A Study on Application of the Net Gap in High-speed Railway Earthquake Early-warning and Monitoring System

Jingsheng Li[1*], Shi Zhang[2] and Lin Zhao[3]

[1]Postgraduate Department, China Academy of Railway Sciences, Beijing, 100081, China

[2]Shenyang Train Operation Depot, China Railway Shenyang Group Co., Ltd., Shenyang, Liaoning, 110000, China

[3]Railway Science and Technology Research & Development Center, China Academy of Railway Sciences Corporation Limited, Beijing, 100081, China

[*]Corresponding author's e-mail: wonderful740@126.com

Abstract: This paper puts forward a solution for ensuring data security of the internal network of railway while the earthquake early-warning and monitoring system for high-speed railway (EEMS) exchanges data with national or provincial earthquake networks. The solution is based on the principle of Net Gap, and fulfils the security needs of data exchange between the internal and external network of railway when the EEMS and national or provincial earthquake networks are interconnected. It guards the data exchange between the two and fulfils security needs during the exchange while ensuring security isolation, thus is more secure than conventional security methods.

1. Introduction

China High-speed Railway Earthquake Early-warning System(CRES for short) is composed of two parts: High-speed Railway Earthquake Early-warning and Monitoring System(EEMS for short) and On-board Earthquake Emergency Treatment Device (EETD for short). The earthquake is a harmful disaster[1], especially for the high-speed railway, even a small magnitude of earthquake may lead to major safety accidents of train operation. The CRES can effectively prevent or mitigate the impact of earthquake disasters on the safety of railway transportation and avoid significant casualties and economic losses[2-3]. At present, the earthquake monitoring stations of CRES are almost along the railway, and the scope of its monitoring was limited. Compared with the data monitored by the national earthquake networks, it is hard for the earthquake monitoring stations along the railway to monitor the earthquake parameters more precisely, which makes it difficult to provide the basis for stop and recovery the train[4]. In order to fully integrate and utilize various seismic resource and information, and obtain more comprehensive and accurate seismic data, the CRES is supposed to interconnect from national/provincial earthquake networks, the data monitored by the railway department and the earthquake department should be shared[5]. However, the EEMS builds the network by the railway network, and interconnects from the earthquake authorities by public network[6], how to ensure the security and integrity of data exchanged between the internal and external network of railway is one of the important issues that need to be solved. Although the traditional methods and means of security protection are widely used, they cannot completely guarantee the security of the network because they are still connected from the network. The Net Gap is a kind of security device, which can guarantee the isolation of the internal and external network of railway, meanwhile realize the data exchange, it makes up the deficiency of traditional security protection methods[7]. This paper analyzes the principle of the Net Gap and applies it to the interconnection between the EEMS and national/provincial earthquake networks, in this way, security transmission of data exchange between the EEMS and national/provincial earthquake networks is realized.

2. The Net Gap Technology

The Net Gap technology was first appeared in foreign countries. The first Net Gap product in China was developed in 2000. Now the Net Gap has been widely used in the government, finance, transportation and other fields in our country[7].

2.1. The Structure of the Net Gap

The Net Gap is also called Security Isolation and Information Exchange System, it could achieve the exchange of data between the two networks by the means of information ferrying while disconnecting the two different security levels of physical network connections and network protocols at the same time. The Net Gap is consisted of three parts, i.e. external processing unit, internal processing unit and security isolation hardware, and in which the security isolation hardware including solid state storage medium and control circuit[8]. The external processing unit is connected from the external network, while the internal processing unit is connected from the internal network. The structural diagram of the Net Gap is shown in figure 1.

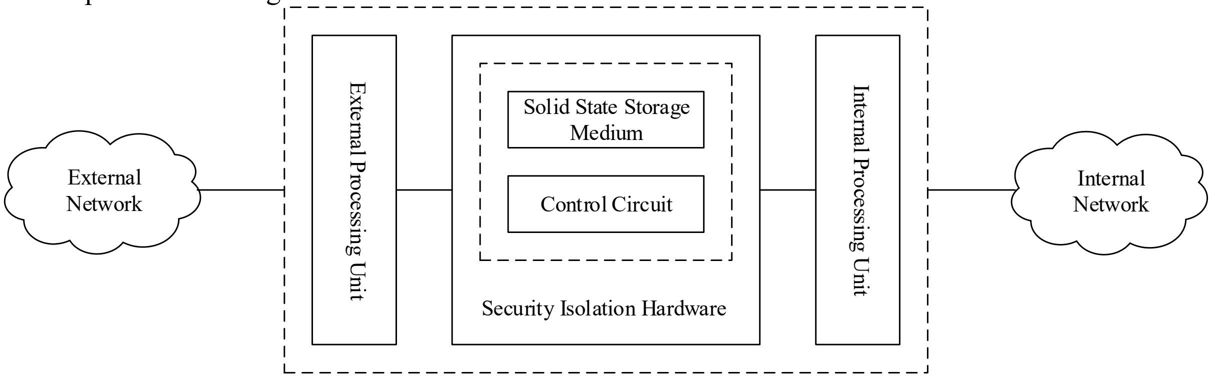

Figure 1. Structural diagram of the Net Gap.

2.2. The Principle of the Net Gap

As the internet is achieved based on TCP/IP protocols, the loopholes could be prevented and thus the network could be prevented from being attacked by disconnecting the TCP/IP connection. The internal and the external network cannot be connected simultaneously, and the TCP/IP connection between the internal and the external network was break by the Net Gap, and the internal and external network cannot communicate by protocols, by which the Net Gap was achieved.

2.3. The Procedure of Data Exchange

2.3.1. No Data Exchange. The Net Gap, external network and internal network is completely disconnected if there is no data exchange, while the solid state storage medium is dominated by the control circuit of the security isolation hardware to connect from either the external processing unit or the internal processing unit at the same time, which ensuring the physical isolation between the external network and the internal network. At this time, the state of the switch controlled by the control circuit is shown in figure 2[9].

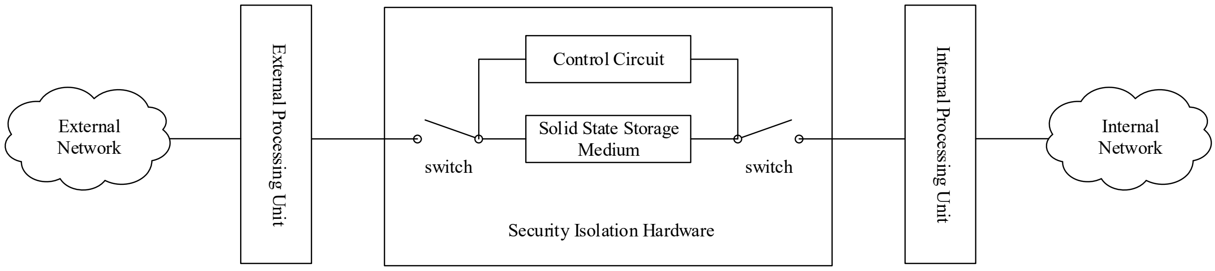

Figure 2. Both of the internal and external processing unit disconnected from the solid state storage medium.

2.3.2. Data Exchange from the External Network to the Internal Network. The external processing unit initiates non TCP/IP protocol connections to the security isolation hardware when exchanging data from the external network to the internal network. After all the protocols have been stripped, the original data will be written to the solid state storage medium. At this time, the state of the switch controlled by the control circuit is shown in figure 3. The data can be checked for safety and integrity if necessary. The network connection between the security isolation hardware and the external processing unit will be interrupted immediately after the data is written to the solid state storage medium, and non TCP/IP protocol connections to the internal processing unit will be initiated by the security isolation hardware, the data in the solid storage medium will be pushed to the internal processing unit. At this time, the state of the switch controlled by the control circuit is shown in figure 4. The data will be encapsulated according to the TCP/IP and application protocols immediately after it is received by the internal network, and then the encapsulated data will be transmitted to the internal network. The connections between the Net Gap and the internal network will be cut off immediately after data transmission. At this time, the state of the switch controlled by the control circuit is shown in figure 2.

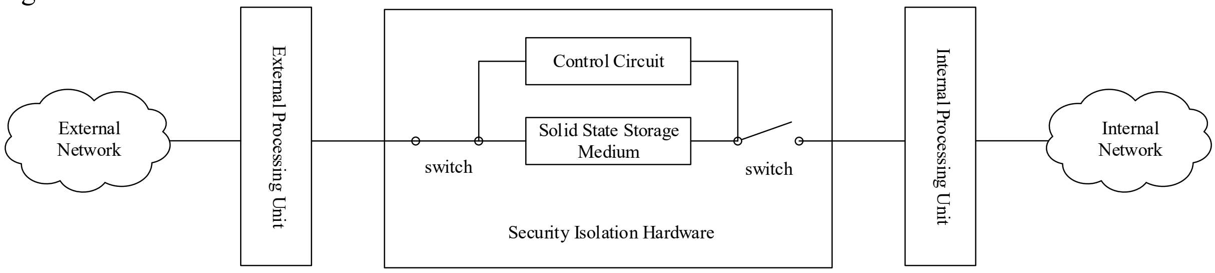

Figure 3. The external processing unit connected from the solid state storage medium while the internal processing unit disconnected from the solid state storage medium.

2.3.3. Data Exchange from the Internal Network to the External Network. When data is exchanged from the internal network to the external network, the similar process will be followed, but in opposite direction. The internal processing unit initiates non TCP/IP protocol connections to the security isolation hardware when exchanging data from the internal network to the external network. After all the protocols have been stripped, the original data will be written to the solid state storage medium. At this time, the state of the switch controlled by the control circuit is shown in figure 4. The data can be checked for appropriate if necessary. The network connection between the security isolation hardware and the internal processing unit will be interrupted immediately after the data is written to the solid state storage medium, and non TCP/IP protocol connections to the external processing unit will be initiated by the security isolation hardware, the data in the solid storage medium will be pushed to the external processing unit. At this time, the state of the switch controlled by the control circuit is shown in figure 3. The data will be encapsulated according to the TCP/IP and application protocols immediately after it is received by the external network, and then the encapsulated data will be transmitted to the external network. The connections between the Net Gap and the external network will be cut off immediately after data transmission. At this time, the state of the switch controlled by the control circuit is shown in figure 2[10].

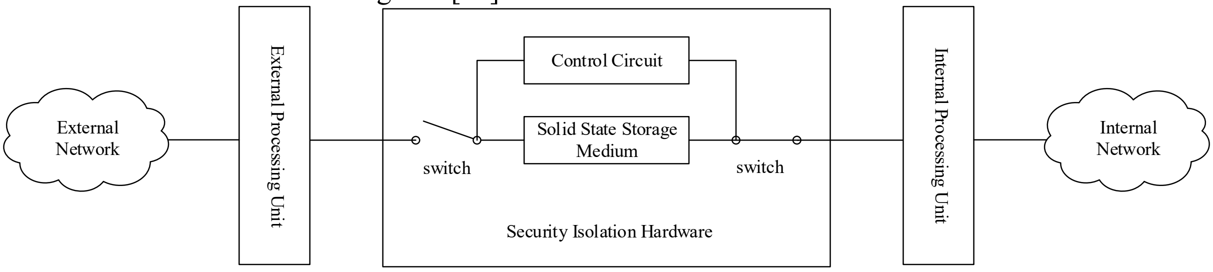

Figure 4. The internal processing unit connected from the solid state storage medium while the external processing unit disconnected from the solid state storage medium.

3. Deployment of the Net Gap in EEMS

Two tier architecture is used by the EEMS, the first tier is earthquake early warning and monitor central system of railway administrator, and the second tier is locale monitoring device. The network interface server in the hardware device of earthquake early warning and monitor central system of railway administrator is used to exchanging data with national/provincial earthquake networks[6]. As one interface of the earthquake early warning and monitor central system of railway administrator, the network interface server is connected from the railway network, it will cause great losses once it is attacked, and it belongs to the internal network of the railway. On the other side of the network interface server is public network, and it belongs to the external network of the railway. The Net Gap should be deployed outside the network interface server in order to resist the attack of the external network of the railway. The deployment of the Net Gap in EEMS is shown in figure 3.

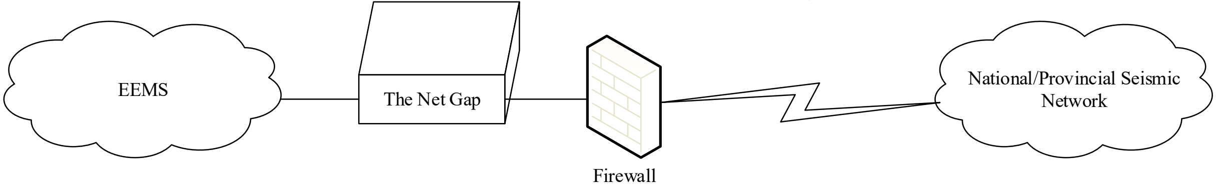

Figure 5. Deployment of the Net Gap in EEMS.

4. Conclusion

In this paper, a solution for security data transmission based on the Net Gap technology was provided by analyzing the security requirements of data exchange between the EEMS and the national/provincial earthquake networks, by which the internal and the external network of the railway was isolated and data was exchanged safely. The solution could meet the security requirements of data exchange across different secure domain networks, and has certain reference values for research and application in the future.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (High Speed Railway Joint Fund)(No. U1534202).

References

[1] Norio, O., Ye, T., Kajitani, Y., Shi, P.J., Tatano, H. (2011) The 2011 eastern Japan great earthquake disaster: Overview and comments. International Journal of Disaster Risk Science, 2(1): 34-42.

[2] Yuan, Z., Shan, X., Xu, S., Li, J., Li, J., Qiao, Y. (2007) An overview of earthquake early warning technology. Journal of Natural Disasters, 16(6): 216-223.

[3] Yamamoto, S., Tomori M. (2013) Earthquake early warning system for railways and its performance. Journal of JSCE, 1(1): 322-328.
[4] Zhou, Y., Zhang, S., Guo, K., Zhang, Y. (2015) High speed train control strategy in earthquake early warning system. Technology for Earthquake Disaster Prevention, 10(1): 116-125.
[5] Zhai, L., Huang, Z., Yang, C., Wei, X., Liu, X. (2015) Research of high-speed railway system and national earthquake network on information access and sharing method. Technology for Earthquake Disaster Prevention, 10(3): 646-656.
[6] CHINA RAILWAY, China Earthquake Administration (2016) Interim specifications for high-speed railway earthquake early-warning and monitoring system. Beijing.
[7] Wang, B. (2014) Design and implementation of netgap system for physical isolation. Xidian University, Xi'an.
[8] Fu, L., Zhu, J., Rao, Y. (2016) Design and implementation of an across netgap data transmission system. Computer & Digital Engineering, 44(10): 1996-2000.
[9] Dai, L., Zeng, F., Huang, H., Ji, X., Yang, T. (2013) Construction of the hospital clinical appointment-making platform based on security gap technology. China Medical Education Technology, 27(4): 454-457.
[10] Hu, J., Li, X., Zhou, B. (2010) GAP-based security scheme for hospital intranet. Chinese Medical Equipment Journal, 31(7): 44-45, 58.