IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SMART LOCKING AND UNLOCKING SYSTEM FOR VEHICLE THEFT CONTROL

A. Divya,
PG Scholar,
ME – CSE,
Vandayar Engineering College,
Thanjavur.

S.Ponmaniraj,
Assistant Professor,
SCSE,
Galgotias University,
Greater Noida,

Goukl Rajan V,
Assistant Professor,
SCSE,
Galgotias University,
Greater Noida,

Sanjay Sharma,
Assistant Professor,
SCSE,
Galgotias University,
Greater Noida,

S. Saranya
PG Scholar,
ME – Applied Electronics
Salem Engineering and Technology
Salem

***Abstract* – Nowadays vehicle thefts are increasing all over the world. Everyone is very concerned about securing their vehicles. This paper design and develop vehicle theft control systems used to prevent or control vehicle theft. The system is designed using the mobile phone supplied with the vehicle with a connector to connect the engine control module (ECM) via the control network (CAN) bus, which in turn is transmitted to the ECM. The secure communication mode between the smartphone and the vehicle is carried out via the GSM network. Using a smartphone, the owner can lock or unlock the vehicle and detect it in case of theft. By reading the signal received by the mobile phone, the engine ignition can be controlled and tell owner to immediately lock or turn off the engine. And again, it will return to normal only after entering a strong password. The operation of this circuit is mainly dependent on the MEM sensor. The actual position of the MEM sensor should be 90 degrees with respect to the ground. If there is a change in the actual position of the MEM, a control signal will be sent to the ADC. The ADC converts the analogue signal to digital signal and sends this digital signal to the microcontroller.**

Keywords – Theft Control Unit, GSM, GPS, Control Area Network Bus (CAN), Engine Control Unit (ECU), Mobile Phone, Engine Ignition Control Module (ECM), Subscriber Identity Module (SIM), Data Encryption Standard (DES).

I. INTRODUCTION

The number of vehicle thefts is increasing in our country. Every year more than 45000 vehicles are stolen in our country, mainly in metropolitan areas and less than 10000 vehicles are identified according to reports by Government of India, New Delhi.

The rapid rate at which vehicle thefts has been increasing across the world has involved increasing thrust with in the field of auto anti-theft systems. This is especially true for Expensive vehicles and who those go behind the expensive cosmetic modifications. Vehicle anti-theft systems have two functions,

1) Identifying vehicle theft and controlling false alarms.
2) Alerting the vehicle's owner.

When developing an anti-theft system, the focus is on the same combination of the above functions. The most important feature is the vehicle's security from theft and it's provided with three levels of anti-theft production. First, only authorized persons are allowed to enter the vehicle using finger print reader. In advance, the finger prints of the owner and other authorised person are stored in database and when entering the vehicle, the scanned finger prints are verified using database. The Biometric schemes are used as the main layer production because the potentiality of their duplication is minimal. And additional vibration sensors are installed on all windows to prevent intruders from breaking the glass of the vehicle and entering it.

II. RELATED WORK

Triple DES uses 3 DES keys K1, K2 and K3, each key with 56 bits (excluding parity bits), for encryption. We can use smartphones to control and access vehicles [1]. Vehicles can be protected against theft by activating a password mechanism that prevents unauthorized access, and users can be notified of the state of the vehicle. Bluetooth can be used as a short-range communication mode for vehicle control, and safety algorithms can be applied to ensure safety [2]. Various types of threats to Bluetooth communication must be prevented to ensure secure communication, because Bluetooth is an insured communication device that has been eliminated using security algorithms. Secure communication can be used over wireless networks such as Bluetooth [3].

Commercially available vehicle anti-theft systems are very expensive. Vehicle tracking devices can integrate a GPS tracking system with an existing vehicle alarm system, or provide an alarm function when someone interferes with its

owner's vehicle [4]. This allows security threats to be detected before the vehicle is launched and enables vehicle tracking via the internet. The ability to track vehicles via the internet is addressed with global positioning satellites. Data such as global position, speed, and time (PVT) is transmitted over a cellular network. The information sent by the tracking tool is disseminated and stored in your personal confidential account or sent over a wireless network. The data is cross-referenced on a street level map for viewing [5].

The location information provided is a cross-reference to the nearest geographic address and is displayed in home / business address format. The main disadvantage of the current system is that the system only provides a broad geographic address scheme, provides and does not provide street addresses [6]. The speed of vehicles and machines is not controlled at all by the existing system, which exposes the vulnerability of the system, which only provides tracking [7].

III. CAN BUS

Controller Area Network (CAN) Bus is an automotive bus standard to enable microcontrollers and to communicate devices with one another in a vehicle without a host computer. Can bus could also be a message-based protocol specially designed for automotive applications. But it's now also utilized in other areas like aerospace, marine, industrial automation, and for medical equipment. CAN may be a standard serial bus with multiple masters for connecting ECUs.

A. CAN Architecture

CAN may be a multi-master serial bus standard for connecting Electronic Control Units (ECUs) also referred to as nodes. Two or more than two nodes are required on CAN network for communication. All nodes are connected with two wire bus. This bus uses two signals such as CAN high (CANH) and CAN low (CANL).

Each node requires following mechanisms.

1. **CPU** or network processor or the host processor
   - Host processor to decide what the message it receives means and what the message it wants to send itself.
   - Sensors, actuators, and control devices can be connected to the main processor.
2. ***CAN controller*:** is always an integral part of the microcontroller
   - **Receiving**: The CAN controller retains the serial bits received from the bus until the entire message is available, which can then be received by the host processor (usually the CAN controller that caused the interference).
   - **Sending**: The host processor saves it by sending a message to the CAN controller, which continuously sends the bits to the bus when the bus is free.
3. ***Transceiver*:**
   - **Receiving:** It converts the data stream from the CAN bus layer to the one used by the CAN controller. It usually has a protection circuitry to protect the CAN controller.
   - **Transmitting:** It converts the data stream from the CAN controller to the CAN bus layer.

B. Working Principle

Data messages sent from any node on the CAN bus do not contain an address from the transmitting node or any intended destination node. Instead, the content of the message is marked with a unique identifier on the network. All other nodes on the network receive the message and every performs an acceptance test on the identifier to work out if the message, and thus its content, has relevancy there to particular node. If the message is related, the message will be processed or else it is ignored [8].

This identifier is the main part of the CAN arbitration field located at start of each CAN message. The identifier identifies the type of message, but also the priority of the message. Bits in CAN messages can be sent high or low. Least Significant Bit always dominates, which means that if one node tries to send low and another node tries to send high, the results on the bus will be low. The transmitter node always listens to the current bus while transmitting. Nodes that send a high level to the arbitration field and detect a low level know it exists lost the arbitration. It stops sending, allowing another node with a higher priority message to continue without interruption. Two nodes on the network cannot send messages from the same identifier. If two nodes attempt to send a message with an equivalent ID at the same time, there'll be no arbitration working. Instead, one among the transmitting nodes will find that its message is corrupted from the outside of the arbitration field. The node will then use the CAN processing error, which in this case is the end [9].

IV. IMPLEMENTATION DESIGN

This section provides complete information on the design and implementation of theft control for an automobile, used to prevent or control theft of vehicles. Systems developed using embedded systems and nGSM / GPS technology.

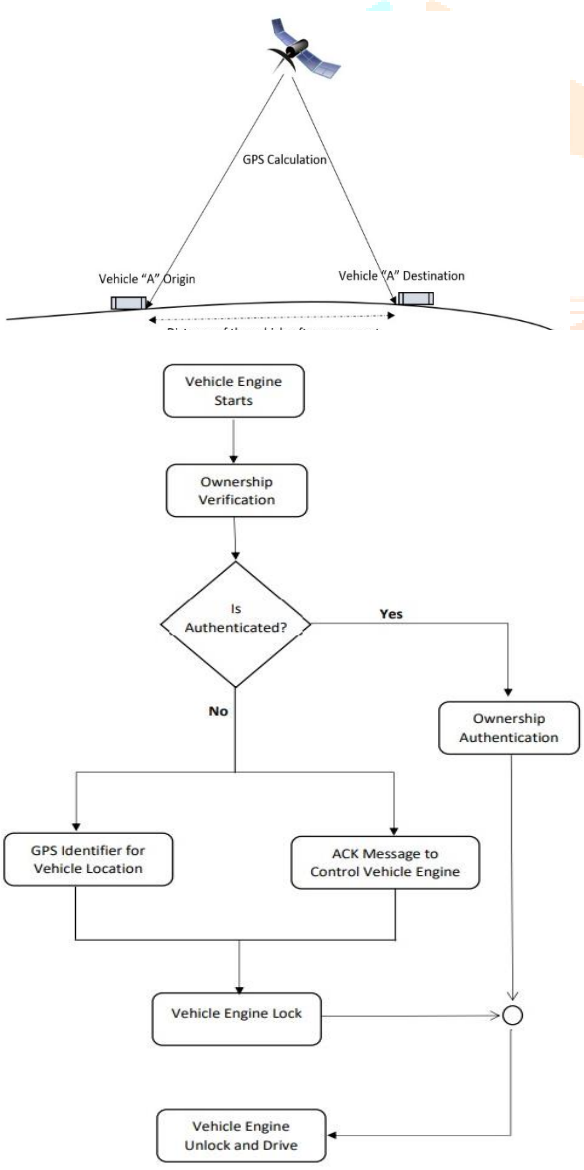
The proposed system installed in the vehicle can be easily controlled by the vehicle owner by sending messages from your mobile phone to the vehicle engine, interacting with CAN and GSM buses modem [10].

The proposed system is very reliable when there is a cellular network and a tracking device is connected, it is sending data to the server, when the network is not available the device data is stored in internal memory and will later send the saved data to the server where the network becomes available again. Vehicle tracking has been done by setting a box to a vehicle powered by batteries or connected to the vehicle's power system. For launching a detailed vehicle and tracking it is still the main method, but many companies are increasingly interested in the latest cellular technology for tracking various functions such as sales people and their

vehicles. The system also offers tracking the call, text and use of the internet use and usually provides many options [11].

A. Operating Principle

Every time the vehicle is started, a message appears with the GPS coordinates of the vehicle's location and send an SMS to the owner's number. RFID devices can be installed on vehicles to provide information about specific places such as hotels, hospitals etc., every time a vehicle crosses that instance. After receiving the message, the owner can send a response to the stopped key or anti-blocking to stop the vehicle. First the system checks and clarify the owner's number and then it checks the sent SMS and performs the related action. All these processes are achieved through the CAN Network. While the engine is on, it will send information to the main CAN node, which in turn, receives the coordinates of the associated location and generates an SMS. Upon receipt of the lock or anti-lock code, it will send



instructions to the slave node that performed the intended action. If the vehicle is in danger, then vehicle speed will be reduced by using a DC motor. While the buzzer also warns when vehicles are in danger [12]. The following figure 1 shows that overall architecture of the proposed research work.

Fig. 1. Overall Architecture Model for Vehicle Theft Identification

B. Vehicle Location Retrieval

There is two ways to find the location of the vehicle. Initially, the latitude and longitude of the vehicle must be obtained from the satellite.

$$Beat\ Phase = distance\ to\ vehicle + constant \quad \ldots(1)$$

The resulting latitude and longitude values are used for further calculations of geographic addresses using geocoders. Owners can pick up locations only after sending a private message. This separate message is set by its owner before using the system [13]. The above Eq.1 is used to measure the vehicle distance using phase is given.

Only after receiving the appropriate message code, the application will start the service. How confirmation, latitude, longitude and geographic address are sent to the owner. Portable networks become a concern because only when there is significant network coverage are there individual message and its receipt is possible. The design of the location search module is taken into account both network factors and user code validation. Only after receiving a confirmed code previously determined, the location is sent to its owner. Therefore, user code verification as well considered [14].

C. Vehicle Distance Measurements / Mathematical Expressions

Fig. 2. GPS Module for vehicle's distance calculation

Fig. 2. is to measure the vehicle distance from satellite [14]. The benefit of "single differencing" is to remove satellite clock bias. Consider the monitoring equations for two receivers, A and B, which detect the same satellite, j,

$$L_A^j = \rho_A^j + c\tau_A - c\tau^j + Z_A^j - I_A^j + B_A^j$$

$$L_B^j = \rho_B^j + c\tau_B - c\tau^j + Z_B^j - I_B^j + B_B^j \quad \ldots(2)$$

The single difference phase is defined as the difference between these two:

$$\Delta L_{AB}^j \equiv L_A^j - L_B^j$$

$$= \left(L_A^j = \rho_A^j + c\tau_A - c\tau^j + Z_A^j - I_A^j + B_A^j\right) -$$

$$\left(L_B^j = \rho_B^j + c\tau_B - c\tau^j + Z_B^j - I_B^j + B_B^j\right)$$

$$= \left(\rho_A^j - \rho_B^j\right) + \left(c\tau_A - c\tau_B\right) - \left(c\tau^j - c\tau^j\right) +$$

$$\left(Z_A^j - Z_B^j\right) - \left(I_A^j - I_B^j\right) - \left(B_A^j - B_B^j\right)$$

$$= \Delta\rho_{AB}^j + c\Delta\tau_{AB} + \Delta Z_{AB}^j - \Delta I_{AB}^j + \Delta B_{AB}^j \quad \ldots(3)$$

Haversine Formula is used to measure a distance between 2 coordinates and it separate into 4 columns Lat1, Lon1, Lat2, Lon2 in decimal degrees and the distance were calculated in meters [15].

$$Distance = 2 * 6371000 * ASIN\left(SQRT\left(\left(SIN\left((LAT2 * (3.14159/180) - LAT1 * (3.14159/180))/2\right)\right)^2 + COS\left(LAT2 * (3.14159/180)\right) * COS\left(LAT1 * (3.14159/180)\right) * SIN\left(\left((LONG2 * (3.14159/180) - LONG1 * (3.14159/180))/2\right)\right)^2\right)\right) \quad \ldots(4)$$

The simplified Haversine Formula is

$$Distance, d = 3963.0 * arccos\left[\left(sin(lat1) * sin(lat2)\right) + cos(lat1) * cos(lat2) * cos(long2 - long1)\right] \quad \ldots(5)$$

D. Engine / Fuel Control of the Vehicle

The design of the engine / fuel control module includes incentives to control the process. This incentive obtained through the owner's message. After obtaining the location of the vehicle, the owner can start or stop on the engine ignition. The calculated parameters are taken into account in this module receives a message from the owner about the need for further action. Other design parameters are considered a confirmation of the true fact of the message [16]. Design involves rework message only if it's from the owner. Even if the lock code is known to others, the lock cannot to be fulfilled. Owner has discrete control over engine ignition. The design includes controlling the ignition of engines located in remote locations by sending messages [17].

$$v_v[m/s] = v_w[m/s] = \frac{N_e \cdot \pi \cdot r_w}{30 \cdot i_x \cdot i_0} \quad \ldots(6)$$

The above equation is to calculate wheel speed, engine speed, gear box and differential gear ratios. If the speed is calculated in *kph* the formulas become:

$$V_v[kph] = V_w[kph] = \frac{3.6 \cdot N_e \cdot \pi \cdot r_w}{30 \cdot i_x \cdot i_0} \quad \ldots(7)$$

After receiving the message and checking its confirmation, the microcontroller sends a signal to reset relay to lock or unlock the engine. A SIM card on GSM installed to the vehicle for receiving the message and it forward the message to the microcontroller. MAX 232 will perform drive and receiver actions to forward messages to and from microcontroller as show in **Fig. 3**.

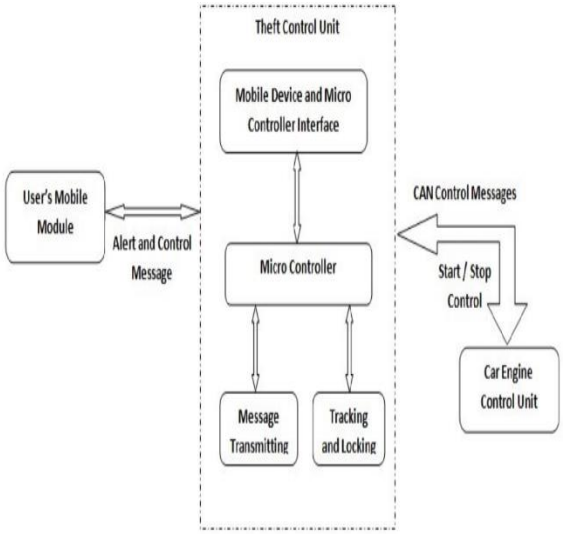


Fig. 3. Block Diagram of ECM

LCD is used for notification When a new message arrives, a message is displayed on the LCD. while the engine is locked or running. However, this kit is not required for use of a real system and is used for demonstration purposes only.

V. Result and Observation

This section provides the details of the experimental results of the proposed approach. The implementation of locking and unlocking of the vehicles using Can document is completed successfully. Communication works well, with no interruptions between different modules in the design. The design is made taking into account all the features and technical requirements. In Fig. 4 shows the Hardware part of this project. The kit consists ARM Controller, GSM module, Relay circuit and LCD are connected in one board and built in one board which is built to a vehicle control unit. The relay is connected to the Vehicle Engine Unit block.

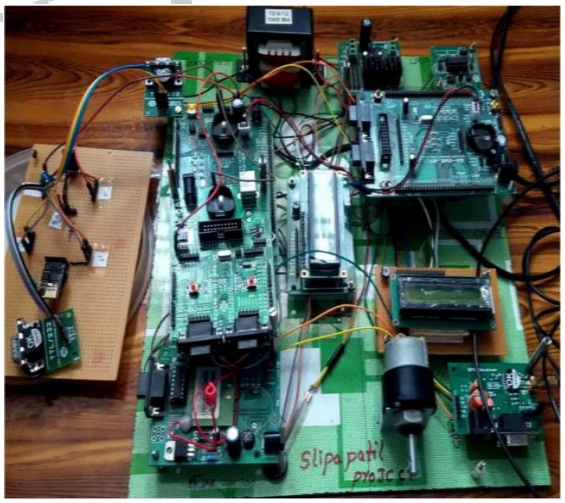


Fig. 4. Hardware Part

When the message "OFF" sent by the vehicle owner to a mobile phone inserted into the control system device, the controller displays a message on the LCD as shown in **Fig. 5** and activates the relay connected to the vehicle engine, which stops the fuel supply, thus blocking the vehicle engine with sends messages via the CAN bus in a readable CAN format.

Fig. 5. LCD Display "Engine Off"

Fig. 6: LCD Display "Engine On"

When the vehicle's owner sends an "ON" message to the mobile phone inside the control unit, the controller will display the message on the LCD as shown in Fig. 6 and activate a relay connected to the vehicle engine, which in turn enables fuel consumption by unlocking the vehicle engine by sending a message via the CAN bus.

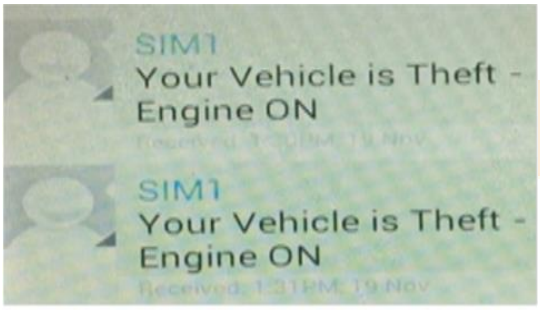


Fig. 7: Message Display

Fig. 7, 8 shows a message that displays in mobile and displays the location in terms of

latitude, longitude and the geographical address of the place [17].

Fig. 8: Location Details

VI. Features and Application

Features:

1) Long distance communication using a GSM modem from anywhere in the world.
2) GPS -based location determination.
3) Send locations in the form of latitude and longitude.
4) Automatic notification of the scene to the police / ambulance.
5) Theft control using GSM short message service.

Application:

1) VIP vehicle tracking.
2) Can also be used to track children or animals.
3) Vehicle safety applications.
4) Tracking ambulances.
5) Navigation system.

VII. Conclusion

The developed system during this paper for avoiding vehicle theft makes use of a mobile that's embedded within the vehicle with an interfacing to Engine Control Module (ECM) through Control Area Network (CAN) Bus, which is successively communicated to the ECM. The vehicle being stolen can be stopped by using GPS feature of mobile and this information is employed by the owner of the vehicle for future processing. The owner sends the message to the mobile which is embedded in the vehicle which has stolen which successively controls the vehicles engine by locking the working of the engine immediately. The developed system accepts the message and broadcasted to the Vehicle Network through CAN Bus. The engine is often unlocked only by the owner of the vehicle by sending the message again. The goal behind the planning is to develop security for vehicles and embedded system to speak with engine of the vehicle.

Acknowledgment

I'm (A. Divya), thanking Mr. Sanjay Sharma to guide me for circuit configuration and Mr. Gokul Rajan to help me on report generation. Finally, I would like to thank Mr. S. Ponmaniraj for supporting me in all the way of my entire research work.

References

[1] LI Gangyan, Xu Jun, "An Information Acquisition Method of City Bus Integrated Control Network", IEEE Computer Society, 2008.
[2] Ganesh G.S.P, Balaji B and Varadhan T.A.S, "Anti-theft Tracking System for Automobiles", IEEE International Conference on Anti-counterfeiting, Security and Identification (ASID), 2011.
[3] Huaqun Gao, Cheng H.S, Wu Y.D and Venkatasubramanium A.K, "An Automotive Security System for Anti-theft", Eighth International Conference on Networks, 2011.
[4] Sadagopan V.K, Rajendran U and Francis A.J, "Anti-theft Control System Design using Embedded System", IEEE International Conference on Vehicular Electronics and Safety (ICVES), 2011.
[5] Amol S. Dhotre, Abhishek S. Chandurkar and S. S. Jadhav, "Design of a GSM Cell-Phone Based Vehicle Monitoring & Theft Security System", International Journal of Electrical and Electronics Engineering (IJEEE), 2012.
[6] Feng Huang, Shanyu Tang, and Jian Yuan, "Vehicle Location Based System", IEEE Transactions on no information forensics and security, 2011.
[7] Bhagavathy P, Dhaya R and Devakumar T, "Real-Time Car Theft Decline System Using ARM Processor", Third International Conference on Advances in Recent Technologies in Communication and Computing, 2011.
[8] CAN in Automation (CiA), Controller Area Network (CAN). Avaliable: http://www.cancia.org.
[9] Karan Siyal and G. Gugapriya, "Anti-Theft Vehicle Locking System using CAN", Indian Journal of Science and Technology", 2016.
[10] Daniel Switkin, "Android Application Development", 2010.
[11] Ch. Bhanu Prakash, K. Sirisha, "Design and Implementation of a Vehicle Theft Control Unit using GSM and CAN Technology" International Journal of Innovative Research in Electronics and Communications (IJIREC), 2014.
[12] Korivi Soumya, "Anti-Theft Security System for Vehicles using Embedded Controller", International Journal of Current Engineering and Scientific Research (IJCESR), 2018.
[13] http://www.nbmg.unr.edu/staff/pdfs/blewitt%20basics%20of%20gps.pdf
[14] Ms. S.S. Kanase et.al., "GSM & GPS Based Vehicle Theft Control System", International Research Journal of Engineering and Technology (IRJET), 2018.
[15] https://www.geeksforgeeks.org/program-distance-two-points-earth/
[16] https://www.movable-type.co.uk/scripts/latlong.html

[17] https://x-engineer.org/automotive-engineering/chassis/vehicle-dynamics/calculate-wheel-vehicle-speed-engine-speed/

[18] Shilpa Patil, Dr. Sarika Tale, "CAN Based Control of Theft Vehicles", International Journal of Science and Technology Research (IJSETR), 2016.