Application Note

Detecting Signals Hidden In Plain Sight

In the past, signals have been hidden by various means, including placing them next to a large signal such as an AM broadcast carrier or using spread spectrum technology to create low probability of detection (LPOD) signals. More recently the development of various digital modulation formats has provided a new means for signals to be hidden in plain sight. The presence of digitally modulated signals is commonplace now, to the point that if a signal looks familiar, such as a CDMA "Bart's head," it can easily be ignored as a known signal.

That may be a big mistake as people intent on hiding transmitters may be creating signals that look like CDMA, GSM or LTE signals but have something completely different under the hood. It is becoming necessary to confirm that a signal is actually what it appears to be. To do this requires more than measuring the shape and bandwidth of the signal, but also demodulating the signal to confirm that all the expected signaling is present on the signal. These measurements are easily done with an antenna attached to a handheld signal analyzer such as the BTS Master or Spectrum Master. That is how all the signals shown in this application note were measured.

CDMA

Signal Appearance

CDMA and EVDO signals look the same in the frequency domain – a Bart's head that is approximately 1.24 MHz wide as shown in figure 1.

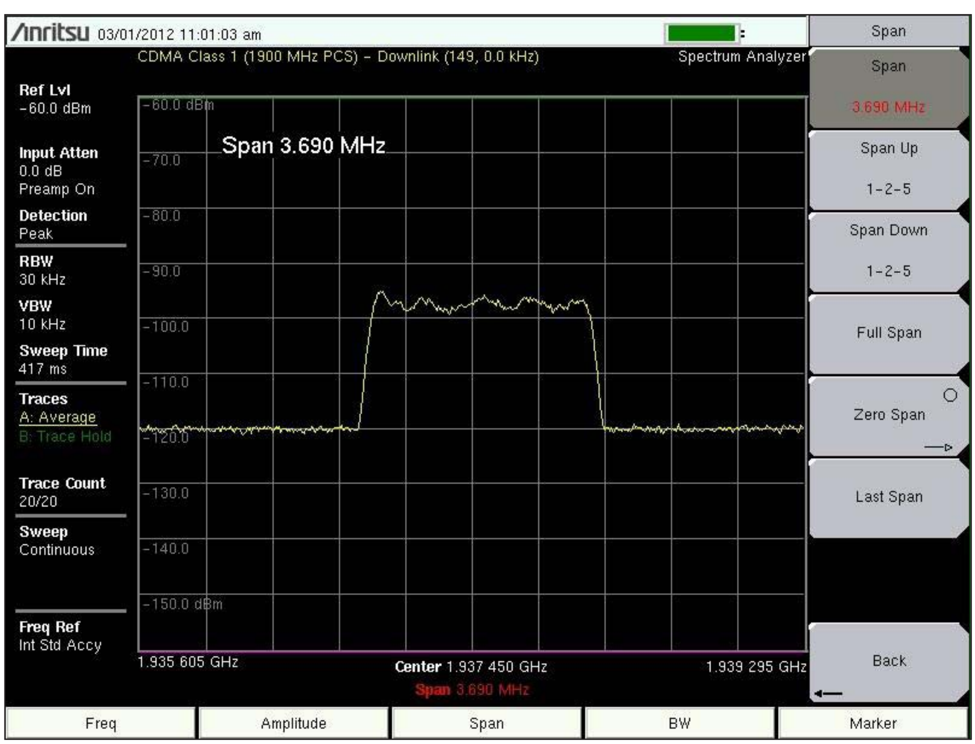

Figure 1. CDMA Bart's Head

Often there are multiple signals adjacent to each other so you may see a Bart's head that is two or three times as wide – shown in Figure 2. In this case there is an amplitude difference between the two signals so it is easy to see that there are two signals there. Often it is hard to tell that there are two separate signals. Note the amplitude dip that marks the end of one signal and the beginning of the next one.

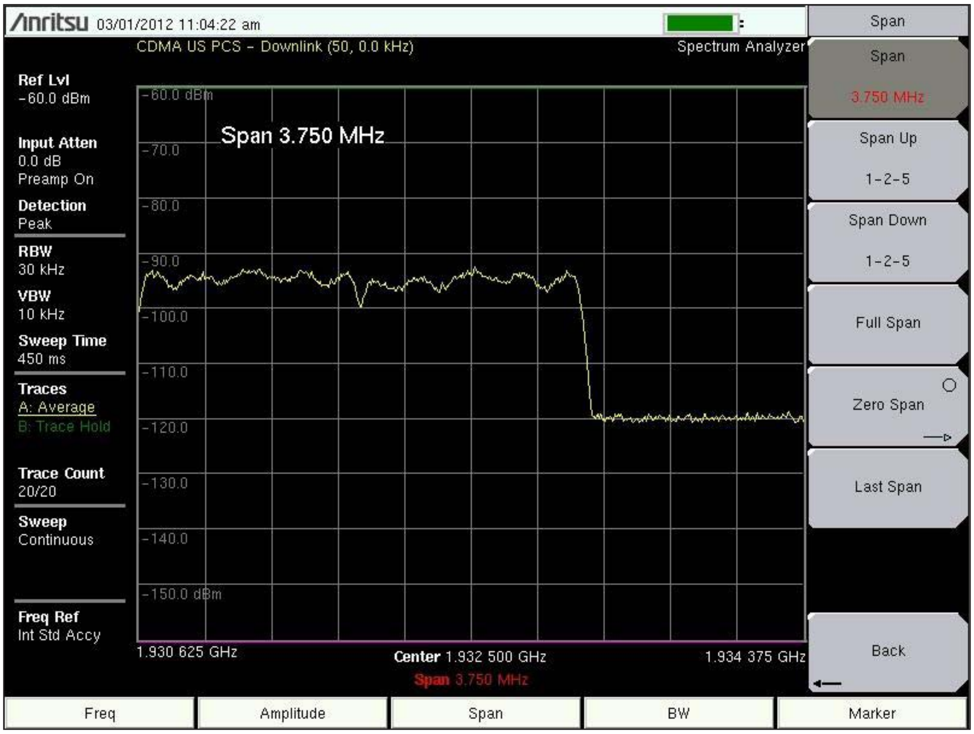

Figure 2. Two Adjacent CDMA Signals

CDMA and EVDO signals can be distinguished from each other by demodulating them. In the CDP (code domain power) display, a CDMA signal should exhibit a varying number of payload segments (shown in orange) with a steady paging signal (shown in green). You should also see pilot signals (shown in red) and sync signals (shown in blue). To be sure the instrument is on exactly the right frequency, it is wise to have the GPS option installed and running. When the instrument is synchronized with GPS the frequency accuracy improves to 25 parts per billion or better. GPS is desirable for all 3G and 4G modulation formats.

If you are looking at an EVDO signal using the CDMA measurement tools, you will see a warning message that states "Short Code not Found". If you see this message on a signal that is strong enough to measure, try measuring it using the EVDO tools. If you can't measure it there, you may have found a hidden signal. This same message is generated if there is no signal to measure.

Figure 3a. CDMA CDP on Heavily Loaded Site

Figure 3b. CDMA CDP on Lightly Loaded Site

Minimum requirements to be sure it is a legitimate CDMA signal.

Assuming that the signal can be demodulated, a CDMA signal must always have the pilot signals, shown in red on codes 0 & 64, in figures 3a and 3b, the paging channel shown in green on codes 1 and 65, and the sync channel shown in blue on channels 32 and 96. There will be a varying number of users on the signal (shown in orange) and they should change frequently as calls are terminated and new calls are started. The instrument updates the CDP display every five seconds. Be suspicious if the graph doesn't change at every update interval. The vertical segments in the chart represent the Walsh codes that are used to separate all the CDMA signals on a channel into separate conversations. The bottom half of the chart is a zoomed-in portion of the top half. The blue background shows the area that is zoomed.

If the signal can't be demodulated, it may be an EV-DO signal, the center frequency may not be set correctly or it may not be a legitimate CDMA signal. If the center frequency on the spectrum analyzer is off by more than about 1.5 kHz from the actual center frequency of the signal, a CDMA signal won't be demodulated and the instrument will display the "Short Code Not Found" message. Using the instrument's signal standard list the closest channel can be determined for a signal you are investigating. If you are using GPS, be sure it is turned on and locked.

EVDO

Signal Appearance

An EVDO signal is indistinguishable from a CDMA signal in the frequency domain; it simply looks like a 1.24 MHz wide Bart's head. If you are looking at an EVDO Bart's head using the CDMA measurement functions you will get a warning message that says "Short Code Not Found." Likewise if you are looking at a CDMA signal using the EVDO measurement functions, you will get the same warning message. The CDP MAC appearance is different than a CDMA CDP scan. There is no paging channel, and only one pilot (in red on code 4) and a varying number of data signals, shown in yellow and orange. If you look at the modulation summary, the Data Modulation may show as idle, QPSK, 8-PSK, or 16-QAM and will change frequently due to the signal quality measurement being sent to the base station from a handset. The instrument updates the CDP MAC graph every four seconds. Be suspicious if the graph doesn't change every time the graph is updated. On a real site the number of users is extremely dynamic and changes continually.

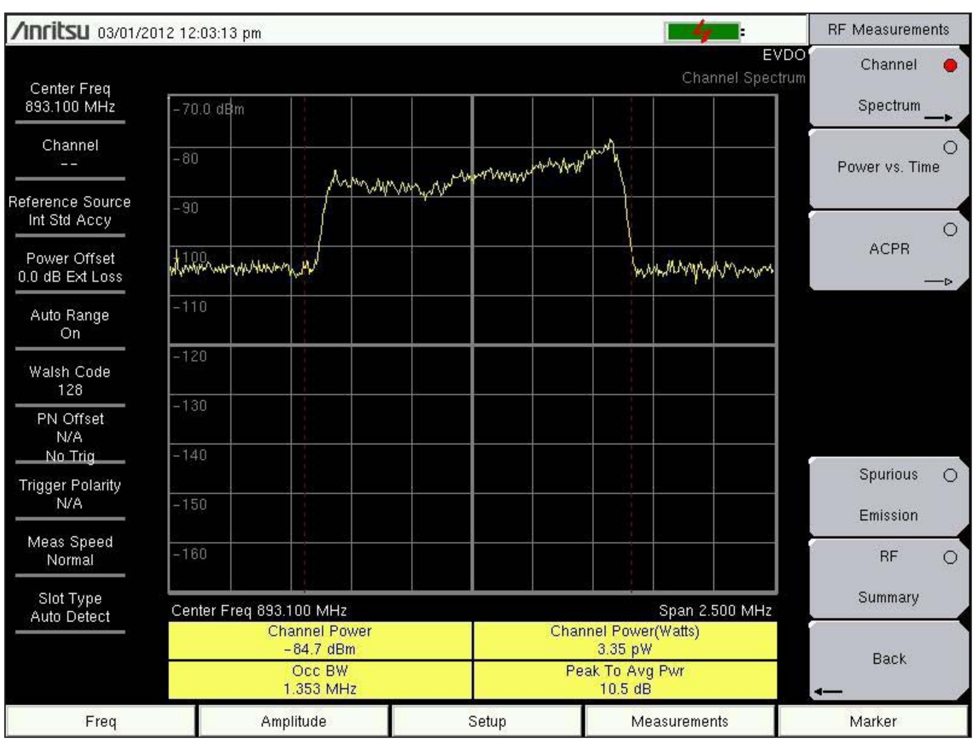

Figure 4. EVDO Signal

Minimum requirements to be sure it is a legitimate EVDO signal.

To be sure it is an EVDO signal you need to check the data modulation type, which can be QPSK, 8-PSK, or 16-QAM. There will be times when the data modulation type is shown as IDLE. Seeing the modulation type change is a good indication that you are looking at a real EVDO signal. You can see the modulation type both in the MAC graph as shown here and in the modulation summary table.

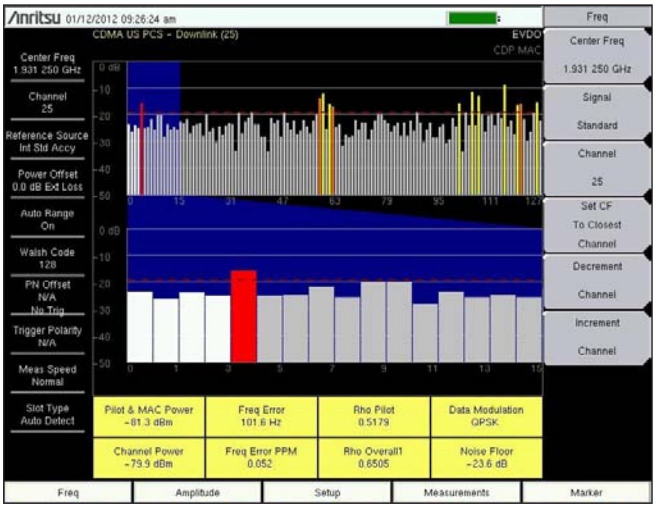

Figure 5a. EVDO MAC of a lightly loaded site

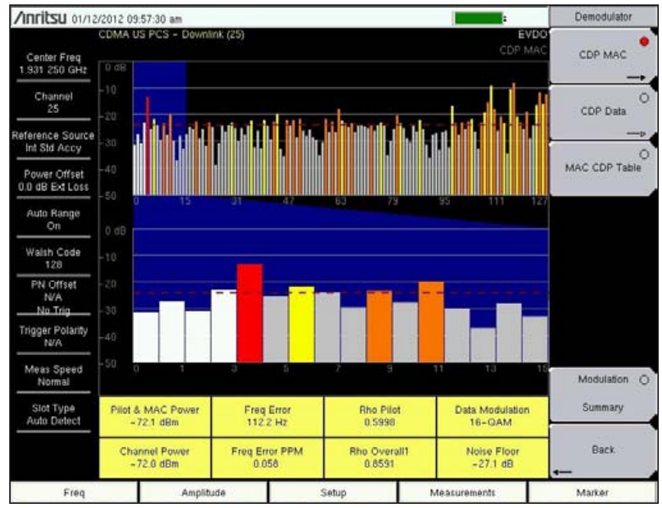

Figure 5b. EVDO MAC of a heavily loaded site

Values should be filled in for the eight parameters shown at the bottom of the EVDO MAC display. For an over-the-air signal generally the pilot and overall Rho values won't be very good – values close to 1 are better. Channel power and Pilot & MAC Power will normally be very close to each other – less than 2 dB difference while the frequency error must be less than 1.5 kHz to be able to demodulate the signal.

GSM/GPRS/EDGE

Signal Appearance

A GSM signal looks like a Gaussian curve.

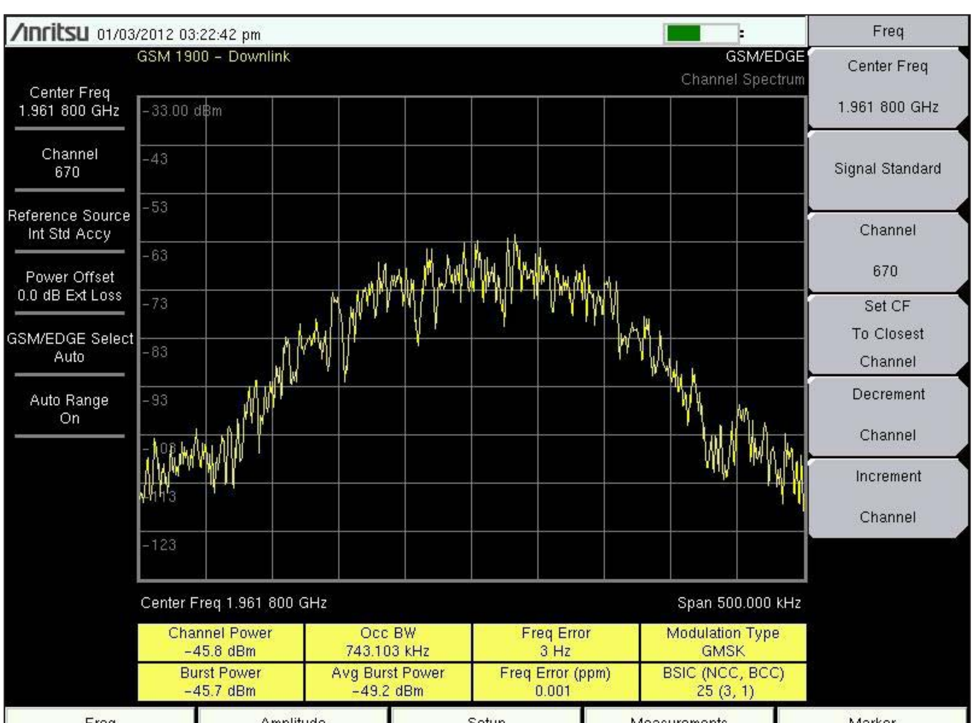

Figure 6. GSM Signal

Minimum requirements to be sure it is a legitimate GSM signal.

A GSM signal is divided into frames and slots. Each user is assigned a slot within a frame. For a signal to be a real GSM signal, you must be able to see the power drops that occur between each frame within a slot and between frames as shown in figures 7 and 8.

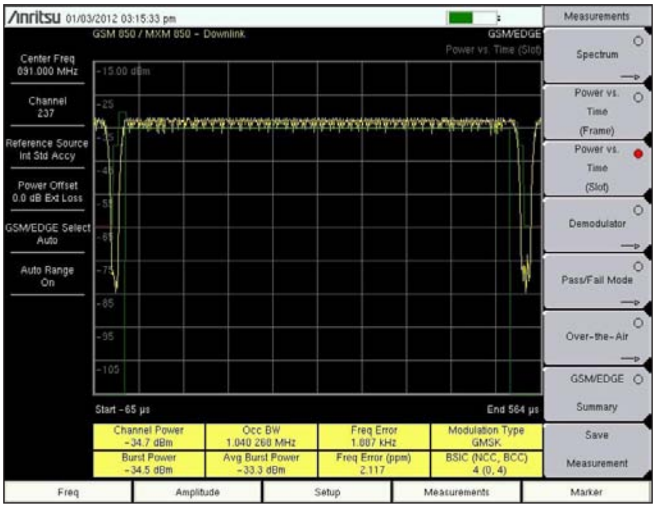

Figure 7. GSM Slot Measurement

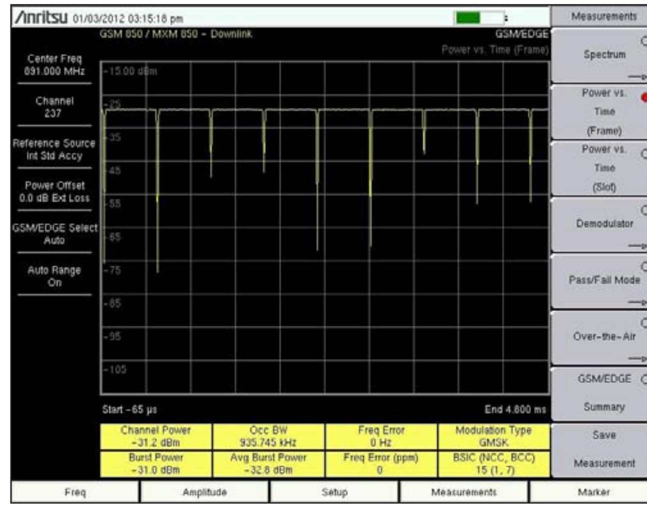

Figure 8. GSM Frame Measurement

Once you have determined that the shape of the RF signal is right and that the slots and frames occur as they should, there are a couple more things that should be present to be sure it is a real GSM signal. The BSIC (Base Station Identity Code) value in the summary table should be filled in if there is a good enough carrier to interference ratio to properly demodulate the signal. If the signal to noise ratio is >12 dB but no BSIC value is shown, that is a cause for suspicion. The BSIC consists of a 3-bit Network Color Code (NCC) and a 3-bit Base station Color Code (BCC). The NCC is assigned to each network provider so that a handset can determine which base-stations to listen to. The NCC of different providers must be different. The BCCHs (Broadcast Control Channel) of each base station is assigned by the network operator, and are assigned such that no neighbor stations have equal BCCH and thus equal BSIC. In the example below the NCC value is 1 and the BCC value is 0. The BSIC value is created by joining the 3 bits of the NCC and the 3 bits of the BCC and calculating a hexadecimal value from them.

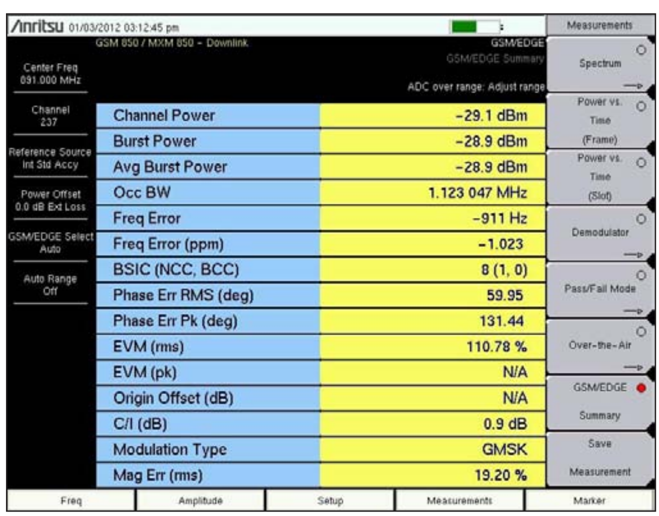

Figure 9. GSM Summary

W-CDMA/HSDPA/HSPA+

Signal Appearance

A W-CDMA/HSDPA/HSPA+ signal is a 5 MHz wide Bart's head. This modulation format is also known as UMTS (Universal Mobile Telephone System).

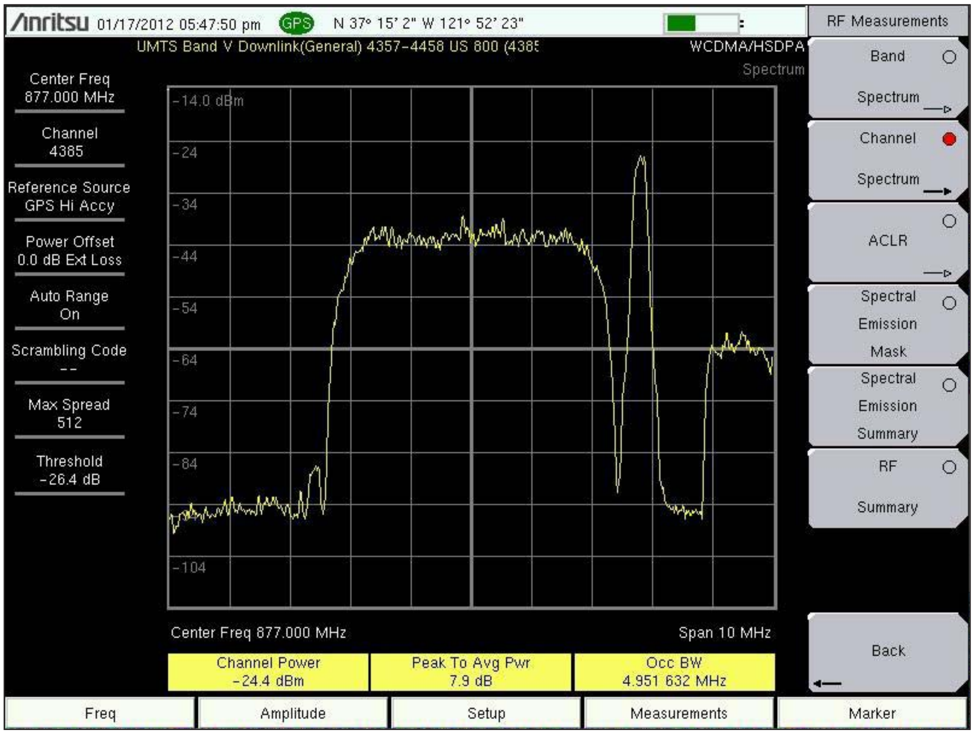

Figure 10. W-CDMA Signal with a GSM signal nearby

Minimum requirements to be sure it is a legitimate W-CDMA signal.

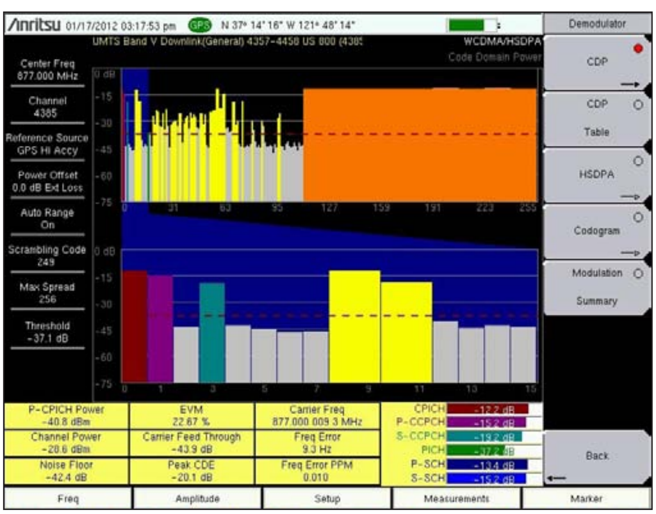

Figure 11. A busy W-CDMA site

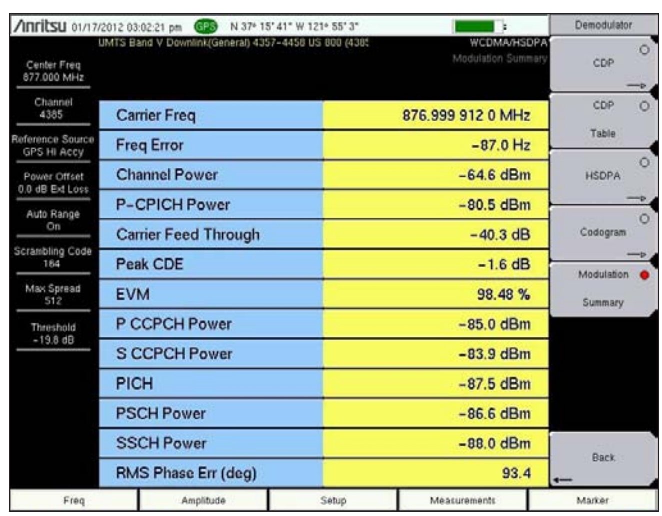

Figure 12. W-CDMA Modulation Summary

There are a few things to look at to get good assurance that the signal is a legitimate W-CDMA signal. Start by determining a signal standard and channel number for the signal. Do this by pressing **Signal Standard** in the **Frequency** menu. Note the frequency of the signal you are looking at then choose the signal standard that includes the frequency of the signal. Key in the frequency and then press **Set CF To Closest Channel**.

On the Demodulator CDP screen (see figure 11) observe activity on the signal. First, make sure the number of users changes frequently. There may be short periods with no users. When looking at the modulation summary, the power levels of the numerous control signals (PICH, PSCH power, SSSCH power) should be nearly equal in power within 1 or 2 dB. The frequency error should be small, indicating that the signal is on a standard W-CDMA channel. If the frequency is incorrect by more than 1 kHz, be suspicious. To achieve the required level of frequency accuracy, lock the instrument to GPS before starting measurements.

LTE

Signal Appearance

An LTE signal is a Bart's head that is roughly 1.4, 3, 5, 10, 15 or 20 MHz wide. Verizon and AT&T have deployed 10 MHz systems and MetroPCS has a 5 MHz system. There are some 20 MHz systems in Europe.

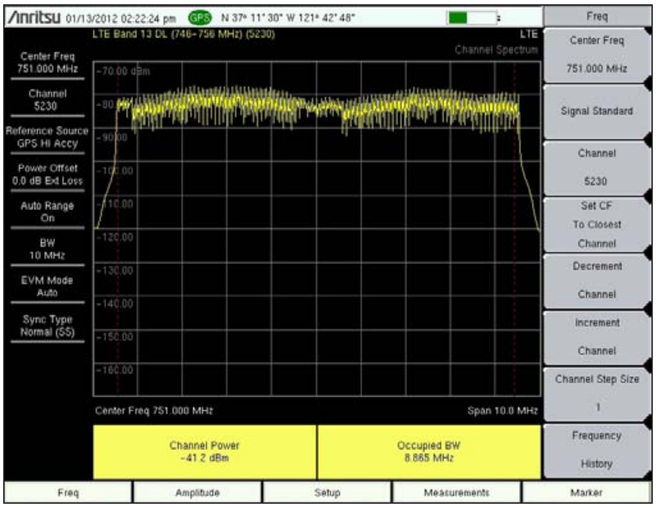

Figure 13a. LTE Signal in a 10 MHz channel

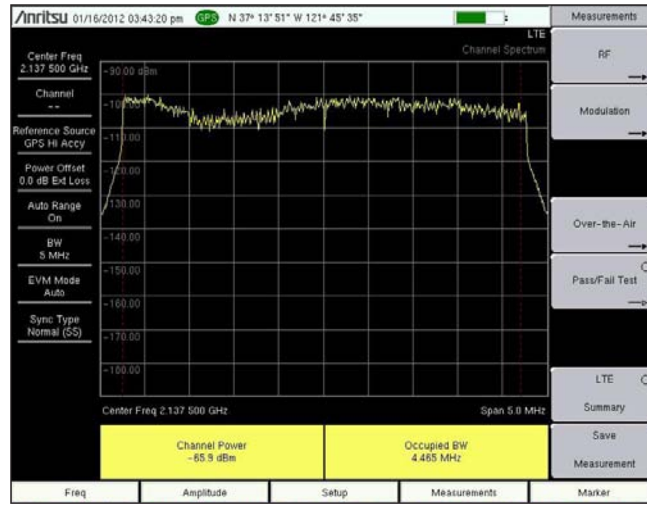

Figure 13b. LTE Signal in a 5 MHz channel

Minimum requirements to be sure it is a legitimate LTE signal.

To be reasonably confident that the signal you are seeing is an actual LTE signal, make sure there is a Cell ID number and that the control channel power levels are very close to the same power. In addition the frequency error should be very small. To achieve the required level of frequency accuracy, lock the instrument to GPS before starting measurements

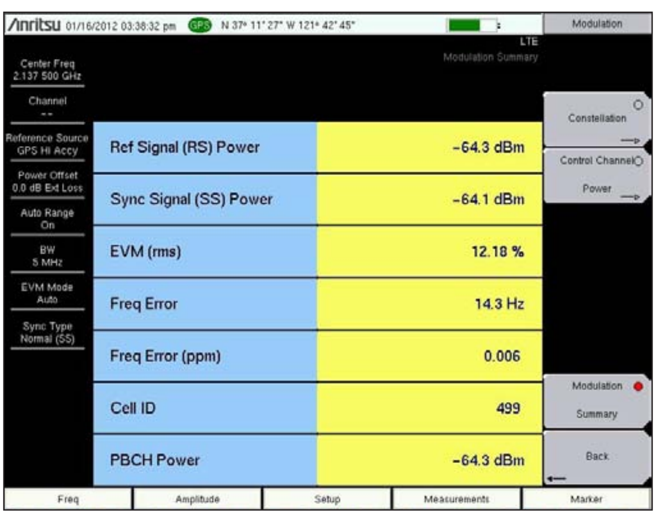

Figure 14a. LTE Modulation Summary

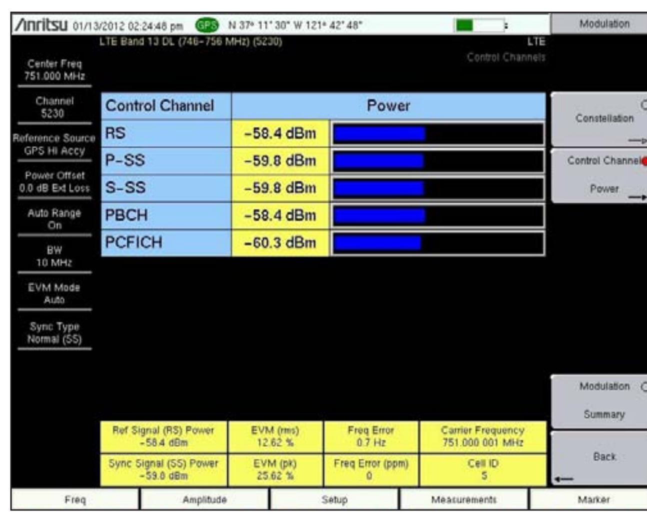

Figure 14b. Control Channels

WiMAX

Signal Appearance

A WiMAX signal is another example of a Bart's head. Bandwidths of 3.5, 5, 7, 8.75 and 10 MHz are allowed in the WiMAX signal standard (802.16). Under ideal conditions the Bart's head should have a flat top and almost vertical edges. The signal shown in figure 15 is a real-world measurement and shows the effects of selective fading on the signal – the reduction in amplitude on the left part of the signal. Depending on the exact conditions, the effects of fading and multipath can show up as single or multiple dips in the signal amplitude.

Figure 15. WiMAX Signal in Frequency Domain

Minimum requirements to be sure it is a legitimate WiMAX signal.

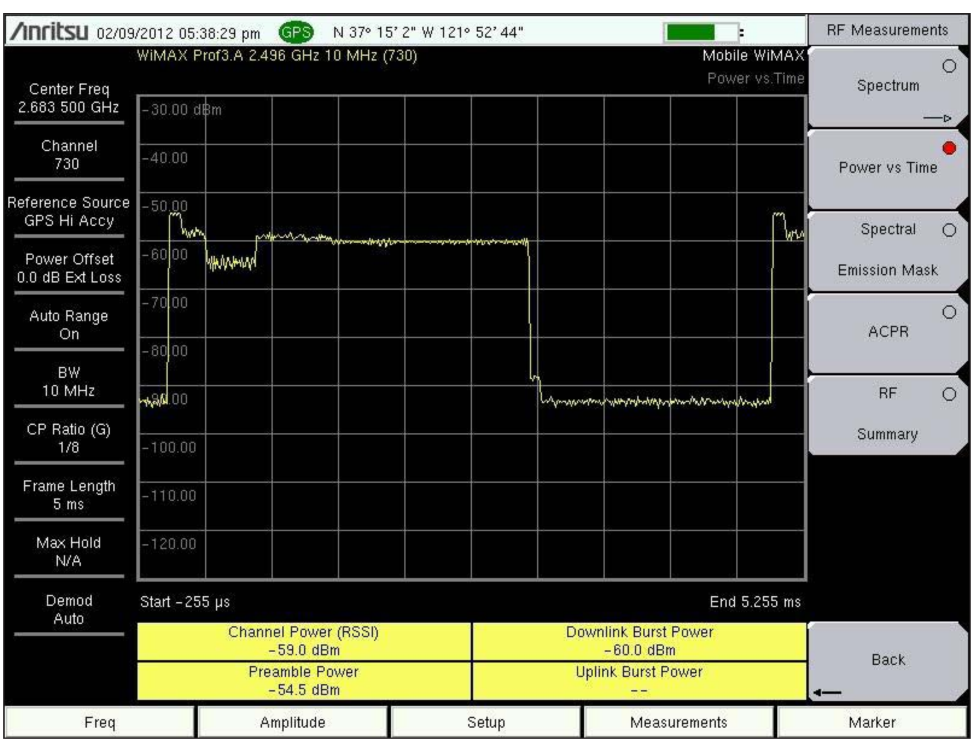

Figure 16. WiMAX Power vs. Time

One of the most important characteristics of a mobile WiMAX signal is the fact that there is a time when the base station transmitter is turned off so communication from user equipment can be heard. A full cycle takes approximately 5 ms, as shown in figure 16 and includes the period when the transmitter is off. That can be seen on the far left and the right half of the signal in figure 16. Modulation formats allowed for WiMAX include BPSK, QPSK, 16QAM and 64QAM. Generally BPSK is only used on the control channels where high data rates aren't critical.

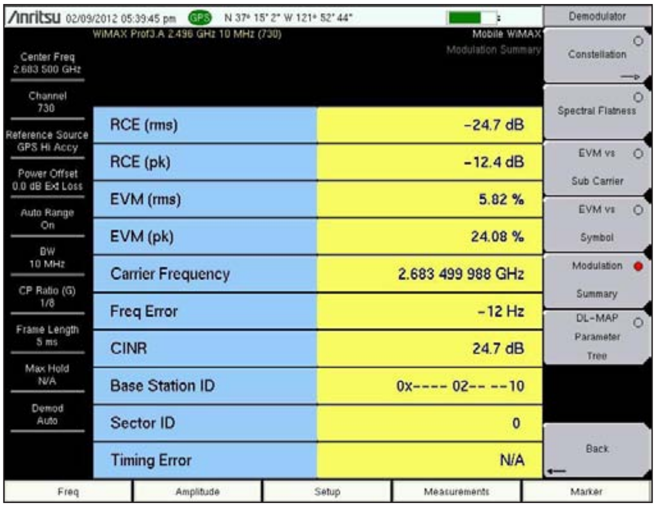

Figure 17. WiMAX modulation summary

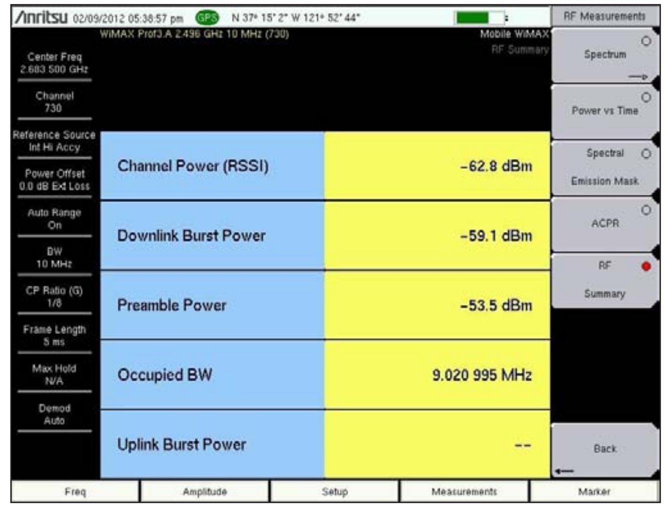

Figure 18. RF Summary

A legitimate base station must have a Base Station ID and be on a frequency licensed for WiMAX. The measurements shown here were done while the spectrum analyzer was locked to GPS to assure that the frequency measurements were accurate.

Summary

In the on-going game of cat and mouse with people attempting to listen-in on private conversations, and security people working to stop them, this is yet another step in the continuing efforts to hear what is intended to be private. Sometimes the hidden transmitter will do a very good job of emulating a base station so other more traditional means will need to be employed to find the transmitter while in other cases it will be possible to identify a rogue transmitter using the techniques discussed in this note. There are more cellular signal standards than are covered in this application note. The ones that aren't here aren't presently deployed in The Americas, Europe or Africa. Particularly, TD-SCDMA is only deployed in China so it is unlikely that someone wishing to hide a signal in plain sight would use it outside China. TD-LTE may be deployed widely, but it isn't yet.

Refer to Anritsu's Troubleshooting Guides for more information on these and other signals. They may be downloaded at no charge from the Anritsu web site at www.anritsu.com. At the time this is written troubleshooting guides are available for CDMA2000 1x, CDMA2000 1x EVDO, Fixed WiMAX, Mobile WiMAX, GSM/GPRS/EDGE, LTE, TD-LTE, TD-SCDMA/HSPDA and W-CDMA/HSDPA and other non-cellular topics. An easy way to find them on the site is to enter the term "troubleshooting guide" into the search

• United States
Anritsu Company
1155 East Collins Boulevard, Suite 100,
Richardson, TX, 75081 U.S.A.
Toll Free: 1-800-ANRITSU (267-4878)
Phone: +1-972-644-1777
Fax: +1-972-671-1877

• Canada
Anritsu Electronics Ltd.
700 Silver Seven Road, Suite 120,
Kanata, Ontario K2V 1C3, Canada
Phone: +1-613-591-2003
Fax: +1-613-591-1006

• Brazil
Anritsu Electrônica Ltda.
Praça Amadeu Amaral, 27 - 1 Andar
01327-010 - Bela Vista - São Paulo - SP - Brazil
Phone: +55-11-3283-2511
Fax: +55-11-3288-6940

• Mexico
Anritsu Company, S.A. de C.V.
Av. Ejército Nacional No. 579 Piso 9, Col. Granada
11520 México, D.F., México
Phone: +52-55-1101-2370
Fax: +52-55-5254-3147

• United Kingdom
Anritsu EMEA Ltd.
200 Capability Green, Luton, Bedfordshire LU1 3LU, U.K.
Phone: +44-1582-433280
Fax: +44-1582-731303

• France
Anritsu S.A.
12 avenue du Québec, Batiment Iris 1-Silic 612,
91140 VILLEBON SUR YVETTE, France
Phone: +33-1-60-92-15-50
Fax: +33-1-64-46-10-65

• Germany
Anritsu GmbH
Nemetschek Haus, Konrad-Zuse-Platz 1
81829 München, Germany
Phone: +49 (0) 89 442308-0
Fax: +49 (0) 89 442308-55

• Italy
Anritsu S.r.l.
Via Elio Vittorini 129 00144 Roma Italy
Phone: +39-06-509-9711
Fax: +39-06-502-2425

• Sweden
Anritsu AB
Borgafjordsgatan 13, 164 40 KISTA, Sweden
Phone: +46-8-534-707-00
Fax: +46-8-534-707-30

• Finland
Anritsu AB
Teknobulevardi 3-5, FI-01530 Vantaa, Finland
Phone: +358-20-741-8100
Fax: +358-20-741-8111

• Denmark
Anritsu A/S (for Service Assurance)
Anritsu AB (for Test & Measurement)
Kay Fiskers Plads 9, 2300 Copenhagen S, Denmark
Phone: +45-7211-2200
Fax: +45-7211-2210

• Russia
Anritsu EMEA Ltd.
Representation Office in Russia
Tverskaya str. 16/2, bld. 1, 7th floor.
Russia, 125009, Moscow
Phone: +7-495-363-1694
Fax: +7-495-935-8962

• United Arab Emirates
Anritsu EMEA Ltd.
Dubai Liaison Office
P O Box 500413 - Dubai Internet City
Al Thuraya Building, Tower 1, Suite 701, 7th Floor
Dubai, United Arab Emirates
Phone: +971-4-3670352
Fax: +971-4-3688460

• Singapore
Anritsu Pte. Ltd.
60 Alexandra Terrace, #02-08, The Comtech (Lobby A)
Singapore 118502
Phone: +65-6282-2400
Fax: +65-6282-2533

• India
Anritsu Pte. Ltd.
India Branch Office
3rd Floor, Shri Lakshminarayan Niwas, #2726, 80 ft Road,
HAL 3rd Stage, Bangalore - 560 075, India
Phone: +91-80-4058-1300
Fax: +91-80-4058-1301

• P. R. China (Shanghai)
Anritsu (China) Co., Ltd.
Room 1715, Tower A CITY CENTER of Shanghai,
No. 100 Zunyi Road, Chang Ning District,
Shanghai 200051, P.R. China
Phone: +86-21-6237-0898
Fax: +86-21-6237-0899

• P. R. China (Hong Kong)
Anritsu Company Ltd.
Unit 1006-7, 10/F., Greenfield Tower, Concordia Plaza,
No. 1 Science Museum Road, Tsim Sha Tsui East,
Kowloon, Hong Kong, P.R. China
Phone: +852-2301-4980
Fax: +852-2301-3545

• Japan
Anritsu Corporation
8-5, Tamura-cho, Atsugi-shi, Kanagawa, 243-0016 Japan
Phone: +81-46-296-1221
Fax: +81-46-296-1238

• Korea
Anritsu Corporation, Ltd.
502, 5FL H-Square N B/D, 681,
Sampyeong-dong, Bundang-gu, Seongnam-si,
Gyeonggi-do, 463-400 Korea
Phone: +82-31-696-7750
Fax: +82-31-696-7751

• Australia
Anritsu Pty Ltd.
Unit 21/270 Ferntree Gully Road,
Notting Hill, Victoria 3168, Australia
Phone: +61-3-9558-8177
Fax: +61-3-9558-8255

• Taiwan
Anritsu Company Inc.
7F, No. 316, Sec. 1, Neihu Rd., Taipei 114, Taiwan
Phone: +886-2-8751-1816
Fax: +886-2-8751-1817

Anritsu prints on recycled paper with vegetable soybean oil ink.

Application Note No. 11410-00649, Rev. A Printed in United States 2012-03