Survey on Evidence Collection in Car Black box Using Android Application

[1] Chaitrashree.V, [2] VertikaSharma,

[1] *M.Tech CSE Gsssietw,mysore*
[2] *Assistant professor Gsssietw,mysore*

Abstract - This research work presents an advanced step to the concept of car black-box in developing a comprehensive vehicle safety system which would not only record the video and audio, but also try to prevent a possible collision by limiting the speed of the vehicle in accident-prone areas. In case of an accident, the time and location (co-ordinates) is sent through GSM to a preset number for immediate rescue and treatment. Recorded data can also be used for forensics, revealing the problems that caused the accident and give manufacturer an idea for improvement. So the motto is to develop an embedded integrated system consisting of a microcontroller, a power supply unit, sensors, memory, a motor driver unit and a GPS/GSM modem.

Keywords: Evidence Collection System, Car Black Box, Smart phone, Sensors.

I. INTRODUCTION

The Black-box is a digital video-audio event data recorder. The concept is similar to the “black box” data recorders on airplanes. It records all the information, like speed & temperature of the cabin/engine, time and location, before and after the accidents so that it can be used to analyze the accident accordingly. It includes a web-camera, a microphone, a real- time clock, and other electronic components, all controlled by a microprocessor with embedded software and fully self-contained in a tiny, rugged black box that installs unobtrusively on the dash board [1] . Benefits customers receive are accurate, real time, easy to interpret data, a tamperproof system, and additional security. Other benefits include being able to see what the driver could see, hear, and feel in a crash. The user interface is very simple and has been designed to minimize driver distractions. A green indicator light shows that the system is armed and ready to capture an event. As soon as a collision is detected automatically, the indicator light will turn red and start recording all the relevant data during a pre-defined period before and after the accident. Video can take place by a camera which can be easily stored in a flash memory/SD card. Captured video and audio is date and time-stamped and can be downloaded to a laptop computer or VCR for viewing and/or long-term storage.

II. THE PROPOSED SCHEME

In this section, we make assumptions and describe our proposed scheme in detail. Our scheme is proposed under the following assumptions: Every car is equipped with smart phone, car black box, and Global Positioning System (GPS). Car black box and smart phone can communicate with each other in order to transmit data by using wireless communication, e.g. Bluetooth. In addition, they share a symmetric key in advance for mutual authentication. All of drivers use evidence collecting system and the devices are always turn on when car moves. Each smart phone is installed with special software which we developed. Besides, in order to communicate with police station server, a driver needs to have a user ID and password which are already preset in smart phone.

Process flow in our proposed scheme is shown in Figure

1. We are going into the detail of our scheme which includes the following steps:

Step 1- Updating the accident list from police station server – Firstly, smart phone uses its own ID and password in order to authenticate server. After smart phone is authenticated successfully, it frequently sends a request message to the police server station to update accident list. Whenever server receives a request message, it will send the newest accident list to the requesting user. Significantly, the response message from server contains MAC (Message Authentication Code) which is generated by user’s password in order to provide data integrity.

Step 2 - Smart phone gets critical video clips which are related to the accident list from car black box – Before transmitting data, smart phone and car black box must authenticate mutually by using pre-shared key. Because they use wireless connection to communicate, an unauthenticated user can get users’ privacy information. Therefore, the mutual authentication process prevents anonymous users from accessing privacy information, for example home location information, itinerary

information. After the mutual authentication process is successful, smart phone transmits accident list to car black box. Car black box checks whether it has any video data related to the accident list by comparing GPS-based position information and time of recorded videos with accident list receiving from the police station server. If car black box has any appropriate video, the data video will be transmitted to smart phone. In this step, moreover, driver can use smart phone to select accident videos which will be sent to police station server. This selection process helps driver to avoid sending the privacy information unexpectedly.

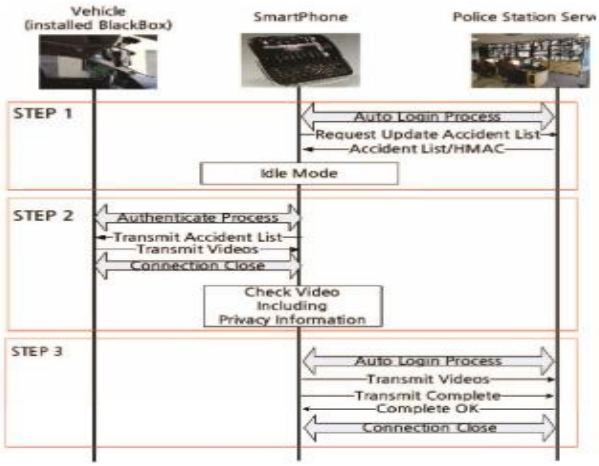

Fig. 2.1 Process flow in our proposed scheme

Step 3 – Uploading the critical videos which are selected in step 2 – It is similar to step 1, in the initiation of step3, smart phone must authenticate to server. Then, the appropriate videos, which are selected by driver, are uploaded to the police station server from smart phone. Finally, the connection will be closed after the transmission finishes.

III. DEMONSTRATION SCENARIO

A Demonstration Environment Figure 4.1 shows our demonstration environment in which a laptop plays a role as a car equipped with car black box, and GPS. Besides, we use a smart phone that is installed Android OS and has ability to access WLAN and 3GPP network. In our demonstration, smart phone accesses public network by connecting to the WLAN AP (Access Point) which plays a role as a base station in VANET environment. The WLAN AP may also be a 3GPP Node-B in the real environment.

In addition, the police station server and WLAN AP are on the same LAN which is public network in practice.

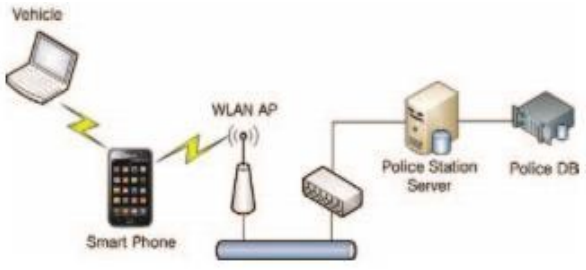

Fig. 3.1 Demonstration Environment

B. Demonstration Scenarios

1) Case 1: Smart phone gets critical videos from car black boxes. In this scenario, by using wireless connection, smartphone can connect to car black box which is a laptop in our demonstration in order to get accident videos related to the received accident list. Besides, driver can use smart phone UI as shown in Figure 3(a) to cancel upload process or select appropriate videos which is not related to driver's privacy. Moreover, this scenario also illustrates that a Smartphone cannot access car black box to get data videos without authentication process.

2) Case 2: Police station server collects critical videos. This scenario illustrates network communication between car and police station server. The police station server has an accident database which is built from reported accident information. As shown in Figure 3.2, this accident database indicates where and when the accident occurred, what kind of the accident was, for example car accident, vehicle theft, or child kidnap. Whenever a car sends a request updating message to server, the police station server responds with the newest accident list. If there is any matching video in car black box and driver allows uploading videos, the appropriate videos will be sent to server for evidence

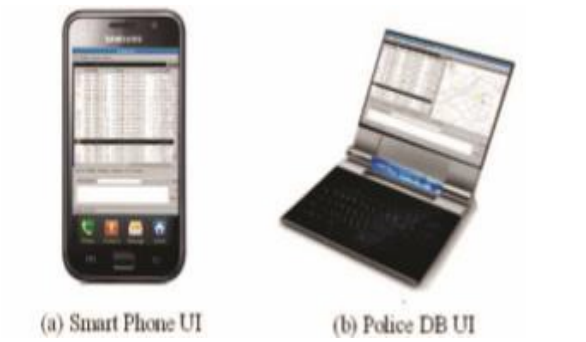

Fig. 3.2 User Interface (UI) of Smart phone and Server

IV. PROPOSED METHODOLOGY

The registration number of vehicle along with relative's phone number, emergency services number feed into the source code of the system. Consider a car had an accident the sensor will activated automatically and start its surveillance mode. If user is not in critical condition and can help himself then he will stop surveillance mode within given time period else system will consider user need assistance and start auto contacting with call center and specified person. Once the system started in assistance mode first of all system will gather the car location using GPS device in the form of longitude and latitude. Then it records car details like car owner details, car number, car model, car speed if possible and convert this data in to formatted SMS and send this data to call center and person's relative where person need to provide contact person details manually before starting drive. Once the call center get the car status it will search to find nearest police station, hospital, ambulance service and contact then to reach at accident location to help the person. About vehicle security concern, when a vehicle is about to thief, the door is about to open, then a attached system automatically generate a phone call to the user registered mobile number. The moment the user received the call from the vehicle, user can send reply SMS to stop the car engine or can take any immediate action to save the vehicle. This will provide immediate alert without any time delay so that proper action can performed within the period

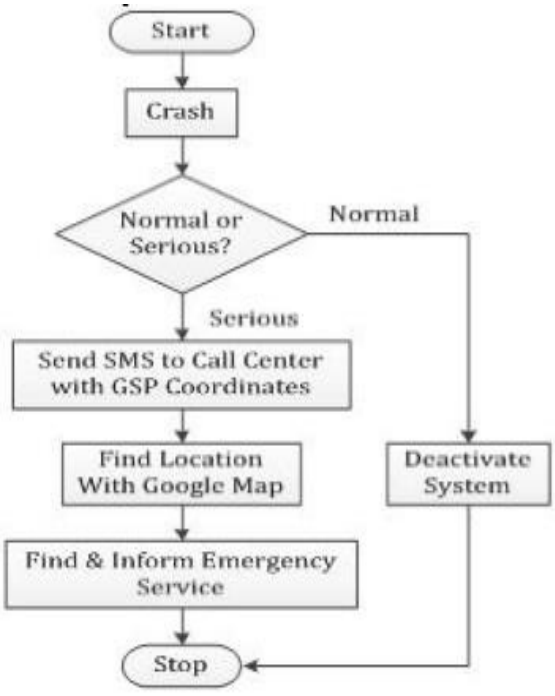

Fig. 4.1 Data flow diagram

V. RESULT

In our demonstration, the evidence collection system uses the Sensor, Raspberry Pi, USB Camera, GPS Modem and GSM module. Sensor detects the collision, USB Camera captures when collision occurs, GPS modem sends longitude and latitude values to GSM modem. GSM modem receive and sends a message to registered mobile number and also transmit all the collected evidences which indeed collected and stored in storage device like pen drive. Following are the data collected at receiver end. The collected parameters are vehicle location, time, images respectively from the prototype designed, in this demonstration data collected only when collision is occurred. The collected data by controller not only transmitted to the server but also saved to the memory at transmitting end which in case of wireless transmission failure will be helpful for data extraction. It is more flexible to watch the generated reports to the person/institution have authority for that like police, insurance company etc.

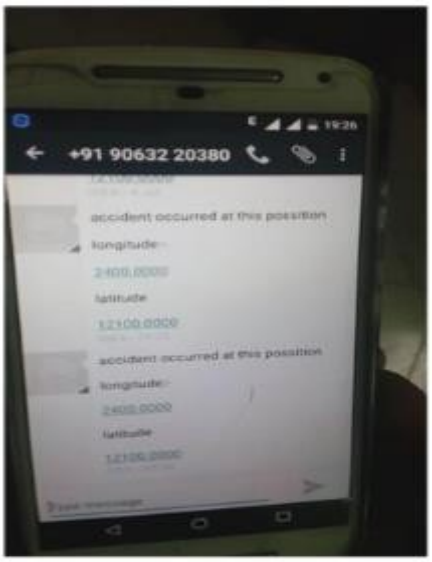

Fig. 5.1 Snapshot of location coordinates message received in mobile.

VI. CONCLUSION

This research work focuses on solving driver privacy concerns and communication and management overheads. Our contribution is that we propose a feasible and useful scenario for public safety. It develops Evidence Collection System from Car Black Box with Raspberry microprocessor as its main controller and sensor and to find location vehicle collision to save victims. With a perfect support of the embedded system technology, we believe that the Evidence Collection System from Car Black Box will have better performance and broader market prospect.

VII. FUTURE SCOPES

This project will used in different type of vehicles and also used for security purpose.

REFERENCES

[1] A. Kassem, R. Jabr, G. Salamouni, and Z. K. Maalouf, "Vehicle Black Box System," in System Conference, pp. 1-6, April 2008.

[2] D. Jiang, and L. Delgrossi, "IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments," in Vehicular Technology Conference (VTC), pp. 2036-2040, May 2008..

[3] X. Ni, Z. Yang, X. Bai, A. C. Champion, and D. Xuan, "DiffUser: Differentiated user access control on smartphones," in Mobile Adhoc and Sensor Systems (MASS), pp. 1012-1017, October 2009.

[4] Kugamoorthy Gajananan, Alfredo Nantes, Marc Miska, Arturo Nakasone, and Helmut Prendinger-―An Experimental Space for Conducting Controlled Driving Behavior Studies based on a Multiuser Networked 3D Virtual Environment and the Scenario Markup Language‖ IEEE TRANSACTIONS ON HUMAN- MACHINE SYSTEMS, VOL. 43, NO. 4, JULY 2013.

[5] Liewei Jiang and Chunxuan Yu. ―Design and Implementation of Car Black Box Based on Embedded System‖. 2010 IEEE DOI 10.1109/iCECE.2010.860

[6] Kangsuk Chae, Daihoon Kim, Seohyun Jung, Jaeduck Choi, and Souhwan Jung. ―Evidence Collecting System from Car Black Boxes‖.2010 IEEE

[7] Dae Geun Lee, Se Myoung Jung , Myoung Seob Lim.System on Chip design of Embedded Controller for Car Black Box‖. 2007 IEEE Intelligent Vehicles Symposium Istanbul, Turkey, June 13- 15, 2007

[8] Eunryung Lee, Jung Wook Lee, Jeongho Son, Automobile SW Platfrom Research Team, ETRI.OSEK/VDX-Based Gateway for Car Blackbox‖. 2011 IEEE International Conference on Consumer Electronics (ICCE).

[9] Dheeraj Pawar, Pushpak Poddar, ―Car Black Box withSpeed Control in Desired Areas for Collision Avoidance‖, ETASR - Engineering, Technology & Applied Science Research Vol. 2, _o. 5, 2012, 281-284. [10] P. Ajay Kumar Reddy, P.Dileep Kumar, K. Bhaskar reddy, E.Venkataramana, M.Chandra sekhar Reddy,BLACK BOX FOR VEHICLES‖, International Journal of Engineering Inventions Volume 1, Issue 7(October2012).