Implementation Method Of Remote Assistance Instruction Based On Hardware Secure Encryption

Birong Huang\textsuperscript{1,4}, Zhansheng Hou\textsuperscript{2,3*}, Peng Lin\textsuperscript{2,3}, Fei Zhou\textsuperscript{2,3}

\textsuperscript{1}Zhangjiagang Power Supply Branch of State Grid Jiangsu Electric Power Co. LTD, Jiangsu, China

\textsuperscript{2}Global Energy Interconnection Research Institute, Nanjing, Jiangsu, China

\textsuperscript{3}State Grid Key Laboratory Of Information & Network Security, Nanjing, China

\textsuperscript{4}First author’s e-mail: huangbirong@jji.sgcc.com.cn

*Corresponding author’s e-mail: houzhansheng@geiri.sgcc.com.cn; 275512643@qq.com

Abstract. As a public service enterprise related to energy security and national economy and people's livelihood, the safe work is related to all walks of life and thousands of households. In power scenarios, the remote cooperative guidance needs to ensure the security of data communication. The implementation method of remote cooperative guidance in power scenarios based on hardware security encryption realizes the functions of terminal registration, user online and offline management, message call, control signaling negotiation, audio and video real-time call, graphic guidance and target tracking and labeling. Configuration TF card encryption at the mobile terminal chip and video server configuration high speed encryption card, WIFI / 4 g wireless networks to establish encryption channel, remote collaborative guidance terminal power scene registration messages, messages, call, and by guiding and structured data security encryption transmission, the unstructured data such as audio stream and video stream is encrypted. It not only realizes the secure encryption of message communication, but also guarantees the high-speed transmission of audio and video streams.

1. Introduction

With the development of Internet information and communication technology, the development of audio and video communication technology has mainly experienced four development stages: local analog signal audio and video system, pc-based multimedia remote assistance system, Web server-based remote audio and video cooperation system, and mobile terminal audio and video cooperation system. At present, the development of audio and video technology is in the stage of remote assistance system based on mobile terminal\cite{1}. The mature products of mobile terminal mainly include Skype, QQ and wechat audio and video call. As a public service enterprise related to energy security and national economy and people's livelihood, the safe work is related to all walks of life and thousands of households.
The power system is large in scale, various in equipment and complex in structure, which requires remote experts or on-site audio and video cooperation and guidance during power operation. In order to prevent user data, message communication data, and power equipment information from being stolen, data communication security needs to be guaranteed in audio and video cooperation guidance. However, in power operation scenarios, due to the large electromagnetic and noise interference of power equipment and the unstable wireless network, especially the low processing performance of mobile terminal hardware, audio and video streams are not encrypted to ensure the real-time smooth transmission of audio and video data on mobile terminals. Therefore, how to ensure the safe transmission of message communication and user data as well as the smooth transmission of audio and video data under the conditions of low processing performance of mobile terminals and interference and instability of wireless networks is an urgent problem to be solved[1].

In order to solve the above problem, developed based on the hardware security encryption method to realize the remote collaborative guidance power scene, in power scene network bandwidth is not high and the power performance of mobile terminals limited cases, for power scene remote collaborative guidance message communications security encryption, to unencrypted transmission of audio and video stream, both achieve power scene remote collaborative guidance message communications security encryption, It also realizes the high-speed transmission of audio and video streams.

2. Remote collaborative video server design
The remote collaboration guide for power scenarios includes mobile terminals and video servers, and mainly implements message services and media services. Secure the communication of remote cooperative guidance messages in power scenarios, and transmit audio and video streams without encryption. TF card encryption chip is configured in mobile terminal and high-speed encryption card is configured in video server. Encryption channel is established through WIFI/4G wireless network, and terminal registration, heartbeat message, call message, control signaling negotiation, drawing guidance and annotation information are transmitted on the encryption channel[2].

Video server includes system management, message service and media service, as shown in Figure 1.

![Fig 1. Terminal and server services architecture](image)

The remote collaboration terminal and server include two parts: message control service and audio and video streaming service.
2.1. Message control service
Message control services include user registration, group management, message receiving, message forwarding, message processing, signaling negotiation messages, transmission control messages, user online and offline messages, and target tag tracing messages. The specific functions are as follows:

2.1.1. Terminal registration
On the basis of a TCP connection, the client to the message server registration function, user ID, user name, send message server, the server according to user's ID and reverse the query the user IP address, user name video calling port, the conference room information such as ID and the meeting room name, and in the cache to maintain a user information table, after the success of the registration, The message server returns an ACK acknowledgement[3].

2.1.2. Group management
Message server maintains a user online form in the cache, each new user registration, to the entire network radio users online information, and each user to keep the heart function, when the user logoff or disconnected, the news broadcast to the entire network user logoff, client configuration interface if people can see the user list online news[3].

2.1.3. Message sending and receiving
To create, send, and receive messages between terminals and servers.

2.1.4. Message processing
After receiving a message from the peer, the terminal and server parse the message fields, extract the message content according to the IP address, port, and session Id of the peer, and process the message.

2.1.5. Signaling negotiation messages
The port number, session Id, and packet header field are negotiated between terminals and servers, and between terminals.

2.1.6. Transmission of control messages
Transfer control, congestion control, and bandwidth management functions are implemented between terminals and servers and between terminals. Based on the terminal network adaptive transmission rate control technology, the low-delay flow transmission control, bandwidth management and congestion control technology are studied to ensure the real-time transmission and management of audio and video data streams in the process of remote assistance[4].

2.1.7. User login and logout messages
Launched after each meeting, in the message server cache maintained in a conference room personnel list, when the new message to join the meeting personnel, multicast to online meeting room personnel, at the same time meeting room for personnel list will be distributed to the newcomer, when a user exit meeting, will withdraw from the message server meeting message to the conference room other personnel of multicast[5].

2.1.8. Target labeling tracking information
Based on the audio and video assistance technology, this paper studies the interactive superposition technology of information guidance of two-dimensional vector map, picture and
text, and realizes the information superposition operation of text, picture and vector map, so as to realize the remote audio and video assistance and text guidance information. Assume that terminals A, B, and C, in the process of video collaboration: Annotate the video collected by B on intelligent terminal A and send the annotated information to B and C through the message server; Terminal B and C are used to annotate the drawing text again, so as to realize graphic guidance and target tracking annotation. Firstly, the target is guided by drawing, and then the target object is recognized, matched and tracked by the feature based target tracking and recognition algorithm[6].

2.2. Audio and video streaming services
Audio and video streaming services include audio and video stream collection, audio and video codec, audio and video stream synchronization, audio and video stream push, audio and video stream receive, video quality enhancement, audio echo cancellation, target tracking and labeling overlay, etc. Audio codec uses AAC, PUS, and PCM, and video codec uses H264. The video resolution supports VGA (640x480), SVGA (800x600), and 720P (1280x720). Research on audio and video codec technology in mobile terminal, achieve fast and efficient audio and video data codec algorithm compatible with multi-platform mobile terminal equipment, improve the fluency and compatibility of remote collaboration business[7]. Based on the relative time stamp algorithm and audio and video data processing algorithm, the multi-party audio and video data stream synchronization technology is studied to realize the synchronous transmission of audio and video in the process of remote assistance and ensure the consultation quality of remote assistance. Based on the characteristics of the noise environment, the active noise reduction technology is adopted to reduce the noise of the sound and improve the clarity of the audio call. The high-speed phase correlation motion estimation algorithm is used to reduce the influence of jitter and enhance the video image. In the face of the network bandwidth change, the adaptive adjustment technology of video resolution is used to provide appropriate audio and video quality[8].

3. Hardware encryption data security method
In view of the information security risks that the system may face, reasonable and effective security protection measures shall be taken to ensure the safe and stable operation of the system, the security of system service data, and the normal operation of the system business. Ensure data security, resist the main security risks faced by the system, and ensure the safe, stable and reliable operation of applications; Ensure the confidentiality, integrity and availability of system data; It provides a safe and reliable operating environment for system services and supports the safe and stable development of services. In accordance with information security protection requirements, multi-layer defense measures are adopted to strengthen data transmission and encryption of sensitive indicators[9]. In the power scenario, remote cooperation guides secure encryption: Messages are transmitted over secure encryption channels, while audio and video streams are transmitted over unencrypted channels, as shown in Figure 2.
3.1. Message communication encryption
Asymmetric encryption algorithms (such as RSA, DSA, and ECC) are used to manage the secret keys of symmetric algorithms, and symmetric encryption algorithms (such as DES, 3DES, and AES) are used to encrypt data. TF card encryption chip is configured for mobile terminal, high-speed encryption card is configured for video server, and hardware encryption channel is established through WIFI/4G wireless network[10]. The hardware encryption mode is used for encryption, and the terminal registration, heartbeat message, call message, control signaling negotiation message, instructional drawing, and target tracking annotation information are transmitted over the encryption channel.

3.2. Audio and video transmission
Audio and video streams are transmitted through non-encrypted channels, which not only realizes the secure encrypted transmission of remote cooperative message communication in power scene, but also realizes the high-speed and smooth transmission of audio and video streams.

4. Conclusions
The implementation method of cooperation guidance based on hardware security encryption, including mobile terminal and video server, mainly realize the function of message service and media service. Secure the communication of remote cooperative guidance messages in power scenarios, and transmit audio and video streams without encryption. TF card encryption chip is configured in mobile terminal and high-speed encryption card is configured in video server. Encryption channel is established through WIFI/4G wireless network, and terminal registration, heartbeat message, call message, control signaling negotiation, drawing guidance and annotation information are transmitted on the encryption channel.
Under the conditions of low network bandwidth and limited performance of power mobile terminals in power scenarios, the secure encryption of remote cooperative guidance message communication in power scenarios and the non-encrypted transmission of audio and video streams not only realize the secure encryption of remote cooperative guidance message communication in power scenarios, but also realize the high-speed transmission of audio and video streams.

Acknowledgments
This work was financially supported by the science and technology project to State Grid Corporation.

Reference
[1] Zhang, Y. H., Ma C. Y. (2017) Digital Communication World, (06) : 22-24.
[2] Ji, X. D., Zhang, H. (2019) Application of DES data encryption algorithm in computer communication. Information recording materials, 20 (08) : 90-91.
[3] George, W. (2009) Object-Oriented Software Engineering, Addison-Wesley Press, pp. 34-39.
[4] Liao, K. J. (2011) Browser/Server Platform Solution to the financial Software of Management Type, Computer Engineering & Science, pp. 78-91.
[5] James, A. K. (2009) Analyzing Systems, Prentice-Hall Press, pp. 67-71.
[6] Perez-Luque, M. J., Little, T. D. C. (2003) A Temporal Reference Frame work for Multimedia Schronization. IEEE Journal on Selected Aieas in Conllnunlcations, 14(l): 36-37.
[7] Chen, C. (2020) Application of data encryption technology in computer network information security. whoSatellite TELEVISION and Broadband Multimedia, (18): 99-101.
[8] Wang, J. (2019) Application of data encryption technology in computer network information security. Network security technology Surgery and Application, (5) : 31-32.
[9] Bertino, E., IEEE, M., Ferrari, E. (2008) Temporal Synchronization Models for Multimedia Data[C]. IEEE Transaction on Knowledge and Data Engineering, 10(4): 612-631.
[10] Liu, J. B. (2010) Design and implementation of streaming media player for real-time monitoring. Beijing: Beijing university of posts and telecommunications, pp. 20-25.