Privacy Preservation for Appliance Control Application

Depeng Li, Zeyar Aung, John Williams and Abel Sanchez

Technical Report DNA #2012-09

May 2012

Data & Network Analytics Research Group (DNA)
Computing and Information Science Program,
Masdar Institute of Science and Technology,
PO Box 54224, Abu Dhabi, UAE.

Privacy Preservation for Appliance Control Application

Depeng Li and Zeyar Aung
Masdar Institute Science and Technology
Abu Dhabi, UAE,
{dli, zaung}@masdar.ac.ae

John Williams and Abel Sanchez
Massachusetts Institute of Technology (MIT)
Cambridge, Massachusetts, USA
{jrw, doval}@mit.edu

***Abstract*—To address recently emerging concerns on privacy violations, this paper investigates possible sensitive information leakages in the appliance control, which is one of the handiest and most visible applications in smart grids. Without a consistent privacy preservation mechanism, the appliance control system can capture, model and divulge customers' behavior, activities, and personal information at almost every level of society. We investigated a privacy threat model for appliance control application and further design and implement a protection protocol. Experiment results demonstrate that our protocol merely incurs a substantially light overhead on the appliance control application, but is able to address and solve the formidable challenges both customers and utility companies are facing.**

Keywords-Data Privacy, Privacy Preservation, Smart Grid;

I. INTRODUCTION

Smart grids, or the intelligent electricity grid have the potential to shave the power consumption peak, to optimize energy loss, to reduce customers' power bills, and to provide better power recovery capabilities. However, the digitized move to replace dumb meters with smart meters implies an intrinsic link between electricity customers and ambient smart devices. High-resolution smart data such as power consumptions, control commands, events, alarms and bills are generated and archived in smart grids. These data vividly demonstrate every customer's daily activities, individual behavior models and Personally Identifiable Information (PII) [23], [6]. The data's potential usability could potentially go beyond the original purposes for which they are collected and stored.

The privacy violation in smart grids is a pressing challenge today and increasingly affects all of us as the smart data can be misused to infer personal matters. Some pioneer studies, e.g., [24], explore means to monitor major appliances in a dwelling by examining the power usage data collected every 15 minutes. However, there has been little discussion of appliance control which can also leak customers' privacy. Example data includes commands to turn on/off an air conditioner or adjust its thermostat settings sent from the control center. Direct access to detailed, individualized appliance control command data can easily infer customers' activity patterns such as occupancies of their residences. Some uses of data maybe still unknown nowadays, however critical decades later hence. Consequently, privacy-protecting technologies are highly requested.

This paper takes the first step in exploring the privacy preservation for appliance control applications by investigating benefits from cryptographic primitives.

Contributions:

- As the best of our knowledge, this paper is the first to observe privacy leakages for the appliance control application. Furthermore, we are the first to practically discuss corresponding privacy threat and attacks.
- We propose the fine-grained privacy-preserving protocol (P3) through the usage of Attribute-Based Encryption (ABE) system.
- We are the first to design and develop a practical appliance control system with the support of P3 in which we illustrate diverse interaction means to control appliance in smart grids, and demonstrate how privacy is protected.

II. APPLIANCE CONTROL IN SMART GRIDS

A. Appliance Control Examples

1) Remote appliance control

Some utility companies provide remote appliance control service in such a way that the customers can control their own home appliance through smart grids. They, for instance can turn their air conditioner on or off or set its thermostat remotely. One example is such that, before leaving offices, a working person can turn on air conditioners in his home. Then, his residence can be chilled when the person is commuting to home. After arriving at home, the person can relish the joyful temperature. Another example is that some customers may forget to turn off the high-level power consumption appliances e.g. swimming pool pumper, air conditioner, etc. when leaving home. Customers are enabled to turn off these appliances remotely for saving.

2) Autonomous demand-response from loads

To alter the power consumption, the automatic response controllers can turn it on or off or change its settings for appliance utilizing in dwellings [17]. Examples include dish washers, air conditioners, etc. To save power consumptions, the designed algorithm can automatically turn off the dish washers at peak time or turn off the air conditioners when the residence is empty.

B. Appliance Control Model

In smart grids, multicast is extensively deployed in the smart grid because of its scalability, its efficiency and its functionality across network segments. Appliance control applications also take advantage of it for sake of efficiency.

In this paper, we let S demonstrate n smart meters, M a multicast message, C an n-dimensional vector of appliance control commands and $ATTR$ the attributes corresponding to commands in a given regular time interval, T, in a given electricity area.

$$S = \{s_i\} \quad where\ |S| = n; i \in [1, n]; s_i: smart\ meter \quad (1)$$

$$M = \{C_i\} \quad where\ |M| = m; i \in [1, m] \quad (2)$$

$$C = \{ATTR; \quad A; \quad C; \quad P; \quad t\} \quad (3)$$

$$where\ A: Appliance; \qquad C: command;$$

$$P: parameters; \qquad t: time\ to\ execute$$

$$ATTR = \{attr_x\} \qquad where\ |ATTR| = n; x \in [1, n] \quad (4)$$

We assume that some residences have smart meters s_i installed at their homes. Note that in our implemented application, attributes represent residential addresses or a set of residential addresses which are used to identify one or a set of smart meters. For example, we used the following attribute in our applications: $attr_1$= "*street number*"; $attr_2$ = "*street name*"; $attr_3$ = "*ZIP value*"; $attr_4$ = "*city name*". Therefore, when a command C contained in a message M is associated with all four attributes, the command multicasts. Only smart meters matching with four attributes accept and execute it. When there are three attributes (excluding $attr_1$ = "*street number*"), the command can only be executed by smart meters in the specific street.

C. Privacy Threat and Attack Model

In this paper, a privacy threat [25], [28], [18] occurs when an adversary can associate an appliance control command data with personal information e.g. customers' private information, activity models, preferences, etc.

Privacy for residence occupancy: An appliance control command $\{C\}$ can let an adversary infer that the resident is presence or absence (also referred as *absence privacy*).

Example I: Alice sends a remote control command to $address\ A$ aiming to shut down the air conditioner when the local temperature outdoor is high (e.g. 104°F/40°C). Eve can probably infer that residence with $address\ A$ may possible be empty and then he can take the chance to break in.

Privacy for appliance ownership: The history of appliance control commands $\{\dots C_i \dots\}$ let an adversary surmise whether the residence has a specific appliance installed.

Example II: Alice had sent home the remote appliance control commands associated with heaters, dish washers and dryers but otherwise air conditioners. Eve extrapolates that it is highly possible for Alice to not own an air conditioner yet. The commercial information is valuable.

Privacy for personal activities model: The appliance control commands can let the adversary generalize the residence's activity model.

Example III: Alice always remotely turns on his air conditioner half an hour earlier before arriving at home. Eve finds that theses control commands are sent out at 5:30pm from every Tuesday to Thursday but, 6:30pm every Monday. Eve can draw Alice's life pattern in the future based on it.

III. Protocol, Architecture and Applications

In this section, we first inestigate the adversary model and security assumption. Depending on them, means of comprehensive privacy protection is proposed, including a system model to integrate ABE with smart grid devices, a protocol to shield sensitive appliance control messages and a designed appliance control system as a practical sample.

A. Adversary Model and Security Assumption

Adversary Model: like other researches in areas of privacy preservation [8], [12], [13], [26], we follow the semi-honest adversary model in which smart devices (e.g. smart meters, etc.) obey our mechanism but meanwhile they are also curious about messages they learn (or share) and have the intension to combine these information if possible. Therefore, any participating smart devices should relay unicast or multicast packets and also intend to uncover others' privacy by studying sensitive messages received.

Security Assumption: we assume that smart devices such as smart meters, etc. are tamper-resistant, and have sensors deployed against malicious activities launched by hackers, business spies, electricity thieves, etc. Furthermore, we also assume the availability of the trusted certification authority deployed in the utility control center to issue / revoke / renew valid certifications [21]. Moreover, we assume that device attestation approaches are deployed to validate smart meters, etc. Hence, it is impossible to deploy, install or download any malicious software on smart devices. At last, the protocol proposed in this research mainly focus on the confidentiality service to protect the privacy. The authentication and integrity services guaranteed by digital signatures and one-way hash functions are also important but beyond its scope.

B. System Model

We demonstrate the basic system model and integrated cryptography primitives in P3 system. The P3 system has three participants: smart meters installed in the customer residences as well as control servers and trusted Key Distribution Center (KDC) deployed in utility control centers. The responsibility for KDC is to issue private and public key pairs to control servers and smart meters. That of the control server is to encrypt appliance control commands and multicast the ciphertext to smart meters. That of the smart meters is to decrypt received ciphertext if its attributes match with that of the ciphertext.

To protect multicast communication which sends crucial appliance control commands from the control server to multiple smart meters in P3 system, we adopts an ABE encryption system [9], [3], [27] (refer to Appendix B for details) rather than group key schemes e.g. [13] as group key schemes leak messages to inside group members. In P3, it is crucial that the control server can efficiently encrypt the commands by a policy written over attributes to accomplish

specific appliance control tasks. Smart meters can decrypt ciphertext in an efficient manner if its private key reflects the set of attributes which exactly satisfy the policy specified by the ciphertext.

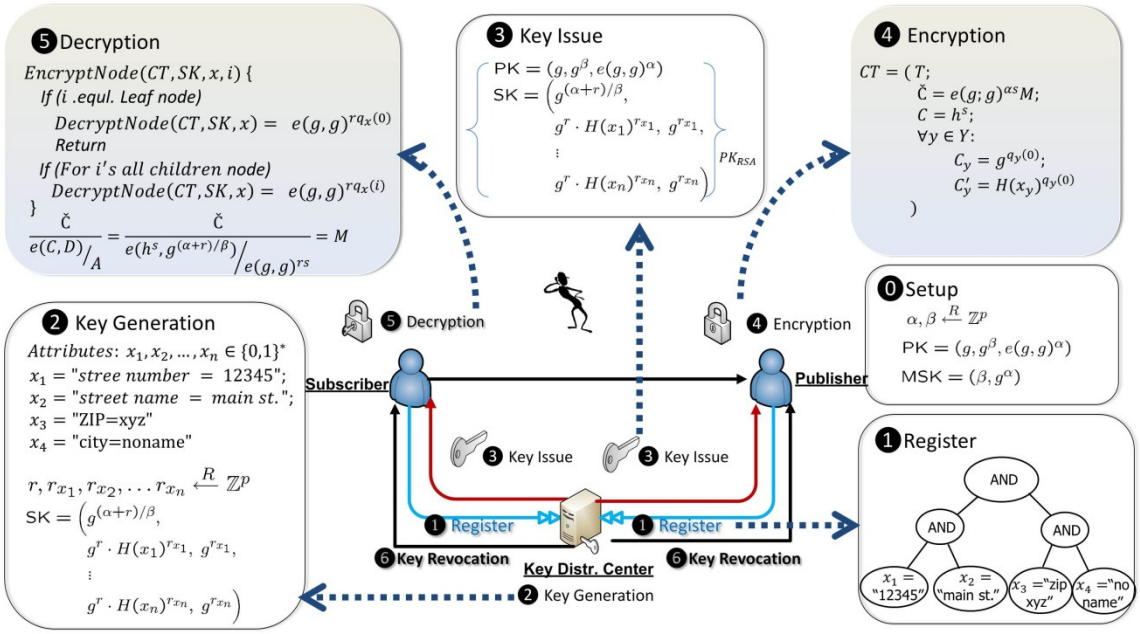

Figure 2. System Model

A detailed view about how P3 adopts the ABE encryption cryptography system is illustrated in Figure 2: at setup ⓪ phase, ABE Public Key (PK) and ABE Master Secret Key (MK) are generated by the trusted Key Distribution Center (KDC) deployed in the utility control center. The next step for every participant (e.g. smart meters, control servers) is to register ① with detailed attribute sets. For example, a smart meter is requested to provide detailed attributes: {*street_number: 12345; street name: main street; ZIP: xyz; city: noname*}. After that, following the successful authorization, the corresponding ABE Secret Key (SK) will be generated ②. Thereafter, SK is issued ③ to a smart meters in a secure channel (e.g. encrypted by the smart device's RSA public key or physical touch) labeled with the specific set of attributes. The control server receives all ABE public key (PK) corresponding to SKs issued to all smart meters. Then, plaintext can be encrypted ④ by the control server with ABE public keys (PK) representing attributes for every entry inside the appliance control command list. The resulted ciphertext is multicast to smart meters in this area. After receiving ciphertext reflecting the attribute set matching their attributes, smart devices can decrypt ⑤ the ciphertext. In case that smart devices are compromised, failed, or their certificates are expired, their secret key ASK_{device}^{att1} should be revoked ⑥.

C. Protocol

The essential goal of P3 is to realize an efficient privacy preservation mechanism satisfying time-critical and scalability requirements of the smart grid without any privacy exposures. P3 system will realize a privacy preservation system aiming to conceal sensitive data occurred in appliance control applications via integrating the ABE encryption system and in conformance with regulations of the smart grid.

Before the P3 is executed, the prepare operation should be accomplished: KDC processes $ABEKeySetUp$, $ABEKeyReg$ and $ABEKeyGen$ to setup the public key and master keys, register attributes and calculate public and private key pairs for all participates, the control server and smart meters. All private keys and public keys are issued to corresponding nodes. Hence, our P3 is illuminated in Fig. 3: the control server multicast participating smart meters the appliance control command lists, M. Each command entry should be encrypted by ABE algorithm via public key PK reflecting the attributes $ATTR_i$ associated with this command entry. Smart meters participating the multicast service decrypts the first block of ciphertext it received. If decryption operations success and the attributes inside the command entry matches with that of the smart meter, the smart meter executes the command. Otherwise, the smart meter just ignores the ciphertext. Thereafter, if results or statuses are requested by the appliance control command, e.g. the air conditioner status, the smart meter is responsible to send feedback to the control server to notice that the operation is accomplished successfully. The smart meter could use the control server's public key to encrypt the feedback and send the ciphertext to the control server. The control server could decrypt it by using its own private key. It is the verse vice of the command list delivery operation. Therefore, we do not explain it in detail for the sake of space limit.

As a security protocol, messages M transmitted in P3 requires not only confidentiality but authentication and

integrity services. They can be supported by digital signature technology and one-way hash function [29].

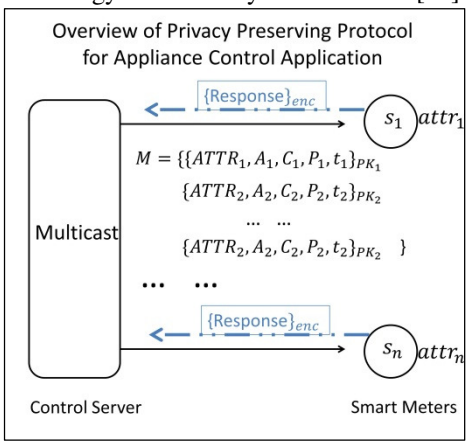

Figure 3. Overview of Privacy Preserving Protocol

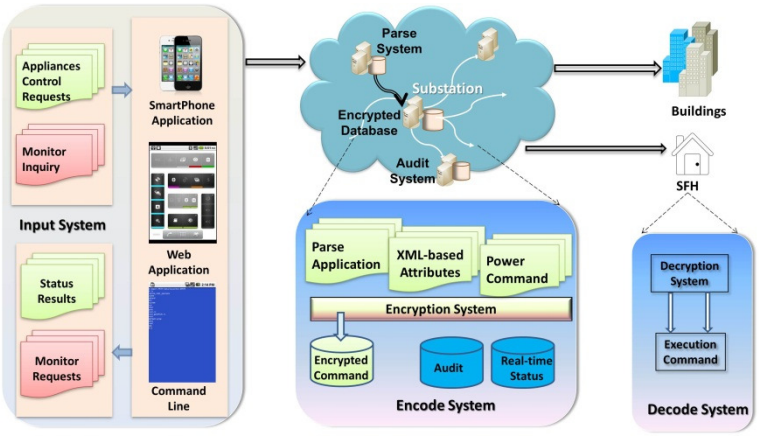

Figure 4. System Architecture of Appliance Control Application

D. System Architecture of Appliance Control Application

In this subsection, we design and develop an appliance control system with privacy preserving service by utilizing P3 as the cornerstone. It is not only a practical application deployed in the smart grids but a concrete example demonstrating our P3's feasibility. The rest will focus on its two fundamental subsystem, (i) input system, (ii) encode and decode subsystem, as illustrated in Fig. 4.

1) Input subsystem:

Requests to control appliances in smart grid systems are generated and managed by the input system. There are two sets of input sources: 1) manual. Part of requests can be released by authorized electricity customers or power dispatchers via smart phones, web services, command line applications, etc. An electricity customer could send messages via smartphone applications to accomplish services e.g. turning off high-load appliances at his/her home for a time window. 2) automatic. The vast majority of requests are executed by the smart grid' components inside. Demand response services, for example, multicast control commands to execute the appliance control tasks or inquire appliances' statuses. Notice that the smart phone used in this application is only for command input purpose. Its security is outside the scope of this paper.

2) Encode and Decode subsystems:

In the Encode subsystem, requests inputted manually or automatically will be processed through three steps listed below, one by another, to achieve the encode/decode functionality: 1) parse process; 2) XML-based transfer process; 3) encryption process.

Parse process: the parse process is hosted by the substation to repeatedly poll activated requests and dedicate to understanding the goal of each request sent from different sources. Although accomplishing the same task, various applications demonstrate different formats. For example, to achieve the turning-off function for appliances, smart phone applications send out messages like

$*\ \mathbf{100}\ *\ \mathbf{12345}\ \boldsymbol{Main\ Street\ ZIP\ XYZ, Noname\ city}.*\ 3\ *\ 2$

Here, "**100**" means appliances service, "**123 *Rd.***" etc. stands for the address, "**3**" means air condition and "**2**" represents the shutdown command. In contrast, web service may ask the customer filling out a form indicating parameters aforementioned. No matter how many formats or sources deployed in the input system, they all need to be parsed into a standardized format in such a way that the smart grid can understand e.g. a set of attributes which is represented with XML-based language. Both command payload and XML-based attributes will be combined together for encryption purpose.

Meanwhile, the control center should also validate the authentication for the request via the credentials or token or smart cards. It is not in the scope of this paper.

Encoding and decoding subsystems: in our system deploying P3, the raw command data will not be forwarded and received directly. It mediates the interaction between the publisher and subscriber ends in which encoding and decoding subsystems are installed, respectively. All raw data will be encoded by encoding subsystem to prevent privacy leakage. The decoding subsystem can decode the multicast ciphertext if its private key reflects the same set of attributes defined by the received ciphertext.

Hence, P3 system makes the change: any outgoing data from the control server should be associated with a set of attributes which are decided by the data's purpose. Then, the encoding system encrypts both the raw multicast messages and the attributes by the key associated with the attributes. After receiving the incoming ciphertext, the decoding system unveils it if its private key reflects the bounded attributes.

One particular feature about our Encode / Decode system is that it does not assume that any server storing the input messages are secure. Any server, even inside the substations could possibly be compromised. In our system, appliance control data are encrypted by the ABE encryption algorithm prior stored in the system. Therefore, except the operator or the automatic control system algorithm, the privacy cannot be disclosed to anyone even they can access the file system since the data are already encrypted. Then,

the ciphertext can either be put in the queue waiting for the multicast component's process or stored in the log file on the server for late retrieval. Furthermore, some data will be delivered later, as scheduled rather than in real-time.

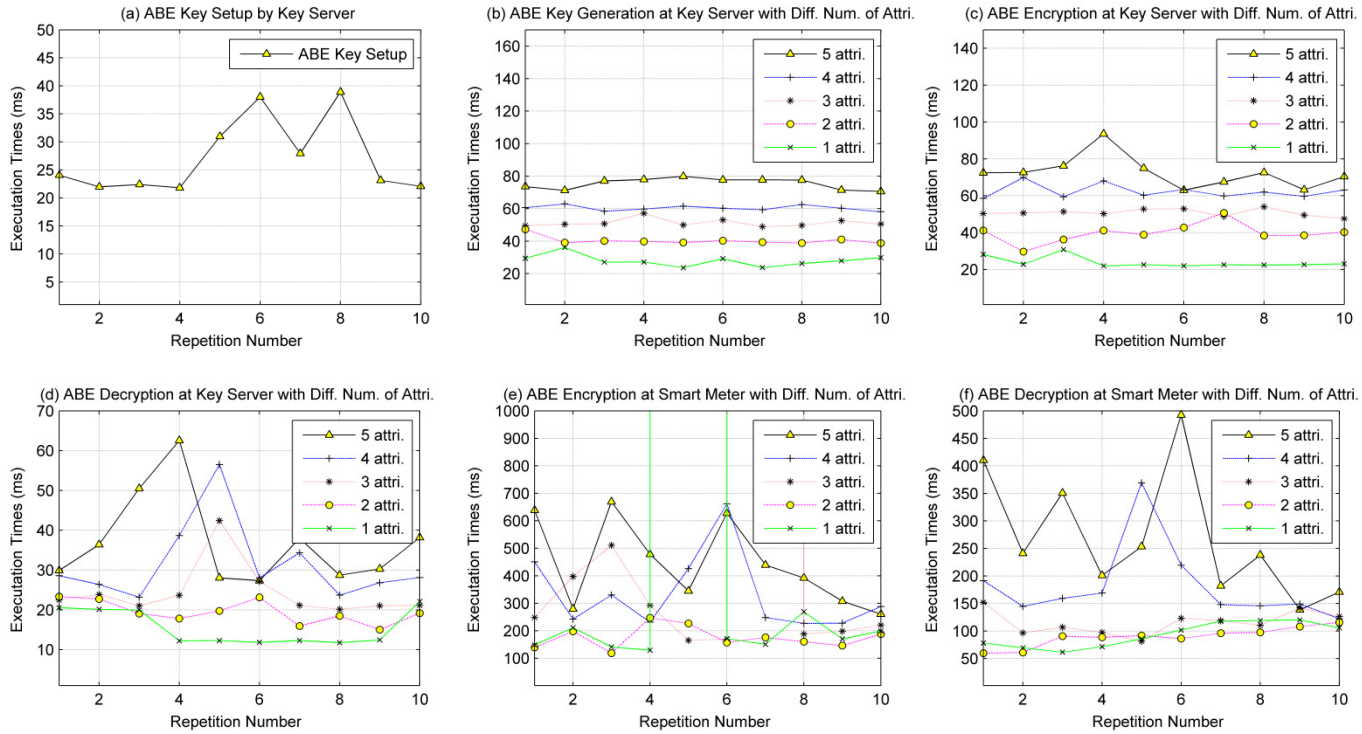

Figure 5. Performance Test Result for Key Generation, Encryption and Decryption. MNT elliptic curve of embedding degree 6 with order 160 bits length and base field order 512 bits length were utilized in P3. We collected executions of ABE operations including key setup, key generation, encryption, and decryption on a key server as well as encryption and decryption at a smart meter for ten times (randomly selected number). The numbers of attribute were ranging from 1 to 5 (randomly selected number) for key generation, encryption, and decryption. The key server and smart meter were both virtual machines hosted by Oracle's VirtualBox installing Ubuntu 11.10. The detailed configuration of the key server was - Memory: 496MB; CPU 2.67GHz; Disk 7.9 GB. That of the smart meter was -- Memory: 64MB; CPU 333MHz, the same configuration of an ARM Cortex 926EJS processor powered for a real smart meter.

IV. Performance Evaluation

The running times of the *Command Input on Console* component, *Command Input on Smart Phone* component, *Request* component and *Parse* component in P3 are trivial. We will not further discuss the performance of them due to the limit of space. The dominating part of P3's running time is occupied by the *Publisher Encryption System* and *Subscriber Decryption System* component, both of which are embedded into the client and the server ends respectively in a smart device e.g. smart meter, IED, etc. In this subsection, our emphasis focuses on their efficiency via validating their acceptable performance based on smart grid' regulation or guide.

ABE encryption and decryption algorithms are the core of the *Publisher Encryption System* and *Subscriber Decryption System* components, respectively. We implement them based on Pairing-Based Cryptography (PBC) library [19] built on the GNU Multiple Precision arithmetic (GMP) library [1]: GMP library provides arbitrary precision arithmetic APIs which are invoked by PBC to support pairing-based cryptosystem.

In our application, we use the pairing-friendly elliptic curves $E(\mathbb{F}_{2^{379}}): y^2 + y = x^3 + x + 1$ and $E(\mathbb{F}_p): y^2 = x^3 + Ax + B$ with a 512-bit prime. Furthermore, to satisfy the performance requirement, we deploys MNT elliptic curve to implement the ABE system.

In Figure 5, we demonstrate that the *ABEKeySetUp, ABEKeyGen, ABEEncrypt,* and *ABEDecrypt* functions' performance for a key server and a smart meter. Regarding the running times, we notice that so far P3 system can satisfy delay-tolerance communication which can be tolerant for delays ranging from seconds to hours [22]. However, near real-time messages (e.g. power control commands in smart grid that demands less than 4ms delay [22]) cannot be protected in this paper. As the best of our knowledges, the appliance control command can be tolerant to a few minutes. Therefore, our solution's performance is acceptable.

V. Related Works

Main privacy preservations approaches in smart grids include *battery* [10], [11], [20], *ID anonymization* [7], *disturbance* [15] and *cryptographic primitives* [8], [12], [13], [26] are reviewed.

Battery: through the use of a rechargeable battery, privacy protections are presented: G. Kalogridis *et al.* [11] utilize the electric power routing to run partial power consumption demands off a battery rather than off the power grid directly. G. Kalogridis *et al.* [10] proposed the *ElecPrivacy* system to detect ongoing or upcoming privacy threats, reconfigure the power routing and eventually mask load signature for appliances. S. McLaughlin *et al.* [20]

propose the Non-Intrusive Load Leveling (NILL), a new class of algorithms to mask the appliance's power usage signature. However, there is still a small number of event disclosure and a rechargeable battery demands extra cost (around $1,000 [20]), installment expense and unpredictable maintenance fees. Furthermore, smart appliances such as dryers, clothes washers, etc. can directly communicate with utility operators. Hence, installing one rechargeable battery cannot mask all appliances' load signatures.

Cryptographic Techniques: F. Li *et al.* [13] focus on smart metering data aggregation protection in which, all messages are encrypted via homomorphic encryption algorithm. F. D. Garcia and B. Jacobs [8] proposed a privacy-friendly protocol by using homomorphic (Paillier) encryption and additive secret sharing. A. Rial and G. Danezis [26] use zero knowledge proofs and commitments to preserve smart meters' privacy. In [12], K. Kursawe, *et al.* proposed four different protocols based on Diffie-Hellman Key-exchange, etc. to protect data aggregation privacy. However, no solutions are provided against appliance control privacy leakage.

Anonymity: C. Efthymiou and G. Kalogridis [7] proposed a trusted key escrow service to anonymize frequent readings with pseudonymmous IDs rather than unique identifiers along with randomized time intervals. Nevertheless, anonymity approaches masking customers' identity cannot preserve customers' behavior once the escrow service is compromised.

Disturbance: H. Li *et al.* [15] proposed a compressed meter reading approach that enhances its privacy through the use of random sequence. But its Access Points (AP) is assumed never to be compromised.

CONCLUSIONS AND FUTURE WORKS

Appliance control applications are convenient services in smart grids. However, the inferred privacy leakage also raises customers' concerns. Appliance control commands are easily be mined to expose customers' privacy such as absence, appliance ownership, daily activity models, etc. We propose a privacy preserving protocol to protect the customers' sensitive information through the use of ABE encryption system. Our experiment results show that its performance is acceptable.

Meanwhile, revoking of invalidate keys for ABE system is a critical component for P3. How to minimize its vulnerable window is the goal for our future research. Moreover, we are going to unravel some pairing-friendly elliptic curves demonstrating the faster decryption process as most subscribers e.g. smart meters in are low-end.

REFERENCES

[1] http://gmplib.org/

[2] P. Barreto, B. Lynn, and M. Scott, Efficient implementations for Pairing-based Cryptography. *Journal of Cryptology,* 17, pp.321-334, 2004.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[4] D. Boneh, B. Lynn, and H. Shacham. Short Signatures from the Weil pairing, *Journal of Cryptology*, 17, pp. 297-319, 2004.

[5] D. Boneh and M. Franklin. Identity-based encryption from Weil pairing. In *Proc. of Crypto 2001,* LNCS vol. 2139, pp. 213-229, 2001.

[6] H. S. Cho, T. Yamazaki, and M. Hahn. AERO: Extraction of user's activities from electric power consumption data. *IEEE Transactions on Consumer Electronics*, 56, pp. 2011-2018, 2010.

[7] C. Efthymiou and G. Kalogridis. Smart Grid Privacy via anonymization of smart metering data. In *IEEE (SmartGridComm'10)*, pp. 238-243, 2010.

[8] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. *Security and Trust Management,* LNCS vol. 6710, pp. 226-238, 2011.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *13th ACM CCS'06.*

[10] G. Kalogridis, R. Cepeda, T. Lewis, S. Denic, and C. Efthymiou. ElecPrivacy: Evaluating the Privacy Protection of Electricity Management Algorithms. *IEEE Transactions on Smart Grid: Special Issue on Cyber, Physical, and System Security for Smart Grids*, 2011.

[11] G. Kalogridis, C. Efthymiou, S.Z. Denic, T. A. Lewis and R. Cepeda. Privacy for smart meters: towards undetectable appliance load signatures. In *Proc. of the 1st IEEE SmartGridComm'10*, pp. 232-237.

[12] K. Kursawe, G. Danezis, M. Kohlweiss. Privacy-friendly aggregation for the smart-grid. In *Privacy Enhancing Technologies*, 2011.

[13] D. Li and S. Sampalli, "A hybrid group key management protocol for reliable and authenticated rekeying," *International Journal of Network Security*, vol. 6, no. 3, pp. 270-281, 2008.

[14] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. In *SmartGridComm'10*, pp. 327-332.

[15] H. Li, R. Mao, L. Lai, and R. C. Qiu. Compressed meter reading for delay-sensitive and secure load report in smart grid. In *SmartGridComm'10*, pp. 114-119.

[16] Q. Li and G. Cao. Multicast Authentication in the Smart Grid with One-Time Signature. *IEEE Transactions on Smart Grid*, 2, pp. 686-696, 2011.

[17] S. Lu, N. Samaan, R. Diao, M. Elizondo, C. Jin, E. Mayhorn, Y. Zhang, H. Kirkham, Centralized and decentralized control for demand response. Pp. 1-8, *ISGT 2011*.

[18] M. A. Lisovich and S. B. Wicker. Privacy concerns in upcoming residential and commercial demand-response systems. *IEEE Proceedings on Power Systems*, 1, pp. 1-8, March 2008.

[19] B. Lynn. The Stanford Pairing Based Crypto Library. http://crypto.stanford.edu/pbc/

[20] S. McLaughlin, P. McDaniel and W. Aiello. Protecting consumer privacy from electric load monitoring. In *Proc. of the 18th ACM CCS'11,* 2011.

[21] A. R. Metke and R. L. Ekl. Security Technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1, pp. 99-107, 2010.

[22] NIST, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NISTIR 7628. August, 2010.

[23] NIST, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, NISTIR 7628. August, 2010.

[24] E. L. Quinn. Privacy and the new energy infrastructure. Social Science Research Network (SSRN). Feb. 2009. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1370731

[25] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, Smart meter privacy: A utility-privacy framework, *In IEEE SmartGridComm'11*, 2011.

[26] A. Rial and G. Danezis. Privacy-preserving smart metering. In *Proc. of ACM CCS WPES'11*, 2011.

[27] A. Sahai and B. Waters. Fuzzy identity based encryption. *In Advances in Cryptology – Eurocrypt*, LNCS vol. 3494, pp. 457-473. 2005.

[28] L. Sankar, S. Kar, R. Tandon, and H. V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. In *SmartGridComm'11*.

[29] Q. Wang, H. Khurana, Y. Huang; K. Nahrstedt,Time Valid One-Time Signature for Time-Critical Multicast Data Authentication, *IEEE INFOCOM 2009*, pp. 1233 - 1241

APPENDIX

A. Bilinear map

Bilinear map [2], [4], [5] works as the basis of our approach. $\mathbb{G}$ and $\mathbb{G}_{\mathbb{T}}$ are a cyclic additive group and a cyclic multiplication group generated by P with the same order q, respectively. A mapping $\hat{e}: \mathbb{G} \times \mathbb{G} \longrightarrow \mathbb{G}_{\mathbb{T}}$ satisfies the following properties:

- **Bilinear:** for all $u, v \in \mathbb{G}; a, b \in \mathbb{Z}$, we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$, where = is an equation;
- **Computable**: there exists an efficient computable algorithm to compute $\hat{e}(u, v), \forall u, v \in \mathbb{G}$;
- **Non-degenerate**: for the generator g of $\mathbb{G}$, p is the order of $\mathbb{G}$, we have $\hat{e}(g, g) \neq 1 \in \mathbb{G}_{\mathbb{T}}$;

B. Attribute-based encryption (ABE) [9], [3], [27]

Access Tree – an access structure is represented by the tree in which a leaf node is associated with a specific attribute and an intermediate node works as a "AND" or "OR" gate. We say that a set of attributes γ satisfies access tree if the root nodes' gate is true via recursively calculating roots' children nodes.

Setup()→ (PK, MK);
/* *public key PK; master secret key MK; */*

- Randomly selects two credentials $\alpha, \beta \overset{R}{\leftarrow} \mathbb{Z}_p$;
- Calculates

$$PK = \left\{ \mathbb{G}_0;\ \ g;\ \ h = g^{\beta};\ \ f = g^{1/\beta};\ \ e(g,g)^{\alpha} \right\};$$
$$MK = (\beta,\ g^{\alpha});$$

Key Generation $(MK, S) \rightarrow SK$
/* MK master key; a set of attributes S; Secret key SK */

- Generate a random $r \overset{R}{\leftarrow} \mathbb{Z}_p$.

For each attribute $j \in S$,

- Choose corresponding random $r_j \overset{R}{\leftarrow} \mathbb{Z}_p$
- Calculate

$$SK = \{\ D = g^{\frac{\alpha + r}{\beta}};\ \{\ \forall j \in S: D_j = g^r \times H(j)^{r_j};\quad D_j' = g^{r_j}\};$$

- For all $i \in \mathcal{T}$ the private keys components are:

$$D_i = g^{q(i)} T(i)^{r_i},$$
$$d_i = g^{r_i},$$
$$where\quad T(i) = g^{x^i} \prod_{j=1}^{n+1} t_j^{\Delta_{j,N}(i)}$$

Encrypt $(PK, M, T) \rightarrow\ CT$
/ public key PK; message M ; tree access structure $\mathcal{T}$ Ciphertext CT*/*

- For each node x in the tree $\mathcal{T}$, select a corresponding polynomial q_x; then assign its degree: $d_x = k_x + 1$ where d_x is the degree of polynomial q_x and k_x is the threshold value of a node x.
- Beginning at the root node R, first assigns $q_R(0) = s$ where $s \in \mathbb{Z}_p$ is a random. Second, randomly selects d_R other points for q_R to complement the definition of the polynomial q_R.
- Process the rest nodes x on the tree T by following the top-down manner: sets $q_x(0) = q_{parent(x)}(index(x))$ where function $parent(x)$ returns node x's parent node and function $index(x)$ returns the ordering number of node x's sibling nodes. Ordering numbers are assigned by x's parent node. Then, randomly selects d_x other points for q_x to complement the definition of the polynomial q_x.
- Ciphertext is output as:

$$CT = \{\ \mathcal{T};\ \ \tilde{C} = Me(g;g)^{\alpha s};\quad C = h^s;$$
$$\{\ \forall y \in Y:\ C_y = g^{q_y(0)}; C_y' = H(\boldsymbol{att}(y)^{q_y(0)})\ ;$$
$$\};$$
$$\}$$

where function $\boldsymbol{att}(\boldsymbol{x})$ returns attributes associated with the leaf node;
$H: \{0,1\}^* \rightarrow \mathbb{Z}_p$ is a collision-resistant hash function;

Decrypt (PK, CT, SK) → M
/ Public Key PK: Ciphertext CT ; Private key SK; */*

The $DecryptNode(CT, SK, x)$ function below will be invoked recursively starting at root node R to verify if the access tree T can be satisfied by S:

- If the node x is a leaf node, set $i = \boldsymbol{att}(x)$;

If $i \notin S$,
$DecryptNode(CT, SK, x) = \perp$
If $i \in S$,
$DecryptNode(CT, SK, x)$

$$= \frac{e(D_i, C_x)}{e(D_i', C_x')} = \frac{e\left(g^r \cdot H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= \frac{e\left(g^r, g^{q_x(0)}\right) \cdot e\left(H(i)^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$
$$= e(g,g)^{r q_x(0)}$$

- If the node x is not a leaf node,

For all nodes z which are node x's children nodes, call function $F_z = DecryptNode(CT, SK, z)$. Assign S_x with an arbitrary k_x −sized set of child nodes in such a way that $F_z \neq \perp$. If we cannot find such set, it means that the node cannot be satisfied, and the function returns $\perp$.

Otherwise, calculate:

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S'_x(0)}} = \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_z(0)}\right)^{\Delta_{i,S'_x(0)}}$$
$$= \prod_{z \in S_x} \left(e(g,g)^{r \cdot q_{parent(z)(index(x))}}\right)^{\Delta_{i,S'_x(0)}}$$
$$= \prod_{z \in S_x} \left(e(g,g)\right)^{r \cdot q_x(i) \cdot \Delta_{i,S'_x(0)}} = e(g,g)^{r \cdot q_x(i)}$$

where $i = index(z)$ and $S'_x = \{index(z) : z \in S_x\}$

- Decrypt ciphertext

$$\frac{\check{C}}{e(C,D)/A} = \frac{\check{C}}{e(h^s, g^{(\alpha+r)/\beta})/e(g,g)^{rs}} = M$$