ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

# To Prevent Wireless Attack Happens in Automobile is Rectified by a Security Protocol Using CAN

P.Vinoth, P.Priya Dharsini

PG Student, Department of ECE, Rajas Engineering College, Raja Nagar, Vadakkangulam, Tamil Nadu, India

Assistant Professor, Department of ECE, V.V College of Engineering, Tisayanvillai, Tamil Nadu, India

**ABSTRACT:** Vehicle-IT convergence technology is a rapidly rising paradigm of modern vehicles, in which an electronic control unit (ECU) is used to control the vehicle electrical systems, and the controller area network (CAN), an in-vehicle network, is com- monly used to construct an efficient network of ECUs. Unfortunately, security issues have not been treated properly in CAN, although CAN control messages could be life-critical. With the appearance of the connected car environment, in-vehicle networks (e.g., CAN) are now connected to external networks (e.g., 3G/4G mobile networks), enabling an adversary to perform a long-range wireless attack using CAN vulnerabilities. In this paper we show that a long-range wireless attack is physically possible using a real vehicle and malicious smart phone application in a connected car environment. We also propose a security protocol for CAN as a countermeasure designed in accordance with current CAN specifications. We evaluate the feasibility of the proposed security protocol using CANoe software and a DSP-F28335 microcon- troller. Our results show that the proposed security protocol is more efficient than existing security protocols.

## I. INTRODUCTION

### 1.1 Automotive communications-past, current and future

A state-of-practice (SOP) overview of automotive communication technologies, including the latest technology developments. These networking technologies are classified in four major groups: (1) current wired, (2) multimedia, (3) upcoming wired and (4) wireless. Within these groups a few technologies stand out as strong candidates for future automotive networks. The goal of this paper is to give an overview of automotive applications relying on communications, identify the key networking technologies used in various automotive applications, present their properties and attributes, and indicate future challenges in the area of automotive communications.

Also, many subsystems are safety-critical. A big issue that automotive industry has to deal with is the high number of existing networking technologies. From an engineering perspective, it is therefore desirable to move from using many technologies to use fewer and more general ones. To reduce the complexity it is desirable to commit on a set of networking technologies that can be used in most of the applications typically found in an automotive system. In order to support the automotive systems of tomorrow, these networking technologies need to be interconnected.

This interconnection should provide timeliness, compensability and fault tolerance across the whole "network of networks". A modern car contains a lot of electronic devices such as advanced safety systems, power train control, sensors, and means for diagnostics. These subsystems have evolved over time, relying on various communication services provided by different networking technologies. The existing and upcoming automotive networking technologies, identifying traditional and novel automotive application requirements and addressing to what extent existent and upcoming networking technologies are able to meet such requirements. The paper has discussed the next steps in automotive communications, with a specific focus on x-by-wire systems and wireless applications.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

### 1.2 Experimental security analysis of a modern automobile

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular networks. While this transformation has driven major advancements in efficiency and safety, it has also introduced a range of new potential risks. In this paper we experimentally evaluate these issues on a modern automobile and demonstrate the fragility of the underlying system structure.

An attacker who is able to infiltrate virtually any Electronic Control Unit (ECU) can leverage this ability to completely circumvent a broad array of safety- critical systems. Over a range of experiments, both in the lab and in road tests, we demonstrate the ability to adversarial control a wide range of automotive functions and completely ignore driver input dash including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, and so on.

Today's automobile is no mere mechanical device, but contains a myriad of computers. These computers coordinate and monitor sensors, components, the driver, and the passengers. Indeed, one recent estimate suggests that the typical luxury sedan now contains over 100 MB of binary code spread across 50–70 independent computers Electronic Control Units (ECU) in automotive vernacular in turn communicating over one or more shared internal network buses.

### 1.3 Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes

Modern vehicles contain an in-vehicle network consisting of a number of electronic control units (ECU).These ECUs are responsible for most of the functionality in the vehicle, including vehicle control and maneuverability. To date, no security features exist in this network since it has been isolated. However, an upcoming trend among automobile manufacturers is to establish a wireless connection to the vehicle to provide remote diagnostics and software updates. As a consequence, the in-vehicle network is exposed to external communication, and a potential entry point for attackers is introduced. Messages sent on the in- vehicle network lack integrity protection and data authentication; thus, the network is vulnerable to injection and modification attacks. A message authentication code is calculated on a compound of successive messages and sent together with the subsequent messages, resulting in a delayed authentication.

An upcoming trend for automotive manufacturers is to create a wireless connection to a vehicle to provide remote diagnostics and remote software updates. As a result, the previously isolated in-vehicle network is exposed to external communication, and thus a whole new range of threats, collectively known as cyber attacks, are introduced. These attacks target a critical infrastructure, namely the drivers, vehicles, and other people in the traffic.

### 1.4 Efficient Protocols for Secure Broadcast in Controller Area Networks

Controller Area Network is a bus commonly used by controllers inside vehicles and in various industrial control applications. In the past controllers were assumed to operate in secure perimeters, but today these environments are well connected to the outside world and recent incidents showed them extremely vulnerable to cyber-attacks. To withstand such threats, one can implement security in the application layer of CAN. The refine and implement a broadcast authentication protocol based on the well-known paradigm of using key-chains and time synchronization, a commonly used mechanism in wireless sensor networks, which allows us to take advantage from the use of symmetric primitives without the need of secret shared keys during broadcast. But, as process control is a time critical operation we make several refinements in order to improve on the authentication delay

As for in-vehicle security, recent research showed current automobiles to be unexpectedly vulnerable to external adversaries and it is likely that many other environments in which CAN operates are not completely isolated from the outside world.

### 1.5 Real-Time Data Collection for Product Carbon Footprints in Transportation Processes Based on OBD2 and Smart phones

Calculating product carbon footprints (PCF) is a central function of Environmental Management Information Systems (EMIS). Collecting accurate data for EMIS in general and PCF in particular is a critical issue. Nowadays, emission data of transportation processes are mostly based on averages and estimations, as data on actual emissions of transportation processes are costly to collect.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

A cost-efficient system for real-time data gathering for PCF in transportation processes based on vehicle on-board systems and smartphones. The system architecture, outline the application logic and based on a generic multiechelon transportation network its application and integration into EMIS.
The system combines OBD2 real-time data gathering with GPS and a smartphone in order to provide high quality data for the PCF calculation. This system enables the calculation of actual emission data for individual products. The system architecture, outline the application logic and based on a generic multiechelon transportation network we specify its application and integration into EMIS. A system for calculating the PCF of individual products' transportation processes.

### 1.6 Security Aspects of the In-Vehicle Network in the Connected Car

The aim is to highlight current research within the area, so that new directions can be taken in the future. Equipping the vehicle with a wireless connection will create many opportunities for new services, e.g. firmware update over the air (FOTA) and remote diagnostics. However, those very attractive features come with great challenges.
The internal as well as external communication must be properly secured. This is particularly important, since the in vehicle network is safety-critical and it is imperative to avoid that security problems lead to disastrous safety implications. Therefore, we are concerned about some recent papers that report about significant insecurity of the connected car. By connecting to the On-Board Diagnostics II (OBD-II), they were able to, among other things, issue commands to disable the breaks while driving. Although these attacks were performed through the diagnostic interface, which so far requires physical access to the vehicle, we expect that these attacks will be possible to perform through a wireless connection in a coming version of the connected car.

### 1.7 Secure Firmware Updates over the Air in Intelligent Vehicles

Modern intelligent vehicles have electronic control units containing firmware that enables various functions in the vehicle. New firmware versions are constantly developed to remove bugs and improve functionality.
Automobile manufacturers have traditionally performed firmware updates over cables but in the near future they are aiming at conducting firmware updates over the air, which would allow faster updates and improved safety for the driver. A protocol for secure firmware updates over the air.
Moreover, the same results as those of physical attacks can be realized by performing cyber-attacks. These attacks target a critical infrastructure, including both vehicles and drivers, and can potentially be performed on a large scale with little effort. Successful execution of such attacks, e.g., installing malicious versions of firmware, can have disastrous consequences endangering human life.
The protocol provides data integrity, data authentication, data confidentiality, and freshness. In our protocol, a hash chain is created of the firmware, and the first packet is signed by a trusted source, thus authenticating the whole chain. Moreover, the packets are encrypted using symmetric keys.
The practical considerations that exist for implementing our protocol and show that the protocol is computationally efficient, has low memory overhead, and is suitable for wireless communication. Therefore, it is well suited to the limited hardware resources in the wireless vehicle environment.

### 1.8 Cyber-Security for the Controller Area Network (CAN) Communication Protocol

A security mechanism to help prevent cyber-attacks i.e. masquerade and replay)in vehicles with architecture based on Controller Area Network (CAN). We focus on CAN as it will likely continue being used in upcoming in-vehicle architectures. The CAN protocol contains no direct support for secure communications. Retrofitting the protocol with security mechanisms poses several challenges given the very limited data rates available since bus utilization may significantly increase.
On a security mechanism which keeps the bus utilization as low as possible. Through our experimental results, we show that our security mechanism can achieve high security levels while keeping communication overheads at reasonable levels.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

Modern automotive electronics systems are distributed as they are implemented with software running over networked Electronic Control Units (ECU) communicating via serial buses and gateways. Most systems have not been designed with security in mind.

Communication networks are vulnerable as they enable unauthorized access in a relatively straightforward manner as all the communications between the ECUs in the vehicle are performed with no authentication. Authentication mechanisms ensure that sender and receiver identities are not compromised and thus, the sender and the receiver are who they are claiming to be.

Unfortunately, current communication network protocols, including Controller Area Network (CAN), Flex Ray, MOST, and LIN have no authentication and send their messages in the clear. Hence, room for fraudulent communications between ECU exists.

A security mechanism that can be used to retro-fit the CAN protocol to protect it from cyber-attacks such as masquerade and replay attacks. The mechanism is suitable for this protocol because it has a low communication overhead and does not need to maintain global time. Besides, the solution is software-only, hence, it is not overly expensive to implement. Experimental results showed that our security mechanism can achieve high security level without introducing high communication overhead in terms of bus load and message latency.

## II. PROPOSED SYSTEM

The aim is to reduce long-range wireless attack is physically possible using a real vehicle and malicious Smartphone application in a connected car environment. A long-range wireless attack is physically possible using a real vehicle and malicious Smartphone application in a connected car environment.A security protocol for CAN as a countermeasure designed in accordance with current CAN specifications. The feasibility of the proposed security protocol using CAN Android software and a Atmega128 microcontroller.

Our results show that the proposed security protocol is more efficient than existing security protocols with respect to authentication delay and communication load. A practical wireless attack using a real vehicle in a connected car environment, in which a driver's smartphone is connected to the in-vehicle CAN.Our attack experiment consists of two phases: preliminary and actual attack. In the preliminary phase, before launching an actual attack, an attacker first acquires a CAN data frame to force control of the target vehicle using a diagnostic tool. In fact, the same model vehicles could be used.A diagnostic tool is used to get a CAN data frame to force control of an ECU and does not need to be attached to the target vehicle during an actual attack. The attacker also manufactures a malicious self-diagnostic app that masquerades as a normal one and uploads it onto application markets. By using a self-diagnostic application such as "Torque," "Car Gauge Pro," and an OBD2 scan tool such as "EML327," "PLX KiWi," a driver can monitor CAN status information even while driving. Once the driver of the target vehicle downloads the malicious self-diagnostic app, the Smartphone is under the control of the attacker.

### 2.1 BLOCK DIAGRAM:

Fig 2.1 Connected car environmentAlong with the practical wireless attack experiment, we also propose a security protocol to remedy the vulnerabilities of CAN satisfying the requirements in the following.

1. The data encryption and authentication techniques ensure real-time data processing in the in-vehicle CAN.
2. The method using a message authentication code (MAC) considers the limited data payload of the CAN data frame.
3. Key management techniques support secure connectivity between external device and the in-vehicle CAN.

The security and performance of the proposed security protocol using a manufactured Secure ECU, similar to a real ECU and a commonly used commercial software tool.

1. Demonstration of a practical long-range wireless attack experiment using a malicious smart phone app in a connected car environment.
2. Design of a security protocol that can be implemented on an ECU, accommodating the limited resources available and the current CAN data frame format.
3. Analysis of the security and performance of the proposed security protocol using Secure-ECU and CAN.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

## 2.2 CAN

A controller area network (CAN) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. It is a message-based protocol, designed originally for multiplex electrical wiring within automobiles, but is also used in many other contexts.The CAN is a high-integrity serial data communication technology developed in the early 1980s by Robert Bosch GmbH for efficient communication between automotive applications. CAN is a multimaster broadcast communication bus system based on sender ID that allows ECUs to communicate on a single or dual wire network with data rates up to 1 Mb/s.CAN protocol is divided into two modes, i.e., CAN 2.0A and CAN 2.0B, according to the length of the ID field. As CAN 2.0B supports compatibility with CAN 2.0A, we only describe CAN 2.0B in this paper. The data frame format of CAN 2.0B is shown in Fig. 3.1. CAN 2.0B has a 29-bit ID field divided into two parts: Base ID field and Extended ID field

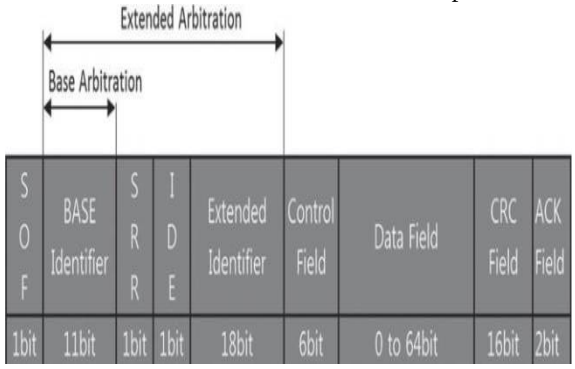



Fig 2.2 Data frame format of CAN 2.0B protocol

The CAN protocol allowed auto makers to reduce the complexity and cost of in-vehicle network wiring; hence, ISO established CAN as the international standard in 1993. In the CAN protocol, each ECU transfers information to other ECUs using a data frame. A sender ECU transmits data frames that include its own ID. Other ECUs retrieve data frames selectively after identifying the ID of the sender ECU in the data frame.CAN protocol is divided into two modes, i.e., CAN 2.0A and CAN 2.0B, according to the length of the ID field. As CAN 2.0B supports compatibility with CAN 2.0A, we only describe CAN 2.0B in this paper. The data frame format of CAN 2.0B is shown in Fig. 3.1. CAN 2.0B has a 29-bit ID field divided into two parts: Base ID field and Extended ID field.

The ID field is used to set the message priority. The IDE field determines the use of the 18-bit Extended ID field. The data field is a maximum of 8 bytes and includes information to be transmitted from the sender ECU to others. The cyclic redundancy check (CRC) field is used for error detection of the transferred data frame.
The modern automobile may have as many as 70 electronic controlunits (ECU) for various subsystems. Typically the biggest processor is the enginecontrol unit. Others are used for transmission, airbags, antilock braking/ABS, cruisecontrol, electric power steering, audio systems, power windows, doors, mirror adjustment, battery and recharging systems for hybrid/electric cars, etc. Some of these form independent subsystems, but communications among others are essential. A subsystem may need to control actuators or receive feedback from sensors.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

**2.3 BLUETOOTH**

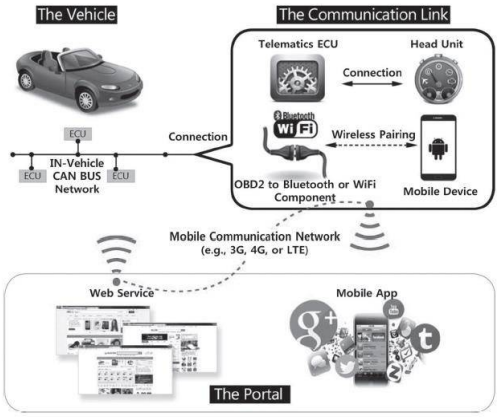
Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices, and building personal areanetworks (PAN). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 25,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development of the specification, manages the qualification program, and protects the trademarks. A manufacturer must make a device meet BluetoothSIG standards to market it as a Bluetooth device. A network of patents apply to the technology, which are licensed to individual qualifying devices.

A master Bluetooth device can communicate with a maximum of seven devices in a piconet, though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master.

The Bluetooth Core Specification provides for the connection of two or more piconets to form a scatternet, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

To use Bluetooth wireless technology, a device must be able to interpret certain Bluetooth profiles, which are




definitions of possible applications and specify general behaviours that Bluetooth-enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parametrize and to control the communication from start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective.

**2.4 WIFI**

Wi-Fi is a local area wireless computer networking technology that allows electronic devices to network, mainly using the 2.4 gigahertz, UHF and 5 gigahertz SHFISM radio bands.The Wi-Fi Alliance defines Wi-Fi as any "wireless local area network" (WLAN) product based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. However, the term "Wi-Fi" is used in general English as a synonym for "WLAN" since most modern WLANs are based on these standards. "Wi-Fi" is a trademark of the Wi-Fi Alliance. The "Wi-Fi Certified" trademark can only be used by Wi-Fi products that successfully complete Wi-Fi Alliance interoperability certification testing.

Many devices can use Wi-Fi, personal computers, video-game consoles, smart phones, digital cameras, tablet computers and digital audio players. These can connect to a network resource such as the Internet via a wireless network accesspoint. Such an access point has a range of about 20 meters indoors and a greater range outdoors.Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.Wi-Fi can be less secure than wired connections, such as Ethernet, precisely because an intruder does not need a physical connection. Web pages that useTLS are secure, but unencrypted internet access can easily be detected by intruders. Because of this, Wi-Fi has adopted various encryption technologies. The early encryption WEP proved easy to break.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

Higher quality protocols were added later. An optional feature added in 2007, called Wi-Fi Protected Setup (WPS), and had a serious flaw that allowed an attacker to recover the router's password.

**2.5 TELEMATICS CONTROL UNIT**

A TCU consists of:

1. A global positioning system (GPS) unit, which keeps track of the latitude and longitude values of the vehicle;
2. An external interface for mobile communication, which provides the tracked values to a centralized geographical information system (GIS) database server;
3. An electronic processing unit;
4. A microcontroller, in some versions; a microprocessor or fieldprogrammable gate array (FPGA), which processes the information and acts on the interface between the GPS;
5. A mobile communication unit;
6. Some amount of memory for saving GPS values in case of mobile-free zones or to intelligently store information about the vehicle's sensor data.

The main components of any in-vehicle telemetric control unit can be represented based on functionality as follows: Application Process Block Wireless Interface Block Vehicle Interface Block Debug Interface Wireless Network Voice/Mic Vehicle Communications Bus Discrete I/O, Sensors Diagnostics Interface Application Process Block – The APB provides the platform for all the application level services provided by a TCU.

The APB has an interface with the Wireless Interface Block and the Vehicle Interface Block. The APB interfaces with the other vehicle components through the VIB and interfaces with the Telematics network-side using the WIB. The APB is responsible for maintaining the state machines of all services and features and also controlling the other TCU blocks based on provisioning state and power modes amongst other factors.

Features such as over the air provisioning and ECU software downloading allow the vehicle OEMs to keep all the ECUs in vehicle up to date with all the essential and critical software updates reducing vehicle recalls and maintenance cost significantly. The debugging functionality/Interface for engineering development is also a part of the APB functionality and aids in diagnosing and preventing potential system shortcomings.

The APB should have the capability to detect and recover from any kind of software failures in any of the TCU modules. This can be enforced by strict health monitoring of all the TCU components, accurate diagnosis or the problem and the ability to take the corrective steps to recover from the problem. The APB should also manage the power states of the TCU to conserve the power usage in accordance with the ignition state.

## III. RESULTS AND DISCUSSION

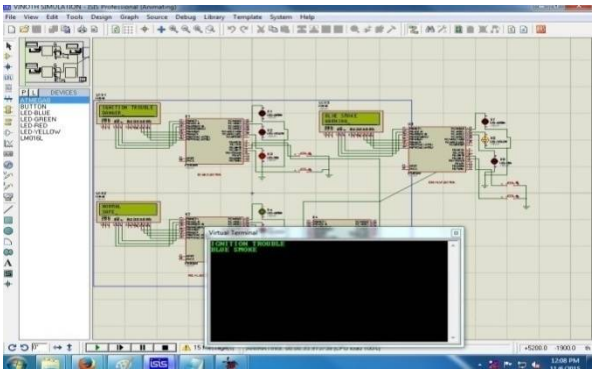


Fig 3.1 Overall design

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]

On 10th & 11th March, 2016

Organized by

Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

The figure 3.1 shows the overall design in which the CAN protocol is implemented by communicating with the different controllers. It includes three sections Such as engine, exhaust and pedal sections. Three sections communicate with each other.

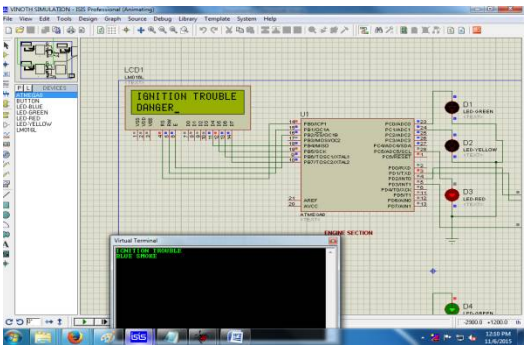



Fig 3.2 Representation of engine trouble

The figure 3.2 shows the engine section which indicates that the ignition is in trouble and is indicated by red light as danger.

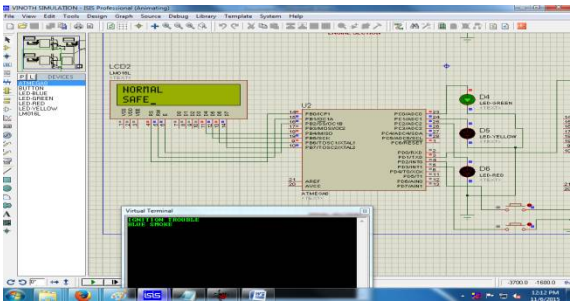



Fig 3.3 Representation of normal mode

In figure 3.3 it is shown as normal and is indicated by green light.

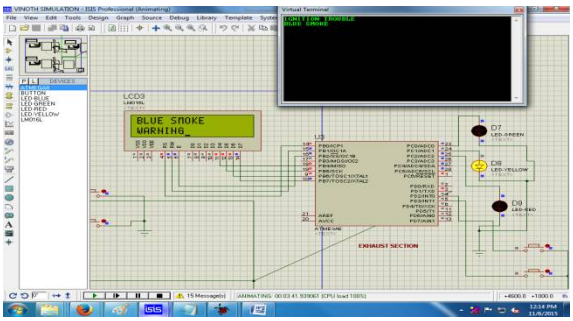



Fig3.4 Representation of warning signal

In figure 3.4 it shows the warning signal and is indicated by the yellow signal. In this case the vehicle will not be stopped but it needs the immediate repair.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]

On 10th & 11th March, 2016

Organized by

Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

## IV. CONCLUSION

Recently, many studies on the vulnerability of in-vehicle CAN have been done. However, such attack models are unrealistic because they require significant effort and complex technology such as reverse engineering and carjacking. An actual attack model using a malicious smartphone app in the connected car environment and demonstrated it through practical experiments. After demonstrating the attack model with an analysis of the vulnerability of in-vehicle CAN, we designed a security protocol that could be applied to the car environment. Furthermore, we analyzed the security and performance of the proposed security protocol through an evaluation based on both Secure-ECU and CAN. To improve the performance of the proposed security protocol with an implementation of the encryption and hash algorithms on hardware to optimize our security technology.

## REFERENCES

1.B. Groza and S. Murvay, "Efficient protocols for secure broadcast in controller area networks," IEEE Trans. Ind. Informa., vol. 9, no. 4, pp. 2034–2042, Nov. 13.
2.H. Hilpert, L. Thoroe, and M. Schumann, "Real-time data collection for product carbon footprints in transportation processes based on OBD2 and smartphones," in Proc. Conf. Syst. Sci., 2011, pp. 1–10.
3. T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," Rel. Eng. Syst. Safety, vol. 96, no. 1, pp. 11–25, Jan. 2011.
4. T. Hoppe and J. Dittman, "Sniffing/replay attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted CERT taxonomy," in Proc. Conf. Embedded Syst. Security, 2007, pp. 1–6.
5. K. H. Johansson, M. Torngren, and L. Nielsen, "Vehicle applications of controller area network," in Handbook of Networked and Embedded Control Systems. New York, NY, USA: Springer-Verlag, 2005, pp. 741–765.
6. K. Koscher et al., "Experimental security analysis of a modern automobile," in Proc. IEEE Security Privacy. Symp., Oakland, CA, USA, 2010, pp. 447– 462.
7. P. Kleberger, T. Olovsson, and E. Jonsson, "Security aspects of the in- vehicle network in the connected car," in Proc. IEEE Intell. Veh., Symp., 2011, pp. 528–533.
8.C. W. Lin and A. Sangiovanni Vincentelli, "Cyber-security for the Controller Area Network (CAN) communication protocol," in Proc. Conf. IASE Int. Conf. Cyber Security, 2012, pp. 344–350.
9. E. Nickel, "IBM automotive software foundry," in Proc. Conf. Comput. Sci. Autom. Ind., Frankfurt, Germany, 2003.
10.D. K. Nilsson, U. E. Larson, and E. Jonsson, "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in Proc. Conf. IEEE 68th Int. Conf. Veh. Technol., Calgary, BC, Canada 2008, pp. 1–5.
11. D. K. Nilsson, U. E. Larson, and E. Jonsson, "Creating a secure infrastructure for wireless diagnostics and software updates in vehicles," in Proc. Conf. Comput. Safety, Rel., Security, Tyne, UK., Newcastle upon Tyne, U.K., 2008, pp. 207–220.
12.T. Nolte, H. Hansson, and L. L. Bello, "Automotive communications-past, current and future," in Proc. IEEE Int. Conf. Emerging Technol. Factory Autom., 2005, vol. 1, pp. 992–999.
13. A. Saad and U. Weinmann, "Automotive software engineering and concepts," GI. Jahrestagung., vol. 34, pp. 318–319, 2003.