International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 2, Issue1

Improvement in Automobile Security System Controlled by Personal Computer via RF Link

Dependra Nath Saikia, Abhilasha Choudhary, Aditi Sardesai

***Abstract*— This article presents an accurate, fast and very efficient Automobile (especially Car) security system which will improve the owner's ease. This system is based on wireless sensor network (WSN). A WSN consists of distributed autonomous sensors to monitor physical conditions such as vibration, pressure, motion and to cooperatively pass their data through the network to a main location. Previously Remote Keyless Entry (RKE) System was developed which provides door locking and ignition starter, which had drawbacks. To overcome them Car Security System (CSS) can be developed and this is achieved by employing locking techniques and wireless sensors inside the car. Locking techniques include Central locking, Ignition circuit breaker, Fuel supply lock and Transmission lock. Different wireless sensors utilized are Tilt sensors, Pressure sensors which continuously monitor the physical changes occurring in the car, communicated with the Electronic Control Module (ECM) having software CSS controlled by owner's computer via (49 MHz) RF link.**

***Index Terms*— CSS, RF, RKE, WSN.**

I. Introduction

The recent tremendous growth in car thieves leads to develop security systems which can rang the alarm as well as protect the car. Due to this, car companies develop remote keyless entry system. An RKE [1] system consists of an RF transmitter in the key fob (or key) that sends a short burst of digital data to a receiver in the vehicle, where it is decoded and made to open or close the vehicle doors or the trunk via receivercontrolled actuators. The wireless carrierfrequency [7]is currently 433.92MHz (ISM band) inIndia. In India the modulation is frequency-shift keying (FSK), but in most other parts of the world, amplitude -shift keying, orASKisused.The carrierisamplitude modulated between two levels: To save power, the lower level is usually near zero, producing complete on-off keying (OOK).

In the vehicle, an RF [4] receiver captures that data and directs it to another microcontroller, which decodes the data and sends an appropriate message to start the engine or open the door. Multi-buttons key fobs give the choice of opening the driver's door, or all doors, or the trunk, etc.

The digital data stream, transmitted between 2.4kbps and 20kbps, usually consists of a data preamble, a command code, some check bits, and a "rolling code" that ensures vehicle security by altering itself with each use. Without this rolling code, your transmitted signal might accidentally unlock another vehicle or fall into the hands of a car thief who could use it to gain entry later.

RKE [6] is strictly a short-range technology, up to 20 meters, or 1 to 2 meters for passive RKE systems. Ensuring even a short transmission distance on low power and a low-cost design budgetcan be

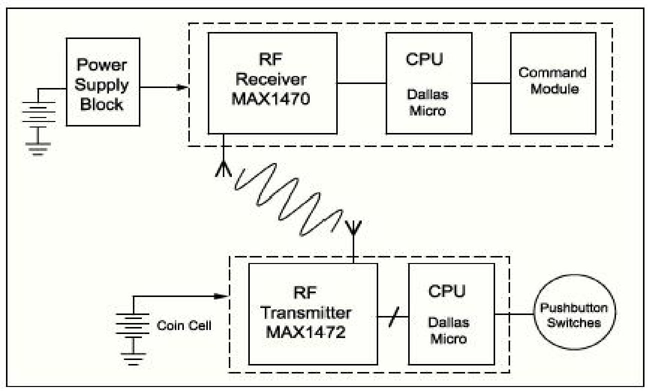

Figure 1.1: An RKE system consists of a key fob circuit (lower part of the figure) transmitting to a receiver in the vehicle (upper part of the figure).

challenging the RF circuitry. For simplicity, the transmitter and receiver antennas consist of a circular or rectangular loop of copper trace on a small PC board, with a simple LC network to match the antenna impedance to the transmit or receive chip.

The system [5] shown in fig.1.1 uses 8-bits rolling code. The transmitter's and receiver's controller chip has a memory location that holds the current 8-bit code. When you push a button on your key fob, it sends that 8-bit code along with a function code that tells the car what you want to do (lock the doors, unlock the doors, open the trunk, etc.).

Both the transmitter and the receiver use the same pseudo-random number generator. When the transmitter sends a 40-bit code, it uses the pseudo-random number generator to pick a new code, which it stores in memory. On the other end, when the receiver receives a valid code, it uses the same pseudo-random number generator to pick a new one. In this way, the transmitter and the receiver are synchronized. The receiver only opens the door if it receives the code it expects.

If you are a mile away from your car and accidentally push the button on the transmitter [2], the transmitterandreceiverareno longer synchronized. The receiver solves this problem by accepting any of the next 256 possible valid codes in the pseudo-random number sequence. This way, you (or your three-year-old child)could "accidentally" push a button on the transmitter up to 256 times and it would be okay -- the receiver would still accept the transmission and perform the requestedfunction.However,ifyou accidentally push the button 257 times, the receiver will totally ignore your transmitter. It won't work anymore.

But this system has limitations, like:

- It wouldn't work more than 20m range [3].
- If a thief monitors the signal sent by the same key fob for 20-30 times, then he could easily understand the pattern of code generation by the pseudo code generator and easily copy on Radio Frequency transmitter.
- Desynchronizing problem causes headache to the user.

II. PROPOSEDCARSECURITYSYSTEM

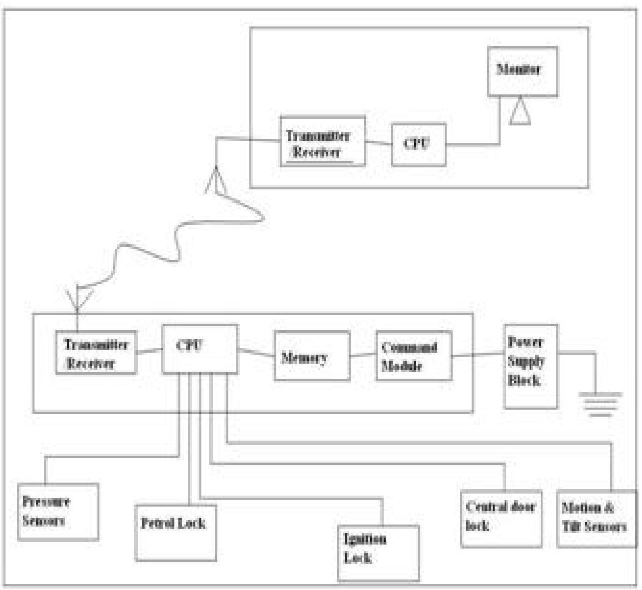

Figure 2.1: Proposed car security system.

In the above figure 2.1, there are two parts: one at the computer side and the other at the car side. Now at the car side, the ECM comprises of Transmitter/Receiver, CPU and Memory module. At the computer side, CSS software controls all operations of ECM. It communicates with the Receiver/ Transmitter at the computer side through RF Link. Moreover, the CPU at the ECM commands the various locks and sensors connected to it. ECM is mounted on the lower part of the bonnet.

A. *Different Locks and Sensors Utilized-*

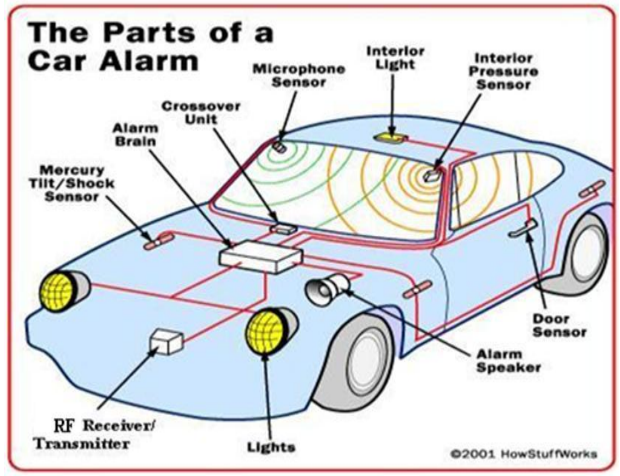

Figure 2.2: Various sensors used for car security

1) *Centraldoorlock*

Figure 2.3: An actuator used in modern cars.

The locking/unlocking of power doors lock is actually performed by actuators shown in fig.2.3.These are placed in the doors. Two types of actuators are in common use:

1. Solenoid: The solenoid is an electromagnetic switch. It locks the doors when current passed in it by the ECM in one direction and unlocks when the direction of current is reversed.

2. Motor: In place of solenoid, DC motors can also be used as actuator as shown in fig.2.4. The rotary motion of the motor is converted to linear motion by means of rack and pinion mechanisms. Again by changing the directions of current rotation direction of motor is changed .Thus it locks for one direction of current decided by the ECM and unlocks for opposite direction.

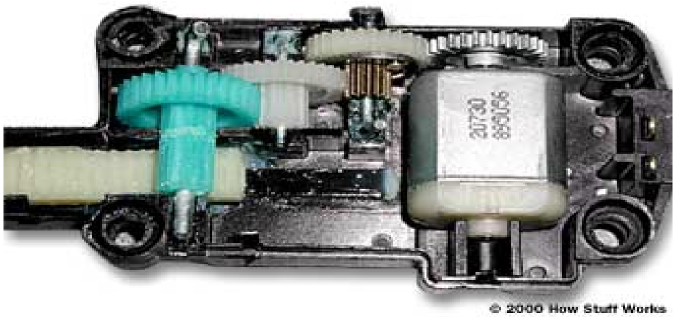

Figure 2.4: Internal view of actuator

2) Ignition Lock

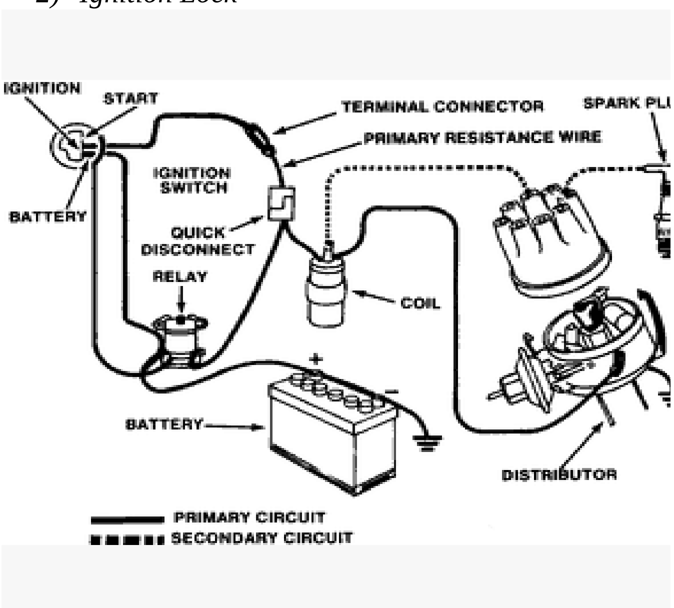

Figure 2.5: Ignition circuit of a car.

An ignition system is mainly a circuit comprising of battery, relay, connector to crank shaft shown if fig.2.5. Until completion of circuit, it will not work; this feature is used in ignition lock system. Even if key is inserted and Relay is not on, circuit not completed. Relay is controlled by Car Electronic Control Module (ECM).ECM is command by car's owner computer.

3) Fuel SupplyLock

As Shown in fig.2.6, Motor controlled valve is present in the pipe from petrol tank to engine. The motor's linear movement is used to open/close the valve. When relay is magnetized, it completes the circuit and motor works in forward direction to close the valve.

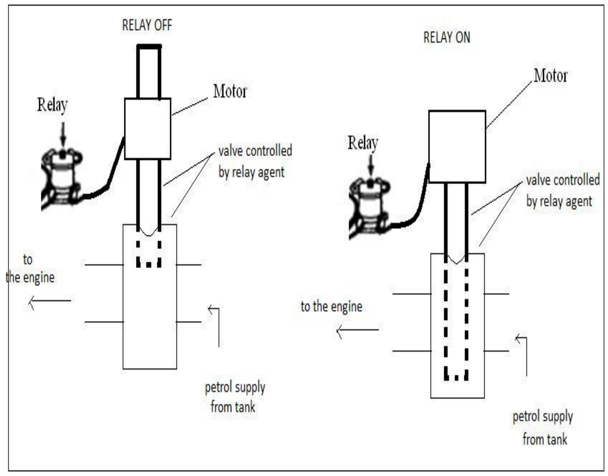

Figure 2.6: Relay controlling the valve in petrol pipeline by using motor.

When relay is demagnetized, motor gets positive charge from current line and open relay connection work as ground and circuit is complete, motor works in reverse direction and open the valve.By this, if a thief able to break the ignition break then also he couldn't start the car.

4) Transmission Lock

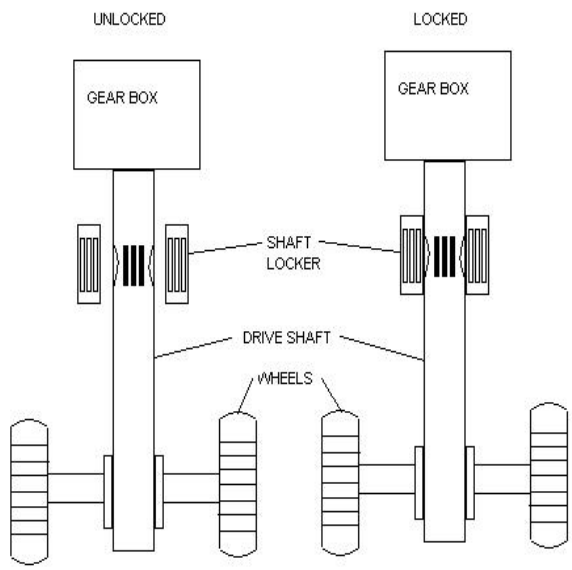

Figure 2.7: Drive Shaft lock in a car.

Transmission power of engine goes to rear wheels of a car through the drive shaft. If a thiefis able to hijack fuel supply lock and starts engine, he can take away the car. But we created Transmission locking system shown in fig. 2.7., which blocks supply to the rear wheels by locking the drive shaft.

5) Pressure Sensors

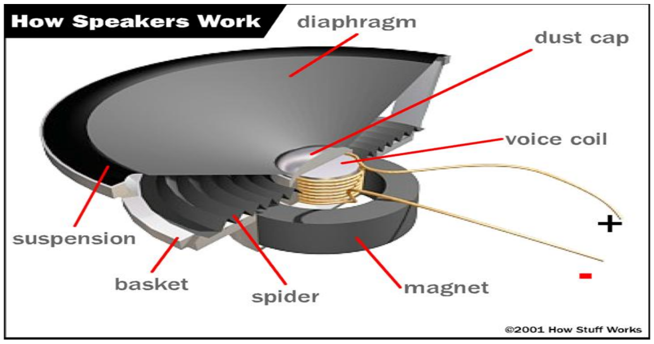

Figure 2.8: This is the basic mechanism of a speaker driver. A car's speakers make for effective alarm systems, as they can be used to measure variations in air pressure.

Another way to detect breaking glass, as well as somebody opening the door, is to measure the air pressure inthecar. Even if there is no pressure differential between the inside and outside, the act of opening a door or forcing in a window pushes or pulls on the air in the car, creating a brief change in pressure.

In the fig.2.8, showing speaker, when you play music, an electric current flows back and forth through the electromagnet, which causes it to move in and out. This pushes and pulls theattachedcone,forming air-pressure fluctuations in the surrounding air. We hear these fluctuations as sound.

Above system can work in reverse, which is what happensin a basicpressuredetector. Pressure fluctuations move the cone back and forth, which pushesandpulls the attached electromagnet that generates an electrical current. When thebrainregistersasignificantcurrent flowing from this device, it knows that something has caused a rapid pressure increase inside the car. This suggests that somebody has opened a door or window, or made a very loud noise.

6) Tilt Sensors

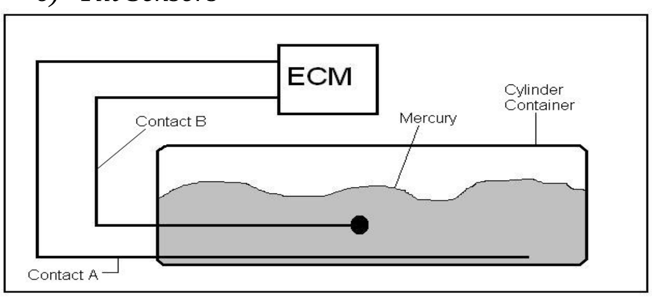

Figure 2.9: Showing operations of Tilt sensor.

Many car thieves aren't after your entire car; they're after individual pieces of it. These car strippers can do a lot of their work without ever opening a door or window. And a thief armed with a tow truck can just lift up your car and drag the entire thing away.

To protect against car thieves with tow trucks, some alarm system have "tilt detectors" shown in fig.2.9. The basic design of a tilt detector is a series of mercury switches. A mercury switch is made up of two electrical wires and a ball of mercury positioned inside a contained cylinder. Mercury is a liquid metal --it flows like water, but it conducts electricity like a solid metal. In a mercury switch, one wire (let's call it wire A)goes all the way across the bottom of the cylinder, while the other wire(wire B) extends only part way from one side. The mercuryis always in contact with wire A, but it may break contact with wire B. When the cylinder tilts one way, the mercury shifts so that it comes into contact with wire B. This closes the circuit running through the mercury switch. When the cylinder tilts the other way, the mercury rolls away from the second wire, opening the circuit.

In some designs, only the tip of wire B is exposed, and the mercury must be in contact with the tip in order to close a switch. Tilting the mercury switch either way will open the circuit. Car alarm tilt sensors typically have an array of mercury switches positioned at varying angles. If a thief changes the angle of your car (by lifting it with a tow truck or hiking it up with a jack, for example), some of the closed switches open and some of the open switches close. If any of the switches are thrown, the central brain knows that someone is lifting the car.

III. Implementation Aspects

To the computer side, we attach RF card to communicate with ECM controlled by car security system. A .NET Based software interface is made for the user which also has a database for storing login and user notification information. It has first a login screen and if username and password is correct, then it goes to menu showing options like-Lock (Central door, Fuel supply, Ignition), Unlock (Central door, Fuel supply, Ignition), Activate (Pressure sensors, Tilt sensors), Deactivate (Pressure sensors, Tilt sensors).

The choices the options according to his wish and computer command CSS according to it.Car security system controls ECM which handles all sensors and locks. According to CSS commands, ECM activates/deactivates the sensors.

ECM also performs locking and unlocking. By activating the central door lock, all doors are completely locked and vice versa. By select the fuel supply lock, it close the relay operated valve as block the fuel supply flow to engine and reverse also. By click on ignition lock, it breaks the ignition circuit with the help of relay and when relay is magnetized, it completes the circuit.Command module is used to program the CSS. Owner computer is connected to CSS wirelessly by RF link (range-70m).

IV. CONCLUSION

The proposed system provides different locking such as central locking, ignition locking, fuel supply locking and transmission locking. Due to central lock, it is difficult for thieves for opening the doors, bonnet or trunk. If tried, then also CSS will raise the alarm of high pitch. By presence of ignition lock, transmission lock and fuel supply lock, it is impossible to start the car.

Also it provides different sensors like pressure sensors and tilt sensors. By using different sensors for pressure analyzing in windows, if a burglar tries to break the glass, then alarm will be raised. Tilt sensor measures the balance of the car and if a robber tries to remove any part of the car which causes alteration in balance then ECM will notify the user.The paper concludes that, using the above system owner need not worry about the car and it also reduces the car theft rate.

REFERENCES

1. **PARIS KITSOS, YAN ZHANG, RFID Security: Techniques, Protocols and System-on-Chip Design,** Springer Publication**, First Edition, pp. 21-26, 2008.**
2. C .T. McCartney, “New vehicle security assessment-a practical insurance approach”, European Convention on Security and Detection, IEEE, pp.239-243, Aug 2002.
3. R.Livermore, “ATTACK TESTINGNEW VEHICLES”, published by the IEE. Savoy Place, London *WCPR* OBL. UK.,pp.9/1-9/3,1993.
4. Mohammed Benaissa, “Secure and Privacy Aware RFIDs”, submitted to IEEE IDT, 2009.
5. Requirements of Remote Keyless Entry (RKE) Systems,APPLICATION NOTE 3395, Nov, 2004.
6. J A Howard, “Smart cards (for car security applications)”, IEE Colloquium on Vehicle Security, pp. 4/1-4/3, Aug 2002.
7. C.M. Roberts, "Radio frequency identification (RFID)",Elsevier-Sciencedirect, computers & security, Vol.25, pp. 18 – 26,2006.
8. **Sabrie Soloman,Sensors Handbook,** McGraw-Hill Publication, **Second Edition, pp.45-85,105-133, 2010.**
9. Joseph J. Carr, Secrets of RF Circuit Design, McGraw-Hill Publication, Third Edition, pp.18-26, 2001.
10. Philip L. Skousen, Valve Handbook, McGraw-Hill Publication, Second Edition, pp.142-166, 2004.
11. James L. Kirtley Jr., Richard H. Lyon, Steven B Leeb, Nirmal K Ghai, H. Wayne Beaty, Electric Motor Handbook, McGraw-Hill Publication, Second Edition, pp.78-106, 1998.
12. Joseph E. Shigley, Charles R. Mischke, Thomas Hunter Brown, Jr., Standard Handbook of Machine Design, McGraw-Hill Publication, Third Edition, pp.69-78, 2004.
13. **Buczek Greg, ASP.NET: Developers Guide,** McGraw-Hill Publication, Second Edition, 2008.
14. Otey Michael, Otey Denielle,and Microsoft SQL Server 2005: developers guide, McGraw-Hill Publication, Fourth Edition, 2007.

AUTHOR’S PROFILE

Dependra Nath Saikia
Appeared in B.E. Computer, Computer Engg. Dept., Sandip Institute of Technology and Research Centre, Nasik, Maharashtra, India.

Abhilasha Choudhary
Appeared in B.E. Computer, Computer Engg. Dept., Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India.

Aditi Sardesai
Appeared in B.E. Computer, Computer Engg. Dept., Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India.