Cellular Networking Perspectives

David Crowe [Editor] • Phone: 1-800-633-5514 • Fax: 403-289-6658 Vol. 5, No. 3 March, 1996

In This Issue...

The Editor at Wireless '96!

David Crowe, editor of *Cellular Networking Perspectives*, will be prominent in spoken and written words at Wireless '96. Two of his articles will be in the Cellular Business show dailies, and he will be speaking at the "Incumbency 101" session on March 26 at 11am and also at the IFAST meeting on March 27-28.

Look forward to your next issue on: April 4, 1996

CTIA Agreement on Emergency Services

The CTIA announced an agreement on February 12, 1996 with three groups with an interest in promoting enhanced access to 9-1-1 from wireless phones:

- NASNA - National Association of State Nine-One-One Adminstrators
- NENA - National Emergency Number Association
- APCO - Association of Police Communications Officials

This agreement has been presented to the FCC as an industry consensus, with a request to adopt it as their rulemaking. Currently, it is out for comments as CC Docket No. 94-102.

The agreement proposes a two phased approach. Phase I will be completed within 18 months of adoption of FCC rules, and will provide:

- Caller's phone number.
- Caller's approximate location (cell/sector).
- Access to speech- and hearing-impaired callers.
- Callback to a recent 9-1-1 caller.

Phase II will be completed within 5 years and will provide location accuracy better than 125 meters, about 2/3 of the time.

Fees charged to cellular subscribers to fund wireless carrier and public safety investments would be in the range of 75 cents a month.

The CTIA will continue to work with the wireless industry to develop technology to meet the agreement, as well as with NASNA, NENA and APCO. The TIA TR-45.2 standards committee ad hoc group on enhanced wireless emergency services, chaired by Jeff Crollick of GTE TSI will play a critical role in the development of standards. This ad hoc group currently has wide industry representation, including a CTIA representative, and also meets with NENA, APCO and NASNA representatives to validate decisions made in the course of standardization.

More details on some of the other wireless emergency services requirements can be found in the October 1994 issue of Cellular Networking Perspectives. ❐

CTIA Accelerates Authentication

The CTIA has included authentication as a requirement for achieving their Gold Seal terminal certification, as of February 1, 1996. Now, rumour has it that the CTIA is pressing the industry to commit to a July 1, 1996 date, beyond which all new cellular equipment would be manufactured authentication capable.

US IMSI Administrator Appointed

Relationships between the CTIA and Bellcore over numbering issues must be improving. In 1992, the CTIA blasted Bellcore for "dragging its feet in assigning N00 codes to cellular". Yet, more recently, the CTIA and PCIA have worked to have Bellcore's Numbering Consulting Group (NCG) take over day to day administration of International Mobile Station Identity (IMSI) codes from the US Dept. of State.

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 or 1-403-289-6609. Fax: 403-289-6658. Subscriptions: CDN$250 in Canada (incl. GST), US$250 in the USA and US$300 elsewhere. Payment by cheque, money order or American Express Card. Issues are faxed or mailed 1st class. Copies: Each subscriber may make up to 10 copies of each issue. Rates are available for more copies.
Discounts: Educational and small business rates: CDN$150 (incl. GST), US$150 and US$200, by mail only. Back Issues: Phone for price list and table of contents.

Effective immediately, all requests for IMSI Home Network Identifier (HNI) codes should be addressed to the NCG, attention Nancy Fears, PYA 1G278, 6 Corporate Place, Piscataway, New Jersey 08854- 4157 (phone: 908-699-5656). Obtaining an HNI will require a US wireless license and likely a processing fee. Within a short time, version 1.0 of the US IMSI Guidelines will be published. It will differ from the current draft mostly in the assignment of the administrator.

For background, the HNI is composed of a US Mobile Country Code (MCC - 3 digits) and a 3 digit Mobile Network Code (MNC). Together, these codes will form the part of an IMSI that identifies the home system for a mobile. The remainder of the 15 digit IMSI identifies the specific mobile station. IMSI is defined in ITU-T standard E.212.

More details on the adoption of IMSI by the AMPS wireless industry are provided in the June, 1995 issue of Cellular Networking Perspectives. ❒

The IS-95 Standard for CDMA Digital Wireless Communication, Part II: Capabilities, Services and Options

Basic Capabilities

CDMA systems have to provide the basic capabilities of handoff, location management and terminal identification, but do it in a different way than other systems.

Handoff

Soft Handoff

Soft handoff allows a mobile to simultaneously communicate with up to 6 sectors. A mobile selects the best frame (of voice or data information) from each cell, allowing it to gradually make the transition from one cell to another. "Softer" handoff refers to communicating with multiple sectors within one cell.

Hard Handoff

A hard handoff, with mobile assistance, is possible at any time, but is required to handoff across a system boundary, from one 1.25 MHz channel to another, from a PCS channel to cellular or from CDMA to analog. The method used is similar to that used in IS-54 or IS-136 TDMA mobile assisted cellular.

Analog/CDMA Handoff

CDMA to analog handoff is possible but "you can never return". An analog to CDMA handoff is currently not possible.

Location Management/Registration

There are 50 ways to leave your lover according to Paul Simon's song and almost as many ways to trigger a registration in IS-95. All the registration triggers are configurable, and can be turned on or off by cellsite parameters. Some of the registration triggers were inherited from older standards…

SID

A mobile will register when it sees a new SID.

Power Up

A mobile can be made to register when it is turned on. This is logically required if Power Down deactivation of call delivery is implemented. This type of registration was first found in the IS-54 TDMA standard.

Power Down

A mobile can be made to register when it is turned off. This allows call delivery to be suppressed immediately, rather than by waiting to determine by timing that a mobile is inactive. This type of registration was first found in the IS-54 TDMA standard.

Other optional registration triggers are unique to IS-95…

Zone

Each cell is in a zone (with possibly several cells in one zone). A mobile will not register when entering a new zone if it remembers being in the zone recently. Zones are deleted from the mobile's internal list when the list overflows or when a zone timer expires.

Zone based registration can be used to resolve border cell problems, by allowing a mobile to be registered in two zones in border cells, but only one cell in the inner cells. This will reduce the rate of registration in border areas, allowing call delivery in the border area through IS-41 inter-system paging. Inter-system paging is eliminated in inner cells which specify that a mobile may only be registered in one zone and for mobiles that stay on one side of a border area for a long duration (by stopping inter-system paging once the zone timer expires).

NID

A mobile can be made to register when it enters a cell with a different Network ID. A NID can be considered as an extension to the SID.

Distance

A mobile can be made to register when it travels a certain distance, based on the latitude and longitude of the cell where the mobile last registered and the cell it is currently monitoring.

Time

A mobile can be made to register at a regular interval. This replaces the arcane REGID method of time based registration in analog and TDMA systems.

Mobile Identification

IS-95 Rev. 0 mobiles were identified by the traditional MIN (identifying a subscription) and ESN (identifying a terminal). Revision A extended the mobile identification from a 10 digit MIN to the 15 digit IMSI (International Mobile Station Identity). The advantage of IMSI over MIN is that it identifies the home country for a phone, unlike a MIN where the home country has to be guessed at. In the IS-95 implementation of IMSI, unlike IS-136 TDMA, the IMSI is composed of a new 5 digit prefix followed by the MIN. This makes a gradual transition to a non-MIN based IMSI more awkward in IS-95 than IS-136. However, the network implementation of IMSI for IS-95 phones is simpler, as the MIN is always available.

J-STD-008 and IS-95 Rev. B mobiles may also be identified by a TMSI (Temporary Mobile Station Identity) which is a more efficient (i.e. smaller) identifier than either MIN or IMSI and provides a degree of privacy by hiding the real identity of the phone. The use of TMSI will reduce fraud, by reducing the availability of MIN and ESN information to wannabe cloners.

Services and Features

Service Options

The IS-95 family of CDMA standards is built around the concept of service options. A service option is simply a package of capabilities that can optionally be built into a phone, and that are defined by a separate public standard or by a private agreement. Service options that have been defined or that are currently being developed include:

- IS-96-A Basic variable rate voice coder (9600 bps).
- Enhanced variable rate voice coder (EVRC, also 9600 bps).
- 14.4 kbps voice coder (CDG recommendation).
- Asynchronous data and group III fax (9600 bps).
- 14.4 kbps asynchronous data and group III fax.
- Point-to-point short message service.
- Broadcast short message service (to all mobiles in a cell, or a selected subgroup of mobiles).
- Packet data (similar in concept to CDPD).
- Traffic Channel Test (both the IS-126 loopback test, and a non-standard statistical channel quality test have been defined).
- STU-III for highly secure voice, used by several US government agencies.

Other Features

The following features are not service options, but provide additional capabilities in other ways:

- Service redirection.

  This allows a mobile to be redirected from one frequency band to another, if there is a business reason for doing so. The entire implementation of this feature (including the network portion) is known as Network Directed System Selection (NDSS).

- Over-the-air activation (OTA).

  A mobile may be programmed, or re-programmed using the radio interface. Through complex encryption algorithms for mutual network/mobile authentication, it is believed that this can be done securely, even though authentication information, such as the A-Key, must be transmitted over the air interface.

Data

Digital wireless standards have a problem with transmitting data over modems because modem tones do not pass through the voice coders that are optimized to compress human utterances. This is ironic, because the intent by both the user and the modem is to transmit digital information. The solution is to provide a way to eliminate the voice coders when in data mode and to connect an interworking function to perform the digital to modem tone conversion.

An additional problem with the transmission of data involving modems occurs when an inter-system handoff is performed. If a new modem was allocated in the new MSC, a regular trunk between the Anchor and Serving MSCs could be used to transmit the voice frequency tones. However, this is not possible due to the nature of modems. Consequently, a new protocol needs to be developed that will use the raw bits on the inter-system trunk (usually a 56 or 64 kbps DS0) to transmit the data. The only problem to overcome is to ensure that the same bits are taken out as are put in, as there are several times more bits in a DS0 than can be transmitted over the radio interface. This protocol is known as ISLP (Intersystem Link Protocol).

A radio interface data standard has been produced by subcommittee TR-45.5 (IS-99, published in July, 1995). A subcommittee TR-45.2 ad hoc group on data is currently defining network requirements for the transmission of data from CDMA (and TDMA) phones (including the ISLP and modifications to IS-41 messages). Their conclusions will be published in IS-41 Rev. D.

Short Message Service

Short message service can be considered a restricted data service, with the big advantage that it can be provided to a regular cellular phone without a hookup to a fax machine or computer. With this application in mind, the CDMA short message service allows an alphanumeric message (using the ASCII or the NAMPS 6 bit character set) to be transmitted to a phone, that will display it to the user. Messages can be up to about 250 characters long. It is possible to generate a message from a phone, but that is unlikely in practice because of the primitive keyboard on cellular phones that makes typing letters a pain at best.

Broadcast short message service allows one message to be sent simultaneously to groups of mobiles in a cell. Some filtering of messages can be done, to allow only sub-groups of mobiles to process each message.

Authentication

The TIA CAVE algorithm is used as a method for CDMA systems to be sure that a phone is not a clone. CAVE authentication, which is applicable to analog and TDMA as well, is described in the December, 1995 and January, 1996 issues of *Cellular Networking Perspectives.*

Privacy

A number of methods are provided for enhancing the privacy of people using CDMA phones:

Public Long Code Mask

All voice traffic is encoded by the public long code mask, based on the ESN. This provides a minimal amount of privacy from scanners.

Private Long Code Mask

Voice encryption can be used as a byproduct of inclusion of the CAVE authentication algorithm (see above). This algorithm is moderately strong, vastly stronger than an unprotected analog cellular transmission, although not as strong as the STU-III encryption used by some US government agencies.

Signaling Message Encryption

Certain fields (I could tell you which ones, but then I would have to shoot you) of signaling messages are encrypted with the CAVE algorithm to enhance the security of the system, and also privacy of sensitive user data.

TMSI

An IS-95 system can assign a mobile a Temporary Mobile Station Identity, that will disguise the true identity of the mobile. A potential cloner would have to capture the TMSI assignment transaction to associate the TMSI with the MIN or IMSI. While this is certainly possible, the TMSI assignment hides the true identity most of the time.

The IS-95 version of TMSI is more

sophisticated than that used in IS-136, and consequently requires more network support. An IS-95 TMSI may be valid across system boundaries, and therefore requires new VLR-to-VLR IS-41 transactions to be defined (as in GSM), to associate the TMSI with the MIN or IMSI over the network. These transactions will be included in IS-41 Revision D. For systems that do not support these transactions, a TMSI reassignment would be necessary, which reduces the security benefit of TMSI.

Data encryption

A data encryption standard known as ORYX is being developed by the TIA TR-45 Ad-Hoc Authentication Group (AHAG). The voice encryption standard defined in CAVE cannot be used because it is based on a fixed encryption mask, which is not secure with data, which often contains long stretches of repeated zeros that would reveal the mask. The ORYX algorithm uses a rotating mask (i.e. the string of bits that is exclusive-ored with the data changes with every frame).

Standards

The CDMA system discussed in this article is defined by TIA (Telecommunications Industry Association) interim standards, most notably IS-95 and J-STD-008. A complete list of standards related to various aspects of CDMA cellular and PCS systems is found on page 6.

IS-95-B Enhancements

Several items are being considered for inclusion in IS-53 Revision B:

- Enhanced Over-the-Air Activation for dual band enhanced roaming.
- Incorporation of TSB-74 (permitting 14.4 kbps data and voice). The provision of a raw bit rate of 14.4 kbps, will allow higher speed data and higher quality voice.
- Priority Access and Channel Assignment (PACA)

  This feature allows terminals to be queued in priority order when all traffic channels are in use. This is particularly oriented to emergency situations, when cellular systems often experience much higher loading than normal. There may be up to 15 levels of priority, assigned based on the caller's profile or dialed digits (e.g. 9-1-1).
- Calling Name Presentation

  The name of the calling party may be displayed, instead of just the number.
- PCS (incorporating J-STD-008)

  Operation in the PCS frequency bands will be added, allowing terminals to roam and handoff freely between cellular and PCS frequencies.
- Simultaneous voice and data.
- Technical Corrections

  Not even the best get it quite right the first time!

CDG

The CDMA Development Group (CDG) is a group of companies that are committed to the development of CDMA equipment, or provision of CDMA service (see sidebar listing CDG member companies). Their charter is to be:

> "committed to the definition of CDMA features, services, technical requirements and other activities that promote the availability of CDMA (IS-95 based) cellular and (J-STD-008) PCS systems worldwide. The group shall work toward the goal of securing early and complete interoperability between and among systems."

For more information on the CDG, consult their Web page, which can be reached, along with related links, at http://www.cnp-wireless.com/cnp-wireless.

Summary

CDMA systems are going to have an enormous impact on future wireless communications. Whether the time is yet ripe for them to overthrow TDMA systems for the digital crown has not been decided. In cellular, TDMA has a significant edge, but in PCS systems the commitment is clearly towards CDMA.

We hope that in these two issues, we have hoped to clarify how this important technology fits into a cellular or PCS network. As always, we welcome your comments.

Acknowledgements

I would like to acknowledge the assistance of Dr. Edward Tiedemann, Alejandro Holcman and Sam Broyles, all of Qualcomm. ❒

Table 1: The CDG Companies

Business	Category	Company
Carrier	USA	AirTouch
		ALLTEL
		Ameritech
		Bell Atlantic
		NYNEX
		Comcast
		GTE
		NextWave
		PCS PrimeCo.
		Sprint Cellular
		Sprint Spectrum
		(STV)
		US Cellular
		US West
	International	Shinsegi
Manufacturer	Network Equipment	Lucent
		Motorola
		Nortel
		Qualcomm
		Samsung
	Terminals	Alpine
		AT&T
		Audiovox
		Fujitsu
		Goldstar
		Hyundai
		Maxon
		Motorola
		NEC America
		OKI
		Qualcomm
		Sony
	Test Equipment	Comarco
		Hewlett Packard
		LCC
		SAFCO
		Tektronix
		Wavetek
	Other	Telecommunications
		Allen Telecom
		Celcore
		Comsearch
		ETRI
		Gemplus
		Internet Mobility
		Primary Access
		Texas Instruments
		Voice Processing

Information courtesy CDMA Development Group

TR-45.2 Standards Update

The status of each major outstanding TR–45.2 project is listed below, in approximate order of completion:

In Press

Cellular Dialing Plan (IS-52 Rev. A, ANSI/TIA/EIA-660)
- IS-52 Rev. A is in press, with minor modifications, as ANSI/TIA/EIA standard 660.

Subscriber Features (IS-53 Rev. A, ANSI/TIA/EIA-664)
- IS-53 Rev. A is in press, with no changes, as ANSI/TIA/EIA standard 664.

IS-41 Revision C (SP-3588)
- In press as a TIA interim standard. Approved for ANSI ballot as Standards Proposal SP-3588.

Nearing Completion

PCS Multi-band (TSB-XX, PN-3624)
- This TSB will define 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. Approved for ballot in February, 1996.

Online Call Record Transfer (IS-124 Rev. A, PN-3293)
- Currently in V&V (Verification & Validation), with ballot scheduled for April, 1996. Rev. A includes a variety of improvements and corrections over Rev. 0, including internationalization. Not included are major changes to support intelligent network peripherals and data. These will be incorporated in a subsequent TSB or IS-124 Rev. B.

International Applications (TSB–29 Rev. B, PN-3173)
- TR–45.2 WG VI approved a section on global title translation at its February, 1996 meeting. A section on TCAP may be added at the March, 1996 meeting. V&V is scheduled to start at this meeting, followed by TIA letter ballot.

Subscriber Features (IS-53 Rev. B, PN-3362)
- A number of new features, including asynchronous data and fax (ADS), calling name presentation, enhanced emergency service (E9-1-1), incoming call screening (ICS), network directed system selection (NDSS), non-public service, over-the-air activation (OTA), speech option selection (SOS), user-group id (UGID) and voice controlled services. Scheduled for ballot in June, 1996.

In Development

Inter-System Link Protocol (ISLP) (PN-3660)
- A new inter-MSC protocol is required to support the transmission of data from digital phones following an inter-system handoff. It is scheduled for ballot as an interim standard starting July, 1996.

Emergency Services (PN–3581)
- Liaison with the CTIA, NENA, NASNA and APCO is underway to define the requirements for emergency services. Scheduled for ballot in July 1996 as a separate TSB or Interim Standard, or possibly for inclusion in IS-41 Rev. D and IS-93 Rev. A.

TDMA DCCH (PN-3579)
- Definition of network support for new features inherent in the IS-136 digital control channel (IS-136). Scheduled for incorporation in IS-41 Rev. D.

CDMA Capabilities (PN-3619)
- The definition of features based on IS–95 Rev. A capabilities. Scheduled for incorporation in IS-41-D.

Data Services (no PN)
- CDMA and TDMA digital cellular phones cannot currently transmit data because voice coders are incompatible with analog modem tones. Solutions are being developed for inclusion in IS-41-D.

IS-41 Rev. D
- Task groups, working on the projects listed above, are developing text for each of the capabilities in IS-41 Rev. D. This revision will include IS-53-B features and non-feature capabilities, such as IMSI. The ballot is currently scheduled for August, 1996. Some task group work may be released prior to publication of IS-41-D.

Law Enforcement Intercept (PN–3580)
- Law enforcement requirements are intended to be met by a new standard that was scheduled for ballot in May, 1996. However, that date was recently slipped to August, 1996 to allow for harmonization with the official statement of law enforcement requirements due in the TILU Electronic Surveillance Interface document, scheduled for release at the end of February, 1996.

WIN: Wireless Intelligent Network (PN-3661)
- An ad hoc group, meeting outside TIA TR-45.2 subcommittee meetings, is developing a call model and IS-41 procedures to support WIN features. Currently, target features include Incoming Call Screening, Voice Controlled Services and Calling Name Presentation. Scheduled for ballot in June 1996, but don't hold your breath.

On Hold

Multiple HLR Queries (PN-3528)
- On hold due to a relatively low priority, due to rejection by Mexican carriers as the solution to their international roaming problems.

Interconnection (IS-93 Rev. A, PN-3295)
- On hold. No changes have yet been identified to IS-93 Rev. 0. ❒

Surfing the NET??

Visit *Cellular Networking Perspectives* at our EXCITING NEW web page at:
http://www.cadvision.com/cnp-wireless

Test your knowledge and have some FUN!

Take our quiz...

TIA TR-45.5 CDMA Digital Air Interface Standards

Cellular Networking Perspectives

Editor David Crowe • Phone: 1-800-633-5514 • Fax: 403-289-6658 *Last Published 02/95*

CDMA Digital Air Interface Standards - First Generation (Cellular)

IS- / TSB-	Description	Status
IS-95	CDMA Dual-Mode Air Interface Standard	Published 07/93
IS-96	CDMA Option 1: Voice Coder	Published 04/94
IS-97	Base Station minimum performance standards	Published 12/94
IS-98	Mobile minimum performance standards	Published 12/94
IS-126	Option 2: Loopback	Published 12/94
TSB-66	Technical Corrections to IS-95	Closed, see IS-95-A

CDMA Digital Air Interface Standards - Second Generation (Cellular & PCS)

Identity	PN #	Description	Status
IS-95-A	***published***	**IS-95 Revised**	**Published 05/95**
IS-96-A	***published***	**CDMA Voice Coder**	**Published 05/95**
IS-99	***published***	**Data Services (Fax and Circuit Switched Data)**	**Published 07/95**
IS-125	***published***	**Voice coder performance standards**	**Published 05/95**
IS-637	**PN-3423**	**Short message service**	**In Press**
IS-687	**PN-3473**	**Data interworking function**	**Ballot**
J-STD-008	**PN-3384**	**IS-95 adapted for 1800 MHz frequency band**	**In press**
J-STD-018	**PN-3385**	**Mobile minimum performance standards (for J-STD-008)**	**Ballot**
J-STD-019	**PN-3383**	**Base station minimum performance standards**	**Ballot**
TSB-58	**PN-3139**	**Administration of parameter value assignments**	**In Press**

CDMA Digital Air Interface Standards - Third Generation (Cellular & PCS)

Identity	PN #	Description	Status
IS-95-B	***pending***	**IS-95 for 800 MHz and 1800 MHz frequencies (including J-STD-008)**	**Development**
IS-96-B	**PN-3649**	**CDMA voice coder (8 kbps)**	**Development**
IS-97-A	**PN-3645**	**Base Station minimum performance standards (including J-STD-019)**	**V&V**
IS-98-A	**PN-3647**	**Mobile minimum performance standards (including J-STD-018)**	**V&V**
IS-126-A	**PN-3646**	**Service Option 2: traffic channel loopback test capability**	**Ballot**
IS-127	PN-3292	Option 3: enhanced variable rate voice coder (EVRC)	Development
IS-657	PN-3472	Packet data services	Ballot
IS-STU	**PN-3571**	**STU-III (strong voice encryption)**	**Development**
IS-XXX	**PN-3648**	**Minimum performance standards for EVRC voice coder**	**Development**
TSB-74	**PN-3570**	**14.4 kbps radio link protocol and inter-band operations**	**In Press**
TSB-DATA	***pending***	**14.4 kbps option for data**	**Development**
PN-xxxx	**PN-xxxx**	**14.4 kbps data services**	**Development**
IS-xxx	**PN-xxxx**	**Minimum performance standards for TSB-74 voice coder**	**Development**

Note:
1. IS- Interim Standard, J-STD- TIA/ATIS Joint Technical Committe standard, PN- Project Number, SP- ANSI Standards Proposal, TSB- Telecommunications Systems Bulletin.
2. Bold Type indicates modification since the previous publication of this report.
3. The same authentication standards are used in analog and TDMA systems. For details, see the January, 1996 issue of Cellular Networking Perspectives (page 6).