From jmmm@ee.uva.es Fri Mar 24 18:11:36 2000
From: "Jose María Muñoz" <jmmm@ee.uva.es>
Newsgroups: sci.geo.satellite-nav
Subject: RE: Garmin protocol and pseudoranges
Date: Fri, 24 Mar 2000 14:09:49 +0100
Organization: Universidad de Valladolid - Spain
Lines: 42
Message-ID: <8bfpcn$egb$1@simancas.uva.es>
References: <38D7861C.1270E689@cru.fr> <38D7A46A.6756B955@cwnet.com>
<38D89CBB.1ADC2E3B@cru.fr> <3sdhdskegmet24s0vvtct38va76l93rl7o@4ax.com>
<x7wvmvm6vr.fsf@capsicum.wsrcc.com>
NNTP-Posting-Host: gauss.ele.cie.uva.es
X-Trace: simancas.uva.es 953903319 14859 157.88.41.126 (24 Mar 2000 13:08:39
GMT)
X-Complaints-To: usenet@news.uva.es
NNTP-Posting-Date: 24 Mar 2000 13:08:39 GMT
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
Path: panoramix.fi.upm.es!ntred.ccupm.upm.es!news-
3.rediris.es!news.rediris.es!news.uva.es!not-for-mail
Xref: panoramix.fi.upm.es sci.geo.satellite-nav:82585

Wolfgang Rupprecht <wolfgang@dailyplanet.wsrcc.com>  writes:

> The commands may turn out to be strikingly similar in the data layout,
> but they are not the same.  The 25/35 uses command 0x29 len 0xE2.  The
> other garmins don't.  My suspicion is that on the other garmins its a
> combination of async commands 0x36, 0x37, 0x38.  Anyone with access to
> a real gps that outputs pseudorange might be able to spot which
> long-word in these messages corresponds to the current psuedoranges.
>
> -wolfgang
> --

My work with a Garmin GPS12. (Firmware revision: 4.53 ) confirms partially your ideas:
I think that this unit ouputs pseudoranges AND both phase and integrated phase info.
All these data are contained in asyncronous messages sent from the unit when enabled. The best way to test them is to enable all async events.

With a lot of guess, I think I have found the following data:

| Message: | Data |
|---|---|
| 0x16 | pseudorange and perhaps doppler info |
| 0x1A | elevation, phase and signal quality |
| 0x33 | Position, velocity, time |
| 0x36 | a 50Hz counter and some obscure data (for each tracked satellite) |
| 0x38 | Pseudorange, integrated phase, signal strength, Time of week, 1KHz counter and 511500Hz counter (Half of the bit rate of the C/A code ) |

There is a lot of data not yet analyzed.

Of course,  more info on this subjet is wellcome.

 Jose María.
jmmm@ee.uva.es

From jmmm@ee.uva.es Fri Mar 31 08:55:33 2000
From: "Jose María Muñoz" <jmmm@ee.uva.es>
Newsgroups: sci.geo.satellite-nav
Subject: About Garmin protocol
Date: Thu, 30 Mar 2000 14:07:33 +0200
Organization: Universidad de Valladolid - Spain
Lines: 273
Message-ID: <8bvg2h$lp2$1@simancas.uva.es>
NNTP-Posting-Host: gauss.ele.cie.uva.es
X-Trace: simancas.uva.es 954418065 22306 157.88.41.126 (30 Mar 2000 12:07:45 GMT)
X-Complaints-To: usenet@news.uva.es
NNTP-Posting-Date: 30 Mar 2000 12:07:45 GMT
X-Priority: 3
X-MSMail-Priority: Normal
X-Newsreader: Microsoft Outlook Express 5.00.2615.200
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2615.200
Path: panoramix.fi.upm.es!ntred.ccupm.upm.es!news-3.rediris.es!news.rediris.es!news.uva.es!not-for-mail
Xref: panoramix.fi.upm.es sci.geo.satellite-nav:83374

In the last few weeks, it seems that some people is interested
in the Garmin proprietary communications protocol. In particular
in the extraction of raw GPS data from "low end" handheld units.

With some work, a lot of guess and with a reduced set of data, I have
obtained this information. Some data that I have considered constant,
may not be so constant (mainly the high bytes of some counters) due
to the above said narrow time slot used.

Of course!, I am in no way related to Garmin, and all this information
is ONLY my opinion about the meaning of the stream of data.

First of all, I want to thank William Soley for the compilation of his
document about the undocumented commands.

old address:
http://playground.sun.com/pub/soley/garmin.txt

currect as of March 2015 address:
http://www.abnormal.com/~thogard/gps/bill-garmin.txt

My preliminary observations on the more or less documented features
of the Garmin protocol start in the above document and are:

Unit: GPS12. Software revision: 4.53

When the unit is connected the first time, it sends periodically
few packets, but  after sending to the unit a message type
 1C (EnableAsyncEvents) with data FF FF, it starts sending at
least the following:
(This status is not cleared by a power (off - on) cycle.)

The types with * will be analyzed in more detail

| type | Len(dec.) | comment: |
|---|---|---|
| 0x00 | 4 | ? |
| 0x01 | 4 | ? |
| 0x02 | 4 | ? |
| 0x0D | 8 | Event * |
| 0x14 | 84 | Time/Latitude/Longitude ...* |
| 0x16 | 21 | ? (one per satellite) * |
| 0x17 | 52 | Position error and more * |
| 0x1A | 96 | Satellite status * |
| 0x27 | 2 | ? |
| 0x28 | 4 | ? |
| 0x33 | 64 | Position, Velocity, Time * |
| 0x36 | 9 | ? (one per satellite) * |
| 0x37 | 33 | time and ? * |
| 0x38 | 37 | sat. info (one per sat.) * |
| 0x39 | 35 | ? |

In addition:
0x0A  2  to be sent to the unit. Request *

**********
Message 0x0D (8 bytes)

Similar to the message shown in the Soley document, except
the time information.

| bytes | type | comment |
|---|---|---|
| 1-2 | int | Event type. Not yet analyzed in detail |
| 3-4 | int | Subtype |
| 5-8 | long | GPS clock time. Increments 1000 /s |

---
Message 0x14 (84 bytes)

Seems to be a mixture of position - time information

| bytes | type | comment |
|---|---|---|
| 1-2 | int | type of fix. (2D, 3D, etc) |
| 3-4 | int | repeated the above information (always the same number) |
| 5-12 | double | Time of Week (seconds and fractions from 00:00 of Sunday) |
| 13-20 | double | repeated the above information (always the same number) |
| 21-24 | long | counter 1000/s (approx.) |
| 25-28 | long | counter 515500/s |
| 29-36 | double | latitude in radians |
| 37-44 | double | longitude in radians |
| 45-48 | float | altitude over the ellipsoid * |
| 49-52 | float | speed in the east direction |
| 53-56 | float | speed in the north direction |
| 57-60 | float? | speed up ? |

61-64 ?  ?
65-68 ----  always FF
69-76 double? ???
77-80 float? ???
81-84 float? ???

* The altitude and speeds are the same as in message 0x33 (PVT)
documented in the Garmin info.
The type of the last items are only a guess. I don't know the
contents, but the way they change suggest the types shown.

---

Message 0x16  (21 bytes)

one for each tracked satellite, sent successively

bytes type  comment
1-4 long  ? (1)
5-8 ?  ? byte 5 always 0, byte 8 near 0x3c or 0xBE
9-16 double  pseudorange
17-20 ?  ? byte 20 similar to byte 8
21 byte  satellite number minus 1

I don't know if the pseudorange is corrected for ionospheric
or other retardation in some way.

(1): The information in the 1-4 bytes varies coherently for all the
satellites (speed or Doppler? ) My observation site has a clear
sky only in the north- northwest direction. One can expect
mainly that the radial speed of all the satellites have the same sign?
More research in necessary.

---

Message 0x17 (52 bytes)

bytes type  comment
1-4 float  Estimated Horizontal Position Error
5-8 float  Estimated Vertical Position Error
9-12 float  Estimated Position Error
13-52 ?  ?

33-36 and 41-44 seems to change from a constant value to
a variable one with the first 3D fix. The information shown
was obtained comparing this message with the 0x33 (Position-
Velocity-Time) as documented in Garmin manuals.

---

Message 0x1A (96 bytes)

Array of 12 (0x0C) blocks of data
Each block has the following structure:

bytes type  comment
1 byte  satellite number minus 1
2 byte  elevation
3-4 word  phase info? (1)

5-6 int  signal quality
7 byte  tracking?
8 byte  some type of flag (2)

(1): byte 4 takes values from 0 to 7
byte 3 fluctuates apparently at random
if we take bytes 3 and 4 as a unsigned int., then
we have 11 bits of changing data. The same data length
can be found in the phase info from GPS25 boards.
And the values change almost randomly...
This is only a tentative idea...

(2): Byte 8 takes only 0-1 values (mainly 0)
byte 7: 1->?
 2-> no tracking
 4-> tracking

---

Message 0x33 (64 bytes)

PVT (position, velocity, time) data

| bytes | type | comment |
|---|---|---|
| 1-4 | float | altitude over the ellipsoid |
| 5-8 | float | Estimated Position Error |
| 9-12 | float | Estimated horizontal Position Error |
| 13-16 | float | Estimated vertical Position Error |
| 17-18 | int | type of fix (2D, 3D, diff.) |
| 19-26 | double | Time of week |
| 27-34 | double | Latitude |
| 35-42 | double | Longitude |
| 43-46 | float | East velocity |
| 47-50 | float | North velocity |
| 51-54 | float | Up velocity |
| 55-58 | float | ellipsoid height above sea level |
| 59-60 | int | dif. between GPS and UTC times |
| 61-64 | long | start of week day number |

All of these data are explained in "Garmin GPS interface
specification", taken from the Garmin website.
In the same manual, Garmin says "None of the products
in the table (including GPS12) implements PVT Data transfer" !!

---

Message 0x36  (9 bytes)

one for each tracked satellite, sent successively

| bytes | type | comment |
|---|---|---|
| 1-2 | word | counter 50/s |
| 3 | byte | always 0x81 ? |
| 4 | byte | some flags ? |
| 5-8 | ? | seems to vary randomly |
| 9 | byte | satellite number minus one |

Nothing know about bytes 5-8

---

Message 0x37 (33 bytes)

bytes type comment
1-22 ? ?
23-30 double Time Of Week
31-33 ? ?

---

Message 0x38 (37 bytes)

one for each tracked satellite, sent successively

bytes type comment
1-2 ? ?
3-4 word increases 900 - 1100/s
5-8 long? (1)
9-10 word (2)
11-14 long Number of cycles (Integrated phase) (3)
15-22 double Pseudorange
23-26 long Counter (4)
27-28 word S/N ratio or signal strength
29-36 double Time of week
37 byte satellite number minus one

(1): For the satellites with best signal, the value is almost constant. For the weak ones, fluctuates. If we consider it as a unsigned (double word), the values are close to 1.5E7 or close to 1E9. If we suppose a signed long integer, the values seem to group around +-1.5E7 or -3.4E6. On the other hand, all of this can be wrong and byte 8 (values only 00 and FF) can be a flag.

(2): Varies slowly, with some noise (greater in the weak satellites), increasing or decreasing, but most of the time, increasing. In average, 1 unit each 2 seconds.

(3): If the bytes 15-22 are actually the pseudorange, then bytes 11-14 must be the accumulated phase. If we calculate the wavelength (change in pseudorange / change in accumulated phase) we obtain 0.1903 for all the satellites. The correct value (in vacuum) is 0.1902936.. I think is enough.

(4): The same value for all the satellites in each group of messages. Counts from the start of acquisition at (511500+-3)/s Half of the bit rate of the C/A code

---

Requests sent TO the GPS12.

In addition to the (more or less) documented ones, I have found the following:

Bytes sent Action
0x0F 0x00 GPS sends 121 messages type 0x27 with 22 bytes each.
0x11 0x00 GPS sends 4? message(s) type 0x28 with 6 bytes
0x20 0x00 GPS sends a lot of messages type 0x45 with 15 bytes
0x2F 0x00 GPS sends messages type 0x55 of 91 bytes,
  type 0x1B of 2 bytes, 0x23 of 60 bytes, and then
  RESETS itself, erasing all the stored data and

starts "searching the sky".

At this point I stopped sending things to te GPS for obvious reasons.

None of these messages are analyzed, and probably their type, number and length may vary depending the amount of data stored in the GPS.

---

And, of course, some or all of this information may be totally wrong.

---

One interesting set of data not yet found is the ephemeris. Probabily the unit will send these data in response to a command, but which one?.
For the GPS25 is (according to manual) type 0x0D, len. 4, data: 0x02,0x0C,0x00,0x00
but in the GPS12 does not work. Is interesting to note that is a "event" message, not a "request" one.