Energy Efficient, Secure and Spectrum Aware Ultra-Low Power Internet-of-Things System Infrastructure for Precision Agriculture

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

Ziyue Xu
Electrical and Computer Engg.
Northeastern University
Boston, USA
xu.ziy@northeastern.edu

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

***Abstract*—This paper presents a robust, energy efficient, and spectrum aware infrastructure to support the IoT system deployed for precision agriculture to reduce the power consumption to a level where they can be powered through harvested energy. We present system modeling-based approach to identify key optimizations which are then translated to a more feasible ultra-low power (ULP) IoT system realization. We present the measurement results of ULP infrastructure for the information receiver (Rx) comprising of ULP received signal strength detector (RSSI) and wake-up-radio (WuRx) which have been implemented in a 65-nm CMOS technology and have power consumption in few nano-watts. We present a *lightweight* energy-detection-based countermeasure against energy depletion attacks (EDA) in the IoT network. We also propose how the IoT sensor node can co-exist in the increasingly congested network of devices while also opportunistically gaining to strengthen its energy system to potentially achieve a self-powered and self-perpetual IoT system.**

***Index Terms*—Internet of things (IoT), received signal strength indicator (RSSI), wake-up radio, hardware security, spectrum sensing, jamming attacks, energy harvesting, beamforming, system modeling, precision agriculture.**

I. Introduction

In recent years, an unprecedented growth of Internet of Things (IoT) sensors deployed for precision agriculture and smart farming has revolutionized the agriculture sector [1]–[7]. In Fig. 1, we visualize one such IoT network deployed for sensing-monitoring application in an agricultural field. A majority of these IoT sensors have to operate in a resource constrained environment where the energy system to support key communication and computation capabilities is expected to either operate from harvested energy [8] or have several years of battery lifetime. An all-time connectivity which requires these sensors to remain connected in the network for the exchange of useful information, comes at the expense of power hungry radios. In addition to this, not only do these system have limited security capability when compared to a more conventional computing system, they are also prone to attacks where available resources can be further exhausted to effect new kinds of security attacks [3], [6], [9], [10]. Further, scaling of this IoT network to realize a comprehensive sensing-monitoring system leads to an increased congestion in the shared wireless medium and disrupts network services. The resulting unavailability of spectrum for communication, constraints the IoT node to stay in active mode further depleting its limited available energy. Therefore, to prolong the lifetime of the deployed IoT system and fulfill the *'deploy and forget'* mission, we propose an energy efficient, secure and spectrum aware infrastructure for the IoT system to address the existing shortcomings.

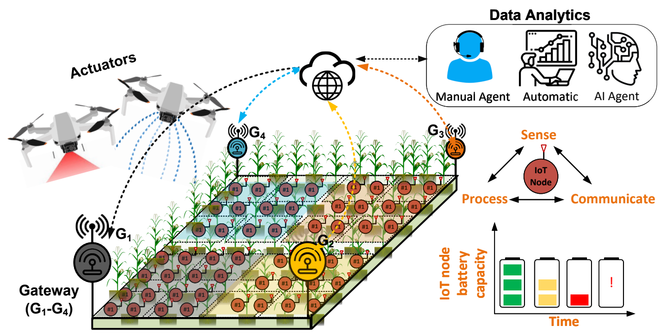

Fig. 1. IoT sensor system deployed for precision agriculture. IoT node drops-out of the network when its limited energy system is exhausted.

We summarize the main contribution as follows:

1) We present a generalized system graph of IoT system deployed for precision agriculture and identify critical system optimizations aimed to enhance energy efficiency, security and spectral awareness of the IoT system.
2) We translate these model-based key optimizations to a practical IoT sensor system and propose circuits to implement a robust IoT system driven by an enhanced energy system to potentially enable a self-powered IoT system infrastructure for precision agriculture.

The rest of paper is organized as follows. In Section II, we present a generalized system model of the ultra-low power (ULP) IoT system, identify key optimizations, and establish a feasible ULP IoT system framework. Section III discusses the design of ULP infrastructural blocks to improve the energy efficiency, security and spectrum awareness of the information receiver. Section IV presents an energy receiver for the ULP IoT system which can boost the IoT node's energy system. Finally, conclusions are presented in Section V.

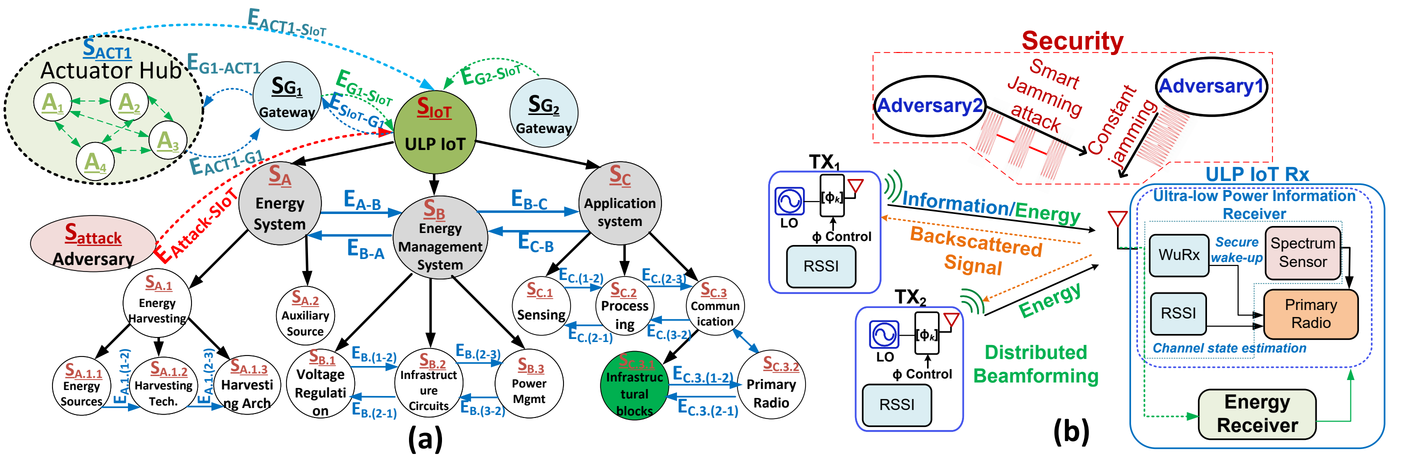

Fig. 2. (a) System graph model to identify key system components and interconnections for holistic optimization of the ULP IoT system, (b) Proposed framework for the ULP IoT system to enhance energy efficiency, security and co-existence in the network.

TABLE I
SYSTEM GRAPH MODEL AND PROPOSED OPTIMIZATIONS

Graph Nodes (V)	
System Component	**Proposed System/Model**
Energy System (S_A)	Efficient Rectifier ($S_{A.1}$)
Communication System ($S_{C.3}$)	RSSI and WuRx design optimization ($S_{C.3.1}$)
Actuator Hub (S_{ACT1})	-
Gateway Hub (S_{G1}, S_{G2})	-
Network Adversary (S_{attack})	Constant and Deceptive Jammer
Graph Edges (E)	
Gateway-IoT node link ($E_{G_{1,2}} - S_{IoT}$)	Distributed Beamforming (S_{G_1}, S_{G_2})
Attacker-IoT node link ($E_{attack} - S_{IoT}$)	Energy detection-based countermeasure

II. SYSTEM ARCHITECTURE

We have applied the generalized system's theory, which has considerably optimized physical [11], and socio-economic systems [12], [13], to model the ULP IoT system deployed for precision agriculture. We then translate the identified key optimizations to develop the infrastructure for the IoT system.

A. Generalized System Model

In Fig. 2(a), we present the generalized system model for the ULP IoT system. We have limited the system components in our model without compromising the generalized representation to illustrate the systems philosophy [11] applied to ULP IoT system optimizations.

The system model comprises of ULP IoT node (S_{IoT}) which interacts with the gateway devices (S_{G1}, S_{G2}). Relevant physical parameters (soil, water, air, crop quality) are routed, upon request ($E_{G_1-S_{IoT}}$), to (S_{G1}) through the communication system ($S_{C.3}$). (S_{G1}) performs analysis on the gathered data from the multiple IoT sensors. Actuator hub (S_{ACT1}) comprises of in-field stationed or unmanned aerial vehicles (UAV) actuators and performs an appropriate action (irrigation, pest spray etc.) based on the command received from (S_{G1}). This process of *sensing-communication-processing-actuation* is modeled by the graph edges ($E_{G_1-S_{IoT}} \rightarrow E_{C.3.(1-2)} \rightarrow E_{S_{IoT}-G_1} \rightarrow E_{G_1-ACT_1} \rightarrow E_{ACT_1-S_{IoT}}$).

(S_{IoT}) activates *sleep mode* for its power hungry subsystems particularly primary radio ($S_{C.3.2}$) which otherwise in an *always-on* mode would significantly overload the energy system (S_A) and decrease IoT node's lifetime. Wake-up Radio (WuRx), a subsystem of ($S_{C.3.1}$), wakes-up ($S_{C.3.2}$) upon gateway request. Once it communicates the sensed data, ($S_{C.3.2}$) re-enters into *sleep mode* to conserve it's limited available energy. Recent PHY/MAC layer attacks like energy depletion attack (EDA) target this energy-saving mechanism of (S_{IoT}) by sending commands over the network forcing frequent wake-ups and depriving them the energy savings of *sleep mode*. Presence of such adversary (S_{attack}) necessitates additional *lightweight* countermeasure which can provide defense against such attacks ($E_{Attack-S_{IoT}}$) while ensuring a minimal loading of (S_A). An extensive monitoring of agricultural field is accomplished through a network of multiple gateway devices which cater to their allocated IoT nodes. This consequential network scaling implies an increased level of radio frequency (RF) energy and congestion in the shared wireless channel. Apart from a disrupted quality of service, IoT node is forced to stay in the *awake state* continuously monitoring for the availability of channel further draining its limited available energy.

We propose to address this spectral congestion by a fast-spectrum sensing across a wide range of spectral band and opportunistically transmit in the first available spectral band. Further, we propose to opportunistically benefit by efficiently harvesting this increased RF energy from gateway hub (S_{G1}, S_{G2}) through ($E_{G_1-S_{IoT}}$, $E_{G_2-S_{IoT}}$) to enhance/replenish (S_A). Therefore, we observe that lifetime of the IoT node not only depends on the nature of its subsystems but a crucial factor in the design of robust and reliable energy system is the due considerations to its systemic interactions which can either adversely diminish or enhance it opportunistically.

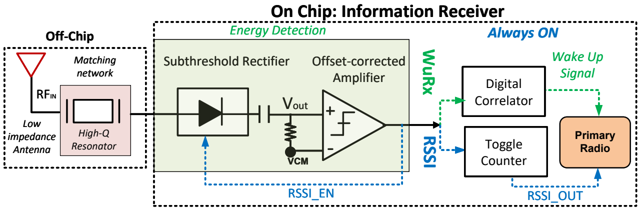

Fig. 3. Proposed information receiver comprises of energy efficient WuRx and RSSI circuit.

B. Proposed ULP IoT System Architecture

In Table I, we enumerate the key optimizations and corresponding circuit and system implementation. In Fig. 2(b), we present the proposed infrastructure for the ULP IoT system. The information receiver comprises of energy detection-based WuRx and received signal strength indicator (RSSI) circuit to perform signal detection and strength characterization. To impart security to the IoT node, we utilize the RSSI circuit to detect an unusual energy pattern in the system and mitigate the energy depletion attack. To co-exist in the congested network of devices, spectrum sensor locates the available channel for communication by fast scanning a wide spectral band. Together with information receiver, harvesting energy from multiple transmitters in the network enables the IoT radio to also function as an energy receiver. Through a closed loop beamforming technique, we efficiently harvest the available RF energy in the network.

III. Ultra-low power Information Receiver

A. Received Signal Strength Indicator

In [14], we present the circuit implementation of our RSSI circuit which is one of the first reported method to combine comparator, rectifier, and digital reset technique to detect the power level of the incoming signal directly into the digital domain. Fig. 3 shows the architecture of our RSSI circuit. The RSSI circuit is implemented in a 65-nm CMOS process with a 1V supply. Measurement results show that our RSSI circuit achieves a dynamic range of 26dB, accuracy of $\pm$0.5dB and consumes a power of 6nW. Our ULP RSSI circuit enables an accurate link assessment of the wireless channel which generally suffers from spatio-temporal fluctuations. In addition to this, it can be deployed to monitor the level of RF monitoring of harvested energy otherwise expensive due to a high power consumption of the conventional RSSI circuit. We also propose a *lightweight* hardware security system to detect and mitigate PHY layer attacks, implemented using our energy efficient RSSI circuit.

B. Wake-up Radio

System with WuRx can cut down the power consumption by turning-on the primary radio only upon communication request [15], significantly enabling lower power consumption than currently available radios leveraging the duty-cycling technique. In Fig. 3, we present energy detection based passive front-end-based WuRx with an ultra-low power consumption of 10nW. The proposed WuRx is based on co-design

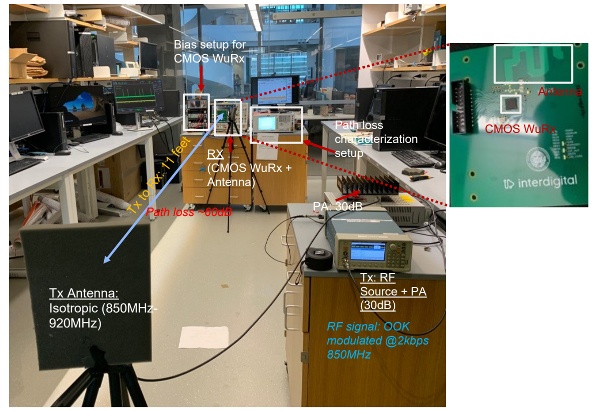

Fig. 4. Wireless setup for characterizing WuRx with RF passive front-end.

TABLE II
Measurement Results of WuRx with passive front-end

Technology	65nm CMOS
Sensitivity (dBm)	**-60**$^{\#}$ | **-45***
Frequency	850MHz
Supply Voltage(V)	1
Data Rate	10kbps
Power consumption	10nW
Silicon Area (mm^2)	0.04
Bandwidth (GHz)	0.75

$^{\#}$*Measured at* 850*MHz using off-chip matching network*, **Measured at* 900*MHz without off-chip matching network*

methodology with the RF front-end which comprises of low impedance antenna and MEMS resonator [16]. In Fig. 4, we show the measurement setup for over-the-air experiment with $\approx$ 12-feet distance between the transmitter and receiver. We have tabulated the measurement results in Table II.

C. Hardware Security

An adversary in the IoT network can launch jamming attack where IoT device is forced to transmit repeatedly. This leads to frequent wake-ups which drains its limited available energy. Energy detection-based mechanism which use RSSI circuit to indicate jamming attacks [17], [18] can consume several milliwatts (mWs) of power which overloads the energy limited ULP IoT system. We extend the application of ULP RSSI circuit discussed in Section III-A as a *lightweight* hardware security solution to mitigate effect of constant and deceptive jamming attacks on the information receiver.

1) Constant Jamming Attack: Fig. 5-(a) shows the measurement result for a constant jammer. Under a constant jamming attack, the rectifier circuit output settles to its corresponding DC voltage level which is *filtered* through AC-coupling (Fig. 3). Thus, the proposed RSSI circuit only responds to the primary RF signal and toggle count/*wake up signal* is unaffected even in the presence of constant jammer.

2) Deceptive Jamming attack: Deceptive jammer sends a continuous stream of data bits to deceive the ULP IoT into assuming a legitimate communication-request depriving the desired sleep mode with frequent wake-ups. Fig. 5-(b) shows the measurement results of the proposed ULP RSSI circuit under a deceptive jamming attack. In the presence of deceptive

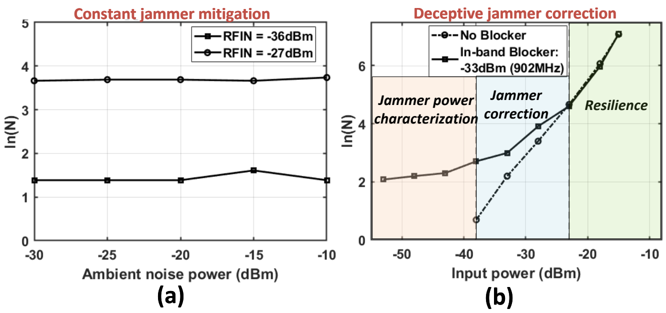

Fig. 5. Measurement results of our RSSI circuit to be deployed as a *lightweight* security system to mitigate (a) Constant jamming attacks, (b) Deceptive jamming attacks.

jammer, for low power of primary RF signal, the output toggles are entirely attributed to deceptive jammer *(jammer power characterization* in Fig. 5-(b)). This toggle count is set as threshold in the digital correlator to prevent frequent wake-up of the primary radio *(jammer correction* in Fig. 5-(b)). At higher power of the primary RF signal, the toggle count is unaffected because of the increased signal to interfere ratio (SIR) (*Resilience* in Fig. 5-(b)).

D. Spectrum Sensing

Spectrum sensing is needed for co-existence in the congested spectrum to sense a broad RF spectrum for the presence of RF signals from the primary user. Spectrum sensing techniques reported in the literature [19]–[25] include sampling of the RF signal using a high bandwidth ADC followed by a digital FFT block [24]. Energy detection-based techniques measure the power level of RF signal in the band of interest and compare it with expected noise power in the absence of RF signal [25]. An analog implementation is more suitable for high frequency application but accurate sensing of noise level is needed. In Fig. 6, we present the simulation results of a narrow-band, programmable, on-chip filter for spectrum sensing. The on-chip filter performs energy detection in a narrow band around the selected (programmed) frequency. We propose a fast convergence ($< 10\mu s$) spectrum sensing technique to sense ($0.4-6$GHz) frequency band for communication. A fast sensing enables IoT node to identify available channel and use it for communication with the gateway device reducing its waiting time which can enable a better co-existence in the shared spectrum and an extended battery lifetime.

IV. Energy Receiver

In Fig. 7, we present the energy receiver for the ULP IoT system which comprises of a high-efficiency passive RF rectifier and distributed beamforming technique to opportunistically harvest an increased level of RF energy from the congested network of IoT devices and gateways.

A. High Efficiency Rectifier

The proposed Self-biased gate (SBG) rectifier topology [26] mitigates the "dead zone" of Dickson multiplier in low input power by forming a high impedance path to bias the gate of the pumping transistor and also, prevents the reverse

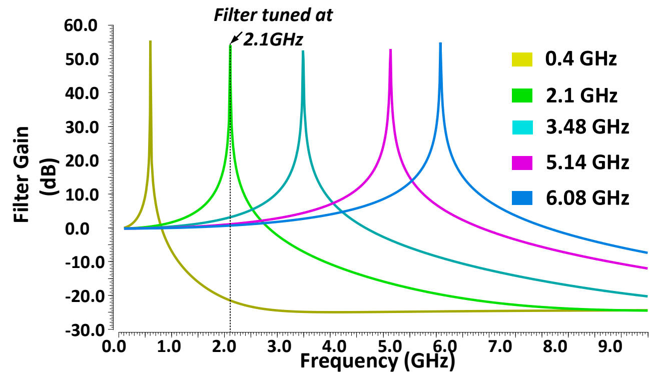

Fig. 6. Simulation results of the proposed narrow-band programmable on-chip spectrum sensor.

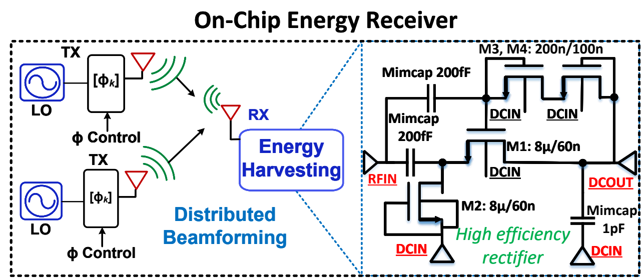

Fig. 7. The proposed energy receiver consists of a high-efficiency rectifier and distributed beamforming technique to boost the IoT node's energy system.

leakage in high input power condition. Hence, it realizes the high efficiency operation over a wide input power range. The measured peak efficiency is 31% at 1dBm input power with $100k\Omega$ load.

B. Distributed Beamforming

Distributed RF beamforming is a promising technique to transfer energy to a remotely located receiver [27]–[33] however, its efficacy depends on how well the transmission phases are aligned at the receiver. Commonly used techniques based on channel state information (CSI) and RSSI have higher power consumption and require baseband signal processing capability often not viable in low power, low-cost sensing devices. In Fig. 7, we visualize a closed-loop RF beamforming wireless power transfer scheme using a ULP received power sensing technique and backscattering communication to enable feedback-based optimization. These techniques can enable closed-loop beamforming with nano-watts power overhead leading to enhanced energy system for the ULP IoT system.

V. Conclusions

This paper presented an energy efficient, secure, and spectrum aware infrastructure for ULP IoT system to support sensing-monitoring for precision agriculture. We presented a system graph model and identified critical optimizations for the ULP IoT system. We presented measurement results of energy detection-based infrastructural blocks (WuRx and RSSI) which improve energy efficiency and security of the IoT system. We proposed a fast-scanning spectrum sensor for better spectrum co-existence. Finally, we presented an energy receiver which can potentially enable IoT system to be driven by the harvested energy leading to self-powered and self-perpetual system.

REFERENCES

[1] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, "A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming," *IEEE Access*, vol. 7, pp. 156 237–156 271, 2019.

[2] Y. Chen and Y. Li, "Intelligent Autonomous Pollination for Future Farming - A Micro Air Vehicle Conceptual Framework With Artificial Intelligence and Human-in-the-Loop," *IEEE Access*, vol. 7, pp. 119 706–119 717, 2019.

[3] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for Smart Precision Agriculture and Farming in Rural Areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[4] R. K. Singh, R. Berkvens, and M. Weyn, "AgriFusion: An Architecture for IoT and Emerging Technologies Based on a Precision Agriculture Survey," *IEEE Access*, vol. 9, pp. 136 253–136 283, 2021.

[5] M. Ayaz, M. Ammad-Uddin, Z. Sharif, A. Mansour, and E.-H. M. Aggoune, "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk," *IEEE Access*, vol. 7, pp. 129 551–129 583, 2019.

[6] P. Anand, Y. Singh, A. Selwal, M. Alazab, S. Tanwar, and N. Kumar, "IoT Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges," *IEEE Access*, vol. 8, pp. 168 825–168 853, 2020.

[7] S. Qazi, B. A. Khawaja, and Q. U. Farooq, "IoT-Equipped and AI-Enabled Next Generation Smart Agriculture: A Critical Review, Current Challenges and Future Trends," *IEEE Access*, vol. 10, pp. 21 219–21 235, 2022.

[8] N. Shafiee, S. Tewari, B. Calhoun, and A. Shrivastava, "Infrastructure circuits for lifetime improvement of ultra-low power iot devices," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. PP, no. 99, pp. 1–13, 2017.

[9] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[10] A. Mittal and A. Shrivastava, "Detecting Continuous Jamming Attack using Ultra-low Power RSSI Circuit," in *2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2022, pp. 49–52.

[11] M. Jamshidi, *Systems of systems engineering : principles and applications*. CRC Press, 2009.

[12] P. S. Satsangi and J. B. Ellis, "A generalized system-theoretic framework for modelling large scale national economic systems in dynamic, structural and spatial terms†," *International Journal of Systems Science*, vol. 2, pp. 213–223, 1971.

[13] P. S. Satsangi, "A Physical System Theory Modeling Framework for Transportation System Studies," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 7, no. 11, pp. 763–778, 1977.

[14] A. Mittal, N. Mirchandani, G. Michetti, L. Colombo, T. Haque, M. Rinaldi, and A. Shrivastava, "A ±0.5 dB, 6 nW RSSI Circuit With RF Power-to-Digital Conversion Technique for Ultra-Low Power IoT Radio Applications," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 9, pp. 3526–3539, 2022.

[15] R. Piyare, A. L. Murphy, C. Kiraly, P. Tosato, and D. Brunelli, "Ultra Low Power Wake-Up Radios: A Hardware and Networking Survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2117–2157, 2017.

[16] G. Michetti, G. Giribaldi, M. Pirro, A. Mittal, T. Haque, P. Cabrol, R. Pragada, H. Elkotby, L. Colombo, A. Shrivastava, and M. Rinaldi, "Hybridly Integrated MEMS-IC RF Front-End for IoT with Embedded Filtering and Passive Voltage Amplification," in *2021 IEEE Sensors*, 2021, pp. 1–4.

[17] 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

[18] 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.

[19] D. Cabric, S. Mishra, and R. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, 2004, pp. 772–776 Vol.1.

[20] N.-S. Kim and J. M. Rabaey, "A High Data-Rate Energy-Efficient Triple-Channel UWB-Based Cognitive Radio," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 4, pp. 809–820, 2016.

[21] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: requirements, challenges and design trade-offs," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 32–39, 2008.

[22] J. Park, T. Song, J. Hur, S. M. Lee, J. Choi, K. Kim, K. Lim, C.-H. Lee, H. Kim, and J. Laskar, "A Fully Integrated UHF-Band CMOS Receiver With Multi-Resolution Spectrum Sensing (MRSS) Functionality for IEEE 802.22 Cognitive Radio Applications," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 1, pp. 258–268, 2009.

[23] K. Banović and T. C. Carusone, "A sub-mW spectrum sensing architecture for portable IEEE 802.22 cognitive radio applications," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2017, pp. 1–4.

[24] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Experimental Study of Spectrum Sensing Based on Energy Detection and Network Cooperation," in *Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum*, ser. TAPAS '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 12–es. [Online]. Available: https://doi.org/10.1145/1234388.1234400

[25] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[26] Z. Xu, A. Khalifa, A. Mittal, M. Nasrollahpourmotlaghzanjani, D. Das, M. Onabajo, N. X. Sun, S. S. Cash, and A. Shrivastava, "A 30% Efficient High-Output Voltage Fully Integrated Self-Biased Gate RF Rectifier Topology for Neural Implants," *IEEE Journal of Solid-State Circuits*, vol. 57, no. 11, pp. 3324–3335, 2022.

[27] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless Networks With RF Energy Harvesting: A Contemporary Survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 757–789, 2015.

[28] S. Timotheou, I. Krikidis, G. Zheng, and B. Ottersten, "Beamforming for MISO Interference Channels with QoS and RF Energy Transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 5, pp. 2646–2658, 2014.

[29] Y. Zeng and R. Zhang, "Optimized Training Design for Wireless Energy Transfer," *IEEE Transactions on Communications*, vol. 63, no. 2, pp. 536–550, 2015.

[30] X. Chen, C. Yuen, and Z. Zhang, "Wireless Energy and Information Transfer Tradeoff for Limited-Feedback Multiantenna Systems With Energy Beamforming," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 407–412, 2014.

[31] J. Xu and R. Zhang, "Energy Beamforming With One-Bit Feedback," *IEEE Transactions on Signal Processing*, vol. 62, no. 20, pp. 5370–5381, 2014.

[32] S. Kashyap, E. Björnson, and E. G. Larsson, "On the feasibility of wireless energy transfer using massive antenna arrays in Rician channels," in *2015 IEEE 16th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2015, pp. 46–50.

[33] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 1989–2001, 2013.