短信猫软件的实现(C#)<三>PDU 格式短信发送

作者：给我一杯酒 来自：博客园

AT 指令收发短信主要有两种模式：Text 模式和 PDU（Protocol Data Unit，协议数据单元）模式。使用 Text 模式收发短信代码简单，很容易实现，最大缺点不支持中文短信。PDU 模式不仅能发送中文短信，也能发送英文短信。PDU 收发短信有三种编码可用：7-bit、8-bit 和 UCS2 编码。7-bit 编码用于发送普通的 ASCII 字符，即英文短信，最多可发送 160 字符。8- bit 编码通常用于发送数据消息。UCS2 编码用于发送 Unicode 字符，可发送中文字符，最多发送 70 字符。

短信发送实例：

Text 模式（向号码为 15050850677 的手机发送"TEST"）：

```
1:  AT                          //发送 AT 返回 OK 连接成功
2:
3:  OK
4:
5:  AT+CMGF=1                   //设置为 Text 模式
6:
7:  AT+CMGS="15050850677"       //发送指令，双引号内改为对用手机号码
8:
9:  > TEST(+^z,十六进制的 1A)//返回字符串中有 OK 发送成功 >号为设备返回字符
```

PDU 模式（向号码为 15050850677 的手机发送"你好"）：

```
1:  AT                          //发送 AT 返回 OK 连接成功
2:
3:  OK
4:
5:  AT+CMGF=0                   //设置为 PDU 模式
6:
7:  AT+CMGS=19                  //发送指令，更改为对应 PDU 编码的长度计算方法在后面
8:
9:  > 0011000D91685150800576F70008C4044F60597D(+^z,十六进制的 1A)//返回字符串中有 OK 发送成功
```

有的“猫”用“串口调试器”发送总是失败：Text 模式接收到的是乱码，PDU 模式发送不出去。我用的这个就是这个样子，给我郁闷了很多天，后来发现在串口调试器中我们摁下的“回车”被解析为”\r\n”，而我用的这个 modem 只有在只发送 AT 指令+”\r”时才能正确的发送短信。发现后发送短信都能成功，高兴了好一会儿。不说废话了，开始 PDU 短信编码的解析。这是我的理解，更多详细资料参考下列标准：

GSM 03.04　着重介绍短信发送中对字符集的控制部分
GSM 03.08
GSM 03.41
GSM 07.05　介绍 at 的一些控制命令
GSM 07.07　着重介绍 at 的短信相关命令，可以说是 at 的 sms 规范

元素	名称	长度	描述
SCA	Service Center Address	1-12	短消息服务中心号码
PDU-Type	Protocol Data Unit	1	协议数据单元类型
MR	Message Reference	1	所有成功的短信发送参考数目（0..255）
OA	Originator Address	2-12	发送方地址（手机号码）
DA	Destination Address	2-12	接收方地址（手机号码）
PID	Protocol Identifer	1	参数显示消息中心以何种方式处理消息内容（比如 FAX,Voice）
DCS	Data Coding Scheme	1	参数显示用户数据编码方案
SCTS	Service Center Time Stamp	7	消息中心收到消息时的时间戳
VP	Validity Period	0,1,7	参数显示消息有效期
UDL	User Data Lenghth	1	用户数据长度
UD	User Data	0-140	用户数据

发送方 PDU 格式：

SCA	PDU-Type	MR	DA	PID	DCS	VP	UDL	UD
1-12	1	1	2-12	1	1	0,1,7	1	0-140

示例：

向 15050850677 发送一条短信，内容“Test”

0011000D91685150800576F70000C404D4F29C0E

向 15050850677 发送一条短信，内容“你好”

0011000B815150800576F70008C4044F60597D

SCA	PDU-Type	MR	DA	PID	DCS	VP	UDL	UD
1-12	1	1	2-12	1	1	0,1,7	1	0-140

00	11	00	0D91685150800576F7	00	00	C4	04	D4F29C0E
00	11	00	0B815150800576F7	00	08	C4	04	4F60597D

接收方 PDU 格式：

SCA	PDU-Type	OA	PID	DCS	SCTS	UDL	UD
1-12	1	2-12	1	1	7	1	0-140

示例：

从 15050850677 接收一条短信，内容“Test”

0891683110402505F0240BA15150800576F70000011120816030230 4D4F29C0E

从 15050850677 接收一条短信，内容“你好”

0891683110402505F0240BA15150800576F70008011120816004230 44F60597D

SCA	PDUType	OA	PID	DCS	SCTS	UDL	UD
1-12	1	2-12	1	1	7	1	0-140
08916831104025 05F0	24	0BA151508005 76F7	00	00	01112081603 023	04	D4F29C 0E
08916831104025 05F0	24	0BA151508005 76F7	00	08	01112081600 423	04	4F6059 7D

SCA:短消息服务中心地址格式

服务中心地址包含三个部分：1-12 个 8 位位组 第一个位组指示服务中心地址长度，第二个位组指示服务中心类型，第三个位组为服务中心地址。

示例：0891683110402505F0

Lenghth	Type	Address
08	91	683110402505F0

Lenghth：服务中心地址长度 指示 Type+Address 部分位组长度（例中：91683110402505F0 中位组 8 个：08）
如果 Lenghth 部分为“00”则不提供后面部分，发送时终端将自动从 SIM 卡中读取并填充 SCA

Type：短信中心地址的类型（81：指国内的号码 91：指国际的号码 91 最常用）
91H=10010001B 具体意义如下表：

BIT No.	7	6	5	4	3	2	1	0
	1	类型	类型	类型	号码鉴别	同 3	同	同 3

类型：000-未知　001-国际　010-国内　111-留作扩展

号码鉴别：0000-未知　0001-ISDN/电话号码（E.164/E.163）　1111-留作扩展

SCA 示例：

短信中心	PDU 编码
+8613010452500	0891683110402505F0
13010452500	07813110402505F0
123456	0481214365

注：AT 指令中 AT+CMGS=<Len> Len 不包含此段位组的长度

PDU Type:是发送和接受短信的 PDU 中的第一个 8 位位组

发送方：例 11h=00010001b

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRR	VPF	VPF	RD	MTI	MTI
	0	0	0	1	0	0	0	1

接收方：例 24h=00100100b

Bit No.	7	6	5	4	3	2	1	0
	RP	UDHI	SRI			MMS	MTI	MTI
	0	0	1	0	0	1	0	0

RP:应答路径，
0-未设置
1-设置

UDHI:用户数据头标识（User Data Header Indicator），
0-用户数据（UD）部分不包含头信息
1-用户数据（UD）开始部分包含用户头信息

SRR：请求状态报告（Status Report Request），
0-不需要报告
1-需要报告

SRI:状态报告指示（Status Report Indication），此值仅被短消息服务中心设置，
0-状态报告将不会返回给短消息实体（SME）
1-状态报告将返回给短消息实体（SME）

VPF:有效期格式（Validity Period Format），
00-VP 段没有提供（长度为 0）

01-保留
10-VP 段以整型形式提供（相对的）
11-VP 段以 8 位位组的一半形式提供（绝对的）

RD:拒绝复本（Reject Duplicate）
0-通知短消息服务中心（SMSC）接受一个消息（SMS-SUBMIT），即该消息是先前已提交过的，并还存在与 SMSC 中未发送出去。MS 重复的条件是：消息参考（MR）、接收方地址（DA)及发送方地址（OA）相同
1-通知 SMSC 拒绝一个重复的 SMS

MMS:有更多的消息需要发送（More Message to Send），此值仅被 SMSC 设置
0-在 SMSC 中有更多的信息等待 MS
1-在 SMSC 中没有更多的信息等待 MS

MTI:信息类型指示（Message Type Indicator）
不太理解 有待于再查资料

MR：信息参考 不太理解 置为 00 即可

DA/OA：接收方与发送方地址

DA 与 OA 编码方式是一样的 2-12 个 8 位位组

例：0D91685150800576F7

Lenghth	Type	Address
0D	91	685150800576F7

Lenghth：地址长度 指 8615050850677 的长度。与 SCA 中不一样！
Type：地址类型 指示国内（81） 还是国际（91）

示例：

号码	PDU 编码
+8615050850677	0D91685150800576F7
15050850677	0B815150800576F7
123456	0681214365

PID:协议标识（Protocol Identifier）

对于标准情况下的 MS-to-SC 短消息传送，只需设置 PID 为 00

DCS：数据编码方案（DataCoding Scheme）

Bit No. 7 6 5 4 3 2 1 0 描述

示例： 0 0 0 0 0 0 0 0 00h 7bit 数据编码 默认字符集

1 1 1 1 0 1 1 0 F6h 8bit 数据编码 Class1

0 0 0 0 1 0 0 0 08h USC2（16bit）双字节字符集

Bit No.7 与 Bit No.6：
一般设置为 00

Bit No.5：
0-文本未压缩
1-文本用 GSM 标准压缩算法压缩

Bit No.4：
0-指示 Bit No.1 Bit No.0 为保留位，不含信息类型信息
1-指示 Bit No.1 Bit No.0 含信息类型信息

Bit No.3 与 Bit No.2：
00-默认的字符集，每字符占 7bit，此时最大可发送 160 字符
01-8bit，此时最大可发送 140 字符
10-USC2（16bit），发送双字节字符集
11-预留

Bit N0.1 与 Bit No.0：
00-Class 0，短消息直接显示在屏幕上
01-Class 1，
10-Class 2（SIM 卡特定信息），
11-Class 3

示例：

DCS	字符集	信息 Class
00	7-bit	No Class
F0	7-bit	Class 0（Immediate Display）
F1	7-bit	Class 1（Mobile Equipment-specific）
F2	7-bit	Class 2（SIM specific Message）
F3	7-bit	Class 3（Terminate Equipment-specific）
F4	8-bit	Class 0（Immediate Display）
F5	8-bit	Class 1（Mobile Equipment-specific）
F6	8-bit	Class 2（SIM specific Message）
F7	8-bit	Class 3（Terminate Equipment-specific）
08	16-bit	No Class
18	16-bit	Class 0（Immediate Display）

VP：信息有效期（Validity Period）

第一种情况（相对的）：VPF=10 VP=AAH（四天）

第二种情况（绝对的）：VPF=11

年	月	日	时	分	秒	时区
03	80	02	90	54	33	20

表示：03-08-20 09:45:33

VP 段以整形或半个 8 位位组形式提供

第一种情况，VP 为一个 8 位组，给定有效期的长度
从消息被 SMSC 接收开始计算

VP	相应的有效期
00-8F	（VP+1）*5 分钟　从 5 分钟间隔到 12 小时
90-A7	12 小时+（VF-143）*30 分钟
A8-C4	（VP-166）*1 天
C5-FF	（VP-192）*1 周

第二种情况，VP 为七个 8 位组，给定有效期终止的绝对时间　时间形式与 SCTS 形式一致

SCTS：服务中心时间戳（Service Center Time Stamp）

占用 7 个 8 位组，格式和 VP 第二种情况一致，请参考其中的表格

UDL：用户数据长度（User Data Lenghth）

UDL 以整形形式提供，指示后面用户数据段的长度（UD 的 8 位组的个数）

UD：用户数据（User Data）

英文编码：7bit 编码，依次将下一位的后几位移至前面形成新的 8 位编码
示例：Test

T:01010100　e:01100101　s:01110011　t:01110100

去最高位 0，变为 7 位

T：1010100　e：1100101　s：1110011　t：1110100

后面低位移至前面形成 8 位编码

Test:11010100111100101001110000001110

UD:D4F29C0E　UDL:04

中文编码：取 USC2 编码　高低字节交换即可

注：AT+CMGS=<Len><cr>中 Len 为出 SCA 外 8 位组的个数

参考资料：SMS with the SMS PDU-mode