*Send Orders for Reprints to reprints@benthamscience.ae*

*The Open Electrical & Electronic Engineering Journal*, 2016, *10*, 181-188

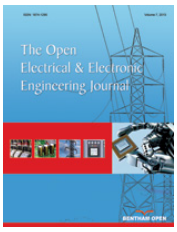

BENTHAM OPEN

CrossMark

The Open Electrical & Electronic Engineering Journal

Content list available at: www.benthamopen.com/TOEEJ/

DOI: 10.2174/1874129001610010181



RESEARCH ARTICLE

# Research on Video Monitor Data of Transmission Lines Accessing Through the Secure Access Platform

Qindong Sun[1,*], Kaixuan Gao[1], Xiaojun Hou[2], Fei Cao[1], Zuomin Luo[1] and Xinbo Huang[3]

[1]*Shaanxi Key Laboratory of Network Computing and Security, Xi'an University of Technology, Xi'an, China*
[2]*Network and Information Center, Xi'an University of Technology, Xi'an, China*
[3]*College of Electronics and Information, Xi'an Polytechnic University, Xi'an, China*

Received: June 13, 2016 Revised: August 27, 2016 Accepted: November 11, 2016

**Abstract:** Due to the unidirectional isolation characteristics of state grid secure access platform, it is an important research problem of the full tracking of transmission line. Furthermore, it is crucial for full tracking transmission line to be succeeded to transfer the data of video monitoring network to the internal network smoothly. In this paper, we analyze the structure of the secure access platform and the characteristics of the video data transmission process and propose a new method to solve the problem of the internal and external video data exchanging, which can ensure the video data crossing through the safety access platform. We deploy an intranet server and an extranet server, moreover, the extranet server sends the UDP heartbeat packets to the intranet server to maintain the network connection *via* SIP port. So the video inviting command could be transferred through the secure access platform. The experimental results show that the method can solve the problem of secure platform isolation effectively, and ensure the data of video arriving monitoring at the internal network successfully.

**Keywords:** Secure access platform, Transmission lines, UDP, Video monitoring.

## 1. INTRODUCTION

In recent years, for the rapid growth demand for electricity, the coverage rate of high voltage transmission lines is increasing, so it is a crucial problem for guaranteeing the security of transmission lines to inspect the transmission lines just in time. There are some factors, such as weather *etc.*, which make the inspection of the transmission lines delayed [1].

With the rapid development of monitoring technology [2, 3], it is convenient to track the real-time information of transmission lines by video monitor system which is installed in the camera of the high-voltage line tower, the dynamic information of the video monitor system is transmitted by 3G wireless transmission technique into monitor center for data analytics in order to fully track transmission lines. The dynamic information is the basis of recondition for monitoring personnel [4, 5]. Analyzing the dynamic information from video monitoring of transmission lines just in time has become an important part of the transmission line safety prevention system.

Previous video monitoring system was unable to satisfy the development and actual deployment demand of video monitoring system of transmission line [6]. One of the most critical problems is how to establish an interactive video data and succeed to approach secure access platform of National Grid for a smooth video streaming [7]. The national Grid secure access platform protects the security of devices in the National Grid internal network, and it also prevents the normal access of the video flow [8, 9]. Especially due to the disparity in network structure of domestic area and the barrier of secure access platform, access technology of the video stream is more important. There is another problem on the implementation and deployment of video monitoring system in power industry, which mainly focuses on the realization of the system itself and not how to the secure access platform block.

* Address correspondence to this author at the Shaanxi Key Laboratory of Network Computing and Security, Xi'an University of Technology, Xi'an, China; Tel: 029-82312231; E-mail: sqd@xaut.edu.cn

In this paper, we analyze the structure of the secure access platform and put forward a scheme for accessing secure access platform of the national power grid. Experiments cover a certain area of the northwest power debugging data network as the testing data. Experimental results show that this method can stably transmit camera video data to each client accurately, with guaranteeing a better image quality, remarkably real-time performance and low delay. We build a successful system, and the system achieves a better monitoring effect, certifying its practical value to ensure the security of transmission lines.

## 2. NETWORK STRUCTURE ANALYSIS OF SECURE ACCESS PLATFORM

Secure access platform is an important power system equipment to access Internet for the National Grid. This platform can assume the following functions of Smart Grid, such as real time monitor of intelligent terminal, secure access, secure communication and active defense and forewarning in complex environment [10].

### 2.1. The Framework of Secure Access Platform

The network secure access platform is a data filter based on the business rules pre-established by users. In order to support the separate establishment for each line filter rules, the granularity of the rules should be refined to every field including the type, scope, length, enumeration, default value, special field, character encoding, image field license *etc*. System integration stream antivirus engine can identify the SQL statement in the exchange content and can effectively prevent all SQL submission attack [11] for protecting internal business system server of a company or enterprise, as shown in Fig. (**1**).

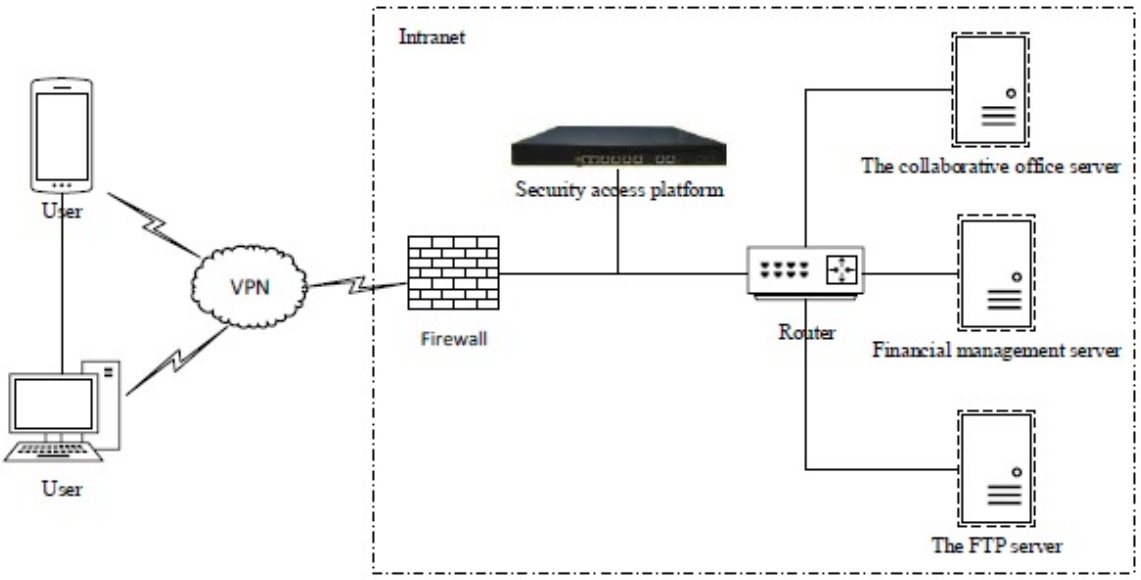



**Fig. (1).** The framework of secure access platform.

The intranet shown in Fig. (**1**) is the internal working network of state grid, and in principle, is physically separated from the external. Stem from commercial consideration the data exchange between intranet and extranet is inevitable. At present, there are two main ways for data exchange between intranet and extranet which are as follows:

1. Using encrypted USB flash disk for copying data. Due to the smallness, large storage, convenience and cheap price, USB flash disk has been widely used in enterprise information construction. More and more private information, enterprise information and sensitive information are stored in USB flash disk devices. Consequently, during the data exchanging process the USB flash disk can be the carrier of viruses or malicious code which can cause information leakage and propagation of computer viruses.
2. Filtering the external network access by secure access platform. The most outstanding feature of secure access platform is one-way data transmission. The data could enter through the external network to secure access platform, but cannot be allowed to go through the secure access platform to the extranet.

Based on the above analysis, we can see that National Grid isolates the external data by the secure access platform, which can ensure the safety of internal network. Meanwhile, it ensures the safety of the platform data by data encryption which has the function of anti-virus, while interacting with the external. The secure access platform can effectively protect the normal operation of the internal server and prevent the leakage of important internal information.

### 2.2. The Basic Composition and Function of Secure Access Platform

For the structure, the secure access platform includes two parts, the system equipment of secure access platform and the terminal device, as shown in Fig. (**2**).

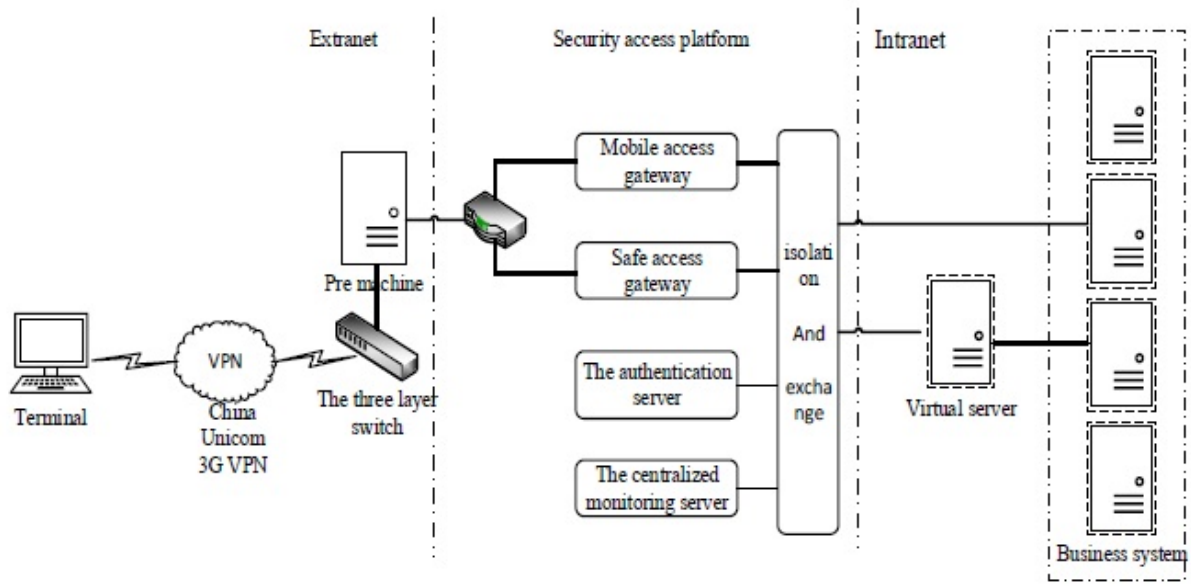



**Fig. (2).** Components of the secure access platform.

The main functional components are as follows:

#### *2.2.1. Mobile Access Gateway*

Based on the encryption of transmission data and encrypted tunnels, it provides a secret data transmission function between the mobile terminal devices and the mobile access gateway for a variety of mobile application systems.

#### *2.2.2. Security Access Gateway*

It solves the security problem of data transmission between the internal network and the external network.

#### *2.2.3. Identity Authentication System*

It is used to authenticate user's identity and builds the LDAP service in the authentication server for user identity by LDAP. There are two ways to verify the identity of each user, one is to combine user name and password, the other is digital certification [12, 13].

#### *2.2.4. Centralized Management System*

By setting the corresponding strategy, the secure terminal (client) can connect with the centralized supervision server and download the corresponding strategies to achieve the centralized monitoring and the management of terminal. After the client connected to the server, the server can monitor and manage uniformly.

#### *2.2.5. Data Filtering System*

It has the functions such as strong authentication, detection, screening and filtering operation to the data in and out of the Intranet.

#### *2.2.6. The Virtual Server*

The tablet terminals access into the integrated platform is conducted by the virtual server [14].

#### *2.2.7. Safety Terminal Device*

The secure mobile terminals, including the secure PDA and the laptop are all operated by users.

### 2.3. The Data Transmission Characteristics of Secure Access Platform

Analysis of the data transmission characteristics of secure access platform is important to data communication. As discussed in section 2.1, the prominent feature of secure access platform is to only allow extranet users to send data in one-way model through the platform to the intranet, prohibiting the intranet users to actively send any data to the outside network [15], as shown in Fig. (**3**).

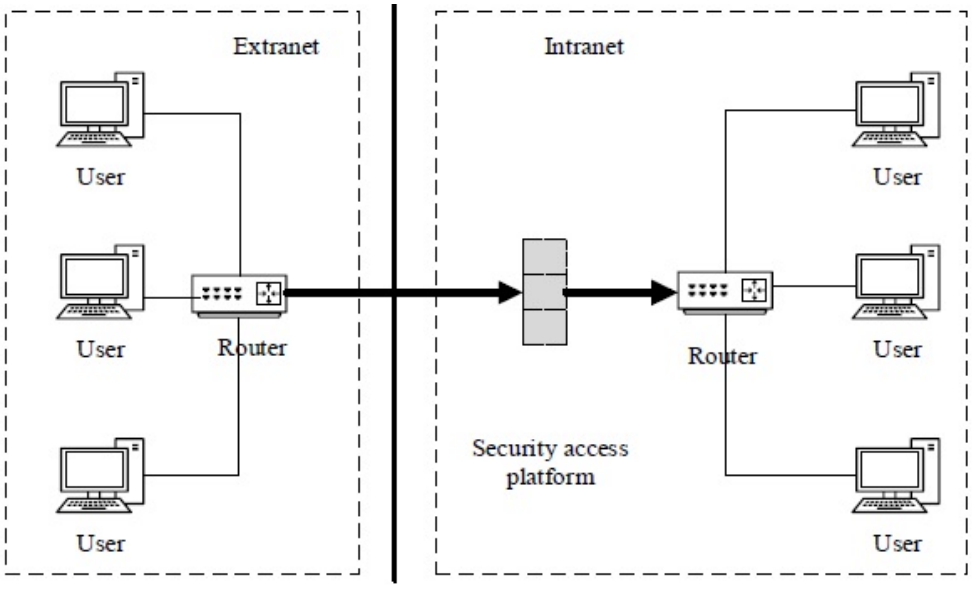



**Fig. (3).** The directions of data transmission in secure access platform.

For the network structure in a certain area in Northwest China, we learned that the intranet is part of the internal network of state grid. Which protects important information of the internal department and the normal operation of network server by Limiting users to connect with the outside. After several experiments, we organize the following two characteristics of data interaction transmitted through the network secure platform:

1. While a data package is successfully transmitted from extranet to intranet, the routing tunnel will allow data transmission in a two-way model in 15 seconds. Within the 15 seconds, intranet user can send data to extranet through this tunnel, which shows that users can actively send data to the outside hosts by penetrating the secure access platform from intranet and finally reach the goal of two-way data traffic.
2. The data to the external from the intranet will go through the proposed equipment, configured with two NICs of which one is for the external network with an address and the other is for the internal network with an address. So, the external port of proposed equipment must be known, and could be mapped to an internal network through the safety program, then, the data transmission path is completed.

## 3. VIDEO DATA ACCESS IN SECURE PLATFORM

According to the preceding analysis, we can see that, in order to realize the video streaming access in transmission line in external network from intranet staff computer, and it must be able to get through the security platform isolation. The penetration and the general NAT, named NAT penetration, is not exactly the same. NAT penetration is to resolve accessing problem without public IP. What will be discussed in this paper are the network penetration aimed at safety protective isolation and how to realize the sharing of data and data exchange under the premise of network safety. Furthermore, the deployment of video monitoring system based on power transmission line is also an important aspect

in our study.

Taking the structure of a certain area network as an example, as shown in Fig. (**4**). The camera data transmitting through China Unicom APN finally can be routed to the proposed equipment, equipped with secure access platform client software, and the data can be sent to uniformed video platform with the service center authorization of the secure access platform.

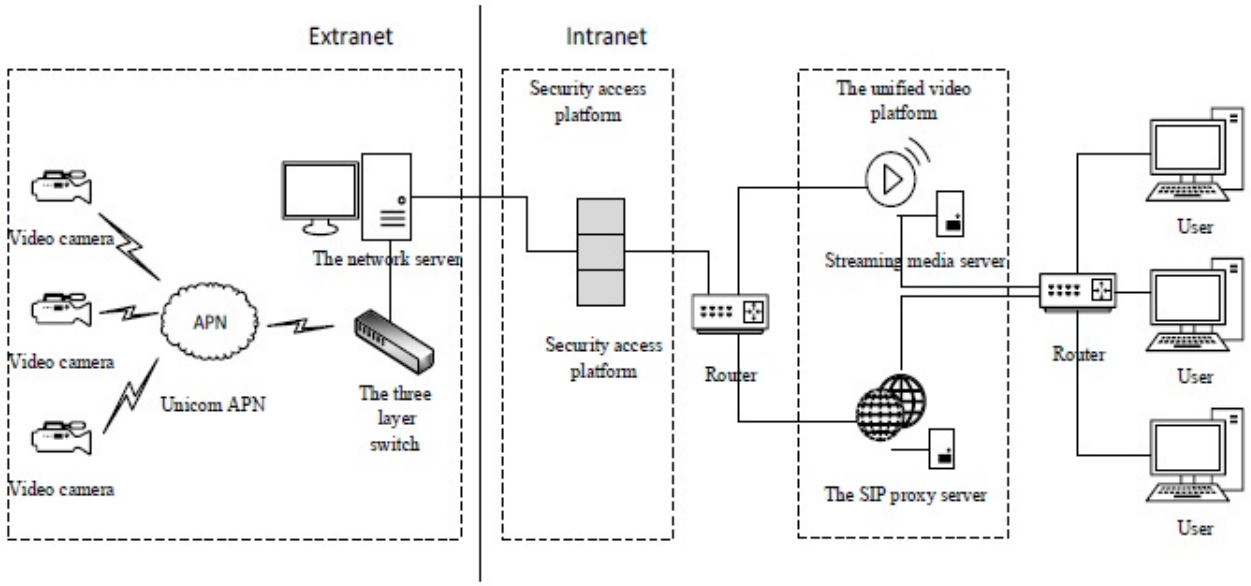



**Fig. (4).** The network topology in a company.

During the realization process of intranet secure access platform, due to the one-way feature, the video request initiated by users cannot reach the front camera. The features of data transmission in secure access platform have been illustrated in section 2.3. According to the analysis results, a solution is put forward in view of the network topology of a certain solution case in Northwest China, as shown in Fig. (**5**).

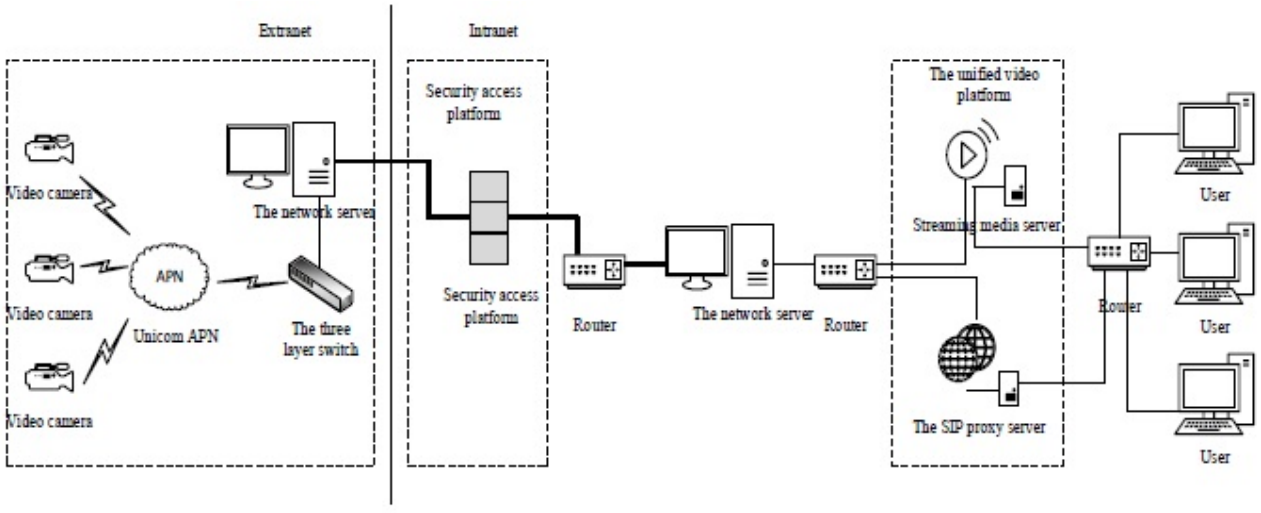



**Fig. (5).** A solution of secure access platform.

Comparing the results shown in Figs. (**4** and **5**), the key factor of data successfully passing the secure access platform is adding the intranet server as a hardware.

The video request initiated by users must be the process: intranet user sends the video request to the external camera by the user client, which means that, intranet data is unsolicited sent to the extranet. In order to ensure that the video

command can go through the secure access platform, an intranet server is installed specially. Different server programs are respectively arranged in servers in the inside and outside networks. To keep the command of video request within a 15-seconds link continuing to get through the secure access platform to the extranet server, UDP heartbeat packets will be sent off from SIP port to the intranet, which can achieve data interworking effect. Then, the server in extranet can be utilized as the second agent to send the video request from the intranet to the fore-end camera.

## 4. EXPERIMENTAL RESULTS

The proposed method of video access is verified and analyzed in this section. The client and server used for the experiments are based on Windows7 32 bit desktop operating system CPU Pentium (R) Daul-Core E5800 3.20GHz and memory in 2G. The experimental data are extracted from the specific implementation of Department of electric power system in a certain area in Northwest China. The employed networks are China Unicom broadband and China Unicom 3G network. We apply LDAP directory database as our database and utilize Wireshark as our capture tools in the experiments process.

The consecutive UDP heartbeat packets sent off from SIP port are shown in Fig. (**6**).

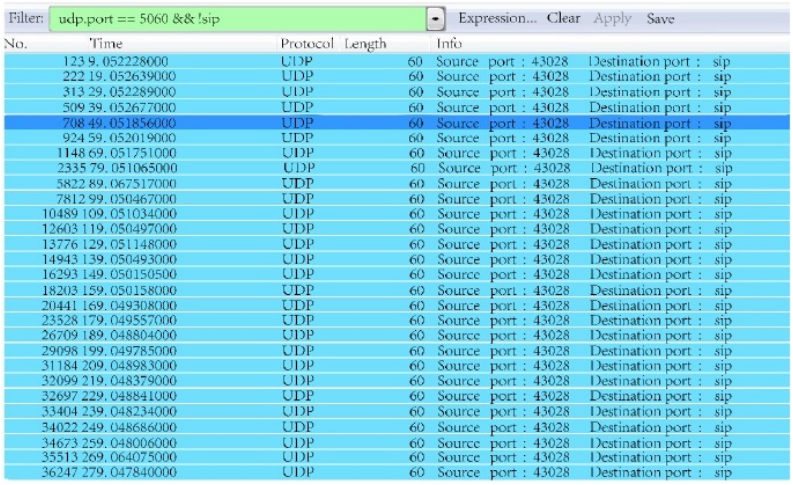



**Fig. (6).** The UDP heartbeat packets.

The captured data, from the SIP shows the process of video request, as shown in Fig. (**7**). The red line represents the packet of video request by the users in intranet. The first blue line is the packet data requested by fore-end device of No. **0012 user. The second line represents the packet of the previous, retransmitted by the intranet server. Fig. (**8**) shows the action of capturing data from the network server SIP.

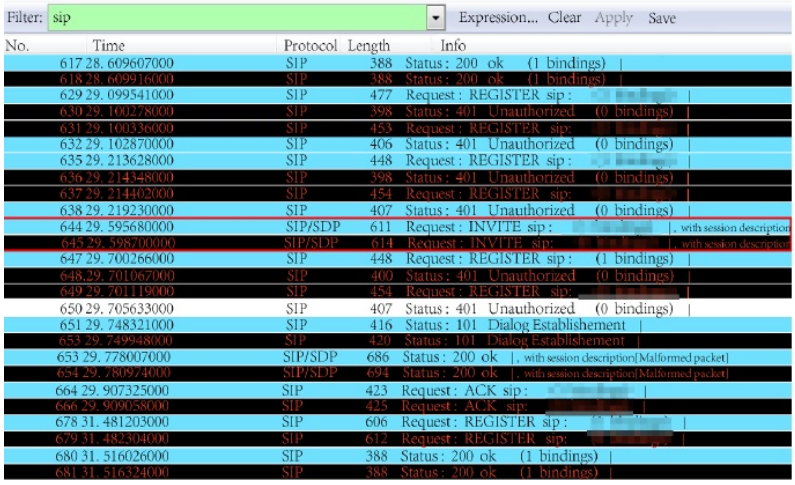



**Fig. (7).** The SIP packets from intranet server.

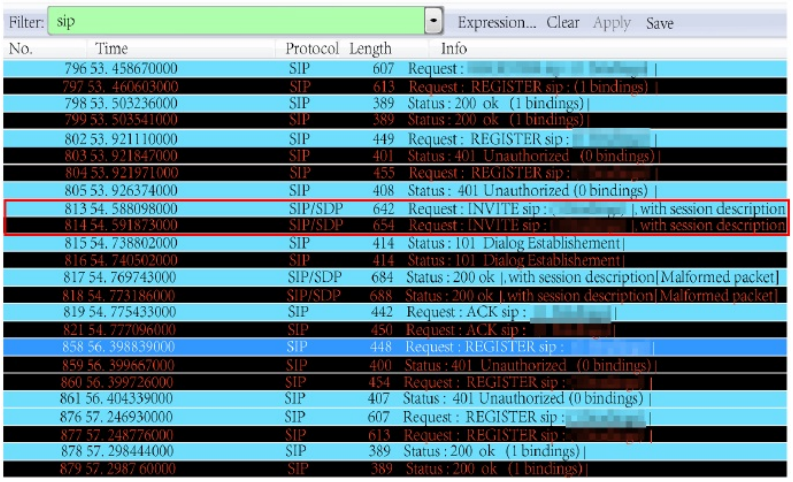



**Fig. (8).** The SIP packets of extranet sever.

The packet, requested by No. **0012 user from the intranet, captured from SIP server is shown in the red line in Fig. (**8**). The circled part in Figs. (**7** and **8**) are the server information, which cannot be provided, due to commercial privacy.

The experimental results show that the proposed solution can settle the issue of isolation caused by secure access platform effectively. Our method can ensure that the video monitoring data in transmission lines could get through the intranet successfully.

## CONCLUSION

The successful real-time tracking of transmission lines by video monitoring is correlative with the structure characteristics of power transmission lines and the secure access platform. Thus by analyzing the structure characteristics of power transmission lines and the secure access platform, we can design a framework to monitor the transmission lines and transfer the dynamic data of video monitoring network to the secure access platform.

We conclude three characteristics by analyzing the structure characteristics of power transmission lines and the secure access platform, the first characteristic is that National Grid isolates the external data by secure access platform to ensure the safety of internal network work, and National Grid ensures that the safety of the data through the platform data by data encryption, filtering and antivirus while interacting with the external, effectively protecting the normal operation of the internal server and preventing the leakage of internal important information. The second characteristic based on the secure access platform includes the system equipment of the secure access platform and the terminal device. The third characteristic is that the secure access platform of data transmission is the key factor to solve the data communication. The following two sub-characteristics of data interaction while data transmitted through the network secure platform are: firstly, while data has been transmitted in the secure platform successfully, the tunnel allows two-way transmission in 15 seconds for responding to result whether the data arrives in time; Secondly, the data to the external from the intranet will go through the proposed equipment the port between the external network and the internal network as well as client-side of National Grid. So, the external port of proposed equipment must be known, and could be mapped to an internal network by the safety program, then, the data transmission path is completed.

Based on three characteristics, we propose a real-time video monitoring framework of transmission lines to validate the the dynamic transferring of video monitoring network data of transmission lines to the secure access platform smoothly. The proposed method could be a reference for departments of electric power enterprises in data communication in network.

## CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

## ACKNOWLEDGEMENTS

The research presented in this paper is supported partly by the Project of Xi'an Beilin District Technology Bureau

(No.: GX1411), the Project of Xi'an Technology Bureau (No.: CXY1437-6, CXY1509-5) and Shaanxi Science & Technology Co-ordination & Innovation Project (No.: 2016KTZDGY05-09) and the National Natural Science Foundation of China (No.: 61172124).

## REFERENCES

[1] X.Z. Zhang, J.Q. Fan, and M. Du, "The real-time monitoring system of snowpack on high-voltage power lines", *Computer Technology and Its Applications,* vol. 40, no. 3, pp. 130-132, 2014.

[2] L.H. Mei, "A design of electric power systems video monitoring supporting for new control protocol SIP", *Jisuanji Celiang Yu Kongzhi,* vol. 18, pp. 594-597, 2010.

[3] L.H. Mei, and W.B. Jin, "Design and realization of SIP control system for substation monitoring", In: *Proceedings of the Chinese Society of Universities for Electric Power System & Its Automation,* vol. 22. 2010, no. 6, pp. 62-66.

[4] W. Liu, S. Huang, K. Ma, and H. Chen, "Application of video monitoring system in power system", *Guangdong Electric Power,* vol. 27, no. 4, pp. 57-60, 2014.

[5] X.B. Huang, *Substation Equipment On-line Monitoring and Fault Diagnosis.,* China Electric Power Press, 2013, pp. 165-167.

[6] Z.H. Zhang, "Research and application of online video surveillance system for high-voltage power lines", *Power System Protection and Control,* vol. 16, pp. 149-153, 2013.

[7] H. Yang, T. Guo, and L.G. Xu, "The implementation of data secure access based on unified video monitoring platform", *Electronic Technology & Software Engineering,* vol. 09, pp. 187-189, 2014.

[8] C. Qin, T. Zhang, and W.M. Lin, "Design and implementation of safe access system for electric mobile operation based on PDA", *Dianli Xitong Zidonghua,* vol. 36, no. 11, pp. 82-85, 2012.

[9] M. Xu, Z.S. Hou, and N.G. Li, "Secure access platform improved system based on regional division", *Applied Mechanics & Materials,* vol. 519-520, pp. 273-276, 2014.
[http://dx.doi.org/10.4028/www.scientific.net/AMM.519-520.275]

[10] D.H. Xiao, and L. Lin, "Solution scheme of integrated video surveillance platform of power system", *Dianli Xitong Zidonghua,* vol. 37, no. 5, pp. 74-80, 2013.

[11] K.H. Wu, J.Z. Liu, and T. Zhang, *Security Defense System and Key Technology of Power Information Systems,* Science Press: Bejing, 2011.

[12] L.H. Mei, "Design of a new substation video monitoring system based on SIP", *Dianli Xitong Zidonghua,* vol. 34, no. 3, pp. 66-69, 2010.

[13] J. Zhang, N. Hu, and M.K. Raja, "Digital certificate management: Optimal pricing and CRL releasing strategies", *Decision Support Systems,* vol. 58, pp. 74-78, 2014.
[http://dx.doi.org/10.1016/j.dss.2012.12.043]

[14] A.V. Cleeff, W. Pieters, and R.J. Wieringa, "Security implications of virtualization: A literature study", In: *International Conference on Computational Science and Engineering,* vol. 4. 2009, pp. 353-358.
[http://dx.doi.org/10.1109/CSE.2009.267]

[15] G.M. Huang, and X.S. Zhu, "Research on peer-to-peer model of passing through NAT devices based-UDP protocol", *Computer Engineering and Design,* vol. 2, pp. 317-320, 2010.