Cellular Networking Perspectives

Editor David Crowe • Phone 403-289-6609 • Fax 403-289-6658 Vol. 4, No. 10 October, 1995

In This Issue ...

Next issue due: Nov. 1, 1995

A T-Shirt for a Tip!

We are pleased to offer a unique *Cellular Networking Perspectives* T-Shirt for any tips that lead to a paid subscription. Just give us contact information for your prospects and you will soon be the proud owner of one of our unbleached, recycled cotton shirts. You can contact us at 1-800-633-5514, by fax at +1-403-289-6658 or email at 71574.3157@compuserve.com.◊

North America Now Joined to Asia

North America and Asia have been joined by a thin but powerful connection, that will allow automatic intercontinental roaming with an AMPS cellular phone. The North American Cellular Network (NACN) now has a connection to Hong Kong to allow automatic call delivery, validation and transfer of profile using the TIA IS-41 Revision A and Revision B standards. There are no plans to support inter-system handoff across the Pacific Ocean.

The NACN already directly connects 75 cellular carriers and 14 million cellular customers in the USA, Canada and Mexico. Through connection to 5 other IS–41 signaling networks the NACN can route signaling traffic to most other North American cellular customers. The Hong Kong system will soon be acting as a gateway for other AMPS systems in Asia and Australasia (likely connections include Malaysia, Singapore, Indonesia, New Zealand and Australia). The NACN has also expanded into Mexico and, along with other signaling networks will be expanding further into South and Central America.

There is only one small problem: the NACN is going to have to change its name!◊

Comments Welcome

We welcome comments on the contents and format of this newsletter, suggestions for future topics, letters, submissions and corrections.

Yet More Wireless Features: TIA IS-53 Revision B

IS-53 Revision B, to be published in 1996, defines the third generation of AMPS cellular features, which can also be provided in PCS systems based on the AMPS family of air interfaces (NAMPS, TDMA, CDMA or even just plain analog). While some of these features can already be provided by terminals or locally within a home network, it is the job of IS-53 to define features so that they can be used seamlessly wherever in the network a subscriber roams. IS-41 completes this job by defining an inter-system protocol to allow seamless implementation. While it is dangerous to report the final list of ingredients in a standard before it comes out of the oven, we feel confident that only the following new features will be present when IS-53 Revision B is published:

a. Enhanced emergency service

   Improved service when 9-1-1 is dialed, including reporting of location, subscriber name and address and a callback number to the public service answering point (PSAP).

b. Circuit switched data and Group III fax for digital cellular terminals

   The capability to originate, receive and handoff circuit switched data and fax calls from digital cellular terminals to analog fax or data modems. The need for special handling in digital cellular (which is not required for analog cellular) stems from the use of voice coders which, not surprisingly, are optimized for voice and a low bit rate. This causes the voice coder to distort modem tones. Network requirements for this

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

feature include different alternatives for terminating an incoming call in data or voice mode because the PSTN does not know the difference (such as separate directory numbers for voice and data, but one MIN), providing inter-system transport of data after handoff and interworking between the TIA IS–130 format of the data and what is expected on the digital side of the necessary pool of landline modems.

Data privacy will also be supported, using a different algorithm than currently used for voice privacy.

c. Over-the-air activation

This feature allows semi-automatic programming or reprogramming of a wireless terminal by a carrier using the radio interface. The process will be initiated by a phone user dialing a special number, providing the necessary personal identification and credit information, and then letting the system download a profile into the phone, including MIN or IMSI, home SID, authentication parameters and possibly even preprogrammed phone numbers in memory locations.

d. Voice controlled services (a WIN feature)

This feature will connect all calls by subscribers to a voice recognition device to allow dialing and control of features. This feature is part of the CTIA Wireless Intelligent Network (WIN) initiative, which is intended to offload feature intelligence from MSCs and HLRs to intelligent peripherals, known as SCPs, IPs and SNs.

e. Incoming call screening (a WIN feature)

Incoming calls may be screened in a variety of ways, based on the calling number, a recorded plea by the caller or other information. Handling may be modified by time of day or the status of the subscriber's terminal.

f. Calling *name* presentation (a WIN feature)

The *name* of the calling party may be displayed on a cellular or PCS phone. The presentation of the name may give the called mobile subscriber a chance to manually screen incoming calls.

g. Identity confidentiality

A mobile may access services without revealing its MIN, ESN or IMSI identities. This will utilize air interface Temporary Mobile Station Identifiers (TMSI) to provide greater anonymity to subscribers and reduce cloning fraud.

h. Advanced digital features

Support for advanced IS–136 and IS–95 Rev. A capabilities, such as sleep mode to increase standby time for mobiles, support for private and residential systems, user groups and selection of alternate voice coders.

i. IMSI

The use of the ITU-T (formerly CCITT) Recommendation E.212 International Mobile Station Identifier (IMSI) will resolve many problems with international roaming, and simplify interworking with GSM networks. During the long transition to IMSI, terminals must be supported with only a MIN, only an IMSI, independent MIN and IMSI and also those with IMSI defined as an extension to the MIN.

j. PCS Operation and Interworking

Features should, in general, operate the same way in PCS as in cellular. Also, dual-band PCS/Cellular phones should be able to choose the best local serving system in either band and even handoff from a cellular channel to a PCS channel, or vice-versa.

Observant readers of our March, 1995 issue may note that two features have disappeared. Group broadcast (multicast) of short messages has been eliminated due to a lack of contributions and Lawfully Authorized Electronic Surveillance ("wireless wiretap") will be described in a separate document as an attempt to monitor the dissemination of information about this subject.

Features described in IS-53 Rev. B will be supported for inter-system operations in TIA IS-41 Revision D and possibly other TIA standards and TSBs.◊

Fraud and Countermeasures, Part I: The Land Before Clones

Fraud has been one of the cellular industry's biggest problems for several years. Not only is it costly, but both the fraud and some countermeasures annoy customers, and it consumes immense amounts of time and energy from carrier employees who have another 'real' job to do. The cost of fraud in the United States alone was long estimated at $1,000,000 per day, but is now at about $500,000,000 per year, well on its way to $2,000,000 per day.

In the first part of this article, we will describe fraud and fraud prevention before the advent of cloning. Part II will discuss cloning and many of the countermeasures. Part III will focus on authentication, described by Roseanna DeMaria, Vice-President of Revenue Security at AT&T Wireless Services (McCaw) as "the nuclear weapon of fraud control".

Why Fraud?

It might seem obvious that criminals steal cellular phone service for the value of the service. But this is only one of two major reasons…the other is anonymity. Cellular phone fraud is usually accomplished through theft of an identity, or use of an invalid identity. In either case the caller cannot be identified from the transmitted mobile identification. This accounts for the huge amount of fraud from criminals, such as drug dealers, who could easily afford to pay for the service, but see cellular phone fraud as a convenient, anonymous way to plan their illegal activities. Getting the service for free, is just an incidental bonus.

Amongst those who steal phone service for its value, there are several different motivations:

- Personal use

  Some people use a fraud-phone simply in order to be able to make unlimited calls for free.

- Call sell operations

  Fraudulent cellular phones are often used in portable operations that sell stolen long distance service at reduced rates. Criminals prefer the convenience and mobility of cellular

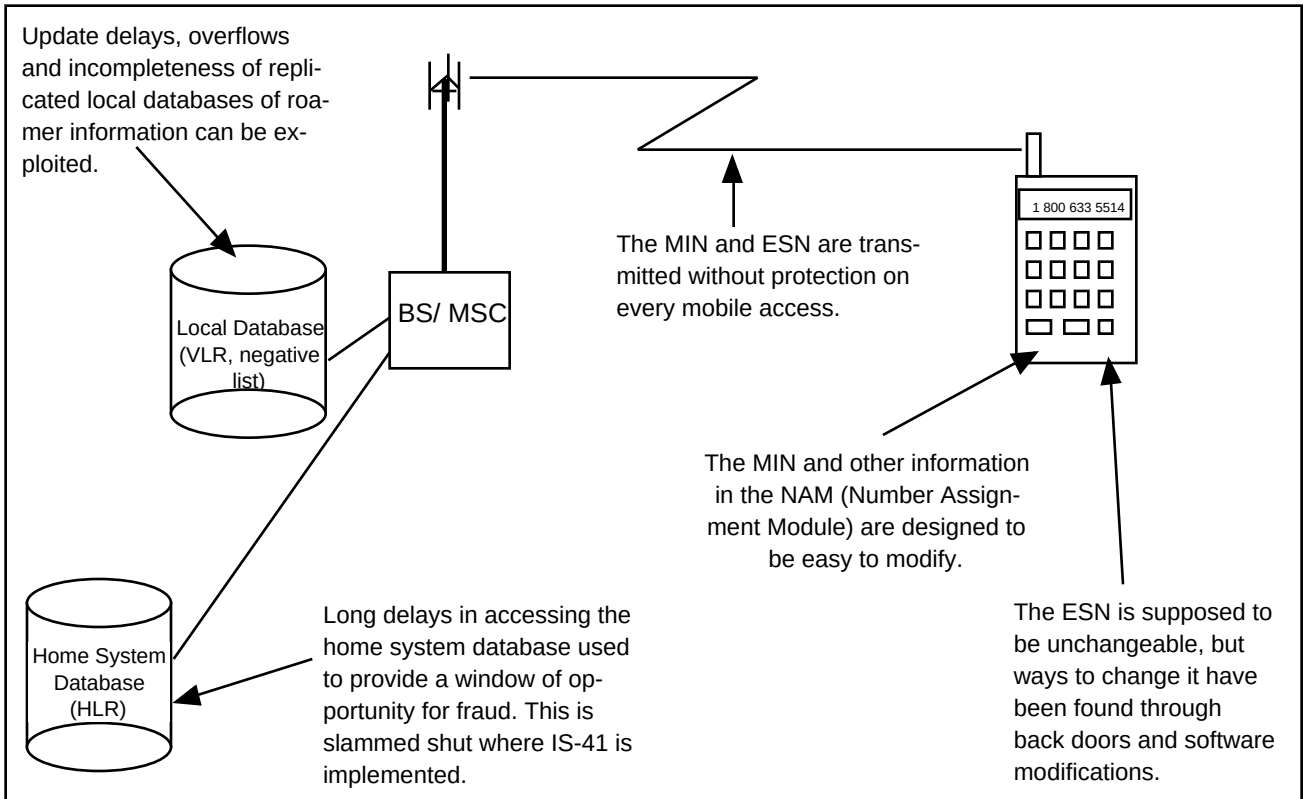

Figure 1: Points of Fraud Attack in Cellular Systems

phones over pay phones.

- Country to Country

  A sophisticated variation on call sell operations is used to bypass regulations that forbid phone communications between certain counties (e.g. Israel and Jordan). A three way call can be set up from a cellular phone in a motel somewhere in the USA to a phone in each of the countries.

Points of Attack

Criminals intent on defrauding cellular systems attack many different points in the network, as illustrated in Figure 1. The major targets have been the phone (to change the MIN and ESN), the radio interface (to pick up MINs and ESNs for cloning) and the signaling network (by using types of fraud that exploit weaknesses in the network).

Customer Impact

Apart from the direct financial impact of fraud on carriers, the most serious problem is on customer service. If a customer receives a huge bill due to fraud, even when the carrier writes off the bill, the customer is still unhappy, possibly angry, nervous and probably less likely to use their phone. Many countermeasures are also a problem, as they may inconvenience customers or deny them service. As examples, a PIN makes dialing longer and less convenient, pulling exchanges with high fraud denies many legitimate roamers service and authentication complicates initial phone setup. Everything that causes a customer service problem, reduces the legitimate usage on the system, changing the ratio of good usage versus fraudulent usage for the worse.

Fraud in Early Cellular Systems

The first cellular systems had almost no protection against fraud. Fraud by roamers would not be discovered until billing records were exchanged and the fraudulent caller discovered to have a MIN from a phone that was stolen, disconnected or never put into service. Fraud could be effected by stealing a phone or by reprogramming a phone with a different MIN.

Negative Lists

The simple types of fraud at first led to the development of a list of bad ESNs, based on the assumption that an ESN could not be changed, whereas a MIN could. Any ESN associated with fraud could be added to the home carrier's list, reported to all other carriers and then that phone would be useless for further fraud. This approach is still in use, but its effectiveness has diminished as fraudsmiths have found methods to modify the ESN, and negative lists are completely superseded by pre-call positive validation.

Positive Validation

It was recognized very early in the development of cellular that an industry-wide realtime validation network was required. Only when the MIN and ESN of a roamer are matched with a valid record in the home system can the serving system be sure of being reimbursed for the call (and the advent of cloning destroyed even that assurance, but that is a story for the next issue). In 1984, the Electronics Industry Association subcommittee TR-45.2 (now within the Telecommunications Industry Association) started development of the IS-41 standard to define inter-system operations for validation and also for handoff,

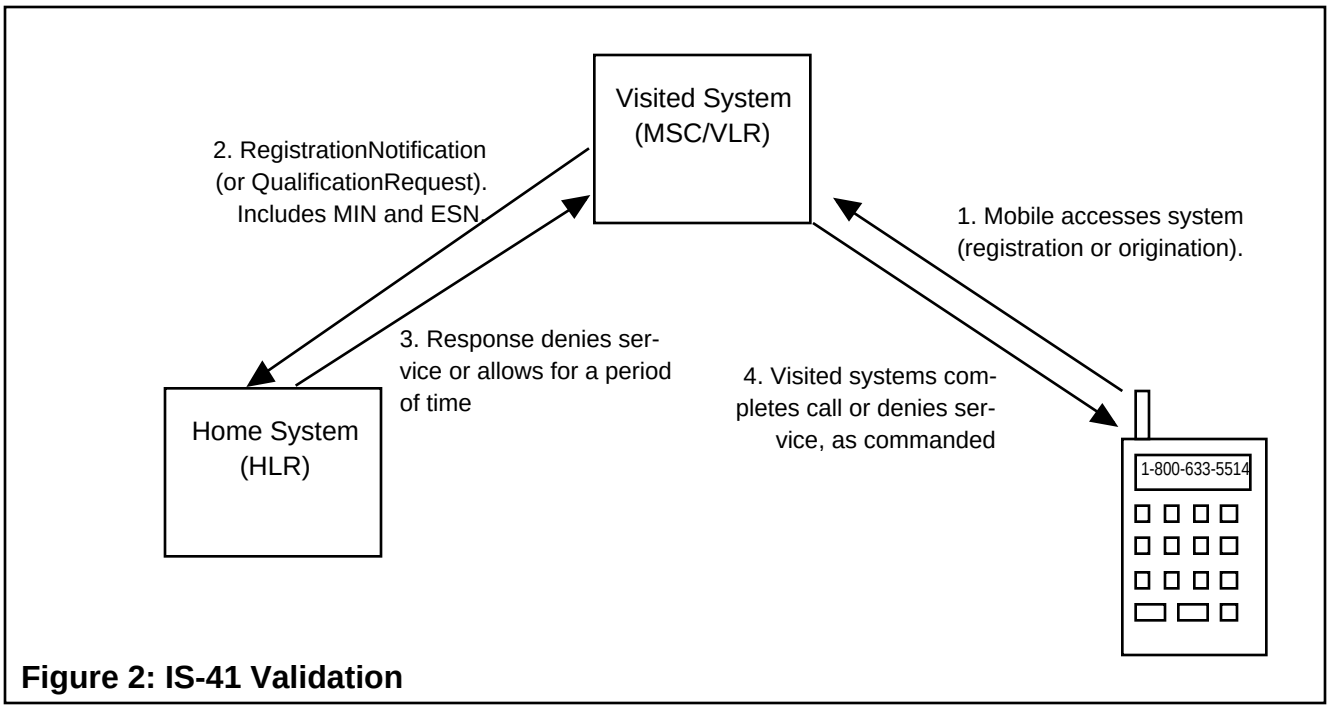

Figure 2: IS-41 Validation

call delivery and other services. Unfortunately, Revision 0 of this standard, published in 1987, did not address the networking issues of validation and it was not until the publication of Revision A in 1990 that a full standard solution for positive validation was available.

Post-Call Validation

Two companies recognized that in the absence of a standard solution, an interim solution would be a good business opportunity, although just for a short time. Appex (now EDS) and GTE TSI were right about it being a good business opportunity, but wrong about it being needed for just a short time, as their Positive Roamer Validation (PRV) and Positive Validation Service (PVS) are still in use today.

These systems were based on one fundamental assumption; *No Switch Changes*. Consequently, they monitored the call detail record output of the switch to determine the MIN and ESN of callers. Using a proprietary network they would route the information to the home system where the validation system would initiate a query of the home switch database (what would now be called the HLR) using man-machine interface commands. If the MIN/ESN combination proved valid, nothing further was done, but if it proved to be invalid, further man-machine commands would be executed at the serving system to take the fraudulent mobile out of service.

These systems lack of intrusiveness was their biggest strength and their biggest weakness. While they were quick to market, they could only react after the first fraudulent call was made (because they used the call detail record output, which is not available until the call is over) and queries would have to be queued for length periods, as man-machine interfaces were not designed for the required high throughput that computer to computer communications often demands.

The consequence of these deficiencies was that the first call with a fraudulent mobile was allowed, and then several more calls might be allowed depending on the length of time it took to determine that a MIN/ESN combination was invalid. In some cases this delay in validating was hours. However, with all the deficiencies of this method, it was vastly better than the other alternatives at the time.

Tumbling ESNs

The first serious threat from fraudulent mobiles that were modified to change their ESN was from ‘tumbling’ phones. These phones could set certain digits in the ESN to any value. If service was denied on one ESN, another could be chosen. This new ESN would not be in any negative lists and thus service would be allowed until post-call positive validation could complete. Smart users of tumbling phones could also re-enable an ESN by flooding the system with so many invalid ESNs that the local negative list would overflow.

Pre-Call Validation

Pre-call validation for roamers requires the TIA IS-41 standard (see Figure 2). Validation services came available in two steps. Revision 0 allowed validation only with a neighbouring system, while Revision A supported validation on a network. Revision 0 saw more use than might have been expected when GTE and EDS supported its use as an improved interface to their proprietary validation systems. Now, IS-41 Revision A is the dominant method of pre-call validation.

IS-41 validation works by sending a query, containing the caller’s MIN and ESN, to the HLR during call setup. The HLR immediately responds with the status of that MIN and ESN, allowing calls to proceed only with the permission of the home system. The validation information can be stored by the visited system for a time determined by the

HLR, to reduce the amount of network traffic.

IS-41 Revision B added no new functionality related to validation, although its use is increasing for other reasons. TIA TSB-51 added support for authentication to IS-41. IS-41 Revision C, scheduled for publication early in 1996, will support the PIN countermeasure.

Table 1: IS-41 Validation Transactions

Transaction	Purpose
RegistrationCancellation	Cancels registration and validation in received location.
RegistrationNotification	Validates mobile, as well as updating HLR location pointer
QualificationRequest	Validates mobile
ProfileRequest	Superseded by QualificationRequest
QualificationDirective	Allows HLR to update validation information for roamer at visited system

Table 1 lists the IS-41 transactions related to authentication.

Continued...

It took several years, but the advent of IS-41 has made it possible to eliminate all electronic fraud except cloning. Unfortunately, cloning is enough of a problem that the absence of others is cold comfort. In our next issue we will discuss cloning and many of the countermeasures against it.◊

TR-45.2 Standards Update: IS-41 Revision C is "this" Close

TIA subcommittee TR-45.2 has completed its initial review of all IS-41 Revision C ballot comments, and is now examining proposals to 'fix' problems noted in ballot discussions to which a general direction, but not specific text, has been agreed to.

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

Cellular Dialing Plan (IS-52 Rev. A, PN-3166) • ANSI ballot complete. Comments have been received by TR45.2, but not yet reviewed. No votes to disapprove were received.

Subscriber Features (IS-53 Rev. A, PN-2977) • ANSI ballot complete. Comments have not yet been received by the TR45.2 subcommittee.

IS-41 Revision C (PN-2991) • Ballot comments being reviewed (see introduction to this article for more detail). Approval for publication is hoped for in November, 1995.

International Applications (TSB–29 Rev. B, PN-3173) • TR–45.2 WG VI is studying the implementation of E.212 mobile identification, international SS7 global title translation requirements and other issues, for incorporation in TSB-29 Revision B, scheduled for ballot in March, 1996. The biggest issue is IS-41 compatibility, to migrate from MIN as an identifier to IMSI without breaking network elements that cannot yet support IMSI.

Multiple HLR Queries (PN-3528) • Development of a method for resolving ambiguous MINs using two or three queries to HLRs in different countries until a MIN/ESN match occurs. While this solution was rejected by Mexican carriers, it may be required elsewhere.

Online Call Record Transfer (IS-124 Rev. A, PN-3293) • TR–45.2 is accumulating modifications to the "DMH" standard for the online transfer of call records for billing, fraud and other purposes. Scheduled for publication in 2Q'96.

Subscriber Features (IS-53 Rev. B, PN-3362) • The features expected in this standard are listed in an article on page 1. Scheduled for publication in 2Q'96.

IS-41 Rev. D • Task groups, working on the projects listed below, 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 has been rescheduled for January, 1996, due to delays in the publication of IS-41 Rev. C. It is possible, as an alternative, that the task groups will first publish TSBs, with the TSBs being incorporated in a much delayed IS-41 Rev. D.

Interconnection (IS-93 Rev. A, PN-3295) • Balloting is scheduled to start in December, 1995, but no changes have yet been received. If changes occur, they will likely be in the area of enhanced 9-1-1 or IMSI support.

TDMA DCCH (PN-3579) • Work is ongoing on the definition of features based on IS-136 TDMA digital control channel capabilities. Scheduled for ballot in 1Q'96.

Law Enforcement Intercept (PN–3580) • The basic requirements and scenarios have been accepted as baseline. This capability is scheduled for ballot as a new standard, separate from IS-41 and IS-93 in 1Q'96.

Emergency Services (PN–3581) • The basic requirements have been agreed to and a definition of transactions and scenarios is underway. Major capabilities include location reporting, callback and reconnect (if a mobile disconnects during a 9-1-1 call). Scheduled for ballot in 1Q'96.

CDMA Capabilities (PN-3619) • The definition of features based on IS–95 Rev. A capabilities is ongoing. Scheduled for ballot in 1Q'96.

WIN: Wireless Intelligent Network (no PN) • The goal is to offload feature intelligence from switches and HLRs, but there are many divergent views on how to do this. Some estimate completion in 1997.

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 possible, but complex, especially in order to support inter-system roaming and handoff.◊