A Thesis

entitled

Security Enhancement of Over-The-Air Update for Connected Vehicles

by

Akshay Ajay Chawan

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the

Master of Science Degree in

Electrical Engineering

_____

Dr. Weiqing Sun, Committee Chair

_____

Dr. Ahmad Y. Javaid, Committee Co-chair

_____

Dr. Hong Wang, Committee Member

_____

Dr. Amanda Bryant-Friedrich, Dean
College of Graduate Studies

The University of Toledo

August 2018

An Abstract of

Security Enhancement of Over-The-Air Update for Connected Vehicles

by

Akshay Ajay Chawan

Submitted to the Graduate Faculty as partial fulfillment of the requirements for the
Master of Science Degree in
Electrical Engineering

The University of Toledo

August 2018

Similar to wireless software updates for the smartphones, over-the-air (OTA) methods are used to update the software and firmware for the various electronic control units (ECUs) in the car. It is an efficient and convenient approach to update the software in the car and it will help customers save their money and time by reducing time to visit the service center to repair small bugs in the software. However, OTA updates open a new attack vector for hackers, who can use the OTA mechanism to steal OEM firmware, to reprogram ECUs, or to control the vehicle remotely. In this thesis, we perform a comprehensive security analysis for the current OTA mechanism to understand its associated threats. We also propose an approach to secure the original OTA software update method by adding a biometric iris scan and cryptographic hash function before updating the software and firmware over the air. With these security enhancements, vehicle owners can ensure that the car can be secure from unwanted and potentially malicious software updates.

To my father *Ajay Narayan Chawan*, my mother *Ashwini Ajay Chawan*, my brother *Aakash Ajay Chawan, my Uncle Shrikant Chavan and my Cousin Mahesh Gawade* for their colossal love, care and determination to raise me to this level and higher in all odds.

Acknowledgements

The achievement of my master's degree is a dream come true because of numerous people who directly or indirectly influenced, motivated and helped me in this journey. I would first like to thank my thesis advisor, Dr. Weiqing Sun, for his incredible support in the form of his motivation, useful comments and guidance throughout the research work of this master's thesis. I wish to express my sincere thanks to Dr. Mansoor Alam, Dr. Ahmad Javaid and Dr. Hong Wang for guiding me and providing ideas through the tough times of my thesis. I am also grateful to Umesh Gurav and Mohammad Majid, who helped me acquire the skills used in my research.

I wish to express my sincere thanks to University of Toledo Information Technology Department's and my managers Teresa Hagedorn and Jeremy Santus for their support. I would like to thank all the members of TAG house, my family away from home who never made me miss my home back in India. I place on record, my sincere thank you to my best friends Janhavi Kondurkar, Shruti Patil and Payal Velhal, who always stood by me during my difficult times. And a big thank you to my mom Ashwini Chawan, dad Ajay Chawan, uncle Shrikant Chawan, my cousins Shrinit Chawan and Mahesh Gawade and my entire family who always believed in me and motivated me as I accomplished my dreams. This accomplishment would not have been possible without all the people mentioned above. Thank you.

Table of Contents

List of Figures

List of Abbreviations

ADR .....Automatic Driver Recognition
AMP .....Arbitration on Message Priority

BCM.....Body Control Module

CAN .....Controller Area Network
CCD .....Charge Coupled Device
CPU.....Central Processing Unit
CRC.....Cyclic Redundancy Check
CSMA/CD.....Carrier Sense Multiple Access / Collision Detection

DBMS .....Database Management System
DLC.....Data Length Code

ECU.....Electronic Control Unit

FBI .....Federal Bureau of Investigation
FOTA .....Firmware Over The Air

GPS .....Global Positioning System
GSM.....Global System for Mobile communications

HD.....Hamming Distance
HVAC .....Heating, Ventilation and Air Conditioning

IEEE.....Institute of Electrical and Electronics Engineers
IOT.....Internet of Things
ISM .....Industrial, Scientific and Medical
ISO .....International Organization for Standardization

LCD.....Liquid Crystal Display

MAC .....Media Access Control

NFC.....Near Field Communication

OBD .....On Board Diagnostic
OEM.....Original Equipment Manufacturer
OTA .....Over The Air

PHY.....Physical layer
PIC .....Peripheral Interface Controller

RTR.....Remote Transmission Request

SHF .....Super High Frequency
SMS.....Short Message Services

TESLA .....Timed Efficient Stream Loss-Tolerant Authentication

UCR .....Uniform Crime Reporting
UHF.....Ultra High Frequency
USA.....United States of America

VIN .....Vehicle Identification Number

WLAN.....Wireless Local Area Network

Chapter 1

Introduction

It is the century of exciting technology with the development of many types of smart devices. Traditional electronic devices are now equipped with an extraordinary level of intelligence. Mobile phones, an example of an electronic device used daily, have become “smarter” far beyond making calls. Wristwatches are now smartwatches that can do more things than just showing time. All these electronic devices bring increasing levels of comfort, convenience, and efficiency to individuals. Most recently, normal cars are becoming smart cars that are capable of more than just transportation. Modern automobiles are slowly transforming into ‘smartphones-on-wheels’ [1] which uninterruptedly generate, process, exchange and store large amounts of data.

Vehicles are evolving into computerized systems with electrical structures replacing or augmenting mechanical ones. Automobile systems can connect to external networks, such as the internet, by using their wireless interfaces and can enhance the consumer experience by enabling new features and services [2]. However, connecting the car to the external networks makes it susceptible to hackers, who can attack the car by seeking and manipulating weaknesses in its computer systems or networks.

Because of such security risks, it is crucial to upgrade and update automobile security systems regularly as the loss of its integrity and confidentiality can have an

adverse effect to the users. The new trends for car automation and security, deemed more feasible and viable as recognized globally in this modern era, have replaced the traditional ways such as using various locking and antitheft systems. Efficient software algorithms have been developed to enable deployment of general biometric based platforms. To remain vibrant in this technological reformation, the development of different car security applications has excited researchers. It results in the shifting the environment from a traditional way of securing one's car to advanced technologies because of the following immediate benefits: accessibility, mobility, feasibility, spontaneity, and real-time communication.

In this thesis, biometric iris authentication technology is used to ensure that only legitimate users can install the available updates from OEM (original equipment manufacturer) servers to the respective ECUs and sensors. Furthermore, a method is proposed to prevent the attacker from making any changes to the settings of the vital sensors in the car that can prove lethal to the life of the driver and passengers in the car.

1.1. Automobile Theft Statistics:

Over-the-air (OTA) updates for software and firmware will provide better safety and convenience. Technological and rising demand from USA and other countries are the major factors driving growth in the connected car security market. FBI's Uniform Crime Reporting (UCR) Program reports that the rate of motor vehicle theft was 216.2 per 100,000 inhabitants and estimated 689,527 thefts of motor vehicles nationwide in 2014. FBI uniform crime reports of 2015 estimated 707,758 motor vehicles theft took place in an academic year and the rate of occurrence of vehicle theft is every 14.6 seconds which is awful for developed nation like USA [3].

The graph in Figure 1-1 shows statistics per the 2010 FBI crime report, indicating most motor vehicle thefts take place in metropolitan counties with large populations of 100,000 and more while vehicle thefts in nonmetropolitan counties with the same population is comparatively low. According to 2014 FBI statistics, there was a loss of more than $4.5 billion due to motor vehicle theft in the US. The average dollar loss per stolen vehicle was $6,537, which does not include the emotional damage it does to the car owner. This amount itself exceeds the cost of maintaining a basic automobile security system in a car. Among the types of property stolen, locally stolen motor vehicles had the highest percentage of property value recovered at 55.2%.

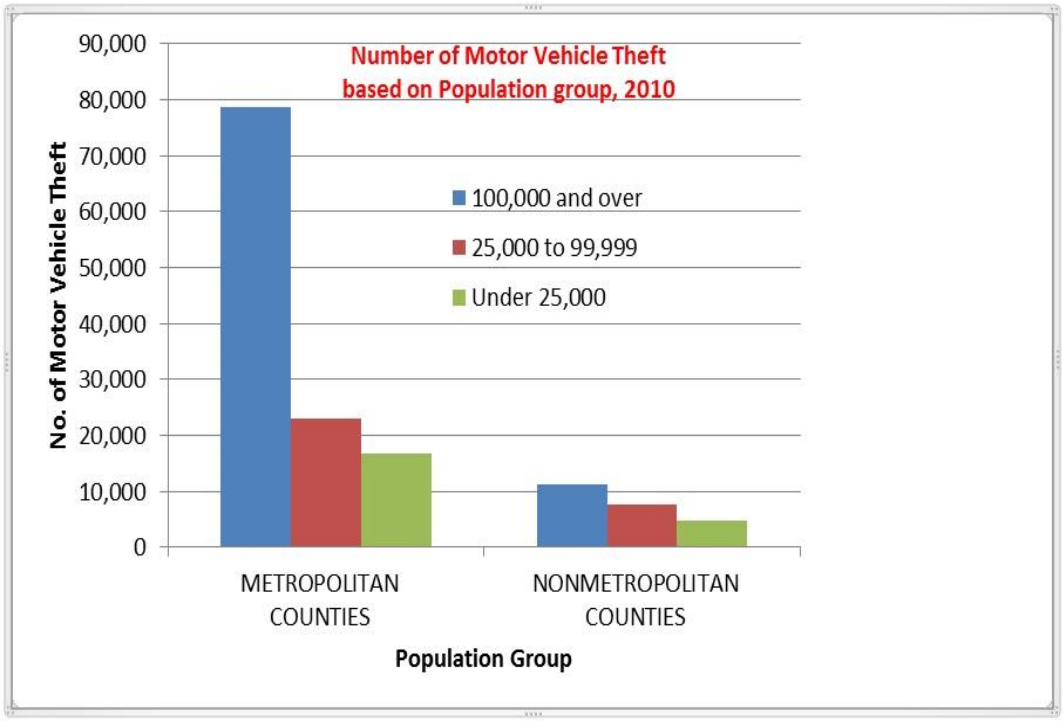

Figure: 1-1. Graph of Motor Vehicle Theft by Population Group [4].

1.2. Terminology

1.2.1. IEEE 802.11 Standard:

To allow computers to communicate via wireless local area networks (WLANs) in the 900 MHz and 2.4, 3.6, 5.0, and 60 GHz frequency bands, the Institute of Electrical and Electronics Engineers (IEEE) created and maintained a set of media access control (MAC) and physical layer (PHY) specifications known as IEEE 802.11. The first version was out in 1997 and IEEE keeps on releasing succeeding amendments. The commercial world briefly denotes proficiencies of their products depending on the amendments incorporated in the newest version of the standard. This makes each amendment to maintain its own standards in the marketplace [5].

1.2.2. Wi-Fi:

Wi-Fi is a trademark of the non-profit organization Wi-Fi Alliance, which restricts the use of term "Wi-Fi Certified" to products that have successfully completed interoperability certification testing. Wi-Fi Alliance defines Wi-Fi as a technology allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another within a wireless local area network. As it is a wireless connection, it uses the ISM radio bands of 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF. WLAN network and wireless access points are used to connect Wi-Fi enabled devices to the internet. These wireless networks or access points can range up to 20 meters (66 feet) indoors and can have a greater range outdoors using multiple overlapping access points. WLAN may be an open network or a secure network protected with a password. Any device in the range of WLAN can be connected to it automatically

if the network is open. Generally, however, it is password protected, which limits the usage to specific devices with the password to access it [6].

1.2.3. Firmware:

Firmware is a software category in electronic systems and computing that provides control, monitoring and data manipulation of engineered products and systems. Devices such as computers, computer peripherals, mobile phones, and digital watches are examples of devices containing firmware. Most of the firmware are capable of receiving updates.

1.2.4. Cellular Device:

A cellular device is a small, handheld computing device powered by a lithium battery that can run various applications using a pre-installed operating system. The device has a virtual keyboard and buttons on the display screen. It can be interconnected to other devices like router or other infotainment systems or to internet using wireless communication techniques like Wi-Fi, Bluetooth or NFC [7].

1.2.5. Smart Device:

A smart device is an interactive electronic device with computing powers that use different wireless protocols to connect to other devices, and, in some cases, may have artificial intelligence. Though portable and small in size, smart device can have a memory of few gigabytes. Mobile phones, iPads, smart watches and smart bands are some of the noteworthy smart devices [8].

1.2.6. Biometric Devices:

A biometric device is a device that uses the physiological or behavioral characteristics of an individual to verify one’s identity. Security protocols of biometric

devices are more effective and efficient than non-biometric devices as they rely on biometric characteristics of an individual that are unique for every person [9].

1.2.7. Cryptography:

Cryptography is needed to carry out a secure wired or wireless communication in the existence of malicious attacker. The major component of cryptography is encryption. A key is used to convert an input into an encrypted output using various algorithms. The input feed to the algorithm is known as plain text while the output received from the algorithm is known as cipher text. If the similar key is used, then same cipher text is obtained from a given algorithm for its corresponding plain text.

1.2.8. Database:

A database is an electronic collection of data. The collected data is organized using tables, schemas reports, queries and other objects in such a way that a computer program can swiftly select desired bits of data when required by the user. To manage the huge amount of data, a computer software application knows as Database Management System is used. DBMS interacts with the user, other applications and database itself to capture and analyze data. MySQL, Oracle, Microsoft SQL server and Sybase are some of the renowned database management systems used now days [10].

1.2.9. ECU:

An electronic control unit (ECU) in a motor vehicle is a standard term for any embedded system that involves hardware and software essential to accomplish the tasks expected from each division of a motor vehicle. The ECU controls various electrical and electronics systems or subsystems in a motor vehicle.

Chapter 2

Literature Review

2.1. Biometric Recognition:

To provide a service or to let a user use an application, we need to confirm the identity of the user by requesting some proof. For example, an individual can provide a pictured document to confirm his identity. Another way to verify identity is by entering the password manually in the system. Unlike these two methods, the use of biometric identification using features such as fingerprints, iris or face does to identify the user does not require the user to carry any documents with him or memorize passwords to verify himself [11].

2.2. Internet of Things:

Internet of Things (IOT) helps us to connect the day to day life activities with the computer and internet based systems. IOT helps to control all the devices using the internet and helps to process the data over internet and network using various protocols. IOT finds an important role in Home Automation system as it can be used to improve the techniques to carry out the daily chores in an efficient way [12]. The IOT devices can be classified in two parts: a.) One way IOT devices that can be used only to notify the user and the devices are not capable of acting on the commands received from the user. b.)

The second way IOT devices not only notifies the user about the changes or warnings but also respond as per the instructions sent out by the operating personnel.

2.3. Effective Biometric Techniques:

Various biometric techniques based on an individual's physical characteristics and behavioral traits are used to uniquely identify an individual. All biometric technologies work on the principle of recording the person's characteristics and store in a secure database and then compare it with the incoming data during verification. Out of all the biometric traits, Iris recognition is gaining attention in today's world as it is one of the strongest verification methods and it is unchanging over time. As iris scan uses the unique pattern of human's iris part of the eye, it can be very challenging for the attackers to forge the iris template stored in the data base which can help to overcome the previous inadequacies [13].

2.4. Updating Car ECUs Using Firmware Over-The-Air (FOTA):

The automobile industry has grown and so has the technology to support it. A telecommunication industry has proven to update the software on mobile devices, the research [14] talks about how we can implement the same technology called the Firmware Over-the-Air (FOTA). The current technology is not flexible to cope with quick changes that take place in the auto industry. This technology has helped give better customer service costs, avoids product recalls. The research talks about the updated methodology used in the automobile industry. After implementation of this technology we will be able to turn the car from iron driven to code driven. This will help us to be safe and to be cost-effective.

2.5. Working of Iris Recognition:

The iris patterns developed by the author have been tested, the trials did not produce any incorrect matches having millions of comparisons data. The research [15] has explained the iris recognition algorithms. It demonstrated the comparisons results from the traits of Britain, USA, Japan and Korea. Iris patterns have raised popularity due to the other technologies weakening. Iris recognition can be helpful where very large databases without any false database matches. The iris gives a great mathematical advantage as the patterns in every person are different. The thesis has talked about the mathematics of iris recognition and have concluded that the databases of the entire nation can be searched in parallel to identify a person in a fraction of a second even by using inexpensive CPU's.

2.6. Making Full Vehicle OTA Update:

The infield software updates helps the car manufacturers save money, enable critical bugs to be patched immediately. Within OTA are systems that are only designed to update infotainment or telematics systems. The research talks about the ability to perform OTA updates to ECU's within the vehicle. Because of the wide variety of ECUs available, one update process will not work for all ECUs. The in-place update approach can be more cost saving but would require the interruption of vehicle usage. The A/B method can be used as a zero downtime update but will cost a lot as compared to in-place update. The entire process can be managed by central gateway ECU like NXP MPC5748G [16].

Chapter 3

Car Security Review

3.1. Existing Car Security Systems

This chapter describes the design and construction of some current and proposed advanced car security system using the Global System for Mobile communications (GSM) and other technologies [17].

3.1.1. Basic Car Theft Security:

Basic care theft security uses GSM networks to transmit alarm signals and control instructions. The control and communication between the user and the proposed system are achieved through a short message services (SMS) protocol available in the mobile phone. If the car door is illegally opened or the car is vibrated, an alarm will be activated and send an SMS message to the owner's mobile phone immediately and automatically. Thus, the user could easily protect and control their car anywhere at any time.

The proposed system consists of both hardware and software parts. The hardware components include vibration sensors, a PIC microcontroller, a GSM modem, LCD and buzzer. The software part includes a program controller interface. The control system is based on the PIC16F877A microcontroller and AT commands. This system senses five parameters for security:

1. Vibration sensing
2. Obstacle sensing
3. Revolution sensing
4. Micro switches (door 1 and door 2 open)
5. Battery sensing

This system sends SMS through GSM modem and generate sound at every sensing point. Microcontroller AT89S52, which is a low-cost and highly-reliable system, is used. By making some required changes in the software we can alter the working of the system. A Buzzer must be incorporated in the car, which will sound when any of the parameter is sensed.

3.1.2. On-Star:

Figure: 3-1. On-Star Control Panel.

OnStar systems operate over a digital cellular network in the United States and just with the push of a button in their cars; its customers can contact the service 24 hours a day. One of the element of OnStar's "three-button system" is, if you get lost on some country back road, you can easily connect with an advisor, and he or she will give you turn-by-turn directions to get you home. OnStar also provides hands-free calling with the push of the second button with an accompanying plan or pre-paid package of minutes. The third button is used to place an emergency call directly to an OnStar "Advisor."

In an emergency, such as a car crash, air bag sensors or other sensors built into an OnStar-equipped vehicle can automatically alert an operator to the condition and location of a vehicle, which then can be used to direct emergency responders. OnStar can also unlock your car if you lose your keys or honk your horn if you're lost in the vast sea of a parking area. This system helps to track stolen cars via GPS and operators can block the ignition of newer models and remotely slow them down during high-speed chases. Its mobile apps for iPhone and Android make features like remote door unlocking even easier. It can cost $199 a year for a basic "Safe & Sound" plan or $299 a year for the "Directions & Connections" plan, which adds in turn-by-turn navigation if you are lost.

3.1.3. LoJack:

LoJack is one of the most famous examples of car security that uses radio tracking to hunt down and recover stolen vehicles. It also uses the same principal as other tracking devices: Small transceivers are hidden inside the car and can be tracked by an outside source tuned to the proper frequency. Because GPS receivers require line-of-sight to an orbiting satellite to acquire a positioning fix, systems like the LoJack have the advantage of tracking cars in some places GPS will fail.

LoJack has close ties with law enforcement organizations hence the devices show up in police computer systems. LoJack units relate to the car's unique vehicle identification number (VIN), so when a car is reported stolen and the VIN is entered the state police crime computer, which automatically triggers the LoJack Unit in the vehicle.

LoJack stands by its product with a 24-hour recovery guarantee. If your car is stolen and cannot be found within 24 hours, you get your money back—for the LoJack, anyway. The disadvantage of LoJack is that the recovery system is only good in certain

counties in the United States and it's expensive. The basic version of LoJack costs $695, but owning one could potentially save you up to 35% on automobile insurance.

3.1.4. BMW Assist and Security Plus:

In 2007 series of car, BMW began offering its own version of OnStar, BMW Assist. BMW Assist includes most of the features like automatic collision detection, communication that make OnStar so popular added with a BMW response specialist and remote door unlocking. BMW claimed that it will work with police to help with stolen vehicle recovery as the system uses a GPS system for tracking and a cellular system for communication.

While BMW Assist was free for the first four years in some 2007 and later vehicles, BMW charges a $199 yearly fee from then on. Not all BMWs include Assist as a standard feature. Some BMW models, for instance, only gets BMW Assist in a premium package.

The BMW X5 Security Plus looks very like a normal BMW X5, but its armor plating can shrug off bullets from an AK47, and several vehicle options like sirens and front- and rear-cameras make it far more secure than your average car. In a slightly less practical but way cool implementation of security features, BMW's X5 Security Plus is the only publicly available vehicle from a large-scale car manufacturer to offer Class 6 bulletproof body and glass.

3.1.5. Carshield:

CarShield essentially outfits older cars with a security and diagnostics system with a small adapter. By simply plugging CarShield into the diagnostics port of any vehicle manufactured since 1996, it can access the vehicle's computer system and

transmit data to an Internet-connected device or a phone using cellular technology. CarShield monitors the car's battery and heat level of the car and can also detect other problems like oil pressure and tampering. The integrated GPS is useful for vehicle tracking purpose. CarShield can also be configured to provide updates or alerts about vehicle status over e-mail or SMS on the phone.

CarShield is one of the least expensive examples of telematics in the market today. Telematics refers to the field of telecommunications and informatics. If you own a car manufactured post-1996 and want to enhance it with telematics abilities, you can install CarShield at a price of $349 and with an annual fee of $159 to cover the system's wireless services and roadside assistance.

3.1.6. Commando FM - 870:

The cars come with a keychain pager, a small device that lets you lock or unlock your car doors from afar. They're a basic accessory for new cars and provide convenient ways to make sure your doors are always locked. The Commando FM-870 is a souped-up keychain pager. It can unlock car doors without a key and start the engine remotely from 2,500 feet (762 meters) away. The Commando includes a small device with an LCD display that monitors doors and trunks open/closed and can detect hard impacts to a vehicle.

Forced entry or engine startup will trigger an alert to the Command FM-870s LCD display. In addition to its remote start and keyless entry functions, the Commando component that's installed in the vehicle also includes a car alarm that can be programmed to trigger based on unauthorized vehicle access. The multi-function Commando FM-870 sells for $169.99 on Commando's Web site. The installation process

for the Commando requires some manual wiring so the vehicle owner should know how to install it before making a purchase.

While the Commando FM-870's LCD-equipped remote helps, it stands out from the crowd, it's far from the only multi-function security system on the market. Next, let's look at the Viper 1002.

3.1.7. Viper 1002:

If the Commando piqued your interest, Viper's 1002 security system is worth considering. The package comes with two, four-button remotes that operate over radio frequencies up to about 1,320 feet (402 meters), a shorter range than the Commando. The Stinger impact sensor detects pressure applied to the vehicle and can respond to lighter occurrences with an alarm chirp rather than a full-on blast of sound from the six-tone siren system. For instance, anyone who happens to lean against your car on the street will be treated to a light warning instead of a blaring alarm that disturbs the entire neighborhood. The Failsafe Starter Kill, which you would activate after parking and getting out of the car, is designed to keep the engine on lockdown. Once enabled, it won't start, even with a key.

The convenience options like remote engine start and keyless entry or trunk opening are here, too. While Viper set an MSRP of $299.99, the Viper 1002 security system retails for considerably less at several stores: Amazon.com sells it for $112.

Now that we've gotten a nice look at multi-function security systems, let's look at a more focused device with a singular purpose: keeping that engine cold, no matter how hard car thieves try to go for a joyride.

3.1.8. Cobra 8510:

U.K. based Cobra produces a range of car accessories, from headrest-mounted DVD players to parking aids. Cobra has a GPS tracking systems. But Cobra also sells a car security device known to stop thieves in their tracks. The Cobra 8510 immobilizer's name alone should give you a pretty good idea about how this car security system works. It's accredited by the Thatcham organization, which tests and rates vehicle security systems. Immobilizers work by disabling components of the engine that are necessary for startup. By shutting down the ignition system, immobilizers make it extremely difficult to hotwire a car and start it up without a key. The Cobra 8510 comes with two keys that can deactivate the system -- if you keep them safe, your car shouldn't be going anywhere without you in it.

The Cobra arms itself automatically -- without a key, car thieves will have serious trouble making off with any car they break into that's fitted with an immobilizer. And compared to GPS solutions or other multi-feature car security solutions, immobilizers come at a low price. The Cobra 8510 costs about $65 on Amazon.co.uk.

3.1.9. Cobra Trak 5:

Cobra's ConraTrak 5 takes the benefits of several disparate Cobra security systems and bundles them together into one powerful system, which earned it a Category 5 placement in the cham system, which means it will help you recover our car. The CobraTrak 5 system is recognized as the top range systems, because its vehicle tracking systems works in a unique way.

An automatic driver recognition (ADR) system forms a link between your car and a card with yourself. If the card is outside the car, the ADR system is armed and instantly alerts Cobra's operating center if the car is moved. If a thief somehow makes off with

your keys but won’t be able to take the ADR card along with them they can be caught easily. The ADR system will be aware that the card isn't in the vehicle with the car thief. Cobra can also initiate remote engine in mobilization. Once a stolen car has been shut off, it would not turn on again. Partnered with GPS tracking system, remote engine immobilization increases the chances that police will be able to find and recover a stolen vehicle.

This is a high-end, pricey security system for car owners who live in Europe. Cobra charges £649 ($1,050) for the system, plus £199 ($322) for an annual monitoring fee. It may not come with GPS tracking or remote engine immobilization, but it will make it a whole lot harder for a carjacker to sell your stolen vehicle to an underground chop shop or an illegal garage.

3.1.10. VINshield:

Every vehicle is allotted its own vehicle identification number (VIN), a series of digits unique to that car. The VIN is located on the console, where it's viewable through the car's windshield. Covering the VIN to hide it from prying outside eyes is a way for car thieves to hide a vehicle's identity. Once a car is stolen and makes it to a chop shop say it a goodbye; it'll be carved up and sold for parts, and a single VIN number would not make any difference. But through a process called VIN etching, you can apply that one-of-a-kind identification number to your car windows, making it difficult and expensive to sell the car off for parts.

VINshield is a product that makes it easy to apply VIN serials to all your car windows. A do-it-yourself kit includes stencils with your VIN and a chemical agent to apply to the window to etch the identification code into the glass. The two warning

stickers that come with VINshield may do an even better job of warding off potential thieves. VIN etching can't track your car by GPS, or immobilize the engine or set off a blaring warning siren, but it can discourage carjackers and make your car more difficult to sell illicitly. Best of all, a single car VINshield kit sells for a mere $19.95, far less than most car security systems.

VINshield is a best practical example for car security, but some of the most amazing high-tech security systems aren't exactly on the market yet. Nissan and Lexus have been working on it to make it better, let’s look at what futuristic car security they are trying to bring into the market.

3.1.11. Nissan Vision 2015:

The goal of Nissan's Vision 2015 project is to develop new car concepts and technologies that aimed at reducing the deaths and injuries caused by motor vehicle accidents. One of Nissan's Vision 2015 concept cars embodies that goal to the fullest, integrating advanced technology into a car to prevent the drivers from driving the car when they are drunk and hence prevent drunken driving accidents.

The car's seat and gearshift are fitted with the sensors which can detect alcohol through the driver's perspiration and prevent the vehicle from being driven. Additionally, a camera is being fitted which continuously watches the driver's eyes. If it detects signs of drowsiness or drunkenness, accordingly the car issues a voice alert to the driver and tightens the seat belt to make the driver alert and stop the car. The car can also detect suspicious driving activity that could indicate someone falling asleep at the wheel or drifting out of the lane. In this case, also the car may give the driver same alert and tighten his seat belt to make him aware of the situation.

3.2. Authentication Frameworks Used in Automobiles:

3.2.1. TESLA:

The TESLA (Timed Efficient Stream Loss-Tolerant Authentication) framework has been designed for low-execution communication frameworks [18]. In TESLA, the sender delivers another symmetric key and calculates the MACs for at least one message. In the wake of accepting the messages, the sender communicates the key on the bus, allowing each recipient to confirm the sender of the earlier message. As the keys are sent alongside the information of the following message, the corresponding over-head of TESLA is insignificant. In any case, the inevitable time delay amongst receiving and confirming a message constrains TESLA's real-time configurations. Further-more, TESLA just provisions fractional recipient validation in communication frameworks without sender identifications, and does not convey stream approval or encryption.

3.2.2. Libra-CAN:

For the vehicle domain, focus has been given on Lightweight Broadcast Authentication Protocol for CAN in the research work known as LiBra-CAN developed by B. Groza [19]. It validates senders at the receipting ECUs by means of Mixed Message Authentication Codes (M-MACs) in which keys are administered to constellations of ECUs. LiBra-CAN does not fret about key trades and needs pre-shared keys.

3.2.3. CANAuth:

The lightweight authentication mechanism CANAuth has been proposed by Herrewege [20]. The keys are allocated for message clusters and it permits broadcast

authentication. Before the authentication can be achieved for message clusters, it calls for pre-shared keys similar to LiBra-CAN and CANAuth.

3.2.4 VeCure:

VeCure is another authentication protocol developed by S. Sawhney [21] in 2014. Centered on trust, the ECUs are split into various classes and then keys are allocated to these classes. It suggests programming these keys at the initial setup of the vehicle and is dependent on pre-programmed keys.

Most of the systems explained in the above research are not satisfactory or operational, as these strategies rely on the basic trust of pre-programmed keys. Due to the long lifetime of vehicles, keys must be updated occasionally in order to dodge different attacks. In addition, the safe generation and programming of keys isn't a minor issue. Thus, the above approaches may not be reasonable for real-world applications.

3.3. Threats to Connected Vehicles:

Presently, encryption is uncommon, and, if accessible, regularly utilizes comparative keys over a progression of vehicles and ECUs. The traditional information transmissions are not encoded or validated and authentication is used while reinventing ECUs. Koscher and Checkoway [22] demonstrated that ECUs can be reconstructed by obtaining pre- modified security keys from the automobile tuning group, and outlined the security issues in contemporary networked vehicles.

The greater part of these attacks has been performed with direct associations with the vehicle, yet in [23] attacks by means of external interfaces like integral telematics unit have also been reported and the same was demonstrated by Checkoway. As of late, as per an analysis of automotive networks and control units by Miller and Valasek in 2013 [24],

various types of vehicles have been evaluated and two vehicles have been attacked widely. Miller and Valasek made use of either vehicle's OBD port or the vehicle's networks to execute these attacks.

In the attacks demonstrated by Mundhenk and Paverd [18], they performed the attack through a cellular connection and have broadened the purpose of the attack. Hoppe in his research [25] discussed the attacks particularly related to the Controller Area Network (CAN), and their countermeasures. In addition, Othmane in his case study [26] did a contextual analysis exploring the probability of attacks on vehicles in light of expert knowledge. Flavio Garcia performed a case of a Rainbow table assault to break the 96-bit Megamos Crypto calculation utilized by numerous vehicle producers. Building the 1.5 Terabyte rainbow table took short of one week, however the comprehensive pursuit just took seconds [27]. As it illustrates that security instruments can be compromised and the vehicle can be stolen without much of a stretch, this can have a potential ramifications for vehicle proprietors. Zhang from Cisco Systems demonstrated that with the use of embedded web programs, on-board diagnostic ports, removable ports and media players, numerous potential instruments can be tainted by malware. He also described the critical danger postured by malware to the vehicle's control framework and the potential ways by which vehicle's security keys can be compromised by the attackers to update the ECU programs [28].

Chapter 4

Biometrics

4.1. Characteristics of Biometrics:

1. Generality: The Biometric trait should be possessed by everyone who is using the system and application. Every individual accessing the application should possess the trait.

2. Peerless: The given attribute should be unique across individuals comprising the population.

3. Stability: Over a period, the biometric feature of an individual should be sufficiently uniform with respect to the algorithm used for the process. The biometric feature that changes with time is not beneficial.

4. Scalable: The Biometric characteristic should be easy to obtain and compute with the devices that do not affect the individual directly. Furthermore, the acquired raw data should be amenable to processing to extract representative feature sets.

5. Performance: The certainty of acceptance and the resources used to obtain the certainty of biometric feature should meet with the restraints applied by the applications used.

6. Creditability: The individuals who will be using or utilizing the technology should be ready to give their consent to offer their biometric characteristics to the system.

7. Abdication: This cites to how comfortless the artifacts can be used to imitate an individual biometric feature. For example, gait of an individual in behavioral trait.

8. Accuracy: The system should be compatible and should be able to accurately obtain the biometric attribute of the individual each time when it is requested.

4.2. Significance of Biometrics:

Biometric techniques for determinative the identity of people, like in security applications, are standard and in use for an extended time currently. There are various techniques under biometric genre to uniquely identify an individual based upon physical features, such as finger or palm print, facial or iris recognition, and retina scans or behavioral traits such as typing rhythm, gait or voice. Biometric technologies differ from each other but all work on a similar basic platform: gathering unique physiological and behavioral characteristics of a person, and storing it in a database or comparing it to already stored templates in database. Iris recognition is one of the strongest methods of biometric authentication as it uniquely differs from person to person [29]. Iris recognition systems are gaining interest and popularity in terms of security and it is becoming stable over time. Iris recognition technology provides positive identification of an individual, at extremely high confidence levels. It uses the unique patterns of the human iris, shows a great promise to overcome previous shortcomings.

4.3. Biometric Techniques

4.3.1. Physiological

a. Hand Geometry

The measurement of an individual's hand along many dimensions to identify an individual by comparing with the measurements stored in the data base is known as

biometric Hand geometry. This technique is based on measuring the physical characteristics of an individual's hand that includes palm dimensions along with length and width of the fingers.

b. Lip Recognition

To determine the characteristics of human lip, left and right corner, upper corner, middle lip corner and lower lip corner are extracted from the lip region. The color and shade of lips are also considered. Lip Biometric system is applicable when other facial organs are covered, lip biometric plays a very significant role.

c. Fingerprint

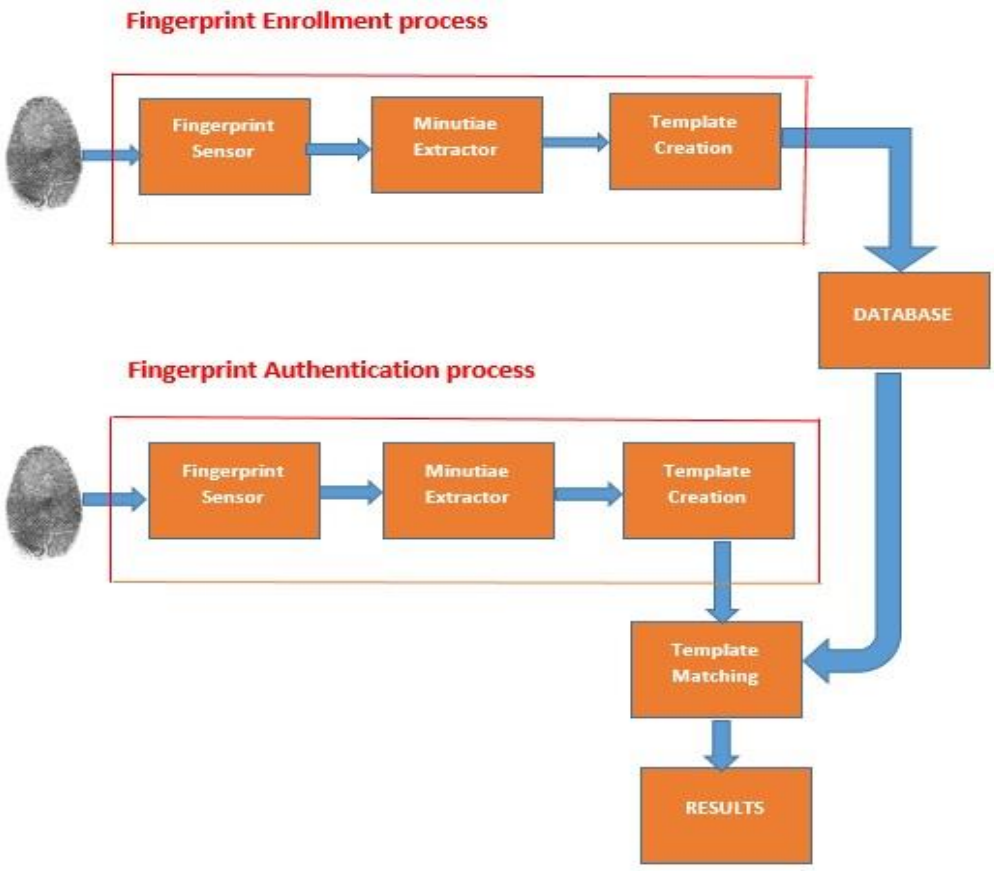

Figure: 4-1. Fingerprint Enrollment Process.

The orderliness of ridges and valleys on the periphery of a fingertip which is formed during the first seven months of fetal development is called a fingerprint. It has been analytically proven that the fingerprints of identical twins are unique and so are the prints on each finger of the same person. The minimal cost required for recording and determining fingerprint have made it more affordable to be used in many securities related applications. Figure 4-1, shows the fingerprint enrollment and fingerprint authentication process.

4.3.2. Geometry

a. Iris

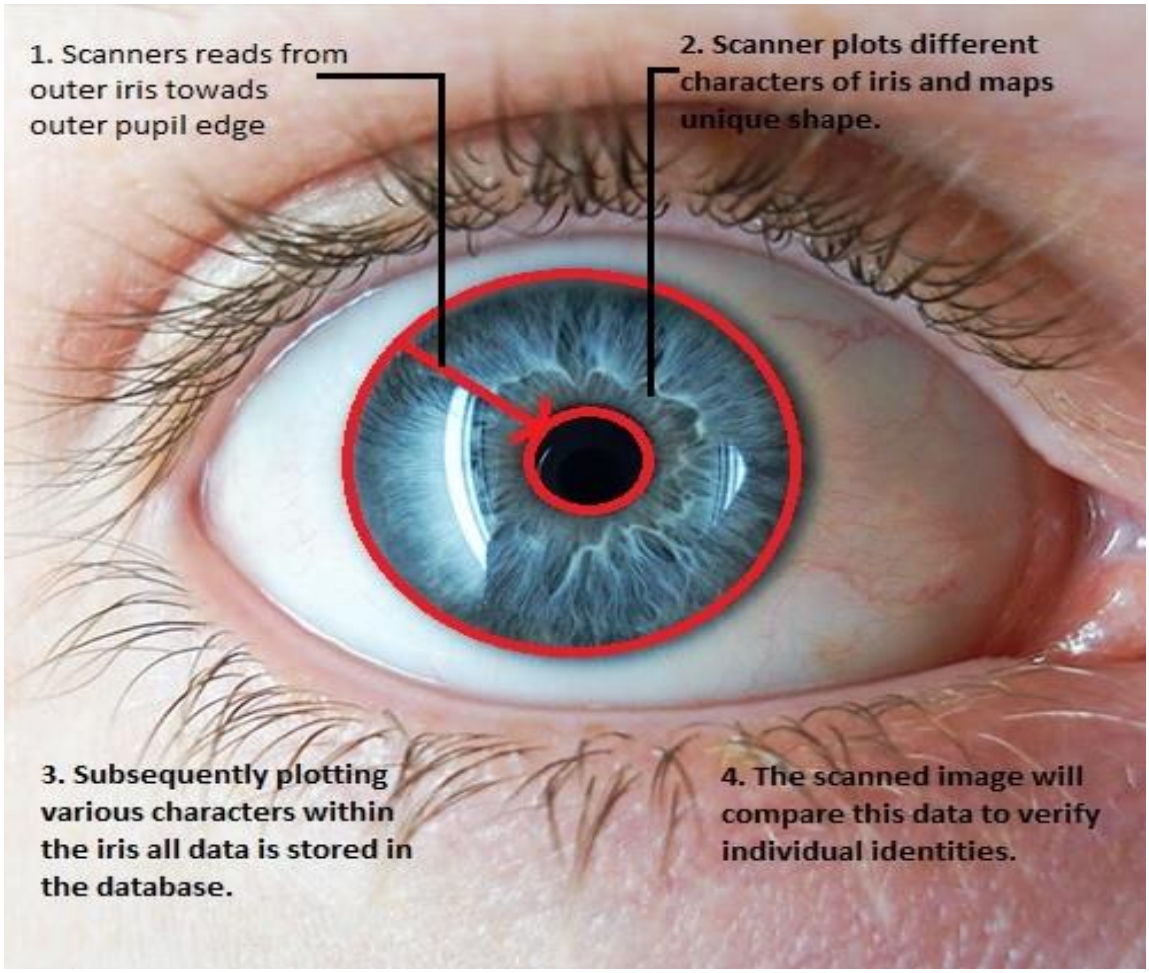

Figure: 4-2. Process for Iris Scan Authentication [30].

The iris lies between cornea and lens of a human eye and consists of number of layers containing Blood vessels, pigment cells and iris muscles. These patterns of iris are formed randomly and are not dependent on genetics factor. These unique characteristics of iris that remains stable throughout the adult life is used as a biometric technique to identify a person. Figure 4-2, shows the steps in which iris of a human eye is scanned, converted into iris code that is stored in the database and which is later on compared with the received iris for authentication.

b. Retina

The unique patterns of blood vessels within a person's retina is mapped in the retinal scan technology. The light is more readily absorbed by the blood vessels within the retina than the neighboring tissue and are effortlessly recognized with suitable lighting. The precise pattern of blood vessels in the retina is not determined by the genetic factors which allows retinal scan technology to even differentiate between identical twins and provide robust identification [31].

c. Vascular Patterns

Each human being have a unique structure of veins throughout their body which is known as vascular patterns. In biometric systems, the veins pattern from person's face or hand are considered. It is believed that the thickness and location of these veins are unique enough to verify a person's identity.

d. Facial

Everyone has a different facial structure depending on the location and shape of facial peculiarity, such as the eyes, eyebrows, nose, lips, and chin and their spatial

relationships. The overall facial image is recorded and then digitized per the various facial attributes.

4.3.3. Behavioral

a. Signature

The way a person signs his name includes several dynamics such as pressure applied on pen while signing, direction of writing and writing speed of persons. As it is a behavioral biometric it is influenced by physical and emotional condition of the person signing and can also change over a period. In recent times, it is not being used as the signatures can be forged to fool the verification system.

b. Typing:

This biometric allows verification of an individual's identity over a session after the person the person is verified using biometrics such as fingerprint or other techniques. Everyone uses the keyboard in a specific way to type in the information. It depends on the typing speed, typing pattern and other factors which can be unique for an individual.

c. Voice Recognition:

Voice biometrics is characterized by the vocal tract which is made up of the oral and nasal air passages. This depends on the movement of the mouth, jaw, tongue, pharynx and larynx to articulate and control speech production. The person should speak in his normal voice that was used to store a sample of his voice in database as the voice is subject to change with the period of time and health and emotional state of the person.

d. Gait:

Gait refers to the style in which a person walks. However, the gait of an individual is determined with several factors such as nature of clothes user is wearing, type of footwear, walking surface, etc.

Chapter 5

Car Computing System

5.1. Controller Area Networks

CAN is a two-wire, serial, half-duplex, high-speed communication network. The transmission takes place by serially transmitting the data bits at a bit rate of up to 1000 kbps on a bus. In CAN only one node gets to communicate on the bus at a time hence it is known as a half-duplex network.

Robert Bosch developed CAN network in 1986 for the automotive industry to fulfill the communication requirements between multiple ECUs in a vehicle. Since point-to-point communication was restrictive, a multi-master communication system was developed. In 1987 Intel corporation fabricated the first CAN chip. Depending on the physical length of CAN network, the CAN bus can have the speeds of 10kbits/s to 1Mbits/s. For example, a CAN network of 1 Mbits/s should not have a bus length of more than 40m.

5.1.1. CAN Basics

CAN network work on CSMA/CD+AMP (Carrier Sense Multiple Access/ Collision Detection with Arbitration on Message Priority) technologies. This means that a CAN node always checks if the bus is busy before it tries to access the bus [32]. This makes sure that the nodes do not try to access the bus while another node is using the bus

to transmit the message, which avoids corruption of the messages transmitted by both the nodes. If the two nodes access the bus simultaneously it is called as a collision.

5.1.2. CAN Identifier

Each CAN message is transmitted along with a message identifier called CAN identifier (CAN ID) and thus the CAN network does not communicate primarily based on device physical addresses. Based on the identifier of the CAN message received by each node on the network, the node decides whether to keep the message or discard it.

5.1.3. Arbitration

When a collision occurs on a CAN network the arbitration mechanism comes into play and decides which node gets to transmit first. A node having lower CAN identifier gets the first preference to send the message in case of a collision. Two nodes wait until the bus is idle and then start transmitting their CAN ID bits on the network. Each node continuously keeps on listening to the bus activity, hence each node knows when a collision is happening but they continue transmitting the CAN ID bits if both are transmitting the same kind of bits. Since all CAN IDs need to be unique, a dissimilar bit transmission happens at some point, the node which transmits ‘0' or a dominant bit wins the arbitration and gets to transmit the rest of the message while the other node should stop transmitting and wait for an idle bus. This technology is called CD+AMP (collision detection and arbitration on message priority).

5.1.4. Frame Types

CAN message transfer is done based on 4 different frames.

1. Data Frame:

Data frame is responsible for carrying the data from transmitter to receiver.

2. Remote Frame:

A remote frame is used by remote node to request another node to send a message.

3. Error Frame:

Error frame is used to notify all the nodes that an error has occurred in transmission.

4. Overload Frame:

Overload frame is used to provide a delay between successive Data or Remote frames.

The CAN network is governed by the ISO standards ISO-11898 for high-speed up to 1Mbps and ISO-11519 for low-speed up to 125kbps. The CAN network communication is also classified based on the number of identifiers a CAN message uses as Standard CAN (V 2.0A) which uses 11-bit identifiers and the Extended CAN (V 2.0B) which uses 29-bit identifiers.

The two CAN networks also differ per the identifier positions in a CAN message and their structure of message frames. Ideally, the CAN V2.0A can have 2032 unique IDs.

5.1.5. CAN 2.0A Protocol and Each Section of the CAN Message

1. Start of Frame:

Beginning of a data frame is known as Start of Frame, it is 1 bit long and is always a dominant bit or ‘0' digital level.

2. Arbitration Field:

It consists of the CAN ID which is 11bits long and the Remote Transmission Request bit (RTR) which is 1one bit long and in a data frame it must be dominant or ‘0'.

3. Control Field:

It is of total 6 bits which carry Data Length Code (DLC – 4bits) and two bits are reserved for future expansion. The DLC is used to specify the number of bits in the data field.

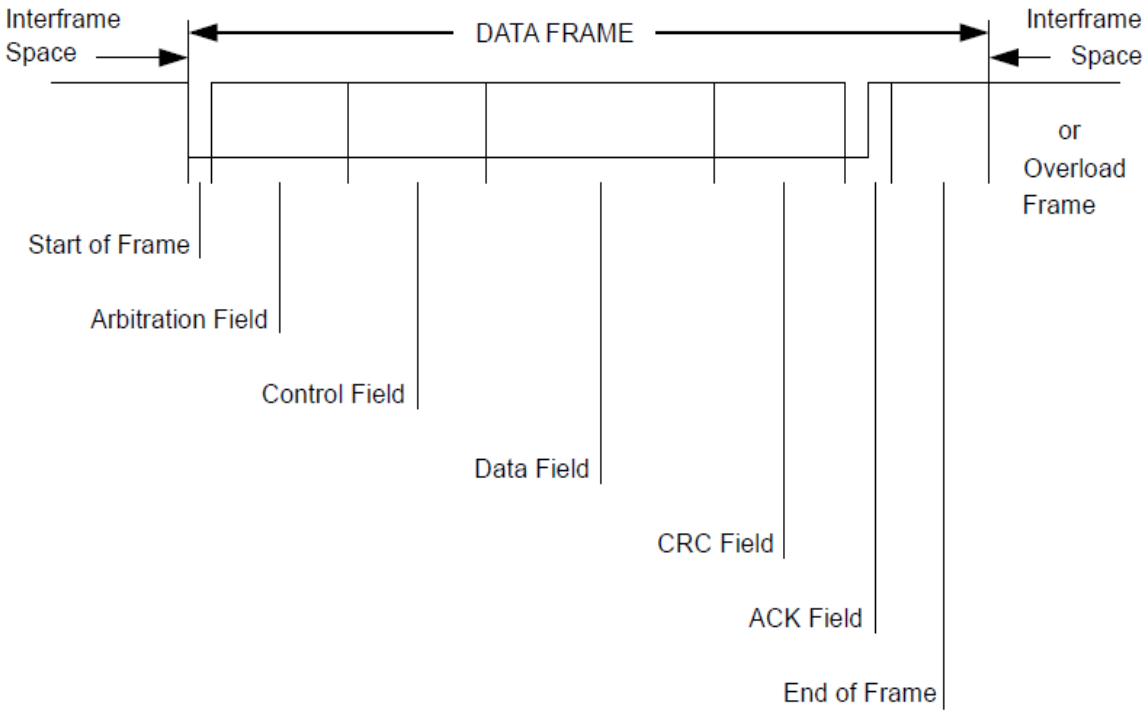

Fig: 5-1. CAN Message Data Frame [33].

4. Data Field:

It is mostly 1 to 8 bytes or 8 to 64 bits long. This field is responsible for carrying the information from one node to another. The information carried by this field is also called as payload.

5. CRC Field:

Cyclic Redundancy Check (CRC) field which is 16 bits long including the delimiter bit is used to carry an error detection mechanism.

6. Acknowledgment Field:

This field consists of two bits. The first bit is transmitted by the transmitter as a recessive bit which confirms the successful reception of the message by the nodes. It is another

form of error detection and reporting scheme. If even one node detects an error and conveys it in the acknowledgment field, all the nodes discard the message and the transmitter retransmits the message. The other bit is a delimiter bit.

7. End of Frame Field:

The field is seven bits long. The end of frame field is followed by a 3-bit inter-frame space after which the bus is idle.

Chapter 6

Over The Air (OTA) Method

6.1. Proposed OTA Software Update:

Figure 6-1 shows the flow of the proposed software update process by downloading and installing the software update from the remote OEM server to the corresponding ECU in the vehicle. Initially, we will create the checksum from the software package along with the OEM's signature by encrypting the checksum using OEM's private key. Then the software package along with the checksum and the OEM's digital signature will be sent to the OEM remote server. The telematics unit on the car receives the update files from OTA servers through the radio links and then transfers them to Central Gateway. In the normal situation, the central gateway directly transfers the updates to the body control module (BCM) and then to the respective ECUs. The central gateway is connected to the firmware control unit that informs the central gateway when a specific update should be sent to the ECU in case of updating multiple ECUs simultaneously. A database is connected to the central gateway as well as to the iris scan authentication unit. It stores the firmware/software updates securely until they are required to be sent to their corresponding ECUs. Before downloading the software update files, the central gateway also verifies the version of the software by comparing it with the information stored in the database.

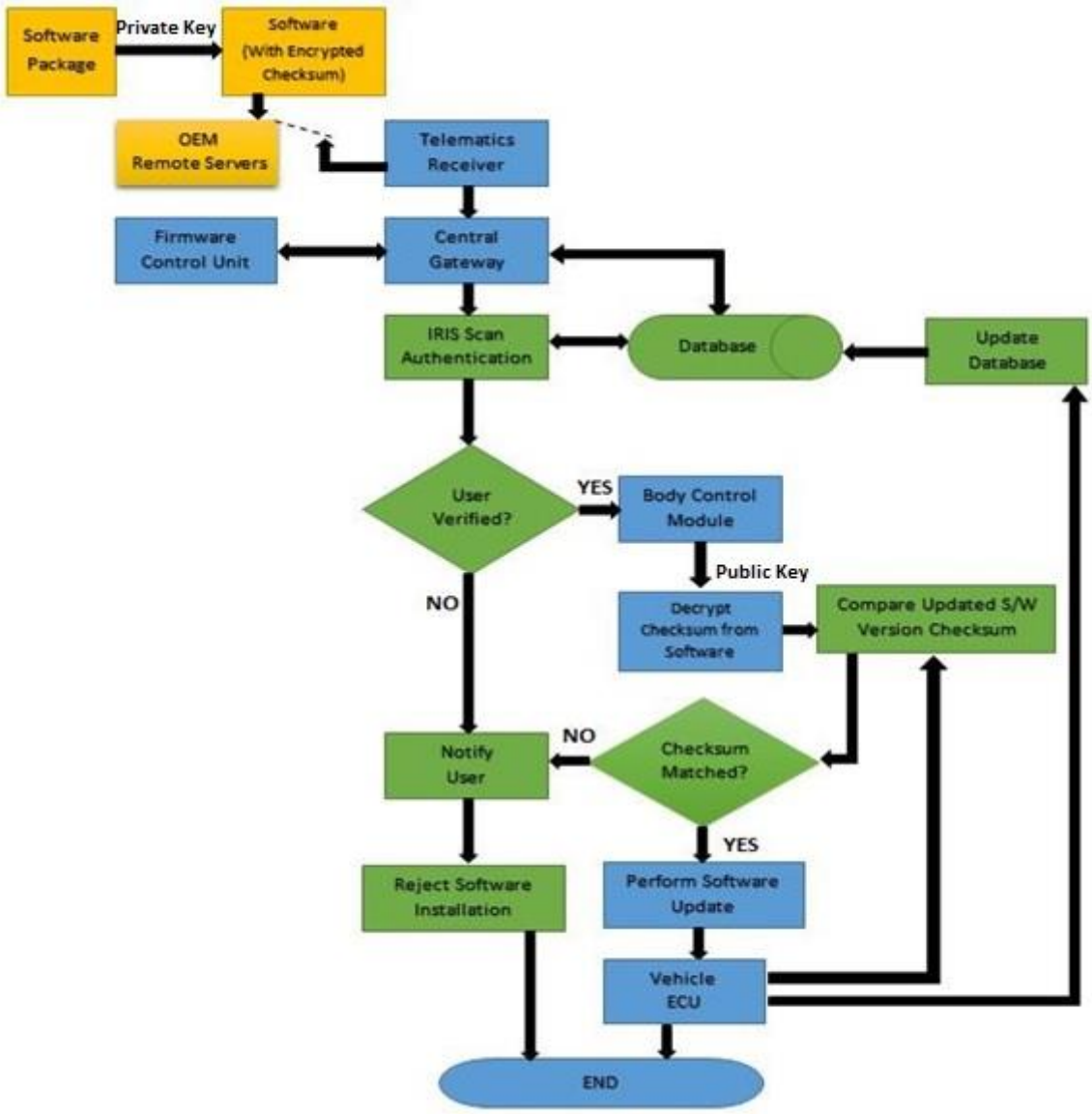

Figure: 6-1. Process of Secure OTA Software Update.

In our proposed method, it is required to go through an additional authentication and verification module before the updates actually arrive at the ECU from central gateway. This authentication module will store car owner's iris scan, which sits between central gateway and body control module. The owner will have the capability to select which updates to install and at what time slots they can be installed to the ECU. In this

case, even if the attacker hacks the central gateway, he/she will not be able to take control of or manipulate the ECU and the sensors connected to them through OTA updates.

If the central gateway receives an update and the owner of the car is not available, the updates will be stored in the database. These stored software/firmware update files would be secured using encryption and authentication protection to avoid any modification. The firmware control unit will hold a table of each ECU containing the information such as the serial number and version of the firmware update received and already installed in the vehicle. Once the owner starts the car it will prompt him/her about the update and with the iris scan camera fitted on the steering wheel he/she can authenticate and give his/her consent, before the BCM receives the updates.

Before the BCM sends the software update files to ECU for installation, it will verify whether the software package is legitimate by checking the attached digital signature. After that, the vehicle ECU will compare the checksum value of the updated version with the version of the software that was previously installed in the car. If the checksum values are not equal, the user will be notified an error condition and then the installation will be terminated. Otherwise, the software update process continues and if the newly triggered software update installs successfully, the ECU approves the updated software version.

After the above steps, the ECU will set the newly installed software update as active, and the formerly active storage memory back to the inactive status. It also conveys the same information to the database to populate it with the information of the latest version of the software. After this, the whole software update procedure ends.

6.2. Iris based Authentication Implementation

Figure: 6-2. Procedure to Detect and Authenticate IRIS [34].

In our proposed approach, the security of the OTA software update process will depend on the iris authentication of the car owner. As soon as a person enters the vehicle, the CCD digital camera scanning the iris will get activated immediately and then will use both visible and near-infrared light to take a clear, high-contrast picture of that person's iris.

As shown in Figure 6-2, either the person looks into an iris scanner, or the camera focuses automatically, a mirror or audible feedback from the system are also used to determine that person’s position accurately. An individual’s eye should be approximately 4-12 inches away from the camera to obtain the clear image from the iris, the camera then

clicks a picture of the subject, and the computing system locates the center of the pupil, edge of the pupil, edge of the iris, eyelids, and eyelashes [35]. A computing system then removes the eyelids and eyelashes from the image and analyzes only the patterns of iris. The core iris pattern will then be encoded compared with the already scanned iris data stored in the database [36] that is connected to the central gateway and iris authentication unit. If the code matches with the iris of the person sitting in the driver's seat with any of the code from the database, it will activate the required system and then proceed to software updates installation over the air.

6.3. Decision Making in Iris:

The decision making process begins with a user recording his biometric data (iris information) in a biometric system. This biometric data is converted into a template (registration template) and stored in the database for progressive comparison. This filtered and enhanced iris images are small files known as 'iris codes'. During authentication the user provides his biometric (iris) data again through the iris scanner fitted on the steering wheel of the car and another 'iris code is generated. Let's call this iris code as the verification template. Once both the iris codes are recorded, the mathematical difference between the iris codes called as Hamming distance is computed [37].

The decision made by this mathematical calculation have four outcomes

1. Correct Accept (CA) - Rate of Accepting Authentics
2. False Accept (FA) - Rate of Accepting Imposters
3. Correct Reject (CR) – Rate of Rejecting Imposters
4. False Reject (FR) – Rate of Rejecting Authentics

The first and third outcomes are the ones required while the second and fourth outcomes are the errors. Figure 6-3, illustrates the idea of decision making in a biometric recognition structure. The two distributions represent authentic and impostor statuses which are improperly distributed. The metric of similarity and dissimilarity is the abscissa which in this case is the hamming distance. The pattern of two distributions in this case is perfectly separated by 0.4 hamming distance criterion [38].

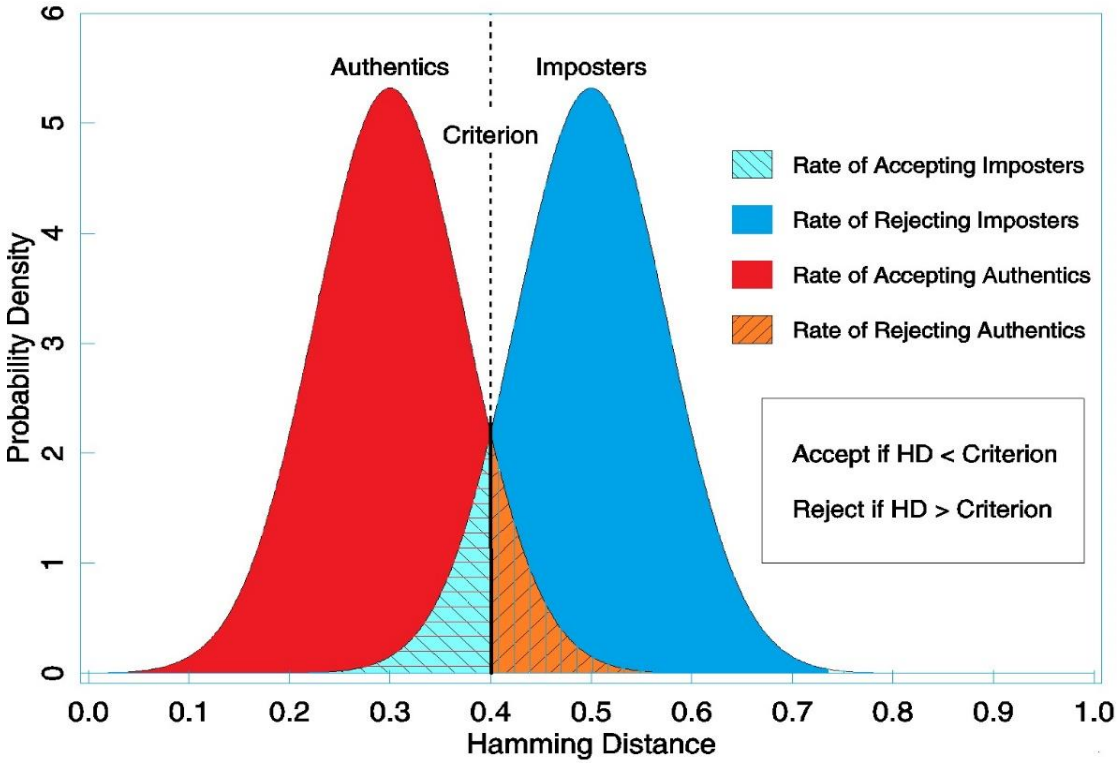

Figure: 6-3. Statistical Decision Theory [38].

In this case if the hamming distance is less than the criterion i.e. 0.4 hamming distance than the outcome will be considered as authentic and the decision will be accepted. If the hamming distance is more than the criterion i.e. 0.4 hamming distance than the outcome will be considered as Impostors and the decision will be rejected.

The figure 6-4, shows the decision made under ideal condition when iris images are captured in the laboratory using the same camera from a fixed distance, with a fixed zoom under fixed illumination. In this case the hamming distance achieved by more than half of this image comparisons were 0.0 and the average hamming distance obtained was 0.019.

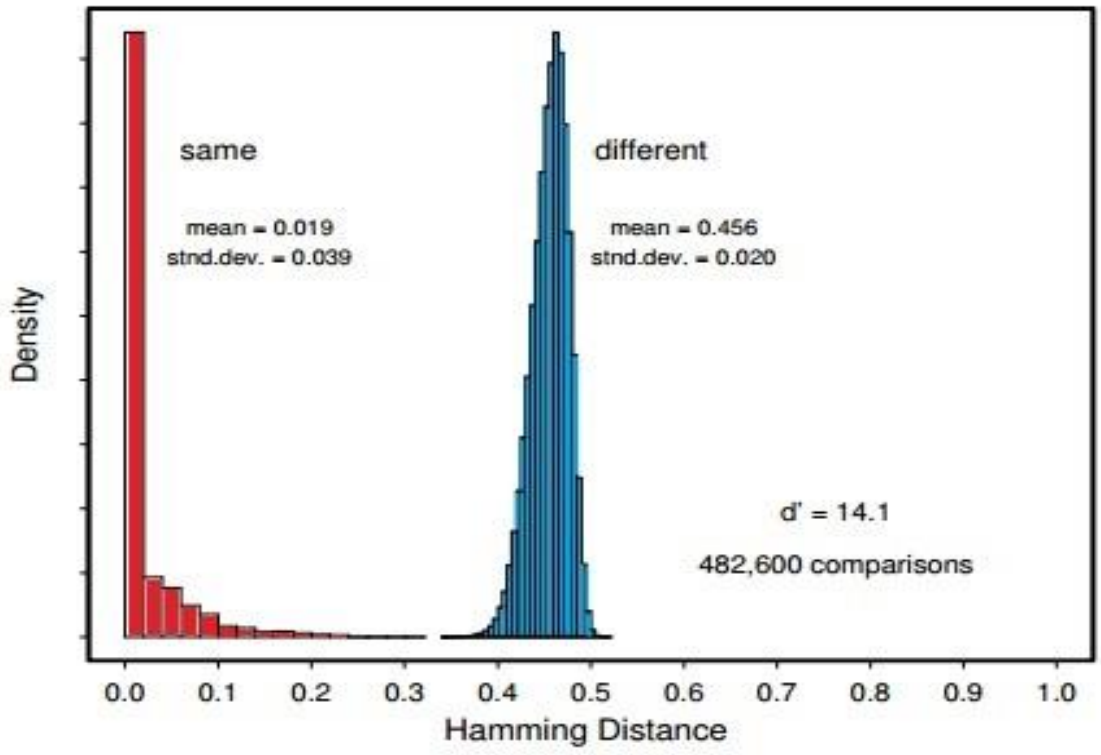

Figure: 6-4. Decision Environment in Ideal Condition [39].

This shows that the distribution of authentics for iris recognition depends intensely on the image acquirement techniques and conditions. However, the distribution of imposters is comparatively independent of the image acquiring techniques and environment.

The decision making in biometrics is measured using the “decidability index” d′.

$$d' = |\mu 1 - \mu 2| / (D12 – D22)1/2/2$$

Where, μ1 and μ2 are the means of authentics and imposters distribution respectively and D1 and D2 are the standard deviations of these two distributions. This decidability factor can be used to calibrate the performance of the iris scanning system.

Figure 6-5, shows decision environment in non-ideal conditions when images of the iris are acquired with different optical conditions and variable surroundings.

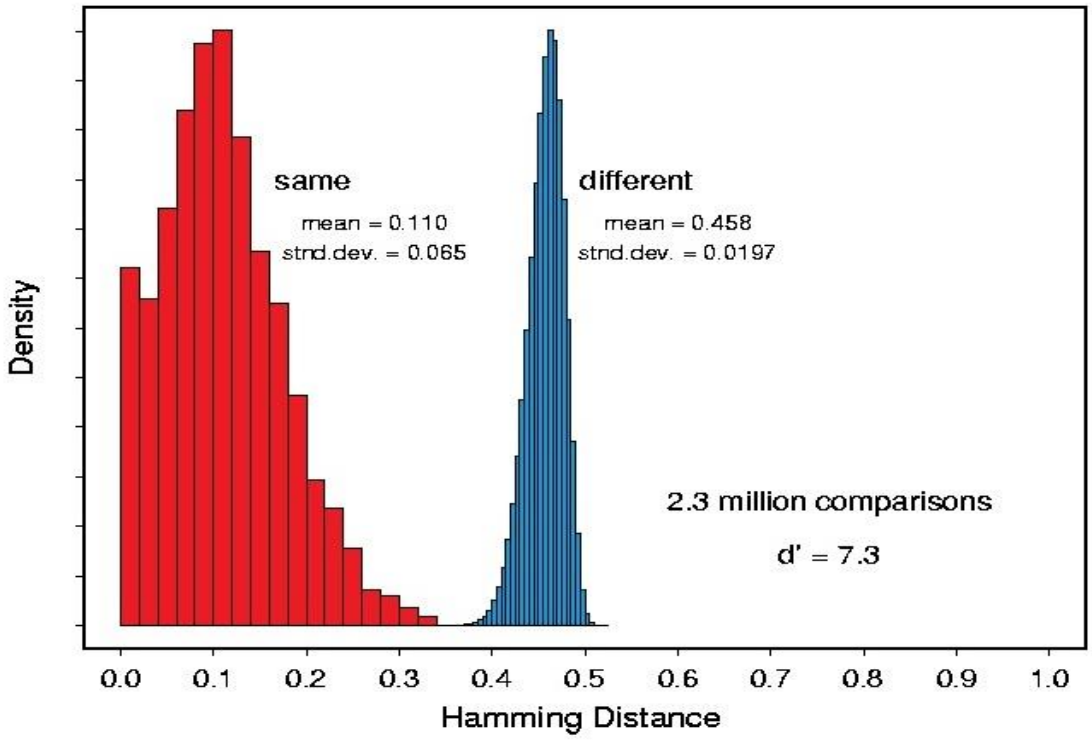

Figure: 6-5. Decision Environment in Non-Ideal Condition [39].

Figure 6-4 and figure 6-5 have almost the same right hand side distribution i.e. the distribution of imposters. But as the authentics distribution depends strongly on the method on which image of the iris is captured, there is a huge variation of the authentics distribution for the decision environment graph in non – ideal condition.

Iridologists' claims that there is a possibility of change in iris pattern due to change in health conditions or because of some disease. But long back in 1979 Simon et al [40] and in 1985 Berggren [41] discredited their claims with the help of their research studies.

6.4. Checksum Comparison Implementation:

Automotive service tool is a programming tool that provides abilities to analyze, repair, debug or monitor a system or product. The type of service tool varies with different manufacturers. A few examples of automotive service tools are CANOE and CanAnalyzer. Service tool is connected to ECU with the help of two buses namely CAN High bus and CAN Low bus.

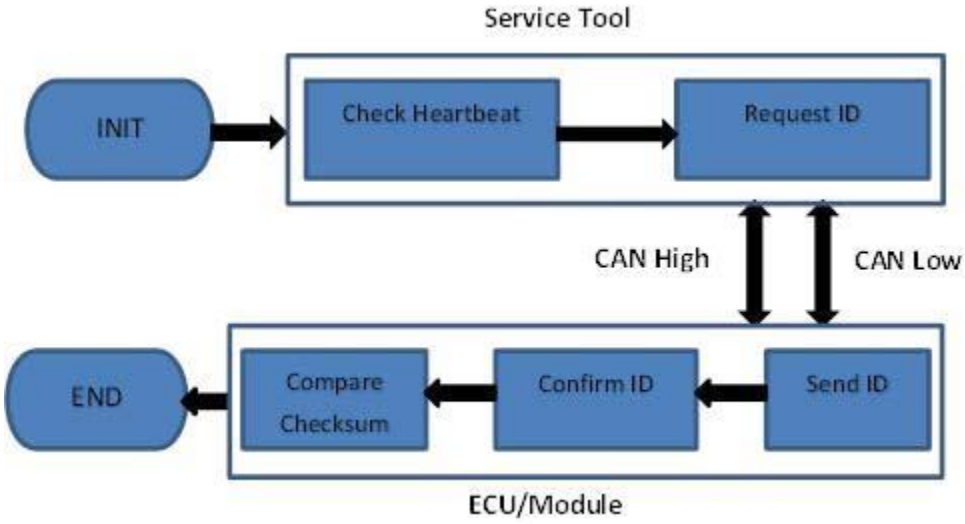

Figure: 6-6. Checksum Comparison Mechanism.

As shown in Fig. 6-6, every module continuously sends heart beat messages to other modules in order to check whether any other module is live at the given time. Each node of the module has its own unique source address. With the use of the source addresses, the module can send out the heart beat messages globally to other modules.

At the communication initiation phase, the service tool requests the module to send its ID. After receiving the module ID, the service tool compares the received ID to see if it matches with the ID present in the service tool database. Now as the communication is established, the service tool requests the specific module to enter the

programming mode. The module processes the request and sends the acknowledgement to enter the programming mode.

Once the service tool receives a positive acknowledgement signal from the module, it requests the controller to enter the programming mode. This is the time when the checksum of the available update or firmware is calculated. The module needs to calculate the checksum of every program to be installed. This calculated checksum is then compared with the OEM's checksum value which is stored in the CAN database.

If both the checksums are the same, the flashing of the program updates will begin until the successful installation of the available update or firmware. On the other hand, if the third party is trying to install a program into the module with its checksum not matching with OEM's checksum, it will inform the module to abort the installation process and throw an error and/or a warning message.

Chapter 7

Experimental Results

7.1. Security Implementation using Iris Scanning System

The method proposed in this thesis states that the car cannot run until and unless the iris scanner fitted on the steering wheel give its approval. There are 2 conditions which are originally required for the iris scanner to give its approval. First the park break should not be set and the second condition is that the ignition is turned ON. Once the driver removes the parking breaks (park break not set) and turns ON the ignition of the car the iris scanner will scan the respective driver's iris and compare it with the iris code stored in the data base. If the iris scanner sends out an acknowledgement bit confirming that the driver's iris matches with ones stored in our database, then only the car will be able to gain the desired speed. We explain our hypothesis with the help of graphs in different conditions. We will take 4 parameters to explain these scenarios.

7.1.1. Condition 1: Initial State of the Car

As shown in figure 7-1, initially the parking brake is not set and the ignition key is turned on throughout the time of our observation. This activates the iris scanner and it starts scanning driver's iris to verify whether the driver is an authorized driver to drive the particular vehicle. At this moment, if the iris of the driver matches with the iris code

in the database, the iris approval system sends out an acknowledgement signal confirming the same and keeps the system ON till the same driver is in the driver's seat or the ignition is ON. In the same way if the park brake is set and even if the ignition is turned ON, the iris scanner system will not be activated.

7.1.2. Condition 2: Driving State of the Car

As explained in condition 1, the car is ready to move. Hence in figure 7-2, we can see that the car attains a speed of 50 km/hr. at a time interval of 368th second and maintains the same speed until 440th second when it is gradually increased to 100 km/hr. as shown in figure 7-3. The car functions normally as the park brake is not set, the ignition is on and thus the iris system is gives acknowledgement signal to ignition to be ON.

7.1.3. Condition 3: Iris Does not Match

In this condition, the driver has removed the parking brakes (park brake is not set) and at 552nd second the ignition is turned off. This will deactivate the iris system, making the car to come to a stop, which can be seen in figure 7-4, that the speed becomes zero. Now we will consider that an intruder tries to turn ON the ignition, the iris system gets activated but the scanned iris of the driver doesn't match with the iris codes in the database. In this case, if the intruder tries to change the gear and put his foot on the accelerator as it is shown at time interval of 589th second, the iris system will send a command to the ignition and will ask the ignition to turn OFF. This will make the car to stop after few seconds. This can be seen in the figure 7-4 that at a time interval of 601st second the ignition is turned off and the car speed is brought back to zero at 604th second. The same cycle is repeated at 625th second and 637th second.

7.1.4. Condition 4: Park Brake is Set (ON)

Per figure 7-5, the park brake is set at a time interval of 810th second and the ignition is turned ON at around time interval of 814th second but as it does not satisfy the required conditions for the iris system to be activated, the iris approval system will be set OFF.

At 880th second the parking brake is removed (park brake is unset) and the ignition is still ON, this will satisfy all the essential conditions required by the iris approval system to be activated and start scanning driver's iris. As the iris matches with the iris code in the data base, it sends out a positive acknowledgement that will keep the ignition ON when the driver changes the gear to drive mode and accelerates the car. This can be seen in the figure 7-5, as the car will start moving at around time interval of 890th second and change speeds accordingly at time intervals of 894th and around 898th second.

7.1.5. Condition 5: OTA Upgrade Mode

We have taken Ignition key, Vehicle speed and Park brake as input signals and we get the corresponding iris approval as the output signal. Ignition key and Park brake are digital inputs to the BCM. The value of these signals is transmitted periodically on the CAN bus by the BCM. Generally, these signals are broadcasted every 100ms on the CAN network. In our setup, these signals are simulated using BCM node simulation.

Scenario:

Assume the car is in a parking area with parking brakes ON or is stationary without the parking brakes ON. It shows that irrespective of the status of the parking brakes, the iris module turns ON and will start authenticating the user, provided the Ignition key is ON and Vehicle speed is zero.

The condition represented in Fig. 7-6 is a manual iris approval system. This condition will be specifically used during the OTA software update process. In this state, the driver can activate the iris system manually when the ignition is ON, irrespective of the parking brake status (set or not set). As shown in before, the iris system is set to OTA mode, hence at time point of around 118th second after the ignition is turned ON, the iris system is activated irrespective of the park break is set at 124th second and at 138th second. At 145th second, the iris system matches the iris code from the database with the iris of the driver and sends a positive acknowledgement to OTA system to upgrade the required software. This will ensure that the software can be upgraded only with the car owner's consent. The car owner will be the only one to decide which software to upgrade at what time. This prevents the car from being attacked by an external source and making changes to the car firmware, which can be fatal to the driver.

The driver can utilize this condition even when he/she decides to wait in the car in some parking area with parking break set. This will help the user to keep the ignition turned on which is necessary for the HVAC system to be activated.

7.1.6. Condition 6: Program Installation Using Checksum Comparison

The graphs in Fig. 7-7, 7-8 and 7-9 represent the different states of the software update process. It determines whether the update will be installed successfully.

HVAC_UPDATE signal is a checksum value of the received software up-date.

HVAC_CHKSM signal is a checksum value of the software that is already install in the HVAC ECU.

Iris_Approval signal is a signal received from the iris module.

Ignition signal is a signal received from BCM.

With the above inputs, we get a corresponding output Program_OK signal which can be in one of the four states (Active, Stop, Inactive and Not available). The update can be installed successfully only after satisfying the following two conditions:

1. It receives a positive iris approval.
2. The checksum of the available update or firmware is the same as that of the respective module checksum already stored in the non-volatile memory of the CAN stack.

We will demonstrate the process by using an example of updating the HVAC module in the following three different conditions.

7.1.6.1. Condition 6 A: Idle Mode

Scenario:

When an unauthorized user turns ON ignition, even though the iris module is ON, the iris approval will fail, as it will not match with iris data from the database. This will ensure that an unknown person cannot install any update in the vehicle.

As shown in Fig. 7-7, the ignition key is set ON at the time of around 7916^{th} second. The checksum of the available HVAC update is determined to be 1443, and it is the same as the one stored in the database and represented by HVAC_CHKSM. In this scenario, the iris approval bit is off through the experiment as the driver is not in front of the iris scanner or an unauthorized individual's iris is scanned. The graph shows that the download process has not started yet and hence the Program_OK bit is in inactive status. However, as the ignition is set ON, the system tries to download the update automatically after a few seconds. In this condition, even if the firmware tries to download the update it will not let the system install the update and the Program_OK bit will change into the

Stop status as it happens at 7931st second as shown in Fig. 7-7. This indicates that the firmware installation is unsuccessful irrespective of having the same checksum value. This will prevent installation of unauthorized applications or firmware to your vehicle by an unauthorized user.

7.1.6.2. Condition 6 B: Iris Enabled Stop to Active Mode

Scenario:

The authorized driver turns ON the ignition key, the car is stationary and connected to the Internet. This activates the iris module and then the iris of the driver will be scanned and then compared with the iris data stored in the database. As the scanned iris is from an authorized person, it moves on to checksum comparison module. In addition, the received update is genuine and from the trusted OEM, the check-sum will match with the checksum of the software already installed in the car. Hence, the update will be installed successfully.

The graph in Fig. 7-8 shows that the ignition key is set ON throughout the experiment. As the ignition is set ON, the update is downloaded and ready to be installed but it is waiting for the iris approval, hence the Program_OK bit is still in the Stop status. In this scenario, the iris approval bit is set to ON status at the 7991st second as the scanned iris matches with the iris data originally stored in the database. Now the system will compare the checksum of the available update with the respective HVAC checksum stored in the system. As the checksum of the HVAC_update available is the same as the HVAC_CHKSM that is sent by the ECU i.e. 1443, the Program_OK bit transforms from Stop status to Active status at the 8022nd second. This helps to complete the installation of the required update without any error.

Assumption: We have assumed both HVAC_update and HVAC_CHKSM value as ‘1443’ for experimental purpose.

7.1.7.3. Condition 6 C: Iris Enabled Inactive to Active Mode

Scenario:

The driver is already driving the car and then receives a message of available software update. The software will not be downloaded at this moment, as the car is moving. As the driver stops the car and connects to the Internet, the software update will be downloaded. As the authorized driver is driving and the update available is genuine, both the conditions are satisfied and hence the update is successfully installed in the car.

The ignition bit is set ON at 8154^{th} second as shown in Fig. 7-9. In this graph, it shows that the Program_OK bit is in Inactive status at the initial stage. This means the system has not downloaded the update yet but it is available for downloading. At around 8186^{th} second, the iris approval bit is set high. At this time, the system starts downloading the update and compares the checksum of the update file with the respective module (for example, the HVAC module) checksum already stored in the system. Once it authorizes that both the checksums are the same, the Program_OK bit will transform directly to the Active state and will enable the system to install the update successfully.

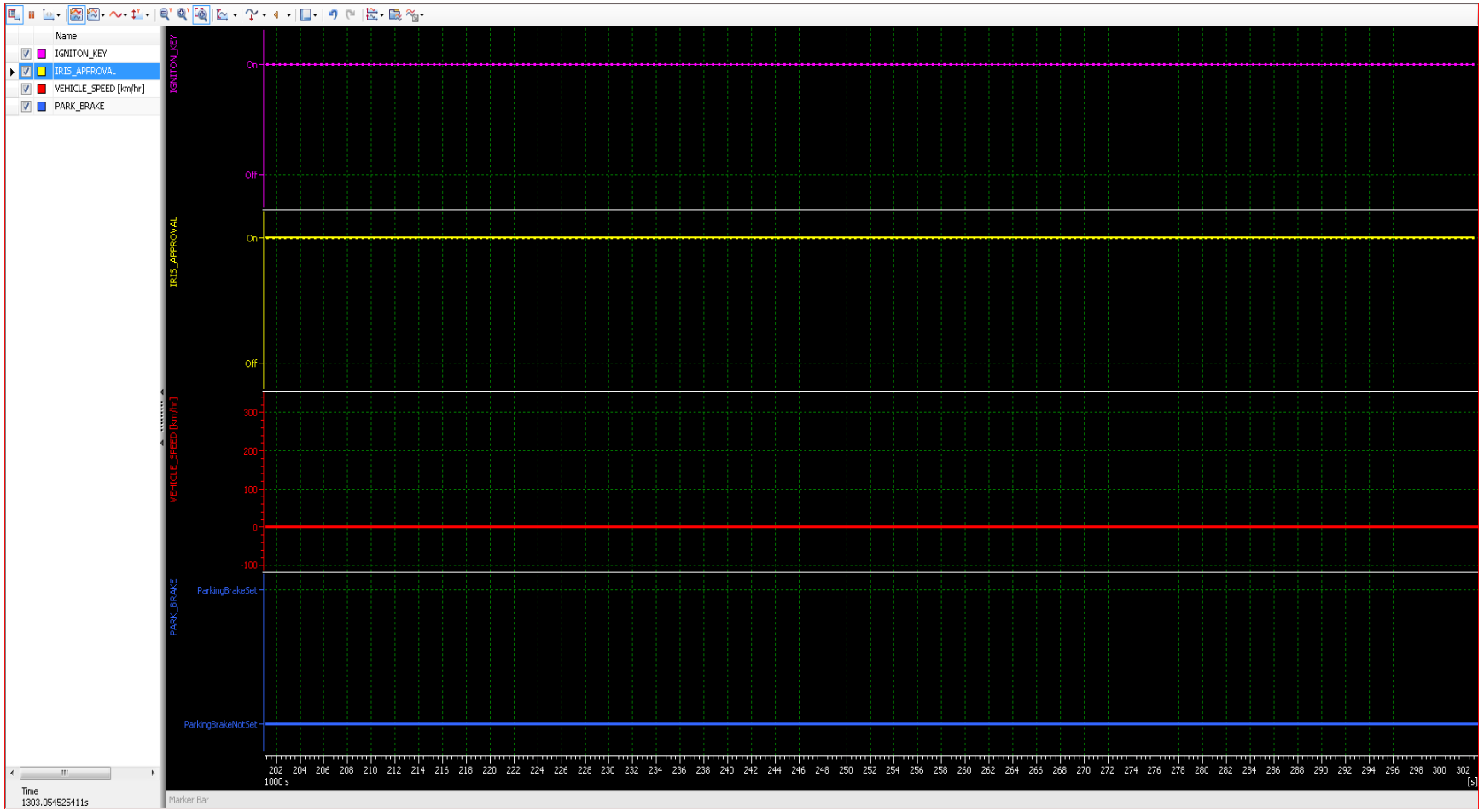

Figure: 7-1. Initial State of the Car.

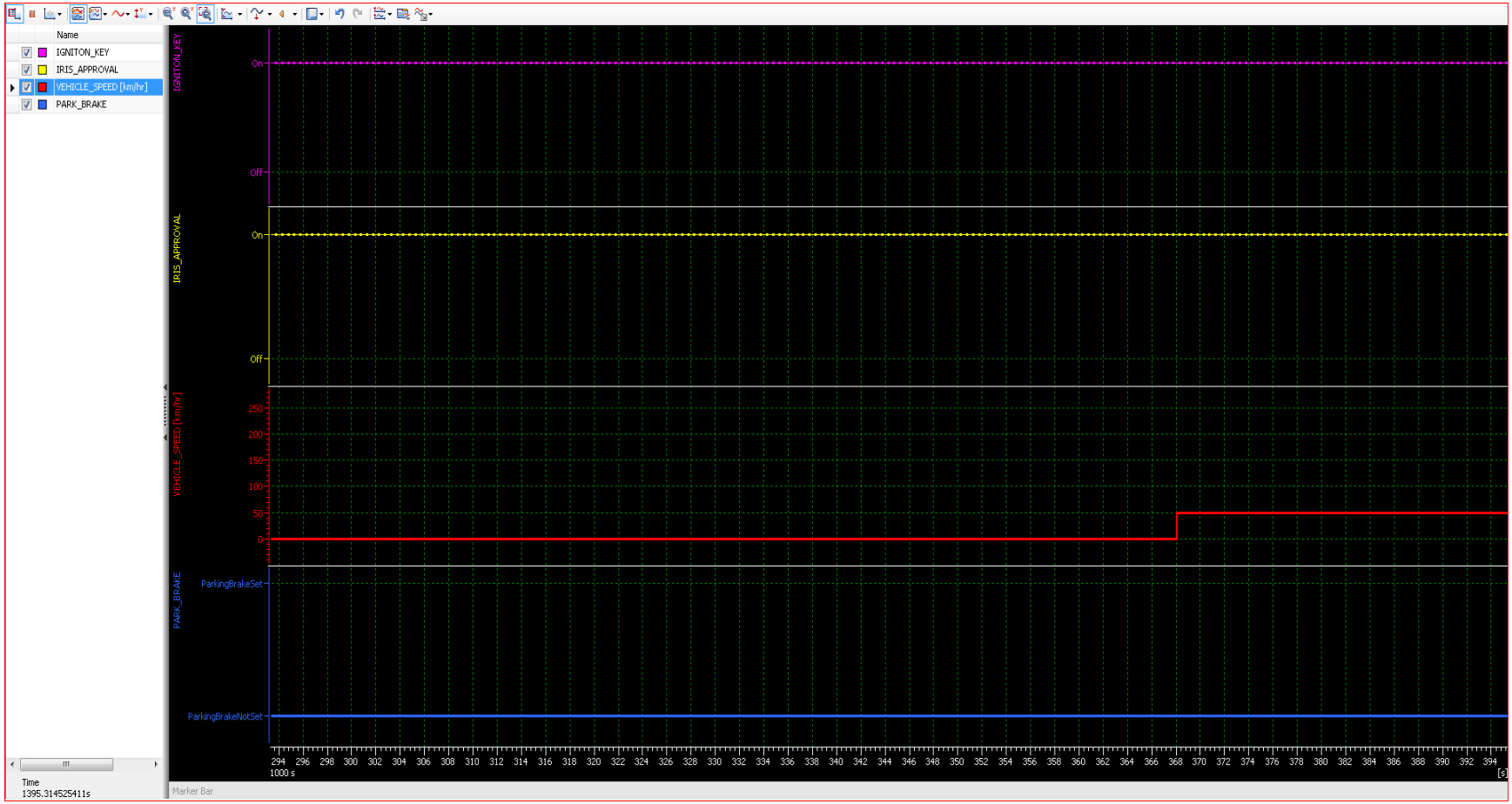

Figure: 7-2. Driving State of the Car (1).

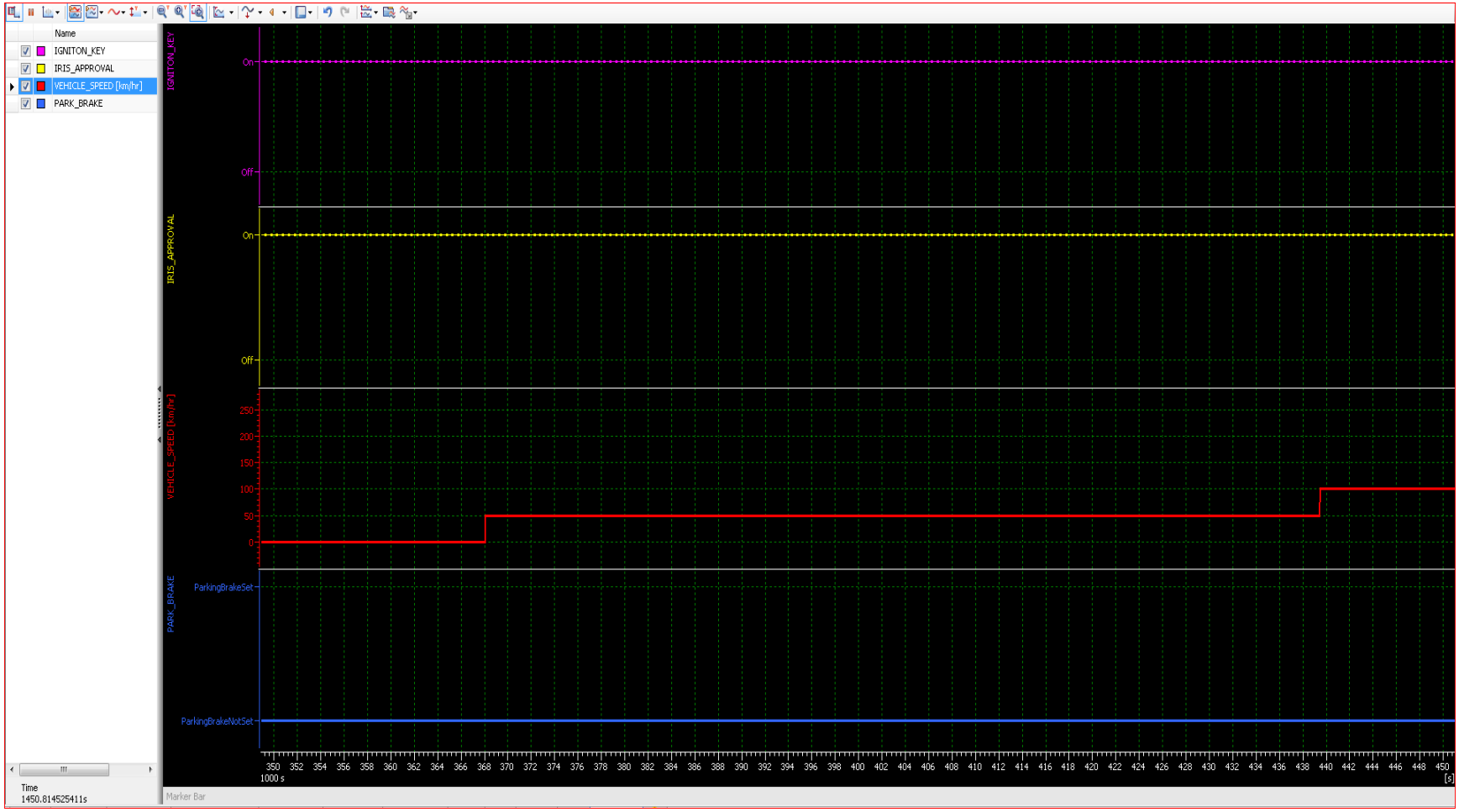

Figure: 7-3. Driving State of the Car (2).

Figure: 7-4. State of Iris Does not Match.

Figure: 7-5. State in which Park Brake is Set.

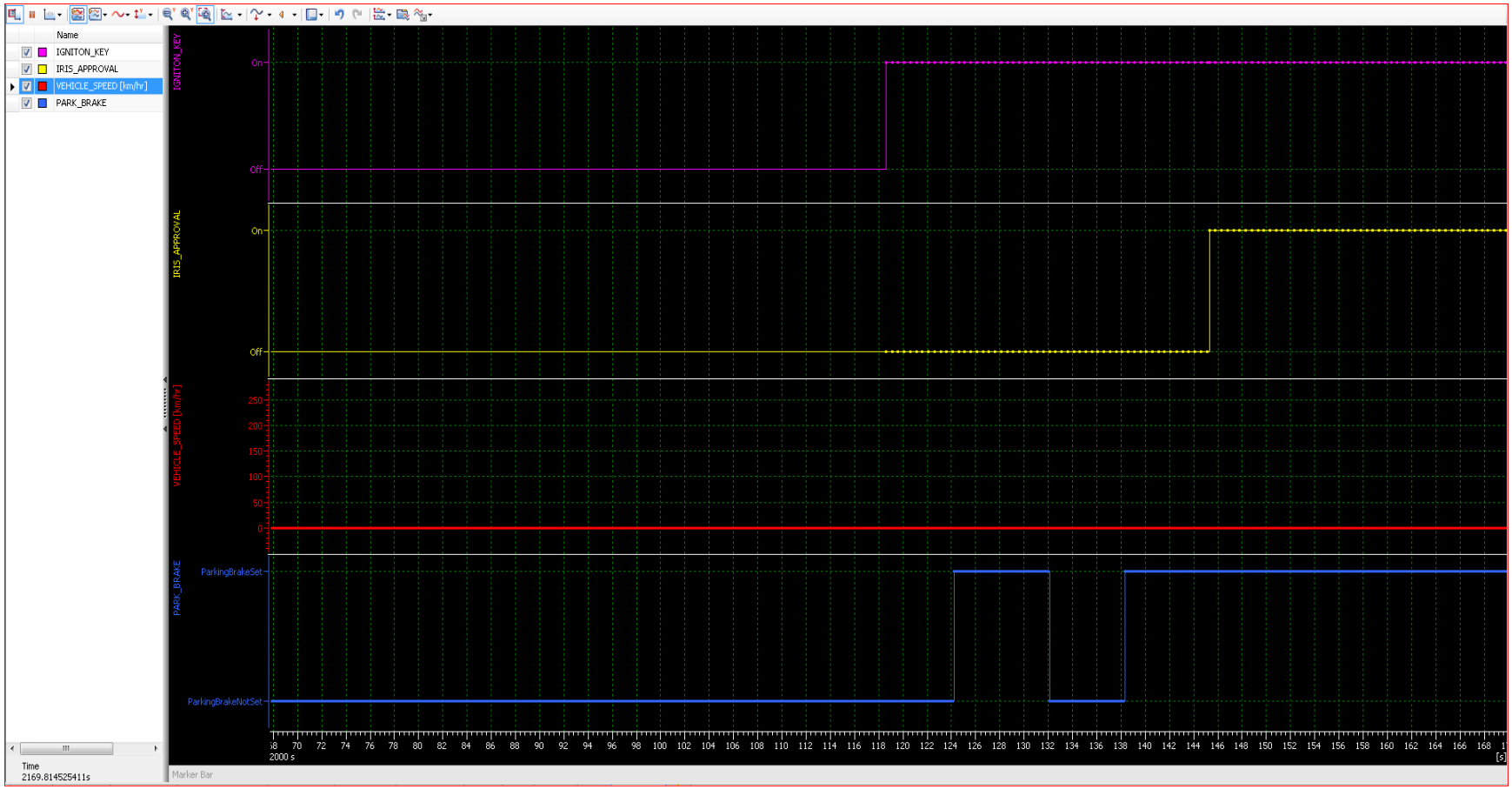

Figure: 7-6. OTA Upgrade Mode.

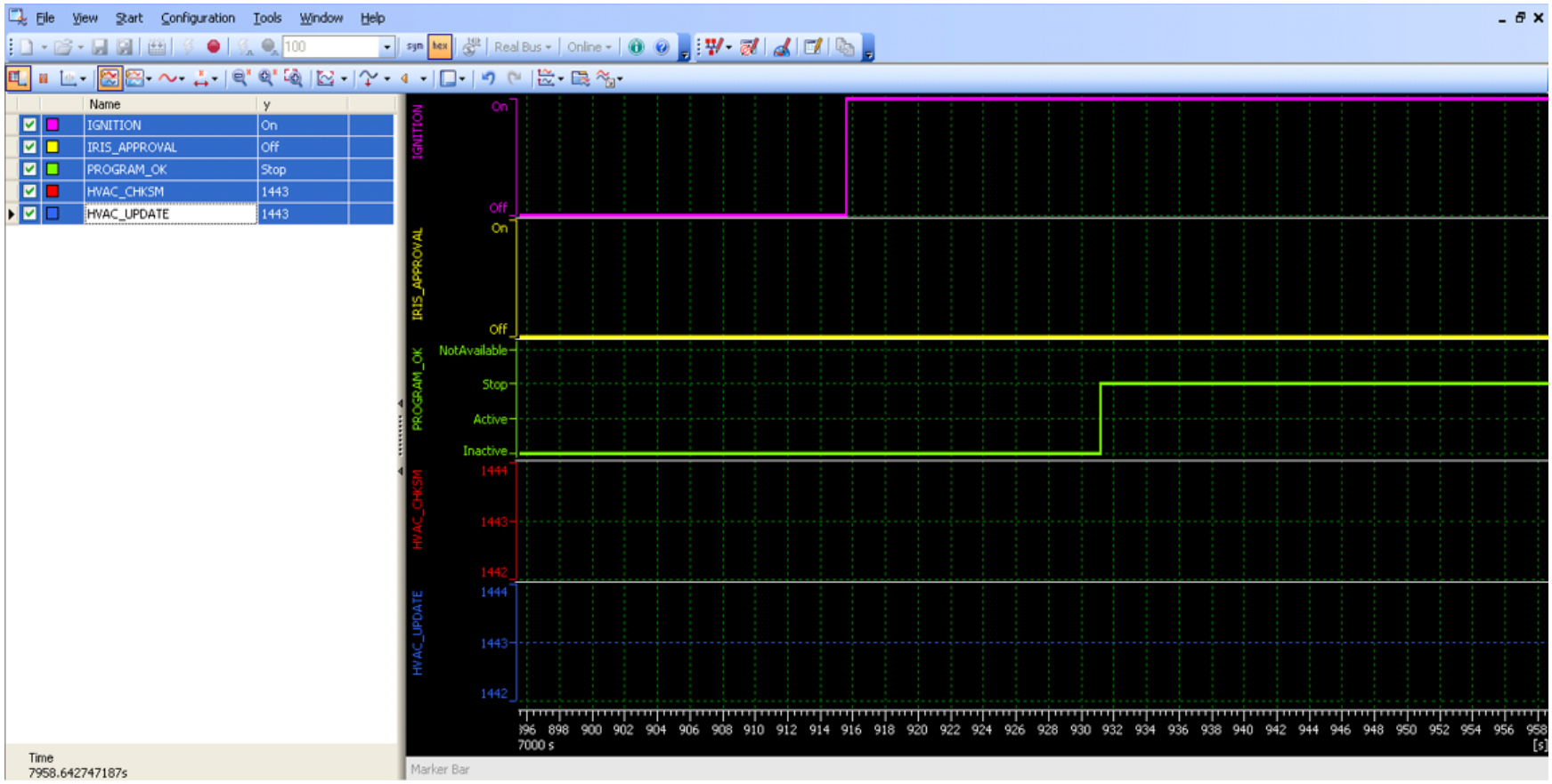

Fig. 7-7. Idle Mode.

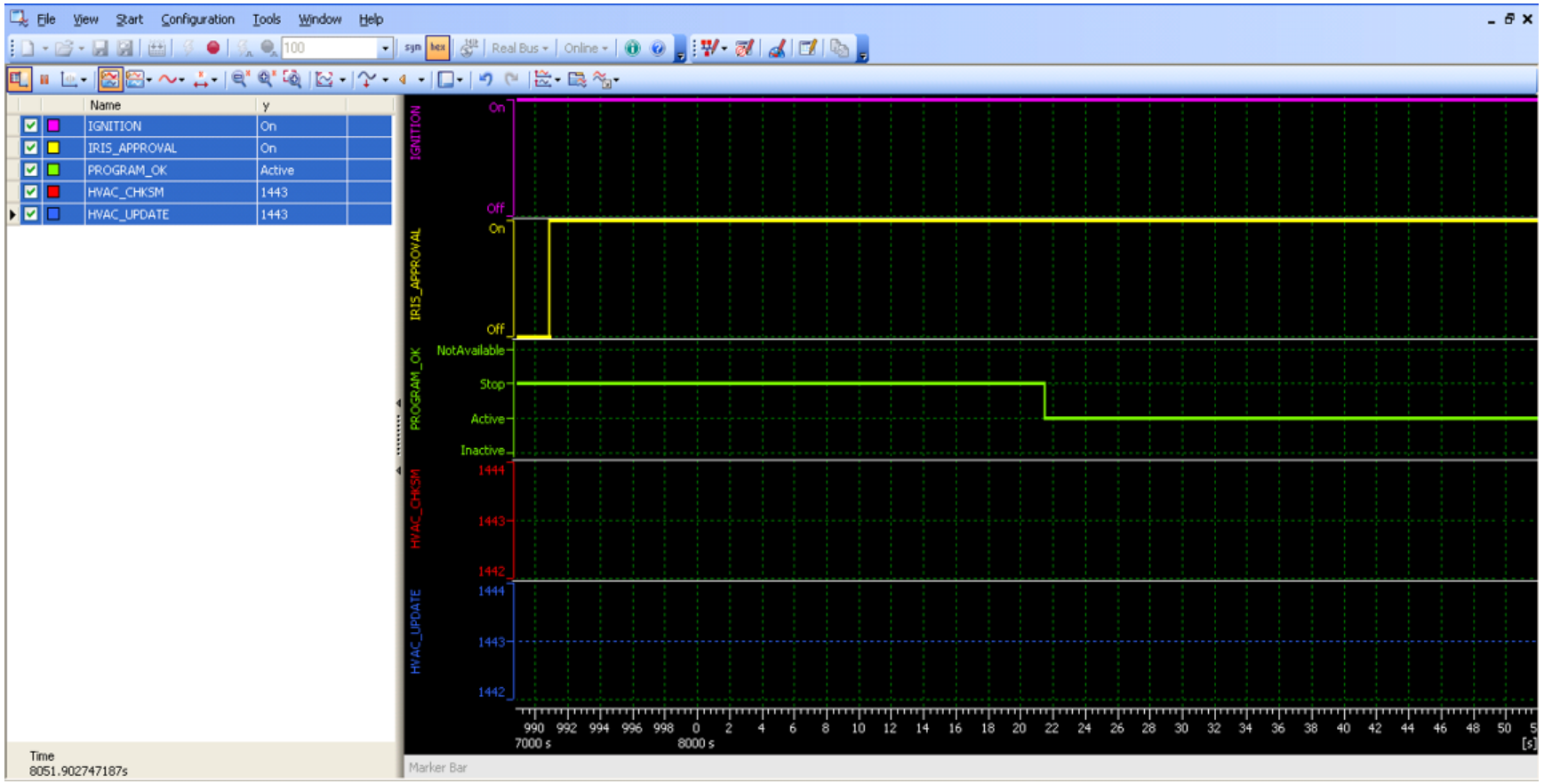

Fig. 7-8. Iris Enabled Stop to Active Mode.

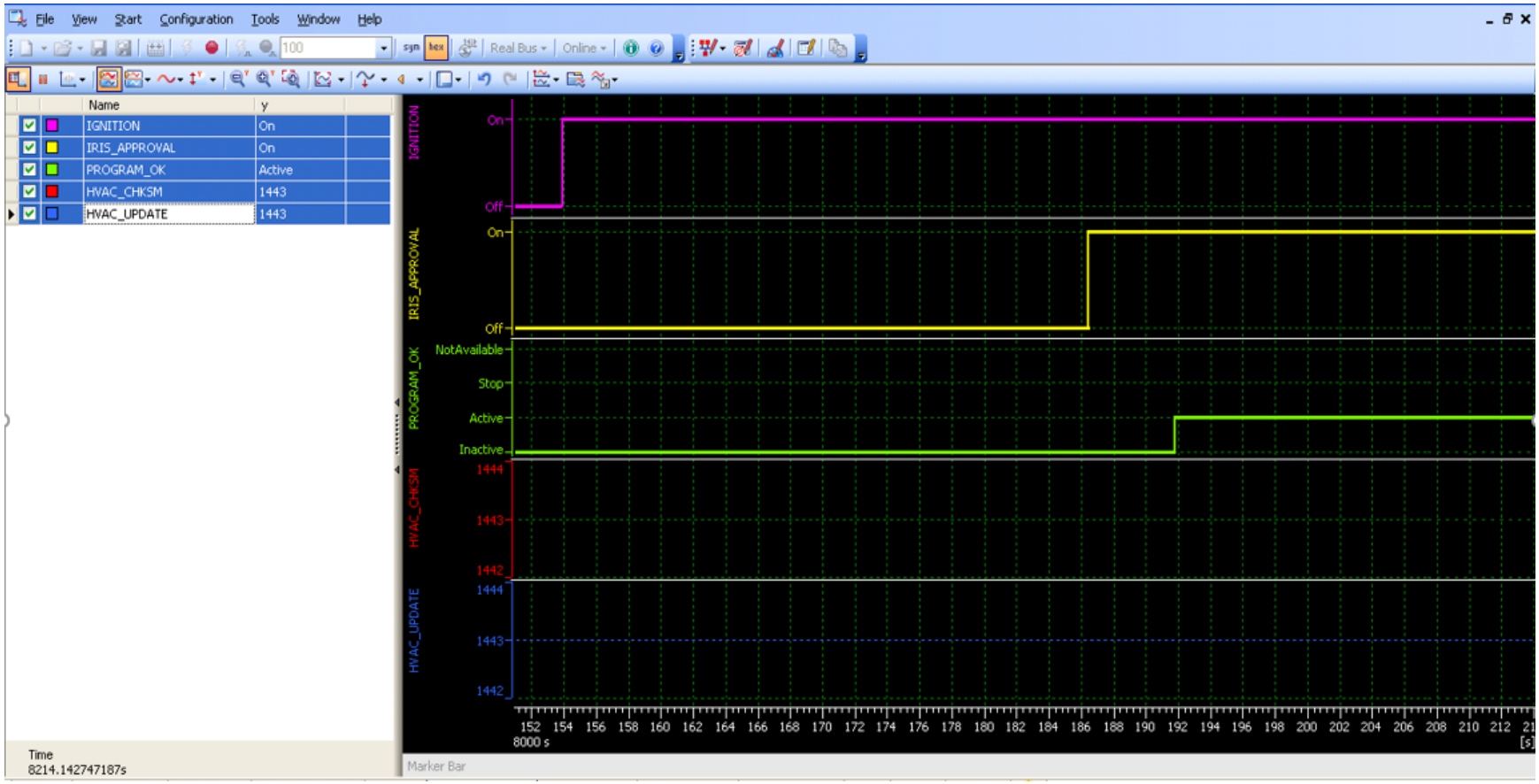

Fig. 7-9. Iris Enabled Inactive to Active Mode.

Chapter 8

Conclusion

In this thesis, we analyzed the cyber threats against OTA on connected vehicles. This suggests that we should emphasize them and consider their potential impact. Having the capacity to compromise a car's ECU is, however, only half the story. The rest of the worry is what an attacker is able to do with those competencies. Numerous car security designs and frameworks using encrypted keys and other technologies have been developed, however, each have some shortcomings. The method of securely installing software updates through OTA, proposed in this thesis, incorporates a 2-step security verification process including iris recognition and checksum comparison, which will help to mitigate the potentially threats associated with OTA software updates. This thesis will encourage the researchers to try new variant of biometric or encryption method for security enhancement of over the air update in connected vehicles. For the future work, we plan to implement and evaluate the proposed approach on real vehicles to gain more insights on its efficiency and usability.

References

[1] T. Roermund, Secure Connected Cars for a Smarter World, NXP Semiconductors, 2015.

[2] A. Birnie and T. Roermund, A Multi-Layer Vehicle Security Framework, NXP Semiconductors, 2016.

[3] "Uniform Crime Report, Crime in United States. Motor Vehicle Theft," U.S. Department of Justice—Federal Bureau of Investigation, 2014.

[4] "U.S. Department of Justice Federal Bureau of Investigation," 2010. [Online]. Available: https://ucr.fbi.gov/crime-in-the-u.s/2010/crime-in-the-u.s.-2010/tables/10tbl18.xls .

[5] "IEEE-SA Standards Board Operations Manual," IEEE-SA, 09 13 2017. [Online]. Available: https://standards.ieee.org/develop/policies/opman/sect8.html.

[6] "Wi-Fi Alliance," 11 2 2017. [Online]. Available: http://www.wi-fi.org/.

[7] "Mobile Device," 11 2 2017. [Online]. Available: https://en.wikipedia.org/wiki/Mobile_device.

[8] "Smart Devices," "Techopedia," 11 2 2017. [Online]. Available: https://www.techopedia.com/definition/31463/smart-device.

[9] J. Wayman, A. Jain, D. MaltoniDario and D. Maio, "An introduction to biometric authentication systems.," Biometric Systems, pp. 1-20, 2005.

[10] "Database – Definition of database by Merriam-Webster," 11 2 2017. [Online]. Available: https://www.merriam-webster.com/dictionary/database.

[11] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology 14.1, pp. 4-20, 2004.

[12] P. Narayanam Sri and N. Venkatram, "Establishing efficient security scheme in home IOT devices through biometric finger print technique," Indian Journal of Science and Technology 9.17, 2016.

[13] N. S. Raghava, "Iris recognition on hadoop: A biometrics system implementation on cloud computing.," in Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. IEEE, 2011.

[14] S. Moshe, A. Gryc and R. Miucic, "Firmware update over the air (FOTA) for automotive industry. No. 2007-01-3523.," SAE Technical Paper, 2007, 2007.

[15] L. Ma, T. Tan, Y. Wang and D. Zhang, "Efficient iris recognition by characterizing key local variations," IEEE Transactions on image processing 13.6, pp. 739-750, 2004.

[16] D. Mckenna, "Making Full Vehicle OTA Updates a Reality," NXP Semiconductors, 2016. [Online]. Available: https://www.nxp.com/docs/en/white-paper/Making-Full-Vehicle-OTA-Updates-Reality-WP.pdf

[17] W. Fenlon, "10 Amazing Car Security Systems," 07 02 2017. [Online]. Available: HowStuffWorks.com. http://auto.howstuffworks.com/under-the-hood/aftermarket-accessories-customization/10-car-security-systems.htm.

[18] P. Mundhenk, A. Paverd, A. Mrowca, S. Steinhorst, M. Lukasiewycz, S. Chakraborty and S. A. Fahmy, "Security in Automotive Networks: Light-weight Authentication and Authorization," ACM Transactions on Design Automation of Electronic Systems (TODAES), vol. 22, 2015.

[19] B. Groza, S. Murvay, A. V. Herrewege and I. Verbauwhede, "LiBrA-CAN: A Lightweight Broadcast Authentication Protocol for Controller Area Networks," in International Conference on Cryptology and Network Security, Darmstadt, 2012.

[20] A. Van Herrewege, D. Singelee and I. Verbauwhede, "CANAuth-a simple, backward compatible broadcast Authentication Protocol for CAN bus," in ECRYPT Workshop on Lightweight Cryptography, 2011.

[21] Q. Wang and S. Sawhney, "VeCure: A practical security framework to protect the CAN bus of vehicles," in International Conference on the Internet of Things, Cambridge, 2014.

[22] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Sacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, "Comprehensive Experimental Anal-yses of Automotive Attack Surfaces," in USENIX Security, San Francisco, 2011.

[23] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Au-tomobile," in Symposium on Security and Privacy, 2010.

[24] C. Miller and C. Valasek, "Adventures in Automotive Networks and Control Units," IO-Active Comprehensive Information Security, 2013.

[25] S. Klitz, J. Dittmann and T. Hoppe, "Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures," in International Conference on Computer Safety, Reliability, and Security, Newcastle, 2008.

[26] L. Ben Othmane, R. Fernando, R. Ranchal, B. Bhargava and E. Bodden, "Likelihood of Threats to Connected Vehicles," Inter-national Journal of Next-Generation Computing (IJNGC), vol. 5, pp. 290-303, 2014.

[27] R. Verdult, B. Ege and F. D. Garcia, "Dismantling megamos crypto: Wirelessly lockpick-ing a vehicle immobilizer," in 22nd USENIX Security Symposium, Washington DC, 2013.

[28] T. Zhang, H. Antunes and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," IEEE Internet of Things Journal, vol. 1, pp. 10-21, 2014.

[29] N. S. Raghava, "Iris recognition on hadoop: A biometrics system implementation on cloud computing.," in Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on. IEEE, 2011.

[30] "An Introduction To Retinal Scanning and Iris Scan," 04 25 2017. [Online]. Available: http://www.divilabs.com/2013/04/an-introduction-to-retinal-scanning-and.html.

[31] "Explainer: Retinal Scan Technology," 07 09 2017. [Online]. Available: http://www.biometricupdate.com/201307/explainer-retinal-scan-technology.

[32] M. Wolf, A. Weimerskirch and C. Paar, "Security in automotive bus systems," Workshop on Embedded Security in Cars, 2004.

[33] B. Hegde, "Modeling of Vehicle Controller Area Network for Control Systems Simulation," Diss. The Ohio State University, 2014.

[34] "Samsung News specialist news site," 08 07 2016. [Online]. Available: http://samsungnews.net/samsung-giai-thich-cach-hoat-dong-cua-may-quet-mong-mat-tren-galaxy-note-7/.

[35] T. V. Wilson, "How Biometrics work," 11 11 2017. [Online]. Available: http://science.howstuffworks.com/biometrics4.htm.

[36] G. Determan, "Security alarm notification using iris detection systems". Patent 10/958,928.

[37] R. L. Allen and D. W. Mills, in Signal analysis: time, frequency, scale, and structure., New York: IEEE Press, John Wiley & Sons Inc, 2004.

[38] J. Daugman, "Biometric decision landscapes.," Cambridge: The Computer Laboratory, University of Cambridge 1999. Report No.: TR482.

[39] J. Daugman, "How iris recognition works," IEEE Transactions on circuits and systems for video technology 14.1, pp. 21-30, 2004.

[40] A. Simon, D. M. Worthen and J. A. Mitas, "An evaluation of iridology.," Journal of the American Medical Association 242:, pp. 1385-1387, 1979.

[41] L. Berggren, "Iridology: A critical review.," Acta Ophthalmologica 63(1), pp. 1-8, 1985.

[42] G. cities, 10 2009. [Online]. Available: http://www.oocities.org/fastforward_consultants/implementation.htm.