

Version: V01

Level: Secret

Shanghai WanWayTech Co., Ltd

GPS

Communication protocol

Important Revision History

2016/03/26 ----- Increase the number of base stations Packet Protocol (0x24)

2016/04/12 ----- Pseudo base stations alarm, tamper alarm .

2017/07/01 ----- Supplement off petrol and electricity description

2018/06/20 ----- Supplement large file transfer protocol (0x8D), recording an increase start uploading instructions

2018/07/09 ----- Modify parameters to start recording upload instructions

Table of Contents

A. Communication protocol.....	3
Two terms, definitions	3
III. Basic rules	4
IV. Packet Format	7
4.1. Start bit.....	7
4.2. Packet length.....	7
4.3. Protocol No.	7
4.4. Information content	7
4.5. Information Serial Number.....	7
4.6 Error checking.....	7
4.7. Stop Bits.....	8
V. Detailed terminal transmits a packet to the server	9
5.1. Login information packet	9
5.2. Positioning packet (GPS, LBS merger packet)	12
5.3 Alarm package (GPS, LBS, combined status information packet).....	15
5.4. Heartbeat packet (status information packet)	21
5.5 Positioning packet (LBS ONLY)	25
5.6. General information transmission packet.....	28
5.7 Large File Transfer.....	29
VI. The server sends the data packet to the terminal.....	32
6.1. The server sends.....	32
6.2. The terminal returns	33
6.3. Off petrol and electricity.....	33
6.4. Restore oil and electricity.....	34
6.5. Adding SOS numbers.....	35
6.6. Delete SOS numbers	35
6.7. Set the center number	35
6.8. Delete center number.....	35
6.9. Vibrate alert.....	36
6.10 Close vibration alarm.....	36
6.11. Turn speed alarm	36
6.12 Close speed alarm	36
6.13. Turn off alarm	37
6.14. Close power alarm	37
6.15. Displacement open alarm	37
6.16. Close alarm displacement	38
6.17. Turn on low battery alarm.....	38

6.18 Close the low battery alarm	38
6.19. Turn fence alarm.....	38
6.20. Close fence alarm.....	39
6.21. The control device reboot.....	39
6.22. Send query information in the server address.....	39
6.23. GPS, phone number lookup address information packet (0X2A)	39
6.24. Start recording made at the server	43
VII. A CRC-ITU attached table lookup algorithm C language code fragment	45
VIII. Annex B exemplary protocol packet fragments.....	47
IX. C attached complete packet format.....	49

Data flow

(including the "Packet Length", "serial number information") is.

If the recipient received information to calculate the CRC error is ignored, discard the packet.

4.7. Stop bits

Fixed value, unified hexadecimal 0x0D 0x0A.

	12		
	11		
	10		
	9		
	8		
	7		
	6		
	5		
	4		
Nibble bit4-bit0	3	What time zone	
	2	No definitions	
	1	Language selection bit	1
	0	Language selection bit	0

Bit3 0 ----- Eastern time zone

1 ----- West time zone

When: Extended position: 0X32 0X00 represent the East eight districts, GMT + 8: 00.

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

Extended bit: 0X4D 0XD8 represent 12 districts west and 3/4 time zone, GMT-12: 45.

Calculated: $12.45 * 100 = 1246$ hexadecimal turn, 0X04,0XDD.

An algorithm is here that the calculated value of the cycle time zone and then left split four time zones east, west, language selection position, in order to save four bytes.

5.1.1.7. Information Serial Number

See packet format 4.5

5.1.1.8. Error checking

See packet format 4.6

5.1.1.9. Stop bits

See Packet Format 4.7

5.1.2. The server response data packet

Explanation		length
Login informatio n packet (18 Byte)	Start bit	2
	Packet length	1
	Agreement No.	1

	Bit3 ~ Bit5	100: SOS distress (not supported)
		011: low battery alarm
		010: power failure alarm
		001: vibration alarm
	Bit2	1: Received power charging
		0: No power charging
	Bit1	1: ACC high
		0: ACC low
	Bit0	1: fortification
		0: Disarm

Such as: 0x44, corresponding to binary is 01000100

It represents a status of a terminal: ON electric oil, GPS positioning has been charged power, the ACC is low, disarmed

5.5.1.10. GSM signal strength level

- 0x00: no signal;
- 0x01: very weak signal
- 0x02: the signal is weak
- 0x03: good signal
- 0x04: signal strength

Such as: 0x03 GSM signal good

5.5.1.11. Information Serial Number

Real-time GPS pass up

0x00 real-time upload

0x01 pass up

5.5.1.12. Information Serial Number

See packet format 4.5

5.5.1.13. Error checking

See packet format 4.6

5.5.1.14. Stop bits

See Packet Format 4.7

			flag for the server, the latter two for the transmission of serial number
	Information Serial Number	2	From the start, every time the transmission data sequence number automatically incremented
	Error checking	2	"Packet Length" to the "sequence number" value of CRC-ITU. If the recipient has received information calculating CRC error is ignored, the packet discard (see attached Algorithm A)
	Stop bits	2	Fixed value, unified 0x0D 0x0A

5.7.2 server response packet

format	Length (Byte)	Detailed
Start bit	2	0x79 0x79

informatio n	Packet length	2	Protocol number = length + + content sequence number error check +
	Agreement No.	1	0x8D
	Receiving state flag	1	0x00 0x01 error normal reception reception
	Information Serial Number	2	From the start, every time the transmission data sequence number automatically incremented
	Error checking	2	"Packet Length" to the "sequence number" value of CRC-ITU. If the recipient has received information calculating CRC error is ignored, the packet discard (see attached Algorithm A)
	Stop bits	2	Fixed value, unified 0x0D 0x0A

6.16. Close displacement alarm

Functional Description: Close displacement alarm

Examples in the send and return string conversion ASCII command generated content

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

6.17. Open low battery alarm

Functional Description: Open low battery alarm

Examples in the send and return string conversion ASCII command generated content

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

NOTE: Alarm 0: internet; 1: + internet message;

6.18. Off Low battery alarm

Functional Description: Off Low battery alarm

Examples in the send and return string conversion ASCII command generated content

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

6.19. Open fence alarm

Functional Description: Open the electronic fence

Examples in the send and return string conversion ASCII command generated content

```
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
```

NOTE: Alarm 0: internet; 1: + internet message;

X = IN / OUT; IN: nominated bar alarm, OUT: a fence alarm, empty showing entrance / exit fence will alarm; default entry / exit fence will alarm;

6.20. Close fence alarm

Functional Description: Open the electronic fence

Examples in the send and return string conversion ASCII command generated content

```
The server sends
FENCE,OFF#
```

```
Terminal returns
Successful return
OK
Failure to return
ERROR: XXX
```

6.21. Control device reboot

Functional Description: After 1 minute, the device is restarted

Examples in the send and return string conversion ASCII command generated content

```
The server sends
RESET #
```

```
Terminal returns
Successful return
The terminal will restart after 1 minute!
Failure to return
ERROR: XXX
```

6.22. Send inquiry address information in the server

Examples in the send and return string conversion ASCII command generated content

The server sends

ADDRESS, the contents of the address, phone number

Note: The contents of the address issued following Chinese UNICODE encoding.

6.23. GPS, phone number lookup address information packet (0X2A)

			telephone number	twenty one
			##	2
	Information Serial Number			2
	Check Digit			2
Stop bits			2	

English address request reply protocol number: 0X97

Instruction content: ADDRESS && && contents of the address telephone number ## (ADDRESS, &&, ## is fixed string)

Examples reply address information in English Example:

```

7878 // start bit
00D1 //Data length
Protocol No. 97 // Reply
00CA // length instruction transmits content information length i.e.
00000001 // server flag
41444452455353 // ADDRESS
2626 && // delimiter
0053004F00530028004C // English position to send UNICODE
0029003A005300680069
006D0069006E00200046
0061006900720079006C
0061006E006400200057
00650073007400200052
0064002C004800750069
006300680065006E0067
002C004800750069007A
0068006F0075002C0047
00750061006E00670064
006F006E00670028004E
00320033002E00310031
0031002C004500310031
0034002E003400310031
0029004E006500610072
00,620,079
2626 && // delimiter
313235323031333739303737343035310000000000 //telephone number
2323 // ## content information terminator
0007 //serial number
72b5 //Check Digit
0D0A // stop bits
    
```

6.24. Server start recording issued

Functional Description: Terminal receives the instruction to start recording instantly upload

Examples in the send and return string conversion ASCII command generated content

The server sends

LY, XX #

XX represents the recording time, 10-300 (in seconds), 999 represents the opening period recordings, continuous recording 0 means closed

Terminal returns

Successful return

OK

Failure to return

ERROR: XXX

七. A CRC-ITU attached table lookup algorithm C language code fragment

CRC-ITU lookup algorithms C language code fragment

```
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,
    0XBD CB, 0XAC42, 0X9ED9, 0X8F50, 0XFB EF, 0XEA66, 0XD8FD, 0XC974,
    0X4204, 0X538D, 0X6116, 0X709F, 0X0420, 0X15A9, 0X2732, 0X36BB,
    0XCE4C, 0XDFC5, 0XED5E, 0XFC D7, 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  
}
```

八. B attachment exemplary protocol data packet fragments

The following data is intercepted from the data communication between the terminal and the server, the hexadecimal display, indicating that the terminal issuing sent, receiving a returned by the server:

Log package:

Issued: 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 packets (06 packets using GPSLBS merger):

Issued: 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

Stateful packet:

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

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

Online off oil and electricity:

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

Issued: 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

Issued under DYD server, # 000000

Reply: DYD = Success!

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

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

Issued: 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

Issued under DYD server, # 000000

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

Online restore oil and electricity:

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

Issued: 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

Under the server sends: HFYD, 000000 #

Reply: HFYD = Success!

Instructions have been issued to restore oil and electricity case:

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

Issued: 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

Under the server sends: HFYD, 000000 #

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

Online inquiry location:

Receiving: 78 78 16 80 10 00 01 A9 67 44 57 58 58 2C 30 30 30 30 30 23 00 A0 06 2D 0D 0A

Issued: 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

Fat content on the terminal: DWXX = Lat: N23.111682, Lon: E114.409217, Course: 0.00, Speed: 0.3518, DateTime: 11-11-15 11:53:43

Terminal to obtain address information from the server:

九. Full packet format attached C

A. Data packets sent by the terminal to the server

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

GPS information packet (26 + N Byte)												
Start bit	Packet length	Agreement No.	information							Information Serial Number	Check Digit	Stop bits
			Date Time	GPS information				Reserve expansion bit				
				GPS information length, the number of satellite positioning participation	latitude	longitude	speed		Course, state			
2	1	1	6	1	4	4	1	2	N	2	2	2

LBS information packet (23 + N Byte)											
Start bit	Packet length	Agreement No.	information						Information Serial Number	Check Digit	Stop bits
			Date Time	LBS information				Reserve expansion bit			
				MCC	MNC	LAC	Cell ID				

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

LBS complete information packet (42 + N Byte)																										
Start bit	Packet length	Agreement No.	Date Time	information																Reserve expansion bit	Information Serial Number	Check Digit	Stop bits			
				LBS information																						
				M	M	L	M	M	N	N	N	N	N	N	N	N	N	N	N					N		
2	1	1	6	2	1	2	2	1	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)																		
Start bit	Packet length	Agreement No.	Date Time	information											Reserve expansion	Information Serial Number	Check Digit	Stop bits
				GPS information							LBS information							
				GPS information length, the number of satellite positioning participation	latitude	longitude	speed	Course, state	Reserve expansion bit	M	M	L	Cell ID					
2	1	1	6	1	4	4	1	2	M	2	1	2	3	M	2	2	2	

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

Satellite SNR information (11 + M + N Byte)					
information					

GPS locator communications protocol

Start bit	Packet length	Agreement No.	The number of satellites involved in positioning	Satellite signal to noise ratio				Reserve expansion bit	Information Serial Number	Check Digit	Stop bits
				1	2	3 n				
2	1	1	1	M				N	2	2	2

Terminal response command (15 + M + N Byte) sent by the server									
Start bit	Packet length	Agreement No.	String content				Information Serial Number	Check Digit	Stop bits
			Instruction length	Server flag	Instruction content	Reserve expansion 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	Agreement No.	Date Time	information													Reserve expansion bit	Information Serial Number	Check Digit	Stop bits		
				GPS information						LBS information					status information							
				GPS information length, the number of satellite positioning participation	latitude	longitude	Speed	Course, state	Reserve expansion bit	LBS length	MC	MN	LA	Cell ID	Reserve expansion bit	Terminal information content					Volume level	GSMSignal 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. Packet sent to the terminal server

The server receives a response (10 Byte) state of the terminal after the transmission of the packet					
Start bit	Packet length	Agreement No.	Information Serial Number	Check Digit	Stop bits
2	1	1	2	2	2

The server transmits the packet to the command terminal (15 + M + N Byte)									
Start bit	Packet length	Agreement No.	information				Information Serial Number	Check Digit	Stop bits
			Instruction length	Server flag	Instruction content	Reserve expansion bit			
2	1	1	1	4	M	N	2	2	2