Research on Secure Communication Mechanism of Traffic Recorder

L. Li, Y.F. Zhu, R.N. Xie
Department of Electronic Information Engineering, Beijing Electronic
Science and Technology Institute
Beijing 100070

F.H. Li
Institute of Information Engineering, Chinese Academy of Sciences
Beijing 100093

***Abstract*—Through the research of the demand for secure communication between traffic recorder and data management platform, a three layer automobile remote diagnostics communication model which contains data aware, network access and application service is proposed, through special access gateway to add device and enhance communication security and scalability. JCM authenticated encryption scheme is adopted to implement a secure data exchange, which guarantees transmission data confidentiality, integrity and reliability of the source in the process of communication.**

Keywords-traffic recorder; remote diagnosis; secure communication; authenticated encryption

I. INTRODUCTION

With the development of computer technology and the increasing requirement for safety management, traffic recorders being able to record and track the real-time operation state of the vehicle, so as to improve vehicle safety and reduce accidents, are promoted in most countries. The use of traffic recorder has brought convenience to the city traffic management, the global database system which described in literature [1] can automatically collect all the vehicle's local database, and generate a report on the map with highlighted traffic hotspots to help identify traffic hazards. Now how to make unified management on collected data, ensure data integrity and authenticity, and strengthen the supervision of car status are still not perfect. Traffic recorders of different manufacturer also have different data transmission formats, interface, which brought certain difficulty for unified management. According to another survey, only a handful of traffic recorders have adopted communication encryption method for data exchange security, most of traffic recorders communicate data in plain text, making the driving status information in unsafe conditions.

Currently, the research on communication security involved in using traffic recorder is not much. This paper has established a kind of remote diagnostic communication model between traffic recorder and the background data management platform. Considering the limited wireless transmission resource and timeliness requirements, authenticated encryption (AE) mode is used to realize a secure data exchange based on car remote diagnostics communication model, making the traffic recorder data can be safely and easily transferred to the backend data management platform, and only the authorized users can access the corresponding driving state information.

II. RELATED RESEARCH

Traffic recorders generally have the function of driving record and accident record. With the development of communication technology, traffic recorder must be combined with other electronic systems, such as Geographic Information Systems (GIS) and Global Positioning System (GPS). The common data communication between traffic recorder and PC are: RS232 and USB mode, IC card mode, wireless LAN mode, GSM short message mode and GPRS etc. Literature [2] designed a mobile traffic recorder based on J2ME, which used the phone as traffic recorder and exchanged data by Bluetooth. Literature [3] applied CAN bus on traffic recorder, and realized remote multipoint communication between traffic recorders.

Literature [4] introduced a kind of secure communication between traffic recorder and control platform, which encrypted interactive data and made identity authentication on both sides of secure communication. But Maimut and Bellare's research showed that it has some flaws and can't provide confidentiality, if the scheme encrypts messages P to generate cipher text C and calculates P to generate Tag, or generates Tag first and then encrypts P and Tag[5] [6]. Authenticated encryption (AE) can realize information's confidentiality and integrity simultaneously. Compared with the method of respectively used of information encryption and signature, AE mode requires smaller communication cost and computation in the realization of data confidentiality, integrity and authentication. The scheme in literature [7] of applied GCM (Galois/Counter Mode) authenticated encryption algorithm to data link layer of subcontracting remote control system, and on the condition of guarantee packet throughput performance, it solves the security threats faced by CCSDS subcontracting remote control system and increase the safety. Literature [8] proposed a general method by AE scheme to achieve a secure channel protocol, which demonstrating AE scheme both IND-CVA security and INT-PTXT security to illustrate a network channel protocol is UC security, described the advantages of AE scheme for achieving secure channel.

III. COMMUNICATION MODEL

Overall framework model is shown in fig. 1, it consists of three levels. The bottom layer is the perception layer, including traffic recorder, sensor and some extension equipments. The middle layer is the access layer, using a GSM module as GPRS network access, and a Wi-Fi module to provide users with different forms of wireless access

choose[9]. The top layer is the application layer, namely data management platform, which composed of server and client. Traffic recorder receives satellite data and obtains the information such as location and speed by GPS module. The received data and other car status information are sent to the access gateway [4] through GPRS module.

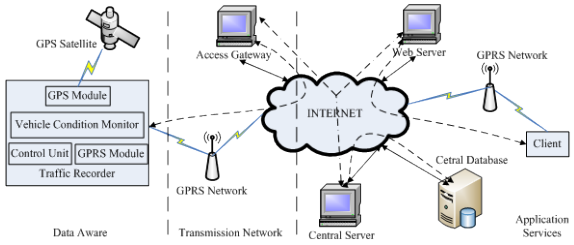

FIGURE I. THE OVERALL MODEL FRAMEWORK MAP.

Due to traffic recorder functions of different manufacturers are not the same, so as the way of data transmission, and in order to facilitate the unified management of the application layer, as well as the extension and upgrade of the remote diagnosis system, the model adopts special access gateway to accomplish data communication work for equipment (traffic recorder), receiving data from all registered equipment. And for the data we do two treatments. (1) In accordance with the contract communication protocol, the response data to the Web side command is sent to the Web server, the equipment data is also copied to the central server. (2) The equipment data is periodically sent to the central server for archive. Dedicated access gateway for equipment is equivalent to a server, and for server is equivalent to a client. By this form, when different manufacturer's equipment needs to access, you can just modify the access gateway program rather than the server program which is convenient to system expansion and upgrade, without affecting the original system's running and stability. And when the system is faulty, it is able to quickly locate the error symptoms to the appropriate access gateway.

Web server is located in the application layer, responsible for handling client requests and receiving data, where the received data has two sources: real-time query from the traffic recorder and historical data query from the central server. Server completes the work of user-oriented data communication, processing received response packets and sending results to the central server, so that the central server can backup data to the database for users' query. The center server and database complete to management and archive of user information and device information, in which the equipment ID list, equipment list of key as well as the history of the equipment list are stored in the center database, without taking the user's device space.

Client use Browser/Server architecture model to communicate with server components, that browsing devices can be a mobile phone, PDA, PC and so on. The architecture ensures that users can conveniently login Server Web page to access the server at any time and any place, such as sending a query to retrieve the device data without having to install client software, system upgrade or maintenance only need to update the server software, which greatly reduces the client's load and costs, reduces the workload of system maintenance and upgrade. On Web page, using GOOGLE map, vehicle condition can be intuitive accessed by calling the static API, so as to achieve real-time monitoring of vehicles' position, direction and speed.

IV. THE CUSTOM PROTOCOL PACKETS

Communication link use a custom protocol based on the TCP/IP protocol. The custom protocol consist of packets protocol header, device ID, the command/reply code, encrypted data, protocol tail and authentication codes, as shown in fig. 2. The protocol header is used to identify the model of communication protocol, as well as the main body of communication (equipment/web server). Devices ID, identifying a specific device number, are a unique identifier of the server to identify equipment, and its length can be set according to the size of the remote diagnosis system. For example, if chosen the device ID is 16bits data, this system can manage 65536 devices. Command code identifies various commands from the server to the device, using 8bits data, and response code identifies the device in response to a corresponding command. The command code based on the system features is divided into the following categories: accessing to equipment location, reading time, setting time, changing passwords, data reporting time interval, the work mode and speed information, etc. Data is encrypted, and for the response data, it's specific meaning is determined by the command code. The tail identifies the end of the packet, which usually is represented by special characters, such as "# *".

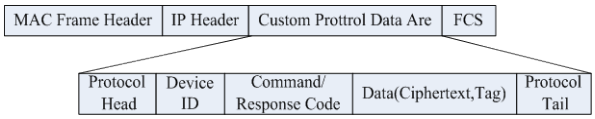

FIGURE II. CUSTOM PROTOCOL PACKET FORMATS.

In order to achieve secure communication, data packets are transmitted in cipher text to ensure the stolen information is indecipherable and without leakage when some node is destroyed. The encryption operation of AE scheme JCM (Joint Cypher Mode)[10] is used to encrypt data part of packet, and authentication operation of JCM scheme for protocol head, device ID, command/response code and encryption of data together is used to generate an authentication tag, which can ensure the integrity of data packets during transmission and prevent illegal tampering with the data packet.

V. SECURITY INTERACTIVE DATA

A. *Authenticated Encryption Mode*

In order to achieve real-time tracking of cars state, we hope the data encryption/decryption and authentication process as soon as possible, don't take up too much communication time. Considering the related factors of system safety and maintenance cost, the process of data interaction adopts the model of AE. Lipmaa experiments in Pentium III processor show that the speed of the AE model OCB is about 93.5% of encryption mode CBC and the cost is about 54% of the CBC encryption combined with CBC MAC[11].

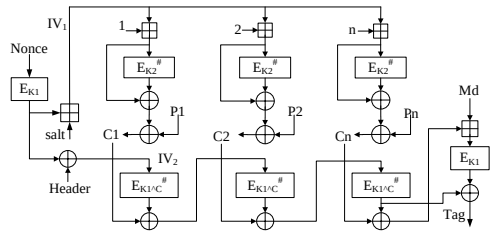

FIGURE III. JCM AUTHENTICATED ENCRYPTION SCHEME.

JCM of AE scheme shown in fig. 3 provides confidentiality and integrity simultaneously, which has the advantage of provable security, high-performance in aspects of hardware and software, and intellectual property right free[12]. JCM's encryption and authentication algorithms are based on one-way hash compression structure Matyas-Meyer-Oseas. The underlying block cipher key of encryption is K2. The authentication key is the result of K1 exclusived with the custom constant C. The key for Nonce encryption and Tag generation is K1. The underlying block cipher uses AES-128, and # represents the number of calling the block cipher which is greater than half of the all-round number and can improve the processing speed without effecting security.

The Nonce encapsulated into the packets can ensures the semantic security and resist selective plaintext attack[12]. Salt is a set of strings generated by system randomly, here salt is generated locally with certain rules to specific bit of Nonce||Header, ensuring the generation of IV1 safety at the Nonce lost, and resisting pre-calculated attack. The Header is equivalent to {protocol head, device ID, command code/reply code}, it participates in IV2 generation to ensure that different Header generates different Tag. Metadata Md is the Tag lengths to ensure that the integrity labels of different lengths produced by the same tuple {K2, salt, data frames $(P_1, P_2, \cdots, P_n)$} are not relevant.

B. Communication Process

Secure communication process between the traffic recorder and access gateway is shown in fig. 4. EIDK() represents encryption of AE, where IDE is the encryption key, Tag expresses authentication code to guarantee the integrity of the data and resist tampered during transmission, "||" indicates connection. Encryption/decryption operation and authentication operation of AE both use the key IDK, which is an agreed key between the traffic recorder and access gateway.

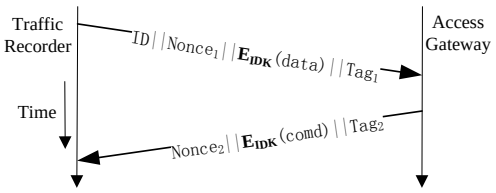

FIGURE IV. AE PROCESS BETWEEN TRAFFIC RECORDER AND ACCESS GATEWAY.

(1) Initiated a connection from the traffic recorder, using the device ID inherent key IDK for JCM encryption operation to encrypt the collect data of car state, and generate cipher text EIDK (data). Authentication operation of JCM generates authentication codes Tag1 for protocol header, device ID, command/response code, Nonce1 and EIDK (data). Traffic recorder packages device ID, EIDK (data) and Tag1, then transmits the package to the access gateway.

(2) When access gateway receives data from the traffic recorder, for protocol header, device ID, command/response code, Nonce1 and EIDK (data), authentication operation of JCM generates authentication code Tag1', which is compared with received Tag1, if equal, go to step 3; otherwise discard this package, go to step 4.

(3) According to received device ID, access gateway checks out the key IDK and decrypts EIDK(data), then transmits it to the Web server and central server.

(4) For the query command of Web server, access gate way use AE encryption operations with key IDK encrypt it to generate cipher text EIDK (comd), and by JCM authentication operation to generate the authentication code Tag2, then Nonce2, EIDK (comd) and Tag2 are packaged and transmitted to the traffic recorder, waiting for the feedback information of the traffic recorder.

In the process of interactive data of traffic recorder and access gateway, because the use of Nonce, different data communication with same device ID transmits different data, which prevents replay attacks. Authentication code is used to achieve the protection of the integrity of the data and prevent falsifying the data. The data in the channel transmission always exists in the form of cipher text, making ensure the data confidentiality. The application of AE model simplifies the process of secure communication, reduces the number of data interaction and improves the transmission efficiency. However, due to the transmission path is not encrypted, it cannot prevent the analysis of communication business.

VI. CONCLUSIONS

Traffic recorder as a device effectively improves traffic safety, which makes the relevant departments or businesses can effectively monitor the cars situation rationally. In this paper, using the GPS, GPRS and Internet resources, through special access network, we proposes a three layers of car remote diagnostic communication model, which comprise data perception, network access and application service. By modifying the program of dedicated access gateway, functionality extended model can be realized to meet a variety of traffic recorder access needs. In view of security protection of the communication data, AE scheme is used to design and implement a way for secure data exchange, which is more efficient and need relatively fewer computing resources.

REFERENCES

[1] Flores V, Mata M, Fernandez J, et al. A multi-agent, in-vehicle database recorder system for supporting traffic hotspots detection, geographical representation and analysis. *Information Fusion (FUSION)*, 2014 17th International Conference on. IEEE, 2014: 1-6.

[2] W.J. Su, Z.F. Yin. The development of the mobile vehicle traveling data recorder. *Computer Systems & Application*, 2011, 20(6): 177-180.

[3] N. Zhang, X.Q. Bi, P.G. Tian. CAN bus in the application of vehicle data recorder. *Electronic Design Engineering*, 2010, 18(9): 126-129.

[4] F. Wu. The safety communication mechanism research between the vehicle traveling data recorder and control platform. *Xi'an: Xidian University*, 2011.

[5] Maimut D, Reyhanitabar R. Authenticated Encryption: Toward Next-Generation Algorithms. *Security & Privacy*, IEEE, 2014, 12(2): 70-72.

[6] Bellare M, Namprempre C. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. *Advances in Cryptology—ASIACRYPT 2000*. Springer Berlin Heidelberg, 2000: 531-545.

[7] L. Zhang, J. Zhou, J.C. Tang. Authentication encryption algorithm in the application of CCSDS telecontrol protocol research. *Journal of Electronics & Information Technology*, 2009, 31(2): 343-348.

[8] Z.Y. Hu, J.C. Jiang, F.C. Sun. Using IND-CVA to achieve security channel. *Science in China (Series F: information Science)*, 12: 004.

[9] X.W. He, A.H. Wang, Y. Ma. GPS vehicle terminal based on GPRS communication technology research. *Journal of Computer Applications*. 2008, 28(11):2952-2955.

[10] Adekunle A A, Woodhead S R. An AEAD cryptographic framework and TinyAEAD construct for secure WSN communication. *Wireless Advanced (WiAd)*, 2012. IEEE, 2012: 1-5.

[11] Rogaway P, Bellare M, Black J. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security (TISSEC)*, 2003, 6(3): 365-403.

[12] Adekunle A A, Woodhead S R. A resourceful combined block cipher mode of operation for packetised network communication. *Next Generation Mobile Applications, Services and Technologies (NGMAST)*, 2010 Fourth International Conference on. IEEE, 2010: 180-185.