Geolocation through Cell ID

2174013-1.0

Author:	Sierra Wireless	Date:	November 18, 2013

APN Content Level	BASIC		INTERMEDIATE	✓	ADVANCED		Confidentiality	Public	✓	Private	

Hardware Compatibility	Product Line	AirPrime	Series	Q26xx	SL60xx
				FXtend	WSxxx
				WMPxx	

Software Compatibility	Series	Q26xx, WMPxxx, SL60xx : FW 7.xx	

1 Version

Application Notes may be updated over their lifetime. To ensure you design with the correct version, please check the application notes page in www.sierrawireless.com for latest versions.

2 Introduction

This Application Note (APN) is provided to Sierra Wireless distributors and clients to aid using the Sierra Wireless portfolio of cellular solutions.

In some applications the ability to know the location of the unit is useful without powering up a GPS, including:

- Applications where position information is not critical but useful, e.g. alarms, meters, etc.
- Where power saving is important, including battery powered applications but knowing the approximate position
- Where position is critical and the cell ID can be used as a complementary service to GPS, like in stolen vehicle recovery applications.

This Application Note describes methods and services through which an application will be able to perform a Geolocation operation through the use of purely CellID's without the need for GPS.

3 Overview

All devices using the mobile networks are aware of their surrounding cell information which is broadcast by the networks so that the unit knows what channels to scan rather than having to permanently scan all of the radio frequencies/codes. Within this broadcast information from the networks are elements of information which can be used to locate a units geographical position.

- Mobile Country Code (MCC) – Each country has an allocated number from 3GPP (3 digits).
- Mobile Network Code (MNC) – Each network has a network code allocated (3 digits in the US, 2 digits ROW).
- Location Area Code (LAC) – Area assigned by a network, this could be the size of a small town and is the smallest area that the network is automatically aware that a unit is in.
- Base station Identity Code (BSIC) – A location area will have a number of base stations within it, the base station this can vary from a macro cell (25km radius) to a pico cell (size of a room).
- Cell ID – Lowest and smallest geographical sized element in the network.
- Timing Advance (TA) – This is a parameter that is calculated by the unit when there is an active link running (not a packet based session i.e. GPRS). It allows for precise calculation of distance to the base station within 5 meters.

4 Glossary

Initials	Definition
CPOL	Preferred Operator List
CS	Circuit Switched (GSM)
FPLMN	Fobidden Public Land Mobile Network
HPLMN	Home Public Land Mobile Network
IMEI	Individual Mobile Equipment Identity
IMSI	Individual Mobile Subscriber Identity
L3	Layer 3 – Network signalling

Initials	Definition
L3MM	L3 Mobility Management
L3RR	Layer 3 Radio resource
MCC	Mobile Country Code
ME	Mobile Equipment
MNC	Mobile Network Code
PS	Packet Switched (GPRS)
SWI	Sierra Wireless

5 Geolocation through cell ID mechanism

The process for geolocation is very simple, a general diagram is shown in Figure 1 below.

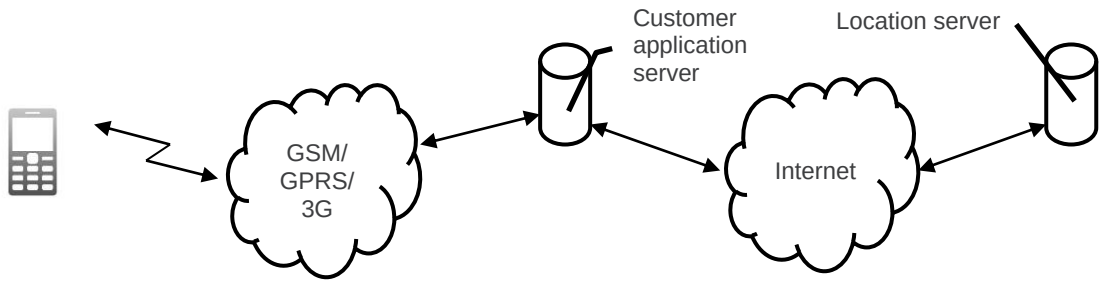

Figure 1. Geolocation General Diagram

1. Application in the field measures all surrounding cell information.
2. Information is then sent back to the application server through whatever data pipe is available i.e. private APN, public, etc.
3. Application server formats a message to a location server (third party or internal) to request an approximate position based on the supplied information which will then be responded to.

The data sets that are able to be accessed and different options that are available are discussed later in this application note.

6 SWI AT commands

The commands that can be used to obtain the information with SWI vary depending on the module and operation that is required to be carried out.

6.1 Q26 Series, SL6087, WMP Series

To get the basic cell/surrounding cell information out the CCED command should be used as shown below.

```
at+cced=0
+CSQ: 25,99
+CCED:
234,30,07d9,8236,12,624,47,,,0,,,0,234,33,0078,d43d,47,781,43,234,30,07d9,8238
,12,654,26,234,30,02dc,a6bc,59,662,16,234,30,088a,,59,682,12,234,30,02dc,,38,6
58,10,234,30,07d9,8237,12,620,20,1
OK
```

Within the CCED command there is an option to command the unit to sequentially communicate with each base station it can see resulting in the timing advance to each. This can significantly improve the accuracy of the returned position as the data base will now the exact distance to the base station.

An example of this is shown below.

```
at+cced=0,16
```

```
+CCED:
234,33,0078,d43d,47,781,,,,255,,,0,234,33,0078,d43e,41,788,28,234,33,0078,d435
,44,858,19,0,0,0
OK
```

The final option is to use the network survey option which gives all of the information for all of the surrounding cells regardless of operator. Due to the fact that the unit has to perform a full network scan of all frequencies this can take up to 2 minutes to return (depending on the number of active radio channels), in addition to this it will have an impact on current consumption as the processing required to do this will be significant.

6.2 WS

There is a single option here to see the surrounding cell information for network provider that the unit is currently camped attached to as shown below.

```
at*psengi=0 //Current serving cell information
*PSSCI: 781,37,37,0,0,45,-678495094,3339315,234,33,120,54333,1,15,6,1,1,255,47
OK
at*psengi=1 //Surrounding cell information
*PSNCI: 788,15,15,0,0,3339315,234,33,120,54334,25,41
*PSNCI: 858,13,13,0,0,3339315,234,33,120,54325,22,44
OK
```

7 Data sets

There are a number of ways to obtain the data sets of the raw cellular information as described above.

- Go to the operators who know exactly where their own base stations are and consequently can calculate with a great degree of accuracy
- Build your own database – If an application has a large enough install base then it is possible for the owner/operator to build up their own database by using the deployed vehicles to report the information discussed . This has the following advantages
  - You are not reliant on a third party.
  - Information that is being gathered is not being used to update a third parties database and hence being resold on for use by potential competitors.
- Third party service providers – This is the most commonly used method and is the only way to really provide full cross network global coverage. Pricing models vary and a user needs to contact the providers to discuss their own individual requirements. Most providers do give a free usage model, generally with up to 100 requests per day. Third part suppliers generally rely on their own users to update and maintain their database for the benefit of all of their other users. This provides them with a strong degree of global and cross network coverage assuming there is a diverse and large enough user base.

8 Service providers

There are a number of service providers which have compiled the data sets required to give positional information, they all use the same method whereby the requester uses the POST message containing the network information as discussed above (MCC, MNC, BSIC, etc.) and an API key identifying the account you have with them.

In the following sections the messaging required for two third party service providers is described.

8.1 Google

Obviously one of the best known names, they leverage all Android handsets position information to update their maps so are probably the most accurate global data set.

As with most services of this type there is free access which is limited to 100 requests per day, to use the service beyond these limits the Geolocation API must be added to any existing Google License.

Geolocation requests are all sent over HTTPS in a JSON format to the below URL:

https://www.googleapis.com/geolocation/v1/geolocate?key=*API key*

8.1.1 Request

All fields that are submitted to the server in the request are optional, however, the more information that is submitted the more accurate the returned location. Below is an example of the

```
{
  "homeMobileCountryCode": 310,
  "homeMobileNetworkCode": 410,
  "radioType": "gsm",
  "carrier": "Vodafone",
  "cellTowers": [
    // See the Cell Tower Objects section below.
  ],
  "wifiAccessPoints": [
    //Not relevant to this application note
  ]
}
```

The all of the cell tower information available needs to be included in the above request body, multiple cell information can be included.

```
{
  "cellId": 42,
  "locationAreaCode": 415,
  "mobileCountryCode": 310,
  "mobileNetworkCode": 410,
  "age": 0,       //Time since the cell was the primary of the unit
  "signalStrength": -60,
  "timingAdvance": 15
}
```

8.1.2 Response

The returned value from the Google server will return a location with a radius circle in meters around the given location.

```
{
  "location": {
    "lat": 51.0,
    "lng": -0.1
  },
  "accuracy": 1200.4
}
```

More detailed information can be found at the below link

https://developers.google.com/maps/documentation/business/geolocation/

8.2 RxNetworks

Another third party provider is Canadian based RxNetworks and operates in much the same way as Google. Again free access is limited to 100 requests per day, after this an ID is required to access the server further.

The base URL for requesting positions is given below through the GET or POST method..

http://developer.xybrid.net:9380/xybridserver/RXNXYBRID

8.2.1 Request

A request is made as before with an ID and the cellular information formatted as per below, all fields are detailed at the link at the bottom of this section.

`servCell or neighCell` `ctype:gsm;mcc:302;mnc:880;lac:11101;cid:72168745;rxlev:-79`

An example request for position would be as per the below.

```
http://developer.xybrid.net:9380/xybridserver/RXNXYBRID?clientId=XYTestKey&mId=LG-P500h-FRG83&un=90420156-025763-0&version=2&requestMask=4194304&servCell=ctype:gsm;mcc:302;mnc:880;lac:11101;cid:72171745;rxlev:-79&neighCell=ctype:gsm;mcc:302;mnc:880;lac:15032;cid:32654329;rxlev:-92,ctype:gsm;mcc:302;mnc:880;lac:65301;cid:73124658;rxlev:-104
```

8.2.2 Response

The response from the server is given in a very simple format as with Google which does not require a full XML parser with both lat/long and altitude with an accuracy measurement. An example is given below.

```
<RxnAssist>
        <RefLocation format=”XML”>
                <Lat>49.2887196</Lat&gt;
                <Lon>-123.12341719999999</Lon>
                <Alt>0.0</Alt>
                <Uncertainty>50</Uncertainty>
        </RefLocation>
</RxnAssist>
```

8.2.3 Measure Position request/response (MPR)

Just as Google will leverage its large Android user base to update and maintain their data base, other service providers such as RxNetworks need to use their own user base to do this. This is done via the Measure Position Request/Response (MPR) mechanism which forms part of the business agreement with RxNetworks.

An MPR can be received after a request for position, it is then required that the application power its GPS receiver up to obtain a known good fix, re measure the cell information and send this back to the RxNetwork server.

More detailed information on RxNetworks and how to work with their server is given at the below link.

http://www.rxnetworks.com/developers/documentation

9 Support

For direct clients: contact your Sierra Wireless FAE

For distributor clients: contact your distributor FAE

For distributors: contact your Sierra Wireless FAE

10 Document History

Revision	Date	History
1.0	November 18, 2013	Creation

11 Legal Notice