A Survey on the Cryptanalysis of Wireless Sensor Networks using Side-Channel Analysis

Terrence Moabalobelo[1, 2], Fulufhelo Nelwamondo[1, 2] and Hippolyte Djonon Tsague[2]
Department of Electronic and Electrical Engineering
University of Johannesburg[1], P.O. Box 524, Auckland Park 2006, South Africa
Tel: +27 12 8413387, Fax: +27 12 8414939
And Council for Scientific and Industrial Research (CSIR) [2]
PO Box 395, Pretoria 0001, South Africa
{TMoabalobelo, FNelwamondo, HDjonon}@csir.co.za

Abstract-Since the inception of side channel attacks, research has gone a long way in proving that embedded devices capable of running cryptographic algorithms are highly susceptible to these attacks. These attacks are non-invasive in which an attacker can obtain confidential information such as secret keys by simply observing the side channel information leakage (such as the power consumption, timing, and electromagnetic emanations). Wireless sensor networks are particularly vulnerable to these attacks as they are deployed in open environments with no protective physical shielding. In this survey paper, we give an overview of the side channel attacks (particularly power analysis attacks) against wireless sensor networks and in addition discuss some of the suggested countermeasures against power analysis attacks.

Index Terms—wireless sensor networks, power analysis attacks, side channel attacks, countermeasures.

I. INTRODUCTION

Wireless Sensor Networks (WSN) have been widely considered as one of the most important technologies of the 21st century [1]. They primarily consist of several autonomous sensors to collaboratively monitor physical and environmental conditions [2]. These sensor nodes are small in size and equipped with sensors, embedded microcontrollers, and radio transceivers. They do not only have sensing capabilities but also data processing and communicating capabilities. They are also application dependent and primarily designed for real-time collection and analysis of low level data in hostile environments [3]. It is this reason that they are well suited to a substantial amount of monitoring and surveillance applications. The examples of applications include; environment monitoring, military surveillance, intelligent communication, observation of critical infrastructure, and industrial process control. Majority of these sensor networks are deployed in hostile environments with active opposition [1] [2] [3]. Thus, the security of these networks is of utmost importance.

WSNs are particularly vulnerable to side channel information attacks. Side channel information is information that is leaked while a cryptographic device is performing cryptographic computations such as encryption/decryption and generation of certificates. If only one node is captured by the attacker, the impact on the complete network can be significant. An attacker can monitor the side channel information leakage, such as power consumption, timing, and electromagnetic emanations, for cryptanalysis if nodes are captured. Thus this serves as motivation to investigate the vulnerabilities of WSN to these types of attacks. Various cryptographic services required for the WSN applications involve not only solutions for data protection but also self-implementation concerns [4]. This paper surveys the feasibility of implementing power analysis attacks on wireless sensor networks and the suggested countermeasures.

The remainder of the paper is organized as follows: Section II introduces the concept of side-channel attacks. Section III presents the hardware characteristics that lead to the vulnerabilities of the wireless sensor nodes to power analysis attacks. Section IV presents a summary of the attacks, and the suggested countermeasures. Section V concludes the findings of this paper.

II. SIDE CHANNEL ATTACKS

The goal of side channel attacks is to extract private information, i.e., a secret key or even the implemented algorithm, from the physical behavior of the target device [4]. The attacker can use different variants of side channel attacks to deduce the inner workings of the software or the hardware of the node [5]. The attacker may use techniques such as power analysis (simple power analysis and differential power analysis), execution cycle frequency analysis, timing information analysis (on data movement into and out of the CPU), electromagnetic radiation analysis, acoustic emission analysis, etc. [5].

Figure 1 presents a classification of the attacks. In principle, any of the above side channels can be considered for an attack. This paper's focus is on the power analysis attacks (exploits the power consumption leakage).

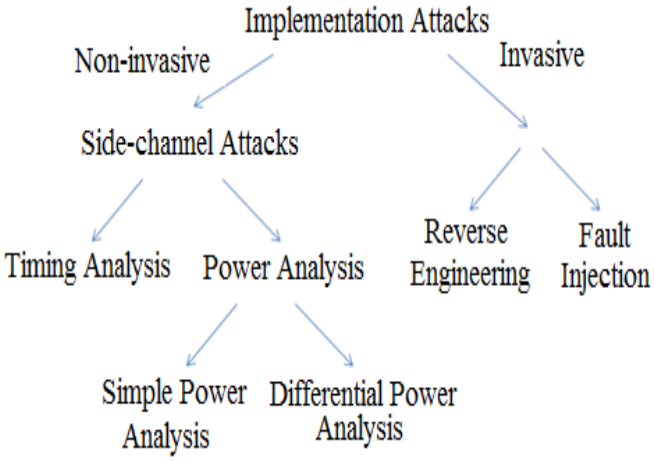

Figure 1: Classification of attacks (adopted from [4])

A. *Power Analysis Attacks*

The concept of power analysis attacks was first introduced by Kocher et al. [6]. This paper presents two basic variants attacks (simple power analysis and differential power analysis attacks). A simple power analysis (SPA) attack is a technique used to directly and visually inspect the power consumption signal measurements collected while a device is performing cryptographic operations. Differential Power Analysis (DPA) attack uses statistical analysis and error correction techniques to extract information correlated to secret keys of a cryptographic device [6]. In SPA, the information of a single power consumption measurement can be used for an attack. However, the attack can only be successful if the signal which the attacker wants to exploit is fully present in the obtained power trace. If the signal which the attacker wants to exploit is covered with a lot of noise, then several power consumption traces can be collected and statistical procedures can be used for signal analysis, which is referred to as DPA. An attacker using SPA is required to have a detailed knowledge of the cryptographic algorithm implementation on the device and also the device under attack; this is not the case for DPA [7]. An important feature of side channel attacks in general is that an attacker only monitors the device's emanations without actively interfering with its computations. Figure 2 show a typical power consumption trace used for an attack.

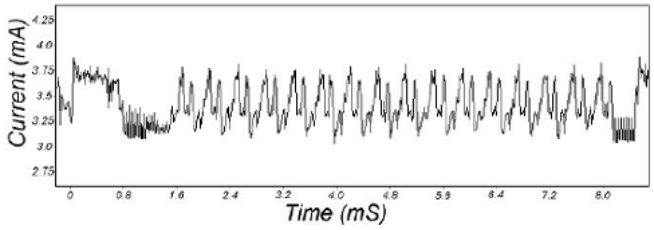

Figure 2: The power consumption of a DES [14].

By visually inspecting the figure one can clearly identify the 16 Data Encryption Standard (DES) rounds. The first round begins at approximately 1.6ms and the 16th ends at approximately 8.2ms.

The common setup for measuring the instantaneous current consumption is resistor-based, that is, a small resistor (of about 50Ω) is connected in series with the ground (V_{SS}) pin of the cryptographic device and the true ground (GND) of the entire measurement setup. An oscilloscope that is capable of sampling voltage differences at high frequencies with high accuracy can be used to measure the power consumption of a cryptographic device. Lee et al. [8] used the same setup described above to measure the energy consumption of AES, RC5, and XXTEA cryptographic algorithms implemented on MicaZ and TelosB nodes. Figure 3 shows the experimental set up for measuring the power consumption of a sensor node.

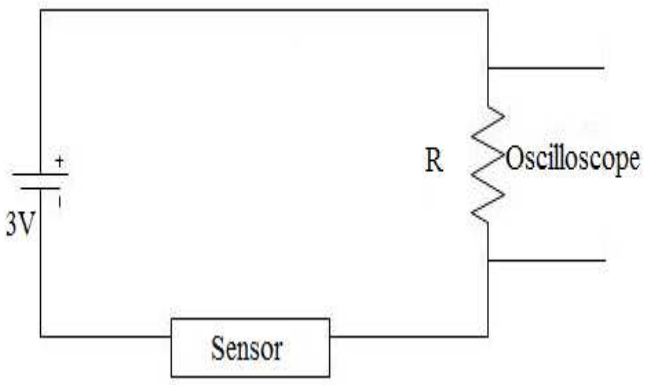

Figure 3: Power consumption measurement setup [8].

Side channel attacks are not supposed to interrupt the normal operation of a device. However, these attacks may not remain unnoticed when implemented to sensor nodes [9]. The reason for this is that, the attacker would have to remove the node from its deployment area to perform a power analysis attack. In wireless sensor networks regular communication with neighboring nodes is usually part of normal network operation [10]. Continuous absence of a node can therefore be considered an unusual condition that can be noticed by its neighbors [10]. Thus, making time a very important factor in evaluating attacks against sensor nodes, as the system might be able to detect such attacks while they are in progress and respond to them in real-time [10]. It is for these reasons that Meulenaer et al. [9] designed a measurement setup that lets the attacker acquire power traces from the node without removing it from the network or disturbing its normal operation.

III. HARDWARE CHARACTERISTICS

Sensor nodes typically consist of embedded hardware with low power consumption, and low computation power [10]. A typical node is comprised of a few sensors (such as motion, light, temperature, etc.), a radio chipset for wireless communication, an EEPROM chip for logging sensor data, a node-to-host communication interface and microcontroller which contains some amount of flash memory for program storage and RAM for program execution. Power is provided by batteries. Typical microcontrollers that are used in sensors nodes are the 8-bit Atmega128 or the 16-bit Texas Instrument MSP430familly [10] [12] [13]. They also have the amount of RAM varying between 2kB and 10kB and flash memory ranging from 40kB to 128kB [10]. External Electrically Erasable Programmable Read-Only Memory

(EEPROM) ranging from 8kB to 1MB. With the speed of radio communication in the order of 100kbit per second.

The microcontroller would be an interesting target for an attack, as it controls the core operation of the sensor node. Sensor networks are particularly vulnerable to side channel attacks due to the lack of protective physical shielding and their deployment in open environments [2]. Unprotected implementations often offer various possibilities for side analysis attack [7].

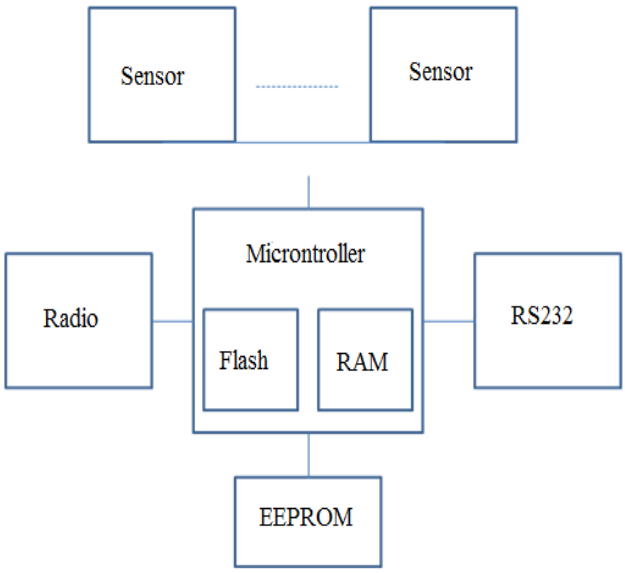

Figure 4: General schematic view of the sensor node hardware [10].

A large number of physical components of a sensor node are exposed giving the attacker sufficient closeness to specific modules of the sensor node in certain cases. Thus, under these circumstances, an attacker can initiate an attack on a part of the node by collecting leaked information that is available at close proximity.

IV. Attacks and Countermeasures

This section presents an overview of some attacks and the countermeasures that could be possible solutions to side channel attacks on wireless sensor networks.

A. *Attacks*

Kocher et al. first introduced power analysis attacks on the Data Encryption Standard (DES) [14]. They demonstrated that by carefully measuring the power consumption of a smart card running a DES algorithm, it was possible to determine the secret key of the algorithm. Subsequently, a lot of researchers took to the task of implementing power analysis attacks on cryptographic devices [15] [16].

Power analysis attacks can also be applied to sensor networks, as they use a microcontroller to run the cryptographic algorithms. Okeya et al. demonstrated the potential threat that is presented by power analysis attacks to sensor networks [17]. They present SPA as well as DPA attacks on Message Authentication Codes (MACs). Their results suggest that several key bits can be extracted through power analysis. Han et al. presented a solid DPA attack on the Advanced Encryption Standard (AES) hardware implementation for wireless sensor networks [4]. They first conducted three traditional power analysis attacks, Single-bit DPA [14], multi-bit DPA [14] and Correlation Power Analysis (CPA) [18], on the intermediated results of the AddRoundKey and the SubBytes. The first two attacks could not retrieve the correct subkey from 6000 power measurements. As for the CPA attack on the intermediate results of the AddRoundKey, the subkey was revealed based on 4000 power measurements. However, none of the three attacks were successful on extracting the correct subkey on the intermediate results of the SubBytes. Based on the results of the successful CPA attack, the authors make a point that the AES hardware implementation had the greatest probability that it could leak data-dependent power during its encryptions. Thus it was concluded that the linear (AddRoundKey and SubBytes) operations in the AES hardware implementations result in more data-dependent power leakages than other round operations [5]. Similar with CPA, the improved power attack extracted the correct subkey for the intermediate results of AddRoundKey from 5120 power measurements.

Side-channel attacks are usually carried out in a context where the possible attacker can control the target device, at least briefly [9]. This is highly impossible against wireless sensor networks. The specificities of wireless sensor networks scenario can be challenging for an attacker for the following reasons: passive acquisition, on-site acquisition, device not controlled, and real-world devices (see [9] for an elaborative description). Node compromise is a critical issue in wireless sensor networks. A popular approach to prevent the problem relies on the detection events that arise during the attack (loss of connectivity, removal of a node, etc.) [9]. Meulenaer et al. presented two solid case studies on power analysis attacks (DPA [19] and template-based SPA [20]) of AES and ECC implementations on two common types of nodes: MICAz and the TelosB [9]. For these attacks the authors considered a typical scenario of wireless sensor networks, where the nodes periodically exchange encrypted messages. These messages are encrypted with AES and ECC. The attacks are also restricted to the case where the on-site acquisition is convenient for the attacker: the nodes are easily accessible and the presence of the attacker at the site is not detected [9]. The authors developed a measurement setup that allows them to measure the power consumption traces of a node without interrupting its network operations (see Section 4 in [9]). This setup allowed the attacker to attack the last round key of AES, using DPA, and by inverting the AES key schedule led to the main key. Less than 40 and 80 traces were sufficient to recover the full second AES key on both MICAz and TelosB node, respectively [9]. Then their template-based SPA attack was on ECC. The authors only demonstrate the feasibility of the attack on both MICAz and TelosB nodes. With this work the authors proved the feasibility of implementing power analysis attacks without being detected in the context of wireless sensor networks.

The achievements presented above on wireless sensor network affirms the notion that power analysis attacks are a serious threat to wireless sensor networks.

B. *Countermeasures*

Power analysis of the power consumption of cryptographic devices depends on the intermediate values of the executed cryptographic algorithms [19]. The goal of every countermeasure is to make the power consumption of a cryptographic device independent of the intermediate values of the cryptographic algorithm. Countermeasures against power analysis attacks are classified into several levels [21]:

i. The transistor level: logic gates and circuits can be built in such a way that the information leakage is reduced. Tiri et al. [22] presented a countermeasure that secure encryption algorithms against DPA using logic gates. Their method makes use of the Sense Amplifier Based Logic, which its power consumption is independent of data signals. Sokolov et al. [23] also presented a concept of using Dual-Rail circuits for security applications;
ii. The program level: the order of operations can be randomized or dummy instructions can be inserted randomly to make the alignment of traces more difficult. This countermeasure interrupts the regular execution of the cryptographic process with dummy instructions [24]. In an Application-Specific Integrated Circuit, this countermeasure can be refined so that the attacker is not able to distinguish between a cryptographic operation from dummy operation that does not contain any activity related to the cryptographic procedure [24];
iii. The algorithm level (Masking): this technique prevents direct operations between key and data by adding a random 'mask' to data prior to the cryptographic operations. Possible solutions using masking as a way to protecting against power analysis attacks were also presented in [25] [26] [27].

With these being possible solutions to protecting against power analysis attacks, developers have to start considering the use of multiple countermeasures on cryptosystems. As a single implementation does not guarantee 100% protection, this would make the attacker's job much more difficult.

V. CONCLUSIONS

According to the observations made here it has been showed how powerful power analysis attacks are and that they are relatively easy to implement, thus making unprotected wireless sensor networks susceptible to these attacks. This is because the sensor nodes are deployed in unguarded environments without proper physical shielding. With regards to the countermeasures, no single countermeasure will provide sufficient protection measures. Thus when designing a cryptosystem, designers should consider implementation of multiple countermeasures (e.g., combination of transistor and algorithmic level).

VI. REFERENCES

[1] Zheng , J. and Jamalipour, A., "Introduction to Wireless Sensor Networks," in *Wireless Sensor Networks: A Networking Perspective. 1*, Zheng J. and Jamalipour A., Ed.: Wiley-IEEE Press, 2009, pp. pp. 1-18.

[2] Pongaliur, K., Abraham, Z., Liu, A., Hiao, L. and Kempel, L., "Securing Sensor Nodes Against Side Channel Attacks," in *High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 3-5 December 2008*, 2008, pp. 353-361.

[3] Padmavathi , G. and Shanmugapryiya, D., "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 4, no. 1&2, pp. 1-9, 2009.

[4] Schellenbrg, F., "Comparing Power and Electromagnetic Analysis of Embedded Devices," Ruhr-Universitat Bochum, Bachelor Thesis 2006.

[5] Han , Y., Zou, X., Liu, Z. and Chen, Y., "Improved Differential Power Analysis Attacks on AES Hardware Implementations," in *International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'07)*, 2007, pp. 2230-2233.

[6] Kocher , P., Jaffe, J. and Jun, B.. (1998) Cryptography Research. [Online]. HYPERLINK " http://www.cryptography.com/dpa/technical" http://www.cryptography.com/dpa/technical

[7] Oswald, E. and Preneel, B., "A survey on passive side-channel attacks and their countermeasures for the Nessie public-key cryptosystems," Technical NES/DOC/KUL/WP5/027/1, 2003.

[8] Lee , J., Kapitanova, K., and Son, S., "The Price of Security in Wireless Sensor Networks. Computer Networks," *Computer Networks*, vol. 54, no. 17, pp. 2967-2978, 2010.

[9] Meulenaer , G., and Standaer, F., "Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks," in *MOBILIGHT2010*, 2010, pp. 229-242.

[10] Benenson , Z., Cholewinski, P., and Freiling, F., "Vulnerabilities and Attacks in Wireless Sensor Networks," *Wireless Sensors Networks Security, Cryptology & Information Security Series (CIS), IOS Press*, pp. 22-43, 2008.

[11] Bucci , M., Giancane, L., Luzzi, R., Marino, M., Scotti, G. and Trifiletti, A., "Enhancing Power Analysis Attacks against Cryptographic Devices," *In IET Circuits, Devices and Systems*, vol. 2, no. 3, pp. 298-305, 2008.

[12] Lynch , C., and O'reilly, F., "Processor Choice for Wireless Sensor Networks," in *In RELWSN: Workshop on Real-World Wireless Sensor Networks*, 2005, pp. 1-5.

[13] Roggen, D., Bharatula, N. B., Stager, M., Lujowicz, P., and Troseter, G., "From Sensors to Miniature Networked Sensor Buttons," in *In Proceedings of the 3rd International Conference on Networked Sensing Systems (INSS06)*, 2006.

[14] Kocher, P., Jaffe, J., and Jun, B., "Differential Power Analysis," *Lecture Notes in Computer Science*, vol. 1666, pp. 398-412, 1999.

[15] Messerges, T. S., Dabbish, E. A., and Sloan, R. H., "Examining Smart-Card Security under the Threat of Power Analysis Attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541-552, 2002.

[16] Mayer-Sommer , R., "Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards," in *Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems – CHES '00*, 2000, pp. 78-92.

[17] Okeya, K., and Iwata, T., "Side Channel Attacks on Message Authentication Codes," *2nd European Workshop on Security and privacy in Ad hoc and Sensor Networks*, vol. 2, pp. 478-488, 2006.

[18] Brier, E., Clavier, C., and Olivier, F., "Correlation Power Analysis with A leakage Model," in *Proc. Int'l workshop on Cryptographic Hardware and Embedded Systems (CHES'04)*, 2004, pp. 16-29.

[19] Mangard , S., Oswald, E. and Popp, T., *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, USA: Springer-Verlag, 2007.

[20] M., and Oswald, E. Medwed, "Template attacks on ECDSA," in *In 9th International Workshop on Information Security Applications (WISA 2008)*, 2008, pp. 14-27.

[21] Bertoni , G., Daeman, J., Peeters, M., and Van Assche, G.. (2009) The Keccak sponge function family. [Online]. HYPERLINK "keccak.noekeon.org/NoteSideChannelAttacks.pdf" keccak.noekeon.org/NoteSideChannelAttacks.pdf

[22] Tiri, K., and Verbauwhede, I., "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," in *CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, 2003, pp. 125-136.

[23] Sokolov, D., Murphy, J., Bystrov, A., and Yakovlev, A., "Design and Analysis of Dual-Rail Circuits for Security Applications," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 449-460, 2005.

[24] Golic, J., and Tymen, C., "Multiplicative Masking and Power Analysis of AES," in *CHES '02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems*, 2003, pp. 198-212.

[25] Pramstaller, N., Gürkaynak, F.K., Haene, S., Kaeslin, H., Felber, N., and Fichtner, W., "DPA Resistant AES Crypto-Chip Design," in *Proc. European Solid-State Circuits Conference (ESSCIRC), IEEE Press*, 2004, pp. 307-310.

[26] Blömer , J., Guajardo, J., and Krummel, V., "Provably Secure Masking of AES," in *Selected Areas in Cryptography: 11th International Workshop, SAC 2004*, 2004, pp. 69-83.

Terrence Moabalobelo received both his B.Sc. (computer science and electronics) and B.Sc. honor's degree at the University of North West in 2010 and 2011, respectively. He is presently studying towards his MEng (electrical engineering) with the University of Johannesburg in collaboration with the Council for Scientific and Industrial Research. His research interest includes side channel analysis and cryptography.