

# M2M

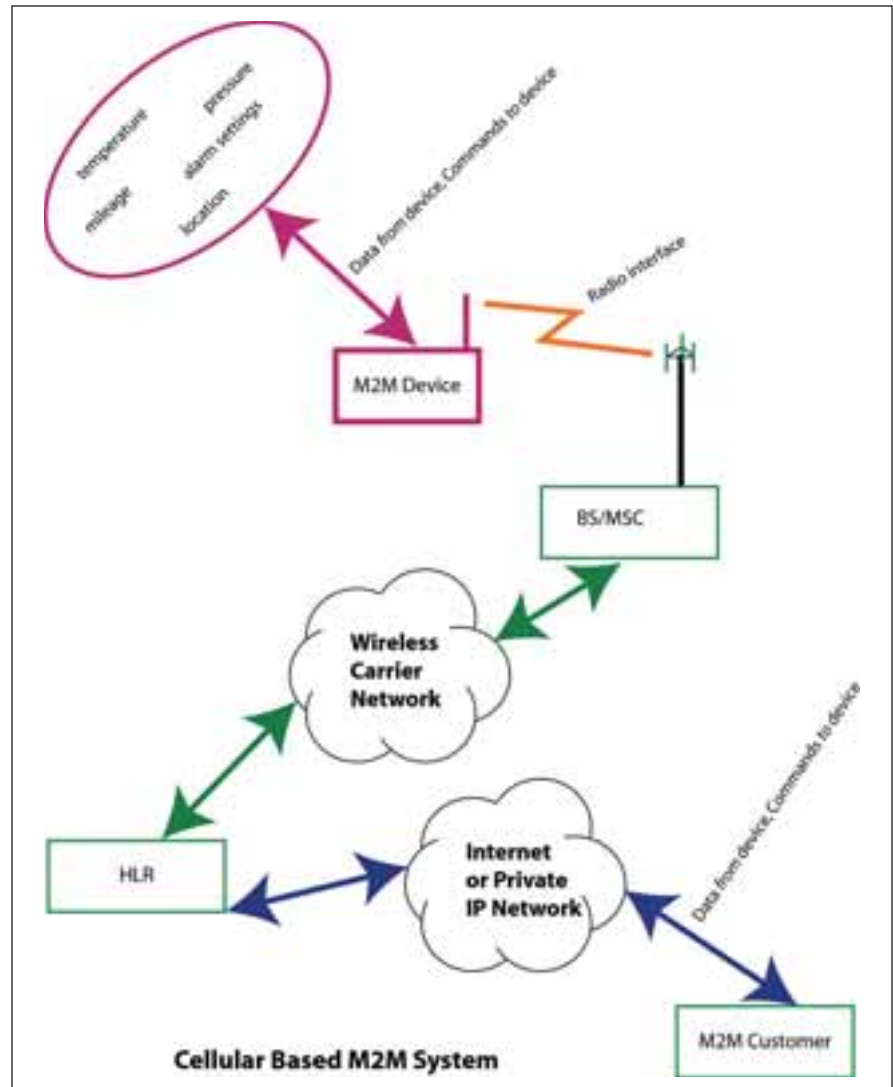
## Machine-to-Machine Communications

By David Crowe

It's 3 a.m. somewhere in Canada and machines are using the cellular network to talk to each other. This is not a sci-fi novel with robots plotting to overthrow humanity and take over the world. Although it is certainly a revolutionary form of communications, it is one that is only benign and beneficial. A stolen truck might be reporting its location as it is being driven hell for leather to the nearest border. A break-in is being reported by an alarm system despite the phone lines being cut. A car is reporting that its airbags have activated to an emergency centre. A bus has reported its mileage and maintenance is being scheduled. An electric utility company is shutting off air conditioners during a time of peak electricity demand for customers who have agreed to this in return for lower electricity rates. A photocopier is reporting that it is running out of toner and a vending machine is reporting that its supply of junk food is dangerously low.

Modern machines increasingly contain computers that produce information that can be useful to make business processes safer and more efficient, to assist operators, and to collect information needed to inform and bill customers.

In many situations, the amount of information is not great – sometimes even a single 'bit' of information such as the on/off status of an alarm – but it can be very important. Wired communication is not always a good



solution, sometimes due to the cost of installing wiring to a large number of devices, and sometimes because the application is mobile, where wiring is not an option at all. Most applications cannot justify the installation of a private radio network, so cellular provides a unique combination of geographic availability, the ability to

use as much or as little capacity as needed, low capital costs to gain access to the network, and high reliability.

There are many justifications for using wireless in fixed applications, when the device itself is not mobile. One example is as communications for an alarm system in case phone lines to a location are cut by thieves. In other

cases, the cost of wiring thousands of devices, perhaps electricity meters, would be too high. In some situations, photocopiers for example, devices might be moved occasionally, so using wireless avoids rewiring costs. Another example is that of vending machines, especially those installed for temporary events.

In many cases, the applications are not just wireless, but also truly mobile. These take advantage of the ability of cellular devices to obtain service in most populated regions of Canada and along most major highways. An example would be a vehicle fleet management service, or a car theft monitoring service. Both the ability of cellular systems to provide communications in many different places and to provide it while a device is in motion are critical.

## **Although SMS messages are often interpreted as text (a string of characters), there is nothing that requires this interpretation – anything goes between two consenting end points.**

The possibilities that arise with virtually instant and automated communications are numerous and surprising in depth and breadth. Take vehicle monitoring, for example. While fleets will clearly benefit from having regular updates on the location of mobiles for scheduling purposes, the information gathered can be used for much more than just that. Sensors in the vehicle can be hooked up to report engine malfunctions, a failure of a refrigeration unit or other specialized equipment, and can indicate when the next maintenance is required. Driving characteristics can also be reported, so that dangerous drivers or those who

are particularly hard on vehicles can be identified. Delivery and pickup instructions can be sent to the driver. If a vehicle is stolen, it can be placed in a mode where it reports its location more frequently, increasing the chance that police can intercept it before it is taken to another jurisdiction or before the freight is offloaded and the vehicle abandoned.

### **Analog Origins**

Machine-to-machine (M2M) communications arose during the peak of popularity for analog cellular (AMPS) in the early 1990s when some bright engineers at two companies, Aeris and Cellemetry (now Numerex), realized that they could use the analog cellular network for digital communications. Perhaps surprisingly, they did not use cellular modems. Not only were these expensive and bulky, but the setup time for a modem using acoustic techniques was long and the reliability of communications was low. Instead, these engineers used the cellular control channel, which is digital even on analog cellular systems.

All cellular systems differentiate between control and traffic channels. A traffic channel carries a single user's voice or data. In the days of analog cellular, one frequency slice would be dedicated to a single user for the duration of a call or data session. Digital systems share a block of frequency between a number of users, providing virtual traffic channels for the exclusive use of one call or data session.

A control channel, by contrast, is a shared resource. When a mobile first enters a cellsite, a registration message will be sent on a control channel, which triggers internal network messaging to determine the validity of the mobile and what privileges it might have in the current serving system. When a mobile is originating or receiving a call, messages are also exchanged on control channels, including the identity of the traffic channel to move to. Text messages to or from mobiles require an exchange of communications on control channels to arrange for delivery of the messages

(and sometimes the message contents are also transmitted on a control channel).

Analog control channels were not designed for transmission of user data, but that did not stop bright minds from designing how to do it.

One technique developed was to use registrations to report up to 32 bits of data (e.g. 32 on/off indicators or a single number between 0 and about 4 billion). In analog cellular systems, both the Mobile Identification Number (MIN) and Electronic Serial Number (ESN) are transmitted for registrations, with the MIN identifying the subscription and the ESN identifying the phone. Only the MIN is needed to route the registration message to the subscriber's Home Location Register (HLR). A normal HLR will use both MIN and ESN to check the validity of the subscriber, determine its subscribed services and store the identity of the system that is currently serving the mobile. M2M systems have different plans.

The MIN is always needed for routing, but not the 32-bit ESN. Therefore, a machine in the network can package its data into a 32-bit number and send that instead of its ESN. What looks like an HLR to the network is actually an interface to a data communications network that can use the MIN to identify a device and interpret the ESN as data associated with it. This pseudo-HLR can then use any available data network to route the received 32-bit number to a particular customer along with an identifier of the device that generated it. This technique provides communication with a low latency (the time between deciding to send data and the first packet reaching its destination).

There is a small problem with this: the serving system will retain the MIN and ESN and validate the next registration against it. This caching reduces the need for network communications to validate that the MIN and ESN are a matched pair. This is a barrier to M2M communications, because transmitting the same MIN with a different 32-bit number would result in rejection of the registration.

Luckily, it was not difficult to think of a simple workaround by simply having the M2M HLR tell the serving system to cancel the registration immediately after receiving the data.

A different method is to send a string of dialed digits to the home system. This again requires some cleverness because dialed digits are usually analyzed at the serving system. But luckily, when digits are dialed that match a certain pattern, such as beginning with a star (\*) or octothorpe (#), a message will be sent to the HLR for processing, rather than interpreting the digits locally. This capability was designed for dialed digit strings that are used to control services such as call forwarding, but since the interpretation of the digits is up to the HLR, they can be used to convey data instead. Digit strings are usually restricted to 16 digits, but each digit can convey 10 different values, so the total amount of data transferred is equivalent to a 50-bit number, almost double the data capacity of the ESN method.

This method too has a wrinkle: as dialing digits like this will result in a traffic channel being established, it is necessary for the device to disconnect the unneeded call.

Both methods over analog systems provide only one-way communications – from the remote device to a central server – and they do not allow for the device to be controlled by the server. It is possible for the server to initiate a page, which could trigger the mobile to initiate an unscheduled report, but page messages contain no user-controlled data, limiting the sophistication of features that can be provided with this method.

### **Transition to Digital**

Early M2M systems used analog service because it was then the most ubiquitous, which was more important than the additional capabilities that TDMA, CDMA and GSM digital service were beginning to provide in limited areas. Once the footprint of digital approached that of analog, the tide started to turn. Now the tide is almost completely out – in February, 2008 the US government will no longer require

that cellular carriers provide analog service, and it is expected that analog service will be shut off fairly rapidly after that. Canada, with its larger surface area and lower population, may need analog a little longer, but clearly this technology has no future for designing new M2M systems.

The first cellular capability provided by digital that was attractive to M2M was not a full-blown data service, but Short Message Service (SMS). Compared to transmitting data in an ESN or feature code, SMS was much more capacious and had none of the side effects of the methods used on analog systems. SMS messages are generally allowed to contain up to 160 characters, which is the equivalent to the same number of 8-bit bytes on CDMA and TDMA systems and 134 on GSM (which uses a compressed alphabet in text messaging). This is 40 times the capacity of the ESN method. Larger strings, perhaps even slightly over 200 bytes, might be transmissible depending on individual wireless carrier network configurations.

Although SMS messages are often interpreted as text (a string of characters), there is nothing that requires this interpretation – anything goes between two consenting end points. M2M systems can encode their data either as binary or as strictly formatted text strings. For example, if the first thing to be transmitted in a message is a number that can be between 1 and 1000, the SMS can either contain four characters (e.g. 0, 0, 3, 7) or a number encoded in 10 bits (e.g. 0000100101). Clearly, binary encoding is about three times more efficient in this example, but text encoding may be more compatible with the data produced by equipment.

For an M2M provider to use SMS, they need to provide an SMSC (Short Message Service Centre) interface to the network. Again, the cellular network will see this no differently than an SMSC used solely for the delivery of text messages to consumers.

As digital systems evolved, they also started to provide packet data services, allowing a full Internet connection.

Packet data is transmitted on a traffic channel (after a setup phase on control channels). This provides possibilities for transmission of much greater quantities of data than SMS, although services directed at the phone are not always possible (unless the device maintains a permanently active packet data session). A workaround for this problem is to send an SMS with the data instead or, if the quantity of data is greater than an SMS can contain, to merely use the SMS to wake the mobile up and have it reestablish the packet data session.

Another capability that emerged in digital systems was the ability to obtain the approximate location of a mobile. This can either be provided autonomously by the network using techniques like triangulation (measuring the angle and strength of a signal as received by multiple cellsites), or through GPS. The ability to get this information is particularly advantageous in mobile M2M applications where the location is almost always useful if not downright essential.

There may be applications requiring communications in remote areas where the coverage of the cellular network may be inadequate. In these cases, cellular M2M systems can be supplemented by satellite communications. This will increase the device size, cost and power consumption, and operational data charges will be higher as well, but it is a good solution when the need to communicate everywhere is paramount.

At the other end of the spectrum, wireless LAN technologies such as Wi-Fi can also be implemented where devices will spend much of their time in a constrained area, such as a warehouse or loading yard. Wi-Fi can provide higher speed transmission and, because it uses unlicensed spectrum, has no usage costs. This is especially applicable when a large amount of data needs to be transmitted at the beginning or end of a journey (where Wi-Fi's bandwidth would be most useful), and smaller amounts when the device is in

motion (e.g. delivery notification and messages to and from the driver).

### Service Packaging

There are two basic styles of packaging of M2M systems. One is to provide a single application that can be used by multiple customers, and the other is to simply provide a network to aggregate and deliver the communications, presenting a simple interface to companies that have custom communications needs. Vehicle tracking is one of the most popular applications, and several companies provide highly sophisticated systems within the budget of smaller companies that could not afford custom development. Billing for a system like this might be based on a monthly fee, or on the usage of the application.

On the other hand, companies with sophisticated needs that use applications that are unique or need better integration of applications with their other business software, can just obtain a virtual M2M communications network from a carrier or aggregator. The end user will install modules, subscribe to service from the aggregator, and then start to receive updates via their data network. The aggregator can present diverse methods of communications in a consistent format, even though systems like SMS and packet data are implemented in very different ways on the cellular networks. In arrangements like this, billing will most likely be usage based.

In the very largest applications, a company may provide the entire application themselves, designing custom hardware and software to optimize performance.

### Is M2M For You?

M2M communication is useful when you have a significant number of devices to communicate with, whether they are mobile or wired interfaces, and when other methods of communication are impractical or otherwise undesirable. The throughput capabilities of the device should match your application. If

mobility is the main need, and data requirements are not high, devices based on SMS or other low throughput capabilities will be suitable. If data requirements are sometimes much greater, packet data devices can be considered. There are a variety of radio systems that provide packet data capabilities, and the data rates and costs vary considerably.

M2M systems continue to grow with the capabilities of wireless systems. They lag only because ubiquity is so

important, so a partially rolled-out service will usually be avoided. The increase in bandwidth of wireless systems means that increasingly audio, still pictures or even video will be complementing simple messaging applications in the expanding world of M2M communication. ■

*David Crowe is a wireless standards, technology and numbering resource consultant based in Calgary. He can be reached at David.Crowe@cnp-wireless.com.*

# Cardo, Setting the New Standard for Bluetooth® Headsets

**THE CARDO SYSTEMS, INC.**

### The Cardo S-800™

**The Perfect Combination of Precision Design and Advanced Headset Technology.**

The superbly styled S-800 offers access to you favorite three numbers with one-touch Hot Dialing, SWAP Technology to switch between two mobile phones, and a unique headset location buzzer to find the headset if misplaced.

### scala-700LX™

Setting a new standard for Bluetooth® headsets

- **SWAP Technology:** Switch between two mobile phones with a touch of a button.
- **Headset Location Buzzer**
- **Missed-call Indicator and Call-back Function**

Auto Answer, Conference Call and more...

### The Cardo S-2™

Wireless Stereo Headphones with Advanced Function and Hip Retro Design

Provides wireless hi-fi stereo and allows hands-free voice control of your mobile phone and MP3 Player all in one product

**HITFAR**  
www.hitfar.com  
1.800.661.1186  
604.873.8355