Detecting Continuous Jamming Attack using Ultra-low Power RSSI Circuit

Ankit Mittal
Dept. of Electrical and Computer Engg.
Northeastern University
Boston, USA
mittal.ank@northeastern.edu

Aatmesh Shrivastava
Dept. of Electrical and Computer Engg.
Northeastern University
Boston, USA
aatmesh@ece.neu.edu

2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) | 978-1-6654-8532-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/HOST54066.2022.9840209

***Abstract*—This paper presents an ultra-low power received signal strength indicator (RSSI) circuit to detect constant jamming attacks in the internet-of-things (IoT) network. The proposed RSSI circuit uses a passive rectifier to convert incoming radio frequency (RF) signal to a DC level. A set of cascaded ultra-low power differential amplifier stages then generate the RSSI level. The circuit is implemented in a commercial 65-nm CMOS process and consumes 25nW. It has a detection sensitivity of −70dBm and a dynamic range of 48dB with a ±1dB accuracy. Simulation results of the RSSI circuit shows its robustness to noise, process, and, temperature variations.**

***Index Terms*—Jamming attacks, Received signal strength indicator (RSSI), internet of things (IoT), hardware security.**

I. Introduction

A sizeable portion of billions of connected internet-of-things (IoT) devices operate in a resource constrained environment where available energy and the computation power are limited. They either operate from harvested energy or have several years of operational lifetime while using a small battery. Consequently, not only do these devices have limited security capability when compared to a more conventional computing system, they are also prone to attacks where available resources can be further stifled to effect new kind of denial-of-service (DoS) and energy depletion attacks [1], [2].

In this category, jamming attacks are of particular interest. Conventionally, jamming attacks were used to deny the network access to radio frequency (RF) media for communication. However, recently they are also being used to launch energy depletion attack. By jamming the network, an adversary can make an IoT device transmit repeatedly losing their stored energy. Low-power IoT devices duty-cycle their communication, and sensing and spend a large portion of their time sleeping to conserve or harvest energy. Jamming attacks target this feature to deprive the intended sleep mode by initiating frequent wake up and repeated communication requests to quickly drain the limited available energy rendering them unusable within hours or days [3]. Energy detection based mechanism using received signal strength indicator (RSSI) circuit has been used to indicate jamming attacks [4], [5]. However, these RSSI-based anti-jamming techniques can consume several milliwatts (mWs) of power making them infeasible for energy limited ultra-low power IoT systems. There is a need to develop ultra-low power security primitives which can continuously detect security attacks, particularly for low power IoT devices.

This work is supported in part by National Science Foundation under grant ECCS 2125222

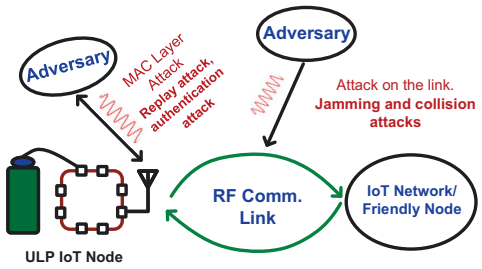


Fig. 1. Threat model of security attacks in an IoT network.

In this paper, we present an ultra-low power RSSI circuit for continuous detection of jamming attacks. The proposed RSSI circuit has a detection sensitivity of −70dBm, a dynamic range of 48dB, and power consumption of 25nW with an accuracy of ±1dB. The paper is organized as follows. Section II discusses jamming attacks and existing energy-detection based countermeasures. Section III provides the details of the ultra low power RSSI architecture. Section IV provides details of the circuit design. In Section V, we present the simulation results of the RSSI circuit. In Section VI we briefly discuss the future work for detecting intelligent jamming attacks. Finally, conclusions are presented in Section VII.

II. Jamming Attacks

Fig. 1 shows the threat model of security attacks in an IoT network which includes replay attacks, broadcast attacks, and jamming attacks. An adversary effect jamming attacks by intentionally disrupting the legitimate communication through the introduction of interference in the physical channel. Fig. 1 includes the threat model of jamming attack where an adversary jams the network by continuously transmitting data/signal often at much higher power levels to interfere with the communication traffic [4].

1) Attack modalities: Fundamentally, jamming attacks are categorized as basic jamming attacks and advanced jamming attacks. Depending on the jamming strategy like length of

Authorized licensed use limited to: Northeastern University. Downloaded on July 21,2023 at 17:53:26 UTC from IEEE Xplore. Restrictions apply.

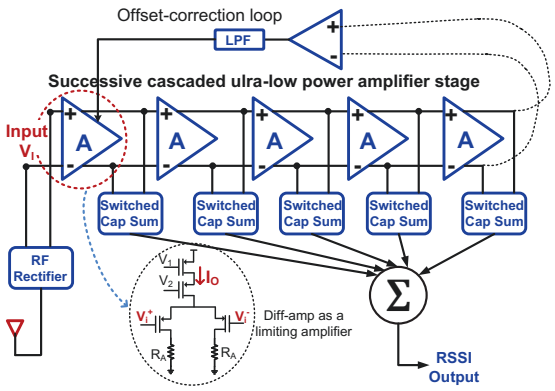


Fig. 2. Ultra-low power RSSI circuit architecture with rectifier stage and offset correction loop.

the jamming window, energy considerations, and functionality, jamming attacks can be further classified into various sub-types [6]. In a constant jamming attack (proactive jamming attack), the adversary emits a continuous jamming signal at power high enough to degrade the signal-to-noise ratio at the legitimate receiver. Higher power jamming attacks can be detected by observing the received signal strength indicator (RSSI) [4], [5] which indicates the power level of the received radio frequency (RF) signal. The host node, after observing an elevated power in the current channel can hop to another channel for communication.

Attackers can also employ an intelligent constant jamming in which they induce power level enough to corrupt the input data but that does not show an appreciable increase in received power. This attack however can be detected using RSSI data in combination with the decline in the packet delivery ratio (PDR) [7]. Existing energy-detection based countermeasures rely on RSSI value provided by the radio receiver. Consequently, RSSI value is only available when the receiver is turned on, yet receivers cannot be always on due to higher power consumption. We present an always-on RSSI circuit that will operate at ultra-low power levels and can enable the IoT node to continuously scan for jamming attacks even when duty cycling the main receiver.

III. Design Architecture

RSSI circuits are routinely used to find the power level of incoming RF signals for controlling the automatic gain control (AGC) loop in a receiver front end. Our ultra-low power RSSI circuit uses passive rectifier-based approach to detect energy of the received signal and correlate it with the expected energy pattern.

Fig. 2 shows the circuit architecture of an RSSI circuit that we implemented using robust, subthreshold analog design technique. A conventional RSSI circuit uses a low noise amplifier followed by successive amplifier stages operating at the carrier frequency (2.4GHz for Bluetooth and ZigBee) which incurs higher power cost in 10s to 100s of mW for the RSSI circuit alone [8]–[10]. We propose an intermediate RF to DC conversion using a rectifier to reduce the bandwidth requirement for amplifying stages. We use a passive rectifier stage which converts the RF to DC voltage which is then amplified to obtain the RSSI level. The RSSI circuit maps a logarithmic input power into a linear function of voltage.

A high power continuous jamming will be detected by this RSSI circuit as it will see an elevated voltage level in the event of an attack. In the absence of a constant jamming attack, the RF communication between the IoT node will occur in a defined pattern. RF to DC conversion reduces the bandwidth requirement for the RSSI circuit which can now be developed at ultra-low power level. An important advantage of the proposed RSSI circuit is that it can continue to observe the channel at ultra-low power level without turning on the radio. This way the IoT node can find out when the channel is available to send the message. On the other hand, an attacker would need to continuously jam the channel which would require higher power and more resources to launch an effective attack making the jamming attack expensive.

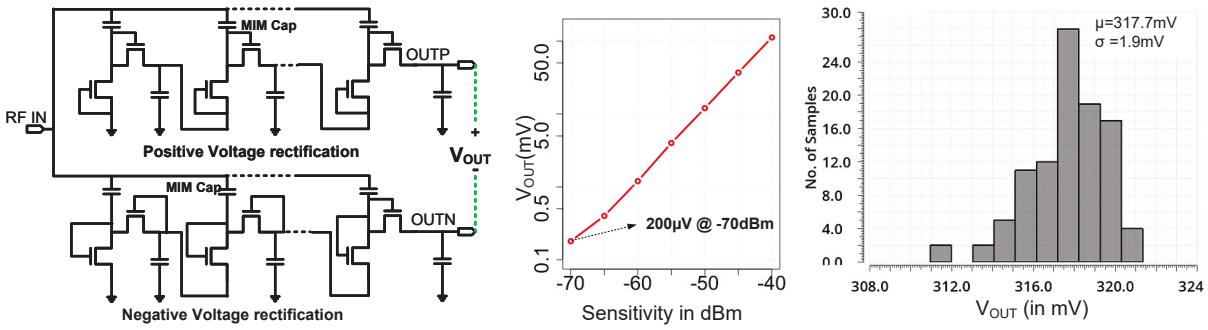
IV. Circuit Implementation

A. RF-to-DC Rectifier

Fig. 3-(a) shows the circuit architecture of the rectifier used for RF-to-DC conversion. The purpose of the rectifier is two-fold. First, it converts the signal from RF to the DC level and second it provides a gain to the received signal. It has a positive voltage and a negative voltage rectification circuit. For the positive rectification circuit, only the positive portion of the received AC signal goes through the rectifier element, which charges the first stage output of the rectifier to the amplitude level of the received signal. For the next stage, the received RF signal will swing on top of the first stage's DC output level which charges the next stage output to twice the amplitude of the received signal. Similarly, each succeeding stage will amplify the received RF signal's amplitude to a higher DC value. Finally, a positive and a negative voltage will be seen on an OUTP and OUTN node. The transistors in Fig. 3(a) are low-threshold voltage (L_{VT}) transistors (in 65-nm CMOS) acting as diodes and capacitors are implemented using metal-insulator-metal (MIM) capacitors as they have low parasitic.

Fig. 3 shows the simulation of the rectifier with an incoming RF signal at different sensitivity levels. The rectifier shows minimum sensitivity of -70dBm, where its output voltage is 0.2mV. The rectifier operates in an open-circuit configuration as it sees small transistor gate as load. Our analysis of open circuit rectifier shows that the output voltage (V_{OC}) is linear with input power in the first order and is given by $V_{OC} = n(V_R - \eta_s V_t/(1+\eta_s))$ (eq. 1) where V_R is the amplitude of RF signal at the input of the rectifier, and η_s is the sub-threshold nonideality factor and V_t is the thermal voltage. The equation shows no dependence on threshold voltage or other process parameter other than η_s. This process independence of the rectifier output is substantiated by the Monte-Carlo simulation result shown in Fig. 3-(c) where 3σ process variation is less than 2%.

Authorized licensed use limited to: Northeastern University. Downloaded on July 21,2023 at 17:53:26 UTC from IEEE Xplore. Restrictions apply.



(a) Rectifier topology with pos and neg output voltage (b) V_{OUT} with input power (c) Monte-Carlo simulation of V_{OUT}

Fig. 3. Rectifier circuit and it's output voltage with RF input power

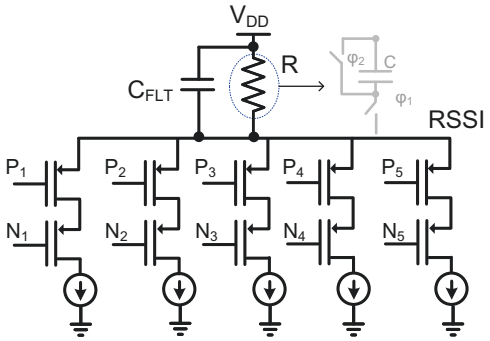


Fig. 4. Wide output voltage-range summing circuit design.

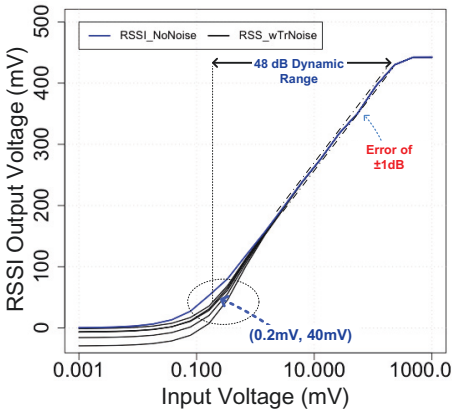


Fig. 5. Simulation results of the output voltage of the RSSI with different input voltage levels and transient circuit noise.

B. Differential Amplifier

We have used a 5-stage cascaded chain of differential amplifiers to implement the amplifying stage of RSSI. The differential amplifier uses a resistive load with each stage biased at 4nA bias current. Since our design targets 4nA bias current, using actual resistor is not feasible due to its size. Therefore, we use switched capacitor resistor which can implement a large resistor using small capacitor. Further, constant transconductance biasing technique was used to remove process and temperature variation [11]. However, to support higher dynamic range, more precisely sensitivity to lower input voltages and robustness against low-frequency noise, we have included a low frequency noise shaping and DC-offset correction loop as shown in Fig. 2.

C. Summing Circuit

We have also developed a wider output voltage-range summing circuit to support higher voltage range. Fig. 4 shows the topology of the summing circuit. Outputs from each differential amplifier stage, P_i and N_i are used to control current source. As each stage saturates, its corresponding current contribution is removed and the IR drop at RSSI is removed leading to an increase in RSSI voltage. Therefore as power increases, RSSI voltage increases. Total bias of the summing circuit is 5nA. To realize a large value of resistor used for biasing the summing circuit, switched capacitor resistor is used where $R = 1/fC$. We use $150fF$ capacitor switching at $32KHz$ to realize a $200M\Omega$ resistor.

TABLE I
POWER CONSUMPTION BREAKDOWN OF DIFFERENT DESIGN BLOCKS

Rectifier	Diff-Amp	Summing	Total
0nW (passive ckt)	5 × 4nW	5nW	25nW

Device mismatch related offset is corrected using RSSI's large gain to feedback to the input as shown in Fig. 2. Its bandwidth will be shaped to remove low frequency noise. It combines the switching diff-amp circuit with a continuous time offset correction loop. The combination is realized by setting the bandwidth of the offset correction loop to lower frequency using a low pass filter (LPF) which also helps in noise shaping and stability. The LPF is implemented using a large resistor which in turn will be realized using switched-cap resistors, like the summing circuit, to keep the area small.

V. SIMULATION RESULTS

Fig. 5 shows the input power variation from 1μV to 1V input voltage level, corresponding to the voltage output from the rectifier. Previously reported studies on RSSI for a constant jamming attack reported a constant signal power level of -70dBm [4], [5] which corresponds to 0.2mV output voltage from the rectifier. Since our design is at ULP level, we also simulated in presence of noise to ensure that we can detect an elevated power level in the presence of noise.

Authorized licensed use limited to: Northeastern University. Downloaded on July 21,2023 at 17:53:26 UTC from IEEE Xplore. Restrictions apply.

TABLE II
COMPARISON OF THE RSSI-BASED JAMMING ATTACK DETECTION

	MobiHoc'05 [4]	SECON'07 [5]	CICC'14 [12]	**This Work**
Tech.	$0.35\mu m$	$0.18\mu m$	$130nm$	$65nm$
Sens.(dBm)	-105	-77	-43.2	**-70***
DR(dB)	55	100	NA	48
Power	≈29mW	≈34mW	116nW	25nW
Freq.(GHz)	1	2.4	2.4	2.4
V_{DD} (V)	3	1.8	1.2/0.5	1
Method	RSSI-based	RSSI-based	Aut. Threshold	RSSI-based
Error (dB)	±2	±3	NA	±1

* Simulation based w/o off-chip matching

A. Noise Analysis

Our simulation result in Fig. 5 shows that we can reliably observe an elevated power level with minimum output voltage of 40mV in the presence of noise. Simulation results show a good margin for such power levels. The RSSI amplifier will require very little calibration for changes due to process or temperature variation because of highly robust subthreshold constant g_m based analog circuits [11]. Furthermore, the RSSI circuit is linear with frequency and input power level, and the power of multiple signals at different frequencies in a given frequency band are summed together as is done in digital implementations. Our simulation results show that the RSSI circuit has an error of less than ±1dB compared to an ideal logarithmic amplifier.

B. Process and Temperature Variation

The rectifier topology shown in Fig. 2 drives the RSSI amplifier and sees small capacitive load of input gates. The output voltage of the rectifier circuit in the unloaded condition is mostly independent of the process variation and only depends on the received input voltage level. Fig. 3-(c) shows the simulation result using foundry supplied device mismatch models where 3σ process mismatch results in less than 2% variation. Further, use of constant transconductance design keeps process, temperature variation of complete RSSI circuit below 2%.

Table II compares our design with some of the other reported works as a countermeasure to the constant jamming attack. In [4], [5], a standard radio chip is used to perform RSSI based detection of the constant jamming attack which consumes power in mWs in the receiver mode. In [12], an automatic threshold controller (ATC) is used to mitigate the constant jamming attack with maximum interferer level of −20dBm for a Wake-up receiver. Our design achieves a comparable sensitivity to the state of the art while consuming 25nW power. The linearity error of our design also remains low at ±1 dB.

VI. FUTURE WORK

In addition to improving the sensitivity and dynamic range of the proposed RSSI circuit, we also plan to develop the architecture to include an energy monitoring based detection and mitigation of intelligent jamming attacks. In the absence of an attack, the RSSI voltage level and its duration will constitute a set of features which can be extracted and learned on-chip. In the event of a jamming attack, the extracted features can help in classifying an intelligent jamming attack.

VII. CONCLUSIONS

In this paper we have presented an RSSI circuit to detecting constant jamming attacks in the IoT network. The ultra-low power RSSI circuit to detect jamming attacks is implemented in a commercial 65-nm CMOS process. It consumes a power of 25nW and has a detection sensitivity of −70dBm with a dynamic range of 48dB and ±1dB accuracy. We have presented simulation results to show that the proposed circuit is robust to noise, process and temperature variance. Finally, we also discussed briefly on detecting and mitigating intelligent jamming attacks as the future work.

REFERENCES

[1] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 367–380, Jan 2009.

[2] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Energy Depletion Attacks in Low Power Wireless Networks," *IEEE Access*, vol. 7, pp. 51 915–51 932, 2019.

[3] J. Uher, R. G. Mennecke, and B. S. Farroha, "Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov 2016, pp. 1231–1236.

[4] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," ser. MobiHoc '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 46–57. [Online]. Available: https://doi.org/10.1145/1062689.1062697

[5] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," in *2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, 2007, pp. 60–69.

[6] K. Grover, A. Lim, and Q. Yang, "Jamming and Anti-Jamming Techniques in Wireless Networks: A Survey," vol. 17, no. 4, p. 197–215, dec 2014. [Online]. Available: https://doi.org/10.1504/IJAHUC.2014.066419

[7] Wenyuan Xu, Ke Ma, W. Trappe, and Yanyong Zhang, "Jamming sensor networks: attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May 2006.

[8] C.-P. Wu and H.-W. Tsao, "A 110-MHz 84-dB CMOS programmable gain amplifier with integrated RSSI function," *IEEE Journal of Solid-State Circuits*, vol. 40, no. 6, pp. 1249–1258, 2005.

[9] J. Choi, J. Lee, Y. Xi, S.-S. Myoung, S. Baek, D. H. Kwon, Q.-D. Bui, J. Lee, D. Oh, and T. B. Cho, "Wide Dynamic-Range CMOS RMS Power Detector," *IEEE Transactions on Microwave Theory and Techniques*, vol. 64, no. 3, pp. 868–880, 2016.

[10] C. Li, C. C. Boon, X. Yi, Z. Liang, and K. Yang, "Compact Switched-Capacitor Power Detector With Frequency Compensation in 65-nm CMOS," *IEEE Access*, vol. 8, pp. 34 197–34 203, 2020.

[11] N. Mirchandani and A. Shrivastava, "High stability gain structure and filter realization with less than 50 ppm/° c temperature variation with ultra-low power consumption using switched-capacitor and sub-threshold biasing," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2018, pp. 1–5.

[12] S. Oh, N. E. Roberts, and D. D. Wentzloff, "A 116nW multi-band wake-up receiver with 31-bit correlator and interference rejection," in *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference*, 2013, pp. 1–4.

Authorized licensed use limited to: Northeastern University. Downloaded on July 21,2023 at 17:53:26 UTC from IEEE Xplore. Restrictions apply.