XEXUN Devices and Server Data Protocol

Content

1. Protocol

1.1 Communication brief

The protocol adopts TCP communication protocol.

1.2 Data type

Data type of protocol see as below table：

Data type	Description and requirements
BYTE	Unsigned single byte integer (byte, 8 bits)
WORD	Unsigned double-byte integer (byte, 16 bits)
DWROD	Unsigned four-byte integer (double word, 32 bits)
BYTE[n]	N byte
BCD[n]	8421 code,n byte
STRING	UTF8 encoding, if it is data, leave it blank

1.3 Transmission rules

The protocol uses big-endian network byte order to transfer word and double words. The transmission convention is as follows:

One BYTE : transmitted as a byte stream;

One WORD: firstly,transmit the high eight bits, then transmit the low eight bits;

Double word (DWORD): firstly,transmit the high 24 bits, secondly, transmit the high 16 bits, then transmit the high eight bits, and finally transmit the low eight bits.

1.4 Message Composition

1.4.1 Message structure

Each message is composed of Flag bit, Message header，Message structure see as below:

Flag bit	Message header	Message body	Flag bit

1.4.2   Flag bit

Use 0xfa 0xaf to indicate that if 0xfa 0xaf or 0xfb 0xbf appears in the message header and message body, it must be escaped. The escape rule is as below:

0xfa 0xaf -> 0xfb 0xbf 0x01
0xfb 0xbf -> 0xfb 0xbf 0x02
The escaping process is as below:
Sending message: message encapsulation -> calculate and fill in ECC -> escape;
Receiving message: escape restoration -> verify ECC -> parse the message.
*ECC is located in the message header

Example:
Send a data packet whose content is 0x30 0xfa 0xaf 0x08 0xfb 0xbf 0x55, then the package is as follows: 0xfa 0xaf 0x30 0xfb 0xbf 0x01 0x08 0xfb 0xbf 0x02 0x55 0xfa 0xaf

1.4.3   Message header

Message header content is as below table:

Start byte	Word	Data type	Description and Requirements
0	Message ID	WORD	
2	Serial number	WORD	In order of sending, start from 0 and add up
4	IMEI	BCD[8]	15 digit IMEI，second-string 0
12	Message body attributes	WORD	See message body attribute structure chart
14	ECC	WORD	Verify the message content data

Message body attribute structure chart

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Keep save						Message body length									

1.4.4 ECC

ECC: Error Correction Code, Code is as below:
java Code:

```
public static int checksum(byte[] data, int len) {
```

```
        int sum = 0;
        for (int j=0; len > 1; len--) {
            sum += data[j++]&0xff;
            if ((sum & 0x80000000)>0) {
                sum = (sum & 0xffff) + (sum >> 16);
            }
        }
        if (len == 1) {
            sum += data[data.length-1]&0xff;
        }
        while ((sum >> 16)>0) {
            sum = (sum & 0xffff) + sum >> 16;
        }
        sum=(sum == 0xffff) ? sum& 0xffff : (~sum)&0xffff;
        return sum;
    }
```

C Code：

```
    unsigned short sw_tcp_checksum(unsigned char *data,int len)
    {
        unsigned long sum=0;
        for(;len>1;len-=1)
        {
            sum+=*data++;
            if(sum&0x80000000)
                sum=(sum&0xffff)+(sum>>16);   }
        if(len=1)
        {
            unsigned short i=0;
            *(unsigned char *)(&i)=*(unsigned char *)data;
            sum+=i;
        }
        while(sum>>16)
            sum=(sum&0xffff)+sum>>16;
        return (sum==0xffff)?sum:~sum;
    }
```

2. Data Format

2.1 Devices data uploading

Devices data including device version information, device position data, device alarm

trigger,

Message ID 0x00014, see details in protocol [3.0 x14 Type Data Upload].

2.2 Server response ：

Server will response after well received device data.

Device response message body see as below table:

Start byte	Word	Data type	Description and Requirements
0	Response	BYTE	1 byte any response, no requirement

Example:Response(Example 2.1.1)wifi Position data:

FA AF 00 14 00 04 86 39 21 03 34 75 38 80 00 01 FF FE 01 FA AF

2.2.1 Remote setting

Server can modify some parameters of the devices through remote settings. Refer to the document " Server command".

Message ID 0x0007, Command content refer to【4. Remote control command】

For Example: Send Setting "gps=1"

FA AF 00 07 00 01 86 39 21 03 34 75 38 80 00 06 FE 47 67 70 73 3D 31 00 FA AF

2.2.2 Devices response

Devices will response with the same packet

For Example：response after well Received command of Example 2.2.1

FA AF 00 07 00 01 86 39 21 03 34 75 38 80 00 06 FE 47 67 70 73 3D 31 00 FA AF

3. 0x14 Position type data

3.1 0x14 Position packet structure

Dimension description domain	Position packet data domain

3.1 Dimension description domain

Describes the number and size of all position packets

Start byte	Data type	Byte Length	Description	Remarks
0	U8	1	Number of position packets	Number of packet For Example : 0x03 0x00 0x5 0x00 0x07 0x00 0x16, means it have 3 position packets, and their size is 0x5，0x7，0x16
1	U16	2	Size of position packets	Size of 1st packet
3	U16	2	……	Size of 2nd packet... (Lists the size of all position packets in order)

3.2　Position packet data domain

Lists the content of all position packets in order, its description is as below:

3.2.1　Position packet structure

Start byte	Data type	Byte Length	Description	Remarks
0	U8	1	Serial Number of Position packet	1-255arbitrary value
1	U32	4	Timestamp	UNIX standard timestamp
5	U8	1	CSQ	Current LTE module CSQ signal value 0-31
6	U16	2	Battery and charging state	Bit15 means charging or not，bit0-7 means battery percentage

8	U8	1	Position data type	bit means bit0　Alarm data， bit1 Position data， bit2 N/A bit3 Fingerprint data, bit4 Version data， bit5 Devices tof parameters bit6 NFC data bit7Extended data
9	DATA	*	Data content	In data packet type bit from low to high order

3.2.2 Alarm data

Start byte	Data type	Byte Length	Description	Remarks
0	U32	4	Alarm bit	bit 0, //SOS bit 1// Dismantle alarm bit 2// N/A bit 3// N/A bit 4//charging bit 5//N/A bit 6//Turn on bit 7// State of the heart rate bit 8//PIN　Check switch bit 9//Disconnect bit 10// Connection bit 11// Gravity alarm switch bit 12// Movement bit 13// Static bit 14//　N/A bit 15//　Fall down alarm bit 16// Optical sensors switch bit 17// Not touched bit 18//　Touch bit 19// Ankle bracelet tags offline bit 20// Ankle bracelet tags over distance bit 21//　Coordinates out of bounds bit 22//　Car power down

3.2.3   Position data

Start byte	Data type	Byte length	Description	Remarks
0	U8	1	Position type	bit means 0 GPS, 1 WIFI, 2 LBS, 3 TOF, 4 N/A 5 SPEED 6 High precision GPS （Differential gps）
1	DATA	*	Position data content	In bit from low to high order

3.2.3.1   Position data- gps data

0	U8	1	Number of satellites	
1	FLOAT	4	Longitude	Positive number means E, negative number means W
5	FLOAT	4	Latitude	Positive number means N， negative number means S

3.2.3.2 Position data- wifi data

0	U8	1	WIFI numbers	Numeral indicates how many groups of wifi are behind MAC~RSSI MAX=6
1	BCD	6	MAC address	001C429D0D1D 00-1C-42-9D-0D-1D
7	U8	1	RSSI	Wifi Signal strength

3.2.3.3 Position data-- lbs data

0	U8	1	LBS numbers	Numeral indicates how many groups of wifi are behind MCC~RSSI MAX=6
1	U16	2	MCC	
3	U16	2	MNC	
5	U32	4	LAC	
9	U32	4	CID	
13	U8	1	RSSI	Signal value

3.2.3.4 Position data-TOF data

0	U8	1	TOFnumbers	Numeral indicates how many groups of wifi are behind Start time ~ update time MAX=4
1	U32	4	Binding serial number	
5	U32	4	Update time	1601082000
9	U16	2	Ranging distance (CM)	1721 17.21meters
11	U16	2	Base station battery and charging status	Bit15 means charging or not，bit0-7 means battery percentage

3.2.3.5 Position data-speed data

0	U16	2	Movement speed	Multiply kilometers per hour by 10. Range (0-9999)
2	U16	2	Movement direction	Multiply the degree by 10, take true north as 0 degree, and increase clockwise. Range (0-3599)

3.2.3.6 Position data-high precision Differential GPS data

0	U8	1	Number of satellites	
1	DOUBLE	8	longitude	Positive number means E, negative number means W, format DDDMM.MMMMMMM
9	DOUBLE	8	latitude	Positive number means N，negative number means S，format DDDMM.MMMMMMM

3.2.4   Fingerprint data

0	U32	4	Fingerprint data	

3.2.5   Version data

0	STRING	20	Version data	SHA200901|20090101 Upper version|Bottom version
20	BCD	8	IMSI	460080109106092
28	BCD	10	ICCID	8986048119207 0146092

3.2.6 Devices tof parameters

0	U8	1	Time zone	8
1	U16	2	Positioning interval	Second
3	U8	1	Packet sending interval	Minute
4	U8	1	TOF binding number	There are as many as you bind Start time~Bind ID MAX=4
5	U8	1	Starting time	183 18:30
6	U8	1	End Time	71 07:10
7	U8	1	Ranging threshold (M)	Meter
8	U32	4	Binding ID	32894477 Binding ranging ID

3.2.7 NFC data

0	U8	1	NFC Data type	Bit4 Loan Bit5 Return
1	U8	1	Number of cards	Max 6pcs
2	U8	3	Card ID	D1D241

3.2.8 Extended data

0	U32	4	Extended Data type	bit0 Temperature bit1 Human body data
1	DATA	*	Data content	In bit from low to high order

3.2.8.1 Extended data-Temperature

0	float	4	Temperature	
4	float	4	Raw temperature	
8	float	4	Temperature calibration value	

3.2.8.2 Extended data- Human body data

0	U8	1	Heart rate	
1	U8	1	Low pressure	
2	U8	1	High pressure	
3	U16	2	Step data	
5	U8	1	Blood oxygen	

3.2.9 Example

For example：Device upload three groups of wifi position data

FA AF 00 14 00 04 86 39 21 03 34 75 38 80 00 AF B7 D2 03 00 38 00 38 00 38 F9 60 8A 7B 80 1E 00 60 82 02 05 78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D3 78 44 FD B9 04 65 CF B4 FB F9 46 B0 E8 CE F6 39 09 58 03 F8 CC 00 00 00 02 35 00 00 00 40 00 FA 60 8A 7B A8 1E 00 60 82 02 05 78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D2 F6 39 09 58 03 F8 CF B4 FB F9 46 B0 E8 CE 78 44 FD B9 04 65 CD 00 00 00 02 35 00 00 00 40 00 FB 60 8A 7B D0 1E 00 60 82 02 05 78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D2 F6 39 09 58 03 F8 CF B4 FB F9 46 B0 E8 CE 78 44 FD B9 04 65 CD 00 00 00 02 35 00 00 00 40 00 FA AF

Analysis：

FA AF 00 14 00 04 86 39 21 03 34 75 38 80 00 AF B7 D2   //packet header

03   // means have 3 groups data--**Refer to 3.1**

00 38 00 38 00 38   // Means the first date size is 0x38，Second group size is 0x38，third group 0x38 --**Refer to 3.1**

F9   //   Data number --**Refer to 3.2.1**

60 8A 7B 80   // means Positioning time, unix timestamp--**Refer to 3.2.1**

1E   //Wireless module signal value (0-31)--**Refer to 3.2.1**

00 60 // Bit15 is 0 means no charging, 0x60 means 96% power--**Refer to 3.2.1**

82   // Bit1 is 1, means positioning data Position data, bit7 is 7, means extended data--**Refer to 3.2.1**

02   // bit1 is 1,means WIFI positioning --**Refer to 3.2.3**

05   //means that there are 5 groups of scanned wifi signal sources--**Refer to 3.2.3.2**

78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D3 78 44 FD B9 04 65 CF B4 FB F9 46 B0 E8 CE F6 39 09 58 03 F8 CC   //The mac address of 5 groups of wifi signal sources, and the rssi value--**Refer to 3.2.3.2**

00 00 00 02   //Bit1 is 1, means that the extended data is human body data--**Refer to 3.2.8**

35   //   Heart rate is 51--**Refer to 3.2.8.2**

00   //   Low pressure is 0--**Refer to 3.2.8**

00   // High pressure is 0--**Refer to 3.2.8**

00 40 //   Step count data is 64--**Refer to 3.2.8**

00   //   Blood oxygen value is 0--**Refer to 3.2.8**

FA 60 8A 7B A8 1E 00 60 82 02 05 78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D2 F6 39 09 58 03 F8 CF B4 FB F9 46 B0 E8 CE 78 44 FD B9 04 65 CD 00 00 00 02 35 00 00 00 40 00 //The second group of wifi data

FB 60 8A 7B D0 1E 00 60 82 02 05 78 8A 20 5D F5 23 D9 78 44 FD B9 04 43 D2 F6 39 09 58 03 F8 CF B4 FB F9 46 B0 E8 CE 78 44 FD B9 04 65 CD 00 00 00 02 35 00 00 00 40 00 //The third group of wifi data

FA AF //end of packet

4. Remote control command

Item	Command	Remarks
Shutdown	of=1	
Tracking frequency & sending time	tracking_send =60,300	60seconds tracking once，300seconds sending once
Positioning time configuration	tracking_time =[start time,end time]	T1 is the start time of positioning,T2 is the end time of positioning. For example, tracking_time=0105,1750, which means positioning starts at 1:05 and ends at 17:50
Change the IP address	ip=p.xexun.co m:38899	ip=[Domain name or ip]:[Port]
Tracking mode	gps=	0， only have wifi tracking mode 1,TOF ranging is the best , GPS priority positioning, WiFi assistance (no TOF project can also use this parameter). Performance (TOF |GPS | WiFi) 2，TOF ranging is the best, WiFi priority positioning,GPS assistance(no TOF project can also use this parameter).(TOF | WiFi | GPS) 3， TOF ranging only 4， Both TOF ranging and GPS or WiFi Positioning are needed.(TOF &(GPS | WiFi) 5，Both TOF ranging and WiFi or GPS positioning are needed. (TOF & (WiFi | GPS) 6， Only GPS tracking mode 7， GPS first, WiFi second, LBS last
Text message	mg=	mg=[Message content],"Message content" means the message you want to send.
Adjust time zone	tz=	When time zone is east 8,the command is "tz=8" When time zone is west 4,the command is "tz=-4"

4.1 Example

For example: Send setting "gps=1"
FA AF 00 07 00 01 86 39 21 03 34 75 38 80 00 06 FE 47 67 70 73 3D 31 00 FA AF