Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 12, December 1996

In This Issue...

Look forward to your next issue on: January 6, 1997

Our Editor: Now Appearing in Cellular Business Magazine

The Editor of *Cellular Networking Perspectives,* David Crowe, now has a monthly column entitled "Networks" in Cellular Business magazine, that started with the September, 1996 issue. His column will address many of the same issues as in this bulletin, although in less detail, due to space constraints. His first four columns addressed the International Forum on AMPS Standards Technology (IFAST), the Telecommunications Industry Association TR-45 standards setting process, the use of authentication to combat cloning fraud and enhanced wireless emergency services. ❑

TACS Cellular Around the World

TACS is probably the third most popular cellular technology around the world, after GSM and AMPS. It is a sister technology to AMPS analog cellular, operating in the 900 MHz frequency band (as opposed to 800 MHz for AMPS), and with a slightly modified control channel. The countries that have TACS systems installed are shown in the map on page 6. ❐

RF Fingerprinting Carves a Niche Out of Fraud, Part II

In Part I of this article (November, 1996) we described how RF Fingerprinting works, and how it compares with other anti-fraud methods, such as authentication and profiling, noting some of the synergies between the different methods. We conclude with more detail on the advantages and disadvantages of RF Fingerprinting, and also provide a list of installed or planned equipment installations.

Pros and Cons

Like the other anti-cloning systems discussed in Part I, RF Fingerprinting is not a perfect solution. Its big advantages are that it can work on virtually any phone and that its operation is transparent to most legitimate subscribers most of the time. Its disadvantages are the cost of installing new equipment at every cell-site, its inability to detect all clones and interoperability between the three different vendors to support roamers.

Pro: Works on Any Phone

RF Fingerprinting today monitors the analog control channel, and consequently works with any phone operating in that mode. Exceptions are IS-95 CDMA and IS-136 TDMA digital cellular phones operating on a digital control channel and PCS phones. There is no apparent need for RF Fingerprinting (at least for fraud applications) on these phones, as they all support authentication.

Cellular Networking Perspectives (issn 1195-3233) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cr. NW, Calgary AB T2N 3W1, Canada. Phone: 1-800-633-5514. Fax: 403-289-6658. Subscriptions: CDN$300 in Canada (incl. GST), US$300 in the USA and US$400 elsewhere. A surcharge of up to US$200 per year is required for faxing to international subscribers. Payment by cheque, money order or American Express. Issues are faxed, mailed 1st class or emailed. Copies: Subscribers may make up to 10 copies of each issue. Rates available for more copies. Discounts: Educational & Small business 25% off any order, by mail only. Back Issues: Phone for price list and list of contents.

Pro: Little Customer Impact

Subscribers should not be able to detect that RF Fingerprinting is in operation (although hopefully cloners will notice!), except that a small percentage (claimed to be less than 1%) of legitimate calls will be denied. The impact on legitimate customers will be highly positive if RF Fingerprinting reduces service denial due to loading on cellsites in high fraud areas and reduces the possibility of customers receiving heart-stopping, multi-thousand dollar cloner bills.

Con: Cost per cellsite

RF fingerprinting equipment has to be installed at every cellsite, making its cost high compared with other techniques. The cost per cellsite is in the $20,000 to $30,000 range, making it a substantial capital expense. Although, to put this in perspective, the cost of implementing RF Fingerprinting in all US cellsites is similar to the cost of fraud for one year. Manufacturers are trying to offset the perception of high cost by promoting the advantages of having a sophisticated RF platform at each cellsite (see "Other RF Platform Benefits", below). Dick Cahill of CTS claims that "customers will experience a pay-back within 12 months, which is a pretty good ROI."

Con: Letting Clones Slip Away

RF Fingerprinting can discriminate a clone from a good mobile with the same MIN and ESN about 85%-98% of the time (this may include the impact of profiling in parallel). Allowing a small percentage of cloning calls through is not a serious problem (especially as compared to today's cloner detection rates) as long as cloners do not find combinations of legitimate phones that are hard to fingerprint reliably and clone phones that are sloppy within the same range.

Con: Giving Good Guys Grief

With any heuristic decision making method, no matter how sophisticated, it is possible to make mistakes in either direction. Much more attention is paid to whether an anti-cloning method reliably catches the cloners, but it is also important not to falsely catch legitimate subscribers, at least not very often. Profiling can help with these cases, as a suspicious fingerprint without an accompanying change in calling patterns is probably a false clone alert. Manufacturers claim less than 1% of interdicted calls are false positives. The customer impact, in these cases, will be that this percentage of calls will be dropped shortly after pressing SEND. Since this occasionally happens anyway, customers will likely re-originate the call. Manufacturers claim that all mobiles can be fingerprinted reasonably reliably, and that false positives are not significantly more common on any group of phones. Although it is possible to turn fingerprinting off for selected MINs, Bill Taliaferro of Corsair claims that "in one market with over a million subscribers, this feature was only used a dozen times". In most cases, the feature is used to verify that RF fingerprinting is not the cause of a hard to resolve customer complaint.

Con: Interoperability

The biggest challenge for the RF Fingerprinting industry is to solve the interoperability problem for roamers. All three systems have either provided, or promise, complete interoperability between like systems. However, this will not catch all cloners using roamer MINs. Note that the legitimate phones may be roamers, but the cloners will likely be local crooks, as it is easy to change a local clonable phone to imitate any legitimate roaming phone by just programming a new MIN and ESN. The interoperability problem will likely affect purchase decisions, as carriers will tend toward purchasing the same equipment as their roaming partners. An A Side/B Side split between Corsair and CTS is already evident (although far from absolute).

The interoperability problem has been recognized by carriers, and discussions are underway between the three manufacturers, facilitated by the CTIA. Because the manufacturers use different methods, their internal condensed fingerprints are quite different. Describing how this information should be interpreted would reveal proprietary secrets. On the other hand, simply shipping the raw fingerprint around would result in high bandwidth requirements. One possibility is to have a neutral (and trusted) third party provide a method of translating one manufacturer's fingerprint into another. This would prevent competitors (and others) from knowing the ingredients for the other 'secret sauces'. There are no indications currently that RF Fingerprint information, in whatever format is chosen, will be transported over the IS-41 network (and, indeed, this may not even be possible), so a new nationwide (and eventually international) network will need to be developed, although the number of gateways between different manufacturer's equipment networks could be minimal.

Another interoperability problem occurs when MINs are used from systems without RF Fingerprinting. One solution is to do nothing (which will cause cloners to attack these MINs preferentially and probably will result in loss of roaming privileges for these MINs unless they support authentication), another is to install listen-only fingerprinting monitors to capture valid fingerprints and the third is to install RF Fingerprinting or other fraud fighting technology in those systems.

Other RF Platform Benefits

Manufacturers of RF Fingerprinting equipment promote the benefits of having an RF platform at every cellsite, both to persuade their customers that the value is greater than just the immediate application, to ensure the customer that their investment will not become obsolete when authentication finally takes over clone fighting and also to promote future sales of value added hardware and software.

Several other applications of an RF platform are possible:

i. Monitoring base station transmissions for quality.

ii. Monitoring mobile transmissions to identify mobiles that are not within specifications, and may be causing the system, and other mobiles, problems.

iii. To identify spurious emissions from sites that are either not supposed to be transmitting at all (e.g. P.A. systems), or are transmitting mainly in another band, with only spurious emissions in the 800 Mhz band. According to Bob Shaw of Signal Science, “Wideband receivers can monitor for bad emitters, locate, demodulate and identify non-cooperative signals.”

iv. Determining the location of a mobile, for pinpointing cloners, 9-1-1 callers and, in the presence of an appropriate warrant, suspected criminals. Also, it is possible to provide value added services by selectively routing calls based on the location of the caller.

The Players

Three companies are providing RF fingerprinting equipment, Corsair (spun off in 1994 from TRW) with their PhonePrint™ product and Cellular Technical Services (CTS) with their PreTect™ product running on their Blackbird™ platform have commercially deployed equipment. Signal Sciences has their CellWatcher™ application running on their SuperCell™ platform in the “trial/proposal mode”, according to spokesman Shaw. Table 1 shows the current status of implementation, with Corsair in the lead in A-band markets and CTS in B-band markets.

Note that many of these markets (and others) already have, or soon will have authentication installed. When both techniques are available in the same market, authentication will protect some phones from some markets for all calls, and RF Fingerprinting will protect all phones from some markets in most calls.

Summary

RF Fingerprinting is one of the strongest anti-cloning technologies around today. It has good potential for widespread implementation, especially if the manufacturers can solve the interoperability problem for roamers. It will co-exist with profiling with, indeed, considerable synergy between them. Authentication will eventually replace RF Fingerprinting, but gradually over the next 5-10 years, not immediately. By then, if the manufacturers have proven the advantage of their RF platforms, the equipment will gradually be given over to other applications. ❒

Table 1: RF Fingerprinting Installations

Carrier	Market	A/B	Equipment
AirTouch	Atlanta	A	CTS PreTect
	Detroit	A	CTS PreTect
	Los Angeles	B	CTS PreTect (incumbent) Corsair PhonePrint
	Ohio	A	CTS PreTect
	San Diego	B	CTS PreTect (incumbent) Corsair PhonePrint
Ameritech	All markets	B	CTS PreTect
AT&T Wireless	New York	A	Corsair PhonePrint
Bell Atlantic/NYNEX	Boston	B	CTS PreTect
	All A-side	A	Corsair PhonePrint
	New York	B	CTS PreTect
	New Jersey	B	CTS PreTect
	Philadelphia	B	CTS PreTect
	Wash./Balt.	B	CTS PreTect
BellSouth	N. Illinois	A	Corsair PhonePrint
	Wisconsin	A	Corsair PhonePrint
Cellular One (AirTouch/AT&T)	San Francisco	A	CTS PreTect
	San Jose	A	CTS PreTect
Cellular One (SWB)	Boston	A	Corsair PhonePrint
	Chicago	A	Corsair PhonePrint
	Wash./Balt.	A	Corsair PhonePrint
Centennial	Several markets	A	Corsair PhonePrint
Comcast	Delaware	A	Corsair PhonePrint
	New Jersey	A	Corsair PhonePrint
	Philadelphia	A	Corsair PhonePrint
GTE Mobilnet	San Diego	A	Corsair PhonePrint
	San Francisco	B	CTS PreTect
	San Jose	B	CTS PreTect
LA Cellular (AT&T/BellSouth)	Los Angeles	A	Corsair PhonePrint
Telcel	Mexico	B	Corsair PhonePrint

An Introduction to Muneerah Vasanji, our Customer Service & Marketing Manager

Muneerah Vasanji has been working as *Cellular Networking Perspectives'* Customer Service and Marketing Manager for over a year. It is long past due that we introduce her to you! Many of you have talked to Muneerah and recognize her commitment to help you meet your information needs. Her responsibilities include providing information about the *Cellular*

Networking Perspectives bulletin to prospective subscribers, taking orders for subscriptions and back issues, resolving problems with delivery and providing a 'fax or email on demand' service for those that want back issues or other information in a hurry. Muneerah also manages our monthly website quiz (www.cnp-wireless.com) and distributes the prizes.

Muneerah is available to assist you, whether you have a problem, want to request a sample for a colleague or if you have a comment on the bulletin. Our number one priority is providing a top quality source of information every month, and part of that is keeping you, our customer, happy. After all, the information is of no use to you if it is not on your desk when it should be!

Muneerah holds a Bachelor of Arts degree in Communications from the University of Calgary and a Graphic Design certificate from the Southern Alberta Institute of Technology. She is continually upgrading her skills in desktop publishing, marketing and customer service. Muneerah brings a solid background in market research, corporate communications and graphic design.

Muneerah, and her husband Shaynoor, are expecting their first child early in 1997. But, after a brief respite, Muneerah insists she will be back! ❏

Status of IS-41 Rev. C (TIA/EIA-689 Rev. 0) Implementation

Cellular Networking Perspectives

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *First Publication*

Vendor1	Status	Date	Features	Other Vendors	Carriers	Locations
Alcatel SEL	Lab Trial		A S	*n/a*	*n/a*	*tbd*
Ericsson	Field Trials		A S	*n/a*	*n/a*	*tbd*
GTE	Lab Trial	2Q'97	A	*n/a*	*n/a*	*tbd*
Lucent	Field Trial		A	*n/a*	*n/a*	*tbd*
Motorola	Planning		*tbd*	*n/a*	*n/a*	*tbd*
Nortel	Lab Trial	mid'97	CM	*n/a*	*n/a*	*tbd*

Explanation:	Status:	Development, Planning, Lab Trial, Field Trial or Commercial.
	Date:	Date of actual or expected completion of listed phase of testing.
	Features	Features Being Tested
	A	Authentication
	C	Calling Number Identification
	M	Message Waiting Notification
	S	Short Message Service
	Other Vendors:	Other equipment vendors involved in trials.
	Carriers:	Carriers involved in trials.
	Locations:	Locations of trials.

Note: IS-41 Revision C is in the early stages of implementation, and some vendors have not yet revealed their plans for implementation. There are several differences in the implementation of IS-41 Rev. C versus IS-41 Rev. B:

i. IS-41 Revision C implementation will occur a feature or two at a time, with the early candidates being Authentication (kills fraud dead), Calling Number Identification (sells digital), Message Waiting Notification (sells air-time) and Short Message Service (sells digital).

ii. Complete vendor-vendor pairwise testing will not be required, a trend that was apparent towards the latter stages of IS-41 Rev. B implementation. Vendors and carriers have more confidence in their ability to install IS-41 solutions after testing with only selected vendors, and the ability to resolve compatibility issues in the field.

iii. TIA/EIA-689 Revision 0 has not been published yet, however for all practical purposes, implementations of this ANSI standard will be indistinguishable from IS-41 Rev. C.

Warning: There is a slim possibility that the ANSI standard will be given a different identifier, such as TIA/EIA-1541 (do you get the visual pun?).

TIA TR-45.2 Standards Update

A new batch of standards are ready to hatch, including inter-system support for data, enhanced TDMA and CDMA features, over-the-air service provisioning, emergency services and lawfully authorized intercept. They will form the basis for IS-41 Revision D (which will probably be published as TIA/EIA-689 Rev. A). Currently these standards were either approved for ballot at the November TIA TR-45.2 meeting or are very close to this state. Following the ballot period (usually 30-60 days) and review and incorporation of ballot comments, these documents can be published as TIA TSB's or interim standards. (IS's).

Recently Published

PCS Multi-band (TSB-76, PN-3624)

- This TSB defines modifications to IS-41 messages and procedures to allow interoperability between Cellular and PCS systems, and between the different licensed frequency bands within Cellular and PCS systems. *Published September, 1996.*

Ballot

Online Call Record Transfer (IS-124 Rev. A, PN-3293)

- This call detail and billing record network standard includes a variety of improvements and corrections over Revision 0, such as internationalization (i.e. support of IMSI) and some support for data calls. Due to the large number of ballot-induced changes, *a second ballot is necessary,* which will delay publication for several months.

IS-41 Rev. C ANSI Ballot (TIA/EIA-689, SP-3588)

- The "IS-41 Rev. C" ANSI ballot review was completed at the September, 1996 TR-45.2 meeting. It is currently undergoing editorial review, with publication to follow.

International Applications (TSB–29 Rev. B, PN-3173)

- This revision adds lists of known non-NANP MIN usage, a list of applicable global titles and a recommendation to use ANSI TCAP even if ITU SCCP and MTP SS7 layers are used. Out for ballot until Christmas Eve, 1996. The IFAST (International Forum on AMPS Standards Technology) has requested that publication be delayed until no sooner than the April, 1997 meeting.

TDMA DCCH (PN-3579)

- Definition of network support for the IS-136 Rev. A features "User Group" and "Non-public mode service". *Approved for ballot in November 1996.*

Inter-System Link Protocol (ISLP) (PN-3660)

- A new inter-MSC rate adaption protocol is required to support the transmission of data from digital phones following an intersystem handoff. *Approved for ballot in November 1996.*

Over-The-Air Service Provisioning (PN-3769)

- OTASP will provide the ability to program, or re-program, digital (TDMA or CDMA) mobiles over the radio interface. *Approved for ballot in November, 1996.*

In Development

Subscriber Features (IS-53 Rev. B, PN-3362)

- A major change in direction for this standard has been accepted, which will see Rev. B published with only minor enhancements from Rev. A, and with no new features. Features will be published in separate, standalone documents, such as those listed below (TDMA DCCH, Inter-System Link Protocol, etc.).

Data Services (PN-3770)

- Transmitting data from CDMA and TDMA digital phones is more complex because voice coders are incompatible with analog modem tones. While air interface solutions have been published, solutions to allow automatic roaming and intersystem handoff will *likely be approved for ballot in December, 1996.*

Law Enforcement Intercept (PN–3580)

- Squeezed between the cost concerns of the industry, the constraints of the US CALEA law and the demands of law enforcement, a new standard for intercept is emerging. It will apply to both IS-41 and GSM based wireless networks. This standard will be considered for *V&V in December, 1996* and subsequently will be sent for joint TIA/T1 ANSI Ballot.

Enhanced Wireless Emergency Services (PN–3581)

- A standard to use normal PSTN signaling (Feature Group D MF or SS7 ISUP signaling) to support the FCC-mandated Phase I for enhanced wire less 9-1-1 is nearing completion. It will apply to both IS-41 and GSM based wireless networks. Both cell/sector location and mobile identification will be transmitted to the emergency services system. This standard may be approved for *ballot in 1Q'97.*
  A proposal to use a datalink to the ALI (Automatic Location Information Database) to minimize signaling modifications by the emergency services system is under consideration. This approach may be postponed to the Phase II development, which requires more accurate location information, and will probably require this technique.

CDMA Capabilities (PN-3619)

- The definition of advanced features based on IS–95 Rev. A capabilities, such as TMSI is scheduled for *ballot in December, 1996.*

WIN: Wireless Intelligent Network (PN-3661)

- The description of intelligent networking for IS-41 based mobility networks is complete at a high level. The definition of IS-41 transaction and parameter modifications is under development. The schedule for *ballot is May-June, 1997.*

TIA/EIA-689 Rev. A (was IS-41 Rev. D)

- Work on TIA/EIA-689 Rev. A will begin in earnest once the TIA/

EIA-689 Rev. 0 document is published, as it will be the baseline. This standard will be focussed more on protocol modifications, descriptions of message flows will be retained in the individual capability/feature standards and TSBs listed above.

Interconnection (IS-93 Rev. A, PN-3295)

- Modifications to this PSTN interconnection standard to support emergency services are being considered in the development of PN-3581 (see above).

Call Detail/Billing Records (IS-124-B, PN-3725)

- A new project has been initiated to study modifications to IS-124 to fully support data services and intelligent peripherals. Work will begin once the re-ballot of IS-124 Rev. A is completed.

Cancelled

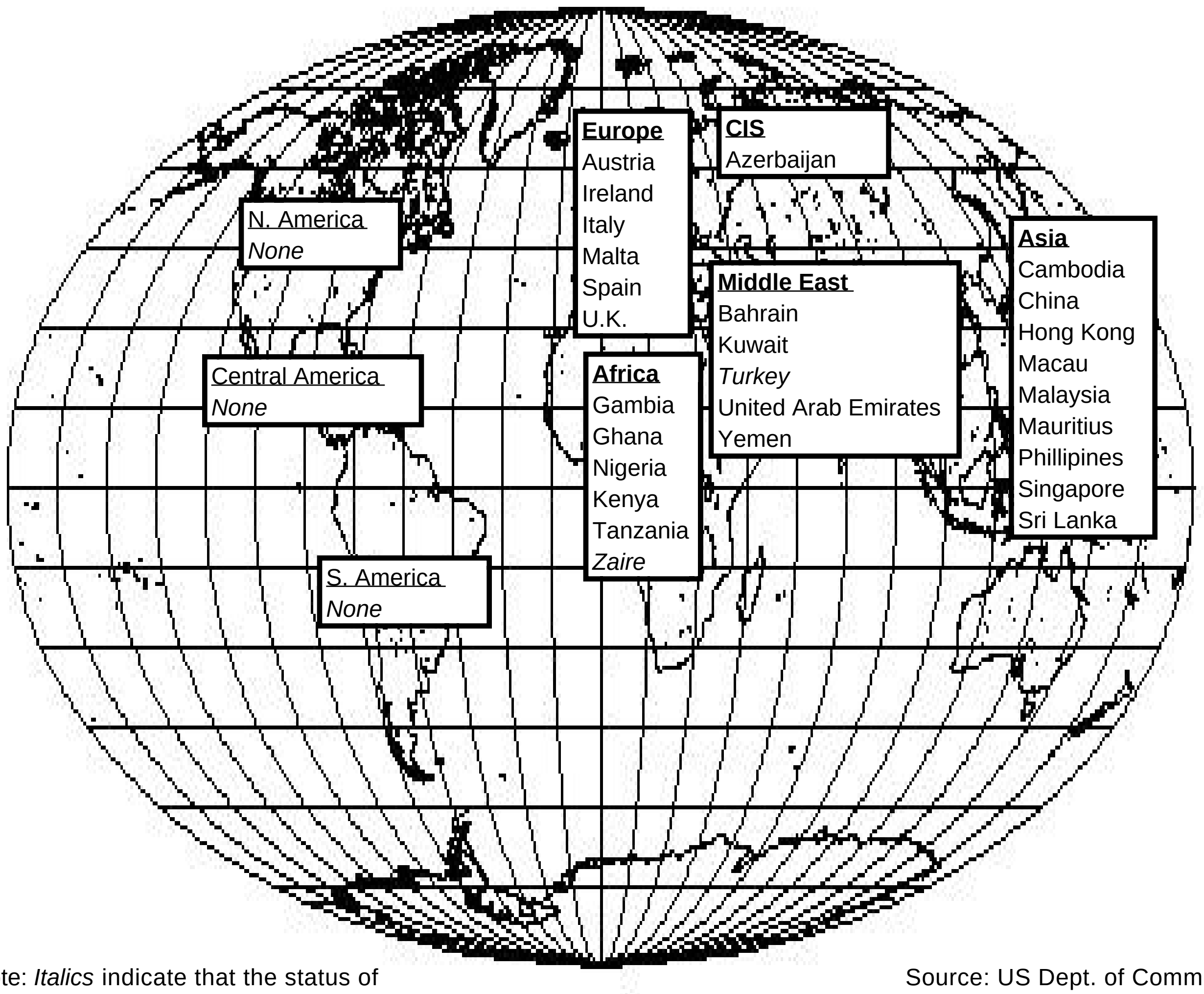
Multiple HLR Queries (PN-3528)

- Cancelled due to a lack of interest, and availability of other solutions to international roaming problems. ❐

Quote of the Month:

> "Authentication will protect some phones from some markets for all calls, and RF Fingerprinting will protect all phones from some markets in most calls."
>
> – see RF Fingerprinting article, Page 1.

"TACS" Cellular Around the World



Note: *Italics* indicate that the status of the TACS system is unknown

Source: US Dept. of Commerce