Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks

Giacomo de Meulenaer * and François-Xavier Standaert **

UCL Crypto Group
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
`giacomo.demeulenaer@uclouvain.be,fstandae@uclouvain.be`

Abstract. Node capture is considered as one of the most critical issues in the security of wireless sensor networks. A popular approach to thwart the problem relies on the detection of events that arise during the attack such as the removal of a node for instance. However, certain attacks, such as side-channel attacks, might be furtive and defeat this type of defense. This work clarifies this question by performing a case study on power analysis attacks of AES and ECC implementations on two common types of nodes: the MICAz and the TelosB. From our experiments, the attacks can be carried out in a stealthy manner. As a result, stealthy node compromises should be considered when securing wireless sensor networks. Also, the moderate complexity of our attacks underlines the importance of low-cost side-channel countermeasures for sensor nodes.

Key words: Wireless Sensor Networks, Node Compromise, Power Analysis Attacks.

1 Introduction

Wireless Sensor Networks (WSN) constitute a promising technology that enables the easy gathering and treatment of physical data from an environment. Integrated in wider networks, they offer the connectivity to the physical world in an easy and reliable way. They provide attractive solutions to many applications, including sensitive tasks such as perimeter protection, pollution detection, medical monitoring, etc. Within these networks, the sensor nodes are deployed in a potentially hostile environment and are therefore under the threat of various types of attacks. Among them, the node compromise is usually considered as one of the most challenging issues in the security of WSN [1].

In a node capture attack, an adversary tries to physically tamper with a node in order to extract the cryptographic secrets. This attack can be very harmful depending on the security architecture of the network. Moreover, it can give rise to many subsequent powerful insider attacks [2].

Two main directions exist to circumvent this important threat. The first one consists in improving the tamper resistance of the nodes in order to increase the

---

effort of the attacker. However, tamper-resistant mechanisms are costly for small sensor nodes and are therefore usually not present on these devices.

The second alternative adopts a surveillance-based approach, usually at the level of the network, which tries to detect events related to the node compromise. It assumes that a node capture will provoke some noticeable events, such as a loss of connectivity, a displacement or removal of a node, a loss of the node internal state, etc [2]. Defenses following this approach are attractive as they might even protect low-cost sensor devices vulnerable to physical attacks from the node capture attack. Such defenses are for instance proposed in [3, 4] and [5, 6], where a captured node is identified based on the detection of a suspicious behavior and a modification in its software code respectively. However, it remains to be verified whether any kind of node compromise really implies the detectable events upon which the defenses are built.

Side-channel attacks (SCA) may be able to avoid the detection of node compromise countermeasures. They are well-known to efficiently enable the recovery of the cryptographic secrets by exploiting the physical data available from the target device. In their passive form, these attacks are not supposed to interfere with the device operations. These attacks have been largely shown to be very efficient on a large variety of devices such as smart cards [7], PDAs [8], RFIDs [9], etc. So far, however, they have not been shown to enable stealthy node compromise in the context of WSN yet. As a result, the feasibility of these attacks in a furtive way remains to be assessed.

In this work, we clarify the question of possible furtive sensor node compromise by performing a case study on side-channel attacks in WSN. In particular, we carry out power analysis attacks of implementations of well-known cryptographic algorithms, the Advanced Encryption Standard (AES [10]) and the Elliptic Curve Cryptography (ECC [11]), on two popular sensor devices, the MICAz and the TelosB [12]. Using our setup, the attacks are not detectable by the usual surveillance-based node compromise defenses.

Organization. Section 2 first presents the related works and our contributions. Next, Section 3 explains the practical challenges of furtive SCA in WSN. Then, Section 4 explains our attack configuration to perform furtive SCA. Afterwards, Section 5 and Section 6 provide the results of our power analysis attacks on the MICAz and TelosB nodes. Section 7 later discusses the vulnerability of other nodes to these attacks. Finally, Section 8 analyzes the implications of stealthy node compromises on the security of WSN and Section 9 concludes this work.

2 Related Work and Contributions

The node capture attack has been illustrated in several works in the context of WSN. In [13], Hartung et al. recover the cryptographic secrets on a MICA2 sensor node by dumping its internal memory through the JTAG interface. The attack is extended in [14], where Becher et al. show how to access several node

hardware components such as the external memory, the bootstrap loader or the JTAG interface. They propose to disable the programming interfaces in order to prevent unauthorized accesses to the microcontroller. They underline that the node capture requires the absence of the node from the network for a substantial period, which could be useful to detect captured nodes.

In [15], Goodspeed relates that some sensor node transceivers embedding a cryptoprocessor present major weaknesses. The secret key can be extracted by sniffing the SPI bus between the transceiver and the microprocessor or by gaining access to the transceiver internal memory through the debugging interface.

Software-based attacks can also efficiently compromise nodes. In [16], Gu and Noorani introduce an attack by means of *mal-packets*, which exploit a buffer overflow to remotely perform a limited and transient execution of an external code. This attack is extended in [17], where Francillon et al. describe a powerful remote code injection attack that permanently injects an arbitrary malicious code on the targeted sensor.

All the node capture attacks mentioned above (except the bus sniffing attack) have the particularity of provoking a noticeable event during the attack, such as a temporary exclusion of a node from the network or a modification in the memory of a sensor device. Therefore, a class of countermeasures has emerged, based on the assumption of detectable node captures. Several countermeasures against node capture are based on this observation, such as the defenses proposed in [14, 4].

Side-channel attacks have drawn relatively little attention in the context of Wireless Sensor Networks. In [18], Okeya and Iwata point out the importance of side-channel attacks for sensor devices and show how message authentication codes can be attacked with power analysis in a chosen-plaintext attack scenario. More general side-channel attacks on sensor nodes are listed in a taxonomy by Pongaliur et al. in [19] but their potential to enable stealthy attacks has not been demonstrated in a practical study yet.

Contributions. Following these works, the contributions of this paper are:

1. We practically prove the feasibility of stealthy node compromises in the context of WSN. We analyze the implications of these attacks and discuss the main directions that can be followed to secure WSN against them.
2. We illustrate the efficiency of side-channel attacks within the framework of WSN. Our case study clarifies the effort required by the attacker to capture a node with power analysis attacks. The moderate complexity of our furtive attacks underlines the need of robust and low-cost protections against side-channel attacks for sensor nodes.

3 Stealthy Side-Channel Attacks

Side-Channel Attacks (SCA) are well-known to be efficient against unprotected cryptographic implementations. Advanced SCA are now able to break many

cryptographic primitives with a small number of physical data records (or traces). For instance, the most advanced power analysis attacks performed in [20] break unprotected implementations of the symmetric block cipher AES on 8-bit microcontrollers with less than 10 traces. Unprotected implementations of public key cryptography, such as Elliptic Curve Cryptography (ECC) [11], may even face a key recovery based on a single trace using Simple Power Analysis [21].

Side-channel Attacks are usually carried out in a context where the attacker can control the target device, at least briefly. This is not possible in the context of stealthy attacks in WSN. Indeed, to remain furtive, the attacks must be performed on-site and without generating any of the detectable events listed earlier. The specificities of the WSN scenario can be challenging for an adversary for the following reasons:

– **Passive acquisition:** Achieving fully passive SCA might be difficult with the usual measurement setups. For instance, power analysis classically requires the insertion of a small resistor in the power line, depackaging the chip might be needed to efficiently measure electro-magnetic emanations, etc. This should be done without disrupting the device operations.
– **On-site acquisition:** The target node cannot be moved to a convenient place to carry out the attack (typically, in a laboratory). Instead, the attacker must bring his equipment to the target node, the accessibility of which depends on the context. Moreover, his presence at the target node might reveal the attack.
– **Device not controlled:** The attack should be feasible based on known cipher-texts and a few measurements since the frequency of use of the cryptographic primitive is beyond the control of the adversary. Moreover, the extraction of the useful portions in the acquired physical data cannot be made easier by the use of triggers.
– **Real-world device:** With respect to a board dedicated to side-channel analysis, more noise is expected due to the presence of many components working simultaneously. Also, elements filtering the power supply make power analysis more difficult.

In the following, we describe how these challenges can be surmounted with our case study on furtive power analysis attacks.

4 Attack Configuration

Before focusing on the scenario and the setup of our stealthy power analysis attacks, we briefly describe the sensor node platforms used in this work.

4.1 Sensor Node Platforms

Sensor nodes are mainly composed of a microcontroller, a transceiver, a battery, an external memory and sensors. As the currently available platforms embed various types of hardware, we chose two representative sensor node platforms: the

MICAz and the TelosB [12]. Interestingly, their microprocessors have different word sizes : 8-bit for the MICAz and 16-bit for the TelosB. Both nodes support the popular TinyOS operating system and share the same CC2420 transceiver. Their main design features are displayed in Table 1.

Table 1. Features of the MICAz and TelosB sensor nodes.

Device	Microcontroller (Freq. , RAM)	Transceiver (Throughput)	Software
MICAz [12]	ATmega128L (7.37MHz, 4kB)	CC2420 (250kbps)	TinyOS
TelosB [12]	MSP430 (4MHz, 10kB)	CC2420 (250kbps)	TinyOS

4.2 Attack Scenario

We consider a typical WSN scenario where the nodes periodically send a report concerning the acquired data. The packets are encrypted with AES and ECC is used to establish shared secret keys between pairs of nodes. For simplicity, we restrict ourselves to the case where the on-site acquisition is convenient for the adversary: the nodes are easily accessible and the presence of the adversary at the target node is not detected (e.g., in a large outdoor WSN).

4.3 Attack Setup

For the acquisition of the power traces, we replaced the node power supply with a supply containing a 10-Ω sense resistor in its circuit. To obtain meaningful traces, we had to remove several capacitors and inductors filtering the power supply. Special care was taken to prevent any transient failure in the power supply while handling its circuit. In this view, we temporarily introduced an additional power supply line to go on feeding the node components while interrupting the original power line. This temporary supply line is shown in Figure 2 for the TelosB. To avoid the introduction of a short circuit while unsoldering, an independent power supply was used for the soldering iron.
 Throughout these manipulations, we checked the stability of the supply voltage with an oscilloscope. Only minor variations were observed. The smooth running of the node was also verified by checking the regularity and the content of the broadcasted messages. As a result, the introduction of our measurement setup does not provoke any significant event: it therefore defeats the proposed surveillance-based node capture defenses.
Remark that it appears feasible for an attacker to put the node board back in its original state in order to avoid any subsequent visual detection of the attack.
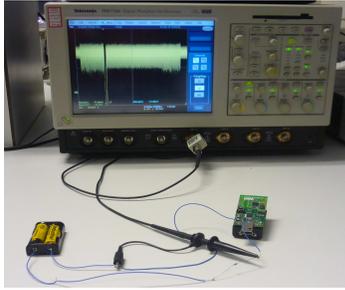
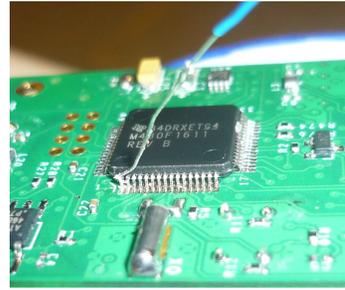**Fig. 1.** Measurement setup of our power analysis attack on the TelosB node.

Fig. 2. Detail of the TelosB with its temporary supply line introduced to go on feeding the node while interrupting its original supply circuit.

Our measurement setup is shown in Figure 1. The voltage drop across the resistor is measured on a Tektronix TDS7104 oscilloscope at a sampling frequency of 250 MHz. A more portable device could be used, like a PC-based oscilloscope for instance [22].

5 DPA Attack on AES

Our first attack concerned a Differential Power Analysis (DPA [21]) on a software implementation of AES on the MICAz and TelosB. We first shortly describe the DPA attack, then explain how it was achieved based on the attack configuration of Section 4 and finally present the results and the applicability of the attack.

5.1 Description

The DPA attack is the most popular power analysis attack. Its inputs are a sufficient number of traces of the cipher and the corresponding plaintexts (or ciphertexts). This attack exploits the data dependency of the power consumption. It targets a cipher round key, which is attacked by pieces, called subkeys (typically the key bytes). For each of the plaintexts (or ciphertexts), predictions of the power consumption are stated for every possible subkey. These hypothetical consumptions are then compared with the acquired traces with a statistical test, such as the correlation coefficient, which measures the linear relationship between two random variables [23]. The closest hypothetical consumption leads to the right subkey guess if there are sufficient traces. The recovery of the full round key easily reveals the AES main key. A detailed description of the DPA attack can be found in Chapter 6 of [21].

5.2 Implementation in the Context of WSN

The DPA attack performed in this work was based on the ciphertexts broad-casted by the target node and the traces acquired using the setup described in Section 4. The collection of the ciphertexts allowed the attack on the last round key. Inverting the AES key schedule led to the main key.

The rough trigger used to acquire the power traces was the brief transmission state of the node transceiver. However, a DPA requires well aligned traces such that the time samples of all traces correspond to the same instructions. Resynchronizing the traces was successfully performed using a pattern matching method suggested in Section 8.2.2 of [21]. This method finds the correct relative position of a trace with respect to another one by minimizing their mean square error. As later illustrated in Figure 5 for our attacks on ECC, this technique was very precise.

5.3 Results

Our own implementation of AES with 128-bit keys was the target of our DPA attack. It is written in TinyOS and is reasonably efficient. It requires a moderate memory occupation (272 B of RAM and about 1kB of ROM on both devices). The attack was shown to succeed with a relatively small complexity in terms of required power traces. We illustrate its results for the first subkey in Figures 3 and 4 on the MICAz and TelosB respectively. In these figures, the correlation coefficients of each of the 256 subkey guesses are plotted in function of the number of traces on the point of interest in the traces which provides the larger correlation for the correct subkey guess. The coefficient of the right guess remains at a high value (around 0.7) while the coefficients of the wrong guesses converge to lower values. It is already clearly distinguishable with less than 20 traces for the MICAz and 60 traces for the TelosB. Deducing the number of required traces for a successful attack from these figures is not adequate if the attacker does not know the point of interest in the traces. Therefore, we also studied the complexity of the attack when this point is unknown beforehand. In this case, all subkeys were recovered with about 40 traces and 80 traces on the MICAz and TelosB respectively. The higher complexity for the TelosB was expected, considering its 5-fold inferior power consumption [24]. Moreover, its 16-bit word size is superior to the number of bits considered in a subkey (i.e., 8). Therefore, the 8 remaining bits cause a power consumption that is not considered in the power model, known as algorithmic noise. This noise is not present on the MICAz because of its 8-bit word size microcontroller.

The small complexity of our DPA attack on sensor devices is in fact of the same order of magnitude as these obtained in [20] for advanced DPA attacks on small 8-bit microcontrollers.

5.4 Applicability in a Practical WSN Scenario

Our DPA attack against AES on the MICAz and TelosB has a complexity in terms of traces that is clearly within the reach of an attacker. Even for nodes
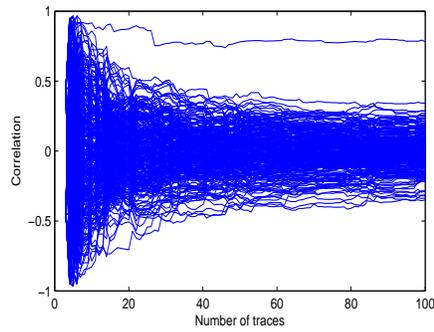
Fig. 3. Correlation coefficients of the 256 subkey guesses in function of the number of traces (MICAz). The right guess is already visible with less than 20 traces.
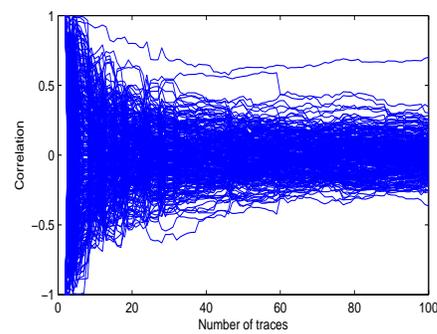
Fig. 4. Correlation coefficients of the 256 subkey guesses in function of the number of traces (TelosB). The right guess is already visible after 60 traces.

transmitting encrypted messages infrequently, acquiring the sufficient number of traces appears to be realistic. For instance, in an application where nodes transmit a packet every 10 minutes, the secret key of a TelosB can be recovered by an attacker in about $80 \cdot 10/60 \approx 13$ hours with our DPA attack. Conversely, a MICAz transmitting a packet every second is exposed to a key recovery within a few minutes.

6 Template-based SPA Attack on ECC

Our second attack was a template-based SPA attack on ECC [25]. We first explain the attack, then detail how we implemented it in the context of WSN. After that, we expose the attack results on the MICAz and TelosB and the relevance of the attack in a practical WSN context.

6.1 Description

The point multiplication is the basic operation of ECC. It is usually computed by iterations, in which an intermediary point can be transformed in several possible points, depending on one or few key bits (see [11]). It can be attacked in one trace with the Simple Power Analysis. This technique exploits the dependency on operations of the power consumption. However, most implementations of ECC include optimizations, such as windowing (see Section 3.3 in [11]), which prevent the recovery of the full key using SPA.

The template-based SPA, which relies on the dependency on both operations and data of the power consumption, can be a powerful alternative to SPA to obtain the full key in one trace, as suggested in Section 4.3 of [25]. It begins with the online phase of the attack, i.e., the acquisition of a single ECC trace on the target device. Then the offline phase of the attack is performed, made of

the following two steps, repeated for each iteration of the point multiplication (starting with the first iteration):

– **The template building step**. First, the attacker builds templates corresponding to the computation of an iteration of the point multiplication. Templates are statistical models deduced from traces for a subset of the key space. They are collected offline on a similar device running the same implementation (see Section 5.3 in [21] for more details).
– **The template matching step**. After that, the templates are compared with the trace acquired in the online phase. As templates correspond to the computation of the possible iteration results, this comparison determines which intermediary values were actually computed by the target device, leading to the recovery of the key bits involved in the iteration.

To achieve these steps on an iteration, the iteration input point has to be known. This is not a problem for the first iteration since its input point is a known parameter. For the other iterations, the intermediary point is revealed by the matching step of the previous iteration. When all the iterations are successfully processed, the full key is obtained.

6.2 Implementation in the Context of WSN

The online phase of the attack was carried out using our setup of Section 4. As ECC operations are infrequent, we relied on the format of the exchanged messages to roughly select the portion of the power consumption corresponding to ECC calculations.

Concerning the offline phase, the templates were built from the acquisition of traces on a similar node running the same implementation (the TinyECC library [26]). To achieve the matching step, a precise synchronization is required between the templates and the corresponding portion of the trace. In this view, we used the same technique as in the case of the DPA: The correct template is assumed to match the corresponding portion of the trace and thus minimize their mean square error when their correct relative position is found. Our experiments proved that this method was accurate, as depicted in Figure 5 for the TelosB.

6.3 Results

In our experiments, we carried out the online phase of the attack and the offline phase for the first iteration of the point multiplication. As the same attack steps are repeated for all the iterations, focusing on one iteration is enough to determine the feasibility of the whole attack.

In the building step, we built two templates as one single key bit was handled per iteration of the point multiplication under attack. For this, we collected on a similar device a set of 100 traces for each of the two possible results. Then, in each of these sets, we selected the sequences of samples corresponding to the
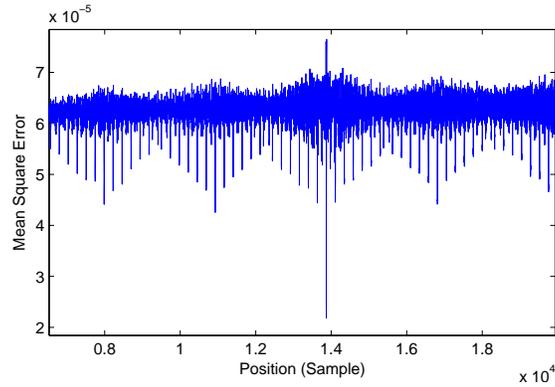
Fig. 5. Mean Square Error between the correct template and the reference power trace when synchronizing them (TelosB). The lowest error clearly reveals the right relative position.

targeted iteration and averaged them. To speed up this process, we restricted the template size to 100,000 samples.

In the template matching step, we compared our two templates with the trace obtained in the online phase. The criterion used to determine which intermediate point was actually computed in the iteration was the least-square test between the trace samples of interest and the two templates. As indicated in [21], this test can be seen as a maximum-likelihood decision rule.

The matching step successfully led to the recovery of one key bit on the MICAz and TelosB. Repeating the matching step 100 times showed that the targeted key bit could be recovered with very high confidence. Consequently, the whole attack appears feasible on both platforms.

6.4 Applicability in a Practical WSN scenario

The online complexity of the attack is minimal. With the measurement setup described above, an attacker only needs to wait for a single ECC operation on the target node.

In the offline phase, the adversary does not face the detection of the attack any more. This phase requires the access to a identical device running the same ECC implementation. It is realistic assuming commercially available nodes (or at least, their microcontrollers) and the use of a freely available ECC implementation, such as the TinyECC library [26] that we used in this work. With 160-bit keys, our choice of 100 traces per template leads to $100 \cdot 2 \cdot 160 = 32000$ traces to acquire on the similar device. This can be done within $32000/3600 \approx 9$ hours with an automated setup acquiring one trace per second. The complexity of the offline phase is thus perfectly reachable for an attacker. As a result, the template-based SPA can be a severe threat to ECC implementations in the context of WSN.

7 Other Nodes

The current generation of sensor nodes is constituted by many heterogeneous devices. Apart from the platforms based on 8-bit or 16-bit microcontrollers as the MICAz and TelosB studied in this work, other larger nodes exist, that are based on 32-bit more powerful microcontrollers, such as the Sun SPOT [27] or the IMote 2 [12]. These platforms differ from usual smaller nodes by being much less restricted in terms of computation and memory constraints. For instance, the ARM 920T of the Sun SPOT runs at 180MHz and contains 512kB of RAM. These devices, based on the standard CMOS technology, do not have inherent protection against side-channel attacks. In the literature, many attacks have been successfully applied on 32-bit based embedded device. For instance, the template-based SPA of Medwed et al. [25] is carried out on a 32-bit ARM7 processor. Therefore, the vulnerability of these larger nodes to furtive side-channel attacks is real. However, the larger word size of their processor should make the attacks more difficult, because of a larger algorithmic noise. The more powerful nodes are also better equipped to resist to side-channel attacks because of their larger memory resources, which could include advanced (and costly) countermeasures.

8 Implications

The feasibility of stealthy node compromises has major implications on the security of WSN. By nature, these attacks cannot be thwarted by the existing surveillance-based node capture defenses. These countermeasures are however far from being useless as they prevent many kinds of node compromise. Moreover, they also prevent an adversary from actively speeding up the acquisition phase of furtive SCA (e.g., by injecting messages to stimulate the use of the cryptographic primitives on the target node).
Stealthy node captures enable an adversary to compromise node-by-node large parts of unprotected networks. WSN should thus be protected against these severe attacks. For this purpose, we identify three approaches.

1. The conditions of stealthiness of the attack could be repressed. One could assure that the nodes are never left without visual surveillance, but it may be costly depending on the application and the size of the network. Alternatively, defenses could be provided on every node to attempt to detect when they are being attacked. For instance, a system detecting a small transient supply voltage variation could launch an alarm concerning power analysis attack. Such countermeasures may however not be reliable for any type of attack setup or any kind of physical attack, while having a significant cost.
2. Side-channel countermeasures could be added on the nodes to complicate the recovery of the secret keys. They are usually not included in cryptographic implementations for sensor nodes (with the notable exception of [28]). These defenses should have a moderate cost and be hopefully as strong as the cryptographic algorithms employed. Their level of security should be known and properly assessed.

3. A third possibility would be to use security protocols tolerant to node capture attacks. This approach is not new. For instance, the protocol presented in [29] considers an adversary model where an attacker is able to compromise a limited number of nodes, without making any assumption regarding the node capture process. However, such protocols may be hard to achieve depending on the functionality of the protocol.

Protecting WSN against stealthy node compromises seems thus a non-trivial problem. A combination of defenses at the level of the network and in the nodes themselves is likely to offer the highest level of security in WSN.

9 Conclusion

In this work, we prove the feasibility of furtive power analysis attacks in the context of WSN. Using our setup, these attacks can be undetectable for surveillance-based node capture defenses. While limited to situations where the nodes are easily accessible and the adversary presence is not detected, they remain of concern in many realistic scenarios of WSN. They involve the manipulation of the power supply circuit without disturbing the node, which can be challenging if some of its components are hard to access. However, for a skilled adversary, the furtive power analysis attacks represent a really attractive option: the amount of power traces to record is small, as illustrated in our attacks of AES and ECC implementations on the MICAz and TelosB.
The existence of furtive physical attacks seriously jeopardizes the security of WSN. To remain secure, WSN should either use security protocols which tolerate stealthy node compromises or make use of nodes that are protected against these attacks. Our work underlines the need of robust and low-cost side-channel defenses for small devices like sensor nodes.

References

1. Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.
2. Christoph Krauß, Markus Schneider, and Claudia Eckert. On handling insider attacks in wireless sensor networks. *Inf. Secur. Tech. Rep.*, 13(3):165–172, 2008.
3. Issa Khalil, Saurabh Bagchi, and Cristina Nina-Rotaru. DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks. In *1st Int. Conf. on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM)*, 2005.
4. Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. Emergent properties: detection of the node-capture attack in mobile wireless sensor networks. In *WiSec '08: 1st conference on Wireless network security*, pages 214–219. ACM, 2008.

5. Arvind Seshadri, Adrian Perrig, Leendert Van Doorn, and Pradeep Khosla. Swatt: Software-based attestation for embedded devices. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2004.
6. Christoph Krauß, Frederic Stumpf, and Claudia M. Eckert. Detecting node compromise in hybrid WSN using attestation techniques. In *ESAS*, pages 203–217, 2007.
7. T. S. Messerges, E. A. Dabbish, and R. H. Sloan. Examining smart-card security under the threat of power analysis attacks. *Computers, IEEE Transactions on*, 51(5):541–552, 2002.
8. Catherine H. Gebotys, Simon Ho, and C. C. Tiu. EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA. In Springer, editor, *CHES*, volume 3659 of *LNCS*, pages 250–264, 2005.
9. Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and EM attacks on passive 13.56 MHz RFID devices. In *CHES '07: 9th international workshop on Cryptographic Hardware and Embedded Systems*, pages 320–333. Springer, 2007.
10. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.
11. Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
12. CrossBow. Wireless Sensor Networks Module Portfolio. http://www.xbow.com/Products/productdetails.aspx?sid=156.
13. Carl Hartung, James Balasalle, and Richard Han. Node compromise in WSN: The need for secure systems. Technical Report CU-CS-990-05, Colorado University, 2005.
14. Er Becher, Zinaida Benenson, and Maximillian Dornseif. Tampering with motes: Real-world physical attacks on wireless sensor networks. In *Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC)*, pages 104–118, 2006.
15. T. Goodspeed. Extracting keys from second generation zigbee chips. Work in progress, Black Hat USA 2009. http://www.blackhat.com/presentations/bh-usa-09/GOODSPEED/BHUSA09-Goodspeed-ZigbeeChips-PAPER.pdf.
16. Qijun Gu and Rizwan Noorani. Towards self-propagate mal-packets in sensor networks. In *WiSec '08: Proceedings of the first ACM conference on Wireless network security*, pages 172–182, New York, NY, USA, 2008. ACM.
17. Aurélien Francillon and Claude Castelluccia. Code injection attacks on harvard-architecture devices. In *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*, pages 15–26, New York, NY, USA, 2008. ACM.
18. Katsuyuki Okeya and Tetsu Iwata. Side channel attacks on message authentication codes. In Springer, editor, *ESAS*, volume 3813 of *LNCS*, pages 205–217, 2005.
19. Kanthakumar Pongaliur, Zubin Abraham, Alex X. Liu, Li Xiao, and Leo Kempel. Securing sensor nodes against side channel attacks. In *HASE : Proceedings of the 11th IEEE High Assurance Systems Engineering Symposium*, pages 353–361, 2008.
20. François-Xavier Standaert, Benedikt Gierlichs, and Ingrid Verbauwhede. Partition vs. Comparison Side-Channel Distinguishers:an Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices. *Information Security and Cryptology — ICISC 2008*, pages 253–267, 2009.
21. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer-Verlag New York, 2007.
22. PicoTechnology. Portable High Perf. PC Oscilloscope. http://www.picotech.com/picoscope5000.html, Jan. 2010.

23. Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In Marc Joye and Jean-Jacques Quisquater, editors, *CHES*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.
24. Giacomo de Meulenaer, François Gosset, François-Xavier Standaert, and Olivier Pereira. On the energy cost of communication and cryptography in wireless sensor networks. In *WIMOB '08: Proceedings of the 2008 IEEE International Conference on Wireless & Mobile Computing, Networking & Communication*, pages 580–585, Washington, DC, USA, 2008. IEEE Computer Society.
25. Marcel Medwed and Elisabeth Oswald. Template attacks on ECDSA. In *Information Security Applications: 9th Int. Workshop, WISA 2008*, pages 14–27. Springer, 2009.
26. An Liu and Peng Ning. TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. In *IPSN*, pages 245–256, April 2008.
27. SUN. Sun SPOT (Sun Small Programmable Object Technology) . http://www.sunspotworld.com/, September 2009.
28. Christian Lederer, Roland Mader, Manuel Koschuch, Johann Großschdl, Alexander Szekely, and Stefan Tillich. Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks. In *Information Security Theory and Practices — WISTP 2009*, pages 112–127. Springer Verlag, LNCS 5746, September 2009.
29. Bryan Parno, Adrian Perrig, and Virgil Gligor. Distributed detection of node replication attacks in sensor networks. In *SP '05: Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 49–63, Washington, DC, USA, 2005.