Energy-Harvesting Based Jammer Localization: A Battery-Free Approach in Wireless Sensor Networks

Ahmed Hussain*, Pietro Tedeschi†, Gabriele Oligeri‡, Amr Mohamed*, Mohsen Guizani§

*Computer Science and Engineering, College of Engineering — Qatar University — Doha, Qatar
†Technology Innovation Institute, Autonomous Robotic Research Center — Abu Dhabi, United Arab Emirates
‡Division of Information and Computing Technology, Hamad Bin Khalifa University — Doha, Qatar
§Mohamed Bin Zayed University of Artificial Intelligence — Abu Dhabi, United Arab Emirates

Email: *{ahmed.hussain, amrm}@qu.edu.qa, †pietro.tedeschi@tii.ae, ‡goligeri@hbku.edu.qa, §mohsen.guizani@mbzuai.ac.ae

***Abstract*—Wireless enabling technologies in critical infrastructures are increasing the efficiency of communications. Most of these technologies are vulnerable to jamming attacks. Jamming attacks are among the most effective countermeasures to attack and compromise their availability. Jamming is an interfering signal that limits the intended receiver from correctly receiving the messages. Localizing a jammer deployed by the adversary in wireless sensor networks becomes difficult, if not impossible, due to the inaccessibility of the affected sensors in the network. This paper proposes an effective yet efficient jammer localization scheme where battery-free wireless sensors harvest the energy from the signal emitted by a powerful jammer. We compute the distance and estimate the actual jammer location based on the power received at each energy-harvesting node. We conduct extensive simulations campaign to test and illustrate the effectiveness of the proposed scheme. Finally, we demonstrate the possibility of deploying the proposed scheme with off-shelf equipment and consuming only 0.2175 mJ.**

***Index Terms*—Energy-harvesting, Battery-free, Jammer localization, Security, Cyber-physical Systems, Wireless Communication**

I. Introduction

Jamming is the act of disturbing wireless radio communications by reducing the Signal-to-Noise Ratio (SNR), or overlapping signal with more power through the use of a device called "jammer". This type of denial of service attack aims to disrupt the communication and prevent a transmitter and one or more receivers from exchanging legitimate messages in a target area such as airports, seaports, pipelines, or sensitive military scenarios [1], [2]. Nowadays, the massive demand of Software Defined Radios (SDRs) technology decreased the complexity and the cost to deploy and launch a jamming attack with minor modifications in software such as GNU/Radio. Indeed, Jamming attacks can be easily carried out due to the availability of the cheap off-shelf components that facilitate these attacks [3]. According to recent forecasts by leading specialized companies, the business driving factors also indicate a bright future for the Anti-Jamming Market. Indeed, according to a dedicated research report by Verified Market Research, "Anti-Jamming Market Size And Forecast", the Anti-Jamming Market size was valued at USD 4.00 Billion in 2020 and is projected to reach USD 7.50 Billion by 2028, growing at a Compound Annual Growth Rate (CAGR) of 8.29% from 2021 to 2028. At the time of writing this paper, many solutions have been proposed in the last decade for jamming localization. However, besides being effective only in particular scenarios with specific constraints, none of the currently-available solutions entirely took a battery-less approach into account. Indeed, a jammer-localization procedure involves at least the deployment of collaborating 3 powered up nodes that sample the wireless jammer transmission and estimate the jammer position. Despite the provided glaring gap, the integration of energy harvesting capabilities exploiting solar, mechanical, thermoelectric, and electromagnetic sources into embedded devices has further exasperated the vested energy budget issue. Indeed, the availability of the energy source from the jammer and the limitations in the overall available power supply have led to challenging system trade-offs. Thanks to the increased hardware miniaturization capabilities, energy harvesting technologies nowadays represent a sustainable, manageable, and relatively low-cost alternative to batteries that can be adopted in critical scenarios such as the jammer localization [4]. Thus, the existing literature currently misses an effective energy harvesting-based jammer localization algorithm and architecture, not involving the adoption of energy-consuming devices but being reliable and efficient even in hostile scenarios.

Contribution. The main contributions of our work can be summarized as follows: (I) We propose a novel battery-free localization scheme that allows estimating the location of an active jammer based on the power emitted. Our scenario assumes that the adversary targets a critical infrastructure, i.e., an airport, by jamming a specific frequency; (II) we utilize physical-layer properties to perform the estimation based on a set of deployed energy-harvesting wireless sensor nodes. Namely, the power received by the nodes is computed and employed to determine the position of the jammer; (III) we consider an on-site guard who visits each deployed battery-

free tag and reads the power received. Our evaluation adopts the log-normal shadow path-loss model to estimate the distance from the received signal; (IV) we consider realistic and extreme conditions as well as complex and harsh operating environments; (V) we conducted an extensive simulation campaign where we encompassed different shadowing (σ), path loss exponents (γ), and different numbers of nodes to prove the effectiveness of the proposed approach; (VI) we illustrate the possibility and applicability of the proposed scheme to be deployed on low-powered micro-controllers with the use of energy harvesting devices through evaluating the energy required to operate and collect readings on off-shelf equipment.

Roadmap. The rest of this manuscript is organized as follows: Section II introduces a few related work correlated with the topic. Section III discusses the scenario, and threat model assumed in this paper. Section IV illustrates the localization procedures and highlights the simulations results. Section V epitomizes the theoretical and experimental evaluation. Finally, Section VI wraps up the findings in this paper and discusses the future work.

II. Related Work

The authors in [5] proposed SparseTag, a sparse Radio-Frequency Identification (RFID) tag array-based system where tags are placed at different distances from each other to achieve high precision backscatter indoor localization. SparseTag design combines sparse array processing, difference co-array design, Direction of Arrival (DoA) estimation using a spatial smoothing-based approach, and a DoA-based localization method. A robust channel selection method is implemented to minimize the multipath effect. The proposed system experimental results show that the SparseTag system has high efficacy and localization accuracy.

Luo *et al*. [6] introduced ShieldScatter. This lightweight system purposefully creates multipath signatures by attaching multiple low-cost backscatter tags to an access point or Internet of Things (IoT) device to secure IoT device pairing and data transmission. ShieldScatter secures IoT devices without requiring costly antennas or modifying existing hardware. They concluded that even if the attacker is only 15 cm away from a legitimate device, ShieldScatter with only three backscatter tags can mitigate 97% of spoofing attack attempts while triggering false alarms on only 7% of legitimate traffic.

Van Huynh *et al*. [7] proposed an anti-jamming solution that can utilize the signal generated by the jammer to transmit data. Using the backscatter approach, the energy is harvested from the signal transmitted by the jammer. Besides, the reinforcement learning approach was adopted to estimate the optimal policy, maximizing the transmitter network throughput and delay.

III. Basic Scenario and Assumption

The scenario in this work is depicted in Figure 1. We consider an adversary that targets a critical infrastructure, e.g., an airport (or sea-port), intending to disrupt and block a generic

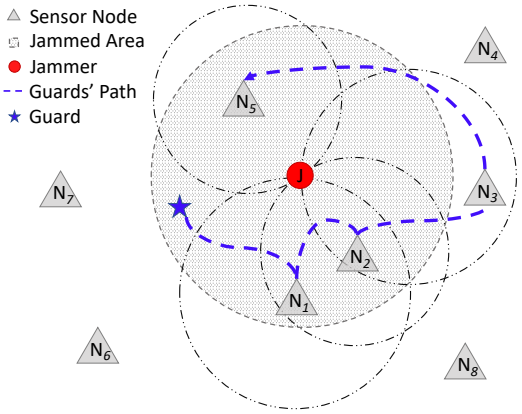


Fig. 1: Scenario assumed in this work. A random deployed jammer emits noise to block the communications over a wireless channel in a critical infrastructure. A mobile entity (e.g., a guard) detects the jamming and performs a channel measurement by traversing only the nearest nodes, so to estimate the position of the jammer.

wireless communication. We assume that a jammer device is randomly deployed in a specific area. It emits a constant high-power signal on a particular bandwidth $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$, where f_0 is the central frequency. The aim of the jammers is to disrupt all the wireless communications on this RF spectrum. We assume a jammer that emits a Additive White Gaussian Noise (AWGN) or a single-tone interference on the communication channel. Moreover, we assume that the jammer is provided with an omnidirectional antenna in order to disturb the communications across all directions. The jammer is also placed randomly to make the localization process more challenging. At the same time, we aim to localize the jammer by leveraging the power received by the RFID tags distributed within the infrastructure's premises. The randomly deployed nodes are able to harvest energy from the jammer and extract the path loss samples over a specific bandwidth B around the central frequency f_0 (i.e., the frequency range is $\left[f_0 - \frac{B}{2}, f_0 + \frac{B}{2}\right]$). We assume that a guard is in charge of localizing the jammer. Acquiring and correlating the *status* measurements of the closest nodes at different locations, the guard visits only the nearest nodes by computing the minimum Euclidean distance between the current nodes and all the nodes until he/she achieves a good estimation about the jammer's position. We consider a Line of Sight (LoS) link between the jammer and the sensing nodes by assuming the shadowing and the multipath fading effects. This assumption is reasonable because the jammer has the goal to maximise its disruptive effect in a critical infrastructure and making the localization process very hard [8].

Path loss Model. We assumed the log-normal path loss model as shown in Eq. 1 to estimate the power received $P_{RX}(d_i)$ at each node and estimate the distance d_i based on the received power, where P_{TX} represents the power transmission of the jammer, $P_L(d_0)$ represents the path loss at

the reference distance d_0 (i.e., the length of the path) computed by leveraging the Free Space model [9], γ is the path loss exponent. At the same time, X_g defines the attenuation due to the flat fading modeled as a Gaussian random variable with zero mean and a standard deviation σ. The inverse of the path loss model (Eq. 2) is adopted to estimate the distance between the jammer and the active tag(s). We define as path loss $P_L(d_i) = P_{TX} - P_{RX}(d_i) - P_L(d_0)$ the signal attenuation experienced by a tag when receiving a wireless message transmitted by a source located at distance d_i from the jammer.

$$P_{RX}(d_i)[dBm] = P_{TX} - P_L(d_0) - 10 \cdot \gamma \cdot log_{10} \frac{d_i}{d_0} - X_g \quad (1)$$

$$d_i = d_0 \cdot 10^{\frac{PL(d_i)}{\gamma 10}} \quad (2)$$

We summarize the simulation parameters and the notation used in this paper in Table I.

TABLE I: Notation used throughout the paper.

Notation	Description	Value
f_0	Channel Central Frequency.	915 MHz
N	Number of times hearing the channel.	500
$\mathcal{P}_t$	Power Transmitted.	30 dBm
$\mathcal{G}$	Grid Size.	[40 × 40]
σ	Logarithmic Standard Deviation of the Shadowing.	0.1 : 0.1 : 3
γ	Path Loss Exponent.	2
$\mathcal{T}$	Set of Tags IDs.	–
$\mathcal{C}$	Set of Tags Coordinates.	–
$\mathcal{A}$	Set of Active Tags IDs.	–
$\mathcal{RS}$	Receiver Sensitivity.	−40 dBm
d_0	Reference Distance.	1 m
PL_0	Path Loss at the Reference Distance.	0 dBm

IV. Localizing a Jammer with Battery-Free Nodes

In this section, we first introduce our solution in a nutshell (Sec. IV-A), followed by the details of the algorithm of the proposed solution (Sec. IV-B). Finally, in (Sec. IV-C) we discuss and illustrate all the simulations results.

A. Our Solution in a Nutshell

The proposed solution estimates the position of a potential jammer threatening a critical infrastructure by evaluating the power received from the harvesting nodes. To this aim, our technique builds on three enabling components, (i) we deploy random energy harvesting wireless sensor nodes in the critical infrastructure, (ii) we identify the active nodes, i.e., the nodes that can harvest the energy from the jammer, and (iii) we visit only the nearest tags to estimate the jammer's position. Our solution adopts a standard localization technique, namely linear least square (LLS), to estimate the jammer's position. We perform an extensive simulation campaign under conservative assumptions of multipath fading and the shadowing effects related to the wireless channel by varying the number of the involved nodes, the path loss exponent, and the fading component.

B. Jammer Localization Algorithm

This subsection introduces the algorithm that we adopted to localize the jammer and the performance of such schema. The jammer position estimation procedure is the following:

1) Select the starting Tag as a random Tag ID denoted with c_{tag_id} from the Deployed Tags set $\mathcal{T}$.
2) Check the status of each Tag with coordinates $(x_\mathcal{T}, y_\mathcal{T})$ by using the function *checkTagStatus()*. The function receives tag_id as an input, and returns 1 if the Tag is active, otherwise 0.
3) If the Tag is active, add the Tag ID to the Active Tags set ($\mathcal{A}$) and remove it from the deployed Tags set ($\mathcal{T}$).
4) Compute the Tag position by using the function *nextTag()*. It takes tag_id as an input, computes the nearest Tag based on the Euclidean distance, and returns the next Tag ID.
5) Repeat the steps 2 and 3 for the remaining Tags in $\mathcal{T}$.
6) Check, in each iteration, the Active Tags set $\mathcal{A}$.
7) If the set has 3 or more active Tags, the jammer position is estimated.
8) Update the next position with the new Tag position and remove the current Tag from the set $\mathcal{T}$.

The aforementioned steps are used to estimate the jammer's location. Step 6 to 8 are repeatedly performed depending on the size of the Active Tags set ($\mathcal{A}$). Algorithm 1 summarizes the aforementioned steps through pseudo-code.

Algorithm 1: Pseudo-code of the jammer estimated position.

Input: $\mathcal{T}$, $\mathcal{C}$;
Result: Estimated Jammer Position (x_J, y_J);

$\mathcal{A} \leftarrow \emptyset$;
// Selecting a Random reference Tag
tag_id $\leftarrow U[\mathcal{T}]$;
// Check if the Tag is powered
tag_status $\leftarrow$ *checkTagStatus*(c_{tag_id});
if *tag_status = 1* **then**
  $\mathcal{A} \leftarrow \mathcal{A} \cup t_{tag\_id}$;
end
$\mathcal{T} \leftarrow \mathcal{T} \setminus t_{tag\_id}$;
next_tag_position $\leftarrow$ *nextTag*(t_{tag_id});
for $i \leftarrow 2$ **to** $|\mathcal{T}| - 1$ **do**
  tag_status $\leftarrow$ *checkTagStatus*($c_{next\_tag\_position}$);
  if *tag_status = 1* **then**
    $\mathcal{A} \leftarrow \mathcal{A} \cup t_{next\_tag\_position}$;
  end
  // Estimate the jammer position
  if $|\mathcal{A}| \geq 3 \wedge$ *tag_status = 1* **then**
    $(x_J, y_J) \leftarrow$ *estimateJammer*($\mathcal{A}$);
  end
  // Update the next position
  if $i \leq |\mathcal{T}|$ **then**
    next_tag_position $\leftarrow$ *nextTag*(t_i);
    $\mathcal{T} \leftarrow \mathcal{T} \setminus t_i$;
  end
end

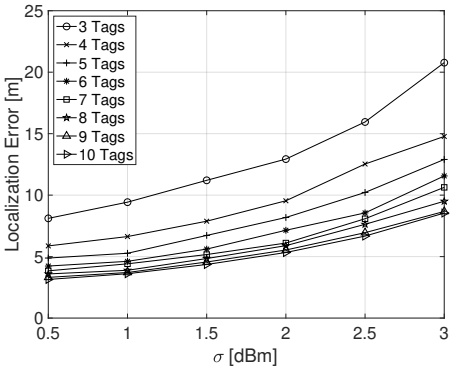


Fig. 2: Mean localization error as a function of σ (0.5 dBm $\leq \sigma \leq$ 3 dBm) and the visited nodes ($3 \leq N \leq 10$). Increasing the number of tags used dramatically improves the localization accuracy while increasing the value of σ decreases the localization accuracy.

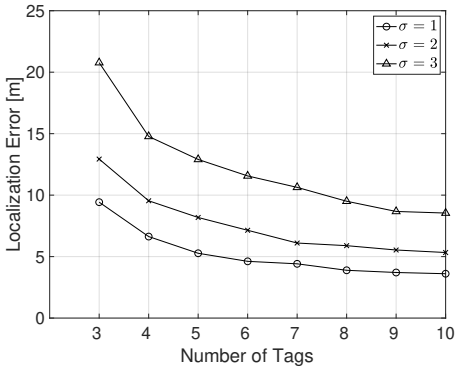


Fig. 3: Number of visited tags as a function of the mean localization error when $\sigma \in [1, \ldots, 3]$. Regardless of the value of σ, the localization error decreases with increasing the number of Tags used for localization.

C. Simulation

This subsection discusses the implementation and the analysis of the previously introduced localization algorithm.

To test the effectiveness of the proposed localization scheme, we ran $10,000$ simulations. We measured the jammer position by estimating the error while varying the number of Tags and the value of σ. In each simulation, the Tags are uniformly and randomly distributed. Figure 2 illustrates the mean localization accuracy to the actual jammer location. It can be noticed that when increasing the number of the visited Tags, the localization error decreases. On the contrary, when increasing the σ value, the localization error increases regardless of the number of the visited Tags. Further, a detailed analysis is presented in Figure 3 where σ is set to the value of 1. The mean localization error dramatically decreases when increasing the number of visited Tags used for estimation.
We start our analysis by considering the impact of the shadowing on the wireless channel with a variance σ that ranges between 0.5 dBm and 3 dBm. Further, we vary the number of the deployed tags N between 3and 10. Figure 2 depicts the mean localization error as a function of σ and N. The localization error has been computed as the euclidean distance between the real jammer position and the estimated one for the reference scenario. Finally, our results consider the average value of $10,000$ simulation runs and an average of 500 jamming signal readings.

Figure 3 depicts the localization error of the estimated jammer position with different values of σ and the number of deployed nodes in the network. The localization error is significantly higher when σ is high, and the number of visited nodes is low. It is worth noticing that even assuming the optimal configuration, with $N = 10$ nodes and $\sigma = 1$ dBm the localization error is about 4.5 meters. Furthermore, we note that the localization process becomes significantly more efficient when there are fewer nodes deployed in the network, i.e., when $3 \leq N \leq 5$, and it does not yield any crucial advantage when there are more nodes deployed ($N > 6$). Figure 4 reports the mean localization error (with the 95 % confidence interval highlighted in red) of a jammer as a function of σ (0.5 dBm $\leq \sigma \leq$ 3 dBm) with 10 sensing nodes in the network. The localization error was computed as the Euclidean distance between the real jammer position and estimated jammer position. We demonstrate that the maximum localization error for $N = 10$ and $\sigma = 3$ dBm is approximately 10 m.

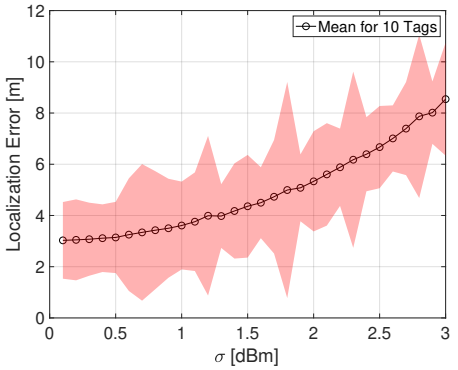


Fig. 4: Confidence Interval for the Localization Error as a function of σ (0.5 dBm $\leq \sigma \leq$ 3 dBm) when using 10 Tags. The error bound is less when $\sigma \leq 1$. When $\sigma > 1$, the error bound increases.

We now consider the average distance (with the 95 % confidence interval highlighted in red) travelled by the guard as a function of the visited tags in an area of 40×40. Figure 5 shows that in order to localize a jammer with an accuracy of $5 - 15$ m, the guard should visit $N = 5$ nodes by travelling an average distance of 61 m. Moreover, increasing the number of tags ($N > 6$) does not give any significant

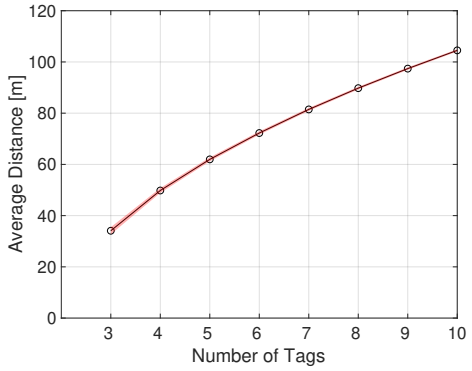


Fig. 5: Average travelled distance by the guard as a function of the visited Tags.

advantage in the localization process in terms of travelled distance and spent time to estimate the jammer position. In order to localize the jammer, we refer to the same approach used by the authors in [10], [11]. We estimate and combine the distances $\{d_1, \ldots, d_N\}$ from the ranging process in order to estimate the jammer position $[x_J, y_J]$. This is a classical linearization problem where starting from one sensor (x_n, y_n) and its related distance to the jammer (d_n) as a reference, and by subtracting it to the $n-1$ equations, we obtain a system of $n-1$ equations in the form $Az = b$, yielding:

$$A = -2 \times \begin{pmatrix} (x_1 - x_n) & (y_1 - y_n) \\ (x_2 - x_n) & (y_2 - y_n) \\ \vdots & \vdots \\ (x_{n-1} - x_n) & (y_{n-1} - y_n), \end{pmatrix}$$

$$b = \begin{pmatrix} x_n^2 + y_n^2 - y_1^2 - x_1^2 + d_1^2 - d_n^2 \\ x_n^2 + y_n^2 - y_2^2 - x_2^2 + d_2^2 - d_n^2 \\ \vdots \\ x_n^2 + y_n^2 - y_{n-1}^2 - x_{n-1}^2 + d_{n-1}^2 - d_n^2 \end{pmatrix}$$

Leveraging the Linear Least Square (LLS) method, we can estimate the position of the jammer by solving the system $Az = b$, as reported in Equation (3):

$$z = [x_J, y_J]^T = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T b \tag{3}$$

V. Theoretical and Experimental Evaluation

The proposed approach can be evaluated in a Wireless Sensor Network (WSN) scenario by adopting the following equipment:

1) A PowerCast Transmitter (915MHz).
2) Evaluation Board with P2110B Power Harvester Chip.
3) Texas Instruments (TI) MSP430FR5994 LaunchPad Development Kit.

We performed an experimental campaign using the parameters of the Powercast energy harvesting development kit and Texas Instruments MSP430FR5994 LaunchPad development kit [12], aimed at measuring the cost and applicability of introduced solution on an actual energy harvesting deployment in terms of time and energy.

A. Experimental Setup

In this setup, we consider that the MSP430FR5994 kit is powered by the energy harvested through the Powercast Evaluation Board. In order to estimate the energy consumption by the MSP430FR5994, we considered Powercast Evaluation Board equipped with the Powerharvester P2110B chip that is capable of producing an output voltage between 1.8 V to 5.25 V (depending on the distance) and operating on a frequency between 850 MHz and 950 MHz, as the energy source to power the MSP430FR5994. On the other hand, the MSP430FR5994 supports seven different operating modes [12]. The MCU features one active mode and seven software-selectable optimized ultra-low-power modes (LPM) of operation. An interrupt event can wake up the device from low-power modes LPM0-4, serve the request, and then return to low-power mode on return from the interrupt program. Low-power modes LPM3.5 and LPM4.5 deactivate the core supply to reduce power consumption. We considered 2 operating modes, namely active and low-power mode 0 (LPM0). The number of devices used is set to three devices, as the minimum number of devices required to preform triangulation is three. Besides, the number of samples acquired from each energy harvesting node is $\approx 1,000$ samples for 1, 2, and 3 meters, and $2,000$ samples for 4 meters. Once the readings are collected, the jamming location is estimated. We computed the contributions of the processing and radio chip to the overall energy consumption of our protocol through Eq. 4.

$$E[mJ] = V \cdot \int_0^T i(t)dt, \tag{4}$$

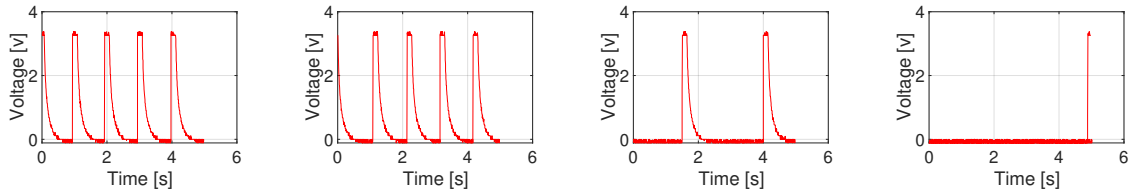
being V the input voltage and $i(t)$ the instantaneous drained current.

B. Results and Considerations

Device (Mode)	Operating Frequency	Sampling Rate $[Hz]$	Current $[mA]$	Voltage $[V]$
EVB P2110B	915 MHz	2	50	3.5
MSP430FR5994 (Active)	16 Hz	2	1.888	3
MSP430FR5994 (LP Mode 0)	16 Hz	2	0.290	3

TABLE II: Theoretical Evaluation Parameters.

From Figure 6a to Figure 6d, we see that the interference from multiple energy transmissions depends on both the distance of the PowerCast Transmitter and the evaluation board. As the distance increases, the time needed to harvest the energy increases, and vice versa. Figure 7 depicts the energy harvested by the P2110B as a function of the distance from the transmitter (jammer) and the energy consumed by the MSP430FR5994 in both modes (Active and Low-power). The distances from the transmitter are 1, 2, 3, and 4 meters, respectively. At



(a) 1 meter from the transmitter (b) 2 meters from the transmitter (c) 3 meters from the transmitter (d) 4 meters from the transmitter

Fig. 6: Voltage as a function of time received at PowerCast P2110B energy-harvesting node.

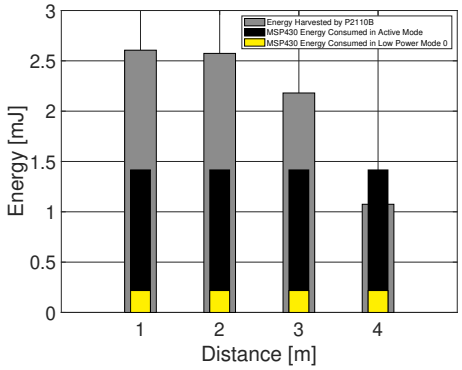


Fig. 7: Energy harvested by the P2110B as a function of the distance, and consumed by the MSP430.

1 m, the P2110B harvests 2.606 mJ of energy, while an MSP430 consumes in active mode consumes 1.4160 mJ and 0.2175 mJ in low power mode at the same distance, i.e., the 54.3% and the 8.34% of the harvested energy. In the worst case, i.e., when the sensor has a distance of $\approx$ 4 m from the transmitter, the MSP430 requires more energy in active mode, i.e., 1.4160 mJ compared to the energy harvested from the P2110B of $\approx$ 1.0749 with an overhead of 31.74%. On the other hand, if the MSP430 works in low power mode, it consumes roughly only 20.23% of the harvested energy. Finally, we remark that the MSP430 low power mode requires only 0.2175 mJ compared to the 1.4160 mJ in active mode, regardless of the distance. Table II summarizes all the considered parameters adopted in the theoretical evaluation of the system. The introduced battery-free solution provides many features such as: portability, ease of deployment, and a low-cost maintenance.

VI. Conclusion and Future Work

In this paper, we presented a novel battery-less jammer-localization technique. We proved that a jammer could be localized, leveraging the harvested energy from a jammer without consuming energy from external batteries. The proposed approach leverages a deployment of battery-free devices that constantly harvest energy from an external RF source, e.g., a jammer. The results clearly demonstrate that the conceived strategy ensures the best trade-off among energy consumption, number of adopted deployed tags, and distance traveled by the guard to localize the jammer. As reported by our performance evaluation, we demonstrated that a jammer could be localized with high precision and high efficiency with a MSP430 in low power mode by consuming only 0.2175 mJ when the distance from the jammer is $1 \sim 4$ m. Future research activities in this direction intend to deeply investigate the novelty of the proposed approach and evaluate the performance achieved herein. We believe that this contribution paves the directions for further research directions in the academia and industrial sector.

References

[1] R. Di Pietro *et al.*, "JAM-ME: Exploiting Jamming to Accomplish Drone Mission," in *2019 IEEE Conference on Communications and Network Security (CNS)*, 2019, pp. 1–9.

[2] S. Sciancalepore and R. Di Pietro, "Bittransfer: Mitigating Reactive Jamming in Electronic Warfare Scenarios," *IEEE Access*, vol. 7, pp. 156 175–156 190, 2019.

[3] P. Tedeschi *et al.*, "Modelling a Communication Channel under Jamming: Experimental Model and Applications," in *IEEE International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage (IEEE SpaCCS)*, October 2021.

[4] ——, "Security in Energy Harvesting Networks: A Survey of Current Solutions and Research Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2658–2693, 2020.

[5] C. Yang *et al.*, "SparseTag: High-precision backscatter indoor localization with sparse RFID tag arrays," in *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 2019, pp. 1–9.

[6] Z. Luo *et al.*, "ShieldScatter: Improving IoT Security with Backscatter Assistance," in *Proceedings of the 16th ACM Conference on Embedded Networked Sensor Systems*, ser. SenSys '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 185–198.

[7] N. Van Huynh *et al.*, "Ambient Backscatter: A Novel Method to Defend Jamming Attacks for Wireless Networks," *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 175–178, 2020.

[8] W. Aldosari *et al.*, "Jammer localization through smart estimation of jammer's transmission power," in *2019 IEEE National Aerospace and Electronics Conference (NAECON)*. IEEE, 2019, pp. 430–436.

[9] S. Kurt *et al.*, "Path-Loss Modeling for Wireless Sensor Networks: A review of models and comparative evaluations." *IEEE Antennas and Propagation Magazine*, vol. 59, no. 1, pp. 18–37, 2017.

[10] W. Wang *et al.*, "A grid-based linear least squares self-localization algorithm in wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, p. 317603, 2015.

[11] P. Tedeschi *et al.*, "Localization of a Power-Modulated Jammer," *Sensors*, vol. 22, no. 2, 2022.

[12] Texas Instruments Incorporated. MSP430FR5994 Datasheet. Accessed: 23 August 2022. [Online]. Available: https://www.ti.com/document-viewer/MSP430FR5994/datasheet