Research Paper Engineering

# Super-Lock: Next Generation Auto Theft Prevention System Using Smart Gravitational Lock

**Kirubasri.G**

Assistant Professor, PSNA College of Engineering and Technology Dindigul, India.

ABSTRACT

Vehicle theft is one of the major issue in this technological society. We propose a novel method to tackle security related issues. Applications such as vehicle tracking, sending Short Message Service (SMS) alerts, blocking petrol tank is explained in this project. Tracing and protecting the vehicle by SMS alerts. So with this project we can trace the vehicle when it is stolen by unauthorized person. The owner of the vehicle sends and SMS to the SUPER LOCK SYSTEM in the vehicle so that the system can be active and it immediately blocks the petrol tank and we can trace the vehicle using the GPS system. Here we use the combination of GPS, MIWI P2P wireless protocol, and embedded protocols such as CAN, SPI, UART. Also we use DC motors, microcontrollers to control the motion of the vehicle. The microchip here we use is ARM which possess rich features and delivering higher performance.

**KEYWORDS**

Global Positioning System (GPS), Smart Gravitational Lock, Cortex-M3, Universal Asynchronous Receiver/Transmitter.

## 1. INTRODUCTION

The Global Positioning System (GPS) is a location system based on a constellation of about 24 satellites orbiting the earth at altitudes of approximately 11,000 miles. GPS has proven to be a useful tool in non-military mapping applications as well. GPS satellites are orbited high enough to avoid the problems associated with land based systems, yet can provide accurate positioning 24 hours a day, anywhere in the world. Uncorrected positions determined from GPS satellite signals produce accuracies in the range of 50 to 100 meters. When using a technique called differential correction, users can get positions accurate to within 5 meters or less.

MiWi and MiWi P2P are proprietary wireless protocols designed by Microchip Technology that uses small, low-power digital radios based on theIEEE 802.15.4 standard for wireless personal area networks (WPANs). It is designed for low data transmission rates and short distance, cost constrained networks, such as industrial monitoring and control, home and building automation, remote control, low-power wireless sensors, lighting control and automated meter reading [1] [2]. The ARM Cortex™-M3 processor is the industry-leading 32-bit processor for highly deterministic real-time applications and has been specifically developed to enable partners to develop high-performance low-cost platforms for a broad range of devices including microcontrollers, automotive body systems, industrial control systems and wireless networking and sensors. The processor delivers outstanding computational performance and exceptional system response to events while meeting the challenges of low dynamic and static power constraints. The processor is highly configurable enabling a wide range of implementations from those requiring memory protection and powerful trace technology through to extremely cost sensitive devices requiring minimal area. The above can be used to detect the theft vehicles by sending SMS alerts. Section 2 reviews the body of related work, and Section 3 describes proposed system methodologies with assumptions, and Section 4 discusses system architecture and Network model. and section 5 concludes this paper.

## 2. Literature survey

At present the vehicle theft is found by using GPS and alarm systems. To improve this process of automatic one can use MIWI protocol to send and receive SMS alerts between two hosts. Whenever the vehicle is touched by unknown person the alarm system will be active automatically.

**(i) Remote keyless entry system:** refers to a lock that uses an electronic remote control as a key which is activated by a handheld device or automatically by proximity.

**ii) Immobilizer:** It is an electronic security device fitted to an automobile that prevents the engine from running unless the correct key or other token is present. This prevents the car from being "hot wired" after entry has been achieved.

Due to the simple and poor nature of these security systems, auto theft incidents worldwide are on the rise [3]. Here are some of the major problems with the existing auto theft prevention system.

i) It offers no protection when the key fob is stolen. So a smart key fob sold in the market is not actually smart.
ii) Vehicle tracking devices will not be able to locate a vehicle in GPS denied environments such as within buildings, underground and dense city regions, resulting in the loss of vehicle.
iii) The currently used motion and tilt alarms will alert the owner even for an unintentional touch by a passing person or an accidental hit by a ball from a playing child.
iv) Limited or to be accurate no central user interface to configure and customize the vehicle security system.

The Vehicle's owner can get the current updates about their vehicle when theft by SMS alerts. We can also enquire the vehicle location by sending message to the SUPER LOCK SYSTEM which is fitted inside the vehicle. In this proposed we system also have the mechanism to maintain security.

## 3. PROPOSED METHODOLOGY

### 3.1 GLOBAL POSITIONING SYSTEM

The Global Positioning System (GPS) is a location system based on a constellation of about 24 satellites orbiting the earth at altitudes of approximately 11,000 miles. GPS was developed by the United States Department of Defense (DOD), for its tremendous application as a military locating utility. The DOD's investment in GPS is immense. GPS has proven to be a useful tool in non-military mapping applications as well.

GPS satellites are orbited high enough to avoid the problems associated with land based systems, yet can provide accurate positioning 24 hours a day, anywhere in the world. Uncorrected positions determined from GPS satellite signals produce accuracies in the range of 50 to 100 meters. When using a technique called differential correction, users can get positions accurate to within 5 meters or less.

### Location Determination by GPS

In a nutshell, GPS is based on satellite ranging - calculating the distances between the receiver and the position of 3 or more satellites (4 or more if elevation is desired) and then applying some good old mathematics. Assuming the positions of the satellites are known, the location of the receiver can be calculated by determining the distance from each of the satellites to the receiver. GPS takes these 3 or more known references and measured distances and "triangulates" an additional position

GPS satellites are orbiting the Earth at an altitude of 11,000 miles. The DOD can predict the paths of the satellites vs. time with great accuracy [4]. Furthermore, the satellites can be periodically adjusted by huge land-based radar systems. Therefore, the orbits, and thus the locations of the satellites, are known in advance. Today's GPS receivers store this orbit information for all of the GPS satellites in what is known as an almanac. Think of the almanac as a "bus schedule" advising you of where each satellite will be at a particular time. Each GPS satellite continually broadcasts the almanac. Your GPS receiver will automatically collect this information and store it for future reference.

The Department of Defense constantly monitors the orbit of the satellites looking for deviations from predicted values. Any deviations (caused by natural atmospheric phenomenon such as gravity), are known as ephemeris errors [5]. When ephemeris errors are determined to exist for a satellite, the errors are sent back up to that satellite, which in turn broadcasts the errors as part of the standard message, supplying this information to the GPS receivers

### Computing the Distance between object Position and the GPS Satellites

GPS determines distance between a GPS satellite and a GPS receiver by measuring the amount of time it takes a radio signal (the GPS signal) to travel from the satellite to the receiver. Radio waves travel at the speed of light, which is about 186,000 miles per second. So, if the amount of time it takes for the signal to travel from the satellite to the receiver is known, the distance from the satellite to the receiver (distance = speed x time) can be determined. If the exact time when the signal was transmitted and the exact time when it was received are known, the signal's travel time can be determined.

In order to do this, the satellites and the receivers use very accurate clocks which are synchronized so that they generate the same code at exactly the same time. The code received from the satellite can be compared with the code generated by the receiver. By comparing the codes, the time difference between when the satellite generated the code and when the receiver generated the code can be determined. This interval is the travel time of the code. Multiplying this travel time, in seconds, by 186,000 miles per second gives the distance from the receiver position to the satellite in miles.

### 3.2 MIWI

MiWi and MiWi P2P are proprietary wireless protocols designed by Microchip Technology that uses small, low-power digital radios based on theIEEE 802.15.4 standard for wireless personal area networks (WPANs). It is designed for low data transmission rates and short distance, cost constrained networks, such as industrial monitoring and control, home and building automation, remote control, low-power wireless sensors, lighting control and automated meter reading.

The MiWi protocols are supported on certain Microchip PIC and dsPIC microcontrollers. When developing for these platforms, proprietary SDKs and hardware development tools, such as the ZENA wireless packet sniffer, may be used. Being ZigBee compliant, and capable of communicating using MiWi wireless protocols, it is based on the IEEE 802.15.4 Wireless PAN standard. Designed only for low-data rates and being low-cost, it has an integrated PCB antenna. In 2008, Microchip released a 2.4 GHz wireless transceiver module that is compatible with certain Microchip PIC and dsPIC microcontrollers (the Microchip MRF24J40MB), and can be used in production devices. The Microchip ZENA (formerly, Zigbee Enhanced Network Analyzer) is a wireless packet sniffer and network analyzer following the IEEE 802.15.4 specification on the 2.4 GHz band.

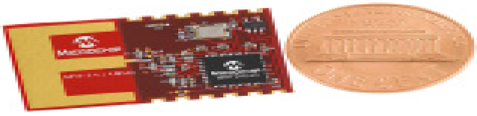


**Fig.1 Microchip ZENA**

We have three modules

1. Sending theft information
2. Processing and blocking vehicle movement
3. Sending SMS alert back to the owner about the location.
4. SYSTEM ARCHITECTURE AND NETWORK DESIGN

IEEE 802.15.4 and the MiWi P2P stack support two topologies: Star and Peer-to-Peer.

### (i)Star Topology

A typical star topology is shown in Figure 2. From a device role perspective, the topology has one Personal Area Network (PAN) coordinator that initiates communications and accepts connections from other devices. It has several end devices that join the communication. End devices can establish connections only with the PAN coordinator[4]. As to functionality type, the star topology's PAN coordinator is a Full Function Device (FFD). An end device can be an FFD with its radios on all the time, or a Reduced Function Device (RFD) with its radio off when it is Idle. Regardless of its functional type, end devices can only talk to the PAN coordinator.

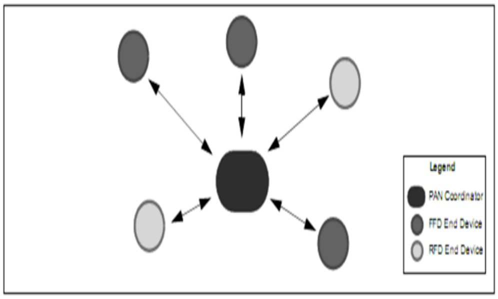


**Fig.2 Star Topology**

### (ii)Peer-To-Peer (P2P) Topology

A typical P2P topology is shown in Figure 2. From a device role perspective, this topology also has one PAN coordinator that starts communication and the end devices. When joining the network, however, end devices do not have to establish their connection with the PAN coordinator. As to functional types, the PAN coordinator is an FFD and the end devices can be FFDs or RFDs. In this topology, however, end devices that are FFDs can have multiple connections. Each of the end device RFDs, however, can connect to only one FFD and cannot connect to another RFD.

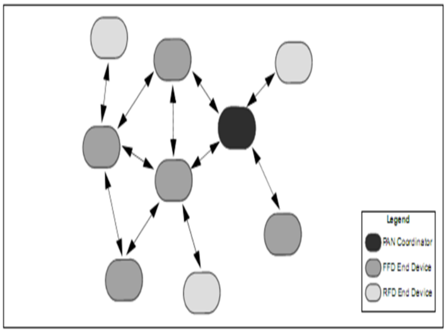


**Fig.3 Peer-To-Peer (P2P) Topology**

### 4.1NETWORK TYPE

The MiWi P2P stack supports only non-beacon networks. In a non-beacon network, any device can transmit data at any time, as long as the energy level (noise) is below the predefined level. Non-beacon networks increase the power consumption by FFD devices because they must have their radios on all the time. These networks reduce the power consumption of RFD devices, however, because the RFDs do not have to perform the frequent synchronizations.

### 4.2ARMCortexM3

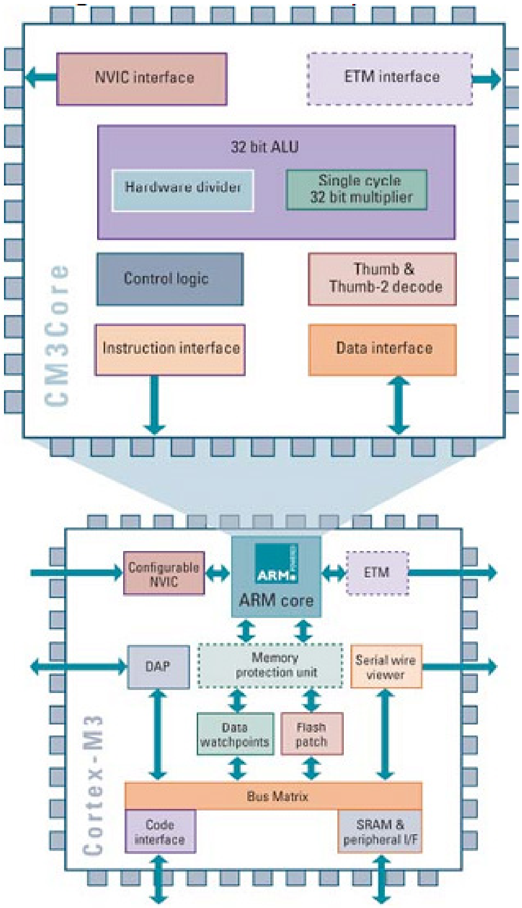


**Fig.4 ARM Cortex-M3 Architecture**

The ARM Cortex™-M3 processor is the industry-leading 32-bit processor for highly deterministic real-time applications and has been specifically developed to enable partners to develop high-performance low-cost platforms for a broad range of devices including microcontrollers, automotive body systems, industrial control systems and wireless networking and sensors. The processor delivers outstanding computational performance and exceptional system response to events while meeting the challenges of low dynamic and static power constraints. The processor is highly configurable enabling a wide range of implementations from those requiring memory protection and powerful trace technology through to extremely cost sensitive devices requiring minimal area.

### Advantages of Cortex-M3

Delivering higher performance and richer features
Performance and Energy Efficiency
Full featured
Rich connectivity
ARM Cortex-M code size advantage explained

### 4.3 Master SSP (MSSP) Modules

The Master Synchronous Serial Port (MSSP) module is a serial interface, useful for communicating with other peripheral or microcontroller devices. These peripheral devices may be serial EEPROMs, shift registers, display drivers, A/D converters, etc. The MSSP module can operate in one of two modes:

- • Serial Peripheral Interface (SPI)
- • Inter-Integrated Circuit (I$^2$C)
- - Full Master mode
- - Slave mode (with general address call)

The I2C interface supports the following modes in hardware:
- • Master mode
- • Multi-Master mode
- • Slave mode

### I$^2$C Mode

The MSSP module in I$^2$C mode fully implements all master and slave functions (including general call support) and provides interrupts on Start and Stop bits in hardware to determine a free bus (multi-master function). The MSSP module implements the standard mode specifications, as well as 7-bit and 10-bit addressing.

**Two pins are used for data transfer:**
- • Serial clock (SCL) – RC3/SCK/SCL
- • Serial data (SDA) – RC4/SDI/SDA

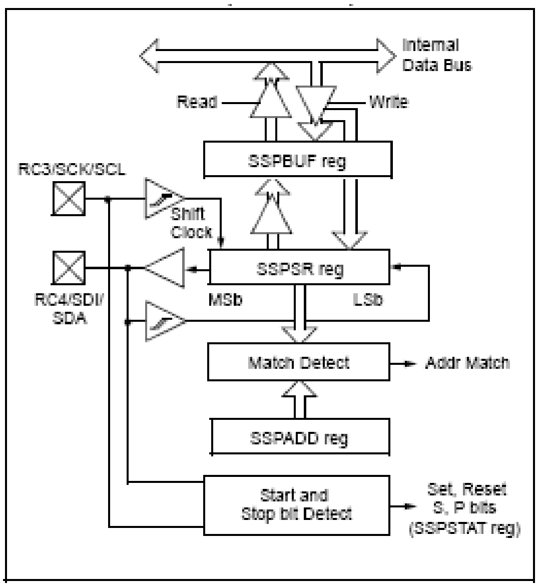


**Fig.5 MSSP Block Diagram**

The MSSP module has six registers for I2C operation.

These are:
- • MSSP Control Register (SSPCON)
- • MSSP Control Register 2 (SSPCON2)
- • MSSP Status Register (SSPSTAT)
- • Serial Receive/Transmit Buffer Register (SSPBUF)
- • MSSP Shift Register (SSPSR) – Not directly accessible
- • MSSP Address Register (SSPADD)

SSPCON, SSPCON2 and SSPSTAT are the control and status registers in I2C mode operation. The SSPCON and SSPCON2 registers are readable and writable. The lower six bits of the SSPSTAT are read-only[5]. The upper two bits of the SSPSTAT are read/write. SSPSR is the shift register used for shifting data in or out. SSPBUF is the buffer register to which data bytes are written to or read from. SSPADD register holds the slave device address when the SSP is configured in I2C Slave mode.

### 4.4 PULSES WITH MODULATION

Pulse width Modulation or PWM is one of the powerful techniques used in control systems today. They are not only employed in wide range of control application which includes: speed control, power control, measurement and communication.

**Basic Principal of PWM**
Pulse-width Modulation is archived with the help of a square wave whose duty cycle is changed to get a varying voltage output as a result of average value of waveform. A mathematical explanation of this is given below.

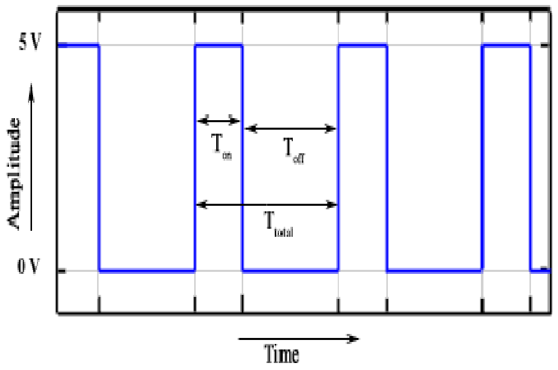


**Fig.6 Square Wave**

As shown in the figure 6 $T_{on}$ is the time for which the output is high and $T_{off}$ is time for which output is low. Let $T_{total}$ be time period of the wave such that,

$$T_{total} = T_{on} + T_{off}$$

$$D = \frac{T_{on}}{(T_{on} + T_{off})} = \frac{T_{on}}{T_{total}}$$

The output voltage varies with duty cycle is

$$V_{out} = D \times V_{in}$$

$$V_{out} = \frac{T_{on}}{T_{total}} \times V_{in}$$

**4.5 EMBEDDED PROTOCOLS**
Set of rules governing communication between electronic devices and computing endpoints.A standard way of communicating across a network. A protocol is the “language” of the network. A method by which two dissimilar systems can communicate.

**UART (Universal Asynchronous Receiver Transmitter)**

```
     start|<- five to eight data bits ->| stop bit(s)
              0    ---- - - - - - - - - - -           Space (logic
low)
                   | | | | | | | | | | | | |
                   | S | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | S | S |
                   | | | | | | | | | | | | |
              1      - - - - - - - - - - - --------   Mark (logic
high)
```

**Figure 7.Asynchronous Code Format.**

The right-most bit is always transmitted first. If parity is present, the parity bit comes after the data bits but before the stop bit(s).

UART stands for the *Universal Asynchronous Receiver/Transmitter*.

In asynchronous transmitting, **teletype**-style UARTs send a “start” bit, five to eight data bits, least-significant-bit first, an optional “parity” bit, and then one, one and a half, or two “stop” bits[4]. The start bit is the opposite polarity of the data-line’s idle state. The stop bit is the data-line’s idle state, and provides a delay before the next character can start. (This is called **asynchronous start-stop** transmission). In mechanical teletypes, the “stop” bit was often stretched to two bit times to give the mechanism more time to finish printing a character. A stretched “stop” bit also helps resynchronization.

The parity bit can either makes the number of “one” bits between any start/stop pair odd, or even, or it can be omitted. Odd parity is more reliable because it assures that there will always be at least one data transition, and this permits many UARTs to resynchronize.

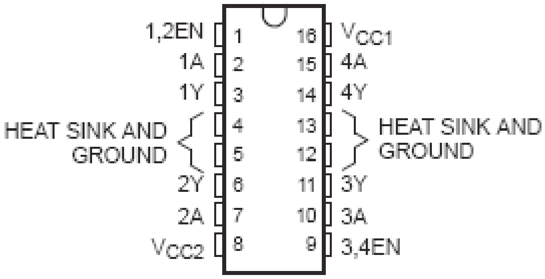
In *synchronous* transmission, the clock data is recovered separately from the data stream and no start/stop bits are used. This improves the efficiency of transmission on suitable channels since more of the bits sent are usable data and not character framing. An asynchronous transmission sends nothing over the interconnection when the transmitting device has nothing to send; but a synchronous interface must send “pad” characters to maintain synchronism between the receiver and transmitter[5][6]. The usual filler is the **ASCII** “SYN” character. This may be done automatically by the transmitting device.

USART chips have both synchronous and asynchronous modes.

**4.6 MOTOR DRIVER DESCRIPTION**
The L293D is designed to provide bidirectional drive currents of up to 600-mA at voltages from 4.5 V to 36 V. devices are designed to drive inductive loads such as relays, solenoids, dc and bipolar stepping motors, as well as other high-current/high-voltage loads in positive-supply applications. All inputs are TTL compatible. Each output is a complete totem-pole drive circuit, with a Darlington transistor sink and a pseudo-Darlington source [5]. The Device is a monolithic integrated high voltage, high current four channel driver designed to accept standard DTL or TTL logic levels and drive inductive loads (such as relays solenoids, DC and stepping motors) and switching power transistors. To simplify use as two bridges each pair of channels is equipped with an enable input. A separate supply input is provided for the logic, allowing operation at a lower voltage and internal clamp diodes are included. This device is suitable for use in switching applications at frequencies up to 5 kHz. The L293D is assembled in a 16 lead plastic package which has 4 center pins connected together and used for heat sinking

**Features**
Wide Supply-Voltage Range: 4.5 V to 36 V
Separate Input-Logic Supply
Internal ESD Protection
Thermal Shutdown
High-Noise-Immunity Inputs
Output Current 1 A Per Channel (600 mA for L293D)
Peak Output Current 2 A Per Channel (1.2 A for L293D)
Output Clamp Diodes for Inductive Transient Suppression (L293D)

**4.7 PIN CONNECTIONS**



**5. Conclusion**

In the proposed method an innovative Super-Lock: Next Generation Auto Theft Prevention System using 3-axis MEMS Accelerometer, 3-axis MEMS Magnetometer, IEEE 802.15.4 wireless networking protocol, TFT display, GPS Receiver, GSM cellular modem has been developed for vehicle. We call it the real smart key fob. A central user interface to configure and customize the vehicle security system which is not present in the previous vehicle designs. Hence This approach described here presents a technique to prevent the vehicle theft by implementing smart gravitational lock, cryptographic keyless entry, adjustable motion alarm sensitivity, and also used for track and monitor the vehicle by owners at anytime from anywhere.

## REFERENCES

H. Je, J. kim, and D.kim (, Aug. 2007) Hand gesture recognition to understand musical conduction action, presented at IEEE Intconf, Robot &Human Interactive Communication. | Jacques George, and Chris Gooda (May 2012) , Vehicle Navigator using a Mixture Particle Filter for Inertial Sensors/Odometer//Map Data/GPS Integration, IEEE Transactions on Consumer Electronics, Vol 58, NO.2. | J.C. Juang, and Y-H Chen (May 2009.): Accounting for data intermittency in a software GNSS receiver, IEEE Trans. Consum. Electron, vol 55,NO.2, | Kichun Jo and MyounghoSunwoo(March 2012), IEEE: Interacting Multiple Model Filter-Based Sensor Fusion of GPS With In-Vehicle Sensors for Real-Time Vehicle Positioning ,IEEE Transactions on intelligent transportation systems, vol.13, NO. 1 | Ruizexu, Shengli Zhou, and Wen J.Li (May 2012), IEEE: MEMS Accelerometer Based Nonspecific- User Hand Gesture Recognition, IEEE Sensors journal, vol.12, NO.5. | T. Senthil kumar1, K. Praveen, International Journal of Scientific Engineering and Technology,Design of Next Generation Auto Theft Prevention System, Volume 2 Issue 3, PP : 133-136