Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT

SASWAT KUMAR RAM*, Department of Electronics and Communication Engineering, Amrita Vishwa Vidhyapeetham, Amrita School of Engineering
SAUVAGYA RANJAN SAHOO, Analog Design Engineer, Marquee Semiconductor
BANEE BANDANA DAS, Department of Computer Science and Engineering, SRM University
KAMALAKANTA MAHAPATRA, National Institute of Technology, Rourkela, India
SARAJU P. MOHANTY, University of North Texas, Denton, USA, USA

Recently, harvesting natural energy is gaining more attention than other conventional approaches for sustainable IoT. System on chip (SoC) power requirement for the internet of things (IoT) and generating higher voltages on chip is a massive challenge for on-chip peripherals and systems. In this paper, an on-chip reliable energy harvesting system (EHS) is designed for IoT with an inductor free methodology. The control section monitors the computational load and the recharging of the battery/super-capacitor. An efficient maximum power point tracking (MPPT) algorithm is also used to avoid quiescent power consumption. The reliability of the proposed EHS is improved by using an aging tolerant ring oscillator. The effect of Trojan on the performance of energy harvesting system is analyzed, and proper detection and mitigation mechanism is proposed. Finally, the proposed ripple mitigation techniques further improves the performance of the aging sensor. The proposed EHS is designed and simulated in CMOS 90nm technology. The output voltage is in the range of 3-3.55 V with an input 1-1.5 V with a power throughput of 0-22μW. The EHS consumes power under the ultra-low-power requirements of IoT smart nodes.

CCS Concepts: • **Hardware → Application specific integrated circuits**.

Additional Key Words and Phrases: Aging Tolerant, Analog Trojan, Ripple-Less, Sustainable IoT, Energy Harvesting System (EHS), Maximum Power Point Tracking (MPPT), Charge Pump (CP).

ACM Reference Format:
Saswat Kumar Ram, Sauvagya Ranjan Sahoo, Banee Bandana Das, Kamalakanta Mahapatra, and Saraju P. Mohanty. 2022. Eternal-Thing 2.0: Analog-Trojan Resilient Ripple-Less Solar Harvesting System for Sustainable IoT. 1, 1 (December 2022), 26 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

Authors' addresses: Saswat Kumar Ram, Department of Electronics and Communication Engineering, Amrita Vishwa Vidhyapeetham, Amrita School of Engineering, Amrita Nagar, Coimbatore, Tamil Nadu,India, 641-112, saswatram01@gmail.com; Sauvagya Ranjan Sahoo, Analog Design Engineer, Marquee Semiconductor, Patia, Bhubaneswar, Odisha,India, 751-024, srs.sahoo85@gmail.com; Banee Bandana Das, Department of Computer Science and Engineering, SRM University, Mangalgiri, Guntur, Andhra Pradesh,India, 522-240, banee.bandana@gmail.com; Kamalakanta Mahapatra, National Institute of Technology, Rourkela, India, Sector-1, Rourkela, Odisha,India, 769-008, kkm@nitrkl.ac.in; Saraju P. Mohanty, University of North Texas, Denton, USA, Texas, USA, saraju.mohanty@unt.edu.

1 INTRODUCTION

Advancement in fabrication technologies and scaling down of MOSFETs leads to use of tiny devices for various applications including Internet of Things (IoTs) and consumer electronics. The IoT inspires every aspect of life by making things smarter with increasing number of users. The IoT consists of end node devices (sensor nodes), gateways and cloud [4, 32]. An IoT node to become self-sustainable, the energy requirement of the power hungry sensors should be taken care of, as the batteries are having a limited lifetime. A smart node in IoT has the capability of sensing, processing and communicating required information. To design a state of art energy harvesting system (EHS) is a demanding exercise and factors affecting its performances are also equally important and are discussed in this paper. Rechargeable batteries/super-capacitors were investigated and are found to be economical and safe [47]. Harnessing natural energy and storing in supercapacitor is a suitable alternative. Solar energy is preferred, due to its wide availability and no mechanical parts are involved in its conversion to electrical energy among various available natural resources as solar [44], thermoelectric [6, 32, 51], radiofrequency (RF) [31], piezoelectric [42, 50], and wind [32]. The solar power is affected by low conversion efficiency but can be overcome by using suitable conditioning techniques. The charge pump is preferred as converter for boosting solar output, which are suitable for on-chip implementation [45] and to drive loads for various applications [8, 19, 28, 39, 49]. An IoT smart node comprises of energy source (solar), harvesting system, SoC, sensors, and transceivers [23, 38]. The reliability of the EHS is also measured in terms of its resilience against various types of attacks. The causes may be due to the intentional aging or by attack due to some specific analog kind of Trojan. The analog circuits are more resemblances with the attacks made by adversaries, and it is difficult to counter the attacks [5, 7, 12, 20, 24, 26, 30]. To make the energy harvesting system reliable, the Trojans that may affect the behavior of the energy harvesting system should be addressed [11, 30, 40, 52]. In recent times analog Trojans are used to degrade the circuit's reliability. The empty spaces in the layout are targeted to insert hardware Trojans that affect the behavior of circuits. A detailed analysis of attacks due to Trojan should be discussed, and mitigation mechanisms are adopted to improve the reliability of the entire harvesting system. The aging tolerant mechanisms should be investigated and incorporated to prevent the IC from the intentional aging type of attack. The recycler may use the Burn-in mechanism for intentional aging. By using a suitable aging tolerant mechanism, the performance of the aging sensor [10, 40, 53] in the harvesting system can be further improved.

The rest of the paper is organized in the following manner: Section 2 discusses the reliability issues and resilient IoT node as Eternal-Thing. Section 3 describes the related prior research. Section 4 presents the novel contribution of this research paper. Section 5 elaborates the reliable secure solar harvesting system (RSSEHS). Section 6 discusses the reliability issues with detection and mitigation mechanisms. Section 7 presents the simulation results, and finally, Section 8 concludes the paper with future research directions.

2 THE ISSUE OF RELIABILITY AND OUR VISION OF RESILIENT IOT NODE AS ETERNAL-THING

In this work, our primary focus is on identifying the causes affecting the performance of the energy harvesting system. The reliability and security are given prime importance in designing the system with circuit-level modifications and adding new circuits to improve the reliability. The harvesting system must face many challenges from fabrication to deployment in handling the IoT end node devices. The critical reliability degradation issues may be categorized as follows:

- The presence of ripples at the output due to the fluctuations in supply voltage.
- The tracking time of MPPT is affected due to switching frequency variation.

- The boosting performance of converter affected by variation in switching frequency.
- The adversary may affect the reliability of EHS through insertion of malicious agents (Trojans) into the design or through intentional aging by subjecting the EHS to higher temperature.

2.1 Impact of Switching Frequency (f_{ossc}) on Reliability

The variation in supply voltage affects the switching frequency, leading to the presence of more ripples at the output of the energy harvesting system. It degrades the performance of EHS, causing heating of devices, increase in noise level causing distortions, and can reduce the life span of devices. An efficient and reliable energy harvesting system must have fewer ripples. The ripples are mainly due to the following reasons as (a) optimizing the size of the capacitors and output current by fast switching of MOSFETs, (b) low on-resistance, and (c) rapid charging and discharging of pumping capacitors. Further, the change in switching frequency also affects the tracking time in MPPT operation and the conversion efficiency of the converter.

2.2 Attack Methods

In this research we discussed and presented how a fabrication-time attacker can leverage analog circuits to create a hardware attack that is small and stealthy (requires a trigger sequence before affecting the chip performance). The open spaces in an empty and routed design can be used to place these types of attacks. Outsourcing the chip fabrication opens the doors for hardware attacks. The most pernicious fabrication-time attack is the dopant-level Trojan. This type of Trojans converts the trusted circuitry into malicious circuitry by changing the dopant ratio on the input pin to the victim transistor. It either connects the input to a logic-0 or logic-1. The detection of it is very difficult and can be known post fabrication from the performance [3, 21, 46]. To defend against malicious hardware inserted during fabrication, researchers adopts two basic terminologies i.e., (a) use side channel information (power and temperature) to characterize acceptable behavior in an effort to detect the malicious behavior [1, 16, 29, 33] (b) to use additional circuits to detect the dramatic changes in the functionality (when malicious circuits gets activated) [17, 22, 48].

There are different types of attacks caused by analog Trojans in the existing circuitry to degrade the reliability. The attacker may affect the frequency circuitry or any sensitive wire in the system that can dominate the system performance. There are few attacks by the adversary using A2 Trojan that uses the inherent characteristics of the circuits that has charge sharing and capacitative coupling to disturb the entire circuit operation.

The oscillating frequency (f_{ossc}) coming from the ring oscillator (RO) is one of the crucial parameters that can predict reliability. The RO section of the energy harvesting system is one of the prime targets for attackers to age the RO section by subjecting it to a higher temperature. The adversary may subject higher temperature intentionally to age the RO section, which ultimately affects the oscillation frequency of the RO leading to performance degradation of the EHS. Hence, the RO should be designed with an aging tolerant feature to safeguard the EHS. In this chapter, our focus is also in designing a aging tolerant ring oscillator (prone to aging and intentionally subject to higher temperature) to improve the overall reliability of the EHS.

We envision sustain end node of internet of things (IoT) with energy harvesting and security and/or reliability capability as “Eternal Thing 2.0”. Fig. 1 shows the high-level structure of an reliable Trojan resilient IoT smart node. As depicted in Fig. 1 the supply to end node devices, SoCs and trans-receivers are supplied from the EHS. Any deviation in supply cause malfunction in these devices, so the harvesting system should be resilient and reliable enough to different type of attacks caused by adversary. The design of harvesting system addressing these unavoidable things motivate us

to design an reliable Trojan resilient harvesting system ("Eternal Thing 2.0") and as per authors knowledge security and reliability of EHS never discussed in earlier literature.

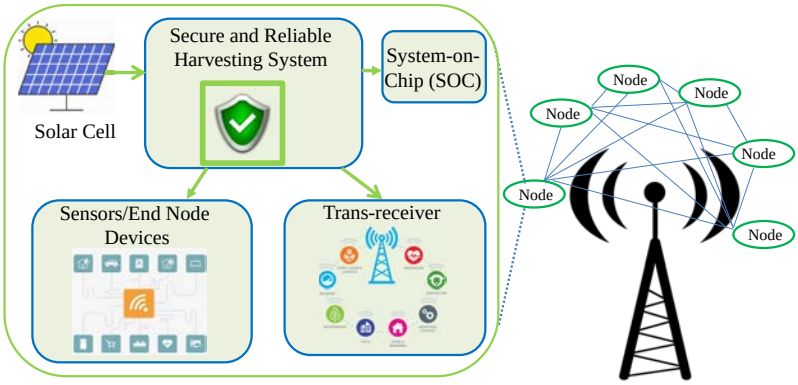

Fig. 1. An Reliable Trojan Resilient IoT Smart node.

3 RELATED PRIOR RESEARCH

Various control techniques for different type of input energy sources are available in literature [4, 6, 25, 32, 39, 44] for energy harvesting system [18, 27, 34, 41, 51]. Photovoltaic (PV) is a prominent energy source due to its wide local availability, sustainability, environment friendly nature, no moving parts, and no carbon emission. By adopting suitable conditioning techniques, energy can be extracted for supplying computational load and is stored for blackout periods in rechargeable battery/supercapacitors [15, 35, 40].The self-sustainable energy harvesting system design for IoT nodes uses DC-DC converters for boosting as the output achieved is non-conditioned. To achieve a maximum power, various maximum power point tracking (MPPT) algorithms used in literature [32, 34, 40]. In [43], authors discussed aging tolerant methodologies for sustainable operation of circuits [23, 40].

In our earlier research [40, 41] we have discussed and addressed the energy harvesting system design along with security issues and used physically unclonable function (PUF) and aging sensor to safe guard our EHS. The further challenges in terms of improving the reliability and security of the system is crucial and should be addressed. The reliability and security issues includes aging influence on EHS performance along with various type of attacks made by adversaries. The summary of the related work is presented in Table 1.

3.1 A2 Trojan Attack

The globalization of the semiconductor industry leads to various hardware security issues and is gaining researchers' attention. Among various hardware security threats, the insertion of a hardware Trojan in the circuitry is a significant concern and needs to be addressed. The hardware Trojans are not always digital; analog Trojans are present that can target the events occurring in the circuit to be triggered [2]. The Trojan circuits are small and can be inserted into the most sensitive wires that can affect the entire operation of the system. These threats must be identified, and a proper signal is generated that can indicate the presence of a Trojan. Based on the signal obtained, the effect of the Trojan should be mitigated in the run time and can be termed as a run time detection and mitigation of Trojan. Hou et al. in [13, 14] designed a processor, inserted Trojan into it, and successfully detected the same. Deng et al. in [9] used a

configurable structure with a control mechanism termed BIAS, inserted in the nets, and successfully detected Trojan using run-time detection techniques. As per the research, it is evident that the analog Trojan can drastically degrade the system performance in an integrated circuit. Based on these challenges, this research paper focuses on the security issues of the harvesting system by correctly detecting and mitigating the A2-based Trojan during run-time. A detailed discussion on the activation, detection and mitigation of the analog A2-Trojan will be discussed further in the section 6.3.

Table 1. Summary of Related Research Works

Works	**Methodology Used**	**Salient Features**
Shao, et al. [44]	DC-DC Converter (Charge Pump) with Variable Switching Frequency for maximum output Power control	⇒ Inductor less Design. ⇒ MPPT with variable Switching Frequency. ⇒ Variable switching frequency needs extra hardware.
Carreon, et al. [6]	Dynamic Impedance Matching with Thermoelectric generators (TEG) as source	⇒ TEG as an alternative energy source. ⇒ Impedance matching of boost converter and TEG. ⇒ TEG output needs conversion to DC adding more cost.
Kim, et al. [19]	Regulated Charge Pump with Optimum Power Point Algorithm (OPPT)	⇒ Inductor less design with regulated charge pump. ⇒ Optimum power point algorithm (OPPT) for MPPT for Indoor light conditions. ⇒ Application limited to indoor lightning.
Shih, et al. [45]	DC-DC converter (Charge Pump) with Band gap Reference output Controller	⇒ Four-phased charge pump design. ⇒ Bandgap reference circuit in the feedback path for regulation through comparators. ⇒ Clock generation scheme is complex.
Kim, et al. [18]	Successive Approximation Register (SAR) MPPT with Active and Power down Mode	⇒ SAR MPPT for low power consumption in Indoor light conditions. ⇒ Limited to indoor lightning.
Mondal, et al. [27]	Adaptive MPPT for harvesting System	⇒ Harvesting system design using current starved VCO for frequency adjustment during MPPT. ⇒ Negative feedback control for MPPT. ⇒ Additional circuits for frequency adjustment.
Ram, et al. [40] (Eternal Thing)	Ultra low power secure solar harvesting system design using existing circuitry with aging detection mechanism	⇒ Secure self-sustainable harvesting system design. ⇒ Converter with adiabatic charging scheme for reduction in power. ⇒ Physically unclonable functionality (PUF) used for securing the harvesting chip. ⇒ Aging sensor incorporated within chip to detect counterfeiting of ICs.
Current Paper (Eternal Thing 2.0)	**Analog Trojan resilient ripple-less reliable ultra low-power energy harvesting system**	⇒ Reliable solar energy harvesting system resilient to Analog Trojan. ⇒ Detailed discussion on ripples at output and its mitigation. ⇒ Trojan Detection and mitigation mechanism. ⇒ Embedded with improved recycled EHS-IC detection mechanism.

4 NOVEL CONTRIBUTIONS OF THE CURRENT PAPER

The current paper addresses an unified energy harvesting system design that analyzes the reliability and security issues in designing a self-sustainable reliable secure solar energy harvesting system.

4.1 Research Question and Challenges Addressed in the Current Paper

The design of an harvesting system itself is a tough task. To choose a suitable energy source and its proper conditioning needs a lot of effort. As per the deployment and usage the aging affect is a concern along with security. The reliability degradation of the EHS IC is due to several type of attacks. These issues arises lot of questions and the authors tried their level best to address these challenges in this research paper.

4.2 Proposed Solution of the Current Paper

The review based on various researchers work, and their outcomes encourages us towards designing of a reliable EHS. The hill-climbing algorithm for maximum power point tracking (MPPT) is appropriate with low hardware cost and ease of design. The capacitor value modulation (CVM) scheme is adopted using digital capacitor banks as variable frequency for tuning MPPT needs additional control circuits, thereby consuming more area on-chip. To counter the attack due to analog Trojan (intentionally varying the temperature and A2 Trojan) and the ripple analysis with proper mitigation for a secure reliable ripples-less EHS is designed in this paper for sustainable IoT.

4.3 Novelty of the Proposed Solution

The systems discussed in the earlier literature may suffer from the presence of ripples at the output, attack due to Trojans, security related issues and none of the researchers addressed these challenges. The contribution of this paper is as follows:

- Design of a novel ultra-low-power self-sustainable reliable solar energy harvesting system (PV-EHS).
- A novel aging tolerant mechanism is implemented to improve the reliability of EHS.
- A novel methodology to mitigate the effect of Trojan caused by increasing temperature of RO intentionally and A2 Trojan detection with mitigation technique for EHS.
- Improvement in Performance of Aging Sensor for Recycled EHS-IC Detection.

5 PROPOSED RELIABLE SECURE SOLAR ENERGY HARVESTING SYSTEM (RSSEHS)

The proposed reliable, secure solar energy harvesting system (RSSEHS) is depicted in Fig. 2, which is capable of converting the lower level solar voltage to higher level voltages using DC-DC converters to drive the computational load and rechargeable battery. The control section consists of a digital controller (FSM) [37], which controls the operation of the current sensor and MPPT module. The proposed PV-EHS is designed using (a) aging tolerant ring oscillator (RO) (b) a non-overlapping clock generator (c) auxiliary charge pump with level shifter (d) Converter , (e) current sensor (f) MPPT module with digital controller, (g) Trojan detection and mitigation unit, (h) aging sensor. The security using PUF and aging sensor was addressed in [40]. The circuits in EHS whose performance will get degraded due to aging and attacks by adversaries are discussed briefly.

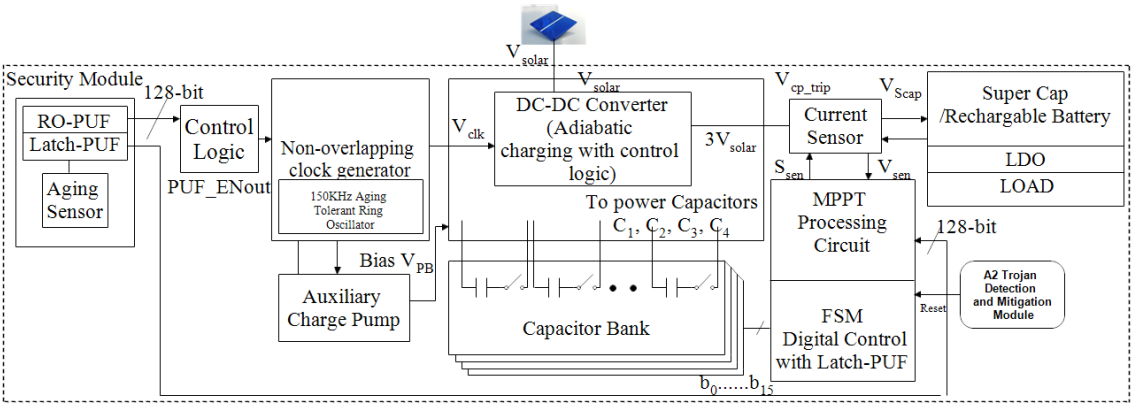

Fig. 2. Block Diagram of Proposed Secure Reliable Energy Harvesting System.

5.1 Non-overlapping Clock Generator with Level Shifter and Auxiliary Charge Pump

The reliable ring oscillator generates the essential clock frequency (150 KHz) and is given to non-overlapping clock generator (NOCG). The NOCG generates two non-overlapping clocks for the auxiliary charge pump (ACP) and the level shifter (LS) with reduced shoot through effect. The LS and ACP provides the switching signals and other biases needed for voltage booster. The level shifter is used to boost the clock amplitude for reducing the losses due to charge transfer during voltage boosting.

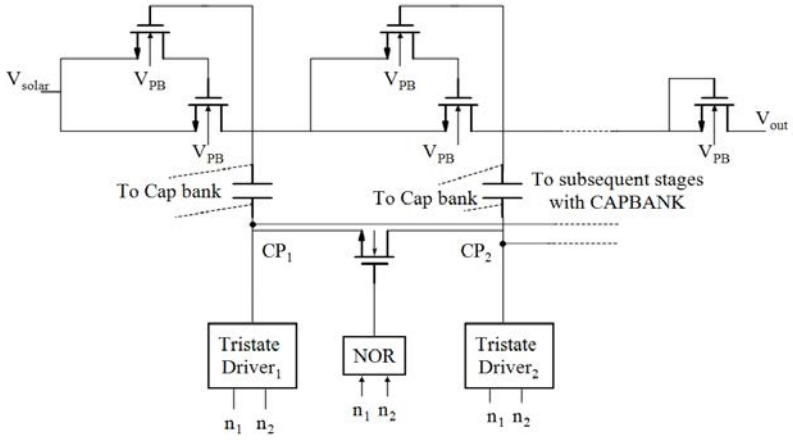

Fig. 3. Two Phase Clocking with Two-Step Charging Charge Pump with Separate Body Bias.

5.2 Adiabatic-Charging and Charge-Sharing Charge Pump with Separate Body Bias

Fig. 3 depicts the circuit diagram of a charge pump (CP) as a voltage tripler. A two-stage adiabatic charging and charge sharing charge pump are used to minimize the power consumption. The two-stage charging with charge sharing reduces

the energy delivered by the voltage source to 50% as compared to one-step charging. the connection of capacitor banks with the charge pump capacitors for achieving the impedance matching between solar cell and converter. A capacitor value modulation scheme is adopted for tuning the capacitor banks for impedance matching. The power conversion efficiency is used to boost the input voltage by the conversion ratio (CR). It can be represented by the expression in equation 4. The control circuit consists of two tri-state drivers and signals n_1 and n_2, which are meant for charging and discharging the capacitors C_{a1} and C_{a2} [40].

The boosting of voltages in the charge pump is achieved by applying alternative clock pulses to charge the solar energy across the capacitors C_u (includes power capacitors C_1, C_2, C_3, C_4) and level up the negative plate by the same potential. The DC-DC converter used has the conversion ratio (CR) of three (CR=3).

The impedance of the converter can be expressed by:

$$Z_{cp} = \frac{V_{solar}}{I_{in}} = \frac{1}{2f_s C_u} \frac{1+\alpha}{\left(3 - \frac{V_{out}}{V_{solar}}\right)\alpha} \tag{1}$$

Equation. 1 indicates that the impedance of the charge pump is inversely proportional to C_u. α is the capacitor ratio between the first and second stage. The capacitor C_u is connected to programmable capacitor banks for impedance matching through CVM. From the small signal model of the converter, it can be observed as:

$$[2V_{solar} - (V_{out} - V_{solar})] \times \alpha C_u = \frac{1}{2} \times \left(\frac{T \times V_{out}}{R_L}\right), \tag{2}$$

where T and R_L are the switching period and load of the SoC, respectively. By rearranging equation 2, it can be written as:

$$V_{solar} = \left(\frac{1}{2} * \frac{T}{R_L} * \frac{1}{\alpha C_u} + 1\right) * \frac{1}{3} * V_{out} \xrightarrow{Match} V_{MPP} \tag{3}$$

From equation. 3, it is found that the MPPT is achieved by varying the frequency f and capacitor C_u. As the frequency is constant here, so a variable C_u is proposed for impedance matching. The power capacitors are digitalized as capacitor banks; as digital implementation consumes less power with reduced noise.

The power conversion efficiency (PCE) is a measure of boosting of input as per conversion ratio and is given by:

$$PCE = \frac{V_{out}}{V_{solar} \times CR} \times 100\% \tag{4}$$

5.3 MPPT Module

The variation in irradiance level and temperature degrades the PV-cell performance. To extract the maximum power, an energy efficient hill-climbing MPPT technique is used, which senses the voltages after capacitor value modulation (CVM) and then process it through iterations for taking final decision on MPPT achievement. The MPPT algorithm with CVM is depicted in [40]. The MPPT procedure is controlled by a digital controller (FSM) and finite state machine (FSM) for one MPPT cycle is well presented in [36, 40, 41]. An environment sensor triggers the MPPT procedure by enabling signal S. The period till S is zero the solar cell provides supply to load and rechargeable battery but when the signal S goes high the MPPT circuit is triggered. The total current during sensing phase is passed to the sample and hold circuits at equal intervals for storage, comparison and final decision. A digital controller comprising of FSM that generates the necessary control signals for the entire MPPT procedure [40, 41]. A current sensor is used to sense the power information from the output of the DC-DC converter. The current sensor, in this design is controlled by the FSM signals S_{sen} and S_{senbar}. When S_{senbar} is low, the total current of the converter is used for sensing and at that instant

the supercapacitor provides the reference current to the current sensor. When the MPP is achieved, S_{sen} is low and the current is used to charge the supercapacitor (S_{cap}) again.

6 PROPOSED METHODS FOR IMPROVING RELIABILITY WITH PROPER DETECTION AND MITIGATION

In our proposed EHS, the presence of different modules like RO, counter in FSM are the major source of reliability degradation. The paper also addresses the reliability and security issues as: (1) reliability analysis with proposed mitigation technique, (2) Trojan detection with mitigation techniques, and (3) Improvement in Performance of Aging Sensor [40]. These reliability issues and appropriate mitigation techniques are briefed in this section.

6.1 Reliability Issue due to Variation in Switching Frequency (f_{ossc})

The oscillation frequency (f_{ossc}) of RO is driving maximum modules in the EHS. The f_{ossc} of the CMOS RO is influenced by various parameters like voltage, aging etc,. The change in f_{ossc} causes various adverse effects on the output and MPPT performance and are discussed further.

6.1.1 Causes of Frequency Degradation of CMOS RO. The frequency degradation is mainly due to the variation in supply volatge and due to aging (as the IoT node has to be ON for Longer period) and are discussed.

Against Supply Voltage Variation:

In conventional CMOS inverter-based RO, the f_{ossc} is a function of supply voltage ($f_{ossc} \propto V_{solar}$). The variation in supply voltage affects the propagation delay of the inverter; as a result, a shift in f_{ossc} is observed. The frequency deviation in conventional CMOS RO driven by V_{solar} is shown in Fig. 4. As it is earlier discussed that our EHS is tuned for a solar voltage of 1.22 V for better efficiency. Hence, we assume the f_{ossc} of RO at this voltage is the reference f_{ossc}. The degradation in frequency observed for a solar voltage fluctuation from 1 to 1.5 V as shown in Fig. 4. The degradation is measured as follows.

$$\%\Delta f\Big|_{V_{solar}} = \frac{f_{ossc}\Big|_{V_{solar}=1.22V} - f_{ossc}\Big|_{V_{solar}}}{f_{ossc}\Big|_{V_{solar}=1.22V}} \tag{5}$$

The result shows, conventional CMOS RO used in harvesting system experience a maximum degradation in f_{ossc} of 12 %. The degradation in frequency from its reference value (150 kHz) causes ripple at the output. The ripples caused by this type of variation are temporary because once the RO returns to its nominal supply voltage (1.22 V), the output becomes ripple-free.

Frequency Degradation due to Aging:

Further, the impact of aging on f_{ossc} of RO is also observed. From our earlier discussion, NBTI and HCI are the major cause of degradation in f_{ossc} of RO. The impact of aging on conventional RO is presented in Fig. 5 (a) and (b). In the non-oscillation mode of RO, the impact of the NBTI effect is more pronounced, as depicted in Fig. 5 (a). In conventional RO, as in Fig. 5 (a) half of the PMOS are always in NBTI stress due to negative bias at the gate input ($V_{GSp} = -V_{solar}$). The impact of HCI is shown in Fig. 5 (b). The impact of HCI is more pronounced during the oscillation mode of RO due to switching (0 to V_{DD}) at the gate terminal of NMOS. Fig. 6 depicts the rate of degradation in the oscillation frequency of CMOS RO due to aging over 20 years. The result shows that the conventional CMOS RO experiences a maximum frequency degradation of 25%.

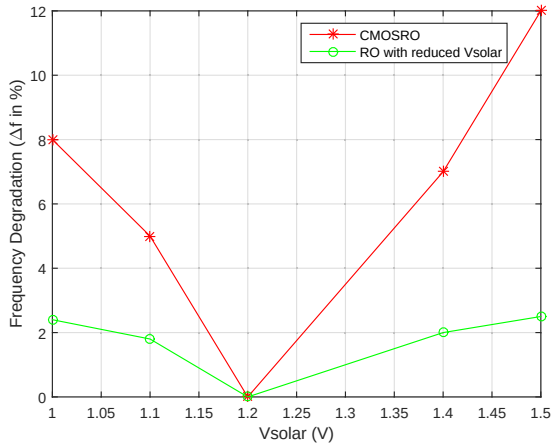

Fig. 4. Degradation of Oscillation Frequency (in %) with V_{solar}

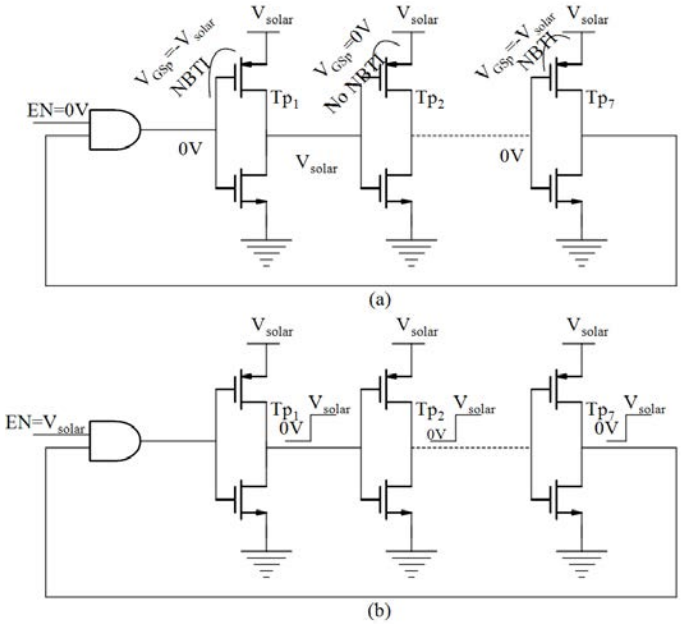

Fig. 5. CMOS RO (a) NBTI (b) HCI

From the above discussion it is clear that, the variation in supply voltage causes temporary degradation in oscillation frequency f_{ossc}, whereas aging causes permanent degradation. Both these factors influence the reliability of EHS, either temporarily or permanently. The impact of degradation in f_{ossc} on reliability are discussed further.

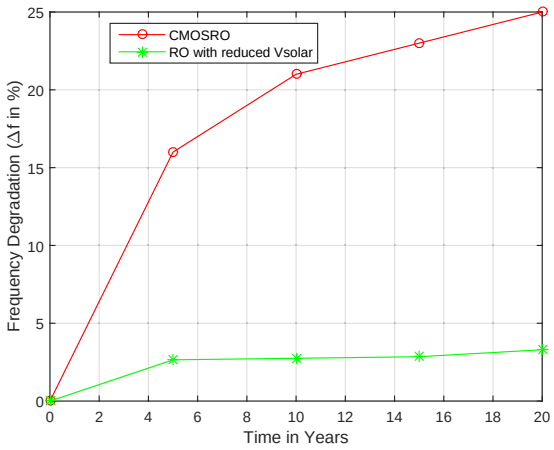

Fig. 6. Degradation of Oscillation Frequency with Time.

6.1.2 Impact of Frequency Degradation on Ripples. In a MOSFET the path from source to drain is diagrammatic by a linear resistance adequate to R (R_{on}) as in equation. 6:

$$R_{on} = \left(\frac{1}{\mu_n C_{ox} \frac{W}{L} (V_{GS} - V_T)} \right). \tag{6}$$

The charge transfer occurs from one capacitor to another through switches in the charge pump. The clock signal is applied with the needed frequency for switching of the MOS switches [15]. The voltage transfer in charge pumps can be explained as depicted in Fig. 7.

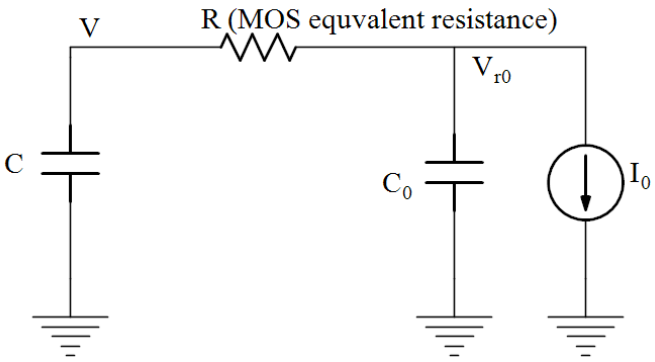

Fig. 7. Simplified Equivalent Circuit at Output Stage of Charge Pump.

By applying KCL, the differential equation in time domain for the above circuit depicted in Fig. 7 can be written as

$$C\frac{dV}{dt} = -C_0\frac{dV_{r0}}{dt} - I_0 \tag{7}$$

$$-C\frac{dV}{dt} = \frac{V - V_{r0}}{R} \tag{8}$$

Substituting equation 7 in 8 and taking the derivative w.r.t. time gives

$$\frac{RC_0 d^2V_{r0}}{dt^2} = \frac{dV}{dt} - \frac{dV_{r0}}{dt} \tag{9}$$

The derivative of V in equation 9 can be evaluated using equation 9, then rearranging the term yields

$$\frac{d^2V_{r0}}{dt^2} + \left(\frac{1}{C} + \frac{1}{C_0}\right)\frac{dV_{r0}}{Rdt} = -\frac{I_0}{RCC_0} \tag{10}$$

Since the charge transfer from one capacitor to another has to occur in the time interval T/2 requires some time to pass through the MOS equivalent resistance R. Thus V_{r0} increases from zero to $V_{r0,\max}$, which is the ripple and return to zero. Therefore, the boundary conditions for equation 10 are given by equation 11 and 12.

$$V_{r0}(t = 0) = 0 \tag{11}$$

$$V_{r0}\left(t = \frac{T}{2}\right) = 0 \tag{12}$$

With these boundary conditions, the differential equation for V_{r0} can be derived as

$$V_{r0} = \frac{TI_0\left(\exp^{-\frac{t}{RC_p}} - 1\right)}{2\left(C + C_0\right)\left(\exp^{-\frac{T/2}{RC_p}}\right)} - \frac{I_0 t}{C + C_0} \tag{13}$$

Where $C_p = C \,||\, C_0 = (1/C + 1/C_0)^{-1}$.
The C_0 is in parallel with C. RC_p is much less than T/2. V_{r0} can be approximated as equation 14.

$$V_{r0} = \frac{TI_0}{C + C_0}\left(1 - \exp^{-\frac{t}{RC_p}}\right) - \frac{I_0 t}{C + C_0} \tag{14}$$

If V_{r0} is assumed to achieve its maximum value $V_{r0,\max}$, at time $t_{\max}$, then $V_{r0,\max}$ can be obtained by solving $dV_{r0(t=tmax)}/dt = 0$. The result yields $t_{\max}$ as given by equation 15.

$$t_{\max} = RC_p \ln\left(\frac{T/2}{RC_p\left(1 - \exp\left(-T/2RC_p\right)\right)}\right) \tag{15}$$

By substituting $t_{\max}$ into equation 13 we can obtain the output of maximum ripple as

$$V_{r0,\max} = \frac{TI_0}{2\left(C + C_0\right)} - \frac{RI_0CC_0}{\left(C + C_0\right)^2}\left(1 + \ln\left(\frac{T/2}{RC_p}\right)\right) \tag{16}$$

From equation 16, it is clear that, the ripples at the output voltage depends on the f_{ossc} (f_{ossc}=(1/T)), R, I_0, and the load capacitor. By tuning R of the MOSFET, ripples can be reduced, but it may affect boosting efficiency. A large on-chip load capacitor leads to area-overhead. So we have chosen the f_{ossc} as the major parameter for ripple mitigation.

6.1.3 Impact of Frequency Degradation on Converter and MPPT. The f_{ossc} coming from the RO is used for switching of MOS devices to pump voltages through capacitors into the converter. The degradation in f_{ossc} can directly affect the boosting efficiency of the converter, thereby reducing its conversion efficiency and results in ripples at the output. Further, any degradation in the f_{ossc} affects the MPPT procedure. The degradation largely influences the time required for achieving MPP in f_{ossc}. More number cycles are needed to achieve MPP if there is a degradation in f_{ossc}. The f_{ossc}

of RO must be stable enough, although the operation of EHS to avoid these issues, so a RO with stable frequency needs to be designed.

From the above discussion, we have observed that the frequency degradation affects the ripples at the output, boosting the efficiency of the converter and the performance of the MPPT module. The f_{ossc} must undergo a lower deviation from its nominal value, i.e., 150 kHz. The degradation in the f_{ossc} must be investigated. Towards resolving these issues, we have used a RO that lowers the frequency degradation due to supply voltage variation and lowers the impact of aging [43]. The change in V_t due to temperature variation and aging causes the delay to increase which leads to degradation in oscillation frequency. The modified CRO in [43] is preferred in our design for better reliability and area-efficient design. This architecture is similar to conventional RO but driven by a reduced supply voltage through an NMOS switch. The architecture of RO with reduced supply voltage to lower the variation in f_{ossc} is discussed further.

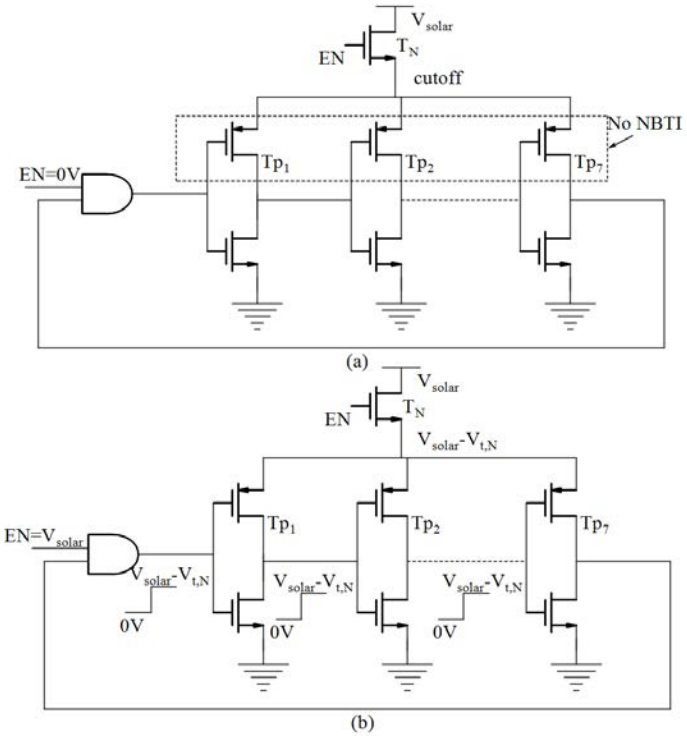

Fig. 8. RO with Reduced V_{solar} (a) NBTI (b) HCI.

6.2 Reliability Improvement by Lowering Frequency Degradation

The proposed architecture of RO with its mode of operation is shown in Fig. 8. In the oscillation mode, the cascaded inverters in the RO operate at a reduced supply voltage of V_{solar}-V_T. The impact of supply voltage variation and aging on f_{ossc} is discussed as follows.

Against Supply Voltage Variation:

Fig. 4 presents the degradation in frequency of RO with reduced V_{solar}. The variation in frequency is less at 1.22 V, and as the voltage deviates from this point, the frequency deviation increases. The result from Fig. 4 shows that this architecture experience a maximum frequency shift of 2.25% from its nominal value of 150 kHz. It signifies that, by using RO with reduced V_{solar}, a small variation in f_{ossc} is observed, which leads to less ripple at the output.

Frequency Degradation due to Aging:

The impact of aging, i.e., both NBTI and HCI stress on the RO with reduced supply voltage, is shown in Fig. 8. From Fig. 8, it is clear that the impact of both NBTI and HCI stress is significantly reduced as compared to conventional RO. As shown in Fig. 8, during the non-oscillation mode, the RO is getting cut-off from the supply voltage. Hence all the PMOS becomes stress-free (V_{GS}=0), as compared to half of the PMOS under NBTI stress in conventional CMOS RO. Further, in oscillation mode, the gate of all the NMOS experiences a reduced logic swing of 0 to V_{solar}-V_T. This reduction in swing (as compared to 0-V_{DD}) in CMOS) lowers the impact of HCI stress. As a result, the impact of aging on this RO is significantly lowered. Hence very lower degradation in f_{ossc} is observed over a time interval of 20 years.

The frequency degradation of RO is shown in Fig. 6. This result is obtained by applying both NBTI and HCI stress continuously for 20 Years. From Fig. 6, it is clear that RO with reduced supply voltage experiences a very low degradation in f_{ossc} of 2.25% as compared to 25% in CMOS RO.

From the above discussion, it is observed that the RO with reduced supply voltage undergoes lower frequency degradation as compared to the conventional CMOS RO. This leads to lower ripples at the output. The boosting efficiency of the converter is less affected as the frequency degradation is less. The MPPT tracking time is also less influenced. As a result, both temporary (due to supply voltage variation) and permanent (due to aging) reliability issues can be addressed, which is briefed in the simulation result.

6.3 Resilience Against Attack

A hardware attack consists of a trigger and a payload. The malicious circuits are similar in nature of the actual circuits and activate the attack payload. We have shown a fabrication time attack A2 that is small, stealthy, and controllable. Based on this we have developed our circuit, which is based on charge accumulating on a capacitor from infrequent events inside the System. If the charge-coupled infrequent events occur frequently enough, the capacitor will fully charge and the payload is activated, which deploys a privilege escalation attack. The attacks on EHS are possible in different ways to affect the system's performance. Different types of Trojans can affect the circuit performance, leading to erroneous results. For example, a Trojan can be inserted into the design to influence the MPPT operation in EHS. The energy harvesting system is more sensitive to A2-based Trojans, mainly the counter module in the MPPT circuit. A brief discussion on Trojan affecting circuit behavior and a suitable mitigation technique is discussed in this section. Further, we discussed the impact of the intentional aging attack by the adversary.

6.3.1 A2 Trojan Detection and Mitigation circuit. Our design uses a particular analog hardware Trojan (A2) that uses the capacitative principles to charge from relative values in wires as they switch in between logic levels. Fig. 9 depicts the circuit diagram of A2 Trojan based on charge-sharing and capacitative-coupling. As depicted in Fig. 9, a voltage gets build up in the payload by charging from the nearest supply voltage to set the V_{wire}. The instant the capacitor (payload) is fully charged, it affects the actual circuit performance. This voltage level ultimately targets the sensitive wires like a reset of the MPPT module.

Our main objective is to detect the A2 Trojan to check the voltage building on the RST node of the counter during its operation in MPPT achievement. The process of detecting the Trojan with a proper mitigation technique is presented

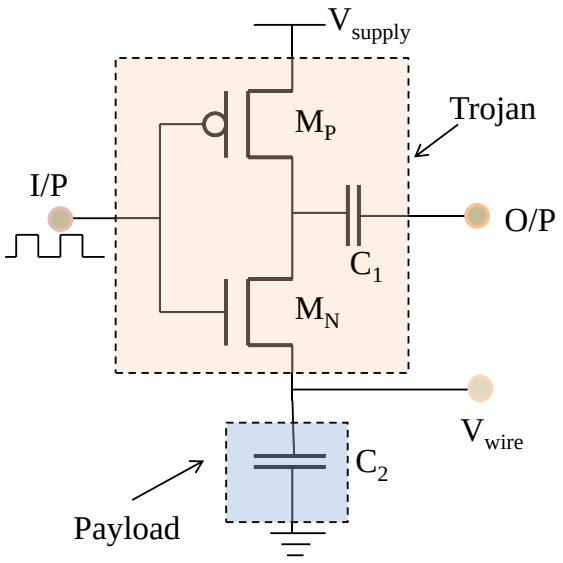

Fig. 9. Schematic Diagram of a Analog Malicious Trojan (A2) Hardware.

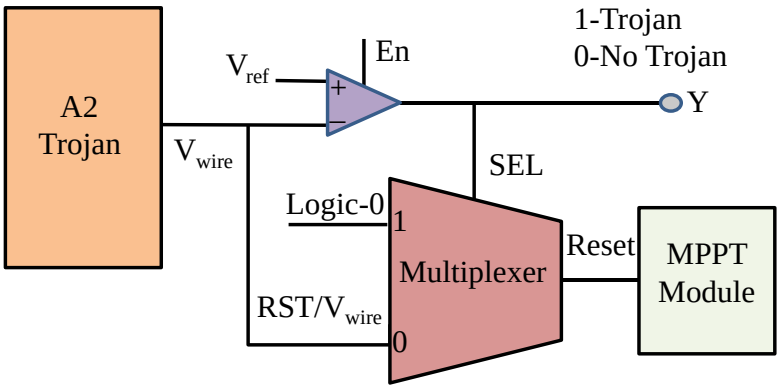

Fig. 10. Proposed Detection and Mitigation Mechanism for A2 Trojan.

in Fig. 10. The Trojan is used to charge the payload, and once V_{wire} gets charged it triggers the reset input of the MPPT. It affects the MPPT procedure to end before MPP achievement due to the premature counter reset. The MPPT operation is triggered by an environmental sensor S. Once S is triggered the MPPT operation gets initiated and the corresponding circuits get activated. That is the particular time when the counter in the FSM generates the control signals and clocks for required operation. The voltage from the nearby wires can be used to charge the payload gradually and once it crosses V_{ref} thereby affecting the functionality. The V_{wire} is the reset input of the MPPT module and if premature changes have occurred in it that resets the MPPT procedure thereby degrading the performance of the system. The output Y is the Trojan detection circuit's output, which is 1 or 0 as per the comparison with V_{ref}, so Y detects for

presence or absence of Trojan. That is ultimately the signal can be used for mitigating the issue. The present design uses a multiplexer that is not affected by Trojan and is a part of the mitigation circuit proposed, so Trojan effects on multiplexer is not considered. The detection circuit is mainly for the A2 Trojan as the circuit resembles with the converter circuits used in this system. The MPPT circuit will be ON periodically as per the environmental sensor S, and as per the timing of the MPPT cycle the *En* of the comparator is active, that leads to limited scope for the other attacks to jeopardise the activity of MPPT.

Timing Calculation during A2 Attack:

- In this energy harvesting system, one MPPT cycle constitute of 32-clock cycles, Hence total time for one MPPT cycle= 6.66μS X 32=213.12μS.
- The total MPPT cycles in the process of MPPT achievement = one MPPT cycle * number of thermometer bits =213.12μS X 16=3410μS=3410μS.
- The time 3410μS indicates the total MPPT cycles once the MPPT module is triggered by environmental sensor *S*.
- In detection circuit as depicted in Fig. 10, the *En* signal is made high for 3410μS by the controller to detect the occurrence of Trojan. The process of detecting the A2 Trojan and its mitigation procedure is discussed below. The adversary may use A2 Trojan for premature reset by changing the logic level of reset through the payload at V_{wire} within 3410μS.

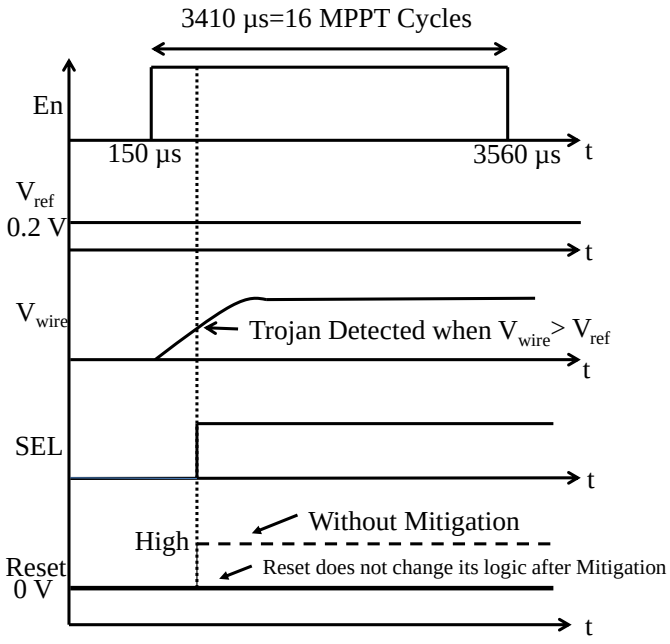

Fig. 11. Timing Diagram for A2 Trojan Detection and Mitigation

The detection and mitigation of A2 Trojan, once is initiated by an adversary is discussed further and is shown in Fig. 10.

- When En=1, the comparator compares the V_{wire} with V_{ref} (0.2 V), if $V_{wire} > V_{ref}$ then Y=1 else 0 (Y=1 indicates a Trojan detected).
- The comparator output (Y) is used a select line for the multiplexer. The period till SEL=0, indicates that there is no Trojan and the reset input of the counter is low which is the wire voltage V_{wire}. This does not affect the MPPT operation as counter is in normal operating mode.
- The instant at which a voltage gets build up in the V_{wire}, it is compared with V_{ref} and the output of the comaprator is high. This indicates the occurrence of a Trojan (Y=1). The selection line of the multiplexer becomes high (SEL=1) makes the reset of the counter to maintain its logic level without doing reset. This leads the MPPT operation to continue without any interruption due to occurrence of A2 Trojan. The detail procedure of Trojan detection and mitigation is well explained by the timing diagram depicted in Fig. 11. The process of A2 Trojan detection and mitigation is validated and briefed in result section.

6.3.2 Intentional Aging. As discussed earlier, the sensitivity of oscillation frequency of the ring oscillator against aging allows the adversary to affect the functionality of the harvesting system. The adversary may subject higher temperature intentionally to age the RO section, which ultimately affects the oscillation frequency of the RO leading to performance degradation of the EHS. Hence, the RO should be designed with an aging tolerant feature to safeguard the EHS. By keeping this in mind, the RO with reduced supply voltage is used in the RO module in place of conventional RO. The influence of intentional aging on EHS performance is briefed in the result section.

7 SIMULATION RESULTS

7.1 Simulation Setup

The reliable, secure solar-EHS is designed in CMOS 90nm technology library. The capacitors used in designing of the converter and capacitor banks are Metal-Insulator-Metal (MIM) capacitors. The solar input is in the range of 1-1.5 V (with temperature 27°C). The load is designated with a potentiometer, whose resistance can be varied from 200KΩ to 10MΩ in parallel with a supercapacitor having 33mF value. The Relxpert simulator in the virtuoso environment is used for aging analysis. It uses the model library given by the foundry, which supports both NBTI and HCI effects. Both fresh (at time t=0) and aged netlist are extracted at different aging intervals (t = 5, 10, 15, 20 years) to estimate the ripple at the output. The ripple against supply voltage variation and aging is observed for both conventional CMOS RO and RO with reduced supply voltage.

The effect of Trojans on EHS by the adversary is presented. Towards implementing the A2 Trojan, a circuit as shown in Fig. 9 is implemented. By applying a suitable supply and clock, the payload is charged to set the voltage at the output (V_{wire}) of A2 Trojan after 150μS (this is the time to trigger MPPT operation by environmental sensor S in this simulation set up). The performance improvement of the aging sensor is addressed after incorporating the RO with reduced supply voltage in this design.

7.2 Reliability Analysis

7.2.1 Ripple Analysis. The ripple analysis against the supply voltage variation and aging are analyzed and presented in Fig. 12 and Fig. 13. As per the analysis, both the ROs, i.e., CMOS RO and RO with reduced supply voltage, are examined by varying the V_{solar} in the range 1 V-1.5 V. The ripple due to variation in supply voltage is depicted in Fig. 12. The nominal voltage for efficient operation of EHS is 1.22 V, so any deviation from this will cause more ripples at the output. The RO with reduced supply voltage experiences a lower ripple than CMOS RO over the entire range of supply voltage

variation. The RO with reduced supply voltage reduces the ripples by 80% than CMOS RO and is due to its lower frequency degradation as presented in Fig. 4.

Further, the impact of aging on ripple is analyzed by subjecting continuous stress at an aging interval of 5, 10, 15, 20 years, and ripples at the output are shown in Fig. 13. It is observed from the simulation results that RO with reduced solar voltage experiences fewer ripples as compared to CMOS RO against aging. It is due to the aging resilience property of the RO with reduced solar voltage. The RO with reduced solar voltage experiences ripples within 100 mV over continuous aging of 20 years.

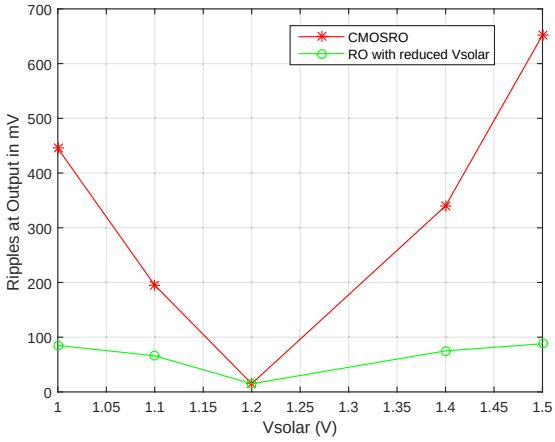

Fig. 12. Ripples at Output with Variation in V_{solar}

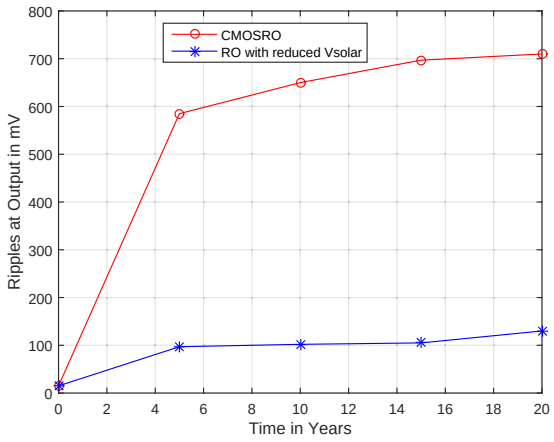

Fig. 13. Ripples at Output of Charge Pump (in mV) v/s Time.

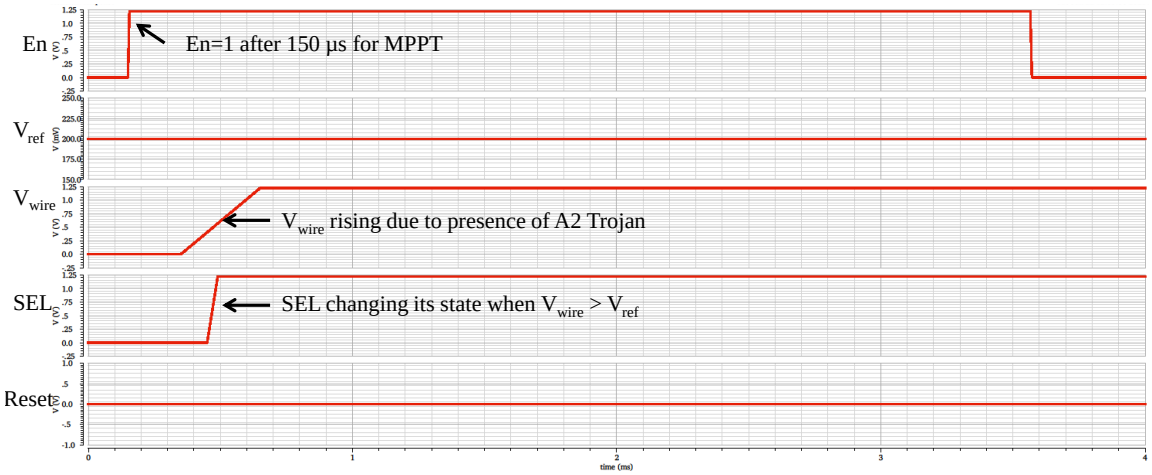

Fig. 14. Simulation Result of Detection and Mitigation Mechanism of A2 Trojan.

7.2.2 Reliability in terms of Resilience to Various Attacks. As discussed, the adversary may use different types of attacks (Trojans) to influence the EHS operation. The attack due to the insertion of a suspicious element (A2 Trojan) and intentional aging in the EHS is presented.

A2 Trojan Detection and Mitigation:

The simulation result in Fig. 14 shows the detection and mitigation mechanism for A2 Trojan. As the MPPT operation uses a counter and the reset input of the counter is more crucial for MPPT timings. The A2 Trojan tries to build a voltage in the wire (V_{wire}) of reset input, which ultimately resets the counter, thereby affecting the MPPT operation to come to an end before the specified period. The enable bit *En* of the comparator takes care of the timing of the complete MPPT operation (i.e., 16-MPPT cycles =3410 μS). As shown in Fig. 14, within 3410 μS, the voltage is getting build up in the V_{wire} by the payload. The comparator output is high (comparator output Y is used as select line SEL for multiplexer), indicating a Trojan is detected. The logic high in SEL ensures logic-0 at the reset input of the MPPT module as shown in Fig. 14. Reset continues to become low till the completion of the MPPT operation. The above discussion indicates that the A2 Trojan detection and mitigation are achieved, and this harvesting system is prone to A2 Trojan.

Intentional Aging with High Temperature:

The conventional RO and RO with reduced supply voltage are intentionally aged by subjecting to a higher temperature to observe the impact on ripples. It is found that the RO with reduced supply voltage causes fewer ripples as compared to CMOS RO as achieved in Fig. 15 and is due to the aging tolerant feature of RO with reduced supply voltage.

7.2.3 Performance Improvement of Aging Sensor. After observing the performance improvement in RO with reduced supply voltage, the RO_{REF} is replaced by it and the frequency difference i.e. F_{DIF}= F_{REF}-F_{STR} is further improved. The improvement in the performance of aging sensor using RO with reduced supply voltage is presented in Table 2. It is found that the modified aging sensor module can detect a recycled EHS-IC if the sensor module experience continuous aging for one year.

From the above results obtained by analyzing the performances of different ROs, it is observed that replacing the conventional CMOS RO with aging tolerant RO with reduced supply voltage causes fewer ripples. The aging tolerant

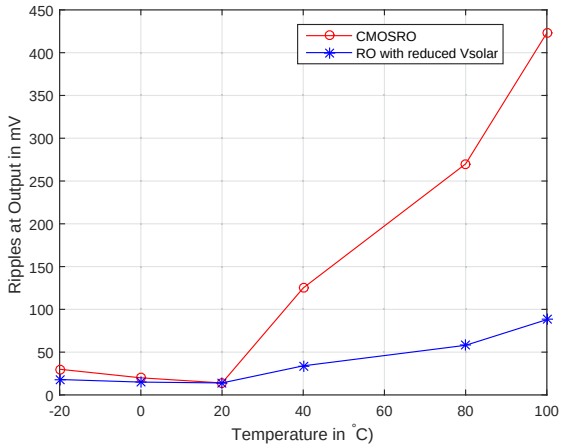

Fig. 15. Ripples at Output with Different Temperatures

Table 2. Frequency Degradation of f_{ossc} over Time (improved performance over [40]).

Years (Y)	F_{REF} in kHz	F_{STR} in kHz	F_{DIF} in kHz
T=0	150	150	0
T=1	148.5	136.6	11.9
T=2	147.9	127.4	20.5
T=3	147.1	121	26.1
T=4	146.8	116.5	30.3
T=5	146	113	33

RO also shows performance improvement in terms of temperature rise with aging. Hence we used the aging tolerant RO with reduced supply voltage in our design, which causes fewer ripples at the output of the RSSEHS.

7.3 Reliable Secure EHS Simulation with MPPT

The simulation results for clock, higher bias voltage for self-sustainable operation of the RSSEHS is presented in Fig. 16.

- The simulation results in Fig. 16 shows the clock signal (*RSC_CLK*) generated by the RO with reduced supply voltage (f = 150 KHz). V_{PB} is the higher bias voltage (V_{PB}=3V) generated is used as a body bias for the MOSFETs in the converter. $V_{cp-trip}$ is the output of the converter after getting required adiabatic charging clock and bias signal.

The simulation result in Fig. 17 depicts the sequence of control signals generated by the controller during MPPT operation. A complete MPPT cycle constitute of 32-clocks. As per the change in V_{solar} due to the environmental conditions the MPPT circuit gets triggered. An environmental sensor (S) triggers MPPT operation.

- Once the sensor S triggers MPPT the set of control signals issued by the controller are S_1, S_2, S_{sen}, S_3, S_4, S_5 as shown in Fig. 17, along with the thermometer codes.
- In this simulation S remains low for 150μS normal mode of operaton of RSSEHS without MPPT. When S become high after 150μS, MPPT is triggered.

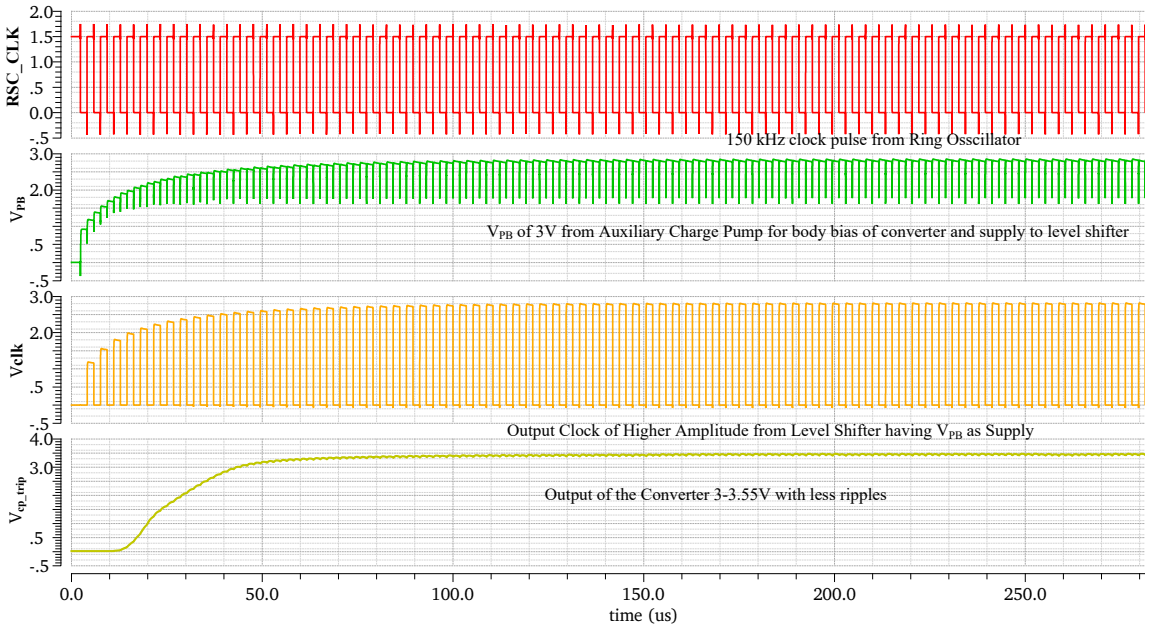

Fig. 16. Clocks and Bias Generation using RO, NOCG, ACP, and LS

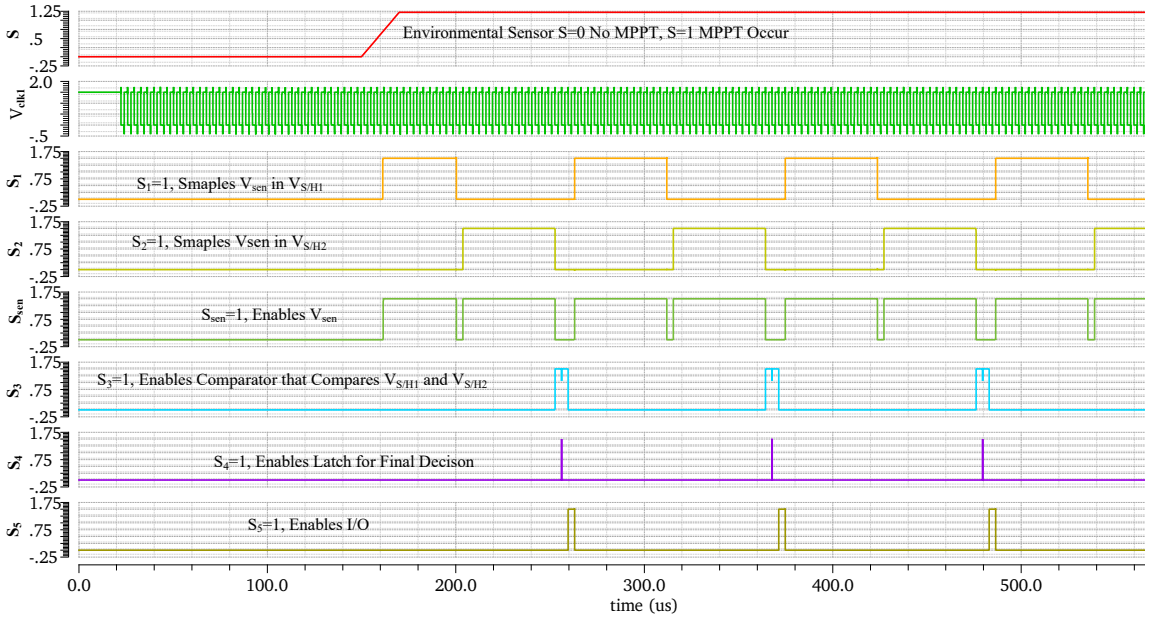

Fig. 17. Control Signals Related to FSM for MPPT

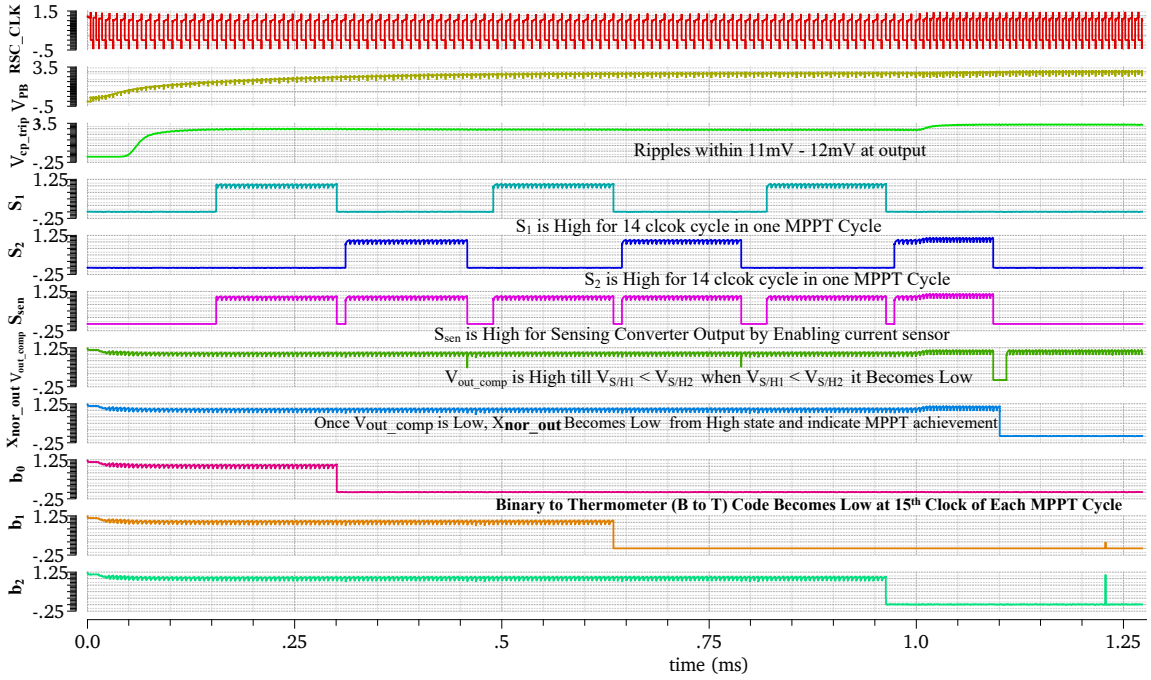

Fig. 18. Simulation Result of EHS including Control Signals with MPPT Achievement

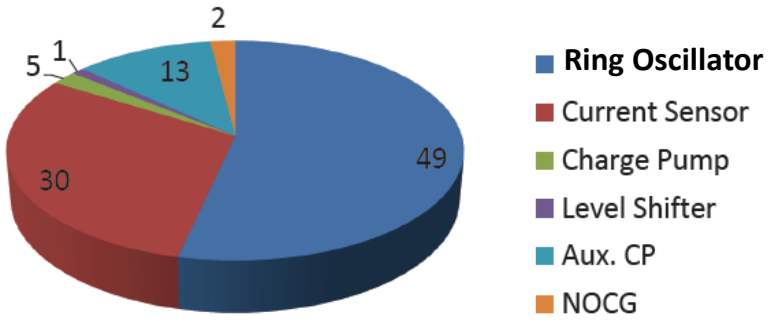

Fig. 19. Power Consumption (in %) by Each Module in the EHS.

- Once MPPT module get initialized the control signals become active for required clock cycles by the controller. S_1, S_2 become active to sense P_n and P_{n+1} as shown in Fig. 17. S_{sen} changes its state for CVM in specific period.
- S_3, S_4 active at appropriate timing towards end of a MPPT cycle for comparing and decision making about MPPT achievement as depicted in Fig. 17. S_5 initiates I/O operation (if any at the end of 31^{st} cycle).

Fig. 18 shows the simulation result about the number of MPPT cycles needed to reach MPP. Once the MPP is achieved, the needed change in the control signals is also shown. The thermometer codes b_0 to b_{15} becomes low one after another in each MPPT cycle for modulating the capacitor values in the capacitor banks, connected to the converter. At the end

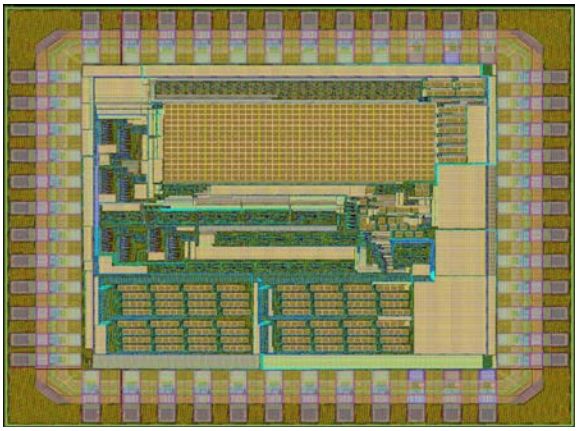

Fig. 20. DIE Photo of Proposed EHS.

of each MPPT cycle, the comparator compares the power information and changes its output V_{out_comp} to low if P_n is higher than P_{n+1}, else remain high. It is passed to the final decision circuit consists of the XNOR gate and Latch. The XNOR output (X_{nor_out}), which is initially high switched to low, indicates MPPT achievement as shown in Fig. 18.

Table 3. Comparison of different low energy solar harvesting systems.

Works	**Feature/ Characteristics**								
	Technology	Fully Integrated	Self-Sustaining	Input Range (V)	Output Range (V)	Power Throughput (μW)	Aging Sensor (For Counterfeiting IC)	Security Features Incorporated	Reliable (Aging Tolerant+ Trojan Detection mechanism)
Shao, et al. [44]	350nm	Yes	No	2.1-3.5	3.6-4.4	100-775	No	No	No
Kim, et al. [19]	350nm	Yes	No	1-2.7	2	0-80	No	No	No
Qian, et al. [34]	250nm	No	Yes	0.5-2	0-5	5-1000	No	No	No
Shih, et al. [45]	130nm	Yes	Yes	1.8	1.4	< 10	No	No	No
Kim, et al. [18]	350nm	No	Yes	1.5-5	0-4	800	No	No	No
Liu, et al. [23]	180nm	Yes	Yes	1-1.5	3-3.5	0-29	No	No	No
Ram, et al. [40] (Eternal Thing)	90nm	Yes	Yes	1-1.5	3-3.55	0-22	Yes	Yes	No
Current Paper (Eternal Thing 2.0)	90nm	Yes	Yes	1-1.5	3-3.55	0-22	**Yes**	Yes	**Yes**

The sequence of operation in Fig. 18 shows that once the MPP is achieved it is locked, thereby resetting the control signal to regain the normal mode of RSSEHS. In this simulation, after three MPPT cycle, the MPP is achieved. There is a rise noted in the converter output after MPP achievement. The same sequence of operation gets repeated as per the triggering of the environmental sensor S. The use of RO with reduced supply voltage in conventional CMOS RO makes the secure EHS more reliable. Due to less frequency degradation of the RO with reduced supply voltage, the converter experience less ripple and is safe for the devices connected to it. The Tracking time to achieve MPP is also less affected due to the lower frequency degradation. The EHS operation with MPPT is a safeguard by using the A2 Trojan detection and mitigation mechanism to avoid premature reset. The reliability of the EHS is enhanced after using RO with reduced supply voltage and suitable techniques to counter attacks by the adversary.

7.4 Power Consumption

Fig. 19 represents the power consumed by each module in the EHS. The RO with reduced supply voltage and the current sensor is the primary power-consuming module, which consumes 80% of total power. The continuous oscillating mode

of RO is responsible for its higher power consumption. The current sensor is periodically ON during the MPPT process only to reduce the power consumption. The die photograph of proposed EHS is shown in 20.

The power consumed by the RSSEHS is under the ultra-low-power range (which is < 1mW), which justifies that the harvesting system is designed for ultra-low-power IoT requirements. This RSSEHS is compared with Eternal-thing 1.0 in Table 3. The power throughput of the proposed RSSEHS is 0-22μW.

8 CONCLUSION AND FUTURE WORK

The failure due to the supply of a sensor node could be a ruinous state of affairs. The denial of service sort attack might cause information loss in IoT. The reliable secure solar energy harvesting system (RSSEHS) is a state of art technology outcome towards clean energy and handling of IoT end-node devices. The RSSEHS designed is similar temperament for a minimum voltage of 1.22 V as MPP within the vary of 1-1.5V. The ensuing output is 3-3.55 V, that is the demand of the many IoT edge node devices. The efficiency of the DC-DC converter is in the range of 90%- 97%. The entire module is powered by the solar cell and the higher bias voltages needed are generated on-chip. The aging tolerant RO makes the long-run IoT node prone to attacks due to intentional aging by subjecting it to a higher temperature by an adversary. It is also causing fewer ripples at the output due to less degradation in oscillation frequency. The A2 Trojan detection and mitigation mechanism in the MPPT module make the harvesting system prone to analog Trojans (A2). The entire reliable, secure solar EHS with the anti-aging concept is self-sustainable, and no external power supplies are needed. The aging tolerant reliable energy harvesting system proposed is consuming power in the ultra-low-power realm range with a power throughput of 0-22μW. The aging analysis of other modules of the EHS can be studied further in future.

ACKNOWLEDGMENTS

This research work is supported by Special Manpower Development Program for Chips to System Design (SMDP-C2SD) of Government of India.

REFERENCES

[1] Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. 2007. Trojan detection using IC fingerprinting. In *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 296–310.

[2] G Aishwarya, Hitha Revalla, S Shruthi, VS Ananth, and N Mohankumar. 2018. Virtual instrumentation-based malicious circuit detection using weighted average voting. In *Microelectronics, Electromagnetics and Telecommunications*. Springer, 423–431.

[3] Georg T Becker, Francesco Regazzoni, Christof Paar, and Wayne P Burleson. 2014. Stealthy dopant-level hardware trojans: extended version. *Journal of Cryptographic Engineering* 4, 1 (2014), 19–31.

[4] Naveed Anwar Bhatti, Muhammad Hamad Alizai, Affan A Syed, and Luca Mottola. 2016. Energy harvesting and wireless transfer in sensor network applications: Concepts and experiences. *ACM Transactions on Sensor Networks (TOSN)* 12, 3 (2016), 24.

[5] Lauren Biernacki, Mark Gallagher, Zhixing Xu, Misiker Tadesse Aga, Austin Harris, Shijia Wei, Mohit Tiwari, Baris Kasikci, Sharad Malik, and Todd Austin. 2021. Software-driven Security Attacks: From Vulnerability Sources to Durable Hardware Defenses. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 17, 3 (2021), 1–38.

[6] Salvador Carreon-Bautista, Ahmed Eladawy, Ahmed Nader Mohieldin, and Edgar Sánchez-Sinencio. 2014. Boost converter with dynamic input impedance matching for energy harvesting with multi-array thermoelectric generators. *IEEE Transactions on Industrial Electronics* 61, 10 (2014), 5345–5353.

[7] Xiaotong Cui, Elnaz Koopahi, Kaijie Wu, and Ramesh Karri. 2018. Hardware Trojan detection using the order of path delay. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 14, 3 (2018), 1–23.

[8] Banee Bandana Das, Pradeep Kumar, Debakanta Kar, Saswat Kumar Ram, Korra Sathya Babu, and Ramesh Kumar Mohapatra. 2019. A spatio-temporal model for EEG-based person identification. *Multimedia Tools and Applications* (2019), 1–21.

[9] Ding Deng, Yaohua Wang, and Yang Guo. 2020. Novel design strategy toward A2 Trojan detection based on built-in acceleration structure. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 39, 12 (2020), 4496–4509.

[10] Ujjwal Guin, Domenic Forte, and Mark Tehranipoor. 2015. Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 24, 4 (2015), 1233–1246.

[11] Xiaolong Guo, Huifeng Zhu, Yier Jin, and Xuan Zhang. 2019. When Capacitors Attack: Formal Method Driven Design and Detection of Charge-Domain Trojans. In *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 1727–1732.

[12] Kaveri Hatti and C Paramasivam. 2022. Design and Implementation of Enhanced PUF Architecture onFPGA. *International Journal of Electronics Letters* 10, 1 (2022), 57–70.

[13] Yumin Hou, Hu He, Kaveh Shamsi, Yier Jin, Dong Wu, and Huaqiang Wu. 2018. On-chip analog trojan detection framework for microprocessor trustworthiness. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 38, 10 (2018), 1820–1830.

[14] Yumin Hou, Hu He, Kaveh Shamsi, Yier Jin, Dong Wu, and Huaqiang Wu. 2018. R2d2: Runtime reassurance and detection of a2 trojan. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE, 195–200.

[15] Boy-Yiing Jaw and Hongchin Lin. 2012. An analysis of output ripples for PMOS charge pumps and design methodology. In *2012 IEEE Asia Pacific Conference on Circuits and Systems*. IEEE, 424–427.

[16] Yier Jin and Yiorgos Makris. 2008. Hardware Trojan detection using path delay fingerprint. In *2008 IEEE International workshop on hardware-oriented security and trust*. IEEE, 51–57.

[17] Shane Kelly, Xuehui Zhang, Mohammed Tehranipoor, and Andrew Ferraiuolo. 2015. Detecting hardware trojans using on-chip sensors in an asic design. *Journal of electronic testing* 31, 1 (2015), 11–26.

[18] Hoonki Kim, Sangjin Kim, Chan-Keun Kwon, Young-Jae Min, Chulwoo Kim, and Soo-Won Kim. 2013. An energy-efficient fast maximum power point tracking circuit in an 800-μW photovoltaic energy harvester. *IEEE Transactions on Power Electronics* 28, 6 (2013), 2927–2935.

[19] Jungmoon Kim, Jihwan Kim, and Chulwoo Kim. 2011. A regulated charge pump with a low-power integrated optimum power point tracking algorithm for indoor solar energy harvesting. *IEEE Transactions on Circuits and Systems II: Express Briefs* 58, 12 (2011), 802–806.

[20] Prabhakar Krishnan, Kurunandan Jain, Rajkumar Buyya, Pandi Vijayakumar, Anand Nayyar, Muhammad Bilal, and Houbing Song. 2021. MUD-based behavioral profiling security framework for software-defined IoT networks. *IEEE Internet of Things Journal* 9, 9 (2021), 6611–6622.

[21] Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, and Ilia Polian. 2014. Parametric trojans for fault-injection attacks on cryptographic hardware. In *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*. IEEE, 18–28.

[22] Jie Li and John Lach. 2008. At-speed delay characterization for IC authentication and Trojan horse detection. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*. IEEE, 8–14.

[23] Xiaosen Liu and Edgar Sánchez-Sinencio. 2015. A highly efficient ultralow photovoltaic power harvesting system with MPPT for internet of things smart nodes. *IEEE Transactions on Very Large Scale Integration (VLSI) systems* 23, 12 (2015), 3065–3075.

[24] Nico Mexis, Nikolaos Athanasios Anagnostopoulos, Shuai Chen, Jan Bambach, Tolga Arul, and Stefan Katzenbeisser. 2021. A Lightweight Architecture for Hardware-Based Security in the Emerging Era of Systems of Systems. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 17, 3 (2021), 1–25.

[25] Harin M Mohan, Santanu Kumar Dash, Saswat Kumar Ram, and Wahyu Caesarendra. 2022. Performance assessment of three-phase PV tied NPC multilevel inverter based UPQC. In *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*. IEEE, 1–5.

[26] N Mohankumar, M Jayakumar, and M Nirmala Devi. 2022. Lightweight Logic Obfuscation in Combinational Circuits for Improved Security—An Analysis. In *Expert Clouds and Applications*. Springer, 215–225.

[27] Saroj Mondal and Roy Paily. 2017. On-chip photovoltaic power harvesting system with low-overhead adaptive MPPT for IoT nodes. *IEEE Internet of Things Journal* 4, 5 (2017), 1624–1633.

[28] Clemens Moser, Jian-Jia Chen, and Lothar Thiele. 2008. An energy management framework for energy harvesting embedded systems. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 6, 2 (2008), 1–21.

[29] Seetharam Narasimhan, Xinmu Wang, Dongdong Du, Rajat Subhra Chakraborty, and Swarup Bhunia. 2011. TeSR: A robust temporal self-referencing approach for hardware Trojan detection. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, 71–74.

[30] K Nimmy, Sriram Sankaran, and Krishnashree Achuthan. 2021. A novel lightweight PUF based authentication protocol for IoT without explicit CRPs in verifier database. *Journal of Ambient Intelligence and Humanized Computing* (2021), 1–16.

[31] Taeho Oh, Dilruba Parvin, Omiya Hassan, Samira Shamsir, and Syed Kamrul Islam. 2020. MPPT integrated DC–DC boost converter for RF energy harvester. *IET Circuits, Devices & Systems* 14, 7 (2020), 1086–1091.

[32] Amzar Omairi, Zool H Ismail, Kumeresan A Danapalasingam, and Mohd Ibrahim. 2017. Power harvesting in wireless sensor networks and its adaptation with maximum power point tracking: Current technology and future directions. *IEEE Internet of Things Journal* 4, 6 (2017), 2104–2115.

[33] Miodrag Potkonjak, Ani Nahapetian, Michael Nelson, and Tammara Massey. 2009. Hardware Trojan horse detection using gate-level characterization. In *2009 46th ACM/IEEE Design Automation Conference*. IEEE, 688–693.

[34] Yao Qian, Hongguang Zhang, Yanqin Chen, Yajie Qin, Danzhu Lu, and Zhiliang Hong. 2017. A SIDIDO DC–DC converter with dual-mode and programmable-capacitor-array MPPT control for thermoelectric energy harvesting. *IEEE Transactions on Circuits and Systems II: Express Briefs* 64, 8 (2017), 952–956.

[35] Saswat Kumar Ram, Shubham Chourasia, Banee Bandana Das, Ayas Kanta Swain, Kamalakanta Mahapatra, and Saraju Mohanty. 2020. A solar based power module for battery-less IoT sensors towards sustainable smart cities. In *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE, 458–463.

[36] Saswat Kumar Ram and Banee Bandana Das. 2013. Comparison of different control strategy of conventional and digital controller for active power line conditioner (APLC) for harmonic compensation. In *2013 12th International Conference on Environment and Electrical Engineering*. IEEE, 209–214.

[37] Saswat Kumar Ram and Banee Bandana Das. 2016. Digital controller design for three phase active power filter for harmonic and reactive power compensation using FPGA and system generator. In *2016 International Conference on Inventive Computation Technologies (ICICT)*, Vol. 3. IEEE, 1–6.

[38] Saswat K. Ram, Banee B. Das, Kamalakanta Mahapatra, Saraju P. Mohanty, and Uma Choppali. 2021. Energy Perspectives in IoT Driven Smart Villages and Smart Cities. *IEEE Consumer Electronics Magazine* 10, 3 (2021), 19–28. https://doi.org/10.1109/MCE.2020.3023293

[39] Saswat Kumar Ram, Banee Bandana Das, Ayas Kanta Swain, and Kamala Kanta Mahapatra. 2019. Ultra-Low Power Solar Energy Harvester for IoT Edge Node Devices. In *2019 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*. IEEE, 205–208.

[40] Saswat Kumar Ram, Sauvagya Ranjan Sahoo, Banee Bandana Das, Kamalakanta Mahapatra, and Saraju P. Mohanty. 2021. Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT. *IEEE Transactions on Sustainable Computing* 6, 2 (2021), 320–333. https://doi.org/10.1109/TSUSC.2020.2987616

[41] Saswat Kumar Ram, Sauvagya Ranjan Sahoo, K Sudeendra, and Kamalakanta Mahapatra. 2018. Energy efficient ultra low power solar harvesting system design with MPPT for IOT edge node devices. In *2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*. IEEE, 130–133.

[42] Aldo Romani, Matteo Filippi, Michele Dini, and Marco Tartagni. 2015. A sub-μ A stand-by current synchronous electric charge extractor for piezoelectric energy harvesting. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 12, 1 (2015), 1–17.

[43] Sauvagya Ranjan Sahoo, Sudeendra Kumar, and Kamalakanta Mahapatra. 2018. A novel configurable ring oscillator PUF with improved reliability using reduced supply voltage. *Microprocessors and Microsystems* 60 (2018), 40–52.

[44] Hui Shao, Chi-Ying Tsui, and Wing-Hung Ki. 2009. The design of a micro power management system for applications using photovoltaic cells with the maximum output power control. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 17, 8 (2009), 1138–1142.

[45] Yi-Chun Shih and Brian P Otis. 2011. An Inductorless DC–DC Converter for Energy Harvesting With a 1.2μW Bandgap-Referenced Output Controller. *IEEE Transactions on Circuits and Systems II: Express Briefs* 58, 12 (2011), 832–836.

[46] Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino. 2015. Reversing stealthy dopant-level circuits. *Journal of Cryptographic Engineering* 5, 2 (2015), 85–94.

[47] Prabha Sundaravadivel, Elias Kougianos, Saraju P Mohanty, and Madhavi K Ganapathiraju. 2017. Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health. *IEEE Consumer Electronics Magazine* 7, 1 (2017), 18–28.

[48] Adam Waksman and Simha Sethumadhavan. 2011. Silencing hardware backdoors. In *2011 IEEE Symposium on Security and Privacy*. IEEE, 49–63.

[49] Wensi S Wang, Terence O'Donnell, Ningning Wang, Michael Hayes, Brendan O'Flynn, and C O'Mathuna. 2008. Design considerations of sub-mW indoor light energy harvesting for wireless sensor systems. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 6, 2 (2008), 1–26.

[50] Justin Wenck, Jamie Collier, Jeff Siebert, and Rajeevan Amirtharajah. 2008. Scaling self-timed systems powered by mechanical vibration energy harvesting. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 6, 2 (2008), 1–24.

[51] Justin Wenck, Jamie Collier, Jeff Siebert, and Rajeevan Amirtharajah. 2010. Scaling self-timed systems powered by mechanical vibration energy harvesting. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 6, 2 (2010), 5.

[52] Kaiyuan Yang, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester. 2016. A2: Analog malicious hardware. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 18–37.

[53] Xuehui Zhang and Mohammad Tehranipoor. 2013. Design of on-chip lightweight sensors for effective detection of recycled ICs. *IEEE transactions on very large scale integration (VLSI) systems* 22, 5 (2013), 1016–1029.