PRIVACY PROTECTION THROUGH LIMITED LOAD SIGNAL DISTORTION

BY

THOMAS NICOL

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2011

Urbana, Illinois

Adviser:

Professor Thomas J. Overbye

ABSTRACT

Advanced techniques of Non-Intrusive Load Monitoring (NILM) can provide power consumers with opportunities to easily and accurately track their own energy usage. However, as with any other powerful technology, there is a darker side to NILM. Since detailed monitoring requires only information about the overall power draw over a period of time, sources of such information could be used for any number of purposes. While some legal protections exist for personal information reported to a utility, and digital defenses make it difficult for unauthorized parties to obtain meter data, such measures are not infallible. They do nothing to prevent abuse by the utility itself or the surreptitious installation of a monitoring device outside a residence, place of business, embassy, etc. Therefore, a method to reduce the ability of attackers to deduce private information from an observed power signal is proposed, using some knowledge of the loads being hidden to offset identifiable load signatures in the signal for maximum ambiguity.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

An Unmet Need

The development of effective Non-Intrusive Load Monitoring (NILM) technology has many potentially useful applications. With a single device hooked into a system, the complicated combination of loads can be untangled from the total power being pulled from the grid, so individual power-consuming devices can be tracked and compared. Inefficiency and waste can easily be identified, large loads can be tagged for potential participation in demand response, and it becomes possible to verify that these devices respond correctly to a demand response event. NILM is a valuable tool for those wishing to better understand and control their own consumption.

However, the very same techniques so helpful to a facility manager seeking to eliminate inefficiencies in system operation can be turned (for example) to purposes of industrial espionage. In a residential setting, a recent study found that detailed tracking of power consumption could lead to highly accurate tracking of the residents as well [1], resulting in decreased privacy and increased vulnerability (e.g., a savvy criminal could easily case a neighborhood undetected, or a stalker could monitor a target's daily routine). As smart meters are being deployed across the country, the potential consequences of their adoption and the detailed metering data they will make available are worth consideration.

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000097.

Ethical questions about the pursuit of such technology were raised over two decades ago [2]; but to date – despite the recent push toward detailed power data on a network of digitally enabled meters – little has been done to prevent unauthorized monitoring. An innovative Automatic Metering Infrastructure (AMI) system architecture designed to avoid the central collection of fine-granularity consumption data in a form identifiable with individual energy customers has been proposed [3]. This system, if implemented, serves to deter misuse of data by the utility or someone who gains access to the utility's database. However, it does not prevent targeted invasions of individual customers, such as a company estimating a competitor's production by monitoring the power drawn by a manufacturing facility. Present-day defenses focus exclusively on protecting the metered data – not the personal information embedded in that data and the power signal itself.

Figure 1 illustrates the current state of defenses at the major points of attack: the meters, the data transmission system, the data stored at the utility, and the power signal close to the particular facility of interest . (Figures appear at the end of each chapter.) As the facility's power signal is mixed in with others through the distribution and transmission system, it becomes significantly more difficult to tie any specific aspect of the aggregate signal to the particular facility in question and therefore poses little threat with sufficient separation. While there are undoubtedly some legal issues attached to hacking a meter or eavesdropping on the transmission of power data to the utility, people willing to employ such methods are not primarily deterred by their illegality – thus the most effective line of defense is currently digital. Likewise, while data stored at the

utility is likely to have some sort of digital protection, it is easily accessible to various parties. The primary deterrents to abuse of that data are the legally defined guidelines for their use. Access to the data in the power signal itself is prevented only by the practical problem of installing a sensor on the line (or near enough to the line to measure the magnetic field) somewhere in the distribution system before the signal is drowned out by neighboring loads .

The potential harms born of this grid upgrade have been explored more extensively elsewhere [1], [2], [4], [5]. Presented here is one technological defense against unauthorized and unwanted monitoring using targeted alterations to the signal, reducing the transmission of personal information. The sketchy protections currently in place are not sufficient to adequately preserve privacy. Further defenses must be developed so that the benefits of a smarter grid can be enjoyed while the potential harms are mitigated.

Figures

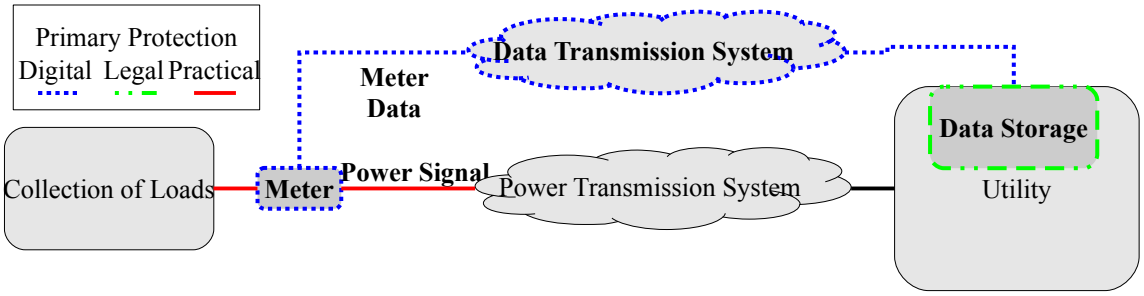

Fig. 1: Primary protections against abuse in a smart meter system

CHAPTER 2: BACKGROUND

Inadequacies of Current Protections

The two major types of existing protection against invasive analysis of one's power signal are legal and digital. However, despite these efforts to prevent access to the data by unauthorized third parties (and abuse by authorized parties), they still do not significantly limit the ability of outside parties to gain access to, and analyze, anyone's power signal.

One major weakness of the current system is that it still puts unnecessarily revealing information about a person's activity and habits in the hands of at least one outside entity: the utility. A utility needs to know how much to bill a customer for the power he or she uses, but there's no reason to give the utility information about the customer's personal habits. Yet this is exactly what detailed metering will do if that information is left intact within the power signal. Power customers need an alternative to putting that sort of unnecessary trust in their utility.

In some states, utilities are legally restrained from releasing personally identifying information to a third party without written consent from the customer [6]. However, most states do not have standard definitions of “personally identifying information,” or formal privacy policies addressing the proper use of power data [7]. The consumer has no recourse but to simply trust the utility itself not to abuse the information which could be gleaned from the detailed metering; and as indicated by the lawsuits against utilities in

the wake of smart meter installations [8], such trust in the good intent of utilities is not likely to be forthcoming.

On top of that, large exceptions are made for law enforcement. In at least one case, this loophole has led to extensive police perusal of numerous customers' usage data, looking for usage they consider “unusual.” This exception even went so far as law enforcement having its own password to the utility's database [9]. The police are required to have a warrant to monitor the phone lines going into a home but are not currently constrained legally from watching through the power lines, despite the constitutionally questionable nature of such action [6].

Existing laws can only discourage, not prevent, abuses by individuals within the utility or law enforcement – or by hackers with the ability to compromise the utility's data storage, communication with the meters, or even the meters themselves. Attempts at digital protections of the measured data are in place but are severely flawed. Even as smart meters are beginning to be deployed across the country, gaping security holes are being uncovered. Several vulnerabilities have been reported in AMI devices, allowing an attacker (with physical access to the device) to obtain the usage data and network authentication keys, giving the attacker access to all user data being transmitted from other devices as well [10]. The protocols on which the wireless communication of metering data takes place also have known vulnerabilities [11], so an attacker need not have physical access to a meter to be able to intercept data in transmission.

Such paltry protections are entirely inadequate for the preservation of individual privacy. Moreover, even if we assume digital protections can prevent unauthorized

parties from hijacking usage information from the meter, data transmission system, or data storage – and that legal protections of the data will prevent misuse or release of usage information – nothing is to stop someone from intercepting the power signal itself except for the minor inconvenience of concealing the monitoring device. In order to obscure this information from all avenues of abuse, we must go to the source, preventing that information from being carried by the power signal at all. To do so, we must first examine how NILM can be used to extract personal information from a power signal.

How Personal Information Is Extracted

Current and developing techniques for NILM are fairly diverse in approach. Some of the more popular techniques use genetic algorithms to develop profiles for different devices or use clustering algorithms to link patterns in the signal to other patterns caused by the same (or similar) devices. However, all depend on the analysis of one or more features of the power signal: real power, reactive power, the resulting power factor, various harmonics, etc. Inferences about the sources of the signal are made based on the values (and changes in the values) of these features. Use of a greater number of features allows for more precise identification of disaggregated appliances or machines, as there can be a great deal of overlap between different devices on some features. For example, the real power consumption of a blow-dryer might be very similar to the real power consumption of a toaster; but if the reactive power is factored into the feature profile for each device, the inductive motor of the blow-dryer can easily be differentiated from the toaster's heating elements.

Information can be gleaned from the different features of a power signal in a variety of ways. Figure 2 shows a breakdown of some basic approaches. In this framework, features can be analyzed based on

- Instantaneous or average value
- Changes in the value of the feature

These values can be evaluated based on

- The magnitude of the value (or change) itself
- The time at which the value or change was measured.

This framework helps to separate specific methods of extracting personal information from the power signal into rough categories and allows for the development of targeted defenses against those categories. A defense against one category of attack will not necessarily protect against an attack from another category. For example, altering the net power factor of a facility would help to disguise its loads from instantaneous/average-value-based extraction techniques but would provide little help against techniques based on changes in power factor.

While the steady state values of applicable features can give some information about their source, the points where feature values change are more commonly used when attempting to disaggregate a collection of loads. The change in the value of the feature is generally indicative of some state change of an individual load and so gives specific information about that load's contribution to the aggregate signal. Again, these changes can be analyzed based on magnitude or on the time at which they occur (either absolute

time or in the context of some sort of periodic signal).

In order to obscure the potentially revealing information inadvertently encoded in the power signal, these features must be modified. An effective technological defense against unauthorized monitoring combines various techniques to hide the identifying characteristics in both the levels and changes in each applicable feature.

Personal Information Derived From Aggregate Levels

Some information can be gleaned without even needing to disaggregate the individual load signals, just by looking at the overall power consumption over some period. Current low-resolution data collected by manual meter readings can be used to make inferences about the activities and devices combined to create that data. This method is exactly how police in Austin, Texas, conducted what effectively amounted to warrant-less searches of private homes, looking for "disproportionate" usage – warrantless searches covering thousands of Austin residents [9]. Fortunately, the amount and granularity of information extractable from the data is severely limited, and the activity in Austin is currently just one isolated incident. It is a minor vulnerability in comparison to what can be done with higher-resolution data.

When a time dimension is added to the aggregate load signal, far more opportunities for deduction arise. In a recent study, the researchers' software was able to deduce a subject's sleeping habits and detect whether or not the inhabitant was home, with about 90% accuracy. These results were acquired using only real power usage data over time at 15-second resolution [1]. Periods with very low activity could indicate that a

person is away or sleeping. Periods of high usage/activity give information about a person's lifestyle; is he a night person or a morning person, habitual or spontaneous, Luddite or technophile, etc.? Even without the signal-processing power necessary for detailed load disaggregation, a running measure of power usage within a home, office, manufacturing plant, government research facility, etc. provides an easily exploited window into the activities of the inhabitants and the nature of the devices contributing to the signal.

Such information would be of interest to a number of different parties currently without such direct access to information about personal habit. Insurance companies are always eager to obtain detailed information about their customers for rate calculation; perhaps a person seen to have poor sleeping habits would be given higher health insurance rates, or a person who often arrives home around the time bars close will be flagged by his auto-insurer as a drunk-driving risk. Marketers would certainly be interested in getting information about the lifestyles of potential customers, to allow for more focused ad campaigns. These examples of potential privacy violations and the examples to come (as well as many others) have been proposed elsewhere [5].

Personal Information Derived From Level Changes

As instantaneous data gains resolution, it becomes possible to isolate distinct changes in feature values and to read information from those level differentials. These recognizable level shifts are the basis of most load disaggregation techniques. When individual load events can be isolated and compared to other load events, patterns emerge

and can lead to precise load identification (see Figure 3). Once individual load signals can be separated out, it becomes possible to make inferences about the nature of the appliances. Perhaps a particular shift in signal features is caused by a security system being activated or deactivated, or a particular brand of refrigerator may have a discernibly different impact on the overall load signal than a competing brand.

Again, marketers would have a strong incentive to obtain such information if possible. The ability to separate those who already use your product from those who use a competitor's product (and from those who do not currently use any similar device) would give an incredible advantage to any company planning targeted advertising. On a more sinister note, a criminal using hacked meter data to canvass an upscale neighborhood could conceivably target specific houses for the particular devices seen to be in use there.

Once individual loads are identified and separated, a great deal of information can be gathered by watching their usage over time. An observer would be able to track which devices one uses more frequently than others, deduce one's daily routine from which devices are run consistently at specific times, or infer other personal characteristics from one's device usage. Thankfully, the well of personal information available in every power signal has not yet been tapped to its full potential; however, with the expansion of data introduced by smart meters, it's only a matter of time before that information is extracted and put to use.

Figures

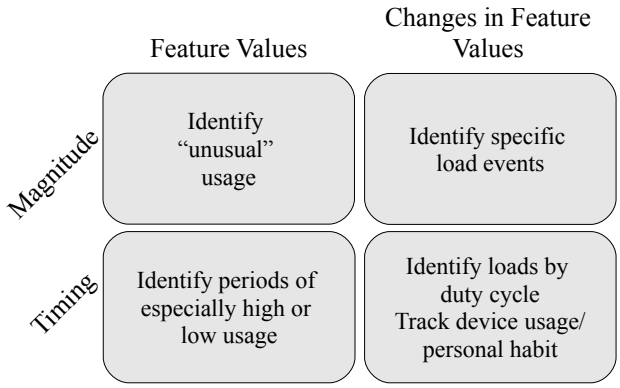

Fig. 2: A breakdown of the ways personal information can currently be deduced from one's power signal

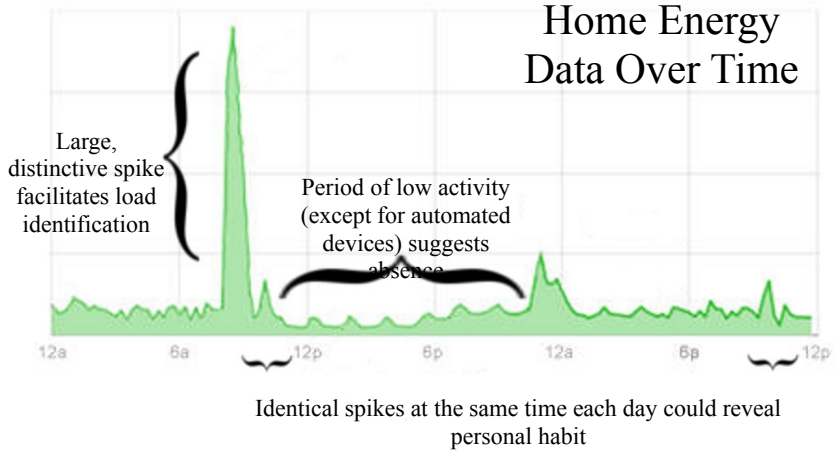

Fig. 3: Examples of revealing data embedded in power consumption data

CHAPTER 3: APPROACH

Theoretical Hardware Specification

The method described in this paper causes actual changes in the power signal drawn by a particular facility, and therefore requires the use of some extra hardware to create these distortions. Figure 4 shows the basic setup simulated for testing purposes.

The particular electronics enabling the implementation of the method laid out in this paper are not critically important. Any number of setups can be used, provided they can provide fast changes to power signal level. A high-level model was used for testing purposes, whose behavior can be specified using just a few parameters. It is worth noting that while the hardware simulated for testing used only power drawn from the grid, similar masking behavior could be achieved with fewer constraints using on-site generation.

Testing Model

An abstract, highly simplified hardware model was used in testing (Figure 5). The particular electronic implementation of such hardware is outside the scope of this paper – the use of a loosely defined model allows for the data obfuscation techniques discussed here to be implemented on a variety of different hardware setups. The focus of this thesis is on how to obscure load information in the externally visible power signal using such a device, not how to build one.

The simulated hardware used in testing can be described simply, using only two parameters: maximum charge rate and storage capacity. Conceptually, it can most easily be described as a controller hooked up to a bank of energy storage hardware, with the controller monitoring the unaltered power signal generated by the target loads and dictating current flow into and out of storage based on that input. However, with just a few more parameters, a wider range of implementations could be used as well (for example, integrating on-site renewable energy sources to alter the signal rather than storing/releasing grid power). For testing purposes, the limits on charge and discharge rates are assumed to be identical.

Existing Analog

The closest existing approximation of the hardware needed to physically implement these techniques would be equipment used to manage the output of variable, intermittent resources, such as wind farms. The peak times for power output of wind turbines are largely during troughs in demand, and vice versa. When the turbines are generating, the precise level of wind input cannot be controlled, only how much of the available power is harnessed. Equipment to store excess power until it is needed allows the wind farm to utilize more of the available power. A hardware system to serve this function has been proposed [12] and could potentially be re-purposed to mask load signals.

In principle, the interaction of the wind turbines and this storage equipment is the same as the interaction of the simulated hardware and load data used here. The only

difference is in scale and purpose of the signal modification. Similar hardware could just as easily distort the externally visible load signal generated by a facility as control the output of a wind farm.

The Load Signal

A number of different characteristics of the power signal might be used to identify and monitor the individual contributing loads, but the two major features observed by smart meters are real power and power factor. A simple real power signal has been used to deduce private activity within a residence [Error: Reference source not found]; while use of power factor as well could certainly give additional distinctions between similar loads, its usefulness is secondary to real power consumption. Therefore, the distortion method analysis here will focus on the real power component of the signal. A similar approach might be employed to disguise the power factor signal given the right hardware. The constraints on distortion level would be structured somewhat differently, but the core principles carry over.

Probability Metric

The probability measure used here is one designed for statistical clustering applications. Given a list of cluster centroids, it provides $p_i(x)$: the probability that any given point *x* should be associated with cluster *i* based on its proximity to all known centroids. $d_i(x)$ is the distance of point *x* from centroid *i*. In this application, $d_i(x)$ is defined as Euclidean distance. This metric, given in (1), was designed such that

$p_i(x)d_i(x)=c_i$ for some constant c_i [13].

$$p_i(x)=\frac{\prod_{j\neq i} d_j(x)}{\sum_{k=1}^{m}\prod_{j\neq k} d_j(x)} \tag{1}$$

This allows any observed level change x to be related statistically to each known load. Such a relation will prove useful to this investigation.

Ambiguity Metric

The masking technique discussed here is based on the idea of quantified ambiguity, an objective measure of the difficulty in discerning the motivating load event in an observed change in the power signal.

In Information Theory, uncertainty is quantified with the idea of entropy, a metric of disorder. Given a collection of m states, each with an associated probability p_i (for $i = 1,2,...m$), the entropy of the system is defined in (2):

$$S=-\sum_{i=1}^{m} p_i \log_2(p_i) \tag{2}$$

If the probabilities are defined as functions of an observed event x, the system entropy may also be expressed as a function of such observations and plotted over various values of x (as in Figure 6).

Distortion Techniques

Just as a number of techniques can be used to extract information from the signal,

different approaches can be taken with the aim of obscuring that same information. Even within the subset of analytic techniques focused on changes in signal level, different methods of obfuscation can give varied levels of protection. Two approaches were compared in testing: simple fuzzing and targeted entropy maximization.

Fuzzing

Simple fuzzing applies a randomly selected offset in power draw at certain points. To utilize the available storage strategically, the range of possible offsets is weighted low when storage usage is high, and high when usage is low. It offsets individual events simply, without requiring the controller to have any knowledge of the loads it is obscuring (time series example in Figure 7). Because of its simplicity, it was used as a control during testing.

Targeted Entropy Maximization

Targeted entropy maximization is based on a plot of entropy values as a function of observed event magnitude, evaluated over a specified collection of known loads. It uses some knowledge of the system being masked to make more efficient use of the resources available, picking an offset level with maximum impact on the ability of an external observer to distinguish between signal changes generated by different loads. A time series example of this sort of masking is given in Figure 8.

Using information about the various loads contributing to the signal, this method is able to make more informed choices of offset to apply. While the fuzzer sees each

event in isolation, this method can use information about how other loads will affect the signal to find the best choice for this set of loads. With some idea of what other events will appear in the signal later, strategic offsets can be made to minimize the ability of a third party to infer anything about the activities generating the observed power signal. Plotting the entropy of various potential event magnitudes based on a set of loads allows the controller to clump the appearance of actual events in more ambiguous areas, reducing the ability of an outside observer to pin down the load connected with any given event.

Applying Distortions

Both approaches used in testing are governed by the same rules defining when signal offsets are applied or adjusted. The application of offsets have two different goals, often in opposition. The primary end of the masking signal is, of course, to hide identifiable load events; however, as the simulated hardware has limited storage capacity, resource usage can be a consideration as well. When the available storage is nearing full charge, the controller's ability to offset the signal downward is crippled; likewise, as the storage approaches complete discharge, the controller is limited in its ability to raise the observed signal. Maintaining mid-level storage usage allows the most flexibility to apply offsets in either direction as needed.

Three conditions prompt the controller to reevaluate the applied offset:

1. A significant change in signal level is detected.
2. Storage is approaching full or empty.

3. A specified timeout is triggered.

In the event of any of these three conditions, the controller changes the flow of energy to or from storage, raising or lowering the observable signal level. Depending on which obfuscation approach the controller is using, different considerations are given different weights while determining the appropriate offset to apply (as laid out in Figure 9).

A condition 1 trigger puts obfuscation as the highest priority. At the moment of an observable load event it is far more important to obscure the event than to maintain a strategic usage level in storage. However, it still takes the current storage utilization into consideration. If the storage is nearing capacity, potential offsets which would require unsustainable levels of charging are not considered – instead, the entropy values of various discharge rates are compared. Likewise, when storage is nearly empty, charging offsets are favored over discharging masks.

Conditions 2 and 3 put a higher priority on pulling storage toward a strategically flexible level. As there are no actual load events to obscure, any change in either direction will provide some level of misdirection to an attempted analysis of the observable signal. Condition 2 is, naturally, more urgent from a storage management standpoint; condition 3 may not even come into play if the storage capacity is small relative to the magnitude of the masks being applied (causing the storage unit to charge and discharge fairly rapidly). Condition 3 allows extraneous signal events to be inserted (independently of the available storage capacity), camouflaging the timing of genuine load events.

Figures

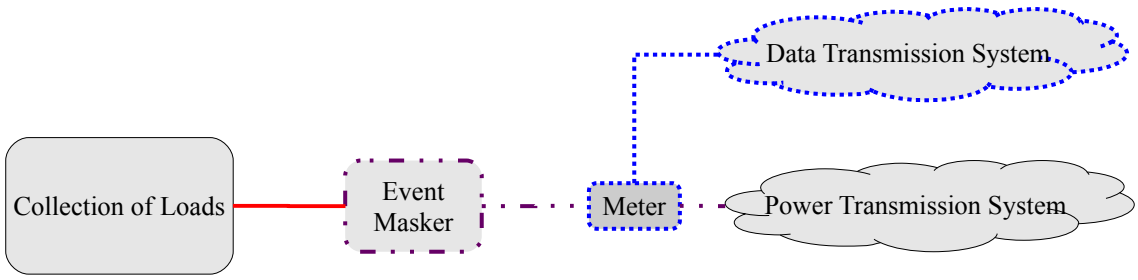

Fig. 4: Positioning of masking hardware in the power system

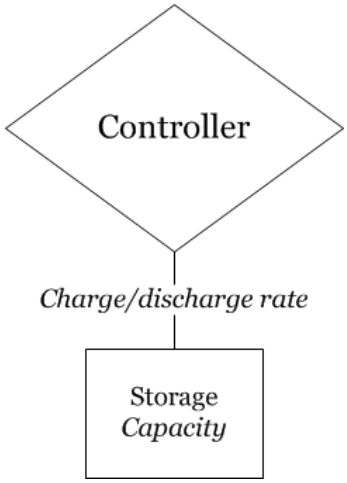

Fig. 5: Model of simulated hardware

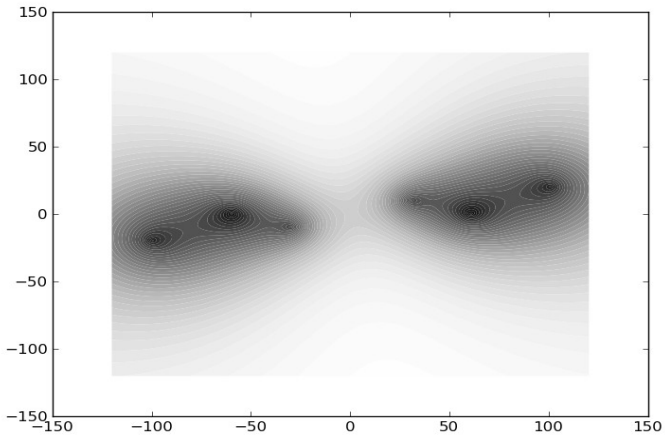

Fig. 6: An example of an entropy map plotted on the PQ plane (W vs. VAR)

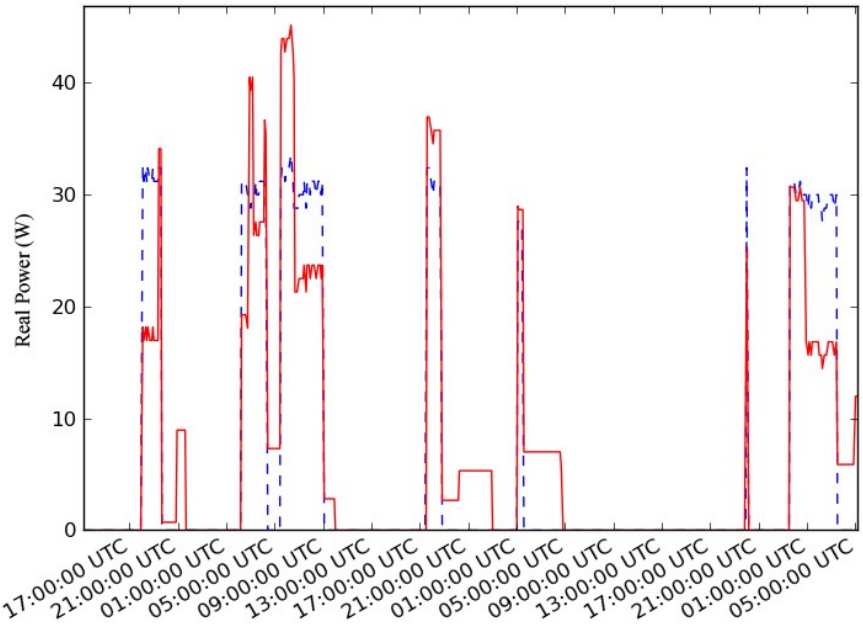

Fig. 7: Example time series plot of a raw power signal and its fuzzed output

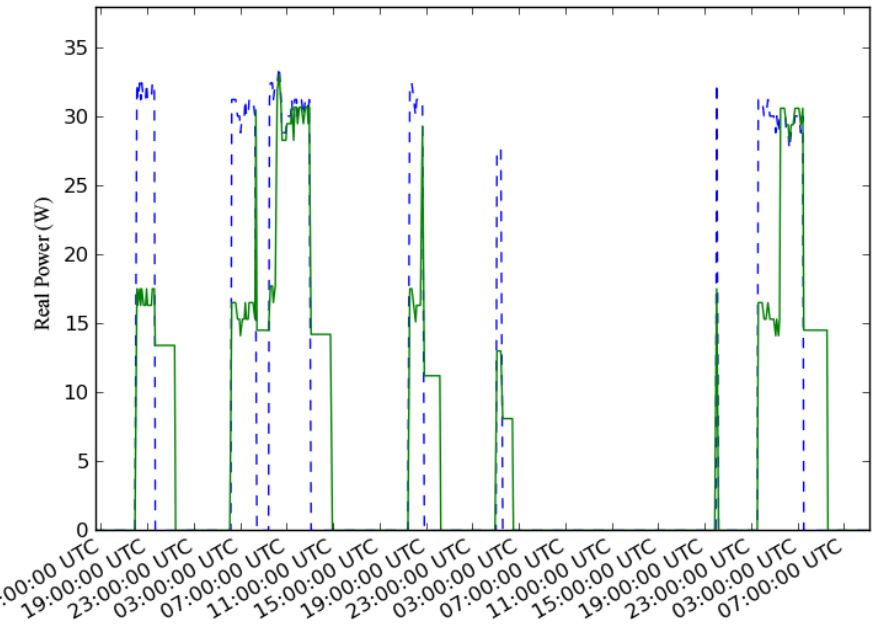

Fig. 8: Example time series plot of a raw power signal and its masked output

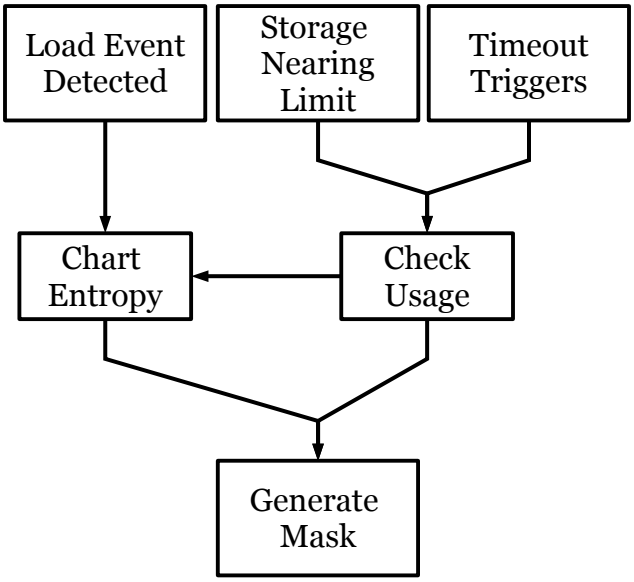

Fig. 9: Masks are generated in different ways depending on the triggering condition

CHAPTER 4: PERFORMANCE METRICS

Given the variety of approaches to power signal analysis which could facilitate a breach in privacy, it is difficult to define a single metric to evaluate a defensive method's effectiveness. While multiple metrics are used here, even together they cannot give a complete quantification of the described defensive methods' ability to prevent invasive analysis. However, by using multiple, granular metrics based on inherent properties of the information in the signal, different methods can be compared to one another and a general sense of their relative effectiveness can be established.

For the purposes of evaluating and comparing the targeted masking approach to a simple fuzzing scheme, two metrics are used: one to measure the distortion of individual, identifiable events in the signal and one to examine the information revealed by emergent patterns over time. The first metric looks at the individual methods' abilities to prevent observed load events from being classified correctly, and the second shows how well they can mitigate the use of multiple load events to deduce the load composition of the signal.

Single-Event Metric

The focus of the masking technique described here is load events, observed as changes in signal level. Analytic techniques applied to these observed events will seek to match an event (or sequence of events) to a known load, to isolate its effect on the overall signal. In order to evaluate a masking technique's ability to prevent such analysis, a general metric is needed which will quantify the ability of any number of analytic

approaches to correctly classify observed events.

The distance-based probability measure described earlier allows for a general evaluation of a masking technique's effectiveness on this front. Given knowledge of the unmasked signal (and the loads creating it), the probability that an observed event will be associated with the correct device can be calculated easily. This evaluation does not constitute a precise metric of success. Certain attacks might be more likely to classify the event correctly; certain others might be less likely to get it right. However, it does give a granular metric for evaluating the relative effectiveness of different masking techniques without relying on the strengths or weaknesses of a specific attack.

Combined-Event Metrics

These give measures of the error introduced to attempts at identifying loads statistically, gathering data from many events over time. They are not concerned with the odds of specific, individual events being classified correctly but instead look at the overall distribution of visible events and their timing.

An analytic technique using an unguided learning approach to load disaggregation will use event trends to determine characteristics of the loads creating them. A masking technique may distort individual events but leave the overall signal vulnerable to statistical analysis. By comparing what information might be gleaned from the obscured signal to the actual load composition, a technique's ability to prevent such deductions can be evaluated. Two combined event metrics were used to evaluate the performance of the distortion methods: event cluster centers and average event frequency.

The first method, based on event cluster centers, aggregates all actual events and finds their cluster centers. This approach gives a sense of how events are altered independent of the additional, spurious changes in signal level injected by the controller managing the storage. If an attacker were to use some unmasked characteristic of the signal (for instance, power factor) to differentiate between actual load events and red herrings created by the controller, this metric evaluates what information could be gleaned. Additionally, cluster information including the spurious events created by the controller could provide some additional insight; however, the clusters created by the controller-created events vary significantly over different runs and are therefore difficult to track over consecutive simulations. Using only the altered magnitudes of the real events provides a cleaner picture of the effects of different methods and different simulation setups.

The second metric is the expected number of events per hour. While the raw signal probably is not predictably periodic, if the mask is changed too often then its effects can be filtered out. It is worth noting that under some circumstances drastically increasing the event frequency can be desirable (for instance, if one wishes to hide an actual decrease in activity); however, increasing the frequency is a simple matter of setting the desired time-out in the controller. Strategic use of available storage will have a smaller necessary impact on the frequency of observed events, making it more difficult to filter out the masker's effects.

CHAPTER 5: TEST CASES

Power Signal Used

The data used in testing is the real power consumption of a 30W lamp over the course of two weeks. This provides a simple case which should allow for easy identification of the load (absent any obfuscation). The lamp is a basic two-state device with no significant variation of consumption in either state. When it is turned on, its power draw stays within a few watts of 30; it draws no current at all when turned off. Low levels of noise exist in the signal, so a noise threshold of 5W was used in analysis (of both the raw and distorted signal). Observed events above 5W were considered significant; events below 5W were disregarded as noise.

Permutations of Relevant Hardware Parameters

In order to investigate the marginal benefits of each hardware parameter – maximum charge rate and storage capacity – a range of values was used in testing.

Maximum Charge Rate

The rate at which the storage can draw power from (or inject power into) the unmasked signal at any given time defines its ability to alter identifiable load events in the power signal. Increases in charge rate directly impact the nature of the resulting, obfuscated signal.

Since the magnitude of the signal being masked is the primary factor in determining how effective a given offset value is, the values of maximum charge rate tested were based on the scale of the test load. Tests ranged over limiting values from 5W to 60W in 5W increments to evaluate how masking ability changed as the model's ability to completely mask the 30W magnitude on/off events increased.

Storage Capacity

The available energy storage at any given time defines the amount of time the hardware can sustain a particular level of masking. High-capacity storage gives the controller more freedom to draw or inject higher levels of power for more extended periods. Low-capacity storage requires the controller to operate with many short charge/discharge cycles.

The important factor for storage is not the absolute size of the storage but its size in relation to the maximum charge rate. A setup with a low maximum charge rate will not require as much storage as a setup with a high charge rate. Therefore, to allow a comparative analysis of “low” storage capacity and “high” storage capacity, the total amount of energy storage available was defined by how long it could sustain a constant charge at the given rate. Values up to 3 hours of charging (in 15-minute increments) were used at each of the given charge rates. Therefore, a 5Wh storage capacity for a 5W charge rate could be roughly compared to a 30Wh capacity for a 30W setup. This approach allowed for evaluation of the effect storage size had on performance independent of the charge rate being used.

CHAPTER 6: RESULTS

Influence of Charge Rate

Simulated hardware setups were tested with charge rates ranging from 5W to 60W (twice the magnitude of the load events being hidden) in 5W increments.

Single-Event Metric

As shown in Figure 10, the effectiveness of both fuzzed and masked approaches steadily increased until reaching the 30W magnitude of the actual load events, and then both level out. Figure 11 shows just the points of continued improvement for each method, which show a strongly linear progression in both but with steeper improvements using the targeted masking approach.

Combined-Event Metrics

Figures 12 and 13 show the distribution of all observed signal events using a variety of charge rates (up to 30W). On the far left is the unaltered distribution of the raw signal, and each subsequent column shows the distribution of a separate run with the charge rate incremented by 5W. With a charge rate as low as one-third of the actual load event magnitude, each method is able to begin mixing the load events with spurious level shifts. Figures 14 and 15 give a cleaner view of the event distribution at this point. No clear distinction is apparent between distorted load events and events created by the controller.

Figures 16 and 17 remove the spurious events and show the distortion of events stemming from the actual load. The separation is not perfect (as suggested by the presence of 0 magnitude "events" and outlying noise points), but the cluster shifts over each iteration are apparent.

Figure 18 shows the trends of the observable cluster centers belonging to actual load events. While both fuzzing and targeted masking tend to drift the centers toward zero, masking does so more directly.

Influence of Storage Capacity

Different levels of storage capacity were used in testing, defined relative to the charge rate limit of each run. Storage capacities able to support up to 3 hours of constant charge or discharge were tested, in 15-minute increments. Storage capacity was not found to have a notable impact on the success of masking individual events, as shown in Figure 19. It did, however show an evident influence (over a certain range) on the observed event frequency, as shown in Figure 20.

Figures

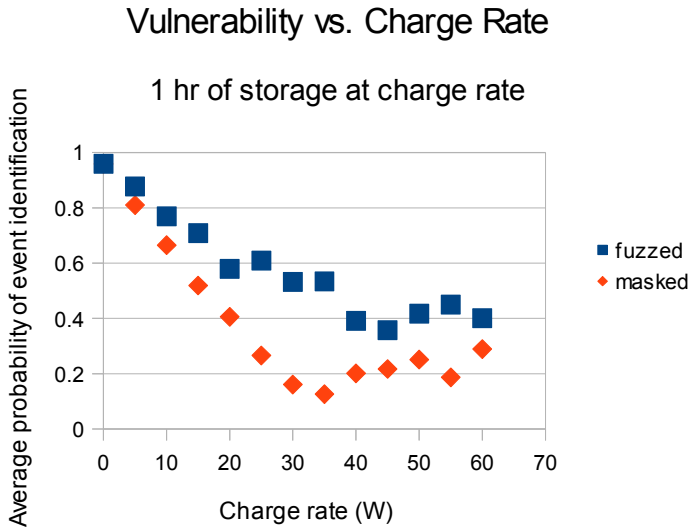

Fig. 10: Gains from increased charge rate level out or diminish past the level of the load.

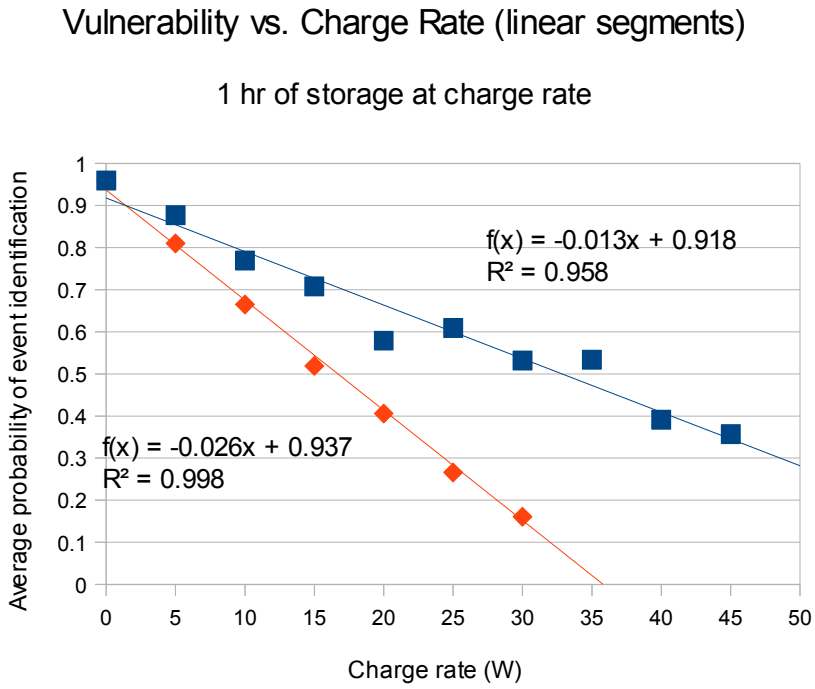

Fig. 11: The effectiveness of the mask increases linearly as the charge rate approaches the load level.

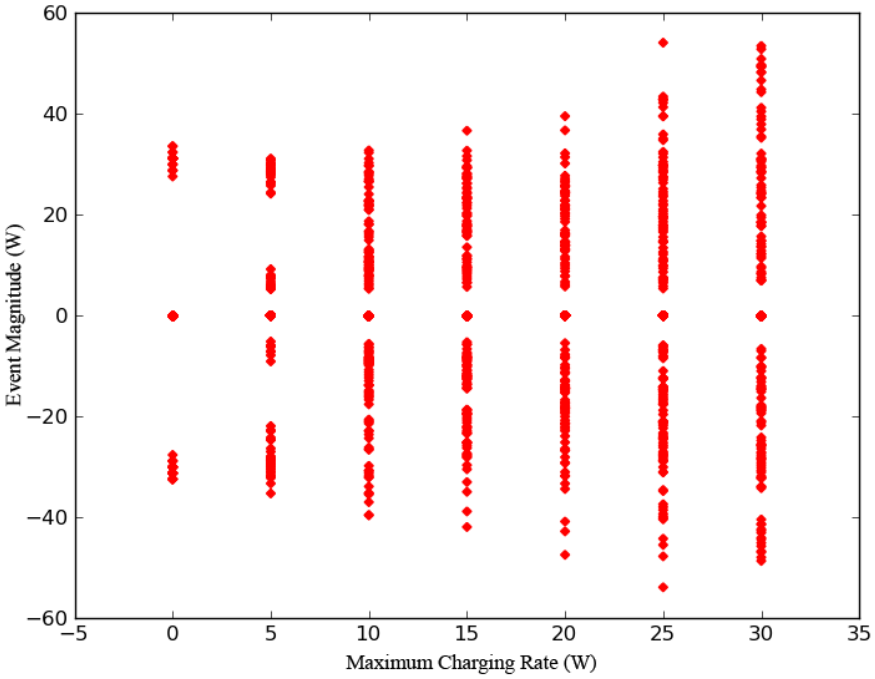

Fig. 12: Observed event clusters over 6 runs of fuzzing with varied charge rate limits

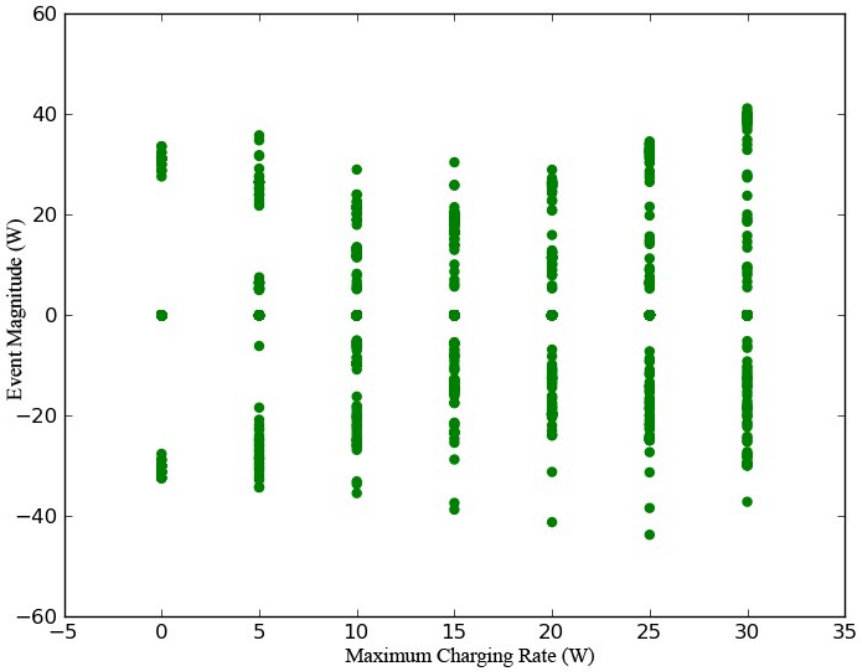

Fig. 13: Observed event clusters from 6 runs of targeted masking with varied limits on charge rate

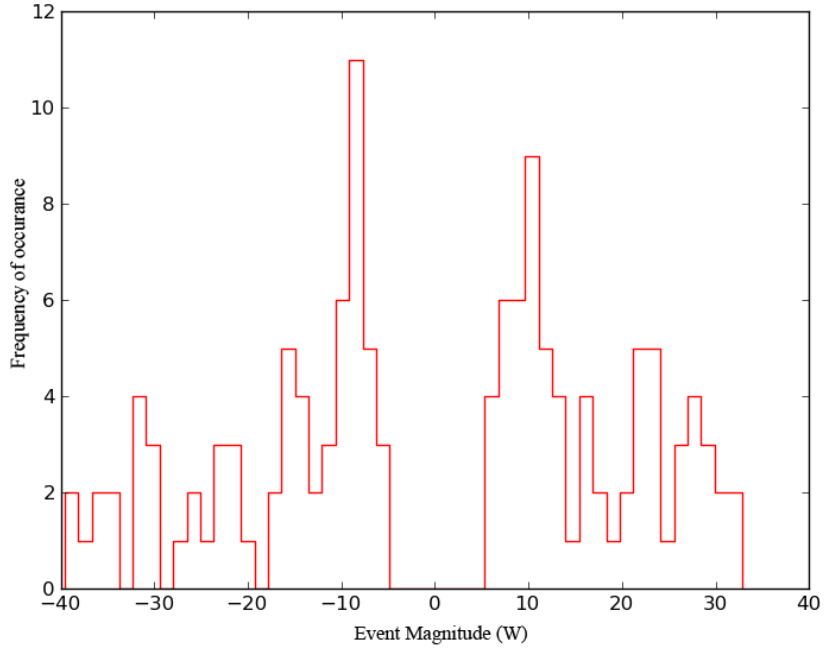

Fig. 14: Histogram of fuzzed events at 10W charge rate with 10Wh of storage

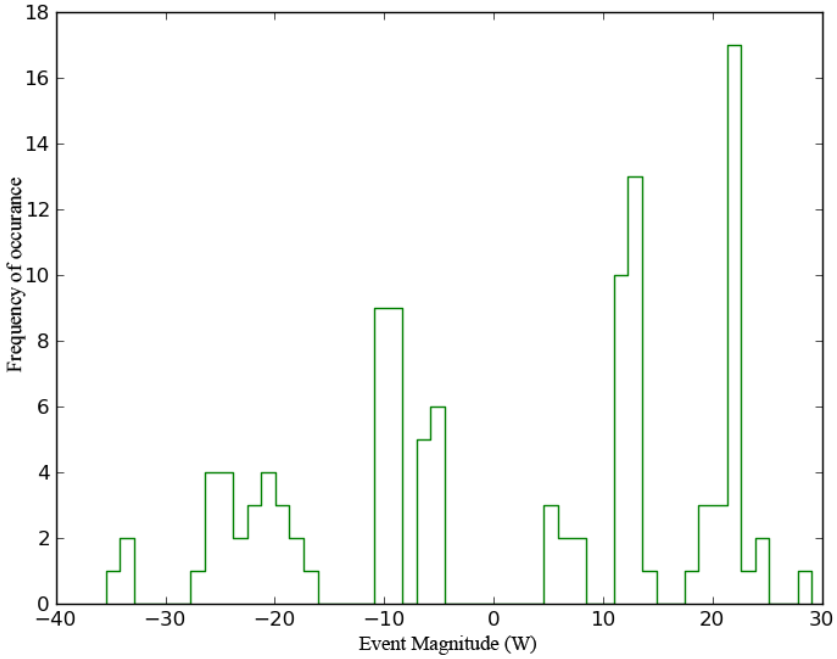

Fig. 15: Histogram of masked event distribution at 10W charge rate with 10Wh of storage

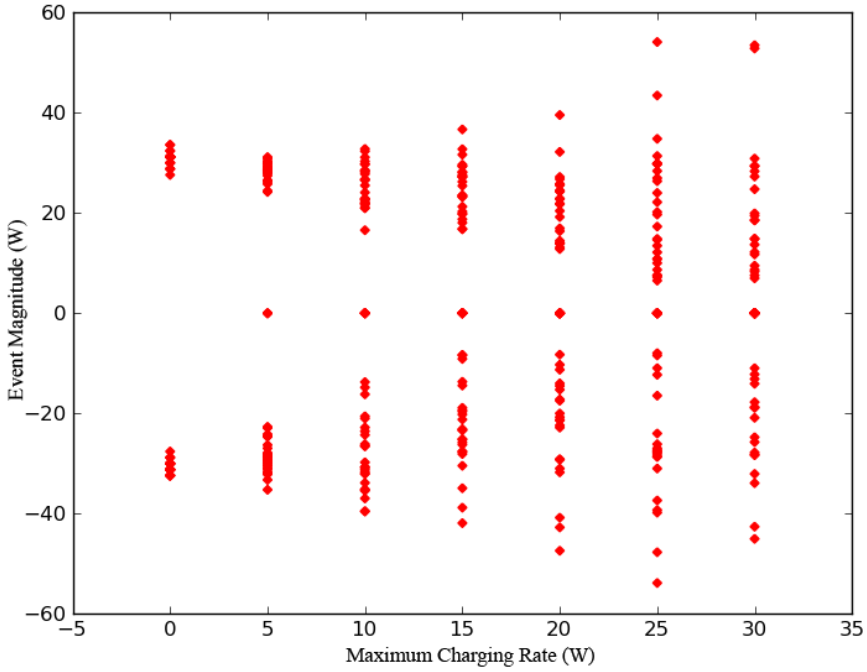

Fig. 16: Fuzzed load events

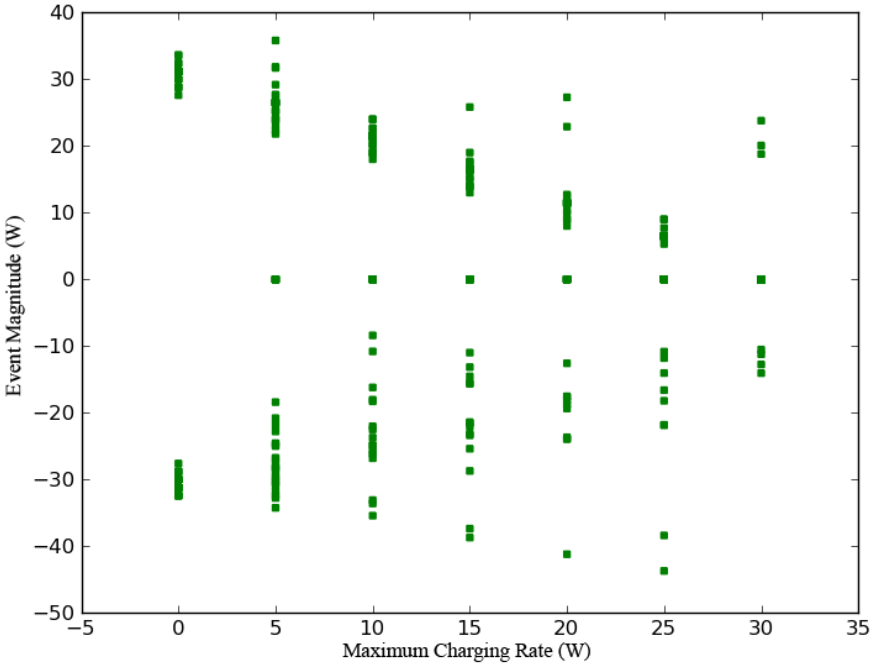

Fig. 17: Masked load events

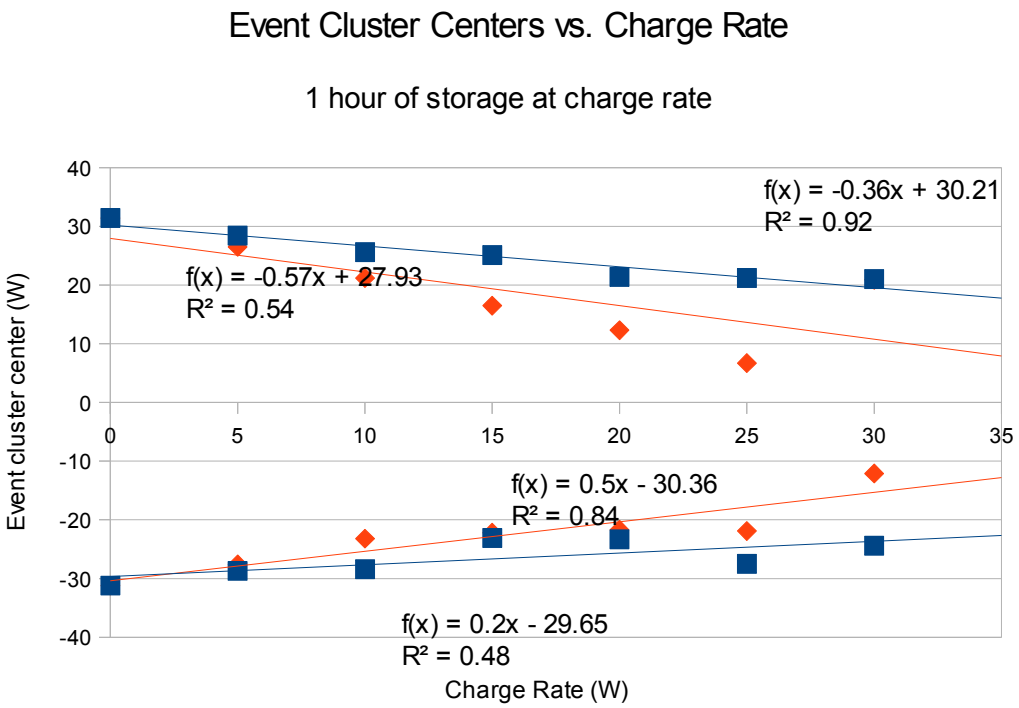

Fig. 18: Trends of cluster centers (fuzzed and masked) over varied charge rates

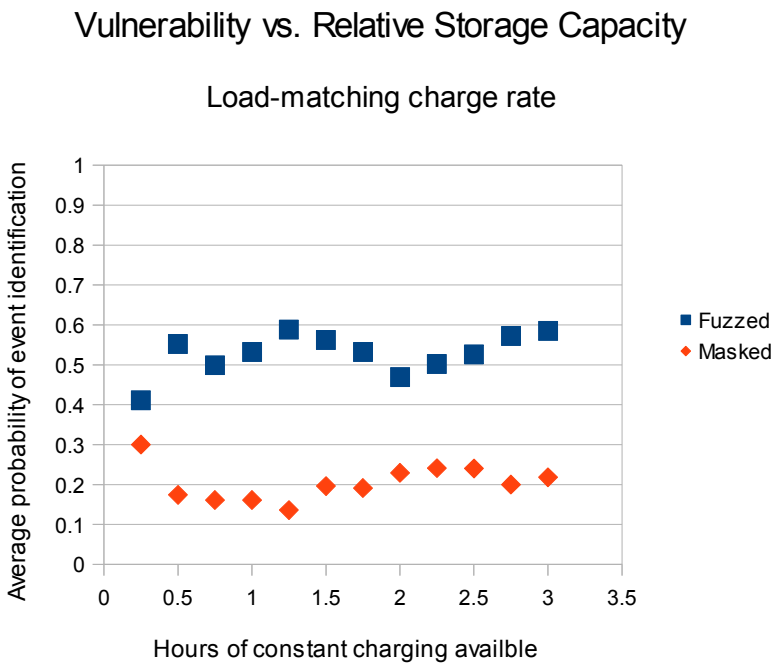

Fig. 19: Increased storage capacity does not improve the masking of individual events.

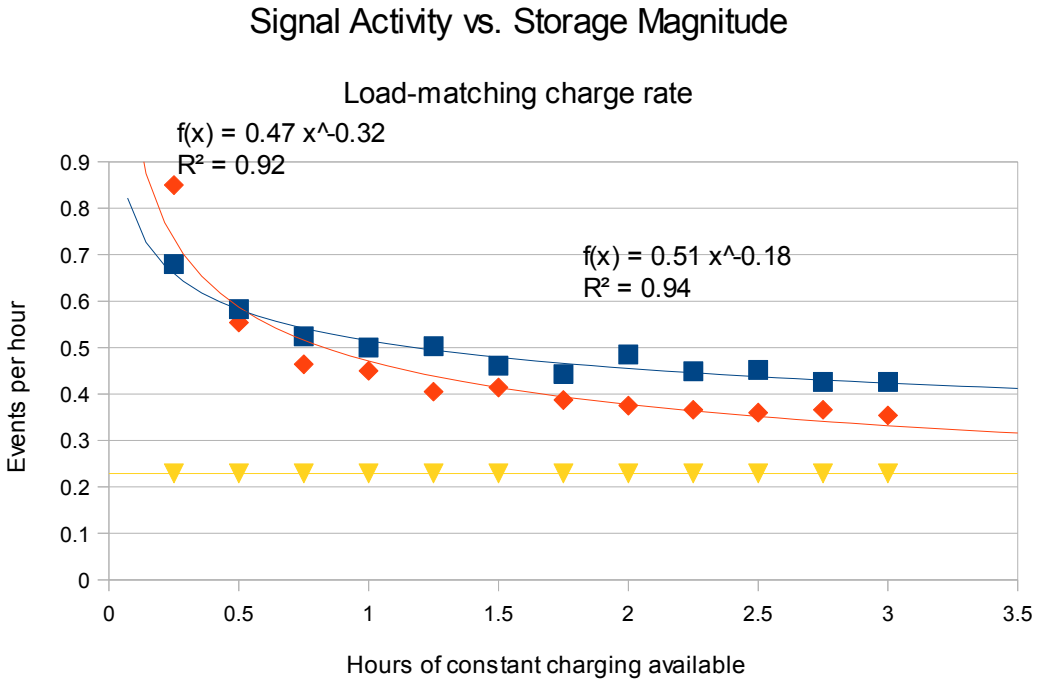

Fig. 20: The impact of storage capacity on observed event frequency

CHAPTER 7: CONCLUSIONS

Targeted Masking

In each of the performance metrics defined for these tests, the targeted masking approach outperformed the control method.

Single-Event Metric

As shown in Figure 11, the targeted masking approach makes significantly more effective use of the available charge rate when obfuscating individual events. Both methods display linear improvements with respect to maximum charge rate, but targeted masking achieves a slope twice as steep as random fuzzing. For any given charge rate, targeted masking is able to obscure load events roughly twice as effectively as random fuzzing.

Combined Event Metrics

The results in Figure 18 are not as definitive (given the traces of noise in the clusters), but targeted masking still shows the same gains as observed by the single-event metric (as would be expected, given both of their dependence on the average event offset). These results are not entirely redundant, however, as the clusters allow the positive and negative events to be compared independently.

Figures 16 and 17 show another advantage of targeted masking – less quantitative but certainly worth note. As the charge rate available increases, the fuzzing method

naturally spreads out the load events, but targeted masking draws them all in toward the noise threshold. When the charge rate reaches the same level as the signals being obscured, the fuzzed events are strewn about, but the masked events are mostly indistinguishable from noise. An outside observer would have significant difficulty determining that an actual load event had occurred at all.

Event-Frequency Metric

As shown in Figure 20, smaller storage capacities have a large impact on the frequency of observed events. Anything larger than about 1.5 hrs of storage levels out for both targeted masking and fuzzing; however, again, masking makes better use of available resources than fuzzing. The raw signal shows an event approximately every 4 to 5 hours. Both distortion methods increase the event frequency (to maintain strategic storage levels); however, the increase injected by masking is notably lower than that of random fuzzing. Some runs with enormous storage (6 hrs, 12 hrs, 18 hrs, and 24 hrs of charging supported) showed the fuzzed signal frequency levels out at .44 events/hr, and the masked signal frequency level at .34 events/hr (compared to the raw frequency of .23 events/hr).

Hardware Parameters

Based on the simulated results, some recommendations can be made in regards to physical implementation of the modeled hardware. Whether or not current energy

storage technology can deliver on these recommendations, or do so economically, depends greatly on the nature of the loads being protected.

Charge Rate

It was found that charge rate was the primary factor in determining the ability of the controller to obscure individual load events. Rates approaching the magnitude of the signal being distorted gave linearly increasing protection; rates higher than the target signal did not provide any additional advantage.

When combined with the spurious signals generated by the controller, relatively low charge rates provided reasonable levels of protection. This finding suggests that facilities wishing to disguise some large load events need not obtain distortion hardware capable of giving an offset equal to the largest load. As shown in Figures 12, 13, 14, and 15 a fraction of that level can provide a reasonably garbled distribution. As similarly sized load events tend to merge into one another, the hardware required to provide adequate protection will be determined by the largest gap between known load event magnitudes.

Storage

Storage capacity proved to have little influence on the effectiveness of either approach beyond a certain base level. Where that base level falls depends on the raw event frequency, but subsequent increases in storage space have little effect on the performance of the masker.

Potential Improvements

The effectiveness of this system has been demonstrated on a simple case; however, some improvements could be made to cope with more complicated attacks or complex loads.

Revise Probability Metric

The current probability metric relies on discrete, consistent, single events. Many loads display a more complicated profile in the power signal, and an updated probability metric to better represent those sorts of loads would allow this method to more effectively hide those patterns.

Time/State-Sensitive Entropy Mapping

The current system uses one, precalculated entropy map to determine optimal event offsets. However, some attacks may use knowledge of load timing or state to aid in identification. While recalculating the entropy map on the fly may be complicated for some systems, use of a number of precalculated maps for different circumstances would allow a more effective response to such attacks.

REFERENCES

[1] M. Lisovich, D. K. Mulligan, and S. Wicker, "Privacy concerns in upcoming demand-response systems," in *Proc. of the Clemson University Power Systems Conference*, 2008.

[2] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, no. 2, pp. 12–16, June 1989.

[3] S. Wicker and R. Thomas, "A Privacy Aware Architecture for Demand Response Systems," in *Proc. of the Hawaii International Conference on System Sciences,* 2011, pp. 1-9.

[4] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy Magazine*, vol. 7, no. 3, pp. 75-77, May/June 2009.

[5] E. L. Quinn. (Fall 2008). Privacy and the new energy infrastructure. Center for Energy and Environmental Security, working paper no. 09-001. [Online]. Available: http://ssrn.com/abstract=1370731

[6] D. K. Mulligan et al. (March 2006). Privacy and the law in demand response energy systems. Samuelson Law, Technology and Public Policy Clinic, presentation. [Online]. Available: http://www.truststc.org/pubs/36/

[7] Cyber Security Coordination Task Group, A. Lee, lead, and T. Brewer, ed., "Cyber security strategy and requirements," National Institute of Standards and Technology, draft NISTR 7628, Sept. 2009.

[8] J. Hood. (8 Nov. 2009). Class action accuses PG&E of overcharges. ConsumerAffairs.com. [Online]. Available: http://www.consumeraffairs.com/news04/2009/11/pge_suit.html

[9] J. Smith. (16 Nov. 2007). APD pot-hunters are data-mining at AE. The Austin Chronicle. [Online]. Available: http://www.austinchronicle.com/news/2007-11-16/561535/

[10] T. Goodspeed, D. R. Highfill, and B. A. Singletary, "Low-level Design Vulnerabilities in Wireless Control Systems Hardware," in *Proc. of the SCADA Security Scientific Symposium*, 2009.

[11] W. Boyer and S. A. McBride, "Study of security attributes of smart grid systems—current cyber security issues," Idaho National Laboratory, tech. rep. INL/EXT-09-15500, April 2009.

[12] M. Bottu, M.L. Crow and A.C. Elmore, "Design of a Conditioner for Smoothing Wind Turbine Output Power," in *Proc. of the North American Power Symposium*, 2010.

[13] A. Ben-Israel and C. Iyigun, "Probabilistic D-Clustering," *Journal of Classification*, vol. 25, no. 1, pp. 5-26, June 2008.