GPS Tracker
Communication Protocol

CONFIDENTIAL

Copyright

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. Terms, Definitions

Terms, Abbreviation	Definition in English	Definition in Chinese
CMPP	China Mobile Peer to Peer	中国移□点□点□□
GPS	Global Positioning System	全球□星定位系□
GSM	Global System for Mobile Communication	全球移□通信系□
GPRS	General Packet Radio Service	通用无□分□□□
TCP	Transport Control Protocol	□□控制□□
LBS	Location Based Services	□助定位服□
IMEI	International Mobile Equipment Identity	国□移□□□□别□
MCC	Mobile Country Code	移□用□所属国家代号
MNC	Mobile Network Code	移□网号□
LAC	Location Area Code	位置区□
Cell ID	Cell Tower ID	移□基站
UDP	User Datagram Protocol	用□数据□□□
SOS	Save Our Ship/Save Our Souls	遇□求救信号
CRC	Cyclic Redundancy Check	循□冗余校□
NITZ	Network Identity and Time Zone	□区
GIS	Geographic Information System	地理信息系□

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 will be sent by the terminal after three minutes to regularly confirm the connection.

2) If the GPRS connection is established unsuccessfully, the terminal will not be able to send the login message packet. The terminal will start schedule reboot in twenty minutes if the GPRS connection is failed three times. Within twenty minutes, if the terminal successfully connects to the server and receives the data packet from the server as the server's response to the login message packet sent by the terminal, the schedule reboot will be off and the terminal will not be rebooted; otherwise, the terminal will be rebooted automatically in twenty minutes.

3) After receiving the login message packet, the server will return a response data packet. If the terminal doesn't receive packet from the server within five seconds after sending the login message packet or the status information package, the current connection is regarded as an abnormal connection. The terminal will start a retransmission 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) If the connection is regarded to be abnormal, and the data packet as a response 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) In case of the 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 effectiveness of the connection, the terminal will send status information to the server at regular intervals, and the server will return response data packets to confirm the connection.

7) For the terminal which doesn't register an IMEI number, the server will reply the terminal with a login request response and heartbeat packet response, rather than directly disconnect the connection. (If the connection is directly disconnected or the server doesn't reply to the terminal, it will lead to a continuous reconnected by the terminal and the GPRS traffic will be consumed heavily

CONFIDENTIAL

iv. Data Packet Format

The communication is transferred asynchronously in bytes.
The total length of packets is (10+N) Bytes.

Format	Length(Byte)
Start Bit	2
Packet Length	1
Protocol Number	1
Information Content	N
Information Serial Number	2
Error Check	2
Stop Bit	2

4.1. Start Bit

Fixed value in HEX 0x78 0x78.

4.2. Packet Length

Length = Protocol Number + Information Content + Information Serial Number + Error Check, totally (5+N)Bytes, because the Information Content is a variable length field.

4.3. Protocol Number

Type	Value
Login Message	0x01
Location Data /(Positioning Data（UTC）)	0x12 /0x22(V3 Protocol)
Status information	0x13
String information	0x15
Alarm data	0x16
GPS, query address information by phone number	0x1A
Command information sent by the server to the terminal	0x80

In V3 protocol, the location data can be reported by 0x22, which can include: ACC status, blind spot mark and mileage data.

Other messages are like the regular GT06 protocol. After SZCS # GT06SEL=1, the device software is only compatible with this one message type.(ID: 0x12 in standard protocol, switch to V3 protocol, report 0x22 in uploading location data)

CONFIDENTIAL

4.4. Information Contents

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 data packet such as GPS, LBS) sent after booting is '1', and the serial number of data sent later at each time will be automatically added '1'.

4.6. Error Check

A check code may be used by the terminal or the server to distinguish whether the received information is error or not. To prevent errors occur during data transmission, error check is added to against data misoperation, so as to increase the security and efficiency of the system. The check code is generated by the CRC-ITU checking 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.

CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet.

4.7. Stop Bit

Fixed value in HEX 0x0D 0x0A.

CONFIDENTIAL

v. Details about Data Packet sent by Terminal to Server

The commonly used information packages sent by the terminal and those sent by the server will be interpreted separately.

5.1. Login Message Packet

5.1.1. Terminal Sending Data Packet to Server

The login message packet is used to be sent to the server with the terminal ID so as to confirm the established connection is normal or not.

	Description	Bits	Example
Login Message Packet(18 Byte)	Start Bit	2	0x78 0x78
	Packet Length	1	0x0 D
	Protocol Number	1	0x0 1
	Terminal ID	8	0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45
	Information Serial Number	2	0x00 0x01
	Error Check	2	0x8C 0xDD
	Stop Bit	2	0x0D 0x0

CONFIDENTIAL

5.1.1.1. Start Bit

For details see Data Packet Format section 4.1.

5.1.1.2. Packet Length

For details see Data Packet Format section 4.2.

5.1.1.3. Protocol Number

For details see Data Packet Format section 4.3.

5.1.1.4. Terminal ID

The terminal ID applies IMEI number of 15 bits.

Example: if the IMEI is 123456789012345,

the terminal ID is 0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45.

5.1.1.5. Information Serial Number

For details see Data Packet Format section 4.5.

5.1.1.6. Error Check

For details see Data Packet Format section 4.6.

5.1.1.7. Stop Bit

For details see Data Packet Format section 4.7.

Protocol **5.1.2. Server Responds the Data Packet**

	Description	Bits	Example
Login Message Packet (18Byte)	Start Bit	2	0x78 0x78
	Packet Length	1	0x0 5
	protocol	1	0x01
	Information Serial Number	2	0x00 0x01
	Error Check	2	0xD9 0xDC
	Stop Bit	2	0x0D 0x0A

The response packet from the server to the terminal: the protocol number in the response packet is identical to the protocol number in the data packet sent by the terminal.

5.1.2.1. Start Bit
For details see Data Packet Format section 4.1.

5.1.2.2. Packet Length
For details see Data Packet Format section 4.2.

5.1.2.3. Protocol Number
For details see Data Packet Format section 4.3.

5.1.2.4. Information Serial Number
For details see Data Packet Format section 4.5.

5.1.2.5. Error Check
For details see Data Packet Format section 4.6.

5.1.2.6. Stop Bit
For details see Data Packet Format section 4.7.

5.1.3. Examples

Examples of the login message packet sent by the terminal to the server and the response packet sent by the server to the terminal are as follows: (in the examples, the terminal ID is 1234567890123456789).

Example of data packet sent by the terminal 78 78 0D 01 01 23 45 67 89 01 23 45 00 01 8C DD 0D 0A

Explain

0x78 0x78	0x0D	0x01	0x01 0x23 0x45 0x67 0x89 0x01 0x23 0x45	0x00 0x01	0x8C 0xDD	0x0D 0x0A
Start Bit	Length	Protocol No.	Terminal ID	Serial No.	Error Check	Stop Bit

Example of response packet returned by the server

78 78 05 01 00 01 D9 DC 0D 0A

Explain

0x78 0x78	0x05	0x01	0x00 0x01	0xD9 0xDC	0x0D 0x0A
Start Bit	Length	Protocol No.	Serial No.	Error Check	Start Bit

CONFIDENTIAL

5.2. Location Data Packet (combined information package of GPS and LBS)

5.2.1. Terminal Sending Location Data Packet to Server

	Format		Length(Byte)	Example
Information Content	Start Bit		2	0x78 0x78
	Packet Length		1	0x1F
	Protocol Number		1	0x12
	GPS Information	Date Time	6	0x0B 0x08 0x1D 0x11 0x2E 0x10
		Quantity of GPS information satellites	1	0 xCF
		Latitude	4	0x02 0x7A 0xC7 0xEB
		Longitude	4	0x0C 0x46 0x58 0x49
		Speed	1	0x00
		Course, Status	2	0x14 0x8F
	LBS Information	MCC	2	0x01 0xCC
		MNC	1	0x00
		LAC	2	0x28 0x7D
		Cell ID	3	0x00 0x1F 0xB8
	Serial Number		2	0x00 0x03
	Error Check		2	0x80 0x81
	Stop Bit		2	0x0D 0x0A

5.2.1.1. Start Bit

For details see Data Packet Format section 4.1.

5.2.1.2. Packet Length

For details see Data Packet Format section 4.2.

5.2.1.3. Protocol Number

For details see Data Packet Format section 4.3.

5.2.1.4. Date Time

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

CONFIDENTIAL

Example: 2010-03-23 15:30:23
Calculated as follows: 10(Decimal)=0A(Hexadecimal)
3 (Decimal)=03(Hexadecimal)
23(Decimal)=17(Hexadecimal)
15(Decimal)=0F(Hexadecimal)
Then the value is: 0x0A 0x03 0x17 0x0F 0x32 0x17

5.2.1.5. Length of GPS information, quantity of positioning satellites

The field is 1 Byte displayed by two hex digits, wherein the first one is for the length of GPS information and the second one for the number of the satellites join in positioning.

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

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

5.2.1.6. Latitude

Four bytes are consumed, defining the latitude value of location data. The range of the value is 0-162000000, indicating a range of 0°-90°. The conversion method thereof is as follow:

converting the value of latitude and longitude output by GPS module into a decimal based on minute; multiplying the converted decimal by 30000; and converting the multiplied result into hexadecimal.

Example: 22°32.7658′=(22X60+32.7658)X3000=40582974,
then converted into a hexadecimal number:
40582974(Decimal)= 26B3F3E(Hexadecimal)
at last the value is 0x02 0x6B 0x3F 0x3E.

5.2.1.7. Longitude

Four bytes are consumed, defining the longitude value of location data. The range of the value is 0-324000000, indicating a range of 0°-180° .

The conversion method herein is same to the method mentioned in Latitude (see section 5.2.1.6).

5.2.1.8. Speed

One byte is consumed, defining the running Speed of GPS. The value ranges from 0x00 to 0xFF indicating a range from 0 to 225km/h.

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

CONFIDENTIAL

5.2.1.9. Course Status

Two bytes are consumed, defining the running direction of GPS. The value ranges from 0° to 360° measured clockwise from north of 0° .

BYTE_ 1	Bit7	0
	Bit6	0
	Bit5	GPS real-time/differential positioning
	Bit4	GPS having been positioning 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 status information in the data packet is the status corresponding to the time bit recorded in the data packet.

For example: the value is 0x15 0x4C, the corresponding binary is 00010101 01001100:

BYTE_1 Bit7 0
BYTE_1 Bit6 0
BYTE_1 Bit5 0 (realtime GPS)
BYTE_1 Bit4 1 (GPS has beenpositioned)
BYTE_1 Bit3 0 (East Longitude)
BYTE_1 Bit2 1 (North Latitude)
BYTE_1 Bit1 0
BYTE_1 Bit0 1
BYTE_2 Bit7 0
BYTE_2 Bit7 1
BYTE_2 Bit7 0
BYTE_2 Bit7 0
BYTE_2 Bit7 1
BYTE_2 Bit7 1
BYTE_2 Bit7 0
BYTE_2 Bit7 0

→Course 332° (0101001100 in Binary, or 332 in decimal)

which means GPS tracking is on, realtime GPS, location at north latitude, east longitude and the course is 332° .

CONFIDENTIAL

5.2.1.10. MCC

The country code to which a mobile user belongs, i.e., Mobile Country Code(MCC).
Example: Chinese MCC is 460 in decimal, or 0x01 0xCC in Hex (that is, a decimal value of 460 converting into a hexadecimal value, and 0 is added at the left side because the converted hexadecimal value is less than four digits).
Herein the range is 0x0000 ~ 0x03E7.

5.2.1.11. MNC

Mobile Network Code(MNC)
Example: Chinese MNC is 0x00.

5.2.1.12. LAC

Location Area Code (LAC) included in LAI consists of two bytes and is encoded in hexadecimal. The available range is 0x0001-0xFFFE, and the code group 0x0000 and 0xFFFF cannot be used.

5.2.1.13. Cell ID

Cell Tower ID (Cell ID), which value ranges from 0x000000 to 0xFFFFFF.

5.2.1.14. Information Serial Number

For details see Data Packet Format section 4.5.

5.2.1.15. Error Check

For details see Data Packet Format section 4.6.

5.2.1.16. Stop Bit

For details see Data Packet Format section 4.7.

5.2.2. Examples of Packet Sent from Terminal to Server

Example of sending by the terminal

78 78 1F 12 0B 08 1D 11 2E 10 CC 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

Explain

0x78 0x78	0x1F	0x12	0x0B 0x08 0x1D 0x11 0x2E 0x10	0xCC	0x02 0x7A 0xC7 0xEB
Start Bit	Packet Length	Protocol No.	Date Time	Quantity of GPS information satellites	Latitude

0x0C 0x46 0x58 0x49	0x00	0x14 0x8F	0x01 0xCC	0x00	0x28 0x7D	0x00 0x1F 0xB8	0x00 0x03
Longitude	Speed	Course Status	MCC	MNC	LAC	Cell ID	Serial No.

0x80 0x81	0x0D 0x0A
Error Check	Stop Bit

CONFIDENTIAL

5.2.3. Location packet sent by terminal（V3 Protocol,use the ID: 0X22）:

		Length	Description
Start Bit		2	0x78 0x78
Packet Length		1	Length = Protocol Number + Information Content + Information Serial Number + Error Check
Protocol Number		1	0x12 (UTC)
Information Content	Date Time	6	Year（1byte）Month（1byte）Day（1byte）Hour（1byte）Min （1byte）Second（1byte） （converted to decimal）(Date Time)
	Quantity of GPS satellites	1	The first character is GPS information length. The second character is positioning satellite number（converted to a decimal）
	Latitude	4	Convert to a decimal and divide 1800000
	Longitude	4	Convert to a decimal and divide 1800000
	Speed	1	Convert to a decimal
	Course, Status	2	Convert to binary number of 16 bits and calculate by bits (see the following diagram)
	MCC	2	Mobile Country Code(MCC) (converted to a decimal)
	MNC	1	Mobile Network Code(MNC)(converted to a decimal)
	LAC	2	Location Area Code (LAC) (converted to a decimal)
	Cell ID	3	Cell Tower ID(Cell ID)(converted to a decimal)
	ACC	1	ACC Status ACC low: 00, ACC high: 01（not available for 06 ）
	Data Upload Mode	1	GPS data upload mode（06 series are excluded） 0x00 Upload by time interval 0x01 Upload by distance interval 0x02 Inflection point upload 0x03 ACC status upload 0x04 Re-upload the last GPS point when back to static. 0x05 Upload the last effective point when network recovers.
	GPS Real-Time Re-upload	1	0x00 Realtime upload 0x01 Re-upload（06 series are excluded）
	Mileage	4	The unit defaults to km.
Serial Number		2	Serial number of data sent later at each time will be automatically added '1'
Error Check		2	Error check (From "Packet Length " to"Information Serial Number ") are values of CRC-ITU. CRC error occur when the received information is calculated, the receiver will ignore and discard the data packet.
Stop Bit		2	Fixed value:0x0D 0x0A

Example：78 78 12 22 0F 0C 1D 02 33 05 C9 02 7A C8 18 0C 46 58 60 00 14 00 01 CC 00 28 7D 00 1F 71 00 00 01 00 08 20 86 0D 0A

CONFIDENTIAL

5.2.3.1. Course & Status

Two bytes are consumed, defining the running direction of GPS. The value ranges from 0° to 360° measured clockwise from north of 0°.

BYTE_1	Bit7	0
	Bit6	0
	Bit5	GPS real-time/differential positioning
	Bit4	GPS having been positioning 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	

For example: the value is 0x15 0x4C, the corresponding binary is 00010101 01001100:

BYTE_1 Bit7 0
BYTE_1 Bit6 0
BYTE_1 Bit5 0 (real time GPS)
BYTE_1 Bit4 1 (GPS has been positioned)
BYTE_1 Bit3 0 (East Longitude)
BYTE_1 Bit2 1 (North Latitude)
BYTE_1 Bit1 0
BYTE_1 Bit0 1
BYTE_2 Bit7 0
BYTE_2 Bit6 1
BYTE_2 Bit5 0
BYTE_2 Bit4 0
BYTE_2 Bit3 1
BYTE_2 Bit2 1
BYTE_2 Bit1 0
BYTE_2 Bit0 0

→ Course 332° (0101001100 in Binary, or 332 in decimal)

which means GPS tracking is on, real time GPS, location at north latitude, east longitude and the course is 332°.

5.2.3.2 Server location packet response

Location packet server no response

CONFIDENTIAL

5.3. Alarm Packet (GPS, LBS, combined status information packet)

5.3.1. Terminal Sending Alarm Data Packet to Server

Format			Length (Byte)
Information Content	Start Bit		2
	Packet Length		1
	Protocol Number		1
	Date Time		6
	GPS Information	Quantity of GPS information satellites	1
		Latitude	4
		Longitude	4
		Speed	1
		Course, Status	2
	LBS Information	LBS Length	1
		MCC	2
		MNC	1
		LAC	2
		Cell ID	3
	status Information	Terminal Information Content	1
		Voltage Level	1
		GSM Signal Strength	1
		Alarm/Language	2
	Serial Number		2
	Error Check		2
	Stop Bit		2

Alarm packet is consisted by adding status information to location packet, so does the encoding format of the protocol.

5.3.1.1. Start Bit

For details see Data Packet Format section 4.1.

5.3.1.2. Packet Length

For details see Data Packet Format section 4.2.

5.3.1.3. Protocol Number

For details see Data Packet Format section 4.3.

5.3.1.4. Date Time

For details see Location Data Packet Format section 5.2.1.4.

5.3.1.5. Length of GPS information, quantity of positioning satellites

For details see Location Data Packet Format section 5.2.1.5.

5.3.1.6. Latitude

For details see Location Data Packet Format section 5.2.1.6.

5.3.1.7. Longitude

For details see Location Data Packet Format section 5.2.1.7.

5.3.1.8. Speed

For details see Location Data Packet Format section 5.2.1.8.

CONFIDENTIAL

5.3.1.9. Status and Course

For details see Location Data Packet Format section 5.2.1.9.

5.3.1.10. MCC

For details see Location Data Packet Format section 5.2.1.10.

5.3.1.11. MNC

For details see Location Data Packet Format section 5.2.1.11.

5.3.1.12. LAC

For details see Location Data Packet Format section 5.2.1.12.

5.3.1.13. Cell ID

For details see Location Data Packet Format section 5.2.1.13.

5.3.1.14. Terminal Information

One byte is consumed, defining various status information of the mobile phone.

Bit		Code Meaning
BYTE	Bit7	1: oil and electricity disconnected
		0: gas oil and electricity connected
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~ Bit5	100: SOS
		011: Low Battery Alarm
		010: Power Cut Alarm
		001: Shock Alarm
		000: Normal
	Bit2	1: Charge On
		0: Charge Off
	Bit1	1: ACC high
		0: ACC Low
	Bit0	1: Activated
		0: Deactivated

Example: 0x44, corresponding binary value is 01000100,indicates that the status of the terminal is: oil and electricity connected, GPS tracking is on normal without any alarm, charge on, ACC is low, and deactivated.

5.3.1.15. Voltage Level

The arrange is 0~6 defining the voltage is from low to high.

0: No Power (shutdown)

1: Extremely Low Battery (not enough for calling or sending text messages, etc.)

2: Very Low Battery (Low Battery Alarm)

3: Low Battery (can be used normally)

4: Medium

5: High

6: Very High

Example: 0x02 indicates very low battery and a Low Battery Alarm is sending.

5.3.1.16. GSM Signal Strength Levels

0x00: no signal;

0x01: extremely weak signal;

0x02: very weak signal;

0x03: good signal;

0x04: strong signal.

Example: 0x03 indicates the GSM signal is good.

5.3.1.17. Alarm/Language

0x00 (former bit) 0x01 (latter bit)

former bit: terminal alarm status (suitable for alarm packet and electronic fence project) latter bit: the current language used in the terminal

former bit	0x00: normal
	0x01: SOS
	0x02: Power Cut Alarm
	0x03: Shock Alarm
	0x04: Fence In Alarm
	0x05: Fence Out Alarm
	0x06:Overspeed Alarm
	0x09:Out of the fence alarm
	0x0E:External voltage-low voltage alarm
	0x13:Remove alarm
	0x14:car door alarm
	0x19:Battery low voltage alarm
	0xF0:Urgent acceleration alarm
	0xF1:Rapid deceleration alarm
	0xFE:ACC on alarm
	0xFF:ACC off alarm
latter bit	0x01: Chinese
	0x02: English

Examples:

No Alarm and Language is Chinese: 0x00 0x01

No Alarm and Language is English: 0x00 0x02

To increase the reliability of alarm information, labeling the alarm information repeatedly; in most cases, the alarm information keeps consistent with information of former terminal, while the inconsistencies are as follows:

A. Low Battery Alarm occurred in the information of the terminal

B. Fence in and out Alarm in the Alarm/Language information

5.3.1.18. Information Serial Number

For details see Data Packet Format section 4.5.

5.3.1.19. Error Check

For details see Data Packet Format section 4.6.

5.3.1.20. Stop Bit

For details see Data Packet Format section 4.7.

5.3.2. Examples

Examples of terminal transmission

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

Explain

0x78 0x78	0x25	0x16	0x0B 0x0B 0x0F 0x0E 0x24 x01D	0xCF	0x02 0x7A 0xC8 0x87
Start Bit	Length	Protocol No.	Date Time	Quantity of GPS information satellites	Latitude

0x0C 0x46 0x57 0xE6	0x00	0x14 0x02	0x09	0x01 0xCC	0x00	0x28 0x7D	0x00 0x1F 0x72
Longitude	Speed	Course Status	LBS Length	MCC	MNC	LAC	Cell ID

0x65	0x06	0x04	0x01 0x01	0x00 0x36	0x56 0xA4	0x0D 0x0A
Terminal Information Content	Voltage Level	GSM Signal Strength	Alarm/Language	Serial No.	Error Check	Stop Bit

Note: The status information in the data packet is the status corresponding to the time bit recorded in the data packet.

5.4. Heartbeat Packet (status information packet)

Heartbeat packet is a data packet to maintain the connection between the terminal and the server.

5.4.1. Terminal Sending Heartbeat Packet to Server

Format			Length (Byte)
Information Content	Start Bit		2
	Packet Length		1
	Protocol Number		1
	Status Information	Terminal Information Content	1
		Voltage Level	1
		GSM Signal Strength	1
		Alarm/Language	2
	Serial Number		2
	Error Check		2
	Stop Bit		2

5.4.1.1. Start Bit

For details see Data Packet Format section 4.1.

5.4.1.2. Packet Length

For details see Data Packet Format section 4.2.

CONFIDENTIAL

5.4.1.3. Protocol Number

For details see Data Packet Format section 4.3.

5.4.1.4. Terminal Information

One byte is consumed defining for various status information of the mobile phone.

Bit		Code Meaning
BYTE	Bit7	1: oil and electricity disconnected
		0: gas oil and electricity
	Bit6	1: GPS tracking is on
		0: GPS tracking is off
	Bit3~ Bit5	100: SOS
		011: Low Battery Alarm
		010: Power Cut Alarm
		001: Shock Alarm
		000: Normal
	Bit2	1: Charge On
		0: Charge Off
	Bit1	1: ACC high
		0: ACC Low
	Bit0	1: Activated
		0: Deactivated

Example: 0x44, corresponding binary value is 01000100,

indicates that the status of the terminal is: oil and electricity connected, GPS tracking is on,normal without any alarm, charge on, ACC is low, and deactivated.

5.4.1.5. Voltage Level

The arrange is 0~6 defining the voltage is from low to high.

0: No Power (shutdown)

1: Extremely Low Battery (not enough for calling or sending text messages, etc.) 2: Very Low Battery (Low Battery Alarm)

3: Low Battery (can be used normally)

4: Medium

5: High

6: Very High

Example: 0x02 indicates very low battery and a Low Battery Alarm is sending.

5.4.1.6. GSM Signal Strength Levels

0x00: no signal;

0x01: extremely weak signal;

0x02: very weak signal;

0x03: good signal;

0x04: strong signal.

Example: 0x03 indicates the GSM signal is good.

CONFIDENTIAL

5.4.1.7. Alarm/Language

0x00 (former bit) 0x01 (latter bit)

former bit: terminal alarm status (suitable for alarm packet and electronic fence project).

latter bit: the current language of the terminal

former bit	0x00: normal
	0x01: SOS
	0x02: Power Cut Alarm
	0x03: Shock Alarm
	0x04: Fence In Alarm
	0x05: Fence Out Alarm
	0x06:Overspeed Alarm
	0x09:Out of the fence alarm
	0x0E:External voltage-low voltage alarm
	0x13:Remove alarm
	0x14:car door alarm
	0x19:Battery low voltage alarm
	0xF0:Urgent acceleration alarm
	0xF1:Rapid deceleration alarm
	0xFE:ACC on alarm
	0xFF:ACC off alarm
latter bit	0x01: Chinese
	0x02: English

Examples:

No Alarm and Language is Chinese: 0x00 0x01

No Alarm and Language is English: 0x00 0x02

5.4.1.8. Information Serial Number

For details see Data Packet Format section 4.5.

5.4.1.9. Error Check

For details see Data Packet Format section 4.6.

5.4.1.10. Stop Bit

For details see Data Packet Format section 4.7.

CONFIDENTIAL

Protocol **5.4.2. Server Responds the Data Packet**

	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 response packet from the server to the terminal: the protocol number in the response packet is identical to the protocol number in the data packet sent by the terminal.

5.4.2.1. Start Bit

For details see Data Packet Format section 4.1.

5.4.2.2. Packet Length

For details see Data Packet Format section 4.2.

5.4.2.3. Protocol Number

For details see Data Packet Format section 4.3.

5.4.2.4. Information Serial Number

For details see Data Packet Format section 4.5.

5.4.2.5. Error Check

For details see Data Packet Format section 4.6.

5.4.2.6. Stop Bit

For details see Data Packet Format section 4.7.

CONFIDENTIAL

5.4.3. Examples

Example of data packet sent by the terminal

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

Explain

0x78 0x78	0x0A	0x13	0x4B 0x04 0x03	0x00 0x01	0x00 0x11	0x06 0x1F	0x0D 0x0A
Start Bit	Length	Protocol No.	Information Content	Reserved bit (Language)	Serial No.	Error Check	Stop Bit

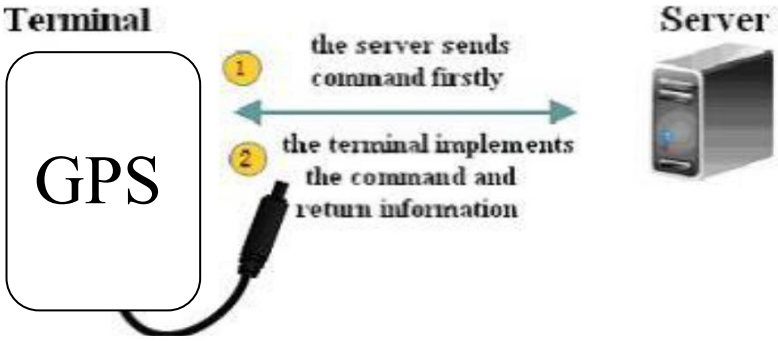
Example of response packet returned by the server

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

Explain

0x78 0x78	0x05	0x13	0x00 0x11	0xF9 0x70	0x0D 0x0A
Start Bit	Length	Protocol No.	Serial No.	Error Check	Stop Bit

vi. Data Packet Sent From Server to Terminal



6.1. Packet Sent by Server

Format		Length (Byte)
Start Bit		2
Packet length		1
Protocol Number		1
Information Content	Length of Command	1
	Server Flag Bit	4
	Command Content	M
Information Serial Number		2
Error Check		2
Stop Bit		2

6.1.1. Start Bit

For details see Data Packet Format section 4.1.

6.1.2. Packet Length

For details see Data Packet Format section 4.2.

6.1.3. Protocol Number

The Protocol Number of terminal transmission is 0x80.

6.1.4. Length of Command

Server Flag Bit + Length of Command Content

Example: measured in bytes, 0x0A means the content of command occupied ten bytes.

6.1.5. Server Flag Bit

It is reserved to the identification of the server. The binary data received by the terminal is returned without change.

6.1.6. Command Content

It is represented in ASC II of string, and the command content is compatible with text message command.

6.1.7. Information Serial Number

For details see Data Packet Format section 4.5.

6.1.8. Error Check

For details see Data Packet Format section 4.6.

6.1.9. Stop Bit

For details see Data Packet Format section 4.7.

CONFIDENTIAL

6.2. Packet Replied by Terminal

Format		Length (Byte)
Start Bit		2
Packet Length		1
Protocol Number		1
Information Content	Length of Command	1
	Server Flag Bit	4
	Command Content	M
	Language	2
Information Serial Number		2
Error Check		2
Stop Bit		2

6.2.1. Start Bit

For details see Data Packet Format section 4.1.

6.2.2. Packet Length

For details see Data Packet Format section 4.2.

6.2.3. Protocol Number

The terminal responds to the command sent by the server. The format of data packet is consistent with "the command sent by the server to the terminal", but the Protocol Number herein is different and is 0x15.

6.2.4. Length of Command

Server Flag Bit + Length of Command Content

Example: measured in bytes, 0x0A means the content of command occupied ten bytes.

6.2.5. Server Flag Bit

It is reserved to the identification of the server. The binary data received by the terminal is returned without change.

6.2.6. Command Content

It is represented in ASC II of string, and the command content is compatible with text message command.

6.2.7. Language

A bit indicates the current language used in the terminal.

Chinese: 0x00 0x01

English: 0x00 0x02

6.2.8. Information Serial Number

For details see Data Packet Format section 4.5.

6.2.9. Error Check

For details see Data Packet Format section 4.6.

6.2.10. Stop Bit

For details see Data Packet Format section 4.7.

CONFIDENTIAL

vii. Appendix : a fragment of example of data packet of communication protocol

The following data displayed in hexadecimal are intercepted from the communication between a terminal and a server, wherein "transmission" means sending by the terminal and "reception" means returned from the server:

Login packet:

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

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

GPS data packet (06 means adopting combined information package of GPS and LBS):

transmission: 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:

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

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

disconnect oil and electricity online:

reception: 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

transmission: 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 the server sending DYD,000000#

reply: DYD=Success!

Command sent during disconnection of oil and electricity:

reception: 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

transmission: 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
the server sending DYD,000000#

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

Connect oil and electricity online:

reception: 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

transmission: 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 sending: HFYD,000000#

reply: HFYD=Success!

Command sent during connection of oil and electricity:

reception: 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

transmission: 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 sending: HFYD,000000#

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

CONFIDENTIAL

Protocol **Querying address information online:**

reception: 78 78 16 80 10 00 01 A9 67 44 57 58 58 2C 30 30 30 30 30 30 23 00 A0 06 2D 0D 0A
transmission: 78 78 64 15 5C 00 01 A9 67 44 57 58 58 3D 4C 61 74 3A 4E 32 33 2E 31 31 31 36 38 32 2C 4C 6F 6E 3A 45 31 31 34 2E 34 30 39 32 31 37 2C 43 6F 75 72 73 65 3A 30 2E 30 30 2C 53 70 65 65 64 3A 30 2E 33 35 31 38 2C 44 61 74 65 54 69 6D 65 3A 31 31 2D 31 31 2D 31 35 20 20 31 31 3A 35 33
3A 34 33 00 02 00 23 07 AE 0D 0A
content sent by the terminal:
DWXX=Lat:N23.111682,Lon:E114.409217,Course:0.00,Speed:0.3518,DateTime:11-11-15 11:53:43

The GT06 protocol setting：

reception: 78 78 18 80 12 00 00 00 01 53 5A 43 53 23 47 54 30 36 53 45 4C 3D 31 00 1F 0D E6 0D 0A
transmission: 78 78 21 15 19 00 00 00 01 53 45 54 4F 4B 3A 20 47 54 30 36 53 45 4C 3D 31 2C 53 5A 43 53 00 01 00 44 FD D8 0D 0A
the server sending SZCX#GT06SEL=1
reply: SETOK:GT06SEL=1

【Location data report (V3)】：
transmission: 78 78 26 22 17 08 1D 03 24 18 C6 02 6C C7 F8 0C 36 7D 70 00 14 90 01 CC 00 25 EF 00 E8 8D 00 00 01 00 00 00 00 00 B9 63 A2 0D 0A

The GT06 protocol query：
reception: 78 78 16 80 10 00 00 00 01 43 58 43 53 23 47 54 30 36 53 45 4C 00 20 62 31 0D 0A
transmission: 78 78 22 15 1A 00 00 00 01 52 45 41 44 4F 4B 3A 20 47 54 30 36 53 45 4C 3D 31 2C 43 58 43 53 00 01 00 1F 02 85 0D 0A
the server sending :CXCS#GT06SEL
reply: READOK: GT06SEL=1

ICCID upload server settings：
reception: 78 78 1A 80 14 00 00 00 01 53 5A 43 53 23 47 54 30 36 49 43 43 49 44 3D 31 00 23 73 B7 0D 0A
transmission: 78 78 23 15 1B 00 00 00 01 53 45 54 4F 4B 3A 20 47 54 30 36 49 43 43 49 44 3D 31 2C 53 5A 43 53 00 01 00 09 50 EA 0D 0A
the server sending :SZCS#GT06ICCID=1
reply: READOK: SETOK: GT06ICCID=1

【ICCID data reporting (using 79 79 reporting)】：
transmission: 79 79 00 20 94 0A 01 23 45 67 89 06 66 68 04 60 08 54 52 70 84 10 89 86 04 D4 22 22 80 22 84 10 00 0C 90 73 0D 0A
reception: 79 79 00 06 94 0A 00 0C E9 22 0D 0A

CONFIDENTIAL

Status query of the ICCID number upload server：

reception: 78 78 18 80 12 00 00 00 01 43 58 43 53 23 47 54 30 36 49 43 43 49 44 00 21 5B 93 0D 0A

transmission: 78 78 24 15 1C 00 00 00 01 52 45 41 44 4F 4B 3A 20 47 54 30 36 49 43 43 49 44 3D 30 2C 43 58 43 53 00 01 00 2C 03 08 0D 0A

the server sending: CXCS#GT06ICCID

reply: READOK: GT06ICCID=0

Set the external electric voltage report：

reception: 78 78 1B 80 15 00 00 00 01 53 5A 43 53 23 47 54 30 36 49 45 58 56 4F 4C 3D 32 00 25 BB 59 0D 0A

transmission: 78 78 24 15 1C 00 00 00 01 53 45 54 4F 4B 3A 20 47 54 30 36 49 45 58 56 4F 4C 3D 32 2C 53 5A 43 53 00 01 00 1C 33 6E 0D 0A

the server sending: SZCS#GT06IEXVOL=2

reply: READOK: SETOK: GT06IEXVOL=2

【Terminal uploads the external voltage data packets】：

transmission:79 79 00 08 94 00 04 C4 00 20 30 34 0D 0A

External power voltage report status bit query：

reception: 78 78 19 80 13 00 00 00 01 43 58 43 53 23 47 54 30 36 49 45 58 56 4F 4C 00 24 73 C1 0D 0A

transmission: 78 78 25 15 1D 00 00 00 01 52 45 41 44 4F 4B 3A 20 47 54 30 36 49 45 58 56 4F 4C 3D 30 2C 43 58 43 53 00 01 00 1A 4D 7E 0D 0A

the server sending CXCS#GT06IEXVOL

reply: READOK: GT06IEXVOL=0

Set the V3 protocol mileage unit：

reception: 78 78 1A 80 14 00 00 00 01 53 5A 43 53 23 47 54 30 36 4D 45 54 45 52 3D 31 00 10 9E 06 0D 0A

transmission: 78 78 23 15 1B 00 00 00 01 53 45 54 4F 4B 3A 20 47 54 30 36 4D 45 54 45 52 3D 31 2C 53 5A 43 53 00 01 00 34 A5 9A 0D 0A

the server sending: SZCS#GT06METER=1

reply: READOK: SETOK: GT06METER=1

Query the V3 protocol mileage unit：

reception: 78 78 18 80 12 00 00 00 01 43 58 43 53 23 47 54 30 36 4D 45 54 45 52 00 0F A4 87 0D 0A

transmission: 78 78 24 15 1C 00 00 00 01 52 45 41 44 4F 4B 3A 20 47 54 30 36 4D 45 54 45 52 3D 31 2C 43 58 43 53 00 01 00 32 C9 C6 0D 0A

the server sending: CXCS#GT06METER

reply: READOK: GT06METER=1

CONFIDENTIAL