Shepherd: Sharing Energy for Privacy Preserving in Hybrid AC-DC Microgrids

Zhichuan Huang[*], Ting Zhu[*], Yu Gu[†], and Yanhua Li[‡]
[*]University of Maryland, Baltimore County
[†]IBM Watson Health
[‡]Worcester Polytechnic Institute

ABSTRACT

Renewable energy becomes increasingly popular due to its zero carbon dioxide emissions and increasing energy demand. To better utilize renewable energy, hybrid Alternative Current (AC)-Direct Current (DC) microgrids have been proposed because the most common renewable energy that can be harvested in residential homes is solar energy, which provides DC power. However, a major issue in a hybrid AC-DC microgrid is privacy leakage because power consumption information of each home can be exposed through the power lines or compromised neighbors in the microgrid. Power consumption data then can be used to reveal precise information about appliances' activities with non-intrusive load monitoring algorithms. To mitigate leakage of human behaviors in homes, battery-based load hiding (BLH) is widely studied. In this approach, a battery is used to store and supply energy to appliances to hide the actual power consumption. However, BLH requires to deploy large and expensive batteries at each home. In this paper, instead of using batteries, we propose to leverage the unique features of hybrid AC-DC microgrids to hide power consumption information. Specifically, we design *Shepherd*, a privacy protection framework to hide power consumption information from different types of power consumption detection techniques. To minimize energy transmission among neighboring homes, we provide an optimal offline solution and an efficient heuristic online solution. We conducted extensive system evaluations with 40 homes. Results indicate that our proposed approach can i) significantly reduce the detection ratio from 33% to 13% compared to BLH, and ii) effectively hide consumption information even with 25% compromised neighbors.

1. INTRODUCTION

With the increasing demand of energy consumption and the desire to reduce carbon dioxide emissions, renewable energy has become an important alternative choice. The government is encouraging the utilization of renewable energy and expects the renewable energy can reach up to 33% of total energy supply by 2020 [1] [2]. However, renewable energy that can be harvested in residential homes is typically DC power (e.g., solar energy), while the power grid nowadays is only providing AC power. In fact, many appliances in residential homes are operated using DC power, such as TVs, computers, DC water heaters and lighting. According to the government survey, these DC appliances consume around 20% to 30% energy in residential homes [3]. Furthermore, with the popularity of the electrical vehicles, the DC appliances will consume much more energy in residential homes. To utilize the renewable energy in existing AC power grid, DC power from renewable energy must be converted to AC and then converted back to DC again to power DC appliances. The conversion loss of DC-AC-DC can be as high as 50% [8]. Therefore, instead of using the existing AC grid, researchers are studying the possibility of the hybrid AC-DC microgrids, in which homes obtain AC power from existing AC power grid to power AC appliances (e.g., air conditioners, compressors, etc.) and utilize DC power from renewable energy (e.g., solar energy) and batteries to power DC appliances (e.g., TVs, computers, DC water heaters, etc.). The advantages of the hybrid AC-DC microgrids are: i) higher energy efficiency for DC appliances because DC appliances can directly use DC power, which reduces energy conversion from renewable energy of DC power to AC and conversion from AC power to DC to power DC appliances; ii) lower conversion loss for batteries because they can be charged and discharged in DC power; and iii) lower cost of utilizing renewable energy because with higher energy efficiency for DC appliances and lower conversion loss for batteries, the amount of renewable energy needed is smaller and the investment cost of renewable energy (e.g., solar panels) can be lower. Recently, system architecture of co-existence of AC and DC power lines has been proposed [20] and the homes in a microgrid can utilize DC power line to share renewable energy to minimize the energy cost [10]. It is highly possible that in the near future we will witness a paradigm shift from a centralized AC power grid to a hybrid AC-DC microgrids in residential communities. Therefore, it is essential to explore this frontier in advance.

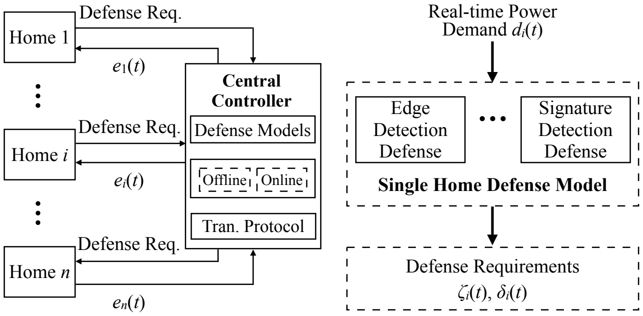
Although hybrid AC-DC microgrids have many advantages, they impose a major challenge on privacy leakage. This is because homes are connected to both AC and DC power lines, which provides vulnerability for malicious users to reveal power consumption information of neighboring homes in power lines. For example, illegal eavesdropping on the wireless communication of smart meters is investigated in [12]. In this paper, the authors discover two novel possible vulnerabilities for malicious users to obtain the accurate power consumption of individual homes under the infrastructures of the hybrid AC-DC microgrids: i) high accuracy power consumption leakage via voltage based on the power-voltage relationship; and ii) monitoring energy sharing from compromised homes in DC power line to obtain power consumption information of neighbors. Therefore, malicious users or third-parties can easily utilize these vulnerabilities to obtain the high granularity power consumption data of homes in the hybrid microgrids.

With the high granularity power consumption data, Non-Intrusive Load Monitoring (NILM) can be applied to analyze the data for revealing appliances' activities [9]. The widely used technique is the edge detection [11], which looks for the sharp edges that reveal the significant changes in the steady power consumed by the household. More seriously, we demonstrated a new signature detection technique which can reveal appliances' usage more accurately than existing approaches. Appliances usage information can then be used to reveal private information of occupants. For example, usage time of certain appliances (e.g., water heater) can reveal the number of people living in the home. Furthermore, changes of appliances usage patterns can also reveal private information (e.g., health conditions). For example, if a person usually turns off all the lights when he/she sleeps, and suddenly he/she turns on and off the lights frequently in the night while other appliances' usage patterns stay the same; this indicates that he/she may be sick or has a sleeping problem. Thus, it is critical to protect power consumption information and prevent privacy leakage for occupants in individual homes.

To achieve this, researchers proposed battery-based load hiding (BLH) algorithms in [13] [19], which utilize batteries to partially supply the net demand load from the home to alter the external load as seen by the smart meter. The battery is charged and discharged at a specific time to hide the power consumption. However, battery-based algorithms have three limitations: i) they have to cope with limited battery capacity and discharge rates or need batteries with large capacities; ii) they need to charge and discharge batteries frequently, which will significantly decrease the battery's lifetime; and iii) they lack a generic model for privacy preserving under different types of attacks. To overcome these limitations of BLH, we leverage the unique features of hybrid AC-DC microgrids and propose *Shepherd*, a privacy protection framework to effectively protect occupants' privacy. In Shepherd, we provide a generic model for energy consumption hiding from different types of detection techniques. We also propose a novel approach of coordinating AC and DC power lines to hide energy consumption in individual homes. Specifically, each home obtains partial energy from neighboring homes to power its DC appliances and hide its own power consumption information while protecting the actual power consumption information from its neighbors. Because power consumption collected by the smart meter of each home is different from the actual amount of energy consumed by its own appliances, the power consumption information of each home can be protected. To ensure that every home is correctly billed based on the amount of energy consumed by its own appliances instead of shared or obtained energy, we propose the energy sharing control protocol for control and billing. The main contributions of the paper are as follows:

• We study the privacy leakage problem in hybrid AC-DC microgrids and discover two novel vulnerabilities for malicious users to obtain power consumption information of individual homes without occupants' authentication.

• We leverage the unique features of hybrid AC-DC microgrids and propose Shepherd, a privacy protection framework to allow homes in a microgrid to coordinate with each other to hide power consumption information. Because different homes need to coordinate with each other, we also analyze how compromised neighbors in a microgrid can be used to provide energy consumption information to malicious third-parties. The corresponding defense models are proposed and we present an optimal offline solution and an efficient heuristic online algorithm so that the transmission loss is minimized.



(a) Architecture of Shepherd (b) Home Controller

Figure 1: Overview of Shepherd

• We conduct real-world experiments by deploying energy meters in multiple homes to collect the consumption signatures of individual appliances. We also run large-scale simulation with the empirical power consumption traces from 40 homes. Results show that Shepherd can i) significantly reduce the detection ratio from 33% to 13% compared to BLH, and ii) effectively hide consumption information even with 25% compromised neighbors.

The rest of the paper is organized as follows: the overview of Shepherd is introduced in §2; generic security models for energy consumption information hiding in a single home and with compromised neighbors are presented in §3 and §4; implementation and simulations are provided in §5; related work is discussed in §6; finally, we conclude the paper in §7.

2. OVERVIEW OF SHEPHERD

In this paper, we leverage the unique feature of hybrid AC-DC microgrids to enable homes to help their neighbors hide the power consumption information from the malicious third parties on the traditional power grid. To hide power consumption information for homes in a microgrid, we propose *Shepherd*, a privacy protection framework in hybrid AC-DC microgrids. The overview of our design is shown in Figure 1(a), which contains two components: a home controller at each home and a central controller.

The detailed design of the home controller is shown in Figure 1(b). It collects real-time power demand from smart meter measurements. Then we analyze the single home adversarial model based on different detection techniques of power consumption (§ 3.1). To defend from the adversarial model, we propose a generic single home defense model to calculate the amount of power required to defend from the single home adversarial model (detailed discussion in § 3.2). The defense requirements would be sent to central controller.

The central controller collects defense requirement from homes in the community in order to generate energy sharing solution for homes to defend from single home adversarial model. We also analyze the adversarial model with compromised neighbors in hybrid AC-DC microgrids (detailed discussion in § 4.1) and propose corresponding defense model to protect privacy of occupants (detailed discussion in § 4.2). The defense model is then illustrated as a convex optimization problem. To solve the optimization problem, we propose an optimal solution for energy sharing so that

Notations	Definitions
$d_i(t)$	Power demand of home i at t
$e_i(t)$	Real power consumption home i at t
c_i	Power capacity of home i
$\zeta_i(t)$	Min power increase to avoid both detections
$\delta_i(t)$	Min power decrease to avoid both detections
$p_i(t)$	Power difference between $d_i(t)$ and $e_i(t)$
$\eta_i(t)$	Energy transmission efficiency of home i at t
$m_j(t)$	Modelled power of appliance j at t
g_{ij}	Power of appliance j for edge detection at home i
$\rho_{ij}(t)$	Similarity between appliance signature j and $e_i(t)$

Table 1: Definitions of notations

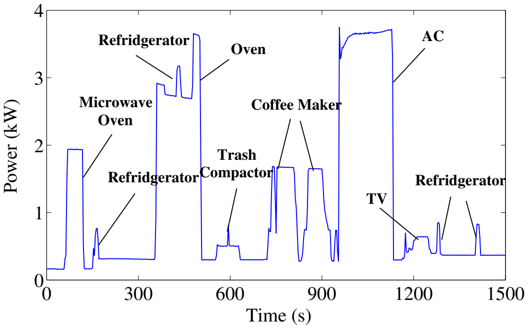


Figure 2: An example of detection results

the transmission loss can be minimized (detailed discussion in § 4.4). To further reduce the computation complexity, we also propose an efficient heuristic online algorithm (detailed discussion in § 4.5). The generated energy sharing solution will return to each home controller through transmission protocol (detailed discussion in § 4.6).

3. SECURITY MODEL IN A SINGLE HOME

In this section, we analyze the generic security models for power consumption information hiding in residential homes. We provide the adversarial model in a single residential home and propose the corresponding defense model. All the notations used in this paper are summarized in Table 1.

3.1 Single Home Adversarial Model

The single home adversarial model is to detect appliances' activities based on the real-time power consumption of a single home. The detection techniques are widely studied [14] and the key idea is to match detected power consumption with labelled power consumption of appliances. We present case studies for two representative detection techniques.

3.1.1 Edge Detection

Edge detection technique looks for significant changes in the energy being consumed by the household [19]. Such changes are characterized by sharp edges in the energy consumed by the appliances. These edges are then clustered and matched against known appliance profiles. Let power consumption of appliance k at home i for edge detection be g_{ik}, We define the appliance j detected by edge detection with power consumption $e_i(t)$ at home i as follows:

$$|g_{ij} - e_i(t)| = \min_k |g_{ik} - e_i(t)| \qquad (1)$$

For instance, if someone turns on/off a $20W$ lamp, then the net power consumption increases/decreases by $20W$. The algorithm detects the pair of edges with equal magnitude and opposite direction, and matches them against the electric profile for a $20W$ lamp.

3.1.2 Signature Detection

While edge detection methods are simple, they are often inaccurate, because they fail to capture the complex power usage patterns of different loads. Recently, researchers revealed the empirical power consumption signature of different electrical loads [5]. Electrical loads are categorized into five consumption signature models. With the energy consumption signatures of different appliances, we design a more efficient method than edge detection to reveal appliances' usage patterns with a home's energy consumption data. The key idea is to detect appliances' usage by the similarity between real power consumption and appliances' consumption models. If consumption model of an appliance a_i is most similar to real power consumption, then it is highly possible that appliance a_i is working but not other appliances. In this paper, we propose a Euclidean distance-based function to quantify the similarity between two vectors. Let $e(t)$ be the real energy consumption and $m_i(t)$ be energy consumption data generated by models at time t, where $length(a_i)$ is the signature length of appliance a_i. The similarity between two vectors can be calculated as:

$$\rho_i = \frac{1}{1 + l_{(e,m_i)}} \qquad (2)$$

where

$$l_{(e,m_i)} = \frac{1}{length(a_i)} \sum_{t=1}^{length(a_i)} (e(t) - m_i(t))^2 \qquad (3)$$

Equation (3) is used to calculate the distance between two vectors. Because different appliances' models have different lengths of signature sequences, we use $1/T$ to normalize the distance of two vectors. For example, the signature sequences of a lamp are short due to the on-off model; while the signature sequences of TV is long due to dynamic power consumption during usage. Equation (2) is used to transfer distance to similarity within range of [0, 1].

Based on the similarity between consumption models of different appliances and real consumption data, we detect the appliances' usage patterns. Suppose that appliance i has the highest similarity with real power consumption from time t, we then consider that appliance i is working. Because several appliances can be working at the same time, we can remove the detected appliance's model from real data and then repeat the detection process again. When the similarity between rest of appliances and real consumption is low, we end the detection process for time t and continue the detection process from the time when detected appliances stop working. An example of detection results are shown in Figure 2. In our experiment results, our proposed consumption signature detection method can detect appliances' activities 30% more accurate than edge detection method and can still detect 70% appliances' activities when the power consumption is processed with BLH.

Note that there are many other detection techniques too [4]. However, the detection techniques are mostly based on matching between detected power consumption and labelled power consumption, which provides us opportunities to alter power consumption to hide from these detection techniques.

3.2 Single Home Defense Model

To defend from the single home adversarial model, each home can increase or decrease its power consumption by sharing energy with neighbors in a microgrid. We define the minimum change of power consumption ζ (increase) or δ (decrease) as follows:

$$\zeta_i(t) = \min\{p \in \mathbb{R}_{>0} | A_i(e_i(t)) \neq A_i(e_i(t) + p)\} \quad (4)$$
$$\delta_i(t) = \min\{p \in \mathbb{R}_{>0} | A_i(e_i(t)) \neq A_i(e_i(t) - p)\} \quad (5)$$

$A_i(e_i(t))$ is the detected appliance based on power consumption $e_i(t)$ at home i with a given adversarial model. Equations (4-5) show that ζ and δ are the minimum change of power consumption to avoid detection from a given adversarial model. Here we present two case studies for the calculation of the minimum change of power consumption. Note that our defense model is generic. The minimum changes of power consumption for specific detection methods can be calculated based on Equations (4-5).

• For edge detection, we assume the appliance's modeled data $m_{i(j-1)}(t)$ $((m_{i(j-1)}(t) < d_i(t))$ with minimum $d_i(t) - m_{i(j-1)}(t)$ and appliance's modeled data $m_{i(j+1)}(t)$ $(m_{i(j+1)}(t) > d_i(t))$ with minimum $m_{i(j+1)}(t) - d_i(t)$. Based on Definition (1), we have the minimum change of power consumption $\zeta_i(t) = [m_{i(j+1)}(t) - d_i(t)]/2$ and $\delta_i(t) = [d_i(t) - m_{i(j-1)}(t)]/2$.

• For signature detection, we not only need to change power consumption based on current power consumption, but also power consumption in history because signature detection can detect appliances usage by their unique consumption patterns. The consumption signature is based on similarity of real consumption and model, thus we can hide power consumption based on minimizing the probability of detection. The key idea is to let the probability of detection decrease with new power consumption. Let $e_i(t)$ be the real power consumption, $d_i(t)$ be the power demand of the appliance, and $\rho_i(t)$ be the similarity of consumption and demand data, where $t = 1, 2, ..., T$. Then at time T, we need to make sure with $e_i(T)$ that $\rho_i(T) \leq \rho_i(T-1)$. To find minimum change of power change $\zeta_i^s(T)$ or $\delta_i^s(T)$, we first solve the equation $\rho_i(T) = \rho_i(T-1)$. With definition of similarity in Equation (2) and (3), we can rewrite the equation as:

$$\frac{1}{T}\sum_{t=1}^{T}[e_i(t) - d_i(t)]^2 = \frac{1}{T-1}\sum_{t=1}^{T-1}[e_i(t) - d_i(t)]^2 \quad (6)$$

Theorem 1. *There exist two solutions $e_i^1(T)$ and $e_i^2(T)$ of Equation (6), and $e_i^1(T) < d_i(T) < e_i^2(T)$.*

The detailed proof is in the Appendix. After solving Equation (6), we can calculate minimum power change. Let $e_i(T) < e_i^1(T)$, because $e_i^1(T) < d_i(t)$, with Equation (2) and (3), we have $\rho_i(T) \leq \rho_i(T-1)$. Thus $\zeta_i^s(T) = \sqrt{l_{(e_i,d_i)}(T-1)}$. Similarly, we can also have $\delta_i^s(T) = \sqrt{l_{(e_i,d_i)}(T-1)}$.

For the homes that need to defend against different detection techniques, we select the minimum change of power consumption as the maximum of minimum change of power consumption for all detection techniques. Note that our defense model is generic to any detection techniques. To defense a new detection technique, we only need to analyze the technique to obtain $\zeta_i(t)$ and $\delta_i(t)$, then our defense model can be applied to defend from the detection technique.

4. SECURITY MODEL WITH COMPROMISED NEIGHBORS

With the minimum power change calculated, we can ensure that the power consumption pattern cannot be detected by power consumption data collected by smart meter in a single home. However, in a hybrid AC-DC microgrid, homes can share extra energy from renewable energy through DC line. Thus, it is possible that some compromised homes can use their power consumption change to detect their neighbors' power consumption. In this section, we analyze the adversarial model with compromised neighbors and propose the defense model. Then we illustrate the defense model as a convex optimization problem and provide optimal and heuristic solutions.

4.1 Adversarial Model with Compromised Neighbors

With the compromised neighbors in hybrid AC-DC microgrids, it is possible that some homes can use their power consumption change to detect their neighbors' power consumption. For example, home i turns on the lamp for $20W$. To hide from edge detection, it finds the appliance with closest power consumption is laptop with $100W$. Then based on single home defense model, we have $\zeta_i = 40W$. In a microgrid, home i can share energy to home j and k for $20W$ to defense single home adversarial model. However, if home j is compromised by third-parties and provides them the information that home i shares $20W$ energy to home j. Then based on single home adversarial model, malicious third-parties can know the power consumption increase of home i is $40W$ instead of $60W$. Although it is not totally accurate as $20W$, malicious third-parties can detect lamp is turned on at home i but not laptop based on edge detection. We define the condition that compromised homes can reveal real appliances' activities of other homes.

Definition 1. *Let home set that home i shares energy to be D_i and compromised home set be C_i, the condition for adversarial model with compromised neighbors to work at time t is*

$$\sum_{j \in D_i \& j \notin C_i} p_j(t) \geq \zeta_i(t) \quad (7)$$

Clearly, if enough homes are compromised by malicious third-parties, the third-parties can get enough information of energy sharing among homes. Then with the energy sharing information, the appliances' activities can be with the power consumption of home i.

4.2 Defense Model with Compromised Neighbors

To defend from adversarial model with compromised neighbors, we propose that each home's power change should not be balanced by only one home, but several homes to hide power consumption from neighbors. Because homes do not know that which homes are compromised, we propose the defense model to avoid detection from given number of compromised neighbors. For practical solutions, we also propose an online solution in §4.5 to work under the scenario that the number of compromised neighbors is unknown. To avoid detection from k compromised neighbors for home i, we need to ensure that any k neighbors are compromised, the appliances' activities are still protected. We propose two approaches for defense model with compromised neighbors: i) sharing energy with more homes to reduce detection probability. Because it reduces the amount of energy shared to one single home, it also reduces the probability of detection from multiple homes adversarial model. ii) sharing the same amount of energy to other homes. If homes i shares more energy to home j and less energy to home k, when home j is compromised, home i may not be protected. If home i shares same energy to home j and k, any single home of j or k would not affect the protection of home i.

4.3 Problem Formulation of Defense Models

Because we need to hide power consumption from detection techniques, the amount of power consumption to be hidden is determined by detection techniques. We already gave the formulation to calculate the minimum power change to avoid those detection techniques. A simple approach is to generate random power consumption for each home to avoid those detection techniques. Then the power consumption to be hidden can be calculated by real power consumption and generated random power consumption. The problem is to generate random power consumption for each home, which would require homes to either i) use large batteries to randomize power consumption; or ii) exchange a lot of energy among homes. Solution i) is limited because large batteries cost lots of money and the capacity of batteries decreases with frequent charging and discharging operations. Solution ii) may be limited because each home has its own maximum power consumption from the power grid and energy transmission introduces some transmission loss. Thus we try to minimize the energy to be transferred to hide the power consumption information of each home.

Based on the above definitions and defense models, we theoretically formulate the problem and illustrate it as a convex optimization problem. The design goal is to minimize energy transmission in alternative local power lines while hiding power consumption information of homes from both the utility company and their neighbors:

We categorized homes in a hybrid AC-DC microgrid and define two terms as follows:

- **Supplier set $\boldsymbol{S}$**: A set of homes in a microgrid that need to hide power consumption information by decreasing their power consumption.
- **Demander set $\boldsymbol{D}$**: A set of homes in a microgrid that need to hide power consumption information by increasing their power consumption.

Note that a home can increase its power consumption at one time and decrease its power consumption at another time; thus, a home can belong to different sets at different time.

$$
\begin{array}{lll}
\min & \sum_{i=1}^{N} |p_i(t)| & (3.1) \\
s.t. & \sum_{i=1}^{N} p_i(t) \cdot \eta_i(t) = 0 & (a) \\
 & p_i(t) \geq \gamma \cdot \zeta_i(t), \;\; i \in S & (b) \\
 & p_i(t) \leq \gamma \cdot \delta_i(t), \;\; i \in D & (c) \\
 & p_i(t) + p_j(t) \geq \gamma \cdot \zeta_i(t), \;\; i \in S; \;\; j \neq i & (d) \\
 & p_i(t) + p_j(t) \leq \gamma \cdot \delta_i(t), \;\; i \in D; \;\; j \neq i & (e) \\
 & d_i(t) + p_i(t) \leq c_i, \;\; i = 1, ..., N & (f)
\end{array}
$$

$\eta_i(t)$ is the energy efficiency of home i at time t. If home i supplies energy to other homes, then $\eta_i(t) = 1$; if home i demands energy from other homes, then $\eta_i(t)$ is the transmission efficiency between home i and its suppliers. Constraints (b) and (c) indicate that the power change of each home is larger than the minimum power change to defend against detection models. Constraints (d) and (e) indicate that even with one neighbor's real power consumption data, the power consumption data of other homes still can be protected. γ is used to control power consumption to hide. To hide appliances' usage patterns, γ should be larger than 1. Constraint (f) indicates that the real power consumption of each home should not exceed its own maximum power consumption. Because all the constraints are linear functions, which are always convex; and the objective function is also convex, our problem is a convex optimization problem.

4.4 Optimal Solutions

With the formulation of defense models, in this section, we develop an optimal solution with convergence and complexity analysis.

4.4.1 Barrier Method

To solve the convex optimization problem, we use the barrier method to provide an optimal solution. The key idea of the barrier method is to make the inequality constraints implicit in the optimization objective and convert the original problem into a sequence of linear equality constrained minimization problems. The solutions of these linear equality constrained minimization problems are called central points in the central path related to the original problem. The central point will be more accurately approximated to the optimal solution as the parameter s increases. For the minimization problem (3.1), we first need to remove all inequality constraints into a logarithmic barrier function $\phi(\boldsymbol{p})$:

$$
\begin{aligned}
\phi(\boldsymbol{p}) = & -\sum_{i=1}^{N} log(c_i - p_i(t) - d_i(t)) \\
& - \sum_{i \in S} (log(p_i(t) - \gamma \cdot \zeta_i(t)) + \sum_{j \neq i} log(p_i(t) + p_j(t) - \gamma \cdot \zeta_j(t))) \\
& - \sum_{i \in D} (log(-p_i(t) + \gamma \cdot \delta_i(t)) + \sum_{j \neq i} log(-p_i(t) - p_j(t) + \gamma \cdot \delta_j(t)))
\end{aligned}
\quad (8)
$$

Then we write $f(\boldsymbol{p}) = \sum_{i=1}^{N} |p_i(t)|$ and rewrite the minimization problem with a certain parameter s as:

$$
\begin{array}{lll}
\min & \psi(\boldsymbol{p}) = -s \cdot f(\boldsymbol{p}) + \phi(\boldsymbol{p}) & (4.1) \\
s.t. & \boldsymbol{Ap} = 0 & (a)
\end{array}
$$

where

$$
A_{i,j} = \begin{cases} 1 & i = j \\ 0 & otherwise \end{cases} \quad (9)
$$

The optimal solution to problem (4.1) is an approximation of the original problem. As s increases, the approximation is much closer to the optimal solution. At the centering step of the barrier method, Newton's method is employed to compute the central point.

The details of algorithm are described in Algorithm 1. First, we need to find a feasible starting point that satisfies the constraint of Equation (Line 1). Then we select proper α and β to apply Newton's method (Lines 2-3). With Newton's method, we calculate centering path until $\lambda^2/2 \geq \varepsilon_n$ is fulfilled (Lines 4-11). Then we update p and $p^\star(s)$ (Lines 12-13). Finally, we check if threshold ε is fulfilled, if not, increase t by μ; otherwise, the algorithm ends (Lines 14-17).

Algorithm 1: Barrier Method

```
Input: Home's $d$, $c$ and $\delta$ and $\zeta$
Output: Home's $p$.
 1: Find strictly feasible point $p$, $s \geq 0$, tolerance $\varepsilon \geq 0$,
    $\mu \geq 1$;
 2: Centering path: Compute $p^{\star}(s)$;
 3: Starting point $p$, subject to $Ap = 0$, tolerance
    $\varepsilon_n \geq 0, \alpha \in (0, 1/2), \beta \in (0, 1)$;
 4: Compute $\Delta p$ and $\lambda = - \bigtriangledown \psi_s(p)\Delta p$;
 5: if $\lambda^2/2 \geq \varepsilon_n$ then
 6:     Go to Line 4;
 7: end if
 8: Backtracking line search on $\psi_s(p)$ and $h = 1$;
 9: while $\psi_s(p + h\Delta p) \geq \psi_s(p) - \alpha h \lambda^2$ do
10:     $h = \beta h$;
11: end while
12: Update $p = p + h\Delta p$;
13: Update $p^{\star}(s) = p$;
14: if $(N + 2)/t \geq \varepsilon$ then
15:     Increase $s = \mu s$;
16:     Go to Line 2;
17: end if
```

4.4.2 Solution Analysis

With the barrier method, it is guaranteed that we can achieve any desired accuracy we need. In this section, we analyze the number of iterations to converge to our desired accuracy and computation complexity.

Convergence Result. Given the desired accuracy $\varepsilon \geq 0$, the convergence speed can be calculated by using Theorem 2.

Theorem 2. *The centering steps to achieve a desired accuracy ε is:*

$$I = \frac{log(m/\varepsilon s_{(0)})}{log\mu} \tag{10}$$

where $s_{(0)}$ is the original s we choose and m is the number of inequality constraints which in our case is $N+2|S|+2|D|$, Convergence analysis for the barrier method is straightforward. Assuming that $sf_0 + \phi$ can be minimized by Newton's method for $s = \{s_{(0)}, \mu s_{(0)}, \mu^2 s_{(0)}, \cdots\}$, the duality gap after the initial centering step, and k additional centering steps, is $m/(\mu^k t^{(0)})$. Thus, the centering steps to achieve ε are $\frac{log(m/\varepsilon s_{(0)})}{log\mu}$. The detailed proof can be found in [6].

Algorithm Complexity. The computational complexity of the barrier method is mainly for the computation of Newton's method that needs matrix inversion with the complexity of $O(N^3)$. However, because we don't know whether a home should be a supplier or demander to minimize the total energy transmission, we need to try every combination of the homes' status, which can be 2^N combinations, then the complexity of the offline solution will be $O(2^N \cdot N^3)$.

4.5 Online Solutions

To reduce the complexity of the offline solution, we propose an efficient heuristic algorithm. Furthermore, the offline solution does not require the information of the number of compromised neighbors. The key idea is that when a home shares power to another home, the amount of power should be larger than its minimum power change, and less than enough to detect other homes' power consumption.

Algorithm 2: Heuristic Algorithm

```
Input: Home's $\delta$ and $\zeta$
Output: Home's $p$.
 1: Fetch home $i$ with largest value of $\delta_i$ or $\zeta_i$;
 2: Calculate minimum energy transmission needed $r_i$ and
    number of homes needed $n_i$ in Algorithm 3;
 3: if $i \in$ D then
 4:     for Home $j$ in F and S do
 5:         Fetch home $j$ with largest value of $\zeta_j$;
 6:         $\zeta_j = \zeta_j - r_i/n_i$; $\delta_i = \delta_i - r_i/n_i$;
 7:         Add ($j$, $i$) to energy sharing pair;
 8:     end for
 9: else
10:     for Home $j$ in D do
11:         Fetch home $j$ with largest value of $\delta_j$;
12:         $\delta_j = \delta_j - r_i/n_i$; $\zeta_i = \zeta_i - r_i/n_i$;
13:         Add ($i$, $j$) to energy sharing pair;
14:     end for
15: end if
```

Theorem 3. *If k homes are selected to share energy to home i, to avoid detection from l compromised neighbors, $l + 1$ homes should at least share $\zeta_i(n)/(k - 1)$ to home i.*

Proof. k homes are selected to share energy with home i. To avoid detection from l compromised neighbors, any $k - l$ neighbors should share more energy than $\zeta_i(n)$. Then for first $k - l$ neighbors, at least one home k_1 shares more energy than $\zeta_i(n)/(k-l)$. Similarly, $k-l$ neighbors without home j should also share more energy than $\zeta_i(n)$ to avoid detection, therefore, there would be another l homes that share more energy than $\zeta_i(n)/(k-l)$. Finally, at least homes k_1 and other l homes share more energy than $\zeta_i(n)/(k - l)$ with home i. □

Based on Theorem 3, we can have a basic idea of the total energy transmission with k homes shared to home i. This is because there are l homes which share more than $\zeta_i(n)/(k-l)$ and any $k-1$ neighbors share more than $\zeta_i(n)$. Thus, for k homes, the total energy shared to home i should be larger than $\zeta_i(n) \cdot k/(k - l)$. Because $k/(k - l)$ decreases with the increase of k, it would be better to hide the real power consumption with more homes to reduce energy transmission. Based on the result, we propose an online solution for calculating real-time energy sharing pairs. The overview of online solution is shown in Figure 3. Because sharing energy with more homes can reduce energy transmission, we find the maximum number of homes to share energy with minimum transmission. Let r_i be the minimum transmission of n_i homes to protect home i, we have

$$r_i = \frac{n_i}{n_i - 1}\zeta_i + \sum_{\delta_j < \frac{1}{(n_i-1)}\zeta_i} (\frac{1}{(n_i - 1)}\zeta_i - \delta_j) * (n_i - 1) \tag{11}$$

Then we check if all the homes are protected, if yes, then our solution ends, otherwise, it assigns energy sharing pairs and update $\zeta_i(t)$ and $\delta_i(t)$ and then continue the process again until all the homes are protected.

Algorithm 2 is proposed to calculate the amount of real-time shared energy. First, we fetch the home with the largest value of δ_i or ζ_i (Line 1). We then use Algorithm 3 to calculate the minimum energy transmission needed and number of homes needed (Line 2). If home i is a demander, then we find a match in supplier set S and free set F, and update the power change they need (Lines 3-8). If home i is a supplier, then we find a match in demander set D, and update power changes they need (Lines 9-15).

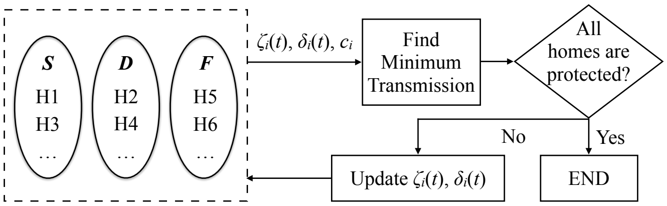

S
H1
H3
…
D
H2
H4
…
F
H5
H6
…
$\zeta_i(t)$, $\delta_i(t)$, c_i
Find Minimum Transmission
All homes are protected?
No
Yes
Update $\zeta_i(t)$, $\delta_i(t)$
END

Figure 3: Overview of online algorithms (*S* and *D* is the set of homes that need to hide consumption by increasing and decreasing their power consumption; *F* is the set of homes that do not need to hide power consumption)

Algorithm 3: Calculation of Minimum Energy Transmission

```
Input: A homes' $d_i$, $c_i$, $\delta_i$ and $\zeta$ of homes in F and S
Output: Minimum energy transmission $r_i$ and number of homes needed $n_i$.
 1: Fetch two homes in F and S with largest $\zeta_j$ and $\zeta_k$;
 2: $r_i = \delta_i$; $n_i = 2$;
 3: for Home $j$ in F and S do
 4:     Fetch $n_i + 1$ homes $j$ with largest value of $\zeta_j$;
 5:     Calculate $r'_i$ for $n_i + 1$ homes based on Equation (11);
 6:     if $r'_i > \theta \cdot r_i$ then
 7:         break;
 8:     else
 9:         $r_i = r'_i$, $n_i = n_i + 1$;
10:     end if
11: end for
```

Because we need to minimize energy transmission, another problem is to find the minimum energy transmission for each home. The detailed algorithm is described in Algorithm 3. Because a single home cannot provide protection by itself, the first step is to calculate the minimum energy transmission with two homes (Lines 1-2). Then we increase the number of homes to hide the power consumption of home i (Lines 3-5). If the energy transmission increases, we select two homes for energy transmission; otherwise, we continue to find the minimum energy transmission by increasing the number of homes (Lines 6-11). θ is used to control the number of homes to hide the power consumption of home i. Because it is more likely to hide power with more homes, a larger θ can decrease the detection ratio with one compromised neighbor.

4.6 Energy Sharing Control

With the solutions described in above, we can calculate how much energy each home should share to its neighbors to protect privacy. However, energy sharing in the microgird introduces billing issues among homes. Thus, we present how homes only pay the utility company for their actual power consumption which does not include energy sharing.

To ensure homes share energy based on results generated by our solution, we develop a transmission protocol to schedule energy transmission. The detailed communication protocol is shown in Protocol 4. The controller first collects energy data for every interval w and runs Algorithm 2 and 3 to get the sharing results (Line 1). Then it sends TRANS_START and power consumption results to the homes (Line 2). It monitors TRANS_END signal from homes to ensure power consumption for every home is correctly stored in order to calculate bills for each home (Line 3). The last thing for the central controller is to send TRANS_END to all homes after interval w (Line 4). For every home, it sends energy data to the controller at a new window (Line 1). It then waits for TRANS_START signal to start power consumption (Line 2) and sends back power consumption details to the controller after a TRANS_END signal. The controller needs consumption details to calculate bills for each home. The TRANS_START signal should contain the home id and amount of energy while TRANS_END signal should contain the home id and amount of energy each home consumes.

Protocol 4: Energy Transmission Protocol

```
For controller
1: Collect energy data from homes and execute
   Algorithm 2 and 3 for every interval $w$;
2: Send TRANS_START and energy consumption
   instruction to homes;
3: If receive TRANS_END from home $i$, store energy
   consumption for home $i$;
4: If time $w$ runs out, send TRANS_END to homes.
For every home
1: Send energy data to controller;
2: If receive TRANS_START, consumes energy according
   to instruction from controller.
3: If receive TRANS_END, send back energy consumption
   details.
```

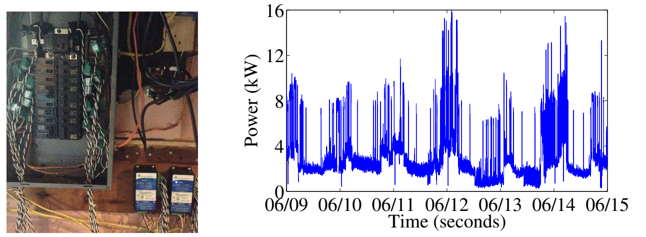
We then show that the utility company can still charge homes for their actual power consumption without energy sharing. The current price model of the utility company charges consumers based on power consumption at every window (for example every hour). The controller can add the amount of energy home i shared to other homes and get from other homes the aggregated amount of energy each home consumes in the previous window. The utility company can charge homes with the readings from smart meters for every window. Because the controller has the differences between real power consumption without sharing and readings from smart meters, it can charge homes with their real power consumption instead of reading from smart meters. Note in our paper, we consider that the data in controller is not publicly available and the controller also deletes power consumption every window after billing calculation.

5. IMPLEMENTATION AND EVALUATION

In this section, we evaluate the performance of Shepherd. We collect the empirical data of power consumption from 40 homes and load events at one home. Then we evaluate the detection ratio and energy transmission of our solutions compared to existing approaches. Finally, we verify that our approach also works well using the microgrids with homes of similar power consumption patterns.

5.1 Data Collection

We deploy eGauge power meters at individual homes to collect the total power consumption data every one second. Experiment setup at one home is shown in Figure 4(a). In our simulation, we use the power consumption traces that we collected from 40 homes. We also collect the load events of one home to get the consumption signature of all the electrical loads (e.g., TV, oven, etc.). With the collected consumption signature, other homes' load events are detected as ground truth.



(a) Setup of energy measurement (b) Power consumption of one home in six days

Figure 4: Experiment setup and data collection

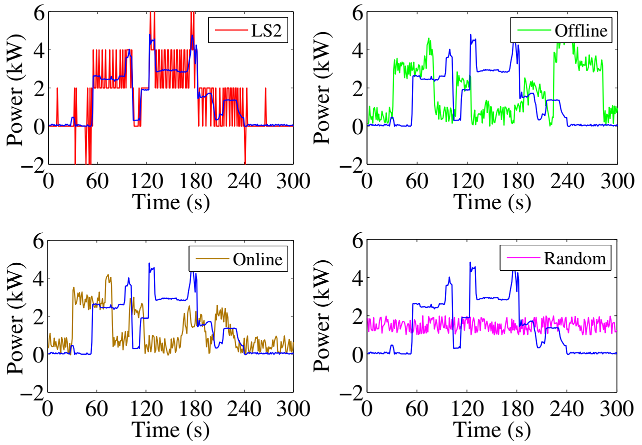


Figure 5: Original load and hidden load (blue lines in figure are original load)

5.2 Evaluation Baseline and Metrics

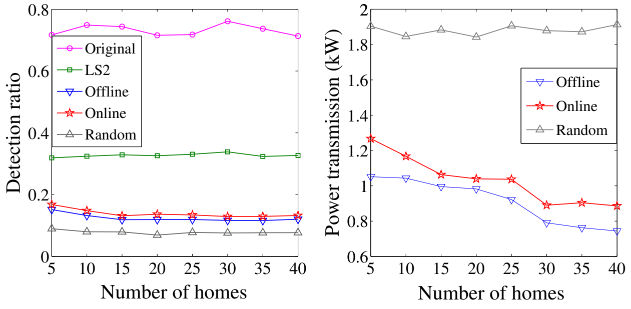
Baselines. To verify the efficiency of Shepherd, we compare Shepherd with two baselines. i) Battery-based stepping algorithm (LS2) [19]. Yang et al. proposed four battery-based algorithms to hide power consumption. In our paper, we select LS2 because LS2 performs the best in most scenarios. ii) Random energy sharing. Each home aims to randomize its power consumption by energy sharing.

Metrics. We use two metrics to evaluate the performance: i) **detection ratio**: the number of events detected divided by the total number of events; ii) **power transmission**: average power transmission over the additional AC line.

5.3 Basic Evaluation Results

In this section, we evaluate the effectiveness of our proposed offline and online solutions. All results are simulated with six days empirical data of power consumption. The battery we use to implement LS2 algorithm has $1kWh$ capacity and $2kW$ maximum charging rate. The parameter γ and θ are both selected as 1 in this set of simulations.

Power Consumption. We show the power consumption of four algorithms with comparison of the original loads in Figure 5. To make the difference between four algorithms' consumption visible, we show only 300 seconds of consumption data in one home. The LS2 tries to maintain power consumption at certain levels, thus its consumption can be only -$2kW$, $0kW$, $2kW$, $4kW$ and $6kW$. However, we can still find that the shape of LS2 is similar to the original load. For offline and online solutions, we can find their consumption is totally different. Because their consumption is either sharing energy with other homes or shared by other homes. Most of the time, power consumption for the online and offline solutions are similar. For the random algorithm, each home tries to consume random amount of energy at any time, thus it has no relationship with the original load.



(a) Detection Ratio (b) Power transmission

Figure 6: Detection ratio, power transmission for 40 homes

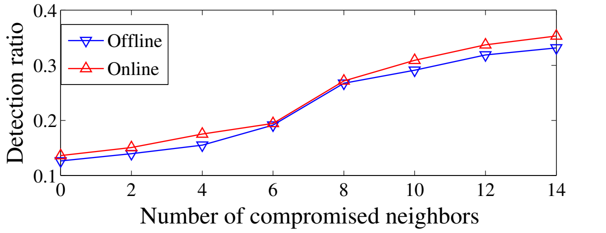


Figure 7: Detection ratio with compromised neighbors

Detection Ratio. With power consumption results of four algorithms, we then use both edge and signature detection methods to detect load events. The average detection ratio of 40 homes is shown in Figure 6(a). Because with LS2, the power consumption shape is still similar to the original load, it can be detected by signature detection method. Because LS2 is adjusting power consumption at each home, detection ratio is not relevant to the number of homes. For offline and online solutions, the detection ratio gradually decreases with the increase in the number of homes. This is because with more homes in a microgrid, it is more likely you can find some homes to share energy. Power consumption with the random algorithm is not relevant with original consumption, thus detection ratio is low.

Power Transmission. Because we propose energy sharing to hide power consumption for homes, we also evaluate the amount of energy transmission for offline, online, and random algorithms. Even though random algorithm can achieve lower detection ratio, we show in Figure 6(b) that it costs nearly two times of energy transmission than online and offline solutions, which increases the burden of DC line and produces more transmission loss. This means that for one day, the random algorithm needs to transfer energy $20.47kWh$ more than offline and $15.28kWh$ more than online solutions. Assuming that energy transmission loss through AC line is as low as 1%, it wastes 5-$6kWh$ in a month.

5.4 Advanced Evaluation Results

In this section, we evaluate our design for homes with compromised neighbors in the community, similar power consumption patterns and different parameter settings to verify the robustness of our design.

5.4.1 Impact of Compromised Neighbors

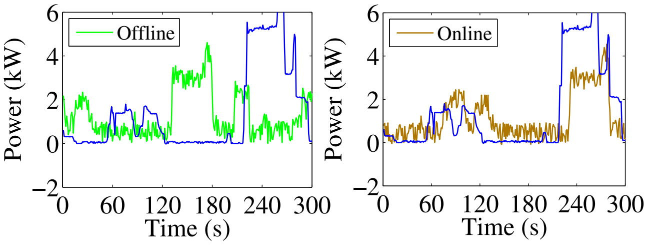
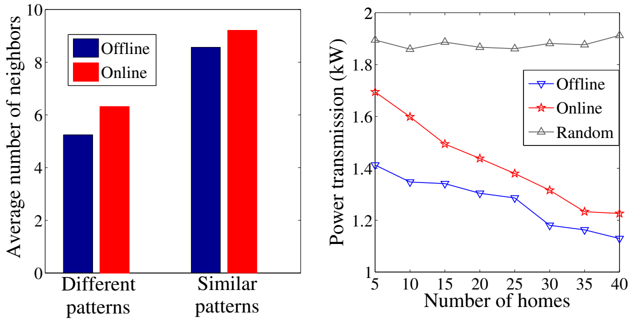


Figure 8: Original load and hidden load with similar consumption pattern (blue lines are original load)



(a) Avg. number of neighbors (b) Power transmission

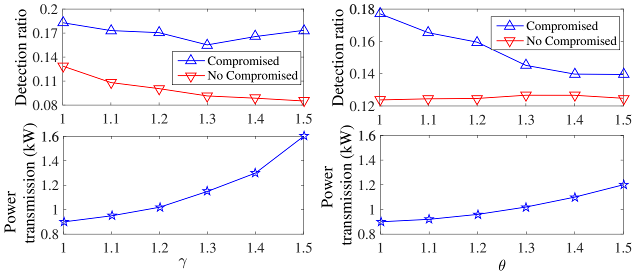
Figure 9: Average number of neighbors and power transmission with similar consumption pattern

Because homes share energy with each other to hide power consumption, homes can reveal a portion of their power consumption information to their neighbors in a microgrid. Thus we also evaluate if neighbors are compromised, whether homes in the microgird can still hide power consumption. Because homes randomly share energy in random algorithms, neighbors do not reveal much information, we only evaluate online and offline solutions for 40 homes in the microgrid. The results are shown in Figure 7. With more compromised homes, the detection ratio of two solutions increases. However, even with 10 compromised homes (25% of total homes), the detection ratio of Shepherd is still lower than LS2.

5.4.2 Impact of similar consumption pattern

The consumption data we used in the above simulations comes from 40 different homes. Thus, their consumption patterns can be different and provide us an opportunity to balance energy transmission over AC line by consuming energy at different times. However, when homes have similar consumption patterns, homes may not be available for hiding power consumption for other homes. In this section, we use data of 40 homes with similar consumption pattern to verify that our design also works in this scenario.

We show the power consumption of online and offline algorithms in comparison to the original loads in Figure 8. For LS2 and random algorithm, the results are the similar because LS2 and random algorithm do not take advantage of neighbors' power consumption. However, for offline and online solutions, we can find their consumptions are quite similar to the consumption that shifts the original load over some time. This is because when homes have similar consumption patterns, our solutions shift power consumption for some time to avoid detection.



(a) Impact of γ (b) Impact of θ

Figure 10: Impact of differenet parameters

The results are almost the same for detection ratio of online and offline solutions. Thus, only average power transmission of 40 homes are shown in Figure 9(b). The average power transmission of online and offline solutions increases only with $0.1kW$ and $0.16kW$ and the gap between two solutions also increases. Overall, even in scenario where homes have similar consumption patterns in a microgrid, our proposed approach can achieve relatively low detection ratio and power transmissions. We also show the average number of neighbors for energy sharing for similar and different energy patterns in Figure 9(a). For homes with similar energy patterns, each home needs to find more homes to share energy because many homes have similar sharing needs. Thus, average number of neighbors for energy sharing increases from around 5-6 (different energy patterns) to 8-9 (similar energy patterns).

5.4.3 Impact of different parameters

In basic evaluation results, the detection ratio with or without compromised neighbors is still around 15%. In reality, some homes especially some business buildings may need to protect their information better. In our design, we allow the user to tune the parameter γ to achieve even lower detection ratio and the parameter θ to achieve lower detection ratio with one compromised neighbor.

The detailed results for impact of γ and θ are shown in Figure 10(a) and 10(b). With a larger γ, homes try to hide more energy from real power consumption, thus the detection ratio decreases. However, it does not help to decrease the detection ratio with compromised neighbors. This is because that with larger γ, every home hides more energy but still with the same neighbors. Then with compromised neighbors, the detection ratio is still high. For average power transmission, it increases since more energy transmission is needed to hide more energy.

With a larger θ, homes try to hide energy with more homes, thus even with compromised neighbors, the detection ratio decreases. However, it does not try to hide more energy for any home, thus the detection ratio without compromised neighbors is stable. For average power transmission, it increases with larger θ. This is because it needs more energy transmission when hiding energy with more homes. However, the increase of average power transmission for a larger θ (1.32kW for $\theta = 1.5$) is much less than with larger γ (1.68kW for $\gamma = 1.5$). However, combined with larger γ and θ, our design can achieve low detection ratio both with and without compromised neighbors.

6. RELATED WORK

This work aims to protect the privacy of power consumption data in a microgrid. The related work includes:

• **Non-Intrusive Load Monitoring**. The large-scale placement of smart meters has introduced leakage of private and valuable information about occupants' activities [7]. NILM algorithms have been widely used in the research of residential settings to reveal the usage of individual appliances with consumption data [14]. In [11], NILM algorithms are extended to evaluate the threat to individual privacy by considering the results on potential disclosure from smart-meter data. An off-the-shelf statistical technique is used to develop a simple approach to discover people's life patterns [4]. In this paper, we develop a new detection technique based on the consumption signature of appliances that achieves a higher detection ratio.

• **Battery-Based Load Hiding**. The basic idea of BLH is to use a rechargeable battery to store and supply power to home appliances at strategic times to hide the appliances' consumption from smart meters [19]. The BE algorithm [16] tries to avoid charging the external load whenever possible, and when the actual demand is different from the external load, the battery can be charged or discharged to counteract the difference. The NILL algorithm [13] has three states and attempts to maintain a different constant load for each state.

Instead of using batteries, we propose a battery-free approach, which addresses the limitations of the above approaches. By leveraging the alternative local power line built in a microgrid, our online and offline solutions can enable homes to share energy with their neighbors to hide the real power consumption from the malicious third parties.

7. CONCLUSION

In this paper, we study the privacy leakage problem in hybrid AC-DC microgrids and discover two novel vulnerabilities for malicious users to obtain power consumption information of individual homes without occupants' authentication. To protect the occupants' privacy, we leverage the unique feature of hybrid AC-DC microgrids and propose Shepherd, a privacy protection framework, to allow homes in a microgrid to coordinate with each other to hide power consumption information. We analyze the adversarial models in a single home and with compromised neighbors and propose corresponding defense models to defend from these two models. With the empirical data from more than 40 homes, we conduct extensive system evaluations. Results show that Shepherd can i) significantly reduce the detection ratio from 33% to 13%, and ii) effectively hide consumption information even with 25% compromised neighbors.

8. ACKNOWLEDGMENTS

This project is supported by NSF grant CNS-1503590 and UMBC COEIT Strategic Plan Implementation Grant. Yanhua Li is partly supported by a gift funding from Pitney Bowes, Inc.

9. REFERENCES

[1] State of California Executive Order S-21-09. http://gov.ca.gov/executive-order/13269, 2009.

[2] Database of State Incentives for Renewables and Efficiency. http://www.dsireusa.org, 2010.

[3] Residential Energy Consumption Survey (RECS). http://www.eia.gov/consumption/residential, 2013.

[4] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin. Private memoirs of a smart meter. In *BuildSys*, 2010.

[5] S. Barker, S. Kalra, D. Irwin, and P. Shenoy. Empirical characterization and modeling of electrical loads in smart homes. In *IGCC*, 2013.

[6] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University, 2004.

[7] S. Clark, H. Mustafa, B. Ransford, J. Sorber, K. Fu, and W. Xu. Current events: Identifying webpages by tapping the electrical outlet. *Lecture Notes in Computer Science*, 8134:700–717, 2013.

[8] K. Garbesi. Catalog of dc appliances and power systems. 2012.

[9] G. Hart. Residential energy monitoring and computerized surveillance via utility power flows. *IEEE Technology and Society Magazine*, 8(2):12–16, 1989.

[10] Z. Huang, T. Zhu, Y. Gu, D. Irwin, A. Mishra, and P. Shenoy. Minimizing electricity costs by sharing energy in sustainable microgrids. In *BuildSys*, 2014.

[11] M. Lisovich, D. Mulligan, and S. Wicker. Inferring personal information from demand-response systems. *IEEE Security Privacy*, 8(1):11–20, 2010.

[12] 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.

[13] S. McLaughlin, P. McDaniel, and W. Aiello. Protecting consumer privacy from electric load monitoring. In *CCS*, 2011.

[14] S. N. Patel, T. Robertson, J. A. Kientz, M. S. Reynolds, and G. D. Abowd. At the flick of a switch: Detecting and classifying unique electrical events on the residential power line. In *Ubicomp*, 2007.

[15] T. Short. *Electric Power Distribution Handbook*. Taylor & Francis, 2003.

[16] T. Carpenter, S. Singla, P. Azimzadeh, and S. Keshav. The impact of electricity pricing schemes on storage adoption in ontario. In *e-Energy*, 2012.

[17] C. Valli. The not so smart, smart grid: Potential security risks associated with the deployment of smart grid technologies. In *Australian Digital Forensics Conference*, page 63, 2009.

[18] C. Valli, A. Woodward, C. Carpene, P. Hannay, M. Brand, R. Karvinen, and C. Holme. Eavesdropping on the smart grid. 2012.

[19] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel. Minimizing private data disclosures in the smart grid. In *CCS*, 2012.

[20] T. Zhu, Z. Huang, A. Sharma, J. Su, D. Irwin, A. Mishra, D. Menasche, and P. Shenoy. Sharing renewable energy in smart microgrids. In *ICCPS*, 2013.

APPENDIX

Proof of Theorem 1

THEOREM 1. *There exist two solutions $e_i^1(T)$ and $e_i^2(T)$ of Equation (6), and $e_i^1(T) < d_i(T) < e_i^2(T)$.*

PROOF. With Equation (3), we have:

$$l_{(e_i,d_i)}(T-1) = \frac{1}{T-1}\sum_{t=1}^{T-1}(e_i(t) - d_i(t))^2$$

Then we can rewrite Equation (6) as follows:

$$\frac{1}{T}\sum_{t=1}^{T}[e_i(t) - d_i(t)]^2 - \frac{1}{T-1}\sum_{t=1}^{T-1}[e_i(t) - d_i(t)]^2$$

$$=\frac{1}{T}\{[e_i(T) - d_i(T)]^2 - l_{(e_i,d_i)}(T-1)\} = 0$$

Since $l_{(e_i,d_i)}(T-1) \geq 0$, thus we have solutions of Equation (6): $e_i^1(T) = d_i(T) - \sqrt{l_{(e_i,d_i)}(T-1)} < d_i(T) < d_i(T) + \sqrt{l_{(e_i,d_i)}(T-1)} = e_i^2(T)$. □