Research Article

Thwarting Nonintrusive Occupancy Detection Attacks from Smart Meters

Dapeng Man,¹ Wu Yang,¹ Shichang Xuan,¹ and Xiaojiang Du²

¹Information Security Research Center, Harbin Engineering University, Harbin, China

²Department of Computer and Information Sciences, Temple University, Philadelphia, PA, USA

Correspondence should be addressed to Wu Yang; yangwu@hrbeu.edu.cn

Received 29 June 2016; Accepted 5 October 2016; Published 10 January 2017

Academic Editor: Kim-Kwang R. Choo

Copyright © 2017 Dapeng Man et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Occupancy information is one of the most important privacy issues of a home. Unfortunately, an attacker is able to detect occupancy from smart meter data. The current battery-based load hiding (BLH) methods cannot solve this problem. To thwart occupancy detection attacks, we propose a framework of battery-based schemes to prevent occupancy detection (BPOD). BPOD monitors the power consumption of a home and detects the occupancy in real time. According to the detection result, BPOD modifies those statistical metrics of power consumption, which highly correlate with the occupancy by charging or discharging a battery, creating a delusion that the home is always occupied. We evaluate BPOD in a simulation using several real-world smart meter datasets. Our experiment results show that BPOD effectively prevents the threshold-based and classifier-based occupancy detection attacks. Furthermore, BPOD is also able to prevent nonintrusive appliance load monitoring attacks (NILM) as a side-effect of thwarting detection attacks.

1. Introduction

Due to the development of information control and communication technologies, conventional power grids are being converted into smart grids. It brings higher reliability, security, and efficiency to power systems [1]. In 2013, US electric utilities had 51,924,502 advanced (smart) metering infrastructure (AMI) installations [2]. About 89% were residential customer installations. The AMI periodically gathers smart meter data from the terminal user and transmits the data to the remote utility, which provides companies with unprecedented capabilities for forecasting demand, understanding customer usage habits, decreasing probability of outages, and more [3].

While smart grids yield energy efficiency and increase reliability and robustness, smart metering deployments have been plagued with privacy concerns [4]. Reference [5] lists a number of privacy-sensitive features that may be inferred from power consumption data ranging from house occupancy to personal habits and routines. An important example of simple and private information that smart meters leak is occupancy whether or not someone is home and when

[6]. According to the report, occupancy is routinely cited as the most important factor in considering burglary target selection: burglars prefer unoccupied targets [7]. In addition, some other privacy information could be inferred from occupancy, such as daily routines and travel times. This information could then be used for targeted advertising [8].

New research suggests an attacker can easily monitor the occupancy of a home by analyzing the smart meter data [9, 10], since there are several power consumption features highly correlated with occupancy. To be more exact, the electricity load generally have a higher mean, standard deviation, and variation range when the home is occupied.

To protect end-user privacy, various technological approaches have been proposed in recent years. Besides those methods based on encryption and data aggregation [4, 11–16], some approaches are prone to use of rechargeable batteries to modify the external load [1, 17–20], which is called battery-based load hiding (BLH). However, these techniques only focus on how to prevent nonintrusive appliance load monitoring attacks (NILM), which infer appliance usage from load data with the help of load signature libraries [21–24]. Since the previous methods are not designed to change

or hide those power consumption features that correlate with occupancy, they cannot thwart occupancy detection attacks.

To prevent occupancy detection, [5, 25] propose a combined heat and privacy (CHPr) method, which uses the thermal energy storage of electric water heaters to make it look like someone is always home. The authors also provide a real prototype and corresponding evaluations. Though CHPr does not waste any energy and does not increase electricity costs, according to the latest surveys [26], about 50% of US households use natural gas water heaters; in contrast, electric water heaters only account for 41%. Thus, replacing a gas water heater with an electric water heater is not only complicated for a household, but also expensive and results in serious waste. In addition, once the water heater does not have enough capacity to heat up (the water temperature has reached the upper limit), the home's raw smart meter data will be exposed, since the heater cannot run out of hot water and inject cold water automatically to continue heating up.

To address the above problems, we propose a battery-based preventing occupancy detection method (BPOD), which enhances the external load to increase both true positives and false positives of occupancy detection attacks by charging the battery when the home is unoccupied and properly discharges the battery when the home is occupied. In particular, this method not only prevents occupancy detection attacks but also protects other private information, such as appliance usage signatures, since the external load has been changed.

In doing this, we make the following contributions:

- (i) We investigate the current occupancy detection attacks and BLH methods and show that the BLH methods represented by Nonintrusive Load Leveling (NILL) and Lazy Stepping (LS) are unable to prevent occupancy detection attacks. In addition, we point out that the CHPr method still has some shortcomings.
- (ii) We present a framework of BPOD to combat occupancy detection attacks. BPOD monitors a home's occupancy in real time and chooses to charge or discharge according to the monitoring results, thus making a delusion that someone is always home.
- (iii) We evaluate BPOD using data from real-world energy consumption and show that it effectively increases both the true positives and the false positives of various state-of-the-art occupancy detection attacks. We also demonstrate that BPOD is able to prevent nonintrusive appliance load monitoring attacks (NILM) as a side-effect of preventing occupancy detection attacks.

2. Background

2.1. Occupancy Detection. Occupancy is one of the most important privacy issues for residents security. However, the latest research shows that detecting whether someone is home according to statistical metrics of power usage is especially easy. For example, a high mean power consumption is likely to be caused by presence in the household, and a high standard deviation may be caused by occupants

turning on some appliances. Occupancy detection attacks are currently divided into two classes: the threshold-based and the classifier-based. The accuracy of all the methods is higher than 80%.

2.1.1. Threshold-Based. Reference [9] proposes a threshold-based algorithm that records the power's mean, standard deviation, and change range over a time window to infer whether the home is occupied or unoccupied. The author defines a 15-minute epoch length and computes the above three metrics over each epoch. If one of the metrics exceeds a threshold, it is recorded as a potential occupancy point. At last, the author clusters the points using a one-hour time threshold. If two points are within the time threshold, it can be considered that the home is occupied during the interval between the points.

2.1.2. Classifier-Based. Reference [10] uses several classification algorithms, such as HMM, SVM, and KNN, to detect a home's occupancy. The power's mean, standard deviation, and the sum of absolute differences between adjacent measurements are considered as features. The author computes the above metrics over 15-minute intervals and then plots the point, labeled occupied or unoccupied, in a 3D feature space. Finally, new data points are classified by the classifiers.

2.2. Battery-Based Load Hiding. BLH methods try to hide true load demand by charging or discharging a battery. Various BLH methods have been proposed over the past few years. Nonintrusive Load Leveling (NILL) and Lazy Stepping (LS) are two of the most classic BLH algorithms.

2.2.1. Nonintrusive Load Leveling (NILL). The idea of NILL is using a battery to keep the external load constant, thus protecting appliance power signatures [19]. When an appliance turns ON, the actual demand load will be above the prior external load. Thus, NILL will discharge the battery to maintain the external load as unchanged. Likewise, NILL will charge the battery when the actual demand load is below the prior external load.

2.2.2. Lazy Stepping (LS). The LS method is designed to prevent a precise load change recovery attack which is effective against NILL [20]. The method makes the external load more coarse-grained, using step functions, thus hiding the appliance features. There are four algorithms in the stepping framework. They are Lazy Stepping (LS1 and LS2), Lazy Charging (LC), and Random Charging (RC), respectively. The evaluation results show that LS2 is the most effective algorithm.

Figure 1 is the occupancy detection results using the threshold-based method. The data of (a), (b), and (c) is raw smart data of one day from a real home, altered by NILL and LS2, respectively. As Figure 1 shows, the detection results of (b) and (c) are similar to (a), where the home is unoccupied from 10:00 a.m. to 4:00 p.m. The reason is that though NILL and LS2 hide appliance usage signatures, they are all unable to change some statistical metrics of actual demand load,

FIGURE 1: Occupancy detection attack against raw smart meter data and altered data by NILM or LS2.

FIGURE 2: Framework of BPOD.

such as power mean and variance, thus leaking the occupancy information.

3. Framework of BPOD

The framework of BPOD is similar to NILM methods [19, 20], as shown in Figure 2. It includes two parts: (1) it monitors the occupancy by analyzing the real power demand and (2) according to the monitoring results it regulates the external load using a battery.

For monitoring the occupancy of a home, BPOD uses a threshold-based detection method to process the raw smart meter data in real time. As Figure 3(a) depicts, when some statistical metrics, such as power mean and variance, are lower than the predefined thresholds over a time window, BPOD will predict the home is unoccupied and vice versa.

As Figure 3(b) shows, to thwart occupancy detection attacks, the battery charges and makes the power features exceed the thresholds when the home is unoccupied. Since the capacity of the battery is limited, the battery properly discharges when we detect that someone is home. Because the battery's charging or discharging is just based on the thresholds, the computational complexity of BPOD is very low.

Before we describe the detailed framework of BPOD, we propose two hypotheses.

Hypothesis 1. Once BPOD finds that there is someone in the household after 9:00 p.m., the home may be considered to be occupied until 5:00 a.m. next morning, no matter how small the statistical metrics of power consumption are during this period.

We believe that Hypothesis 1 is reasonable, since occupants scarcely go out after 9:00 p.m. and stay out all night. The reason causing the small power usage is that the occupants are more often sleeping during this period. Thus, it is not necessary to charge the battery and make it look like someone is home.

Hypothesis 2. The features of power usage between 1:00 a.m. and 4:00 a.m. are similar to the daytime's, when the home is empty.

No matter the threshold-based occupancy detection or classifier-based occupancy detection, it is obligatory to know the power consumption features of the unoccupied household before launching an attack. However, the attacker has no idea what characteristics of the electricity usage represent the home being empty. Thus, the characteristics of power

FIGURE 3: Original power usage (a) and modified power usage (b).

consumption after midnight are used as a reference to infer the features of power usage when the home is unoccupied [9]. In this paper, we set the thresholds based on the electricity usage after midnight as well. It is to be noted that we have no consideration for the case that using some appliances, such as air conditioners, may lead the power consumption after midnight to be higher than the unoccupied time's. This question will be researched in the future.

The framework of BPOD works for three cases: (A) unoccupied home, (B) occupied home, and (C) sleeping before dawn. In fact, sleeping before dawn is a special case of an occupied home. Next, we will present the details of BPOD.

3.1. Unoccupied Home. When BPOD finds that the home is unoccupied, the battery will charge for enhancing the statistical metrics of power usage. It should be pointed out that there exists one case, where the occupants are at home but not using any electrical devices. In this case, the detection algorithm of BPOD may make some false negatives, leading the battery to charge. We think the charging is reasonable, because if the attacker misjudges that the home is empty and breaks into the house, it will pose a great threat to the safety of the occupants.

Three kinds of charging modes exist. One is injecting random noise into the demand as [27] proposed. However, an experienced attacker may perceive such abnormalities from smart meter data, resulting in the failure of masking occupancy. The second method injects real electrical appliance signatures into the demand. The libraries of electrical signature provide various electricity signatures, such as a television, microwave oven, and printer [28, 29]. The last method replays the occupied power usage of a few days ago. In this paper, we choose the second method.

When the battery is full, the raw smart meter data may be exposed, since BPOD cannot inject any power signatures into the demand. In this case, the occupancy information may be leaked. However, other privacies, such as appliance

FIGURE 4: State transition between charging and discharging.

signatures, still need to be protected. Thus, the battery should discharge slowly when it is about to be full. Figure 4 shows the state transition between charging and discharging. In the picture, $C(t)$ is used to represent the battery's state of charge (SOC), C is used to represent the state that the battery is charging (home is unoccupied or nobody is using any appliances), D is used to represent the state that battery is discharging (occupants are using an appliance), and D_s is used to represent the state that the battery is discharging slowly (nobody is using any appliances and SOC is at high level).

Being similar to the method that [20] proposed, when the battery is under state D_s , the external load profile $e(t)$ is calculated by formula (1), where $d(t)$ is used to represent real demand and β is a constant. To avoid $e(t)$ equal to zero and to let the battery discharge slowly, we set β to a relatively small value (approximately 100 W to 200 W)

$$e(t) = \left\lfloor \frac{d(t)}{\beta} \right\rfloor \cdot \beta. \quad (1)$$

3.2. Occupied Home. The state will be transformed into state D , when BPOD detects the home is occupied. Under state D ,

the battery needs to discharge. Let $e(t) = d(t) - b(t)$, where $b(t)$ is the battery's discharging rate at time t .

In fact, $b(t)$ is related to $C(t)$, C_H (the battery's capacity), $M_{\text{Threshold}}$ (the power mean thresholds of BPOD), and β_D (the maximum discharging rate). The higher the remaining battery power is, the faster the battery should discharge. Thus,

$$e(t) = \begin{cases} d(t) - (d(t) - M_{\text{Threshold}}) \times \frac{C(t)}{C_H}, & \text{if } d(t) > M_{\text{Threshold}}, b(t) \leq \beta_D \\ d(t) - \beta_D, & \text{if } d(t) > M_{\text{Threshold}}, b(t) > \beta_D \\ \left\lfloor \frac{d(t)}{\beta} \right\rfloor \cdot \beta, & \text{if } d(t) \leq M_{\text{Threshold}}, b(t) \leq \beta_D. \end{cases} \quad (2)$$

3.3. Sleeping before Dawn. Sleeping before dawn is a special case where the statistical metrics of power usage are very similar to the unoccupied home's, but the household is actually occupied. According to Hypothesis 2, there is no need to inject any appliance signatures into the demand when occupants are sleeping before dawn. In contrast, the battery should continue discharging during this period if there still exists some power in the battery. There are two motivations to do this. On one hand, the battery needs to prepare for the charging next daytime. On the other hand, doing this is helpful to further increase the false positives of occupancy detection attacks, since the attacks always take the power consumption features during this period as reference.

We have investigated smart* dataset which includes one-minute resolution smart meter data of 443 homes over 24 hours. We find the power means for most of the homes are below 300 W when occupants are sleeping. Thus, if the power means are higher than 300 W, the battery will continue discharging.

4. Experimental Evaluation

4.1. Dataset. In our experiments, we use smart* dataset, a one-second resolution dataset, to measure the performance that BPOD resists various occupancy detection attacks. The dataset is collected in three houses over the course of three months. We choose the meter data of Home A as experimental data. Home A is located at Western Massachusetts. It is a two-story, 1700-square-foot home with three full-time occupants. The home has a total of eight rooms including its basement. There are various sensor data in the dataset, including average real apparent power every second for the home and each circuit, on-off-dim events at nearly all of the home's wall switches and real power usage from nearly all of the home's plug loads [30, 31].

The dataset also includes a variety of events related to occupancy. For example, motion sensors have been deployed in all eight rooms of a home, and door sensors have been attached to the refrigerator and basement freezer. From these occupants motion events and interaction with electrical loads, we obtain the ground truth occupancy. There is one possibility that the occupants are home, but not operating any appliance or moving in the house. In this case, we regard the

we let $b(t) = (d(t) - M_{\text{Threshold}}) \times C(t)/C_H$, if $b(t) \leq \beta_D$, and $b(t) = \beta_D$, if $b(t) > \beta_D$. It is noted that even if the battery is under state D , there is a likelihood that $d(t) \leq M_{\text{Threshold}}$. In this case, it is not necessary to let $e(t) > M_{\text{Threshold}}$ by charging. We just need to protect the appliance signatures. In conclusion, $e(t)$ is calculated by the following:

home as unoccupied in the ground truth. Doing so would lead to increase of false positives (detects occupancy and the home is unoccupied) of occupancy detection attacks and decrease of true positives (detects occupancy and the home is occupied), when using BPOD to prevent the attacks. However, we believe it has little effect on evaluating the effectiveness of BPOD, since our main goal is to increase the sum of the true positives and false positives.

We also use REDD dataset, a one-second resolution dataset, to verify whether BPOD is able to protect households load signatures. REDD is the largest dataset for disaggregation with the true loads of each house identified [28, 32]. The dataset consists of whole-home and circuit/device specific electricity consumption for a number of real houses over several months time. We launch an NILM attack to infer the component device electricity consumption from the aggregated electricity signal and compare with the real device consumption.

Furthermore, we note that some of the electricity consumption data in these two datasets is lost as well as other datasets. Therefore, short time period gaps were patched using interpolation as introduced in [10].

We inject a real power signature using ACS-F1, a ten-second resolution database of appliance consumption signatures. The database includes about 100 home appliances divided into 10 categories, such as coffee machines, computer stations (including monitors), and microwave ovens. Specific details of the database can be found in [29, 33].

4.2. Preventing Occupancy Detection Attacks. We use TP, TN, FP, and FN to represent true positives, true negatives, false positives, and false negatives, respectively. Since the aim of BPOD is to make a delusion that the home is always occupied, TP + FP is the most important indicator to evaluate the effectiveness that BPOD prevents occupancy detection attacks. The high value of TP + FP illustrates that BPOD is able to thwart the occupancy detection attacks effectively.

We quantify the effectiveness of various occupancy attacks on both raw smart meter data and battery-modified data from a home over one week. The attacks are based on threshold, SVM, KNN, and HMM, respectively. Specific details of the implementation of these attacks can be found in [9, 10].

TABLE 1: Performance of threshold-based attacks on raw smart meter data compared with 6 KWh battery-modified data.

Attack	Data type	TP	TN	FP	FN	TP + FP
Threshold	Original	59.73%	23.80%	1.58%	14.89%	61.31%
	BPOD	78.73%	1.90%	18.22%	0.49%	96.95%
SVM	Original	67.77%	10.47%	12.5%	9.18%	80.35%
	BPOD	71.54%	4.65%	18.17%	5.64%	89.71%
KNN	Original	61.17%	17.19%	7.64%	14.0%	68.81%
	BPOD	69.28%	4.89%	18.94%	6.89%	88.22%
HMM	Original	57.03%	21.12%	2.1%	19.76%	59.13%
	BPOD	76.78%	7.7%	14.51%	5.17%	91.29%

Table 1 shows the performance of the occupancy detection attacks on the raw smart meter data and 6 KWh battery-modified data. As Table 1 indicates, the accuracy of all the attacks against original smart meter data exceeds 78%. Moreover, the TN + FN of these attacks is especially high. For example, the TN + FN of HMM-based attack is higher than 40%. TN means the home is really unoccupied. There is the risk of theft. FN means the attacker believes the home is unoccupied, but the home is actually occupied. It is extremely dangerous for resident when the attacker breaks into the house. From Table 1, we can also see that both the TP and the FP of the attacks are increased sharply by BPOD. It comes up to what we expect, trying the best to make attackers believe that the home is occupied. The threshold-based attack is the least robust to BPOD. The TP + FP is enhanced from 61.31% to 96.95%. That is somewhat expected, since we also use the threshold-based method to detect occupancy in BPOD. This makes BPOD be more effective for the threshold-based attack. Furthermore, though the KNN-based attack is the most robust to BPOD, the TP + FP also exceeds 88%. There is another remarkable fact that the TN and the FN are reduced by BPOD. This is helpful for enhancing the occupants property and personal safety.

Figure 5(a) plots a home's load profile and ground truth occupancy over a week. Figures 5(b) and 5(c), respectively, depict the results of threshold-based detection attacks against original smart meter data and modified data. As the pictures show, the detected occupancy of the original data and the ground truth are nearly coincident. Figure 5(c) clearly manifests that BPOD masks occupancy effectively by injecting appliance consumption signatures when the home is empty or occupants are not operating any electrical devices. There are three gaps in Figure 5(c). The gaps represent that the battery is full when the home is empty for a long time. Though BPOD is also able to protect the appliance signatures of the home, it still failed to mask the occupancy, since the statistical metrics of power usage are not changed.

As with other BLH methods, battery capacity is a key factor of BPOD effectiveness. In order to demonstrate the relationship between the performance of BPOD and the battery capacity, we select one-day power consumption data of a home from smart* dataset and launch the attack based on threshold to the data. Figure 6 depicts the performance that BPOD prevents the attack under different battery capacity.

From Figure 6 we see that the TN and the FN continuously descend as the battery capacity increases. Consequently, the TP and the FP go up. However, the ascending rate of the TP begins to slow down when the battery capacity is larger than 6 KWh, since the TP is almost consistent with the ground truth. The ascending rate of the FP also decreases with the battery capacity enlarging. TP + FP is 92.74% at 6 KWh battery capacity, and is 95.65% at 10 KWh battery capacity. Therefore, we should consider the tradeoffs between the effectiveness of BPOD and the battery costs in practical applications.

4.3. Preventing NILM Attacks. Though the main aim of BPOD is to prevent occupancy detection attacks, it is also able to thwart the NILM attacks. To evaluate the performance of preventing NILM attacks, we first use the previous 7 days' smart* dataset to compare BPOD with the NILL and LS2 algorithms under the mutual information metrics, which is used in [20]. In probability theory and information theory, the mutual information, transinformation, of two random variables is a measure of the variables' mutual dependence.

In this paper, we use mutual information under the independence assumption to measure how much common information is embedded in e' and d' [20]. The more the mutual information between e' and d' , the higher the probability that the attacker can infer d' from e' .

Since both e' and d' are continuous, we must discretize $e'(t)$ and $d'(t)$ into K discrete values at first (we set $K = 600$ in our experiment). According to the definition of mutual information, the mutual information of $e'(t)$ and $d'(t)$, $I(e'; d')$, can be calculated as follows:

$$\begin{aligned}
 I(e'; d') &= \sum_{i=1, \dots, T} I(e'(i); d'(i)) \\
 &= \sum_i \sum_{e'(i)} \sum_{d'(i)} p(e'(i), d'(i)) \log \frac{p(e'(i), d'(i))}{p(e'(i)) p(d'(i))}, \quad (3) \\
 p(e'(t) = a; d'(t) = b) \\
 &= \frac{\sum_{i=1}^T \delta(e'(i) = a \wedge d'(i) = b)}{T}.
 \end{aligned}$$

The resolution of the dataset we used is one second. In order to facilitate the calculation, we convert the resolution to one minute. We calculate the mutual information of three BLH methods under different battery capacity, from 1 KWh to 10 KWh.

Figure 7 depicts the mutual information value of BPOD, NILL, and LS2 under different battery capacity. As Figure 7 shows, LS2 has the best performance under the small battery capacity. When the battery capacity is 1 KWh, the mutual information value of LS2 is only 0.23, while NILL and BPOD are 0.51 and 0.42, respectively. It is not contrary to our expectations, since LS2's designed idea decides that it does not require too much battery capacity to work well. However, the mutual information value of LS2 does not decrease sharply as the battery capacity enlarges. It just descends by 33%, when the battery capacity increases from 1 KWh to 10 KWh. On the other hand, though the mutual information

FIGURE 5: The occupancy ground truth (a), as well as the threshold-based occupancy detection attack against raw smart meter data (b) and modified data (c).

FIGURE 6: State transition between charging and discharging.

FIGURE 7: State transition between charging and discharging.

of NILL is the largest at the beginning, the decline rate is the highest of all. Its performance becomes better than BPOD when the battery capacity increases to 4 KWh. Its performance even becomes better than LS2, when the battery capacity increases to 8 KWh. It denotes that the battery capacity is more important for NILL than the other two methods. The downward trend of BPOD is similar to NILL.

The mutual information value of BPOD is lower than NILL at the beginning and is a little higher than NILL when the battery capacity exceeds 4 KWh. It is theoretically proven that BPOD has the ability to resist the NILM attacks.

In order to examine the actual effect that BPOD prevents the NILM attacks, we make another experiment. Since REDD

FIGURE 8: State transition between charging and discharging.

dataset is widely accepted for verifying the performance of NILM algorithms [28], we select one-day power consumption data of a home from the dataset and launch a state-of-the-art unsupervised NILM attack based on factorial HMMs (FHMMs) to the data [28, 34]. FHMMs-based NILM algorithm proved that it outperforms the other unsupervised methods and is capable of accurately disaggregating power data into per-appliance usage information. A famous open source NILM toolkit (NILMTK) provides the implementation of the FHMMs algorithm [35].

We choose normalized error in inferred power as the accuracy metric of the NILM algorithm, which is depicted in [30, 32]. We calculate the sum of the differences between the inferred power usage and actual power usage of appliance n in each time slice t and normalize it using the appliance's total energy consumption. Let $\hat{y}_n(t)$ denote inferred power usage of appliance n at time t and $y_n(t)$ denote actual power usage of appliance n at time t ; then the normalized error in inferred power α is defined as

$$\alpha = \frac{\sum_{i=1}^N \sum_{t=1}^T |\hat{y}_n(t) - y_n(t)|}{\sum_{i=1}^N \sum_{t=1}^T y_n(t)}. \quad (4)$$

From formula (4), we can conclude that the larger the value of α is, the better performance the BLH method has. There is not any effectiveness of the BLH method on preventing the NILM attack when equaling zero.

Figure 8 depicts the normalized error in inferred power after BPOD, NILL, and LS2 masking the raw power usage data under different battery capacity. As Figure 8 shows, the normalized error is 1.01, when we launch the FHMMs-based NILM algorithm to the raw data. As expected, the normalized error increases when using BPOD, NILL, and LS2 to mask the raw data. However, the normalized error of LS2 increases slowly and is always the lowest of the three methods under different battery capacity. BPOD outperforms NILL and LS2.

This is due to the fact that the unsupervised NILM algorithms are more effective in detecting large loads, while NILL and LS2 are unable to effectively decrease the large loads. On the contrary, BPOD can reduce the loads by charging the battery when the power usage is high. Though BPOD does not have an obvious advantage of preventing the NILM attack under small battery capacity, it becomes more effective than the two other methods as battery capacity increases.

5. Conclusion

In this paper, we present a battery-based method (BPOD) for preventing occupancy detection attacks. We show that previous BLH methods do not prevent occupancy detection attacks and describe how the BPOD works when a home is occupied or unoccupied. We evaluate BPOD using various real-world smart meter datasets. The experimental evaluation demonstrates that BPOD increases the true positives and the false positives, thus effectively preventing both the threshold-based and the classifier-based occupancy detection attacks. Moreover, our experimental results show that though BPOD is designed to thwart occupancy detection attacks, it is also able to protect appliance electricity signatures as a side-effect and outperforms NILL and LS2 in preventing unsupervised NILM attacks.

Disclosure

Dapeng Man is currently an Assistant Professor in Harbin Engineering University. His main research interests include network security and mobile computing.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported in part by the US NSF under Grant CNS-1564128, the US Air Force Research Lab under Grant AF16-AT10, the Qatar National Research Fund under Grant NPRP 8-408-2-172, and the China Fundamental Research Funds for the Central Universities under Grant HEUCF160605. The authors are grateful for the valuable smart* home dataset provided by LASS Laboratory of UMASS and REDD dataset provided by CSAIL Laboratory of MIT. They also greatly appreciate the appliance consumption signature database provided by WATT ICT.

References

- [1] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 486–495, 2015.
- [2] Advanced Metering Count by Technology Type, 2014, https://www.eia.gov/electricity/annual/html/epa_10_10.html.
- [3] IBM Corporation Software Group, "Managing big data for smart grids and smart meters," Whitepaper, IBM Corporation, 2012.

- [4] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin, "Smart meter aggregation via secret-sharing," in *Proceedings of the 1st ACM Workshop on Smart Energy Grid Security (SEGS '13)*, pp. 75–80, Berlin, Germany, November 2013.
- [5] E. L. Quinn, "Smart metering and privacy: existing laws and competing policies," *SSRN Electronic Journal*, 2009.
- [6] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2426–2434, 2015.
- [7] M. Comeau, Burglary series: Motivation and target selection, 2014, <https://www.rit.edu/cja/criminaljustice/sites/rit.edu.cja.criminaljustice/files/docs/WorkingPapers/2014/Michell%20RPD%20Repeat%20and%20Near.pdf>.
- [8] D. Engel, "Wavelet-based load profile representation for smart meter privacy," in *Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference (ISGT '13)*, pp. 1–6, IEEE, Washington, DC, USA, February 2013.
- [9] D. Chen, S. Barker, A. Subbaswamy, D. Irwin, and P. Shenoy, "Non-intrusive occupancy monitoring using smart meters," in *Proceedings of the 5th ACM Workshop on Embedded Systems for Energy-Efficient Buildings*, pp. 1–8, ACM, Roma, Italy, November 2013.
- [10] W. Kleiminger, C. Beckel, T. Staaake, and S. Santini, "Occupancy detection from electricity consumption data," in *Proceedings of the 5th ACM Workshop on Embedded Systems For Energy-Efficient Buildings*, pp. 1–8, ACM, 2013.
- [11] R. Jiang, R. Lu, and K. K. R. Choo, "Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data," *Future Generation Computer Systems*, 2016.
- [12] B. Li, R. Lu, W. Wang, and K. K. R. Choo, "DDOA: a dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, 2016.
- [13] J. Peng, K. K. R. Choo, and H. Ashman, "User profiling in intrusion detection: a review," *Journal of Network and Computer Applications*, vol. 72, pp. 14–27, 2016.
- [14] V. Prokhorenko, K. K. R. Choo, and H. Ashman, "Context-oriented web application protection model," *Applied Mathematics and Computation*, vol. 285, pp. 59–78, 2016.
- [15] V. Prokhorenko, K. K. R. Choo, and H. Ashman, "Intent-based extensible real-time PHP supervision framework," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 10, pp. 2215–2226, 2016.
- [16] V. Prokhorenko, K.-K. R. Choo, and H. Ashman, "Web application protection techniques: a taxonomy," *Journal of Network and Computer Applications*, vol. 60, pp. 95–112, 2016.
- [17] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: towards undetectable appliance load signatures," in *Proceedings of the 1st IEEE International Conference on Smart Grid Communications (SmartGridComm '10)*, pp. 232–237, IEEE, 2010.
- [18] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Data Privacy Management and Autonomous Spontaneous Security*, pp. 194–212, Springer, Berlin, Germany, 2014.
- [19] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*, pp. 87–98, ACM, October 2011.
- [20] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS '12)*, pp. 415–427, ACM, Raleigh, NC, USA, October 2012.
- [21] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.
- [22] C. Laughman, K. Lee, R. Cox et al., "Power signature analysis," *IEEE Power and Energy Magazine*, vol. 1, no. 2, pp. 56–63, 2003.
- [23] Y.-H. Lin and M.-S. Tsai, "An advanced home energy management system facilitated by nonintrusive load monitoring with automated multiobjective power scheduling," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1839–1851, 2015.
- [24] W. Wichakool, Z. Remscrim, U. A. Orji, and S. B. Leeb, "Smart metering of variable power loads," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 189–198, 2015.
- [25] D. Chen, S. Kalra, D. Irwin, P. Shenoy, and J. Albrecht, "Preventing occupancy detection from smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2426–2434, 2015.
- [26] M. DiMascio, Water heaters get an efficiency makeover courtesy of the department of energy, <http://aceee.org/blog/2015/02/water-heaters-get-efficiency-makeover>.
- [27] D. Egarter, C. Prokop, and W. Elmenreich, "Load hiding of household's power demand," in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm '14)*, pp. 854–859, Venice, Italy, November 2014.
- [28] J. Z. Kolter and M. J. Johnson, "Redd: a public data set for energy disaggregation research," in *Proceedings of the Workshop on Data Mining Applications in Sustainability (SustKDD '11)*, vol. 25, pp. 59–62, San Diego, Calif, USA, August 2011.
- [29] C. Gisler, A. Ridi, D. Zujferey, O. A. Khaled, and J. Hennebert, "Appliance consumption signature database and recognition test protocols," in *Proceedings of the 8th International Workshop on Systems, Signal Processing and Their Applications (WoSSPA '13)*, pp. 336–341, IEEE, Algiers, Algeria, May 2013.
- [30] S. Barker, A. Mishra, D. Irwin, E. Cecchet, P. Shenoy, and J. Albrecht, "Smart*: an open data set and tools for enabling research in sustainable homes," *SustKDD*, vol. 111, article 112, 2012.
- [31] Smart* Dataset, 2016, <http://traces.cs.umass.edu/index.php/Smart/Smart>.
- [32] Redd Dataset, 2016, <http://redd.csail.mit.edu/>.
- [33] Watttict Dataset, 2016, <http://www.watttict.com/web/index.php/databases/acs-fl>.
- [34] H. Kim, M. Marwah, M. F. Arlitt, G. Lyon, and J. Han, "Unsupervised disaggregation of low frequency power measurements," in *Proceedings of the SIAM International Conference on Data Mining (SDM '11)*, pp. 747–758, SIAM, Mesa, Ariz, USA, 2011.
- [35] N. Batra, J. Kelly, O. Parson et al., "NILMTK: an open source toolkit for non-intrusive load monitoring," in *Proceedings of the 5th ACM International Conference on Future Energy Systems (e-Energy '14)*, pp. 265–276, ACM, Cambridge, UK, June 2014.