Advances in Automobile Engineering
ISSN: 2167-7670

Haider et al., Adv Automob Eng 2017, 6:3
DOI: 10.4172/2167-7670.1000169

Research Article Open Access

# A Smart Wireless Car Ignition System for Vehicle Security

**Arslan Haider, Aamer Anwer Hayat Khan and Mouloud Denai***

*Department of Engineering and Technology, University of Hertfordshire, Hatfield, Hertfordshire, UK*

**Abstract**

The paper proposes a novel car ignition system to replace the traditional wired technology and enhance vehicle security. This new system uses wireless transmissions to start the engine and hence eliminates the ignition wire behind the dashboard. It also allows the user to set a password of his/her choice to keep the system protected. A theft alarm that goes ''ON'' when an unusual activity is sensed and/or when the wrong password is attempted to unlock the system is integrated in the system. Moreover, important factors such as economic feasibility, adaptability to the new vehicle technologies and customers' preferences have been taken into consideration in the design of the proposed vehicle security system.

**Keywords:** Ignition system; On-board diagnostics (OBD) port; Password; Security; Wireless; Arduino board; Bluetooth

## Introduction

Car theft has become a source of concern in almost all parts of the world. This is, very often, the case of countries facing social crisis such as extreme poverty and unemployment. These problems give rise to further predicaments and robbery is one of them. According to the World Bank statistics, 71% of the world's population live with an income of $10 dollar a day or less [1]. In Pakistan, around 21,000 cars are stolen every year, whose overall cost is estimated at 5 Billion (PKR) [2]. In India, about 44,000 vehicles have been stolen over the last three years. In 2013, an estimated number of 699,595 cars were stolen in USA [3]. Because of this escalating phenomenon, vehicle owners have expressed deep concern on how to protect their cars against this serious offense.

Current popular anti-theft systems include vehicle tracking and alarming systems. These security systems generally involve usage of immobilizers, alarm systems, GPS and some basic steering wheel locks to prevent vehicles from being stolen. However, there are certain limitations and major security gaps that these technologies are not able to deal with and thus, theft and robbery of cars still occurs. The major reason behind this is the lack of up-gradation and adaptability of the security systems to the latest technologies that makes it easier for professional thieves to overcome. These robbers not only steal the car but also go a step ahead by re-selling the vehicles' parts [4]. Moreover, greater costs are incurred in the purchase and maintenance of these systems. For example, GPS system often comes with a yearly monitoring fee. Yet despite spending huge money on these systems, car theft rate does not seem to be declining. Therefore, some circuit is required to protect the starting mechanism of the cars to make them safe.

The authors propose an improved vehicle security solution to overcome all the problems stated above. It converts the wired ignition system to wireless with antitheft features.

The remaining of the paper is organised in five sections. Section II, presents an overview of the proposed security ignition system. Section III presents the design and implementation techniques of the system. Section IV describes the optional features available to the users. Finally, the results and conclusions are presented in Section V and VI respectively.

## System Overview

This system is designed to overcome most of car theft techniques and prevents the car from theft and damage. It has been observed that the car security system currently in the market is not efficient enough to prevent 100% theft. An extensive research has been carried out to determine the reason behind the escalating number of cars stolen [4]. The conclusion was that the major problem of theft is car ignition wire which is connected to the On-Board Diagnostics (OBD) Port of the car. If OBD Port of the car can be reset by numerous devices available in the market, hence the security of the car ignition system has the chances of being compromised. This is because car OBD works as "the brain" which controls all the functionalities of the car. Moreover, there are other reset systems available online that companies offer only for registered garages to fix their car problems but are also easily accessible by thieves who use them to steal cars. Therefore, in order to prevent this situation, a new system is introduced having 'two brains' in the car to control the mechanisms of the car and to provide double security to the car ignition. In this system, ignition wires are not controlled using OBD port but will have their own computer or brain. Another new concept of modular vehicles can also be included where there is not a single wire in the car and every component has its own circuit which will interact with the brain of the computer using wireless communication. In many cases, thieves just hotwire the old cars and steal them [5]. Similarly, in GSM tracking security systems, the alarm wire is pulled first followed by the usage of an anti-tracker device to block the GSM signals which then makes it easier for thieves to take away the car. Moreover, programmable laptops that reset the computer of immobilizers and electronic key security cars, which result in quick thefts, are also being used.

While developing this project, all these system bugs and loopholes including economic benefit for the consumers have been considered in order to develop a better and much cheaper security system (Figure 1).

This system will be incorporated in the car audio system or the LCD

***Corresponding author:** Mouloud Denai, Department of Engineering and Technology, Mouloud Denai, University of Hertfordshire, Hatfield, Hertfordshire, UK, Tel: +44 (0)1707 284800; E-mail: m.denai@herts.ac.uk

**Received** August 07, 2017; **Accepted** September 15, 2017; **Published** September 19, 2017

**Citation:** Haider A, Anwer A, Khan H, Denai M (2017) A Smart Wireless Car Ignition System for Vehicle Security. Adv Automob Eng 6: 169. doi: 10.4172/2167-7670.1000169

unit and will also act as another brain or primary side of the security system, without any interaction with the car OBD Port. And both sides have microcontroller within them (Figure 2).

The ignition system of the car is converted to wireless with password feature so that it cannot be Hotwired. The signal-blocking device (Anti Tracker device) will prevent car thefts to a greater extent. Moreover, unlike immobilizers, it cannot be reset through any port. The car audio system is connected to the switch of the car through wires, which are then wirelessly connected to the engine, therefore completely abolishing the concept of hotwiring in the car (Figure 3).

The user will have to apply the correct password in order to establish the wireless connection between the switch and an engine. This is done by moving the key in car's switch followed by the transmission of a special signal from the primary to the secondary unit, which on matching the correct password, will allow the car to start. Both control units consist of bluetooth module for wireless transmission and both of

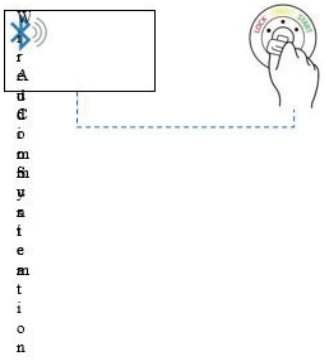

**Figure 1:** Primary side (switch side).

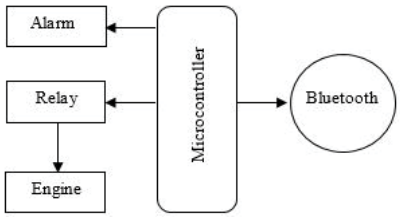


**Figure 2:** Secondary side (engine side).


**Figure 3:** Block diagram.

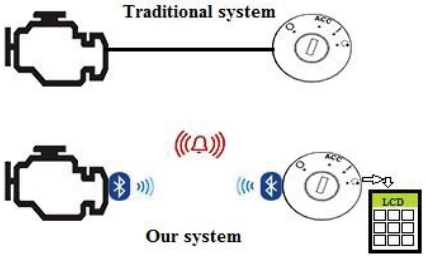


**Figure 4:** Comparison of traditional system with our system.

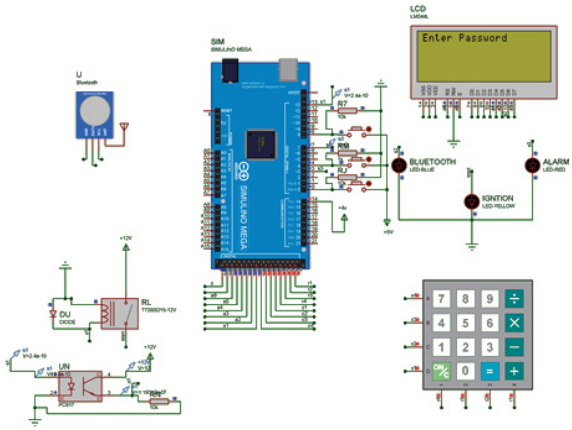


**Figure 5:** Proteus diagram of the primary side.

these systems are placed safely behind the dashboard in a place where the intruder or thieves will have to use hard tools to access by cutting the body of the car which will result in excessive noise, risk, time and effort.

## System Design and Implementation

By default, the spark ignition and the fuel pump circuits of a car are open [6]. Initially, the system starts working from the password. As the user sits in the car and moves the ignition key, a customized audio system asks for the password. The key switch is connected to the customized audio system of the car through wired connection, which further connected to 12 V power supply to turn ON the audio system upon moving of key. When the password is entered correctly, a wireless connection is established between the engine and primary side (car audio system). Then, if the user wants to start the car then he/she will have to turn the key again. However, the car will not get started if the wrong password is attempted.

This security system basically focuses on the wireless ignition starting of a car. Therefore, there is no chance of any interruption between the established connections which also made it more secure. In this system, there is no ignition wire behind the speedometer or dashboard as in all cars. This system is designed in such a way that other customized features can also be added according to the consumers' requirements. These features may include a GPS and GSM system, camera for face detection, usage of android technology for controlling the car through a mobile phone. However, such add-ons features will incur extra costs (Figure 4).

## Discussion

### Demonstration and working of the system

The purposed system has been successfully tested first on computer using Proteus Software for simulations and then on a vehicle. The primary side consist of key switch, arduino microcontroller, LCD, keypad and bluetooth module. The key switch is wired to the LCD

which is supplied from the 12 V car battery. A Proteus implementation of the primary and secondary side of the system are shown in Figures 5 and 6 respectively.

The secondary side consist of Arduino microcontroller, relay system, alarm and the bluetooth. The relay further connected with ignition wires of the car (Figure 6).

As the key is moved, the LCD system turns on and shows the display

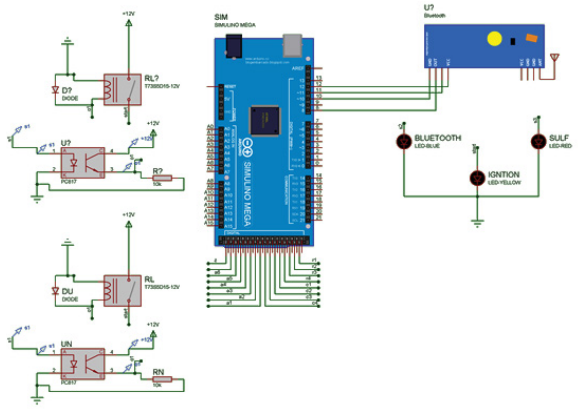


**Figure 6:** Proteus diagram of the secondary side.


**Figure 7:** Receiving code in serial communication.


**Figure 8:** The primary control unit functions password on the given key position, when the key is moved in switch for the first time.

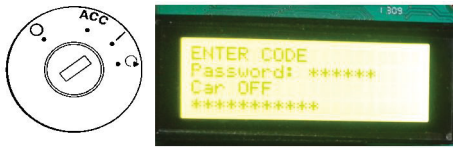


**Figure 9:** The primary control unit functions password is correct; a wireless connection will be established.

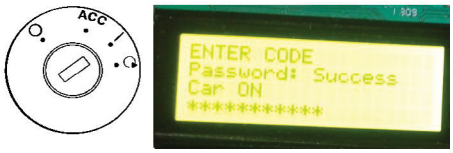


**Figure 10:** The primary control unit functions correct password and moving the ignition key to the next position this causes the fan, AC and other car accessories to be turned on.

of entering password. As the correct password is being verified by the system, a connection is established between the two control units. This is the result of serial communication, which after receiving the correct password on the transmission, enables the receiver end to receive a "tb" to perform the function and in the same way different codes are fed in the system via programming so as to perform different functions.

On every single step a different code is sent via Bluetooth and upon receiving the desired code, the receiver end performs the function accordingly (Figure 7).

Once the password is successfully verified, the wireless connection is established. As the user moves the key further in switch, a code will be sent to the engine side circuit which triggers the relay circuit for controlling the car ignition and other things like AC and fan etc. and the alarm circuit. Now as the key is standing on second point of the switch so the AC and fan will be turned on. Moving the key further in the switch will send another code to the engine, which in turn switches on the car engine and starts the car. Moreover, the primary side microcontroller also checks the state of the key in the switch before sending the write code.

Now to turn off the car, the user again moves the key backward. A code will then be sent from the audio system (primary side) and the engine will be turned off. However, the wireless connection will not be lost until the key is fully moved back. Once the key is fully turned backwards, the wireless connection is disabled and to start the car again, the process should be repeated. However, multiple wrong password attempts or intrusion into the system will be sensed and generate an alarm. The Primary control unit functions are carried out in the following sequence:

1. The system asks for password on the given key position, when the key is moved in switch for the first time (Figure 8).

2. The password is entered into the system. If the password is correct, a wireless connection will be established (Figure 9).

3. Upon receiving the correct password and moving the ignition key to the next position this causes the fan, AC and other car accessories to be turned on (Figure 10).

4. Moving the Ignition key towards car ignition position will start the engine and the key is released as in the conventional starting mechanism (Figure 11).

5. Now the car engine is on.

Once the car is started, the system goes back to the previous stage by displaying that the car is "ON" and when a user switches the key backward towards "ACC" it will turn off the engine. All the starting mechanism of the car remains the same except the way the engine is started. Working result of the prototype can be seen on the link below https://www.dropbox.com/s/0psjbxx95hufhd3/Video%20editing.mp4?dl=0.

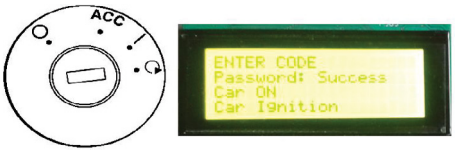


**Figure 11:** The primary control unit functions Ignition key towards car ignition position will start the engine and the key is released as in the conventional starting mechanism.

## Conclusion

In this project, a novel security system for starting a vehicle is proposed. The system is based on wireless technology and uses a password-protected technique to enhance the car security and prevent automobile theft. The car wireless ignition security system has been successfully designed and tested. The system can be easily upgraded with GPS and GSM modules to determine the location of the car and turn Off and on its car engine with SMS. Furthermore, by using android technology and IoT, the car can be controlled through a smartphone. The proposed system will improve the security and reduce theft. Alternatively, to the password system, a face recognition system can be implemented. It will detect the face of the owner of the vehicle as soon as he moves the ignition key and all the remaining mechanism remains the same. In addition, if an unauthorized user sits in car, the camera captures his/her image and sends it to the owner using GSM Module through GPRS.

### References

1. Luhby T (2015) 71% of the world's population lives on less than $10 a day, New York, USA.
2. Nurul HS, Arun KB (2013) Vehicle monitoring and theft prevention system using ARM. Int J Adv Res Techno 2: 992-997.
3. Omer AI (2013) Development of a microcontroller based security lock for a car engine. Proceedings of the Global Virtual Conference, ISBN: 978-80-554-0649-7.
4. Kamkar S (2015) Drive it like you hacked it: New attacks and tools to wirelessly steal cars. Presentation at DEFCON, Las Vegas, USA.
5. Koscher K, Czeskis A, Roesner F, Patel F, Kohno T, et al. (2010) Experimental security analysis of a modern automobile. In 31st IEEE Symposium on Security and Privacy (S&P 2010), IEEE Computer Society. pp. 447-462.
6. Garcia FD, Oswald D, Kasper T, Pavlidès P (2016) Lock it and still lose it-on the (In)security of automotive remote keyless entry systems, 25th USENIX Security Symposium, Austin, USA.