Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 149649, 9 pages
http://dx.doi.org/10.1155/2014/149649

Research Article

Two-Dimensional Key Table-Based Group Key Distribution in Advanced Metering Infrastructure

Woong Go[1] and Jin Kawk[2]

[1] *ISAA Lab, Department of Information Security Engineering, Soonchunhyang University, Eumnae-ri, Shinchang-Myeon, Asan-si, Chungcheongnam-do 336-745, Republic of Korea*
[2] *Department of Information Security Engineering, Soonchunhyang University, Eumnae-ri, Shinchang-Myeon, Asan-si, Chungcheongnam-do 336-745, Republic of Korea*

Correspondence should be addressed to Jin Kawk; jkwak@sch.ac.kr

Received 13 November 2013; Accepted 21 January 2014; Published 14 May 2014

Academic Editor: Jongsung Kim

A smart grid provides two-way communication by using the information and communication technology. In order to establish two-way communication, the advanced metering infrastructure (AMI) is used in the smart grid as the core infrastructure. This infrastructure consists of smart meters, data collection units, maintenance data management systems, and so on. However, potential security problems of the AMI increase owing to the application of the public network. This is because the transmitted information is electricity consumption data for charging. Thus, in order to establish a secure connection to transmit electricity consumption data, encryption is necessary, for which key distribution is required. Further, a group key is more efficient than a pairwise key in the hierarchical structure of the AMI. Therefore, we propose a group key distribution scheme using a two-dimensional key table through the analysis result of the sensor network group key distribution scheme. The proposed scheme has three phases: group key predistribution, selection of group key generation element, and generation of group key.

1. Introduction

A smart grid is a digitally enabled electrical grid that gathers, distributes, and acts on information about the behavior of all participants (suppliers and consumers) in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. The smart grid is a new generation grid system that efficiently manages electricity consumption using two-way communication between users and power companies. Thus, users can check their electricity consumption in real time, and power companies can efficiently control the generation and supply of electricity. In order to achieve two-way communication, the advanced metering infrastructure (AMI) is used in the smart grid as a core infrastructure. This infrastructure consists of smart meters, data collection units (DCU), maintenance data management systems (MDMS), and so on [1–3].

However, the potential security problems of the AMI increase owing to the application of the public network. In particular, if the electricity consumption data is modified or exposed, it will lead to critical security problems because electricity consumption data is important information for charging. Thus, encryption is required for secure transmission of data. In addition, a key management and distribution scheme is needed for encryption [4, 5].

There are many devices and hierarchical structures for an AMI environment. If AMI uses a pairwise key for each device, the DCU and higher-level devices will be managing multiple keys. Therefore, the group key distribution scheme is more efficient than pairwise key distribution [3].

Therefore, we propose a two-dimensional key table-based group key distribution in AMI. The proposed scheme has three phases: key table predistribution, selection of group key generation element, and generation of group key. During the key table predistribution phase, the power company directs an input key table to the secure memory of the DCU and smart meter. Thus, the key table is not transmitted via the public network. During the selection of group key generation element phase, the DCU and smart meter select a group key

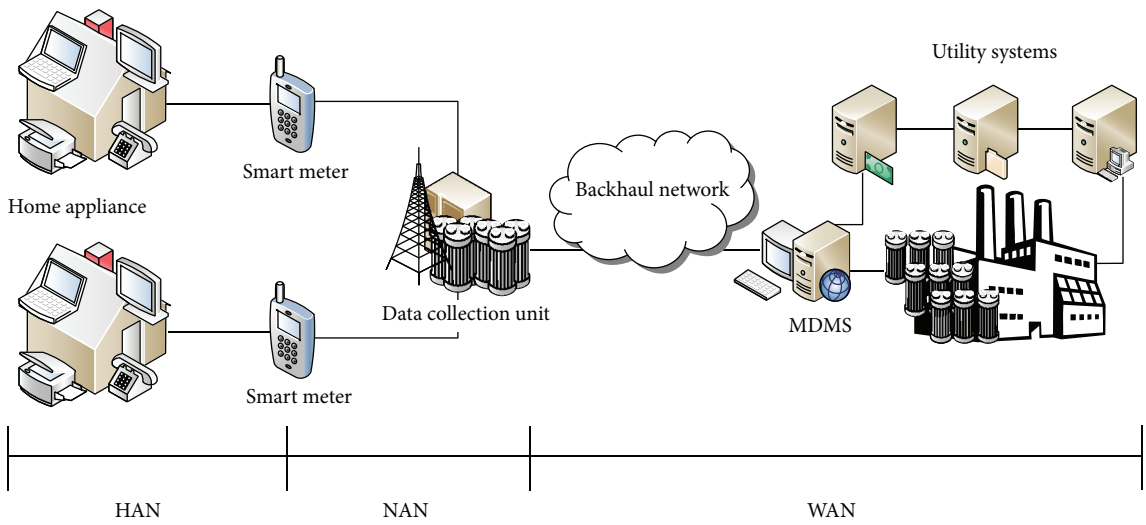


Figure 1: Overview of AMI structure.

generation element using the location information. Finally, the DCU and smart meter generate a group key using the group key generation element during the generation of group key phase.

The remainder of this paper is organized as follows. Section 2 describes the AMI infrastructure and analyzes previous studies of key distributions in AMI. In Section 3, we present our proposed two-dimensional key table-based group key distribution. Section 4 compares our proposed scheme with existing schemes. Finally, Section 5 concludes this paper.

2. Related Work

2.1. Advanced Metering Infrastructure. AMI are systems that measure, collect, and analyze energy usage and communicate with metering devices such as electricity meters, gas meters, heat meters, and water meters, either on request or on a schedule [6]. Figure 1 presents the basic AMI architecture.

This system provides two-way electric communication between users and power companies, and the core technology is based on a smart meter for realizing the demand response mechanism. AMI architecture has three fields of networks: home area network (HAN), neighborhood area network (NAN), and wide area network (WAN) [6].

(i) HAN. A HAN is a dedicated network that connects devices at home, such as displays, load-control devices, and home appliances, seamlessly into the overall smart metering system. It also contains turnkey reference designs of systems to monitor and control these networks. Home area networks are required in the user domain to monitor and control smart devices in the user premises and to implement new functionalities. Within the user premises, a secure two-way communication interface called energy services interface (ESI) acts as an interface between the utility system and the user [7, 8].

(ii) NAN. In smart grid applications, the cognitive NAN collects power consumption information from households in a neighborhood and delivers them to a utility company through either open or private wide area networks. NANs typically comprise multiple utility meters, each of which is installed on or outside a house [7, 9].

(iii) WAN. Wide area networks form the communication backbone to connect highly distributed smaller area networks that serve power systems at different locations. When control centers are located far from the substations or end consumers, real-time measurements taken by the electric devices are transferred to the control centers through the wide area networks. Conversely, the wide area networks undertake the instruction communications from control centers to the electric devices [7, 8].

2.2. Group Key Distribution

2.2.1. Kamto et al.'s Scheme. In 2011, Kamto et al. [10] proposed lightweight key distribution and management for AMI (see Figure 2). The proposed scheme focuses on HAN and designs a group ID-based mechanism to establish both the pairwise and group keys with a small overhead. The notations of Kamto et al.'s scheme [10] are as in Table 1.

However, this scheme is vulnerable to a man-in-the-middle (MITM) attack. In the first transmission in this scheme, the gateway sends m_{gw} in plaintext. In addition, Node I sends m_i in plaintext. If an attacker eavesdrops on a data transmission, he/she can identify IDs, ID_{gw}, and ID_i, the public keys X_{gw}, X_i, and the hash data h_{gw}, h_i. Furthermore, an attacker can generate new transmitted data $m_{ia} = h_{ia} \mid ID_{ia} \mid X_{ia}$ and $m_{gwa} = h_{gwa} \mid ID_{gwa} \mid X_{gwa}$ (a = attacker) and send these messages to both entities. Then, each entity verifies the attacker's hash data and accepts him/her, as this message does not include any identification element of the other entity. This means that an attacker can generate the symmetric keys K^i_{gwa}, K^{ia}_{gw}. Thus, this scheme has problems of the MITM attack.

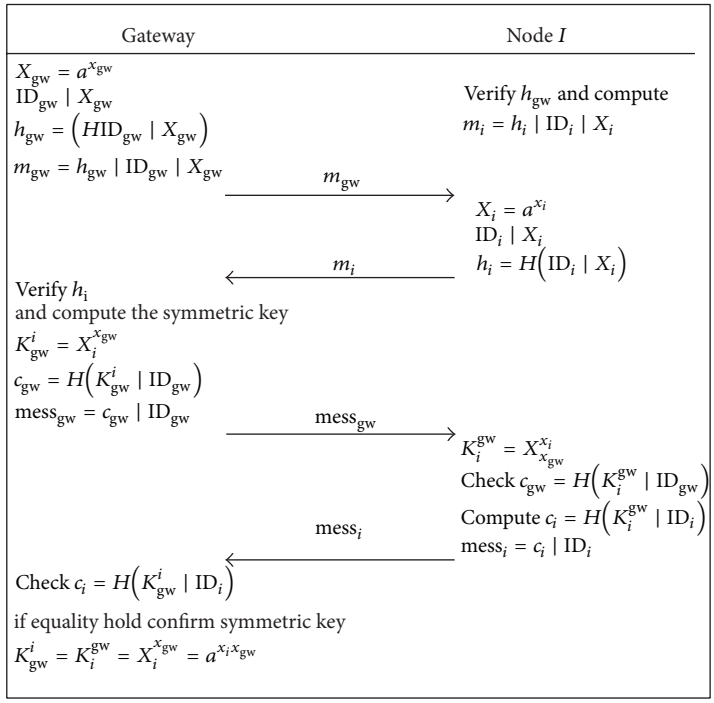


Figure 2: Kamto et al.'s proposed protocol.

Table 1: Notations used in Kamto et al.'s scheme [10].

Notation	Description
$H(m)$	Hash value of m
K_q^*	Multiplicative group
a	Primitive roots of q
i	Node
x_i	Security value of node
$E_k(m)$	Message encryption using key k
q	Prime number, prime order of K_q^*
gw	Gateway
x_{gw}	Security value of gateway
ID_*	ID of $*$ ($*$ = gw, i)

Table 2: Notations used in Xia and Wang's scheme [11].

Notation	Description
TA	Trust third party
S	Service provider
x	Random nonce (security key, $x \in z_q^*$)
$\varepsilon(\cdot), D(\cdot)$	Symmetric key encryption algorithm
k_i	Security key ($H_1 = ID_i^x \bmod p$)
f	Pseudorandom generation function (PRF)
M	Smart meter
p, q	Prime number ($p = 2q + 1$)
ID_m, ID_s	ID of smart meter and service provider
H_n	Hash function ($n = 1, 2$)
$r \leftarrow R_k$	Input randomly k-bit to r

2.2.2. Xia and Wang's Scheme. Xia and Wang [11] analyzed the key management scheme proposed by Wu-Zhou and showed that it is vulnerable to an MITM attack. Then, Xia and Wang [11] proposed a new key distribution protocol and demonstrated that it is secure and efficient for a smart grid network (see Figure 3).

Their proposed scheme has three entities: service provider, smart meter, and trusted third party. The service provider manages electricity and sends electrical signals to the smart meter. When the smart meter receives electrical signals, it authenticates and responds to these electric signals. The trusted third party manages key distribution between the service provider and the smart meter. In order to generate a security key for all entities, the trusted third party uses the master key and hash function. The trusted third party selects large primes p, q and a random nonce x (master key). Further, the supposed security key is stored in a tamper-proof memory and the smart meter gathers data using sensors that are located at home [11].

The notations of Xia and Wang's scheme [11] are as in Table 2.

3. Proposed Scheme

3.1. Overview of Basic Structure. In this section, we propose a secure group key distribution scheme in the AMI. To achieve group key distribution between a smart meter and a DCU, our proposed scheme uses a key table. This scheme has three phases, that is, key table predistribution, selection of group key generation elements, and generation of group key phase. Figure 4 presents the basic structure of the proposed scheme.

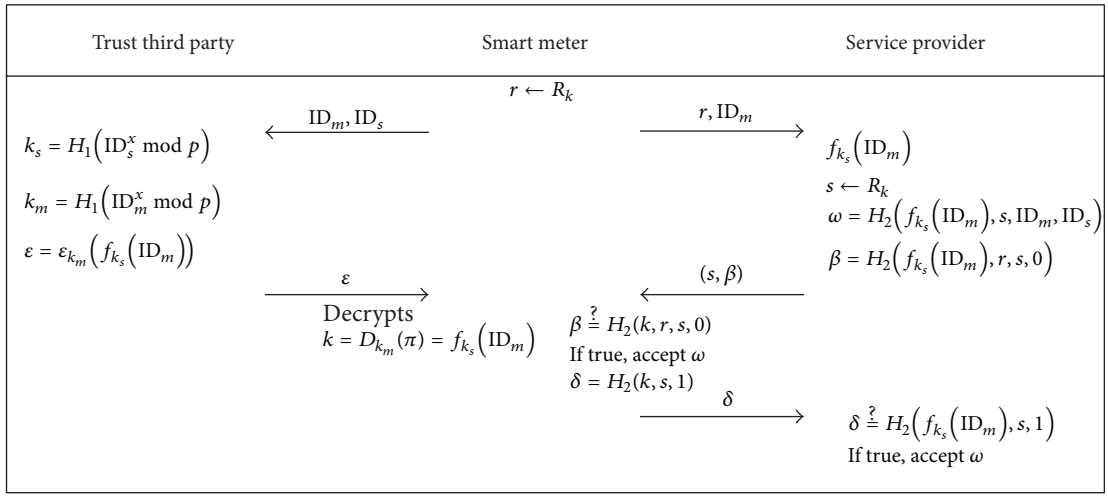


Figure 3: Xia and Wang's proposed protocol.

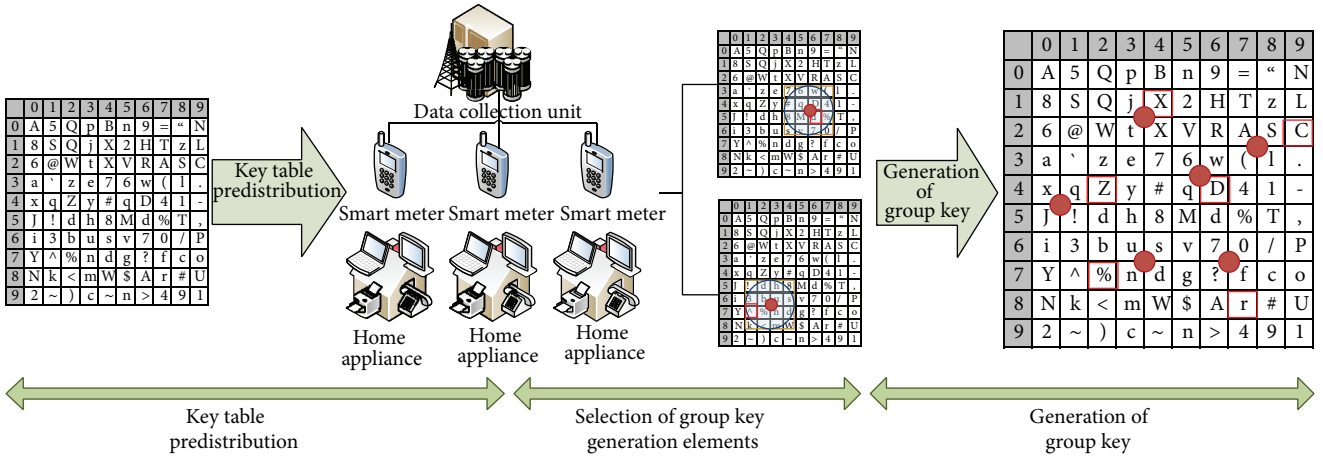


Figure 4: Basic structure of proposed scheme.

3.2. Notation. The notations in Table 3 are used throughout this paper.

3.3. Key Table Predistribution Phase. This phase is the key table predistribution step, and it operates when the power company installs a DCU and smart meter. The power company directs the input key table to the secure memory of a DCU and smart meter. Thus, the key table is not transmitted via the public network.

To generate a key table, the power company selects a pseudorandom number generator and seed value. Then, the power company generates a key table that is a two-dimensional array. This key table includes group key generation elements. Each element can be expressed by $\mathrm{KT}[i][j]$ because of the two-dimensional array, and the size of each element is 1 byte. Figure 5 shows a pseudocode to generate a key table.

(i) ArrayKT(): this function stores group key generation elements, which are generated by PRNG(·) on a two-dimensional array.

(ii) PRNG(), pseudorandom number generation: this function generates a random nonce that is used for the key table.

The size of the key table reflects the actual size of the area where a smart meter and DCU are located. To achieve this, the area is divided into a certain size and is mapped to each element of the group key generation. For example, if the area is 10 km^2 and the size of the division is 1 km^2, the total number of divided areas is 100. Thus, the key table is a 10×10 array, and a 100-byte memory is sufficient for the key table because the size of each element of the group key generation is 1 byte.

Figure 6 is an example of mapping between an actual area and a key table.

3.4. Selection of Group Key Generation Element Phase. The purpose of this phase is to select an element from the key table using the location information (coordinates) of each DCU and smart meter. Moreover, these elements are randomly selected in a valid range.

Table 3: Notations used in proposed scheme.

Notation	Description
Sn	Smart meter ($n = 1, 2, 3, \ldots, i$)
DCU	Data collection unit
PRNG(·)	Pseudorandom number generator
$H(\cdot)$	Hash function
Ex, Ey	Row (Ex) and column (Ey) in KT
Ele	Selected group key generation element ($\mathrm{DCU}_{\mathrm{Ele}}$, Sn_{Ele})
rad	Radius of circle for valid range
Sm_{Ele}	Excluded group key generation element of smart meter in $\mathrm{ALo}_{\mathrm{Ele}}$
Sn_{ID}	Smart meter ID ($n = 1, 2, 3, \ldots, i$)
KT	Key table
Seed	Seed value for PRNG(·)
Lo_*	Location of $*$ ($* = Sn$, DCU)
Sel	Function of group key generation elements ($\mathrm{DCU}_{\mathrm{Sel}}$, Sn_{Sel})
Ex_{Ele}, Ey_{Ele}	Row (Ex) and column (Ey) of group key generation element
$\mathrm{ALo}_{\mathrm{Ele}}$	Elements set of group key generation
K_g	Group key

	0	1	2	3	4	5	6	7	8	9
0	A	5	Q	p	B	n	9	=	“	N
1	8	S	Q	j	X	2	H	T	z	L
2	6	@	W	t	X	V	R	A	S	C
3	a	`	z	e	7	6	w	(	l	.
4	x	q	Z	y	#	q	D	4	1	-
5	J	!	d	h	8	M	d	%	T	,
6	i	3	b	u	s	v	7	0	/	P
7	Y	^	%	n	d	g	?	f	c	o
8	N	k	<	m	W	$	A	r	#	U
9	2	~	)	c	~	n	>	4	9	1

```
char tmp;
PRNG(Seed)
{
if tmp != NULL;
   srand(Seed);
tmp ← random();
Return tmp;
}
ArrayKT(Ex, Ey, Seed)
{
Input KT[i][j];
for i ← 1 to Ey − 1 do
   for j ← 1 to Ex − 1 do
      KT[i][j] ← CALL PRNG (Seed);
return KT;
}
```

Figure 5: Pseudocode for key table.

This phase uses two components in order to select an element: location information of the DCU and smart meter and a valid range.

(i) Location information:

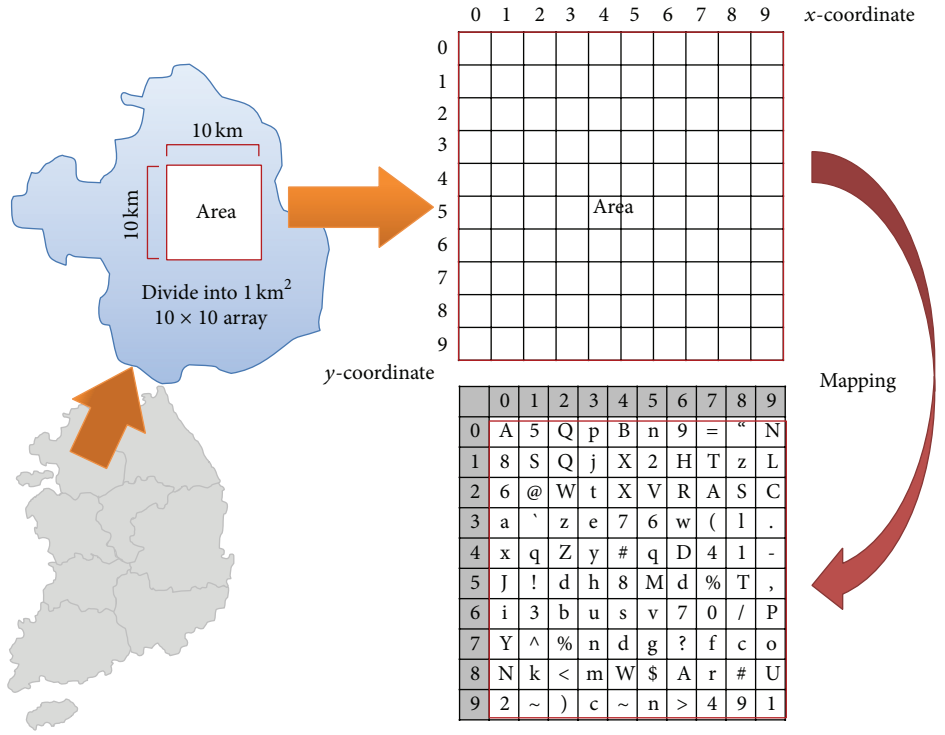
(a) coordinates of the key table;
(b) expressed by KT[x][y] ($x, y = 1, 2, 3, \ldots, n$);
(c) the same as the location of a divided block that a DCU and smart meter are installed in and the actual size of the area.

(ii) Valid range:

(a) selection range of group key generation elements;
(b) each coordinate of a DCU and smart meter is the center of a valid range;
(c) size of range is a square circumscribed about a circle with a specific radius;
(d) radius is randomly selected.

If this phase does not use a valid range, all locations are marked on the same area of the two-dimensional key table when smart meters are installed in a building. Despite the same area, the proposed scheme can select different group key generation elements because of the valid range. In addition, this valid range increases the number of cases of element that can be selected. As you can see in Figure 7, the DCU and smart meter select a different element in the valid range.

In order to select a group key generation element in a valid range, the DCU and smart meter calculate the maximum and minimum coordinates of the valid range. For this, the proposed scheme uses the exclusive-OR operation. The exclusive-OR operation facilitates the selection of a group key generation element within the limit of a valid range.



	0	1	2	3	4	5	6	7	8	9
0	A	5	Q	p	B	n	9	=	“	N
1	8	S	Q	j	X	2	H	T	z	L
2	6	@	W	t	X	V	R	A	S	C
3	a	`	z	e	7	6	w	(	l	.
4	x	q	Z	y	#	q	D	4	1	-
5	J	!	d	h	8	M	d	%	T	,
6	i	3	b	u	s	v	7	0	/	P
7	Y	^	%	n	d	g	?	f	c	o
8	N	k	<	m	W	$	A	r	#	U
9	2	~	)	c	~	n	>	4	9	1

Figure 6: Example of mapping between an actual area and a key table.

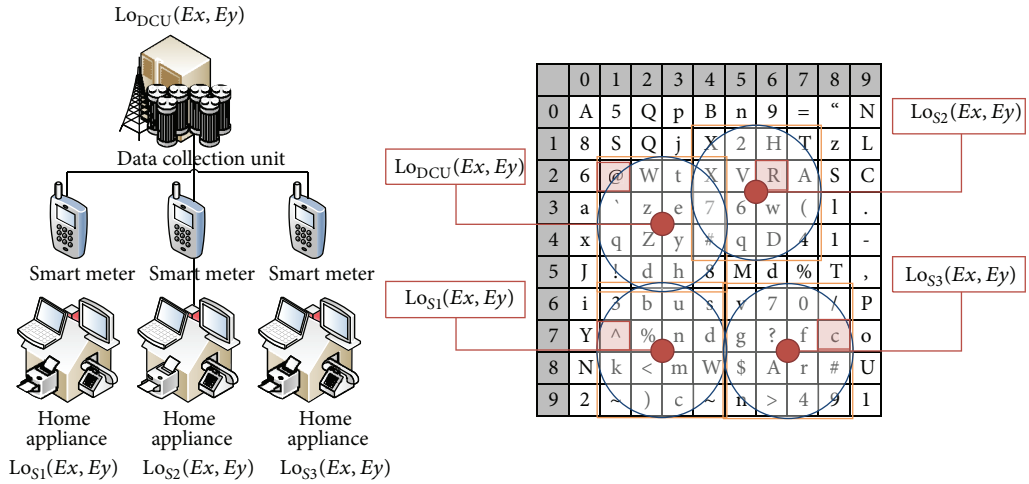


Figure 7: Selection of group key generation element.

For example, if the radius of valid range is 10, a group key generation element is selected as Algorithm 1.

If a smart meter (S1) is located at x-coordinate 50 and y-coordinate 40 in key table, it is denoted by Ex and Ey. These coordinates will be the center of a valid range. In order to select a group key generation element of $S1$ in a valid range, $S1$ calculates the coordinates of the group key generation element between the maximum and minimum coordinates of the valid range. To calculate this, the x and y coordinates are transferred to the maximum coordinates of a valid range initially. Then, subtract the specific number randomly selected between 0 and 20 (diameter of valid range) using pseudorandom number generation (PRNG(·)) from the maximum coordinate. The calculation result yields valid coordinates of the group key generation element. If the selected number is 20, the coordinates of group key generation elements equate to the minimum coordinates of the valid range. Ex_{Ele} is the x-coordinate of group key generation element and Ey_{Ele} is the y-coordinate of group key generation element.

3.5. Generation of Group Key Phase. In these phases, each DCU and smart meter generate a group key using the selected group key generation element. The group key is hash data that

Location of smart meter ($S1$)
$S1 \rightarrow \text{Lo}_{S1}(Ex, Ey) = \text{Lo}_{S1}(50, 40)$
Coordinates of $S1 \rightarrow Ex = 50, Ey = 40$

Group key generation element of $S1$ on key table
$S1_{\text{Ele}} = S1_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}}) = S1_{\text{Sel}}(Ex, Ey) = S1_{\text{Sel}}(50, 40)$
$Ex_{\text{Ele}} = (Ex + 10) - (\text{PRNG}(\cdot) \bmod 20)$
$= (50 + 10) - (\text{PRNG}(\cdot) \bmod 20)$
$Ey_{\text{Ele}} = (Ey + 10) - (\text{PRNG}(\cdot) \bmod 20)$
$= (40 + 10) - (\text{PRNG}(\cdot) \bmod 20)$

Algorithm 1: Example of selection of group key generation element.

concatenates all group key generation elements. All DCU and smart meters generate the same group key. This phase follows four steps in order to generate a group key (see Algorithm 2).

Step 1. After the selection of group key generation element, all smart meters send it to the DCU. The transmitted data consists of the smart meter ID and coordinates of the group key generation element. They do not send the value of the group key generation element. The smart meter ID is used to avoid a duplication of the element because of network latency or a replay attack and so forth.

Step 2. The DCU identifies all group key generation elements of each smart meter using the received data and coordinates Ex_{Ele} and Ey_{Ele}. Then, the DCU concatenates his group key generation element with others and generates a group key using a hash function with a concatenated element. When the generation of a group key is complete, the DCU calculates ALo_{Ele} and H_1. ALo_{Ele} is a set of coordinates of the group key generation elements, which excludes each specific smart meter that receives ALo_{Ele}. In addition, H_1 is hash data with an exclusive-OR operation performed on the group key generation element. The purpose of H_1 is to verify the integrity of each group key generation element.

Step 3. In this step, the DCU sends ALo_{Ele} and H_1 to each smart meter in order to generate the same group key.

Step 4. Each smart meter selects a group key generation element of DCU and other smart meters using ALo_{Ele}. Then, they perform an exclusive-OR operation and a hash function with their group key generation element. Finally, they compare it with the received H_1. If the result of the comparison is correct, they calculate the group key using the hash function.

4. Security Analysis

4.1. Integrity of Group Key. Kamto et al.'s scheme generates a public and private key based on the Diffie-Hellman key exchange scheme and the exchange key between a gateway and node using the exponentiation operation. They also use a hash function ($H(\cdot)$) to protect the integrity of the data transferred over the network. The data consists of the IDs of gateways and nodes ($\text{ID}_{\text{gw}}, \text{ID}_i$), the result of the exponentiation operation (X_{gw}, X_i), and the hash value of integrity verification (h_{gw}, h_i).

However, the hash value is generated using data transferred over the network ($h_{\text{gw}} = H(\text{ID}_{\text{gw}} \mid X_{\text{gw}})$, $h_i = H(\text{ID}_i \mid X_i)$). Therefore, it cannot guarantee the integrity of the data, because anyone can generate a hash value (h_{gw}, h_i) using the data transferred over the network.

In the proposed scheme, when the DCU sends a set of group key generation elements (ALo_{Ele}) and a hash value (H_1) to each smart meter, the DCU does not send any information to generate the hash value (H_1). The transmitted data consists of coordinates of group key generation elements and the ID of a smart meter. Thus, an attacker who does not have a valid key table cannot generate a hash value (H_1) (see Table 4).

If an attacker changes the group key generation element of a smart meter, the smart meter can verify the modification. For example, the data integrity verification of the smart meter ($S1_{\text{ID}}$) is as follows:

(i) attacker (A):

(a) data eavesdropping: $S1_{\text{ID}} \parallel Ex_{\text{Ele}} \parallel Ey_{\text{Ele}}$;
(b) changing coordinates of the group key generation element: $S1_{\text{ID}} \parallel \underline{Ex_{\text{EleA}}} \parallel \underline{Ey_{\text{EleA}}}$;

(ii) DCU:

(a) select the group key generation element and generation group key: K_g

$$K_g = H(\text{DCU}_{\text{Ele}} \parallel \underline{S1_{\text{EleA}}} \parallel S2_{\text{Ele}} \parallel S3_{\text{Ele}} \parallel \ldots Sn_{\text{Ele}});$$

(b) generate the hash value and a set of group key generation elements: $H_1, \text{ALo}_{\text{Ele}}$;

(1) $H_1 = H(\text{DCU}_{\text{Ele}} \oplus \underline{S1_{\text{EleA}}} \oplus S2_{\text{Ele}} \oplus S3_{\text{Ele}} \oplus \cdots \oplus Sn_{\text{Ele}})$;
(2) $\text{ALo}_{\text{Ele}} = \text{DCU}_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}}) \parallel S2_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}}) \parallel S3_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}}) \parallel S4_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}}) \parallel \cdots \parallel Sn_{\text{Ele}}(Ex_{\text{Ele}}, Ey_{\text{Ele}})$ (Exclude $S1_{\text{Ele}}$);

(c) send to smart meter ($S1_{\text{ID}}$): $H_1 \parallel \text{ALo}_{\text{Ele}}$;

(iii) smart meter:

(a) select the group key generation element using ALo_{Ele};
(b) generate and compare the hash value with the group key generation element of $S1_{\text{ID}}$;

(1) $H_1' = \text{DCU}_{\text{Ele}} \oplus S1_{\text{Ele}} \oplus S2_{\text{Ele}} \oplus S3_{\text{Ele}} \oplus \cdots \oplus Sn_{\text{Ele}}$;
(2) $H_1' \neq H_1$;

(c) result of comparison is incorrect.

Step 1. DCU ← Smart meter (Sn)
$Sn_{\mathrm{ID}n} \parallel Ex_{\mathrm{Ele}} \parallel Ey_{\mathrm{Ele}}$ $(n = 1, 2, 3, \ldots, n)$

Step 2. DCU
Duplicate check for smart meter $Sn_{\mathrm{ID}n}$
Select group key generation element
$\{S1_{\mathrm{Ele}}, S2_{\mathrm{Ele}}, S3_{\mathrm{Ele}}, \ldots, Sn_{\mathrm{Ele}}\} \leftarrow \{S1_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), S2_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), S3_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), \ldots, Sn_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}})\}$
Generate group key
$K_g = H(\mathrm{DCU}_{\mathrm{Ele}} \parallel S1_{\mathrm{Ele}} \parallel S2_{\mathrm{Ele}} \parallel S3_{\mathrm{Ele}} \parallel \cdots \parallel Sn_{\mathrm{Ele}})$
Generate hash data to verify integrity
$H_1 = H(\mathrm{DCU}_{\mathrm{Ele}} \oplus S1_{\mathrm{Ele}} \oplus S2_{\mathrm{Ele}} \oplus S3_{\mathrm{Ele}} \oplus \cdots \oplus Sn_{\mathrm{Ele}})$
Caculate $\mathrm{ALo}_{\mathrm{Ele}}$ (exclude $Sm_{\mathrm{Ele}}(Ex, Ey)$) $(m = 1, 2, 3, \ldots, n)$
$\mathrm{ALo}_{\mathrm{Ele}} = (\mathrm{DCU}_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}) \parallel S1_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}) \parallel S2_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}) \parallel \cdots \parallel Sn_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}})) - Sm_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}})$

Step 3. Smart meter (Sn) ← DCU
$H_1 \parallel \mathrm{Alo}_{\mathrm{Ele}}$

Step 4. Smart meter (Sn)
Select group key generation element
$\{\mathrm{DCU}_{\mathrm{Ele}}, S1_{\mathrm{Ele}}, S2_{\mathrm{Ele}}, \ldots, Sn_{\mathrm{Ele}}\} \leftarrow \{\mathrm{DCU}_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), S1_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), S2_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}}), \ldots, Sn_{\mathrm{Ele}}(Ex_{\mathrm{Ele}}, Ey_{\mathrm{Ele}})\}$
Generate and compare hash data
$H_1' = H(\mathrm{DCU}_{\mathrm{Ele}} \oplus S1_{\mathrm{Ele}} \oplus S2_{\mathrm{Ele}} \oplus S3_{\mathrm{Ele}} \oplus \cdots \oplus Sn_{\mathrm{Ele}})$
$H_1' \stackrel{?}{=} H_1$
If result of comaprison is correct,
$K_g = H(\mathrm{DCU}_{\mathrm{Ele}} \parallel S1_{\mathrm{Ele}} \parallel S2_{\mathrm{Ele}} \parallel S3_{\mathrm{Ele}} \parallel \cdots \parallel Sn_{\mathrm{Ele}})$

Algorithm 2: Generation of group key.

Table 4: Comparison with existing scheme and proposed scheme.

	[10]'s scheme		[11]'s scheme		Proposed scheme	
Methodology	Diffie-Hellman based group key distribution		Trust third party based group key distribution		Key table-based group key distribution	
Integrity of group key	X	Vulnerable of man-in-the-middle attack	O	Trust third party verify security key	O	Each smart meter can verify Integrity of group key
Confidentiality of group key	O	Hash function and Exponentiation	X	Session key can be calculated by user information	O	The group key and group key generation element do not send over the network.

4.2. Confidentiality of Group Key. Xia and Wang's scheme claims that the session key is secure because only TA knows the prime number (p) and master key (x). Thus, if an attacker know the user's secret key (k_i, $i = m, s$), he cannot calculate the session key because of the discrete mathematics problem. In fact, an attacker can calculate the session key when he knows a secret key and eavesdrops on a data transmission over the network.

However, our proposed scheme can provide confidentiality of the group key because this scheme does not send the group key and group key generation element. In addition, an attacker who does not possess the key table (KT) cannot identify the correct group key generation element because the transmitted data is just bit string, that is, coordinates. Moreover, an attacker cannot generate the correct group key owing to the same reason.

If an attacker eavesdrops on a set of group key generation elements ($\mathrm{ALo}_{\mathrm{Ele}}$) and hash value ($H_1$) when the DCU sends it to each smart meter, he cannot determine the group key (K_g). The hash value is generated by all group key generation elements. These elements are calculated by exclusive-OR operations. It is difficult to determine the group key generation element owing to the characteristics of the hash function. Thus, an attacker cannot generate a valid hash value. As noted above, a set of group key generation elements ($\mathrm{ALo}_{\mathrm{Ele}}$) consists of coordinates of each smart meter's group key generation element from the key table. Thus, an attacker cannot determine the group key generation element without the key table (KT), and he cannot generate the group key (K_g) (see Table 4).

5. Conclusion

Recently, smart grid systems have been widely considered as fundamental components for improving the monitoring and control of a power distribution infrastructure. In order to manage and facilitate two-way communication, the AMI

is used in smart grids as the core infrastructure. However, the potential security problems of the AMI increase owing to the application of the public network. In particular, if the electricity consumption data is modified or exposed, it can result in critical security problems owing to the important information for charging. Thus, encryption is needed to secure this transmission. Moreover, a key management and distribution scheme is required to aid encryption. Further, if AMI uses a pairwise key for each device, the DCU and higher-level devices will have to manage multiple keys. Because the AMI has many devices and a hierarchical structure, the group key distribution scheme is more efficient than pairwise key distribution. Therefore, many studies on smart grids are being conducted to efficiently manage power distribution globally.

Therefore, we proposed a two-dimensional key table-based group key distribution in AMI. The proposed scheme has three phases: key table predistribution, selection of group key generation element, and generation of group key. These phases manage keys efficiently and provide data security. Therefore, the proposed scheme is expected to improve data security.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (MSIP) (no. NRF-2012R1A2A2A01010886). This work was supported by the Soonchunhyang University Research Fund.

References

[1] W. Go and J. Kwak, "Privacy-enhanced secure data transaction system for smart grid," *International Journal of Security and Its Applications*, vol. 6, pp. 37–44, 2013.

[2] S. M. Dragan, Z. Dejan, B. Irina, P. Ranko, and C. Dragan, "Smart power grid and cloud computing," *Renewable and Sustainable Energy Reviews*, vol. 24, pp. 566–577, 2013.

[3] M. P. McHenry, "Technical and governance considerations for advanced metering infrastructure/smart meters: technology, security, uncertainty, costs, benefits, and risks," *Energy Policy*, vol. 59, pp. 834–842, 2013.

[4] G. Chen, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: a hybrid approach based on complex networks," *Physica A*, vol. 389, no. 3, pp. 595–603, 2010.

[5] Y. Wang, D. Ruan, D. Gu et al., "Analysis of smart grid security standards," in *Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE '11)*, vol. 4, pp. 697–701, June 2011.

[6] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews*, vol. 15, no. 6, pp. 2736–2742, 2011.

[7] H. K. Reduan and Y. K. Jamil, "A comprehensive review of the application characteristics and traffic requirements of a smart grid communications network," *Computer Networks*, vol. 57, pp. 825–845, 2013.

[8] W. Wang, Y. Xu, and M. Khanna, "A survey on the communication architectures in smart grid," *Computer Networks*, vol. 55, no. 15, pp. 3604–3629, 2011.

[9] R. Yu, Y. Zhang, and Y. Chen, "Hybrid spectrum access in cognitive neighborhood area networks in the smart grid," in *Wireless Communications and Networking Conference*, pp. 1478–1483, 2012.

[10] J. Kamto, L. Qian, J. Fuller, and J. Attia, "Light-weight key distribution and management for advanced metering infrastructure," in *Proceedings of the IEEE GLOBECOM Workshops*, pp. 1216–1220, December 2011.

[11] J. Xia and Y. Wang, "Secure key distribution for the smart grid," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437–1443, 2013.