Survey on power analysis attacks and its impact on intelligent sensor networks

Shanthi Rekha Shanmugham, Saravanan Paramasivam

Abstract: Smart or intelligent sensors are integrated physical units embedded with sensors, processors, and communication devices. The sensors also known as edge nodes form the lower-most tier in the internet of things architecture. These devices rely on cryptographic technique to ensure ‘root of trust’ for the users. The implementation attacks namely side-channel attacks (SCAs) pose a dangerous threat for the cryptographic implementation in the edge nodes since the attacks are undetectable by nature. Among the different categories of SCAs proposed in the literature, power analysis attacks (PAAs) are vastly studied and widelyemployed because it can be mounted with relatively inexpensive equipment. In this study, the different categories of PAAs along with the countermeasures are reviewed in detail. The impact of the SCA on the edge nodes is examined along with a case study on medical sensor nodes.

1 Introduction

Internet of things (IoT) is the concept of connecting any device ranging from cell phones, refrigerators, vehicles, wearable or implantable devices, and many others with the aim of monitoring and management of information [1]. The IoT architecture consists of sensors for data gathering, processors, actuators to control the device, protocols for communication and automation software. The sensors form the first tier of the IoT architecture [2]. Many challenging issues need to be addressed to realise the vision of IoT [3]. Recent scientific advances in the growth of intelligent sensors offer minimum cost, improved reliability, performance, and scalability since the data is processed and communicated on the same device. Meeting the stringent area and power demands of the sensors or edge nodes (used interchangeably in the rest of the paper) are important and are addressed in many works recently. However, more focus is required on guaranteeing trust, security, and privacy of the users and their data [4, 5].

Ensuring the security of the edge nodes is a prime focal point to achieve its desired benefits. This requires sufficient protection at the device level and can be achieved through a combination of design, data, and hardware security [6]. Cryptography is the widely adopted technique to ensure that data is communicated securely. It can be achieved using symmetric-key techniques namely advanced encryption standard (AES) [7], data encryption standard (DES) [8] or asymmetric-key techniques namely Rivest-Shamir-Adleman (RSA) [9], elliptic curve cryptography (ECC) [10] etc. These algorithms can be realised using software or hardware implementations [11]. Hardware implementations are preferable to achieve better security and performance and can be realised using dedicated crypto-processors or hardware security modules, which can be integrated into the edge nodes. Identification of a suitable encryption technique for these sensor nodes is an important challenge due to the limitation of energy, computation capability, and storage resources. Moreover, the sensor nodes should be resilient against side-channel attacks (SCAs) that rely on the inherent physical leakage of the cryptographic algorithm and are very difficult to detect. The different variants of leakages namely power consumption, electromagnetic (EM) radiation, time taken for the computations and recently sound emanations from a key pad [12] are leveraged to expose the secret key. Among the different side channels, power analysis attack (PAA) has received more attention.

The sensor networks in the IoT have been deployed for various applications at home, office, educational institutions, hospitals, industries, healthcare, research centres, security, surveillance, tourism, and entertainment. Among the various applications, any security breach in the healthcare application needs immediate attention in order to protect patient privacy. The medical devices in the healthcare applications are categorised as wearable or implantable ones, which are used to monitor the various physiological conditions. It consists of dedicated sensor networks, an interconnection of medical sensor nodes that depend on cryptographic techniques for providing the necessary security services. SCA can be used against these networks for privacy invasion [13] and it is possible to modify the data or device operation, leading to a life-threatening impact on the patient. In our work, the side-channel security of these devices is briefed as a case study.

The major contributions of this work are described as follows:

i. We review the different categories of PAA. The individual contributions in each category are:

- Simple power analysis (SPA): We consolidate the existing works in SPA attacks, relevant countermeasures and highlight the applications of SPA.
- Differential power analysis (DPA): We emphasise the advantages of adopting emerging devices and technology for rendering DPA resistance.
- Leakage power analysis (LPA) attacks: We categorise the different ways of performing LPA based on the models adopted or attack methodologies. We also summarise the metrics used in such attacks and the existing countermeasures to thwart the same. According to our best knowledge, there is no survey paper in detail on LPA and its countermeasures. Hence our work becomes the first one for such a contribution.

ii. Our work reviews the vulnerability of the edge nodes and the communication protocols in the IoT environment to SCA. Ours is the first of its kind to study the impact of SCAs on medical sensor nodes.

Our paper is organised as follows. Section 2 presents our survey on PAA and Section 3 summarises the available literature for SCAs on edge nodes. Section 4 concludes the paper.


2 Power analysis attacks (PAAs)

Complementary metal oxide semiconductor (CMOS) is the most popular semiconductor technology, which consists of P-type metal oxide semiconductor (PMOS) (p-channel) transistors in the pull-up network and N-type metal oxide semiconductor (NMOS) (n-channel) transistors in the pull-down network to realise the logic. A CMOS inverter is shown in Fig. 1. The power dissipation of a CMOS circuit is contributed by a dynamic component caused by switching activities of the circuit and a static or leakage component related to the logical state of the circuit.

The most significant source of dynamic power dissipation is the charging and discharging of capacitance. The static or leakage current is conducted by metal oxide semiconductor transistors operating in the cut-off region. PAA can be devised to exploit the static or dynamic power dissipation of the circuit by measuring the current across a resistor in series with the power line.

PAA can be classified as SPA, DPA, and LPA. SPA exploits the fact that the power consumption depends on the operation being executed inside the device while DPA exploits the data dependence of the device. Though it seems like SPA can be prevented easily than the DPA, the work in [14] has shown that the SPA is a powerful attack performed with a single power trace. Hence the SPA provides a more dangerous threat to real applications and it is important to review the same. Since DPA and its variant correlation power analysis attack (CPA) along with its countermeasures are surveyed in detail [15, 16], we have provided an overview of the latest trends in DPA/CPA from the nano-devices and latest technology perspective. LPA is reviewed in detail along with its metrics and countermeasures.

2.1 SPA attack

An SPA attack involves providing an input to the cryptographic device and visually inspecting the power consumption. The single power trace is used for further processing to reduce the key space [17] or to extract the secret key [18]. SPA depends on particular vulnerabilities in the cipher design [19] and was proposed by Kocher [20]. Messerges et al. [21] used the simulated power traces to extract the hammer weight (HW) of the key byte with knowledge of the clock cycle at which the key byte is accessed, for a DES crypto-core. Thereby, they reduced the key space, which improves the efficiency of a brute-force attack. Mangard performed an attack using the same concept on the AES key scheduling [17]. Compton et al. were the first to assess the susceptibility of Serpent [19] and Two-fish [22] block ciphers to SPA. Xiao et al. analysed the SPA vulnerability of Camellia's key schedule in [23, 24].

Banciu and Oswald [25] implemented and compared the two ways of performing SPA: a trivial technique described by Mangard in [17] performed on key scheduling block (mentioned as a pragmatic approach), and an algebraic attack methodology performed on the encryption rounds (described as an elegant approach). The idea of algebraic SCAs is to build a system of equations to describe the algorithm, AES in this case and provide the necessary side-channel information to standard SAT solvers in order to extract the secret key. Finally, the pragmatic approach showed better noise leakage tolerance with a substantial reduction of the key space. An improvement to Mangard's work [17] is reported in [18]. The idea is to break the 128-bit key into 16 bytes and exploit the relationships between the round keys by using an optimised search algorithm. Computing the HW of these bytes thereby resulted in correct key guess and the proposed method takes only 16 ms to guess the 128-bit key. On the countermeasures part, Mangard has proved in [17] that a combination of randomisation and masking countermeasure for an AES software implementation provides sufficient resistance against SPA, DPA, and higher-order DPA [26].

Reference [27] is one of the latest works, which reports an SPA on additive modulus operator. The authors have retrieved the secret data based on the observation that whenever modular reduction occurs, the time taken and power consumption increases. They have further proposed a modified additive modulus operator that uses bit checking instead of branch operation with indistinguishable time and power characteristics for achieving SPA resistance.

2.1.1 Applications of SPA attack: When SPA is performed on RSA cryptosystem, the two distinct operations of RSA, namely multiplication and squaring, were distinguished [28]. To increase the information leakage, chosen-message attacks for RSA using specific input data were proposed in [29, 30].

The usage of the SPA to analyse stream ciphers has been identified in [31]. Reference [32] is an extension to [31], which considers multiple linear feedback shift registers (FSRs) and [33] is the latest work in this area in which SPA is used to identify the bit values of nonlinear FSR (NLFSR) with acceptable complexity. The adversary is aware of the underlying operation performed in the device under attack or target device. SPA requires only a single power trace to reduce the key space. Hence these attacks are very handy in scenarios where the target device is available only for a short period of time for the adversary. This highlights the importance of imparting strong countermeasures for prevention of such attacks. SPAs find an interesting application to identify the bit values of NLFSRs.

2.2 DPA attack

DPA first proposed by Kocher [20] has been extensively studied in the literature. DPA and its variant CPA [34, 35] is one of the types of PAA that exploit the data-dependent property of the power consumption of the circuit. DPA uses the difference of means method to predict the key while CPA uses a statistical distinguisher namely Pearson's correlation coefficient (CC) to correlate between the measurements obtained and predictions made. The success of the attack depends on the accuracy of the measurements obtained from the target device and the model of predictions or attack model of the selection function. Different variants of DPA have been proposed namely higher-order DPA [36–38], collision-based attacks [39, 40], template or profiled attack [41, 42], algebraic SCA [43–45] etc.

2.2.1 Countermeasures: The existing countermeasures are categorised based on the design abstraction levels as: (i) algorithmic level: hiding, duplication [46], masking [47, 48] random precharge logic [49], and secure double data rate registers [50]; (ii) logic level: dual rail logic [51, 52] adiabatic techniques [53, 54] and masking [55]; (iii) architecture level: noise insertion [20], random clock frequency [56], randomisation of the instruction streams [57] or random insertion of dummy instructions into the execution sequence of the algorithm [58], register renaming, adopting low-power techniques namely dynamic voltage frequency scaling and inductive voltage regulator [59]. Since there are detailed reviews about DPA and CPA methods, the different models used and their countermeasures [15, 16], we have reviewed the on-going trend in that area.

Nano-scale devices are recently being investigated for their PAA tolerance due to their decreased power consumption at lower technology nodes. For example, tunnel field effect transistors (TFETs) are used in the construction of a lightweight KATAN32 cipher in [60] and proved to have 15 times lesser energy than its CMOS counterpart. Yu Bi et al. have performed CPA on TFET-current mode logic (CML) and TFET-static-based KATAN32 implementations. They have shown that the CC of TFET-CML
gates is less significant, thereby counteracting the CPA whereas TFET-static based implementation was vulnerable [60]. Similarly, Fin Field-effect transistor (finFET)-based AES implementation is evaluated for its CPA resistance by exploiting the active power management characteristics of the device [61]. The idea is to generate noise and suppress the secret key information by utilising the back gate bias modulation. Hence the power obtained from the circuit is uncorrelated with the secret key, thereby tolerating CPA. The authors have also developed a simple power model which considers both dynamic and leakage power for the attack.

Himanshu et al. have employed FINFET- and TFET-based symmetric pass gate adiabatic logic for the construction of PRESENT cipher and compared its power and energy consumption in detail in [62]. Similarly, MOSFET-like carbon nanotube field effect transistor (M-CNTFET)-based adder multiplier circuit is constructed in [63]. SPA performed on the circuit resulted in a success factor of 0.35 and in case of CPA, the difference of CC of the correct key and closest wrong key was <0.42. Similar CPA results are also achieved for the PRESENT block cipher implementation using M-CNTFETs. The three-dimensional (3D) integration technology is evaluated for CPA resistance [64] by developing an attack model that adds the power distribution noise from other planes to the crypto-module’s power. Thereby, the CC value is decreased and an improved guessing entropy (the number of guesses required for a successful CPA) using a hamming distance (HD) model is obtained with a manageable delay overhead. Alasad et al. have used the specific magnetisation property of all-spin-logic-devices (ASLD) [65], in which the power consumption is constant during low-to-high and high-to-low switching. ASLD-based gates are constructed which are further used to build AES crypto-core. Simulation-based CPA conducted using HW and HD models shows an unsuccessful attack in which the CC of the correct key was not extractable. A summary of the emerging devices and their PAA tolerance is analysed and tabulated in Table 1.

Summary: CPA and its variant CPA have been well studied in literature and researchers are actively working on how well it can be mitigated. Each of the countermeasure developed has its own area or power or delay overheads and the designers have to make a careful choice on how much compromise can be made on these factors for security. A recent literature [66] has proved that the countermeasures developed for one type of SCA can increase the weakness to other types of SCA. Hence ensuring PAA protection of a device becomes very challenging.

Based on the simulation results of the mentioned literature, it can be concluded that the emerging nano-scale devices and the emerging technology such as 3D integration, can be leveraged for providing the required SCA security with a lower-power consumption. However, SCA analysis on hardware realisations of nano-scale devices is lacking to confirm the hypothesis.

### 2.3 LPA attack

CMOS is the dominant technology of today’s mobile world era because of its very low-power consumption. However, with ever shrinking feature sizes, the total power consumption of the CMOS circuits is dominated by leakage power and PAA based on this power is feasible and effective. Leakage power depends strongly on the input of digital circuits and hence can be exploited to extract the secret key [67]. Therefore, PAA based on leakage is an attractive research area. To the best of author's knowledge there is no review paper on the PAA based on leakage power and hence this section is dedicated to giving a complete description of the same, countermeasures proposed with an added note on the metrics used to evaluate the attack resistance.

### 2.3.1 Metrics: A brief summary of the metrics used for LPA attacks and countermeasures is summarised in Table 2.

### 2.3.2 Attack: Most of the papers published on LPA are simulation based. It is quite easy to capture the leakage traces compared to dynamic traces since the leakage traces are constant when captured after the settling time. Also, leakage traces can be captured in scenarios where the adversary is able to attain sufficient control over clock, i.e. by stopping the clock after a particular instant, steady state is reached and the leakage current can be obtained.

### Dependence on input data: The first category is based on the property that leakage power is dependent on the data being processed. The very first idea of using leakage power as a side channel to extract the secret key was proposed in [80]. Their methodology is based on the well-known data-dependent property of leakage power. The authors have derived postulates for guessing the secret key, based on the knowledge of the input vectors that produce minimum and maximum leakage power by performing an experimental analysis on the SCA resistant design flow chip with an AES-crypto core.

With a similar view, Dhanuskodi et al. [75] show a successful LPA attack by exploiting the dependence of leakage current on the logic state of each gate. They have adopted a leakage prediction scheme wherein the internal leakage current of the gates is calculated for all possible input combinations and stored in a column vector. By multiplying a row vector with appropriate inputs to the gates, the theoretical leakage power for the circuit is obtained. The practical leakage power measurements obtained from the device under attack are then correlated with the theoretical values. The authors have claimed that the proposed method is faster, achieves a good success rate (SR) (around 60%) in the presence of process variations. They have used profiling to characterise the leakage power which further improves the SR to 100%. The major drawback of this work is that the authors have not discussed the effort needed in terms of time and tools/other resources for the pre-characterisation step, since practical cryptographic circuits involve a huge number of gates and one needs to check the feasibility to obtain the leakage power for all input combinations applied to the gates.

### Dependence on HW of internal data: In this category, the attack model is based on the property that the leakage power depends linearly on the HW of the input data being processed. Our analysis reveals that depending on the type of modelling file used (in simulation), the leakage power either increases or decreases linearly with the HW. Furthermore, depending on the number of leakage current samples considered for one trace, the attacks can be categorised as univariate or multivariate.
The authors have also shown that the DPA countermeasures such as wave dynamic differential logic (WDDL) and masked dual rail pre-charge logic (MDPL) leaked more information than the standard CMOS under static current measurements. The proposed univariate attack procedure is carried out on a CMOS and WDDL implementations of the PRESENT-80 block cipher in [81] and the measurements of disclosure (MTD) for CMOS is shown to be almost an order of magnitude higher than the WDDL case.

Multivariate: Alioto et al. were the first to come up with a precise procedure to perform LPA by exploiting the linear dependence of the HW of the inputs and the leakage power in [74], with a theoretical background for the linear model in [82]. The number of leakage current samples considered in this work is more than one. Based on the fact that the attack point considered is at the output of the substitution box (S-box) and the linear dependence of the leakage power and HW of the inputs is considered, the attack procedure is similar to CPA. However, substituting dynamic power with leakage power has shown promising results. Alioto et al. have initially proved the linear dependence on a register file and extended the work to bit-sliced implementations. Furthermore, they had thoroughly analysed the leakage-HW dependence for non-bit sliced implementations, such as serpent S-box where the data path is designed with input and output registers to enhance the linearity [67].

When we summarise the LPA works in the literature, the trend of most of the works is to demonstrate their attack procedure successfully on DPA countermeasures as in [70, 71]. In specific, LPA based on this category is performed with 70–100% SR on the WDDL and MDPL logic styles, with a comparatively lesser rate of about 17% for sense amplifier-based logic (SABL) style and is proved unsuccessful against delay-based dual-rail pre-charge logic (DDPL) (MTD > 100,000) styles [70]. Djukanovic et al. [71] studied the impact of process variations on LPA and the effect of temperature on leakage current.

Moradi et al. have summarised the first practical results of performing static power-based PAA on side-channel attack standard evaluation boards (SASEBO) [72]. They have analysed the different power consuming components of field-programmable gate array (FPGA) and have discussed the feasibility of performing first- and second-order SPA on the masked and shuffled AES S-box. Based on these results, Moradi et al. have performed a comparative analysis of DPA attacks and static power analysis attacks (SPAA) on the 26th round of PRESENT-80 cipher's threshold implementation on a 150-nm application-specific integrated circuit prototype chip in [73]. The evaluation is performed on a SASEBO-R board and the temperature control is obtained using a climate chamber. The DPA and SPAA performance is based on the CPA method, which uses HWM and collision-based moments-correlating DPA. The conclusion on the performed experiment is that SPAA has a higher time complexity, i.e. the time required for the measurement of traces is very high in the range of ∼25–59 h for first- and third-order analysis compared to DPA, which required less than half an hour for first-order and ∼12 h for third-order analysis. However, SPAA exhibits fewer data complexity, i.e. it requires less number of traces for key retrieval. For example, 4.9 million dynamic traces versus 193,000 static traces.

**Difference of means methodology:** The LPA attack procedure is performed with a similar approach to DPA. An attack procedure which involves choosing an appropriate selection function and calculating the difference of means (as in DPA), using static power named as leakage-based DPA (LDPA) is proposed in [68]. The authors have proved that LDPA comparatively requires lesser rounds of attack for key retrieval. The efficiency of the proposed

### Table 2  LPA metrics summary

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Definition</th>
<th>Usefulness</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>number of attack rounds</td>
<td>number of rounds of attack required for successful key retrieval</td>
<td>to compare the attack effectiveness</td>
<td>[68]</td>
</tr>
<tr>
<td>coefficient of variation</td>
<td>ratio between the standard deviation and the mean of the n measured currents i/j</td>
<td>to evaluate the dependence of leakage current on the inputs</td>
<td>[69, 70]</td>
</tr>
<tr>
<td>MTD</td>
<td>the cross-over point of the CC curve of the correct key with respect to the curves of the other key guesses</td>
<td>for quantifying the resistance of a crypto implementation against LPA in terms of minimum number of plaintexts for discovery of the key</td>
<td>[70–73]</td>
</tr>
<tr>
<td>asymptotical gain (G)</td>
<td>the ratio between correct CC and maximum of wrong CC</td>
<td>to provide an assessment of the implementation’s leakage tolerance</td>
<td>[70]</td>
</tr>
<tr>
<td>SR</td>
<td>the number of sample circuits which were successfully attacked with a MTD not exceeding the maximum number of measurements</td>
<td>to evaluate the effectiveness of LPA on the sample circuits</td>
<td>[70, 71, 74, 75]</td>
</tr>
<tr>
<td>information theory metrics</td>
<td>mutual information and posterior probability</td>
<td>to examine the amount of static power information useful to attack the device</td>
<td>[69]</td>
</tr>
<tr>
<td>success value indicator (SVI)</td>
<td>compares the results of the statistical distinguisher used, if the SVI is strictly positive, the correct key is successfully recovered among wrong keys</td>
<td>assesses how soundly the correct key can be renowned from wrong keys</td>
<td>[76]</td>
</tr>
<tr>
<td>point Bi-serial CC (PBC)</td>
<td>the correlation between the leakage current and the input pattern of a logic circuit when one variable is dichotomous</td>
<td>directly reveals the LPA resistance of the circuit</td>
<td>[77]</td>
</tr>
<tr>
<td>co-efficient of deviation (CoD)</td>
<td>the average value of the difference of power consumption for all the combination of inputs</td>
<td>to estimate the data dependency of the DPA countermeasures that are evaluated for LPA resistance</td>
<td>[78, 79]</td>
</tr>
</tbody>
</table>

**Fig. 2  LPA categorisation**

---

**Univariate:** The work in [69] considers the static power consumption measurements as a univariate model since it is proved theoretically that the static current sample is related to the logic state of a device during a period of elaboration, in contrast to all the other papers in this domain which considers the static power as a multivariate model. Hence a single current sample is sufficient for one specific input which drastically reduces memory resources and time. Apart from proving the attack using the HW model (HWM), for the first time, information theory metrics are used to quantify the information obtained from the leakage measurements. The authors have also shown that the DPA countermeasures such as wave dynamic differential logic (WDDL) and masked dual rail pre-charge logic (MDPL) leaked more information than the standard CMOS under static current measurements. The proposed univariate attack procedure is carried out on a CMOS and WDDL implementations of the PRESENT-80 block cipher in [81] and the measurements of disclosure (MTD) for CMOS is shown to be almost an order of magnitude higher than the WDDL case.

**Multivariate:** Alioto et al. were the first to come up with a precise procedure to perform LPA by exploiting the linear dependence of the HW of the inputs and the leakage power in [74], with a theoretical background for the linear model in [82]. The number of leakage current samples considered in this work is more than one. Based on the fact that the attack point considered is at the output of the substitution box (S-box) and the linear dependence of the leakage power and HW of the inputs is considered, the attack procedure is similar to CPA. However, substituting dynamic power with leakage power has shown promising results. Alioto et al. have initially proved the linear dependence on a register file and extended the work to bit-sliced implementations. Furthermore, they had thoroughly analysed the leakage-HW dependence for non-bit sliced implementations, such as serpent S-box where the data path is designed with input and output registers to enhance the linearity [67].
methods is validated on the last round of DES S-box implemented using DPA-resistant logic style (SABL). However, Alioto et al. [67] have proved that the LDPA method is weak compared to the LPA procedure performed with multivariate HWM, by performing an experimental analysis of the LDPA method. The drawback of LDPA is apart from the correct key there were several other key values whose DPA peak was closer to the correct key value.

**Template attack methodology:** Template attacks proposed previously in the literature used dynamic power measurements. The idea of using static power in place of dynamic power was conceived in [76], under the name of template attack exploiting static power (TAESP). The authors have successfully attempted a univariate TAESP on the PRESENT-80 cipher and compared the results with a multivariate TAESP with a temperature variant. They have concluded that multivariate TAESP is more powerful with noise and process variations since it requires only 1900 measurements to recover the secret key whereas the univariate attack could not recover the key even with 15,000 measurements. MTDs for three different process corners namely slow–slow, fast–fast and typical–typical are reported.

**Information theoretic methodology:** The LPA Attack methodology in this category is based on the information theoretic approach to quantify the data obtained from the static power measurements. As a further extension to the univariate HWM-based LPA work in [69], the same authors have performed the attack considering the leakage samples as multivariate, i.e. for different temperatures, leakage samples are measured since the mutual information metrics showed a better value for increasing temperature [83]. The attack procedure in this work does not need a priori model to characterise the leakage power. A summary of the approaches is given in Table 3.

**Summary:** Based on the existing works on PAA using static or leakage power, five different ways of performing these attacks are summarised. Pozzo et al. [84] have analysed under what scenarios the static power consumption becomes a prominent side-channel leakage source and how the noise effects can be removed. The main conclusion of this work is that static leakage can be a useful information source for side-channel adversaries which are able to control the clock signal.

In these cases, reducing the frequency can make the static parts of the traces arbitrarily long, hence allowing us to use these long traces to reduce/remove the noise through averaging. While this can be an issue in unprotected implementations, the impact of static leakages can become much more critical, e.g. in (Boolean) masked implementations.

Djukanovic et al. [83] have shown that Alioto et al.’s multivariate HWM-based LPA procedure, the first and precise model, is weak for lower operating temperature (MTD > 100,000) and only at 100°C, the feasible range of MTD = 19.1k is observed. This is a greater concern to be addressed because it is not possible to alter the operating temperature of the target device for a successful LPA and hence it is important for the LPA procedure to be feasible at room temperature. Also, Moradi et al.’s work on implementing LPA on SASEBO boards [72] showed a greater impact of temperature on the measurements. Hence the challenges of performing LPA in real-time is to overcome the temperature dependence of leakage current and to capture the static noise-free samples of the target device.

### Table 3 LPA attacks summary

<table>
<thead>
<tr>
<th>LPA model</th>
<th>References</th>
<th>Cores attacked</th>
<th>Countermeasure/weakness</th>
<th>Metrics achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependence on input data</td>
<td>[75]</td>
<td>AES, serpent S-box</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>[80]</td>
<td>DES S-box</td>
<td>—</td>
<td>59% SR with process variations, 100% SR with profiling and a MTD &lt; 3300</td>
</tr>
<tr>
<td>dependence on HW of internal data</td>
<td>[69]</td>
<td>serpent crypto core</td>
<td>time enclosed logic [60]</td>
<td>mutual information metric plot</td>
</tr>
<tr>
<td>univariate</td>
<td>[81]</td>
<td>PRESENT-80</td>
<td>—</td>
<td>MTD for CMOS is higher by an order of magnitude than WDDL, mutual information metric</td>
</tr>
<tr>
<td>multivariate</td>
<td>[70, 71, 74]</td>
<td>serpent S-box</td>
<td>LPA proved unsuccessful against DDPL countermeasure</td>
<td>SR of 70–100% for WDDL, MDPL and 17% SABL</td>
</tr>
<tr>
<td></td>
<td>[72, 73]</td>
<td>AES S-box</td>
<td>—</td>
<td>a higher MTD (&gt;10 times) for SPA than DPA</td>
</tr>
<tr>
<td>DoM methodology</td>
<td>[68]</td>
<td>PRESENT-80</td>
<td>power balanced circuits Alioto’s LPA method proved effective</td>
<td>40–60% decrease in the number of rounds of attack</td>
</tr>
<tr>
<td>template attack methodology</td>
<td>[76]</td>
<td>PRESENT-80</td>
<td>—</td>
<td>SVI value of 0.2–0.8.</td>
</tr>
<tr>
<td>information theoretic methodology</td>
<td>[83]</td>
<td>PRESENT-80</td>
<td>—</td>
<td>increase of maximum value of perceived information by 91%.</td>
</tr>
</tbody>
</table>
authors have not performed the attack to prove their logic’s LPA tolerance. The work in [89] is a recent countermeasure which extends the work in [90]. The idea is to add false keys to the original input data, to generate a control signal that alters the supply voltage scaling. Hence the measured leakage profile correlates with wrong data with the MTD exceeding 10 million. The same authors have proposed a voltage converter along with a discharge resistor and frequency sensors [91] as a countermeasure to LPA. Under the LPA scenario when the clock frequency is less than a particular range, the voltage converter sinks current through the discharging resistor which is further reshuffled to alter the original noise. Thereby the proposed methodology eliminates the dependency of the leakage current on the inputs. The authors have shown a reasonable improvement in the MTD values. Summary of the countermeasures available in the literature for the leakage-based PAA is given in Table 4.

**Summary:** Though LPA is a prominent attack similar to DPA, the number of available methods to defend the attacks is very less. Among the available ones such as [85, 86], there is a serious area overhead since it requires double the actual transistors for any circuit. In [89], how the circuit detects an LPA attack is not discussed, which is the starting point to apply the countermeasure. Hence it is important to develop more efficient techniques to scramble the leakage power profile and to validate its effectiveness against LPA.

### 3 Side-Channel security of intelligent sensor networks

The recent advancement in IoT technology drives us to review the security of the devices involved. The IoT architecture can be described using (i) a three-level model which is an extension of wireless sensor networks (WSNs), (ii) a five-level model and (iii) CISCO’s seven-level model in which the edge or computing nodes such as sensors and radio frequency identification readers form the first level [92]. It is important to ensure confidentiality and privacy of the data being used in the edge nodes and in network protocols for data transfer. This can be achieved by using cryptographic algorithms.

Finding a suitable light-weight cryptographic algorithm to satisfy the stringent power and area requirements of the nodes is one direction of research and is out of the scope of this study. This section is dedicated to the review of existing literature on SCAs in the edge nodes and the network layer, the countermeasures proposed for IoT applications, followed by a case study on SCA vulnerability of medical sensor nodes.

The categorisation of the available literature in SCA performed on IoT is pictorially represented in Fig. 3. The text under each attack shows the attack platform considered in each work.

#### 3.1 SCA on edge nodes

In most of the cases, the sensors are placed in remote locations without sufficient protection and are easily available to the users.

---

**Table 4** LPA countermeasures summary

<table>
<thead>
<tr>
<th>Technique name</th>
<th>Implementation</th>
<th>Overhead/weakness</th>
<th>Metrics achieved</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDRL [85, 86]</td>
<td>2-input NAND, AES crypto-core</td>
<td>area and power overhead (n-inverters, 2n-NAND gates, n-XOR gates for a n-input S-box circuit)</td>
<td>50% reduction in standard deviation</td>
</tr>
<tr>
<td>random ring oscillators [87]</td>
<td>AES S-box</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>power balanced circuits [77]</td>
<td>serpent S-box</td>
<td>50% decrease in PBC value for LDPA compared to CMOS</td>
<td>—</td>
</tr>
<tr>
<td>normalised DDPL [78, 79]</td>
<td>2-input NAND gate</td>
<td>area overhead; 2 transistors (1 PMOS + 1 NMOS), LPA resistance not verified</td>
<td>89.4% decrease in CoD than DDPL</td>
</tr>
<tr>
<td>false key controlled voltage scaling [89]</td>
<td>AES S-box</td>
<td>6.4% area overhead and a slight increase in leakage power consumption</td>
<td>—</td>
</tr>
<tr>
<td>voltage converter [91]</td>
<td>AES S-box</td>
<td>negligible power overhead</td>
<td>lowest MTD improved by a factor of 6145</td>
</tr>
</tbody>
</table>

---

**Fig. 3** SCA literature categorisation in IoT environment

Let us consider a typical IoT scenario in smart cities where smart sensors with integrated actuators are widely deployed to monitor and regulate traffic signals. These sensors will not be protected with tamper-proof bodies due to cost limitation [93]. Any compromise on the security of these sensor nodes will lead to malfunctioning of the devices thereby resulting in traffic congestion on the road and several accidents. The exposure of the cryptographic implementations fused in the edge nodes in an IoT environment to SCAs is studied in [94]. A proof of concept for the same is reported in [95] where the different components of smart home technology, a prominent realisation of IoT is attacked.

Nia and Jha [92] have discussed the IoT security at three levels namely at the edge node level, communication level, and edge computing level and have emphasised the dangers of SCA attack at each level. While Roosta [96] discussed the importance of security in sensor networks, the authors of [97–101] have briefly surveyed on the different physical attacks that are possible in these networks thereby emphasising the possibility of SCA in sensor devices.

Okeya and Iwata [102] were the first one to show the chances of SCA on message authentication codes with the assumption that underlying block ciphers are secure. Okeya et al. have described the various postulates for performing SPA to extract several key bits and DPA by selective forgery in a chosen plaintext scenario on encrypted message authentication code, one-key cipher block chaining message authentication code and parallelizable message authentication code. Based on the study in [102], the work in [103] has pointed out the possibility of timing-based SCA in sensor networks because of the specific property of the operating system running on the sensor nodes.

In [104], the authors have discussed invasive, semi-invasive and non-invasive attacks, their physical requirements and have shown a successful SPA attack on ECC and RSA implementations. The authors have also discussed the applicability of various countermeasures for these attacks in WSN environment. In [105], CPA with Hamming distance model (HDM) is conducted on the S-box output of triple data encryption standard (3DES) on a 32-bit central processing unit smart card and the whole 112 key bits of 3DES are recovered with moderate effort, which is around 80,000 power traces. Pongaliur et al. [93] have coined a three-phase attack
model for SCA in sensor networks and have presented taxonomy of the same. They have proposed a new technique, called process obfuscation, which can be used as a countermeasure for a variety of SCAs on sensor nodes. Furthermore, they have conducted EM-based SCA (EMA) on popular Tmote-skysensor nodes, using the commercially available equipment.

Apart from SCA, another challenging issue in the security of WSN is the node compromise, where an adversary causes physical damage to extract the secret key. SCA on edge nodes can avoid the detection of node compromise countermeasures [106]. To demonstrate this fact, De Meulenaer and Standaert [106] have performed successful DPA on 128-bit AES implementation on MICAz and TelosB motes with only 20 and 60 traces, respectively, for key retrieval. In the same work, their template-based SPA on 160-bit ECC implementation took around 9 h for 100 traces per template and has therefore highlighted the importance of robust and low-cost side-channel defences for small devices such as sensor nodes. A successful CPA with <30,000 power traces has achieved in [107] with a discussion on the various possibilities of EMA on the AES-128 engine on a Cookie WSN node. A very recent work on PAA on wireless sensor nodes is [108], where the AES algorithm implemented on nodes equipped with Atmel ATMega128RFA1 on IEEE 802.15.4 stack is successfully attacked. This work has created an alarm on the implications of SCA on similar wireless nodes and other IEEE 802.15.4 based protocols.

Han et al. [109] present an alternative way to enhance PAA on AES hardware implementations for WSN nodes by using a power model that adopts HD of intermediate results and suggests ordering plaintext inputs to improve the attack efficiency. In [110], a correlation EM analysis (CEMA) based interceptive SPA is proposed to attack the 16-byte secret key of the AES-128 engine for IoT applications by establishing a communication link using two ATmega-processor based Arduino boards. The key is retrieved successfully, using HD and 20,000 EM traces. In the implementation considered, data is accessed from a static random access memory along with 8-bit data bus and FLASH memory, which produces maximum EM radiation. A recent work in this domain is [111] where the visible light communication technology is shown vulnerable to PAA. The underlying principle is to exploit the intensity change of the light emitting devices in the transmitter unit, which is directly proportional to the power consumption. The PAA attack is carried out by placing a current sensor in the power line of the transmitter unit and by differentiating the current levels for a binary ‘0’ and ‘1’ data.

3.2 SCA on network protocols

An EM-based attack is conducted successfully in an emerging network and communication stack for smart homes namely, Thread [112]. The authors have performed the attack on a software implementation of the stack and have insisted on the need for efficient protection against SCA on all IoT communication protocols. Biryukov et al. have performed a successful CEMA on the software implementation of AES in a network protocol scenario [113], by varying only part of the inputs. AES is the standard cipher used in popular network protocols namely LoRaWAN and IEEE 802.15.4 where it is not possible to vary all the input bytes as assumed in most of the PAA works. 1300 EM traces were sufficient to retrieve the key byte and hence unprotected AES implementations should not be employed in any application.

3.3 Countermeasures

On the countermeasures part, [113] has suggested masking to avoid DPA, which is a general technique applicable to an unconstrained device since masking incurs area and delay overhead. Tsagou et al. [114] have suggested the use of high-k dielectrics to reduce the leakage current of CMOS-based devices, suitable for IoT applications. However, the authors have not performed PAA to prove their concept. Power-aware hiding [115] combined with masking is proposed as a block-level technique to balance the internal power with a knowledge of HW. The proposed technique is incorporated into the AES S-box and the fabricated results show comparatively lesser energy with sufficient DPA resistance and hence it is suitable for IoT applications.

Summary: Our work has discussed the possibilities of SCAs on the edge nodes and the communication protocols used in IoT. Since more and more devices are connected to the internet, it is highly important to devise effective countermeasures for such a resource constrained environment, where general purpose methods are not applicable. Recently, the awareness of SCAs has increased tremendously such that the cryptographic implementations on graphics processing unit, which are popular for cryptographic accelerators have been analysed against SCAs [116].

The importance of sensor network security in a healthcare application was mentioned in the introduction section. A real-life scenario that demands us to assess the same is the incident where in, the telemetry interface on the implanted pacemaker of Vice President Dick Cheney was disabled [117, 118]. Hence, any concerns regarding trustworthiness in medical devices must be addressed aggressively and proactively since it risks an individual’s life.

3.4 Case study: SCA security of medical sensor node

Sawand et al. [119] pointed out the strong convergence between the healthcare, IoT and cloud computing evolving as an application domain to improve the quality of service. Compared to WSN, achieving SCA security on medical sensor nodes is more challenging because of the more rigid memory and energy requirements [120]. Hence more research is required in understanding the weakness of these devices to SCA and to propose relevant methodologies to overcome the same. Furthermore, the medical sensor nodes are used in e-healthcare-based applications in which the patient’s vital data is communicated to the healthcare providers over wireless networks. Bradley et al. [121] have described the adoption of IoT technology in healthcare and pointed out the impact of SCA in the healthcare-IoT environment.

In [122], metadata-based privacy attack on an insulin pump was used to monitor the number of injections of insulin given to the patient and EM radiation from the blood pressure (BP) monitor was used to monitor the BP level of the patient. With the assumption that the communication link is fully encrypted, the possibility of using acoustic signals from the human body and the implanted medical devices as a leakage source is mentioned. The authors have suggested that signal strength reduction, information reduction, and noise addition techniques could be possible countermeasures for such kind of attacks.

4 Conclusion

IoT is the most promising future generation technology and it is important to preserve data security. Cryptography plays a major role in attaining the ‘root of trust’ for the devices that are involved in the IoT architecture. The edge devices namely sensor nodes that form the lower most level of IoT architecture are susceptible to SCA, which exploits the implementation leakages to extract the secret information. Our work has reviewed the most popular SCA namely PAA in detail, which depends on the power consumption of the target device. The PAA are categorised as SPA, DPA, and LPA. The existing works of SPA are summarised along with their applications. Rapid scaling of MOSFET technology accelerates the possibility to extend CMOS into nano-scale MOSFET structures and these alternative devices prove to be potential candidates for achieving the desired security. Hence the recent trends in DPA towards using nano-devices and adopting emerging technologies are reviewed. For the first time in the literature, the different ways of performing LPA is reviewed in detail, along with the emphasis on the countermeasures and metrics for the same.

Our paper has also reviewed the SCA scenarios on the edge devices and the communication protocols and has pointed out the vulnerabilities of healthcare applications as a case study. More research is required to make the sensitive data processed by the edge nodes and transmitted in the network layer, SCA resistant which makes ‘design for security’ an important aspect. When traditional CMOS technology is considered, the domination of

© The Institution of Engineering and Technology 2018
leakage power is a motivation to research the possibility of LPA on the sensor nodes and find a suitable solution to enhance IoT security.

5 Acknowledgments

This work has been done from the grant received from Visvesvaraya PhD Scheme of Ministry of Electronics and Information Technology, Government of India, being implemented by Digital India Corporation. This work was also supported by Special Manpower Development Programme for Chips to System Design (SMDP-C2SD) project sponsored by the Department of Electronics and Information Technology (DeitY), Government of India.

6 References

