Journal of Engineering Science and Technology Review 6 (2) (2013) 90-94

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Research Article

Ethernet-based Mass Volume Train Security Detection Network

D. Q. He*, X. F. Zhong , C. H. Ren and L. F. Xu

Guangxi Key Laboratory of Manufacturing System & Advanced Manufacturing Technology, Dept. of Mechanical Engineering, Guangxi University, Guangxi, Nanning 530004- China

Received 15 May 2013; Accepted 25 July 2013

Abstract

As the existing train communication network transmission rate is low, large capacity status and fault diagnosis data, the event log data, passenger information which are stored in different vehicles equipments, it is difficult to realize fault diagnosis and intelligent maintenance efficiently and timely. Based on the train level and vehicle level Ethernet network, this paper will focus on network construction technology and real-time performance of mass volume onboard security detection network. The research results will improve control and network function of train.

Keywords: Train Security detection network, Rolling stock, Mass volume, Ethernet

1. Introduction

With the development of rolling stock, it will become technology development trend through the onboard communication network to realize the whole train real-time control and all kinds of information transmission. For train based on electric multiple units require onboard communication network to transmit traction and braking information so as to make the motor units to go harmoniously. Status of all motors and trailer cars is transmitted through the network to the central control unit in cab for condition monitoring and fault diagnosis. In practice, onboard security detection network not only can decrease length of onboard train wire, and reduce the total weight of train, also improve the system integration, reliability and maintainability. Train onboard security detection network based microcomputer is used to transmit operating controlling, condition monitoring, fault diagnosis and passenger service information. It refers to all bus technology to connect onboard embedded subsystem to form onboard local area network so as to realize resource sharing, cooperation, distributed monitoring [1], [2], [3].

There are lots of onboard mechanical, electrical and auxiliary equipment, and a large number of distributed sensors and intelligent nodes fixed in vehicle. The coupling relationship between the onboard nodes are become more complex, as well as security detection and fault diagnosis system of train require that security detection network has highly real-time performance, good maintainability and expansibility, high broadband and interoperability, distributed task processing and data fusion. TCN (Train Communication Network) having the low transmission rate, can not meet the requirements of onboard mass data transmission and security detection system. Therefore, train security detection network which can transmit mass capacity data is becoming a developing trend. Ethernet based on IEEE 802.3 standard, as the field bus with mass capacity data transmission has been widely applied in industry field, such as Ethernet/IP, PROFINET, Ethernet PowerLink, EtherCAT, MODBUS-IDA, and EPA real-time Ethernet [4], [5].

Rolling stock has rugged environment, vehicles often need to be coupled and uncoupled. Compared to conventional TCN, Ethernet devices will reduce costs and increase functionalities. The IEC/TC9 WG43 group is revising TCN standard and add Ethernet as train backbone, in order to promote Ethernet technique widely used train communication network. Regional trains in Germany and the Netherlands are currently being delivered by BOMBARDIER with an onboard Ethernet network. This is the world’s first example of Ethernet protocol being used for train control data management and security detection data transmission. The Bombardier Transportation system will integrate all the intelligent devices onboard into one Ethernet network which will fully replace the TCN in two or three years. SIEMENS is studying how to use the industrial Ethernet PROFINET as the train communication network. Japan Railway union is studying based on Ethernet INTEROS (*INtegrated Train communication/control networks for Evolvable Railway Operation System*) train communication network. ALSTON is studying train and consist Ethernet, and cooperating with the French rail operator SNCF to test the onboard Ethernet performance of all TGV train [6], [7].

TSDN (*Ethernet-Based Train Security Detection Network*) has higher data transmission rates, larger bandwidth, interoperability, real-time and adaptability for onboard environment. This paper is organized in the following order. Section 2 analyses onboard devices topology of security detection network. Section 3 introduces logical relationship. Section 4 analyses real-time performance of this network, Section 5 builds the simulation model and analyses the delay estimation of data transmission

* E-mail address: hdqlqy@gxu.edu.cn

ISSN: 1791-2377

under different tasks and bandwidth, to be concluded in Section 6.

2. Topology of Train Security Detection Network

The system and devices connect with train security detection network comprises all sensors, AP (*Access Point*), FP (*Fusion Point*), ND (*network noDe*), CP (*Center Point*), DSM (*Diagnostic Service Machine*), and onboard wireless communication platform. The main function of these devices is as follows:

AP1 (*Access Point 1*) is responsible for connecting the sensor (power, running, brake system and vehicle body balance testing) and the FP, and convert sensor signal to the data identified by the FP with a unified communication protocol. AP1 includes conditioning devices which realize data preprocessing and diagnosis of the above onboard intelligent sensors.

Bogie AP2 (*Access Point 2*) is responsible for connecting bogie sensor、axle-case composite sensor and composite nodes, and convert the sensor signal to the data identified by the FP with unified communication protocol. AP2 also includes conditioning devices which realize data preprocessing and diagnosis of onboard intelligent sensors.

FP (Fusion Point) is physically responsible for connection to the AP and ND, and logically in charge of data management of its coach AP and vehicle network management.

CP (*Central Point*) is onboard system gateway. CP is responsible for dynamic networking, network management and maintenance, onboard network interface configuration, flow distribution, onboard data message cache, and using TCP/IP protocol to send data.

ND (*Network noDe*) is responsible for data transmission with 100Mbps broadband, and realizes the network management of train level, VLAN division, priority control, and dynamic networking.

DSM (*Diagnostic Service Machine*) transmits data with the CP, mobile channel control devices through the security detection network and receives data from the FP. According to the running, traction, braking, auxiliary and surveillance subsystem, the DSM is responsible for encoding and decoding data packet, controlling and storage date flow, and making safety assessment and prioritization, realizing fault diagnosis and early warning.

OMCP (*Onboard Mobile Communication Platform*) includes an onboard wireless communication host, real-time channel unit and antenna, static channel unit and antenna. The OMCP communicates with the CP, diagnostic service host machine through security detection network, and mainly realize the data cache, confirm real-time and off-line large capacity transmission mechanism, data packing, control the dynamic transmission unit and static transmission unit, via static and dynamic modulation achieve data transmission.

As taking comprehensive consideration of onboard devices physical location and topology, train security detection network comprises three vehicles couple, its topology model is shown in Fig. 1, the ND acts as CP. Equipment layout of train security detection network is as follows, equipment mounted in car A mainly performs train ground communication which performs real-time and static channel unit, diagnostic services display terminal and the antenna, the TCN gateway which is respectively mounted in car A as master and slave. The special equipment installed in 19 inch standard cabinet of car B, includes AP, CP, ND and CP which is respectively mounted in car B as master and slave. The special equipment installed in 19 standard cabinet of car C, includes AP, CP, ND, DSM which is only mounted in one car C, OMCP which is only mounted in one car C and other equipment related.

3. Onboard Devices Logic Relation of Train Security Detection Network

The logic relation of train security detection network is shown in Fig. 1. Data from onboard intelligent sensors will transmit from AP, FP, ND to train level network. The existing TCN network data will be converted by TCN gateway, then through the ND transmit to train level network. The DSM and the OMCP connect the train level network directly through the ND. The CP is responsible for the management and control of train level network through the ND. The DSM sends data to ground system through the OMCP.

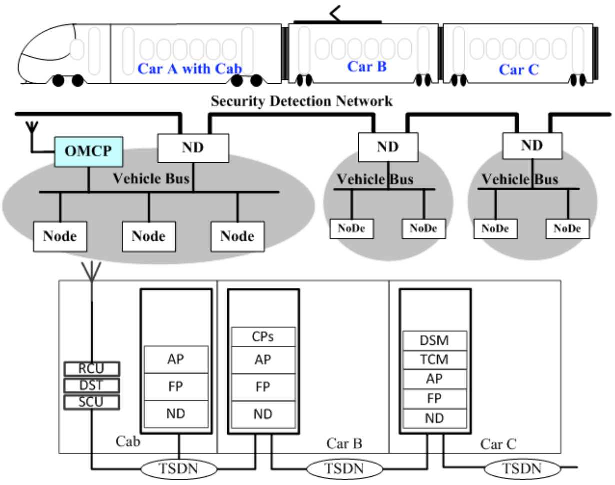


Fig. 1. The train security detection network topology

Train security detection network based Ethernet/IP technology, using TCP/IP protocol, divided into train level ETDN (*Ethernet Train Detection Network*) and vehicle level EVDN (*Ethernet Vehicle Detection Network*). The ETDN network throughout the train, includes networking as couple train, to realize the train network management, VLAN division, priority, dynamic networking, and so on. The ETDN network includes a single, two, three, four or more vehicles consisting of fixed organization, in charge of data and network management of local vehicle and group. The ETDN network is composed by zero, one, two or more the EVDN sensing network. As one fixed operation urban train, the ETDN can be ignored, the train is simplified as one EVDN network.

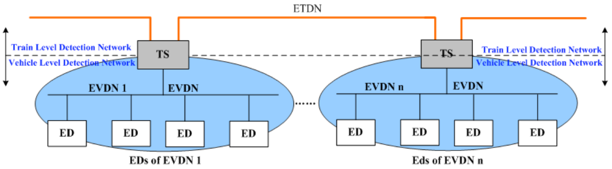

ETDN
Train Level Detection Network
Vehicle Level Detection Network
TS
TS
Train Level Detection Network
Vehicle Level Detection Network
EVDN 1
EVDN
EVDN n
EVDN
ED
ED
ED
ED
ED
ED
ED
ED
EDs of EVDN 1
Eds of EVDN n

Fig. 2. The train security detection network architecture

Train security detection network architecture is shown in Fig. 2, TS (*Train Switch*) mainly refers to the ND, which can realize the ETDN and the EVDN network data conversion and the train and vehicle level network gateway. VS

(*Vehicle Switch*) includes NP and FP. ED (*End Device*) comprises a variety of sensor, AP, CP, DSM and OMCP, other devices provides data source for the TS and VS. The Devices of ETDN and EVDN network will communicate with devices interface specification and protocol which refer to the OSI physical layer to application layer [8].

The MADB (*Maximum Allowable Delay Bound*) and MATI (*Maximum Allowable Transfer Interval*) are set as the real-time performance and reliability of train security detection network.

4. Analysis of Real Time Performance of Train Security Detection Network

As the stable MADB and MATI time of mass volume train security detection network is millisecond level, transmission delay and fault healing time of existing industrial Ethernet technology is too long, which is unable to meet the needs of train security detection network. Train security detection network uses data link layer protocol of ISO/IEC 8802-3, IEEE 802.11 and IEEE 802.15. CSME (*Communication Scheduling Management Entity*) is added between the logical link control layer and data link service users by extend the data link layer of ISO/IEC 8802-3 agreement, which is shown in Fig. 3.

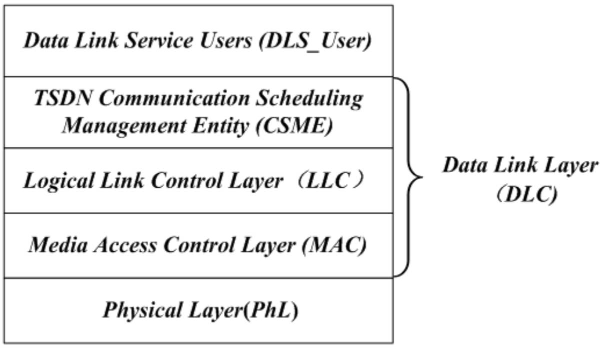

Data Link Service Users (DLS_User)
TSDN Communication Scheduling Management Entity (CSME)
Logical Link Control Layer（LLC）
Media Access Control Layer (MAC)
Physical Layer(PhL)
Data Link Layer（DLC)

Fig. 3. The data link layer model of train security detection network

According to configured sequence control and priority, the TSDN Communication Scheduling Management Entity will transfer the DLS_User data to the LLC, processed by the DLE, then, send to the TSDN network by the PhL, which will avoid the collision of data frames from two onboard devices.

The CSME based on deterministic communication scheduling procedures, control time of the DLS_User data transmission to the LLC. The communication scheduling rules divide communication time into TSDN communication macro cycle $\left(T^{evdn}_{macro}\right)$, and according to the different characteristics of the data transmission, which can be divided into periodic and non-periodic data frames. The periodic data frames refer to sampling data and control data which need highly real-time performance, such as traction and braking data. The non-periodic refers to the data frames which its communication cycle is not fixed, such as variables reading and writing data, event notification, trend report, and ARP, RARP, HTTP, FTP, TFTP, ICMP and IGMP application data.

As a result, as shown in Fig. 4, a TSDN communication macro cycle is divided into two stages, the first phase is periodic data frame transmission phase (T_p), the second is non-periodic data frame transmission phase (T_{np}).

The TSDN network uses basic TDMA (*Time Division Multiple Access*) algorithm in the stage of cycle time. Onboard devices call TSDN bus by dividing each time slice of these devices. Delivery order of data frames is guaranteed by each device to monitor dispatching data frame in the bus, and combine with priority algorithm in the stage of cycle time. According to the scheduling rule, it will avoid the data conflict and ensure determinacy and real-time communication. On the other hand, in order to meet the requirements of communication reliability of onboard security inspection system, the TSDN architecture has the distributed fault detection and recovery methods which called DRP (*Distributed Redundancy Protocol*). In order to realize fast failure detection and recovery, the DRP adopts active link detection technology which respectively detects the failures of switch equipment and communication link, and it will realize rapid recovery according to the result of fault detection. All switch devices are put end to end and form a ring structure in ring network system based on distributed fault detection and recovery. Onboard end devices access to the ring TSDN network by means of one train or vehicle switch.

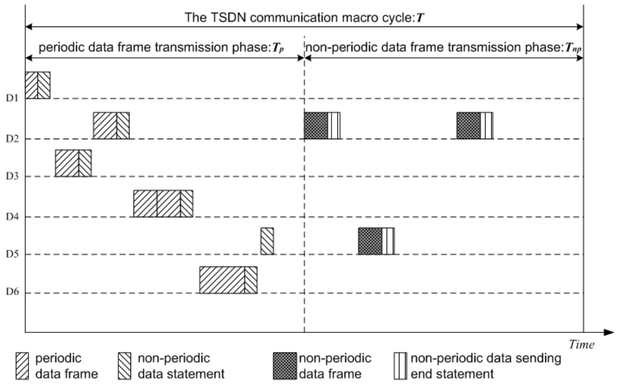
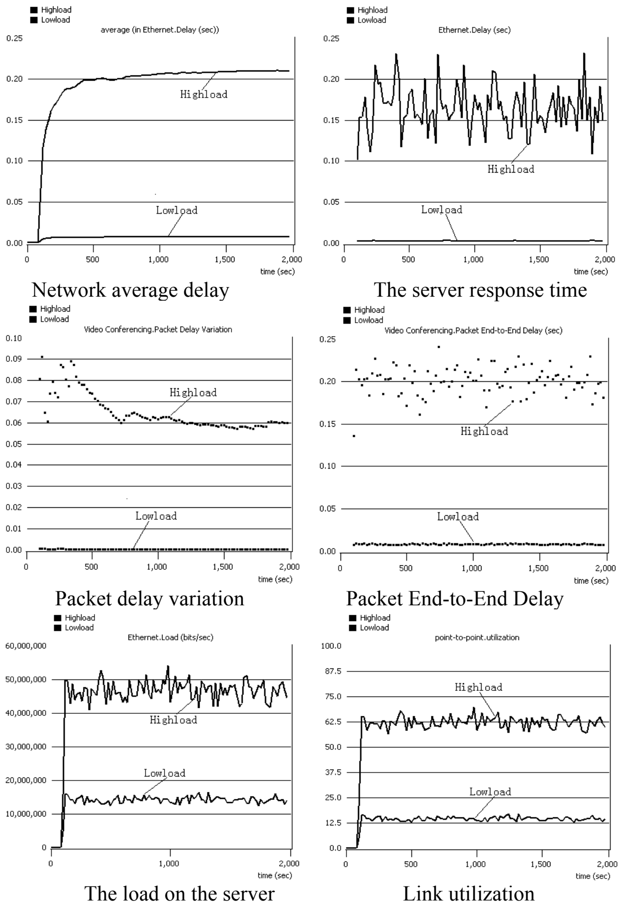

The TSDN communication macro cycle:T
periodic data frame transmission phase:Tp
non-periodic data frame transmission phase:Tnp
D1
D2
D3
D4
D5
D6
Time
periodic data frame
non-periodic data statement
non-periodic data frame
non-periodic data sending end statement

Fig. 4. The TSDN Deterministic communication scheduling schemes

5. The Delay Estimation of Data Transmission under Different Tasks

This section uses the OPNET to analysis the delay estimation of data transmission based on train security detection network under different network bandwidth. According to the train specification, the maximum cars number will up to 8. There is a vehicle level switch in each car, so the network is divided into many smaller collision domains and each collision domain achieves the isolation through the vehicle switches. The connecting way of vehicle level switch is bus topology structure and the train level switch in driving cab is connected to 2 workstations. And one is used to the transmission of mass volume information and set up the FTP application business to simulation, while the other is used to monitor the information transmission of each device status and set up the Video Conferencing application business to simulation.

The two scenarios are set to the Lowload and Highload application system respectively and the application link bandwidth are set up to 100Mbps. As mass volume transmission is the key factor of affecting the application network delay, so we discuss the performance of the application network mainly through changing the video load. Load different application traffic flux in the two scenarios. In the first scenario, the application business flux of the Ftp and Video Conferencing are set to Low Load and Low Resolution Video, and both are low traffic load. Meanwhile, the application business flux of the Ftp and Video Conferencing are set to High Load and High Resolution Video in the second scenario, and both are high traffic load. The simulation results are shown in Fig. 5.



Network average delay The server response time

Packet delay variation Packet End-to-End Delay

The load on the server Link utilization

Fig. 5. The 100Mbps Mass Volume Network Performance

The Fig.5 shows that the train security detection network average delay of 100 Mbps network is small in transmitting low resolution video, which is only about 10ms, and has well delay stability. It means that the train security detection network perform is well in transmitting low flux information. Low resolution video displaying and monitoring can be transferred fluently in the train security detection network. However, the train security detection network average delay is more than 200 ms in transmitting high resolution video(mass volume data). It is obviously that the network suffers a big hit, and such delay can not satisfy the real-time transmission requirement of mass volume information. From Fig. 5, we can see that the network load is very big when high traffic load is added to, and it will lead to increasing the server processing time delay. As is shown in Fig. 5, the link utilization rate is only about 15% when low flux load is transmitting but it is more than 60% when high flux load is added. Because the bandwidth utilization rate of common train security detection network should not be more than 50%, so it is confidently that such high link utilization will cause network congestion and the delay of train security detection network will increase greatly. In additional, the network delay under the low load is less than it under high load according to the network delay, packet End-to-End delay and packet delay variation. Although it is low load but it is relative to the high load of this design. The 15Mbps network transmission rate is already very high compared with the traditional train communication network. The delay of train security detection network can be guaranteed below 10 ms at 15Mbps communication rate, which indicates that the mass volume application system based on train security detection network has more improvement in the network performance than traditional train network system. So, mass volume information should be multicast to onboard devices so as to save bandwidth.

6. Conclusions

In recent years, bandwidth requirements due to the installation of new embedded system onboard trains are growing rapidly. Now, the revising standard IEC 61375 is much extended. Mass volume onboard security detection network based Ethernet runs in parallel to the existing TCN or solely used for all kinds of communication in a train. Train security detection network is one of the most important onboard buses for the application of Ethernet on rolling stock, it will help to improve security, stability, reliability, comfort and speed of train. In the next stage of our research, we intend to carry out a series of simulations to test the network model performance of onboard security detection network by transmission experiments.

7. Acknowledgements

This work is financially supported by the National Natural Science Foundation of China under project grant number 51165001,Guangxi Natural Science Foundation Program(Grant No. 2013GXNSFAA019297), and Guangxi Key Laboratory of Manufacturing System & Advanced Manufacturing Technology (Grant No. 10-046-07S05).

References

1. Verstichel S., Hoecke S.V., Strobbe M., Berghe S.V., Turck F.D., Dhoedt B., Demeester P., Vermeulen F., "Ontology-driven Middleware for Next Generation Train Backbones", Science of Computer Programming 66(1), 2007, pp. 4-24.
2. Valter L., Guido P., Stefano ., Antonio M. C., "An ID-Card Based Security System for Railway Applications", Procedia - Social and Behavioral Sciences, 48, 2012, pp. 234-245.
3. Aziz M., Raouf B., Riad N., Daoud Ramez M., Elsayed H. M., "The Use of Ethernet for Single On-board Train Network", Proc. Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on , 6-8 April 2008, pp. 1430-1434.
4. Rodriguez M.C., Alexandres S., Munoz J.D., "Broadband system to increase bitrate in train communication networks", Computer Standards & Interfaces 31(2), 2009, pp. 261-271.
5. Alessandra F., Paolo F., Daniele M. , Emiliano S., Andrea T., "Wired and wireless sensor networks for industrial applications", Microelectronics Journal 40, 2009 , pp. 1322–1336.

6. Mohammad Z. A., Chin K. W., “TrainNet: A transport system for delivering non real-time data”, Computer Communications 33, 2010, pp. 1850-1863.
7. Junji K., Makoto S., Akihiko S., Kentarou H.,Yutaka S., Koichi N., Takashi M., Tetsuo K., “Development of 100Mbps-Ethernet-based Train Communication Network”, Proceedings of 9th World Congress on Railway Research, 22-26 May 2011, pp. 1-12.
8. Zeng Z., Ding, R.J., Yang W. F., Lu X.Y., Feng J. H., “A Distributed Comparison Algorithm for Train Inauguration Protocols over Ethernet”, Proc. E-Product E-Service and E-Entertainment (ICEEE), 2010 International Conference on , 7-9 Nov.2010, pp.1-5.