DESIGN AND SIMULATION OF A CAR ANTI-HIJACKING SYSTEM

Ankush Laxman, *Z. Tracy Austina

Department of Computer Engineering, M. S. Ramaiah School of Advanced Studies, Bangalore

*Contact Author e-mail: tracy@msrsas.org

Abstract

Across the world, vehicle theft is a matter of grave concern that leads to huge monetary loss for vehicle owners. Tracking of stolen vehicles by police officials is difficult as criminals involved in vehicle theft often operate across the different states of the country. Hence there is a pressing need for a simple and cost-effective anti hijacking technique which will curtail vehicle theft and allow tracking of the stolen vehicle.

In this work, the focus is to develop a simulation model for an anti hijacking system using Labcenter Proteus. It is based on a secured technique of driver authentication by a two-factor authentication method using RFID and GSM. ECUs for authentication, Car Anti-hijacking System (CAS) and engine control were designed and modelled using PIC18F458 microcontrollers in Proteus. They were connected to each other on an I2C bus. The authentication ECU has RFID reader and a transponder that are used to authenticate a valid driver's RFID tag and communicated to the vehicle owner via a GSM module. After detecting a valid driver's tag the CAS ECU prompts the driver for a password for driver authentication. Once the driver is authenticated the engine control ECU permits the driver to start the vehicle. In case of the vehicle being hijacked, the engine control ECU sounds an alarm by checking engine idle condition and engine off condition. The engine ECU also retrieves a vehicle's location which is sent to driver's mobile phone by the CAS ECU.

The Embedded C code for this system was developed using MPLAB IDE. To parse location co-ordinates for the GPS receiver, string manipulation was implemented. The authentication ECU was tested successfully to identify two valid drivers and an invalid driver. The data communication in CAS ECU was tested by sending messages to two different mobiles. The developed model can be prototyped and integrated on a CAN bus in a vehicle to prevent hijacking. An Inertial Navigation System can also be integrated with the vehicle to locate the vehicle in the absence of GPS signal.

Key Words: Vehicle security, RFID, GPS, GSM, Anti-hijack system

Abbreviations

CAN	Controller Area Network
CAS	Car Anti-hijacking System
CCD	Charge-Coupled Device
CDMA	Code Division Multiple Access
ECU	Electronic Control Unit
GPS	Global Positioning System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
RFID	Radio Frequency Identification
SMS	Short Messaging Service

1. INTRODUCTION

Over the years, various technologies; such as vehicle immobiliser, car alarms, steering locks, online GPS tracking and the electronic transponder ignition key have been introduced to reduce the chances of vehicle theft. With the increasing cost of ownership of a vehicle, potential and existing vehicle owners anticipate a vehicle security system from vehicle manufacturers. An ideal Car Anti-Hijacking System allows for user authentication, vehicle tracking and notifying the user of theft.

2. LITERATURE REVIEW

Many researchers have proposed innovative methods for authenticating a driver and tracking a stolen vehicle. Methods ranging from the use of wireless sensor nodes to terrain-based tracking have been suggested by researchers for vehicle tracking.

In [1], the authors have proposed a vehicle anti-theft system based on face recognition. The system, known as POLLUX by the researchers uses a CCD camera to identify an authorized driver. If an authorized user is not found, the car owner is notified using CDMA or GPRS networks. The system can identify a maximum of five authorized drivers and captures images at a resolution of 64x64 pixels.

To test the system, 5 authorized drivers and 50 unauthorized drivers were used. The system was able to detect all the unauthorized drivers, who were used in the tests 100 times. The authorized drivers were tested 100 times with and 100 times without glasses. The POLLUX system detected the authorized drivers with glasses approximately 90-95% of the time and without glasses, was able to detect the authorized drivers 85-90% of the time.

In [2], the authors have proposed an RFID-based anti-theft system with an immobilizer. The research also takes advantage of the fact that unique tags with large character sets can be generated with active RFID tags. The RFID receiver is integrated with the ignition ECU, power supply ECU and the automatic gear changing

ECU, thereby allowing the vehicle to be immobilised in case of theft.

The intelligent vehicle unit is based on PIC16F84 microcontroller which communicates with the power supply ECU, ignition control ECU and the automatic gear changing ECU. If the receiving unit identifies a disabling tag from the transponder the intelligent vehicle system communicates with these ECUs to bring the vehicle to a stop after approximately 1.5kms. The RFID-based anti-theft system was tested by the researchers under different climatic conditions and different transmitting signal distortion conditions.

Under different climatic conditions, the system was found to have a range of 170 – 200m, 170m under rainy weather conditions and 200m under sunny weather conditions. To test the system under different distortion conditions, the first tag sent by the transmitting unit was deliberately distorted and then the correct tag was sent. Test results showed that the receiving unit was able to successfully identify the correct tag even if a distorted signal was received.

Rather than using GPS to track a vehicle, in [3] the authors from TCS Innovation Labs have proposed the use of wireless sensor devices for vehicle tracking. The system primarily consists of wireless sensor nodes, a gateway node and a central server. The wireless sensor nodes are installed in the vehicle while the gateway node can be installed in buildings, lampposts or similar supporting structures on either side of the road. The gateway node receives information from the wireless sensor nodes and transmits them to the central server. The central server, upon querying the gateway node, processes wireless sensor node information that it receives from the gateway node. The researchers assume that the gateway nodes are installed at regular intervals to successfully track a vehicle, and the nodes communicate with the central server via the internet using appropriate cables buried in the road.

To simulate their proposed tracking system, the researchers used Qualnet network simulator. Two metrics were used to analyze the simulation's performance – Packet Error Rate (PER) and Average End-to-End Delay. PER, which measures the percentage of packet loss during communication, was used to analyse the effects of varying antenna heights (of gateway nodes) such that packet loss is minimized while receiving information from the vehicle. To analyze the latency of packet reception from the gateway nodes due to an increase in the number of gateway nodes, the Average End-to-End Delay metric was used. This metric measures the average one-way latency of packets between the instant they are transmitted and the instant they are received. The results of the simulation showed that the vehicle can successfully be tracked by the central server by the second, with the assumption that the delay between the gateway node and the central server is negligible.

Using RFID for authentication and GSM for notifying the user, the authors of [4] have proposed a low-cost method to prevent vehicle theft. A passive RFID transponder is used to communicate with the RFID reader. The RFID reader is read/write capable so that the user can modify the code on the transponder. A match between the code on the transponder and the code stored in the microcontroller's memory will allow the vehicle to start. If no match is found, the system enables audio and visual alerts. The microcontroller also communicates with the engine ECU which can be stopped if theft is detected.

The control circuit for the system is based on STM8AF51AA microcontroller. It is an 8-bit microcontroller with built-in support for UART and CAN. The circuit also includes the LM7805 voltage regulator and the PCA82C250 CAN transceiver from NXP semiconductors. For the RF interface circuit, the 13.56 MHz MFRC522 RFID reader from NXP semiconductors is chosen. Rather than UART, the SPI interface is chosen for communication between the controller and the RFID reader. The SIM300DZ from Simcom is chosen as the GSM module. Overall, the software for the system is designed using interrupts for controlling the system's various inputs and outputs. However, to identify an authorized user, polling is used.

3. NEED FOR THIS WORK

According to the Criminal Investigation Department (CID), approximately 36,000 vehicles amounting to a total worth of Rs. 115 crores are stolen every year in India. The CID has also observed that two-thirds of all vehicle thefts take place after dark with 90% of vehicle thefts involving individuals under the age of 25 [5]. With this increase in vehicle thefts, a low-cost CAS system is needed which will aid the vehicle owners to keep track of his/her vehicle at all the times. In this work, a prototype of a Car Anti-hijacking System is designed and simulated in Proteus. Various test cases are established to test the simulation prototype and the results of the tests are discussed.

4. PROBLEM DEFINITION

Vehicle theft can occur if the thief attempts to hijack the car when the engine is idling (such as at traffic signals) or tow the vehicle when the ignition is switched off. A system, called the Car Anti-hijacking System (CAS), is proposed to notify the vehicle owner via SMS and sound an alarm if an attempt is made to hijack the vehicle when it is idling or an attempt is made to tow the vehicle.

5. METHODOLOGY

Literature survey for driver authentication and vehicle tracking as proposed by different researchers was carried out by referring to research papers. Top-level block diagram based on literature review was identified along with suitable components for the proposed system. A simulation of the CAS ECUs was developed using Labcenter Proteus, a Serial port emulator, a GPS simulator, an RFID module and a GSM module was carried out. Testing of the simulation was carried out using suitable test cases. The results of the test cases were analysed and discussed.

6. TOP-LEVEL BLOCK DIAGRAM

The block diagram for the CAS is shown in Figure 1. The system consists of three ECUs – the authentication ECU, CAS ECU and the engine ECU. The major components used in the system are the RFID module, GSM module and the GPS simulator. The RFID module, GSM module and the GPS simulator, all communicate with the controller via its UART module. Since the controller has only one UART module, it was decided to allocate one module to each controller. The engine ECU receives inputs from the neutral gear safety switch, the engine start/stop switch, the engine speed sensor, the wheel speed sensor and the GPS simulator. Based on these inputs, the controller outputs appropriate control signals for the door locks, an audio alarm and the vehicle display. There are two possible situations in which vehicle theft can be attempted – when the vehicle is parked with the engine switched off and when the vehicle is idling. Theft is not likely to be attempted while the vehicle is moving.

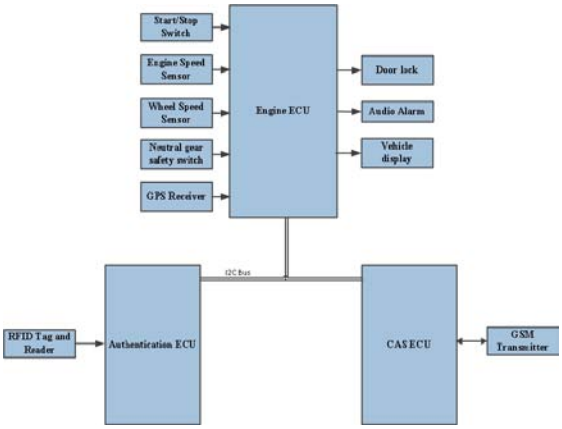

Fig. 1 Block Diagram for the CAS

7. CONTROL LOGIC

Figure 2 shows the flowchart for user authentication. The system searches for an RFID tag. If a valid tag is found, the user is prompted for an authentication code via the GSM module. Upon receipt of a valid code, the system unlocks the vehicle's doors, otherwise the doors remain locked and entry to the vehicle is denied.

Figure 3 shows the control logic that is largely implemented in the engine ECU. After the neutral gear is engaged, the system allows the vehicle to be started. When the system detects that the engine is idling, it searches for a valid RFID tag. If the tag is not found, the system sounds the alarm, notifies the vehicle's GPS location to the user and brings the vehicle to a stop.

Figure 4 shows the control logic that notifies the user if the vehicle is towed away. The controller checks for a valid RFID tag and the start/stop switch. If no tag is available and the vehicle ignition off, the controller decides that the vehicle is parked. Under these conditions the CAS checks the wheel speed sensor reading. A changing reading indicates that the vehicle is being towed. The system sounds the alarm and notifies the user.

Figure 5 shows the control logic for notifying the user during engine idling.

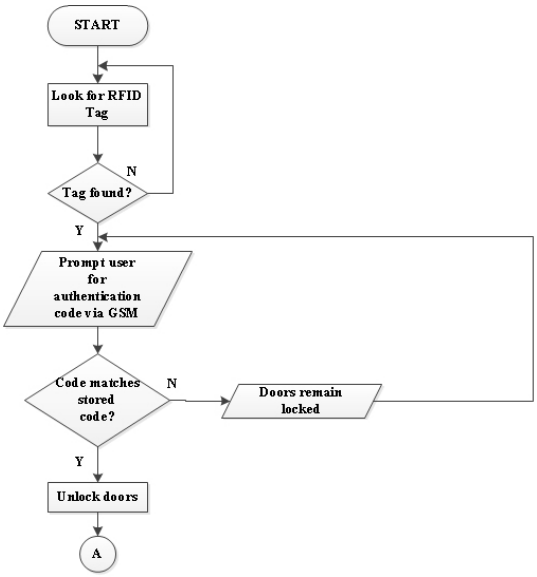

Fig. 2 Control Logic for Authenticating the User

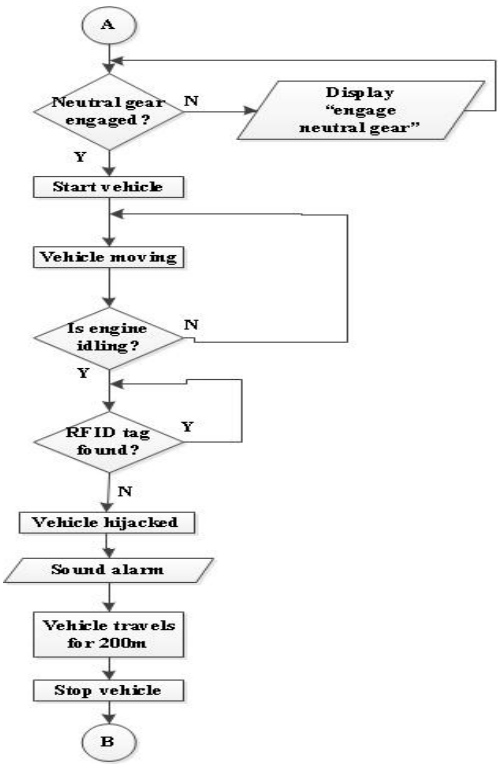

Fig. 3 Control Logic Implemented in the Engine ECU

8. PROTEUS SIMULATION

8.1 Choosing the Crystal Frequency

The crystal frequency Fosc was first determined using the following formula:

Fosc = desired baud rate*[64(X+1)] ... Eqn. (5.1)

From the PIC18F458 datasheet, an error of 0.16% is present at 16MHz and X=25, where X is the decimal value of the baud rate generator register. The desired baud rate for serial communication is 9600bps. Substituting these values in equation (5.1), equation (5.2) is obtained.

Fosc = 9600*[64(25+1)] = 15.9744 MHz ... Eqn. (5.2)

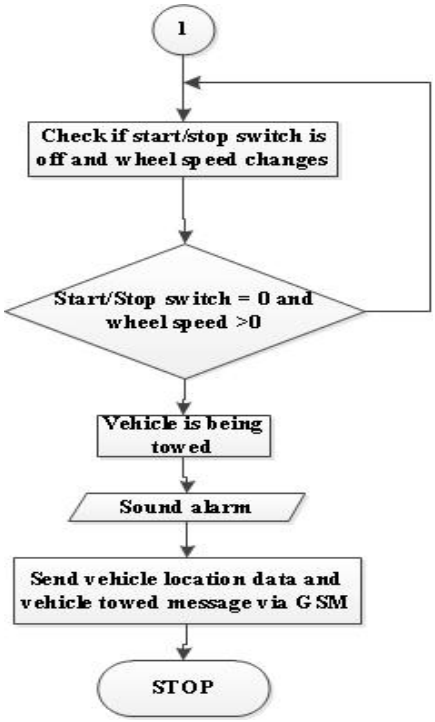

Fig. 4 Control Logic for Notifying the User (Vehicle Towed)

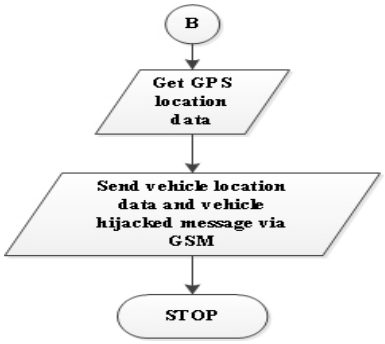

Fig. 5 Control Logic for Notifying the User (Engine Idling)

8.2 Authentication ECU

The authentication ECU detects a valid user's tag. Once a valid tag is found, it sends a signal via the I2C bus to the CAS ECU. It also transmits the tag's number to the engine ECU when requested. The RFID reader is interfaced with the host PC via an RS232 interface board and a USB-Serial adapter.

Figure 6 shows the Proteus model for the authentication ECU. A virtual connection was created between the COM15 physical port and the COM1 virtual port using Serial Splitter.

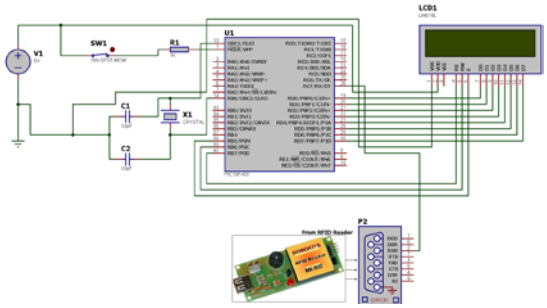

Fig. 6 Authentication ECU Proteus Model

8.3 Engine ECU

Figure 7 shows the circuit of engine ECU. As with the authentication ECU, the LCD's data lines were interfaced with Port D, its R/S, RW and E pins were interfaced with the RB7, RB6, and RB5 pins on Port B. In-line with the pre-requisites for the simulation, a value of 15.9744 MHz was chosen as the crystal frequency. With the exception of the CAN Rx and CAN Tx pins, the remaining pins on Port B were configured as output pins for the door lock indicator, the buzzer, and a motor to signify a rotating wheel. The AN0 channel was configured as an analogue input to which a potentiometer was connected to signify the engine speed sensor.

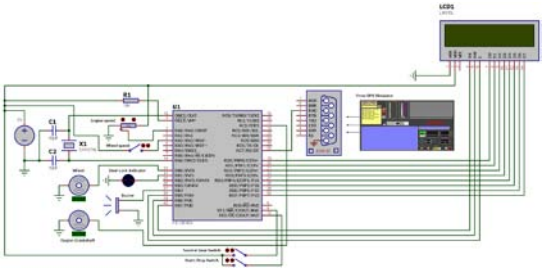

Fig. 7 Engine ECU Proteus Model

The AN2 channel was configured as a digital input to which a switch was connected. This switch signified two conditions, a changing wheel speed sensor reading and a zero wheel speed sensor reading. The wheel speed sensor reading is important only as long as it changes, i.e. the numerical value of the reading is considered only if the sensor reading is zero or changing (true condition, if the vehicle is towed. Channels AN6 and AN7 were configured as digital inputs for the neutral gear safety switch and the vehicle's start/stop switch.

The CCP1 bit on Port C was cleared for PWM output which was fed to a motor to signify a rotating crankshaft. Bit RB0 was cleared for software PWM control of a motor representing the vehicle's wheel. This bit was toggled with a 25ms delay for software PWM control of the motor.

8.4 CAS ECU

The Proteus circuit for the CAS ECU is shown in Figure 8. As with the engine and authentication ECUs,

the LCD's data lines are interfaced with Port D of the PIC18F458 microcontroller. The LCD's RS, R/W and enable pins are interfaced with pins RB7, RB6 and RB5 on Port B, respectively. The Rx and Tx pins of the microcontroller are connected to the Rx and Tx pins of the COMPIM component. The COM2 port is selected in the COMPIM component and the Virtual Terminal component is connected to the Rx pin of the COMPIM component to verify reception of data and to the Tx pin of the component to verify transmission of data. The Virtual Terminal component is used for testing purposes only and is not necessary in the final circuit of the CAS ECU. A 15.9744 MHz crystal is connected in the circuit.

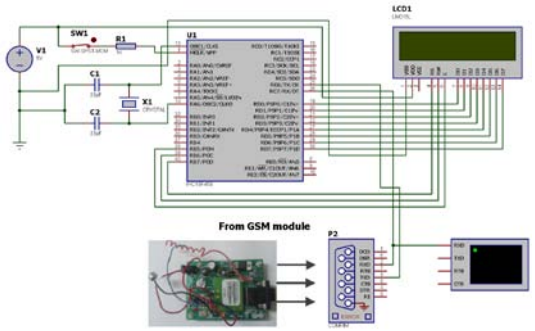

Fig. 8 CAS ECU Proteus Model

9. TESTING THE CAS

Various test cases were generated to ensure error-free functioning of the authentication ECU and the engine ECU. While testing the ECUs individually, the embedded 'C' code was modified to simulate different conditions under which the CAS was tested. These test cases were then applied to both ECUs and the working of the control logic. Test setup was created as shown in Figure 9.

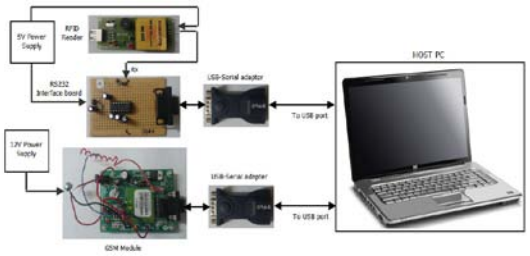

Fig. 9 Test Setup for the Simulation

9.1 Authentication ECU Test Cases

The embedded software for the authentication ECU was designed such that the vehicle can be operated maximum up to two users. Two transponders were used for the valid users while a third transponder is used for an invalid user. The following test cases were generated to test the authentication ECU:

Test 1: Valid user found. The transponders for the valid users were read by the RFID reader. Under this condition, the controller is expected to correctly identify two valid users and an invalid user.

Test 2: Valid user not found. The transponder for the invalid user was read by the RFID reader. Under this condition, the controller is expected to correctly identify an invalid user.

9.2 Engine ECU Test Cases

The Engine ECU was tested under two conditions – when the vehicle is parked and when it is moving. For the first test case, it is assumed that an attempt is made to steal the vehicle when it is switched off (parked). For the second test case, it is assumed that a valid user is in the vehicle when the vehicle is idling.

Test 1: Vehicle parked. For this test, the controller uses inputs from the start/stop switch, the wheel speed sensor and the RFID reader. If the controller does not find any tag and the start/stop switch is off the controller determines that the vehicle is parked. Under these conditions, a changing wheel speed will indicate that the vehicle is being towed away. There are two scenarios in this test:

Wheel speed sensor signal does not change, no tag found and the start/stop switch is off: Under this condition, the controller determines that the vehicle is not being stolen. The system does not do anything under this case, waits for a valid tag and monitors the wheel speed sensor.

Wheel speed sensor signal changes, no tag is found and the start/stop switch is off: Under this condition, the controller determines that the vehicle is being stolen. The expected response of the system is to sound the alarm and notify the vehicle's location to the user.

Test 2: Vehicle idling. For this test, the start/stop switch is on (neutral gear is engaged) and the engine is idling. To determine if the vehicle is idling, the controller first checks the engine speed sensor signal to determine if the vehicle is idling. In this condition the system checks for a tag from a valid user. The transponders are passive and the reader cannot search for them constantly. Hence for the Engine ECU simulation to work properly, the user is requested to "swipe" the tag when applicable. There are two possible scenarios in this test:

Valid tag not found: The controller requests for a valid tag. If the tag is not found, the controller's expected response is to sound the alarm. It also immobilises the vehicle and brings it to a halt

Valid tag found: Under this condition the controller does not do anything and monitors the engine speed sensor reading to determine if the vehicle is idling or moving. A condition for theft to occur when a vehicle is moving was not considered as a vehicle is more likely to be stolen when it is either parked or idling.

9.3 CAS ECU Test Cases

The CAS ECU is tested for transmission of two messages – one was a prompt for the user's authentication code and the other, a message containing latitude and longitude co-ordinates. These messages were sent to two different numbers representing two different users. The GSM module's response was observed on the terminal window.

10. RESULTS

The test cases were generated for both authentication and engine ECUs and their operation was verified to determine if implementation of the control algorithm in both the ECUs worked as expected as per the test cases.

10.1 Authentication ECU Test Results

Test 1: Valid tag not found

Result: The system was able to correctly identify an invalid user.
Comments: Test passed

Test 2: Valid tag found

Result: The system was able to identify two users correctly.
Comments: Test passed

Figure 10 shows that the authentication ECU was able to detect two valid users and an invalid user.

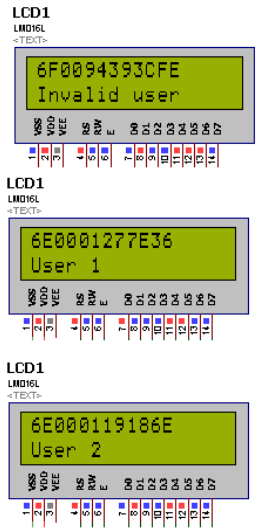

Fig. 10 Authentication ECU Test Results

10.2 Engine ECU Test Results

Test 1: Vehicle parked

Scenario 1: Wheel speed sensor signal does not change, start/stop switch is off and there is no received tag number.

Result: System continues to monitor the wheel speed sensor and the start/stop switch. It also checks for a tag.
Comments: Test passed

Figure 11 shows the test result when the system does not detect hijacking.

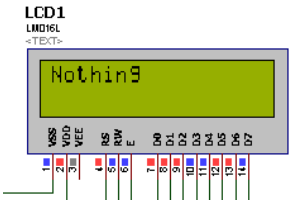

Fig. 11 Engine ECU Test Result for Test 1, Scenario 1

Scenario 2: Wheel speed sensor signal changes and the start/stop switch are off

Result: System sounds buzzer, displays vehicle hijacked message and retrieves GPS information. If no GPS signal is found, system displays vehicle hijacked and no GPS signal message. The absence of a GPS signal does not allow the vehicle to be tracked. Hence, under this condition the CAS does not allow the vehicle to be tracked and only notifies the user that the vehicle has been stolen and brings the vehicle to a stop.
Comments: Test passed. The user cannot track the vehicle if a GPS signal is absent.

Test 2: Vehicle idling

Scenario 1: Valid tag not found

Result: System sounds buzzer, stops vehicle, displays vehicle hijacked message and retrieves GPS information. If no GPS signal is found, system displays vehicle hijacked and no GPS signal message. Like the second scenario in the first test, the CAS does not allow the vehicle to be tracked and only notifies the user that the vehicle has been stolen and brings the vehicle to a halt.
Comments: Test passed. The user cannot track the vehicle if a GPS signal is absent. Figure 12 shows the PWM signal with 25% duty cycle (vehicle idling) and 95% duty cycle (vehicle moving).

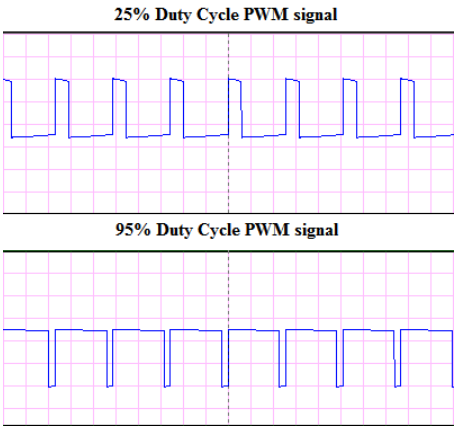

Fig. 12 PWM Signal with 25% Duty cycle (vehicle idling) and 95% Duty cycle (vehicle moving)

Scenario 2: Valid tag found

Result: System continues to monitor the engine speed sensor reading.
Comments: Test passed

10.3 CAS ECU Test Results

The simulation for serial transmission implemented with the CAS ECU showed that the code prompt message and the message containing the GPS co-ordinates were successfully transmitted to the two mobile phone numbers. Every message sent is followed by a "+CMGS: xxx" and "OK" response from the GSM module. These responses were observed in the terminal window as shown in Figure 13.

Fig. 13 CAS ECU Terminal Window

11. CONCLUSION

The literature survey showed that CAS systems proposed by researchers use either a method of authenticating and vehicle tracking or a method of authentication and user notification. However, all three functions have not been previously implemented in a CAS. The CAS proposed in this work integrates RFID (authentication), GPS (tracking) and GSM (authentication/notification) for a robust vehicle security solution.

In this work, the GPS parsing algorithm was developed using string manipulation and implemented in the engine ECU.

12. FUTURE WORK

Since the simulated system is meant for automotive applications, it would be advantageous if the CAN bus is used instead of I2C.

Instead of using the input from the engine speed sensor, wheel speed sensor and the start/stop switch to determine if the vehicle is hijacked, an Initial Navigation System can be used. This will eliminate the need for customizing the software to use a specific engine's idle speed and also allow the vehicle to be tracked in the absence of a GPS signal.

13. REFERENCES

[1] Liu Z., He G.A., *Vehicle Anti-theft and Alarm System Based on Computer Vision*, Proceedings of IEEE International Conference on Vehicular Electronics and Safety, Wuhan University, Oct. 14-16, 2005.

[2] Jayendra G., Kumarawadu S., Meegahapola L., *Vehicle Anti-theft and Alarm System Based on Computer Vision*, Proceedings of IEEE International Conference on Vehicular Electronics and Safety, Wuhan University, Oct. 14-16, 2005.

[3] Aravind K.G, Chakravarty T., Chandra G., Balamuralidhar P., *The Architecture of Vehicle Tracking System using Wireless Sensor Devices*, Proceedings of Ultra Modern Telecommunications & Workshops, ICUMT '09', TCS Innovation Labs, Oct. 12-14, 2009.

[4] Hongzhi O., Xinlin W., Weihua Z., Yuehua L, *Design of Auto-guard System Based on RFID and Network*, Proceedings of International Conference on Electric Information and Control Engineering (ICEICE), Univ. of South China, April 15-17, 2011.

[5] Unknown, *CID West Bengal Vehicle Theft Prevention*, www.cidwestbengal.gov.in, Retrieved on 3rd December, 2012.