CAR BLACK BOX

Asha M[1]
Final year M.Tech student, E&C Engg. Dept.,
PES College of Engineering, Mandya
ashaatani@gmail.com

Dr. Radhakrishna Rao K A PhD [2]
Professor, E&C Engg. Dept.,
PES College of Engineering, Mandya
karkrao@yahoo.com

Abstract-This demonstration shows a process to collect critical video clips from car black boxes using smart phones. Critical video clips in the black box are hashed to provide data integrity, before being transmitted to the police server. Without VANET infrastructure, smart phones are very useful communication media for car black boxes.
Car black box is a device to record driving history which can be used for car forensics in case of car accident or related crimes. Car black box stores video clips that could be critical clues for investigating car-related accidents or crimes. Those video clips can be collected to police server via 2G phones. Especially, smart phones are very useful for this purpose. This demonstration shows the whole process to collect video proofs using smart phones through Bluetooth. Some cryptographic mechanisms were used to provide video integrity and privacy.

I. INTRODUCTION

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. We use a smart phone that is installed Android OS and has ability to access WLAN and 3GPP network.

Controller collects information from the temperature sensor, ultrasonic sensor & IR based opto coupler and displays the collected information on the LCD. GPS will collect the location co ordinates it will be stored in the controller. If accident occurs means collected information along with the video will be sent to the laptop & it will be updated in the police station server. For the demo concern videos stored in laptop will be used.

Smart phone accesses public network by connecting to the WLAN AP (Access Point) which plays a role as a base station. The police station server and WLAN AP are on the same LAN which is public network in practice. 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.

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. 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.

II. WORKING PROJECT

1) THE PROPOSED SCHEME

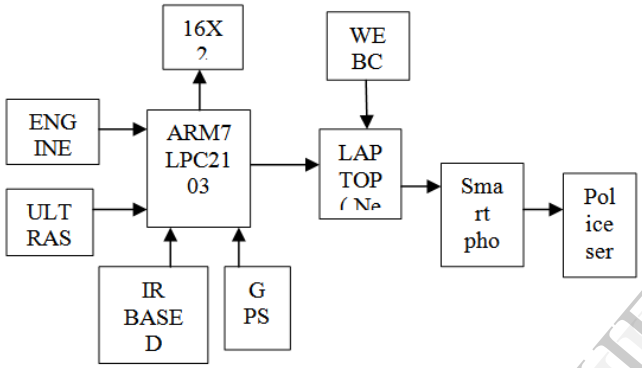
This section, we make assumptions and describe our proposed scheme in detail. Our scheme is proposed under the following assumptions:
[1]Every car is equipped with smart phone, car black box, and Global Positioning System (GPS).
[2]Car black box and smart phone can communicate with each other in order to transmit data by using wireless communication, e.g. Bluetooth. In addition, they share a symmetric key in advance for mutual authentication.
[3]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 – Hardware module detect the engine temperature, location (GPS)., tilt information, obstacle presences & door status. It send to the black box.

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.



III. DETAILED DESIGN

Module 1 – Hardware

Controller collects information from the temperature sensor, ultrasonic sensor & IR based opto coupler and displays the collected information on the LCD. GPS will collect the location co ordinates it will be stored in the controller. If accident occurs means collected information along with the video will be sent to the laptop & it will be updated in the police station server. For the demo concern videos stored in laptop will be used.

Smart phone accesses public network by connecting to the WLAN AP (Access Point) which plays a role as a base station. The police station server and WLAN AP are on the same LAN which is public network in practice. 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.

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.

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.

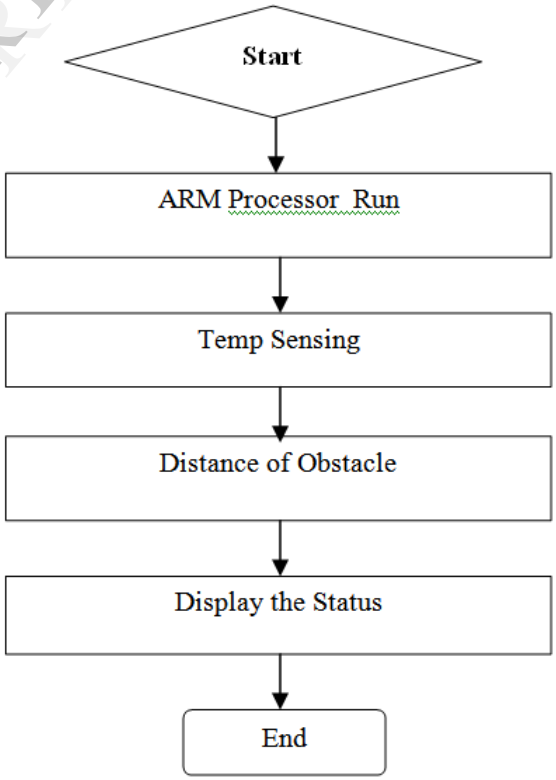


Fig 1 : Module - 1

Module -2: Software

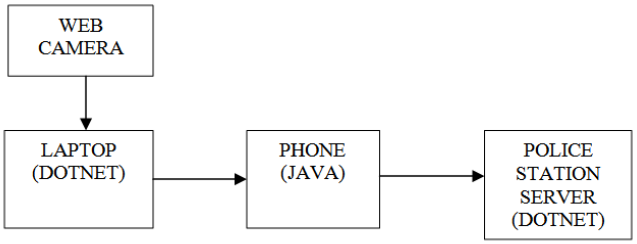


Fig 2: Module – 2

This section, we make assumptions and describe our proposed scheme in detail. Our scheme is proposed under the following assumptions:
[1]Every car is equipped with smart phone, car black box, and Global Positioning System (GPS).
[2]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.
[3]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.

Module 3 : System Design

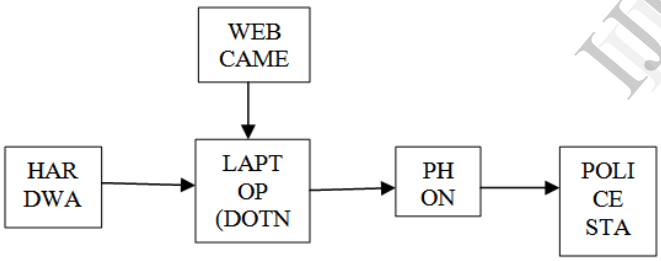


Fig 3: Module – 3

Controller collects information from the temperature sensor, ultrasonic sensor & IR based opto coupler and displays the collected information on the LCD. GPS will collect the location co ordinates it will be stored in the controller. If accident occurs means collected information along with the video will be sent to the laptop & it will be updated in the police station server. For the demo concern videos stored in laptop will be used.

Smart phone accesses public network by connecting to the WLAN AP (Access Point) which plays a role as a base station. The police station server and WLAN AP are on the same LAN which is public network in practice.

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.

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.

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.

VI. ANDROID ARCHITECTURE

The following diagram shows the major components of the Android operating system. Each section is described in more detail below.

The Android APIs: The core of the SDK is the Android API libraries that provide developer access to the Android stack. These are the same libraries used at Google to create native Android applications.

Development Tools: To turn Android source code into executable Android applications, the SDK includes several development tools that let you compile and debug your applications.

The Android Emulator: The Android Emulator is a fully interactive Android device emulator featuring several alternative skins. Using the emulator, you can see how your applications will look and behave on a real Android device. All Android applications run within the Dalvik VM so that the software emulator is an excellent environment — in fact, as it is hardware-neutral, it provides a better independent test environment than any single hardware implementation.

Full Documentation: The SDK includes extensive codelevel reference information detailing exactly what's included in each package and class and how to use them. In addition to the code documentation, Android's reference documentation explains how to get started and gives detailed explanations of the fundamentals behind Android development.

Sample Code: The Android SDK includes a selection of sample applications that demonstrate some of the possibilities available using Android, as well as simple programs that highlight how to use individual API features.

Online Support: Despite its relative youth, Android has generated a vibrant developer community. The Google Groups at http://code.google.com/android/groups are active forums of Android developers with regular input from the Android development team at Google.

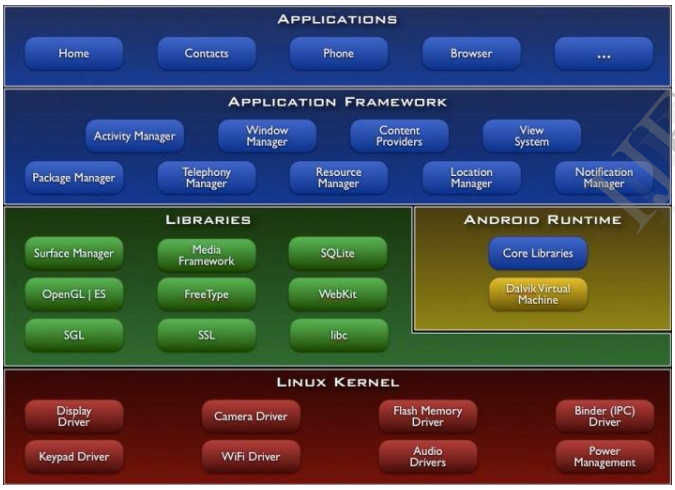


Fig 4: Architecture

Applications
Android will ship with a set of core applications including an email client, SMS program, calendar, maps, browser, contacts, and others. All applications are written using the Java programming language.

Application Framework
By providing an open development platform, Android offers developers the ability to build extremely rich and innovative applications. Developers are free to take advantage of the device hardware, access location information, run background services, set alarms, add notifications to the status bar, and much, much more.

Underlying all applications is a set of services and systems, which includes:

[1]A rich and extensible set of Views that can be used to build an application, including lists, grids, text boxes, buttons, and even an embeddable web browser
[2]Content Providers that enable applications to access data from other applications (such as Contacts), or to share their own data
[3]A Resource Manager, providing access to non-code resources such as localized strings, graphics, and layout files
[4]A Notification Manager that enables all applications to display custom alerts in the status bar
[5] An Activity Manager that manages the lifecycle of applications and provides a common navigation back stack.

V. DEMONSTRATION SCENARIO

Demonstration Environment Figure below 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 5: Demonstration environment

Case 1:

Smart phone gets critical videos from car black boxes.
In this scenario, by using wireless connection, smart phone 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 smart phone cannot access car black box to get data videos without authentication process.

(a) Smart Phone UI (b) Police DB UI

Fig6: User Interface (UI) of smart phone and server

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(b), 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.

VI. CONCLUSION

In our demonstration, the evidence collecting system, which uses smart phone not only to transmit critical videos to the police station server, but also to manage information obtained from car black box, was proposed. In fact, it is very hard to fully deploy VANET infrastructure. As a result, even though the communication between car black box and police station server which use VANET infrastructure could be possible, it is not easy to apply in practice. In addition, our demonstration also shows how to apply security functions in evidence collecting system. In our proposed scheme, therefore, security services are guaranteed, e.g. access control and data integrity.

REFERENCES

[1]Muhammad Ali Mazidi & Janice Gillispie Mazidi, "The 8051 Microcontroller and embedded systems", 6th edition, Pearson Education.
[2] J. Casper, "Human-Robot Interactions during the Robot-Assisted Urban Search and Rescue Response at the World Trade Center", MS Thesis, Computer Science and Engineering, USF, South Florida, 2002.
[3] "The 8051 micro controller and embedded systems using assembly and C" Muhammad Ali Mazidi , Rolin.D.McKinlay,Janice Gillispie Mazidi
[4] "Embedded System Design" Frank Vahid and Tony Givargis, John Wiley
[5] www.carblackbox.co.uk/