The Attacks Against and Suggestions for the Privacy-Preserving Recording & Gateway-Assisted Authentication of Power Usage Information for Smart Grid

Xiaole Mao[1, a], Xingwen Zhao [2, b]

[1] School of Telecommunication Engineer, Xidian University, Xi'An 710071, China

[2] School of Network & Information Security, Xidian University, Xi'An 710071, China

[a]email:happy_maoxiaole@163.com, [b]email:sevenzhao@hotmail.com

Keywords: Smart grid; Privacy-preserving; Deniable attack; Conflicting-plans submission attack

Abstract. The privacy protection in the smart grid is particularly significant, since sometimes the leak of the user power usage habits may lead to serious consequences. In 2015, Siu-Ming Yiu and Jin Zhong have proposed a privacy-preserving scheme which can protect each user's future power usage plan. However, some insecure factors exist in this scheme. In this paper, we show two major problems about the scheme. Firstly, it cannot resist the denial attack in which a user can deny having sent certain power plan. Secondly, the gateway smart meter doesn't detect the action that some users may send several different or even contradictory power usage plans to the upper gateway simultaneously, which will lead to the result that the user can always avoid punishment when he use more electricity than usual or obtain discount when he use less electricity than usual. We also put forward our suggestions to avoid the problems at the end of the article.

Introduction

In recent years, the smart grid has attracted wide attention. It will provide great convenience to our lives, if the smart grid can be safely and effectively used. It will not only help us to use power resources effectively, but also to better protect environment with the help of the smart grid, because the power station will be able to know the total amount of electricity requested in order to produce appropriate electricity according to the actual demand. We can clearly understand that the future of the smart grid is very bright.

In the existing researches, there are different model to describe the smart grid system. Two-way information exchange infrastructure between power suppliers and consumers called AMI (advanced metering infrastructure) can be considered as the core of smart grid [2-4]. Do-Eun Cho proposed an authentication method [5] for privacy protection in smart grid environment whose main contribution is that the access authentication method blocks the unauthorized external access and enables secure remote access to home network and its device with a secure message authentication protocol. In a recent work [6], a set of privacy-preserving protocols is proposed for a user to combine smart meter readings with a certified tariff policy to generate an electricity bill, which is then transmitted to the service provider together with a zero-knowledge proof to ensure its correctness and to avoid information leakage.

Recently, Siu-Ming Yiu and Jin Zhong proposed a model to regards the smart grid system as a hierarchical architecture [1] different from the model in scheme [2-4], in which there are home area networks at the user end, building area networks at the building feeder and neighborhood area networks among substations. Basically, there is one control center, belonging to the power operator and located at the power plant, connected to multiple substation areas. Each substation area contains one Neighborhood Area Network (NAN) gateway smart meter connecting to buildings. Each substation building contains one Building Area Network (BAN) gateway smart meter connecting to houses. Each house in turn contains one household or Home Area Network (HAN) gateway smart meter connecting to all electric appliances in the house. However, the scheme can't resist the deniable attack and the conflicting-plans submission attack. In more detail, the user can deny having

sent the power plan at the final billing. And he can take advantage of sending several contradictory plans in the preliminary stage to obtain discount or avoid punishment.

Our contributions

1)We show that the scheme cannot resist deniable attack, by describing the user submitted the plan can deny having sent the plan to the gateway smart meter.

2)We also show that the legal user can send two conflicting power usage plans including increasing the power usage plan and decreasing the power usage plan, so he will only prove one of the power plans to the control center which is consistent with his actual power usage in order to obtain the discount or to avoid punishment at the end of each billing period.

3)We come up with some suggestions to keep the system from the above attacks.

Organization

The remainder of this paper is organized as followed. In section 2 we briefly review Siu-Ming Yiu and Jin Zhong's privacy protection scheme [1]. In section 3 we describe the denial attack process and the conflicting-plans submission attack process in detail. We give out our suggestions in section 4. Section 5 concludes our paper.

Review of Siu-Ming Yiu and Jin Zhong's Privacy Protection Scheme

Firstly, we review Siu-Ming Yiu and Jin Zhong's privacy protection scheme [1] which can protect the forthcoming power usage plans. The scheme regard the smart grid system as a hierarchical architecture, including the home area networks at the user end, building area networks at the building feeder and neighborhood area networks among substations and the control center. The system structure is shown in Fig 1 and the list of the notations in this paper is shown in table 1.

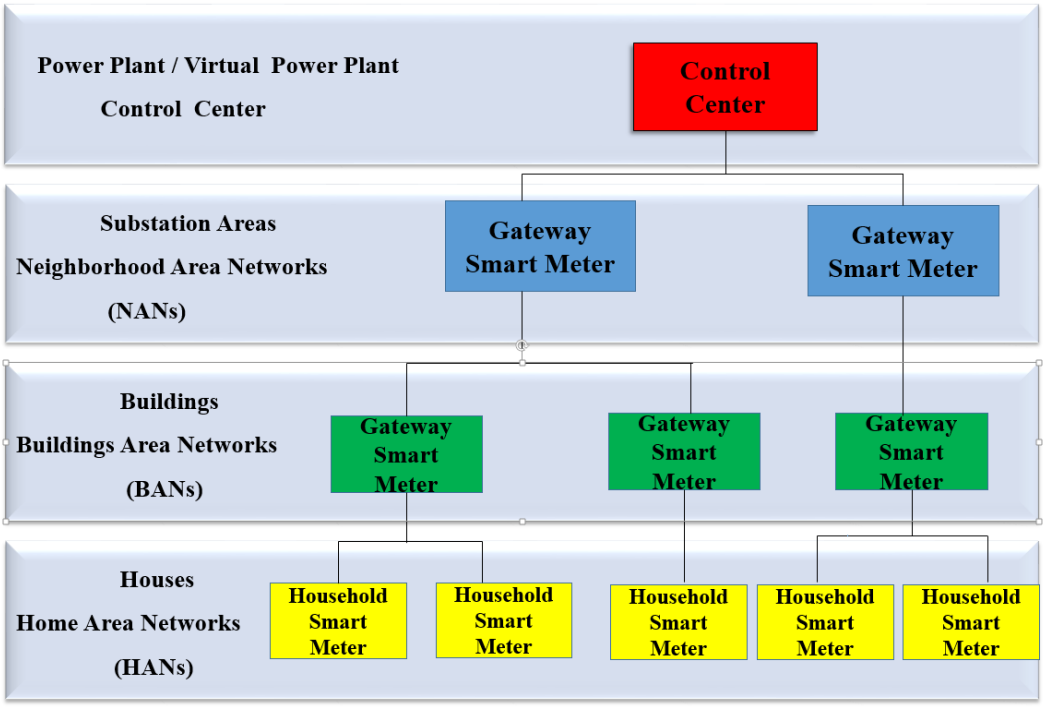

Fig.1. The smart grid system architecture

Table 1: The list of notations in this paper

Symbol	Meaning
PK_{CC}	Public key of control center
SK_{CC}	Private key of control center
HSM_i	Household smart meter i
$HSMID_i$	Identity of HSM_i
PK_{HSM_i}	Public key of HSM_i
SK_{HSM_i}	Private key of HSM_i
BSM_i	BAN gateway smart meter i
$BSMID_i$	Identity of BSM_i
PK_{BSM_i}	Public key of BSM_i
SK_{BSM_i}	Private key of BSM_i
NSM_i	NAN gateway smart meter i
$NSMID_i$	Identity of NSM_i
PK_{NSM_i}	Public key of NSM_i
SK_{NSM_i}	Private key of NSM_i
s	System master secret
n	Number of pre-defined sub-periods
U_i	Power usage plan by HSM_i
u_{ix}	Amount of additional power requested or power reduction agreed by HSM_i in j^{th} sub-period
E_i	Encrypted power usage plan by HSM_i
T	Current timestamp
CK_i	Commitment key of HSM_i
DK_i	De-commitment key of HSM_i
$Commit(M, CK_i)$	Commitment on M
$Check\,\mathrm{Re}veal(C, M, DK_i)$	Reveal M with commitment C
H_i	Hash of $HSMID_i$, T and U_i by HSM_i
C_i	Commitment of H_i with CK_i by HSM_i
AE_j	Aggregated E_s by BSM_j
HBF_j	Bloom filter for storing Hs by BSM_j
CBF_j	Bloom filter for storing Cs by BSM_j
AAE_k	Aggregated AE_s by NSM_k
$ENC_x(M)$	Encryption of plaintext M using key x
$SIG_x(M)$	Signature on message M using key x
$HMAC_x(M)$	HMAC on message M using key x

The four processes, including preparation phase, power plan submission phase, power plan processing phase, reconciliation phase, will be described as followed.

Preparation Phase

In this step, the control center sets up system parameters, including the public keys PK_i and private keys SK_i of the control center, each household smart meter, each BAN gateway smart meter and each NAN gateway smart meter. In the meanwhile, the control center generates the system master s. Then the identity and its public keys of the smart devices are stored into the control center's database while the corresponding private keys are preloaded into the smart devices. These keys are used for the purpose of initial transmission or updating of system master secret.

Power Plan Submission Phase

If an end user begins to request for additional power or express the intention to reduce power, he should follow the below steps.

- Assume that there are altogether n pre-defined sub-periods in the forthcoming power provisioning period. $U_i = \lfloor u_{i0}, u_{i1}, ...u_{i(n-1)} \rfloor$, u_{ix} represents the amount of additional power required or power reduction agreed by the household smart meter HSM_i in the xth sub-period.
- Encrypts U_i using the control center's public key to form: $E_i = \lfloor e_{i0}, e_{i1}, ..., e_{i(n-1)} \rfloor$ where $e_{ix} = ENC_{PK_{CC}}(u_{ix})$. In this way, no gateway smart meter can know the value of any u_{ix}
- Generates a pair of commitment and de-commitment keys, namely CK_i and DK_i, and saves them locally.
- Computes the hash of the array together with other parameters as $H_i = h(HSMID_i, T, U_i)$.
- Commits H_i to form: $C_i = Commit(H_i, CK_i)$.
- Computes the $HMAC$ signature with the system master s as the key on E_i, H_i and C_i to form $HMAC_s(E_i, H_i, C_i)$ where || stands for simple concatenation.
- Sends $ENC_{PK_{BSM_j}}(E_i, H_i, C_i, HMAC_s(E_i \| H_i \| C_i))$ to its upper level BAN gateway smart meter BSM_j.
- Stores CK_i, DK_i, T, U_i and C_i locally.

Power Plan Processing Phase

The BAN gateway smart meter BSM_j does not forward the received power plans immediately. Instead, it should receive more than one power plans during such an interval and forwards these plans to the NAN gateway smart meter, that is to say, it only performs such an action of forwarding at regularly intervals. Upon the time of forwarding, BSM_j performs the following steps:

- For each $ENC_{PK_{BSM_j}}(E_i, H_i, C_i, HMAC_s(E_i \| H_i \| C_i))$ received, BSM_j decrypts the block using its private key to verify whether the information is sent by a valid user smart mater and also it is not modified by anyone.
- Aggregates the received power usage plans to form: $AE_j = \lfloor ae_{j0}, ae_{j1}, ..., ae_{j(n-1)} \rfloor$ where $ae_{jx} = e_{0x} \times e_{1x} \times ...e_{(m-1)x}$, if there are m power plans received and to be aggregated.
- Prepares two bloom filters HBF_j and CBF_j to reduce the total traffic volume. Then BSM_j adds $H_0, H_1, ..., H_{m-1}$ into HBF_j and adds $C_0, C_1, ..., C_{m-1}$ into CBF_j.
- Computes the $HMAC$ signature $HMAC_s(AE_j \| HBF_j \| CBF_j)$.
- Forwards $ENC_{PK_{NSM_K}}(BSMID_j, AE_j, HBF_j, CBF_j, HMAC_s(BSMID_j \| AE_j \| HBF_j \| CBF_j))$ to its upper lever NAN gateway smart meter NSM_k.

Upon receiving from multiple BANs, the upper lever NAN gateway smart meter NSM_k performs the similar thing as the BANs gateway, except that NSM_k forwards the aggregated

data to the control center.

After the control center receives the plans aggregated, it verifies that the sender is valid or not and validate the information is modified or not by re-computing the *HMAC* values. Then, aggregates the received data in the same as what the BAN or NAN gateway smart maters do and decrypts each entry to obtain the aggregated power demand information. Finally, stores $\langle BSMID_j, HBF_j, CBF_j \rangle$ into its own database.

Reconciliation Phase

This phase is carried out at the end of each billing period. The control center requests each household smart meter to prove that it has submitted a certain power plan earlier to get the discount or penalties.

Having receiving the request, an end user responds by sending its identity $SMID_i$, the time stamp used T, the original array U_i, the commitment C_i and the de-commitment key DK_i to the control center.

The control center then performs the following steps:

- Computes $H_i = h(HSMID_i, T, U_i)$ and compares it with the received information.
- Verifies the commitment information by invoking the function $check\,\mathrm{Re}veal(C_i, H_i, DK_i)$ to see whether it returns a positive value.
- If yes, compare the agreed power plan and the actual power usage to set the charge scheme.

The Attacks against the Privacy-Preserving Recording & Gateway-Assisted Authentication of Power Usage Information for Smart Grid

In this section, we will describe the process of the deniable attack and the conflicting-plans submission attack.

The deniable attack is that the user can claim he didn't send the power usage plan earlier to avoid punishment, if the actual power is not consistent with the power plan.

The conflicting-plans submission attack is that a user can submit many power plans, such as the normal power plan, the additional power plan, the reducing power plan and so on. When his actual amount of power usage is too much, he can just verify that he has submitted the additional power plan to avoid punishment. When his actual amount of power usage is less, he can verify that he has submitted the reducing power plan to get the discount. And the attacks in detail are followed.

The deniable attack

We assume that the user m have made the power plan and $U = \lfloor u_0, u_1, ...u_{(n-1)} \rfloor$ is the amount of additional power required or decreasing power in the each sub-period.

- Computes the encrypted entry $E = \lfloor e_0, e_1, ..., e_{(n-1)} \rfloor$ using the control center's public key $PKcc$.

Generates the CK and DK for the subsequent commitment and de-commitment in the billing period.

- Computes $H = h(HSMID, T, U)$, $HSMID$ is the identity of the user household smart meter and T is the timestamp for the moment.
- Commits H to form $C = Commit(H, CK)$
- Computes the $HMAC$ signature with the system master secret s as the key on E, H and C to form $HMAC_s(E, H, C)$.
- Sends $ENC_{PK_{BSM_j}}(E, H, C, HMAC_s(E \| H \| C))$ to its upper level BAN gateway smart meter BSM_j.
- Stores CK, DK, T, U and C locally.

After receiving the $ENC_{PK_{BSM_j}}(E, H, C, HMAC_s(E \| H \| C))$, the BAN gateway smart meter

decrypts and verifies the information. The result will illustrate whether the identity is valid or not and the information has been modified or not.

After lots of information is aggregated by the BAN gateway smart meter and the NAN gateway smart mater, the aggregated information will be send to the control center in the end.

However, if the user has known that the actual power used is not consistent with his submitted plan earlier, he can deny that he has submitted such a plan to avoid punishment. As the master secret of the control center is known by every valid smart device and BAN gateway smart meter only requires $HMAC_s(E,H,C)$ to ensure the safety, any legal user can pretend to be the other user to send information. For instance, user A can pretend to be B by sending a message $ENC_{PK_{BSM_j}}(E,H,C,HMAC_s(E \| H \| C))$ where $H = h(HSMID_B,T,U)$ is computed using household smart meter identity of B. And at the process of verifying the received information, the BAN gateway smart meter can only verify the message is valid or not and can't decide whether the message is from the actual user or from an imposter. Because of the above issue, any user can declare that he didn't send the plan if he found that the plan was not consistent with his actual power usage. The primary cause of this problem is that the submitted plan doesn't contain the user's authentication information such as digital signature.

The conflicting-plans submission attack

Following the same steps above, we assume that the user m has made two contradictory power plans, respectively are $U_1 = \lfloor u_{10}, u_{11}, ...u_{1(n-1)} \rfloor$ and $U_2 = \lfloor u_{20}, u_{21}, ...u_{2(n-1)} \rfloor$. U_1 is the amount of additional power required and U_2 is the amount of reducing the power in the forthcoming sub-period.

- Computes the encrypted entry $E_1 = \lfloor e_{10}, e_{11}, ...e_{1(n-1)} \rfloor$ and $E_2 = \lfloor e_{20}, e_{21}, ...e_{2(n-1)} \rfloor$ using the control center's public key $PKcc$. Generates the CK and DK for the subsequent commitment and de-commitment.
- Computes the $H = h(HSMID,T,U)$, $HSMID$ is the identity of the user household smart meter and T is the timestamp for the moment.
- Commits H to form $C = Commit(H, CK)$
- Computes the HMAC signature with the system master secret s as the key on E, H and C to form $HMAC_s(E_1,H,C)$ and $HMAC_s(E_2,H,C)$.
- Sends $ENC_{PK_{BSM_j}}(E_1,H,C,HMAC_s(E_1 \| H \| C))$ and $ENC_{PK_{BSM_j}}(E_2,H,C,HMAC_s(E_2 \| H \| C))$ to its upper level BAN gateway smart meter BSM_j.
- Stores CK, DK, T, U and C locally.

After receiving the $ENC_{PK_{BSM_j}}(E_1,H,C,HMAC_s(E_1 \| H \| C))$ and $ENC_{PK_{BSM_j}}(E_2,H,C,HMAC_s(E_2 \| H \| C))$, the upper BAN gateway smart meter decrypts and verifies the submitted information to ensure the validity of the message and the information is not modified during transmission.

Then, the aggregated data by the BAN gateway smart meter is sent to the NAN gateway smart meter to verify and aggregate. The aggregated information will be send to the control center in the end.

At the end of billing, the user has known the actual power, he only verifies one of the plans to the control center that makes him to get more discounts or avoid punishment. That is, he will only declare that he have submitted the additional power plan to use more power if the actual amount of power usage is too much. Another situation is similar. He will only declare that he have submitted the reduction plan to use less power if the actual power is less than the usual. The BAN gateway smart meter can only verify the message is valid or not, it doesn't verify the uniqueness of the plans. More specifically, it doesn't verify that whether the user sent more than one plans simultaneously.

In a word, the scheme cannot achieve its designed goal since any user can get discount or to avoid punishment by sending conflicting plans.

The suggestion to avoid the deficiency of the scheme

Yiu and Zhong's scheme [1] is subject to the above described attacks, due to the fact that the submission does not include authentication of the sender and BAN gateway smart meter does not restrict the malicious use's behavior of multiple submissions. Thus, we suggest that two methods be used to avoid the shortcoming.

First, we can add the signature algorithm based on the hash algorithm, in other words, we need to compute the signature $SIG_{sk_{HSM}}\left(HMAC_s\left(E,H,C\right)\right)$ to replace the hash $HMAC_s\left(E,H,C\right)$ to the first situation. So the upper gateway can obtain the accurate information about the sender by decrypting the $SIG_{sk_{HSM}}\left(HMAC_s\left(E,H,C\right)\right)$ with the PK_{HSM}. In this way, we can avoid the denial behavior by adding a digital signature, which will add the personal authentication information to the submitted plan.

Second, we need to add some additional information including the identity of the household smart meter *HSMID* and T to show the uniqueness. The information will be $ENC_{PK_{BSM_j}}\left(T,HSMID,E,H,C,SIG_{SK_{HSM}}\left(HMAC_s\left(E\parallel H\parallel C\right)\right)\right)$ after adding identification information. After the upper lever BAN gateway smart meter receiving the information $ENC_{PK_{BSM_j}}\left(T,HSMID,E,H,C,SIG_{SK_{HSM}}\left(HMAC_s\left(E\parallel H\parallel C\right)\right)\right)$, it can compare the identity *HSMID* with the timestamp to check whether the same meter send more than one plans. If yes, it refuses to forward the information to the BAN gateway smart meter, or it can report the malicious behaviors to the control center. In this way, we can avoid conflicting-plans submission attack.

Conclusion

Recently, Siu-Ming Yiu and Jin Zhong have proposed a privacy-preserving smart grid scheme by aggregating data submitted by the smart meters. We show that the user can deny submitting the plan or send two contradictory plans to get the discount or avoid punishment. There are two main reasons. First, master key is common among all the smart devices and the system cares only about the hash value which does not contain the user's signature. Second, the BAN gateway smart meter can't and doesn't verify the uniqueness of the plan due to the lack of the uniqueness identification information. We show the process of the deniable attack and the conflicting-plans submission attack in detail. Finally, we add the timestamp T, the identity of the household smart meter *HSMID* to the information and attach a signature to avoid the aforementioned problem.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (No.61272457), the National 111 Program (No.B08038) and the Research Fund for the Doctoral Program of Higher Education of China (No.20130203120003).

References

[1] Chim T W, Yiu S-M, Li V O K, Hui L C K, Zhong J. PRGA： Privacy-Preserving Recording & Gateway-Assisted Authentication of Power Usage Information for Smart Grid[J], IEEE transactions on dependable and secure computing, 2015, 12(1):85-97.

[2] Gunther E W, Snyder A, Gilchrist G, Highfill D R, Smart Grid Standards Assessment and Recommendations for Adoption and Development[Z], California USA: California Energy Commission, February 2009.

[3] NIST, Report to NIST on the Smart Grid Interoperability Standards Roadmap[R], Gaithersburg, USA: National Institute of Standards and Technology, SB1341-09-CN-0031, 2009.

[4] Kang D J, Park J H, Yeo S Sl. Intelligent Decision-Making System with Green Pervasive Computing for Renewable Energy Business in Electricity Markets on Smart Grid[J]. EURASIP Journal on Wireless Communications and Networking, 2009, (2009):1-12.

[5] Cho D E, Yeo S S, Kim S J. Authentication Method for Privacy Protection in Smart Grid Environment[J]. Journal of Applied Mathematics, 2014, (2014):1-10.

[6] A. Rial and G. Danezis, “Privacy-preserving smart metering,” in Proc. 10th Annu. ACM Workshop Privacy Election. Soc, Dec. 2011, pp.49-60.