Talking When No One is Listening: Piggybacking City-scale IoT Control Signals Over LTE

Kunal Sankhe, Ufuk Muncuk, M. Y. Naderi, and Kaushik Chowdhury
Electrical and Computer Engineering Department, Northeastern University, Boston, MA, USA
Email: sankhe.ku@husky.neu.edu, umuncuk@coe.neu.edu, naderi@coe.neu.edu, krc@ece.neu.edu

***Abstract*—This paper presents FreeIoT, a control plane paradigm that allows fine grained signaling for city-scale IoT deployments without installing any additional infrastructure. FreeIoT overlays control/wake-up information for sensors over existing standards compliant LTE through the following contributions: First, we develop a novel encoding scheme that changes the spatial positioning of Almost Blank Subframes (ABS) within a standard LTE frame to convey control information. ABS was originally defined in the standard to allow coexistence between the macro-cell eNB and nearby small cells, which FreeIoT leverages as a side channel for IoT signaling. Our approach works with any number of ABS settings chosen by the LTE eNB, and accordingly adjusts the encoding of control messages at maximum possible transmission rates. Second, a session management protocol is introduced to maintain contextual information of the control signaling. This allows FreeIoT to handle situations where the control message may span multiple frames, or when the LTE operator temporarily reduces the number of ABS. FreeIoT also incorporates an error detection and correction mechanism to counter channel and fading errors. Finally, we implement a proof of concept testbed to validate the operation of FreeIoT using a software defined LTE eNB and custom-designed RF energy harvesting circuit interfaced with off-the-shelf sensors.**

I. Introduction

The Internet of Things (IoT) revolution is rapidly altering our vision of collecting and analyzing real time data to optimize applications and services related to transportation, environmental monitoring, security, among others. The success of the IoT paradigm rests on (i) the ability to deploy sensors at scale, in the order of thousands of devices spread across the city [1], and (ii) controlling their operations in a coordinated manner to retrieve data of interest only when needed. These dual considerations require simple design of the sensor hardware, efficient wake-up and signaling mechanisms to ensure on-demand energy consumption, and low operational cost of the infrastructure that will perform the data querying. So far, there is no clear pathway for supporting city-scale IoT control operations: standards are still-evolving, diverse heterogeneous sensor and radio platforms introduce compatibility issues, licensing dedicated spectrum and maintaining an IoT control infrastructure is difficult for resource strapped public entities, like city administration. Our approach, called FreeIoT, challenges this status quo by allowing any type of deployed sensor (even without an LTE modem) to be controlled with today's standards-compliant LTE infrastructure.

A. FreeIoT Operational Overview

FreeIoT is a radically different approach that results in an *infrastructure-free* IoT deployment, with the only operational cost being that of installing and maintaining the physical sensors. The high level idea is simple, as illustrated by the network architecture in Fig. 1a: The deployed sensors are off-the-shelf products that remain in a default energy conserving deep sleep state, unless woken up with specific directives. Sensors may have any type of on-board radio, ranging from ultra-low power Bluetooth Low Energy chips for proximity-based data reporting or long-range narrow-band transmission radios like LORA/Sigfox [2], [3]. FreeIoT poses no constraints on the sensor design, save that its on-board microcontroller accept an external hardware interrupt to wake-up the main radio. The framework of freeIoT is shown in Fig. 1b. The control/wake-up information for the IoT network is conveyed by changing the spatial positioning of the Almost Blank Subframes (ABS) within a standard LTE frame. We call this technique as ABS index modulation (AIM). ABS is currently incorporated in LTE Release 10 onwards, where certain subframes do not carry data to facilitate interference-free picocell operation [4]. Our proposed wake-up module based on RF harvesting technology will deliver overlay control signals when interfaced with the sensor. As shown in Fig. 2, LTE users (for example UE_2) located in an expanded cell region of the small cell are scheduled within ABS, whereas the remaining subframes are allocated to the users (such as UE_1) within the macro-cell.

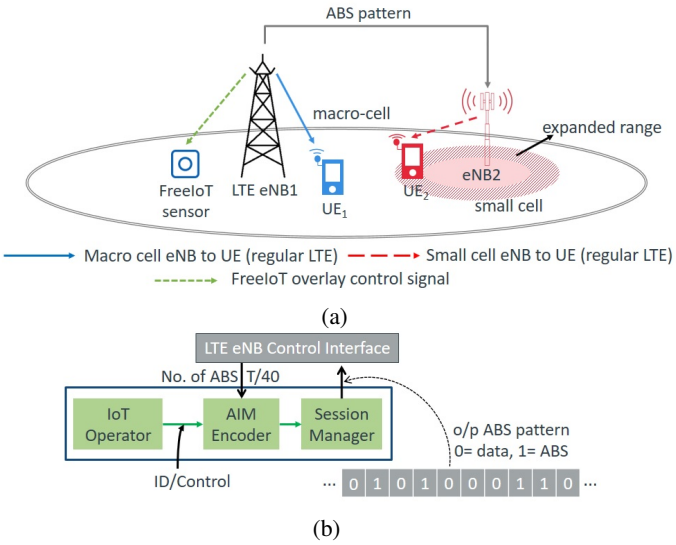


Figure 1: (a) LTE network with the eNB and a given small cell, with spectrum sharing through ABS subframes, (b) FreeIoT framework: The control/wake-up information is conveyed by the position of ABS within a standard LTE frame.

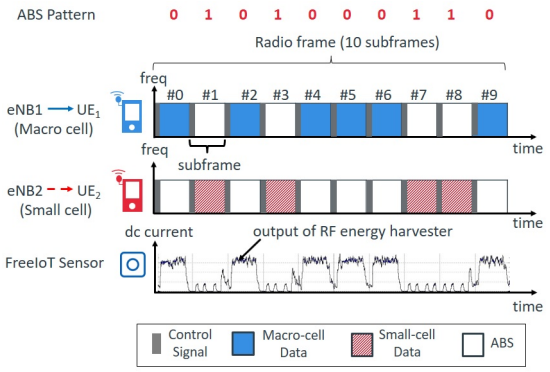


Figure 2: Use of ABS to serve cell edge users of the small cell. FreeIoT sensors detect the ABS pattern using an RF energy harvester.

LTE operators freely set the macro-cell ABS patterns that best serve their network need. FreeIoT introduces an automatic rate adaptation mechanism to correctly interpret the implications of the ABS locations. This allows the LTE operator full freedom in deciding the number of ABS, while overlaying control messages for an entirely different IoT network.

B. FreeIoT Innovation and Contributions

We briefly discuss the practicality and innovation of the FreeIoT design in this section: The systems level innovation lies in the design of the wake-up module that interfaces within the sensors. This module itself is composed of an adaptive decoder functional block and an RF energy harvester (RF-EH) circuit that is designed to operate in the LTE frequency band of 700 MHz with high sensitivity to the changing signal patterns within the LTE subframes. To enable decoding, the circuit must respond in a short time window of 1 ms that corresponds to a single LTE subframe, registering a discrete 'high' (ABS absent = 0) or 'low' (ABS present = 1) pulse that is an input to the adaptive decoding block. We conducted a set of experiments to test the sensitivity of our designed RF-EH circuit. RF-EH was allowed to harvest energy transmitted by an RF source in an alternate 1 ms periods using ON-OFF keying (OOK) modulation. Fig. 3 confirms that RF-EH has high sensitivity and fast responsiveness to the ON/OFF transitions (rise/fall time is of the order of a few tens of μs).

The proposed AIM technique of encoding the IoT control signals within the ABS positions at the LTE eNB operates seamlessly for any choice of ABS in the window (7, 19) per 40 subframes.This window sits comfortably within typical ABS selections in the range of 8–15 subframes [5]. We recall that ABS patterns are signaled in the form of bitmaps indicated on a total length 40 subframes (hence, the choice of 40 above), or over 4 frames. This number can change every set of 40 subframes, e.g., 10 in set 1, 15 in set 2, and so on. Thus, FreeIoT should not require static mapping of a particular ABS configuration to a corresponding sensor ID and control signal. Furthermore, as IoT deployments evolve, it is certainly possible that the downlink control information is composed of lengthy codewords.For flexibility, FreeIoT must incorporate a session management protocol that allows unrestrained downlink data capability, spanning across multiple sets of 40 subframes.

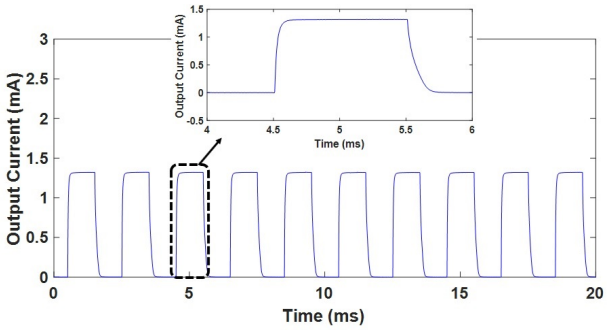


Figure 3: The output current of RF-EH with RF input signal transmitted using OOK modulation with period 1 ms.

In summary, the contributions of this paper are as follows: (i) We present FreeIoT, a novel communication framework that allows overlaying control information for IoT over an existing standards compliant LTE eNB without any hardware modifications to existing LTE infrastructure. (ii) We develop a novel encoding scheme, called ABS-index modulation (AIM), which allows encoding signals by spacing ABS within a set of 40 subframes. AIM adjusts to the number of ABS chosen by the eNB seamlessly through automatic rate adaptation, and also has a session management protocol for spanning signaling over multiple sets of frames, or handling possible interruptions caused by complete absence of ABS. We integrate an ABS-code error detection and correction mechanism by introducing ABS parity frame that will be transmitted along the information bits and enhance system resiliency against channel and fading errors. (iii) We implement a proof-of-concept testbed which shows FreeIoT operation using an LTE eNB and RF energy harvesting circuits interfaced with off-the-shelf TI eZ430-RF2500 sensor, with comprehensive analysis of its practical performance.

II. FreeIoT Framework Design

This section presents the details of FreeIoT, covering the (i) ABS index modulation (AIM) concept, (ii) AIM encoding with dynamic ABS patterns, (iii) session management protocol, (iv) adaptive overlay decoding, and (v) ABS-Code error correction technique.

A. ABS Index Modulation (AIM) Concept

In this section, we introduce ABS index modulation (AIM), used by FreeIoT to encode overlaying control/wake-up information directed towards the sensors without disrupting the LTE downlink transmissions. Consider a standard LTE frame composed of 10 subframes, each indexed as $0, 1, \ldots, 9$. As per the LTE standard specification, 0^{th} and 5^{th} subframes carry the primary and secondary synchronization signals for LTE UEs. AIM ignores these subframes as *don't care* subframes. This implies that the information bits are mapped to the remaining 8 subframes, depending upon the presence or absence of ABS in

Table I: Summary of AIM rate-dependent settings

Rate	Min ABS	Max ABS	Overlaid Bits	Throughput (bps)
$R=1$	7	13	9	225
$R=2$	10	16	12	300
$R=3$	13	19	15	375

each of them. A single ABS within the LTE frame represents 3 bits of information (if one ABS is present in a subframe, then that location =1, the rest are 0). Extending this concept, if r is the available number of ABS within a frame, the number of possible combinations is $\binom{8}{r}$. To convey information in binary format, the number of combinations must be power of two, and so $N = 2^k$ combinations are used to transmit 'k' information bits, where $k = \lfloor \log_2 \binom{8}{r} \rfloor$.

The number of ABS allocated for a set of 40 subframes (or 4 LTE frames) is known at a time, but this can also vary dynamically in future 40-subframe sets. This change occurs with varying number of cell-edge users or throughput requirements. Thus, static mapping of ABS that represents fixed rate encoding is not a suitable solution for FreeIoT. We next introduce an automatic rate adaptation technique, which allows the AIM module to seamlessly adapt to the time-changing number of ABS as per the LTE operator's choices.

B. AIM Encoding with Dynamic ABS Patterns

Out of four LTE frames, one frame is configured to convey a rate-defining preamble, called as *R-preamble*. It not only indicates the beginning of overlay data transmission, but also helps the receiver to determine the rate of control signal transmission. Out of the total available ABS (T), we allocate four ABS to represent different types of *R-preamble*. The remaining $(T-4)$ ABS are distributed among other three frames carrying overlay control data.

We first allocate $R = \text{int}\big((T-4)/3\big)$ ABS in each of these three frames. As shown in Fig. 4, AIM maps a block of 'k' information bits to various ABS locations (henceforth referred as *indexes*) using the mapping table of R ABS, where $k = \lfloor \log_2 \binom{8}{R} \rfloor$. Since the total number of combinations $\binom{8}{R}$ decreases for $R > 4$, we limit the rate R to 3. Additionally, the remaining $M = \big((T-4) \mod 3\big)$ ABS are assigned to the *don't care* 0^{th} and 5^{th} subframes within any of three overlay data frames.

As an example, assuming the total number of available ABS $T = 10$, the encoding rate would be selected as $R = \text{int}\big((10-4)/3\big) = 2$ and $M = 0$. Using the ABS mapping table, FreeIoT maps $k = 4$ information bits to positions of $R = 2$ ABS within each overlay data frame. Information bits '0010' are mapped to ABS index '1' and '4' within the first overlay data frame, information bits '1111' are mapped to ABS positions '3' and '7' in the second frame, whereas information bits '0111' are mapped to ABS index '2' and '3' in the third frame.

In order to support rate R, FreeIoT requires a certain minimum number of ABS and supports a specific maximum number of ABS. For example, 4 ABS represents $1-preamble$ and 3 ABS distributed in three overlay data frames. Thus,

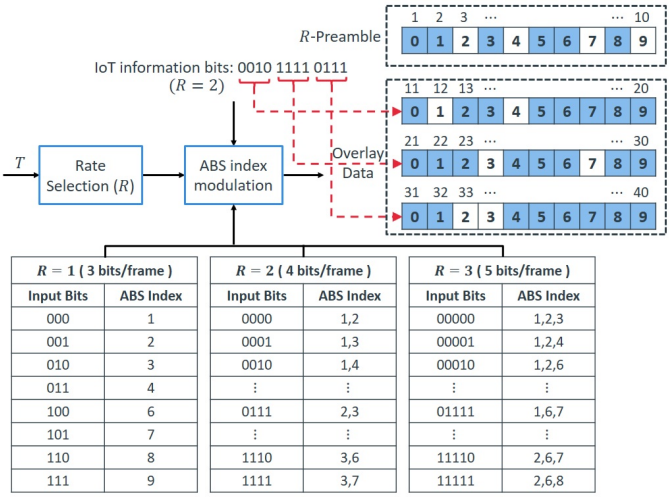


Figure 4: Illustrating rate adaptive ABS Index Modulation. For e.g., for $R = 2$, information bits '0010' map to ABS index of '1' and '4' within LTE frame.

minimum of 7 ABS and maximum 10 ABS (i.e. 4 ABS for $R-preamble$, 1 ABS to represent data, and 2 ABS in *don't care* subframes in each of three overlay data frames) would be supported by $R = 1$. The rate R allows transmission of 'k' information bits per overlay data frame, where $k = \lfloor \log_2 \binom{8}{R} \rfloor$. For e.g., $R = 2$ allows transmission of 4 information bits per frame, i.e., total of $4 \times 3 = 12$ information bits in three overlay data frames. Since, $R-preamble$ does not carry any useful information, the total of $k \times 3$ information bits are transmitted in 40 subframes, which has total duration of $40ms$. The throughput in bits per second (bps) can be calculated as $(k \times 3)/(40ms) = k \times 75$ bps. Table I summarizes the minimum number of ABS required, maximum number of ABS supported, useful information bits transmitted in 40 subframes, and throughput in bps for different rates.

C. Session Management Protocol

FreeIoT needs to maintain contextual information of the signaling, as control directives may be spread over multiple 40 subframe sets. We call the complete addressing and information delivery interval for any one IoT device as a *session*. We next show how FreeIoT constructs sessions to span multiple LTE frames, and when sufficient numbers of ABS are not available, manages interruptions within the session. To incorporate a session-oriented protocol, we define few additional reserved control signals: '`SYNC`' to synchronize IoT sensors, '`ID`' a unique identifier for the targeted receiver, '`R-Preamble`' to indicate the beginning of data transmission and to inform the rate R, '`Overlay Control`' which contains information for the receiver IoT and '`END`' to terminate the session for that device.

The start of a session begins by alerting all IoT devices that control information is soon to follow. To this end, FreeIoT encodes an ABS pattern as *Barker sequence* [6] within `SYNC` frame. We select Barker sequence of length 13 ('$+1+1+1+1+1-1-1+1+1-1+1-1+1$', where $+1$:

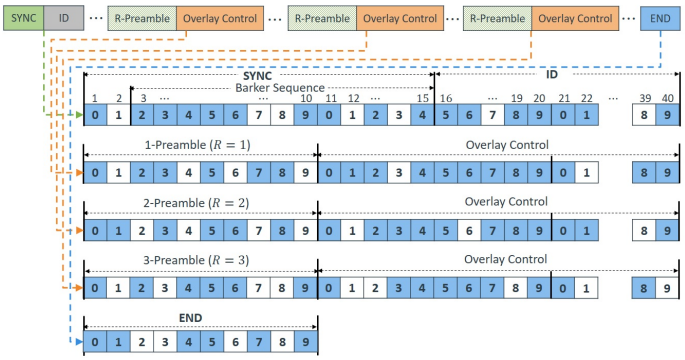


Figure 5: Session management using control signals `SYNC`, `ID`, `R-Preamble`, `Overlay Control` and `End`.

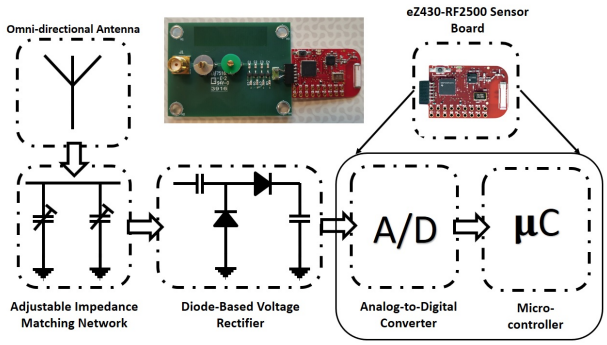


Figure 6: The circuit schematic of FreeIoT receiver.

ABS absent, -1: ABS present), as it has strong autocorrelation properties and is frequently used for synchronization in various practical communication systems. As shown in Fig. 5, 5 ABS are allocated in the first 15 subframes to represent `SYNC`. The remaining available ABS are allocated in the subsequent 25 subframes in `ID`. Out of these 25 subframes, we ignore 0^{th} and 5^{th} don't care subframes. ID is represented within the remaining 20 subframes using a combination of 5 ABS indexes. Accordingly, FreeIoT can support maximum of up to $\binom{20}{5} = 15504$ different sensors, each with a unique ID per base-station. Once each sensor detects the `SYNC`, it matches the ABS pattern in the subsequent subframes representing `ID` with sensor's own unique ID pattern. If the `ID` is a match, the corresponding IoT sensor will start the session. Otherwise, it will wait for the next `SYNC`.

FreeIoT informs the change in the ABS-depending information rate to the sensor, so that the latter may correctly decode the bit pattern corresponding to the ABS locations. In order to cope with such situations, we define three separate preambles, i.e., `1-Preamble`, `2-Preamble`, and `3-Preamble`, for $R = 1$, $R = 2$, and $R = 3$ respectively. In this revised model, the preamble not only indicates the start of the next overlay control signal, but also informs the rate of transmission. The knowledge of R helps the receiver to select appropriate ABS mapping table to decode the information. The ABS patterns for each preamble are shown in Fig. 5.

`Overlay Control` consists of 3 frames, which carries the control information for a specific IoT sensor identified by the `ID`. AIM maps a group of information bits to the index of R ABS within each frame. Recall that 0^{th} and 5^{th} subframes are *don't care* subframes since they are not used while encoding. The remaining number of ABS left after encoding can be scheduled in these positions if necessary. Finally, `END` frame indicates the end of session. The sensor terminates its own reception session once it receives `END`, and waits for the next `SYNC`.

III. Receiver Energy Harvesting and Decoding

FreeIoT relies on a custom-designed RF-EH circuit interfaced with an off-the-shelf sensor [7]. The harvester extracts and interprets the energy in the incident LTE signal, and then wakes up the sensor/main radio through hardware interrupts when the received energy levels match a pre-decided reference. Fig. 6 shows a high level schematic and fabricated circuit connected to a Texas Instruments (TI) eZ430-RF2500 sensor.

A. Harvesting in LTE Bands

Our basic RF-EH design is updated in FreeIoT with an adjustable impedance matching network, which allows tuning the harvester at the center frequency of the desired LTE 700 MHz band (734-756 MHz) with bandwidth up to 2 MHz. The diode-based voltage rectifier removes the carrier frequency from the received LTE signal and converts the incident power into electrical current. Since the output current linearly varies with the input power, it can capture the variations in power levels due to the presence or absence of ABS. The output current is sampled using harvester's analog-to-digital converter (ADC) to perform simple averaging and comparison. The voltage multiplier is a fully passive circuit that consumes zero power, whereas the state-of-the-art ADC and micro-controller consumes significantly low power in the order of few tens of μW [8] thereby allowing the RF-EH to operate as an energy neutral device.

B. Detecting Presence or Absence of ABS

Fig. 7 summarizes how the output of the RF-EH is used to detect the presence or absence of ABS, which is the first step in decoding. To overcome the effect of noise and channel-induced signal fluctuations in the output current of the RF-EH, the on-board ADC computes a moving average across N samples to smoothen these variations. In order to minimize errors in the decision of presence/absence of ABS, the receiver must know a valid threshold value and a reference sampling instance so that it can make a decision after comparing the output with the threshold.

In order to find these reference points, the receiver executes Algorithm 1, which finds dominant peaks across the moving average output. Once the peak is detected, the corresponding peak amplitude and peak location are stored. The decision threshold is set to half of the peak amplitude, whereas the peaks give the best sample instances (decision instances) for the decision (line 6). At these decision instances, the output of the moving average is compared with the threshold to determine the presence or absence of ABS (line 12). If it is

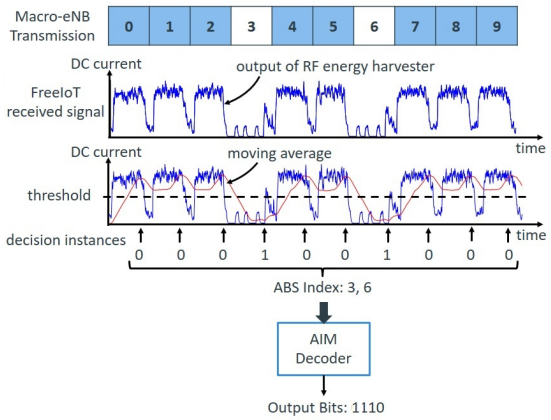


Figure 7: An example of detecting the presence or absence of ABS using the output of RF-EH.

Algorithm 1 To detect the presence or absence of ABS

Input : $e(k)$; RF energy harvester output samples
Output: $y(n)$; 0: ABS is absent 1: ABS is present
Initialize: $N, M, L, interval, stop\_find \leftarrow false$

while RF-EH listening is enable **do**
  $avg(k) \leftarrow avg(k-1) + \frac{1}{N}e(k)$
  if $(stop\_find == false)$ **then**
    $[peak\_loc, peak\_amp] \leftarrow peak\_detection(avg(k-M+1:k))$
    if $peak\_loc$ *is not empty* **then**
      $threshold \leftarrow peak\_amp/2$, $dec\_instance \leftarrow peak\_loc$,
      $stop\_find \leftarrow true$
    end if
  end if
  if $(dec\_instance$ *is not empty*$)$ **then**
    if $(k == dec\_instance)$ **then**
      if $(avg(k) < threshold)$ **then**
        $y(n) \leftarrow 1$
      else
        $y(n) \leftarrow 0$
      end if
      $n \leftarrow n+1$, $dec\_instance \leftarrow dec\_instance + interval$
    end if
  end if
  $k \leftarrow k+1$
  if $(k\%L == 0)$ **then**
    $stop\_find \leftarrow false$
  end if
end while

less than the threshold, ABS is present in the subframe, else it is a regular LTE data subframe with higher energy subcarriers. The decision is stored in $y(n)$, where '0' represents absence of ABS and '1' represents presence of ABS. In addition, since the receiver knows the sampling frequency, it can easily set the next decision instance by introducing a fixed time delay (equal to number of samples in 1 subframe duration). Therefore, the receiver can disable the peak detection function for next several samples, once the dominant peak is found. However, to periodically update the threshold value, Algorithm 1 enables the peak detection function after an interval of L samples.

• **Detecting sync, R-preamble and AIM Decoder:** Here, we describe how FreeIoT receiver uses a sequence of ABS decisions $y(n)$ to initiate and maintain the session, as well as to decode the overlay control information. In order to follow the session management protocol, consider four states, namely: *waiting_sync*, *matching_ID*, *waiting_preamble*, *msg_in_progress*. In the *waiting_sync* state, the receiver is waiting for a SYNC. Upon receiving the ABS decision $y(n)$, the receiver compares a sequence of ABS decisions (comprising of current $y(n)$ and its previous 14 values) with a known binary sequence *sync_pattern*. A *sync_pattern* is defined as '01000001100101', which represents the ABS pattern within SYNC, including the Barker sequence of length 13. Once the *sync_pattern* is detected, the receiver switches to *matching_ID* state. In this state, the receiver stores the ABS decision values $y(n)$ in a buffer till it completely receives decision values of the remaining 25 subframes, which represents ID control frame. As defined by the protocol, a unique ID for each sensor is represented by the positions of 4 ABS within 20 subframes, which is stored in the bit pattern as *sensorID*. By removing bits from the buffer corresponding to don't care subframe positions, the extracted 20 bits of *ID* are compared with *sensorID*. If they match, the receiver switches to *waiting_preamble* state, else the receiver interprets that the message is not intended for it and therefore, switches to *waiting_sync*. In the *waiting_preamble* state, the receiver waits for the rate-aware *R-preamble* using the ABS pattern of 10 subframes. Therefore, the receiver stores the current ABS decision $y(n)$ along with previous 9 values in a preamble buffer. It is then compared with *R-preamble* for each rate $R = 1, 2,$ and 3. Once it is matched with either of the *R-preamble*, the receiver switches to $msg\_in\_progress$ state and stores the information of rate R. The knowledge of the rate R helps the receiver to select the ABS mapping table. In $msg\_in\_progress$ state, the receiver first buffers 10 values of ABS decisions $y(n)$ in *buffer_frame*, since information is overlaid in ABS index within each overlay data frame i.e. 10 subframes. The bit sequence in *buffer_frame* is mapped to the index of ABS, while ignoring the index of 0^{th} and 5^{th} subframes. Using the ABS mapping table for rate R, the ABS indexes are decoded into information bits.

C. ABS-Code Error Detection and Correction

Since the control information is overlaid in the position of the ABS, even a single detection error can result in erroneous interpretation of the entire frame. In the following, we describe an error detection and correction mechanism.

• **Error Detection:** In FreeIoT, the receiver uses the rate-aware $R - preamble$ to determine the rate R. The value of R suggests that a group of information bits are mapped into the corresponding indexes of R ABS in each of the three overlay data frames. The rate R is not only used by the receiver to choose the valid ABS mapping table while decoding, but also to detect errors. To illustrate this, consider an example rate $R = 2$. When the receiver detects $2 - preamble$, it will interpret that the information is overlaid in indexes of $R = 2$ ABS in each overlay data frame. However, if the receiver detects more or less than 2 ABS, the receiver interprets this as an error, and consequently discards the frame. In addition, since 2 ABS are used in each frame, there are $\binom{8}{2} = 28$ possible combinations of the ABS index. However, only 16 combinations are used to represent 4 bits of information.

Figure 8: Illustration of ABS-code correction mechanism for rate $R = 2$.

Therefore, the remaining combinations of ABS index are considered as invalid and discarded by the receiver. For $R = 2$, a frame with ABS index '4' and '6' is considered as invalid and therefore discarded by the receiver.

• **Error Correction:** To make control signaling reliable, we transmit a parity frame in the third overlay data frame, along with useful information in first 2 overlay data frames. As shown in Fig. 8, an XOR operation is performed on the information bits to be transmitted in two overlay data frames. The resultant parity bits are then transmitted in the third data frame. For example, for rate $R = 2$ a group of 4 information bits are mapped to index of 2 ABS. Assuming that 8 bits of information '00011111' is to be transmitted in two overlay data frames, AIM encodes (i) '0001' bits into ABS index of '1' and '3' in the first overlay data frame, and (ii)'1111' is encoded into ABS index of '3' and '7'. An XOR operation is performed on '0001' and '1111' and then the resultant XORed data '1110' is mapped to ABS index '3' and '6' and finally transmitted in the third overlay data frame. At the receiver, if any of the overlay data frame gets discarded due to error, the receiver can extract the corresponding data frame by combining bits in the overlaid frame with parity frame using XOR operation.

IV. Theoretical Analysis

In this section, we derive an expression of a symbol-error-rate (SER) for the given RF-EH-integrated receiver design. We use a binary hypothesis testing to derive the SER [9]. Let H_0 be the hypothesis to test that the output current sample x_n at sampling instant n represents an ABS, while H_1 be the hypothesis that it is not ABS (denoted as N-ABS). The binary hypothesis testing problem for a given i^{th} subframe is as follows:

$$T(\boldsymbol{x}_i) = \frac{1}{N}\sum_{n=1}^{N} x_{n,i} \underset{H_0}{\overset{H_1}{\gtrless}} \lambda \tag{1}$$

where N denotes number of samples used for averaging, $\boldsymbol{x}_i$ is a $N \times 1$ vector for i^{th} subframe defined as $\boldsymbol{x}_i = [x_{1,i}, \ldots, x_{N,i}]$, $T(\boldsymbol{x}_i)$ is the test statistic, and λ is the pre-determined threshold.

Based on the central limit theorem, $T(\boldsymbol{x}_i)$ under hypothesis H_1 can be approximated as a real Gaussian random variable with mean current I_{out} and variance σ_w^2/N and $T(\boldsymbol{x}_i)$ under hypothesis H_0 can be approximated as a real Gaussian random variable with mean 0 and variance σ_w^2/N. The value of I_{out} is proportional to the received input power as $I_{out} = \beta V_{in}^2$, where β is a constant that depends on the electrical properties of the energy harvester including input-output power conversion efficiency. The noise variance σ_w^2 is also energy harvester circuit dependent parameter.

$$T(\boldsymbol{x}_i) = \begin{cases} \mathcal{N}(I_{out}, \sigma_w^2/N) & \text{under } H_1 \\ \mathcal{N}(0, \sigma_w^2/N) & \text{under } H_0 \end{cases} \tag{2}$$

Defining, $\mu_1 = I_{out}$, $\mu_0 = 0$ and $\sigma^2 = \sigma_w^2/N$, the test hypothesis $T(\boldsymbol{x}_i)$ can rewritten as follow:

$$T(\boldsymbol{x}_i) = \begin{cases} \mathcal{N}(\mu_1, \sigma^2) & \text{under } H_1 \\ \mathcal{N}(\mu_0, \sigma^2) & \text{under } H_0 \end{cases} \tag{3}$$

The probability of error in detecting ABS P_{abs} can be computed as follows:

$$\begin{aligned} P_{abs} = \int_{\lambda}^{\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu_0)^2}{2\sigma^2}} &= \mathcal{Q}\Big(\frac{\lambda-\mu_0}{\sigma}\Big) \\ &= \mathcal{Q}\Big(\frac{\lambda}{\sigma_w}\sqrt{N}\Big) \end{aligned} \tag{4}$$

Similarly, the probability of error in detecting non-ABS is:

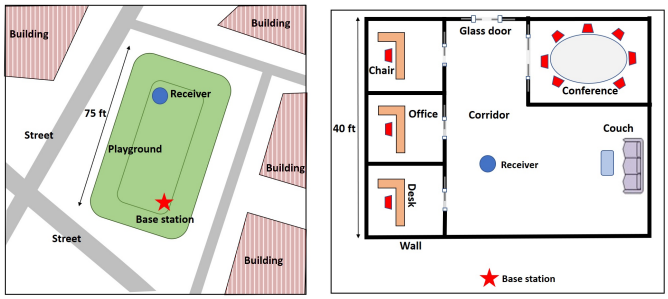
$$\begin{aligned} P_{nabs} = \int_{-\infty}^{\lambda} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu_1)^2}{2\sigma^2}} &= 1 - \mathcal{Q}\Big(\frac{\lambda-\mu_1}{\sigma}\Big) \\ &= 1 - \mathcal{Q}\Big(\frac{\lambda-I_{out}}{\sigma_w}\sqrt{N}\Big) \end{aligned} \tag{5}$$

Based on the available number of ABS, FreeIoT selects the rate R, in which a group of information bits is encoded in ABS pattern of R ABS out of 8 subframes within a LTE frame. Therefore, the probability that all the subframes are decoded correctly is $P_s = (1-P_{nabs})^{8-R}(1-P_{abs})^R$. Substituting for P_s, the symbol error probability P_e is:

$$P_e = 1 - P_s = 1 - (1-P_{nabs})^{8-R}(1-P_{abs})^R \tag{6}$$

V. Performance Evaluation

In this section, we first experimentally evaluate the performance of FreeIoT using the metrics of symbol error rate (SER) and throughput. We then perform a trace-driven simulation to show how FreeIoT performs for city-scale sensor deployments. We setup an LTE BS with USRP B210 software defined radio. The output power of the radio is set to 13 dBm. The BS transmits standards-compliant LTE signal in the 915 MHz frequency band with bandwidth of 1.4 MHz. We used a MathWorks LTE System toolbox to generate LTE frames for different ABS pattern configurations. The FreeIoT receiver uses our custom-designed energy RF-EH (see Fig. 6) that is connected to the TI eZ430-RF2500 sensor and is tuned to the same transmission frequency and bandwidth. The output current of the RF-EH is discretized by the ADC operating at sampling frequency of 32 KHz. We study two sensor



(a) (b)

Figure 9: a) *Outdoor* receiver, and b) *Indoor* receiver scenarios.

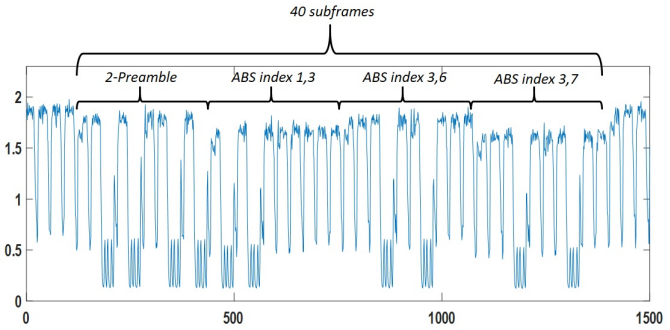


Figure 10: Raw samples of output current of the RF energy harvester for Rate $R = 2$. The plots show the ABS pattern of $2 - preamble$ and overlay control frames with 2 ABS.

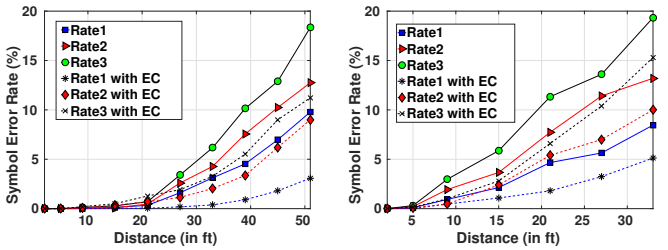
deployments, both indoor and outdoor as shown in Fig. 9, with the BS fixed at the outdoor location. The sensor-BS separation distance is increased from 2 ft to 70 ft.

A. Mapping raw signals to ABS at receiver

Fig. 10 plots the collected raw samples, which shows that the received current from the voltage rectifier shows variation in accordance with the absence or presence of ABS within the LTE frame. It is clearly seen that ABS pattern within 40 subframes represents 2-Preamble and three overlay frames each having 2 ABS. The receiver establishes the communication by identifying the ABS pattern of `SYNC`, followed by `ID`. Once the sensor has been identified, the receiver decodes the transmitted overlaid information after receiving rate specific $R-$preamble.

B. Symbol Error Rate

Since a group of control bits are mapped to the ABS index within an overlay control frame, we define SER as the number of overlay control frames decoded incorrectly per the total number of transmitted overlay frames by FreeIoT. The BS sends 7500 symbols that are decoded at the receiving sensor. The SER for the *outdoor* scenario is plotted in Fig. 11a. Since the output current of the RF-EH is a function of received input power, the SER increases as the distance between the BS and the receiver increases. FreeIoT achieves less than 1% SER for the communication range up to 20ft. In reality, the LTE base station uses transmission power of 46 dBm, and



(a) (b)

Figure 11: a) The SER for *outdoor* receiver scenario, and b) The SER for *indoor* receiver scenario.

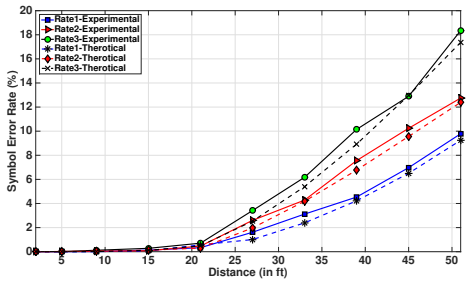


Figure 12: The comparison of the experimental and theoretical SER for the outdoor scenario.

therefore, FreeIoT can achieve similar performance for much longer distances. We also note that as the rate R increases, the SER expectedly increases. This is because the probability of errors in detecting ABS increases with increase in the number of ABS, which results in higher SER for higher rate R. We also analyzed the impact of the ABS-Code error detection and correction technique on the SER. In a group of three overlay control frame, FreeIoT can correct one overlay frame using the parity frame. We see that SER is much lower when error correction is used, giving less than 6% SER for a range up to 39ft. Fig. 11b gives the SER for the *indoor* receiver scenario, which is a challenging environment due to higher attenuation and multipath. In this case, FreeIoT achieves less than 6% SER up to a range of 15ft; with error correction this extends to 21ft.

Additionally, the symbol error rate performance evaluated during the experiment is compared with the theoretical SER as derived in Section IV. First, we measured the incident input power received by the RF-EH for each distance. Using the input power - output current relationship, we derived the output current and considered it as mean current I_{out} used for the theoretical analysis. We also estimated the noise variance σ_w^2 in the output current of RF-EH through collected samples when there is simply no transmission. Since, the output current is sampled at 32 KHz, each subframe will have $N = 32$ samples. Using the value of I_{out}, σ_w^2 and N, we calculated the theoretical SER for each distance. Fig. 12 compares the SER performance of the experimental SER for outdoor environment with the theoretical SER. It can be observed that the theoretical SER closely matches with the experimental SER.

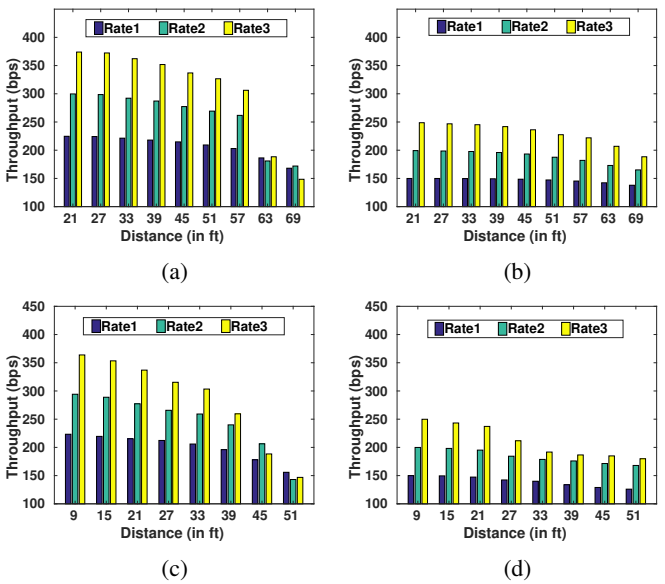


Figure 13: Throughput for baseline *outdoor* receiver scenario (a), and with additional ABS-Code error correction (b). Throughput for *indoor* receiver scenario (c), and with additional ABS-Code error correction (d).

C. Throughput of overlay control signaling

This section studies the throughput of FreeIoT, defined as the number of bits received correctly per unit time. FreeIoT supports maximum throughput of 225 bps, 300 bps, and 375 bps for rate $R = 1, 2$, and 3 respectively. As shown in Fig. 13a, for the given experimental set-up in *outdoor* scenario, FreeIoT achieves the maximum throughput for the communication range up to 21ft. As the range increases, the throughput gradually decreases. For longer distances (63ft and 69ft), the throughput for a lower rate $R = 1$ or 2 may be higher than $R = 3$ as the SER for the latter is greater than for $R = 1$ or 2.

In ABS-Code detection and error correction, the use of extra overlay frame as a parity frame incurs overhead, which reduces throughput. However, from Fig. 13b for communication range of 69ft, we see that FreeIoT achieves higher throughput with error correction than without error correction for $R = 3$. A similar trend is observed for rates $R = 1$ and $R = 2$, for longer distances. Fig. 13c shows the throughput achieved by FreeIoT for the *indoor* receiver scenario. It can be observed that for the given experimental set up, FreeIoT achieves maximum throughput for communication range up to 9ft. Fig. 13d shows that FreeIoT with error correction achieves higher throughput for rate $R = 3$ for distance of 45ft, whereas it achieves higher throughput for rate $R = 2$ and $R = 3$ for the range of 51ft.

D. City-scale Simulations

In this section, the performance analysis of FreeIoT is extended via city-scale simulations. Our characterization studies on the RF-EH reveals the non-linear performance of the circuit, where higher input RF powers operate the RF-EH in greater efficiency regimes (and hence output current), e.g., 10 dBm received power generates 10 mA of current.

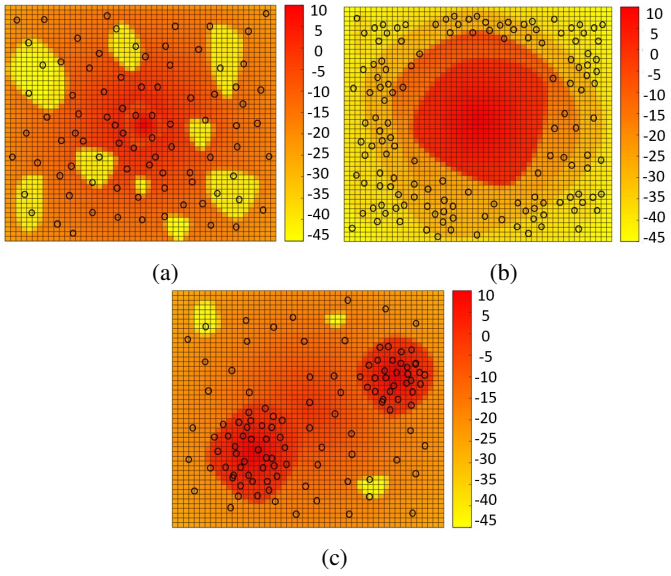


Figure 14: The heatmap of IoT sensors' received power distribution in an area of $250 \times 250m^2$ in (a) residential, and b) stadium, and c) city downtown.

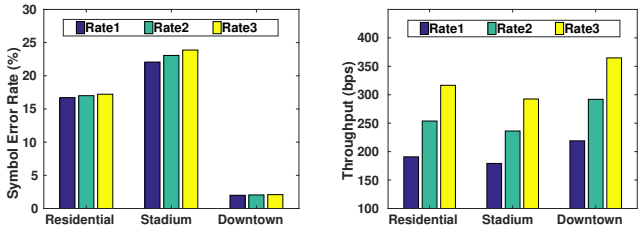


Figure 15: (a) Average SER, b) Average throughput for different environments.

We simulated three city environments a) residential area, b) stadium, and c) city downtown each of area $250 \times 250m^2$ with different distribution of received input power and location of 200 IoT sensors. To capture the input power characteristics of the environment, we divide the geographical area into rectangles of $5m \times 5m$. Each sensor observes received power from a Gaussian distribution, which is a characteristic of the grid rectangle location in which it is located. Each grid location has different mean input power but has same standard deviation of roughly 3dBm. Thus, input power characteristics of each environment is determined by the mean input power values of the grids [10]. Fig. 14 shows the heatmap of received power distributions of three environments a) residential area, b) stadium, and c) city downtown. Residential area has uniform distribution of power. In stadium, the power is concentrated inside of the stadium rather than outside (e.g. parking lots). On the other hand, the downtown has few areas with spikes in received power and other areas with uniform distribution.

The output current of each sensor is determined using its location, the harvester efficiency curves, and the corresponding input power. We calculated the symbol error rate (P_e) by

considering the calculated current as a mean value using the analysis provided in Section V, with over 5000 trials to average results. Subsequently, the throughput of each sensor for rate R is calculated using the derived SER as Throughput $= (1 - P_e) * (k \times 75)$ bps, where k represents the number of information bits overlaid with rate R.

Fig. 15a shows the average SER of the sensors for rate $R = 1, 2$, and 3 in each environment. It can be observed that the SER is much higher for the sensors located in an added test conducted on a stadium environment. It is because the presence of high number of sensors at locations with low input power around the stadium areas, such as parking lots. In addition, the symbol error rate is higher as the rate of transmission increases. Fig. 15b shows the average throughput of the sensors deployed in different environments. It is evident that the average throughput of the sensors in a city downtown is comparatively much higher, since a large number of sensors are densely deployed in regions with high received input power, as seen in Fig. 14c.

VI. Related Work

We mainly focus on the related work in context of cross-technology communication systems, as this is directly related to our work. Most published works focus on cross communication between technologies operating in the same band (eg. WiFi and ZigBee in 2.4GHz). FreeBee [11] shifts the transmission timing of WiFi beacons to convey information. ESense [12], HoWiES [13] enables WiFi to ZigBee communication by modulating the packet length of WiFi packets. Gap Sense [14] uses a special preamble to deliver coordination messages. WiZig [15] encodes the information in multiple energy level. EMF [16] encodes the information by shifting/flipping the packets. B2W2 [17] uses CSI to enable multiple BLE to WiFi communications. The variations in the energy of the signal is used for data communication in [18]. Ambient Backscatter[19] uses ambient RF signals, whereas Wi-Fi Backscatter [20] uses wi-fi signal to enable communication between two battery-free devices. Different from these efforts, we explore the possibility of conveying information by spatially changing the positions of ABS in a standards-compliant LTE frame without introducing special packets, timing changes, or fields within the header. At a device level, we note that our approach can be an after-market addition to a number of long-range IoT sensors/transmitters. Products like LORA [2] and SigFox [3] both have long range uplink, but can also be engineering easily to serve as a FreeIoT receiver with efficient and low-overhead downlink control channels. Finally, many city-wide IoT implementations exist already today, which can immediately benefit from our LTE-based control paradigm without new infrastructure, such as [1].

VII. Conclusion

We proposed FreeIoT - an overlay control signaling method using current LTE infrastructure. By temporally arranging the ABS within LTE frames and relying on a RF harvesting circuit at the receiver end, FreeIoT can target individual sensors for wake-up and issuing directives on the downlink channel, without any modifications to commercially available sensors. Through experiments, we show that our approach can support an effective communication rate of upto 375 bps, and yet limit the symbol error rates in the range of 1- 6% for typical outdoor deployments. Future work will involve testing of the FreeIoT at scale with actual installations of sensors in the city, identifying specific dead/high error zones and devising region-specific error recovery and ARQ mechanisms to increase the resiliency of control signaling.

Acknowledgment

This work was supported by the US National Science Foundation under research grant CNS1452628.

References

[1] L. Sanchez, L. Munoz, J. Galache, P. Sotres, and J. Santana, "SmartSantander: IoT experimentation over a smart city testbed," *Comput. Net.*, vol. 61, pp. 217238, Mar. 2014.

[2] LoRa Alliance. *The LoRa Alliance Wide Area Networks for Internet of Things*, [Online]. Available: https://www.lora-alliance.org/

[3] Sigfox. *SIGFOX-The Global Communications Service Provider for the Internet of Things (IoT)*, [Online]. Available:http://www.sigfox.com/

[4] 3GPP, "Evolved universal terrestrial radio access (E-UTRA) and evolved universal terrestrial radio access network (E-UTRAN); overall description; stage 2" 3GPP tech. spec. TS 36.300, Ver. 10.8.0, Jul. 2012

[5] M. Cierny, H. Wang, R. Wichman, Z. Ding, and C. Wijting, "On number of almost blank subframes in heterogeneous cellular networks", *IEEE Trans. on Wireless Commun.*, vol. 12, no. 10, pp. 5061-5073, Oct. 2013

[6] S. Golomb and G. Gong, "Signal design for good correlation: for wireless communication, cryptography, and radar", Cambridge University Press, Sep. 2005.

[7] L. Chen, S. Cool, H. Ba, W. Heinzelman, I. Demirkol, U. Muncuk, K. Chowdhury, and S. Basagni, "Range extension of passive wake-up radio systems through energy harvesting," *IEEE ICC*, 2013.

[8] N. Verma and A. P. Chandrakasan, "An ultra low energy 12-bit rate-resolution scalable SAR ADC for wireless sensor nodes," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 6, pp. 1196-1205, Jun. 2007.

[9] T. Banerjee, K. Chowdhury, and D. P. Agrawal, "Using polynomial regression for data representation in wireless sensor networks," *International Journal of Communication Systems*, vol. 20, no. 7, pp. 829-856, 2007.

[10] Y. Bejerano, C. Raman, C. Yu, V. Gupta, C. Gutterman, T. Young, H. Infante, Y. Abdelmalek, and G. Zussman,"DyMo: Dynamic monitoring of large scale LTE multicast systems," *IEEE INFOCOM*, 2017.

[11] S. M. Kim and T. He, "Freebee: Cross-technology communication via free side-channel," *ACM MobiCom*, 2015.

[12] K. Chebrolu and A. Dhekne,"Esense: Communication through energy sensing," *ACM MobiCom*, 2009.

[13] Y. Zhang and Q. Li, "HoWiES: A holistic approach to ZigBee assisted WiFi energy savings in mobile devices," *IEEE INFOCOM*, 2013.

[14] X. Zhang and K. G. Shin, "Gap Sense: Lightweight coordination of heterogeneous wireless devices,"' *IEEE INFOCOM*, 2013.

[15] X. Guo, X. Zheng, and Y. He, "WiZig: Cross-technology energy communication over a noisy channel," *IEEE INFOCOM*, 2017.

[16] Z. Chi, Z. Huang, Y. Yao, T. Xie, H. Sun, and T Zhu, "EMF: Embedding multiple flows of information in existing traffic for concurrent communication among heterogeneous IoT devices," *IEEE INFOCOM*, 2017.

[17] Z. Chi, Y. Li, H. Sun, Y. Yao, Z. Lu, and T. Zhu, "B2W2: N-way concurrent communication for IoT devices," *ACM SenSys*, 2016.

[18] R. G. Cid-Fuentes, M. Y. Naderi, S. Basagni, K. Chowdhury, A. Cabellos-Aparicio, and E. Alarcon, "On signaling power: Communications over wireless energy," *IEEE INFOCOM*, 2016.

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

[20] B. Kellogg, A. Parks, S. Gollakota, J. Smith, and D. Wetherall, "Wi-Fi backscatter: Internet connectivity for RF-powered devices," *ACM SIGCOMM*, 2014.