1st International Conference on Sensing Technology
November 21-23, 2005 Palmerston North, New Zealand

Method and Device to Communicate via SMS After a Security Intrusion

Vishy Karri[1], Daniel J.S. Lim[2]
School of Engineering,
University of Tasmania
Hobart, Australia
Vishy.Karri@utas.edu.au & jsdlim@utas.edu.au

Abstract

The invention relates generally to a security device for the protection of vehicles, offices, homes and any other location where foreign access is of concern. In particular, the present invention is a device for notifying the owner when any of the above locations has been accessed or broken into. The device is made up of three components: one or more sensors set up in a remote array depending on the application; a PIC micro-controller; and a GSM module.

Keywords

Remote Monitoring, Security Device, SMS, GSM, One Way Communication, Sensor Technology

1 Introduction

Theft and intrusion are common problems in today's society, ranging anything from a motor vehicle to personal belongings from an office or even a room at home. In many cases these criminal acts go unnoticed by the owner until some time later. It is therefore the purpose of this invention to provide a security device, which gives immediate notification to the owner at the moment the theft occurs. This purpose is accomplished via use of a remote sensor(s), which activates a GSM (Global Service Module) module to send one or more SMS (Short Message Service) messages to the owner at the time of break in.

2 Description of Operation

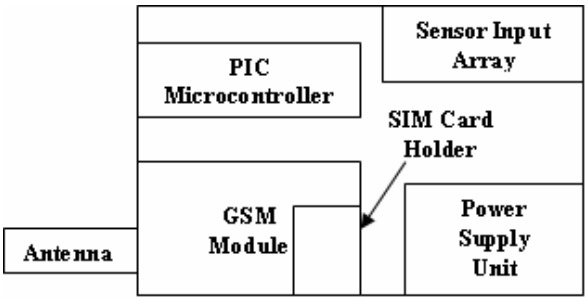

Figure 1: 1st Generation Assembled Prototype

Referring to *Figure 1*, the design hardware prototype of the security device is shown. This is the preliminary moving prototype assembled to carry out the task. The device has a Watchdog timer so that the system can reset whenever it unexpectedly stops functioning. It also has the function for auto detection and warning of low battery. The Security device has a flexible working range of voltage; therefore it is applicable to a variety of vehicles. The system can be activated and deactivated using a remote control. The Remote control is free from imitation with the integration of the frequency Hopping Code, avoiding possible detection or duplication. Therefore, the possibility of using an electronic learning remote controller to interfere with the activated security system is almost impossible.

The sensor is shown as a single entity but could be composed of a number of different sensors depending on the application. The varieties of sensors that can be used are outlined in *figure 2*, namely:

- Alarm signal sensors
- Vibration sensors
- Electromagnetic sensors
- Infrared sensors
- Optical sensors

Alarm signal sensors are used in the case of use in a motor vehicle. The device is connected to motor central lock and the key/ignition switch assembly for detection of door unlock and engine lock intrusion. This then initiates the GSM module to send an SMS message to the owner. The vibration sensors can be used in a motor vehicle or a door in the case of an office or home installation. When using the device for office or home protection, vibration sensors would be attached to the door and an alert sent through the GSM Module to the owner when the door is vibrated. As a consequence, the police station or security guards can also be rapidly informed for checking and searching the target location.

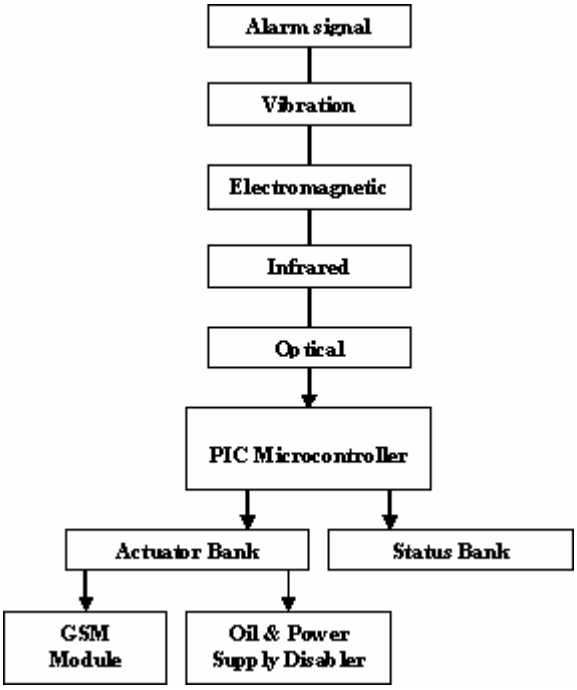

Figure 2: Basic Circuit Diagram

It is important to note, however, that in utilizing the device for an office or household, security doors or windows may not vibrate sufficiently for detection. Hence if the door or window is opened slowly, the trigger to send the SMS message would be initiated by either an electromagnetic, infrared or optical sensor. In the case of an electromagnetic sensor the SMS would be initiated by a +12V supply. This will be attached to the door and when the door is opened the +12V will initiate a current to the security device, initiating the GSM Module to send one or more SMS messages to the owner. Similarly, the Infrared and Optical sensors initiate a current to the GSM Module when the optical or infrared reflection is cut or disturbed when the door or window is opened. Any signals sent from the remote sensors are processed by the PIC micro-controller.

3 Detail of Components

The whole processing of the device is done by a PIC micro-controller. The PIC micro-controller is a small but powerful micro-controller from Microchip [1]. It is shown in *figure 1* and in the functional schematic of *figure 2*.

The PIC micro-controller can handle C language applications of approximately 50,000 C+ statements or 1 MB. Dynamic C is an integrated development system for writing embedded software and is the system used in this device. This language system integrates the following development functions into one program:

- Editing
- Compiling
- Linking
- Loading
- Debugging

In fact, compiling, linking and loading are one function. Dynamic C has an easy-to-use, built-in, full featured, text editor. Dynamic C-Programs can be executed and debugged interactively at the source-code or machine-code level. Pull-down menus and keyboard shortcuts for most commands make Dynamic C easy to use.

The PIC micro-controller is connected to an actuator bank as shown schematically in *figure 2*. The actuator bank comprises a conventional bank of relays. In order to activate the GSM Module a relay is activated from the PIC micro-controller. Since the actuator bank contains more than one relay, a number of functions can be performed in response to the sensor. An optional function of the device in the case of use in a motor vehicle is a power and oil supply disabler. This would be activated by the PIC micro-controller, through a separate relay in the actuator bank, to the power and oil supply disabler.

4 The GSM Network

As aforementioned, and in situations where the device is used in an office or home, the GSM module will be the only component of the device activated through the actuator bank.

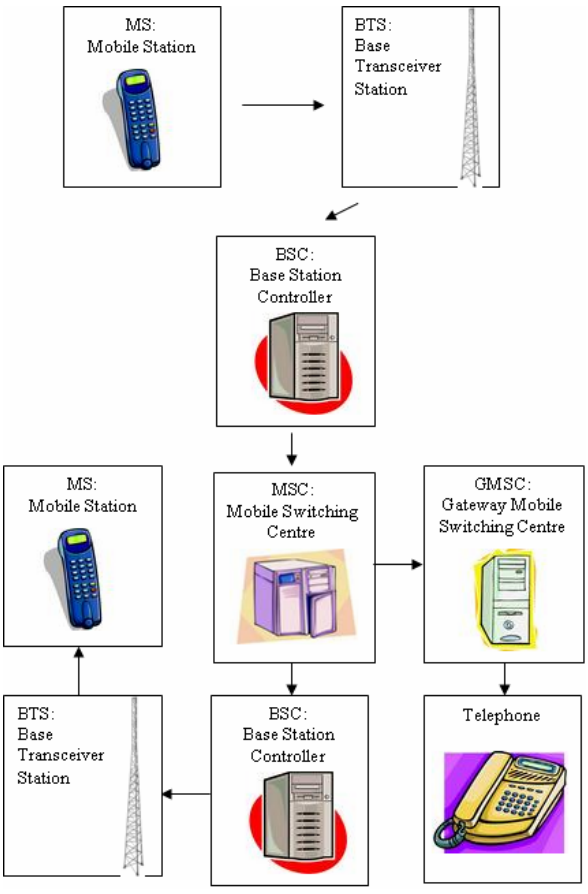

Figure 3: The GSM network infrastructure

The GSM module is essentially a mobile phone [2]. It is used in this device to send SMS messages to the owner when a sensor is activated. Short Messages are two-way alphanumeric messages and binary messages that can be sent and received by GSM modules with Short Message Service (SMS) capabilities. The SMS service is provided by the Global System for Mobile Communications (GSM). Short Messages sent from GSM units are called mobile originated while messages received by GSM units are called mobile terminated. The GSM module sends SMS messages via a GSM network outlined in *figure 3*.

The Mobile Station (MS) is the GSM module inside of the security device. In general however the term Mobile Station refers to a "mobile phone". [3]

The Base Transceiver Station (BTS) is the part of the network that receives and sends data from the Mobile Station. Each BTS sits within a cell and is the centre of the cell. When a MS crosses the boundary to leave the range of a given BTS, it flawlessly latches on to the next adjoining BTS without the end user ever realising it. The coverage or reception of MS is dependent on proximity and transmission of the BTS it is attached to. In urban areas the cells are smaller and closer together to provide for many subscribers in the area while in the suburbs the cells are larger and farther spaced [3] [6].

The Base Station Controllers (BSC) is a digital switching platform that connects a mobile switching centre MSC and the BTS. It also serves to transfer signalling information to and from mobile stations and manages handovers when a MS leaves a cell and enters the next [3] [6].

The Mobile Switching Centre (MSC) deals with the calls it receives from its subscriber from its network and serves to route the call to its destination whether that is on the same network or on the network of another provider [3].

Signal Transfer Points (STP) switch relay messages between network switches and databases. They function to route SS7 messages to the correct outgoing signalling link based on the message field addresses [7].

The Gateway Mobile Switching Centre (GMSC) connects a mobile network to a Public Switched Telephone Network (PSTN) which is the backbone of non-cellular telecommunication. [3]

The term Short Message Entity (SME) refers to any entity which may send and receive short messages. It may be located in a fixed network, a mobile or even an SMSC.

The Home Location Register (HLR) acts as a database storing information on all permanent subscribers [7].

The availability of the SMS service over different mobile networks depends on roaming agreements of the networks, as well as on a mechanism to deliver the messages. It is the network operator's responsibility to inform the user about the success or failure of the message delivery.

The mobile antenna of this device operates on one or more frequency bands. For example in the GSM 900 MHz and DCS 1800 MHz band. This means that the antenna performs well over a range of different frequencies. The goal is to make it resonant in the middle of each band. The term that is important here is bandwidth, i.e., the frequency range that your antenna works well over. One method of judging how well (efficiently) your antenna is working is by measuring VSWR. VSWR is a measure of impedance mismatches between the transmission line and its load. The higher the VSWR, the greater the mismatch. The minimum VSWR – that which corresponds to a perfect impedance match – is unity. Bandwidth is defined per frequency band. A common way to specify bandwidth is to say that VSWR should be better than 3:1 within band limits. A bandwidth around 10% of the frequency with this invention is considered as good [4] [5].

The speed and reliability in the delivery of SMS messages depend on many factors. The role of the network provider and supporting infrastructure heavily influences the performance of message delivery. When the Short Message Service was first introduced, it was meant to be a means of maximizing bandwidth utilization in mobile networks by utilizing the Signalling System 7 (SS7) or out of band network for short bursts of data. SMS messages do not command very high priority and performance is highly dependant on network conditions.

When an SMS is sent by a user, the following steps occur [8]:

1. Message is delivered to the MSC
2. MSC checks with the VLR for permissions
3. VLR returns to MSC with permission
4. MSC sends mobile user message to the SMSC
5. SMSC forwards this to the SME
6. SMSC returns an acknowledgement to the MSC
7. MSC forwards acknowledgement to the user.

As can be seen, each message sent by a user results in a series of messages being transmitted over the mobile network. Thus if a sudden burst of data is received, it is easy to see how the SS7 network becomes congested.

The main points of congestion in the SS7 network when an excessive amount of data is received occur about the STP and HLR. The STP handles SMS traffic and call setup while data stored in the HLR is retrieved almost each time any service on the network is accessed. Overloading of these points may cause delays or even failure at these nodes [8].

During off-peak periods, the messages are delivered nearly instantaneously while during periods of congestion, delays of several minutes are not uncommon. The performance of SMS messages are dependant on the capabilities of the network used and also the physical distance the message has to travel. The actual time taken to travel from one point to another is not so much the issue, however, the further the distance between the point of origin and point of delivery, the more networks the data packets have to traverse. Delays may be introduced at any of these points due to congestion or malfunction.

To minimize the impact of the possibility of lost or delayed warnings, the system is designed to take advantage of the message delivery confirmation service offered by most mobile network service providers. The system awaits the arrival of an acknowledgement receipt from the host network that is generated by the SMSC upon successful delivery of the message to the SME.

The method also includes a timing device that activates upon the delivery of a warning SMS message. If no response is received from the message delivery confirmation service within a set time, the device may resend the message and/or execute default action that is programmed to take place should the sending of the message fail. The system should also be programmed to deliver the initial warning to several users to maximize chances of a successful receipt of warning.

5 The Control program

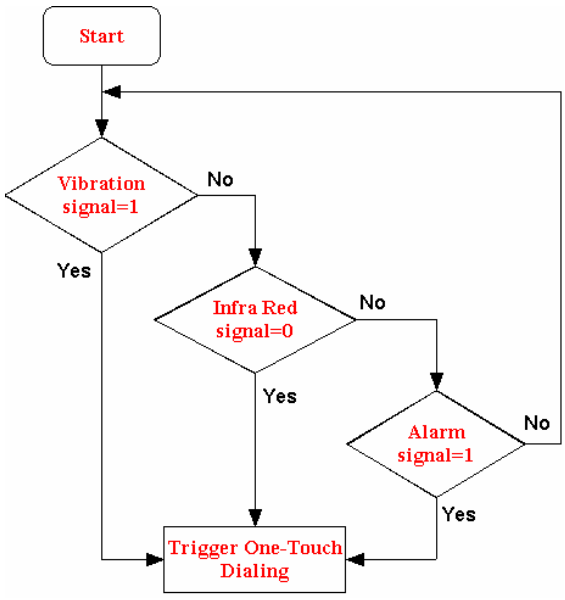

Figure 4: Control Program Structure and Flowchart Logic

When sufficient vibration is detected, a digital signal of 5 Volts corresponding to a logic value of 1 is generated. Similarly, an alarm of logic value of 1 is also received by the micro-controller if the door switch is open. If using the device for office security application, a pair of infrared receiver and transmitter would be used and generating a 12V input to the micro-controller if the infrared light is blocked by an opening door.

The configuration of the phone number that the security device would call can be done by a mobile phone having the "One-Touch Dialling" function and follow the steps below.

1. Place the SIM card into the mobile phone.
2. Choose "Phone Book"
3. Choose "Personal Numbers"
4. Choose "Add Entry"
5. Choose" Add to SIM card memory"
6. Enter the phone number
7. Choose "Phone Book"
8. Choose "One-Touch Dial Setting"
9. Choose "To SIM card memory"
10. Take the SIM card out and place it into the device.

Repeat 2-5 to enter other two numbers.

It is envisaged that there will also be an option for remote configuration of the system using commands issued via SMS.

The programming of the device enables it to send messages to several users at once to maximize the chances of reaching at least one user should the message fail to reach the primary intended recipient. The system then awaits a confirmation of delivery from the messages sent and resends the messages should it fail to receive a confirmation of a set reasonable time.

6 Application Areas

This unit was developed as a security device that is capable of notifying a person or several persons using a SMS message initiated by one touch dialling. The device may be used in stationary applications such as home or commercial security to monitor entrances. Using vibration switches to detect the opening of a door or window, it will effectively alert the person or persons in charge should an intrusion occur.

Mobile applications are also possible with the use of a 12V battery to power the device. Vehicles such as cars, boats or any other motor vehicle may be equipped with this device. The micro-controller of the unit may also be connected to the oil pump or an engine disabling unit on the vehicle. Upon the detection of a theft, the unit may then disable the vehicle until it receives a SMS to unlock the vehicle again.

7 Conclusion

This device provides a means for being able to securely monitor a stationary or mobile plant by use of sensors integrated with a micro-controller and a GSM unit. SMS provides an economical and

convenient way to alert users of a possible intrusion into the property. The use of the existing GSM infrastructure provides a mature and sophisticated platform to build upon and also removes the cost of establishing a dedicated communication channel. The use of mobile handsets as a client device to receive warning messages on implies that the user will not have to carry an additional piece of equipment as most people already have a mobile phone with them most of the time.

8 References

[1] Microchip Technology - *PIC 16F87x Data Sheet*, Microchip 2001.

[2] Telit - *Telit GM862 Software User Guide*, Dai Telecom 2003.

[3] Siegmund M.R., Matthias K.W., Malcolm W.O., *An Introduction to GSM*, Artech House Publishers, London 1995.

[4] Amateur Radio Antenna Magazine Web Article, James G. Lee, "The effects of VSWR on Transmitted Power", http://www.antennex.com/-preview/vswr.htm, visited on 15/03/2005.

[5] John A.K., *Antennas and Transmission Lines*, First Edition, Howard W. Sams & Co., Indianapolis, 1969.

[6] Schiller J., *Mobile Communications*, Second Edition, Addison-Wesley, 2003.

[7] Intel Telecom Solutions - SS7 Glossary of Terms. http://www.intel.com/network/csp/solutions/ngn/7643gls.htm visited on 29th August 2005.

[8] C. Murray, L. Cleary, "A Clearer Channel for SMS", *IEE Communications Engineer, April/May 2004 pp. 28-31*