Towards Secure Targeted Broadcast in Smart Grid

Zubair Md. Fadlullah, *Member, IEEE,* Nei Kato, *Senior Member, IEEE,* Rongxing Lu, *Member, IEEE,* Xuemin (Sherman) Shen, *Fellow, IEEE,* and Yousuke Nozaki, *Member, IEEE.*

***Abstract*—Significant research efforts have recently been directed towards materializing smart grid for the purpose of transforming the aging power grid into an efficient and intelligent electric power distribution system. Conceptually, smart grid can be regarded as a fusion of different advanced technologies, i.e., electrical power engineering meets sensing, control, digital communication, and network information technologies. However, when these advanced technologies converge at smart grid, we will face many new unforeseen challenges, particularly security challenges in smart grid communications. In this article, towards secure targeted broadcast in smart grid, we investigate the applicability of Attribute Based Encryption (ABE) for smart grid communication scenarios. In particular, we focus on the application of Key Policy ABE (KP-ABE), where a smart grid's control center can use KP-ABE to broadcast a single encrypted message to a specific group of users, and each user in the targeted group can individually use the defined key policy to decrypt the message. With this kind of KP-ABE targeted broadcast, it is possible to eliminate the need for issuing multiple unicast messages. As a result, both communication and computation efficiency can be ensured.**

***Index Terms*—Smart Grid, Security, Targeted Broadcast, Attribute Based Encryption (ABE).**

I. Introduction

In order to allow intelligent power control and monitoring, the concept of smart grid has been gaining tremendous attention amongst both researchers and utility providers recently. Specifically, in smart grid, advanced technologies, i.e., sensing, control, digital communication, and network information, as shown in Fig. 1, are merged with power system engineering to effectively address numerous critical issues that limit existing electricity grids, such as the lack of adequate demand response, scalability, energy conservation, reduction of carbon emission, and control of distribution. Smart grid is perceived to transform the energy industry by allowing bi-directional communication between the consumers and the energy producers and/or operators. The necessary devices required for facilitating this two-way communication consist of smart meters [1]–[3]. Smart meters, along with power instrumentation and monitoring sensors, form the core of Advanced Metering Infrastructure (AMI) with aim at maintaining high levels of performance, reliability, and manageability. Nevertheless, researchers have expressed their deep concern for the need for integrating a security infrastructure with the smart grid's AMI [4], [5]. The reason behind this concern is the fact that many smart grid projects are widely using advanced communications networks to link numerous sensors and smart meters for connecting consumers with the utility providers so as to exchange information bi-directionally. However, as evident from the wide variety of malicious threats against existing communication networks such as the Internet, the smart grid communication framework is expected to increase the vulnerability of the grid to cyber attacks [1], [2] such as denial of service attacks, spoofing, privacy leakage, and so forth. As a result, the development of a wide range of communication networks for supporting the integration of open-access energy competition through AMI should set out adequate security provisions for protecting the smart grid communication.

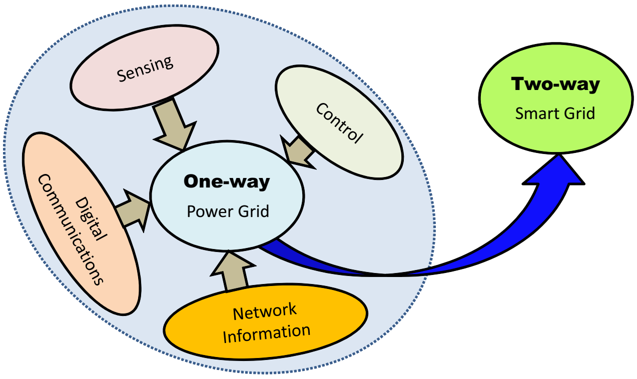

Fig. 1. The transformation of the traditional one-way-communication power grid to two-way-communication smart grid.

From a conventional view point, smart grid security hinges upon authentication, authorization, access control, and encryption technologies. These technologies can facilitate basic security provisioning requirements in smart grid by securing the information on single customer data, incentive plans, and other confidential information. However, in terms of the smart grid's characteristics, the control center in smart grid may also disseminate some sensitive information to a specific group of users, and these sensitive information should be transmitted securely (e.g., through encryption amongst authorized and authenticated provider and customers). If the control center sends the information to each user individually (i.e., in a unicast manner), the communication cost will, indeed, be significantly high. Even worsely, this issue becomes more complex when the control center produces different types of services for different groups of users. Therefore, how to securely and efficiently disseminate sensitive information to the targeted customers or end-user groups is a challenging issue in smart grid communication. Intuitively, to deal with this issue, traditional broadcast encryption techniques may be

Z. M. Fadlullah and N. Kato are with the Graduate School of Information Sciences, Tohoku University, Sendai, Japan. Emails: {zubair, kato}@it.ecei.tohoku.ac.jp

R. Lu and X. Shen are with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada. Emails: {rxlu, xshen}@bbcr.uwaterloo.ca

Y. Nozaki is with NTT Energy and Environment Systems Laboratories, Tokyo, Japan. Email: nozaki.yousuke@lab.ntt.co.jp

utilized, where the control center first selects a set of privileged users, and then sends a single encrypted message to these users, and later only these privileged users can decrypt and read the message. However, when the set of privileged users are dynamically changed, those traditional techniques may not be flexible.

In this article, towards secure and flexible targeted broadcast in smart grid, we consider a new targeted broadcast mechanism with Key Policy Attribute-Based Encryption (KP-ABE) [6], where the control center is allowed to dynamically select user-groups based on their attributes. Since each user in the smart grid is associated with a set of attributes upon which the user's decryption key depends, on receiving an encrypted message transmitted by the control center along with an access policy based on these attributes, only the appropriate users meeting the access policy can decrypt the message.

The remainder of the article is organized as follows. Section II surveys some relevant research works. Section III describes the considered smart grid communication architecture. Section IV formulates the research problem. Then, our proposed KP-ABE targeted broadcast mechanism is described in Section V, followed by a qualitative performance analysis in Section VI. Finally, the article is concluded in Section VII.

II. Related Research Works

Smart grid security. A recent study [7] has prompted the British government to follow a more unified approach to secure smart grid communications. Concretely, the study demonstrates that the current approach to facilitate smart grid security is not adequate, and this may lead to attacks against the British power supply system. In addition, the study also reveals that the security mechanisms of smart grid are fragmented; while smart meter deployment has recently received more attention regarding safety and privacy, the overall smart grid communication security still remains an open issue. In particular, the applicability of recent security mechanisms, such as attribute based encryption schemes [6] in the context of smart grid communication, is yet to be explored extensively.

Attribute Based Encryption. In Attribute Based Encryption (ABE) schemes [6], [8], [9], descriptive attributes and policies (associated with the user) are used to decrypt encrypted messages. A central authority first creates secret keys for the users based on attributes/policies for each user. In order for a user to decrypt an encrypted message, a minimum number of attributes must be satisfied concerning the encrypted message and the user's private key. An enhanced version of ABE, called Ciphertext-Policy ABE (CP-ABE), was constructed by Bethencourt *et al.* [9], where the private key of the user is associated with a set of attributes, and the encrypted message specifies an access policy over the attributes. To decrypt a given ciphertext, the user needs his attributes to satisfy the access policy, which is specified within the ciphertext. An example on how CP-ABE can be applied to smart grid communication can be found in [4], where CP-ABE gives selective access to user-data stored in smart grid data repositories. Key-Policy ABE (KP-ABE) [6] is another variant of ABE, in which every encrypted message is labeled by the encryptor with a set of attributes. Each private key is associated with an access structure that specifies which type of ciphertexts the key can decrypt. In other words, the access structure and ciphertexts in KP-ABE are specified by the private key and the attributes set, respectively. It has been shown that a tree access structure can be adopted in KP-ABE, where interior nodes comprise AND and OR gates, and the leaves represent attributes of different parties or users. A set of users, if they satisfy the tree access structure, can reconstruct the secret. In this work, based on KP-ABE techniques, we exploit how to achieve secure and flexible targeted broadcast in smart grid communication.

III. Smart Grid Communication Architecture

In this section, we describe the basics of smart grid communication architecture. The smart grid power transmission and distribution system delivers power from the power plant to end-users through a transmission substation and a number of distribution substations. Our considered smart grid communication system is separated from the power transmission and distribution system, and can be viewed as an information sharing network comprising a number of hierarchical components as illustrated in Fig. 2. Concretely, we consider the smart grid control centers to be of two types: a Master Control Entity (MCE) at the transmission substation and a number of Neighborhood Control Centers (NCCs) located at various distribution substations.

All the NCCs are directly connected to the MCE, typically over optical fiber technology to sustain delay-sensitive and bandwidth-intensive smart grid communication [2]. The remaining components of the considered smart grid communication topology is divided into a number of networks by following the real-life planning of a metropolitan area. Broadly speaking, a city has many neighborhoods, each neighborhood has many buildings, and each building may have a number of apartments. We consider that each NCC covers a neighborhood area network, which consists of a number of building networks. Note that the term "building", in this work, conveys a generic meaning, which may range from a residence to a commercial installation, e.g., factory, school, hospital, and so forth. Each building network comprises a number of home networks. Thus, our considered smart grid communication architecture features the real-life set-up of a city or a metropolitan area.

In addition, advanced power devices known as "smart meters" are deployed in the home, building, and neighborhood area networks to facilitate two-way communication between the users and power supplier. The smart meters are equipped with both power reading and communication gateway interfaces. The communication technology of the smart meters at home and building/neighborhood are considered to be Zigbee and wireless broadband technologies (e.g., WiMax/3G), respectively [10].

IV. Problem Formulation

In smart grid, it is important to minimize message transmission within the grid as much as possible [2] while securely and flexibly controlling the receivers. We consider

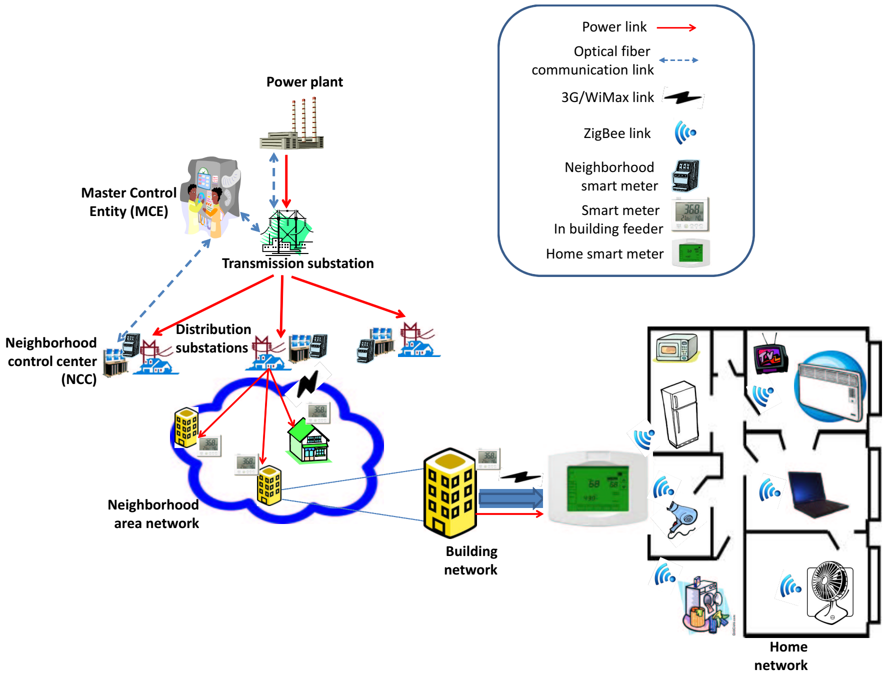

Fig. 2. Considered smart grid architecture.

a scenario in which the MCE needs to transmit different messages to different neighborhoods and different customers. The MCE has two options, either to encrypt and send these messages one by one in a unicast fashion, or broadcast a single encrypted message and allow the appropriate receivers (neighborhood/building/home users) to obtain the information intended for them. Note that by adopting the latter option, the MCE will benefit by only sending once, saving precious processing, memory, and network resources as well as time. The reason behind this is that the latter option allows the receiver or user-side smart meters to decrypt and view the information intended only for them. Then, how to facilitate the latter option in smart grid communication becomes an important issue.

To illustrate the significance of the latter option in smart grid communication, we consider the following scenario, in which two small towns in New York state, namely Hobart and Bovina, are involved. In the scenario, the MCE may only want to send sensitive information to the Hobart residences. Is it possible for the MCE to flexibly only send one encrypted information so that all residences at Hobart are able to read the information while the users of Bovina are not able to decrypt it? Another scenario is when users in smart grid subscribe to different packages, and are due to receive different energy pricing. Then, if the MCE wants to send pricing events to a particular package holders, is it possible for the MCE to flexibly only send one encrypted information so that the appropriate users can read the information? For scenarios such as these, how to issue a secure targeted broadcast message is, indeed, important. Therefore, in the next section, we utilize the KP-ABE to propose a flexible solution to address this challenge in smart grid communication.

V. Proposed KP-ABE Targeted Broadcast Mechanism in Smart Grid

In this section, for securing targeted broadcast in smart grid, we illustrate how the KP-ABE technique [6] can be effectively applied. The reason behind selecting KP-ABE for this purpose is that KP-ABE can provide an efficient public key cryptography primitive for one-to-many encryption.

We assume that all the smart grid users have some attributes. Selecting a proper attributes set is the first step to construct an efficient KP-ABE targeted broadcast for smart grid. Let $\mathcal{U}$ be the universal set of all user attributes, $\mathcal{A}$ be a tree-based access structure comprising logic gates (i.e., AND and OR gates). A sample tree-based access structure for the considered KP-ABE targeted broadcast for smart grid is depicted in Fig. 3. As shown in the figure, each non-leaf node represents a logic gate, and has a threshold. If its threshold equals one, it is an OR gate. If its threshold equals its children number, it is considered as an AND gate. On the other hand, each leaf node is considered as an attribute. All the nodes in the access tree are ordered by index numbers as demonstrated in the figure.

The access tree, $\mathcal{A}$, is used as an important input to the KP-ABE algorithm. KP-ABE algorithm has the following five steps, which are also summarized in Fig. 4.

1) In the system setup, KP-ABE uses a cyclic group G_1 generated by a generator g of prime order p and another cyclic group G_2 of the same order to form a bilinear map $e : G_1 \times G_1 \rightarrow G_2$. Then, MCE generates KP-ABE public key set PK = $(T_1,\ T_2,\ \cdots,\ T_N,\ Y)$ where $Y = e(g,g)^y$ with a random number $y \in Z_p^*$, and master key set MK = (t_1, t_2, ..., t_N, y).

2) Next, a message M is encrypted under k attributes with a random number input s, and the ciphertext C is produced.

3) The secret decryption key, D, is then generated by taking as inputs the leaf nodes of the access tree $\mathcal{A}$ (i.e., the attributes)

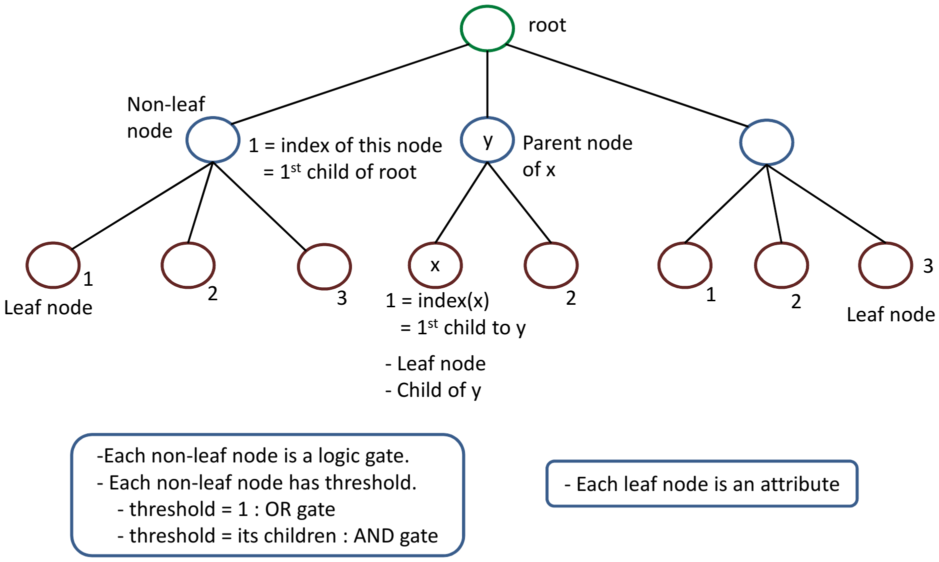
root
Non-leaf node
1 = index of this node = 1st child of root
y
Parent node of x
1
2
3
Leaf node
x
1 = index(x) = 1st child to y
- Leaf node
- Child of y
2
1
2
3
Leaf node
-Each non-leaf node is a logic gate.
- Each non-leaf node has threshold.
- threshold = 1 : OR gate
- threshold = its children : AND gate
- Each leaf node is an attribute

Fig. 3. A sample tree-based access structure ($\mathcal{A}$) for KP-ABE in smart grid.

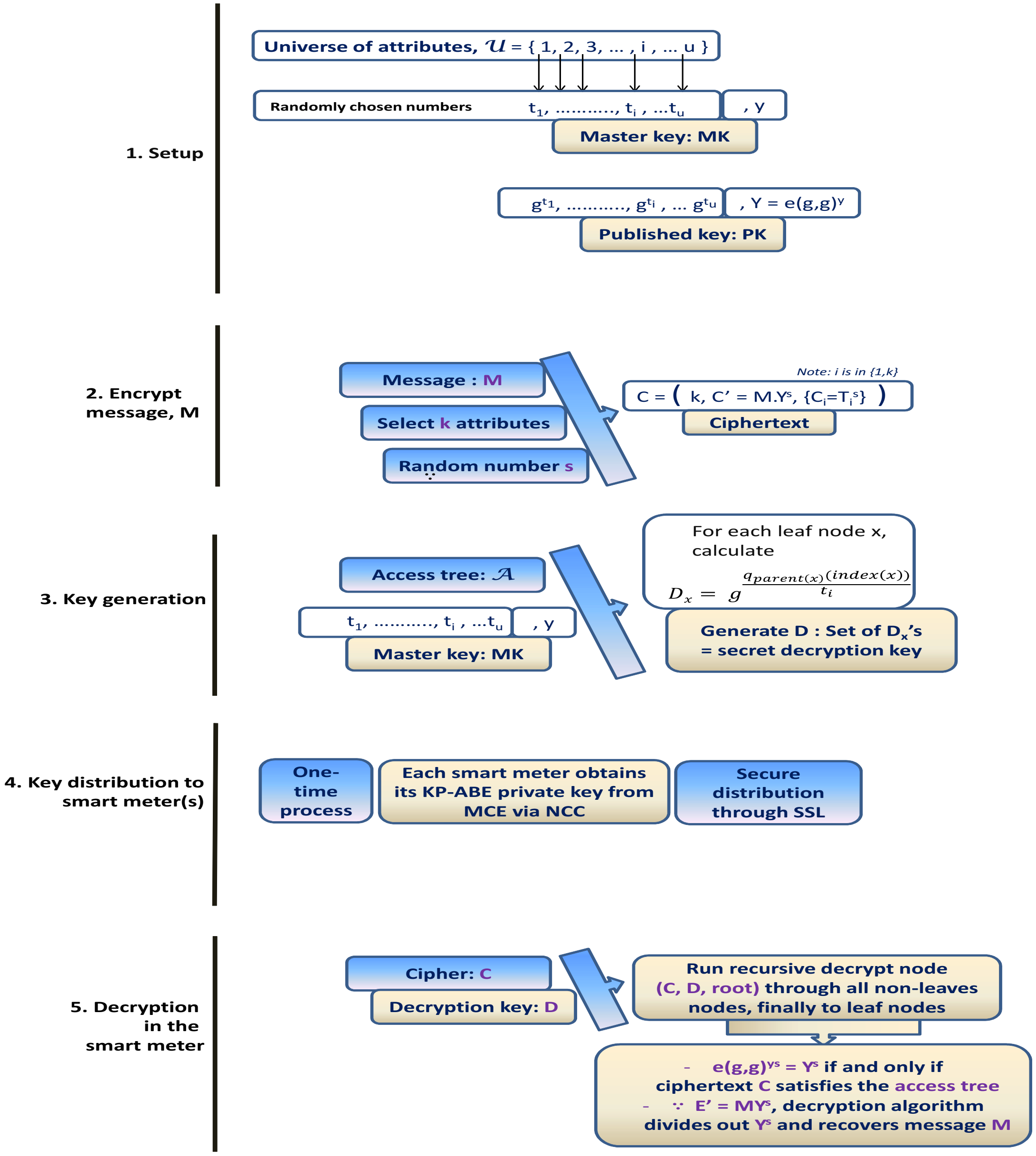
1. Setup
Universe of attributes, $\mathcal{U}$ = { 1, 2, 3, ... , i , ... u }
Randomly chosen numbers t_1, ..., t_i , ...t_u
, y
Master key: MK
g^{t_1}, ..., g^{t_i} , ... g^{t_u}
, Y = $e(g,g)^y$
Published key: PK
2. Encrypt message, M
Message : M
Select k attributes
Random number s
Note: i is in {1,k}
C = (k, C' = M.Y^s, {C_i=T_i^s})
Ciphertext
3. Key generation
Access tree: $\mathcal{A}$
t_1, ..., t_i , ...t_u
, y
Master key: MK
For each leaf node x, calculate
$D_x = g^{\frac{q_{parent(x)}(index(x))}{t_i}}$
Generate D : Set of D_x's = secret decryption key
4. Key distribution to smart meter(s)
One-time process
Each smart meter obtains its KP-ABE private key from MCE via NCC
Secure distribution through SSL
5. Decryption in the smart meter
Cipher: C
Decryption key: D
Run recursive decrypt node (C, D, root) through all non-leaves nodes, finally to leaf nodes
- $e(g,g)^{ys}$ = Y^s if and only if ciphertext C satisfies the access tree
- ∵ E' = MY^s, decryption algorithm divides out Y^s and recovers message M

Fig. 4. Execution steps of KP-ABE targeted broadcast mechanism in smart grid.

and master key MK, where the technical computation of D is depicted in Fig. 4.

4) Each smart meter obtains its KP-ABE private key from MCE via NCC. This is a one-time key-distribution process, which should be performed over secure transmission, e.g., Secure Socket Layer (SSL).

5) When there is an encrypted broadcast transmission from the control center, the smart meters perform decryption operation on the received ciphertext by using its decryption key D. This is a recursive decryption operation, which starts on the root node of the access tree $\mathcal{A}$, and then recursively iterates through all non-leave nodes, finally to the leaf nodes. The complex conditions expressed in Fig. 4 are satisfied if and only if the ciphertext satisfies the tree, and the original message M can, thus, be recovered.

In this way, the ciphertexts are associated with the smart grid users' different attributes, while user secret keys are defined with access structures on attributes. Therefore, a user can decrypt the ciphertext only if the ciphertext attributes satisfy the user's access structure.

Next, we will present an example to illustrate how KP-ABE targeted broadcast performs secure broadcast to targeted users (i.e., smart meters). Consider three types of messages exchanged between the smart grid control center and smart meters: (i) maintenance schedule announcement; (ii) real-time price event; and (iii) meter firmware update request. The smart meters should have the following attributes corresponding to these three considered message types, namely location (zip-code/address), subscription package profile, and firmware version, respectively.

Consider Fig. 5, which depicts the subscription package profile having three values: P_1, P_2, and P_3, that represent governmental, industrial, and residential subscriptions, respectively. If the MCE needs to send the real-time price event only applicable to the industries, it should encrypt the message using the proposed KP-ABE targeted broadcast with the industrial subscription attribute. Similarly, it can also be done to announce for maintenance periods to residents of a specific location. For instance, the MCE can broadcast a firmware update request targeting residential subscribers, which can be decrypted only by the residential smart meters. Obviously, this kind of flexible targeted broadcast is secure and efficient, where the encrypted messages can only be decrypted by the targeted group without the need for multiple encrypted message generation accompanied with multiple unicast transmissions.

VI. Performance Analysis

In contrast with the general ABE approach, most of the existing group key management solutions use auxiliary keys, which are referred to as key encryption keys. Each user is given a unique subset of key encryption keys, and the group controller encrypts re-key messages, with a combination of key encryption keys. This enables only current users to obtain the new data encryption key. In other words, the key encryption keys present a way to differentiate any subset of users from the remaining multicast group. On the other hand, there exist several advantages to utilize attribute based encryption for group key management. First, it is possible to decouple between abstract attributes and actual keys. When a secret key is issued for a set of attributes, the secret key components are calculated based on that set. However, the secret key information are hidden through a combination of randomization factors, which are unique to the secret key. Therefore, even if two users share certain attributes, the group elements in their secret keys are independent. As a result, the secret keys of current users need not be changed during a join or departure event. Thus, the attribute-based encryption methodology based on key policy is different and more effective when compared with the traditional group management schemes, in which all the key encryption keys require to be updated due to membership change.

In Table I, an efficiency comparison among the secure broadcast using KP-ABE and that with two other implementations of CP-ABE (namely BCP-ABE1 and BCP-ABE2) [8] are listed. The size of ciphertext, private key, and public key are compared amongst these three schemes. Note that n and r denote the total number of users and number of revoked users, respectively. t represents the access structure size, which can be at most l. The number of attributes associated with the private key in the considered ABE schemes is denoted by k, which can be maximum up to m. As demonstrated from the comparison, KP-ABE has smaller cipher text size compared to both the BCP-ABE1 and BCP-ABE2. Regarding the private key size, BCP-ABE1 performs better than the KP-ABE approach. On the other hand, the public key size for KP-ABE is significantly smaller than those of the BCP-ABE schemes. With this slight trade-off, KP-ABE appears to be the better choice to be exploited for secure targeted broadcast in smart grid communications in contrast with the other ABE schemes.

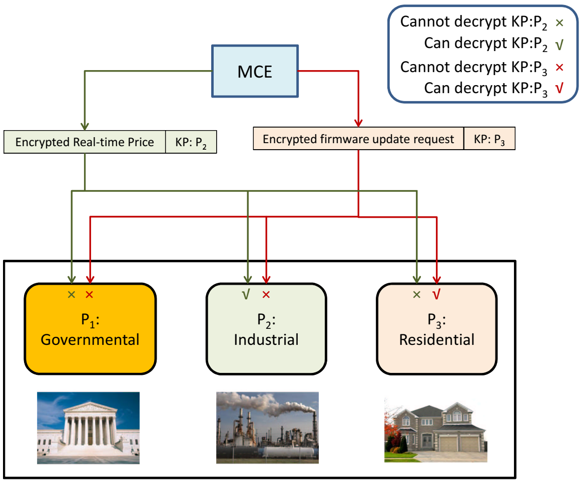

Fig. 5. Example of flexible KP-ABE targeted broadcast for real-time price and firmware update request messages.

VII. Conclusion

In this article, we have proposed a KP-ABE targeted broadcast mechanism for smart grid communications and qualitatively analyzed its performance. Specifically, the proposed KP-ABE targeted broadcast is characterized by (i) placing minimal

TABLE I
COMPARISON OF KP-ABE AND OTHER ABE-BASED BROADCAST [8].

Scheme	cipher size	private key size	public key size
KP-ABE broadcast	$(k+1)+1$	$2t$	$(m+4)+(2n-2)$
BCP-ABE1	$(t+1)+1$	$k+2$	$m+l+3+(2n-1)$
BCP-ABE2	$(t+1)+2r$	$(k+2)+2$	$(m+l+3)+4$

load on the smart grid control center(s) without the need to compose and send encrypted messages to users in a unicast manner; and (ii) directly and flexibly broadcasting encrypted messages with user's attributes. With the mechanism, both communication and computation efficiency can be improved. In our future work, we will study how to ensure the key policy to be hidden in order to avoid potential privacy breach and/or exploitation issues in smart grid communications.

REFERENCES

[1] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, Jan. - Feb. 2010.

[2] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, Dec. 2011.

[3] R. Lu, X. Li, X. Lin, X. Liang, and X. Shen, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28–35, Apr. 2011.

[4] S. Ruj, A. Nayak, and I. Stojmenovic, "A security architecture for data aggregation and access control in smart grids," *CoRR*, vol. abs/1111.2619, 2011.

[5] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. on Parallel and Distributed Systems*, to appear.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *ACM Conference on Computer and Communications Security*, Oct. - Nov. 2006, pp. 89–98.

[7] "New Study Stresses Need for Unified Security Approach for Smart Grid," http://www.smartmeters.com/the-news/smart-grid-news/2389-new-study-stresses-need-for-unified-security-approach-for-smart-grid.html, Jun. 2011.

[8] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," in *Pairing*, 2009, pp. 248–265.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE Symposium on Security and Privacy*, May 2007, pp. 321–334.

[10] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60 –65, Apr. 2011.

Zubair Md. Fadlullah [S'07, M'11] (zubair@it.ecei.tohoku.ac.jp) received B.Sc. degree with Honors in computer sciences from the Islamic University of Technology (IUT), Bangladesh, in 2003, and M.S. and Ph.D. degrees from the Graduate School of Information Sciences (GSIS), Tohoku University, Japan, in 2008 and 2011, respectively. Currently, he is serving as an Assistant Professor at Tohoku University. His research interests are in the areas of smart grid, network security, intrusion detection, game theory, and quality of security service provisioning mechanisms. Dr. Fadlullah was a recipient of the prestigious Deans and Presidents awards from Tohoku University in March 2011.

Nei Kato [M'03, A'04, SM'05] (kato@it.ecei.tohoku.ac.jp) has been a full professor at GSIS, Tohoku University, since 2003. He has been engaged in research on computer networking, wireless mobile communications, and smart grid, and has published more than 200 papers in journals and peer-reviewed conference proceedings. He currently serves as Chair of the IEEE Satellite and Space Communications Technical Community (TC) and Vice Chair of the IEEE Ad Hoc & Sensor Networks TC.

Rongxing Lu [S'09, M'11] (rxlu@bbcr.uwaterloo.ca) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.

Xuemin (Sherman) Shen [M'97-SM'02-F'09] (xshen@bbcr.uwaterloo.ca) received a B.Sc. (1982) degree from Dalian Maritime University, China, and M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey, all in electrical engineering. He is a professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo. His research focuses on mobility and resource management, UWB wireless networks, wireless network security, and vehicular ad hoc and sensor networks. He is currently serving as an Editor-in-Chief for IEEE Network, Peer-to-Peer Networks and Applications, and IET Communications. He is a Fellow of Engineering Institute of Canada, a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of the IEEE Communications Society.

Yousuke Nozaki [M] (nozaki.yousuke@lab.ntt.co.jp) is a project manager, senior research engineer, supervisor, Energy System Project, NTT Energy and Environment Systems Laboratories, Japan. He received B.E. and M.E. degrees in mechanical engineering from Tohoku University, Miyagi, in 1987 and1989, respectively. He joined NTT Laboratories in 1989. Since then he has been engaged in R&D of switching power regulators, photovoltaic and fuel cell power systems, and high-voltage direct current power systems for telecommunications systems. He is a member of IEICE and the Institute of Energy Economics, Japan.