Nguyen, Le Ngu; Sigg, Stephan; Lietzén, Jari; Findling, Rainhard Dieter; Ruttik, Kalle

Camouflage learning : Feature value obscuringambient intelligence for constrained devices

Published in:
IEEE Transactions on Mobile Computing

DOI:
10.1109/TMC.2021.3092271

Published: 01/02/2023

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Nguyen, L. N., Sigg, S., Lietzén, J., Findling, R. D., & Ruttik, K. (2023). Camouflage learning : Feature value obscuringambient intelligence for constrained devices. *IEEE Transactions on Mobile Computing*, *22*(2), 781-796. https://doi.org/10.1109/TMC.2021.3092271

Camouflage learning: Data obscuring ambient intelligence for constrained devices

Le Ngu Nguyen, *Member, IEEE,* Stephan Sigg, *Member, IEEE,* Jari Lietzen, Rainhard Dieter Findling, and Kalle Ruttik, *Member, IEEE*

Abstract—Ambient intelligence demands collaboration schemes for distributed constrained devices which are not only highly energy efficient with respect to distributed sensing, processing and communication, but which also respect data privacy. Traditional algorithms for distributed processing suffer in Ambient intelligence domains either from limited data privacy, or from their excessive processing demands for constrained distributed devices.

In this paper, we present Camouflage learning, a distributed machine learning scheme that obscures the trained model via probabilistic collaboration using physical-layer computation offloading and demonstrate the feasibility of the approach on backscatter communication prototypes and in comparison with federated learning, a popular distributed learning scheme. We show that Camouflage learning is more energy efficient than traditional schemes and that it requires less communication overhead while reducing the computation load through physical-layer computation offloading. The scheme is synchronization-agnostic and thus appropriate for sharply constrained, synchronization-incapable devices. We demonstrate model training and inference on four distinct datasets and investigate the performance of the scheme with respect to communication range, impact of challenging communication environments, power consumption, and the backscatter hardware prototype.

Index Terms—Distributed machine learning, Data obfuscation, Backscatter, Computation offloading, Ambient Intelligence

1 Introduction

The ubicomp and Pervasive computing vision of *computing any time and everywhere* through instrumented and connected environments and objects, has attracted significant attention over the past two decades [1]. Related research on the Internet of Things (IoT) [2], middleware [3], mobile computing [4], sensors [5], [6], microprocessors [7], [8], user interfaces [9], computer networks [10], new materials [11], localization [12] and activity recognition [13] have flourished and advanced this vision.

Computing any time and everywhere demands continuous perception and communication among instrumented objects. This opens challenges with respect to (a) data privacy, (b) extreme energy efficiency for sensing, processing and communication, as well as (c) overhead-less collaboration among constrained devices (cf. figure 1).

To achieve (a), federated learning [14], data obfuscation [15], or homomorphic encryption [16] have been proposed, which demand high processing or communication load or compromise accuracy. *We propose Camouflage Learning*, an efficient and accurate distributed machine learning scheme that obscures the jointly utilized and trained model through non-reversible data aggregation.

Likewise, (b) energy-less operation for sensing, processing and communication has been approached through the development of energy harvesting schemes [17], chemical and organic sensors [18], [19] or, for instance, highly efficient communication schemes, such as LoRa [20], [21]. Our camouflage learning implementation is compatible with any low energy sensor, achieves energy-less computation via *physical-layer computation offloading* and discounts communication cost via backscattering. We show that our scheme outperforms LoRa in energy efficiency for communication.

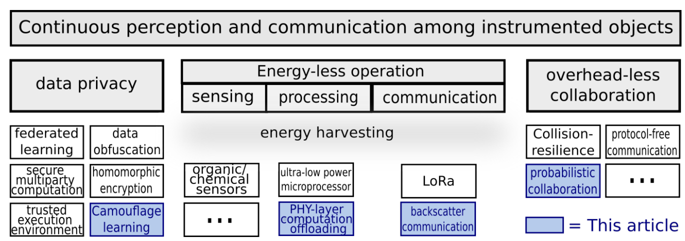


Fig. 1. Concepts and technology to realize the Ubicomp vision of computing to appear anytime and everywhere.

Overhead-less collaboration (c) has been addressed with collision resilient protocols [22] that usually require at least weak synchronization. We utilize *probabilistic collaboration* to dispose synchronization need. Our contributions are:

- A **Camouflage Learning** scheme: distributed machine learning via non-reversible data aggregation (all devices have incomplete model-information).
- **Synchronization agnostic** distributed training and inference via physical layer probabilistic collaboration and wireless channel computation offloading
- A **Proof-of-concept implementation** and evaluation utilizing highly efficient backscatter prototypes
- A **performance comparison** demonstrating higher efficiency than traditional distributed learning.

- *L. Nguyen, S. Sigg, J. Lietzen and K. Ruttik are with the Department of Communications and Networking of Aalto University, Finland. E-mail: {firstname.lastname@aalto.fi}*
- *R. Findling is with Upper Austria University of applied science Hagenberg.*

Manuscript received August 10, 2020; revised ...

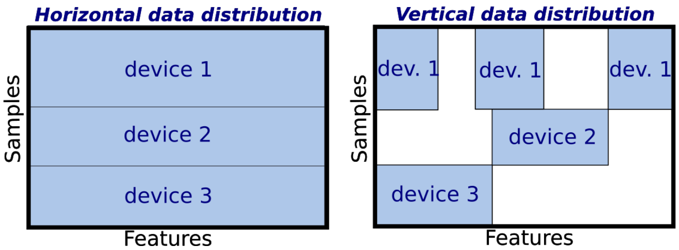


Fig. 2. Horizontal vs. vertical data separation across devices

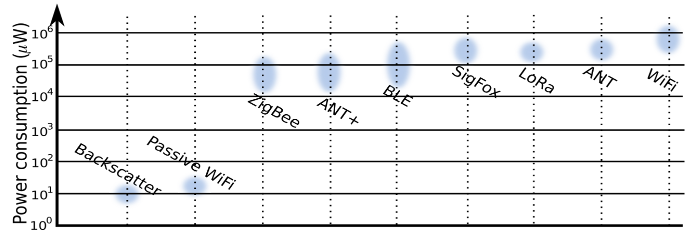


Fig. 3. Energy consumption of various communication technologies

In contrast to existing distributed machine learning, information on the model is scattered across devices (Camouflage Learning). No single device has, at any time, knowledge on the complete model or on other device's data.

2 Related Work

Data science, the extraction of information and patterns from data, has applications in virtually every domain in industry, academia and public [23]. The data d from software or hardware sensors is analyzed with respect to relevant features $\mathbf{x}$ to approximate a target function f that predicts specific target classes $y = f(\mathbf{x})$ [24]. For this, a candidate model $h(\mathbf{x})$ approximates $f(\mathbf{x})$ from the hypothesis space H using historical data for training and testing. The model h combines the weighted features into a mathematical function where the weights $\mathbf{w}$ are chosen such that the errors in the mapping between feature space and target classes are minimized according to the historical data [25].

In Ambient Intelligence, data is collected by distributed sensing devices [26], so that the feature vector $\mathbf{x}$ might be physically spread across the environment. Furthermore, it often contains personal information, that might demand privacy [27] (section 2.1). Furthermore, since energy consumption is of major concern in Ambient Intelligence domains, section 2.2 will discuss advances in energy efficient sensing, processing, and communication. Finally, section 2.3 summarizes low overhead device collaboration mechanisms for Ambient Intelligent environments.

2.1 Distributed Machine Learning and privacy

Classical machine learning assumes a single data set and data distribution, as it is typical in Ambient Intelligence, might require ineffective or sometimes infeasible data dissemination [28]. Distributed machine learning algorithms, originally fuelled by the need to scale up learning algorithms in big data domains [29], [30], [31], [32] are designed to mitigate these shortcomings [33], [34] but heavily rely on data exchange [35], [36].

Ambient Intelligence often distributes data via sensors in the environment while device constraints (e.g. energy, storage) limit data mobility. Data can be fragmented horizontally (distribution of data instances) or vertically (distribution of feature values) [37], [38], [39] (cf. figure 2).

Many distributed learning algorithms share ideas from ensemble learning, where a set of different classifiers are trained on subsets of the data (populating different hypotheses h_i) [40]. Results are then combined according to the ensemble technique [39], [41], [42]. This procedure provably decreases the error with increasing number of classifiers and is more likely to meet constraints of constrained devices by dividing the data and problem complexity into smaller pieces. It is also scalable and respects data privacy due to distributed processing and data [43].

Other approaches comprise effective voting (evaluating statistical significance of classifier performance with paired t tests) [32] and consensus-based methods [39]. However, these are of low relevance in Ambient Intelligence environments with limited inter-device communication means.

Recently, Federated learning (FL) is gaining increased attention, which addresses both data separation and data privacy [44], [45]. In FL, a global model is trained by the individual devices with local data, so that the model is known to all devices while the data is not shared [46].

We propose Camouflage learning, which distributes the data in the same way as vertical federated learning, and in addition obfuscates the model for all devices and for the coordinator. It thereby addresses privacy requirements of sensitive data in Ambient Intelligence, such as medical records, behaviour patterns or identity [47], [48], [49].

Other proposals towards privacy preserving distributed learning [50], [51] comprise, for instance, homomorphic encryption [52], differential privacy [53], [54], [55], cyclic parameter or secret sharing [48], [56], using oblivious transfer [57], as well as multi-party computation [58]. These protocols, however, require additional processing or communication overhead.

Instead, for Camouflage learning we reduce the computation and communication load through backscattering physical layer computation offloading (here physical-layer superposition of weighted features) which simultaneously obscures data from prospective eavesdroppers. Camouflage learning provides differential privacy since nothing can be learned about the individual data provided from the superimposed aggregate. In addition, information on the model (i.e. features and weights) is distributed and not shared fully with any single device or even with the coordinator.

2.2 Efficient sensing, processing and communication

In Ambient Intelligence domains, constrained devices limit the energy budget, which in turn constrains the computational and communication capabilities of devices [59]. Hence, local data processing, sensing and communication must be energy-optimized [60], [61], [62], [63].

We suggest to employ chemical and organic sensors that feature energy consumption in the order of few μW [64], [65], [66]. Some examples of low-power sensors are the MMA865xFC accelerometer (19.8μW), the MPL3115A2

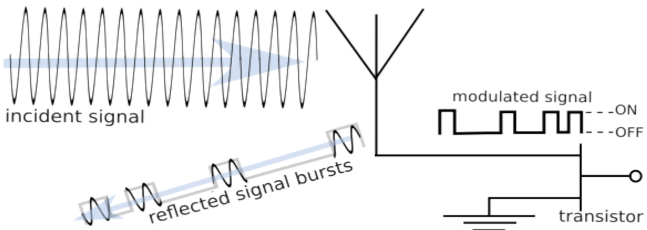


Fig. 4. Conceptional principle of backscattering burst sequences

pressure sensor (26.4μW), the PCT2202UK temperature sensor (4.6μW), the MAG3110 magnetometer (56.8μW)[1], or the 3.3μW vibration sensor [67], [68].

Furthermore, ultra-low power microprocessors are advisable for the use in Ambient Intelligence domains [69], [70]. Battery-free operation can then be achieved via power harvesting [71]. The interested reader is referred to the good overviews available on the topic, for instance, [17], [72], [73], [74] Our approach can be combined with energy harvesting and any sensor or microprocessor as only feature extraction, multiplication with a weight value and evaluation of a stochastic process are required [75].

The communication load can be reduced via algorithmic solutions, such as compressed sensing [76], which can recover sparse signals from far fewer samples than what is predicted by the Nyquist-Shannon sampling theorem [77], [78]. However, it requires complex data preparation, which contradicts the processing and energy constraints in Ambient Intelligence domain. Alternatively, low-power transmission protocols help to reduce the energy consumption through communication [21]. As depicted in figure 3, traditional, even low-power schemes consume significant energy [79], [80], [81], [82]. This involves also LoRa, a Long Range chirp spread spectrum modulation technique [83] that is receiving increased attention recently for its improved efficiency in long range communication [84].

On the other end of the spectrum are backscatter type systems that do not employ an own oscillator and signal generator but instead modulate their signals onto a reflected environmental signal (cf. figure 4) [85], [86]. Due to the absence of a dedicated signal generator and oscillator, the communication cost can be significantly reduced [87]. This mechanism can offer long-range communication by means of frequency synthesizers [79], [88] and oscillators [89] and various authors have considered backscatter communication for ambient Intelligence environments [90], [91]. We utilize a stripped-down (no frequency synthesizer or oscillator) prototype backscatter device that minimizes device complexity, cost and power consumption while compromising the transmission range [89], [92], [93]. We show that the backscatter prototype is feasible for indoor scenarios with a communication range of up to 6 meters. We exploit physical layer probabilistic collaboration for data transmission, to overcome device synchronization overhead and to trade computation cost for communication cost.

[1] Low Power Sensing Whitepaper: http://cache.freescale.com/files/sensors/doc/white_paper/LOWPOWERSENSWP.pdf

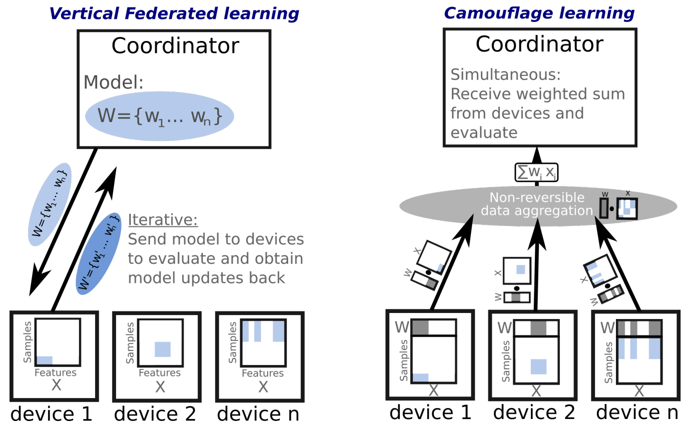


Fig. 5. Concepts of vertical federated learning and Camouflage learning.

2.3 Low overhead device collaboration

In constrained device communication, collision and scheduling of transmissions is a central concern [94], [95], [96]. For ambient backscatter-type communication (in contrast to e.g. RFID [97]), this is of particular concern, as devices are not synchronized by a strong signal to read out the tags [98]. This is addressed by collision-resistant protocols for simultaneous transmission which scale to large number of simultaneously transmitting nodes [22], [99], [100].

We exploit superposition of simultaneously transmitted sequences for data aggregation and to obscure data from distributed transmitters to realize Camouflage learning.

Function computation via superposition of wireless signals was first suggested in [101]. Goldenbaum *et al.* [102], [103], [104], [105] calculated the arithmetic mean, the geometric mean, polynomials and other functions at the time of transmission with suitable pre- and post-processing. This approach requires accurate time synchronization and to control transmit signal power, which is challenging for constrained devices and backscatter communication.

We propose probabilistic collaboration to achieve physical-layer aggregation for non-synchronized distributed devices [106]. In particular, we utilize Poisson-distributed burst sequences to compute the sum of the weighted feature inputs $\sum_{i=1}^{n} w_i x_i$ during simultaneous transmission. Synchronisation with respect to phase, transmit symbols or transmission power is not required.

Related work using physical layer computation offloading has addressed anomaly detection [107], activity recognition [108] and distributed machine learning [109]. From these, [107], [109] are dependent on tight device synchronization as it uses the protocol from [102]. Similar to [108], they use computation-offloading as a helper, but do not spread the model across distributed devices.

Instead, we implement both the training and the inference process on the through function computation on the wireless communication channel and utilize probabilistic collaboration to obscure data for camouflage learning.

3 Camouflage Learning

We propose Camouflage learning, a distributed machine learning scheme that obfuscates part of the model to all participating devices. In Camouflage learning, neither the

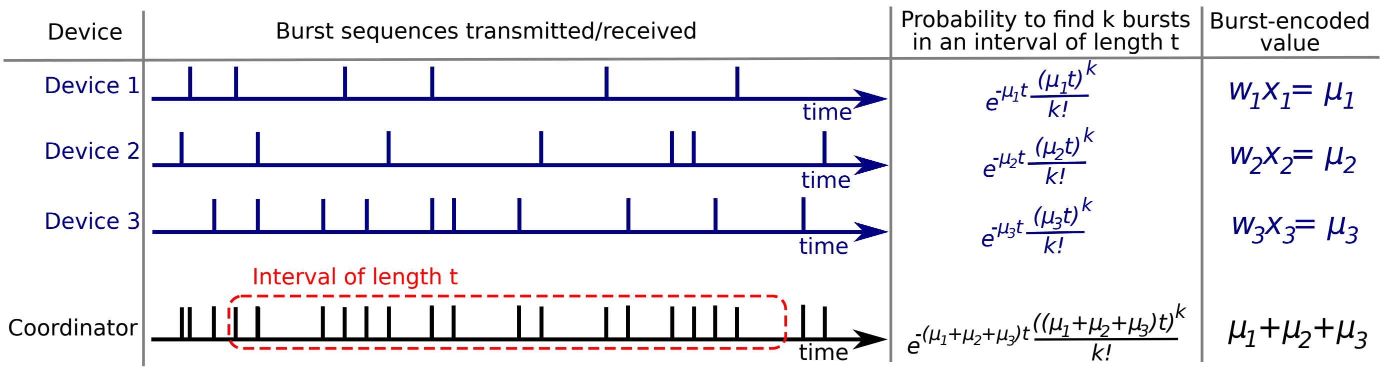


Fig. 6. Computation offloading and aggregation of the weighted feature values $w_i x_i$ during simultaneous superimposed transmission. Weighted feature values are transmitted as the mean $w_i x_i = \mu_i$ of a Poisson-distributed burst sequence. The coordinator estimates the mean $\sum_i \mu_i$ of the convoluted Poisson-distributed sequence to obtain an estimate on $\sum_i w_i x_i$.

coordinator nor any of the participating devices is at any time aware of the complete model. Figure 5 compares vertical Federated learning [34] with Camouflage learning. While in vertical Federated learning devices compute and share local model updates (model known to all devices), in Camouflage learning, the coordinator computes a single model inference from the received aggregated information $\sum_{i=1}^{n} w_i x_i$ for a particular set of inputs $\mathbf{x}$ (section 3.1). For $n > 2$, it is infeasible for the coordinator or any individual device $d_j, j \neq i$ to extract x_i or w_i from $\sum_{i=1}^{n} w_i x_i$. Learning is achieved iteratively between the coordinator and devices, alternatingly sharing the loss and their feature updates (section 3.2).

We demonstrate Camouflage learning for distributed linear regression [110]. Other approaches, that utilize aggregation over weighted feature values (e.g. neural networks, support vector machines), can be realized analogously [111].

Consider an instrumented environment with distributed backscatter-equipped sensors $d_i, i = 1, ..., n$, such as temperature, humidity, light, audio, etc. A device d_i extracts features x_i and holds and updates the weight w_i. (without loss of generality, we assume that a single device extracts a single.) Through non-reversible data aggregation via probabilistic collaboration and physical layer computation offloading, devices share $\sum_i w_i x_i = \mathbf{w}^T \mathbf{x}$ with the coordinator to compute $h(x) = \frac{1}{1+e^{w^T x}} + c$. Learning is achieved through an iterative protocol to minimize the loss $l(\mathbf{w}^T \mathbf{x})$.

3.1 Model inference via probabilistic collaboration

Model inference is achieved via probabilistic collaboration through physical layer computation offloading as depicted exemplarily in figure 6. In particular, when triggered by the coordinator, devices d_i read out their feature value x_i, multiply it with the weight w_i and transmit $\mu_i = w_i x_i$ by modulating signal bursts onto a reflected incident signal. The values μ_i are encoded as a burst sequence that follows a Poisson-distribution with mean μ_i. In particular, for a time duration of T, device d_i repeatedly transmits a burst (ON) with probability $e^{-\mu_i t} \frac{(\mu_i t)^k}{tk!}$ and no burst (OFF) else. Superimposing n such sequences during physical layer computation offloading, again yields a Poisson distributed burst sequence with mean $\mathbf{M} = \sum_{i=1}^{n} \mu_i$ [112] (cf. figure 6). Note that, for $T >> t$, the aggregation is independent of device synchronization in phase, amplitude and time, since bursts are counted irrespective of the signal phase and amplitude and since at any time, device d_i transmits a burst with the same probability $e^{-\mu_i t} \frac{(\mu_i t)^k}{tk!}$, which is only conditioned on $w_i x_i$.

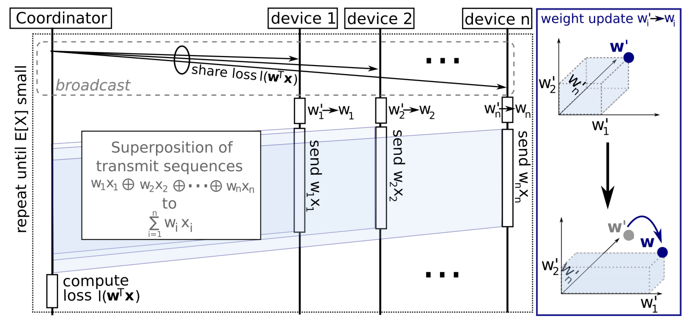


Fig. 7. To train the Camouflage learner, distributed weights are iteratively optimized via gradient descent.

The coordinator decodes a received burst sequence by counting the number of bursts in a pre-defined interval of length t and thereby estimating the mean $\mathbf{M} = \sum_{i=1}^{n} w_i x_i$ of the distribution encoded in the superimposed signal sequence [106]. From this non-reversibly aggregated weighted sum of the individual features, the coordinator then computes the model inference as $h(x) = \frac{1}{1+e^{w^T x}} + c$.

While burst collisions can not be avoided in the scheme, their probability, and hence the accuracy in the estimation of the distribution at the receiver can be controlled repeating the estimation multiple times (for $T >> t$) and by proper choice of k, t and T [106].

3.2 Training distributed weights

For training, we implement a gradient descent variant [110]. Guided by information on the loss shared by the coordinator, distributed devices d_i update their respective weight values w_i following a local random search protocol until convergence is reached (cf. figure 7) [111]. Let's first assume that devices are equipped with a common Rx interface

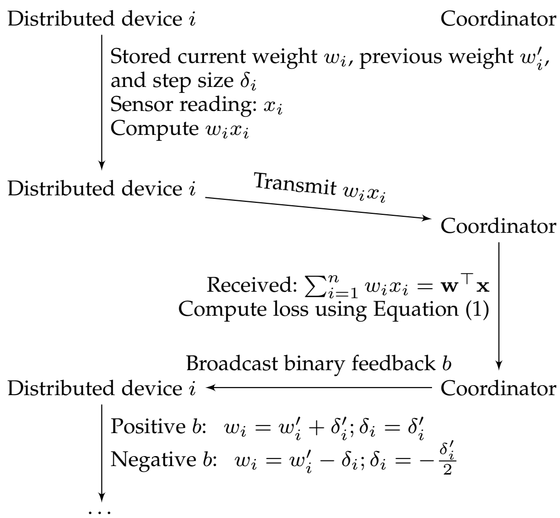


Fig. 8. Update of device d_i weight w_i based on binary input b. The process is repeated until convergence.

receive $l(\mathbf{w}^T\mathbf{x})$ from the coordinator with

$$\begin{aligned} l(\mathbf{w}^T\mathbf{x}) &= -\log\left(L(\mathbf{w}^T\mathbf{x})\right) \\ &= -y\log\left(h(\mathbf{x})\right) \\ &\qquad +(1-y)\log\left(1-h(\mathbf{x})\right) \end{aligned} \tag{1}$$

Since devices d_i are not aware of $w_j, j \neq i$, they are not capable of computing a standard gradient descent update as

$$w_i = w'_i + \lambda \cdot \frac{\partial}{\partial w'_i} l(\mathbf{w'}^T\mathbf{x}). \tag{2}$$

Instead, each device d_i will conduct a local random search on the 1-dimensional space of w_i as

$$w_i = \begin{cases} w'_i + \delta'_i; \quad \delta_i \leftarrow \delta'_i & \text{if } l(\mathbf{w}^T\mathbf{x}) \text{ improved} \\ w'_i - \delta'_i; \; \delta_i \leftarrow -\frac{\delta'_i}{2} & \text{else} \end{cases} \tag{3}$$

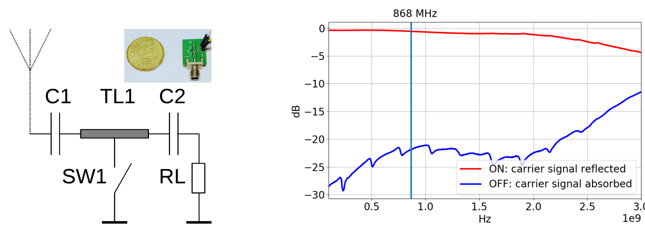
With w'_i and δ'_i we denote the old/previous value of w_i and δ_i, before updating the weights.

Since in Ambient Intelligence domains, devices are expected to be constrained, we implement the feedback from the coordinator as either a broadcast signal transmission ($l(\mathbf{w}^T\mathbf{x})$ improved) or no signal (($l(\mathbf{w}^T\mathbf{x})$ worse). We can read out this information from the backscatter interface by monitoring the voltage change on the interface. Also for the binary feedback, the optimization of the weights follows the update mechanism in equation (3) (cf. figure 8).

4 A PROTOTYPE BACKSCATTER DEVICE

We designed prototype backscatter devices to implement Camouflage learning in an Ambient intelligent environment (cf. figure 9a). For data modulation, we absorb (OFF) or reflect (ON) the signal. The device consists of only five components and can be connected to a microcontroller to guide the modulation onto the reflected signal via the switch (SW1). We used a 50 Ω (Ohm) transmission line, terminated with a power detector circuit matched to 50 Ω[2].

[2]For simple backscattering, only a resistor is needed. The power detector allows communication back from the coordinator (voltage-based data reception for binary feedback)



(a) Schematic (b) Reflected power up to 3GHz

Fig. 9. Schematic for our backscatter prototype. The components are a 50 Ω transmission line (TL1), a power detector circuit matched to 50 Ω and which serves as a terminating resistor (RL), a switch (SW1) and two DC-blocking capacitors (C1, C2).

The signal propagates the transmission line and is absorbed by the power detector circuit (non-reflecting OFF-state). The reflecting ON-state is realized using a current-controlled switch to reflect the signal back.

4.1 Equipment cost

We purchased the components to produce the backscatter devices from Digikey [3]. The highest cost is that of an SMA connector jack WM17359-ND with 3.92 EUR (approximately 4.39 USD). For the final device design with a fixed operating frequency patch antenna printed on the back of the board, this cost can be discarded. The diode (SW1) Infineon Technologies BAR8802VH6327XTSA1 costs less than 0.1 EUR (approximately 0.12 USD). This low device cost is essential to realize smart environments with massive deployment of backscatter-equipped sensors.

For comparison, active system including RF switch (2.5 USD), ultra-low power oscillator (1.8 USD) and a multiplexer (2.6 USD) will raise the cost significantly [89].

4.2 Input return loss

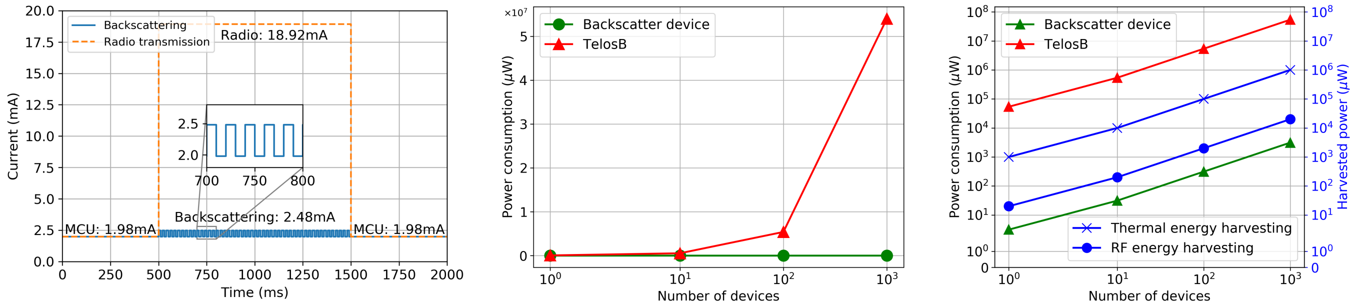
We measured the characteristics of the modulator with a network analyser. In particular, we are interested in the input return loss, which tells how much the back-scattered signal is attenuated in non-reflecting and reflecting states. Figure 9b depicts the average of the measurements for ten of or our backscatter devices. Observe that the received power difference between ON-state and OFF-state is about 20dB up to approximately 2GHz. In addition, the received power for the ON-state is close to 0dB. Due to the regulation of radio frequencies and our available licenses, we select the frequency of 868MHz in our experiments in section 5.

4.3 Power consumption

For signal reflection and modulation, the backscatter device uses 0.5 mA continuously over 10ms. [4]. In addition, the microcontroller operating the voltage-controlled switch demands 1.98mA MCU. For operation, our prototype consumes 0.9mW with an 1.8V operating voltage and 2.5mW

[3]https://www.digikey.com/

[4]The power consumption can be further reduced by using RF switches such as Analog Devices HMC190BMS8 [89]. For instance, using 5 V to control the switch, the current consumption would drop to 1μA, which is small enough to supply with an RF energy harvester [114]



(a) Current consumption during transmission: backscatter prototype vs. CC2420 [113]
(b) Estimated power consumption of our prototype and TelosB [113] for transmission
(c) Power consumption vs. energy harvesting: TelosB and backscatter prototype [114]

Fig. 10. Performance comparison: TelosB [113] vs. backscatter prototype, and estimated amount of energy harvested from ambient sources [114]

INDOOR [115]	OUTDOOR [116]
Environmental information in an office over several days. Modalities: temperature, humidity, CO_2 level, and light intensity. The ground-truth was acquired using a surveillance camera. The target of this dataset is to detect occupancy of the office: whether there are people inside the office or not.	Scattered sensors over $900 \times 300\text{m}^2$, separated by at least 20-40m. Modalities: acoustic (microphone), seismic (geophone), and infrared (polarized IR sensor). The data describes vehicles from two classes: tracked and wheeled.

Fig. 11. Datasets used to feed continuous streams of data to devices in our experiments

with 5 V. For comparison, PLoRa power consumption is 2.591 mW (250× smaller than LoRa) [117].

Figure 10a compares a CC2420 802.15.4 radio transceiver to our backscatter prototype, both operated by a 8Mhz 16-bit TI MSP430 micro-controller [118] (1.98mA MCU). To transmit a packet (0dB), the CC2420 draws a current of 18.92mA-1.98mA= 16.94 mA in 1012ms [119]. We chose the CC2420 and MSP430 for their use by the TelosB [113], [120], which draws less current than, e.g. the LoRaBug [121].

Figure 10b and figure 10c show the power advantage of our prototype[5]. Using -5dBm Tx power, TelosB consumes 54mW (transmit), 60mW (listen), 61mW (receive), and 4.8mW (compute). For fair comparison, we assumed the same backscatter compute power consumption of 4.8mW.

We estimate the average power of communication $P_{MSG} = \frac{E_{MSG}}{T_{MSG}}$ as the amount required to send a message E_{MSG} over the duration between consecutive messages T_{MSG} [122]. For $T_{MSG} = 1$, the average energy amount required to send a message is $0.003125mJ$ using our backscatter device, $0.0035mJ$ using PLoRa, and $4.17mJ$ using LoRa.

5 EXPERIMENTS

We study Camouflage learning and our hardware prototype with respect to transmission range, communication load, classification, training and environmental impacts.

5.1 Distributed model inference and training

We compare Camouflage learning to other distributed machine learning approaches using two datasets (cf. figure 11). These datasets were chosen for their relevance to Ambient Intelligence, diversity in size, number of features, and sensors [115], [116]. We assign one feature to each distributed device. For OUTDOOR [116], we randomly split 75% for training and 25% for testing while for INDOOR [115], we follow the authors approach to use six days for training and the remaining days for testing.

We compared Camouflage learning against a non-distributed logistic regression (using scikit-learn 0.20.1 [6]) and federated learning.

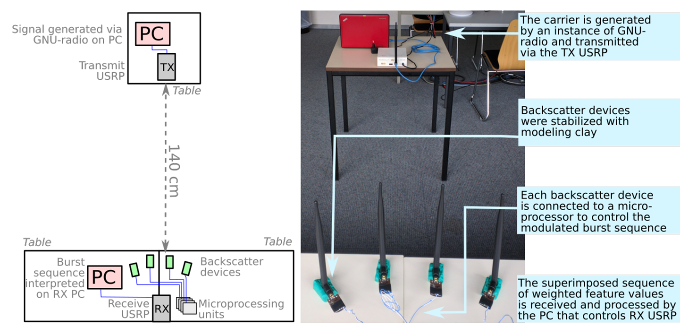


Fig. 12. Device installation for the case study

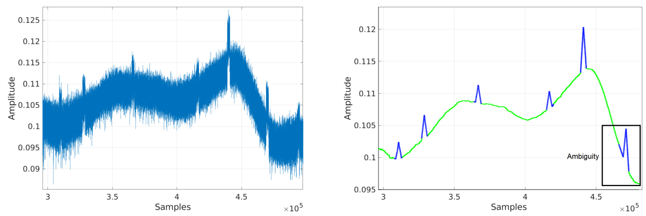
5.1.1 Probabilistic collaboration experiment

To test the burst recognition accuracy for Probabilistic collaboration through physical layer computation offloading, we utilized the *Indoor* dataset and employed four backscatter devices, one for each feature stream (light, temperature, humidity, and CO_2). To generate and read out the modulated signals reflected from the backscatter prototypes, two Ettus N200 USRPs (SBX daughterboards, 868MHz, 1MHz sampling rate) were used as Tx and Rx (cf. figure 12).

Devices modulated their weighted (see section 3.2) feature values ($w_i x_i$) periodically via Poisson-distributed burst sequences onto the reflected signals. The samples were averaged over non-overlapping 60 second feature windows, since each sensor had its own sampling rate. The burst

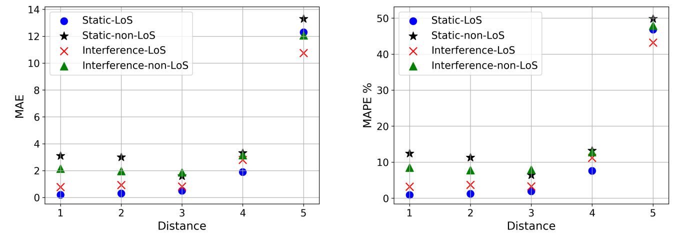
[5] Estimated according to $\frac{1}{2}CV^2F$ [93] with diode capacitance C, voltage V and frequency F)

[6] https://scikit-learn.org/stable/



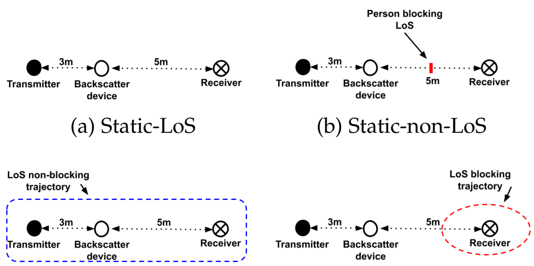
(a) Raw signal amplitude (b) Filtered signal

Fig. 13. Ambiguity of detected bursts when there is movement



(a) Mean Absolute Error (b) MAPE Error

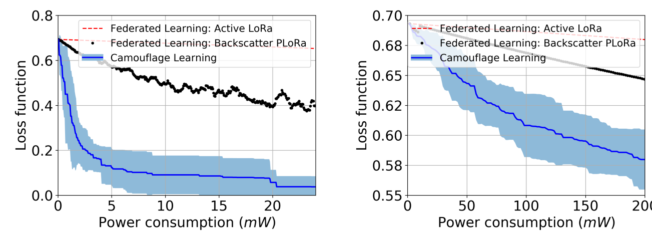
Fig. 15. Burst detection in various environmental conditions



(a) Static-LoS (b) Static-non-LoS

(c) Interference-LoS (d) Interference-non-LoS

Fig. 14. Layout of devices in the experiments on environmental variation



(a) INDOOR [115]: 4 features, 8143 training samples (b) OUTDOOR [116]: 100 features, 73896 training samples

Fig. 16. Power consumption: Camouflage vs. Federated learning

length was 10-20ms and for accurate estimation of the burst recognition accuracy, we maintained the transmission for 60 seconds. For burst detection, our instrumentation achieved a precision of 0.9 and a recall of 0.89. Overall, camouflage learning for the INDOOR dataset achieved an accuracy of 0.82 (F_1 score 0.82). For comparison, training logistic regression via gradient descent on a desktop computer (Intel Core i5 1.8GHz, 8GB RAM, with scikit-learn library version 0.20.1) achieved an accuracy of 0.94 (F_1 score 0.93).

5.1.2 Effect of changes in an environment

Human movement in the monitored area may affect the wireless channel and hence impact the burst detection accuracy [123]. For example, a person blocking the line-of-sight (LoS) between a backscatter device and the receiver (RX) or human movement may increase the noise floor and impair the correct counting of bursts at the receiver (cf. figure 13).

We investigated the impact of four types of human interference, (a) *Static-LoS*: No person in the room or people sitting still and not blocking the line-of-sight, (b) *Static-non-LoS*: A person blocks the line-of-sight between backscatter device and RX), (c) *Interference-LoS*: One person moves around in the room, not blocking the line-of-sight, and (d) *Interference-non-LoS*: One person moves around freely in the room, occasionally blocking the line-of-sight between a backscatter device and RX (figure 14).

In cases, we varied the distance between backscatter and Rx from 3m to 5m while modulating 50 distinct humidity samples x_i from the INDOOR dataset ($16.7 \leq x_i \leq 39.1$; $\sigma = 25.7$, std=5.5) through physical layer probabilistic collaboration. The burst detection Mean Absolute Error (MAE) and Mean Absolute Percentage Error (MAPE) at the Rx is shown in figure 15. The MAE is at most 3.5 within 3m and higher when the signal is blocked or at larger distance. Possible improvements can be achieved by locating devices above human height and by template matching.

5.1.3 Model performance through distributed training

Figure 16a and figure 16b depict the convergence speed of the algorithms. The figures plot the loss along with the confidence interval (10 repetitions). Camouflage learning uses less power to optimize the weights of the logistic regression model. The prediction accuracyies achieved are competitive: INDOOR 0.92 (0.94), OUTDOOR 0.72 (0.78) (cf. figure 17 and figure 18).

The power consumption of our backscatter device is $0.003125mW$. For comparison, that of PLoRa [117] is $0.0035mW$, which implements frequency shifting for backscattering communication, while that of an active LoRa node is $4.17mW$ [117]. Based on these figures, we estimate the power utilized during training on two datasets [115] [116]

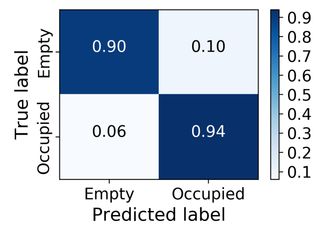
Finally, Camouflage learning also exchanges less data overall (figure 19). This is because federated learning requires active data transmission and reception of all devices.

5.2 Communication range

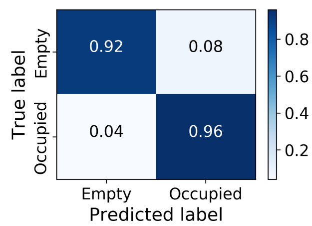
The communication range of ambient backscatter devices is severely limited since the reflected modulated signal is magnitudes lower than that of the original carrier signal [86]. In this section, we investigate the communication range of our ambient backscatter devices in real indoor environments and with respect to different antenna configurations.

5.2.1 Omnidirectional antennas

In our first setting with an early prototype version of our backscatter interface, we investigated the communication range utilizing an omnidirectional antenna (Ettus VERT900

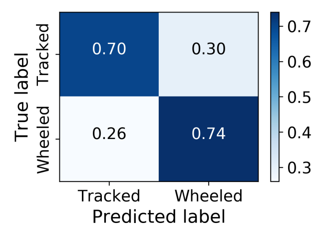


(a) Camouflage learning

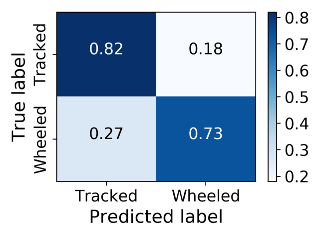


(b) Federated learning

Fig. 17. Confusion matrices for the INDOOR dataset [115]

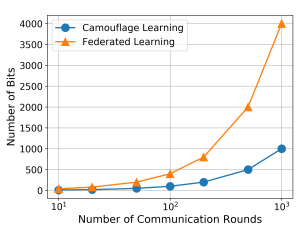


(a) Camouflage learning

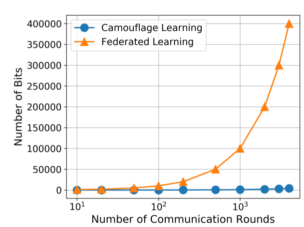


(b) Federated learning

Fig. 18. Confusion matrices for the OUTDOOR dataset [116]



(a) INDOOR dataset [115]



(b) OUTDOOR dataset [116]

Fig. 19. Communication load: Camouflage vs. Federated learning

824 to 960 MHz, 1710 to 1990 MHz Quad-band Cellular/PCS and ISM Band omnidirectional vertical antenna, at 3dBi gain). In this early prototype manufactured on fiber glass circuit board, we used a general purpose diode (1N4148), 470 nF / 50 V ceramic capacitors and a terminating resistor made of two parallel connected 100 Ohm resistors. The device was brought out in line-of-sight between Tx and Rx (Ettus N200 USRPs with SBX daughterboards using the same omnidirectional antenna, see figure 20). Gradually moving Tx and Rx farther away (1m to 1.5m; step size 0.1m), the received power at the backscatter device ranged from approximately 1.1mW to 486μW and after 1.4m the prototype ceased to detect the backscattered binary sequence.

We improved the prototype with superior components: BAR8802VH6327XTSA1 Infineon Technologies diode, 10 nF

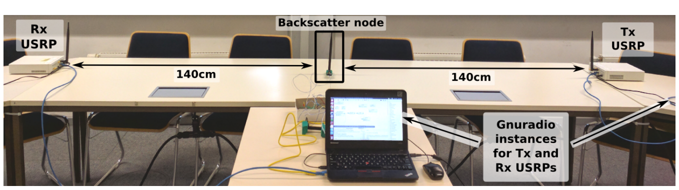
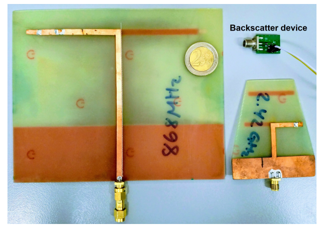
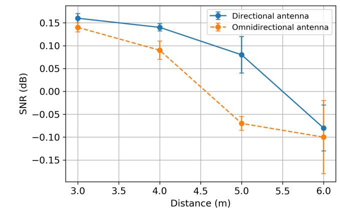


Fig. 20. Measuring the working distance of our first prototype



(a) Semi-directional antennas (868MHz and 2.42GHz) used



(b) Signal-to-noise ratio (SNR) with various distances

Fig. 21. Microstrip antennas (fiber glass board and copper layers, relative permittivity 4.5, maximum gain 4.7dBi) and their impact on the range

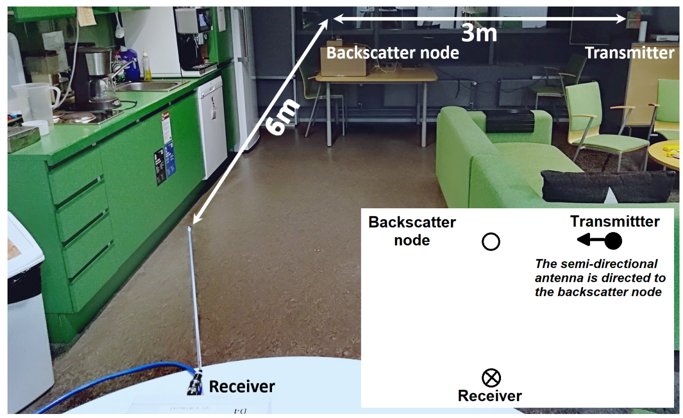


Fig. 22. Layout of our experiments on the operating distance

capacitors, a 49.9 Ohm resistor and directional antennas.

5.2.2 *Semi-directional antennas*

We used semi-directional antennas (figure 21a) to extend the range of the system. In a larger indoor space (figure 22) we placed Ettus N200 USRP devices (SBX daughterboards, 868MHz, 1MHz sample rate) at 3m (Tx) and 1-6m (Rx) from the backscatter prototype.

Measurements were conducted with both omnidirectional and directional-type Tx antennas and repeated 10 times for each distance and antenna type (figure 21b). The signal strength at the prototype with omnidirectional antenna was approximately 121μW. The signal was well received up to 5m, which is sufficient for many indoor environments. To further extend the range, we suggest the use of switching frequency control [124] or frequency synthesizers [79], [89].

6 DISCUSSION

We discuss further aspects of camouflage learning below.

6.1 Backscatter design

While our design does not limit to the operating frequency, the limiting factor is the quality of components used to manufacture the device. With ideal components, the termination resistor would be perfectly matched to the transmission line and the reflection coefficient in non-reflecting state would be 0 while with an ideal switch, all power would be reflected back for a reflection coefficient of -1.

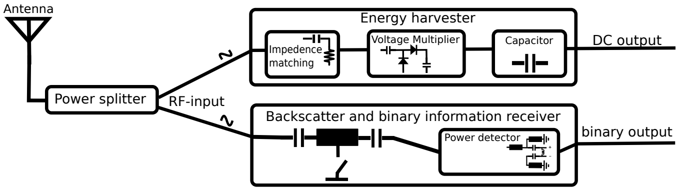


Fig. 23. Schematic of a generic energy harvesting device. Power splitter for simultaneous energy harvesting and information reception.

The switching diode used has a parasitic capacitance of 0.28 pF (OFF) and 2 Ω forward resistance (ON), so that the return loss in ON-state is 0.70 dB. Correspondingly, the reactance of the parasitic capacitor in parallel with the terminating resistor gives a return loss of 28.4 dB in the OFF-state.

A diode requires a constant current to keep it conducting (in this case 0.5 mA). Traditionally, a switching diode is biased backwards when not conducting by applying a negative voltage, thus minimizing the off-state capacitance. For improved results, we suggest, a voltage- instead of current-controlled element, such as a field effect transistor.

The circuit board material used in our experiments is also not optimized for RF applications and the performance therefore starts to degrade above 2GHz frequency.

6.2 Energy harvesting for battery-free operation

For long-term deployments, a maintenance-free operation is desired [125]. The power consumption of the TI CC2650 controlled backscatter device is lower than the power that can be harvested from solar and thermoelectrics [114]. The amount that can be collected from RF sources with 4cm^2 antenna (transmit power 4 W and distance 15 m) and thermal 1cm^2 piezoelectric material is 20μW and 1mW, respectively [114]. Using improved components can further reduce the power consumption of the backscatter prototype.

Figure 23 depicts a generic architecture for energy harvesting devices. In particular, the device is able to exploit the received power both for energy harvesting and, simultaneously, for information reception. We propose to employ power-splitting, as this achieves better tradeoffs between information rate and amount of RF energy transferred when compared to simpler time-slotted schemes [126], [127].

Experiments on the amount of harvested RF energy from ambient RF signals indicate that about 2μW of energy can be harvested from isotropic 2W RF transmitters (such as, for instance, WiFi) in about 25m distance [128], [129] and at about $0.5 - 1.5$V [130], [131]. For comparison, using digital TV signals, even an energy harvesting rate from over 60μW in typical distances of about 4km has been reported in [130]. This enables the operation of the aforementioned low-power or power-less (zero-power) environmental sensing devices.

6.3 Choice of antenna

For a production-level system, we propose to print a patch antenna, which is cheap to manufacture, on the back of the circuit board. Such antenna will need a rectangular space of $\frac{1}{4}$ to $\frac{1}{2}$ of wavelength λ. For instance, a backscatter system with a patch antenna in the 2GHz range could have dimensions smaller than $4\text{cm}\times 4\text{cm}$. Usually, antennas are matched to 50Ω, as all cables and connectors are also 50Ω. The natural impedance of the patch antenna is higher though, for instance, 100Ω. In this case, all circuitry should be matched to the same impedance as the antenna. This minimizes the return loss in ON-state as the ratio of the diode's forward resistance and the impedance of the antenna is bigger.

6.4 Privacy

With our distributed approach, the model is by design not shared but instead distributed among participating devices. Learning the model in our scheme means to reverse-engineer it from the model prediction, or to conduct advanced signal analysis and processing while inside the environment, both of which constitutes a significant effort [49].

Since the model is distributed and not known completely to any individual device, it is harder to steal and thereby to learn properties of the environment or its inhabitants [132]. It is also more difficult for any device, including the coordinator to learn of the feature values, since only the weighted sum is disclosed, which further contributes to improved privacy. Summarizing, we believe that Camouflage learning improves privacy in instrumented environments.

6.5 Camouflage learning with other learners

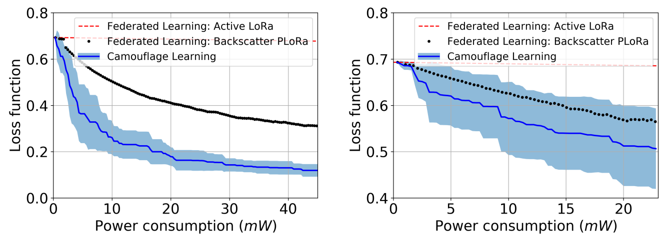
We have demonstrated camouflage learning via physical layer computation offloading with a logistic regression classifier. It is straightforward to extend the model for other learning approaches. For instance, aggregation of the weighted inputs in the first layer of a neural network, aggregation of the weighted features in the mathematical description of a support vector machine or also offloading the product of potential functions in conditional random fields by encoding the product terms as sum of logarithms.

6.6 Computational complexity

The computational complexity of the individual devices is comprised by a single multiplication ($w_i x_i$) and repeated random decisions on whether or not to switch to ON-state according to a Poisson distribution with mean $w_i x_i$. Both of these computations can be realized in hardware. At the receiver, for $10^{\eta-1} < W^T X \leq 10^{\eta}$, the complexity is $\mathcal{O}\left(\eta^{1.465} \cdot \log(\eta)\right)$ [133], where the term $\eta^{1.465}$ is according to 3-way Toom-Cook multiplication [134].

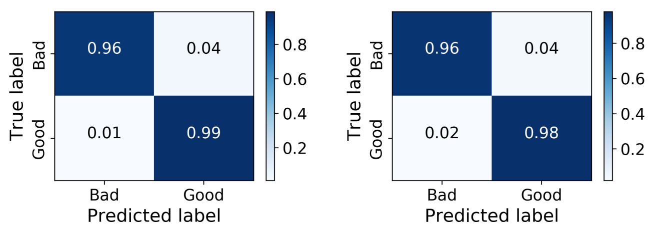
6.7 Application to arbitrary datasets

Camouflage learning can be applied to arbitrary datasets and applications are not restricted to Ambient Intelligence domains. To demonstrate this, we verified camouflage learning on two benchmarking datasets [135] [136]. We achieved classification performances for camouflage (federated) learning 0.98 (0.97) (INTRUSION DETECTION [135]: 494020 samples, 40 features) and 0.75 (0.80) (PHISHING [136]: 11055 samples, 30 features) as depicted in figure 25 and figure 26. Figure 27 shows that Camouflage learning requires strictly less data transmission in both datasets.



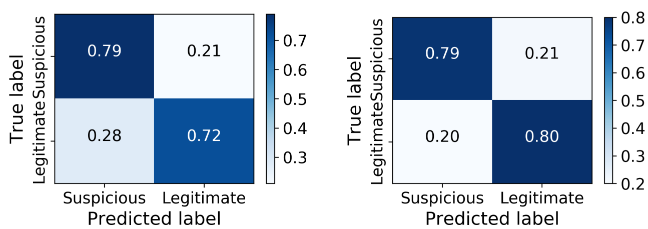
(a) INTRUSION [135] (b) PHISHING [136]

Fig. 24. Power consumption of Camouflage learning and non-distributed logistic regression (Active LoRa Node and PLoRa [117])



(a) Camouflage learning (b) Federated learning

Fig. 25. Confusion matrices for the INTRUSION dataset [135]



(a) Camouflage learning (b) Federated learning

Fig. 26. Confusion matrices for the PHISHING dataset [136]

7 CONCLUSION

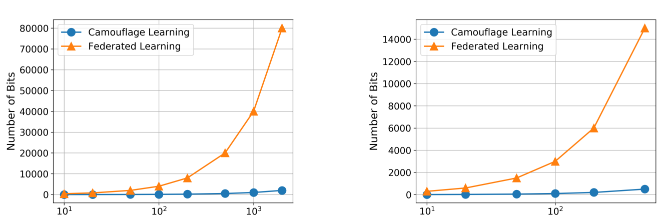
We have proposed Camouflage learning, a distributed machine learning technique for vertically-partitioned data collected by distributed sensing devices. Our approach achieves energy-less computation via physical-layer computation offloading, exploiting interference of backscattered signals for data aggregation. It thereby brings battery-free distributed learning and continuous operation in Ambient Intelligence environments into reach.

Each sensor-equipped device acquires and processes environmental stimuli and modulates the weighted feature values $w_i x_i$ as Poisson-distributed burst sequences onto a reflected electromagnetic signal. The coordinator estimates the weighted sum $\sum_i w_i x_i$ from the superimposed burst sequences to evaluate and guide the model optimization via binary feedback.

None of the devices nor the coordinator is at any time aware of the complete model. Camouflage learning advances the state-of-the-art with respect to (1) *Physical layer Computation offloading*, (2) obscuring the model via *total distribution*, (3) *Model training through distributed random search*, and (4) *Zero-synchronization requirement* thanks to probabilistic collaboration via superimposed Poisson-distributed burst sequences for weighted feature aggregation.

We extensively evaluated the scheme in comparison to traditional approaches with respect to power efficiency, prediction accuracy as well as various aspects and limitations of the prototype hardware.

Camouflage learning was evaluated using prototype backscatter devices deployed in indoor environments.



(a) INTRUSION [135] (b) PHISHING [136]

Fig. 27. Communication load of Camouflage and federated learning [39]

ACKNOWLEDGMENTS

We appreciate partial funding in the Academy of Finland project ABACUS: Adaptive Ambient Backscatter Communications for Ultra-low power Systems.

REFERENCES

[1] G. D. Abowd, “What next, ubicomp? celebrating an intellectual disappearing act,” in *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 2012, pp. 31–40.

[2] O. B. Sezer, E. Dogdu, and A. M. Ozbayoglu, “Context-aware computing, learning, and big data in internet of things: a survey,” *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 1–27, 2017.

[3] V. Raychoudhury, J. Cao, M. Kumar, and D. Zhang, “Middleware for pervasive computing: A survey,” *Pervasive and Mobile Computing*, vol. 9, no. 2, pp. 177–200, 2013.

[4] V. Pejovic and M. Musolesi, “Anticipatory mobile computing: A survey of the state of the art and research challenges,” *ACM Computing Surveys (CSUR)*, vol. 47, no. 3, pp. 1–29, 2015.

[5] L. Atallah and G.-Z. Yang, “The use of pervasive sensing for behaviour profiling—a survey,” *Pervasive and mobile computing*, vol. 5, no. 5, pp. 447–464, 2009.

[6] J. Liu, H. Liu, Y. Chen, Y. Wang, and C. Wang, “Wireless sensing for human activity: A survey,” *IEEE Communications Surveys & Tutorials*, 2019.

[7] J. Šilc, T. Ungerer, and B. Robic, “A survey of new research directions in microprocessors,” *Microprocessors and Microsystems*, vol. 24, no. 4, pp. 175–190, 2000.

[8] Z. Li, C. Huang, X. Dong, and C. Ren, “Resource-efficient cyber-physical systems design: A survey,” *Microprocessors and Microsystems*, p. 103183, 2020.

[9] M. Koelle, S. Ananthanarayan, and S. Boll, “Social acceptability in hci: A survey of methods, measures, and design strategies,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 2020, pp. 1–19.

[10] J. Pan, S. Paul, and R. Jain, “A survey of the research on future internet architectures,” *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.

[11] D. Mendes, F. M. Caputo, A. Giachetti, A. Ferreira, and J. Jorge, “A survey on 3d virtual object manipulation: From the desktop to immersive virtual environments,” in *Computer graphics forum*, vol. 38, no. 1. Wiley Online Library, 2019, pp. 21–45.

[12] F. Gu, X. Hu, M. Ramezani, D. Acharya, K. Khoshelham, S. Valaee, and J. Shang, “Indoor localization improved by spatial context—a survey,” *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–35, 2019.

[13] Y. Wang, S. Cang, and H. Yu, “A survey on wearable sensor modality centred human activity recognition in health care,” *Expert Systems with Applications*, vol. 137, pp. 167–190, 2019.

[14] V. Kulkarni, M. Kulkarni, and A. Pant, "Survey of personalization techniques for federated learning," *arXiv preprint arXiv:2003.08673*, 2020.

[15] R. Shokri, "Privacy games: Optimal user-centric data obfuscation," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 299–315, 2015.

[16] Y. Aono, T. Hayashi, L. Wang, S. Moriai *et al.*, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2017.

[17] T. Soyata, L. Copeland, and W. Heinzelman, "Rf energy harvesting for embedded systems: A survey of tradeoffs and methodology," *IEEE Circuits and Systems Magazine*, vol. 16, no. 1, pp. 22–57, 2016.

[18] S. Han, J. Kim, S. M. Won, Y. Ma, D. Kang, Z. Xie, K.-T. Lee, H. U. Chung, A. Banks, S. Min *et al.*, "Battery-free, wireless sensors for full-body pressure and temperature mapping," *Science translational medicine*, vol. 10, no. 435, 2018.

[19] T. V. Tran, N. T. Dang, and W.-Y. Chung, "Battery-free smart-sensor system for real-time indoor air quality monitoring," *Sensors and Actuators B: Chemical*, vol. 248, pp. 930–939, 2017.

[20] R. S. Sinha, Y. Wei, and S.-H. Hwang, "A survey on lpwa technology: Lora and nb-iot," *Ict Express*, vol. 3, no. 1, pp. 14–21, 2017.

[21] A. Lavric and V. Popa, "Internet of things and lora™ low-power wide-area networks: a survey," in *2017 International Symposium on Signals, Circuits and Systems (ISSCS)*. IEEE, 2017, pp. 1–5.

[22] M. Hessar, A. Najafi, and S. Gollakota, "Netscatter: Enabling large-scale backscatter networks," in *16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)*, 2019, pp. 271–284.

[23] J. D. Kelleher and B. Tierney, *Data science*. MIT Press, 2018.

[24] S. Russell and P. Norvig, "Artificial intelligence: a modern approach," 2002.

[25] C. M. Bishop, *Pattern recognition and machine learning*. springer, 2006.

[26] D. J. Cook, J. C. Augusto, and V. R. Jakkula, "Ambient intelligence: Technologies, applications, and opportunities," *Pervasive and Mobile Computing*, vol. 5, no. 4, pp. 277–298, 2009.

[27] P.-P. Verbeek, "Ambient intelligence and persuasive technology: The blurring boundaries between human and technology," *Nanoethics*, vol. 3, no. 3, p. 231, 2009.

[28] G. Tsoumakas and I. Vlahavas, *Distributed data mining*. Hershey, 2009, pp. 157–171.

[29] E. P. Xing, Q. Ho, P. Xie, and D. Wei, "Strategies and principles of distributed machine learning on big data," *Engineering*, vol. 2, no. 2, pp. 179–195, 2016.

[30] Z. Ning, P. Dong, X. Wang, M. S. Obaidat, X. Hu, L. Guo, Y. Guo, J. Huang, B. Hu, and Y. Li, "When deep reinforcement learning meets 5g-enabled vehicular networks: A distributed offloading framework for traffic big data," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1352–1361, 2019.

[31] J. J. Dai, Y. Wang, X. Qiu, D. Ding, Y. Zhang, Y. Wang, X. Jia, C. L. Zhang, Y. Wan, Z. Li *et al.*, "Bigdl: A distributed deep learning framework for big data," in *Proceedings of the ACM Symposium on Cloud Computing*, 2019, pp. 50–60.

[32] D. Peteiro-Barral and B. Guijarro-Berdiñas, "A survey of methods for distributed machine learning," *Progress in Artificial Intelligence*, vol. 2, no. 1, pp. 1–11, 2013.

[33] M. A. Alsheikh, S. Lin, D. Niyato, and H. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications," *IEEE Communications Surveys Tutorials*, 2014.

[34] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *AISTATS*, 2017.

[35] C. Anglano and M. Botta, "Now g-net: learning classification programs on networks of workstations," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 5, pp. 463–480, 2002.

[36] M. M. Amiri and D. Gündüz, "Computation scheduling for distributed machine learning with straggling workers," *IEEE Transactions on Signal Processing*, vol. 67, no. 24, pp. 6270–6284, 2019.

[37] D. Caragea, A. Silvescu, and V. Honavar, "Analysis and synthesis of agents that learn from distributed dynamic data sources," in *Emergent neural computational architectures based on neuroscience*. Springer, 2001, pp. 547–559.

[38] M. Stolpe, K. Bhaduri, K. Das, and K. Morik, "Anomaly detection in vertically partitioned data by distributed core vector machines," in *Machine Learning and Knowledge Discovery in Databases*, 2013.

[39] B. Ying, K. Yuan, and A. H. Sayed, "Supervised learning under distributed features," *IEEE Transactions on Signal Processing*, 2019.

[40] T. G. Dietterich, "Ensemble methods in machine learning," in *International workshop on multiple classifier systems*. Springer, 2000, pp. 1–15.

[41] J. Vanschoren, "Meta-learning," in *Automated Machine Learning*. Springer, Cham, 2019, pp. 35–61.

[42] P. Vanhaesebrouck, A. Bellet, and M. Tommasi, "Decentralized Collaborative Learning of Personalized Models over Networks," in *AISTATS*, 2017.

[43] Y. Guo and J. Sutiwaraphun, "Probing knowledge in distributed data mining," in *Pacific-Asia Conference on Knowledge Discovery and Data Mining*. Springer, 1999, pp. 443–452.

[44] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated machine learning: Concept and applications," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, no. 2, pp. 1–19, 2019.

[45] J. Konečný, H. B. McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: Strategies for improving communication efficiency," *arXiv preprint arXiv:1610.05492*, 2016.

[46] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserving distributed machine learning with federated learning," *arXiv preprint arXiv:2004.12108*, 2020.

[47] H. Kargupta, B. Park, D. Hershberger, and E. Johnson, "Collective data mining: A new perspective toward distributed data mining," *Advances in distributed and parallel knowledge discovery*, vol. 2, pp. 131–174, 1999.

[48] Y. Dong, X. Chen, L. Shen, and D. Wang, "Privacy-preserving distributed machine learning based on secret sharing," in *International Conference on Information and Communications Security*. Springer, 2019, pp. 684–702.

[49] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *ACM ASIACCS*, 2017.

[50] J. So, B. Guler, A. S. Avestimehr, and P. Mohassel, "Codedprivateml: A fast and privacy-preserving framework for distributed machine learning," *arXiv preprint arXiv:1902.00641*, 2019.

[51] M. Al-Rubaie and J. M. Chang, "Privacy-preserving machine learning: Threats and solutions," *IEEE Security & Privacy*, vol. 17, no. 2, pp. 49–58, 2019.

[52] F. Tang, W. Wu, J. Liu, H. Wang, and M. Xian, "Privacy-preserving distributed deep learning via homomorphic re-encryption," *Electronics*, vol. 8, no. 4, p. 411, 2019.

[53] Z. Huang, R. Hu, Y. Guo, E. Chan-Tin, and Y. Gong, "Dp-admm: Admm-based distributed learning with differential privacy," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1002–1012, 2019.

[54] X. Wang, H. Ishii, L. Du, P. Cheng, and J. Chen, "Differential privacy-preserving distributed machine learning," in *2019 IEEE 58th Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 7339–7344.

[55] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[56] J. Jeony, D. Kimz, and J. Kim, "Cyclic parameter sharing for privacy-preserving distributed deep learning platforms," in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2019, pp. 435–437.

[57] A. Gascón, P. Schoppmann, B. Balle, M. Raykova, J. Doerner, S. Zahur, and D. Evans, "Privacy-preserving distributed linear regression on high-dimensional data," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 4, pp. 345–364, 2017.

[58] X. Ma, F. Zhang, X. Chen, and J. Shen, "Privacy preserving multi-party computation delegation for deep learning in cloud computing," *Information Sciences*, vol. 459, pp. 103–116, 2018.

[59] S. D. Mainwaring, M. F. Chang, and K. Anderson, "Infrastructures and their discontents: Implications for ubicomp," in *International Conference on Ubiquitous Computing*. Springer, 2004, pp. 418–432.

[60] D. McIntire, T. Stathopoulos, S. Reddy, T. Schmidt, and W. J. Kaiser, "Energy-efficient sensing with the low power, energy aware processing (leap) architecture," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 11, no. 2, pp. 1–36, 2012.

[61] Q. Huang, Y. Mei, W. Wang, and Q. Zhang, "Battery-free sensing platform for wearable devices: The synergy between two feet," in *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, 2016, pp. 1–9.

[62] M.-g. Kim, H. Alrowais, C. Kim, P. Yeon, M. Ghovanloo, and O. Brand, "All-soft, battery-free, and wireless chemical sensing platform based on liquid metal for liquid-and gas-phase voc detection," *Lab on a Chip*, vol. 17, no. 13, pp. 2323–2329, 2017.

[63] M. F. Balcan, A. Blum, S. Fine, and Y. Mansour, "Distributed learning, communication complexity and privacy," in *Conference on Learning Theory*, 2012, pp. 26–1.

[64] Z. Lu, M. Dai, K. Xu, J. Chen, and Y. Liao, "A high precision, fast response, and low power consumption in situ optical fiber chemical pco2 sensor," *Talanta*, vol. 76, no. 2, pp. 353–359, 2008.

[65] A. Varshney, A. Soleiman, L. Mottola, and T. Voigt, "Battery-free visible light sensing," in *Proceedings of the 4th ACM Workshop on Visible Light Communication Systems*, 2017, pp. 3–8.

[66] N. Arora and G. D. Abowd, "Zeusss: Zero energy ubiquitous sound sensing surface leveraging triboelectric nanogenerator and analog backscatter communication," in *The 31st Annual ACM Symposium on User Interface Software and Technology Adjunct Proceedings*, 2018, pp. 81–83.

[67] D. Gordon, H. R. Schmidtke, M. Beigl, and G. von Zengen, "A novel micro-vibration sensor for activity recognition: Potential and limitations," in *ISWC*, 2010.

[68] S. Sigg, D. Gordon, G. von Zengen, M. Beigl, S. Haseloff, and K. David, "Investigation of context prediction accuracy for different context abstraction level," *IEEE Transactions on Mobile Computing (TMC)*, 2012.

[69] Y. Lee, D. Blaauw, and D. Sylvester, "Ultralow power circuit design for wireless sensor nodes for structural health monitoring," *Proceedings of the IEEE*, vol. 104, no. 8, pp. 1529–1546, 2016.

[70] T. Jang, G. Kim, B. Kempke, M. B. Henry, N. Chiotellis, C. Pfeiffer, D. Kim, Y. Kim, Z. Foo, H. Kim *et al.*, "Circuit and system designs of ultra-low power sensor nodes with illustration in a miniaturized gnss logger for position tracking: Part i—analog circuit techniques," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2237–2249, 2017.

[71] A. Raj and D. Steingart, "Power sources for the internet of things," *Journal of the Electrochemical Society*, vol. 165, no. 8, p. B3130, 2018.

[72] S. Chalasani and J. M. Conrad, "A survey of energy harvesting sources for embedded systems," in *IEEE SoutheastCon 2008*. IEEE, 2008, pp. 442–447.

[73] S. Sudevalayam and P. Kulkarni, "Energy harvesting sensor nodes: Survey and implications," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 3, pp. 443–461, 2010.

[74] T. Ghomian and S. Mehraeen, "Survey of energy scavenging for wearable and implantable devices," *Energy*, vol. 178, pp. 33–49, 2019.

[75] M. A. Andersson, A. Özçelikkale, M. Johansson, U. Engström, A. Vorobiev, and J. Stake, "Feasibility of ambient rf energy harvesting for self-sustainable m2m communications using transparent and flexible graphene antennas," *IEEE Access*, vol. 4, pp. 5850–5857, 2016.

[76] M. A. Razzaque and S. Dobson, "Energy-efficient sensing in wireless sensor networks using compressed sensing," *Sensors*, vol. 14, no. 2, pp. 2822–2859, 2014.

[77] D. L. Donoho, "Compressed sensing," *IEEE Transactions on information theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[78] Y. C. Eldar and G. Kutyniok, *Compressed sensing: theory and applications*. Cambridge university press, 2012.

[79] V. Talla, M. Hessar, B. Kellogg, A. Najafi, J. R. Smith, and S. Gollakota, "Lora backscatter: Enabling the vision of ubiquitous connectivity," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 2017.

[80] P. San Cheong, J. Bergs, C. Hawinkel, and J. Famaey, "Comparison of lorawan classes and their power consumption," in *2017 IEEE symposium on communications and vehicular technology (SCVT)*. IEEE, 2017, pp. 1–6.

[81] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith, "Passive wi-fi: Bringing low power to wi-fi transmissions," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, 2016, pp. 151–164.

[82] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power consumption analysis of bluetooth low energy, zigbee and ant sensor nodes in a cyclic sleep scenario," in *2013 IEEE International Wireless Symposium (IWS)*. IEEE, 2013, pp. 1–4.

[83] B. Reynders and S. Pollin, "Chirp spread spectrum as a modulation technique for long range communication," in *2016 Symposium on Communications and Vehicular Technologies (SCVT)*. IEEE, 2016, pp. 1–5.

[84] M. N. Ochoa, A. Guizar, M. Maman, and A. Duda, "Evaluating lora energy efficiency for adaptive networks: From star to mesh topologies," in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2017, pp. 1–8.

[85] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, no. 10, pp. 1196–1204, Oct 1948.

[86] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Communications Surveys Tutorials*, 2018.

[87] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Improving backscatter radio tag efficiency," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 6, pp. 1502–1509, 2010.

[88] M. Hessar, A. Najafi, and S. Gollakota, "Netscatter: Enabling large-scale backscatter networks," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, 2019.

[89] A. Varshney, C. Pérez-Penichet, C. Rohner, and T. Voigt, "Lorea: A backscatter architecture that achieves a long communication range," in *ACM Conference on Embedded Network Sensor Systems*, 2017.

[90] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: Detection and performance analysis," *IEEE Transactions on Communications*, vol. 64, no. 11, pp. 4836–4846, 2016.

[91] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: wireless communication out of thin air," *ACM SIGCOMM Comp. Comm. Rev.*, 2013.

[92] R. Zhao, F. Zhu, S. Peng, Y. Feng, X. Tian, H. Yu, and X. Wang, "Ofdma-enabled wi-fi backscatter," in *25th Annual International Conference on Mobile Computing and Networking.*, 2019.

[93] P. Zhang, M. Rostami, P. Hu, and D. Ganesan, "Enabling practical backscatter communication for on-body sensors," in *Proceedings of the 2016 ACM SIGCOMM Conference*, 2016.

[94] Á. San-Salvador and Á. Herrero, "Contacting the devices: a review of communication protocols," in *Ambient Intelligence-Software and Applications*. Springer, 2012, pp. 3–10.

[95] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[96] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: a secure sensor network communication architecture," in *2007 6th International Symposium on Information Processing in Sensor Networks*. IEEE, 2007, pp. 479–488.

[97] V. Chawla and D. S. Ha, "An overview of passive rfid," *IEEE Communications Magazine*, vol. 45, no. 9, pp. 11–17, Sep. 2007.

[98] A. N. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 4, pp. 619–630, 2014.

[99] P. Jakimovski, H. R. Schmidtke, S. Sigg, L. W. F. Chaves, and M. Beigl, "Collective communication for dense sensing environments," *Journal of Ambient Intelligence and Smart Environments*, vol. 4, no. 2, pp. 123–134, 2012.

[100] F. Peper, K. Leibnitz, J.-n. Teramae, T. Shimokawa, and N. Wakamiya, "Low-complexity nanosensor networking through spike-encoded signaling," *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 49–58, 2015.

[101] A. Giridhar and P. R. Kumar, "Toward a theory of in-network computation in wireless sensor networks," *IEEE Communications Magazine*, 2006.

[102] M. Goldenbaum, H. Boche, and S. Stanczak, "Analog computation via wireless multiple-access channels: Universality and robustness," in *IEEE ICASSP*, 2012.

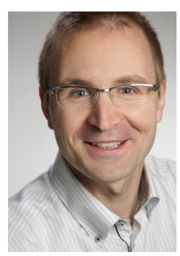
[103] M. Goldenbaum and S. Stanczak, "Robust analog function computation via wireless multiple-access channels," *IEEE Transactions on Communications*, vol. 61, no. 9, pp. 3863–3877, 2013.

[104] ——, "On the channel estimation effort for analog computation over wireless multiple-access channels," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 261–264, 2014.

[105] G. Zhu and K. Huang, "Mimo over-the-air computation for high-mobility multimodal sensing," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6089–6103, 2018.

[106] S. Sigg, P. Jakimovski, Y. Ji, and M. Beigl, "Utilising an algebra of random functions to realise function calculation via a physical channel," in *SPAWC*, 2013.
[107] K. Ralinovski, M. Goldenbaum, and S. Stańczak, "Energy-efficient classification for anomaly detection: The wireless channel as a helper," in *IEEE ICC*, 2016.
[108] S. Sigg, L. Zhong, and Y. Ji, "Activity recognition with implicit context classification," in *CAPS*, 2012.
[109] M. Frey, I. Bjelakovic, and S. Stanczak, "Over-the-air computation for distributed machine learning," *arXiv preprint arXiv:2007.02648*, 2020.
[110] T. M. Mitchell, *Machine learning*, ser. McGraw Hill Series in Computer Science. McGraw-Hill, 1997.
[111] L. Bottou, F. Curtis, and J. Nocedal, "Optimization methods for large-scale machine learning," *SIAM Review*, 2018.
[112] M. D. Springer, *The algebra of random variables*, ser. Wiley series in probability and mathematical statistics, R. A. Bradley, J. S. Hunter, D. G. Kendall, R. G. Miller, and G. S. Watson, Eds. Wiley, 1979.
[113] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research," in *International Symposium on Information Processing in Sensor Networks*, 2005.
[114] M. Ku, W. Li, Y. Chen, and K. J. R. Liu, "Advances in energy harvesting communications: Past, present, and future challenges," *IEEE Communications Surveys Tutorials*, 2016.
[115] L. M. Candanedo and V. Feldheim, "Accurate occupancy detection of an office room from light, temperature, humidity and co2 measurements using statistical learning models," *Energy and Buildings*, 2016.
[116] M. F. Duarte and Y. H. Hu, "Vehicle classification in distributed sensor networks," *J. Parallel Distrib. Comput.*, 2004.
[117] Y. Peng, L. Shangguan, Y. Hu, Y. Qian, X. Lin, X. Chen, D. Fang, and K. Jamieson, "Plora: A passive long-range data network from ambient lora transmissions," in *Proceedings of the 2018 Conference of the ACM Special Interest Group on Data Communication*, 2018.
[118] G. Gobieski, N. Beckmann, and B. Lucia, "Intelligence beyond the edge: Inference on intermittent embedded systems," in *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems*, 2019.
[119] K. Klues, V. Handziski, C. Lu, A. Wolisz, D. Culler, D. Gay, and P. Levis, "Integrating concurrency control and energy management in device drivers," in *Proceedings of Twenty-first ACM SIGOPS Symposium on Operating Systems Principles*, 2007.
[120] G. de Meulenaer, F. Gosset, F. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 2008.
[121] A. Dongare, C. Hesling, K. Bhatia, A. Balanuta, R. L. Pereira, B. Iannucci, and A. Rowe, "Openchirp: A low-power wide-area networking architecture," in *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, March 2017, pp. 569–574.
[122] B. Martinez, M. Montón, I. Vilajosana, and J. D. Prades, "The power of models: Modeling power consumption for iot devices," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5777–5789, 2015.
[123] Z. Yang, Q. Huang, and Q. Zhang, "Nicscatter: Backscatter as a covert channel in mobile devices," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017.
[124] G. Vougioukas and A. Bletsas, "Switching frequency techniques for universal ambient backscatter networking," *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 2, pp. 464–477, Feb 2019.
[125] D. Nilsson, T. Kugler, P.-O. Svensson, and M. Berggren, "An all-organic sensor–transistor based on a novel electrochemical transducer concept printed electrochemical sensors on paper," *Sensors and Actuators B: Chemical*, vol. 86, no. 2, pp. 193–197, 2002.
[126] R. Zhang and C. K. Ho, "Mimo broadcasting for simultaneous wireless information and power transfer," *IEEE TWC*, vol. 12, no. 5, 2013.
[127] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," *IEEE TC*, vol. 61, no. 11, 2013.
[128] M. Stoopman, S. Keyrouz, H. Visser, K. Philips, and W. Serdijn, "A self-calibrating rf energy harvester generating 1v at- 26.3 dbm," in *IEEE VLSIC*, 2013.
[129] M. Stoopman, S. Keyrouz, H. J. Visser, K. Philips, and W. A. Serdijn, "Co-design of a cmos rectifier and small loop antenna for highly sensitive rf energy harvesters," *IEEE J of Solid-State Circuits*, vol. 49, no. 3, 2014.
[130] F. Sangare and Z. Han, "Rf energy harvesting networks: Existing techniques and hardware technology," in *Wireless Information and Power Transfer: A New Paradigm for Green Comm.* Springer, 2018, pp. 189–239.
[131] T. B. Lim, N. M. Lee, and B. K. Poh, "Feasibility study on ambient rf energy harvesting for wireless sensor network," in *IEEE IMWS-BIO*, 2013.
[132] F. Tramèr, F. Zhang, A. Juels, M. K. Reiter, and T. Ristenpart, "Stealing machine learning models via prediction apis," in *Proceedings of the 25th USENIX Conference on Security Symposium*, 2016.
[133] R. P. Brent, "Fast multiple-precision evaluation of elementary functions," *JACM*, vol. 23, no. 2, 1976.
[134] D. E. Knuth, *The Art of Computer Programming*. Addison Wesley, 1997, vol. 2.
[135] W. Lee, S. J. Stolfo, and K. W. Mok, "Mining in a data-flow environment: Experience in network intrusion detection," 1999.
[136] R. M. Mohammad, F. Thabtah, and L. McCluskey, "An assessment of features related to phishing websites using an automated technique," in *Conference for Internet Technology and Secured Transactions*, 2012.

Le Ngu Nguyen is a doctoral student at Ambient Intelligence Group, Aalto University. He completed his bachelor's and master's degree at University of Science, Ho Chi Minh City, Vietnam. His research focuses on usable security and distributed machine learning.



Stephan Sigg received his M.Sc. degree in computer science from TU Dortmund, in 2004. and his Ph.D. degree from Kassel University, in 2008. Since 2015 he is an assistant professor at Aalto University, Finland. He has served as a TPC member of many conferences including IEEE PerCom, Ubicomp, etc. His research interests include Pervasive Computing, activity recognition, usable security and optimization of algorithms in mobile distributed systems.

Jari Lietzén received his M.Sc. degree (with distinction) in Communication Engineering from Aalto University, Finland in 2016. Currently he is pursuing doctoral studies at Aalto University. His research interests include error correction and key growing protocols in quantum key distribution and backscatter communications.

Rainhard D. Findling received his BSc/MSc (2011/2013) in Engineering from the University of Applied Sciences Upper Austria, Campus Hagenberg and his PhD (2017) at the JKU Johannes Kepler University Linz, Austria. From 2017 to 2019 he has been with the Ambient Intelligence Group at Aalto University, Finland, in the Department of Communications and Networking, at the School of Electrical Engineering. His research areas are machine learning and data analysis in mobile environments, such as mobile security and (biometric) authentication, behavior, or other types of patterns such as location fingerprinting.

Kalle Ruttik Kalle Ruttik received his Dipl. Engineer degree from Tallinn Technical University in 1993 Lic. Tech Degree from TKK (former Aalto University) in 1999 and D.Sc. (Tech) Degree from Aalto University in 2011. Since 2015 he is university teacher at Aalto University. His teaching and research interest include software defined radio, low power radio communication, cloud based radio access network.