Research on Direct Load Control Security Mechanism by Using NILM

Chuqi Song[1, a], Zhongwei Sun[1, b]

[1]School of Electrical and Electronic Engineering, North China Electric Power University

Beijing, China

[a]843842759@qq.com, [b]zwsun@ncepu.edu.cn

Keywords: direct load control; non-intrusive load monitoring; data encryption information security; ESAM

Abstract. Direct load control is one of the key technologies in demand response. Moreover, the security of control instruction and credibility of customers must be preserved in direct load control. Non-intrusive load control was used to simplify the process of customer credibility verification. A privacy-preserving data aggregation scheme was adopted to implement the privacy, confidentiality and integrity of power data, which based on homomorphic encryption and Chinese remainder theorem. Embedded secure access module was used to confirm the authenticity and integrity of control instruction. The proposed security scheme provides better security and lower overhead compared with exiting schemes.

Introduction

Direct load control (DLC) is a typical incentive-based demand response program. The existing privacy and security researches on DLC is mostly based on traditional cryptography methods and trusted computing [1], which is not suitable for resource-constrained smart meters or customer's gateway nodes. We found the qualities of non-intrusive load monitoring (NILM) are suitable for utility to guarantee customers credibility on DLC. NILM method has been developed maturely and the detection accuracy can reach 95%-100% [2]. By using this method, we can obtain customers' household appliance power data without intruding into the customers' house. It will simplify the process of customers' credibility verification on DLC. Researchers around the world have done a lot of work on secure data aggregation and many aggregation schemes have been proposed [3-6]. Although they had excellent performance on security, it suffered from heavy computational cost of expensive pairing operations and invalid signatures in batch verification.

System Model

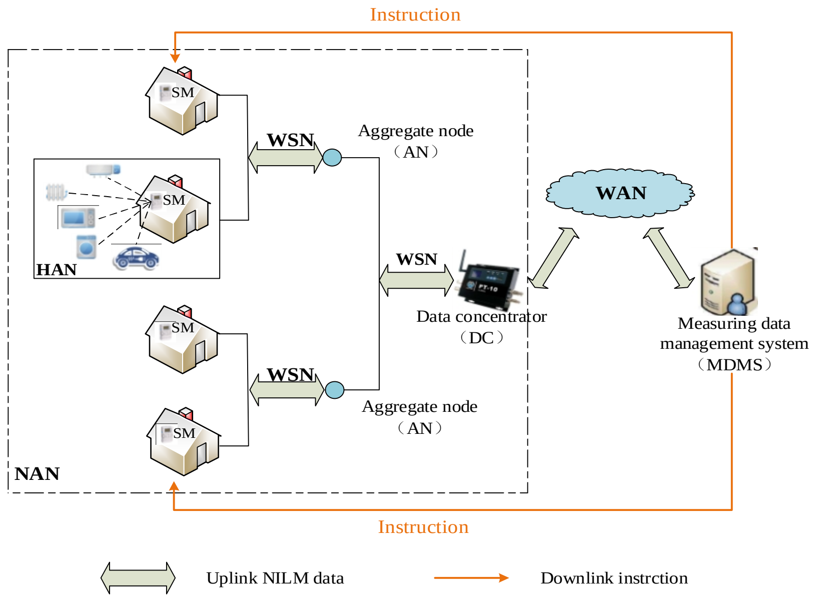

Fig. 1. Architecture of AMI

Network Model. The DR communication network is mainly divided into three parts: wide area network, neighborhood area network, and home area network. It consists of smart meter (SM), aggregation node (AN), data concentrator (DC) and measuring data management system (MDMS). The network structure is shown in Fig. 1.

SMs are deployed in each customer's home to sense and collect responsible power using data for the BS. SMs are usually small and low cost, so they are usually limited on computation, storage, and communication capability. Unlike the SM, DC can achieve the cryptographic and routing requirements of the whole WSN for its large bandwidth, strong computing capability, and sufficient memory. Generally, there are large number of SMs in a WSN, in order to reduce the communication overhead, we should select an aggregation node first to aggregate the data before transmit it to the DC. DLC instructions are directly issued by MDMS to SMs.

Security Scheme for Direct Load Control

In this section, we propose a security scheme for DLC which ensures the security of both uplink data and downlink instructions.

Security of Uplink Data. The uplink data security scheme is composed of five procedures: *Setup*, *Initial*, *Encrypt-Tag generation*, *Aggregate*, and *Decrypt-Verify*.

Table 1. Notations Used

Symbol	***Description***	***Symbol***	***Description***
DC	Data concentrator	AN$_j$	Aggregation note *j*
SM$_i$	Smart meter *i*	$m[i,k]$	substring of *m* from index *i* to *k*, e.g., m=1001_2, *m* [0,1] =10_2
$data_i$	NILM data of SM$_i$	m_i	encoded result of $data_i$
0^e	*e* serial 0 bits	l	bit-length of payload
C_i	ciphertext of m_i	T_i	Tag of $data_i$
C	aggregated ciphertext	T	aggregated tag
k_{Bi}	link key between SM$_i$ and DC	k_{Bti}	key of SM$_i$
||	concatenation	r_{tL}	low 80 bits for validate parameters for data freshness

Setup. This procedure is to prepare and install necessary secrets and figures for the DC and each SM. DC generates k_{Bi} ; selects a big prime *M* which is bigger than $2^{\left[\log_2(D_n)\right]}$, where $D_n = \max\left(data_i\right)$ and randomly select a set of prime numbers p_v, $P = \prod_{v=1}^{N} p_v$ ($P>M$).

Initial. This procedure is to encode the NILM data into one-dimensional binary code.

We assume there has *k* electric appliances, the length of the code is $l = k$. The load is a character string of 0 and 1; each bit corresponds to one load. If a bit is "1", it indicates the corresponding electric appliances is in running state; if the bit is "0", it indicates the load is in closed state.

Encrypt-Tag Generation: This procedure is triggered while a SM decides to send its coded NILM data to the AN. Detailed steps are listed as follows: SM encodes data through $m_i = data_i \,||\, 0^e$, where $e = l\left(i-1\right)$. After encoding, SM$_i$ computes:

Ciphertext:

1)where $k_{Bti} = \text{Hash}\left(k_{Bi}, t\right)$;

2) $C_i = \left(m_i + k_{Bti}\right)\left(\text{mod}\, M\right)$, $k_{Bti} \in \left[0, M-1\right]$.

Tag:

1) $e_{iv} = data_i \left(\text{mod}\, p_v\right)$;

2) $E_{civ} = e_{iv} \,||\, 0^e$;

3) $E_{ci} = \sum_{v=1}^{N} E_{civ}$;

4)Encode $T_i = \left(r_{tL} E_{ci} + k_{Bi} \right) \left(\bmod M \right)$.

c) At the end, SM*i* sends the pair $\left(C_i, T_i \right)$ to AN*j*.

Aggregate. This procedure is triggered after the AN has gathered all $\left(C_i, T_i \right)$ pairs over a period of time. Aggregation operations are given as $C = \sum_{i=1}^{n} C_i \left(\bmod M \right)$ and $T = \sum_{i=1}^{n} T_i \left(\bmod M \right)$,AN then sends the aggregated result $\left(C, T \right)$ to the DC.

Decrypt-Verify. While receiving (C,T) from AN*j*, DC can decrypt the aggregated message and verify each NILM data by $m_{sum} = \sum_{1=1}^{n} m_i = \left(C - \sum_{i=1}^{n} k_{Bti} \right) \left(\bmod M \right)$ and $data_i = m_{sum} \left[\left(i-1 \right) l, il - 1 \right]$ .DC verifies the authenticity and integrity of the decrypted data via checking whether the equation $sum = sum'$ holds or not, if the equation holds, it proves the power data hasn't been tampered.

After completing the above five procedures, the DC can perform any operations if it wants since all individual data are reverted.

Security of Downlink Instructions. The load management center uses the security mechanism between the encryption machine and the ESAM to ensure the authenticity and integrity of the instructions. We choose SM1 algorithm based on Q/GDW 365-2009 smart energy meter information exchange security certification technical specifications. During the identity authentication process, the key dispersion method is used to obtain dispersing key. Detailed steps are listed as follows:

a) Load management center initiates a creating random number instruction and sends it to encryption machine with dispersion factor.

b) After receiving the instruction, the encryptor takes a random number N_1; uses dispersion factor disperse the process key E_g ; obtains C_1 through encrypting N_1 with E_g ; then returns N_1 and C_1 to the load management center.

c) The load management center sends N_1, C_1 and dispersion factors to meter.

d) After receiving the information, meter sends the scatter factor and random number to ESAM, then ESAM uses process key $E_{g'}$ to encrypt the random number C_2 and returns it to smart meter.

e) Smart meter checks whether the equation $C_1 = C_2$ holds or not.

After completing remote identity authentication, the smart meter should perform integrity verification on received instructions. The detail process is as follows:

a) After identity authentication, the smart meter will take 4 bytes of random number N_2 from ESAM, then send N_2 and serial number of ESAM to the utility;

b) Utility receives it and sends it to encrypting machine with DLC instruction.

c) The encryptor receives the message, then computes the process key E_f through serial number of ESAM; uses E_f encrypt N_2 to generate MAC; sends "plaintext+MAC" to utility.

d) The utility receives the message and then sends this to the meter's ESAM. ESAM uses process key $E_{f'}$ and N_2 to generate MAC'; then smart meter compares MAC and MAC'.

Solution Analysis

In this section, we demonstrate the proposed schemes are secure under the attack model.

Security Analysis.

Uplink Data Security. If none of SMs or ANs has been compromised by an adversary. The proposed scheme is secure because each SM encrypts their NILM data through homomorphic encryption before transmitting. Besides, our design generates the T_i for each NILM data. Therefore, an adversary cannot modify or inject any forged messages in data transmission process because he cannot generate for his forged messages without keys.

If a SM has been compromised by an adversary, an adversary can compromise a SM and perform it as a legal one. He can generate T_i for his forged message, if the value of the forged message is in a reasonable range, detecting it is still infeasible. Besides that, because of the added *t*, time changes will bring about the continuous update of the key, so it can resist replay attacks and ensure the freshness of the data. And because of the constant change of k_{Bti}, there is no definite relation between plaintext and cipher text, so it can resist the only secret cipher text attack and the known plaintext attack.

If an AN has been compromised by an adversary. He cannot get any customer NILM data through decrypting the aggregated cipher text or each individual cipher text because no decryption key is stored in an AN.

Downlink Instruction Security.

a) **Authenticity.** Since the dispersion factor which is used to generate E_g and E_f is only known to the sending and receiving sides, so the source authentication of instruction can be realized.
b) **Integrity and freshness of instructions.** The DLC instructions take the form of 'plaintext + MAC', so we can verify the integrity of instructions by comparing the MAC value of the received instruction and the sent instruction. And we can verify the freshness of instructions through random number which is selected differently each time.
c) **Customer credibility.** By using the NILM method, utility can verify whether the customer has followed the contract through analyzing and calculating the total current and terminal voltage data of customers.

Integrity and Freshness of Instructions. In traditional demand response DLC process, the utility needs to use remote attestation method to prove the credibility of the customer to ensure customer follow the DLC contract. If we adopt NILM, we just need to collect and analyze NILM data in a high complexity, low efficiency and uneconomical way. Decomposition of the power load allows utilities formulating more scientific dynamic electricity price and demand response incentive polices.

Conclusion

In this paper, we use a recoverable data aggregation method and the ESAM security module to protect the security and integrity of the uplink data and downlink instruction. The NILM technology is used to achieve the verification of the customer's credibility. It simplifies the complex process of remote attestation technology and has a positive effect on the development of demand response.

References

[1] Muhammad R, Gyorgy D, Daniele M. "Smart meter data privacy: a survey," in *IEEE. Communications Surveys & Tutorials*, 2017,pp(99):1-1.

[2] Srinivasan D, Ng W S, Liew A C. "Neural-network-based signature recognition for harmonic source identification," in *IEEE Transactions on Power Delivery*, 2006, 21(1): 398-405.

[3] J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reverse multicast traffic wireless sensor networks," in Proc. *IEEE Int. Conf. Commun.*, 2005, pp. 3044–3049.

[4] H.M. Sun, Y.H. Lin, Y.C. Hsiao, and C.M. Chen, “An efficientand verifiable concealed data aggregation scheme in wireless sensor networks,” in *Proc. Int. Conf. Embedded Softw. Syst.*, 2008, pp. 19–26.

[5] C.M. Chen, Y.H. Lin, Y.C. Lin, and H.M. Sun, “RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks,” in *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 4, pp. 727–734, Apr. 2012.

[6] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: An efficient andprivacy-preserving aggregation scheme for secure smart gridcommunications,” in *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.