DSP Techniques for Cellular, Paging, and PCS Intercept

Scott L. McCulley
TSR Technologies, Inc.
A division of Grayson Electronics, Inc.
P.O. Box 10727
Blacksburg, VA 24062

Abstract
This paper describes a real-time digital signal processing receiver which is capable of intercepting both cellular telephone transmissions and paging data. This paper also discusses how this technology can help law enforcement personnel use mobile communications to their advantage in monitoring, tracking, and capturing criminals. Specific applications are discussed.

I. Introduction
With the rapid increase of mobile communications, the law enforcement community has encountered numerous problems with monitoring the activity of criminals. It has become necessary to have access to radio intercept equipment that is capable of monitoring the wide variety of wireless communications standards throughout the world. This paper discusses such a cellular and paging monitoring system which uses a digital signal processing (DSP) receiver that can detect cellular, paging, and PCS traffic, from 25 MHz up to 2000 MHz.

By using a distributed array of such DSP receivers, where each receiver is capable of receiving traffic from a local geographic area, it then becomes possible to develop a distributed data collection system whereby instant information on calling patterns, rapid fraud detection, and direction finding becomes possible within a city. Note that there are some law enforcement applications where only a few receivers are needed to intercept the desired traffic, i.e. only one or two DSP receiver(s), and a laptop computer and Yagi antenna for each receiver (see Appendix A: Letter of Testimonial).

TSR Technologies, owned by Grayson Electronics, has developed the patent pending cellular and paging DSP receiver [1] which law enforcement agencies are currently using to monitor criminal activity. TSR Technologies has developed easy-to-use, DOS menu software which controls the CELSCOPE receiver for cellular intercept [2] and the PAGETRACKER receiver for paging intercept and RF coverage analysis [3]. TSR Technologies also has integrated NAVTRACKER, a Global Positioning System (GPS) receiver, into its CELSCOPE and PAGETRACKER receiver to allow position location data to be recorded with all traffic. With this configuration, the user is able to make automated signal measurements while driving through a particular area. CELLPOST and PAGEPOST programs have also been developed by TSR so that quick post-processing, mapping support, and data reduction can be performed on measurements made with the CELSCOPE and PAGETRACKER receivers (NAVTRACKER option is required for mapping support).

The complete DSP interface standard for the CELSCOPE and PAGETRACKER is given in [4] but a quick overview of the standard is necessary to understand how real-time cellular and paging intercept is accomplished. The DSP receiver communicates with a host computer (such as PC) through a full duplex 19.2 kbaud RS-232 data link. Both cellular/paging control data and radio signal strength indicator (RSSI) data are sent to the computer over the RS-232 link and are distinguished at the computer by the serial parity check bit. Cellular control data contains mobile phone numbers (MINs), electronic serial numbers (ESN), dialed digits, voice channel assignments, and other cellular system parameters. Paging control data contains capcodes (PINs) and pager messages (alpha-numeric or numeric message). The DSP receiver is completely controlled by the host computer to enter a particular

1. CELSCOPE, PAGETRACKER, NAVTRACKER, CELLPOST, and PAGEPOST are registered trademarks of Grayson Electronics, Inc.
decoding mode (e.g. U.S. cellular intercept or paging intercept), a frequency (in Hz), and modulation type (frequency modulation, amplitude modulation, or single sideband). The DSP receiver also has the capability of muting or activating the audio speaker, so that only legal telephone conversations can be recorded. The software for the CELLSCOPE and PAGETRACKER receiver automatically handles setting up the DSP receiver for cellular or paging intercept, so that for most law enforcement applications this software can be directly used without any knowledge of the DSP interface. The DSP interface is openly published so that custom applications can be designed around the CELLSCOPE/PAGETRACKER DSP receiver.

II. Cellular Telephone Fundamentals

A cellular system consists of mobile units and base stations. Each mobile unit communicates (voice and data) with the strongest base station (Note: due to radio frequency (RF) propagation and obstructions, a mobile unit may not communicate with the closest base station). A cell defines the RF coverage area of one base station. Each base station uses one of the 21 standard control channels issued by the Federal Communications Commission to transmit and receive cellular data. Mobile phones operate within a cell and are controlled by one base station at a time. When a mobile phone moves from one cell to another cell, the base stations of each cell communicate to hand the mobile from one cell to the other (called a "hand-off"). The cellular base stations are controlled by the mobile telephone switching office (MTSO) which handles the entire system. The MTSO is connected to the public phone company so that all phone conversations must be routed through it. The MTSO is responsible for numerous tasks such as determining hand-off conditions and determining if mobiles are in the system.

The cellular system is a full duplex system where the mobile and base station each have a separate frequency for communicating. For both voice channels and control channels, a U.S. cellular telephone operates at a frequency of 45 MHz below the frequency of the strongest/controlling base station. Each cellular channel operates in a 30 kHz bandwidth for both the forward and reverse channels. The cellular terminology is that the mobile frequencies are reverse channels and the base station transmit frequencies are forward channels. The four different type of cellular channels are: forward control channel (FCC), reverse control channel (RCC), forward voice channel (FVC) and reverse voice channel (RVC). The control channels are used for transmission of system data, call placement, and transmissions of ESN and MINs. Voice channels are used for telephone conversations and control data which is used to hand-off the mobile phone, change power levels, and confirm orders.

The cellular system processes telephone calls in two ways. One way is if the mobile is making a call. The other way is if the mobile is being called. When a mobile is being called, the phone's MIN with a page order is broadcast throughout the entire cellular system within a short period of time. If the mobile is within the cellular system, it then responds to the page on the RCC of the strongest base station. When the base station receives the RCC transmission by the mobile, the call is handed off to a voice channel. When a mobile is making a call, it transmits its request on the RCC of the strongest base station, and the base station then hands the call off to a voice channel. For either call processing case, the mobile sends its MIN, ESN, and dialed digits (if originating a call) on the RCC of the strongest control channel. Additional orders (hand-offs and power level changes) are performed on the FVC and RVC.

III. Paging Fundamentals

A paging system is designed to cover a large area by using one or more transmitting locations. Unlike cellular, paging transmitters are at the same frequency throughout the system. The paging system is designed as a cost effected system were there is only a few expensive high power transmitters and thousands of cheap pagers. Pagers are designed to be a receive-only device at a single frequency. A paging terminal receives all the information and the directs the data simultaneously to all the paging towers in the system. Digital paging
data is sent out in a serial manner with the following form: a capcode (PIN) is transmitted first followed by a digital message (alpha-numeric or numeric) for that capcode. Many paging systems support multiple paging standards, (i.e. POCSAG 512 baud, POCSAG 1200 baud, and GOLAY 300/600 baud). All paging information (capcode and message) with the same baud rate and standard is sent out in a continuous burst of data so that pagers can easily decode the transmission. Each pager has a unique capcode so that when the pager detects its capcode, it then can decode and display the message that follows its unique capcode.

IV. Understanding the DSP receiver and provided software

The DSP receiver includes two software packages, CELLSCOPE for the IS-54 dual mode cellular standard and PAGETRACKER for all digital paging standards (POCSAG, GOLAY, and NEC). Furthermore, the receiver can be used as a spectrum analyzer for frequency monitoring with FM, AM, or SSB demodulation type. This is useful in monitoring cordless telephone conversations and verifying RF coverage areas.

The standard CELLSCOPE and PAGETRACKER receiver provides alarms to activate external devices when particular mobile phone numbers or pagers are accessed or when particular messages (pagers) or digits dialed (cellular) are detected. The software can also be set to automatically print specific traffic as it is received. Each software package offers ways to mask the digital information and to write it to a readable log file with date, time, signal strength, and message. The alarms feature allows other external devices (i.e. auto-dialer or tape recorder) to be activated by the external trigger that occurs when an alarm event happens. The software logs in real-time all decoded data (MINs, ESNs, dialed digits, cellular telephone orders, pager capcodes, and pager messages) to an ASCII text file with time, date, signal strength, and channel number/frequency. The log file can then be easily printed at any time.

Whether a phone originates a call or receives a call, CELLSCOPE is able to track to call from control channel to voice channel. CELLSCOPE is also able to record MIN, ESN, and dial digits, as well as follow the entire voice conversation when the mobile is handed off to different voice channels. CELLSCOPE can be setup to just log the cellular control channel, so that CELLPOST can be used to trace the activity of certain MIN, identify heavy users, and record the history of any MIN. In the same manner PAGETRACKER can be setup to log all the paging traffic on one paging frequencies, so that PAGEPOST can be used to trace the history of a capcode, search for specific messages, and determine heavy users.

The examples discussed below show how the CELLSCOPE or PAGETRACKER software can be used in law enforcement applications. Furthermore, a law enforcement agency or contractor might wish to write their own software using the published open interface [4]. The CELLSCOPE and PAGETRACKER software is written to drive only a single DSP receiver, and a law enforcement agency or contractor may wish to write a high level program that can access multiple DSP receivers by taking advantage of the existing single DSP receiver software. One easy way to do this is to use a "PC on a card" with a 19.2 kbaud modem dedicated to each receiver. All the cards would be placed in a fast PC workstation with land lines running between each receiver and the "PC on a card". The TSR software would run on each "PC on a card" and all the data logged on each card would be directed to the fast PC workstation for easy custom applications using ASCII text files. This setup allows custom applications to be developed without any knowledge of the low-level DSP interface standard.

V. How to use cellular telephone RCC to monitor suspects

Depending on state laws for monitoring digital data on a cellular phone, some of these procedures may require a warrant. These techniques illustrate how a single DSP receiver or an array of DSP receivers can be used to monitor the reverse control channel (RCC) in order to gain valuable information such as calling patterns, digits dialed, and approximate time and location of suspects.

The software included with the CELLSCOPE
DSP receiver provides law enforcement with a multitude of information about the suspect’s mobile phone. A stock CELLSCOPE DSP receiver and PC need to be placed in locations where suspects use their cellular phones the most. The placement of the receiver is important because the relatively weak reverse link mobile phone signal can only be received by the closest base station and a closely located DSP receiver. Each DSP receiver needs to be configured individually and this can be done by using a modem connected to the PC with the CELLSCOPE software and a commercial remote control software package. The CELLSCOPE software will automatically lock each receiver on the strongest control channel. The user can monitor the RCC by pressing F3. The user may also enter the suspects phone number(s) in the MIN masks (OPTIONS window). The user would also enter a log file (OPTIONS window) so that all cellular activity is recorded. Following this simple procedure, the log files can be downloaded each day to a central computing center that can process all the calls made in a geographic area in order to determine calling patterns and approximate time and location of each phone number. Note that this example demonstrates easy use of the software provided with the CELLSCOPE receiver. The central post-processing center can organize the data to determine cell site location of each phone number, the number of calls made, and to whom the calls were made. The user is reminded that CELLPOST can perform a number of these post-processing procedures, so that fast and quick system integration is possible.

The cellular systems in major cities are now using autonomous registration where the mobile unit will automatically register with the cellular system by transmitting, on the RCC, its MIN and ESN every few minutes. An array of CELLSCOPE receivers located in key positions can use this readily available information to track a suspect’s mobile phone. If the suspect is in a key location, then CELLSCOPE will give an accurate record of exactly how long the suspect is in the area by the number of registrations and the time and date stamp.

VI. Problems with cloned cellular phones

Fraud is also a concern to cellular carriers and is becoming a major problem in the cellular radio community. In the U.S. alone, the Cellular Telephone Industry Association estimates that over $1 million in revenue is lost to fraudulent cellular users every day [5]. Law enforcement agencies and cellular providers need to work together to combat these problems. An individual who is performing fraudulent activity with a cellular telephone has a good chance of performing additional illegal acts. With the increase in fraud, most cellular companies are adding the autonomous registration feature to their cellular system. Registration requires that mobile phone be verified before a phone call can be placed. Registration remover "tumbler" phones or phones that change their MIN and ESN pair every phone call. Systems without registration allow the mobile a free first call before the MIN and ESN pair are checked for validity. Thus a tumbler is able to make an unlimited number of calls by tumbling its MIN/ESN pair.

Cellular fraud is now occurring with cloned phones. MIN and ESN pairs are obtained from valid users and then programed into many phones. The cloned cellular phone will work for about a month, until the true owner receives the bill. At which time, the cellular service provider deactivates the MIN/ESN pair and issues a new MIN/ESN pair to the customer. Criminals then replace the cloned phones with a different valid MIN and ESN pair. The integrated network of DSP receivers can determine cloned phones by monitoring a number of base stations for assignments close together in cell site that are far apart. Some of the CELLSCOPE receivers can be setup to follow calls and other receivers can be setup to monitor the FCC. By performing daily post-processing, the system can then find a cloned phone by searching for the times when a MIN is being followed. Cloners are easily identified when a channel assignment occurs to the same MIN during the same time but on a different base station. The array of CELLSCOPE receivers can also be set up to monitor the FCC for channel assignments. A MIN with a large number of channel assignments has a high likelihood of being a
cloned phone. CELLSCOPE has a very powerful capability of recording the activity of 150,000 users all at the same time. An alarm can be set to fire whenever a particular MIN exceeds a specified number of calls.

VII. Monitoring pager

Unlike cellular systems, which require CELLSCOPE receivers to be located in a reasonably close vicinity to the suspect's cellular phone, the paging system has much less stringent requirements. PAGETRACKER merely needs to be located in a reasonably good location within the paging RF coverage area, which is usually hundreds of square miles. The PAGETRACKER receiver replaces the need for a law enforcement officer to provide 24-hours a day monitoring of a cloned pager, and also removes the additional cost and hassle of obtaining such pagers from the paging company. By being an auto-baud detection system capable of decoding any capcode, PAGETRACKER is invaluable when trying to determine the capcode and message of any criminal who is using a pager. Also, the PAGETRACKER message mask trigger feature can be used to determine all pagers which receive certain messages. PAGETRACKER can monitor the activity of thousands of pagers at one time, and PAGEPOST can be used to count the most popular capcode within a certain time period as well as determine all capcodes that receive the same message. Because paging data is transmitted through the entire system, only one PAGETRACKER receiver is need for each paging frequency. The PAGETRACKER driving software is quickly configurable to trigger off any capcode, message, or combination of both capcode and message. Message triggers can be entered using wildcards so that partial data can be detected and recorded. The external alarms can also be used in conjunction with a triggered event, so an external device can easily be connected to a PAGETRACKER receiver. In fact, many remote control applications can be built around PAGETRACKER.

VIII. Conclusion

The CELLSCOPE and PAGETRACKER DSP receiver described here has an extremely easy-to-use computer interface, and is currently in use in over 100 worldwide markets as a flexible, all-in-one cellular, paging, and PCS system measurement tool [6,7]. There are numerous applications that have been discussed in this paper, including distributed monitoring and fraud abatement. With the published open interface standard, customized application receivers can be developed. Multiple DSP receivers can be connected together at a common base, using landline, microwave radio, or existing T1 channels to support real time RS-232 data transmission. A distributed network of CELLSCOPE and PAGETRACKER receivers described in this paper, each with their own local controllers, could provide real time traffic monitoring and intelligent network support for a wide range of law enforcement applications.

IX. References


Ted Rappaport  
TSR Technologies, Inc.  
P.O. Box 10727  
Blacksburg, VA 24062-0727  

January 5, 1993

Dear Ted:

On January 4, 1993 Blue Ridge Cellular, Inc. and the Blacksburg Police Department were able to track down a tumbling phone and arrest the person involved. Without the use of your device, it would have been next to impossible to locate this person.

Through our roaming clearing house we discovered that somewhere on our system there was a cellular phone on which the ESN was able to be tumbled. All we knew were the numbers he was dialing and the cell site he was making the calls. This information was not even available to us until the call was completed. We had no way of knowing exactly where he was or even what channel he was making the call on. We did have radio equipment that we could use as a direction finder but since we had no idea what channel he was on until the call was completed, this equipment was almost useless in locating him.

The solution to this problem was answered very quickly when we brought in CELLSCOPE 2000. By mounting this unit in a vehicle with a directional antenna we were able to follow the call to its source. Cellscope allowed us to monitor all the control messages transmitted between the cell site and the phone. By being able to monitor this data, we were able to trigger on specific pre-call patterns and switch to the correct channel to track the call. After several calls, we were able to locate the unit down to a single apartment. After we positively determined where the cellular phone was, the Blacksburg Police Department obtained a search warrant and confiscated the phone.

Without your device we probably would have never been able to locate the tumbling phone. I would highly recommend your device to help locate and detect any type of cellular fraud.

Sincerely,

John Snapp  
System Engineer