Version： V1.7.4

Confidential

GS503 aged mobile phone Communication Protocol

Shenzhen Concox Information Technology Co., Ltd

document to any person or company is prohibited.

CONTENT

1. Communication Rule

1.1 Instruction

This article defines the instruction of the protocol between GPS senior phone, tracking service platform and application layer interface.

1.2 EMC

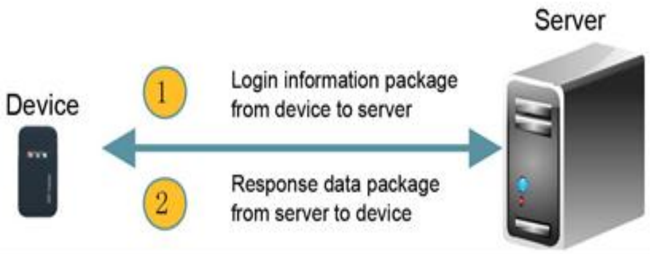
The platform version is suitable for GS503 platform version.

2. Term and definition

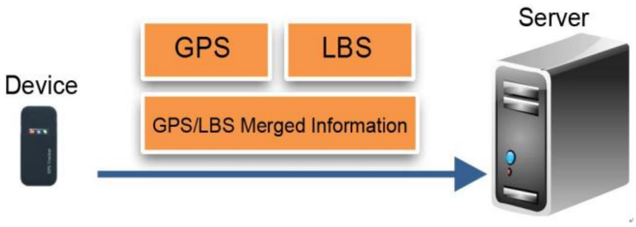
term、A.D.	English meaning	Chinese meaning
CMPP	China Mobile Peer to Peer	中国移动点对点协议
GPS	Global Positioning System	全球卫星定位系统
GSM	Global System for Mobile Communication	全球移动通信系统
GPRS	General Package Radio Service	通用无线分组业务
TCP	Transport Control Protocol	传输控制协议
LBS	Location Based Services	辅助定位服务
IMEI	International Mobile Equipment Identity	国际移动设备识别码
MCC	Mobile Country Code	移动用户所属国家代号
MNC	Mobile Network Code	移动网号码
LAC	Location Area Code	位置区码
CI	Cell ID	移动基站
RSSI	Received Signal Strength Indicator	接收信号强度
UDP	User Datagram Protocol	用户数据报协议
SOS	Save Our Ship/Save Our Souls	遇难求救信号
CRC	Cyclic Redundancy Check	循环冗余校验
NITZ	Network Identity and Time Zone,	时区
GIS	Geographic Information System	地理信息系统

3. Basic rule

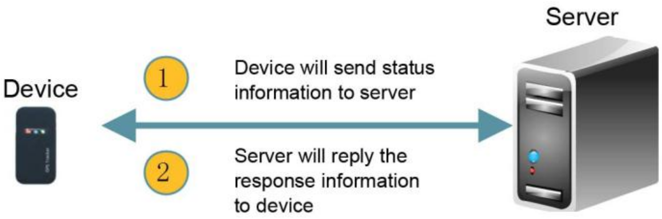
1. The equipment starts login package default sending and waits for the confirmation of the server.


Server
Device
1
Login information package from device to server
2
Response data package from server to device

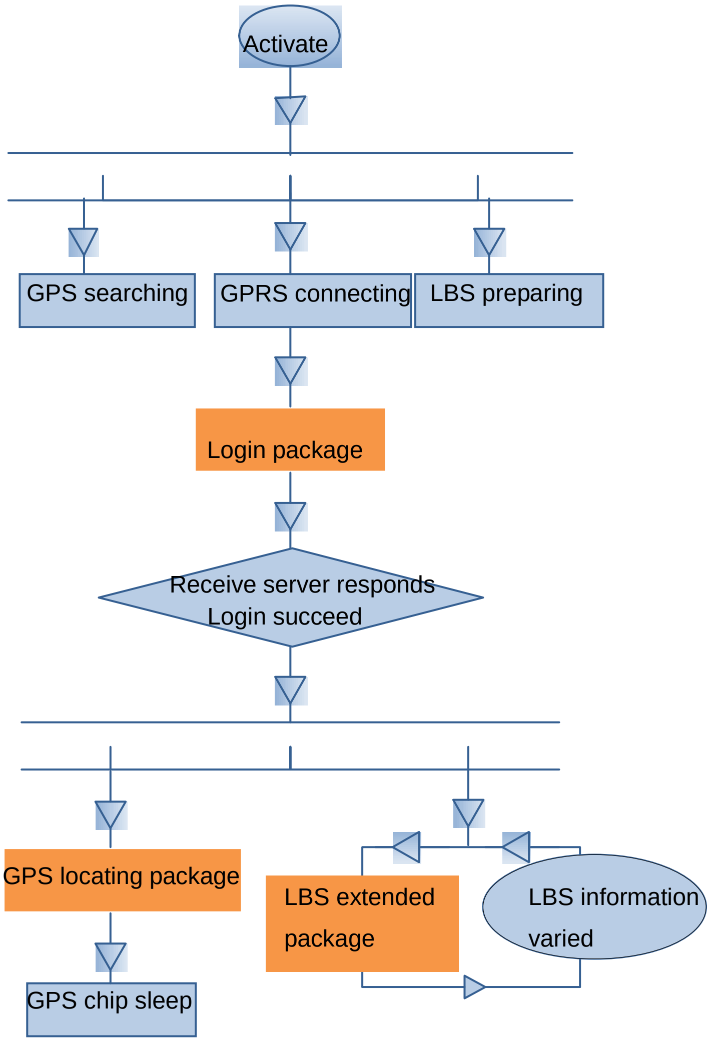
2 .After the connections normally establish and GPS information change, the device will regularly send GPS, LBS combined package or separately send GPS package and LBS package to the server, then sever can set the defaulted sending protocol in according with the instruction.



3. In order to protect the validity of connections，the device will send status information to server at fixed intervals then the server return responding package switching for confirmation.


Server
Device
1
Device will send status information to server
2
Server will reply the response information to device

GS503 Basic work procedure：



4 Data-package format

Communication transmission is in asynchronous mode and takes byte as unit. It transfers serial data stream of every uncertain length data package between device and server.

Data package length：（10+N）Byte

Format	Start Bit	Package Length	Protocol number	Information content	Information serial number	Error checking	Stop Bit
Length(Byte)	2	1	1	N	2	2	2

4.1 Start bit

Fixed value，unified by hexadecimal.0x78 0x78。

4.2 Package length

Length=Protocol number + Information content + information serial number +error check,（5+N）Byte in total, as the information Content is uncertain length data.

4.3 Protocol number

The different protocol numbers are according to different information content.

Type	Value
Login package	0x01
GPS package	0x10
LBS package	0x11
GPS、LBS combined package	0x12
Status package	0x13
Satellite signal noise ratio package	0x14
Character string package	0x15
GPS、LBS、status combined package	0x16
LBS、telephone number address searching package	0x17
LBS extension package	0x18
LBS、status combined package	0x19
GPS、telephone number address searching package	0x1A
GPS、LBS extension package	0x1E
Server send instruction to device package（setting）	0x80
Server send instruction to device package（Searching）	0x82

4.4 Information serial number

After turning on the device, it will send the first item of GPRS data (including heartbeat package and GPS/LBS data package); the serial number of this item is “1”. After that, the serial number will be added on by 1 automatically at every sending process (including heartbeat package and GPS/LBS data package).

4.5 Information content

Connect to different application. Correspond to the “protocol number” and confirm the specific content.

4.5.1 Login package（0X01）

Format	Info content		
	Device ID	Type identity code	Extended bit
Length	8	2	2

Login Information Package is used to confirm whether the connection is normal and submit device ID to server.

Note: Login Information Package has two visions.

Old vision: No extended bit

New vision: With extended bit

4.5.1.1 Information content

4.5.1.1.1 Device ID

Device ID users 15 digits of IMEI number.

For example：123456789012345，

Device ID：0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45

4.5.1.1.2 Type identity code

Type identity code occupies 2 bytes. The type of the device can be judged on the basis of this identity code. GS503 Senior Phone has different type identity code according to functional areas.

Function	Type identity code
GPS+ message sending +Multi-base station	100F
LBS+ message sending + Multi-base station	1010
GPS+ no message + Multi-base station	XX
LBS+ no message + Multi-base station	XX
GPS+ message sending + Single base station	100C
LBS+ message sending + Single base station	100D
GPS+ no message + Single base station	1006
LBS+ no message + Single base station	1009

4.5.1.1.3 Extended bit

Nibble bit15—bit4												Lsb nibble bit4-bit0			
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Value of time zone extended 100												East/West Time Zone	No defin	Language	Language

		ition	Select 1	Select 0

Note:

Bit3 0------East time zone
1------West time zone

If: Extended bit:0X32 0X00 means east eight zone,GMT+8:00.
Computing method：8*100=800，turn to hexadecimal，0X0320

Extended bit：0X4D 0XD8 means west twelve zone and 3/4,GMT-12:45.
Computing method：12.45*100=1246,turn to hexadecimal，0X04,0XDD.

Computing method is to shift 4 bits left of the time zone calculated, then combine with time zone East/West, thus saving 4 bits for language select.

4.5.1.2 Server response

For example：

Device->Server（here the device ID is 123456789012345）

0x78 0x78	0x0D	0x01	0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45	0x10 0x04	0x00 0x01	0x8C 0xDD	0x0D 0x0A
Start bit	length	Protocol number	Device ID	Identity code	Serial Number	CRC verify	End bit

Login package with extended bit:

0x78 0x78	0x11	0x01	0x03 0x53 0x41 0x90 0x30 0x09 0x96 0x21	0x10 0x06	0x32 0x01	0x00 0x01	0x37 0x6C	0x0D 0x0A
Start bit	length	Protocol number	Device ID	Identity code	Extended Bit	Serial Number	CRC verify	End bit

Server-> Device:（The protocol number in response package are the same as the one has been sent by device.）

0x78 0x78	0x05	0x01	0x00 0x01	0xD9 0xDC	0x0D 0x0A
Start bit	Length	Protocol number	Serial Number	CRC verify	End bit

4.5.1.3 Function

When connecting with platform at the first time, the device sends the package so the platform could indicate different ID.

4.5.2 GPS information package （0X10）

Format	Information content						
	Date and Time	GPS information					Reserved extension bit
		GPS information length and satellites involved in locating	Latitude	Longitude	Speed	Course and status	
Length (Byte)	6	1	4	4	1	2	N

4.5.2.1 Date and time

Format	Year	Month	Day	Hour	Minute	Second
Length (Byte)	1	1	1	1	1	1

For example：3:50:23 a.m. Mar 23rd 2010

The value：0x0A 0x03 0x17 0x0F 0x32 0x17

4.5.2.2 GPS information length、the number of the satellites involved in locating

1 byte converts to binary 8 bit, the first 4 bit means GPS info length, the late 4 bit means number of satellite involved in locating.

Note: The length includes 1 byte occupied by itself.

For example: 0x9C means GPS information length is 9 bytes, the number of satellite involved in locating is 12.

4.5.2.3 Latitude

Occupy 4 bytes, representing the latitude value. Number range is from 0 to 162000000, which represents the range form 0°to 90°.Unit: 1/500 second

Conversion method:

A Convert the latitude (degrees, minutes) data from GPS module into a new form which represents the value only in minutes;

B Multiply the converted value by 30000, and then transform the result to hexadecimal number

For example22°32.7658′,（22×60＋32.7658）×30000=40582974,then convert it to hexadecimal number 0x02 0x6B 0x3F 0x3E

4.5.2.4 Longitude

Occupy 4 bytes, representing the longitude value of location data. Number ranges from 0 to 324000000, representing the range form 0°to 180°.Unit: 1/500 seconds, Conversion method is the same as latitude’s.

4.5.2.5 Speed

Occupy 1 bytes, representing the speed of the device; 0x00～0xFF means ranges from 0 to 255,Unit: kilometer/hour.

4.5.2.6 Status/Course

Occupy 2 bytes; representing the moving direction of the device; ranges from 0-360; unit: degree, regards due north as 0 degree; clockwise.

One byte is composed of eight binary. In the first byte, the first six binary represents status. The last two binary and the whole eight binary in the second byte (10 binary in total) represents course

First byte								Second byte							
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1
（undefined）	（undefined）	Real time/gap GPS	GPS location fixed or not	East longitude、west longitude	South latitude、north latitude	course									

0：South latitude　　1：North latitude

0：East longitude　　1：West longitude

0：GPS has not located　　1：GPS has located

0：Real time GPS　　1：Different GPS

Note: The status information refers to the status in a certain time

For example: 0x05 0x4C convert to binary 00001010 1001100, representing GPS has located、 real time GPS、north longitude、east latitude、Course 332°

4.5.2.7 Reserved bit

The reserved bit is 2byte.

Nibble bit15—bit4												Lbs nibblebit4-bit0			
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
No definition														Language Select 1	Language Select 0

Language Select 0=1(or 0), language select 1=0, indicates SMS asking platform to reply location in Chinese.

Language Select 0=0, language select 1=1, indicates SMS asking platform to reply location in English.

For example, extended bit 0x00 0x00 or 0x00 0x01 indicates asking for location in Chinese. 0x00 0x02 indicates asking for location in English.

4.5.2.8 Server response

Need to respond server.

Server response after receiving status package sent by device（10 Byte）					
Start bit	Length	Protocol Number	Serial Number	CRC verify	End bit
2	1	1	2	2	2

4.5.2.9 Function

Upload GPS location after the device connects with platform and locate GPS.
Activate when GPS operate for a long time, for example, when GPS operate for 20 minutes while SOS activate GPS or platform activate GPS online, GPS would upload location data every 20 seconds. If SMS command like DW/WHERE activate GPS, GPS could operate as long as 5 minutes. If locate and upload one GPS location to platform, GPS would be closed. If GPS is not open, this data package would not be uploaded.

4.5.3 LBS information Package（0X11）

Format	Content					
	Date & Time	LBS information				Reserved extend byte
		MCC	MNC	LAC	CI	
Length(Byte)	6	2	1	2	3	N

4.5.3.1 Date& Time

The same as corresponding format in part of GPS information

4.5.3.2 MCC

Affiliated country code of mobile user is Mobile Country Code (MCC). MMC of China is 460(decimal)
Value ranges from 0x0000 to 0x03E7
MMC of China is 0x01 0xCC (460 decimal convert to hex)

4.5.3.3 MNC

China Mobile Network Code (MNC) is 0x00

4.5.3.4 LAC

Location Area Code (LAC) is included in LAI. It is composed of 2 bytes with hex code, ranges from 0x0001—0xFFFE(not include 0x0001 and 0xFFFE). One location area can contain one or more areas.

4.5.3.5 CI(Cell ID)

Cell Tower ID (Cell ID) ranges from 0x000000 to 0xFFFFFF

4.5.3.6 Reserved bit

The reserved bit is 2byte, correspond with GPS data package.

4.5.3.7 Server response

Need to response server

Server response after receiving status package sent by device（10 Byte）					
Start bit	Length	Protocol Number	Serial Number	CRC verify	End bit
2	1	1	2	2	2

4.5.3.8 Function

Upload LBS data package after the device connects with platform.
The device upload LBS data package every two minutes. If the device stays under static status and lac、cell signal is unchanged, LBS data is uploaded every four minutes. Thus save GPRS flow.

4.5.4 Combined Package of GPS and LBS（0X12）

Format	Information content											
	Data & time	GPS information						LBS information				Reserved extension bit
		GPS information length、number of satellite	latitude	longitude	speed	Status course	Reserved extension bit	MCC	MNC	LAC	CI	
Length(Byte)	6	1	4	4	1	2	M	2	1	2	3	N

As for each parameter, please refer to previous explanation

4.5.5 Status package (0X13)

Format	Content			
	Device information	Voltage degree	GSM signal strength degree	Reserved extent byte
Length(Byte)	1	1	1	N

4.5.5.1 Device information

Occupy 1 byte, representing sundry status information of the device. Regard 1 byte as 8bits, the lowest bit is 0, the highest is 7. In the process of the data transmitting, the high one comes first and the low one follows. Each bit represents the detailed meaning as follows:

High bit							Low bit
7	6	5	4	3	2	1	0

Zero bit	Reserved
First bit	Reserved
Second bit	Reserved
Third bit/Fourth bit/Fifth bit	011：Low-power alarm

	100：SOS
Sixth bit	0：GPS has not located 1：GPS has located
Seventh bit	Reserved

Note: The status information refers to the status in a certain time

4.5.5.2 Voltage degree

Decimal, range from 0-6
0：Lowest power and power off
1：No enough power to dial a call or send messages.
2：Low power and alarm
3：Lower power but can work normally
3~6：Work in good condition

4.5.5.3 GSM signal strength degree:

0x00：No signal
0x01：Weaker signal
0x02：Weak signal
0x03：Good signal
0x04：Strong signal

4.5.5.4 Reserved bit

The reserved bit is 2byte, correspond with GPS data package.

4.5.5.5 Server response

Need to response server

Server response after receiving status package sent by device（10 Byte）					
Start bit	Length	Protocol Number	Serial Number	CRC verify	End bit
2	1	1	2	2	2

4.5.5.6 Function

The device uploads status information like electric quantity of battery after connecting with platform.

The device uploads defaulted status package once every five minutes.

4.5.6 Satellite SNR information（0X14）

This package is sent after the device receiving the command from server

Format	Content						
	Number of satellites involved in locating	Satellite SNR					Reserved extend byte
		1	2	3	……	n	
Length(Byte)	1	n					N

4.5.6.1 Number of satellite involved in locating

For example: 12 satellites is 0x0C

4.5.6.2 Satellite SNR

Range: 0x00~0x63(means 0~99dBHZ)

Every satellite occupies one byte.

4.5.6.3 Reserved bit

Reserved bit is 2byte.

Note: This data package is not available currently.

5.7 Character String information （0X15）

Note: This data package is not available currently.

4.5.8 Combined Package of GPS, LBS and Status (0X16)

Format	Content															
		GPS info						LBS info						Status info		
	Date & Time	GPS info length/ Number of satellites involved in locating	Latitude	Longitude	Speed	Course/Status	Reserved bit	LBS length	MCC	MNC	LAC	Cell ID	Reserved bit	Device information content	Voltage degree	GSM signal power degree
Length (Byte)	6	1	4	4	1	2	M	1	2	1	2	3	N	1	1	1

As for each parameter, please refer to previous explanation.

It combines GPS info/ LBS info and status info. What need to notice is that LBS info here has been increased length (includes 1 byte occupied by itself.).Server should make a response when receive package of GPS/Status combined info. Note: Reserved extended bit N=0

4.5.8.1 Extended bit

Bit15---Bit2	Bit1—Bit0
No definition	00----Chinese 01---- Chinese 10----English

4.5.8.2 Server response

Ask for receiving Chinese address or English address via extended command, reply package is not corresponding.
For example, reply package in Chinese:

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for asking Chinese address reply: 0X17

Information content:

Format	Content of information			
	Content -length	Server flag bits	Information content	Reserved bit

Length(Byte)	1	4	M	0

Command content: ADDRESS&&ADDRESS CONTENT&&PHONE NUMBER##
Chinese address is sent by Unicode.

Because one data byte may not be enough for some English or other overseas address, there are two bytes for protocol number of replied English address.

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for asking English address reply: 0X97

4.5.8.3 Function

This status package would send to server when SOS alarm and GPS track the location, asking for location information and sending alarming status.

4.5.9 LBS、Telephone number address checking package(0X17)

Format	Content					
	LBS Information				Phone Number	Reserved extend byte
	MCC	MNC	LAC	Cell ID		
Length(Byte)	2	1	2	3	21	N

Basically same with the Format in LBS information Content but delete Date/Time and add Phone Number for checking location. Note: Reserved extended bit N=2

4.5.9.1 Extended bit

Bit15---Bit2	Bit1—Bit0
No definition	00----Chinese 01---- Chinese 10----English

4.5.9.2 Server response

Request for receiving Chinese address or English address via extended command, reply package is not corresponding.
For example, reply package in Chinese:

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for requesting Chinese address reply: 0X17
Information content:

Format	Content of information			
	Content -length	Server flag bits	Information content	Reserved bit
Length(Byte)	1	4	M	0

Command content: ADDRESS&&ADDRESS CONTENT&&PHONE NUMBER##
Chinese address is sent by Unicode.

Because one data byte may not be enough for some English or other overseas address, there are two bytes for protocol number of replied English address.

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for asking English address reply: 0X97

4.5.9.3 Function

When phones of family number send SMS command DW to device to check location information, the device would send this status package to server to request location information of the device. Then the device would send location information received back to phones of family number.

Device send 0X17 data package to server (Request Chinese address)

```
7878241701CC00266A001E23313235323031333739303737343035310000000000000
1000B1F1A0D0A
```

Server send location information package back to device

```
787884177E00000001414444524553532626624059044F4D7F6E0028004C00420053
0029003A5E7F4E1C77015E7F5DDE5E0282B190FD533AFF17FF15FF144E61905300
28004E00320033002E003300390035002C004500310031002E0039003800380002
996448FD126263133373130383139313335000000000000000000002323010638250D
0A
```

Example of format of replying Chinese address:

```
7878                    // Info header
84                      // Data bit length
17                      // Protocol number
7E                      // Content length
```

```
00000001              // Server serial number
41444452455353    //ADDRESS
2626                  //&& Break
624059044F4D7F6E0028       //Chinese address sent via Unicode
004C004200530029003A
5E7F4E1C77015E7F5DDE
5E0282B190FD533AFF17
FF15FF144E6190530028
004E00320033002E0033
00390035002C00450031
00310032002E00390038
0038002996448FD1
2626                    //&& Break
313337313038313931333500000000000000000000        //Phone number
2323                    //##    Content information end bit
0106                    // Serial number
3825                    // Identifying bit
0D0A                     // End bit
```

Device send 0X17 data package to server (Request English address)

```
7878241701CC00266A001E2331323532303133373930373734303531000000000000
2000B1F190D0A
```

Server send location information package back to device

```
787800D19700CA0000000141444452455353262600053004F00530028004C0029003A
00530068006900 6D0069006E00200046006100690072 0079006C0061006E006400200
```

Example of format of replying English address:

```
7878                  // Info header
84                    // Data bit length
17                    // Protocol number
7E                    // Content length
00000001              // Server serial number
41444452455353    //ADDRESS
2626                  //&& Break
0053004F00530028004C       //English address sent via Unicode
0029003A005300680069
```

```
006D0069006E00200046
0061006900720079006C
0061006E006400200057
00650073007400200052
0064002C004800750069
006300680065006E0067
002C004800750069007A
0068006F0075002C0047
00750061006E00670064
006F006E00670028004E
00320033002E00310031
0031002C004500310031
0034002E003400310031
0029004E006500610072
00620079

2626                    //&& Break
313337313038313931333500000000000000000000        //Phone number
2323                    //##    Content information end bit
0106                    // Serial number
3825                    // Identifying bit
0D0A                     // End bit
```

4.5.10 LBS Extended Information Package (0X18)

Format	Content																								
	Date Time	LBS Information																							Reserved extend bit
		MCC	MNC	LAC	MCI	MRSSI	NLAC1	NCI1	NRSSI1	NLAC2	NCI2	NRSSI2	NLAC3	NCI3	NRSSI3	NLAC4	NCI4	NRSSI4	NLAC5	NCI5	NRSSI5	NLAC6	NCI6	NRSSI6	TA	
Length(Byte)	6	2	1	2	3	1	2	3	1`	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	1	N

4.5.10.1 Date & Time

The same as the last section

4.5.10.2 MCC

The same as the last section

4.5.10.3 MNC

The same as the last section

4.5.10.4 LAC

The same as the last section

4.5.10.5 MCI（Main Cell ID）

Cell Tower ID(Cell ID)，value range is 0x0000 ～ 0xFFFF。

4.5.10.6 RSSI（Received Signal Strength Indicator）

Main estate signal strength, value range is 0x00～0xFF，0x00 is the weakest signal，0xFF is the strongest signal。

4.5.10.7 NLAC1～6

Neighborhood Base Station code, there are 6 in all.

4.5.10.8 NCI1～6（Neighboring Cell ID）

Neighborhood Base Station code is corresponding with the 6 NLAC separately.

4.5.10.9 NRSSI1～6（Near Cell ID Signal Strength）

Neighborhood Base Station signal strength is corresponding with the 6 NLAC separately.

4.5.10.10 TA(Timing advance)

TA could only be gained by phone call or sending SMS time period, which ranges from 0-63.Under other status it’s 255 of no avail. While multiplying 550(meter), it can estimate the distance between device and main district.

4.5.11 Combined Package of GPS and LBS Extended information

Format	Information content																														
	Date/Time	GPS Information						LBS extended information																							
		GPS info length/Number of satellites involved in locating	Latitude	Longitude	Speed	Course/Status	Reserved bit	MCC	MNC	LAC	MCI	MRSSI	NLAC①	NCI①	NRSSI①	NLAC②	NCI②	NRSSI②	NLAC③	NCI③	NRSSI③	NLAC④	NCI④	NRSSI④	NLAC⑤	NCI⑤	NRSSI⑤	NLAC⑥	NCI⑥	NRSSI⑥	TA	Reserved extended bit
Length(Byte)	6	1	4	4	1	2	M	2	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	1	N

As for each parameter, please refer to previous explanation.

4.5.12 LBS、Status package (0X19)

Format	Content							
	LBS info				Status info			Extended bit
	MCC	MNC	LAC	Cell ID	Device info content	Voltage degree	GSM signal strength	Language
Length(Byte)	2	1	2	3	1	1	1	2

Basically same with the Format in LBS information Content.

4.5.12.1 Server response

Need to response server

Server response after receiving status package sent by device（10 Byte）					
Start bit	Length	Protocol Number	Serial Number	CRC verify	End bit
2	1	1	2	2	2

4.5.12.2 Function

After connecting with platform, press SOS button of device and send this package to server to inform alarming status and request LBS location information.

Device send 0X19 data package to server（request LBS location information）:
7878121901CC00266A001E232006040001000993910D0A

Server send location information package back to device:
78787B17750000000141444452455353326267D276025547C53EB003A5E7F4E1C770
160E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E003200330
02E003100310032002C0045003100310034002E003400300039002996448FD1262600
00000000000000000000000000000000000000232300096e6c0D0A

Note: Protocol of package that device request for sending is 0X19, sever reply in language stipulated by extended bit. If in Chinese, server reply: 0X17; if in English, server reply 0X97.

4.5.13 GPS、Telephone number address checking package (0X1A)

Format	Content							
	Date/Time	GPS info					Phone number	Reserved extension bit
		GPS info length, the number of satellite	latitude	longitude	speed	Course, status	21	2
Length (Byte)	6	1	4	4	1	2		

Basically same with the Format in GPS information Content, add phone number to check the address.

4.5.13.1 Server response

Request for receiving Chinese address or English address via extended command, reply package is not corresponding.
For example, reply package in Chinese:

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for requesting Chinese address reply: 0X17

Information content:

Format	Content of information			
	Content -length	Server flag bits	Information content	Reserved bit
Length(Byte)	1	4	M	0

Command content: ADDRESS&&ADDRESS CONTENT&&PHONE NUMBER##
Chinese address is sent by Unicode.

Because one data byte may not be enough for some English or other overseas address, there are two bytes for protocol number of replied English address.

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	0	2	2	2

Protocol for asking English address reply: 0X97

4.5.13.2 Function

When GPS is activated by SMS command DW to request for location information, this package would be sent.

Device send 0X1A data package to server（request Chinese address）：

78782E1A0B03110A1736CF027AC82D0C4657CE0014003132353230313337393037373430353100000000000001000D7F810D0A

Server send location information package back to device：

787880177A000000014144445245535326267CBE786E5B9A4F4D003A5E7F4E1C770160E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E00320033002E00310031003100370030002C0045003100310034002E0034003000390032003100292626313235323031333739303737343035310000000000002323000dda000D0A

4.5.14 Command from server to device (set command)

Format	Content of information			
	Content -length	Server flag bits	Information content	Reserved bit
Length(Byte)	1	4	M	N

Protocol NO.: 0x80

The response command sending from device to server, whose data package format is the same as the format of “command sending from server to device” , protocol NO. is different, with”0x80” or “0x81”. 0x80 stands for setting command. 0x81 stands for checking command..

4.5.14.1 Command length

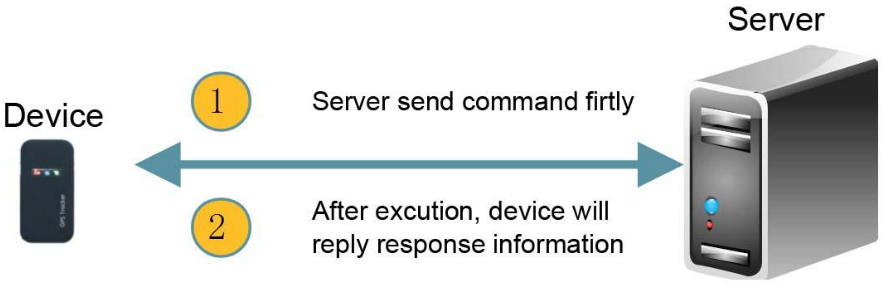
Show with byte, OxOA, means command content occupy 10 bytes

4.5.14.2 Server flag

Left to the server for identification, device will receive data from a binary package stood in the back to return

4.5.14.3 Command content

Show with ASCⅡ character string, command connent is compatible with sms command.


Server
Device
1
Server send command firtly
2
After excution, device will
reply response information

4.5.14.3.1 Activate GPS online

SMS command format:

GPSON#

For example: GPSON#

Function description: Start GPS locating function

Get back:

If Successful, it will return: GPSON =Success!

If failed, it will return: GPSON =Fail!

4.5.14.4 Reserved extended bit

The current reserved extended bit that server send to device N=0

Example of activating GPS online

7878 // Info header

```
10              // Data bit length
80             // Protocol number
0A             // Content length
0000A039     // Server serial number
4750534F4E  //GPSON
23        //#
0001    //Serial number
238d     //CRC verify
0D0A   //end bit
```

4.5.12.4 Command from server to device(checking command)

Format	Content of information					
	Content -length	Command content				Reserved bit
		IMEI NO.	ID(8)	Name(12)	Content(N)	
Length(Byte)	1	M				N

Protocol NO.: 0x82, Reserved extended bit N=0

4.5.12.4.1 Command length

Show with byte, Ox58, means command content occupy 88 bytes

4.5.12.4.2 Command content

Server sends to the device
IMEI NO: identification number when device log in server
Message ID: server send ID serial number
Name: device’s name on server
Content: information content that server sends to the device

Example（Complete data package）：
7878668266000000000000678600000000000 0B7B2673165874FCA003200300031003
0002D00310032002D0031003000200032003100 3A00320038003A0030003500206625
669682B15F007684004D006F00620069006C00656D88606F00300033003200390001
d9130D0A

```
7878                     // Info header
66                       // Data bit length
82                     // Protocol number
66                     // Content length
0000000000006786    //IMEI    NO.
000000000000B7B2    //Message ID
673165874FCA003200300031    //Name
0030002D00310032002D0031003000200032003100 3A00320038003A0030003500206
625669682B15F007684004D006F00620069006C00656D88606F0030003300320039
//Content
0001       //Serial number
d913       //CRC verify
0D0A      //end bit
```

Instruction about login data package and status package

1. If GPRS connection successful, the device will send first login data package to server. Receiving feedback package in 10 seconds will be considered as normal, it starts sending position data(GPS,LBS information package), 5 minutes later status package follows immediately, to confirm the normal communication timely(in every 5 minutes).
2. If the GPRS connection failed, device can not send login data package. When GPRS connection fails for 3 times, device will activate timed-restarting function。（ Note: The restart process will activate once after 20 minutes. If device connect with server and receiving feedback data package to login data　successfully in 20 minutes， the timed-restarting function will be disabled automatically.）
3. If there is no feedback package sent from server in 10 seconds, after device sends login data or status data package, it will be considered as failure to connect. In this case, device will activate the GPS data backup function, disconnect the current GPRS connection, reconnect to the server and send login data package.
4. If connection is considers as abnormal, reconnect to send login data package or status data package but not receiving feedback data package in 3 times, device will activate timed-restarting function.(Note: The restart process will activate once after 10 minutes. If device connect with server and receiving feedback data package in this 10 minutes, the timed-restarting function will be disabled automatically.)
5. Server will not reply feedback data package to device which has not been registered.
6. If the device has not been inserted by sim card, or the GPRS service of this sim card has not been activated, the device will restart automatically once after 20 minutes.

5. Error check

Device or server can judge the accuracy of data received with identifying code. Sometimes, because of the electronic noise or other interference, data will be changed a little in the transit process. In this case, identifying code can make sure the core or associated core do nothing with such kind of wrong data, which will strengthen the security and efficiency of system. This identifying code adopts CRC-ITU identifying method. The CRC-ITU value is from "Package Length' to "Information Serial Number" in the protocol (including "Package Length" and "Information Serial Number ").
If the receiver receives CRC wrong calculating information, then ignore it and discard this data package.

6. Stop bit

Fixed value by hexadecimal 0x0D 0x0A

7. Appendix A: code fragment of the CRC-ITU lookup table algorithm implemented based on C language

```
static const U16 crctab16[] =
{
        0x0000, 0x1189, 0x2312, 0x329b, 0x4624, 0x57ad, 0x6536, 0x74bf,
        0x8c48, 0x9dc1, 0xaf5a, 0xbed3, 0xca6c, 0xdbe5, 0xe97e, 0xf8f7,
        0x1081, 0x0108, 0x3393, 0x221a, 0x56a5, 0x472c, 0x75b7, 0x643e,
        0x9cc9, 0x8d40, 0xbfdb, 0xae52, 0xdaed, 0xcb64, 0xf9ff, 0xe876,
        0x2102, 0x308b, 0x0210, 0x1399, 0x6726, 0x76af, 0x4434, 0x55bd,
        0xad4a, 0xbcc3, 0x8e58, 0x9fd1, 0xeb6e, 0xfae7, 0xc87c, 0xd9f5,
        0x3183, 0x200a, 0x1291, 0x0318, 0x77a7, 0x662e, 0x54b5, 0x453c,
        0xbdcb, 0xac42, 0x9ed9, 0x8f50, 0xfbef, 0xea66, 0xd8fd, 0xc974,
        0x4204, 0x538d, 0x6116, 0x709f, 0x0420, 0x15a9, 0x2732, 0x36bb,
        0xce4c, 0xdfc5, 0xed5e, 0xfcd7, 0x8868, 0x99e1, 0xab7a, 0xbaf3,
        0x5285, 0x430c, 0x7197, 0x601e, 0x14a1, 0x0528, 0x37b3, 0x263a,
        0xdecd, 0xcf44, 0xfddf, 0xec56, 0x98e9, 0x8960, 0xbbfb, 0xaa72,
        0x6306, 0x728f, 0x4014, 0x519d, 0x2522, 0x34ab, 0x0630, 0x17b9,
        0xef4e, 0xfec7, 0xcc5c, 0xddd5, 0xa96a, 0xb8e3, 0x8a78, 0x9bf1,
        0x7387, 0x620e, 0x5095, 0x411c, 0x35a3, 0x242a, 0x16b1, 0x0738,
        0xffcf, 0xee46, 0xdcdd, 0xcd54, 0xb9eb, 0xa862, 0x9af9, 0x8b70,
        0x8408, 0x9581, 0xa71a, 0xb693, 0xc22c, 0xd3a5, 0xe13e, 0xf0b7,
        0x0840, 0x19c9, 0x2b52, 0x3adb, 0x4e64, 0x5fed, 0x6d76, 0x7cff,
        0x9489, 0x8500, 0xb79b, 0xa612, 0xd2ad, 0xc324, 0xf1bf, 0xe036,
        0x18c1, 0x0948, 0x3bd3, 0x2a5a, 0x5ee5, 0x4f6c, 0x7df7, 0x6c7e,
        0xa50a, 0xb483, 0x8618, 0x9791, 0xe32e, 0xf2a7, 0xc03c, 0xd1b5,
        0x2942, 0x38cb, 0x0a50, 0x1bd9, 0x6f66, 0x7eef, 0x4c74, 0x5dfd,
        0xb58b, 0xa402, 0x9699, 0x8710, 0xf3af, 0xe226, 0xd0bd, 0xc134,
        0x39c3, 0x284a, 0x1ad1, 0x0b58, 0x7fe7, 0x6e6e, 0x5cf5, 0x4d7c,
        0xc60c, 0xd785, 0xe51e, 0xf497, 0x8028, 0x91a1, 0xa33a, 0xb2b3,
        0x4a44, 0x5bcd, 0x6956, 0x78df, 0x0c60, 0x1de9, 0x2f72, 0x3efb,
        0xd68d, 0xc704, 0xf59f, 0xe416, 0x90a9, 0x8120, 0xb3bb, 0xa232,
        0x5ac5, 0x4b4c, 0x79d7, 0x685e, 0x1ce1, 0x0d68, 0x3ff3, 0x2e7a,
        0xe70e, 0xf687, 0xc41c, 0xd595, 0xa12a, 0xb0a3, 0x8238, 0x93b1,
        0x6b46, 0x7acf, 0x4854, 0x59dd, 0x2d62, 0x3ceb, 0x0e70, 0x1ff9,
        0xf78f, 0xe606, 0xd49d, 0xc514, 0xb1ab, 0xa022, 0x92b9, 0x8330,
        0x7bc7, 0x6a4e, 0x58d5, 0x495c, 0x3de3, 0x2c6a, 0x1ef1, 0x0f78,
};

        // calculate 16 bits CRC of the given length data.
U16 GetCrc16(const U8* pData, int nLength)
{
U16 fcs = 0xffff; // Initialize
```

```
while(nLength>0){
fcs = (fcs >> 8) ^ crctab16[(fcs ^ *pData) & 0xff];
nLength--;
pData++;
}
return ~fcs; // Negate
```

8. Note B Communication Protocol Package Fragment Example

The data below is hexadecimal data from communication between device and server
Example of communication protocol package

Login information package (Protocol：0x01)：

Old login information package：

78780F01025241903071152410050001F3D70D0A

Reply：

787805010001d9dc0D0A

New login information package：

78781101035341903009962110063201000137 6C0D0A

Reply：

787805010001d9dc0D0A

GPS Package (Protocol:0x10)

787819100B03110A100FCF027AC8570C465735001400000100045283 0D0A

Reply：7878051000045138 0D0A

LBS Package（Protocol：0X11）

787815110000000000000 1CC013182005C83000003F2A3E70D0A

Reply：7878051103f2b3350D0A

Status package (Protocol:0x13)

78780A13000504000003F352940D0A

Reply：7878051303f317040D0A

GPS.LBS.STATUS package（Protocol：0x16)

787825160B03110A1010CF027AC8450C4657410014000901CC00266A001E2360060
40001000A34620D0A

Reply：

78787F17790000000141444452455353267D276025547C53EB003A5E7F4E1C7701

60E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E0032003300
2E00310031003100370031002C0045003100310034002E00340030003900310033002
92626000000000000000000000000000000000000002323000af4250D0A

LBS.PHB package（Protocol：0x17）

7878241701CC00266A001E23313235323031333739303737343035310000000000000
1000B1F1A0D0A
Reply：
78787C1776000000014144445245535326266240590044F4D7F6E003A5E7F4E1C7701
60E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E0032003300
2E003100310032002C0045003100310034002E0034003000390029 96448FD12626313
235323031333739303737343035310000000000 2323000b6ff80D0A

LBS.STATUS package (Protocol:0x19)

7878121901CC00266A001E23200604000100099391 0D0A
Reply：
78787B177500000001414444524553532626 7D276025547C53EB003A5E7F4E1C770
160E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E003200330
02E003100310032002C0045003100310034002E003400300039002996448FD1262600
0000000000000000000000000000000000000232300096e6c0D0A

GPS.PHB package(Protocol：0x1A)

78782E1A0B03110A1736CF027AC82D0C4657CE00140031323532303133373930373
7343035310000000000000 1000D7F810D0A
Reply：
787880177A000000014144445245535326267CBE786E5B9A4F4D003A5E7F4E1C770
160E05DDE5E0260E057CE533A4E915C71897F8DEF003653F70028004E003200330
02E00310031003100370030002C0045003100310034002E00340030003900320031 00
29262631323532303133373930373734303531 0000000000 2323000dda000D0A

Activate GPS package online（Protocol：0x80）

787810800A0000A0394750534F4E230001238d0D0A
Reply 1：GPSON=OverTime Off!
78782080180000CBFC4750534F4E3D4F76657254696D65204F666621000001001A9
4CE0D0A

Reply：GPSON=Success!
78782080180000D4104750534F4E3D537563636573732100000000000000000001C31
DC0D0A

Send message information package online（Protocol：0x82）

78786682660000000000000678600000000000000B7B2673165874FCA003200300031003

```
0002D00310032002D0031003000200032003100 3A00320038003A0030003500206625
669682B15F007684004D006F00620069006C00656D88606F0030003300320039 0001
d9130D0A
```

9. Note C Full format of information packet

Data package from device to server

Old login data package（20 Byte）						
Info header	Content-length	Protocol number	Device ID	Information serial number	Identifying bit	End bit
2	1	1	8	2	2	2

New login data package（22 Byte）						
Info header	Content-length	Protocol number	Device ID	Information serial number	Identifying bit	End bit
2	1	1	8	2	2	2

GPS package(30 Byte)												
Info header	data bit length	Protocol number	Information content							Information serial number	Identifying bit	End bit
			Date &time	GPS information					Reserved bit			
				GPS information length, Number of Satellites involved in locating	latitude	Longitude	Speed	Course, status				
2	1	1	6	1	4	4	1	2	2	2	2	2

LBS package　（26 Byte）											
Info header	Data bit length	Protocol number	Information content						Information srial number	Identifying bit	End bit
			Date & time	LBS information				Reserved bit			
				MCC	MNC	LAC	Cell ID				
2	1	1	6	2	1	2	3	2	2	2	2

LBS Extend information package（62+N Byte）																															
Start bit	Data length	Protocol No.	Information content																									Information serial No.	Identifying bit	End bit
			Date and time	LBS information																							Reserved extend bit			
				MCC	MNC	LAC	CI	RSSI	NLAC1	NCI1	NRSSI1	NLAC2	NCI2	NRSSI2	NLAC3	NCI3	NRSSI3	NLAC4	NCI4	NRSSI4	NLAC5	NCI5	NRSSI5	NLAC6	NCI6	NRSSI6	TA				

2	1	1	6	2	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	1	N	2	2	2

GPS/LBS Information package（74+M+N Byte）																	
Infoheader	Data bit length	Protocol number	Information content												Information serial number	Identifying bit	End bit
			Date&time	GPS information						LBS information				Reserved bit			
				GPS information length, Number of Satellites involved in locating	Latitude	Longitude	Speed	Course, status	Reserved bit	MCC	MNC	LAC	Cell ID				
2	1	1	6	1	4	4	1	2	M	2	1	2	3	N	2	2	2

GPS/LBS Information package（74+M+N Byte）																																					
Info header	Data bit length	Protocol number	Information content	Information content																																	
				GPS information					LBS information																												
				GPS information length, Number of Satellites involved in locating	Latitude	Longitude	Speed	Course, status	Reserved bit	MCC	MNC	LAC	MCI	MRSSI	NLAC①	NCI①	NRSSI①	NLAC②	NCI②	NRSSI②	NLAC③	NCI③	NRSSI③	NLAC④	NCI④	NRSSI④	NLAC⑤	NCI⑤	NRSSI⑤	NLAC⑥	NCI⑥	NRSSI⑥	TA	Reserved bit	Information serial number	Identifying bit	End bit
2	1	1	6	1	4	4	1	2	M	2	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	1	N	2	2	2

Status package（15 Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Device information content	Voltage degree	GSM signal strength degree	Reserved bit			
2	1	1	1	1	1	2	2	2	2

Satellite SNR information（11+M+N Byte）												
Info header	Data bit length	Protocol number	Information content							Information serial number	Identifying bit	End bit
			Number of Satellites involved in locating	Satellite SNR					Reserved bit			
				1	2	3	……	n				
2	1	1	1	M					N	2	2	2

Feedback information from device to server（15+M+N Byte）									
Info header	Data bit length	Protocol number	Character string content				Information serial number	Varifying bit	end bit
			Command length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	N	2	2	2

GPS、LBS status package（40+M+N+L Byte）																						
Info header	Data bit length	Protocol number	Information content																Reserved bit	Information Serial NO.	Identifying bit	End bit
			Date& time	GPS information						LBS information						Status information						
				GPS information length Number of Satellites involved	latitude	Longitude	Speed	Course, status	Reserved bit	LBS length	MCC	MNC	LAC	Cell ID	Reserved bit	Device information	Voltage degree	GSM signal strength de				

				in locating												content		gree				
2	1	1	6	1	4	4	1	2	M	1	2	1	2	3	N	1	1	1	L	2	2	2

B．Data package from server to device

Feedback package sending from server to device after receiving status package（10 Byte）					
Info header	Data bit length	Protocol number	Information serial number	Identifying bit	End bit
2	1	1	2	2	2

Command package sending from server to terminal（15+M+N Byte）									
Info header	Data bit length	Protocol number	Information content				Information serial number	Identifying bit	End bit
			Content length	Server flag	Command content	Reserved bit			
2	1	1	1	4	M	N	2	2	2

ShenZhen Concox Information Technology CO.,Ltd

Tel: +86 755 2912 1200

Fax: +86 755 2912 1290

E-mail: aven@concox.cn.

Add: 4/F, Building B, Gaoxinqi Industrial Park,
Liuxian 1st Road, No.67 Bao'an District, Shenzhen