JICE: Joint Data Compression and Encryption for Wireless Energy Auditing Networks

Sheng-Yuan Chiu[1,2] Hoang Hai Nguyen[1] Rui Tan[1] David K. Y. Yau[1,3] Deokwoo Jung[1]
[1]Advanced Digital Sciences Center, Illinois at Singapore [2]National Tsing Hua University, Hsinchu, Taiwan
[3]Singapore University of Technology and Design, Singapore

***Abstract*—Fine-grained real-time metering is a fundamental service of wireless energy auditing networks, where metering data is transmitted from embedded power meters to gateways for centralized processing, storage, and forwarding. Due to limited meter capability and wireless bandwidth, the increasing sampling rates and network scales needed to support new energy auditing applications pose significant challenges to metering data *fidelity* and *secrecy*. This paper exploits the *compression* and *encryption* properties of compressive sensing (CS) to design a joint data compression and encryption (JICE) approach that addresses these two challenges simultaneously. Compared with a conventional signal processing pipeline that compresses and encrypts data sequentially, JICE reduces computation and storage complexities due to its simple design. It thus leaves more processor time and available buffer space for handling lossy wireless transmissions. Moreover, JICE features a machine-learning-based reconfiguration mechanism that adapts its signal representation basis to changing power patterns autonomously. On a smart plug platform, we implemented JICE and several baseline approaches including downsampling, lossless compression, and the pipeline approach. Extensive testbed experiments show that JICE achieves higher data delivery ratios and lower recovery distortions under a range of realistic settings. In particular, JICE increases the number of meters supported by a gateway by 50%, compared with the pipeline approach, while keeping a distortion rate lower than 5%.**

I. Introduction

In emerging smart grids, *wireless energy auditing network* (WEAN) [1]–[4], which consists of a network of wireless power meters, is a fundamental service to enable various new features such as demand response, usage disaggregation, power quality monitoring, and efficiency diagnosis. These wireless power meters, embedded in smart appliances, switches, and plugs, are designed to support continuous measurements of various physical quantities (e.g., voltage and current) at high frequencies [1]. However, due to their limited computation and storage capabilities as well as the need to simultaneously support multiple real-time energy auditing applications and enable post-event investigations, it is desirable to transmit the raw metering data to central nodes such as backend servers for advanced processing and long-term storage. This data-collection-over-the-air architecture creates two fundamental requirements. First, *data fidelity* at the central nodes must be preserved to assure the quality of the aforementioned new functionality in smart grids. Second, *data secrecy* during the wireless transmissions must be ensured to protect customers' privacy from malicious eavesdroppers, since the power measurements can easily reveal customers' sensitive information such as their daily routines. Moreover, recent studies show that an adversary can infer much fine-grained information such as the TV channel being watched [5] and the web page being browsed [6] based on unencrypted power readings. Indeed, public concern for privacy has derailed planned mandatory deployments of smart meters [7]. Thus, for WEANs to gain acceptance by consumers and utility, efficient technologies must be devised to address the two requirements.

978-1-4673-7331-9/15/$31.00 © 2015 IEEE

Higher sampling rates for power signals capture more operating characteristics of appliances, which is desirable for energy auditing. For instance, to capture routine power activities in harmonics analysis, power meters with wireline communication often sample at 1.6 kHz or higher [8]. However, the highest sampling rate adopted by current WEAN prototypes is just 4 Hz [1]. Moreover, a recent study [3] finds that a WEAN using one smart plug per occupant in a typical commercial office, resulting in 455 plugs deployed totally, can cover only 10% of the appliances. Thus, both the sampling rate and network size need to be increased to improve the spatiotemporal granularity of energy auditing beyond the state of the art. However, the goals impose significant challenges for the capability-limited power meters to meet data fidelity and secrecy requirements. First, a large volume of measurements from individual meters will quickly congest wireless channels. The resulting poor end-to-end data delivery ratio will undermine data fidelity. The problem can be worsened if the wireless channels used by the meters are subject to interference with other wireless communications such as WiFi commonly found in buildings. Second, encryption must be used to achieve data secrecy, but it often incurs severe computational overhead at the meters. Indeed, due to the problem, some off-the-shelf smart meters do not encrypt their measurements at all [9]. A conventional solution that pipelines a compressor and a cipher to reduce transmission volume and ensure secrecy will be too slow at the meters. The resulting long processing delays can jeopardize the data fidelity, when some of the measurements have to be dropped to maintain real-time performance.

This paper proposes a joint compression and encryption (JICE) approach based on compressive sensing (CS) [10] to achieve data fidelity and secrecy simultaneously. CS theory shows that a compressible signal can be represented by a small number of linear projections of the original signal and recovered with high probability. The much reduced transmission volume due to compression helps in turn to reduce channel contention and hence improve data fidelity. CS requires only a simple multiplication between a random matrix and a vector of the original signal, which can be efficiently implemented on capability-limited meters. Moreover, recent studies [11], [12] show that the cryptanalysis of recovering the original signal from a CS-compressed signal is computationally hard without knowing the true random matrix. Thus, CS provides a form of encryption if the random matrix is established as a shared secret between the transmitter and the receiver. Because of these advantages, CS is a promising approach to achieving simultaneously the dual functions of data compression and encryption on capability-limited wireless meters. In particular, compared with the conventional pipeline approach, the CS-based JICE leaves more processor time and available buffer space for handling lossy wireless transmissions.

This paper presents the design of JICE in WEANs and quantifies the advantages of JICE over other plausible solutions through extensive benchmarking and testbed experiments. The major contributions of this paper include:

- As CS design is application-specific, we address all the key design elements systematically for WEANs, which include signal sparsity, representation basis, and measurement matrix, based on real power data traces. The results show that, in contrast to the choice of the measurement matrix, the choice of the representation basis can significantly affect the recovery performance.
- We develop a novel machine-learning-based approach that identifies the best representation basis and reconfigures a JICE system autonomously, to adapt to changing power consumption patterns. Specifically, a computation-intensive learning algorithm is executed at a resourceful gateway, while a lightweight classification algorithm is executed at each capability-limited power meter to select the representation basis based on the learned model and observed power pattern.
- Although an adversary cannot easily recover the measurement data without the random matrix used in the CS, we identify a vulnerability of CS that can leak important statistics information about the measurement data. To solve the vulnerability, we propose a lightweight perturbation approach that adds a random noise signal to the original power signal. We design the noise signal to be sparse in a transform domain, to avoid adverse impact on the CS recovery.
- On a smart plug platform, we implement JICE and several baseline approaches including downsampling, lossless compression, and a pipeline approach that applies a compressor and a cipher sequentially. Extensive benchmarking and testbed experiments show that JICE reduces the computational overhead and achieves higher data delivery ratios and lower recovery distortions under various realistic settings with sampling rates from 8 Hz to 64 Hz. In particular, when the sampling rate is 8 Hz, the number of meters supported by a gateway is increased by 50%, compared with the pipeline approach, while keeping a data distortion rate lower than 5%.

In summary, JICE pushes the Pareto-optimal frontier of the sensor-sampling-rate versus network-size trade-offs under the data fidelity and secrecy requirements, beyond the state of the art including commonly used signal processing pipelines.

This paper is organized as follows. Section II reviews related work. Section III describes CS theory and our problem statement. Sections IV and V design JICE and discuss its secrecy properties, respectively. Section VI presents implementation details and benchmarking results. Section VII presents testbed experiment results. Section VIII concludes and discusses the applicability of JICE to other applications.

II. Related Work

Pervasive sensing is a key element of smart grid technologies. It is estimated that by 2019 more than 100 million wireless sensors will be installed in non-residential buildings, with wireless power meters taking up a major sector [13]. Thus, WEAN has received much research interest in recent years. Early studies have focused on hardware design of the wireless meters [2], as well as networking issues in small-scale deployments [1]. A recent research project [3] deployed 455 meters in a commercial building. Although it is recognized [2] that high sampling rates (multiple to tens of Hz) are important for load disaggregation, all the existing pilot deployments [1]–[3] adopt low sampling rates such as one sample per minute [2]. Data compression to save wireless bandwidth is therefore not critical in these projects. Moreover, they do not address data encryption for privacy in their design.

CS-based data collection protocols that exploit the spatial sparsity of sensor readings have been developed for wireless sensor networks, in the media access control [14] and network [15] layers. These protocols leverage the compression nature of CS to reduce communication cost. In [14], multiple sensors simultaneously transmit their readings amplified by random factors to a sink node over an analog wireless channel, resulting in a projection of all the readings at the sink. From the multiple projections, the sink can recover the readings. In [15], sensors multiply their readings by random vectors and aggregate the vectors in the network, resulting in balanced energy consumption of the sensors. Recent studies have applied CS to various sensing systems including acoustic ranging [16], video background subtraction [17], and soil moisture monitoring [18]. By exploiting the temporal sparsity of a single sensor's data, they apply CS to schedule the sleep of the sensors [18], and reduce transmission volume [16] and computation overhead [17]. In contrast, this paper aims to exploit the low computation and storage complexity of CS to jointly compress and encrypt temporally sparse power signals on embedded wireless power meters. Moreover, none of the earlier studies aim to reconfigure CS to adapt to changing signal patterns, but we do.

It is observed in [11] that CS implements a form of encryption if the measurement matrix is a secret. As the mutual information between the input and output of CS is non-zero [12], like many other ciphers, CS cannot achieve Shannon's *perfect secrecy*. Nonetheless, it is shown that recovering the original signal without the true measurement matrix is computationally difficult [12], [19]. A signal recovered with a wrong measurement matrix is less sparse than the original signal [12]. However, the cryptanalysis that exhaustively searches for a measurement matrix to minimize the sparsity of a candidate recovery is often intractable. Similarly, it is shown that brute force and structured attacks to estimate a Gaussian measurement matrix is practically infeasible [19]. Such secrecy property of CS is used to establish secret communication in asymmetric channels through secure measurement matrices [20]. Although previous studies [12], [19] established the difficulty of signal recovery without the measurement matrix, this paper identifies a vulnerability of CS to leaking statistics of the original signal and proposes an approach to solving the vulnerability.

III. Background and Approach Overview

A. Preliminaries

This section briefly reviews CS theory [10]. Let N denote the length of the input signal. Suppose Ψ is an orthonormal *representation basis* $\Psi = [\psi_1 \psi_2 \cdots \psi_N] \in \mathbb{R}^{N \times N}$, where ψ_i is the ith column of Ψ. The coefficient sequence of a time-domain signal $\mathbf{x} \in \mathbb{R}^{N \times 1}$ on the basis Ψ is denoted as $\hat{\mathbf{x}}$, i.e., $\mathbf{x} = \Psi \hat{\mathbf{x}}$. The signals $\mathbf{x}$ and $\hat{\mathbf{x}}$ are k-sparse if $\hat{\mathbf{x}}$ has k non-zeros. Let $\mathbf{y} \in \mathbb{R}^{M \times 1}$ denote the output signal and $\Phi \in \mathbb{R}^{M \times N}$ denote the *measurement matrix*, where $M < N$. The measurement process of CS is $\mathbf{y} = \Phi \mathbf{x}$. In this paper, the *compression ratio*, denoted by γ, is defined as $\gamma = N/M$. By denoting $\mathbf{A} = \Phi\Psi$, we have $\mathbf{y} = \mathbf{A}\hat{\mathbf{x}}$. The matrix $\mathbf{A}$ complies with the *restricted isometry property* (RIP) of order k if there exists a constant δ_k such that $(1 - \delta_k)\|\hat{\mathbf{x}}\|_{\ell_2} \le \|\mathbf{A}\hat{\mathbf{x}}\|_{\ell_2} \le (1+\delta_k)\|\hat{\mathbf{x}}\|_{\ell_2}$, for any k-sparse signal $\hat{\mathbf{x}}$, where $\|\cdot\|_{\ell_2}$ represents the ℓ_2-norm. Let $\mathbf{x}'$ and $\hat{\mathbf{x}}'$ denote the recovered signal and its transform, respectively. If $\mathbf{x}$ is k-sparse and $\mathbf{A}$ complies with RIP of order k, the original signal $\mathbf{x}$ can be recovered as $\mathbf{x}' = \Psi\hat{\mathbf{x}}'$, where $\hat{\mathbf{x}}'$ is given by $\hat{\mathbf{x}}' = \arg\min_{\hat{\mathbf{z}} \in \mathbb{R}^{N \times 1}} \|\hat{\mathbf{z}}\|_{\ell_1}$, subject to that $\mathbf{y} = \mathbf{A}\hat{\mathbf{z}}$.

It has been shown [10], [21] that $\mathbf{A}$ complies with RIP of order k if Φ is composed of M rows that are randomly selected from an orthonormal basis $\Phi^* \in \mathbb{R}^{N \times N}$ and

$$M \ge C \cdot \mu^2(\Phi^*, \Psi) \cdot k \cdot \log N, \tag{1}$$

where $\mu(\Phi^*, \Psi)$ is the *coherence* between the two orthonormal matrices Φ^* and Ψ [10], [21]. The coherence is formally given by $\mu(\Phi^*, \Psi) = \sqrt{N} \cdot \max_{1 \le i,j \le N} |\phi_i^* \cdot \psi_j| \in [1, \sqrt{N}]$, where ϕ_i^* and ψ_j are the ith row and jth column of Φ^* and Ψ, respectively. In other words, the coherence measures the largest correlation between any row of Φ^* and any column of Ψ. In this paper, we adopt the normalized coherence defined as $\bar{\mu}(\Phi^*, \Psi) = \mu(\Phi^*, \Psi)/\sqrt{N} \in [1/\sqrt{N}, 1]$.

B. Background and Problem Statement

A wireless power meter embedded in smart appliances, switches, and plugs typically consists of a power sensor, a microcontroller unit (MCU), a non-volatile memory, and a Zigbee radio. These meters may draw power from batteries or a power grid. To increase hardware reliability and minimize impact on the power grid, these meters often use low-power hardware components with limited computation, storage, and communication capabilities. For instance, the TI MSP430F1xx, a widely adopted MCU family for these meters [2], [22], has an 8MHz clock rate and 10KB RAM capacity only. As discussed in Section I, to enable various advanced energy auditing applications, it is desirable to transmit the metering data to a *gateway* such as a smart meter or a Zigbee access point, while meeting the data fidelity and secrecy requirements.

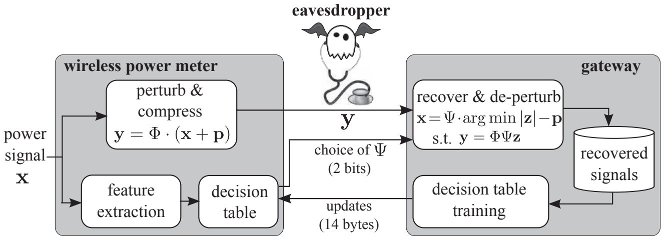


Fig. 1. Overview of JICE.

As power signals are often temporally correlated and hence compressible, data compression can be applied to reduce transmission volume and alleviate the channel contention. Moreover, it allows more retransmission attempts for lost packets, given a transmission deadline that ensures real-time metering. Various ciphers [23] can be employed to ensure data secrecy. However, system designers face strong challenges in pipelining existing compressors and ciphers, as they incur significant computation and storage overhead at the capability-limited meters. For instance, without careful design, the execution time of these algorithms could jeopardize the timeliness of metering easily. As discussed in Section I, CS is a promising approach that jointly achieves fidelity and secrecy while keeping a simple system design of low computation complexity. In this paper, we aim to answer the following basic questions. First, how to design the key elements of CS including representation basis and measurement matrix for WEANs (Section IV)? Second, what are the secrecy vulnerabilities (if any) of CS as a form of encryption (Section V)? Third, can CS bring substantial benefits such as reduced packet losses and recovery errors, compared with other plausible approaches (Sections VI and VII)?

C. Overview of JICE

An overview of JICE is illustrated in Fig. 1. A wireless power meter first perturbs the original power signal $\mathbf{x}$ by adding a perturbation vector $\mathbf{p}$ to fix a secrecy vulnerability of CS identified in this paper (see Section V). It then compresses the perturbed signal by multiplying it by the random measurement matrix Φ. Meanwhile, it extracts a feature vector consisting of three simple statistics of $\mathbf{x}$, and uses a decision table to choose the most efficient representation basis Ψ among a number of candidate bases. This design is motivated by a key observation, from our extensive empirical results, that the representation basis can significantly affect recovery performance. The meter sends the CS-compressed signal and the choice of Ψ to the gateway, which recovers $\mathbf{x}$ using $\mathbf{p}$, Φ, and the chosen Ψ. The gateway may run advanced electricity analytics based on the recovered data and/or forward the data to backend servers through secure wireline links. It also runs a decision table training algorithm periodically based on recently recovered data, and sends the updated decision table to the meter, such that the system can adapt well to changing power characteristics. In JICE, the perturbation vector $\mathbf{p}$ and the measurement matrix Φ are shared secrets between the meter and the gateway, to ensure the secrecy of the data transmissions over air. Moreover, they should be different across the meters, such that leak of the secret of a single meter (e.g., by extracting from the memory of a physically captured meter) will not reveal the secrets of other meters. The details for establishing these shared secrets will be discussed in Section V.

IV. Compressive Sensing for Power Signals

This section analyzes the sparsity of power signals, which is essential to the design of JICE. We then design the rep-

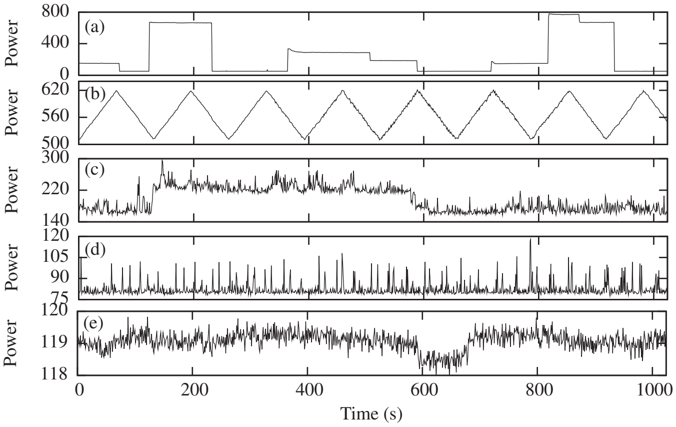


Fig. 2. Various types of power consumption (unit: watt): (a) Duty-cycled (pantry); (b) Periodic (boardroom); (c) Fluctuating (office); (d) Spiky (server room); (e) Silent (boardroom).

resentation basis Ψ and the measurement matrix Φ. There is no systematic way of selecting Ψ and Φ; it is usually done through a trial-and-error approach. This paper similarly adopts such an approach, with guidance by CS theory to make the process more scientific. Finally, we develop a novel machine-learning-based algorithm for the power meters to choose the most efficient representation basis.

A. Power Consumption Traces

This section presents the details of a data set of real power traces collected on one floor of an office building for 18 hours. Based on this data set, we design JICE in the following subsections. The floor has multiple rooms and open areas, which draw power from a total of 39 branches at a main power panel. We install current transducers on the main power panel to measure the power consumption per branch at one Hz. Different appliances have different power consumption patterns. After a comprehensive inspection, the power signals can be generally classified into five categories: *duty-cycled*, *periodic*, *fluctuating*, *spiky*, and *silent*. Fig. 2 shows examples for the different types. Many heating/cooling appliances duty-cycle to achieve the desired temperatures. Fig. 2(a) shows the duty-cycled power consumption in a pantry with a refrigerator and a water dispenser. Fig. 2(b) shows the periodic power consumption of a projector in a boardroom. Computers can generate complex power consumption patterns. Fig. 2(c) shows the power trace of an office room, where the fluctuations of about 40 watts are caused by a desktop computer. Fig. 2(d) shows the power trace of a server room, with power spikes caused by a bursty workload of the servers. Fig. 2(e) shows the power consumption of the boardroom when only ceiling lights are on, where the fluctuations are within one watt.

B. Design of Representation Basis Ψ

The sparsity of signal $\mathbf{x}$ or $\hat{\mathbf{x}}$, denoted by ρ, is defined as $\rho = k/N$. CS theory assumes that $\hat{\mathbf{x}}$ contains $N-k$ zeros (i.e., k-sparse). However, in practice, $\hat{\mathbf{x}}$ typically contains small values rather than zeros. A common approach is to approximate $\hat{\mathbf{x}}$ by $\hat{\mathbf{x}}_{(k)}$, which is obtained by keeping the k largest coefficients of $\hat{\mathbf{x}}$ only and setting the others to zeros [14]. As a result, the setting of k (or ρ) affects the approximation accuracy and the design of CS (e.g., the choice of compression ratio). By denoting $\mathbf{x}_{(k)} = \Psi\hat{\mathbf{x}}_{(k)}$, the *distortion* of $\mathbf{x}_{(k)}$ is defined as

$$\epsilon(\mathbf{x}_{(k)}, \mathbf{x}) = \frac{\|\mathbf{x}_{(k)} - \mathbf{x}\|_{\ell_2}}{\|\mathbf{x}\|_{\ell_2}}. \tag{2}$$

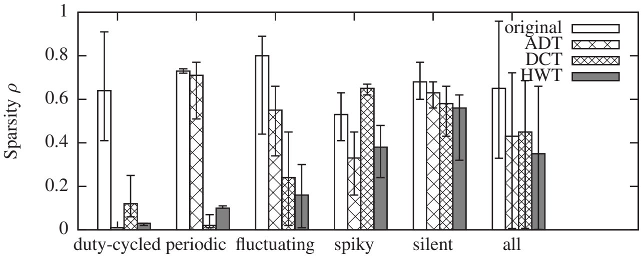


Fig. 3. Sparsity of various power signal categories under different representation bases. ($N = 1024$, the error bars represent min and max values.)

Under the above definition, $\mathbf{x}$ is approximately k-sparse, where k is the minimum of l subject to $\epsilon(\mathbf{x}_{(l)}, \mathbf{x}) \leq \epsilon_0$ and ϵ_0 is a small fixed threshold. The ρ is defined as the *approximate sparsity* of $\mathbf{x}$. In the rest of this paper, we mean approximate sparsity when we say sparsity, and ϵ_0 is set to 1%.

From Eq. (1), it is desirable to choose a representation basis to efficiently sparsify the signal to achieve a better compression ratio. This paper considers three commonly adopted representation bases [15], [18], although JICE can easily encompass other bases. The *adjacent difference transform* (ADT) [18] computes the difference between two adjacent samples and can sparsify a steady signal that occasionally has transient changes. The *discrete cosine transform* (DCT) expresses the signal by a weighted sum of cosine functions of different frequencies, and hence can efficiently sparsify signals with periodic components. The discrete wavelet transform can compactly represent the signal with both temporal correlation and periodicity. In this paper, we consider the *Haar wavelet transform* (HWT), which is commonly used with CS [18]. Let Ψ_A, Ψ_D, and Ψ_H denote the representation bases for ADT, DCT, and HWT, respectively. Their definitions can be found in [18], [24], [25].

We separately evaluate the sparsity of power signals for the different categories under different representation bases. The results are shown in Fig. 3. We can see that all the three transforms can reduce the signal sparsity with respect to the original signal. Moreover, we can see that the most efficient representation bases that minimize ρ for different categories of signals are different. For instance, consistent with intuition, ADT and DCT are most efficient for the *duty-cycled* and *periodic* signals, respectively. Fig. 3 also shows the overall results when all the types of signals are used. HWT outperforms the other two transforms in an average sense. Thus, Ψ_H is a preferable default basis without prior knowledge of the signal structures of power readings.

C. Design of Measurement Matrix Φ

From Eq. (1), to achieve better compression ratios, Φ and Ψ should be chosen to jointly reduce the signal sparsity and coherence. In this paper, we consider three random measurement matrices that have been shown to comply with RIP [26], [27] and employed in various applications [18]:

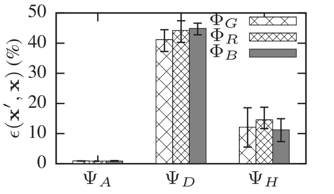
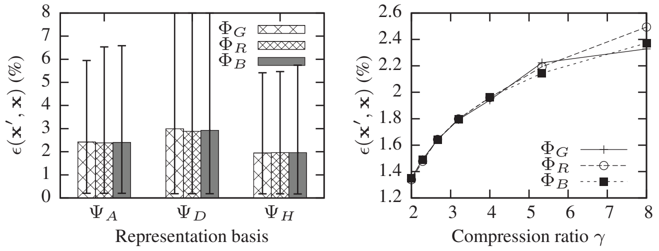


Fig. 4. Distortion of reconstruction for signals collected in pantry.

TABLE I. COHERENCE $\bar{\mu}(\Phi^*, \Psi)$

	Ψ_D	Ψ_H
Φ_G^*	0.154	0.158
Φ_R^*	0.148	0.144

† $N = 1024$



(a) $\gamma = 4$, $S = 8$

(b) $\Psi = \Psi_H$, $S = 8$

Fig. 5. Distortion of reconstruction (excluding pantry). Error bars represent min and max values.

Gaussian matrix Φ_G: Each element of Φ_G is drawn from the normal distribution $\mathcal{N}(0, \frac{1}{M})$, where M satisfies Eq. (1).

Rademacher matrix Φ_R: Each element of Φ_R is either $\frac{1}{\sqrt{M}}$ or $-\frac{1}{\sqrt{M}}$ with a probability of 0.5, where M satisfies Eq. (1).

Binary matrix Φ_B: Each column of Φ_B has S ones and $(M-S)$ zeros. The positions of ones are uniformly distributed. Φ_B complies with an extended RIP where the ℓ_2-norm in the RIP definition in Section III-A is replaced with the ℓ_1-norm [27].

We conduct extensive empirical studies on the performance of combinations of the above three measurement matrices and the three representation bases described in Section IV-B. The compression ratio and distortion of the recovered signal are two important but competing performance metrics for signal compression. In this paper, the distortion is assessed by $\epsilon(\mathbf{x}', \mathbf{x})$, where $\mathbf{x}'$ is the recovered signal and $\epsilon(\cdot, \cdot)$ is defined in Eq. (2). We first evaluate the distortion for the *duty-cycled* signals collected in the pantry under different combinations of Φ and Ψ. The result in Fig. 4 shows that ADT obtains the smallest distortion across all the bases, which is consistent with Fig. 3. Table I lists the normalized coherence for different combinations of Φ and Ψ. Note that as Ψ_A and Φ_B are not orthonormal, the coherence involving them is undefined. Φ_R shows smaller coherence than Φ_G, but the difference is not significant. A similar trend can be found in Fig. 4, where the choice of Φ barely affects the reconstruction error.

Next, we evaluate the distortions for different combinations of Φ and Ψ over all the types of signal except for *duty-cycled*. We assume no prior knowledge of the structure of power readings. Fig. 5(a) shows the distortions based on different combinations of Φ and Ψ. From the figure, we can see that HWT yields a lower distortion than ADT and DCT, but the difference in distortion is not significant compared to *duty-cycled*. It also shows that the choice of measurement matrix has negligible impact on the distortion. This result applies for a range of compression ratios. Fig. 5(b) shows the distortion of HWT under different measurement matrices versus compression ratios. While the distortion increases with γ, it is similar among the measurement matrices. In summary, we have the following important insights on choosing Φ and Ψ. The Φ does not significantly affect the performance of JICE. If the signal structure is known, the optimal choice of Ψ can improve greatly the performance; otherwise, HWT yields a marginal performance gain over ADT and DCT on average.

TABLE II. THRESHOLD-BASED DECISION TABLE.

$r_{\rm ac}$>T_1? (T_1=0.095)	N	N	N	N	Y	Y	Y	Y
$r_{\rm sc}$>T_2? (T_2=0.059)	N	N	Y	Y	N	N	Y	Y
$\sigma > T_3$? (T_3=51)	N	Y	N	Y	N	Y	N	Y
choice for Ψ	Ψ_D	Ψ_A	Ψ_H	Ψ_A	Ψ_H	Ψ_H	Ψ_H	Ψ_H

D. Autonomous and Dynamic Configuration for Ψ

Motivated by the observation in Section IV-C, we design a machine-learning-based lightweight approach to identifying the most efficient Ψ for each signal block. Our approach is based on a three-dimensional feature vector $\mathbf{f} = [r_{\rm ac}, r_{\rm sc}, \sigma]$ for each block, where $r_{\rm ac}$ is the *rate of average crossings*, $r_{\rm sc}$ is the *rate of sharp changes*, and σ is the standard deviation. These metrics are related to the signal structure. Specifically, $r_{\rm ac}$ is the ratio of times when the signal crosses its average value to the block size, which is related to the periodicity of the signal. $r_{\rm sc}$ is the ratio of the number of sharp changes to the block size, which is related to the presence of duty-cycling appliances. The formal definitions of $r_{\rm ac}$ and $r_{\rm sc}$ are omitted here due to space constraints and can be found in [28]. σ indicates the level of dispersion in power consumption. These metrics can be efficiently computed by meters.

The objective is to determine the most efficient Ψ based on $\mathbf{f}$. As it is difficult to discover the statistical distributions for $\mathbf{f}$, statistical classifiers (e.g., Bayesian) are not applicable. Moreover, the classification based on complex decision boundaries of these classifiers will impose substantial computational overhead for meters, potentially negating the benefit brought by choosing Ψ dynamically. In our approach, we adopt a threshold-based *decision table* to determine Ψ from $\mathbf{f}$, which is a look-up table according to the results of comparing $r_{\rm ac}$, $r_{\rm sc}$, and σ with three thresholds (T_1, T_2, and T_3). Table II shows such a table. The thresholds T_1, T_2, T_3, and the last row of the decision table are obtained by a training algorithm based on a training data set. The details of the training algorithm are omitted here due to space constraints and can be found in [28]. Table II also includes the training results based on half of the data set described in Section IV-A. Table III reports the feature vectors for the signals shown in Fig. 2 and the Ψ chosen according to the decision table in Table II, which are the same as the optimal results. We note that the most efficient Ψ may not be consistent with the results shown in Fig. 3 (e.g., spiky and silent), which consider sparsity only. Fig. 6 plots the distortions under fixed Ψ and dynamic Ψ approaches, based on the other half of the data set. It also shows the distortions under the ground-truth optimal Ψ. Compared with fixed Ψ, a dynamic Ψ can reduce the distortion effectively for 15 blocks out of totally 90 blocks. For one block only, our approach chooses a Ψ that is not necessarily the optimal one.

We now discuss a few practical issues for the above dynamic Ψ approach. First, unlike many training-based approaches, our approach needs no ground-truth labels for the

TABLE III. STRUCTURE FEATURES AND CHOSEN REPRESENTATION BASES FOR THE SIGNALS SHOWN IN FIG. 2.

	duty-cycled	period	fluctuating	spiky	silent
r_{ac}	0.00586	0.01758	0.04297	0.39844	0.00391
r_{sc}	0.02051	0.04004	0.62402	0.19629	0.03516
σ	247.5	31.4	30.3	5.1	0.3
Ψ	Ψ_A	Ψ_D	Ψ_H	Ψ_H	Ψ_D

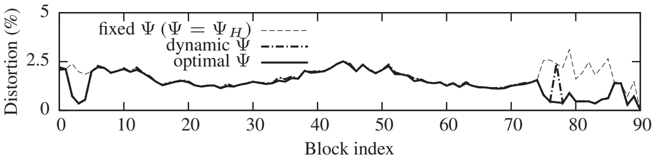


Fig. 6. Distortions of JICE with fixed Ψ, dynamic Ψ, and optimal Ψ.

training data, since the most efficient Ψ can be identified autonomously by the training algorithm, simply by comparing the distortion under different representation bases. Thus, the training can be fully automated. Second, the decision table can be updated periodically (e.g., hourly) by the gateway using the training algorithm and the recently reconstructed signals as training data, such that the WEAN can adapt to changing characteristics or usage patterns of appliances. The updated decision table has to be transmitted to the meter, but this introduces little overhead (14-byte payload in our implementation). In JICE, the gateway computes different decision tables for different meters based on their own data.

V. DATA SECRECY OF COMPRESSIVE SENSING

In this section, we first discuss the secrecy properties of CS, which reveal a vulnerability of leaking statistics. We then propose a perturbation approach to solving the vulnerability.

A. Adversary Model and Leak of Statistics under CS

The adversary model in this paper is that an eavesdropper can capture the wireless communications between a power meter and the gateway, from which the eavedropper aims to recover the original power signals. With the CS-compressed signals only, recovering the original signals is computationally hard, as long as the random measurement matrix Φ is kept secret [12], [19]. A symmetric secret key shared by the meter and the gateway can be used as the seed to generate Φ, where the symmetric key can be hard-coded or established using existing code libraries for key exchange (e.g., [29]) that are often based on public-key cryptography. We note that, although establishment of the symmetric key may introduce some overhead due to the complexity of public-key cryptography, it is a one-time procedure during system initialization only. Different symmetric keys can be established for different meters. As such, the leak of a single meter's key (e.g., by extracting from the memory of a physically captured meter) will not reveal the keys of other meters. A fixed Φ can be estimated by the adversary using regression techniques if she is able to launch known-plaintext attacks. In WEANs, known-plaintext attacks will need physical access to the power wires or retrofit to the meters, making them difficult and detectable. Nevertheless, the meter and the gateway can generate a new Φ every few blocks using the symmetric key, such that the adversary cannot accumulate enough data for the regression. Note that the generation of Rademacher and binary matrices requires little overhead. In our implementation of JICE (cf. Section VI), a new Φ is generated every block.

Although CS prevents the recovery of the original signal under the adversary model defined, we identify the following vulnerability of CS in leaking statistics of the original signal. We first discuss the cases where Gaussian and Rademacher matrices are adopted. By denoting y_i as the ith entry of $\mathbf{y}$, we have $y_i = \sum_{j=1}^{N} \phi_{i,j} x_j$, where x_j is the jth entry of $\mathbf{x}$ and $\phi_{i,j}$ is the (i,j)th element of Φ_G or Φ_R. For both Φ_G and Φ_R, the variance of $\phi_{i,j}$ is $\mathrm{Var}[\phi_{i,j}] = \frac{1}{M}$. As each $\phi_{i,j}$ is independent and identically distributed, we have $\mathrm{Var}[y_i] = \frac{1}{M}\sum_{j=1}^{N} x_j^2 = \frac{1}{M}\|\mathbf{x}\|_{\ell_2}^2$. Given $\mathbf{y}$, the unbiased sample variance of y_i for any i, denoted by s_y^2, is given by $s_y^2 = \frac{1}{M-1}\sum_{i=1}^{M}(y_i - \bar{y})^2$, where $\bar{y} = \frac{1}{M}\sum_{i=1}^{M} y_i$. As $\mathrm{Var}[y_i] \simeq s_y^2$, we can derive $\|\mathbf{x}\|_{\ell_2} \simeq \sqrt{\frac{m}{m-1}\sum_{i=1}^{m}(y_i - \bar{y})^2}$. In other words, the ℓ_2-norm of the original signal can be accurately estimated from the compressed signal. Based on the estimated $\|\mathbf{x}\|_{\ell_2}$, the adversary can further estimate bounds for the mean and standard deviation of $\mathbf{x}$ (denoted by $\bar{x}$ and σ_x respectively). As $x_i \geq 0$, $\bar{x} = \frac{1}{N}\|\mathbf{x}\|_{\ell_1}$. As $\|\mathbf{x}\|_{\ell_2} \leq \|\mathbf{x}\|_{\ell_1} \leq \sqrt{N}\|\mathbf{x}\|_{\ell_2}$, we have $\frac{1}{N}\|\mathbf{x}\|_{\ell_2} \leq \bar{x} \leq \frac{1}{\sqrt{N}}\|\mathbf{x}\|_{\ell_2}$. Moreover, as $\sigma_x = \sqrt{\frac{1}{N}\|\mathbf{x}\|_{\ell_2}^2 - \bar{x}^2}$, we have $\sigma_x \leq \frac{\sqrt{N-1}}{N} \cdot \|\mathbf{x}\|_{\ell_2}$. Note that $\bar{x}$ and σ_x represent important privacy information of the user.

We next discuss the case when the binary matrix is adopted. In this case, it is easy to verify that $\bar{x} = \frac{\sum_{i=1}^{M} y_i}{N \cdot S}$, since each column of Φ_B contains S ones. Thus, the CS based on Φ_B leaks the exact mean of the power consumption. Table IV shows an example of the leak of statistics. We can see that, when Φ_G is used, the ℓ_2-norm of the original signal can be accurately estimated. The estimated upper bound of $\bar{x}$ is close to $\bar{x}$. When Φ_B is used, the $\bar{x}$ can be exactly estimated.

B. Perturbation

To solve the vulnerability, we propose to perturb the power signal. In JICE, the meter and gateway have a shared secret key denoted by $k_p \in \mathbb{R}$. Define a perturbation vector $\hat{\mathbf{p}} = [k_p, 0, \ldots, 0]^{\mathrm{T}} \in \mathbb{R}^{N \times 1}$. Its time-domain counterpart is $\mathbf{p} = \Psi\hat{\mathbf{p}} = k_p\psi_1$, which can be pre-computed by the meter. The meter computes the sum of $\mathbf{x}$ and $\mathbf{p}$ to produce the perturbed signal denoted by $\widetilde{\mathbf{x}}$, i.e., $\widetilde{\mathbf{x}} = \mathbf{x} + \mathbf{p}$. The meter then applies CS to $\widetilde{\mathbf{x}}$ and transmits. As the sparsity of $\widetilde{\mathbf{x}}$, denoted by $\rho_{\widetilde{\mathbf{x}}}$, is at most $\rho + 1/N$, the extra distortion caused by the perturbation is almost negligible. Moreover, for DCT and HWT, the first transform coefficient corresponds to the lowest frequency component, which is typically non-zero. Therefore, the perturbation will not change the signal sparsity. As shown in Table IV that applies two settings for k_p, the perturbation does not lead to significant increases of distortion. As the gateway also knows $\mathbf{p}$, it can remove $\mathbf{p}$ from the reconstructed signal to obtain the original signal. When Φ_G or Φ_R is used, the adversary can estimate $\|\mathbf{x} + \mathbf{p}\|_{\ell_2} = \|\hat{\mathbf{x}} + \hat{\mathbf{p}}\|_{\ell_2}$, but cannot estimate $\|\hat{\mathbf{x}}\|_{\ell_2}$ since $\hat{\mathbf{p}}$ contains an arbitrary number k_p. When Φ_B is used, the adversary can estimate $\bar{x} + \frac{k_p}{N}\sum_{j=1}^{N}\psi_{1,j}$. As $\sum_{j=1}^{N}\psi_{1,j} \neq 0$ and k_p is an arbitrary number, the adversary cannot estimate $\bar{x}$. From the example shown in Table IV, with perturbation, the adversary's estimates for $\|\mathbf{x}\|_{\ell_2}$ and

TABLE IV. AN EXAMPLE OF PERTURBATION.

	Gaussian			binary
	ℓ_2-norm	$\bar{x}$	σ_x	$\bar{x}$
true value	13689	426.8	28.56	426.8
estimate (no perturb)	14445	[14.1, 451.4]	$\leq$451.1	426.8
estimate (k_p=5×10^3)	19773	[19.3, 617.9]	$\leq$617.6	601.3
estimate (k_p=5×10^5)	544336	[531.5, 17010.5]	$\leq$17002	16553.3
distortion (no perturb)	2.47%			2.27%
distortion (k_p=5×10^3)	2.47%			2.31%
distortion (k_p=5×10^5)	2.49%			2.44%

the bounds for $\bar{x}$ and σ_x depend on k_p and they are wrong. Moreover, the perturbation causes little extra distortion in the signal recovery.

VI. IMPLEMENTATION AND BENCHMARKING

We implemented JICE on a smart plug platform called SPlug [30]. An SPlug consists of a Kmote and a power sensor (ADI ADE7763). The Kmote consists of a TI MSP430F1611 MCU (8MHz clock rate and 10KB RAM) and a Chipcon CC2420 Zigbee radio, and runs the TinyOS operating system. To evaluate JICE, we implemented the pipeline approach discussed in Section III-B, a downsampling approach, and a lossless compression approach as baselines. We have released a code package [31] including all these implementations. This section presents the implementation details and summarizes the computation and storage overhead measurement results.

For all the approaches, data is represented as 4-byte integers or floating point numbers. To preserve data fidelity, we adopt a reliable transmission protocol [32], which retransmits a packet if its acknowledgment is not received in time.

JICE: JICE uses two buffers, an *output buffer* and a *transmission buffer*. The sizes of these two buffers are M. When the meter obtains a power reading, it generates a random number, multiplies it with the reading, and adds the result to an entry of the output buffer. For the same reading, it repeats this process for each entry of the output buffer. We generate Gaussian and Rademacher random numbers by Box-Muller transform and thresholding based on uniform pseudo-random numbers, respectively. For the binary measurement matrix, we implement the approach described in [27] to generate binary random numbers. For every N sensor readings, the meter stops sending from the current transmission buffer, switches the roles of the transmission and output buffers by swapping pointers to them (which avoids costly data copying), and starts transmitting from the new transmission buffer. Under this scheme, when the link quality deteriorates, the transmission buffer may not be fully processed when the output buffer is ready, leading to data loss. However, this scheme prevents the new data in the output buffer from being overwritten and ensures real-time metering. In a packet to the gateway, the meter piggybacks the dynamic selection of Ψ and a sequence number to synchronize the measurement matrix generations between the meter and gateway, which takes one byte payload.

Pipeline: The pipeline approach employs a wavelet-based lossy compression algorithm that captures the main principle of most lossy compression schemes. It first computes the transform $\hat{\mathbf{x}}$ from the original signal $\mathbf{x}$, then encodes the largest $\frac{M}{2}$ transform coefficients along with their positions in $\hat{\mathbf{x}}$, resulting in a total of M numbers. This approach employs the Advanced Encryption Standard (AES) algorithm, a representative symmetric-key cipher. Although the SPlug has built-in AES implementation in its CC2420 radio chip, this is not necessarily true of all meters. To preserve the generality of our results, we use a software implementation of AES [33]. In fact, our tests show that the built-in AES is slower than the software implementation. The pipeline approach has two variants regarding the implementation of transforms. A few transforms such as ADT and HWT have efficient implementations without resorting to matrix-vector multiplication. We refer to the resultant variant as *native pipeline*. Other transforms may involve intensive floating-point computation (e.g., cosine in DCT) that incurs unacceptable delays. Instead, they can be implemented as a multiplication of $\mathbf{x}$ and a pre-computed Ψ, which incurs $O(N^2)$ storage overhead, however. We refer to the resultant variant as *matrix pipeline*. We implement both the *native* and *matrix* versions of HWT, which allows us to understand the impact of storage overhead on the overall performance. The pipeline approach also uses a transmission buffer to coordinate data processing and transmission.

Downsampling: This approach transmits raw data to the gateway. For fair comparisons, we downsample the signal in this implementation to have the same transmission volume as those of the JICE and pipeline approaches. We use a circular queue to coordinate the sensor sampling and data transmission. A data packet encapsulating new sensor readings is added to the queue. An infinite loop removes a packet from the queue and transmits it to the gateway. When a new packet is available and the queue is full, the meter stops sending the oldest packet, removes it, and adds the new packet to the queue.

Lossless: This approach first applies SLZW [34], a lossless compression algorithm designed for embedded sensors, then applies AES to encrypt the compressed data. As the compression ratio of SLZW is unpredictable, the lengths of all the signal buffers are set to be N to prevent overflow.

We benchmark the computational and storage overhead of each approach. We use the *maximum sampling rate* (MSR) and *maximum block size* (MBS) to inversely characterize the computational and storage overhead, respectively. Specifically, MSR is the reciprocal of the average processing time for a single reading and MBS is obtained by increasing the block size until the RAM usage reported by the TinyOS compiler exceeds the RAM capacity. The benchmark details are omitted here due to space constraints and can be found in [28]. The measurement results show that 1) JICE with the binary and Rademacher matrices consistently outperforms the pipeline approach in terms of MSR; 2) JICE with the binary matrix leads to the highest MSR; and 3) JICE yields larger MBSs than the pipeline and lossless approaches. As JICE with the binary matrix incurs the lowest overhead, in our testbed experiments presented in Section VII, we adopt the binary matrix.

VII. TESTBED EXPERIMENTS

A. Experiment Methodology

We conduct extensive testbed experiments to compare the performance of the different approaches. To make the results of various approaches (e.g., the recovered signals) comparable, we need them to measure the same power signal. As an SPlug has both plug and socket interfaces, multiple SPlugs

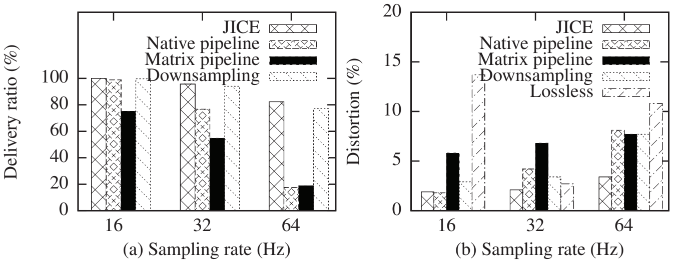


Fig. 7. Data delivery ratio and distortion vs. sampling rate ($\gamma = 4$).

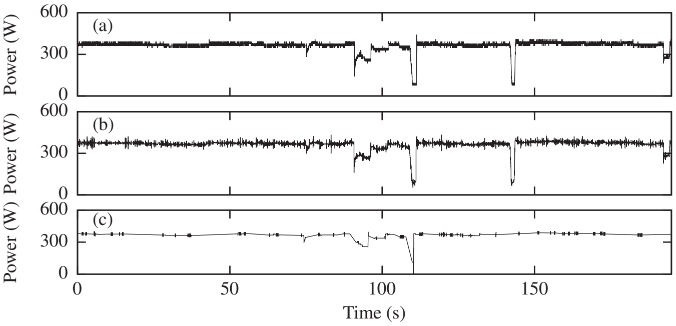


Fig. 8. An example of signal recovery. (a) Ground truth; (b) Recovered signal by JICE; (c) Recovered signal by native pipeline.

can be connected in series to measure the same appliance. We use five SPlugs loaded with JICE, native pipeline, matrix pipeline, downsampling, and lossless approaches, respectively, and a sixth SPlug loaded with a ground-truth data collection program. Each approach adopts its MBS obtained in the performance benchmark [28], to maximize its tolerance to link quality deterioration. The ground-truth SPlug transmits the raw data without any processing. We use two gateways, which are two Kmotes connected to two computers. The five SPlugs with the JICE and baseline approaches communicate with a gateway using the same Zigbee channel, while the ground-truth SPlug communicates with the other gateway using another Zigbee channel. We use our setup to measure the power consumption of a 29-inch LCD that repeatedly displays a video.

B. Experimental Results

1) Data Delivery and Fidelity: Fig. 7(a) shows the data delivery ratios of the various approaches under different sampling rates. We can see that the pipeline approaches do not scale well with the sampling rate. As the downsampling approach uses a large circular buffer which tolerates variable link quality, it yields comparable data delivery ratios as JICE. Note that as the lossless approach generates a variable number of packets, we omit its data delivery ratio. Fig. 7(b) shows the distortions of the signals recovered by the various approaches. Note that the gateway can detect lost packets from the sequence numbers in the received packets. Under JICE, the gateway uses the rows in $\mathbf{A}$ that correspond to the received data points only to recover the signal. For the pipeline approaches, the lost coefficients are set to zeros. For the downsampling approach, omitted and lost readings are interpolated. For the lossless approach, a whole block is discarded if any packets are lost since SLZW requires complete data for decompression. We can see that JICE generally yields the lowest distortions. An exception is the native pipeline approach when the sampling rate is 16 Hz. Under this setting, both JICE and native pipeline have nearly 100% data delivery ratios and hence their distortions are comparable. Fig. 8 plots segments of the ground truth and recovered signals by JICE and the native pipeline, at a sampling rate of 32 Hz and $\gamma = 4$. We can see that JICE well preserves the shape of the signal whereas the native pipeline approach has significant recovery errors.

We conduct another set of experiments similar to the one in Fig. 7, except that we fix the sampling rate to 64 Hz and vary the compression ratio. The results are shown in Fig. 9. When $\gamma = 2$, JICE has a smaller block size [28] and more data to be sent. As a result, JICE experiences a low data delivery ratio (38%). However, from Fig. 9(b), the distortion of JICE is just 4%. For JICE, the effect of packet loss is similar to that of choosing a larger γ. Therefore, the distortions of JICE for $\gamma = 2$ and $\gamma = 4$ are comparable since the data delivery ratio is doubled when γ increases to 4. In summary, JICE outperforms the baseline approaches in terms of distortion.

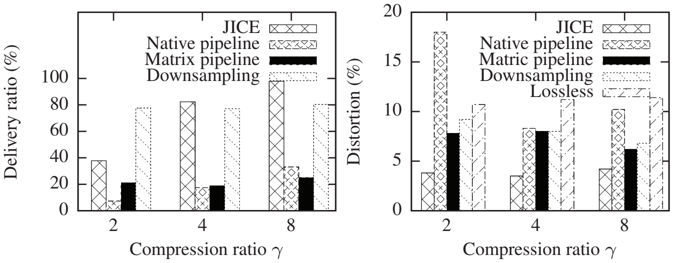


Fig. 9. Data delivery ratio and distortion vs. γ (sampling rate: 64 Hz).

2) Scalability: This section evaluates the scalability of JICE with respect to the network size. For this testbed experiment, we tune down the transmission power of the SPlugs to simulate long distances from the gateway in real large-scale networks. The resultant RSSIs at the gateway are within $[-40, -30]$, a typical range observed in practice when meters use the maximum transmission power. To simulate a large number of meters, we use several Kmotes as *traffic nodes*, which continuously transmit packets. Fig. 10 plots the data delivery ratio and distortion versus the number of traffic nodes, when the sampling rate is 8 Hz. JICE outperforms the native pipeline approach except when the number of traffic nodes is 4. Under this setting, both approaches have comparable delivery ratios and the pipeline approach has a slightly lower distortion. From Fig. 10(b), to maintain a distortion of 5%, JICE can increase the supported meters by 50%, compared with the pipeline approach. According to the generated traffic volume, each traffic node can be projected to 12 nodes running the JICE

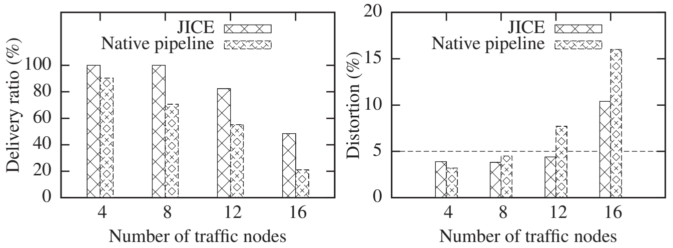


Fig. 10. Data delivery ratio and distortion vs. the number of traffic nodes ($\gamma = 4$, sampling rate = 8 Hz)

or pipeline approaches sampling at 8 Hz. Thus, to maintain a distortion of 5%, JICE supports up to 144 meters.

VIII. Conclusion and Future Work

This paper applied CS to jointly compress and encrypt measurements from wireless power meters in a WEAN. We designed JICE through analysis and extensive empirical studies based on real data traces. We developed a machine-learning-based lightweight algorithm to configure the representation basis of JICE dynamically to optimize performance. For privacy, we identifed leak of statistical information by CS and proposed a perturbation approach to solving the vulnerability. Extensive benchmarking and testbed experiments showed that JICE outperforms various baseline approaches under different realistic settings.

A. Discussion and Future Work

Many pervasive sensing applications based on capability-limited sensors face the same challenges in ensuring data fidelity and secrecy as WEANs. Examples include residential activity sensing and wireless medical monitoring. Sensors for residential activity monitoring often stream their high-resolution data to a central node for complex cognitive processing [4]. However, the data can reveal the user's daily activities, from usage of appliances [35], to keystroke sequence on a computer keyboard [36] if acoustic sensors are used, as in [4]. Mote-class body-worn sensors have been used for monitoring patients' vital signs (e.g., pulse) at low rates in general hospital units [37]. To support cardiac and epilepsy care that requires high-rate (up to 100 Hz) electroencephalography and/or acceleration measurements, compressing and encrypting this privacy-sensitive data become imperative. Although this paper focuses on WEAN, JICE can also be applied to these other emerging applications. Specific best choice of key CS elements such as representation basis and measurement matrix may be application specific. To address the challenge, in this paper we advance generic design elements, such as the dynamic representation basis configuration and the perturbation approach for privacy preservation, which can be readily applied to new application domains. Our future work will realize JICE for some of these other applications.

Acknowledgment

This work was supported in part by Singapore's Agency for Science, Technology and Research (A⋆STAR) under the Human-centered Cyber-physical Systems Programme, in part by Singapore MOE under grant SUTD-ZJU-RES-01-2013, and in part by NSFC under award 61429301.

References

[1] X. Jiang, M. V. Ly, J. Taneja, P. Dutta, and D. Culler, "Experiences with a high-fidelity wireless building energy auditing network," in *SenSys*, 2009.

[2] X. Jiang, S. Dawson-Haggerty, P. Dutta, and D. Culler, "Design and implementation of a high-fidelity AC metering network," in *IPSN*, 2009.

[3] S. Dawson-Haggerty, S. Lanzisera, J. Taneja, R. Brown, and D. Culler, "@scale: insights from a large, long-lived appliance energy wsn," in *IPSN*, 2012.

[4] D. E. Phillips, R. Tan, M.-M. Moazzami, G. Xing, J. Chen, and D. K. Y. Yau, "Supero: A sensor system for unsupervised residential power usage monitoring," in *PerCom*, 2013.

[5] M. Enev, S. Gupta, T. Kohno, and S. N. Patel, "Televisions, video privacy, and powerline electromagnetic interference," in *CCS*, 2011.

[6] S. S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu, and W. Xu, "Current events: Identifying webpages by tapping the electrical outlet," in *ESORICS*, 2013.

[7] BBC, "Smart meter project is delayed," http://bbc.in/1ptjSoq.

[8] Eaton, "Next-generation power quality meters," http://bit.ly/1B9QOst.

[9] I. Rouf, H. Mustafa, M. Xu, W. Xu, R. Miller, and M. Gruteser, "Neighborhood watch: security and privacy analysis of automatic meter reading systems," in *CCS*, 2012.

[10] E. J. Candès and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, 2008.

[11] D. Takhar, J. N. Laska, M. B. Wakin, M. F. Duarte, D. Baron, S. Sarvotham, K. F. Kelly, and R. G. Baraniuk, "A new compressive imaging camera architecture using optical-domain compression," in *IS&T/SPIE Electronic Imaging*, 2006.

[12] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Allerton Conf. Commun., Control, and Comput.*, 2008.

[13] M. Hatler, D. Gurganious, and C. Chi, "Smart building wireless sensor networks: A market dynamics report," ON World Inc., Tech. Rep., 2013.

[14] W. Bajwa, J. Haupt, A. Sayeed, and R. Nowak, "Compressive wireless sensing," in *IPSN*, 2006.

[15] C. Luo, F. Wu, J. Sun, and C. W. Chen, "Compressive data gathering for large-scale wireless sensor networks," in *MobiCom*, 2009.

[16] P. Misra, W. Hu, M. Yang, and S. Jha, "Efficient cross-correlation via sparse representation in sensor networks," in *IPSN*, 2012.

[17] Y. Shen, W. Hu, J. Liu, M. Yang, B. Wei, and C. T. Chou, "Efficient background subtraction for real-time tracking in embedded camera networks," in *SenSys*, 2012.

[18] X. Wu and M. Liu, "In-situ soil moisture sensing: measurement scheduling and estimation using compressive sensing," in *IPSN*, 2012.

[19] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, "On the security and robustness of encryption via compressed sensing," in *MILCOM*, 2008.

[20] S. Agrawal and S. Vishwanath, "Secrecy using compressive sensing," in *IEEE Information Theory Workshop*, 2011.

[21] E. Candes and J. Romberg, "Sparsity and incoherence in compressive sampling," *Inverse Problems*, vol. 23, no. 3, p. 969, 2007.

[22] "Reverse-engineering a smart meter," http://bit.ly/9v4nY8.

[23] "Security and cryptography in tinyos," http://bit.ly/11FqFkk.

[24] MathWorks, "Discrete cosine transform matrix," http://bit.ly/11yqSW1.

[25] ——, "Haar wavelet transform matrix," http://bit.ly/171YHXx.

[26] E. J. Candès, "Compressive sampling," in *International Congress of Mathematicians*, 2006.

[27] R. Berinde, A. C. Gilbert, P. Indyk, H. Karloff, and M. J. Strauss, "Combining geometry and combinatorics: A unified approach to sparse signal recovery," in *Allerton Conf. Commun., Control, & Comput.*, 2008.

[28] S.-Y. Chiu, H. H. Nguyen, R. Tan, D. K. Y. Yau, and D. Jung, "Jice: Joint data compression and encryption for wireless energy auditing networks," ADSC, Tech. Rep., 2015, http://bit.ly/1GSaxmU.

[29] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *IPSN*, 2008.

[30] Sonnonet, http://www.sonnonet.com.

[31] https://github.com/bigbitesaint/compress-sensing-nesc.

[32] "Packet link layer," http://bit.ly/11W2aPL.

[33] "Cryptography algorithms for tinyos," http://bit.ly/rwzDJT.

[34] C. M. Sadler and M. Martonosi, "Data compression algorithms for energy-constrained devices in delay tolerant networks," in *SenSys*, 2006.

[35] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *UbiComp*, 2008.

[36] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," in *CCS*, 2005.

[37] O. Chipara, C. Lu, T. C. Bailey, and G.-C. Roman, "Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit," in *SenSys*, 2010.