Light-Weight Key Distribution and Management for Advanced Metering Infrastructure

Joseph Kamto, Lijun Qian, John Fuller, John Attia
Department of Electrical and Computer Engineering
Prairie View A&M University, Texas A&M University System
Prairie View, TX 77446
Email: {jkamto, liqian, jhfuller, joattia}@pvamu.edu

***Abstract*—Electricity grids must cope with rising demand and complexity in a changing world. Smart grid is a promising solution to address these challenges. Recently, Advanced Metering Infrastructure (AMI) is proposed as an integral part of the smart grid that collect and analyze the measurements of energy consumption using the communication network that links the smart meters. The cyber security issues in AMI become very important to guarantee the trustworthiness of the AMI. In order to achieve data confidentiality, privacy and authentication in AMI, security measures using various crypto algorithms will be needed, thus demand key distribution and management schemes. Since the number of electric appliances and devices need to be monitored in households and commercial facilities is large and the devices may have limited computational power and storage, thus novel key distribution and management schemes would be indispensable for the success of securing AMI from cyber attacks. In this work, we propose a light-weight key distribution and management scheme tailored to AMI. Specifically, a group ID based mechanism is proposed to establish the keys for a large amount of entities with small overhead. Security analysis is performed to evaluate the proposed method.**

I. Introduction

The electric power grid is incontestably the driving force of the human well being as it involves in every domain of our life. It consists of a complex connection system between generating power plants and power consumers through transmission and distribution networks spanning large geographic area. The current power grid is aging and could not withstand the electricity quality requirement for the next century as it is. Smart grid is the key technology that will empower the current power grid with the necessary tools using advanced telecommunications and information technology [1]. It has an overlay of a two-way digital communication infrastructure for the purpose of real time information exchange within the grid.

Recently, Advanced Metering Infrastructure (AMI) is proposed as an integral part of the smart grid that collects and analyzes the measurements of energy consumption using the communication network that links the smart meters. According to the smart grid system report of the US Department of Energy, Advanced metering infrastructure (AMI) is receiving the most attention in terms of planning and investment. In 2009, AMI comprises about 4.7% of all electric meters being used for demand response. Approximately 52 million more smart meters are projected to be installed by 2012 [2]. An AMI includes software, hardware, communication networks, customer-associated systems and meter data management software. As the smart grid becomes reality, the cyber security issues in AMI become very important as AMI is part of the critical infrastructure of the smart grid. In order to achieve data confidentiality, privacy and authentication in AMI, security measures using various crypto algorithms will be needed, thus demand novel key distribution and management schemes [3].

Several works have been done mostly in authentication for AMI, such as [4], [5], [6]. However, most of them have not addressed the key distribution and management in AMI. The authors in [5] propose a device authentication mechanism and key establishment scheme for smart grid Home Area Network (HAN), but with few security properties. On the other hand, the number of electric appliances and devices need to be monitored in households and commercial facilities is large and the devices may have limited computational power and storage. These challenges demand novel key distribution and management schemes for the success of securing AMI from cyber attacks. Hence, in this work we propose a light-weight key distribution and management scheme tailored to AMI. Specifically, *we focus on the HAN and design a group ID based mechanism to establish both the pairwise keys and group keys with small overhead*. The schemes for key update and key revocation are also discussed. Security analysis is performed to evaluate the proposed method.

The rest of this paper is organized as follows. The HAN modeling and problem formulation is given in Section II. Section III provides details on the proposed key distribution and management solution. Security analysis is given in Section IV. Related works and performance comparison are discussed in Section V. Section VI contains the concluding remarks.

II. HAN Modeling and Problem Formulation

Multiple communication technologies and standards will coexist in different parts of the smart grid from the different energy generation points all along the transmission, distribution infrastructures to the homes where the electricity is consumed. This results in a hierarchical communication infrastructure ranging from home area network (HAN) to building area network (BAN), neighborhood area network (NAN), and wide area mesh network (WAN) and the ubiquitous internet.

Electricity user is a major component of the smart grid. The efficient management of energy demand relies on the

978-1-4673-0040-7/11/$26.00 ©2011 IEEE

interactive high data rate information exchange with the utility through the smart meters that provide the end user many valuable abilities, such as reducing peak demand by shifting usage to off-peak hours based on the real-time price from the utility; lowering total energy consumption with possible restoration of its excess of energy back to the grid from renewable energy sources or electric vehicle [7]. Wireless communication technology avoids expensive deployment of wired connections, and is by far the appropriate communication medium that will connect the individual homes to the substations through a NAN centralized at a base station. Short range wireless communication standards like Zigbee (802.15.4) and Wifi (802.11) could be used for the smart meter interface in the HAN. The last miles wireless broadband or cellular network may interface the smart meters with the data collection base station within the NAN [8].

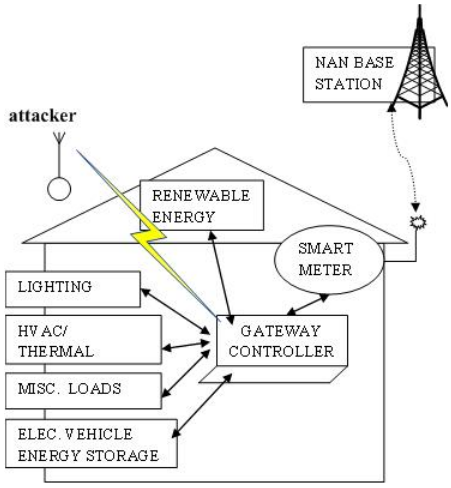

Fig. 1. An example of a Home Area Network and an Outside Attacker.

Although wireless systems provide relatively cheaper and flexible means for smart grid communications, they also suffer from more vulnerabilities to cyber attacks compared to their wired counterpart. For example, it is much easier to eavesdrop on wireless communications due to its broadcast nature. The main focus of this study is on the key distribution and management in a HAN. HAN is the part of the AMI that enhances the aforementioned two-way communication infrastructure between end users and utility provider with a centralized gateway access to the multiple appliances through the smart meter for the purpose of monitoring the energy usage in real-time. The extreme sensitivity of the information exchanged within the HAN necessitates a strong security, privacy and integrity mechanism without which the trustworthiness of the data will easily be questionable by the utility provider as well as the electricity user [9], [10].

Considering the smart appliances as end nodes, a HAN could be modeled as a group of end nodes linked in a star configuration to a gateway node that is in turn connected to the smart meter. The short range wireless communication standard like Zigbee interfaces all of them as well as the home interface of the smart meter. As such, each equipment and the smart meter are one-hop to the gateway. An attacker located in the wireless range of the nodes can eavesdrop the wireless communication within the HAN. The attacker may launch various attacks on the HAN, such as impersonating as legitimate group member and intercepting the message between devices, maliciously modifying the information contributed by the legitimate devices. The communication structure of the HAN and an outside attacker are shown in Fig.1.

In this paper, we focus on the outside attackers and possibly compromised nodes, rather than a cheating customer who try to access the meter configuration through cyber means or try to modify the meter firmware as considered in [11]. In order to achieve data confidentiality, privacy and authentication in HAN, security measures using various crypto algorithms will be needed, thus demand key distribution and management schemes. The aim of this work is to provide a light-weight key distribution and management scheme as the foundation for other security measures such as various crypto algorithms and protocols to guarantee the communication security between the group of devices in the HAN as well as the HAN interface of the smart meter.

III. Proposed Key Distribution and Management

We first consider the creation of pairwise symmetric keys between the gateway and each end node. Then a shared group key is derived from the pairwise keys. We also describe the procedures for key update and key revocation.

A. Generation of Pairwise Symmetric Key

The notation of cryptographic operations are

- $H(m)$: hash value of message (m);
- $E_k(m)$: encryption of message (m) with key (k);
- Z_q^*: a multiplicative group;
- q: a prime number, order of the group Z_q^*;
- a: a primitive root of q, generator of the group Z_q^*.

For all $x \in Z_q^* = \{i | 1 < i \ll q-1\}$, a^x exhaustively represent the group Z_q^* in some permutation. As such, for any value $P \in Z_q^*$, there is a unique x such that $P = a^x$; where x is the discrete logarithm of P. It is computationally not feasible to calculate x given P and a are very large.

Prior to the deployment, every device securely accesses a Certification Authority (CA) to be loaded with the following primitives: The device ID (serial number), the multiplicative group parameters (Z_q^*, q, a); and H (a well-defined cryptographic hash function).

A hash function converts a large amount of data into a small datum with the following properties: it is infeasible to find a message giving its hashed value (one-way property), it is infeasible to find two different messages with the same hash value (collision resistance property). Consider the gateway device, gw, and a neighboring device i of the group. Each of them select a number x_{gw} and x_i from the group Z_q^*, respectively, and proceed as follows:

At the Gateway GW		At Node I
$X_{gw} = a^{x_{gw}}$		$X_i = a^{x_i}$
$ID_{gw} \vert X_{gw}$		$ID_i \vert X_i$
$h_{gw} = H(ID_{gw} \vert X_{gw})$		$h_i = H(ID_i \vert X_i)$
$m_{gw} = h_{gw} \vert ID_{gw} \vert X_{gw}$	m_{gw} $\rightarrow$	
		Verify h_{gw} and compute
	$\leftarrow m_i$	$m_i = h_i \vert ID_i \vert X_i$
Verify h_i and compute the symmetric key $K_{gw}^i = X_i^{x_{gw}}$		
$c_{gw} = H(K_{gw}^i \vert ID_{gw})$		
$mess_{gw} = c_{gw} \vert ID_{gw}$	$mess_{gw}$ $\rightarrow$	
		$K_i^{gw} = X_{x_{gw}}^{x_i}$ check $c_{gw} = H(K_i^{gw} \vert ID_{gw})$
		Compute $c_i = H(K_i^{gw} \vert ID_i)$
	$mess_i$ $\leftarrow$	$mess_i = c_i \vert ID_i$
check $c_i = H(K_{gw}^i \vert ID_i)$ if equality hold confirm symmetric key $K_{gw}^i = K_i^{gw} = X_i^{x_{gw}} = a^{x_i x_{gw}}$		

In the above scenario, the gateway and a neighboring node select two random numbers x_{gw} and x_i in the multiplicative group and create two public keys X_{gw} and X_i per Diffie-Hellman (DH) scheme [12]. Firstly, they compute the hash value of the key, concatenate to their respective identification (e.g. serial number). Secondly, they exchange a message made of a concatenation of their respective hash value, their identification, and public key. After receiving the messages, both devices will re-compute the hash value for the purpose of message authentication that ensure the received messages were not tampered. Then both the gateway and the device can compute the symmetric key independently. They will exchange the hash value of the generated symmetric key to confirm that $K_{gw}^i = K_i^{gw} = X_i^{x_{gw}} = a^{x_i x_{gw}}$.

The pairwise shared key will be used to encrypt any information exchange between the gateway and the end node. The same symmetric key exchange could be performed between the gateway and all the devices in the HAN individually. The HAN group key will result from an aggregation of these keys as described next.

B. Group Key Generation

Now we derive the shared group key from the pairwise keys generated in the previous section. Group key is generated on an equal contribution basis from each and every legitimate node of the group. The unauthenticated group key agreement based on the Diffie-Hellman (DH) key agreement is used as primitive to the group key scheme like in [13], [14], [12], [15]. Suppose N denote the total number of devices including the HAN smart meter interface. Let G_k be the group key for the HAN. The gateway will first generate a symmetric key with each and every device in the HAN as described in the previous section. Then the gateway will aggregate all the symmetric keys in one common group key as follows:

$$\begin{aligned} G_k &= K_{gw}^1 K_{gw}^2 K_{gw}^3 \dots K_{gw}^N \\ &= a^{x_1 x_{gw}} a^{x_2 x_{gw}} \dots a^{x_N x_{gw}} \\ &= a^{x_1 x_{gw} + x_2 x_{gw} + \dots + x_N x_{gw}} \\ &= a^{(x_1 + x_2 + x_3 + \dots + x_N) x_{gw}} \end{aligned}$$

After that the gateway will use the individually shared secret key to encrypt the group key and unicast the message: $mess_i = E_{K_{gw}^i}(G_k)$ to each corresponding device i in the HAN including the smart meter HAN interface.

C. Key Update/Renewal

One of the important key management requirements that arise after a network has been deployed is forward security [16], i.e., if a node is captured and its secret material compromised, an attacker should not be able to decrypt messages that were intercepted by the attacker in the past. Thus, the distributed keys need to be updated/renewed periodically.

The pairwise key can be updated very often with little overhead as follows: when two parties exchange an encrypted message using the j^{th} version of the key K_j, they replace their key K_j by $K_{j+1} = H(K_j)$, and destroy K_j. H is a secure hash function. If either or both parties are compromised, the attacker only comes into possession of the most recent version of the key and is unable to compute any previous version of the key, due to the one-way property of H. This method thus satisfies the requirement of forward security and incurs very little computational overhead due to the efficiency of the hash function and no communication overhead.

The group key can be updated when any pairwise key is updated, however, it is not necessary to update the group key so frequently and it is computationally expensive. Furthermore, it may introduce synchronization issues that the end nodes may end up with different version of the group keys due to communication delay. Hence, we propose to use a timer based scheme at the gateway that determines how often the group key should be updated. When the timer expires, the gateway re-compute the group key and broadcast through HAN. The value of the timer should reflect the tradeoff between security and overhead for computation and communications.

D. Key Revocation

It is not feasible to automatically detect a key compromise. This can be done only by monitoring the HAN for suspicious behavior. Two possible cases of key compromise can occur. Either the group key or pairwise keys could be captured by an attacker.

If the group key is compromised, a revocation process is initiated by the CA and the gateway securely unicast to each

and every end nodes a revocation message encrypted with the corresponding pairwise keys. The format of the message is $message_i = E_{K^i_{gw}}(text)$.

If pairwise keys are compromised, the group key is used to encrypt and securely broadcast the revocation message to the corresponding end nodes as $message = E_{G_k}(text)$.

The revocation text should clearly specify the node identification as well as the compromised key in order to prevent any possible denial of service attacks that the attacker could initiate against the HAN by resending the revocation messages. In the rare case that both the group key and some of the pairwise keys are compromised, the gateway and the end nodes need to reboot and start the process given in Section III-A and III-B.

IV. Security Analysis

A. Authentication

In the symmetric key agreement scheme, the gateway and a neighboring node select two random numbers x_{gw} and x_i in the multiplicative group and create two public keys X_{gw} and X_i per DH scheme. A node that had not been loaded with the group parameters will not be able to generate an acceptable public key giving the hard discrete logarithm problem in the multiplicative group. This provides the means to authenticate the node that seek an agreement with the gateway.

B. Integrity

In the symmetric key agreement two devices compute their hash values (h_{gw}, h_i) of the key concatenated to their respective identification, where $h_{gw} = H(ID_{gw}|X_{gw})$, $h_i = H(ID_i|X_i)$. They then send to each other the messages (m_{gw}, m_i) made of a concatenation of their respective hash value, public key and identification, where $m_{gw} = h_{gw}|ID_{gw}|X_{gw}$, and $m_i = h_i|ID_i|X_i$. Both devices re-compute the hash values. They validate the integrity of the message if and only if the new hash value matches the values received in the messages. As such, the integrity of the public key exchange is ensured.

The procedure is repeated during the computation of the shared key. Each device compute the symmetric key (K^i_{gw}, K^{gw}_i) using the public key (X_{gw}, X_i) received in the above message as follow: $K^i_{gw} = X_i^{x_{gw}}$, $K^{gw}_i = X^{x_i}_{gw}$ and sent to each other the messages $(mess_{gw}, mess_i)$ containing the hash values of their respective key with their identification. They both re-compute the hash value and confirm the message's integrity and validate the symmetric key.

C. Privacy

The gateway proceeds the same way with all the devices in the HAN and generates the group key as described earlier. Each end node only knows its own pairwise symmetric key and cannot deduce other's symmetric key, although they share the same group key. The group key will only be used by every device to encrypt any broadcasting messages within the HAN, thus ensure the privacy of each end node in the HAN.

V. Related Work and Performance Comparison

There are several official documents regarding the security requirements of AMI, e.g., [1], [3], [11]. These documents identify key distribution and management as a critical step for securing AMI. In the academic literature, there are a couple of works on the authentication, data integrity and key management in AMI. In [4], the authors propose an in-network collaborative scheme to secure the data integrity and authentication using cryptographic keys established in the mutual authentications. In [6], the authors use information theory cryptography to provide data security through a novel scheme based on unconditionally secure authentication codes (A-codes) having short authenticators. These works mostly concern the authentication in HAN rather than key distribution and management. The smart metering privacy issue is addressed in [17] by anonymizing the identity of high-frequency metering data through an escrow service.

An authentication and key establishment mechanism for HAN is proposed in [5], which is based on Elliptic Curve Cryptography (ECC) and self-certified public key technique incorporating self-certificate. The Elliptic Curve Cryptography is used as a primitive for the encryption. This is an asymmetric key scheme with the natural advantage to be robust against impersonation attack. It also has the advantage of using a much lower encryption key length to provide an equivalent security result as compare to the public-key encryption. We will compare our proposed scheme with that in [5].

Here we analyze our proposed scheme in terms of the computational and storage overhead. As for storage, each and every end node is loaded with its identification (ID), the multiplicative group parameter (Z^*_q, q, a) and the hash function H. With MD5 as hash function and 128 bits for each element of the multiplicative group as well as the identification, the whole storage requirement will not exceed 1M bits.

As for computation, it mainly emphasizes on evaluating the encryption, decryption and hash function operations in the pairwise key agreement and group key derivation. The computation performance on per node basis as compared with SE-HAN in [5] are shown in Table I. We also calculated the round complexity, where defined as the number of message exchanged. The round complexity of the proposed protocol is 4 (see Table I). It can be seen that our proposed scheme performs better in terms of the computational and storage overhead. Furthermore, in this paper, we provide detailed procedures on key renewal and key revocation, which are not discussed in [5].

TABLE I
Performance evaluation comparison

	Sym Key Enc	Sym Key Dec	Public Key Enc	Public Key Dec	Hash	Comm
$SE-HAN$ [5]	1	1	0	0	6	6
$Proposed$	1	1	0	0	4	4

VI. Conclusions and Future Work

A light-weight key distribution and management scheme is proposed for the Home Area Network (HAN), which is one of the key component in the communication infrastructure of the Advance Metering Infrastructure (AMI). The scheme is shown to provide the integrity, privacy and authenticity in the HAN, without which the trustworthiness of the AMI will be questionable to every user of the grid. Although the proposed scheme targets the HAN, similar methodology may be extended to the remaining part of the AMI, and this will be our next effort.

VII. Acknowledgment

The first author is supported by the HBGI Scholarship. This research work is supported in part by NSF under CNS-1040207 and the DOE Sam Massie Chair Program.

References

[1] *Smart Grid Website*. US Department of Energy. [Online]. Available: http://www.oe.energy.gov/smartgrid.htm

[2] *Smart Grid System Report*. US Department of Energy, July 2009. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/SGSRMain_090707_lowres.pdf

[3] *AMI System Security Requirements*. AMI-SEC Task Force, Dec. 2008. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/14-AMI_System_Security_Requirements.pdf

[4] Y. Yan, Y. Qian, and H. Sharif, "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid," in *IEEE Wireless Communications and Networking Conference (WCNC)*, march 2011, pp. 909 –914.

[5] B. Vaidya, D. Makrakis, and T. Hussein, "Device authentication for smart energy home area networks," in *IEEE International Conference on Consumer Electronics*, 2011.

[6] T. Matsumoto, T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, "Information-theoretic approach to authentication codes for power system communications," in *IEEE Transmission and Distribution Conference and Exposition*, 2010.

[7] F. Mueller, S. Bhattacharya, and C. Zimme, "Cyber security for power grids," in *NCSU Security Open Systems Initiative*, 2008.

[8] A. Bose, "Smart transmission grid. applications and their supporting infrastructure," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, june 2010.

[9] Z. Fan, G. Kalogridis, C. Efthymiou, M. Sooriyabandara, M. Serizawa, and J. McGeehan, "The new frontier of communications research: smart grid and smart metering," in *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking*, ser. e-Energy '10. New York, NY, USA: ACM, 2010, pp. 115–118. [Online]. Available: http://doi.acm.org/10.1145/1791314.1791331

[10] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security and Privacy*, vol. 7, no. 3, pp. 75 –77, may-june 2009.

[11] *Advanced Metering Infrastructure Security Considerations*. Sandia National Lab, 2007. [Online]. Available: http://www.oe.energy.gov/DocumentsandMedia/20-AMI_Security_Considerations.pdf

[12] W. Stallings, *Cryptography and Network Security: Principles and Practices (4th Ed)*. Prentice-Hall, 2006.

[13] M. Lu, S. Yu, W. Lou, and K. Ren, "Group device pairing based security sensor association and key management for body area networks," in *IEEE INFOCOM*, 2010.

[14] D. Stinson, *Cryptography: theory and practice (Discrete Mathematics and its Applications)*. CRC Press, 1995.

[15] A. Metke and R. Ekl, "Security technology for smart grid networks," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 99 –107, june 2010.

[16] C. Gunter, "An identity-based key-exchange protocol," in *EUROCRYPT*, J.-J. Quisquater and J. Vandewalle, Eds. Springer, 1989, vol. LNCS 434, pp. 29 – 37.

[17] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *First IEEE International Conference on Smart Grid Communications (SmartGridComm)*, oct. 2010, pp. 238 – 243.