Version: V02

Level Secret

GPS Tracker

Communication Protocol

Directory

I. Communication Protocol Introduction

This document defines instructions about interface protocol on application layer of vehicles GPS tracker and location-based service platform. Related interface protocol only applies in the interaction between the platform and the position terminal.

II. Definition of Terms

Terms, abbreviations	English meaning	Chinese meaning
CMPP	China Mobile Peer to Peer	China Mobile Point to Point Protocol
GPS	Global Positioning System	Global Positioning System
GSM	Global System for Mobile Communication	Global System for Mobile Communications
GPRS	General Packet Radio Service	General Packet Radio Service
TCP	Transport Control Protocol	Transmission Control Protocol
LBS	Location Based Services	Assisted positioning service
IMEI	International Mobile Equipment Identity	International Mobile Equipment Identity
MCC	Mobile Country Code	Mobile users Country Code
MNC	Mobile Network Code	Mobile network numbers
LAC	Location Area Code	Location Area Code
Cell ID	Cell Tower ID	Mobile station
UDP	User Datagram Protocol	User Datagram Protocol
SOS	Save Our Ship / Save Our Souls	SOS distress signal
CRC	Cyclic Redundancy Check	Cyclic Redundancy Check
NITZ	Network Identity and Time Zone,	Time zone
GIS	Geographic Information System	Geographic Information System

III. Basic rules

1. If a GPRS connection is established successfully, the terminal will send a first login message packet to the server and, within five seconds, if the terminal receives a data packet responded by the server, the connection is considered to be a normal connection. The terminal will begin to send location information (i.e., GPS, LBS information package). A status information package (also known as heartbeat packet) will be sent by the terminal every three minutes to regularly confirm the connection.

2. When the GPRS connection is not established successfully, the terminal cannot send the login information packet. When the GPRS connection fails 3 times, the terminal will start the timer restart function, and the time is 20 minutes. If the terminal successfully establishes a connection with the server within 20 minutes and receives a data packet that the server responds to the login information packet sent by the terminal, the timer restart function will be disabled and the terminal will not restart, otherwise the terminal will automatically restart after 20 minutes.

3. After the server receives the login information packet sent by the terminal, it returns a response packet to the terminal. If the terminal does not receive the server return packet for more than 5 seconds after the login information packet or status information packet is sent, the current connection establishment will be considered abnormal. The terminal will start a re-transmission function for GPS tracking data, which will cause the terminal to disconnect the current GPRS connection, rebuild a new GPRS connection and send a login message packet again.

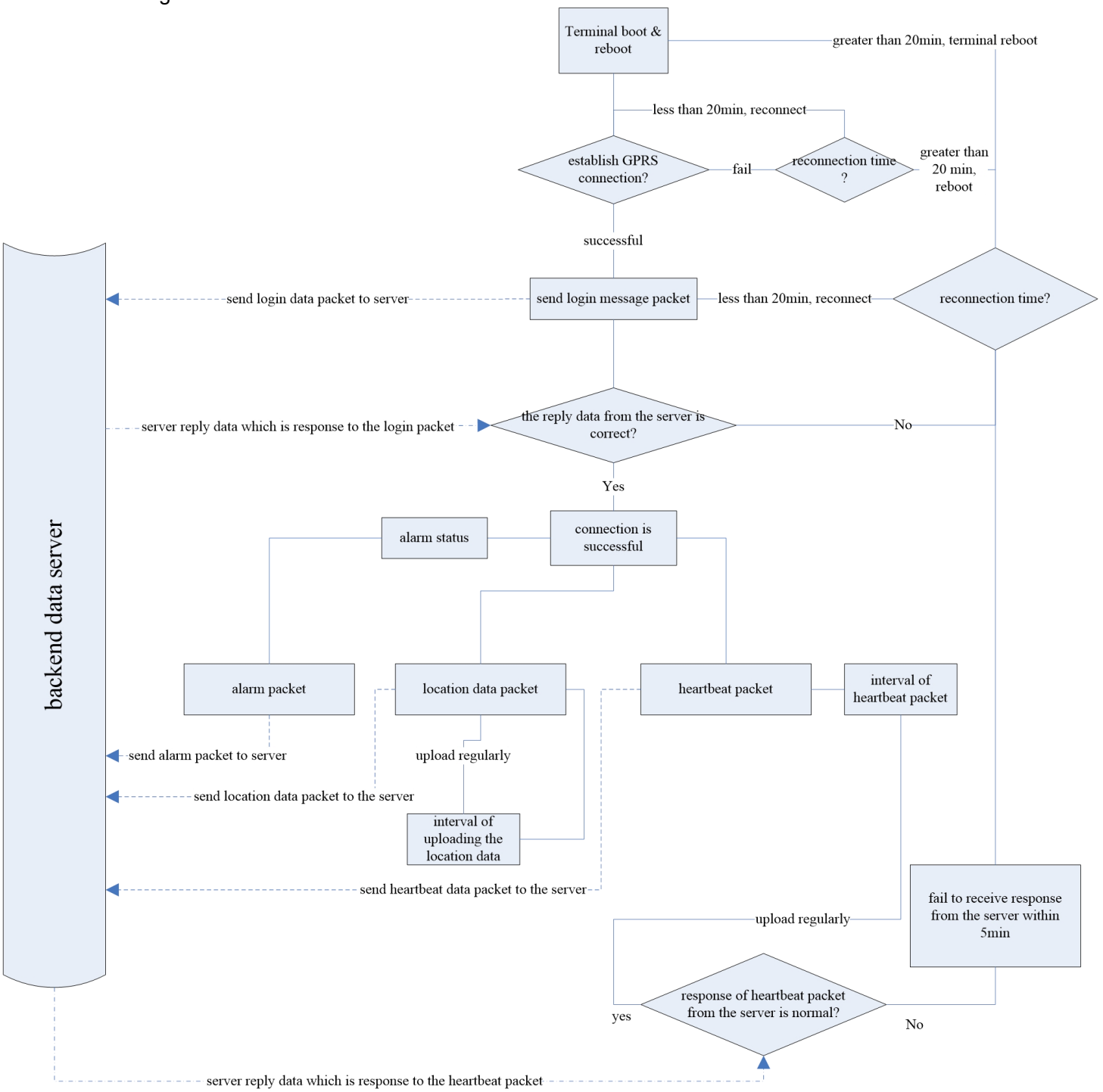
4. When the connection is regarded as abnormal, and the response packet from the server is failed to be received three times after a connection is established, and a login message packet or status information package is sent, the terminal will start schedule reboot and the scheduled time is ten minutes. Within ten minutes, if the terminal successfully connects to the server and receives the data packet responded by the server, the schedule reboot will be off and the terminal will not be rebooted; otherwise, the terminal will be rebooted automatically in ten minutes.

5. If there's a normal connection, the terminal will send a combined information package of GPS and LBS to the server after the GPS information is changed; and the server may set a default protocol for transmission by using commands.

6. To ensure the validity of the connection, the fixed time interval sends status information (heartbeat packet) to the server, the server returns a response acknowledgment packet.

7. For the terminal that has not registered the IMEI number in the server previously, the server should reply with the login request response and the heartbeat packet response, and the server should not directly disconnect the connection. (If the server directly disconnects or does not reply, it will cause the terminal to reconnect continuously, and GPRS data consumption will be very high).

Data Flow Diagram



IV. Packet Format

The communication transmission is asynchronous, and the unit is byte.

Total packet length: (10 + N) Byte

Format	Length (Byte)
Start bit	2
Packet length	1 (2)
Protocol No.	1
Information	N
Information Serial Number	2
Error check	2
Stop bits	2

4.1. Start Bit

Fixed value, unified as hexadecimal 0x78 0x78 (packet length 1) or 0x79 0x79 (packet length 2).

4.2 Packet Length

Packet length=Protocol number+Information content+Information serial number+Error check

A total of (5+N) Bytes, because the information content is a variable length field.

4.3. Protocol Number

Types	Value
Login information	0x01
Positioning data (UTC)	0x22
Status information	0x13
String information	0x21
LBS information	0x24
Alarm data (UTC)	0x26
Time zone	0x27
Query address by phone number	0x2A
WIFI packets	0x2C
Server sends command to terminal	0x80
General package for information transmission like Air con and Door status	0x94

4.4. Information Content

The specific contents are determined by the protocol numbers corresponding to different applications.

4.5. Information Serial Number

The serial number of the first GPRS data (including status packet and GPS, LBS, etc. data packet) sent after power on is '1', and the serial number is automatically incremented by 1 each time when data sent (including status packet and GPS and LBS data packet) after that.

4.6. Error Check

The terminal or server can use the check code to judge whether the received information is wrong or not. In order to prevent data errors during transmission, an error check is added to prevent data misoperation, which increases the safety and efficiency of the system. The error check code adopts the CRC-ITU check method. The check codes of data in the structure of the protocol, from the Packet Length to the Information Serial Number (including “Packet Length” and “Information Serial Number”), are values of CRC-ITU.

If the receiver has a CRC error in the calculation of the received information, the data packet shall be ignored and discarded.

4.7. Stop bits

Fixed value, unified hexadecimal 0x0D 0x0A.

V. Terminal sending data packets to the server

Information packages sent by the terminal and those sent by the server will be interpreted separately.

5.1. Login information packet

5.1.1. The terminal sends data packets to the server

The login information package is used to confirm to the server that the connection is established normally, and submit the terminal ID to the server.

Format		Length	Example
Login information packet (18 Byte)	Start bit	2	0x78 0x78
	Packet length	1	0x11
	Protocol No.	1	0x01
	Terminal ID	8	0x01 0x23 0x45 0xx67 0x89 0x01 0x23 0x45
	Model Identifier	2	0x00 0x00
	Time zone Language	2	0x32 0x00
	Information Serial Number	2	0x00 0x01
	Error check	2	0x90 0x01
	Stop bits	2	0x0d 0X 0a

5.1.1.1. Start bit

See Packet Format 4.1

5.1.1.2. Packet length

See packet format 4.2

5.1.1.3. Protocol No.

See packet format 4.3

5.1.1.4. Terminal ID

If the terminal ID is 123456789012345

It will be shown as: 0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45

5.1.1.5. Model identifier

Model identifier is two bytes. This code is to determine what model of GPS TRACKER is being used.
Air condition & Door status detection device code is 0X00 0X53
Temperature sensor function device code is 0X00 0X54

5.1.1.6. Time Zone Language

<table>
<tr><td rowspan="10">One and a half bit bit15-bit4</td><td>15</td><td colspan="2" rowspan="10">Multiply the value of time zone by 100</td></tr>
<tr><td>14</td></tr>
<tr><td>13</td></tr>
<tr><td>12</td></tr>
<tr><td>11</td></tr>
<tr><td>10</td></tr>
<tr><td>9</td></tr>
<tr><td>8</td></tr>
<tr><td>7</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td></tr>
<tr><td>4</td></tr>
<tr><td rowspan="4">Lower bit bit4-bit0</td><td>3</td><td colspan="2">East or West</td></tr>
<tr><td>2</td><td colspan="2">No definitions</td></tr>
<tr><td>1</td><td>Language selection bit</td><td>1</td></tr>
<tr><td>0</td><td>Language selection bit</td><td>0</td></tr>
</table>

In Bit3 0-------- East time zone

1-------- West time zone

Example one: 0X32 0X00 represents GMT+8 Time zone.

Calculation method: 8 * 100 = 800, convert to hexadecimal, 0X0320

Example two: 0X4D 0XD8 represents GMT-12: 45 Time zone.

Calculation method: 12.45 * 100 = 1245, convert to hexadecimal, 0X04,0XDD.

Please note: The algorithm here is to rotate the calculated time zone value to the left by four digits, and then combine the east/west of the time zone and the language selection bit. The purpose of using this calculation method is to save four bytes.

5.1.1.7. Information Serial Number

See packet format 4.5

5.1.1.8. Error check

See packet format 4.6

5.1.1.9. Stop bits

See Packet Format 4.7

5.1.2. The server responds to log in data packet from terminal

	Description	Bits	Example
Login Message Packet (18 Byte)	Start Bit	2	0x78 0x78
	Packet Length	1	0x05
	Protocol Number	1	0x01
	Information Serial Number	2	0x00 0x01
	Error Check	2	0xD9 0xDC
	Stop Bit	2	0x0D 0x0A

The server responds to the terminal: (The protocol number in the response packet is the same as the protocol number of the data packet sent by the terminal)

5.1.2.1. Start Bit

See packet format 4.1

5.1.2.2. Packet Length

See packet format 4.2

5.1.2.3. Protocol No.

See packet format 4.3

5.1.2.4. Information Serial Number

See packet format 4.5

5.1.2.5. Error Check

See packet format 4.6

5.1.2.6. Stop Bits

See packet format 4.7

5.2. Position Data Packet (GPS, LBS combined packets)

5.2.1. Position Data Packet Sent To Server (With Mileage Data)

format			Length (Byte)	Examples
Information	Start bit		2	0x78 0x78
	Packet length		1	0x26
	Protocol No.		1	0x22
	GPS information	Date Time	6	0x0A 0x03 0x17 0xF 0x32 0x17
		Number of GPS satellites	1	0xCC
		Latitude	4	0x02 0x6C 0x6C 0x82
		Longitude	4	0x0C 0x37 0x16 0x82
		Speed	1	0x00
		Course, Status	2	0x15 0x3E
	LBS information	MCC	2	0x01 0xCC
		MNC	1	0x00
		LAC	2	0x26 0x33
		Cell ID	3	0x00 0x0E 0x7F
	ACC		1	0x01
	Data reporting mode		1	0x00
	GPS re-transmission		1	0x00
	Mileage		4	0x00 0x00 0x00 0x00
	Serial number		2	0x00 0x08
	Error check		2	0x1A 0xCF
	Stop Bit		2	0x0D 0x0A

Position Data Packet Sent To Server (Without Mileage Data)

format			Length (Byte)	Examples
Information	Start bit		2	0x78 0x78
	Packet length		1	0x22
	Protocol No.		1	0x22
	GPS information	Date Time	6	0x0A 0x03 0x17 0xF 0x32 0x17
		Number of GPS satellites	1	0xCC
		Latitude	4	0x02 0x6C 0x6C 0x82
		Longitude	4	0x0C 0x37 0x16 0x82
		Speed	1	0x00
		Course, Status	2	0x15 0x3E
	LBS information	MCC	2	0x01 0xCC
		MNC	1	0x00
		LAC	2	0x26 0x33
		Cell ID	3	0x00 0x0E 0x7F
	ACC		1	0x01
	Data reporting mode		1	0x00
	GPS re-transmission		1	0x00
	Serial number		2	0x00 0x08
	Error check		2	0x60 0xA5
	Stop Bit		2	0x0D 0x0A

5.2.1.1. Start Bit

See Packet Format 4.1

5.2.1.2. Packet Length

See packet format 4.2

5.2.1.3. Protocol No.

See packet format 4.3

5.2.1.4. Date Time

Format	Length (Byte)	Examples
Year	1	0x0A
Month	1	0x03
Day	1	0x17
Time	1	0x0F
Minute	1	0x32
Second	1	0x17

Example: 15:50:23 on March 23rd, 2010

Calculation method	10(Decimal)=0A(Hex) 3 (Decimal)=03(Hex) 23(Decimal)=17(Hex) 15(Decimal)=0F(Hex) 50(Decimal)=32(Hex) 23(Decimal)=17(Hex)
The value is:	0x0A 0x03 0x17 0x0F 0x32 0x17

5.2.1.5. GPS information length, the number of positioning satellites

1Byte with two hexadecimal characters displayed, the first character is the length of GPS information, and the second character is the number of satellites involved in positioning.

Example: When the value is 0xCB, it means that the GPS information length is 12, and the number of satellites involved in positioning is 11.

(C = 12Bit length, B = 11 satellites)

5.2.1.6. Latitude

Occupies 4 bytes and represents the latitude value of GPS positioning data. The value range is 0 to 162000000, which means the range of 0 degrees to 90 degrees. The conversion method is as follows:

Convert the latitude and longitude values output by the GPS module into decimals in cents; then multiply the converted value by 30000, and finally convert the multiplied result into a hexadecimal number.

For example, 22º 32.7658' =(22X60+32.7658) X30000=40582974, then converted to hexadecimal 40582974 (decimal) = 26B3F3E (hexadecimal)
The final value is 0x02 0x6B 0x3F 0x3E.

5.2.1.7. Longitude

Occupies 4 bytes and represents the longitude value of the positioning data. The value range is 0 to 324000000, which means the range of 0 degrees to 180 degrees.

The conversion method is the same as the latitude conversion method.

5.2.1.8. Speed

It occupies 1 byte and represents the operating speed of GPS. The value range is 0x00～0xFF, which means the range is 0～255 kilometers/hour.

Example: 0x00 represents 0 km / h.
0x10 represents 16 km / h
0xFF represents 255 km / h

5.2.1.9. Course and Status

Occupies 2 bytes, indicating the operating direction of GPS, indicating the range of 0～360, unit: degree, with true north as 0 degree, clockwise.

BYTE_1	Bit7	0
	Bit6	0
	Bit5	Real-time GPS / Differential positioning
	Bit4	GPS fix or not
	Bit3	East Longitude, West Longitude
	Bit2	South Latitude North Latitude

	Bit1	Course
	Bit0	
BYTE_2	Bit7	
	Bit6	
	Bit5	
	Bit4	
	Bit3	
	Bit2	
	Bit1	
	Bit0	

Note: The data packet status information is the moment the status bit packet time recorded.

Example: value 0x15 0x4C, change to binary is 00010101 01001100

BYTE_1 Bit7 0

BYTE_1 Bit6 0

BYTE_1 Bit5 0 (Real-Time GPS)

BYTE_1 Bit4 1 (GPS positioned)

BYTE_1 Bit3 0 (Longitude)

BYTE_1 Bit2 1 (Latitude)

BYTE_1 Bit1 0

BYTE_1 Bit0 1

BYTE_2 Bit7 0

BYTE_2 Bit6 1

BYTE_2 Bit5 0 → Heading 332 ° (0101001100Binary to decimal 332)

BYTE_2 Bit4 0

BYTE_2 Bit3 1

BYTE_2 Bit2 1

BYTE_2 Bit1 0

BYTE_2 Bit0 0

That means the GPS is positioned, real-time GPS, location is at north latitude, east longitude, course 332 °.

5.2.1.10. MCC

Mobile Country Code (MCC)

Example: China's mobile country code is: 460 (decimal) 0x01 0xCC (460 converting into hexadecimal is 1CC, and 0 is added at the left side because the converted hexadecimal value is less than four digits).

Value ranges: 0x0000 ~ 0x03E7

5.2.1.11. MNC

Mobile Network Code (MNC)

Example: China Mobile is 0x00.

5.2.1.12. LAC

Location Area Code (LAC) is included in the LAI, consists of two bytes, and uses hexadecimal coding. The available range is 0x0001-0xFFFE, and the code groups 0x0000 and 0xFFFF cannot be used (see GSM specifications 03.03, 04.08 and 11.11).

5.2.1.13. Cell ID

Mobile station Cell Tower ID (Cell ID) Range of values is 0x000000 ~ 0xFFFFFF

5.2.1.14. ACC

ACC Status: ACC low as 00, ACC high as 01

5.2.1.15. Data Reporting Mode

Reserved, currently not using

5.2.1.16. Mileage Statistics (after turned on)

Mileage statistics is calculated and showed by hex. Unit is meter.
Example: 0x00 0x00 0x03 0xe8 represents 1000 meters.

5.2.1.17. GPS Re-transmission

0x00 GPS Real-time upload

0x01 GPS Re-transmission

5.2.1.18. Information Serial Number

See packet format 4.5

5.2.1.19. Error check

See packet format 4.6

5.2.1.20. Stop bits

See packet format 4.7

5.3. Alarm Packet (Combined packet of GPS, LBS, and alarm status)

5.3.1. Terminal sends alarm packets to the server.

Format			Length (Byte)	Example
information	Start bit		2	0x78 0x78
	Packet length		1	0x25
	Protocol No.		1	0x26
	Date Time		6	0x12 0x08 0x1B 0x06 0x00 0x02
	GPS information	Number of GPS satellites	1	0x00
		Latitude	4	0x02 0x6C 0x6D 0x72
		Longitude	4	0x0C 0x37 0x15 0x86
		Speed	1	0x00
		Course, Status	2	0x04 0x21
	LBS information	LBS Length	1	0x08
		MCC	2	0x01 0xCC
		MNC	1	0x00
		LAC	2	0x26 0x33
		Cell ID	3	0x00 0x10 0x04
	Status information	Terminal Information Content(Alarm Info)	1	0x12
		Voltage Level	1	0x06
		GSM Signal Strength	1	0x04
		Alarm / Language / extension bit status	2	0x02 0x01
	Serial Number		2	0x01 0x33
	Error Check		2	0x47 0x9D
	Stop Bits		2	0x0D 0x0A

The alarm packet is composed of the terminal information (alarm information) added on the positioning packet, and the coding format is also the same with the position packet.

5.3.1.1. Start Bit

See packet format 4.1

5.3.1.2. Packet Length

See packet format 4.2

5.3.1.3. Protocol No.

See packet format 4.3

5.3.1.4. Date Time

See packet format positioning 5.2.1.4

5.3.1.5. GPS information length, the number of satellite positioned

See packet format positioning 5.2.1.5

5.3.1.6. Latitude

See packet format positioning 5.2.1.6

5.3.1.7. Longitude

See packet format positioning 5.2.1.7

5.3.1.8. Speed

See packet format positioning 5.2.1.8

5.3.1.9. Status and Course

See packet format positioning 5.2.1.9

5.3.1.10. MCC

See packet format positioning 5.2.1.10

5.3.1.11. MNC

See packet format positioning 5.2.1.11

5.3.1.12. LAC

See packet format positioning 5.2.1.12

5.3.1.13. Cell ID

See packet format positioning 5.2.1.13

5.3.1.14. Terminal Information Content (Alarm Information)

1 byte, it's used to indicate various alarm information of the GPS terminal.

Format		Code Meaning
BYTE	Bit7	1: Oil and electricity Cut
		0: Oil and electricity On
	Bit6	1: GPS positioned
		0: GPS not positioned
	Bit3 ~ Bit5	100: SOS call
		011: Low battery alarm
		010: Power cut alarm
		001: Vibration alarm
		000: Normal

	Bit2	1: Powering and charging
		0: No power connection
	Bit1	1: ACC high
		0: ACC low
	Bit0	1: Defense on
		0: Defense off

Example: 0x44, convert to binary is 01000100

It represents the status of a GPS terminal is as follows: Oil and electricity is ON, GPS is positioned, no alarm, powering and charging, ACC is low, Defense is Off.

5.3.1.15. Voltage Level

Voltage ranges from 0 to 6 to demonstrate low or high.

0: No electricity (Power off)

1: Extreme low power (Not enough to make call or send text messages, etc.)

2: Very low power (Low battery alarm)

3: Low Power (Normal use)

4: Medium power

5: High power

6: Extreme high power

Example: 0x02 represents very low power, it will trigger “Low battery alarm”.

5.3.1.16. GSM Signal Strength Level

0x00: No signal

0x01: Extreme weak signal

0x02: Weak signal

0x03: Good signal

0x04: Strong signal

Example: 0x03 represents GSM signal good

5.3.1.17. Alarm/Language

0x00 (First byte) 0x01 (Second byte)

First byte: Represents the GPS terminal alarm status (used in alarm packet including Geo-fence function). Second byte: Represents the current language-bit

Byte 1	0x00: Normal(No alarm)
	0x01: SOS
	0x02: Power cut alarm
	0x03: Vibration alarm
	0x04: In fence alarm
	0x05: Out fence alarm
	0x06 Speeding alarm
	0x09 Movement alarm
	0x0A Into GPS blind area alarm
	0x0B Out GPS blind area alarm
	0x0C Power on alarm
	0x0E External power low battery alarm

	0x0F External power low battery protection alarm
	0X11 Power off alarm
	0X13 Demolition alarm
	0X14 Door alarm
	0X15 Low-power shutdown alarm
	0X2C Collision alarm
	0x2D Flip Alarm
	0x4C Sharp turn alarm
	0x30 Harsh breaking alarm
	0X29 Rapid acceleration alarm
Byte 2	0x01 Chinese 0x02 English

Example:

0x00 0x01 represents “Normal (No alarm)” in Chinese; 0x00 0x02 represents “Normal (No alarm)” in English:

Please note, to increase the reliability of alarm information, the alarm message is repeatedly sent respectively in Terminal Information Content (5.3.1.14) and Alarm/Language (5.3.1.17), in most cases these two alarm messages are identical, except two alarms are different as follows:

A: Low battery alarm B: In and out of the fence alarm

5.3.1.18. Information Serial Number

See packet format 4.5

5.3.1.19. Error check

See packet format 4.6

5.3.1.20. Stop bits

See packet format 4.7

Note: The status information in the data packet is the state at the moment recorded by the time bit in the data packet.

5.3.2. Server responds to alarm packet

Format		Length (Byte)	Example
Information	Start bit	2	0x78 0x78
	Packet length	1	0x05
	Protocol No.	1	0x26
	Serial number	2	0x01 0x33
	Error check	2	0x5D 0xAB
	Stop bits	2	0x0D 0x0A

The alarm packet is composed of the status information (alarm information) added on the positioning packet, and the coding format is also the same.

5.3.2.1. Start bit

See Packet Format 4.1

5.3.2.2. Packet length

See packet format 4.2

5.3.2.3. Protocol No.

See packet format 4.3

5.3.2.4. Information Serial Number

See packet format 4.5

5.3.2.5. Error check

See packet format 4.6

5.3.2.6. Stop bits

See packet format 4.7

5.3.3. The server reply to alarm packet with address info

5.3.3.1. Server reply with Chinese address

The server reply packet (15 + M + N Byte)	Start bit			2
	Data length			1
	Protocol No.			1
	Information	Command length		1
		Server flag		4
		Command content	ALARM SMS	8
			&&	2
			Address Content	M
			&&	2
			Telephone number	21
			##	2
	Information Serial Number			2
	Check Digit			2
	Stop bits			2

Chinese address reply protocol number: 0X17.

Command content: ALARMSMS&&Address&&Telephone numbers (all zero) ## (ALARMSMS, &&, ## are fixed strings)

Chinese address is encoded in **UNICODE** format.

Example of server replies Chinese address:

7878 //Start bit

85 //Data length

17 // Protocol number

7E // Command length, i.e. information length

00000001 // Server flag bit

414C41524D534D53 // ALARMSMS

2626&& // Separator

624059044F4D7F6E0028 // Chinese address is encoded in UNICODE format

004C004200530029003A

5E7F4E1C77015E7F5DDE

5E0282B190FD533AFF17

FF15FF144E6190530028
004E00320033002E0033
00390035002C00450031
00310032002E00390038
0038002996448FD1
2626&& // Separator
00000000000000000000000000000000000000000000 // Telephone number
2323## // Content info ending mark
0106 //Serial number
3825 //Check digit
0D0A // Stop bits

5.3.3.2. Server reply in English

Considering English or other foreign address is longer than Chinese, the data length is thus increased to 2 bytes. Please note: Data length increasing only applies to the situation which requires address reply.

The server reply packet (15 + M + N Byte)	Start bit			2
	Data length			2
	Protocol No.			1
	Information	Instruction length		2
		Server flag		4
		Instruction content	ALARMSMS	8
			&&	2
			Address Content	M
			&&	2
			Telephone number	21
			##	2
	Information Serial Number			2
	Check digit			2
	Stop bits			2

English address reply protocol number: 0X97

Command content: ALARMSMS&&Address&&Telephone numbers (all zero) ## (ALARMSMS, &&, ## are fixed strings)

Examples of server replies English address:

7979 // Start bit Changes from 7878 to 7979
00D2 // Data length
97 // Protocol No.
00CA // Command length, i.e. information length
00000001 // Server flag
414C41524D534D53 // ALARMSMS
2626&& // Separator

0053004F00530028004C // English address is encoded in UNICODE format
0029003A005300680069
006D0069006E00200046
0061006900720079006C
0061006E006400200057
0065007300740020052
0064002C004800750069
006300680065006E0067
002C004800750069007A
0068006F0075002C0047
00750061006E00670064
006F006E00670028004E
00320033002E00310031
0031002C004500310031
0034002E003400310031
0029004E006500610072
00,620,079
2626&& // Separator
00000000000000000000000000000000000000000000 //Telephone number
2323## // Content info end mark
0007 //Serial number
72b5 //Check digit
0D0A // stop bits

Please Note: Since some alarms do not require the platform to reply with address information, thus the platform does not need to reply address parsing after receiving the alarm packet from the terminal. For example, these three alarms in below do not require the server to reply with address info:

1. Low battery alarm 2. Speeding alarm 3.GPS blind area alarm

5.4. Heartbeat Packet (Status information packet)

A heartbeat packet is a data packet that maintains the connection between the terminal and the server. Please note the external voltage value is added here in the heartbeat packet(in language/extension section), for more details please check 5.4.1.5 and 5.4.1.7.

5.4.1. The terminal sends a heartbeat packet to the server

Format			Length (Byte)	Example
Information	Start bit		2	0x78 0x78
	Packet length		1	0x0A
	Protocol No.		1	0x13
	status information	Terminal information content	1	0x04
		Voltage level	1	0xF0
		GSM signal strength	1	0x04

	Language / extension bit status	2	0x8D 0x01
	Serial number	2	0x00 0x7F
	Error check	2	0x71 0x7F
	Stop bits	2	0x0D 0x0A

5.4.1.1. Start bit

See Packet Format 4.1

5.4.1.2. Packet length

See packet format 4.2

5.4.1.3. Protocol No.

0x13

5.4.1.4. Terminal Information

1 byte, it's used to indicate various alarm information of the GPS terminal.

Place		Code Meaning
BYTE	Bit7	1: Oil and electricity Cut
		0: Oil and electricity On
	Bit6	1: GPS positioned
		0: GPS not positioned
	Bit3 ~ Bit5	100: SOS call
		011: Low battery alarm
		010: Power cut alarm
		001: Vibration alarm
		000: Normal
	Bit2	1: Powering and charging
		0: No power connection
	Bit1	1: ACC high
		0: ACC low
	Bit0	1: Defense on
		0: Defense off

Example: 0x44, convert to binary is 01000100

It represents the status of a GPS terminal is as follows: Oil and electricity is ON, GPS is positioned, no alarm, powering and charging, ACC is low, Defense is Off.

5.4.1.5. Voltage level

Voltage ranges from 0 to 6 to demonstrate low or high.

0: No electricity (Power off)

1: Extreme low power (Not enough to make call or send text messages, etc.)

2: Very low power (Low battery alarm)

3: Low Power (Normal use)

4: Middle power

5: High power

6: Extreme high power

Example: 0x02 represents very low power, it will trigger “Low battery alarm”.

When a GPS terminal is connected with an external power source, it will show 0xFX at this packet. Multiply external voltage by 10, defined as high byte. F is a fixed value, meaning the GPS terminal is currently powering up by external voltage. To determine and calculate the exact voltage value, please check the Language/extension bit section in 5.4.1.7.

5.4.1.6. GSM signal strength level

0x00: No signal

0x01: Extreme weak signal

0x02: Weak signal

0x03: Good signal

0x04: Strong signal

Example: 0x03 represents GSM signal good

5.4.1.7. Language / extension bit status

First byte (for example 0x7E in below) is defined as low byte, combine it together with the high byte 0xF0 in Voltage level 5.4.1.5 to calculate the exact voltage value.

Example: When high byte=0xF0, and low byte=0x7E, ignore and discard fixed value F, and then take 0x007E, convert to decimal is 126, divide it by 10 equals to 12.6. Meaning the external voltage is 12.6V

	Description	Bits	Example
Information	Start Bit	2	7878
	Packet Length	1	0A
	Protocol Number	1	13
	Terminal Info	1	46
	Voltage Level	1	F0
	GSM signal strength	1	02
	Language /extension bit status	2	7E02
	Serial Number	2	006D
	Error Check	2	2878
	Stop Bit	2	0D0A

Second byte: Represents the current language byte

First byte	
Second byte	0x01 Chinese 0x02 English

Example:

No alarm in Chinese: 0x00 0x01

No alarm in English: 0x00 0x02

5.4.1.8. Information Serial Number

See packet format 4.5

5.4.1.9. Error check

See packet format 4.6

5.4.1.10. Stop bits

See Packet Format 4.7

5.4.2. The server responds to heartbeat data packet

The server responds to the terminal: (The protocol number in the response packet is the same as the protocol number of the data packet sent by the terminal).

Format		Length
Heartbeat packet (18 Byte)	Start bit	2
	Packet length	1
	Protocol No.	1
	Information Serial Number	2
	Error check	2
	Stop bits	2

5.4.2.1. Start bit

See Packet Format 4.1

5.4.2.2. Packet length

See packet format 4.2

5.4.2.3. Protocol No.

0x13

5.4.2.4. Information Serial Number

See packet format 4.5

5.4.2.5. Error check

See packet format 4.6

5.4.2.6. Stop bits

See Packet Format 4.7

5.4.3. Examples of data

Examples of terminal sends heartbeat data

78 78 08 13 4B 04 03 00 01 00 11 06 1F 0D 0A

Explanation

0x78 0x78	0x08	0x13	0x4B 0x04 0x03	0x00 0x01	0x00 0x11	0x06 0x1F	0x0D 0x0A
Start bit	Length	Protocol No.	Information	Reserved bytes (language)	Serial number	Error check	Stop bits

Examples of server reply

78 78 05 13 00 11 F9 70 0D 0A

Explanation

0x78 0x78	0x05	0x13	0x00 0x11	0xF9 0x70	0x0D 0x0A
Start bit	length	Protocol No.	Serial number	Error check	Stop bits

5.5.Position Data Packet (LBS ONLY)

5.5.1. Terminal sends LBS position packet to server

Format				Length(Byte)	Example
Information	Start bit			2	0x78 0x78
	Length			1	0x31
	Protocol No.			1	0x24
	Date Time			6	0x11 0x06 0x1b 0x06 0x2f 0x0d
	LBS	TA		1	0x00
		MCC		2	0x01 0xcc
		MNC		1	0x00
		Cell Num		1	0x04
		LBS1	LAC	2	0x26 0x33
			Cell ID	3	0x00 0x0e 0x7f
			RSSI	1	0x00
		LBS2	LAC	2	0x26 0x33
			Cell ID	3	0x00 0x0e 0x8a
			RSSI	1	0x24
		LBS3	LAC	2	0x26 0x33
			Cell ID	3	0x00 0x0e 0x80
			RSSI	1	0x23
		LBS4	LAC	2	0x26 0x33
			Cell ID	3	0x00 0x0f 0xf2
			RSSI	1	0x21
		LBS5	LAC	2	0x00 0x00
			Cell ID	3	0x00 0x00 0x00
			RSSI	1	0x00
	Reserved			1	0x00
	Reserved			1	0x00
	Reserved			1	0x00
	Serial Number			2	0x00 0x06
	Error Check			2	0x9f 0xc8
	Stop Bits			2	0x0d 0x0a

5.5.1.1. Start bit

See Packet Format 4.1

5.5.1.2. Packet length

See packet format 4.2

5.5.1.3. Protocol No.

See packet format 4.3 0x24

5.5.1.4. Date Time

Format	Length (Byte)	Examples
Year	1	0x0A
Month	1	0x03
Day	1	0x17
Time	1	0x0F
Minute	1	0x32
Second	1	0x17

Such as: at 15:50:23 on March 23rd, 2010

Calculation method: 10 (decimal) = 0A (16 hex)

3 (10 hex) = 03 (hex)

23 (10 hex) = 17 (hex)

15 (decimal) = 0F (16 hex)

50 (10 hex) = 32 (hex)

23 (10 hex) = 17 (hex)

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

5.5.1.5. MCC

Mobile Country Code (MCC)

Example: China's mobile country code is: 460 (decimal) 0x01 0xCC (460 converting into hexadecimal is 1CC, and 0 is added at the left side because the converted hexadecimal value is less than four digits).

Value ranges: 0x0000 ~ 0x03E7

5.5.1.6. MNC

Mobile Network Code (MNC)

Example: China Mobile is 0x00.

5.5.1.7. LAC

Location Area Code (LAC) is included in the LAI, consists of two bytes, and uses hexadecimal coding. The available range is 0x0001-0xFFFE, and the code groups 0x0000 and 0xFFFF cannot be used (see GSM specifications 03.03, 04.08 and 11.11).

5.5.1.8. Cell ID

Mobile station Cell Tower ID (Cell ID) Range of values is 0x000000 ~ 0xFFFFFF

5.5.1.9. RSSI

The signal strength value range is 0x00～0xFF. The actual signal strength is a negative value, so in data transfer it's uploaded by its absolute value.

See Glossary - RSSI.

5.5.1.10. Information Serial Number

See packet format 4.5

5.5.1.11. Error Check

See packet format 4.6

5.5.1.12. Stop bits

See Packet Format 4.7

5.6. General information transmission packet

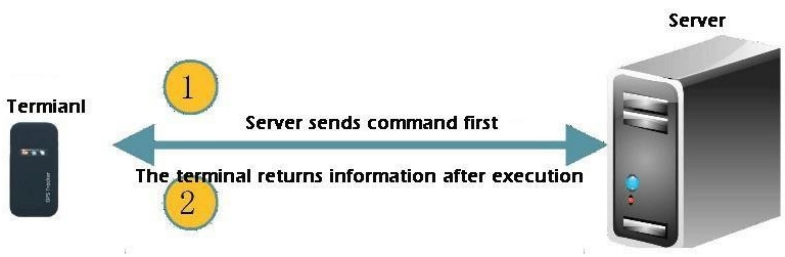
Used to transfer various types of non-location data.

Format		Length	Example
Start bit		2	0x79 0x79
Packet length		2	0x00 0x20
Protocol No.		1	0x94
Information	Message type (Sub protocol number)	1	00 External voltage 01 to 03 (customization) 04 Terminal status synchronization 05 Air con and Door status 08 Self-Inspection parameters 09 Positioning satellite information 0A ICCID and other information ..... to be added
	Data content	N	Depending on the information content
Information Serial Number		2	Serial number automatically increase 1 from power on when sending data
Error check		2	The error check code adopts the CRC-ITU check method. The CRC-ITU value of the part of the data in the protocol body from "packet length" to "information serial number"
Stop bits		2	Fixed value, unified 0x0D 0x0A

When the message type equals 0A, it should transfer the following information in hexadecimal, for example 08 69 81 41 01 11 51 23 04 60 04 24 29 80 22 56 89 86 04 04 10 18 C0 00 22 55

IMEI	8	Example: IMEI number 123456789123456, then the terminal ID should be shown as 0x01 0x23 0x45 0x67 0x89 0x12 0x34 0x56
IMSI	8	Example: IMSI number 0460042429802256, then the terminal ID should be shown as 0x04 0x60 0x04 0x24 0x29 0x80 0x22 0x56
ICCID	10	Example: ICCID number is 898604041018 C0002255, then the terminal ID should be shown as 0x89 0x86 0x04 0x04 0x10 0x18 0xC0 0x00 0x22 0x55
Air con and Door status	1	Example: 0x03 represents Air conditioning and car door are both open Bit7 - Bit2 reserved Bit1 0: 0 Door is close 1 Door is open Bit0 0: 0 Air con is off 1 Air con is on

VI. Server sends the data packet to the terminal



6.1. The server sends

Format		Length (Byte)
Start bit		2
Packet length		1
Protocol No.		1
Information	Command length	1
	Server flag	4
	Command content	M
	Language	2
Information Serial Number		2
Error check		2
Stop bits		2

6.1.1. Start bit

See Packet Format 4.1

6.1.2. Packet length

See packet format 4.2

6.1.3. Protocol No.

0x80

6.1.4. Command length

Server flag+ Command content length

Example: Use byte length as unit, 0x0A, represents flag bit + the command content =10 bytes

6.1.5. Server flag

It is reserved for identification by the server, and the terminal will return the received data in the return package in binary form.

6.1.6. Command content

Expressed as a string of ASCII, the command content is compatible with SMS commands.

6.1.7. Language

Current language in use of the terminal.

Chinese: 0x00 0x01

English: 0x00 0x02

6.1.8. Information Serial Number

See packet format 4.5

6.1.9. Error check

See packet format 4.6

6.1.10. Stop bits

See Packet Format 4.7

6.2. Terminal reply to server

Format		Length (Byte)	Examples
Start bit		2	0x79 0x79
Packet length		2	0x00 0x09
Protocol No.		1	0x21
Information	Server flag	4	0x00 0x00 0x00 0x01
	Content-Encoding	1	
	Content	M	
Information Serial Number		2	0x00 0x01
Error check		2	0xD9 0xDC
Stop bits		2	0x0D 0x0A

6.2.1 Start bit

Fixed value 0x79 0x79

6.2.2 Packet length

2 bytes

6.2.3 Protocol No.

0x21

6.2.4 Server flag

It is reserved for identification by the server, and the terminal will return the received data in the return package in binary form.

6.2.5 Content-Encoding

0x01 ASCII coding

0x02 UTF16-BE coding

6.2.6 Content

Information needs to be transferred.

6.2.7 Information Serial Number

See packet format 4.5

6.2.8 Error check

See packet format 4.6

6.2.9 Stop bits

See Packet Format 4.7

6.3. Cut off petrol and electricity

Functional Description: Cut off vehicle electricity and oil supply.

The example below will send and return the string after converting ASCII to show the commands.

The server sends
RELAY, 1 #

Terminal returns
If successful, return DYD = Success! If fail, return (refer to below description)

6.4. Restore oil and electricity

Functional Description: Restore vehicle oil and electricity

The example below will send and return the string after converting ASCII to show the commands.

The server sends
RELAY, 0 #
Terminal returns
If successful, return If fail, return (refer to below description)

Description:

The following are the various replies after sending cut off petrol and electricity, it's only judged to be success when the word Success can be searched out.

RELAY, ERROR: 104

Command Error

RELAY, ERROR: 103

Command parameter error

RELAY, FAIL! ACC ON, GPS has Not FIXED or speed> 20KM / H, relay delay!!

Off petrol and electricity failure! The fuel cut operation will delay if the ACC is turned on, GPS not positioned or the speed is over 20KM / H,

RELAY, The oil has been cut already!!

Off petrol and electricity failure! Already in electricity off mode.

RELAY, The oil has been Resume already!!

Restore oil and electricity failed! Already in electricity restored mode!

Cut off the fuel supply: Success Speed: ! 0 km / h.

Off petrol and electricity success.

Restore fuel supply: Success!

Restore oil and electricity success.

6.5.Add SOS number

Functional Description: Set phone numbers to receive alarm messages and phone calls.

The server sends
SOS, A, NUM1, NUM2, NUM3 #
Terminal returns
Successful return
OK SOS1:! NUM1SOS2: NUM2SOS3NUM3
Failure to return
ERROR: XXX

6.6. Delete SOS number

Functional Description: Delete phone numbers which are receiving text messages and phone calls.

The server sends
SOS, D, NUM1, NUM2, NUM3 #
Terminal returns
Successful return
OK SOS1:! NUM1SOS2: NUM2SOS3NUM3
Failure to return
ERROR: XXX

6.7. Set center number

Functional Description: Set phone numbers to cut off oil and electricity.

The server sends
CENTER, A, NUM #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.8. Delete center number

Functional Description: Delete phone numbers which are able to cut off oil and electricity.

The server sends
CENTER, D #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.9. Enable vibration alarm

Functional Description: Enable vibration alert

The server sends
SENALM, ON, Alarm #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

Alarm method 0: Platform; 1:Platform+SMS; 2: Platform+ SMS + phone call; 3 Platform+ phone call;

6.10. Disable vibration alarm

Functional Description: Disable vibration alert

The server sends
SENALM, OFF #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.11. Enable speeding alarm

Functional Description: Enable speeding alarm

The server sends
SPEED, ON, TIME, SPEED, Alarm #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

Alarm method 0: Platform; 1: Platform+SMS;

6.12. Disable speeding alarm

Functional Description: Disable speeding alarm

The server sends
SPEED, OFF #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.13. Enable power cut alarm

Functional Description: Enable power cut alarm

The server sends
POWERALM, ON, Alarm #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

Alarm method 0: Platform; 1:Platform+SMS; 2: Platform+ SMS + phone call; 3 Platform+ phone call;

6.14. Disable power cut alarm

Functional Description: Disable power cut alarm

The server sends
POWERALM, OFF #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.15. Enable movement alarm

Functional Description: Enable movement alarm

The server sends
MOVING, NO, radial displacement, Alarm #
Terminal returns
Successful return
OK
Failure to return

ERROR: XXX

Alarm method 0: Platform; 1:Platform+SMS; 2: Platform+ SMS + phone call; 3 Platform+ phone call;

Movement radius:100~1000 meters

6.16. Disable movement alarm

Functional Description: Disable movement alarm

The server sends
MOVING, OFF #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.17. Enable low battery alarm

Functional Description: Enable low battery alarm

The server sends
BATALM, ON, Alarm #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

Alarm method 0: Platform; 1: Platform + SMS;

6.18. Disable low battery alarm

Functional Description: Disable low battery alarm

The server sends
BATALM, OFF #
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX

6.19. Enable Geo-fence alarm

Functional Description: Enable Geo-fence alarm

The server sends

FENCE, ON, 0,Latitude center, Longitude center, Radius of the fence, X,Alarm# E.g:FENCE, ON, 0, N1.2971, E103.822349,61, IN, 0 #
Terminal returns Successful return OK Failure to return ERROR: XXX

Alarm method 0: Platform; 1: Platform+SMS;
X = IN/OUT; IN: In fence alarm; OUT: Out fence alarm; If empty it will alarm both when goes in and out of the fence(In default).

6.20. Disable Geo-fence alarm

Functional Description: Disable Geo-fence alarm

The server sends FENCE,OFF#
Terminal returns Successful return OK Failure to return ERROR: XXX

6.21. Reboot Device

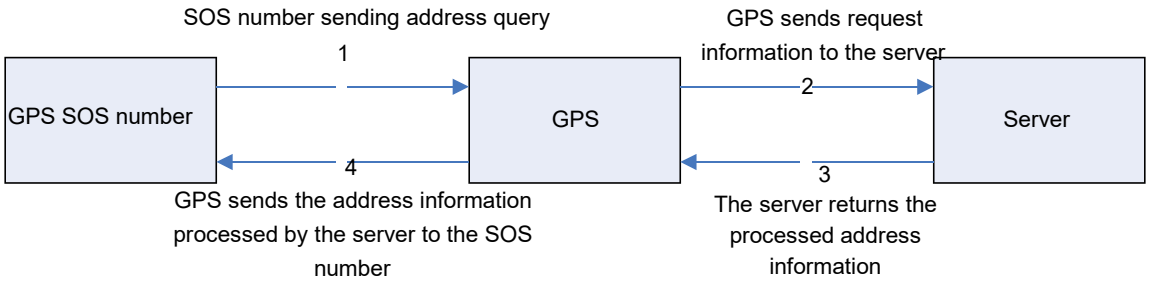
Functional Description: Reboot the device after 1 minute

The server sends RESET #
Terminal returns Successful return The terminal will restart after 1 minute! Failure to return ERROR: XXX

6.22. Server sends address information query request

The server sends
ADDRESS, the contents of the address, phone number
Note: Chinese address will be sent in UNICODE format.

6.23. SOS number request address information packet (0X2A)



6.23.1. Terminal sends data to server

Basically the same format with the previously mentioned GPS information content, added the phone number to make address inquiry.

Format			Length (Byte)
Start bit			2
Packet length			1
Protocol No.			1
Information	Date Time		6
	GPS information	GPS information length, the number of satellites positioned	1
		Latitude	4
		Longitude	4
		Speed	1
		Course, Status	2
	Telephone number		21
	Language		2
Information Serial Number			2
Error check			2
Stop bits			2

6.7.1.1. Start bit

See Packet Format 4.1

6.7.1.2. Packet length

See packet format 4.2

Example: Use byte length as unit, 0x2E, it means that the command content occupies 46 bytes

6.7.1.3. Protocol No.

0x2A.

6.7.1.4. Date Time

See packet format 5.2.1.4

6.7.1.5. GPS information length, the number of satellites positioned

See packet format 5.2.1.5

6.7.1.6. Latitude

See packet format 5.2.1.6

6.7.1.7. Longitude

See packet format 5.2.1.7

6.7.1.8. Speed

See packet format 5.2.1.8

6.7.1.9. Course

See packet format 5.2.1.9

6.7.1.10. Telephone number

SOS number to inquire address, convert to ASCII, add 0 on the right side if less than 21 digits.

6.7.1.11. Language

Current language the terminal is using.

Chinese: 0x00 0x01

English: 0x00 0x02

6.7.1.12. Information Serial Number

See packet format 4.5

6.7.1.13. Error check

See packet format 4.6

6.7.1.14. Stop bits

See Packet Format 4.7

6.23.2. Server response

Reply Chinese or English address based on the command. The reply packet is different.

6.23.2.1. Chinese reply

See format 5.3.3.1

6.23.2.2. English Reply

See format 5.3.3.2

VII. Appendix A: CRC-ITU look-up table algorithm C language code snippet

CRC-ITU look-up table algorithm C language code snippet

```
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,
};

// 16-bit CRC is calculated for a given length of the 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; // negated
}
```

VIII. Appendix B: Example of communication protocol data packet

The following data is intercepted from the communication between the terminal and the server, and displayed in hexadecimal. Sending means sending from the terminal, receiving means receiving from the server:

Login packet:

Sent: 78 78 0D 01 03 53 41 35 32 15 03 62 00 02 2D 06 0D 0A

Received: 78 78 05 01 00 02 EB 47 0D 0A

GPS data packets (Combined GPS and LBS):

Sent: 78 78 1F 12 0B 08 1D 11 2E 10 CF 02 7A C7 EB 0C 46 58 49 00 14 8F 01 CC 00 28 7D 00 1F B8 00 03 80 81 0D 0A

Status packet:

Sent: 78 78 0A 13 44 01 04 00 01 00 05 08 45 0D 0A

Received: 78 78 05 13 00 05 AF D5 0D 0A

Cut off oil and electricity:

Received: 78 78 15 80 0F 00 01 A9 58 44 59 44 2C 30 30 30 30 30 30 23 00 A0 DC F1 0D 0A

Sent: 78 78 18 15 10 00 01 A9 58 44 59 44 3D 53 75 63 63 65 73 73 21 00 02 00 18 91 77 0D 0A

Sent under DYD server, # 000000 Reply:

DYD = Success!

Command sent in the case of oil and electricity has been disconnected:

Received: 78 78 15 80 0F 00 01 A9 61 44 59 44 2C 30 30 30 30 30 30 23 00 A0 3E 10 0D 0A

Sent: 78 78 53 15 4B 00 01 A9 61 41 6C 72 65 61 64 79 20 69 6E 20 74 68 65 20 73 74 61 74 65 20 6F 66 20 66 75 65 6C 20 73 75 70 70 6C 79 20 63 75 74 20 6F 66 66 2C 74 68 65 20 63 6F 6D 6D 61 6E 64 20 69 73 20 6E 6F 74 20 72 75 6E 6E 69 6E 67 21 00 02 00 1C F3 0D 0D 0A

Sent under DYD server, # 000000

Reply: Already in the state of fuel supply cut off, the command is not running!

Restore oil and electricity:

Received: 78 78 16 80 10 00 01 A9 63 48 46 59 44 2C 30 30 30 30 30 30 23 00 A0 7B DC 0D 0A

Sent: 78 78 19 15 11 00 01 A9 63 48 46 59 44 3D 53 75 63 63 65 73 73 21 00 02 00 1E F8 93 0D 0A

The server sends: HFYD, 000000 #

Reply: HFYD = Success!

Instructions have been issued to restore oil and electricity case:

Received: 78 78 16 80 10 00 01 A9 64 48 46 59 44 2C 30 30 30 30 30 30 23 00 A0 8B 1B 0D 0A

Sent: 78 78 55 15 4D 00 01 A9 64 41 6C 72 65 61 64 79 20 69 6E 20 74 68 65 20 73 74 61 74 65 20 6F 66 20 66 75 65 6C 20 73 75 70 70 6C 79 20 74 6F 20 72 65 73 75 6D 65 2C 74 68 65 20 63 6F 6D 6D 61 6E 64 20 69 73 20 6E 6F 74 20 72 75 6E 6E 69 6E 67 21 00 02 00 1F DB BF 0D 0A

The server sends: HFYD, 000000 #

Reply: Already in the state of fuel supply to resume, the command is not running!

Terminal to obtain address information from the server:

Chinese:

Sent: 78 78 2E 1A 0B 0B 0F 0E 21 17 CF 02 7A C8 87 0C 46 57 E3 00 14 02 36 36 33 36 36 00 03 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 34 AD E9 0D 0A

Received: 78 78 94 17 8E 00 00 00 01 41 44 44 52 45 53 53 26 26 4F 4D 7F 6E 00 3A 5E 7F 4E 1C 77 01 60 E0 5D DE 5E 02 4E 91 5C 71 89 7F 8D EF 00 2E 65 87 53 4E 4E 00 8D EF 00 2E 79 BB 60 E0 5D DE 5B 89 4F 17 4F 1A 8B A1 5E 08 4E 8B 52 A1 62 40 7E A6 00 33 00 32 7C 73 00 2E 79 BB 60 E0 5D DE 5E 02 59 16 55 46 62 95 8D 44 67 0D 52 A1 4E 2D 5F C3 7E A6 00 33 00 32 7C 73 00 2E 26 26 36 36 33 36 36 00 03 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 23 23 00 01 E4 2A 0D 0A

Sent contents from server: Location: Huizhou, Guangdong Province Yunshan Road all the way from the Mandarin, Huizhou, the Public Accounting Firm of about 32 meters, about 32 meters from the Huizhou City Foreign Investment Service Center.

Phone number: 66366

English:

Sent: 78 78 2E 1A 0B 0B 0F 0E 1E 08 CF 02 7A C8 A2 0C 46 57 D7 00 14 02 36 36 33 36 36 00 03 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 32 04 3A 0D 0A

Receiving: 78 78 00 E9 97 00 E2 00 00 00 01 41 44 44 52 45 53 53 26 26 00 50 00 72 00 65 00 63 00 69 00 73 00 65 00 6C 00 79 00 20 00 4C 00 6F 00 63 00 61 00 74 00 69 00 6E 00 67 00 3A 00 31 00 30 53 F7 00 20 00 59 00 75 00 6E 00 73 00 68 00 61 00 6E 00 20 00 57 00 65 00 73 00 74 00 20 00 52 00 64 00 2C 00 48 00 75 00 69 00 63 00 68 00 65 00 6E 00 67 00 2C 00 48 00 75 00 69 00 7A 00 68 00 6F 00 75 00 2C 00 47 00 75 00 61 00 6E 00 67 00 64 00 6F 00 6E 00 67 00 2C 00 35 00 31 00 36 00 30 00 30 00 33 00 28 00 4E 00 32 00 33 00 2E 00 31 00 31 00 31 00 37 00 37 00 2C 00 45 00 31 00 31 00 34 00 2E 00 34 00 30 00 39 00 32 00 32 00 29 26 26 36 36 33 36 36 00 03 00 04 00 00 00 00 00 00 00 00 00 00 00 00 23 23 00 01 AF 4D 0D 0A

The content distribution server: Precisely Locating: No. 10 Yunshan West Rd, Huicheng, Huizhou, Guangdong, 516003 (N23.11177, E114.40922)

Phone number: 66366

Alarm package process:

Chinese SMS:

Sent: 78 78 25 16 0B 0B 0F 0E 24 1D CF 02 7A C8 87 0C 46 57 E6 00 14 02 09 01 CC 00 28 7D 00 1F 72 65 06 04 01 01 00 36 56 A4 0D 0A

Received: 78 78 05 16 00 36 95 70 0D 0A

Received: 78 78 BE 17 B8 00 00 00 01 41 4C 41 52 4D 53 4D 53 26 26 7D 27 60 25 54 7C 53 EB 00 3A 5E 7F 4E 1C 77 01 60 E0 5D DE 5E 02 4E 91 5C 71 89 7F 8D EF 00 2E 65 87 53 4E 4E 00 8D EF 00 2E 79 BB 4E 2D 88 4C 00 41 00 54 00 4D 7E A6 00 33 00 31 7C 73 00 2E 79 BB 4E 2D 88 4C 6C 5F 53 17 65 2F 88 4C 7E A6 00 33 00 31 7C 73 00 2E 00 2C 00 31 00 31 00 2D 00 31 00 31 00 2D 00 31 00 35 00 20 00 31 00 34 00 3A 00 33 00 36 00 3A 00 32 00 39 26 26 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 23 23 00 01 B6 D8 0D 0A

SMS content: Emergency call: Huizhou City, Guangdong Province Yunshan Road culture all the way about 31 meters from the Bank of China, Bank of China ATM about 31 meters from the Jiangbei Branch, 11/15/11 14:36:29...

The specific meaning of the command can be found in this document.

IX. Appendix C: Full packet format example

A. Data packets sent by the terminal to the server

Login information packet (18 Byte)						
Start bit	Packet Length	Protocol No.	Terminal ID	Information Serial Number	Check Digit	Stop bits
2	1	1	8	2	2	2

GPS information packet (26 + N Byte)												
			Information									
				GPS information								
Start bit	Packet length	Protocol No.	Date Time	GPS information length, the number of satellite positioned	Latitude	Longitude	Speed	Course Status	Reserved bit	Serial Number	Check Digit	Stop bits
2	1	1	6	1	4	4	1	2	N	2	2	2

LBS information packet (23 + N Byte)											
			Information								
				LBS Information							
Start bit	Packet length	Protocol No	Date Time	MCC	MNC	LAC	Cell ID	Reserved bit	Serial number	Check Digit	Stop bits
2	1	1	6	2	1	2	3	N	2	2	2

LBS complete information packet (42 + N Byte)																								
			Information																					
				LBS information																				
Start bit	Packet length	Protocol No.	Date time	MCC	MNC	LAC	MCI	MCISS	NCI1	NCISS1	NCI2	NCISS2	NCI3	NCISS3	NCI4	NCISS4	NCI5	NCISS5	NCI6	NCISS6	Reserved bit	Serial Number	Check Digit	Stop bits
2	1	1	6	2	1	2	2	1	2	1	2	1	2	1	2	1	2	1	2	1	N	2	2	2

GPS, LBS packet (34 + M + N Byte)																	
			Information														
				GPS information						LBS information							
Start bit	Packet length	Protocol No.	Date Time	GPS information length, the number of satellite positioning participation	Latitude	Longitude	Speed	Course, status	Reserved bit	MCC	MNC	LAC	Cell ID	Reserved bit	Serial Number	Check Digit	Stop bits
2	1	1	6	1	4	4	1	2	M	2	1	2	3	M	2	2	2

Status Packet (13 + N Byte)									
			Information						
Start bit	Packet length	Protocol No.	Terminal information content	Voltage level	GSM signal strength level	Reserved extension bit	Serial Number	Check Digit	Stop bits
2	1	1	1	1	1	2	2	2	2

Satellite SNR information (11 + M + N Byte)								
Start bit	Packet length	Protocol No.	Information			Information Serial Number	Check Digit	Stop bits
			The number of satellites involved in positioning	Satellite signal to noise ratio	Reserve extension bit			
				1 2 3 ..... n				
2	1	1	1	M	N	2	2	2

Terminal responses to command (15 + M + N Byte) sent by the server									
Start bit	Packet length	Protocol No.	String content				Serial Number	Check Digit	Stop bits
			Command length	Server flag	Command content	Reserve extension bit (language)			
2	1	1	1	4	M	2	2	2	2

GPS, LBS, status information packet (40 + M + N + L Byte)																					
Start bit	Packet length	Protocol No.	Information																Reserved bit (Language)	Serial Number	Check Digit	Stop bits
			Date Time	GPS information						LBS information						Status information					
				GPS information length, the number of satellite positioned	latitude	longitude	speed	Course, state	Reserved bit	LBS length	MCC	MNC	LAC	Cell ID	Reserved bit	Terminal information content	Voltage level	GSM signal strength level				
2	1	1	6	1	4	4	1	2	M	1	2	1	2	3	N	1	1	1	2	2	2	2

B. Data Packet Sent by Server to Terminal

Response of Server after receiving Status Packet from Terminal (10 Bytes)					
Start bit	Packet length	Protocol No.	Serial Number	Check Digit	Stop bits
2	1	1	2	2	2

Command Packet Sent by Server to Terminal (15+M+N Byte)									
Start bit	Packet length	Protocol No.	information				Serial Number	Check Digit	Stop bits
			Command length	Server flag	Command content	Reserve extension bit			
2	1	1	1	4	M	N	2	2	2