International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 10, October-2019

Wireless Access Control System for Automobiles

Chakradhar.B
Electronics and Communication Department
PESIT-Bangalore South Campus,
Near Electronic City, Bangalore-560100,
Karnataka, India

Grandhi Pavan Kumar
Electronics and Communication Department
PESIT-Bangalore South Campus,
Near Electronic City, Bangalore-560100,
Karnataka, India

Kakumanu Venkata Sai Sumanth
Electronics and Communication Department
PESIT-Bangalore South Campus,
Near electronic city, Bangalore-560100,
Karnataka, India

***Abstract*—Automobiles are considered to be one of the most valuable properties to own. Higher the value of any property, greater will be the risk of losing it and therefore, more difficult to safeguard. Anti theft system for automobiles aims at reducing the percentage of automobile thefts by 93 % by using components like a microcontroller, GSM (Global system for mobile), FSR (Force sensitive resistor) and Wi-Fi module. The default inbuilt lock system of the vehicle can be replaced by this system. The entire system that is placed in the vehicle communicates using GSM to the user's mobile application and police station. With minor modifications, this system can be implemented in any kind of automobile.**

Keywords—GSM; Wi-Fi Module; Mobile Application

I. INTRODUCTION

An anti-theft system is any device or method used to deter the unauthorised appropriation of items considered valuable. From the invention of the first lock and key to the introduction of Radio Frequency ID tags and biometric identification, anti-theft systems have evolved to match the introduction of new inventions to society.

The main objective of this project is to develop an anti-theft security system for automobiles. The demand for automobiles is growing day by day and the ever increasing demand has also caused many thefts. On an average, 1.65 lakh vehicles are stolen each year in India and 7.21 lakhs of vehicles in the US. When an automobile is thieved, repossession of that has become a complicated task. This means that the safeguards provided by the manufacturers are not up-to the mark. Antitheft systems are needed to be foolproof and they should be designed in such a way that, they should be controlled by the user from the farther distances.

How is our system different?

There are many systems available in the market today to safeguard automobiles. However, the technology used today continues to involve the use of the “key system” directly or indirectly.

Our system takes the existing technology to a new level by incorporating smartphones as keys. In the existing technology, there is no real time user-system communications. This limitation is greatly overcome with our system with specific communication modules.

II. DESCRIPTION

The components used for our project are:

A. Microcontroller(Arduino ATMega)
B. Wi-Fi module (ESP8266)
C. GSM module (SIM 900A)
D. Force Sensor

A. Arduino ATMega

The ATMega 2560 used in this system have 54 digital input/output pins with 16 analogue inputs. The entire system works on signals received or sent by this Microcontroller. This board is compatible with most shields designed for the Uno and the former boards.

B. ESP8266

The ESP8266 is a low-cost small Wi-Fi module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes style commands (i.e. AT commands).

Features:

- 32-bit RISC CPU running at 80 MHz
- IEEE 802.11 b/g/n Wi-Fi
- 16 GPIO pins

C. GSM/GPRS SIM 900A

This UART modem is built with dual-band GSM/GPRS engine-SIM900A works on frequencies 900/1800 MHz. this modem allows you to connect 5V and 3V3 microcontroller directly with any level conversion chips. The baud rate is configurable from 9600 to 115200 through AT commands.

D. Force Sensitive Resistor (FSR)

This is a special type of resistor, whose resistance value varies with respect to the force applied. The FSR is made of 2 layers separated by a spacer. The more one presses, the more the Active Element dots in the flexible substrate touches the semiconductor and makes the resistance go down.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

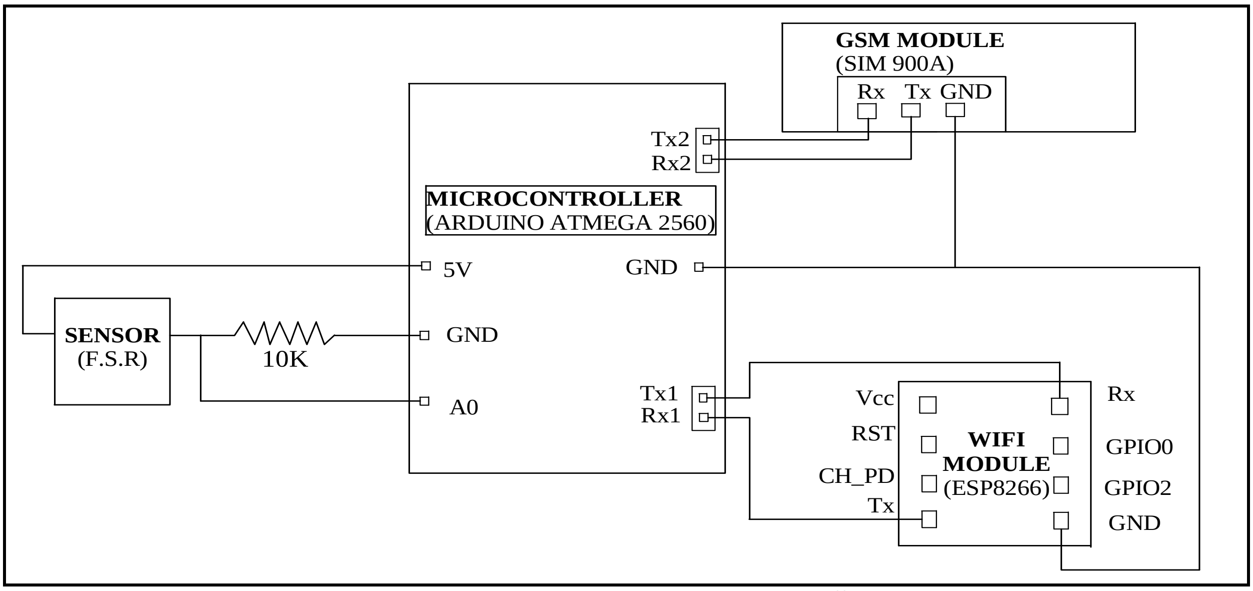

Figure 1: Circuit diagram showing the connections between different modules

App description

Our android application is used to send messages and receive text messages in order to communicate with the user in real time. The app sends encrypted messages in order to ensure that only the authenticated user is altering the system configurations. In the app, there is a provision to enter the phone number of the GSM module which acts like the password to the system. The app has two main buttons that are used to send messages. The first button in the app is called as the check status button. Check status button is basically used in order to let the user know in which mode the system is currently in. The second button is the ignore button that is used only if the user does not wish to alert the police station. The app developed uses Java API and android studio for coding.

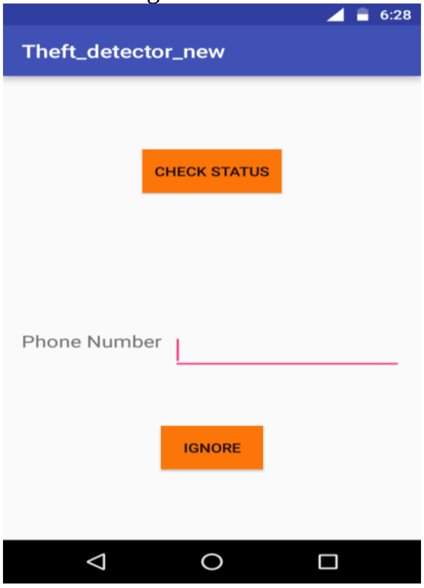

Figure 2: The screenshot of the app designed

III. WORKING

There are 2 modes in the working of this system.

A. Drive Mode

B. Away Mode

With reference to the block diagram (Figure 3), if the ESP8266 is connected to the hotspot created by the user the Wi-Fi module keeps monitoring the signal strength. Depending on the signal strength, the Arduino switches between the two different modes. If the vehicle is in the away mode, then Arduino deactivates the fuel supply and will monitor the force on the FSR. If the force exceeds a threshold value (indicating that some intruder is using the vehicle), a message and a call will be sent to the user’s mobile with the help of GSM. Depending upon the user’s input, via the mobile application, the arduino decides whether to inform the police station about the theft or not. This is done through a dedicated app. After the sequence depicted by the block diagram is executed completely, the ardruino and the Wi-fi module resumes back to check the Wi-Fi signal strength.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

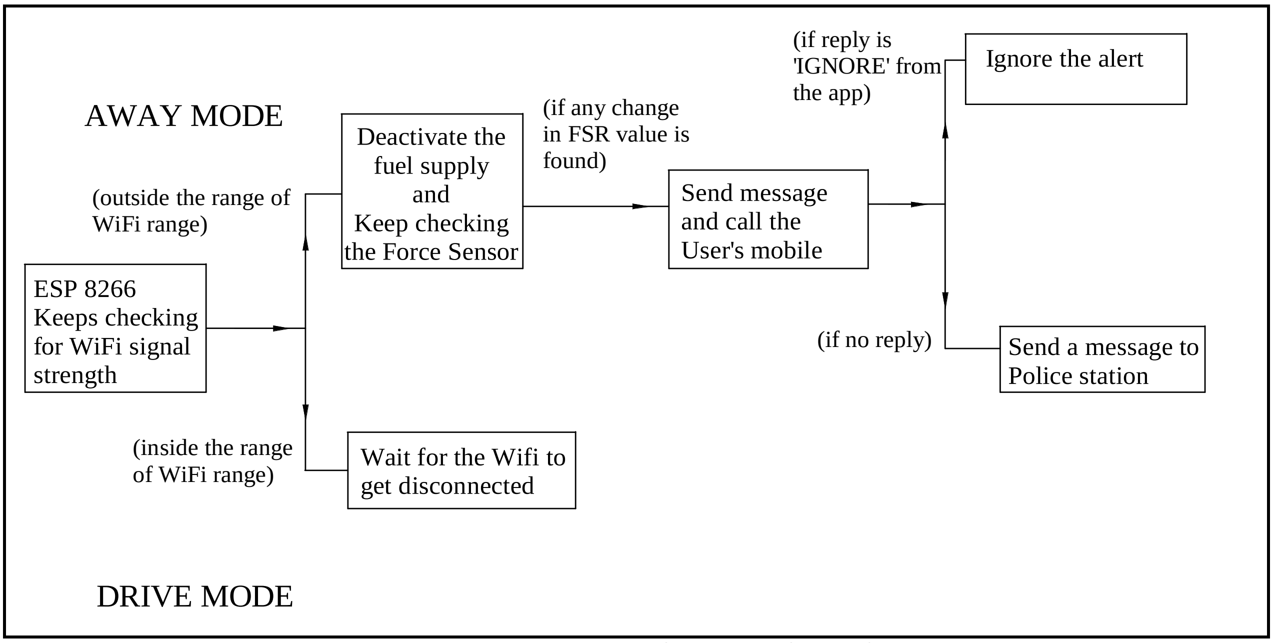
AWAY MODE
(outside the range of WiFi range)
ESP 8266 Keeps checking for WiFi signal strength
Deactivate the fuel supply and Keep checking the Force Sensor
(if any change in FSR value is found)
Send message and call the User's mobile
(if reply is 'IGNORE' from the app)
Ignore the alert
(if no reply)
Send a message to Police station
(inside the range of WiFi range)
Wait for the Wifi to get disconnected
DRIVE MODE

Figure 3: Block Diagram showing the functionality of anti-theft system

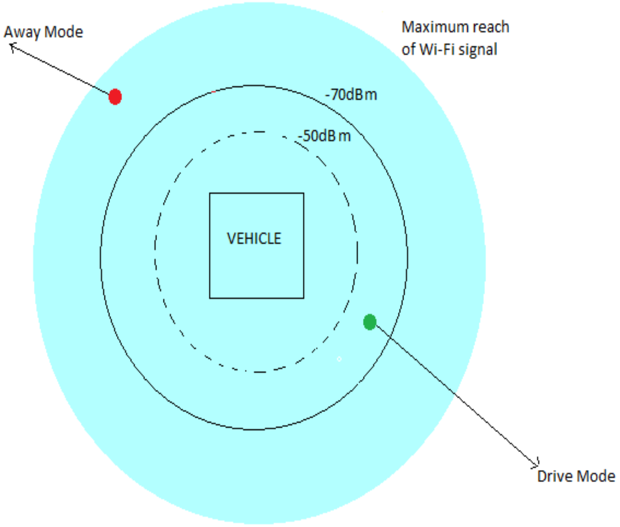

Figure 4: Wi-Fi range to distinguish the modes of operation

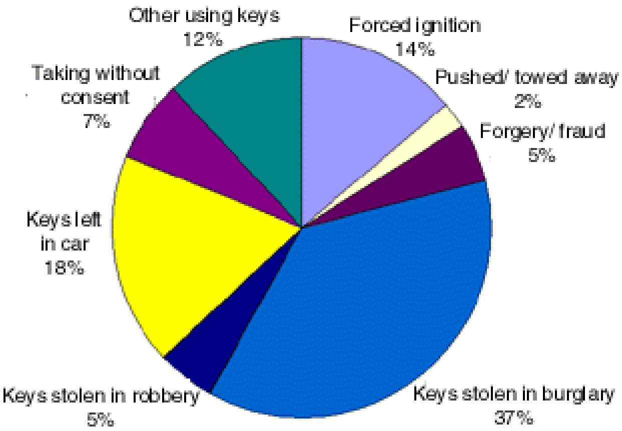

Figure 5: Statistics showing thieving of automobiles.

IV. CONCLUSION

The statistics shown in figure 5 indicates that a majority of the thefts that have occurred are primarily due to keys stolen in a burglary, other using keys and forced ignition. With our new app system and efforts to eliminate the key system results in a drop of a whopping 93 percent. This translates to a reduction of the number of vehicles thieved in India by 1.53 lakhs and by 6.7 lakhs in the US.

Our system can be further improvised to avoid the remaining 7% of the thefts occurring due to “taking vehicles without consent” by installing GPS systems.

ACKNOWLEDGEMENT

We are highly thankful to our learned faculty Dr. Revanasiddappa and Mr. Pattabhi Raman for their guidance, encouragement and co-operation throughout the completion of this paper. We sincerely thank our parents for their support. Lastly, we thank our beloved principal J. Surya Prasad and the management of PES Institute of Technology-Bangalore South Campus, Bangalore.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

REFERENCES

[1] https://en.wikipedia.org/wiki/Anti-theft_system

[2] http://www.circuitstoday.com/interface-gsm-module-with-arduino

[3] https://www.thenewboston.com

[4] https://www.arduino.cc/en/Main/ArduinoBoardMega2560

[5] IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - IEEE 802.11-2016

[6] M. Rahnema - Overview of the GSM system and protocol architecture, IEEE Communications Magazine (Volume: 31 , Issue: 4 , April 1993)

[7] AT command set for User Equipment (UE) (3GPP TS 27.007 version 10.3.0 Release 10), ETSI (European Telecommunications Standards Institute)

(This work is licensed under a Creative Commons Attribution 4.0 International License.)