-of-the-art protocols in WSN, as shown in Table I. From Table I, it is clear that the proposed scheme can resist various security threats existing in previous authentication environment in WSN. In contrast, the protocols presented in [1], [2], [3], [4], and [5] are unable to ensure the clone attack and the capture attack. Even though protocols presented in [6] and [7] can ensure user anonymity property without performing any exhaustive search operation or without having any backend channel; however, these schemes are vulnerable to DoS attack. In addition to that none of the existing scheme can ensure the physical clone attack, which is highly imperative for any session-key based authentication protocol.

5. Conclusion
In this paper, we focus on cloning attack in wireless sensor network where sensor node may be captured by an adversary and reprogram it. We present a new tamper-resistant hardware structure to prevent this kind of attack, which utilize the random delay characteristics of the wires and transistors in the microchip of the WSN node. Even the foundry cannot build two chips with same response, thus the new design is unclonable. The proposed new structure is a lightweight solution since it does not need any extra resources. We demonstrate our new structure on Cypress PSOC 4 and the experimental investigation yielded values of and for uniqueness and reliability, which indicate that the circuits are very secure and robust. The proposed unclonable node design is especial suit for resource limited applications where clone attack may be happened.

6. Acknowledgments
Corresponding author is Mengxian Chen, Email: monicaxian@126.com.
This work is partially supported by the State Grid Corporation Science and Technology Project Funded "Key Technology Research on Trustworthy Identity Authentication of Grid Core Business" (52110418001L).
7. References

[1] Cheng, G.; Guo, S.; Yang, Y.; Wang, F. Replication attack detection with monitor nodes in clustered wireless sensor networks. Proc. the IEEE International Performance on Computing and Communications Conference (IPCCC), 2015, pp. 1–8.

[2] Khandare, P.; Sharma, Y.; Sakhare, S. Countermeasures for selective forwarding and wormhole attack in WSN. Proc. the IEEE International Conference on Inventive Systems and Control (ICISC), 2017, pp. 1–7.

[3] Wang, G.; Kim, S.; Kang, D.; Choi, D. Lightweight Key Renewals for Clustered Sensor Networks. Journal of Networks 2010, 5, 300–312.

[4] Kun, L.; Anna, X.; Fei, H.; Lee, D.H. Anonymous authentication with unlinkability for wireless environments. IEICE Electronics Express 2011, 8, 536–541.

[5] Wang, G.; Cho, G. Clustering-based key renewals for wireless sensor networks. IEICE transactions on communications 2009, 92, 612–615.

[6] Paral, Z.; Devadas, S. Reliable and efficient PUF-based key generation using pattern matching. Proc. the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2011, pp. 128–133.

[7] Guajardo, J.; Kumur, S.S.; Schrijen, G.J.; Tuyls, P. FPGA intrinsic PUFs and their use for IP protection. Proc. the International Workshop on Cryptographic Hardware and Embedded Systems, 2007, pp. 63–80.