When Hardware Security Moves to the Edge and Fog

Longfei Wang
Department of Electrical Engineering
Unviersity of South Florida
Tampa, Florida 33620
Email: longfei@mail.usf.edu

Selçuk Köse
Department of Electrical Engineering
Unviersity of South Florida
Tampa, Florida 33620
Email: kose@usf.edu

***Abstract*—The emergence of edge and fog computing paradigm brings significant advantages to the ubiquitous cloud computing. Reduced response time and energy consumption as well as relaxed communication bandwidth requirement enable rapid advancement of mission-critical applications. Energy harvesting is an efficient and viable solution to realize sustainable operation of edge devices. The lack of continuous network connection, increased number of collaborative end-user nodes, limited energy capacity, and vast deployment of resource constrained edge devices, however, impose unprecedented security concerns. As an essential part of energy-harvesting-powered edge computing devices, an on-chip voltage regulator is leveraged in this perspective paper as a lightweight countermeasure against charging and certain side-channel attacks through, respectively, reconfiguration of the impedance matching network and randomization of the power consumption profile. Security adaptive on-chip power delivery thus enables trustworthy edge and fog computing with negligible power and area overhead.**

I. Introduction

Edge and fog computing is an emerging paradigm and a promising solution to extend the capability of cloud computing to the edge of network to enable energy efficient, fast, and privacy-enhanced applications [1]. By adding computing capability close to the data sources, part of the workload can be offloaded from the cloud to reduce the latency and mitigate the bottleneck induced by limited network bandwidth. The reduced latency and physical proximity further translate into energy savings [2]. Moreover, leveraging localized computation and storage, raw data is processed at the edge instead of directly uploaded to the cloud such that user privacy can be better protected [1]. Such improvements on top of the conventional cloud computing paradigm benefit various applications demanding real-time processing including healthcare and activity tracking, augmented reality, cognitive systems, and smart utility services [3].

Sustainable and long-term operation of edge devices are desirable. Energy harvesting from ambient sources is essential to realize such a goal. A wireless RF energy source is among one of the most promising approaches to power edge devices due to the wide availability, low cost, and easy implementation [4]. Resourced edge devices such as smartphones and tablets have sufficient battery and electronic budget to perform conventional security protocols. It is, however, impractical for energy-harvesting-powered lightweight and cost-effective edge devices to execute such protocols due to limited resources [5]. Meanwhile, such devices are vulnerable to wireless power transfer attacks [6], [7] and side-channel attacks [8], [9]. A malicious receiver within an RF energy harvesting system may implement a charging attack by generating redundant power transfer requests to the transmitter such that the power received by the normal operating receiver nodes is greatly reduced. Furthermore, side-channel attack can be performed by an attacker through monitoring the power consumption or electromagnetic (EM) emission of the load circuit to obtain the secure workload information.

For lightweight energy-harvesting-powered edge devices, due to the fundamental limit of device feature size and battery performance, leveraging existing functions for security enhancement becomes a natural choice. Such approaches include signal processing for authentication and analog characteristics for encoding [5]. As an essential part of an RF energy harvesting system [10], a voltage regulator is utilized to convert the DC voltage generated by the rectifying circuit to another voltage level and regulate that voltage level to adapt to the load circuit. On-chip voltage regulation has several advantages as compared to off-chip implementation such as faster response speed, reduced board area, and applicability for fine-grain power management. On-chip voltage regulator is thus leveraged in this work to realize a security-adaptive on-chip power delivery system to enhance the security level against charging and certain side-channel attacks through reconfiguration of impedance matching network and randomization of the power consumption profile, respectively.

The rest of this paper is organized as follows. Background information regarding RF energy harvesting system and on-chip voltage regulation is provided in Section II. Details regarding the utilization of an on-chip voltage regulator as a countermeasure against, respectively, charging attack and side-channel attack are provided in Sections III and IV. Conclusions are offered in Section V.

II. Background

A. RF energy harvesting systems

A typical RF energy harvesting system includes multiple receiver nodes powered by an RF energy source. RF energy may come from ambient sources such as mobile base stations

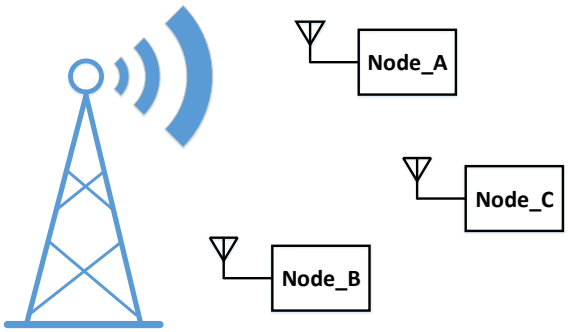

Fig. 1. Illustration of a general RF energy harvesting system.

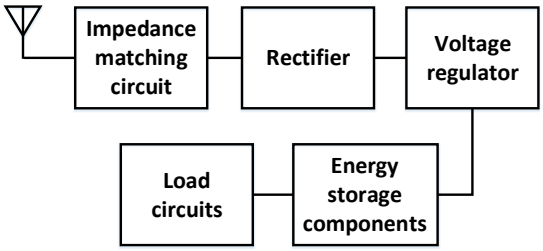

Fig. 2. Block diagram of a receiver node within an RF energy harvesting system.

and WiFi access points and it may also come from dedicated sources such as a sink node [4], with the later as the focus of this paper. A general RF energy harvesting system and the block diagram of a receiver node are illustrated, respectively, in Figs. 1 and 2. The system consists of an RF energy source and one or more receiver nodes. Each receiver node includes an antenna, an impedance matching network, a rectifier, a voltage regulator, energy storage components, and load circuits. RF energy received by the receiver node is converted to a DC voltage through a rectifier and that DC voltage is further converted and regulated to a voltage level applicable to the energy storage components and load circuits. The supply voltage level and power conversion efficiency are largely affected by the impedance matching network [11]. If the supply voltage is too low, it may not be sufficiently strong to power the load circuits. On the other hand, if the power conversion efficiency is low, huge energy loss may lead to hotspots of the chip which are detrimental to the normal operation of voltage regulators [12].

B. On-chip voltage regulation

On-chip voltage regulation has been drawing significant attention within many application domains such as processors [13], energy harvesting systems [14], and wearable devices [15]. Major voltage regulator types including switched-capacitor (SC) converter, buck converter, and low-dropout regulator (LDO) have their respective advantages that can be suitable for various design specifications. An LDO regulator has fast response speed and high efficiency when the difference between input and output voltages is low. Buck converter can achieve a high power efficiency over a wide load current range while SC converter has the benefits of easy integration and high power density. Distributed on-chip voltage regulation [16], [17] where multiple on-chip voltage regulators are distributed across the chip to provide localized voltage regulation has been demonstrated as a promising trend to improve power noise and response time. Significant amount of work has been performed to improve the power conversion efficiency, response speed, and output voltage ripple of voltage regulators [13]–[19]. Meanwhile, various techniques have been proposed to improve the thermal [20], [21] and reliability [12], [22] profile of voltage regulator and the load circuit. As security issues of integrated circuits become more prominent, voltage regulators can be further leveraged to enhance the security level of the load circuit against various attacks [8], [9], [18], [23]–[29].

III. On-chip voltage regulator as a countermeasure against charging attack

A. Charging attack

Wireless power transfer attacks have recently drawn attention due to the popularity of RF-based wireless power transfer networks and potential security flaws. Several security attacks within a wireless power transfer system have been identified, which include safety attacks, charging attacks, interference attacks, spoofing attacks, software attacks, and monitoring attacks [6]. Most of these attacks are directly or indirectly related to the power transfer efficiency or energy that can be harvested by the receiver nodes. Without sufficient power or supply voltage level, the load circuits cannot function properly. Implementation of efficient countermeasures against power failure attacks becomes imperative.

A charging attack targets to decrease the power transferred to the normal receiver nodes. As an example, suppose $Node\_C$ in Fig. 1 is a malicious receiver node. $Node\_C$ may send redundant energy requests to the power transmitter even though sufficient energy has been harvested in $Node\_C$ such that the energy received by $Node\_A$ and $Node\_B$ is reduced. A malicious receiver node $Node\_C$ can also feign the role of the power transmitter to emit the out-of-phase RF waves [7] to degrade the power received by $Node\_A$ and $Node\_B$.

B. Countermeasures against charging attacks

During a charging attack, the available power delivered to the load circuits may demonstrate intermittent behavior. During power failures, the intermediate computations may be interrupted and computation errors can occur within the processing unit of edge devices. To deal with these problems, a secure intermittent-robust computation (SIRC) framework leveraging the non-volatile characteristics of spintronics is proposed in [7]. The intermediate computation states can be stored in non-volatile majority gates built with magnetic tunnel junction-based devices when there is a power outage. When

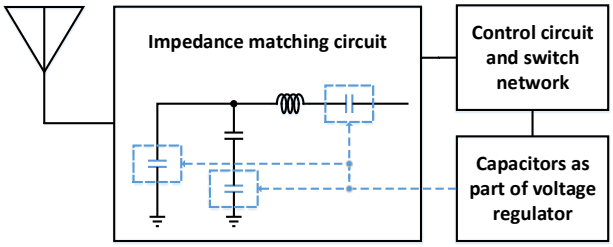

Fig. 3. On-chip voltage regulator as a countermeasure against charging attack.

the supply voltage recovers, the computation can be resumed from where it was stopped. Furthermore, a majority voter can be implemented in the power transmitter based on the power consumption profile of each node to decide if there are any malicious nodes. Such a countermeasure may lead to false positives as different receiver nodes may perform diverse functions at disparate time intervals, which lead to dissimilar power consumption profile. Charging requests from these mistakenly identified receiver nodes may be subsequently neglected by the transmitter to cause permanent power failures.

A proactive countermeasure to reduce the occurence of power failures due to a charging attack and to decrease or even totally cut off the energy transferred to the malicious receiver nodes is more promising. If malicious receiver nodes cannot receive power from the power transmitter and totally powered off after all of the stored energy is exhausted, other wireless power transfer attacks such as interference attack and spoofing attack could also be mitigated. Efficiency of wireless power transfer and supply voltage level at the receiver node are largely affected by the impedance matching network [11]. For a certain impedance matching network, the supply voltage at the receiver node peaks within a narrow RF frequency range. Out of this narrow frequency band, both the supply voltage level and power conversion efficiency sharply drops. Furthermore, a different impedance matching network may have similar frequency band that leads to the peak supply voltage. However, the peak voltage levels can still be different. Similarly, for a certain emitted RF wave from the transmitter, receiver nodes can obtain the required supply voltage level and high power efficiency only when the impedance matching network is optimized. Insufficient supply voltage level and low power efficiency may lead to, respectively, denial of service and hotspots within the receiver chip.

Based on the above observations, the impedance matching network can be configured in synchronization with the RF frequency emitted from the power transmitter to obtain the optimal supply voltage level and power efficiency. Capacitors within the voltage regulator can be leveraged to serve this need as demonstrated in Fig. 3. With the aid of the additional control circuit and switch network, capacitors not in use within the voltage regulator can be reconfigured to different locations of the impedance matching circuit as indicated in Fig. 3 to realize optimal frequency band consistent with the received RF wave.

Popularity of reconfigurable switched-capacitor voltage regulators [18], [30]–[32] within various application domains including energy harvesting systems makes them a natural choice to aid the reconfiguration of impedance matching network. Capacitors typically consume more chip area than the control circuit and switch network. Utilizing the capacitors within the voltage regulator instead of additional dedicated capacitors for the impedance matching network helps to reduce the area overhead. Capacitor within the reconfigurable voltage regulator may not be always in use during each switching phase. Different combination and connection of idle capacitors can form a wide variety of capacitance values. These capacitance values can further be exploited to tailor the impedance matching network. For example, through parallel or series connection of only two idle capacitors and three available locations in the impedance matching network, more than ten different configurations can be realized.

Within an RF-based energy harvesting system, if the RF wave emitted by the power transmitter has a fixed frequency, during a charging attack when power received by the regular edge devices is reduced, supply voltage drop can be detected by the control circuit to dynamically reconfigure the impedance matching network to seek the chance of harvesting energy from other ambient sources to mitigate possible power failure. If the power transmitter is equipped with the capability to dynamically change the frequency of the emitted RF wave, synchronization between the power transmitter and normal edge nodes can be realized to periodically alter the RF frequency and impedance matching network. Such synchronization can be initiated from the transmitter leveraging preambles and pilots of radio communication [5]. Dynamically changing the RF frequency makes it harder for the attacker to implement charging attack.

Based on the charging duration, the total number of available impedance matching network configurations can be adapted accordingly such that the transmitted RF energy cannot be intercepted by the malicious receiver nodes only during one charging interval. This need-based design strategy helps to simplify the control circuit and switch network. The proactive countermeasure essentially provides encryption for power transfer. It complements well with the SIRC framework to enhance the security levels of RF-based energy harvesting edge devices against charging attacks.

IV. On-chip voltage regulator as a countermeasure against side-channel attack

A. *Side-channel attack*

A side-channel attack [33], [34] is a type of non-invasive attack that leverages side-channel leakage information such as power consumption profile and EM emissions to obtain secure information of the chip. Data obtained from the side-channel leakage can be directly analyzed or statistically operated to perform, respectively, simple and differential side-channel analysis attacks. Regarding power and EM leakage, simple power/EM analysis attacks and differential power/EM analysis attacks can be implemented. Typical power analysis attacks

require the measurement of the power consumption profile through the power pins of the chip while EM analysis attacks can be more powerful as a direct contact of the integrated circuits may not be necessary [9]. Edge devices especially energy-harvesting-powered ones can be deployed in the field without continuous monitoring, and more easily accessed by attackers as compared to general purpose devices to implement side-channel attacks [29].

B. Countermeasures against side-channel attacks

The SIRC framework proposed in [7] is also effective to mitigate the power and EM side-channel attacks. For the proposed SIRC architecture, a certain logic operation is realized through magnetic tunnel junction based majority gates. A selector is utilized to generate a selection signal based on the inputs. Combined with the outputs of the spin-based low power and high efficiency true random number generator, majority gates can be configured to equivalent logic realizations with a different power consumption profile. If all of the flip-flops within an original logic design are replaced with the proposed majority gates, the total number of different power consumption profiles can be considerable, thus enhancing the security against power side-channel attack. Furthermore, the state of sensitive non-volatile memory storing secure information can change once exposed to external magnetic field to mitigate EM side-channel attack.

Additionally, an on-chip voltage regulator can be leveraged to further enhance the security of the edge devices against power and EM side-channel attacks. Distributed on-chip voltage regulation is more secure against EM side-channel attack as compared to off-chip voltage regulation as shorter and thinner metal lines enabled by the former lead to less EM emission [9]. Moreover, the input current profile of a multiphase SC converter has a strong correlation with the activation pattern of each single phase. By randomly changing the activation pattern of available phases, the input current profile can be altered under a certain load current condition to increase the power analysis based side-channel attack security [8], [18]. By adding a time-delay to half of the converter phases or withholding a random amount of charge through flying capacitors, time-delayed converter-reshuffling technique [23] and charge-withheld converter-reshuffling technique [24] can be respectively realized to enhance the security against machine-learning-based differential power analysis attacks. A security-adaptive voltage conversion scheme is proposed in [26] as a lightweight countermeasure against leakage power analysis attacks. Redundant current is discharged through a resister to change the power consumption of the load once a leakage power analysis attack is sensed in the proposed framework. Leakage power analysis attack countermeasure can also be realized through false key-controlled aggressive voltage scaling proposed in [27]. Higher correlation coefficients are achieved for the added false keys compared to the correct key to mislead the attacker in the proposed scheme. Efficient countermeasures leveraging the unique characteristics of on-chip voltage regulators within edge devices can be combined to mitigate simultaneously charging and side-channel attacks.

V. Conclusion

Gigantic advantages of edge and fog computing paradigm prompt vast deployment of edge devices as valuable additions to cloud computing, enabling mission-critical applications and enhanced privacy. Energy harvesting is a promising way to realize sustainable operation of edge devices. Due to limited resources, conventional security protocols cannot be practically implemented and energy-harvesting-powered edge devices can be more vulnerable to security attacks. Charging and certain side-channel attacks are emphasized in this work. On-chip voltage regulators are leveraged as lightweight solutions to elevate the security against such attacks through, respectively, dynamic reconfiguration of impedance matching network and randomization of power consumption profile. Such a framework is compatible with the recently proposed secure intermittent-robust computation architecture to further boost security.

Acknowledgment

This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451 and by a Cisco Research Award.

References

[1] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, October 2016.

[2] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30-39, January 2017.

[3] A. V. Dastjerdi and R. Buyya, "Fog computing: helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112-116, August 2016.

[4] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V. C. M. Leung, and Y. L. Guan, "Wireless energy harvesting for the internet of things," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 102-108, June 2015.

[5] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 14-21, February 2015.

[6] Q. Liu, K. S. Yildirim, P. Pawelczak, and M. Warnier, "Safe and secure wireless power transfer networks: challenges and opportunities in RF-based systems," *IEEE Communications Magazine*, vol. 54, no. 9, pp. 74-79, September 2016.

[7] A. Roohi, R. Demara, L. Wang and S. Köse, "Secure intermittent-robust computation for energy harvesting device security and outage resilience," In *Proceedings of the IEEE Conference on Advanced and Trusted Computing*, pp. 1-6, August 2017.

[8] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," In *Proceedings of the IEEE/ACM Design Automation Conference*, pp. 1-6, June 2015.

[9] A. W. Khan, T. Wanchoo, G. Mumcu, and S. Köse, "Implications of distributed on-chip power delivery on EM side-channel attacks," In *Proceedings of the IEEE International Conference on Computer Design*, pp. 329-336, November 2017.

[10] H. J. Visser and R. J. M. Vullers, "RF energy harvesting and transport for wireless sensor network applications: principles and requirements," *Proceedings of the IEEE*, vol. 101, no. 6, pp. 1410-1423, June 2013.

[11] X. Huang *et al.*, "Epidermal radio frequency electronics for wireless power transfer," *Microsystems & Nanoengineering*, vol. 2, October 2016, Art. no. 16052.

[12] L. Wang, S. K. Khatamifard, U. R. Karpuzcu, and S. Köse, "Mitigation of NBTI induced performance degradation in on-chip digital LDOs," In *Proceedings of the Design, Automation and Test in Europe Conference & Exhibition*, pp. 803-808, March 2018.

[13] C. Gonzalez *et al.*, "The 24-core POWER9 processor with adaptive clocking, 25-Gb/s accelerator links, and 16-Gb/s PCIe Gen4," *IEEE Journal of Solid-State Circuits*, vol. 53, no. 1, pp. 91-101, January 2018.

[14] C. Li *et al.*, "A 0.2V trifilar-coil DCO with DC-DC converter in 16nm FinFET CMOS with 188dB FOM, 1.3kHz resolution, and frequency pushing of 38MHz/V for energy harvesting applications," In *International Solid-State Circuits Conference*, pp. 332-333, February 2017.

[15] Y. Park *et al.*, "A design of a 92.4% efficiency triple mode control DC-DC buck converter with low power retention mode and adaptive zero current detector for IoT/wearable applications," *IEEE Transactions on Power Electronics*, vol. 32, no. 9, pp. 6946-6960, November 2016.

[16] S. Köse and E. G. Friedman, "Distributed on-chip power delivery," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, no. 4, pp. 704-713, December 2012.

[17] L. Wang, S. K. Khatamifard, O. A. Uzun, U. R. Karpuzcu, and S. Köse, "Efficiency, stability, and reliability implications of unbalanced current sharing among distributed on-chip voltage regulators," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 11, pp. 3019-3032, November 2017.

[18] O. A. Uzun and S. Köse, "Converter-gating: a power efficient and secure on-chip power delivery system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 169-179, June 2014.

[19] S. Köse, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "Active filter based hybrid on-chip DC-DC converters for point-of-load voltage regulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 4, pp. 680-691, April 2013.

[20] S. Köse, "Thermal implications of on-chip voltage regulation: upcoming challenges and possible solutions," In *Proceedings of the IEEE/ACM Design Automation Conference (DAC)*, pp. 1-6, June 2014.

[21] S. K. Khatamifard, L. Wang, W. Yu, S. Köse, and U. R. Karpuzcu, "Thermogater: thermally-aware on-chip voltage regulation," In *Proceedings of the IEEE International Symposium on Computer Architecture (ISCA)*, pp. 120-132, June 2017.

[22] L. Wang and S. Köse, "Reliable on-chip voltage regulation for sustainable and compact IoT and heterogeneous computing systems," In *Proceedings of the ACM/IEEE Great Lakes Symposium on VLSI (GLSVLSI)*, pp. 1-6, May 2018.

[23] W. Yu and S. Köse, "Time-delayed converter-reshuffling: an efficient and secure power delivery architecture," *IEEE Embedded Systems Letters*, vol. 7, no. 3, pp. 73-76, September 2015.

[24] W. Yu and S. Köse, "Charge-withheld converter-reshuffling (CoRe): a countermeasure against power analysis attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 5, pp. 438-442, May 2016.

[25] W. Yu and S. Köse, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 8, pp. 1152-1163, August 2016.

[26] W. Yu and S. Köse, "Security-adaptive voltage conversion as a lightweight countermeasure against LPA attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 7, pp. 2183-2187, July 2017.

[27] W. Yu and S. Köse, "False key-controlled aggressive voltage scaling: a countermeasure against LPA attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 12, pp. 2149-2153, December 2017.

[28] W. Yu and S. Köse, "Exploiting voltage regulators to enhance various power attack countermeasures," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1-12, 2018.

[29] S. Köse, "Efficient and secure on-chip reconfigurable voltage regulation for IoT devices," In *Proceedings of the ACM/IEEE Great Lakes Symposium on VLSI*, pp. 369-374, May 2017.

[30] W. Jung, D. Sylvester, and D. Blaauw, "A rational-conversion ratio switched-capacitor DC-DC converter using negative-output feedback," In *International Solid-State Circuits Conference*, pp. 218-219, February 2016.

[31] X. Liu, L. Huang, K. Ravichandran, and E. Sanchez-Sinencio, "A highly efficient reconfigurable charge pump energy harvester with wide harvesting range and two-dimensional MPPT for internet of things," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 5, pp. 1302-1312, May 2016.

[32] S. Bang, D. Blaauw, and D. Sylvester, "A successive-approximation switched-capacitor DC-DC converter with resolution of $V_{IN}/2^N$ for a wide range of input and output voltages," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 2, pp. 543-556, February 2016.

[33] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks: revealing the secrets of smart cards," *Springer Science*, 2008.

[34] K. Boris and B. David, "An information-theoretic model for adaptive side-channel attacks," In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 286-296, July 2007.