SMS TRANSMISSION USING PDU MODE AND 7-BIT CODING SCHEME

Andrés Ortiz
Telefónica Móviles S.A.
Madrid

Alberto Prieto
Departamento de Arquitectura y Tecnología de Computadores
Universidad de Granada

ABSTRACT

This paper describes the design and implementation of an SMS transmission system using the PDU (Protocol Data Unit) mode of a GSM (Global System for Mobile Communications) modem. The system may be used in several applications: telemetry or remote control, using short messages from a standard GSM mobile phone, and in other application circuits. In order to perform these applications, coding and decoding of the short messages into PDU mode is required. In other words, the source needs to be coded and the numbers need to be targeted in the PDU. In this instance, the circuit was tested using a Siemens S25 mobile telephone.

KEYWORDS

Wireless Applications, Electronic Data Interchange, Mobile communications, Telecontrol, Telemetry.

1. INTRODUCTION

The success of mobile phones has enabled people to learn to make the most of them, and many people now carry a mobile phone with them. In addition, the reduced cost of sending short messages is the reason why it has become a popular form of communication as the majority of us are aware of the possibility of receiving and sending SMS messages (Short Messages Service) even if we don't use it. In this paper, we introduce a system with a secure method of transmission for carrying out telecontrol and/or supervision operations, which can be used by anyone carrying a mobile phone. Once an SMS is keyed into a mobile phone the message is then converted into a PDU packet before being sent. In this PDU packet, both the target phone number and the text message are coded. The text is introduced into the PDU using an 8-bit per character coding scheme. The inverse operation is carried out at the receiver's end, whereby the text message is extracted from the PDU packet and displayed on the recipient's mobile phone, in 7-bit ASCII format.

The main idea behind this project is the coupling of a mobile phone through its RS232C port to a device connected to an external remote controlled system, for example. The circuit which controls this, uses a microcontroller to extract the PDU, to decode it, and to generate other signals, like inputs for the supervision of a controlled system or the outputs to the actuators, according to the content of the decoded message. When the microcontroller performs the inverse operation, the 8-bit ASCII scheme is converted into the 7-bit ASCII scheme and PDU packets are made for the control system to respond to the recipient's mobile phone. The microcontroller can be connected to a standard PC, thus enabling the user to execute tasks on the PC and receive the generated messages on a mobile phone remotely.

2. SHORT MESSAGE TRANSMISSION PROCESS OVER A GSM NETWORK

A short message is generated in a mobile phone (MS, Mobile Station) and sent to a Message Entity (SME). This operation is done through a Short Message Service Center (SMSC) as shown in figure 1.

In theory, an SMS has to pass through several layers, the most important ones being: the Application Layer (AL), the Transport Layer, the Relay Layer (RL) and the Link Layer (LL). The Application layer interacts with the recipient's application. In The Transport Layer, packets (PDUs) are structured in the sender's mobile phone or extracted in the recipient's mobile phone. The Relay Layer orders the packets in sequence form for the following layer, which transmits PDUs to the SMS network. However in practice, the SMS messages are transmitted through the standard GSM network, as shown in figure 2.

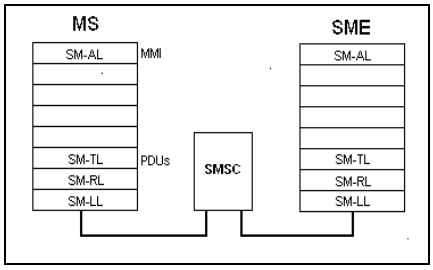

Figure 1. SMS sending scheme

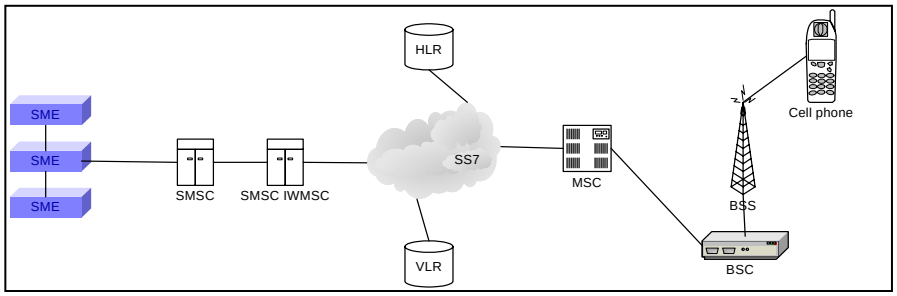

Figure 2. SMS network basic scheme

2.1 SMS Network Basic Scheme

In a GSM Network, Short Messages are sent over SS7 (Signaling System Number 7) network. All the element described in the figure above, are elements present in a basic GSM network architecture.
The Network elements that are directly related with SMS service:

- · SME: Short Message Entity is any entity which is capable to send and/or receive short messages
- · SMSC: Element that sends or store and forward messages from a SME to a MS (Mobile Station).
- · IWMSC: Gateway node for SMS – Mobile Originated service

The SMS sending process can be summarized as follows:

1) The SMS is sent from SME (Short Message Entity) to SMSC (Short Message Service Centre)
2) The SMSC communicates with the HLR (Home Location Register) and retrieves the necessary routing information to get through to the receiver.
3) The SMSC/IWMSC sends the SMS to the MSC (Mobile Switching Centre)
4) The MSC extracts the receiver information from the VLR (Visitor Location Register).
5) The MSC transfers the SMS to the receiver.
6) The MSC returns the results of the transmission operation to the SMSC.

7) If the SME asks for a confirmation, the SMSC will send back a message with the transmission operation result.

The SMS receiving process could be summarized as follows:
1) The mobile phone transfers the SMS to the MSC.
2) The MSC asks the VLR to verify if any network restriction is being overridden.
3) The SMSC sends the SMS to the mobile phone.
4) The SMSC acknowledges a successful transmission.
5) The MSC sends the result of the operation to the mobile phone.

All GSM Network elements have to be took as black boxes, with location, routing, forwarding etc, capabilities.

2.2 PDU Packet Structure

Thanks to the PDU mode, the product is supported by/compatible with other terminals (mobile phones). When using the PDU mode, instead of sending 7-bit ASCII data, the information is coded into a compressed form and octets are sent.
The basic structure of a PDU can be seen in the figure 3.

SCA	PDUT	MR	LON	NAC	DA	PID	DCS	VP	UDL	UD-PDU

Figure 3. PDU basic structure

Where: · SCA: Service Centre Address
· PDU TYPE: Protocol Data Unit Type
· MR: Message Reference
· DA: Destination Address.
· PID: Protocol Identifier
· DCS: Data Coding Scheme
· SCTS: Service Centre Time Stamp
· VP: Validity Period
· UDL: User Data Length
· UD-PDU: User Data PDU

Note that by changing the DCS, it is possible to send PDUs where UD is in 7-bit ASCII format.

The problem is that not all terminals (mobile phones) are compatible with the DCS 7-bit ASCII format. However, the SMS received in a 7-bit coding scheme can be displayed on a standard terminal, since this is the usual format of an SMS.
To obtain the User Data in a compressed form, we use the algorithm shown later in this document.
The Destination Address (DA) is inserted into the PDU as *Decimal Semi Octets*. The target number is built swapping the semi-octets two at a time and if there is an odd number of semi-octets F will be placed at the end. Figure 4, for example, shows how the DA is setted up for the target phone number.

27 83 88 90 00 1**F** (odd digits number -> **F** is added) - > **72 38 88 09 00 F1**

Figure 4. Conversion into Decimal Semi Octets

3. CODING / DECODING FOR A 7-BIT DATA CODING SCHEME

The microcontroller program has been developed using an MPASM assembler and an MPLAB 5.0 simulator environment.
In order to obtain maximum performance of all the routines, the clock cycle consumption had to be improved. The optimal routine is the serial communication one.

3.1 8-Bit Character Coding

The character coding process is shown in figure 5.
The first septet (h) is converted into an octet by adding the least-significant bit of the second septet to the far left side. This bit (least significant bit of the second septet) is eliminated.

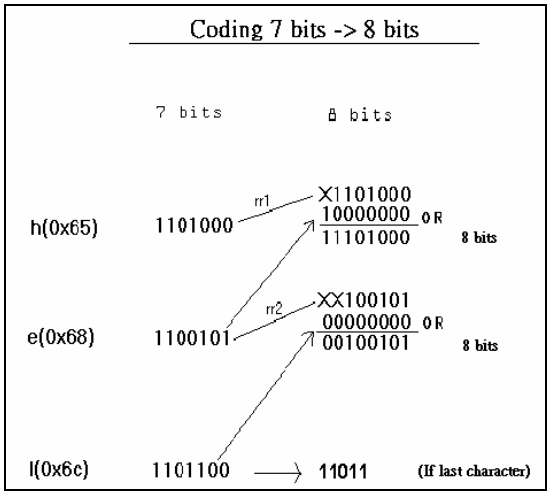

Figure 5. DCS 8-bit coding algorithm

For the second character, septet, two bits are needed (the two least significant bits). When the last character to code is reached, the result of the coding is the part which has not been used in the last OR operation, as shown in figure 4. In this way, the coding process of 8 septets results in 7 octets.
This process has been implemented in a medium-range microchip microcontroller. The routines have been optimised in order to minimize the clock cycle consumption.

3.2 Decoding PDUs

Now the reverse process is required. The algorithm removes the first bit from the octet being decoded, and adds, at the end, the bit which has been removed from the octet before last (which means starting again).

This process of removing bits has been implemented in the microcontroller assembler program, using masks which make AND operations. Therefore, only that part of the mask whose value is 1 is kept. (So, the masks are 10000000, 11000000, 11100000 …etc).

4. SENDING SMS USING THE PDU MODE

In the majority of GSM modems, external devices send SMS messages using AT (AT+C) commands, described in the GSM 07.05 standard. These commands allow an external device to talk to the GSM terminal (in this case, a mobile phone) and to create and send the PDUs to the terminal. User data, such as the destination address (DA), can be sent using a 7 or 8 bit-coding scheme (DCS=00 or DCS=F6 respectively). Messages composed of an 8-bit coding scheme are called Data Messages and are usually used for sending

logos and melodies to a terminal. The only problem when using this coding scheme is that not all the terminals are capable of showing the messages on their display. In this study, a Siemens S-25 was used, which is capable of sending, receiving and showing Data messages on its LCD. However, a PDU mode is needed if this device is to send messages which any terminal can read. For this reason, algorithms and routines have been developed to facilitate the transmission of messages in PDU mode.

4.1. Sending an SMS using AT Commands

The commands used are shown in the following table:

Table 1. AT+C commands used in the application

Command	Operation
AT+CSMA	SMSC
AT+CPIN	Set PIN into terminal
AT+CMGF	SMS mode select (1=Text mode , 0=PDU mode)
AT+CMGS	SMS send
AT+CMGR	Read a SMS from phone's memory
AT+CSMS	Phase 2+ compatibility activation
AT+CMNI	Mode to show incoming SMSs
ATE0	Local echo deactivation

The command sequence for sending SMS with AT+C commands is:

DTE: AT+CPIN="PIN" **CR LF**
DTE: AT+CPIN="PIN" CR LF
DCE: OK **CR LF**
DTE: AT+CMGS=140 **CR LF**
DCE: >
DTE: 0011000981NBCD00F6AA0568656C6C6F **CTRL+Z**
DCE: OK **CR LF**

The SMS is sent.
Note that the characters marked in bold are control characters.

5. SYSTEM DESIGN AND IMPLEMENTATION

Communication with the mobile terminal is carried out through the built-in serial port found in the majority of mobile terminals. This is a normal asynchronous serial port but voltage levels are non-standard (+-5V), different from the industry standard RS232 (+-12V), in order to adapt the port levels to the phones's battery level and minimize battery consumption. Power in mobile phones is usually between 3 and 7 volts and their RS232 ports handle levels of between 0 and 3 or 5 volts. In a Siemens S-25 mobile phone, we found levels of between 0 and 3 volts.

In order to make the circuit compatible with other terminals, we used a MAX232 level converter, and a 10K resistor to protect the microcontroller's input (the inputs of the microcontroller cannot absorb more than 20 mA). We tried to use 3V levels instead of an MAX232 level converter. However, if a 19200 bps serial communication is required (the Siemens S-25 only supports 19200 bps communication), a 8 MHz clock would be needed in order to reach this speed, and the microcontroller's oscillator is not stable enough to operate at 3 volts.

The asynchronous communication parameters are 19200 bps, 1 stop bit and no parity. When an 8 MHz clock is used, extra calculations need to be made, including a PDU conversion and serial communication.

It is possible to use a 4 MHz clock if only SMS sending is required (i.e.: a stand alone SMS sending microcontroller). In fact, the implementation has been carried out using a Microchip 12F675 microcontroller together with a 4 MHZ internal oscillator. This implementation is shown in figure 7.

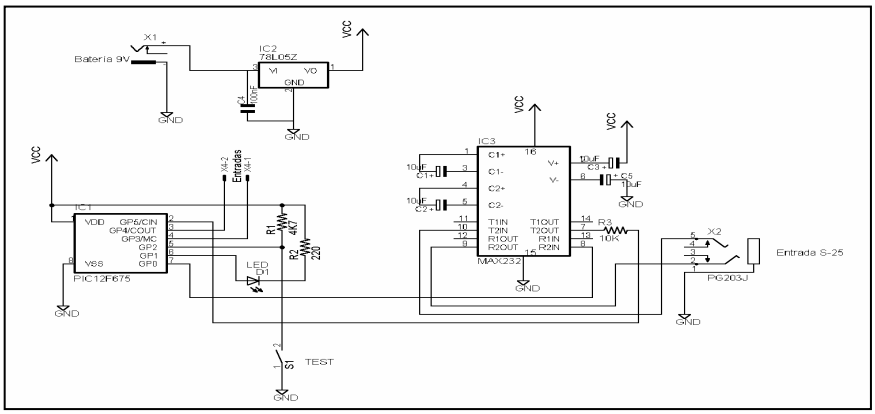

Figure 7. Schematic diagram with a PIC 12F675 microcontroller

6. CONCLUSION

The system described in this paper can be used in any telecontrol system with a GSM network. This allows management systems in places where a fixed network is not available. Furthermore, with a GSM network, we have a secure method of transmission which can feedback confirmation on request. The implementation, based on a simple RISC microcontroller and a standard mobile phone reduces the costs of the final system. The only disadvantage is that the systems will not work in areas where there is no GSM coverage.

Some of the principal applications of the system include alarm systems, process control systems, process or system supervision, GPS (Global Posotioning System)-GSM applications for remote locating systems and other applications involving remote control. And, finally, it also allows PC integration for post-processing work.

REFERENCES

[1] A. Tanenbaum, 2003. *"Computer Networks"*. Prentice Hall, New Jersey

[2] Ericsson. Yokohama, 1999 *"Proposal of how to handle the AT commands from 07.07 and 07.05"*.

[3] ETSI. *"Estándar ETSI GSM 03.40 y GSM 03.48, GSM 07.05 y GSM 07.07"*

[4] Maxim. Dallas Semiconductor. *"MAX232 Datahseet"*

[5] Microchip inc. *"16F84, 12F675 Datasheets"*

[6] M. Predko, 2000. "Programming and customizing PICmicro microcontrollers". McGraw-Hill,

[7] M. Predko, 2001. "PC Interfacing". McGraw-Hill,

[8] Siemens. *"S25 datahseet, SMS and PDU mode with S25"*

[9] Wavecom. "GSM modems datsheet"