A Multi-source Data Oriented Framework of Vehicle Monitoring System

Shuaiqi Liang

College of Information Science and Engineering,
Ocean University of China
Qingdao, China
liang_sq@126.com

Hao Liu*

College of Information Science and Engineering,
Ocean University of China
Qingdao, China
liuhao@ouc.edu.cn
* Corresponding Author

Yuntao Qian

College of Computer Science and Technology,
Zhejiang University
Hangzhou, China
ytqian@zju.edu.cn

Zhiqiang Wei

College of Information Science and Engineering,
Ocean University of China
Qingdao, China
weizhiqiang@ouc.edu.cn

Abstract—**A framework for monitoring system of vehicles is introduced in this paper. The system is applied for real-time monitoring of vehicles. It mainly includes vehicular hardware, remote servers and application terminals. The hardware part insists of various sensors, MCU chips, interface converting modules and hand-held terminals. The system collects a variety of data of vehicles efficiently. And it optimizes the transmission of data base on different bandwidth, delay and other characteristics. At the same time, it accesses to the remote data center perfectly. The data center will implement more complex business analysis considering vehicles as data collection terminals. The system improves the reliability of vehicular system and reduces errors in data transmission. It also has high security. A monitoring system based on the framework is implemented and introduced in this paper. The system makes it possible to monitor vehicles multi-angle and all-around. It is already applied within a certain range and achieved good results.**

Key words: vehicle monitoring; Internet of Vehicles; sensor network; Intelligent Transportation; cloud computing

I. INTRODUCTION

In recent years, the number of vehicles in the world is increasing quickly. Meanwhile, the number of various types of vehicular sensors and the data they get also becomes more than before. Vehicles have gradually become a data acquisition unit of the Internet. In order to improve the safety, economy or other performance of vehicles, many vehicles are equipped with a vehicle monitoring system. The traditional vehicle monitoring system monitors the location, speed and some other basic information of vehicles. But these systems have some disadvantages. First, one system considers only certain aspects of a vehicle. Second, in data transmission, the security is not particularly concerned. Most data are transmitted unencrypted. Third, the transmitting protocol of these systems usually do not adapt to different types of data. This results in low speed when transmitting large amounts of data and wasting bandwidth when transmitting small data. The last, when the network condition is not good, there is no mechanism to avoid high packet loss rate.

A framework for monitoring system of vehicles is introduced in this paper. It mainly includes vehicular hardware, remote servers and application terminals. The hardware part insists of various sensors, MCU chips, interface converting modules and hand-held terminals. And the system is applied to solve the above disadvantages. The system provides real-time monitoring of car information. In addition to the basic car position information, the system also collects and monitors the information of speed, acceleration, tire pressure, tire temperature of the car and real-time video of inside and outside the car. And the system will encrypt the data before transmitting them. Different transport protocols are applied according to different quantity of data. This guarantees the speed and low-cost. Meanwhile, a mechanism is designed to avoid high packet loss rate when the network condition is not good. Then under the premise of information security, people can use the information to monitor cars multi-angle and all-around.

II. RELATED WORKS

With the development of GPS technology, more vehicle monitoring and dispatching systems based on GPS are developed and used. YI Shu-you and ZHOU Mei-jiao establish a vehicle monitoring system using wireless sensor network [1]. Miao Yu et al. establish a vehicle monitoring system using RFID and GPS to monitor the transportation of dangerous goods [2]. Furthermore, Micro-Electro-Mechanical System (MEMS) [3], Cloud Computing [4] and Wireless Communication [5] are also used to establish vehicle monitoring systems. And Ha Duyen Trung et al. design and implement a mobile vehicle monitoring system based on Android smartphone [6]. AES encryption algorithm

is one of the most popular encryption algorithms. Fei Shao et al. increase the computing speed of AES encryption algorithm based on GPU [7]. Priyanka Pimpale et al. amend AES algorithm to implement complex encryption [8].

In data transmission, Sreelakshmi Manjunath and Gaurav Raina use FAST TCP to transmit large amounts of data [9]. And Chen Ao and Lu Ting research data transmission control protocol in wireless channel at very low speed [10]. They present a light-weight data transmission control protocol and implement the data transmission in the condition of a wireless channel at a very low speed. Jianbo Xu et al. research a phased data transmission protocol in mobile sensor networks [11]. Zhang Qun et al. establish a remote Ethernet data transmission system based on hardware protocol stack. And the system implements data transmission of high integration and low-cost [12].

III. PROPOSED SYSTEM

The workflow and main parts of the system are as follows:

- The sensors are the device to get real-time information of the vehicle. They transmit these data to central control module.
- Central control module do verification process of data received from sensors, then transmit these data to intelligent terminal module in cars via Bluetooth.
- Intelligent terminal module in cars transmits data to data center via 3G/4G mobile communication network. And meanwhile check these data. If there are any abnormal conditions, it will alarm the driver. Data center stores and exchanges data and does big data computing and so on.

- Data center transmits received data to application terminals via 3G/4G mobile communication network. Then application terminals show these data for people to monitor cars.

Technology roadmap of the system is shown in Fig. 1. System chart is shown in Fig. 2:

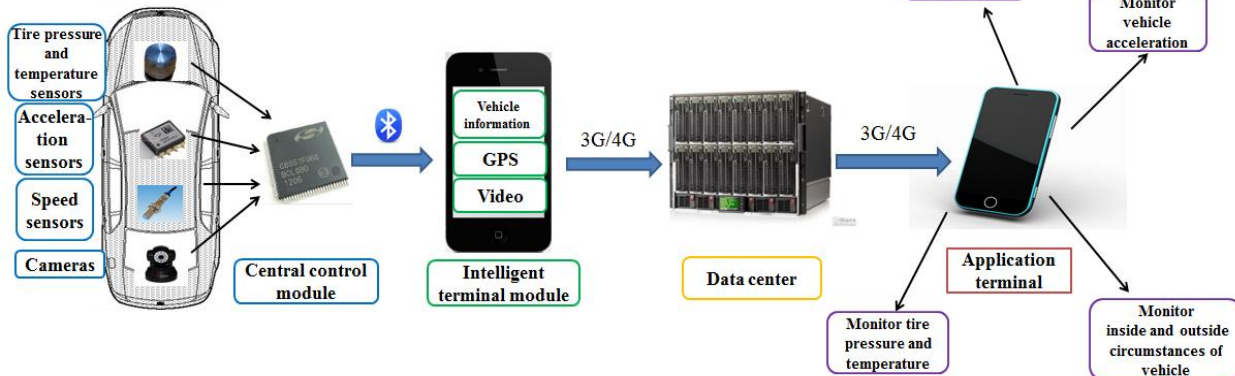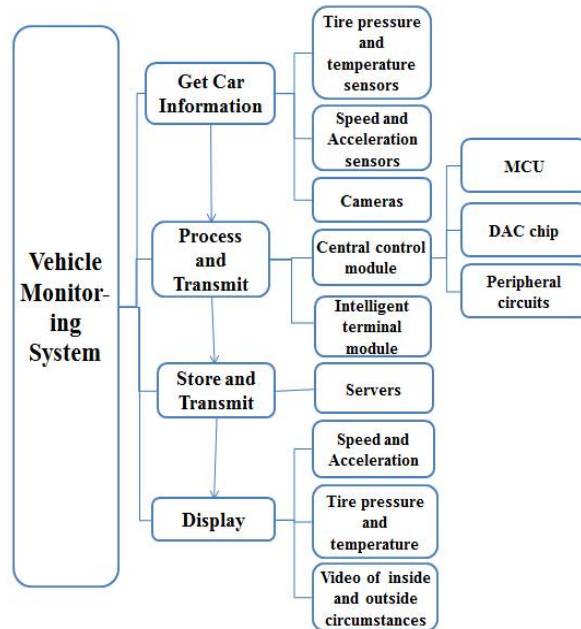Figure 1.   Technology roadmap of the system

Figure 2.   System chart

IV. DESIGN OF HARDWARE

A. Sensors

Sensors are the hardware core of the system. These sensors contain sensing chips modules, signal emission modules and power supply management modules. Data acquisition unit of sensors has a built-in computing power chips. They automatically finish checking encode and encrypting encode in the process of data receiving. According to the amount of acquired data and the frequency of data transmission, these sensors can be mainly divided into four categories as follows:

- Continuously transmit large amount of data, for example, video cameras. The connection established between this type of sensors and the central control module is continuous. It needs to guarantee the continuous transmission of large amount of data. It

needs big bandwidth, but high reliability is not necessary. A few packet losses and a little delay are acceptable.

- Discontinuously transmit large amount of data, for example, photographic cameras. This type of sensors gets data intermittently. So the connection between sensors and the central control module is established only when needed. This saves bandwidth. The connection needs high reliability.
- Continuously transmit small amount of data, for example, tire pressure and temperature sensors. This type of sensors needs to establish a continuous connection with the central control module. Because the amount of data is small, the connection can be established via radio frequency identification. The connection does not need high reliability. A few packet losses and a little delay are acceptable.
- Discontinuously transmit small amount of data, for example, acceleration sensors. This type of sensors establishes a connection with the central control module when needed. Radio frequency identification, which is convenient and efficient, can be applied to establish the connection. The connection needs high reliability and high priority.

B. Central Control Module

The main function of central control module includes programmable tire parameter reception, real-time tire pressure and temperature monitoring, warning the abnormal circumstances, Bluetooth connection and so on. In the implement of prototype system we mainly use ATmega48-20AU microcontroller, TDA5235 and serial-to-Bluetooth module. Central control module gets the data from the sensors by radio frequency. Then do verification process of these data and transmit these data to intelligent terminal module in cars via Bluetooth. The advantages of this module include the following aspects:

- High integration. It integrates functions of power supply, data receiving and data transmission into a unified hardware.
- Versatility. The main input and output module both apply general standards. It can be adapted to all types of vehicles and a variety of different terminal conditions.
- Easy to use. We just need to plug it in the car's cigarette lighter and it will start work automatically.
- Good stability. Each function of it is relatively independent and will not interfere with each other.

V. DATA PROCESSING AND TRANSMISSION

The system needs multi-level transmission scheme to transmit data.

The first level of data transmission is that the data acquisition module sends the data detected by sensors to the center control module in the car. Information security issues faced in this stage include physical attacks, eavesdropping, counterfeiting, fraud, information analysis and so on. It's often difficult for traditional Hash-Lock protocol and Link Aggregation Control Protocol (LCAP) to completely avoid these attacks. So this stage applies hybrid encryption protocol to prevent sensor information from disclosure and tracking. This provides efficient and stable security mechanism for the system to transmit data information. The system combines the AES and Hash algorithm to design a new hybrid encryption security authentication protocol. The system combines the advantages of the two encryption algorithms to encrypt data.

The second stage is that the central control module transmits the data received from various sensors and cameras to the intelligent terminal module in the car. The central control module does verification process of received data and packages the data into a format. In the implement of prototype system we package the data into a format as shown in TABLE I. ID field is applied to distinguish between different sensors. The values of tire pressure, tire temperature, acceleration and speed are acquired by the sensor and these values represent the data of the tire. The length and contents of every field can be defined as required. Then the packet is transmitted to the intelligent terminal module in the car via Bluetooth.

TABLE I.   SENSOR DATA PACKAGE FORMAT

Packet Header	ID	Tire pressure	Tire temperature	Acceleration	Speed	Check	Packet Tail
0x3C	4B	2B	2B	2B	2B	1B	0x3E

The data transmitted between the central control module and the intelligent terminal module also applies AES encryption algorithm. This enhances the security as well as reducing the risk to be deciphered. And the Hash Algorithm is also applied in this protocol. And this adapts to the open environment of the Internet of Things.

The third stage of data transmission is the transmission between the intelligent terminal module and the data center. The third stage is the transmission between the data center and the application terminal. These two transmission processes both apply the TCP connection based on 3G/4G mobile communication network. In the basic data transmission protocols we reserve some interfaces in order to compatible with different standards. In the implement of prototype system, the transmission is compatible with JT / T 808 and JT / T 809 standard of China. And the transmission can be combined well with the existing road transmission monitoring system of China.

When transmits small data like data of sensors, a lightweight reliable data transmission protocol is applied to save bandwidth and reduce costs. The protocol applies lightweight first section, error control and multicast receipt. It adapts to a wireless channel of very low speed. It achieves low load for protocol, reliable and efficient transmission. When transmits large amounts of data, like video data, FAST TCP technology is applied. This technology effectively reduces the response delay of applications and increases the speed of TCP throughput and effective flow. And it improves the utilization of wireless network and WAN bandwidth. Even in high-latency and high packet loss rate of

TCP network environment it also has significant optimization results. So when transmitting a larger amount of data like video data, it greatly increases the transmission speed and reduces the delay.

Meanwhile, before data transmission, the server will judge the status of the network in advance. If the network is in good condition, the system will transmit the data normally. Otherwise, the system will reduce the rate of data transmission and store the unsent data in the buffer. When the network condition turns good, the system will take out the data from the buffer and transmit them sequentially. This will avoid the high packet loss rate and improve the reliability and accuracy of data transmission.

Before transmitting data, intelligent terminal module in cars or data center will firstly package the data in order to make it convenience for the receiver to parse and dispose. In the implement of prototype system, the format we use is shown in TABLE II. The length and contents of every field can be defined as required.

TABLE II.   DATA PACKAGE FORMAT

Packet Header	Command	Packet Length	Data 1	Data 2	…	Check	Packet Tail
0x7E	4B	nB	m_1B	m_2B	…	1B	0x7D

In addition, from the perspective of information security，there are three problems need to be solved—the authentication of data collection terminal, tampering data and eavesdropping when transmitting data. The system applies the cryptographic algorithm based on identity to solve the above problems.

The three main aspects of the algorithm include key generation, data encryption and data decryption. Compared to traditional public key system, the main difference of the algorithm is the key generation link. The system applies a unique device identification of the terminal to report to the key center. Key center generates a private key based on the unique identification. Its biggest advantage is that any identity can be applied as a terminal's public key. Then the identity is obviousness. This property has great attraction for wireless networks. Due to the low storage capacity of wireless network terminal, it is unpractical to store and preserve a large number of public key certificates.

VI. IMPLEMENTATIONS ON APPLICATION TERMINAL

A. Application Terminal Data Acquisition

After the application terminal sets up a TCP connection with data center by 3G/4G mobile communications network, it will send out packets of different formats depending on the requested data. In the implement of prototype system, the login request packet format we use is shown in TABLE III

TABLE III.   THE PACKAGE FORMAT OF LOGIN REQUEST

Packet Header	Command	Packet Length	User Name	Pass Word	Check	Packet Tail
0x7E	0x10	2+10+10B	10B	10B	1B	0x7D

Among them, the packet header and packet tail are respectively the fixed field 0x7E and 0x7D, which are applied to distinguish different packets. The command field is applied to distinguish different commands. Packet length is the length of the packet, namely the length from packet header to packet tail, which is applied to intercept data packets. UserName field is filled in the user name and PassWord field is filled in the password that the user used when he logged in. Check field is applied by the terminal which will receive data to judge whether the data is transmitted correctly.

Then the application terminal encrypts the packaged packet and sends them to data center. After the data center receives the request, it decrypts it first, then package different response packet corroding to the different contents of the command field. At last, data center encrypts response packets and sends to the application terminals using 3G / 4G mobile communication network.

After application terminal receives the response packet from data center, monitoring program will decrypt it first, then to determine whether the packet is the needed according to the command field. If so, get the value from the required fields and displays, otherwise, do nothing. In the implement of prototype system, TABLE IV is the response packet format of login request we use.

TABLE IV.   RESPONSE PACKAGE FORMAT FROM LOGIN REQUEST

Packet Header	Command	Packet Length	Reserved Bits	bResult	Check	Packet Tail
0x7E	0x11	2+4+1B	4B	1B	1B	0x7D

After monitoring program decrypted the packet it will check the command field, if the command field is 0x11, it will take out the values of bResult field. BResult field represents whether the login is successful. If the value is 0, the login is successful, otherwise, the login is failed. Monitoring program will operate differently depending on the value of bResult field. If it is 0, then jump into the main interface, otherwise, indicates login failed.

B. Design Of Application Terminal Interface

Application terminal consists of four main functions: check the list of all monitoring cars; check locations of all monitoring cars; check the videos of all monitoring cars; setting.

Monitoring program first sends a request to the data center to get the data packet of a list of monitoring cars. After receiving the returned packet, monitoring program will decrypt and parse and at last displays them in the form of a list.

After getting the vehicle list, we can choose to check online cars or all of the cars. For online vehicle, we can click the "map" button to check the location of the car and we can click the "video" button to check the videos shot by the cameras in the car.

In map page, we not only can see the position of the car, but also can check the name of the car, the owner's contact information, speed and driving direction of the car by clicking on the car icon.

In the view page, we can check four videos shot by the cameras in the car and the location on map. And we can by clicking on the video screen to make the screen zoom, for a clearer view of the video.

In settings page, we can log out, check if there is an updated version of the software and set the frequency to get the location information.

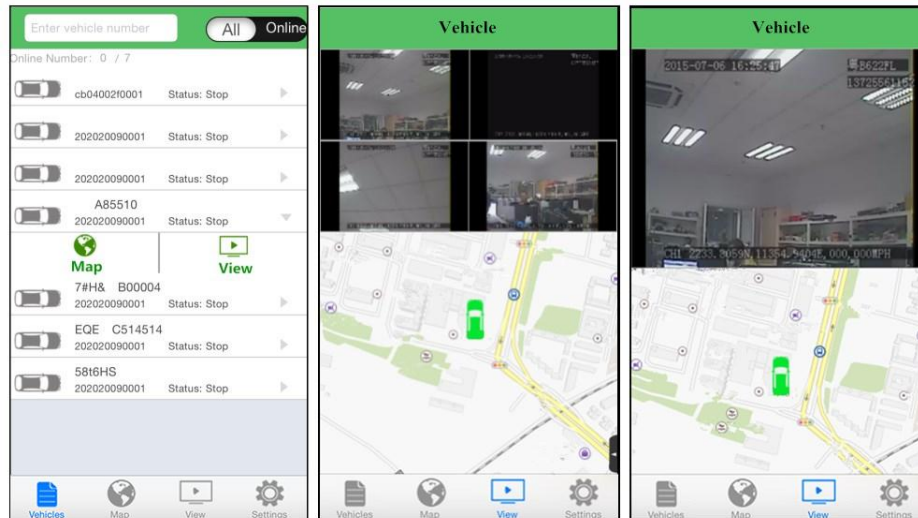The main views of application terminal are shown in Fig. 3:

Figure 3. Application terminal interface

VII. CONCLUSIONS

In recent years, vehicle ownership in the world is increasing quickly. In order to improve the safety, economy or other performance of vehicles, many vehicles are equipped with a vehicle monitoring system. This paper introduces a framework for monitoring system of vehicles and a monitoring system based on the framework. The system collects a variety of data of vehicles through various sensors and the central control module, intelligent terminal module and data center are applied to do data processing and transmitting. And it optimizes the transmission of data base on different characteristics. Meanwhile, it accesses to the remote data center perfectly. The data center will implement more complex business analysis considering vehicles as data collection terminals. The system improves the reliability of vehicular system and reduces errors in data transmission. It also has high security. The system has achieved good results in practical use and has broad prospects for promotion.

REFERENCES

[1] Shu-You Y I, Zhou M J, "Vehicle Monitoring System based on Wireless Sensor Network," Communications Technology, 2013.

[2] Yu M, Deng T and Fu J, "Application of RFID and GPS Technology in Transportation Vehicles Monitoring System for Dangerous Goods," Remote Sensing, Environment and Transportation Engineering (RSETE), 2012 2nd International Conference on. IEEE, 2012, pp. 1-4.

[3] Qin H W, Shi C J and Liu J, " Design of driving behavior and vehicle state monitoring system based on MEMS and GPS," Transducer & Microsystem Technologies, vol.31, 2012, pp.79-82.

[4] Dimil Jose, Sanath Prasad and V.G. Sridhar, "Intelligent Vehicle Monitoring Using Global Positioning System and Cloud Computing," Procedia Computer Science, vol.50, May.2015, pp.440-446.

[5] Ananthanarayanan N, "Intelligent vehicle monitoring system using wireless communication," Advances in Technology and Engineering (ICATE), 2013 International Conference on. IEEE, 2013, pp.1 - 5.

[6] Ha Duyen Trung, Pham Tien Hung, Nguyen Duy Khanh, et al, " Design and Implementation of Mobile Vehicle Monitoring System based on Android Smartphone, " 2013 Third World Congress on Information and Communication Technologies (WICT), 2013, pp. 51-56.

[7] Fei Shao, Zinan Chang and Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU," Communication Software and Networks, 2010. ICCSN '10. Second International Conference on. IEEE, Feb. 2010, pp. 588-590.

[8] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, " Modifications to AES Algorithm for Complex Encryption," Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on. IEEE, July 2014, pp. 499-502.

[9] Manjunath S and Raina G, "FAST TCP: Some queueing models and stability," Signal Processing and Communications (SPCOM), 2014 International Conference on. IEEE, 2014, pp. 1 - 5.

[10] Chen Ao and Lu Ting, "Data Transmission Control Protocol in Wireless Channel at Very Low Speed," Command Information System and Technology, vol.02, 2011, pp. 43-47.

[11] Xu J, Wang J, Liang W, et al, "A Phased Data Transmission Protocol in Mobile Sensor Networks," Journal of Convergence Information Technology, vol.5, 2013, pp. 1083-1091.

[12] Zhang Q, Zhao L and Liang R, " Remote Ethernet Data Transmission System Based on Hardware Protocol Stack," Microcontrollers & Embedded Systems, 2013.