SCA security verification on wireless sensor network node

Wei He, Carlos Pizarro, Eduardo de la Torre, Jorge Portilla, Teresa Riesgo
Universidad Politécnica de Madrid, Madrid, Spain
Centro de Electrónica Industrial

ABSTRACT

Side Channel Attack (SCA) differs from traditional mathematic attacks. It gets around of the exhaustive mathematic calculation and precisely pin to certain points in the cryptographic algorithm to reveal confidential information from the running crypto-devices. Since the introduction of SCA by Paul Kocher et al [1], it has been considered to be one of the most critical threats to the resource restricted but security demanding applications, such as wireless sensor networks. In this paper, we focus our work on the SCA-concerned security verification on WSN (wireless sensor network). A detailed setup of the platform and an analysis of the results of DPA (power attack) and EMA (electromagnetic attack) is presented. The setup follows the way of low-cost setup to make effective SCAs. Meanwhile, surveying the weaknesses of WSNs in resisting SCA attacks, especially for the EM attack. Finally, SCA-Prevention suggestions based on Differential Security Strategy for the FPGA hardware implementation in WSN will be given, helping to get an improved compromise between security and cost.

Keywords: WSN, side channel attack, EMA, power attack, hamming model, AES-128

1. INTRODUCTION

Side channel information, such as power consumption or electromagnetic leakage from a running electronic device are intrinsically data or process dependent. If these side-channel information could be properly gathered and analyzed by special methods, it's possibly to be used to retrieve secret data. Some are especially critical, such as the keys of cryptographic algorithms.

SCA-specific researches have been successfully conducted towards many kind of crypto-algorithm implementation [5][8]. The methods mainly include simple power analysis (SPA), differential power analysis (DPA), correlation power analysis (CPA), electromagnetic analysis (EMA) and fault analysis (FA) [1][15][22].

SCA differs from traditional mathematic crypto-analysis. It doesn't need excellent mathematic background which is normally necessary when making mathematic analysis. In order to avoid these threats, countermeasures could be adopted towards specific scenarios, for instance, masking or hiding[9-12]. However, added security implies added costs. In the realistic scenarios of cost-driven WSN (wireless sensor networks), massive number of nodes always require low cost for each one, low energy consumption, long lifetime and easy maintenance. The inherent characteristic of resource-constraints WSN make it not suitable for most SCA-security methods.

In this paper, we mainly focus our work on the SCA-concerned security considerations on WSN. We present SCA attack to the FPGA implemented AES-128 cryptographic algorithm on our own wireless sensor node. We survey the low-cost oriented setup, and give detailed setup of the platform and analysis to the results of different PA and EMA attacks.

The SCA-setup is based on CEI's WSN node-Cookie [13]. We adopt a broad range of special measures to make the setup low-cost. In a WSN scenario, unintentional EM leakage is more possible. We setup far-field attack environment, and successfully make 1-meters far-field EM attack. The details of the platforms will be given. The selection of EM antenna will also be introduced. SCA-Prevention suggestions of DSS (Differential Security Strategy) for the FPGA hardware implementation in WSN will be given, helping to make an optimal tradeoff between security and cost.

The rest of the paper is structured as follows. The basic knowledge of SCA will be explained in section 1, including side channel leakage sources, the power and EM attack model. In section 3, we analyze WSN's weakness to be attacked and fragility in resisting side channel attacks. EM leakage, which is more possible in WSN environment, will be stressed in large part. In section 4, we show the details of our testing platform of power attack and EM attacks respectively, including also far-field EM attack. The results of the attacks will be analyzed in section 5 and finally give the differential security strategy which aims to optimize the tradeoff between security and cost in WSNs. Section 6 shows the conclusions and future work.

2. SIDE CHANNEL ATTACK FUNDAMENTALS

In this section, we survey the source of side channel leakages, and show how they correlate with the data processed.

2.1 Side channel sources

Side channel attacks try to search and reveal the hidden connection between information and physical signals. The first time to predict the possibility of using electromagnetic leakage (EM) to make side channel attack is in [1]. Soon, the first solid EM side channel attack is done in [6]. Sound, fault, and timing are also studied [14-16]. In our work, we exclusively focus work on power and EM in WSN attacks.

The basic processing element in current digital circuits is the bit. Large number of bits have essentially large number of value possibilities. The state changes for processing different data lead to different physical characteristics. For instance, the different actions of charging, discharging and keeping in each clock cycle consumes different amounts of power in CMOS circuits. SCA primarily explore this type of leakages.

Normally, there are two types of power dissipation, static and dynamic power consumptions, comprising the total power dissipation in CMOS circuit. When the CMOS logic cell switches, the dynamic power dominant the total power consumption. Generally, dynamic power is comprised of charging current and short circuit current [3].

$$P_{char} = \frac{1}{T}\int_0^T p_{char}(t)dt = k_{char} \cdot f \cdot C_L \cdot V_{DD}^2 \quad (1)$$

$$P_{sta} = \frac{1}{T}\int_0^T p_{sta}(t)dt = k_{sta} \cdot f \cdot I_{peak} \cdot V_{DD} \cdot t_{sc} \quad (2)$$

Equation(1) is the description for the power consumption of charging the load capacitance of CMOS cells. Here, k_{char} , f, C_L, V_{DD} respectively stand for the factor, clock frequency, load capacitance, and supply voltage. In equation(2), I_{peak} means the peak short circuit current in each time short circuit occurs. t_{sc} is the time short circuit current exists. Actually, it's not necessary to get deep known about the details. Only the fact that dynamic power consumption is several orders of magnitude larger than the static one is enough and power consumption for charging and discharging actions are in the same order of magnitude. In side channel attack, the work is not to make the detailed research of how power consumption occurs, but to explore a macro regulation which could be used in constructing the general side channel model. Here, we estimate the power consumption from charging and discharging equally as 1 unit. Since different actions lead to different power consumptions, in this estimation, the power consumption could be treated as dada-dependent. Table 1 shows the simplified power model.

Table 1. Power Estimation Model

Actions	Previous Value	Current Value	Power Estimation (A)	Power Estimation (B)
Keeping	0	0	0	0
Charging	0	1	1	1.5
Discharging	1	0	1	1
Keeping	1	1	0	0

One big merit of side channel attack is due to the easiness to construct the attack model. For instance, transition of 0→1 always consumes more power that the transition of 1→0. Therefore power consumption estimation of transition of 0→1

could be set as 1.5 units, meanwhile, transition of 1→0 set comparatively smaller as 1 unit. In different devices, the type of device, type of cells, parasitic parameters differ much. Further, in most of cases, attackers have just very little knowledge about the targeted device, how the algorithm is implemented. All these make the use of very precise and uniform model impractical. However, rough estimation, like we used above, could still be useful in most cases. That means, no matter on which device the algorithm is running, FPGA, ASIC, microprocessor or whatever, rough estimation is effective and practical in most attack scenarios.

Generally, power consumption could be measured by means of directly detecting current in power supply or voltage drop of shunt resisters in the power supply wire. The detailed setup in our platform will be shown in section 4.

Similarly to power, electromagnetic leakages from different actions are also data-dependent. According to Faraday's Law, the electric potential induced V_{EM} is inversely proportional to the changing rate of magnetic flow.

$$V_{EM} = -N\frac{d\emptyset}{dt} \tag{3}$$

and,

$$\emptyset = \iint \vec{B} \cdot d\vec{S} \tag{4}$$

Here, $\vec{B}$ is the strength of magnetic field and $\vec{S}$ is the area $\vec{B}$ penetrates.

In Biot-Savart equation, I is the changing current which is correlated to the data processed. $\vec{B}$ is inversely proportional to the parameter r that represents the distance from the current to the place where the V_{EM} is induced. That means, the closer the distance, the larger $\vec{B}$ is, and subsequently a larger absolute V_{EM} could be obtained.

$$\vec{B} = \frac{\mu_0 I}{2\pi r} \tag{5}$$

In the Electromagnetic test, self-made multi-turn coil antennas are used to pick up the magnetic radiation. Therefore, the antenna should be placed close to the cell which produced the EM signals so as to get better EM radiation.

Since V_{EM} is indirectly correlated to the current I, and I is data-dependent, therefore, V_{EM} is also data-dependent. So, the same estimation as that used in Table 1 is valid as well.

2.2 Power / EM model

The 'Attack model' is the function used to predict the side channel signals. Hamming Weight (HW) and Hamming Distance (HD) models are the two models that are commonly used. In principle, HW model is to count the number of value "1" in digital circuits in one state S_0, represented as HW(S_0). HD model is to count the number of transitions ("'0" to "1" or "1" to "0") before and after a clock edge, therefore it involves two consecutive states S_0 and S_1, represented as HD(S_0, S_1)=HW($S_0 \oplus S_1$). Each model matches different situations.

For instance, for a group of 4 bits in 2 clock cycles, let's assume the previous state S_0= 0101, and next state is S_1= 1100. The term $S_{n.x}$ refers to the xth bit in clock cycle n. So, from S_0 to S_1, 2 bits are changed, i.e. $S_{0.4}$→$S_{1.4}$ ("0"→"1"), $S_{0.4}$ → $S_{1.4}$ ("1"→"0"). Therefore, HD(S_0, S_1)=HW($S_0 \oplus S_1$)=HW(0101⊕1100)=2. The value of 2 is the predicted power consumption from the HD model. In order to use HD model, two assumptions should be matched. changes from 0→1 and 1→0 contribute the same amount of power consumption. These are just the requirements from the estimations in Table 1. That's why HD could be used to reveal the hidden data-dependence. In some cases, the knowledge about the algorithm is too limited that the consecutive value of bits are not known. In these situations, HW model is the only option. HW model assumes the value of bits in either side is constant (all 0, all 1, or any fixed value).

2.3 Attack method

The idea of this attack is simple [3]. We guess all possible keys, and using these keys to predict the power or EM leakages. Then, we compare them with the real measured power or EM traces. Using correlation coefficients equation (6) to find one hypothetic group of side channel trace. For the one which matches the most, the corresponding key is the right key. Each attack round will find one byte (8 bits) of the total 128 bits key for AES-128. Therefore, 16 attack rounds could find the complete key. We emphasize that the same group of power or EM traces is used for different key byte's attacks.

$$r = \frac{\sum_{i=1}^{n}(X_i-\bar{X})(Y_i-\bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i-\bar{Y})^2}} \quad (6)$$

Since calculations depend on the correlation calculation, the more samples we have, the better the analysis results is likely to be. Therefore, in side channel attack, a large number of samples (power or EM traces) is needed. In our attack, we normally use 30,000 traces in power analysis and 10,000 in EM traces.

3. WEAKNESSES IN WIRELESS SENSOR NETWORKS

In this part, a brief security discussion is shown, which includes the WSN concerned threats and related protection mechanisms. Our test platform - Cookies WSN node is also detailed in this section.

3.1 Security issues in WSN

A wide range of applications for wireless sensor networks show much interest to attackers, especially in security sensitive areas, like military, financial and high-tech researches. One major characteristic for WSN is that the nodes in WSN are typically unattended. This provides more conveniences to the attacker to perform sophisticated attacks.

I. Threats to wireless networks

Threats to wireless networks can be classified into two categories. The first is physical attacks. In this kind of attack, attacker simply aims to physically destroy certain nodes in order to ruin parts or paralyze the whole networks. To prevent this attack, it seems there is no better solution than fortifying the nodes with hard protective case. However, this countermeasure more or less brings bad effect to the normal function of nodes.

Fortunately, in majority of case, attacker prefers more meaningful work towards WSNs, not just to physically damage them. These are non-physical attacks in which the attacker performs sophisticated work that could be categorized as invasive and non-invasive attacks [4].

A. invasive attack In this kind of attack, the attacker aims to bring soft errors to make the networks malfunction so as to paralyze the networks or to rob secrets. For instance, they implant malicious code to the node to: 1) Masquerade as the controller of this network to control other nodes; 2) modify the routing information to lead the confidential information to dummy nodes or black hole nodes; 3) Simply generate a lot of junk information to make traffic jam in communication channels.

B. non-invasive attack The difference between this attack and the previous one is that, it leaves very little or even no traces in the targeted networks during and after the attacks. That means, during the whole process of the attack, everything in the networks works normally. The task for non-invasive attacker is simply to steal secrets like keys of cryptographic protocols. After a successful attack, everything in this network is transparent to this attacker if the network users have no clues about it. Side channel attack is one of this kind of attack.

II. Defenses

Defense countermeasures are adopted to ensure the authentication, integrity and confidentiality of the information collected, processed and transmitted in WSN [17]. In order to elaborate these countermeasures clearly, we separate them into two major types, active and reactive.

A. Active protection mechanism In the type of active countermeasures, security protections are always existing and running. That means, no matter whenever the danger occurs, active counter actions could respond immediately. No trigger, no setup time is needed. If a network is protected by active protection mechanism, it's always in defense status. This type includes the existing / non-changeable hardware protection made on the level of circuit structure or non-reconfigurable protection protocols on networks.

B. Reactive protection mechanism Similar to the stress-reaction of animals, this type of protection needs the external trigger to activate the protections. In the safe situation, protection mechanism is in the state of hibernation. Once threats are detected or system enters into the state of security sensitive state, protection mechanism is activated in order to offer security protections. Reactive protection mechanism includes reconfigurable hardware modification and convertible network security protocol changes.

III. Comparisons

Compared with active mechanism, reactive protection greatly reduce the resource usage. In the safe situation, hibernation of protection system only consumes little resources, which consequently render other functions have more resources to use, such as more chip area, longer battery lifetime and bigger computing capabilities. However, this needs more complicated activation control system for the protection mechanism. It also risks missing threats if alarm trigger fails in certain situation.

It should be noticed that the security of any protection is relative. That means, no protection could obtain infinite security assurance. Security depends on the threat types, attack methods, time and attack efforts. For instance, a normal dual rail logic [2] protected circuit is strong in resisting power attack however it's weak in resisting EM attack. Most SCA-resistant protections gradually become weaker when attacker spends long time to analyze much larger number of side channel traces. Therefore, it's suggestive to combine different protections together to obtain a high security assurance, such as using periodically changing key to counter dedicated long time attacks.

IV. Constraints in WSN

Full and high security protections are highly required during the WSN designing. The key factor that limits the security measures is the feature of resource deficiency. WSNs are always constrained in terms of battery, memory, computing capability and data transmitting rate due to the miniaturized node size. The tasks of processing and transmitting data always consume most energy and hardware resources in WSN, especially in the application area of multi-media monitoring. So, the security strategy with high efficiency in resource-scarce environment becomes mandatory. Simply increasing the node size cannot be feasible since the total cost becomes a critical factor when massively deploy the WSN nodes.

3.2 Cookie WSN node

Most of our tests run on the platforms which are based on Cookie WSN node [13]. Cookie is developed by Centro de Electrónica Industrial, Universidad Politécnica de Madrid, focusing on the wide requirements for WSN node with modularity, which makes the node easy to be deployed in a wide range of applications. Cookies are composed of four layers (more layers could be added depending on various requirements in different applications) as shown in figure 1. The four layers are: power layer, communication layer, processing layer and sensor layer, each one carries out their specific functions.

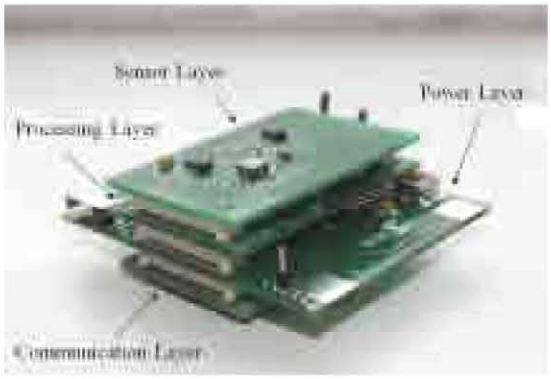

Figure 1. Cookie WSN node

These layers are detailed as follows:

1. Communication layer: The last version of this layer includes a ZigBee module (ETRX2 from Telegesis). This module is controlled by the uC through the UART port.
2. Power layer: This layer generates all the voltages needed within the Cookie. Two versions have been developed, the latest with USB included, which allows power supply from a PC and serial programming for the uC.
3. Processing layer: It's the core part of Cookie node. It includes an 8052 uC from Analog Devices (ADuC841) and a Xilinx XC3S200 Spartan 3 FPGA. The uC and the FPGA share three 8-bit ports for communication.
4. Sensor layer: This layer includes those elements which are intended to take measures from the environment. Up to now, several different layers have been developed for the Cookie. These layers include sensors of acceleration, temperature, humidity, light, infrared, PH value and strain of deformation.

Our SCA platform focus on the processing and power layers. In processing layer's Spartan 3 FPGA, AES-128 is running. We made necessary modifications to power layer for power attack setup, including removing the decoupling capacitor, inserting shunt resister and adding extra capacitor to stabilize the power supply. In EM setup, no changes are needed.

4. POWER / EM ATTACK PLATFORM

The detailed setups of power and EM tests are shown in this part.

4.1 Brief Introduction to AES

We choose AES [7] in our experiments due to its wide utilization in security applications nowadays. The name of AES is the acronym for Advanced Encryption Standard which was chosen as one of the candidates for the substitution of old DES (Data Encryption Standard) in US National Institute of Standards and Technology. It was finally ratified as the federal standard in 2002.

AES is the most recent encryption algorithm approved by US federal. According to modern security definition for cryptographic algorithm, the high security assurance of AES is due to the fulfillment of 2 criterions: first, there is no backdoor in the algorithm to be used to break it, i.e. brute force attack is the only way to find the key of this algorithm. Up to now, no backdoor of AES is found or reported in the literature. Second, depending on the current computing power in the world, breaking the algorithm by brute force is not possible within a acceptable scale of time.

AES is a symmetric cryptographic algorithm. The commonly used key size are 128 bit, 192 bits, and 256 bits. The key and data in AES are processed in block of 128 bits (state). Every state block is divided into 16 sub-blocks of 8 bits each. The complete process involves the cyclic executions of 4 types of operations: SubByte, ShiftRow, MixColumn and AddRoundKey [7]. The number of iterations for AES-128, AES-192 and AES-256 are respectively 11, 13, 15. All

rounds have all 4 types of operations except for the last round that misses the operation of mix column, as shown in figure 2.

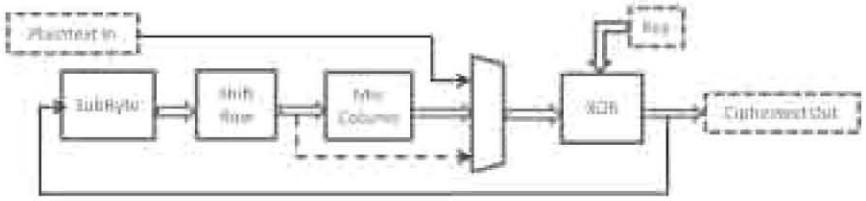

Figure 2. AES Cryptographic Algorithm

AES-128 algorithm [18] in Xilinx Spartan 3 FPGA is implemented in testing platform. We choose the output of the Sbox in the last (11th) AES round as the attack point. For the convenience of the far-field check, an simplified AES is compiled for EM attack. In the simple AES, key and data size are compressed to 8 bits in which only the operations of add round key and sub bytes exist.

4.2 Setup of power consumption attack

Depending on CEI's Cookie WSN node, we setup our SCA testing platform. Setups for both power and EM attack will be shown in this section.

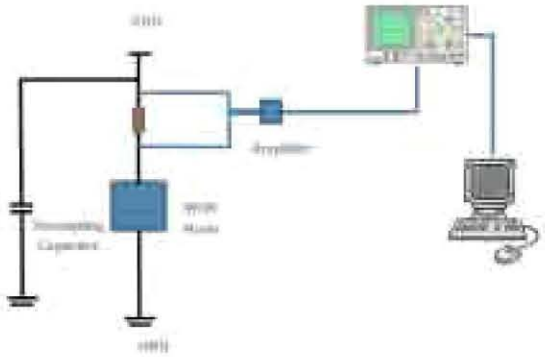

Figure 3. AES Cryptographic Algorithm

Figure 3 is the illustration of power consumption setup. In order to test power consumption of the node, a shunt resistor is inserted into the power supply VDD (small picture in Figure 4). The voltage drop across the resistor is measured and amplified by an analog amplifier. the amplifier is necessary if differential voltage probe is not available in measuring the voltage drop of shunt resister in VDD but not GND. An Agilent oscilloscope is used to repeatedly collect and transfer power traces into the Matlab workspace running on PC. There is no specific rule to choose this kind of trigger. It should be pointed out that the trigger signal is used in our setups in order to repeatedly trigger the oscilloscope to collect and transfer power or EM traces. Actually, in realistic scenarios, there are normally no such existing trigger to be used. Typically, the attacker have to try to find a substitution signal or collect a single and very long trace, and then precisely partition it by some skills [3][19]. We emphasize that it's possible. But it's not a critical issue in our work, so we intentionally generate the trigger signal so as to make our tests easier to be implemented. In real situations, any kind of signal that demonstrates the beginning or ending of the algorithm could be adopted. If no trigger signal is available, alignment method could also be used [19].

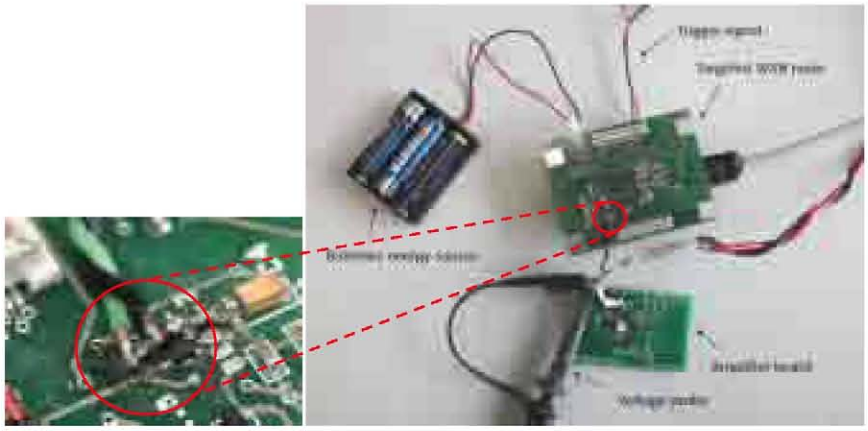

Figure 4. Platform of Power Attack on Cookie WSN node

Actually, power measure is a kind of contacting attack, which render it not so optimal in reality. In the modern WSN application, warning system could be activated in case of any unexpected trigger action.

4.3 Setup of EM attack

The electromagnetic attack is a kind of silent, contactless attack. The EM setup is generally simpler than that of power consumption attack. EM collecting equipment just need to be deployed in certain position near the running cryptographic device, no need to search for the power supply wire, to insert the resistor, to remove decoupling capacitors or to connect the voltage or current probes to the device. In this paper, we first show the near-field EM attack, which is the commonly studied type of EM attack. In principle, far distance attacks allow the attacker to circumvent WSN security protections. Here, we also show the far-field EM setup on which the EM attack could be successfully implemented, with distances of 1 meter, or even further. It should be noticed that the magnetic signal here is not the wireless signal from the communication level.

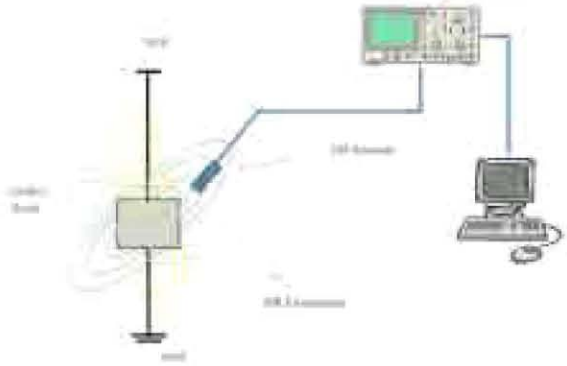

Figure 5. EM attack platform

The designed EM probe is a self-made multi-turn coil antenna [20]. The design parameters are: copper wire diameter: 0.4mm; antenna diameter: 4mm; antenna turns: 25. We checked many antenna types, and this one had the best performance for the close-field attack in our platform. According to equation (5), parameter r should be as small as possible in order to get stronger EM field. A easier result may suggest to decapsulate the chip in order to deploy the antenna in extremely close position. However, such deliberate preparation is not preferable in real situation, even not easy in a well-equipped laboratory. Not to mention that this operation makes the contactless non-invasive attack become an contacting invasive attack.

I. Close-Field EM Setup EM side channel information collected is normally concentrated to a small area around the CMOS cell targeted. That's because we set the antenna precisely to the targeted cell. The EM strength from this cell in this position is much stronger than EM field from other cells. Consequently, the interesting EM radiation counts for a larger part of total. That's why if the EM setup is proper, less measured traces are needed to break the key. As we mentioned before, in majority of cases, it's not easy to search and place the antenna to such a precise position. We retreat to the idea of making power attack, setting the antenna to a close place to the power supply pins or, depending on the attack type, to the output pins of AES algorithm of the chip. It's easier than making a laborious surface scanning to find the position above the tiny targeted registers. Figure 6 shows the EM platform for the close-field attack.

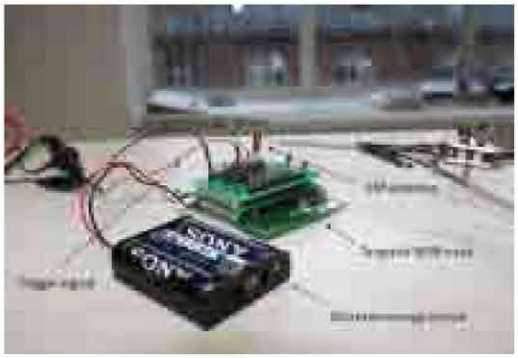

Figure 6. Platform of EM close-field attack on Cookie WSN node

II. Far-Field EM Setup In real application of WSNs, the non-invasive attack to the unattended node from a far distance produces more serious security threats than invasive and close field attack. If it's a successful far-field attack, no trace will be left. Consequently he WSN security mechanism will not be triggered. The Stress-Reaction security strategy will absolutely fail. Therefore, such an attack is the major security threat in the resource-deficient WSN environment. Figure 7 is the setup of our far-field EM attack. The difference here is that we strengthened the EM field by connect the ciphertext output pins of AES-128 to external wires. By this means, output EM field is strengthened and could be detected by self-made EM antenna from a far distance. In our setup, we test it in a distance of 1 meter away with a bigger antenna. According to equation (4), bigger antenna has a larger area $\vec{B}$, it helps to increase the magnetic flux and subsequently increase the induced voltage V_{EM}.

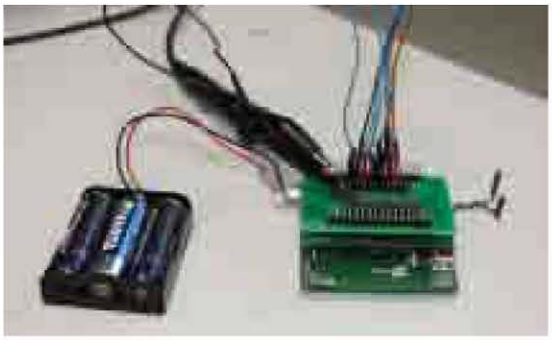

Figure 7. Platform of EM far-field attack on Cookie WSN node

5. ATTACK RESULTS AND ANALYSIS

Both power and EM attacks to WSN node are successful. A detailed result analysis is give in this sections. The possible SCA leakage ways are summarized which should be noticed in the designing for security-concerned WSNs. Primitive idea of strategy security strategy is also discussed.

5.1 Result analysis

Power Attack As we mentioned before, the last round of AES encryption is targeted. The algorithm run repeatedly 1000 times. Depending on Segmented memory, 1000 traces are gathered and then transferred to the PC in each collection time for the side channel analysis. The sampling rate of the oscilloscope is set at 35.1MSa/s. The working frequency of the WSN node is 86.4KHz. Typically, the power variation (voltage) that contains the meaningful information is smaller than 2mV, which is also the normal minimum vertical resolution of oscilloscope. We have to use an amplifier to make such small variation bigger if an active probe is not available. For the amplifier AD623A, when the gain is in the range from 10-100, bandwidth is from 100-10 KHz. In our test, we set gain at 30, so we have to slow down the working frequency to a low level 86.4KHz in order to ensure sufficient distinction of power variations.

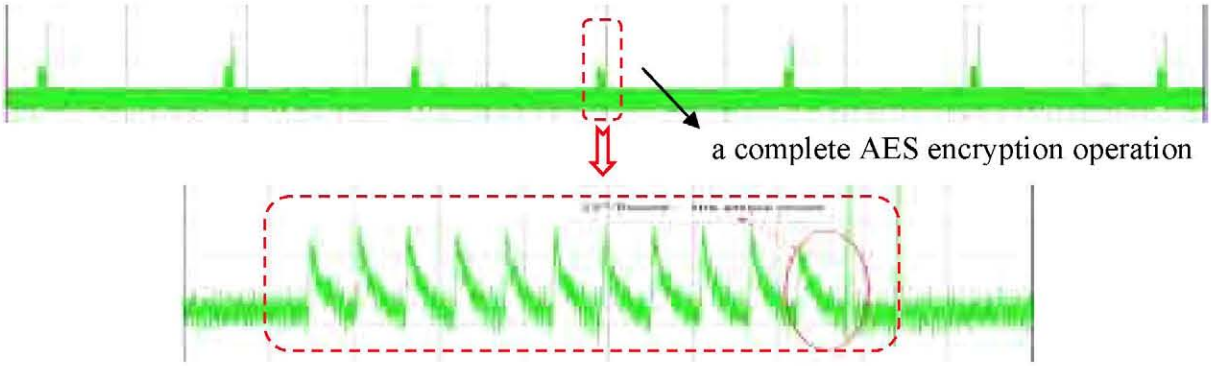

Figure 8. 11 peaks represent the 11 iterations in AES-128, the last peak is the attack round in our test.

Figure 8 shows the power trace collected from the target node. The number of power traces used in each analysis is 30,000. The success rate of getting the right key increases when the number of power traces is increased. This could be clearly seen from Figure 10. This is the correlation trend following the increasing number of power traces. We see that since approximate 5,200 power traces, the correlation traces representing the right key can be differentiated from other keys' correlation traces. That means, the more traces we used in the statistical analysis, the more possibilities to reveal the hidden connection. Normally, we get most of the 16 final round key bytes successfully under 30,000 power traces.

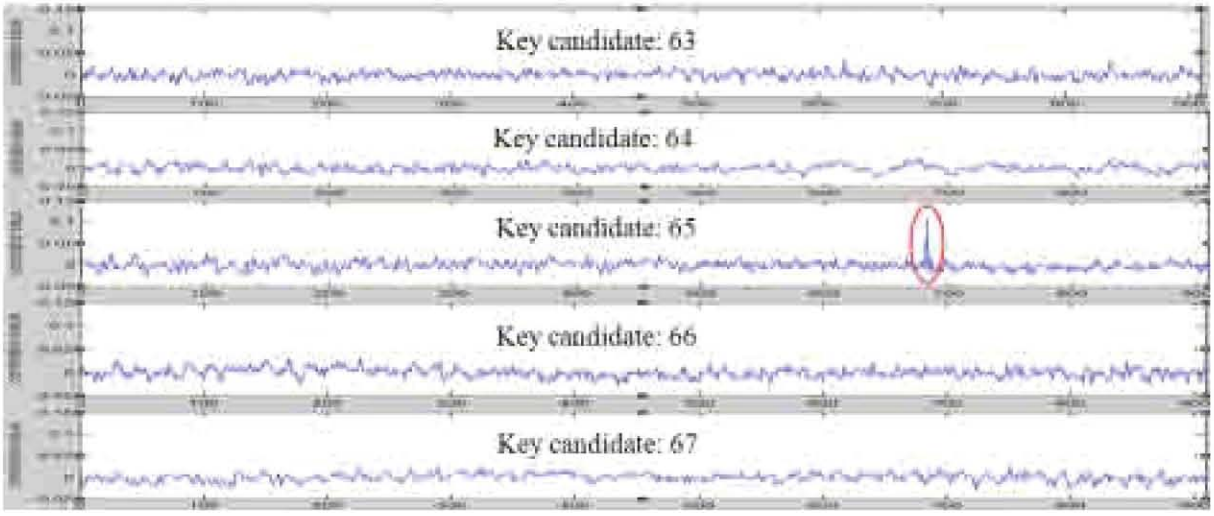

Figure 9. Only the correlation trace representing the right key has a very high peak.

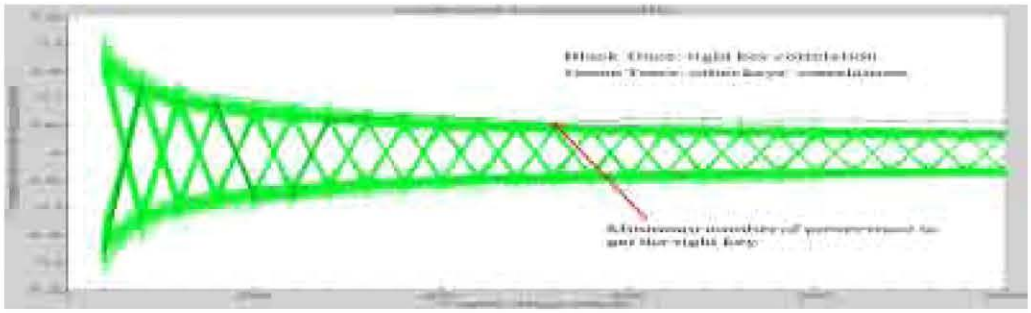

Figure 10. Right key emerges following the increasing number of the analyzed power traces.

EM Attack EM attack typically leads to better results than power attack. Since there is no such rigorous limitation for the bandwidth as in power attack, we set the working frequency of the target to the highest frequency of Cookie node, 11.0592MHz. Here, we use a simplified AES algorithm just for the convenience to connect the outputs to the on-board pins. Firgure 11 illustrates the simplified AES. Here, key and plaintexts are all 8 bits (the basic calculation block in complete AES algorithm). They are processed by bitxor operation and then substituted by AES Sbox to get the 8 bit plaintext. As well, we use all possible key (8 key bits for 256 possibilities) and known plaintext to predict the output of plaintexts, and then use the estimated EM model to transfer them into EM traces. Finally we compare them with the real measured EM traces. Similarly, the one that matches most with the real measure traces represents the right key.

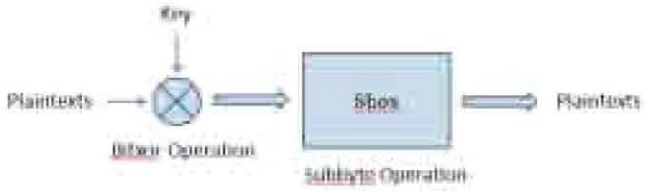

Figure 11. Simplified AES module

The EM trace is illustrated in Figure 12, This peak is caused by the transition of the output register. Since it is induced EM trace, the duration time for it is extremely short, typically less than 10 ns. That's why we could use EM way to attack the algorithm running on a very high clock frequency. However, we must ensure that the oscilloscope could run at a sufficiently high sampling rate. The height of these peaks is related to the changing of the current in the output register. This is just the meaningful information SCA explores.

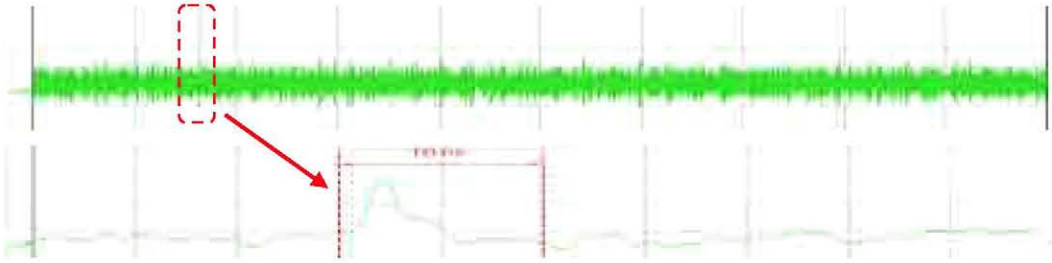

Figure 12. EM trace for the register transition

If the transition peak could be successfully sampled, by using the right analysis, results with high correlation peak could be obtained, as shown in figure 13 and 14. This is due to the characteristics explained in section 4.3. First, the EM trace is very specific to the target actions, not as power trace that contains the information from all the actions in the whole circuits. Second, the fast EM changes avoids much EM noise from the other actions, not likely to be covered by previous action's effects.

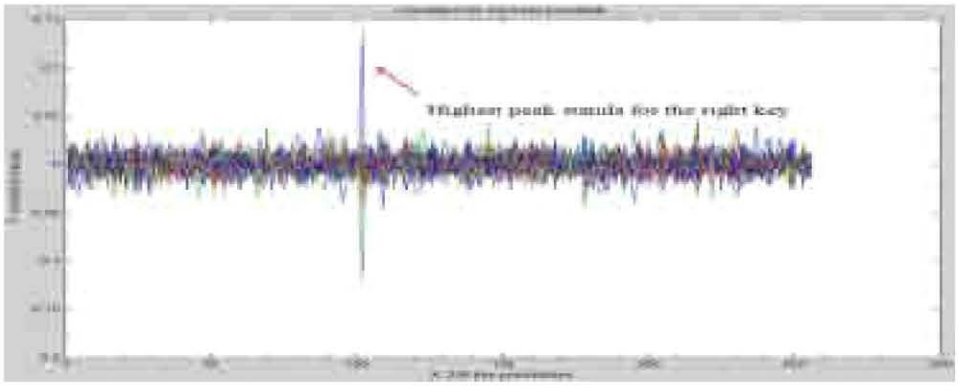

Figure 13. Higher correlation peak means guessed and measured traces are closely matched.

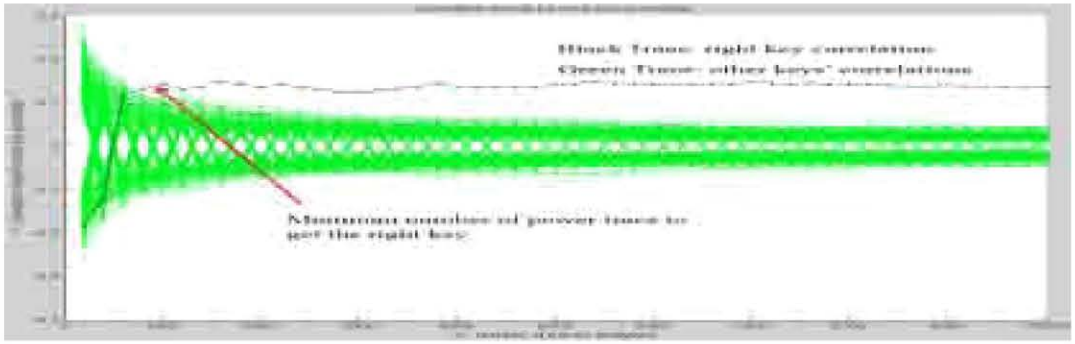

Figure 14. Compared with power attack, EM attack need much smaller number of traces to reveal the right key.

In previous papers, EM attack tests primarily focus on the CMOS cell which produces the interesting EM emanations. Therefore, attackers need to very carefully set the antenna to very precise position, even need to decapsulate the chip package in order to locate the minor targeted cell. Obviously, these deliberate measures reduce the practicability in realistic scenarios. According to the results of our tests, there are at least the following several sources leaking EM characteristics that could be used to make successful EM attacks.

1. The normally studied EM source directly from the targeted CMOS registers.
2. As the setup in figure 6, the onboard pins that connect with the proper outputs of the cryptographic algorithm.
3. The solder ball on the flip-chip BGA package that connect to the proper algorithm outputs, shown in figure 15 [21].
4. The decoupling capacitor that is used to stabilize the power supply for the chip. We emphasize that in power attack the decoupling capacitors tamper the power SCA. Therefore before the execution of power attack, decoupling capacitors are always removed. However, in EM attack, the fast-response decoupling capacitors could be used as the EM emanation source.
5. In some cases, the outputs, i.e. the ciphertexts, need to be transferred to other device. If they are transferred through wires, far-distance EM attack may be successful due to the strong EM leakage from these wires. Depending on a bigger EM multi-turn copper coil antenna, we get successful EM attack at more than 1 meter away from the targeted WSN node.

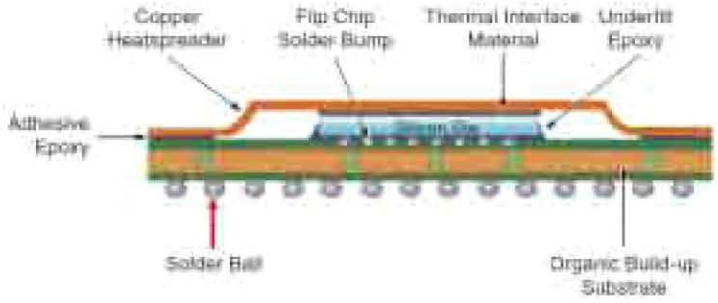

Figure 15. Proper solder balls in the bottom of board leaks EM characteristics.

5.2 Differential security strategy

In WSNs, higher computing, transmitting, processing capabilities are demanded to meet the high performance needs. In order to control the total costs, only mean security measures are adopted for the protections against all sorts of threats. This will or have already imposed critical problems for the security issues in WSNs. Security is always a tradeoff between cost and requirements, but this is particularly true in the WSN applications. Constraints in resource-scare environment, like WSN, greatly limits the freedom to choose the security measures. DSS (Differential Security Strategy) is provided here which aims to find a way to get best match between security and cost.

In a different scenarios, security levels required are different, even in the same WSN, from one node to another. For instance, battlefield monitoring WSN has much higher security needs than security required in PH value detecting networks in a coffee factory. The aggregator node of the WSN in bank systems has more strict security level than the normal payment terminals in the same system. Uniform countermeasures against attack is not suitable to different applications considering the budget because of the mass and diverse applications. The core idea of DSS is classifying and quantizing the security requirements for each node and cost for each measure, and then use mathematical model to find the optimal tradeoff between cost and requirement. We still focus on the threats from side channel attacks and give a simple example as follows.

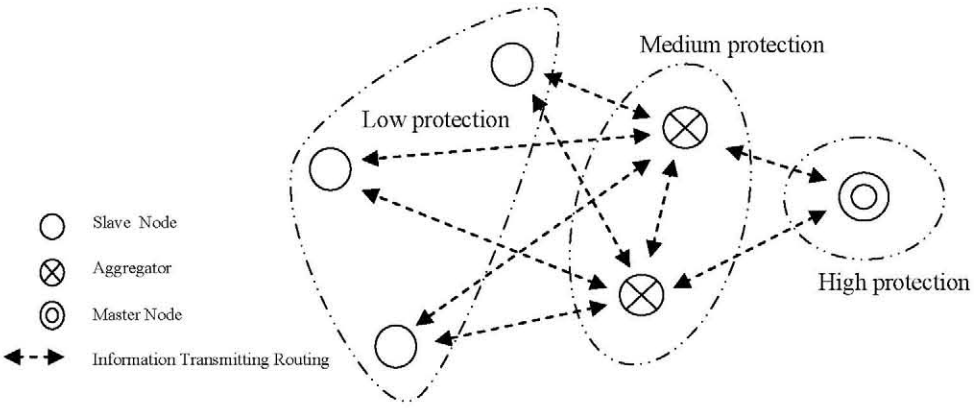

Figure 16. Partition of nodes in WSN

In the WSN network shown in figure 16, three node types are deployed. Slave nodes are responsible for data acquisition. This kind of node is massively deployed and has lower security requirements. Aggregators relay and pre-process the data collected from the slave nodes, they are deployed in a smaller number. They are prone to be attacked since they are the pivots for information transmission. The master node is the final control node which summarizes data, sends orders and controls network states, only one master node is deployed in most cases. In DSS, different security protections are adopted in different nodes. For the slave node, only the information collected around each oneself is transmitted in these nodes, it's not so attractive as the aggregator which replays information from a large number of slave nodes. Therefore, Basic security measures that consume low energy, occupy small chip area and low computing power could be adopted.

For aggregators, they are more attractive targets. Medium protections are suitable. Since the number for these nodes are not great, more expensive hardware resources could be configured in order to meet the medium security requirement. For the master node, it's the most valuable node for the attackers since it contains all information in this WSN. Normally, there is just one of this kind of node in a WSN system. We suggest to configure rich hardware resource so as to employ sophisticated and full protection to it. Quantizing security needs, resource available and costs are possibly to use the mathematical model to calculate the optimal matching point for these different parameters and finally find the best tradeoff between cost and security.

6. CONCLUSIONS AND FUTURE WORKS

We implemented the cryptographic algorithm AES-128 on a WSN node - Cookie, and give the details of our low-cost, but effective power and EM SCA platforms to this WSN node. We surveyed and categorized the threats of modern WSNs, and analyzed the weakness of WSN facing side channel threats, particularly for threats from EM attacks. According to the testing results, we get the merits and demerits of power and EM attack against WSN nodes. Also, the different sources of EM radiation are presented and successful EM attacks results are obtained respectively depending on these different leakage sources. This shows that a wide range of security weaknesses exist on WSN nodes in resisting EM attacks. We also analyze the conditions to execute the far-field EM attacks which impose special security concerns to WSN nodes. Finally, the idea of differential security strategy is shown aiming to get an optimal balance between cost and security requirements.

Future work will focus on the countermeasures against WSN specific power and EM attacks. We depends on the dual-rail [11-12] logic to implement the EM-resistant countermeasures in order to accustom it to the resource-deficient WSN environment. On the other hand, we will try to find suitable mathematical models to properly describe the quantized security and cost factors in differential security strategy suitable for WSNs.

Acknowledgements.

This work was partially supported by the Artemis program under the project SMART (Secure, Mobile Visual Sensor Networks Architecture) with number ARTEMIS-2008-100032.

REFERENCES

[1] Kocher, P., Jaffe, J. and Jun, B., "Differential Power Analysis," Proc. Cryptology (CRYPTO), 388-397 (1999).

[2] Tiri, K. and Verbauwhede, I., "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," Proc. DATE, 246-251 (2004).

[3] Mangard, S., Oswald, E. and Popp, T., [Power Analysis Attacks - Revealing the Secret of Smart Cards], Springer Science+Business Media Publishers, New York, 28-31 (2007).

[4] Healy, M., Newe, T. and Lewis, E., "Security for Wireless Sensor Networks: A Review," Proc. SAS, New Orleans, LA, (2009).

[5] Coron, J. S., "Resistance against differential power analysis for elliptic curve cryptosystems," Proc. CHES, LNCS 1777, 292-302 (1999).

[6] Gandolfi, K., Mourtel, C. and Olivier, F., "Electromagnetic analysis: concrete results," Proc, CHES, LNCS 2162, 251-261 (2001).

[7] "Announcing the advanced encryption standard (AES)," Federal Inforamtion Processing Standards Publication 197, Nov 26, (2001).

[8] Jovan Dj. Golić and Tymen, C., "Multiplicative masking and power analysis of AES," Lecture Notes in Computer Science vol. 2523, 198-212 (2003).

[9] Akkar, M. L. and Giraud, C., "An implementation of DES and AES secure against some attacks," Proc. CHES 2162, 309-318 (2001).

[10] Chari, S., Jutla, C., Rao, J. R. and Rohatgi, P., "Towards sound approaches to counteract power-analysis attacks," Proc. CRYPTO, (1999).

[11] Razafindraibe, A., Robert, M. and Maurine, P., "Analysis and improvement of dual rail logic as a countermeasure against DPA," Proc. PATMOS, 340-351, (2007).
[12] Tiri, K., Akmal, M. and Verbauwhede, I., "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," Proc. ESSCIRC, 403-406, (2002).
[13] Portilla, J., de Castro, A., de la Torre, E. and Riesgo, T., "A modular architecture for nodes in wireless sensor networks", Journal of Universal computer science (JUCS), vol. 12, n° 3, 328 - 339, (2006).
[14] Shamir, A. and Tromer, T., "Acoustic cryptanalysis: on nosy people and noisy machines," Proc. EUROCRYPT, (2004).
[15] Biham, E. and Shamir, A., "Differential fault analysis of secret key cryptosystems," volume 1294, 513-525 (1997).
[16] Kocher, P., "Timing attacks on implementations of diffie-Hellman, RSA, DSS, and other systems," Cryptography Research, (1995).
[17] Zhou, L. and Haas, Z., "Securing ad hoc networks," IEEE Network, vol. 13, 24-30 (1999).
[18] www.aoki.ecei.tohoku.ac.jp/crypto
[19] Kasper, T., Oswald, D. and Paar, C., "New methods for cost-effective side-channel attacks on cryptographic RFIDs," RFIDSec, (2009).
[20] Peeters, E., Standaert, F. X. and Quisquater, J. J., "power and electromagnetic analysis: improved model, consequences and comparisons," VLSI Journal of Integration, 52-60 (2007).
[21] www.xilinx.com/support/documentation/user_guides/ug112.pdf
[22] Brier, E., Clavier, C. and Olivier, F., "Correlation power analysis with a leakage model," Proc. CHES, LNCS 3156, 16-29 (2004).