Data-Driven Approaches for Battery-Free IoT Networks

Saptarshi Hazra
RISE Computer Science
saptarshi.hazra@ri.se

Fehmi Ben Abdesslem
RISE Computer Science
fehmi.ben.abdesslem@ri.se

Thiemo Voigt
RISE Computer Science and Uppsala University
thiemo.voigt@ri.se

I. Introduction

The constant requirement for battery replacements is a significant barrier in the world of the Internet of Things (IoT), with concerns about battery sustainability and effective recycling. These critical challenges motivate the need for the growth of battery-free IoT, in which devices use ambient energy from sources such as photovoltaic or piezoelectric harvesters. However, due to the unpredictable and sporadic availability of ambient energy, there are obstacles in the design and implementation of such devices. The unpredictability of ambient energy emphasizes the requirement for methods that allow for frequent communication with efficient data transmission. Furthermore, because these devices have limited processing capabilities and must balance energy usage for computation with communication, securing them is particularly difficult. In this abstract, we present three pertinent challenges and our data-driven approaches to these challenges.

II. Security of ultra-low power IoT devices

In this section, we focus on securing IoT devices by providing security as an inherent function of the gateways. **Challenge:** Digital certificates are commonly used to secure IoT devices. However, in the case of battery-free IoT devices, the low-power nature, as well as balancing energy consumption between computation and communication, makes it impossible to apply complicated cryptographic methods for device authentication. Physical (PHY)-layer identification can be utilized to authenticate these IoT devices without incurring additional energy expenses. PHY-layer identification identifies a device by detecting minute changes in the transmitted analog signal. These variations are produced by hardware flaws in the analog components of a radio transmitter. Because IoT networks often comprise of heterogeneous wireless access technologies, technology-agnostic techniques based on deep neural networks are more desirable.

However, the fine-tuned set of features learned by the neural network does not generalize well to new devices, and so these methods fail to adapt well to circumstances in which new nodes join IoT networks. However, in practice, IoT deployments often have new devices joining the network as the application's demands grow. The addition of a new device to an existing deployment would necessitate costly data collecting and neural network retraining. This procedure is computationally and time-expensive, making it unsuitable for real-world deployments.

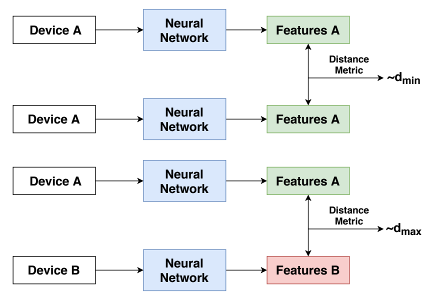
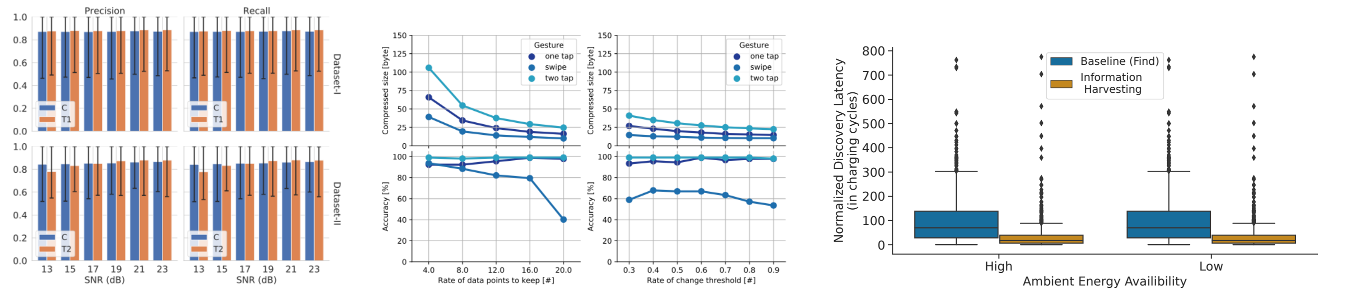


Fig. 1: Our method compares devices to find the similarity of the incoming packet to the reference packets

Method: To simplify the extension of IoT networks and enable PHY-layer identification for new devices, we use a verification neural network based on contrastive learning methods to compare between characteristics of devices. Contrastive-learning methods learn a mapping from a high-dimensional input space to a low-dimensional representation space so that similar inputs are located nearby in the representation space, while dissimilar inputs are located far away. In our approach [1], we store a single radio packet from all the devices in an IoT network as our reference packets. We compare an input packet to the reference packets for all the devices to identify the source device for that input packet using the verification neural network. Our approach is illustrated in Figure 1, by utilizing the distance metric to distinguish between devices.
Results: To evaluate our approach, we created two datasets, comprising 28 and 26 devices each. Each dataset has devices with varied radio chipsets. We segment our dataset into *seen* and *unseen* devices. The *seen* devices (37 devices) are used to train the neural network. For evaluation, we use the *unseen* devices (17 devices). Our results are shown in Figure 2a.

III. Efficient Data Exchange

In this section, we describe the challenges and our approach for efficient data communication.
Challenges: The ubiquitous nature of these devices can also be used to enable various types of interactions such as gesture and activity detection. However, due to the resource-constrained character of these wireless devices w.r.t processing power, memory, and energy budget deploying large, complex models for interaction classification and detection on the devices is



(a) Our method can identify packets from *unseen* devices with precision and recall greater than 80% across varied SNRs.

(b) Our results show that our methods are able to fit a gesture in one IEEE 802.15.4 packet while maintaining high accuracy.

(c) Normalized Discovery Latency vs Energy Availability. Our method is able to discover the neighboring node more efficiently than the baseline regardless of the energy availability.

currently difficult. To successfully detect a user's interaction, a continuous stream of sensor readings is required. However, the intermittent and unpredictable nature of energy availability limits a node's opportunities for communication, making it challenging to transmit data to the gateway.

Method: Our method [2] is based on the insight that in most of these interaction-based applications, the true value of the sensor is insignificant and may be approximated. As a result, we can employ data compression techniques to limit the quantity of data transmitted. To accomplish this, we develop two basic data compression methods tailored to interaction applications and implement them on the Zolertia firefly platform. The gateway extrapolates the compressed data. Data-driven methods such as deep-learning vision models are well established to be generalizable. As a result, in our work, we investigate the feasibility of such models in gesture recognition from compressed data while being trained on uncompressed data. Because of the decoupling between the model and the compression methods, we can use the same gateway regardless of the data compression method.

Results: We use both audio as well as shadow-based gestures in the evaluation of our method. Figure 2b shows the combination of our data compression methods with deep-learning-based gesture identification is able to reduce the data requirement while still maintaining considerable accuracy of gesture identification. Our results highlight the feasibility of a data-driven gateway model to enable efficient data communication.

IV. Enabling Peer-to-peer communication

In this section, we discuss our recent advances to enable peer-to-peer communication between two battery-free IoT devices.

Challenges: One primary challenge of peer-to-peer networking is to ensure two devices discover each other to be able to communicate. Neighbor discovery requires one device to advertise its identity to actively listening devices around. A primary objective of battery-free neighbor discovery is quickly finding neighbors while saving energy, mainly by minimizing active radio usage. However, neighbor discovery protocols typically require sampling the radio medium for long periods or employing deterministic duty cycles. Translating these strategies to battery-free devices is a challenging task, as the duty cycle and possible periods of radio activity are contingent upon the level of ambient energy availability, which is often hard to predict.

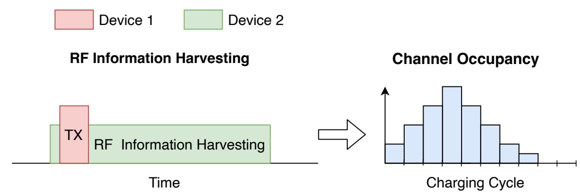


Fig. 3: Battery-free Neighbor Discovery

Method: In order to infer radio channel occupancy, we design a specific hardware for RF information harvesting using passive components. Our method [3] considers a time-slotted operation and exploits the ultra-low power sensing of RF information harvesting to discover time slots with high channel activity.

Figure 3 shows the basic principle of our method. The radio activity of Device 1 is collected by the RF information harvester of Device 2. Results are cumulatively added by Device 2 to measure the channel occupancy for each time slot of a charging cycle. Using the resulting graph, Device 2 can then schedule radio activity for time slots with a higher probability of discovering Device 1.

Results: The ambient energy availability dictates the application scenarios. Furthermore, lower ambient energy availability makes it harder for devices to discover each other due to the reduced duty cycle. Figure 2c show that our method has similar normalized neighbor discovery latency irrespective of energy availability. Furthermore, our method outperforms the baseline in both energy scenarios.

References

[1] S. Hazra, T. Voigt, and W. Yan, "Plio: Physical layer identification using one-shot learning," in *IEEE MASS'21*, 2021, pp. 335–343.

[2] S. Hazra, M. Brachmann, and T. Voigt, "Shadow-based hand gesture recognition in one packet," in *DCOSS'20*, 2020, pp. 27–34.

[3] S. Hazra, F. B. Abdesslem, and T. Voigt, "Poster abstract: Battery-free neighbor discovery," in *IPSN'23*, ser. IPSN '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 318–319. [Online]. Available: https://doi.org/10.1145/3583120.3589829