An Efficient Distributed Approach for Key Management in Microgrids

---

Citation:

Mohamed I. Baza, Mostafa M. Fouda, Adly S. Tag Eldien, and Hala A.K. Mansour, "An Efficient Distributed Approach for Key Management in Microgrids," Proc. of the 2015 International Computer Engineering Conference (ICENCO 2015), Giza, Egypt, December 29-30, 2015.

URL:

http://ieeexplore.ieee.org/document/7416320/

An Efficient Distributed Approach for Key Management in Microgrids

Mohamed I. Baza*[1], Mostafa M. Fouda*[2], Adly S. Tag Eldien*[3], and Hala A.K. Mansour*[4].
*Faculty of Engineering at Shoubra, Benha University, Egypt.
Emails: mohamed.abaza@feng.bu.edu.eg[1], mfouda@feng.bu.edu.eg[2], adlytag@feng.bu.edu.eg[3],
and hala.mansour@feng.bu.edu.eg[4]

***Abstract*—Smart grid (SG) is a new technology which allows the electrical power grid to be smart. Cyber security plays an essential role in the smart grid in order to secure the bidirectional communication between the utility and the consumer side. To pursue confidentiality and integrity, a key management scheme is considered a critical challenge in the SG. As a result, several key management protocols have been proposed in literature. However, many of those proposed protocols have a centralized feature that depends on a single server called Meter Data Management System (MDMS) to distribute keys and update them. In this paper, we propose a distributed key management scheme with authentication capability to avoid the single-point failure problem by removing the need for using an MDMS. Furthermore, we apply our scheme to the microgrid which can be considered a small-scale smart grid and can be isolated from the main grid. The security and performance analysis are conducted to show the effectiveness and scalability of our scheme by considering the communication and computation cost.**

***Index Terms*—Smart grid, cyber security, key management protocol, microgrid.**

I. Introduction

The smart grid is considered as the next generation of the power grid which enables a two-way communication between the end users and the utility with self-healing reliable grid protection [1]. Some of the expected benefits of the SG are (i) preventing blackouts; (ii) allowing new technologies and products like plug-in hybrid electric vehicles (PHEVs); (iii) opening the door to microgrids [2] (iv) Supporting the deployment of renewable energy sources to be integrated with the SG; (v) automatic maintenance and increased reliability and transparency; and (vi) reducing the generation cost of the electricity [3] through demand response (DR) projects [4]. These benefits are arise through communication between smart meters and the utility via Advanced metering infrastructure (AMI) system [5]. Although the previously mentioned advantages for the smart grid, many risks may affect the system like man-in the-middle (MITM) attack, denial of service (DoS) attack, impersonation attack, sniffing on smart meters, spoofing and replay attacks [6], [7], [8].

Several organizations are interested in the deployment of smart grid security, e.g., Cyber Security Working Group (CSWG) led by National Institute of Standards and Technology (NIST) [9] and several work are done to insure security requirements: authentication, availability and integrity. To pursue authentication and integrity in the smart grid, a key management is still a critical problem [10]. This is because (i) the SG consists of a large number of smart meters which differs from one country to another. (ii) the smart meters are considered resource-constrained devices with small memory and limited processor. In literature, many research papers tried to address and solve this problem [11], [12]. In Sec. II we illustrate some vulnerabilities to some of those schemes and illustrate our proposal.

SG can be defined as a network of microgrids. A microgrid is a small scale electrical system which may be isolated from the main grid. However, existing key management schemes do not consider the possibility of isolation of the microgrid. Microgrid shall be discussed in Sec. III.

Our main contributions in this paper can be summarized as follows. (1) we study the existing key management protocols and their weaknesses; (2) we propose our new distributed key management scheme for the microgrids; (3) we show the security and performance analysis of our scheme.

The remainder of this paper is organized as follows. Sec. II presents the main issues of the existing key management schemes. Sec. III presents the system model of the microgrid which we will apply our distributed key management on it and the abbreviations used in our scheme. Sec. IV presents our proposed protocol for management keys in the microgrid. The security and performance analysis are discussed in Sec. V, followed by conclusions of our work in Sec. VI.

II. Problem Statement

In this section, we review some of the existing schemes that have been introduced to solve the key management process in the smart grid. Liu *et al.* [11] proposed a key management scheme for the AMI system that depends on the key graph technique [13]. The key graph technique uses a hierarchical key tree to generate the group keys for large groups. The advantage of using key graph technique is its low computation. However, it has a common type of DoS attacks called de-synchronization attack [12]. Wan *et al.* [12] proposed their key management which directly relies on the one-way function tree technique (OFT) [14]. OFT is a common centralized key management protocol in which nodes are arranged in a binary tree so they can collaborate with a central server called meter data management systems (MDMS) to compute the group key. However, we see that these schemes have some drawbacks like:

1) They are centralized techniques which depend only on the MDMS to manage keys so this considered a single point failure problem.
2) These schemes impose large overhead on the MDMS because the SG consists of large number of smart meters which may reach several millions in some areas.
3) They consider only the way of communication, e.g., unicast, multicast, and broadcast, and not the architecture of the SG. For example, they do not consider how to secure the communication in a microgrid.

Key management techniques can take other forms than being centralized [15]. In this paper, we introduce the idea of using distributed key management protocols in which no central server is required to secure the communication.

SG can be considered a network of microgrids. A Microgrid [16] is generally defined as a low voltage network with distributed generation sources, together with local storage devices and controllable loads (e.g. water heaters and air conditioning). They have a total installed capacity in the range of a few hundred kilowatts to a couple of megawatts. The unique feature of microgrids is that, although they operate mostly connected to the distribution network, they can be automatically be transferred to islanded mode. Therefore, we propose a novel distributed key management protocol tailored for the microgrid. In addition, by performing a security and cost analysis for our proposal, it shows that it is suitable for the smart meters low capabilities.

III. System Model and Notations

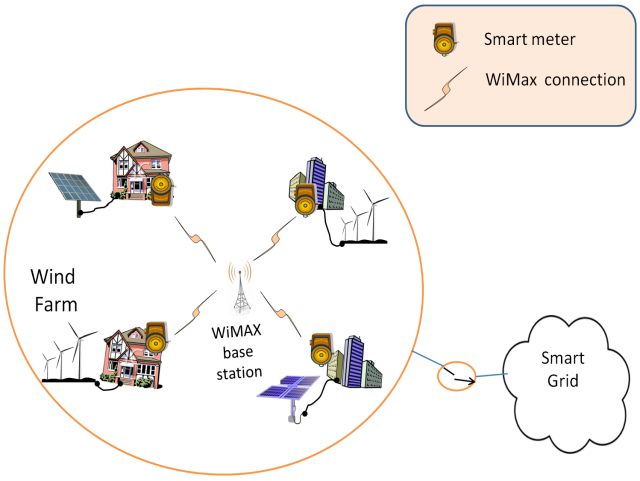


Fig. 1: a Microgrid consisting of four buildings, two wind farms, two solar panel generators and a WiMax Tower. Electricity is exchanged between buildings through power lines. A WiMAX tower can be employed to support communications in the microgrid.

We consider the following model for the microgrid as shown in Fig. 1. The main component of the microgrid are the smart meters which are implemented in hardware to do the following functions:

1) Measuring electricity usage.
2) Responsible for the two-way communication with the utility.
3) Allowing demand response (DR) [3] to increase the usage efficiency [4], [17].

Communication through the microgrid can be done using WiMAX technology [18]. Also, the microgrid can work on either islanded mode or connected to the smart grid as shown Fig. 1. The notations and abbreviations with their definitions through our paper are listed in Table. I.

TABLE I: Notations.

GID	Group identifier.
$\oplus$	An exclusive OR operation.
n	Number of smart meters in a DR project.
$H()$	Secure hash function.
K_G	Group key.
K_{NG}	New group key after a member change.
$\|$	Concatenation operator.
$f(g)$	One way function.
PKT	Public Key Table contains the parent binary code associated with member public key.
$Kgen(1^b)$	A secure b-bit key generation algorithm.
Ti	The recorded time instance of sending the message.
HMAC_{Ki}	Hash-based Message Authentication Code (MAC) generation algorithm by using the shared session key Ki.

IV. Our Proposed Scheme and Tree Architecture

As stated earlier, our scheme has a distributed feature. We adopt one of the recently existing distributed schemes [19] to be employed in the microgrid. The main feature of this scheme is its low communication and computation overheads which is important for the deployment on the smart meters as stated in Sec. II.

The main features of this scheme are as follows:

- The scheme is based on the one-way function tree technique [14]. However, no central server exist. As a result meters can control the key management process with each others.
- Meters are organized in a binary tree as in Fig. 2 in which each node has two codes:
  1) Binary code is used to discover the member position.
  2) Decimal code is used to calculate intermediate nodes key which is used to encrypt data to a specific meters in the group.
- Two types of keys are used by smart meters:
  1) Public key for each meter generated by Diffie-Hellman key agreement.
  2) Symmetric keys are assigned to intermediate nodes which can be used to secure communications within the multicast group.
- The Public Key Table (PKT) is used to store the public key of meters and the decimal code associated with their parent binary code and then is used to share a secret session key between group members. Moreover, the PKT is updated when a smart meter leaves or joins a demand response (DR) project periodically.

- Any smart meter who want to join a specific group can calculate all the decimal codes which it belongs by knowing only its parent code by removing the the last digit from the right as shown in Fig. 3

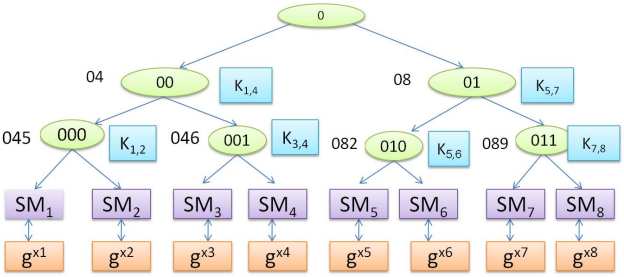


Fig. 2: A group of eight meters consisting a demand response (DR) group are organized in a tree. Each node has two codes: a decimal and a binary one. Also, the leaf nodes are assigned D-H keys.

Fig. 2 shows eight meters arranged in a binary tree (A binary tree is used for the simplicity, but we could design it as a ternary tree). The node 0 is the group identifier (GID), we assume that the microgrid is divided into groups and each group has an identifier to decrease the computation overhead. First the decimal code is determined for each node using this equation:

$$Code_{Child-node} = f(Code_{Parent-node} \| Random - digit)$$

Then it is used to calculate the intermediate node key:

$$K_{Intermediate-node} = f(K_G \oplus Code_{Intermediate-node})$$

For example, the node (00) has a decimal code$= (0||4) = 04$, where 4 is a random number generated by the meter and its intermediate key which can be used to encrypt data between $SM_1, \ldots, SM_4$ is:

$$K_{1,4} = f(K_G \oplus 04)$$

A. Key Establishment in Our Scheme

We adopt our key establishment from Diffie-Hellman key agreement [20]. Let $\mathbb{G} = \langle g \rangle$ be a group of large prime order p. Each smart meter in the group generates a private value ($x_i \in \mathbb{Z}_p^*$), then determines the public key by g^{x_i}. After each meter determines its public key, it broadcasts this key to other meters and stores it in the PKT. For example, the two meters (SM_i, SM_j) can determine a shared session key (K_s) as follows:

$$SM_i \Rightarrow K_s = H((g^{x_j})^{x_i}), SM_j \Rightarrow K_s = H((g^{x_i})^{x_j}) \quad (1)$$

where: x_i and x_j are private values for SM_i and SM_j respectively.

When a smart meter SM_b asks to join a (DR) program, it should be authenticated by the sponsor (say SM_a). This can be done as in [21] in Fig. 4 as follows: (i) suppose SM_a and SM_b have their public and private keys. The public and private keys of SM_a are $Pub_{SM\ a}$ and $Priv_{SM\ a}$. The public and private keys of SM_b are $Pub_{SM\ b}$ and $Priv_{SM\ b}$. (ii) SM_a generates a random number x_a and calculates g^{x_a}. (iii) SM_a sends g^{x_a} encrypted by the public key of SM_b. (iv) SM_b decrypts the received message and replies with g^{x_a} and g^{x_b} encrypted by the public key of SM_a. (v) SM_a checks if received g^{x_a} is the same as the sent one, thus SM_b is authenticated and they both can share a secret session key as in Eq. 1.

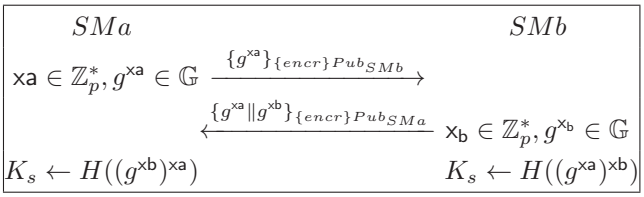


Fig. 4: Authentication scheme.

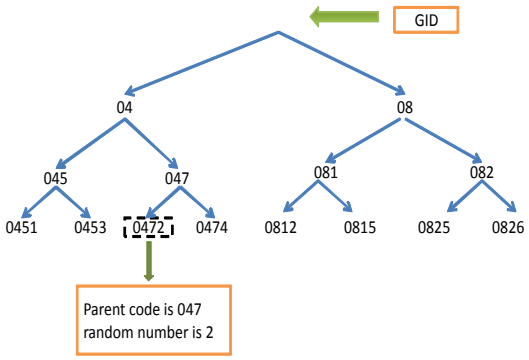


Fig. 3: Calculating decimal codes of intermediate nodes.

B. Multicast Key Management

In this section, we discuss the multicast communication which is required to the demand response (DR) projects which are critical for achieving efficiency in the microgrid.

1. Smart Meter Joining

When a new smart meter asks to join the group. The joining protocol is employed to update the group key and the intermediate node codes. We discuss the join protocol from Fig. 6. When SM_8 wants to join the group, it sends a hello message by making a broadcast asking to join the group. First SM_7 (who has no sibling) should authenticate SM_8 and see if it can join the (DR) program or not as discussed earlier in Fig. 4 by first computing a new public key $g^{x7'}$. Then they both can compute a shared secret session key (K_s) as follows:

$$SM_7 \Rightarrow K_s = H((g^{x8})^{x7'}), SM_8 \Rightarrow K_s = H((g^{x7'})^{x8})$$

SM_7 updates his position from (01) to (011) by and renew the Public Key Table (PKT) as in Fig. 5. SM_7 sends an update to other meters about the change in the (PKT) for node (011). To ensure that two nodes do not have the same decimal code, SM_7 uses its PKT to select 9 as a random number to calculate the decimal code for its parent (011) as in $(S1)$, then it updates the group key by applying a one-way function to the previous group key as in $(S2)$ and sends them to SM_8 encrypted by the shared session key. Also, we employ a Hash-based Message Authentication Code (MAC) generation algorithm by using K_s on the sent message to pursue integrity as in $(S3)$.

$$code_{node_{(011)}} = (08 \| 9) = 089 \Rightarrow (S1)$$

$$K_{\text{NG}} = f(K_{\text{G}}) \Rightarrow (S2)$$

$$SM_7 \rightarrow SM_8 : \{K_{NG}, 089, HMAC_{K_s}\}_{\{encr\}K_s} \Rightarrow (S3)$$

The remaining group members renew the group key by applying $(S2)$. Also, smart meters in the affected path recalculate the intermediate codes as follows:

$$SM_7, SM_8 \leftrightarrow K_{7,8} = f(K_{\text{NG}} \oplus 089) \Rightarrow (S4)$$

$$SM_5, \ldots, SM_8 \leftrightarrow K_{5,8} = f(K_{NG} \oplus 08) \Rightarrow (S5)$$

Node	Decimal Code	Public Key
000	045	g^{x1}, g^{x2}
001	046	g^{x3}, g^{x4}
010	082	g^{x5}, g^{x6}
01	08	g^{x7}

$\Rightarrow$

Node	Decimal Code	Public Key
000	045	g^{x1}, g^{x2}
001	046	g^{x3}, g^{x4}
010	082	g^{x5}, g^{x6}
011	089	$g^{x7'}, g^{x8}$

Fig. 5: PKT update when SM_8 joins.

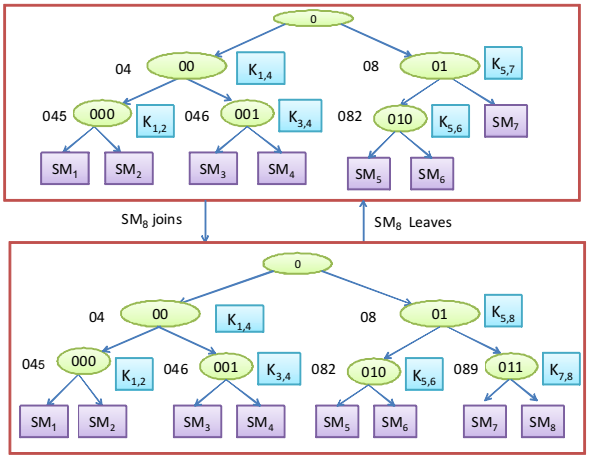


Fig. 6: Smart meter joining and evicting.

2. Smart Meter Evicting

When a smart meter asks to leave the group and to ensure the forward secrecy the group key must be updated using the leave protocol. If SM_8 wants to leave the group, its sibling (SM_7) upgrades his position in the tree to (01) and updates the PKT by deleting the leaving member as shown in Fig. 7, also it informs other meters about that change by sending a broadcast message. SM_7 generates a new group key (K_{NG}) using $Kgen(1^b)$ algorithm and uses his PKT to share a key with any meter in each branch of the tree. Then it sends the new group key to them ($S1$ and $S2$).

$$SM_7 \rightarrow SM_1 : \{K_{NG}, HMAC_{K_1}\}_{\{encr\}K_1} \Rightarrow (S1)$$

$$SM_7 \rightarrow SM_5 : \{K_{NG}, HMAC_{K_2}\}_{\{encr\}K_2} \Rightarrow (S2)$$

Where: $K_1 = H((g^{x_1})^{x_7})$ and $K_2 = H((g^{x_5})^{x_7})$ are shared secret keys between (SM_7 and SM_1) and (SM_7 and SM_5) respectively.

Next, SM_1 and SM_5 use the intermediate codes to encrypt the new group key and send it to other meters in the tree as in ($S3$ and $S4$).

$$SM_1 \rightarrow SM_2, \ldots, SM_4 : \{K_{NG}, HMAC_{K_{1,4}}\}_{\{encr\}K_{1,4}} \Rightarrow (S3)$$

$$SM_5 \rightarrow SM_6 : \{K_{NG}, HMAC_{K_{5,6}}\}_{\{encr\}K_{5,6}} \Rightarrow (S4)$$

To pursue the forward secrecy, the meters in affected branch should update the intermediate node codes i.e.,

$$SM_5, SM_6, SM_7 \leftrightarrow K_{5,7} = f(K_{\text{NG}} \oplus 08) \Rightarrow (S5)$$

Node	Decimal Code	Public Key
000	045	g^{x1}, g^{x2}
001	046	g^{x3}, g^{x4}
010	082	g^{x5}, g^{x6}
011	089	g^{x7}, g^{x8}

$\Rightarrow$

Node	Decimal Code	Public Key
000	045	g^{x1}, g^{x2}
001	046	g^{x3}, g^{x4}
010	082	g^{x5}, g^{x6}
01	08	g^{x7}

Fig. 7: PKT update when SM_8 leaves.

3. Secure Unicast and Multicast Communication

Our scheme adopts the following message transmission methods in order to achieve confidentiality and integrity:

Secure Unicast Communications. When SM_i wants to send a message (mi) to SM_j, they both can use their PKT to generate a shared secret session key (K_s) and send the following message:

$$SM_i \rightarrow SM_j : \{mi, Ti, HMAC_{K_s}\}_{\{encr\}K_s}$$

where: Ti is the recorded time instance of sending the message and used to prevent replay attacks, also $HMAC$ is based on the sent message and is used to ensure integrity of message.

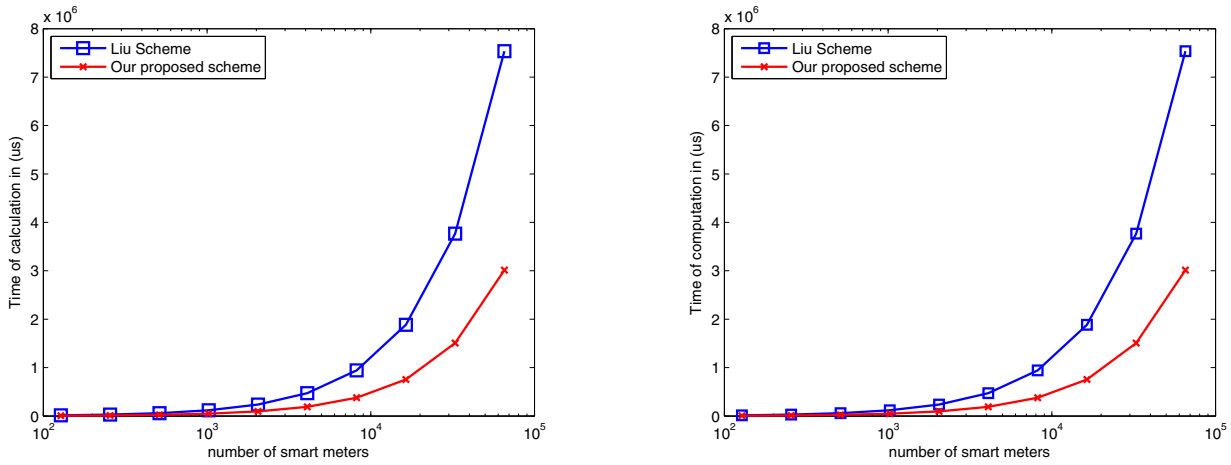
Secure Multicast Communications. The shared group key (K_G) is used to secure the multicast communication. For example SM_1 can send a (DR) message (mi) to other meters in the group as follows:

$$SM_1 \rightarrow SM_{others} : \{mi, Ti, HMAC_{K_G}\}_{\{encr\}K_G}$$

TABLE II: Computation cost comparison for our scheme with Liu [11].

		Liu [11]	**Our proposed scheme**
Adding a Member	MDMS	$(4n+5)C_f + (n+2)C_{\mathcal{E}}$	0
	Smart meter	$4nC_f + nC_{\mathcal{E}}$	$2(nC_f + C_{\mathcal{E}})$
Evicting a Member	MDMS	$(4n+5)C_f + (n+2)C_{\mathcal{E}}$	0
	Smart meter	$4nC_f + nC_{\mathcal{E}}$	$(2n-h+3)C_f + 2(h-1)C_{\mathcal{E}}$

* n is the number of meters in the group, h is height of the key tree. C_f and $C_{\mathcal{E}}$ are respectively the computational cost for calculation of the one-way function and the encryption function $\mathcal{E}$.



(a) Join operation.

(b) Leave operation.

Fig. 8: Simulation results for computation cost.

$HMAC$ and Ti are used to ensure integrity and prevent replay attacks, respectively.

V. Security Analysis and Performance Analysis

In this section, we discuss the security analysis of our scheme from the context of the key management scope. We begin by demonstrating the features of it, then the performance analysis on real-life are conducted.

A. Security Analysis

Our new scheme has the following security features:

Distributed feature: Our model removes the need for the utility (MDMS) to generate or update keys (re-keying process) which is a good feature for microgrid architecture which may be isolated from the main smart grid. Moreover, smart meters at joining phase do not have to exchange keys. Also, at leaving phase, the new group key is forwarded to remaining meters by using intermediate node codes.

Forward secrecy: (from the key management point of view) Is used to prevent a leaving or removed group member to continue accessing the communication within the group. This is illustrated in Sec. IV-B. When SM_8 leaves the group, the tree and the PKT is updated so that member will not be able to decipher group messages encrypted with the new key.

Backward secrecy: Is used to prevent a new member from decoding messages exchanged before it joins the group. In Sec. IV-B before SM_8 joining the group, it should be authenticated and only new group key and the parent binary code is delivered to it, so it only can compute new intermediate codes and can not decipher previous messages even.

B. Performance Analysis:

We analyze the performance of our proposed scheme from two aspects, namely, computation and communication cost. Then we compare these results with another existing protocol [11] (Although Liu's scheme has a centralized feature of key management, we compare our distributed key management with it to demonstrate the effectiveness of our scheme especially on smart meters).

TABLE III: Cryptographic Calculations on MICAZ.

Cryptographic operation	**MICAZ**
AES	0.023 ms
HASH	0.023 ms

1) *Computation cost:* (means that the processing overhead needed by the nodes to update the keys when a node

joins/leaves.) We estimate the computation overhead that is required by smart meters to add or evict a member as shown in Table II. To simulate our scheme on a real life environment: from [22], cryptographic operations are done in wireless sensor node MICAZ which look like smart meters in nature and has 4KB RAM, 128KB ROM and equipped with a low-power ATmega128L micro-controller working at 7.3MHz. We assume that encryption is done by Advanced Encryption Standard (AES). Table III show the time calculations for both AES and HASH operations. We use MATLAB [23] to evaluate the performance of our scheme as shown in Fig. 8 which proves that our model is efficient and scalable especially on the smart meters.

2) *Communication Cost:* Is used to determine the number of messages required to transmit in group re-keying process when a member joins/leaves the group. Communication cost results are given in Table IV. As shown in the Table IV, our scheme only needs one message to be delivered to the new member at joining phase that contains the new key. At the leaving phase, it needs a number of messages of order $\log_2 n$. Only a broadcast message is needed in both join or leave to update the PKT. These results prove that our scheme has a low communication overhead which is very convenient for the microgrid environment.

TABLE IV: Communication cost comparison.

		Liu's [11]	**Our proposed scheme**
Adding a Member	Broadcast	0	1
	Unicast	$2nK$	$1K$
Evicting a Member	Broadcast	0	1
	Unicast	$2nK$	$(2\log_2 n - 2)K$

* n is the number of meters in the group and K is the size of a key in bits respectively.

VI. CONCLUSION

In this paper, we introduced the idea of using distributed key management protocols in the smart grid in which no central server is used to distribute keys or update them when a member's status changes, also we suggest applying this model to the microgrid which can be in islanded mode and the utility has no control on it. The security and performance analysis of our model shows that it has low computation and communication cost while achieving forward and backward secrecy. In the future work, we shall apply the distributed key management for the whole AMI system.

REFERENCES

[1] 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.

[2] European SmartGrids Technology Platform. Vision and strategy for Europes electricity networks of the future, http://www.smartgrids.eu/documents/vision.pdf. 2006.

[3] H. Sle and O. S. Grande, "Demand response from household customers:Experiences from a pilot study in Norway," IEEE Transactions on Smart Grid, vol. 2, no. 1, pp. 102-109, Mar. 2011.

[4] F. Benzi, N. Anglani, E. Bassi, and L. Frosini, "Electricity smart meters interfacing the households," IEEE Transactions On Industrial Electronics, vol. 58, no. 10, pp. 4487-4494, Oct. 2011.

[5] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," IEEE Transactions On Industrial Electronics, vol. 58, no. 4, pp. 1218-1228, Apr. 2011.

[6] M. M. Fouda, Z. M. Fadlullah, and N. Kato, "Assessing Attack Threat Against ZigBee-based Home Area Network for Smart Grid Communications," Proc. of IEEE International Conference on Computer Engineering and Systems (ICCES'10), Cairo, Egypt, Nov. 30 - Dec. 2, 2010.

[7] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An Early Warning System against Malicious Activities for Smart Grid Communications," IEEE Network Magazine, vol. 25, no. 5, pp. 50-55, Sep.-Oct. 2011.

[8] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "Towards a Light-weight Message Authentication Mechanism Tailored for Smart Grid Communications," Proc. of IEEE International Conference on Computer Communications (INFOCOM WKSHPS'11), Shanghai, China, Apr. 10-15, 2011.

[9] The Smart Grid Interoperability Panel, "Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, " National Institute of Standards and Technology, MD, Tech. Rep. NISTIR 7628, Aug. 2010.

[10] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid - The New and Improved Power Grid: A Survey," IEEE Communication Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012.

[11] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," IEEE Transactions On Industrial Electronics, vol. 60, no. 10, pp. 4746-4756, Oct. 2013.

[12] Z. Wan, G. Wang, Y. Yang, and S. Shi, "SKM: Scalable Key Management for Advanced Metering Infrastructure in Smart Grids," IEEE Transactions On Industrial Electronics, vol. 61, pp. 2973-2982, Oct. 2014.

[13] C. K. Wong, M. Gouda, and S. Lam, "Secure group communication using key graphs," IEEE/ACM Trans. Netw., vol. 8, no. 1, pp. 1630, Feb. 2000.

[14] D. A. McGrew and A. T. Sherman, "Key establishment in large dynamic groups: Using one-way function trees," IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444-458, 2003.

[15] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," ACM Computing Surveys 35(3) (2003), 309-329.

[16] Microgrid, avaialble at, http://www.sissolarventures.com/Microgrids.php

[17] M. M. Fouda, Z. M. Fadlullah, N. Kato, A. Takeuchi, and Y. Nozaki, "A Novel Demand Control Policy for Improving Quality of Power Usage in Smart Grid," Proc. of IEEE Global Communications Conference (GLOBECOM'12), Anaheim, California, USA, Dec. 2012.

[18] P. Rengaraju, C. H. Lung, and A. Srinivasan, "Communication Requirements and Analysis of Distribution Networks using WiMAX Technology for Smart Grids," in 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), 2012, pp. 666670.

[19] S. Mortazavi, A. Pour, and T. Kato, "An Efficient Distributed Group Key Management using Hierarchical Approach with Diffie-Hellman and Symmetric Algorithm: DHSA," Computer Networks and Distributed Systems (CNDS), Tehran, pp. 49-54, 23-24 Feb. 2011.

[20] W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT22/6, Nov. 1976, pp. 644654.

[21] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Dec. 2011.

[22] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," Comput. Netw., vol. 54, no. 17, pp. 2967-2978, Dec.2010.

[23] Matlab, avaliable at, http://www.mathworks.com