SMS mangement using AT commands

A Thesis Submitted in Partial Fulfillment of the Requirements for Degree of M.Sc in Telecommunication Engineering

Prepared By: Ahmed Ibrahim Ahmed Abdelkareem
Supervisor: Dr. Abd Elrasoul Gabar Alzubaidi

Jan 2014
قال تعالى:

{قالوا سبحانك لعلمنا إلا ما علمتنا إنك أنت عاليم الحكيم

صدق الله العظيم

الإيّة (32) سورة البقرة
Dedication

I dedicate this research to all knowledge seekers
May you benefit from it.

To all my Family, for there unlimited support.

To the memory of my father, my sister and all the beloved ones
may you rest in heaven.
ACKNOWLEDGEMENT

First of all, I would like to thanks Allah for shedding on me good health and keeping my brain working to the extent completing this research.

Next, to the Center of Engineering And Technical Studies (CETS) and many thanks to my supervisor Dr. Abd Elrasoul Gabar Alzubaidi, especially, I would like to sincerely thank him for his valuable advice and the continuous effort that exerted while I was carrying out this study. Sincere appreciation goes to my parents, wife, son, brothers, sisters and all my friends.
ABSTRACT

This project will focus on developing an enhancement of the computer ability to manage SMS.

Telecommunication getting involved in the everyday life of every person, SMS & AT commands in particular were a transforming technologies. They didn’t change people way of communication only, but the way PC’s communicate too. Which made the Idea of o this project interesting area to explore.

The Project “Managing SMS using AT commands”, aiming to build a computer program that is able to send AT commands to GSM modem to control it for Short Message service, sending, receiving, deletion.. etc.

Program will built using Matlab, C# and VB, will communicate with serial port, initialize the port then send the AT commands and read the response from the serial port and throw it back to the program.

Expected results will be the three running programs that are able to communicate with GSM modem by using AT commands, a comparison table to be built for the results.
المستخلص

يركز هذا المشروع على تطوير وتعزيز القدرة على إدارة جهاز الكمبيوتر لخدمة الرسائل النصية.

الاتصالات أصبحت جزءاً من الحياة اليومية لكل شخص، والرسائل القصيرة وأوامر AT بشكل خاص كانت تكنولوجيات فارقة. أنها لم تغير وسيلة اتصالات الناس فقط، ولكن في طريقة تواصل الحواسيب أيضاً.

الأمر الذي جعل فكرة البحث في هذا المشروع مثيرة للاهتمام والاستكشاف.

مشروع "إدارة الرسائل النصية القصيرة باستخدام أوامر AT" يهدف إلى بناء برنامج كمبيوتر قادر على إرسال أوامر AT لمودم (جي إس إم) للسيطرة عليها لخدمة الرسائل القصيرة، وإرسالها واستلامها، حذف .. الخ

و البرنامج سوف يبني باستخدام VB و C#، Matlab، وال التواصل مع المنفذ التسلسلي، لتهيئة الميناء ومن ثم إرسال الأوامر AT وقراءة استجابة من المنفذ التسلسلي وارجاعها مرة أخرى إلى البرنامج.

النتائج المتوقعة من المشروع إنشاء برنامج تشغيل قادر على التواصل مع مودم (جي إس إم) باستخدام أوامر AT، مع جدول للمقارنة لاحتواء النتائج.
# Contents

1. **Introduction** .................................................................................................................. 1
   1.1 Background .................................................................................................................... 1
   1.2 Problem Statement ........................................................................................................ 2
   1.3 Objective ....................................................................................................................... 2
   1.4 Methodology .................................................................................................................. 2
   1.5 Research plan ............................................................................................................... 3

2. **Literature review** ............................................................................................................ 4
   2.1 GSM ............................................................................................................................... 4
      2.1.1 Evolution of mobile networks .................................................................................. 5
      2.1.2 The GSM network .................................................................................................. 9
   2.2 SMS Service .................................................................................................................. 15
      2.2.1 SMS Network element ......................................................................................... 16
      2.2.2 SMS Flow ............................................................................................................. 19
   2.3 AT Commands ................................................................................................................. 25
      2.3.1 Hayes' commands ................................................................................................. 25
      2.3.2 Hayes' solution ...................................................................................................... 27
      2.3.3 Commands ............................................................................................................. 28

3. **Managing SMS using AT COMMANDS** ...................................................................... 43
   3.1 Interfacing Principle ....................................................................................................... 43
   3.2 Summary of commands .................................................................................................. 45
   3.3 Case #1: Managing SMS via HyperTerminal ............................................................... 46
      3.3.1 Checking the modem configuration ....................................................................... 46
      3.3.2 Connecting using the Hyper Terminal ................................................................. 46
   3.4 Case#2: Managing SMS via Matlab ............................................................................. 50
      3.4.1 Getting INFO ......................................................................................................... 50
      3.4.2 Sending .................................................................................................................. 52
      3.4.3 Listing .................................................................................................................... 53
      3.4.4 Reading ............................................................................................................... 54
3.5 Case#3: Managing SMS via C# ................................................................. 55
  3.5.1 Connecting to serial port ................................................................. 55
  3.5.2 Getting Info ..................................................................................... 56
  3.5.3 Sending ............................................................................................ 57
  3.5.3 Reading ............................................................................................ 58
  3.5.4 Deleting ........................................................................................... 60
  3.5.5 SMS APP (complete source C# code) ............................................. 61
3.6 Case#4: Managing SMS via Visual Basic ............................................. 75
  3.6.1 Connecting to serial port ................................................................. 75
  3.6.2 Sending ............................................................................................ 75
  3.6.3 Reading ............................................................................................ 76
  3.6.4 Deleting ........................................................................................... 78
  3.6.5 SMS APP (complete source VB code) ............................................ 80

4. Results & Discussions ............................................................................. 90
  4.1 Results .................................................................................................. 90
  4.2 Discussion ........................................................................................... 91

5. Conclusion & Recommendations ........................................................... 93
  5.1 Conclusion ........................................................................................... 93
  5.2 Recommendations ............................................................................... 93
4 SMS Interface Description

4.1 Select the SMS type +CSMS

4.1.1 Command Syntax

Command Possible response(s)
+CSMS=<service> <CR><LF>+CSMS:
<mt>,<mo>,<bm><CR><LF><CR><LF>OK<CR><LF>
+CSMS?
<CR><LF>+CSMS:
<service>,<mt>,<mo>,<bm><CR><LF><CR><LF>OK<CR><LF>

HUAWEI UMTS Datacard/Modem AT Command Interface Specification Confidential
All rights reserved Page 33, Total 107

Command Possible response(s)
+CSMS=? <CR><LF>+CSMS: (list of supported <service>s)<CR><LF><CR><LF>OK<CR><LF>

4.1.2 Description

The SET command is used to set the message service type. The returned <mt>, <mo> and <bm> mean whether this service type is supported for the messages received by the terminal, messages sent by the terminal, and the broadcast messages.

4.2 Set message format +CMGF

4.2.1 Command Syntax

Command Possible response(s)
+CMGF[=<mode>] <CR><LF>OK<CR><LF>
+CMGF? <CR><LF>+CMGF:
<mode><CR><LF><CR><LF>OK<CR><LF>
+CMGF=? <CR><LF>+CMGF: (list of supported <mode>s)<CR><LF><CR><LF>OK<CR><LF>

4.2.2 Description

The SET command is used to set the format of the short message. The format has two modes, and depends on the <mode> parameter. The two modes are: PDU mode and text mode. The "text" mode is unable to display Chinese, so currently, only the PDU mode is used. For the format of message in the PDU mode, see also "+CMGS command". The READ command is used to return the current mode selection. The TEST command returns the applicable <mode> values.

4.2.3 Defined Values

<mode>:

HUAWEI UMTS Datacard/Modem AT Command Interface Specification Confidential
All rights reserved Page 34, Total 107

0 PDU mode
1 text mode not supported currently.
If no <mode> is included, it is equivalent to the effect that the <mode> is 0.

4.3 Message arrival indication +CMTI

4.3.1 Command Syntax

Command Possible response(s)
<CR><LF>+CMTI: <mem>,<index><CR><LF>

4.3.2 Description

Indicate that a new message (or new message report) is received.

4.3.3 Defined Values

<mem>: Currently, only "SM" is supported.
"BM" Broadcast message storage
"ME" ME message storage
"MT" ME-associated storage
"SM" (U)SIM message storage
"TA" TA message storage
"SR" State report storage

<index>: Integer value, which indicates the position in the storage.

4.4 Indication of new message reported directly +CMT

4.4.1 Command Syntax
Command Possible response(s)

<CR><LF>+CMT: [<reserved>],<length><CR><LF><pdu><CR><LF>

4.4.2 Description
Received new messages are not stored, but reported to TE directly.

4.5 Newly received message state report +CDSI

4.5.1 Command Syntax
Command Possible response(s)

<CR><LF>+CDSI: <mem>,<index><CR><LF>

4.5.2 Description
Indicate that a new message state report is received, and specify the storage position.

4.5.3 Defined Values
<mem>: Currently, only "SM" is supported.
"SM" (U)SIM message storage
<index>: Integer value, which indicates the position in the storage.

4.6 Indication of new message state report reported directly +CDS

4.6.1 Command Syntax
Command Possible response(s)

<CR><LF>+CDS: <length><CR><LF><pdu><CR><LF>

4.6.2 Description
Received new messages are not stored, but reported to TE directly.

4.7 New message notification setting +CNMI

4.7.1 Command Syntax
Command Possible response(s)

+CNMI=[<mode>[,<mt>[,<bm>[,<ds>[,<bfr>]]]]]<CR><LF>

+CNMI? <CR><LF>
<CR><LF>OK<CR><LF>

+CNMI? <CR><LF>
<CR><LF>+CNMI: (list of supported <mode>s),(list of supported <mt>s),
(list of supported <bm>s),(list of supported <ds>s),(list of supported <bfr>s)
<CR><LF><CR><LF>OK<CR><LF>

4.7.2 Description
The "SET" command is used to set the program of reporting new message to TE, where,
<mode> and <bfr> are used to set the mode of reporting the new message notification
(including four types: +CMT, +CMTI, +CDSI, +CDS) to the TE.
HUawei UMTS Datacard/Modem AT Command Interface Specification Confidential
All rights reserved Page 37 Total 107
<mt> is used to set whether reporting the new message to the TE, or storing the new
message in the MS and reporting the storage position when a new message is received.
<bm> is not in use currently.
<ds> is used to set whether to report the message state report (+CDSI, +CDS).
The TEST command returns the supported parameter values.
Note: The set value of this command will be cleared to 0 after the MS is restarted. In this case, no new message will be reported. The "AT+CNMI=0,0,0,0,0" mode is not recommended.

4.7.4 Informative Examples
For example, set CNMI=1,1,0,1,0.
It indicates that the new class1 messages will be stored in the MS first, and the storage position will be reported (+CMTI: ME,1}; the message state reports will be reported directly (+CDS: ).
When it is impossible to report the message notification (e.g. when in the online data mode), the message notification will be discarded.

4.8 Delete Message +CMGD

4.8.1 Command Syntax
Command Possible response(s)
+CMGD=<index>[,<delflag>]
<CR><LF>OK<CR><LF>
In case of SMS-related error:
<CR><LF>+CMS ERROR: <err><CR><LF>
+CMGD=?
<CR><LF>+CMGD: (list of supported <index>s)[,(list of supported <delflag>s)]<CR><LF><CR><LF>OK<CR><LF>

4.8.2 Description
EXECUTION command deletes message from memory <mem1> location <index>. For the setting of <mem1> and description, see the "+CPMS command". If the second parameter <delflag> is present and not set to 0 then the ME shall ignore <index> and follow the rules for <delflag> shown below. If deleting fails, +CMS ERROR: <err> is returned.
TEST command returns the valid memory locations and the supported values of <delflag>.
The TEST command returns the storage position where the message is currently stored, and the supported <delflag> values.

4.9 New Message Acknowledgement to +CNMA

4.9.1 Command Syntax
Command Possible response(s)
+CNMA[=<n>[,<length>]<CR>]
PDU is given<ctrl-Z/ESC>]]]
<CR><LF>OK<CR><LF>
In case of SMS-related error:
<CR><LF>+CMS ERROR: <err><CR><LF>
+CNMA=? <CR><LF>+CNMA: (list of supported <n>s)<CR><LF><CR><LF>OK<CR><LF>

4.9.2 Description
EXECUTION command confirms reception of a new message which is routed directly to the TE. This acknowledgement command shall be used when +CSMS parameter <service> equals 1. For the usage of this command, see also description of "+CNMI" command.
In PDU mode, it is possible to send either positive (RP-ACK) or negative (RP-ERROR) acknowledgement to the network. Parameter <n> defines which one will be sent. Optionally, an acknowledgement TPDU (SMS-DELIVER-REPORT for RP-ACK or RP-ERROR) may be sent to the network. The entering of PDU is done similarly as specified in command Send Message +CMGS, except that the format of <ackpdu> is used instead of <pdu>. PDU shall not be bounded by double quotes.
MS shall not send another +CMT or +CDS result code to TE before previous one is acknowledged.
If ME does not get acknowledgement within required time (network timeout), ME
should send RP-ERROR to network, and should shall automatically disable routing to 
TE by setting both <mt> and <ds> values of +CNMI to zero.
To make the MS report the message notification again, you need to set <mt> and <ds> 
again.
If the command is executed but no message is available for confirmation, the "+CMS 
ERROR" will be returned: <err>
HUAWEI UMTS Datacard/Modem AT Command Interface Specification Confidential
All rights reserved Page 41, Total 107
The TEST command returns the supported <n> values. If only 0 is supported, it 
indicates that the command does not support TPDU sending.

4.10 Message storage selection +CPMS

4.10.1 Command Syntax
Command Possible response(s)
+CPMS=<mem1>[,<mem2>,<mem3>]

<CR><LF>+CPMS:
<used1>,<total1>,<used2>,<total2>,<used3>,<total3><
<CR><LF><CR><LF>OK<CR><LF>
In case of MS-related error:
<CR><LF>+CME ERROR: <err><CR><LF>
HUAWEI UMTS Datacard/Modem AT Command Interface Specification Confidential
All rights reserved Page 45, Total 107
Command Possible response(s)
+CPMS?

+CPMS:
<mem1>,<used1>,<total1>,<mem2>,<used2>,<total2>,
<mem3>,<used3>,<total3><CR><LF><CR><LF>OK<
CR><LF>
In case of MS-related error:
<CR><LF>+CME ERROR: <err><CR><LF>
+CPMS=?

+CPMS: (list of supported <mem1>s),(list of supported 
<mem2>s),
(list of supported 
<mem3>s)<CR><LF><CR><LF>OK<CR><LF>

4.10.2 Description
The SET command is used to set the message storage media corresponding to the 
message read/write operations, and return the current use state of the selected media.
The READ command returns the name and use state of the currently selected media.
The TEST command returns all the media types supported by the MS.

4.11 Reporting message storage media being full
^SMMEMFULL

4.11.1 Command Syntax
Command Possible response(s)
<CRLF>^SMMEMFULL:<mem_type><CR><LF>

4.11.2 Description
When the message storage media overflow, the event will be reported automatically.

4.11.3 Defined Values
<mem_type>:
String value. It indicates the type of the overflowing media.
"SM", which means the (U)SIM card.
"ME", which means NV

4.12 SMSC number command +CSCA

4.12.1 Command Syntax
Command Possible response(s)
+CSCA=<sca>[,<tosca>]

<CR><LF>OK<CR><LF>
In case of MS-related error:
<CR><LF>+CME ERROR: <err><CR><LF>
+CSCA?
<CR><LF>+CSCA:
4.12.2 Description
The SET command is used to set the SMSC number. For the message in the PDU mode, the setting of this command can be used only if the SMSC-related parameter `sc_len` has the value of 0 (for the PDU format, see the "+CMGS" command) in the PDU.

4.12.3 Defined Values
- `<sca>`: String value. It indicates the SMSC number. The number is composed of "*", "+", ",#" and "0" to "9". The number contains 20 characters at most.
- `<tosca>`: Integer value. It indicates the number type, where "145" means an international call. For the specific values, see also the definition of the "type_addr" parameter in the SC number, as described in the section "Short message sending +CMGS".

If no `<tosca>` parameter is included, it is equivalent to the effect that the `<tosca>` parameter is not modified.

4.13 Message sending +CMGS
4.13.1 Command Syntax
**Command Possible response(s)**
+CMGS=<length><CR>
PDU is given<ctrl-Z/ESC>
<CR><LF><MR>,<ackpdu><CR><LF><CR><LF>OK<CR><LF>

In case of MS-related error:
+CMS ERROR: <err><CR><LF>
+CSCA=?<CR><LF>OK<CR><LF>

4.13.2 Interface Description
Send a message to the network side. The process of sending a message includes two steps:
- First, deliver "+CMGS=<length>" ended with (CR).
- After MS returns `<CR><LF><greater_than><space>` (IRA 13, 10, 62, 32), the TE delivers the PDU packet, which is ended with `<ctrl-Z>` (IRA 26).

4.13.4 Examples
The SMSC number is: 13902900, and the message is sent to the number: 13901000453, and the contents are: 0x53 0x4E 0x4E 0x3A ("华为" for UCS2 encode), then:

**If "+CSCA" has set SCA, then**

- a) When sending the message, the `<SCA>` field can be left uncompleted. The `<SCA>` value is obtained through the value set via "+CSCA" command.

  AT+CMGS=17(CR)
  >81000B813109010054F3001804534E3A \x1A

  (NUAWEI UMTS Datacard/Modem AT Command Interface Specification Confidential All rights reserved Page 53, Total 107

  Note: Data interpretation, 81(<RP~MTI>)00(<MR>)0B(<DA-len>)81(<DA-type>)
  534E3A(\x1A)<ctrl-Z>)

- b) When sending the message, the `<SCA>` field can also be completed, and the `<SCA>` value can be obtained directly from the PDU packet.

  AT+CMGS=17
  >05a13109920081000B813109010054F3001804534E3A \x1A

**If "+CSCA" has not set SCA, then**
When sending the message, the `<SCA>` field must be completed, and the `<SCA>`
4.14 Message storage command +CMGW

4.14.1 Command Syntax

Command Possible response(s)

+CMGW=<length>[,<stat>]<C
R>
PDU is given<ctrl-Z/ESC>
<CR><LF>
In case of SMS-related error:
<CR><LF>+CMS ERROR: <err><CR><LF>
+CMGW=? <CR><LF><CR><LF>OK<CR><LF>

4.14.2 Interface Description

Store a message to the <mem2> storage set via the "+CPMS" command.

4.15 Message list command +CMGL

4.15.1 Command Syntax

Command Possible response(s)

+CMGL=<stat><CR><LF>
In case of pdu mode and successful execution of command:
<CR><LF><index><CR><LF><CR><LF><pdu><CR><LF><CR><LF>OK<CR><LF>
Otherwise:
<CR><LF>+CMS ERROR: <err><CR><LF>
CM GL=? <CR><LF><CR><LF>OK<CR><LF>

4.15.2 Description

The EXECUTION command returns all messages from <mem1>, which are in the
state specified by the parameter <stat>. If the message state is "Unread message that
has been received", the state of the message in the storage will be converted to "Read
message that has been received" after the command is executed successfully.
When the <stat> takes on the default value, the EXECUTION command is equivalent
to the SET command +CMGL=0.
The TEST command returns all the supported stat values.

4.16 Read a message +CMGR

4.16.1 Command Syntax

Command Possible response(s)

+CMGR=<index><CR><LF>
In case of pdu mode and successful execution of command:
<CR><LF><index><CR><LF><CR><LF><pdu><CR><LF><CR><LF>OK<CR><LF>
or:
<CR><LF>+CMS ERROR: <err><CR><LF>
CMGR=? <CR><LF><CR><LF>OK<CR><LF>

4.16.2 Description

The EXECUTION command returns the messages whose storage position is "index"
from <mem1>. If the message state is "Unread message that has been received", the
state of the message in the storage will be converted to "Read message that has been
received" after the command is executed successfully.
The TEST command returns OK.

4.16.3 Defined Values

<index>: Integer value, which indicates the position in the storage.
<stat>: Message type:
0 Unread message that has been received
1 Read message that has been received
2 Unsent message that has been stored
3 Sent message that has been stored
<reserved>: Reserved.
<length>: Integer value, which indicates the number of bytes of PDU data.
<pdu>: Protocol data unit. Its format is the same as defined in section “Message list command”.

4.17 Message bearer domain command +CGSMS

4.17.1 Command Syntax
Command Possible response(s)
+CGSMS=<service> <CR><LF>OK<CR><LF>
+CGSMS? <CR><LF>+CGSMS:<service><CR><LF><CR><LF>OK<CR><LF>
+CGSMS=? <CR><LF>+CGSMS: (list of supported
<service>s)<CR><LF><CR><LF>OK<CR><LF>

4.17.2 Description
The SET command is used to set the message bearer domain, namely, selection of CS/PS domain.
The READ command returns the current message bearer domain.
The TEST command returns the supported parameter values.

4.18 More Messages to Send +CMMS

4.18.1 Command Syntax
Command Possible response(s)
+CMMS=<n> <CR><LF>OK<CR><LF>
+CMMS? <CR><LF>+CMMS:<n><CR><LF><CR><LF>OK<CR><LF>
+CMMS=? <CR><LF>+CMMS: (list of supported
<n>s)<CR><LF><CR><LF>OK<CR><LF>

4.18.2 Description
Set command controls the continuity of SMS relay protocol link. When feature is enabled (and supported by network) multiple messages can be sent much faster as link is kept open.
Test command returns supported values as a compound value.
References


Internet

1. www.msdn.microsoft.com

2. www.google.com

3. www.stackoverflow.com
Abbreviations

- SMS  Short Message Service
- SM   Short Message
- SMC  Short Message Center
- SMSC Short Message Service (Schedule) Center
- MS   Mobile Station
- MSC  Mobile Switch Center
- HLR  Home Location Register
- VLR  Visit Location Register
- SMGW Short Message Gate Way
- DCS  Data Coding Scheme
- ETSI European Telecommunication Standardization Institute
- GSM  Global System for Mobile Communication
- MSISDN Mobile Subscriber ISDN (Telephone number or address of device)
- MS   Mobile Station
- PCI  Protocol Control Information
- PLMN Public Land Mobile Network
- PDU  Protocol Data Unit
- TCAP Transaction Capability Application Part
- UDCP USSD Dialogue Control Protocol
- UDH  User-Data Header (see [GSM 03.40])
- UDHL User-Data Header Length (see [GSM 03.40])
- UDL  User-Data Length (see [GSM 03.40])
- USSD Unstructured Supplementary Service Data
- AT   Attention command
Chapter One
Introduction
Chapter Two

Literature review
Chapter Three

Case studies
Chapter Four
Results & Discussions
Chapter Five

Conclusion & Recommendations