A Secure and Trustable Access Method of Power Business in 5G Networks

Huan Li[1(✉)], Fanbo Meng[2], Dongdong Wang[2], and Zhibin Yang[1]

[1] Electric Power Research Institute of State Grid Liaoning Electric Power Supply Co., Ltd., Shenyang 110006, China
lihuan213@sina.com

[2] State Grid Liaoning Electric Power Supply Co., Ltd, Shenyang 110004, China

Abstract. The 5G power network has gradually adopted mobile terminal access to access the network to manage business. With the continuous expansion of access terminal scale, if the attacker impersonates the terminal or hijack the terminal to attack the master server, it will cause serious consequences. Therefore, this paper proposes a lightweight and efficient terminal secure and trustable access method in 5G power business network. Considering the core idea of security stratification and network special, we design a three-layer security access architecture to ensure the security of terminals in the access process and data protection process. Then, we propose a lightweight secure certification method for large-scale terminal accessing power network. The simulation results show that the proposed method can reduce the communication overhead and provide good security when massive terminals accessing.

Keywords: 5G network · Power business · Secure and trustable access · Communication overhead

1 Introduction

With the construction of smart grid, the information confidentiality, integrity and availability of power grid enterprise have higher requirements [1–3]. At present, the main businesses of power grid, like production, marketing, materials, emergency command, mobile office, have gradually adopted mobile terminals with wireless accessing. The data exchange is conducted through 5G wireless access technology and internal and external networks, and the number of access terminals has continued rapid growth. Based on above, how to ensure that all kinds of decentralized mobile terminals can be safely connected to the smart grid network, and how to monitor and audit the access terminals to realize the confidentiality and controllability in the process of information transmission, has become the urgent problem to be considered and solved with information construction [4–6]. In the future network, with the continuous expansion of access terminal scale, the complexity of access environment and the diversification of access methods, the security, confidentiality and controllability of all kinds of information transmission process will face more severe challenges. The security risks of power grid mainly exist

H. Song and D. Jiang (Eds.): SIMUtools 2020, LNICST 369, pp. 1–11, 2021.
https://doi.org/10.1007/978-3-030-72792-5_1

in terminal, transmission channel and application system. Among them, terminal risks mainly include physical security and data storage security, system vulnerabilities, illegal software installation, equipment non-security management, illegal use risks, etc. The risk of transmission channel includes illegal information interception and tampering and illegal terminal access through private network channel [7–10]. Application system risks mainly include unauthorized access, sensitive data leakage and illegal attacks on the system.

The complete business access process is shown in Fig. 1. Specifically, large-scale power terminal access under 5G wireless communication has the following security access problems:

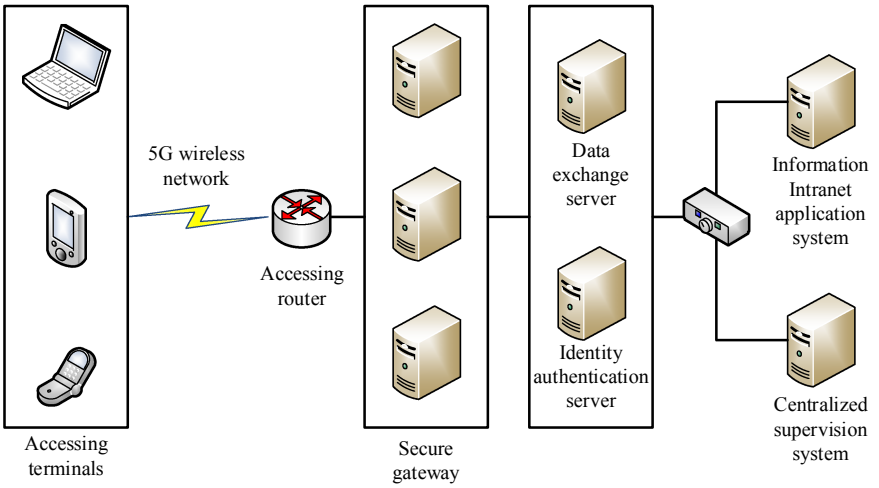

Fig. 1. Terminal secure access framework.

1) **Illegal terminal access.** The power communication network has more and more intelligent terminals accessing. The network security protection boundaries is expended, so that the terminal access requirements for various business are flexible, which has security risks of illegal access [11, 12]. An attacker can counterfeit illegal terminal or taking control terminal, making it a springboard to attack main servers and issue fault information. Once entering the network system, it will be seen as credible user access to the main resources for illegal operation [13, 14], thus causing a wider range of security threats.
2) **Fake master server control.** The main server of power communication network mainly carry out the application functions such as data acquisition and monitoring and analysis in real time. As the core component of intelligent power business network, it will send the control instruction to the intelligent terminals for production operations, dispatching operation and accident repair work to provide business support and direct service [15, 16]. If an attacker impersonates a master server and sends

malicious control instructions to intelligent terminals, causing them to make erroneous actions, there will be incalculable consequences for the entire power system and national infrastructure.

3) **Communication data breach.** Real-time data and operations between the whole system of smart power network and external users are becoming more and more intensive. Data acquisition, storage, communication and processing operation mode has been different from the past distribution network. As the boundaries of data communication networks expand, the risk of data being broken increases greatly. In power communication system, wireless data transmission is used between master server and terminals, including control data and real-time monitoring data. Once the data is tampered, resulting in the destruction of integrity, the intelligent distribution network terminal may make wrong actions, and the intelligent distribution network server may make wrong decisions [16, 17].
4) **Multiple cyber-attacks.** The communication system of intelligent power network has a mixture of communication modes, which can be divided into wireless communication and wired communication. The mixed communication mode makes the power communication system vulnerable to all kinds of communication attacks, such as denial of service attack, replay attack, data injection attack, man-in-the-middle attack and so on [18–20]. For example, a denial-of-service attack on the accessing terminals may make it impossible to get control instructions from the master server in a timely manner, triggering abnormal control instruction settings or business failures, thus greatly reducing the reliability and security of power supply.

Considering the above risks in the 5G power business network, this paper proposes a mobile terminal security access architecture according to the security requirements of the network. The core idea is security stratification and network exclusive utilization. We analyze the mobile applications of power networks and the safety risks of mobile terminals, and design a secure access method according to the proposed architecture to realize terminal access security. Then, considering limitation of the calculation capacity and the communication resources, we propose a lightweight safe access method MTS for 5G power business network.

The rest of this paper is arranged as follows. Section II analyze the access risks of terminals and presents the secure access architecture. Section III propose a lightweight safe access method MTS for 5G power business network. Section IV displays the simulation results and analysis. We then conclude our work in Section V.

2 System Architecture

In order to ensure the access security of power business network, we proposes an intelligent terminal security access architecture, which takes security stratification and network exclusive utilization as the core idea, as shown in Fig. 2. Security stratification refers to the mobile terminal access security protection. The whole process is divided into security terminal layer, security access and transmission layer and application interface layer. Network exclusive utilization refers to the network involved is divided into mobile private network, border security access network and internal business private network,

each network to implement strict access control. The proposed architecture will meet the requirements of data closed-loop secure transmission, prevent information leakage and illegal access. The purpose of the architecture is to protect the integrity of information and fine-grained access control, so as to ensure the secure access of the wireless mobile terminals.

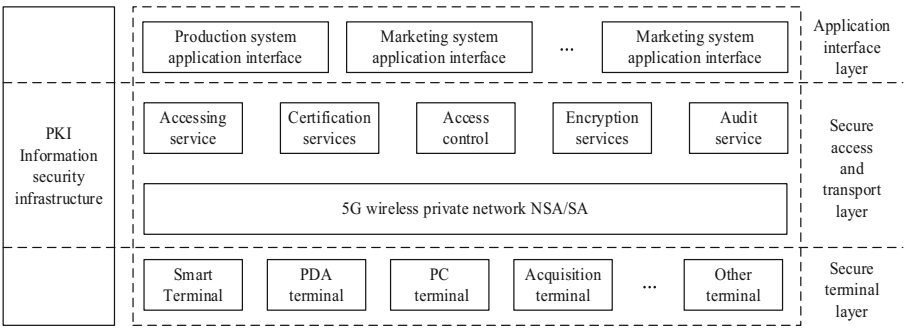

Fig. 2. Secure accessing architecture of power business networks.

As shown in the figure, the whole terminal security access architecture for power business network is divided into three layers:

Terminal Access Layer: According to the application of mobile terminals in power business networks, the terminal access layer mainly includes computer, PDA, smart phone and wireless collection terminal, etc. For these terminals, secure SIM/UIM card, security control software, security inspection module and security communication module are used to ensure the terminal security, improve the reliability of authentication, ensure data transmission security, and prevent the terminal from being counterfeits and data leakage. At the same time, the corresponding management software is installed to standardize the terminal operation to avoid malicious software applications, prevent illegal mobile terminal access.

Secure Transport Layer: The secure transport layer mainly provides the secure access service for all kinds of terminals, including the security of wireless channel transmission and the secure data exchange. Among them, the wireless transmission channel adopts the wireless private network to ensure the integrity and security of data in the transmission process. Between the power business network and the wireless transmission channel, it can set up a secure access area for security isolation and access. Secure transport layer, as the core part of terminal secure access, achieve secure access, identity authentication, data filtering and centralized supervision and other functions. The transport layer transmits various access control data efficiently through the high-speed channels. What's more, it provides access, authentication, access control, encryption, proxy, exchange, filtering, supervision and other security services through various functional components. It coordinates the whole process of secure access of various terminals, and makes all functional components of the system cooperate and work together to form a unified power business network.

Application Interface Layer: The application interface layer is mainly used to realize the application data interface between the security access layer and the production management, marketing management, material management and other systems. t can manage the security data transmitted between the terminal and the master server system. Application services customize security policies through the application interface layer, authorize specific terminal access, and conduct two-way security data interaction.

The above architecture determines each security authentication process in the terminal access process from the system level. Next, we propose a lightweight terminal security access method MTS, suitable for large-scale wireless terminal access in power business network.

3 Secure Access Method

In order to achieve large-scale and lightweight terminal secure access, it is necessary to improve the traditional asymmetric encryption method and reduce the algorithm complexity. At the same time, considering the mobility of the power grid terminal, the primary server and terminal need to maintain a unique identity of mutual authentication [21, 22]. The primary server does not need to re-register the newly accessed terminal if it has been securely registered, thus reducing the overall algorithm complexity. Specifically, the process of the proposed MTS method is as follows.

The initialization algorithm is implemented by the mains server platform. By inputting security parameters of λ bit length, the algorithm outputs the common parameter PB, which is shared among all participating entities in the scheme, specifically including the following steps:

(1) The registry of main server platform selects cyclic group G and large integer group Z_q^* of order q through the security parameters of λ bit length, and the generation element of the group is g. Different Hash functions are selected:

$$H_0 : G \times G \to Z_q^* \tag{1}$$

(2) Two safety parameters n and k are randomly selected. Calculate and generate two prime numbers p and m with length of n/k bits from the group, which satisfy the following requirements:

$$\gcd((p-1),(m-1)) = 2 \tag{2}$$

Then, calculate $N = p^{(k-1)} \times m$. In the power business network, each terminal equipment TU and server MS has its unique identification information ID_{TU} and ID_{MS}, and the terminal equipment sends access request to the server by virtue of its unique identification information ID_{TU}.

(3) The cloud platform first generates a set of pseudo-random numbers $a_1, a_2, \ldots a_z, \in Z_p^*$ randomly through the pseudo-random function generator. Then it generates public key information $MK_{TU} = \left\{MK_{TU,1}, MK_{TU,i} \cdots, MK_{TU,z}\right\}$ according to the personal information ID_{TU} provided by the terminal, where $MK_{TU,i} = g^{a_i}$. Further, it generates anonymous identifying data $PID_{TU} = \left\{PID_{TU,1}, PID_{TU,i}, \ldots, PID_{TU,z}\right\}$,

where $PID_{TU,i} = H_0\big((ID_{TU}||ID_{MS}) \oplus MK_{TU,i}\big)$. In this way, the real identity information of the terminal device is hidden in the anonymous identity.

(4) Formula (3) is used to calculate and generate two secret values K_{TU} and K_{MS}. Then find the integer d by traversal, and $d = K_{TU} \bmod (p-1) = K_{MS} \bmod (m-1)$. Then, calculate $e = d^{-1} \bmod (\phi(N))$. The registry of the main server returns $<MK_{TU}$, PID_{TU}, $\mathrm{K_{TU>}}$ to the terminal device over the secure channel.

$$\begin{cases} \gcd(K_{EU},\ (\mathrm{p}-1)) = 1 \\ \gcd(K_{ES},\ (m-1)) = 1 \\ K_{EU} = K_{ES} \bmod (2) \end{cases} \tag{3}$$

(5) The cloud platform generates the anonymous identity polynomial $acc(x)$ of the terminal device:

$$\mathrm{acc}(x) = g^{\prod\limits_{x \in PID_{TU}} (x - PID_{TU,j})} \tag{4}$$

The coefficients of the polynomial can be represented by the set $\left\{g^1, g^s, g^{s^2}, \ldots, g^{\mathrm{z}}\right\}$. The anonymous information set $\langle Set\_PID,\ K_{MS}\rangle$ of registered terminal devices is signed with the private key of the main server:

$$\mathrm{Sign}_{K_{priv}}\big(\mathrm{Enc}_{PK_{MS}}(\mathrm{Set\_}PID, K_{MS})\big) \tag{5}$$

When the terminal accesses, the private key is used to decrypt and the identity information of the registered terminal device is stored locally.

The authentication phase begins when the registered terminal device TU accesses the master server MS. When the terminal device TU needs to access the master server node MS in that location, generally, the terminal device does not know the identity information of the master server node, but only sends a request to the specific master server [23, 24]. The process is divided into the following 4 steps:

(1) $TU \rightarrow MS$: The terminal device randomly selects $(PK_{TU,i}, PID_{TU,i}, SK_{TU,i})$ from $\{PK_{TU}, PID_{TU}, SK_{TU}\}$. Then, it broadcasts message <HelloMS, PID_{TU}, $T_i>$, where T_i is the current time stamp.

(2) $MS \rightarrow TU$: After the master server receives the access request, it verifies whether the time stamp T_i is expired and whether the terminal device has been registered through Formula (6):

$$\begin{cases} \mathrm{acc}\big(PID_{TU,i}\big) = \prod\limits_{j=1}^{z} g^{s^j \cdot PD_{TU,i}^j} = 1 \\ \mathrm{verify}(T - T_i) \le \Delta T \end{cases} \tag{6}$$

If the verification is passed, it returns $\{ID_{MS}, PID_{TU,i}, T_i\}$ to the terminal device.

(3) $TU \rightarrow MS$: The terminal device first verifies whether the time stamp T_i is expired, then verifies the identification correctness of the primary server through formula (7).

$$\begin{cases} \mathrm{Verify}\big(H_0\big((ID_{TU} \| ID_{MS}) \oplus MK_{TU,i}\big) = PID_{TU,i}\big) \\ \mathrm{cha} = (c + T_i + ID_{MS})^e \bmod (N) \end{cases} \tag{7}$$

Then, randomly selects $c \in Z_p^*$ to generate *cha* of challenge report, and then sends $<cha, T_i>$ to the main server.

(4) $MS \rightarrow TU$: After the master server receives the challenge message, it first verifies whether the time stamp T_i is expired, then recovers the challenge value c' sent by the terminal device by calculating $cha^{K_{ES}} \mod (q)$, and finally calculates the reply message:

$$res = \left(c' + T_i + PID_{TU,i}\right)^{\mathrm{e}} \mod (N) \tag{8}$$

Then, send $<res, T_i>$ to the terminal device.

Finally, the terminal verifies that the challenge value obtained is correct. If the verification is successful, the challenge value can be used as the data encryption key for subsequent communication to ensure the security phase and integrity of communication.

In the proposed method, the identity information of terminals stored in the primary server is shared. Therefore, when the terminal connects to different servers and conducts authentication, the two-way authentication between the terminal and the server can still be completed by repeating the above steps, and the same authentication result can be obtained.

4 Simulation Analysis

In this section, the MTS security access scheme designed in the previous chapter is verified through analysis and experiment in terms of availability and security. In terms of availability, simulation experiments are carried out on communication overhead and network connectivity to verify whether the scheme has lower communication overhead and good network connectivity, and the results are analyzed. Then the storage requirements and computing costs are analyzed. Three attack methods are constructed to verify and analyze the security of the scheme [25, 26]. Under two common attack modes, replay attack and node forgery attack, it is proved to have the ability to resist replay attack and node forgery attack through analysis [27]. Simulation experiments show that the scheme can maintain certain network connectivity under denial of service attacks.

4.1 Simulation Environment

This simulation platform is based on the 5G virtual wireless sensor networks environment. The specific environment is one PC with 2.3 GHz CPU and 8 MB RAM. The software environment is 64-bit windows 10 operating system. We use MATLAB software for experiments. We set the area of the wireless sensor network as a 100 × 100 square, and deployed 100–300 wireless sensor terminals in this area. The characteristics of nodes are the same, such as physical structure unit, communication capability and energy. In the experiment, the communication flow of the nodes is used as the energy factor to measure the nodes, and the nodes all have the function of data fusion. The experimental results are as follows:

4.2 Communication Overhead Evaluation

The study in this paper is not limited to specific power terminals, so the energy consumption model of terminals cannot be obtained. Therefore, this section chooses the consumption of communication traffic and node access time to complete the estimation of communication overhead. The communication overhead is evaluated from the communication traffic consumption, taking Byte as the unit. When the communication traffic is higher, the corresponding terminal energy consumption is higher.

In order to verify the performance of the proposed method, three other terminal access authentication schemes are simulated, namely RCA scheme based on RSA cryptosystem, ECA scheme based on ECC cryptosystem and traditional CA scheme. Under the four schemes, the unified setting node is successfully authenticated for 2 to 14 times. After each successful authentication, the terminal leaves the network and re-initiates the authentication with a delay of 200 ms. The communication traffic consumption under each scheme was recorded respectively, and the simulation results were shown in Fig. 3.

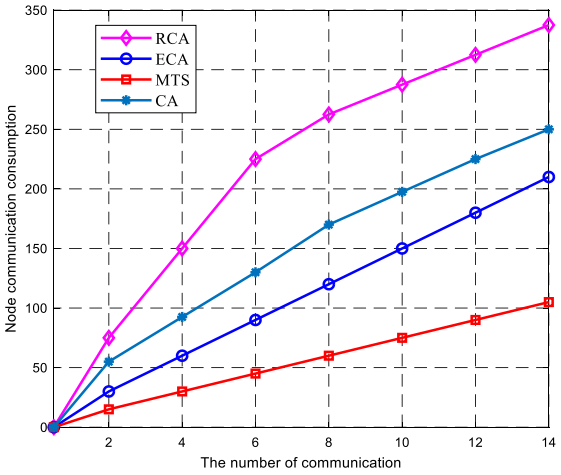

Fig. 3. The comparison of communication consumption of node access.

According to the analysis of simulation results in Fig. 3, the method proposed in this paper has a great advantage in communication consumption because, compared with other schemes, the key of terminal and master server is uniquely stored. In the second access, if the authorized terminal can directly obtain the security access permissions, there is no need to recertification, thus greatly reducing the communication overhead.

Next, we evaluate the communication cost from the access authentication time. The longer the access time is, the higher the corresponding terminal energy consumption will be. Under the four schemes, the unified set node is successfully authenticated for 2 to 14 times. After each successful authentication, the node leaves the network and re-initiates the authentication with a delay of 200 ms. The average access time of each scheme was recorded, and the simulation results were shown in Fig. 4.

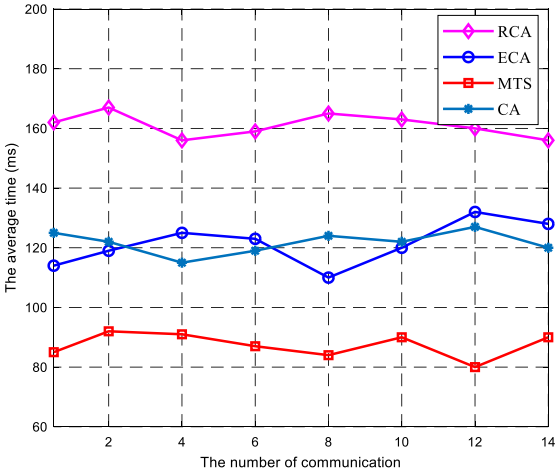

Fig. 4. The comparison of average time of node access.

According to the analysis of simulation results in Fig. 4, the improved MTS in this paper has a great advantage in average access time, because the improved access authentication scheme has a certain advantage in terms of fewer authentication exchange times and the minimum computation required for authentication. To sum up, the MTS method proposed in this paper has some improvements in communication traffic consumption and access time of nodes, which proves that the scheme has a more lightweight improvement in communication overhead.

From the analysis above, we can find that the proposed terminal access scheme can not only realize better secure access efficiency, but also have better performance in communication overhead. This is of great help to large-scale terminal security access under 5G power business network. Therefore, the method presented in this paper is lightweight and effective.

5 Conclusion

This paper proposes a lightweight and efficient terminal secure and reliable access method in 5G power service network. Considering the core idea of security stratification and network special, we design a three-layer terminal security access framework to ensure the security of terminals in the access process and data protection process. Then, we propose a lightweight terminal security access scheme to adapt to large-scale terminal access power network scenario. The simulation results show that the proposed method can reduce the communication overhead and provide good security.

References

1. Wang, Y., Yang, W., Shang, X., Hu, J., Huang, Y., Cai, Y.: Energy-efficient secure transmission for wireless powered internet of things with multiple power beacons. IEEE Access **6**, 75086–75098 (2018)

2. Liming, C., Xuzhu, D., Baoren, C., Jin, L., Qiqi, W.: Reliability enhancement of public wireless communication for remote control services in power distribution in smart grid. In: Proceedings of CICED'18, pp. 1700–1704 (2018)
3. Jiang, D., Wang, Y., Lv, Z., Wang, W., Wang, H.: An energy-efficient networking approach in cloud services for IIoT networks. IEEE J. Sel. Areas Commun. **38**(5), 928–941 (2020)
4. Guo, S., Hu, X., Zhou, Z., Wang, X., Qi, F., Gao, L.: Trust access authentication in vehicular network based on blockchain. China Commun. **16**(6), 18–30 (2019)
5. Lubega, P., Ssettumba, T., Nabuuma, H., Serugunda,J.: A secure energy efficient multi-user selection scheme for SWIPT wireless IoT networks in the presence of cooperative jamming. In: Proceedings of TELFOR'19, pp. 1–4 (2019)
6. Jiang, D., Huo, L., Song, H.: Rethinking behaviors and activities of base stations in mobile cellular networks based on big data analysis. IEEE Trans. Netw. Sci. Eng. **7**(1), 80–90 (2020)
7. Chaudhry, S.A., Alhakami, H., Baz, A., Al-Turjman, F.: Securing demand response management: a certificate-based access control in smart grid edge computing infra-structure. IEEE Access **8**, 101235–101243 (2020)
8. Sha, K., Alatrash, N., Wang, Z.: A secure and efficient framework to read isolated smart grid devices. IEEE Trans. Smart Grid **8**(6), 2519–2531 (2017)
9. Jiang, D., Wang, W., Shi, L., Song, H.: A compressive sensing-based approach to end-to-end network traffic reconstruction. IEEE Trans. Netw. Sci. Eng. **7**(1), 507–519 (2020)
10. Navya, M., Sanjay, H.A., Deepika, K.: Securing smart grid data under key exposure and revocation in cloud computing. In: Proceedings of I4C'18, pp. 1–4 (2018)
11. Chekired, D., Khoukhi, L., Mouftah, H.: Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model. IEEE Trans. Industr. Inf. **14**(3), 1220–1231 (2018)
12. W. Chen, B. Liu, H. Huang, et al. When UAV swarm meets edge-cloud computing: The QoS perspective, IEEE Network, 2019, 36–43
13. Liu, B., Jia, D., Wang, J., et al.: Cloud-assisted safety message dissemination in VANET–cellular heterogeneous wireless network. IEEE Syst. J. **11**(1), 128–139 (2017)
14. Jiang, D., Huo, L., Li, Y.: Fine-granularity inference and estimations to network traffic for SDN. PLoS One **13**(5), 1–23 (2018)
15. Zhou, Y., Zhu, X.: Analysis of vehicle network architecture and performance optimization based on soft definition of integration of cloud and fog. IEEE Access **7**(2019), 101171–101177 (2019)
16. El-sayed, H., Sankar, S., Prasad, M., et al.: Edge of things: the big picture on the integration of edge, IoT and the cloud in a distributed computing environment. IEEE Access **6**, 1–12 (2018)
17. Jiang, D., Li, W., Lv, H.: An energy-efficient cooperative multicast routing in multi-hop wireless networks for smart medical applications. Neurocomputing **2017**(220), 160–169 (2017)
18. Zhang, K., Mao, Y., Leng, S., et al.: Mobile-edge computing for vehicular networks. IEEE Veh. Technol. Mag. **12**, 36–44 (2017)
19. Pu, L., Chen, X., Mao, G., et al.: Chimera: an energy-efficient and deadline-aware hybrid edge computing framework for vehicular crowdsensing applications. IEEE Internet of Things J. **6**(1), 84–99 (2019)
20. Jiang, D., Wang, Y., Lv, Z., Qi, S., Singh, S.: Big data analysis based network behavior insight of cellular networks for industry 4.0 applications. IEEE Trans. Ind. Inf. **16**(2), 1310–1320 (2020)
21. Eldjali, C., Lyes, K.: Optimal priority-queuing for EV charging-discharging service based on cloud computing. In: Proceedings of the ICC'17, pp. 1–6 (2017)
22. Xie, R., Tang, Q., Wang, Q., et al.: Collaborative vehicular edge computing networks: architecture design and research challenges. IEEE Access **7**(2019), 178942–178952 (2019)

23. Jiang, D., Huo, L., Lv, Z., Song, H., Qin, W.: A joint multi-criteria utility-based network selection approach for vehicle-to-infrastructure networking. IEEE Trans. Intell. Transp. Syst. **19**(10), 3305–3319 (2018)
24. Yang, Y., Niu, X., Li, L., et al.: A secure and efficient transmission method in connected vehicular cloud computing. IEEE Netw. **32**, 14–19 (2018)
25. Jiang, D., Zhang, P., Lv, Z., et al.: Energy-efficient multi-constraint routing algorithm with load balancing for smart city applications. IEEE Internet of Things J. **3**(6), 1437–1447 (2016)
26. Kaur, K., Garg, S., Kaddoum, G., et al.: Demand-response management using a fleet of electric vehicles: an opportunistic-SDN-based edge-cloud framework for smart grids. IEEE Netw. **33**, 46–53 (2019)
27. Guo, H., Zhang, J., Liu, J.: FiWi-enhanced vehicular edge computing networks. IEEE Veh. Technol. Mag. **14**, 45–53 (2019)