Shuanggen LIU, Shuangzi ZHENG, Wenbo ZHANG, Runsheng FU, 2022. A power resource dispatching framework with a privacy protection function in the Power Internet of Things. *Frontiers of Information Technology & Electronic Engineering*, 23(9):1354-1368. https://doi.org/10.1631/FITEE.2100518

A power resource dispatching framework with a privacy protection function in the Power Internet of Things

Key words: Power Internet of Things; Cloud-fog cooperation; Elliptic curve; Random oracle model; Certificateless aggregate signcryption

Corresponding author: Shuanggen LIU
E-mail: liusgxupt@163.com
ORCID: https://orcid.org/0000-0002-8188-2820

Motivation

1. Most existing certificateless aggregate signcryption schemes are based on bilinear pairing and exponential operations. However, these two operations are much less efficient than scalar multiplication and point addition on elliptic curves.

2. In addition, existing schemes hardly consider the anonymity of every user and the methods for tracking abnormal users.

Main idea

1. We propose a power resource dispatching framework (PRDF).

2. Moreover, users can send data anonymously.

3. Our scheme can track the true identity of a user who submits abnormal data.

Method

1. PRDF manages power data and the real identity of users separately. In this way, it can prevent attackers from directly obtaining the corresponding relationship between the users' identity and their data.

2. PRDF combines the cloud-fog cooperation mode with certificateless aggregate signcryption technology using pseudonyms. Control center (CC) can analyze power consumption of the whole area and formulate the regional power dispatching strategy without knowing the real identity of the users.

3. Moreover, if a user's data is abnormal, CC will notify the user management center (UMC) to track the abnormal user's real identity.

Method (Cont'd)

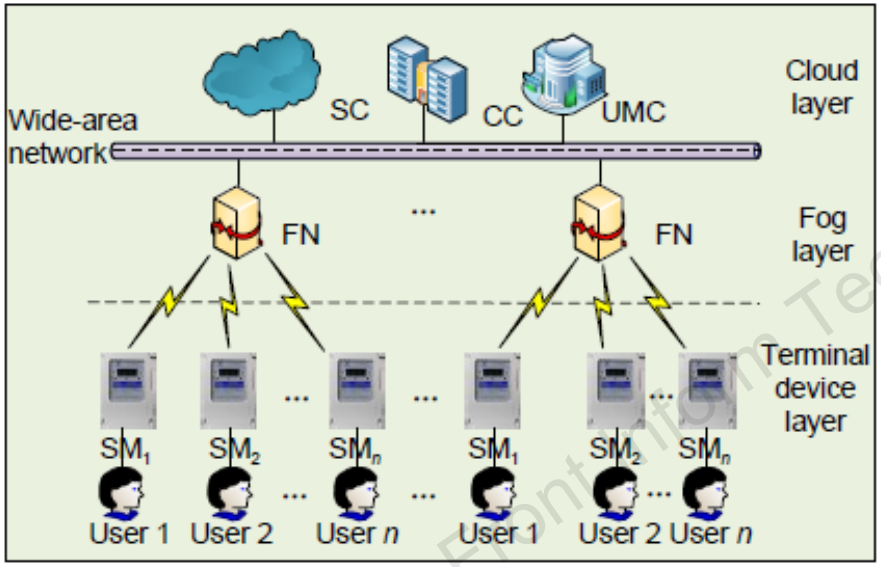

Fig. 2 Architecture of cloud-fog cooperation

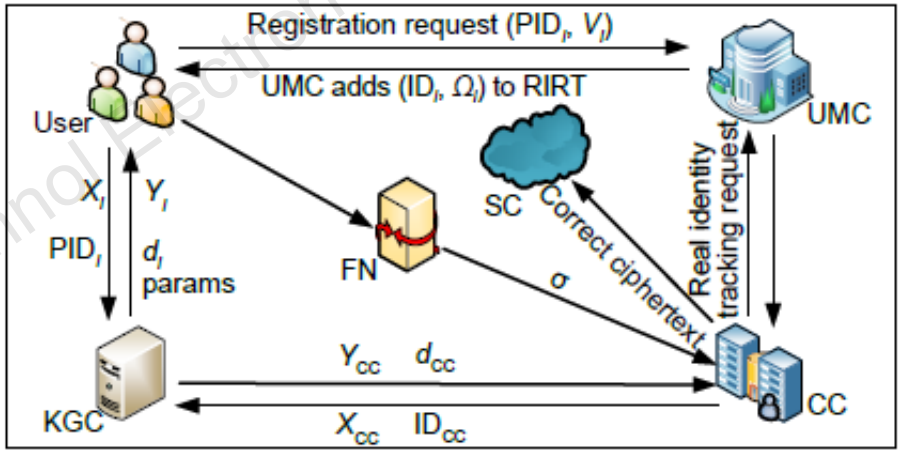

Fig. 3 Model of the power resource dispatching framework (PRDF)

Major results

Table 3 Comparison of safety characteristics

Scheme	Confidentiality	Unforgeability	Relief DDoS attacks	Resistance to replay attack	Eliminating key hosting
Yu CM et al. (2014)'s	×	√	×	√	×
Wang L (2019)'s	×	√	×	√	×
Wang XD et al. (2021)'s	×	√	×	×	×
Chen (2016)'s	√	√	×	√	√
Sui and de Meer (2020)'s	√	√	×	√	×
Xie and Li (2020)'s	√	√	×	√	√
Ours	√	√	√	√	√

Table 5 Efficiency comparison among certificateless aggregate signcryption schemes

Scheme	Time cost (ms)		Communication cost (bit)
	Signcryption aggregation	Decryption verification	Length of ciphertexts
Yu HF and Ren (2022)'s	$(2n+1)E_m + 2nE_a$	$(2n+2)E_m + 3E_a$	$\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$
Zhang SM et al. (2018)'s	$nE_p + nE_m + nE_a$	$3E_p + 2nE_m + nE_a$	$\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$
Nkenyereye et al. (2019)'s	$(3n+1)E_m + nE_a$	$4E_p + 2nE_m$	$\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$
Cui et al. (2019)'s	$2nE_m$	$(4n+1)E_m + 3nE_a$	$\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$
Li C and Qi (2020)'s	$(2n+1)E_m + (2n+2)E_a$	$nE_m + nE_a$	$2\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$
Kim et al. (2020)'s	nE_p	$(3n+2)E_p$	$2\|G\|+\|\mathbb{Z}_q^*\|$
Ours	$(2n+1)E_m + 2E_a$	$(n+2)E_m + (2n+2)E_a$	$\|\mathbb{G}\|+\|\mathbb{Z}_q^*\|$

Major results (Cont'd)

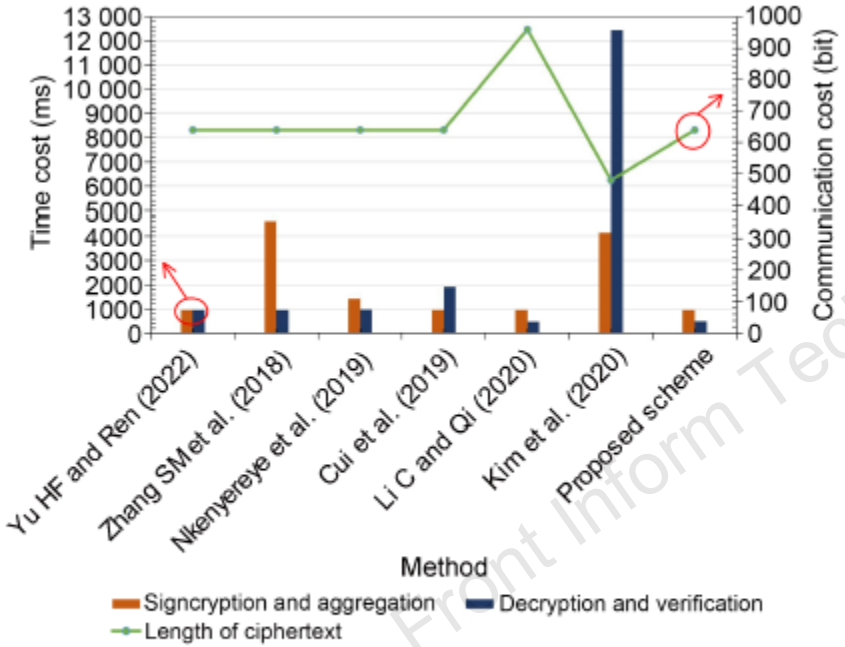

Fig. 4 Comparison of calculation and communication costs of each scheme

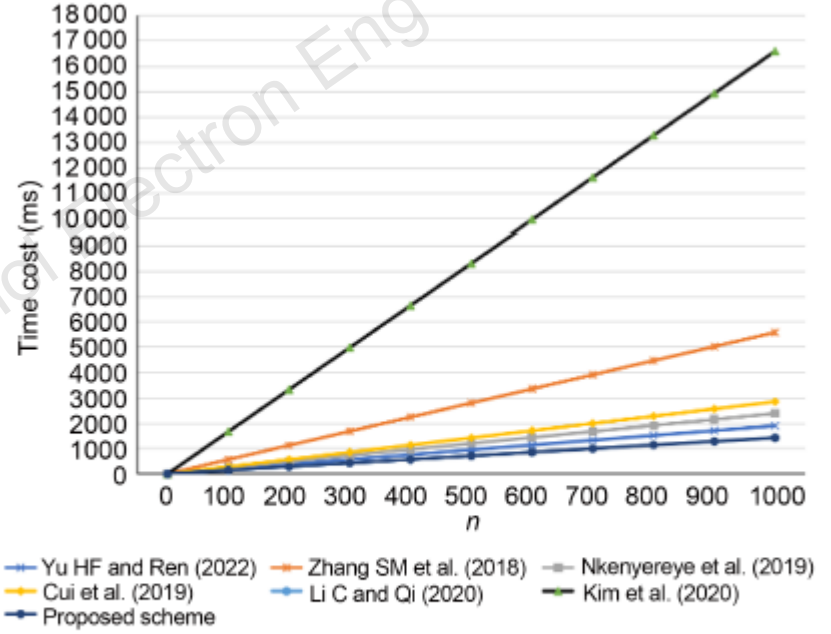

Fig. 5 Comparison of calculation time cost of each scheme ($0 \leq n \leq 1000$)

Conclusions

1. PRDF solved the privacy protection problem of users' power data in the Power Internet of Things and provided users with exclusive power services.

2. Theoretical analysis and simulation results showed that our scheme is more efficient and has more security characteristics compared with traditional methods.

Shuanggen LIU received his PhD degree in cryptography from Xidian University, Xi'an, China, in 2008. He is currently an associate professor with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, China. His recent research interests include cryptography and information security. He is a member of the China Computer Federation and the Chinese Association for Cryptologic Research.

Wenbo ZHANG received his BS and MS degrees from Zhengzhou Information Science and Technology Institute, China, in 2005 and 2009, respectively. He received his PhD degree from Xi'an High-tech Institute, China, in 2013. He is currently an instructor of the Xi'an University of Posts and Telecommunications. His research interests include wireless communication security, blockchain, and network security.