Poster: Toward Energy-Wasting Misbehavior Detection Platform with Privacy Preservation in Building Energy Use

Depeng Li
Department of Information and Computer Sciences
University of Hawaii at Manoa
Honolulu, HI, USA
depengli@hawaii.edu

Sachin Shetty
Department of Electrical and Computer Engineering
Tennessee State University
Nashville, TN, USA
sshetty@tnstate.edu

ABSTRACT
Energy-wasting behavior is a big concern as it wastes around 1/3 of all energy consumption in buildings. Current solutions to address this issue either rarely offer privacy preservation or cannot satisfy occupants' comfort in an acceptable level. In this paper, we first propose an energy-wasting behavior detection platform. Based on that, we address a couple of privacy-related challenges in our platform through utilizing functional encryption to hide video data and by introducing noise disturbance which is mixed with metering data e.g. A/C power consumption signatures. In a privacy framework we proposed, we further quantify the privacy leakage by a set of theoretical models e.g. hidden Markov model and differential privacy. Since our paper is still at its start phase, we plan to further extend our privacy evaluation model, assess privacy leakage on real-world dataset and accomplish experiments and we wish it could inspire colleagues' interests in this area.

Categories and Subject Descriptors
K.4.1 [**Computer and Society**]: Public Policy Issues – *Privacy*;

General Terms
Measurement, Documentation, Theory

Keywords
Energy-wasting; Misbehavior; Privacy Preservation

1. INTRODUCTION
There is a clear demand to reduce or even eliminate the energy-wasting in buildings, given the tremendous energy consumption as well as associated CO_2 emissions. Buildings accounts for more than 40% of electricity consumption in United States and 37% in EU, which is even bigger than industry (28%) and transport (32%) [7]. Surprisingly, around 33% of energy consumption in buildings results from careless behaviors [8]. Wasting energy in buildings not only increases occupants' utility bills, it strains an already overtaxed power grid, which can affect the contribution to climate change, a topical issue the world over.

A number of promising energy-saving technologies, such as demand-response programs, sensing schemes, etc. have been designed and developed to reduce the energy consumption in smart buildings. However, they are not designed to prevent energy-wasting misbehaviors. Here are two examples of poor behavior: (1) to enhance indoor air quality, residents open windows to get fresh air. Meanwhile, they may also leave the Air Conditioner (A/C) turning on to satisfy their comfort in a co-paid residential building. (2) Since they do not need to pay the power consumption bill, in office buildings, some careless employees leave A/C turning on when they leave their offices. Obviously, our society has already paid the attentions to occupants' misbehavior because of the tremendous amount of energy wasting [7]. Though some technologies have been developed to detect the energy-wasting misbehavior, there are still some challenges: (a) how to protect occupants' privacy and (b) how to satisfy occupants' comfort. First, when we integrate energy-wasting detection / energy-saving technologies with cyber-enabled processing, extensive private data e.g. identification of consumers, presence/absence of occupants, real-time usages of appliance, etc. are captured by utility companies or authorized third parties. The privacy violation could potentially prevent residents from participating in the energy saving projects since privacy protection is also important. Second, if the energy-wasting detection could possibly degrade the comfort that customers/residents are used to, they may also refuse the introduction of energy-wasting detection technologies [4].

Our contributions: here, we supply an energy-wasting detection platform. More importantly, our platform is not only protected by a series of privacy protection methodologies but also assessed under our theoretical privacy framework to analyze the privacy leakage through accommodating fundamental functionality e.g. noisy perturbation, differential privacy [9], etc. The aggregated time-series power consumption data and the dataset stored in cloud for smart building system will be evaluated. We not only study potential privacy inference but also try to address corresponding concerns about privacy loss. Our contributions are listed below:

(a) We propose a low-cost energy-wasting detection framework which includes two kinds of technologies: field sensing and power consumption audit operation. The former will utilize sensing and monitoring schemes to detect misbehaviors and identify "indecent guy" in near real-time. The latter, in combination with the former, will locate suspicious, indecent events via intrusively evaluating energy consumption demand. Our future plan is to construct mis-behavior models to detect energy-wasting events, analyze root cause, and provide accountability for energy-saving buildings.

(b) Either energy-saving technologies or energy-wasting detection schemes could potentially leak the privacy of consumers. As privacy is a big concern, we aim to decrease the possibility of privacy violations. Regarding our energy-wasting detection technologies, how to unveil privacy is articulated and how to hide privacy is developed in compliant with original platform. In detail, based on the captured sensing real-time messages, we demonstrate how to unveil residents' activity e.g. residence occupancy. Furthermore, in terms of A/C energy-usage detection schemes, we utilized noise disturbance to hide the occupants' A/C power demand signatures. And we also try to quantify its privacy leakages based on a series of measurement schemes ranging from

CCS'15, October 12-16, 2015, Denver, CO, USA.
ACM 978-1-4503-3832-5/15/10
http://dx.doi.org/10.1145/2810103.2810128

differential privacy to Markov chain, etc. We will validate our proposals through a set of dataset of building power consumption.

2. OUR SOLUTION ARCHITECTURE

2.1 Operable Windows and Misbehavior

Some occupants prefer to open the operable windows e.g. naturally ventilated or mixed-mode, to increase air change rates and also to promote indoor air quality [1]. This is valuable as, according to a widely cited study [11], in buildings with Air Conditioner (A/C), around 30-200% higher incidence of sick building syndrome symptoms is reported as compared with that in naturally-ventilated buildings. Thus, there are 2-5% windows in naturally-ventilated buildings which have been opened for most of the year.

However, a lot of energy goes to waste due to compromised or poor occupants' window-open behavior: Some occupants leave the windows open even when the A/C is still turning on, some occupants leave equipments or devices on when they leave their work stations in office building [7]. It turns out that the dark side of occupants' behavior maybe the weakest link in terms of energy saving since they do not pay electric bills. Without enforcement, there is rare motivation for them to stop wasting energy.

2.2 Architecture of Energy Wasting Detection

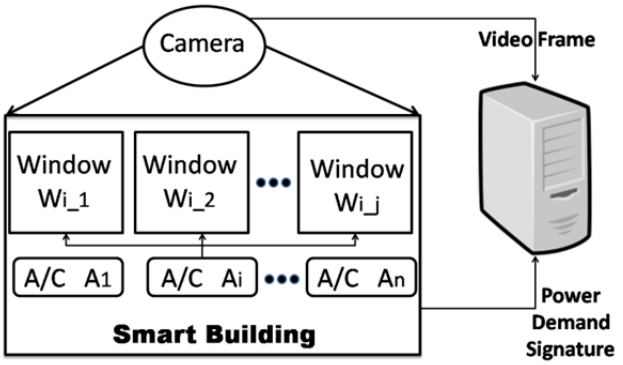

Figure 1 - Architecture of Energy Wasting Detection

As depicted in Fig. 1, our energy wasting detection architecture includes a camera, operable windows and air conditioners in the buildings. The occupants do not need pay the electric consumption bill introduced by the air conditioner. The power demand data generated by the air conditioner will be forwarded to utility or a third-party for purpose of bill generation and bill payment.

Let C denote the camera, W_{i-j} denote a window in which i means the index of the room and j represents the index of the window in room i. Let A_i denote the A/C in room i. We assume that the camera C could cover all windows of the building. The reason is that if it cannot, we can always add a few more cameras.

Our energy detection platform obeys the direct monitoring regarding measuring energy consumption [10]: the camera C is utilized to capture the state of each window e.g. realizing whether a window W_{i-j} is open or not at time point t. Meanwhile, to identify the A/C appliance usage at time point t, we use coarse-grained power consumption monitoring system whose granularity is just one pre-installed power meter – a popular solution in each normal home now. The rationale of this configuration is to keep the cost low (only a camera should be specifically installed) and take advantage of NILM (*Non-Intrusive Load Monitoring*) or NALM (*Non-intrusive Application Load Monitoring*) system which can disassemble A/C load signature though intrusiveness. Our algorithm is that, at time point t and in room i, if one of the windows W_{i-j} is open and the corresponding A/C A_i is turning on, it is identified as a *window-open & A/C turning on* energy-wasting misbehavior.

2.3 Threat Models

As other researches [5] in areas of privacy preservations, we assume that devices e.g. cameras, power meters, etc. in buildings and the cloud/server obey network communication schemes. However, they have the intension to combine the information to peek the privacy if possible. However we need at least a fraction of them (e.g. a majority) are honest.

3. PROBLEM DESCRIPTION

3.1 Privacy Leakage

As mentioned in sub-section 2.2, at every time point t, a camera C record the state of a set of windows, $W = \{W_{i-j}\}$ where i, j are values. Meanwhile, the state of a set of A/C, $A = \{A_i\}$ where i is a value, is collected. Our algorithm could decide the existing of an energy-wasting misbehavior among all rooms in the building.

Privacy leakage of recorded video by camera: some occupants may stand behind the window or operate the window at a time point t. The captured video may leak the occupants' activities as well as their presence at the room.

Privacy for residence occupancy: The turning on/off state of A/C can let an adversary infer that the resident is presence or absence (also referred as *absence privacy*).

Example I: The A/C in Alice's room is turning off when the local temperature outdoor is high (e.g. >104°F/40°C). Eve can probably infer that Alice maybe absent at her room. Eve can be aware of Alice's activity and Eve even can take the risk to break in.

3.2 Requirement Satisfactions

After carefully studying the energy wasting detection system, we realize that the following requirements should be satisfied:

- *Energy-Wasting Misbehavior Detection*: detect occupants' poor / compromised behavior and prevent such kind of behavior from happening.
- *Privacy Preservation*: Quantify the privacy leakage and minimize the possibility that the privacy is unveiled.
- *Comfort Satisfactions*: Provide comfort environment for occupants in the building.
- *Compliant with current system*: the enhanced solution should be compliant with current system and ideally should not add extra hardware.

4. ENHANCED SOLUTION

4.1 Preserve Video via Functional Encryption – Attributed Based Encryption

In our energy-wasting detection platform, a camera C records a series of video frames, $V = \{\dots, v_i, \dots\}$ where v_i is one frame of videos and $v_i = \{t, [p]_{n\times m}\}$ in which t is a time point and $[p]_{n\times m}$ is a matrix containing $n \bullet m$ number of pixels e.g. p_{ij}. Note that our proposal only targets at window related pixels. Since the camera is normally installed by property management companies for purpose of security monitoring, building maintenance, etc., they may use other pixels in frame v_i of V but this is out of the scope of this paper. Our energy-wasting detection platform will only search and examine images containing

window-related pixels but reveal nothing about other images such as occupants' activities, furniture, accompanies, etc.(e.g. pixel-erasing algorithm). We intend to invoke the Functional Encryption (FE) [2], specially, Attribute-Based Encryption (ABE), a special case of FE.

Following FE definition, we let our PE be $P_n: K \times I \rightarrow \{0,1\}$ where $K \coloneqq \{0,1\}^n$ is the set of all n bit string which represents n Boolean expression, I is the index space which is associated with the plaintext pair (ind, m). In our platform the m is window-related pixels p_{ij} and the ind is the window identification, i_j. Finally, the operation of P_n is defined as

$$P_n(D \in K \setminus \{\epsilon\}, ind = \phi \in I) \coloneqq \begin{cases} 1 & if\ \phi(D) = 1 \\ 0 & otherwise \end{cases} \quad (1)$$

where $D = \{d_1, \dots, d_n\} \in \{0,1\}^n$ are Boolean variables and ϕ are Boolean formula, and ϵ is empty key;

When utilizing the ABE algorithm, we assign the attribute set as $attr\hat{A} = \{attr1$="*windows Id*"; $attr2$ = "*window-related*"; $attr3$="*timestamp*"$\}$. Following ABE algorithm, we define access tree based on $attr$, generate public key PK and master public key MK at setup phase, construct secret key SK at key generation phase. Finally, all window-related pixels in each frame is encrypted by ABE algorithm and the other end e.g. cloud or security company server could decrypt it when it is required. Other pixels in each frame could also be encrypted by ABE but with other assigned private keys. Refer detailed ABE design and development in our previous research [6].

4.2 Preserve Privacy of Power Consumption Data via Adding Noise Disturbance

As previous research [9], we introduce instance-based additive noise to our solution when some users send the query f concerning with energy consumption in a community, a building or even a room: the user can obtain $f(x) + N(x)Z$ where Z denotes a randomly generated variable and $N(x)$ the scaling factor which is referred as noise magnitude. Due to space limit, we will not explain it in detail. Refer to [9] for details. In the following, we will assess privacy leakage regarding window-open & dataset.

4.3 Analyze Privacy I - Markov Chain

We assume that the state of an A/C, A_i, (where $A_i \in A = \{A_1, A_2, \dots, A_n\}$, n is the number of A/Cs in the building) is sampled when there is an turning on/off action. $A_i \in \{0,1\}$ where 0 denotes turning off and 1 turning on. Let array A_t^n denote the state of all A/C at time t. There are 2^n possible state of all A/Cs.

Assume there are m windows. The open/close of each window in the building is also monitored as $W_i \in \{0,1\}$ where 0 denotes closed and 1 opened. At the time instant t, the closed of all windows $\{W_1, W_2, \dots, W_m\}$ is denoted as an array P_t^m. There are 2^m possible states of the open/close of all m windows.

Thus, we model the joint probability distribution of the A/C states and the open state over x time instants:

$$P(A_t^n, W_t^m) = \prod_{t=1}^{x} P(A_t^n | A_{t-1}^n) P(W_t^m | A_t^n) \quad (2)$$

Based on (2), we can deduce a hidden Markov model for energy wasting behavior – open window with A/C turning on, which can be characterized by three parameters: (a) the initial presence, (b) a state distribution and (c) a conditional distributions. After defining the 3 inputs with concrete details, our hidden Markov model should assess the interrelated association between the pair (A, W) in which, array W with one elements being 0 and corresponding A/C in array A being 1 is when energy wasting is happening.

4.4 Analyze Privacy II - Differential Privacy

Let I_i denote all A/C state change data related with one smart home or even a community. Denote $I = \sum_i^n I_i$ which is the collected dataset related with n A/Cs $\{ I_1, I_2, \dots, I_n\}$. We demand the following holds

$$\Pr[A(I) = x] \leq e^{\in} \Pr[A(I') = x] \quad (3)$$

where Pr is a probability distribution over randomness of algorithm $A(I)$ where I is the input, I' is the addition or removing of one single A/C, and x is an any value output.

Let $\boldsymbol{Q} = \{Q_1, Q_2, \dots Q_n\}$be any query sequence, we demand the following holds:

$$|Q(I) - Q(I')|_p \ \leq \ \Delta_p(Q) \quad (4)$$

where $p \in \{1,2\}$, $Q(I)$ and $Q(I')$ are each vectors, $\Delta_1(Q)$ measures Manhattan distance $\sum_i |Q_i(I) - Q_i(I')|$ and $\Delta_2(Q)$ Euclidean distance $(\sqrt{\sum_i (Q_i(I) - Q_i(I'))^2})$.

5. DISCUSSION AND FUTURE WORKS

Our future works will focus on privacy preservation via perturbing distributed noisy information to time-series A/C state change data to minimize the privacy loss with lower utility-privacy tradeoff. In addition, how to extend hidden Markov chain method to precisely quantify privacy loss and corresponding counter-measures via differentially private protection will be studied. More importantly, how to design high performance experiences on real-world data will be addressed.

6. ACKNOWLEDGMENTS

This work was supported in part by NSF DGE-1303365 and NSF DUE-1431382 grants.

7. REFERENCES

[1] K. Ackerly, L. Baker and G. Brager. "Window use in mixed-mode buildings: a literature review". Summary Report. CBE, April 2011.

[2] D. Boneh, A. Sahai, and B. Waters. "Functional encryption: definitions and challenges".

[3] V. Fabi, R. V. Andersen, S. Corgnati, B. W. Olesen. "Occupants' window opening behaviour: a literature review of factors influencing occupant behaviour and models", Building and Environment, 58(2012), 188-198.

[4] W. F. Raaij and T. M.M. Verhallen. "Patterns of Residential energy behavior", *Journal of Economic Psychology*, vol 4, 85-106, 1983.

[5] Pan, Jianli, Raj Jain, and Subharthi Paul. "A Survey of Energy Efficiency in Buildings and Microgrids using Networking Technologies.", *IEEE Comm. Survey & Tutorials*, Vol. 16 No. 3, PP. 1709-1731, 2014.

[6] D. Li, Z. Ang, J. Williams, A. Sanchez, "P3: Privacy Preservation Protocol for Automatic Appliance Control Application in Smart Grid", Special Issue on Security for IoT: the State of the Art, *IEEE Internet of Things Journal (IoT-J),* Vol. 1(5), pp. 414-429, Oct. 2014.

[7] O. T. Masoso, L. J. Grobler. "The dark side of occupants' behaviour on building energy use". *Energy and Buildings*, 2009.

[8] T. A. Nguyen and M. Aiello. "Energy intelligent buildings based on user activity: A survey." *Energy and buildings* 56 (2013): 244-257.

[9] K. Nissim, S. Raskhodnikova, and A. Smith. "Smooth sensitivity and sampling in private data analysis", *STOC'07*. pp. 1-10, June, 2007.

[10] A. D. Paola, M. Ortolani, G. L. Re, G. Anastasi, S. K. Das, "Intelligent Management Systems for Energy Efficiency in Buildings: A Survey", *ACM Computing Surveys*, vol. 47(1), Article 13, pp. 1-38, May 2014.

[11] O. Seppanen and W. Fisk. "Association of ventilation system type with sick building symptoms in office workers". *Indoor Air*, 2001, pp. 98-112.