

A Metretek Whitepaper of 29 September 2003

Cellular IP Telemetry Services: Dispelling the Myths

By: Joseph L. Harley, Vice President

Forward:

As an extension of corporate information systems, the managers of telemetry (data acquisition and control) systems are faced with the need to reduce the cost associated with their operations. In this context they are looking to more extensive use of public wireless carriers to replace the historical need to build-out and maintain their own private networks. All things being equal it is clearly cheaper to share a network with others than to build and operate one's own network. This fact has not escaped the cellular companies and they are actively soliciting telemetry customers to absorb excess capacity while generating additional revenue and gross margin. So, in theory, it is a win-win situation. However, since caveats do exist, they must be prudently dealt with. And in fact they can be, provided one has the factual knowledge to do so.

As public wireless carriers migrate their cellular networks from analog technology to digital systems with IP (Internet Protocol) connectivity, the "gold rush" to grab telemetry and M2M (machine-to-machine) customers is leading to a rash of misleading information originating from various organizations with vested interests in promoting their technology or methods. Whether intentional or not, this is confusing to end-users trying to make decisions concerning telemetry and information system deployment and therefore counter-productive to achieving optimized value and security for the enterprise.

Working with Cellular for many years and with Digital Cellular IP for several years, Metretek provide data solutions using it, without bias toward either of the major competing wireless network technologies....CDMA or GSM. It is the intention of this paper to objectively point out facts concerning the use of these technologies and, in layman's terms, raise the red flag where we believe overstatements or myths are proliferating in the market.

Definitions and Concepts:

1. **Eavesdropping:** The practice of accessing a system for the purpose of listening in on a conversation or collecting information. A read-only function that is not directly destructive to the system being read.

2. **Hacking:** The practice of accessing a system for the purpose of manipulating it. Usually a read and write function that is designed to alter, destroy or render the system inoperable.

3. **Server:** A machine that is “listening” or waiting on a network for requests from other machines for connection and service. On IP based networks, servers “listen on” static addresses and port numbers for calls [requests] from clients, in much the same way that a fax machine listens for callers requesting document copy service. It follows then that a server is the most vulnerable node in a network as it is intentionally made accessible. Generally, the more servers that exist in a network the less secure the network will be.

4. **Client:** A machine that initiates a communication session by requesting service from another machine [the server]. Clients do not “listen” on a network for connection requests and are therefore far less vulnerable to security breach.

5. **Public IP address:** An address which can be “seen” as the source IP address of the actual device which is transmitting on the network. It may or may not be directly accessible from anywhere on the public network. Sometimes it is called an external address it is not a translated address. Generally it is the address of a network segment security filter a.k.a. a firewall. However, it can just as easily be the address of a server or client. A public address can be permanently assigned (static) to either a server or firewall or can be dynamically assigned when a server or firewall connects to a network.

6. **Private IP address:** A device source IP address which is “hidden” by the process known as Network Address Translation (NAT) not directly accessible from anywhere on the public network. Sometimes it is called an internal address. These are generally used behind or downstream of firewalls which are protecting network segments. Clients on the segment are dynamically assigned a private address and servers on the segment are typically assigned a static private address so that they can easily “serve” the local clients. Such a server can still be accessed from the public network if the public address of the firewall is translated to the static private address of the server, a.k.a. “Natted”.

7. Polling: In telemetry systems, the process whereby a centrally located computer/program will sequentially and on-demand establish connections to remotely located devices. The remote device will then accept commands from the computer/program and return data to it or execute control functions. Historically, telemetry systems would use **private** wire-lines, **private** radio channels or dial-up public lines for these connections. In this telemetry system architecture the “server” is the remote device (historically called the “slave”) which is listening for a connect request from the “client” (historically called the “master”) which role is played by the centrally located computer/program.

End-users who are comfortable with the polling nature of legacy telemetry applications naturally wish to continue operating with this method even while migrating to the modern world of cellular IP. However, the cellular IP network is fundamentally a client-server network where the remote [wireless] device is the client and the central computer/program is the server. Those who are security conscious will immediately recognize the benefits of having many clients and only one server to protect versus having one client and potentially thousands of exposed servers.

It is paramount to remember that remote devices in many cases are security devices themselves or are capable of controlling [or losing control of] critical local or national infrastructure.

8. On-Demand Connection (ODC): Does the one server many client nature of cellular IP mean we must all invert our processes and forego the comfort of the familiar polling methods of data acquisition and control? The answer is no.

The cellular IP networks provide several service methods (SMS and USSD for example) that can be used by the server to signal the clients that it is time to communicate. Once notified to “call-home”, the clients can do so and the server can authenticate each connection request using standard encryption and security methods. Clearly this architecture and method will dramatically reduce the potential for catastrophic security breaches of remotely located equipment, even while it permits a user interface that appears to function identically to that of the legacy application. An attacker can no longer simply access a serving device at a water pumping station or electric sub-station because

the device, now a client, will NOT serve. It can only originate a session, connecting to the server “master” and then taking instructions from it.

The Myths:

Myth 1: Unlimited numbers of public, static IP addresses are available from cellular carriers for M2M communications.

While Cellular IP systems can, in theory, support such an address space, they were designed to take advantage of the limited address space of Internet Protocol version 4 which is currently the world standard. IPv6, if and when fully deployed in the public internet, ultimately will have an address space which could avail a discreet address for every machine, assuming that were deemed prudent. However at this time, it seems very unclear if and when IPv6 will be fully deployed. For more on this topic you can link to <http://www.ipv6.org/> . The reality is that static IP addresses are not available from the carriers.

What is available from the carriers and usually at additional charge is a limited “pool” of dynamically assigned public addresses. Remote devices acting as servers can retain such an address as long as the device stays connected to the network. Of course disconnects do occur and a new address would be obtained by the device when re-connecting. In order to poll these “servers”, one of two approaches could be used:

1. A client application program would have to issue a numeric format IP address from the pool and then determine which server device actually answered. While this might be considered polling (on-demand) connectivity, it is likely to be quite inefficient with regular uncertainty as to which device will be connected at any point in time or.....
2. Upon connection or re-connection to the network, the server remote device would have to connect to the client application (now temporarily acting as a server) or some other [probably not free] service to report its new IP address assignment. This is the basis of the so-called Dynamic Domain Name System or DDNS. DDNS is being touted by some to be ‘just like’ static IP addressing. Clearly though, it is not. If the newly assigned IP address is reported to a service instead of the client application, such service would then be responsible for updating the DNS. The point of this method is so that the client can directly call the serving remote device using addressing of the form: unitA.companyB.com.

In addition to the potential for significant software development and service charges to implement this method, security is not improved and connectivity may be sluggish as addresses are changing and can take some time to ‘ripple’ thru the DNS update process. Some possibilities of difficulties include:

- a. Loss of assigned address due to inactivity timeout. It is likely that this can be overcome in one of two ways: pay extra charges to the carrier to get them to eliminate the timeout or pay the extra data cost to send “keep alive” data.
- b. Missed connection requests from the client application because the server remote device reported an address, lost connection and had to report another new address to the DNS.
- c. Extra data cost for each server remote device to frequently report new addresses to the DNS.

A practical alternative to the use of dynamically assigned public address pools is to use an ODC architecture as described in point 8 above. Why?

1. Security is much better served by having a client at the remote location and there will be no question about which device is connected when a connection is requested by a client.
2. The ODC architecture requires only **private**, dynamic addresses. These are default issue when purchasing a cellular IP account and therefore have no cost penalty. Private addresses offer the greatest possible security.
3. System throughput will be higher because unintended connections and addressing overhead functions will not delay desired connections.
4. Cost efficiency will be better because unnecessary and system overhead connections (unintended or address management) will be avoided.

Myth 2: GSM/GPRS systems are ‘hack-able’ and CDMA systems are not.

For an easy to understand explanation of this topic Metretek suggest the reader visit http://www.sierrawireless.com/News/docs/2130223_Wireless_Security.pdf

As of this writing, GSM/GPRS systems comprise approximately 80% of worldwide cellular service. These systems have supported many sensitive applications such as point

of sale for many years. Time sharing systems like GSM and CDPD use complex encryption of over the air and network control traffic and this makes for extremely secure use of the network. It is difficult to fathom how GSM could have attained its widespread use and appeal if it posed the security risk that some imply it does.

Likewise but in a different domain, the frequency sharing CDMA networks use sophisticated methods for encrypting transmissions and network control traffic. Like GSM, these systems are extremely difficult to eavesdrop on or hack.

Perhaps some of the thinking behind this myth has resulted from the oft repeated history of CDMA development, i.e. that the fundamental spread spectrum technology was born during the days of World War II and became a staple of the military need for secure communications. What has been lost in this story is that the security breakthrough represented by spread spectrum technology is usually being compared to simple narrowband analog radio, be it cellular or otherwise.

The simple truth is that any system can be compromised if the attacker has the motivation and resources necessary to do it. In the case of both CDMA and GSM, any potential hacker will require enormous amounts of knowledge, motivation, resources and plain old luck.

Myth 3: Your investment now will be protected for 10 years.

Backward system compatibility is usually the code phrase for this. And while both CDMA and GSM carriers tout backward compatibility, at any point in time the availability of such compatibility hinges on two words...**supply** and **demand**.

Technology marches on and we can all be sure today's hot technology will be tomorrow's Model-T. When the demand for the new technology outstrips available supply, then supply is likely to be taken from the pool supporting the old technology. A perfect example is the erosion of analog cellular service due to its frequency band being re-allocated to digital cellular service.

At any stage, if the money is being made from resources dedicated to new technology, then it is extremely unlikely that old technology will continue to be funded. The electronic components market teaches this each and every day. Microprocessor, modem and other chips that were plentiful two years ago are now obsolete. Yes there is a replacement, but it is not free of charge, nor free of the pain of implementation.

Competitors continue to strive for advantage thru product and service differentiation. This leads to technology changes and ultimately this means upgrades will be required of the end-user. Clearly though, this is better than seeing your own expensive, private network become obsolete. Another positive is that sometimes the competing carriers get ahead of themselves and this is currently evident in that both CDMA and GSM carriers have an over supply of capacity even using current technology. So while no one can predict the future (much less ten years into it), the fact remains that pricing for cellular IP telemetry services is very attractive compared to the alternatives and appears to be trending toward even greater value for the end-user in years to come.

In Summary

No doubt there will be those who will take issue with material presented herein. This is a good and healthy result because its effect will likely be to cause end-customers to seriously consider their application and the range of alternatives available to address it.

The fact is that while the core technologies of CDMA and GSM systems are different, the range and quality of services that they provide the subscriber are very similar indeed. The real difference, between the success or failure of legacy and new applications that are ported to cellular IP networks, lies in the hardware and software components offered by third parties that provide the needed interface to the chosen carrier. It is not difficult to put a cellular transceiver in a box. However, achieving a comprehensive, cost-effective and painless transition solution is another matter altogether.