A Method of Detecting the Manipulation Message to Provide a Reliable Demand Response Service

Sun-Hee Han*, Min-Woo Park*, Tai-Myoung Chung**
*Department of Electrical and Computer Engineering, Sungkyunkwan University**
*School of Information Communication Engineering, Sungkyunkwan University***
Suwon, Gyeonggi-do, Republic of Korea
{shhan, mwpark}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

***Abstract*—Customers can adjust their own energy usage if the smart grid notifies real-time energy rate which is determined by the current power consumptions. We call these services Demand Response (DR) services. At the Smart Grid environments, consumers can bi-directionally communicate with components of the smart grid through the Advanced Metering Infrastructure (AMI). So the smart gird can provide Demand Response services for reducing energy usage during hours of peak demand. However Demand Response services can be misused if messages between customers and the smart grid are modified by attackers. In this paper, we propose a method to detect the manipulation of message, while the meter reading value is being transferred from Smart Meter to Meter Data Management System (MDMS) through the AMI. It is expected to provide a reliable Demand Response service, and lead to more efficient power usage, through the detecting scheme of this paper.**

Keywords— AMI, Demand Response, Cumulative hashed value, Manipulation of Message

I. INTRODUCTION

The Smart Grid is an 'intelligent electric power network' that transmits and distributes optimal power from suppliers to consumers using information and communication technology. [1]. The Smart Grid enables interactions between suppliers and consumers by bi-directional communication, and it is provided by Advanced Metering Infrastructure (AMI).

An electric power company can measure, collect, and analyze smart meter usage statistics wireless through AMI network. AMI is an infrastructure which is advanced from Automatic Meter Reading (AMR). It provides bi-directional communication from meter. AMI network connects smart meter to a system, and transfers metering information to consumers and service electric power company.

The AMI can provide services like billing, Demand Response (DR) and so on. Demand Response means that consumers use electricity by checking their daily consumption pattern offered by their local electric power company. Demand response can inform consumers the consumption level and price by collecting and analyzing through AMI network that can do bi-directional communication. Ultimately, Demand Response can cut costs for securing generation assets for Peak Demand, and prepare for emergencies such as blackouts[6]. However, there is a threat that an attacker can manipulate measured consumption level. Also, the attacker can make a system unable to reduce power load to stop the consumer who is participating in incentive-based DR from getting incentives[2]. Thus, this paper suggests how to block the attacks that can occur when an electric power company provides Demand Response service.

This paper is organized as follows: Section II explains about Demand Response and the effectiveness of Demand Response and section III describes security threats. In Section IV, we propose a method to block the attack, and we conclude this paper with future directions.

II. RELATED WORK

The AMI exchanges information through bi-directional communication in real-time. It can cut down consumer themselves consumption of electric power by providing Real-Time Pricing (RTP). This service is called Demand Response, and it provides consumers with a consumer-centered service. This Section is organized as follows: Section II-A discusses Demand Response, and Section II-B explains the effectiveness of Demand Response. Section II-C account for possible attack types when Demand Response is provided.

A. Demand Response

Demand Response collects consumption level and lets the consumers know the information, so it leads the consumers to decide their demanding time slot by themselves[3]. This Section describes the procedure of Demand Response service and the type of Demand Response service. The procedure of Demand Response is as follows:[5]

1) Procedure

- Find out the demand of consumers, through the real-time remote monitoring.
- Raise the rates by the policy when the measured demand is over than a threshold the supplier has decided.
- Provide the raised rates to the consumer in real-time.
- Decide the time when the consumer is going to use based on the real-time rates.
- The supplier makes a Load Control command, when the consumption level is high despite of the raised rates.

This Demand Response could be used in the power grid. Demand Response can provide service by incoming electric consumption and power price through remote meter reading in real-time. To provide Demand Response by collecting electricity usage, the AMI system is needed. The AMI system can measure real-time electricity usage, real-time price through bidirectional communication, and supply Demand Response by providing Real-Time Pricing (RTP). The AMI system consists of Meter Data Management System (MDMS), Automated Data Collection System (ADCS), Data Collection Unit (DCU), and Smart Meter. Explanation about a role of each device is as Table 1.

Table 1. Components of the AMI

Devices	Description
MDMS	The MDMS handles a meter reading value and manages a power resource by integrated management system
ADCS	The ADCS takes a role in collecting a meter reading value and meter reading information from a number of DCU devices periodically, and sending them to the MDMS
DCU	The DCU collects a metering value from the Smart Meter, and is placed on a telegraph pole
Smart Meter	The Smart Meter is a device to measure the amount of electricity consumption, which installed in every household. It measures and records the amount of electricity consumption of every appliance in home network

2) Type of Demand Response: Demand Response services are categorized as either price-based DR service or incentive-based DR service.

- ***Price-based DR:*** Price-based DR changes consumer's electricity consumption pattern by applying graded price[6]. Table 2 shows kinds of price-based DR.

- ***Incentive-based DR :*** Incentive-based DR is run by power supplier or electricity system operator. It recruits consumers to participate in Demand Response service and when necessary, it makes the participants to reduce the level consumption and gives them incentives in return[6]. Table 3 explains kinds of incentive-based DR.

Table 2. Price-based Demand Response

Type	Descriptions
TOU	A method to charge fixed rate by time slot
CPP	Meter rate that a supplier can apply peak premium rate when reliability problem is found in electricity system or wholesale price is sharply risen
RTP	Meter rate reflecting wholesale price in the electricity market which is decided on a real-time basis

Table 3. Incentive-based Demand Response

Type	Description
Direct Load Control	When reliability or stability problem is found, they block participants' overload remotely with a short-term notice and gives them incentives for that.
Demand Bidding	Provides incentives to the customers to reduce the electric load according to the voluntary bid based on the load reduction events
Emergency Demand Response	Provides incentives to consumers who reduced the electric load in peak periods
Capacity Market	It is similar to the concept of insurance. It can cut down a certain amount of consumption when needed

B. Effectiveness of Demand Response

Demand Response service can be an alternative to a gas thermal power plant in the peak period at low cost. According to Thomas Weisel Partners research in 2007, Demand Response service spends only about 24 million dollars to produce 1MW while the gas thermal power plant spends about 40 million dollars to get an equal amount of power. Thus, there is a 40% of cost saving effect in the peak period by Demand Response service in comparison to the gas thermal power plant.

C. Attack in Demand Response service

This Section discusses type of attack when Demand Response is provided

1) An attack making the rates set higher by manipulating consumer's consumption level to the peak.

2) An attack preventing the consumer from seeing the rates or making them unable to adjust the time he or she wants to use.

This paper proposes a method to prevent message manipulation. It is anticipated that a threat of message manipulation sent between the DCU and the ADCS in Wide Area Network (WAN) section will occur frequently. It might have a Man-in-the-Middle Attack by the malicious third-party participation between two devices, the DCU and the ADCS.

III. AN ADVANCED SCHEME TO DETECT MANIPULATED MESSAGE

A proposal method of this paper is advanced in [7]. The DCU periodically transmits the meter value collected by the Smart Meter to the ADCS. In this time, the section of the DCU and the ADCS is connected with the WAN that there is a threat to a malicious third-party intervene to the communication except two devices. In this paper, we propose a scheme for the detection of message manipulation that can

occur between those ADCS and the DCU sections as explained in Section II.D.

A. *Assumption*

- The initial value sets by the trusted administrator.
- The ADCS and the DCU is assumed trusted node.
- The cumulative hashed value is compared in an interval of a day.

B. *Manipulated Message Detection Proceeding Through Cumulative Hashed Value*

We propose a method to detect the manipulated message by accumulating and hashing between the DCU and the ADCS. Figure 1 illustrates the flow chart about the manipulated message detection procedure.

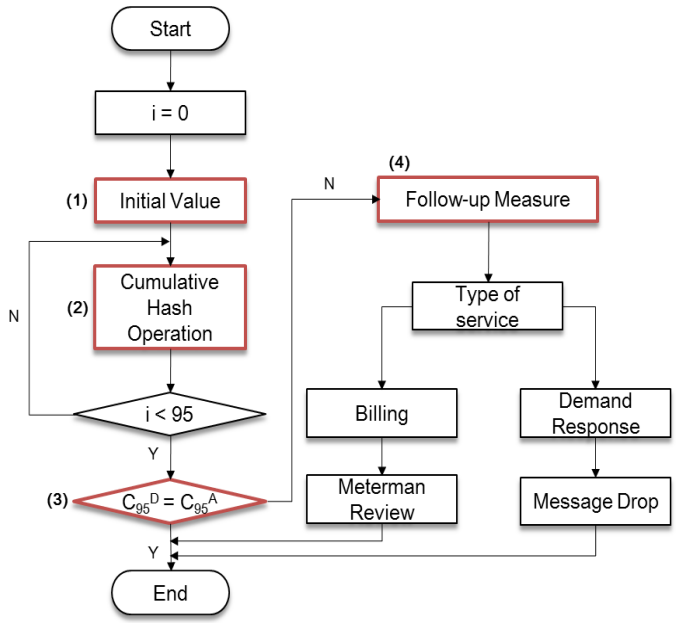

Figure 1. Flow chart for manipulated message detection

1) *Step 1 : Initial Value Setting*

The messages that are being transferred have a threat to be eavesdropped by a malicious third party in the section. If an attacker eavesdrops from the first place of the communication, the attacker can generate a random cumulative hashed value, and deceive the receiver. To avoid this attack, another shared secret key except communication message is needed. It is defined as the Initial Value (IV), and it is set by the administrator when the DCU is installed. A calculation procedure of setting the IV is as follows:

$$IV = H(device\_ID \,||\, admin\_ID) \qquad (1)$$

In this time, the hash algorithm is calculated by using the SHA-1 algorithm. A device_ID means a unique value of the device, and an admin_ID shows a unique value of the trusted administrator to the IV. Through the detection method of this paper, even if the malicious third-party manipulates massages while DCU and ADCS communicate each other, if the attacker does not know IV, the manipulated messages could be detected by the detection node.

2) *Step 2 : Cumulative Hash Operation*

The cumulative hashed value is independently stored in a send-receive device. The DCU stores all the sent messages by accumulating and hashing, and the ADCS stores all the received messages by accumulating and hashing [4]. The cumulative hashed value can be calculated by concatenating previous cumulative hashed value and by the new message. Equation (2) finds the cumulative hashed value by hash function technique. The first hashed value is calculated by concatenating the IV and the first message. This detection method prevents a malicious third party from eavesdropping in the verification process by using the IV in operation.

$$C_1 = H(M_1 \,||\, IV)$$
$$C_n = H(C_{n-1} \,||\, M_n) \; (0 \leq n \leq 94) \qquad (2)$$

The DCU transfers message to the ADCS per 15 minutes. So, the hash values of the 96 values are accumulated in a day.

Figure 2 is the process for storing cumulative hashed value in each device. The IV is the Initial Value set by an administrator. C_n^D shows the *n*th cumulative hashed value of the DCU, C_n^A shows the *n*th cumulative hashed value of the ADCS, M_n is the *n*th message of the DCU. At this point, the C_n^D and the C_n^A needs not much storage space, because it cumulatively stores the hashed value.

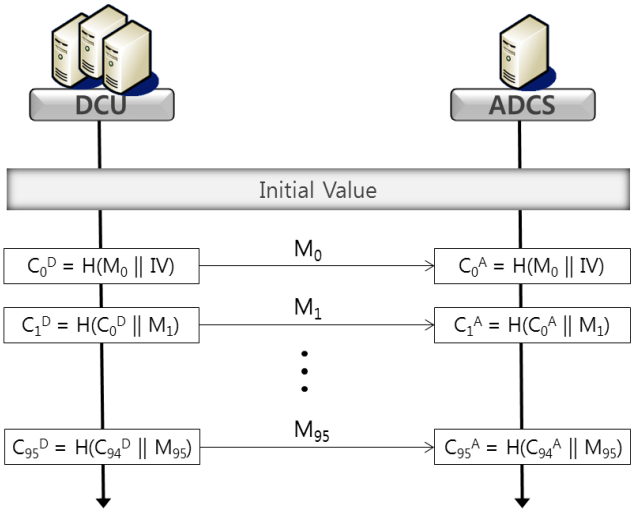

Figure 2. Cumulative hash operation

3) *Step 3 : Verification*

To detect the manipulated message by the cumulative hashed value, the verification node is needed. In this paper, we assume that the ADCS performs to verify the process. It transfers the cumulative hashed value of the DCU to the ADCS, and carries out the verifying process by Equation (3). It is the verifying process for detecting manipulated message.

$$C_n^D = C_n^A \quad (3)$$

If the above works, it could prove the message integrity, and if it does not, it becomes a modified message, and then it should take follow-up measures to get an accurate metering value.

4) Step 4 : Follow-up Measures

If the message manipulation is detected, the follow-up measures are performed depending on the type of service. If it is detected as billing service, it sends a meterman to have an accurate metering value. If it is detected as Demand Response service, it discards the message and takes a step not to influence the applicable metering value.

C. Algorithm for detecting manipulation

The Steps from Step 1 to Step 3 show the procedure to detect the manipulation of message as shown in Table 4. And the Step 4 shows the algorithm for follow-up measures, as shown in Table 5. If the 95th message of each device is the same return value is 0, if it is not, the return value is 1.

Table 4. Algorithm for manipulation message detection

Algorithm 1. detect_manipulated_msg()

```
init = strcat(admin_ID, device_ID);
IV = hash(init);
dcu = strcat(M[0], IV);
C_dcu[0]  = hash(dcu);
adcs = strcat(M[0], IV);
C_adcs[0]  = hash(adcs);

for i = 0 to i  = 94{
        C_dcu[i+1] = hash(strcat(C_dcu[i] , M[i+1]));
        C_adcs[i+1] = hash(strcat(C_adcs[i] , M[i+1]));
}

if(strcmp(C_dcu[95], C_adcs[95])){
        send the messages to MDMS;
        return 0;
}
else{
        follow_up( );
        return 1;
}
```

Table 5. Algorithm for follow-up measures

Algorithm 2. follow_up()

```
if(Demand_Rsponse){
        discard the message;
        return 0;
}
if(Billing){
        a meterman review;
        return 0;
}
```

Table 6 shows notations used in the operation.

Table 6. Notations

Notation	Description
IV	initial value provided by the administrator by the time of device installation
M_n	nth message
C_n	nth cumulative hashed value
H()	hash function using the SHA algorithm
||	concatenate the messages
C_n^D	nth cumulative hashed value of the DCU
C_n^A	nth cumulative hashed value of the ADCS

IV. CONCLUSION AND FUTURE WORKS

In this paper, we proposed a method to detect the manipulation of message when the Demand Response service is provided through the cumulative hashed value. The method proposed in this paper can detect the manipulation message by setting an Initial Value, to prevent a malicious third party from generating random hashed value. If the manipulated message is detected, it takes follow-up measures depending on billing service or Demand Response service. As a result, the provider can adjust the rates, reflecting consumer's electricity consumption, and consumers can be provided with a reliably set price. Therefore, our proposed method is expected to be able to elicit the minimum use of electricity that customer who receive price set by time-slot reduces electricity consumption. Our future works will be a study on the methods to apply these Demand Response service in the cloud computing environment. Furthermore, we will study on finding methods for consumers to decide their consuming time and to receive a reliable price by Demand Response service, when they share resources.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MKE/KEIT. [KI001810039260, Integrated dev-environment for personal, biz-customized open mobile cloud service and Collaboration tech for heterogeneous devices on server]

REFERENCES

[1] Tony Flick, Justin Morehouse, "Securing the Smart Grid : Next Generation Power Grid Security", SYNGRESS, pp. 1-18, Sep. 2010.

[2] "Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security", The Smart Grid Interoperability Panel Cyber Security Working Group, Sep. 2010.

[3] Coalton Bennett, Darren Highfill, "Networking AMI Smart Meters", IEEE Energy2030, pp.1-8, Nov. 2008.

[4] D.Liu and Q.Dong. " Detecting misused keys in wireless sensor networks", IPCCC 2007, pp272-280, Apr. 2007.

[5] Michael LeMay, Rajesh Nelli, George Gross Carl A. Gunter, "An Integrated Architecture for Demand Response Communications and Control", Proceedings of the 41st Hawaii International Conference on System Sciences, pp.174-183, Jan. 2008.

[6] Mithila Paranjpe, "Security and privacy in demand response systems in smart grid", California state university, 2010.

[7] Sun-Hee Han, Min-Woo Park, Sung-Min Jung, Tai-Myoung Chung, "The Cumulative Hash Technique for Detecting the Modification of Messages in the AMI Network", The 6th International Conference on Ubiquitous Information Technologies & Applications, pp.98-101, Dec. 2011.