GSM Air Interface Security

David Burgess[1] Harald Welte[2]

[1]OpenBTS, Kestrel Signal Processing (USA)

[2]OpenBSC, hmw-consulting.de (Germany)

DeepSec conference, November 2009, Vienna/Austria

Introduction

Our Goals in this Workshop

- Familiarize you with the internals of GSM systems.
- Examine security weaknesses in GSM systems.
  - Theoretical weaknesses.
  - Demonstrations.
  - Products and practices.
- Describe countermeasures to avoid these weaknesses ...where possible.

About David A. Burgess

dburgess@kestrelsp.com

- Degrees in Electrical Engineering (BEE) and Computer Science (MSc).
- Signal processing experience: audio synthesis and simulation, radar, sonar and electronic warfare.
- First introduced to GSM in 1998 in SIGINT project.
- Provide software for fielded intelligence systems in use today.
- Started the OpenBTS project in mid-2007.

About Harald Welte

hwelte@hmw-consulting.de

- Using + playing with Linux since 1994
- Kernel, bootloader, driver, firmware development since 1999
- IT security specialist, focus on network protocol security
- Board-level Electrical Engineering
- Interested in various protocols (RFID, DECT, GSM)
- netfilter/iptables, OpenPCD, OpenMoko, librfid, OpenEZX
- Main developer of OpenBSC project

Legal Disclaimer

- We are demonstrating normal GSM operations and security flaws using a private network and informed participants.
- By leaving your GSM handset turned on during this workshop, you consent to participate in these demonstrations.
- Nothing we do will damage your handset, but you may suffer temporary disruptions in service, unsolicited text messages and other annoyances.
- Not all of the software used to demonstrate security weaknesses is not part of the normal OpenBTS or OpenBSC distributions.

Applicable Law – US

- 47 USC 302 and 18 USC 2512 ban distribution or advertisement of jammers or intercept devices to the general public, limits import and manufacture.
- 47 USC 333 bans interference with licensed operations.
- 18 USC 2511 bans unauthorized intercept of communications “not available to the public”.
- 47 USC 605 bans publication of intercepted content.

Applicable Law – US

US laws control “devices”. That normally means complete HW/SW systems. Whether or not these laws can be applied to pure software is probably an open question. We do not intend to become test cases. Another key phrase in some of these laws is “primary purpose”. User interfaces, default configurations, documentation and statements of intention are important in establishing “primary purpose”.

Applicable Law – EU

- Laws on jammers vary across Europe. Legal to own in some places, generally illegal to use but several countries make exceptions for jails.
- EMC Directive 2004/108/EC: Use of equipment. Not applicable for R&TTED devices
- R&TTED Directive 1999/5/EC: Declaration of Conformity sufficient, no strict need to invove certification lab
- 2000/299/EC: Classification of radio equipment – GSM900/GSM1800 equipment is "Class 1", can be redistributed all over Europe

Applicable Law – DE

- §317 StGB: Stoerung von Telekommunikationsanlagen
  - Causing interference with or deactivating public telecommunications networks
  - Punishable up to 5 years imprisonment
  - Even the attempt is punishable
- §202a StGB: Ausspaehen von Daten
  - Accessing data intended for other recipients and which are specially protected against unauthorized access
  - Punishable up to 3 years imprisonment
- §303a StGB: Datenveraenderung
  - Unauthorized deletion, modification or suppression of data
  - Punishable up to 2 years imprisonment
  - Even the attempt is punishable
- §149 (1) Satz 10 TKG: Bussgeldvorschriften
  - Transmitting without an apropriate license
  - penalty of up to EUR 1,500 plus EUR 600/900

Information Sources

- All information presented here is available form public sources
- Most of the information presented here is readily derived from public specifications, *if you actually take the time to read them*
- Nothing presented here is subject to trade secret restrictions
- Nothing presented here was received under a government security clearance agreement

Outline of Part I

Outline of Part II

Outline of Part III

Outline of Part IV

Outline of Part V

Outline of Part VI

GSM/3G protocol level security

- Observation
  - Both GSM/3G and TCP/IP protocol specs are publicly available
  - The Internet protocol stack (Ethernet/Wifi/TCP/IP) receives lots of scrutiny
  - GSM networks are as widely deployed as the Internet
  - Yet, GSM/3G protocols receive no such scrutiny!
- There are reasons for that:
  - GSM industry is extremely closed (and closed-minded)
  - Only about 4 closed-source protocol stack implementations
  - GSM chipset makers never release any hardware documentation

The closed GSM industry

Handset manufacturing side

- Only very few companies build GSM/3.5G baseband chips today
  - Those companies buy the operating system kernel and the protocol stack from third parties
- Only very few handset makers are large enough to become a customer
  - Even they only get limited access to hardware documentation
  - Even they never really get access to the firmware source

The closed GSM industry

Network manufacturing side

- Only very few companies build GSM network equipment
  - Basically only Ericsson, Nokia-Siemens, Alcatel-Lucent and Huawei
  - Exception: Small equipment manufacturers for picocell / nanocell / femtocells / measurement devices and law enforcement equipment
- Only operators buy equipment from them
- Since the quantities are low, the prices are extremely high
  - e.g. for a BTS, easily 10-40k EUR

The closed GSM industry
Operator side

- Operators are mainly banks today
- Typical operator outsources
  - Billing
  - Network planning / deployment / servicing
- Operator just knows the closed equipment as shipped by manufacturer
- Very few people at an operator have knowledge of the protocol beyond what's needed for operations and maintenance

The closed GSM industry
Security implications

The security implications of the closed GSM industry are:

- Almost no people who have detailed technical knowledge outside the protocol stack or GSM network equipment manufacturers
- No independent research on protocol-level security
  - If there's security research at all, then only theoretical (like the A5/2 and A5/1 cryptanalysis)
  - Or on application level (e.g. mobile malware)
- No open source protocol implementations
  - which are key for making more people learn about the protocols
  - which enable quick prototyping/testing by modifying existing code

Security analysis of GSM

How would you get started?

If you were to start with GSM protocol level security analysis, where and how would you start?

- On the handset side?
  - Difficult since GSM firmware and protocol stacks are closed and proprietary
  - Even if you want to write your own protocol stack, the layer 1 hardware and signal processing is closed and undocumented, too
  - Known attempts
    - The TSM30 project as part of the THC GSM project
    - mados, an alternative OS for Nokia DTC3 phones
  - none of those projects successful so far

Security analysis of GSM

How would you get started?

If you were to start with GSM protocol level security analysis, where and how would you start?

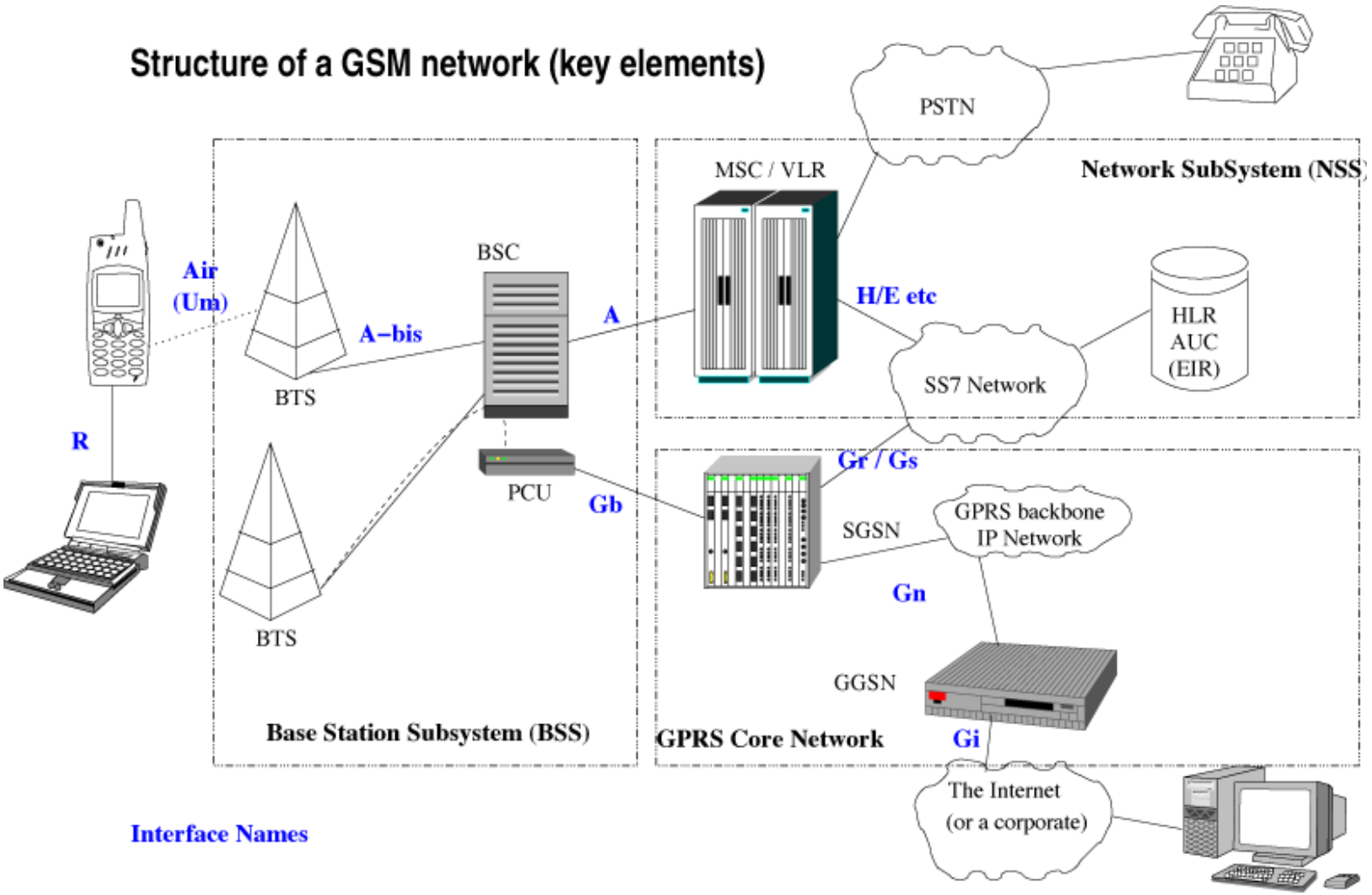
- On the network side?
  - Difficult since equipment is not easily available and normally extremely expensive
  - However, network is very modular and has many standardized/documented interfaces
  - Thus, if equipment is available, much easier/faster progress
  - Also, using SDR (software defined radio) approach, special-purpose / closed hardware can be avoided

Security analysis of GSM
The bootstrapping process

- Read GSM specs day and night (> 1000 PDF documents)
- Gradually grow knowledge about the protocols
  - OpenBSC: Obtain actual GSM network equipment (BTS)
  - OpenBTS: Develop SDR based GSM Um Layer 1
- Try to get actual protocol traces as examples
- Start a complete protocol stack implementation from scratch
- Finally, go and play with GSM protocol security

Part I – The GSM network

The GSM network



GSM network components

- The BSS (Base Station Subsystem)
  - MS (Mobile Station): Your phone
  - BTS (Base Transceiver Station): The *cell tower*
  - BSC (Base Station Controller): Controlling up to hundreds of BTS
- The NSS (Network Sub System)
  - MSC (Mobile Switching Center): The central switch
  - HLR (Home Location Register): Database of subscribers
  - AUC (Authentication Center): Database of authentication keys
  - VLR (Visitor Location Register): For roaming users
  - EIR (Equipment Identity Register): To block stolen phones

GSM Network Structure

BTS Generates the actual radio interface. Mostly an L1/L2. Serves a single cell sector.

- **TRX** Transceiver inside a BTS, serves one physical channel (ARFCN)

BSC Manages radio resources and some mobility functions. Serves up to a few dozen BTSs in a “location area”.

MSC Actual call switching and top-level mobility functions. May serve dozens of location areas.

HLR (and VLR) The subscriber databases, routing databasses and authentication centers.

GSM network interfaces

Um Interface between MS and BTS
- the only interface that is specified over radio

A-bis Interface between BTS and BSC

A Interface between BSC and MSC

B Interface between MSC and other MSC

GSM networks are a prime example of an *asymmetric distributed* network, very different from the end-to-end transparent IP network.

Think ISDN (E1/T1), not 802.11

- Many computer networking people assume that cellular is similar to WiFi. It is NOT!
- Cellular interfaces are modeled after TDM trunk lines, not Ethernet
  - multiplexed L1 with dedicated channels
  - HDLC-style L2
  - ISDN-style L3
- Channel establishmend often takes *seconds*
- Bandwidth is a scarce resource
- Message source and destination not part of every packet but implicitly known based on TDMA assignment.

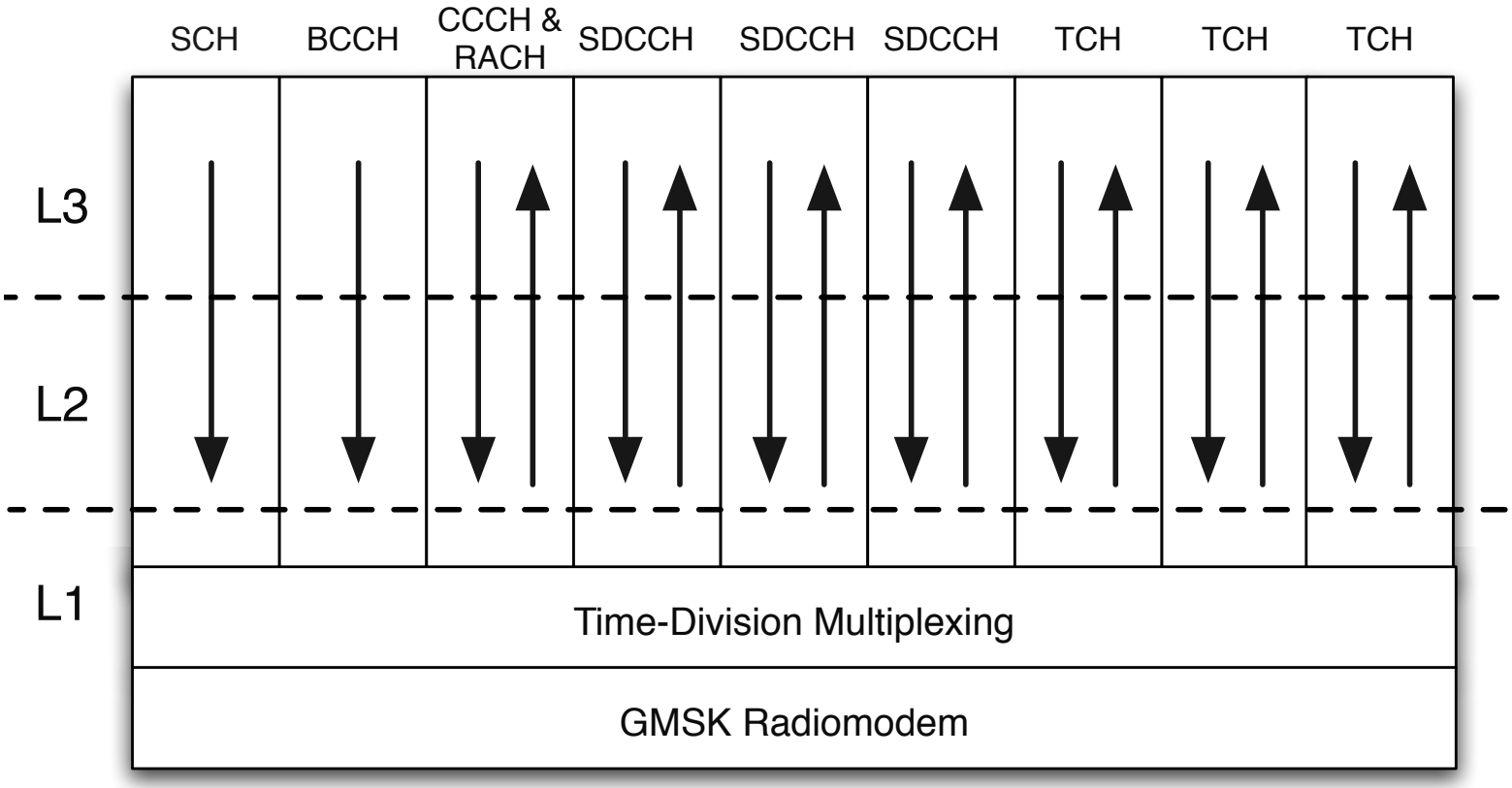
GSM Identity & Address Types

IMSI	15 digits, universally unique to the subscriber
TMSI	32 bits, assigned temporarily within a network
IMEI	15 digits, universally unique to the handset
MSISDN	a permanently-assigned E.164; the subscriber's phone number
MSRN	a temporary E.164 for routing to a mobile subscriber

Understanding Um
Overview

- Modeled after the U interface of ISDN
- Broadcast channels: SCH, BCCH, FCCH
- Common channels: CCCH (PCH & AGCH), RACH
- Dedicated Channels:
  - Dm SDCCH, FACCH, SACCH
  - Bm TCH/H, TCH/F

Understanding Um
Channels & Layers



Understanding Um
TDM Structure

- ARFCN (Absolute Radio Freq. Chan. Num.)– A 270,833 Hz radio channel. ARFCNs within a BTS numbered C0, C1, etc.
- 8 timeslots per frame on each ARFCN, numbered T0..T7.
- “physical channel” – one slot on one ARFCN, designated C0T0, C0T1, C1T5, etc.
- Physical channel TDM follows a 26- or 52-frame multiframe, carrying multiple logical channels.

Understanding Um –TDM Example

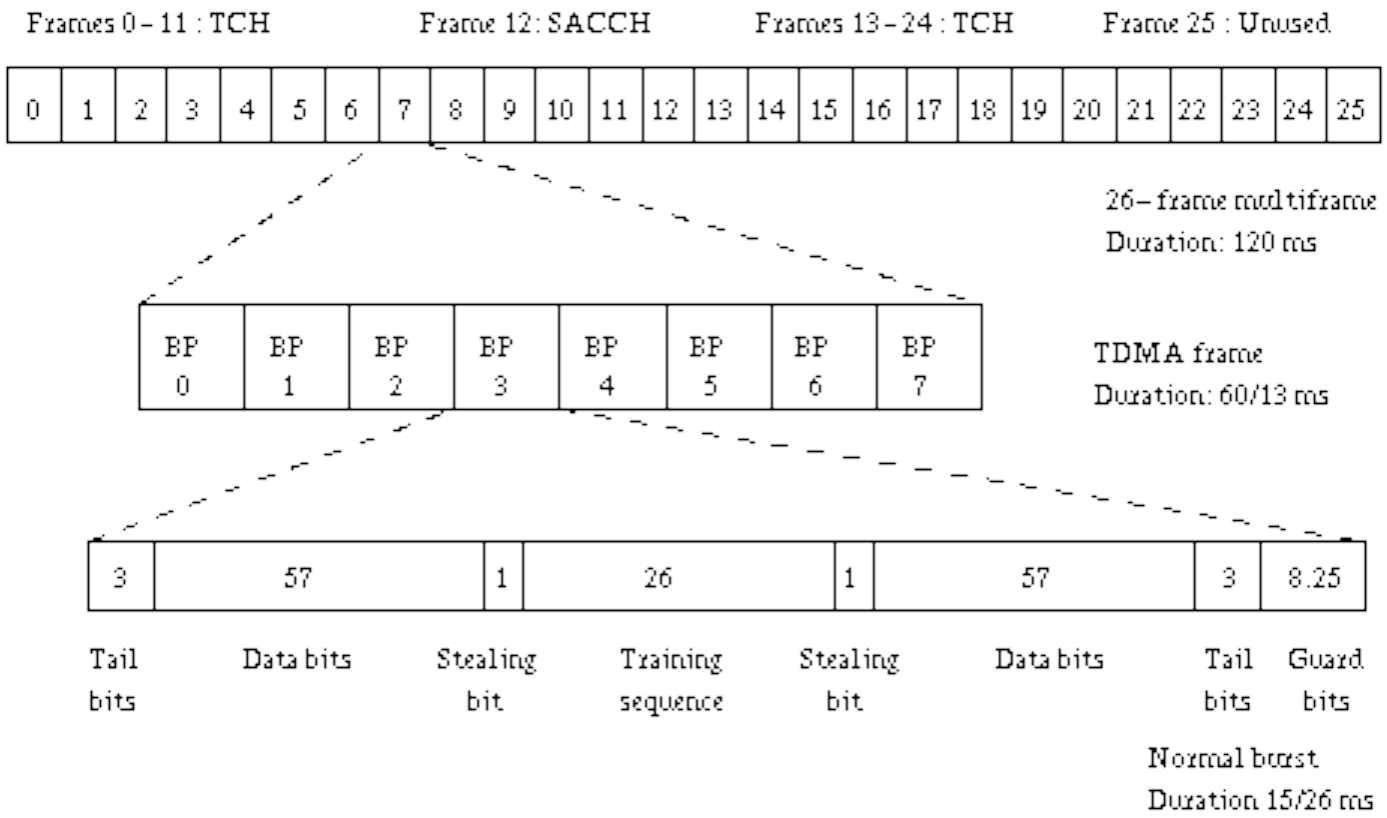


Figure: Example of traffic channel TDM

Understanding Um

The Beacon

The beacon is always on C0T0 and always constant full power

- SCH (Sync.) – TDM timing and reduced BTS identity
- FCCH (Freq. Corr.) – Fine frequency synchronization
- BCCH (Broadcast Control) – Cell configuration and neighbor list
- CCCH (Common Control) – a set of unicast channels
  - PCH paging channel for network-originated transactions
  - AGCH access grant channel
  - RACH uplink access request

Understanding Um
SCH – Synchronization CHannel

- First channel acquired by a handset
- T1, T2, T3' – TDM clocks for GSM frame number
- BCC – 3 bits, identifies BTS in the local group
- NCC – 3 bits, identifies network within a region
- BSIC is NCC:BCC

Understanding Um
BCCH – Broadcast Control CHannel

- Second channel acquired by the handset.
- A repeating cycle of system information messages.

  Type 1 ARFCN set
  Type 2 Neighbor list
  Type 3 Cell/Network identity, CCCH configuration
  Type 4 Network identity, cell selection parameters
  GPRS adds a few more (7, 9, 13, 16, 17)

Understanding Um
CCCH – Common Control CHannel

PCH Paging

- Unicast. Handsets addressed by IMSI or TMSI, never IMEI.
- Handset sees paging request and then requests service on RACH.

RACH Random Access

- Handset requests channel with RACH burst, 8-bit tag.

AGCH Access Grant

- BTS answers on AGCH, echoing tag and timestamp.

Understanding Um
Dm Channels

SDCCH Most heavily used control channel: registration, SMS transfers, call setup in many networks. Payload rate of 0.8 kb/s.

FACCH Blank and burst channel steals bandwidth from traffic. Used for in-call signaling, call setup in some networks. Payload rate up to 9.2 kb/s on TCH/F.

SACCH Low rate channel muxed onto every other logical channel type. Used for timing/power control, measurement reports and in-call SMS transfers.

Understanding Um

Bm Channels

- Full rate TCH/F 22.7 kb/s raw rate, occupies a full slot
- Half rate TCH/H 11.4 kb/s raw rate, 2 per slot using every other frame
- Payloads:

  Speech HR, FR, EFR, AMR

  Fax

  CSD Circuit Switched Data

Understanding Um – Connectivity and "Presence"

- A handset is connected to the network only when it is assigned to a dedicated channel, otherwise it is *IDLE* and listening passively to the beacon.
- Creation of a dedicated channel can take *several seconds*.
- The network can only guess the status of an idle handset based on the last transaction or transaction attempt, which may be several minutes old even under *the best* conditions.
- Even in a connected state, the signal between the handset and the network can disappear for several seconds at a time without resulting in loss of the channel.

Frequency Hopping

- Intended to improve radio performance through diversity in fading and interference
- Two ways to implement hopping
  - Baseband hopping: *N* fixed-frequency transceivers are connected to *N* baseband processors through a switch or commutator. Allows CA of *N* ARFCNs. C0 can be in the CA.
  - Synthesizer hopping: Each of *N* baseband processors connects to a dedicated transceiver. This requires transceivers that can be retuned and settled in less than 30 μs. Allows CA to have $\gg$ *N* ARFNCs. C0 is not in the CA.
- Some networks implement synchronous hopping to prevent collisions of hopping bursts from neighboring cells.

Frequency Hopping Parameters

A *hopping sequence* is an ordered list of ARFCNs used by a given physical channel (PCH), synced to the GSM frame clock. Each PCH can have an independent hopping sequence.

CA Cell Allocation, set of ARFCNs used for hopping in BTS

HSN Hopping Sequence Number, parameter used in pseudorandom algorithm generating hopping sequence

MA Mobile Allocation, subset of CA used by a particular PCH

MAIO MA Index Offset, offset added to hopping sequence when indexing MA.

- CA is the same for every PCH in the BTS
- HSN, MA and MAIO can be different for every PCH, usually only MAIO is unique

Understanding Um
GPRS

- More like a separate service running parallel to GSM.
- PCCCH and PBCCH used to make short-term assignments onto PDTCHs.
- Burst data rates up to 50 kb/s for half-duplex handset on GMSK network.
- Burst data rates up to 250 kb/s for full duplex handset on EDGE network.

Understanding Um
The Layers

The Layers are not exactly the ISO model, but a similar theme.

- L1 The radiomodem, TDM and FEC functions
- L2 Frame segmentation and retransmission
- L3 Connection & mobility management
- L4 Relay functions between BSC and other entities

Understanding Um

The Layers

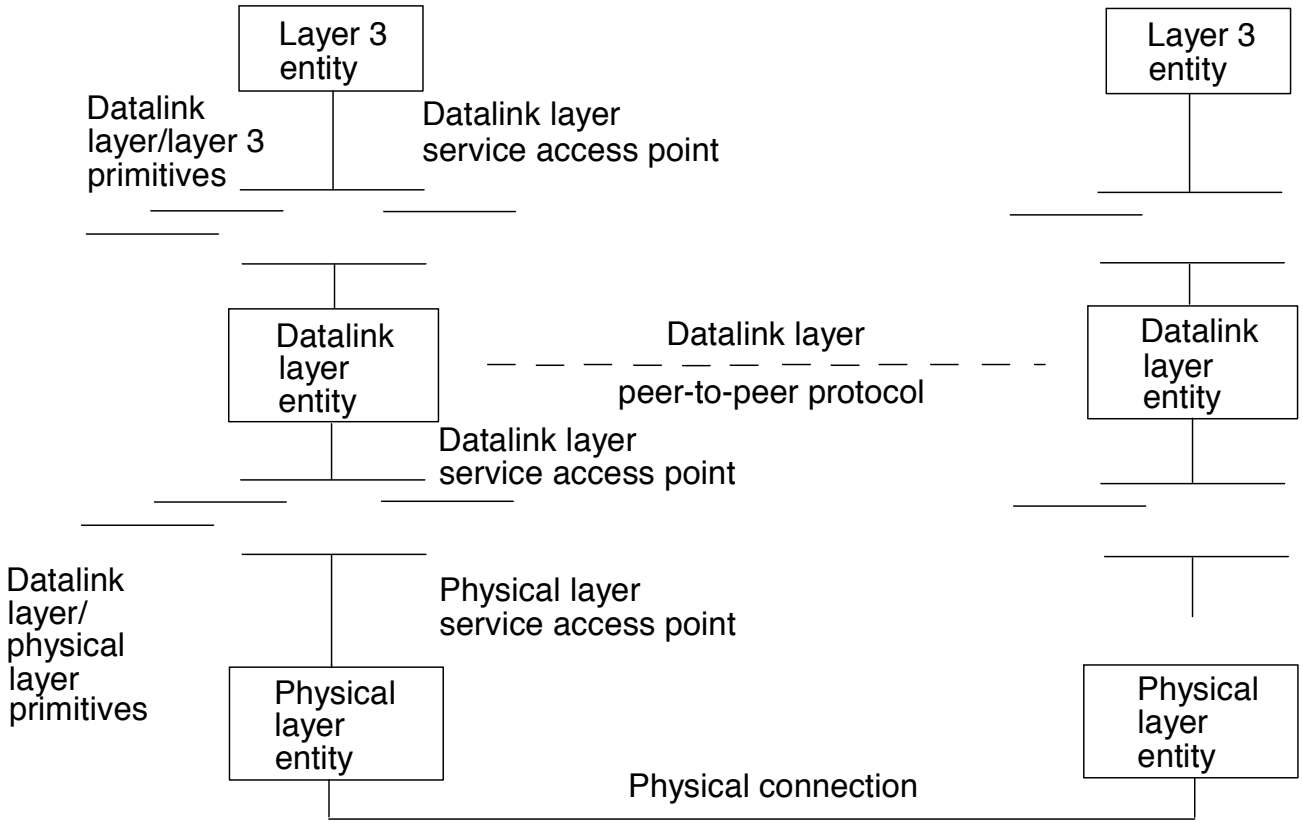


Figure: Layers of a Dm channel

Understanding Um
L1

- Analog radio path (transceiver, amplifiers, duplexer, antenna)
- GMSK or GMSK/EDGE radiomodem (“L0”)
- TDM to define logical channels
- FEC (Forward Error Correction)
  - Rate-1/2 convolutional code is typical.
  - 40-bit Fire code parity word on most control channels.
  - 4-burst or 8-burst interleaving is typical.

L1 Overview (see handout)

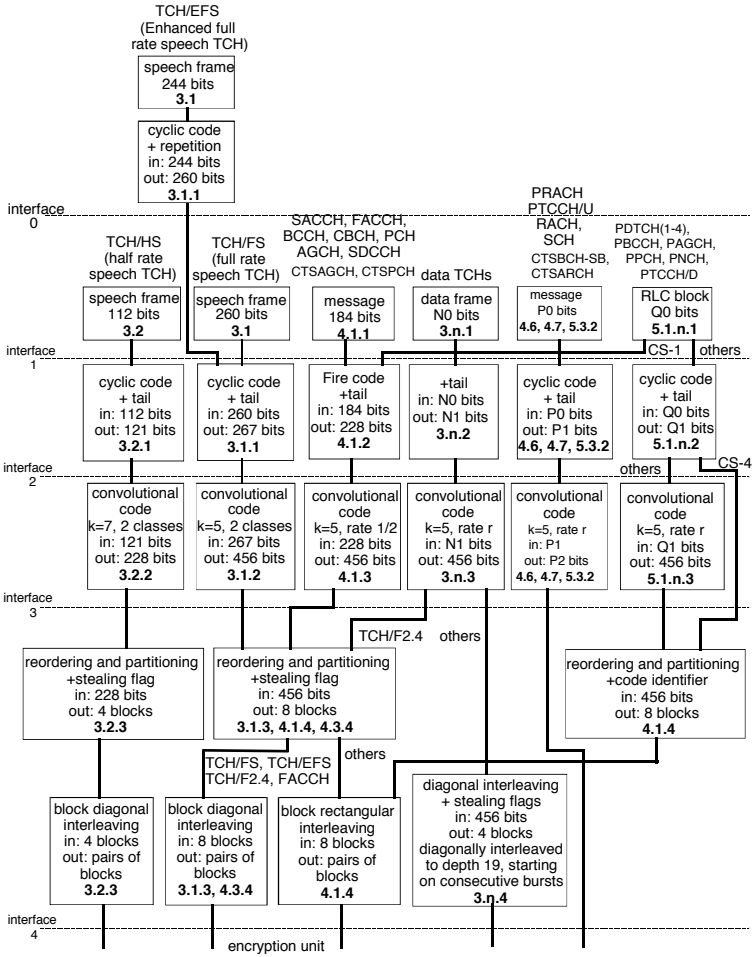


Figure 1a: Channel Coding and Interleaving Organization

Example – OpenBTS L1 Dm Receive Path

1. Tune, filter and decimate down to a 270.833 kHz baseband channel.
2. Demodulate GMSK with Laurent approximation, one burst at a time, to get probability estimates channel bits. (Soft-output demod.)
3. Demux burst to the the logical channel based on current frame number.
4. Deinterleave bursts according to T2 or T3. Mark bits from missing bursts as unknown bits.
5. Apply soft input Viterrbi decoder to L1 frame to recover L2 frame and parity word.
6. Compute parity word for received L2 frame.
7. If parity computed and received parity match, pass frame up to L2.

Um Radiomodem

- Gaussian Minimum Shift Keying – constant modulus to simplify amplifier design
- Each timeslot carries a radio burst:
  - guard period (between slots)
  - tail bits (at start and end of modulated data)
  - midamble (in center of burst)
  - payload bits (on each side of midamble)

Um “Normal” Burst

8.25	3	57	1	26	1	57	3
Guard period	Tail bits	Payload	Stealing bit	Midamble	Stealing bit	Payload	Tail bits

Guard period
: 8.25-symbols at the start of the burst

Midamble
: 26-bits for equalizer training at the center of the burst

"Stealing bits"
: each side of the midamble, used to distinguish control and traffic payloads

Payload
: two 57-bit fields, symmetric about the burst

Tail bits
: 3-bit field, at each end of the burst

(From Wikipedia.)

Um L1 Interleaving

- Every GSM data frame is spread over 4 or 8 radio bursts.
  - 4-burst block interleave on most channels
  - 8-burst diagonal interleave on TCHs
- Loss of one burst means 1/4 or 1/8 missing channel bits, scattered throughout a frame.
- Allows a slow-hopping system to achieve many performance gains associated with fast-hopping.

Um L1 Decoding

- Most channels use a rate-1/2 4th-order convolutional code.
- With a soft-input decoder, you can discard 1/2 of the input bits and still recover a frame.
- Dm channels use a 40-bit Fire parity code, designed to correct burst errors up to 12 bits long.
- Parity coding on Bm channels is media-specific.

Um Training Sequence

- used to train equalizer for multipath mitigation
- 26 symbols long, intended for use with 16-symbol correlator (12 dB processing gain)
- chosen for good autocorrelation, low cross-correlation
- with midamble & tails, GSM TCH is 22% known bits, 38 dB processing gain over 1 second

Um Clock Control

- MS has VCTCXO with natural error of a few kHz.
- BTS has VCOCXO with natural error of a few Hz, calibrated regularly.
- MS makes an initial search over a wide frequency window, then uses FCCH to calibrate VCTCXO to the BTS.
- Once locked, the MS will not make another wide search unless it loses service completely.
- GSM Specification mandates an accuracy of the carrier clock 30 ppb, that's less than 50 Hz @ 900MHz

Um Timing Advance

- Guard period 30 μs, a round trip distance of 4.5 km.
- If a burst arrives delayed by more than 30 μs it can collide with the next timeslot at the receiver.
- Avoid collisions with with active timing advance (TA) control.
  - BTS measures timing error of arriving burst midamble.
  - MS reports current TA value in physical header on SACCH
  - BTS calculates new TA and sends it back on the SACCH physical header
- Maximum TA of 63 symbols limits normal GSM range to 35 km.

Um Uplink Power Control

- BTS controls uplink power to reduce dynamic range requirements in the receiver.
- Power is controlled in roughly 2 dB steps in a closed loop:
  - BTS measures power of arriving burst.
  - MS reports current tx power value in physical header on SACCH.
  - BTS calculates new tx power and sends it back in physical header on the SACCH.

Um Downlink Power Control

- BTS can use downlink power control on carriers other than C0 to minimize interference with other BTSs.
- Power is controlled in a closed loop:
  - MS measures power of arriving bursts.
  - MS reports current RSSI in measurement reports on SACCH.
  - BTS adjusts its output power on that MS's timeslot to meet RSSI target.

Um Discontinuous Transmission (DTX)

- On average, a participant in a call is silent half of the time.
- GSM allows an MS or BTS to suspend transmission during silent periods, just sending an occasional keep-alive frame.
- Vocoders generate “comfort noise” during silent periods.
- For the MS, this saves battery power.
- For the BTS, this minimizes interference with other cells.

Understanding Um
L2

- L1 drops frames, but L3 assumes a reliable link.
- L1 uses fixed-length frames, but L3 uses variable-length messages.
- L2 (Data Link Layer) bridges the gap with segmentation, sequencing and retransmission.
- ISDN uses LAPD for L2, derived from HDLC, derived from SDLC, dating back to IBM's SNA mainframe networks.

Understanding Um
L2

- LAPDm on Dm channels, a HDLC derivative, similar to ISDN's LAPD but simplified.
- LLC on GPRS channels, another HDLC derivative.
- GSM defines no L2 in Bm channels.
  - Speech/fax are just media and have no L2.
  - CSD typically used with PPP for L2.

Understanding Um
L2 LAPDm

- Frame types UI, UA, SABM RR, REJ, I.
- Address, Control and Length fields in header. Some fields implied on some channel types.
- Asynchronous Balanced Mode (ABM, “multiframe mode”)
  - 3-bit sequence numbers, in RR-, REJ- and I-frame control headers. NS for sent, NR for acked
  - T200 timeout for repeating unacked frames
  - channel abandoned after too many timeouts
- Idle frame filling.

Understanding Um

L3 Sublayers

RR Radio Resource – assigns and releases logical channels. Terminates in BSC

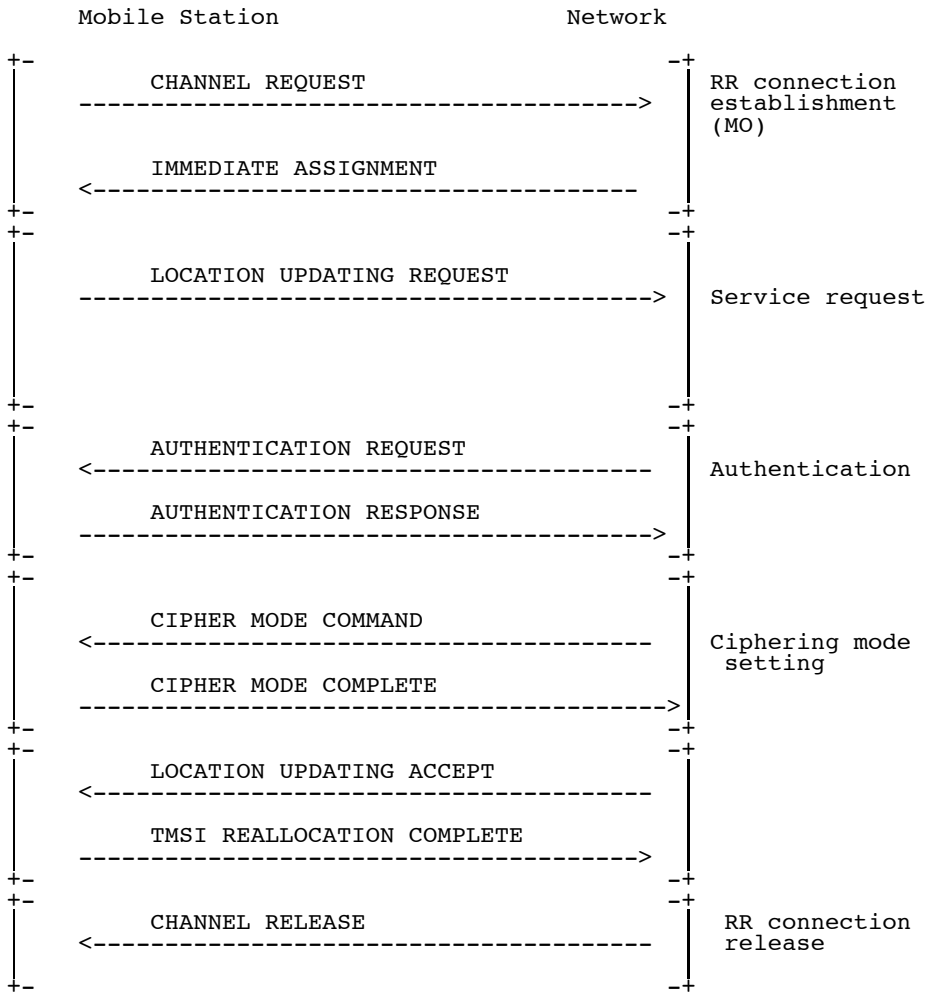
MM Mobility Management – location, authentication. Terminates in BSC and MSC

GMM (GPRS Mobility Management) – location, authentication. Terminates in BSC and SGSN

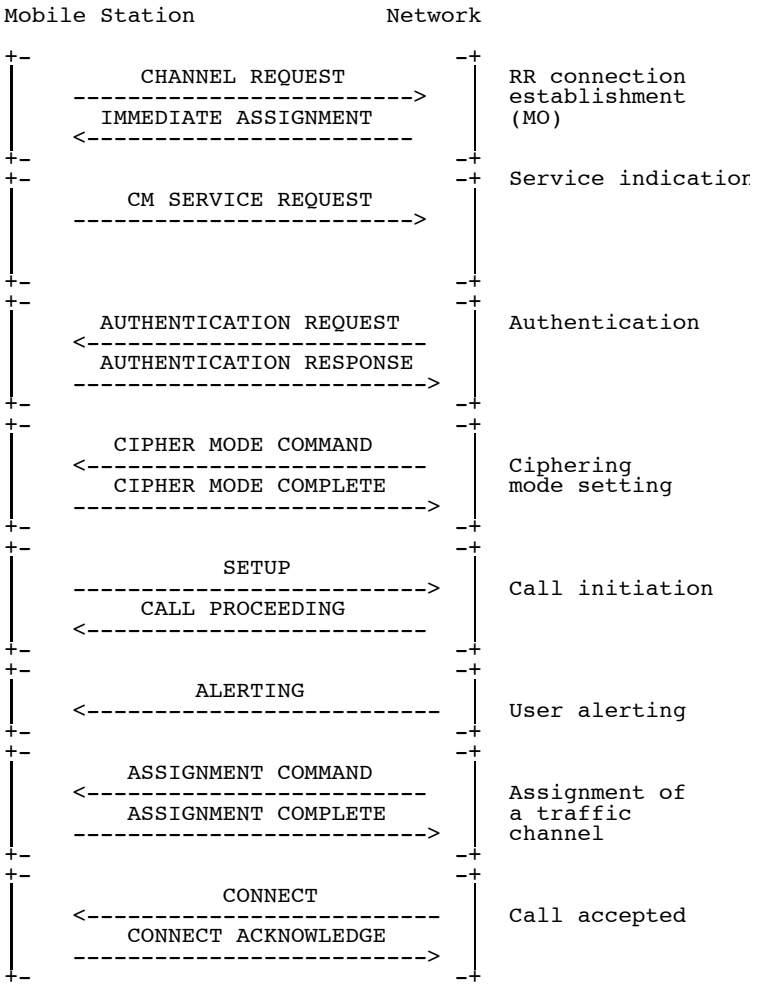
CC (Call Control) – Q.931, like ISDN. Terminates in MSC

SMSCP (SMS Connection Protocol) – tunnel from handset to SMSC

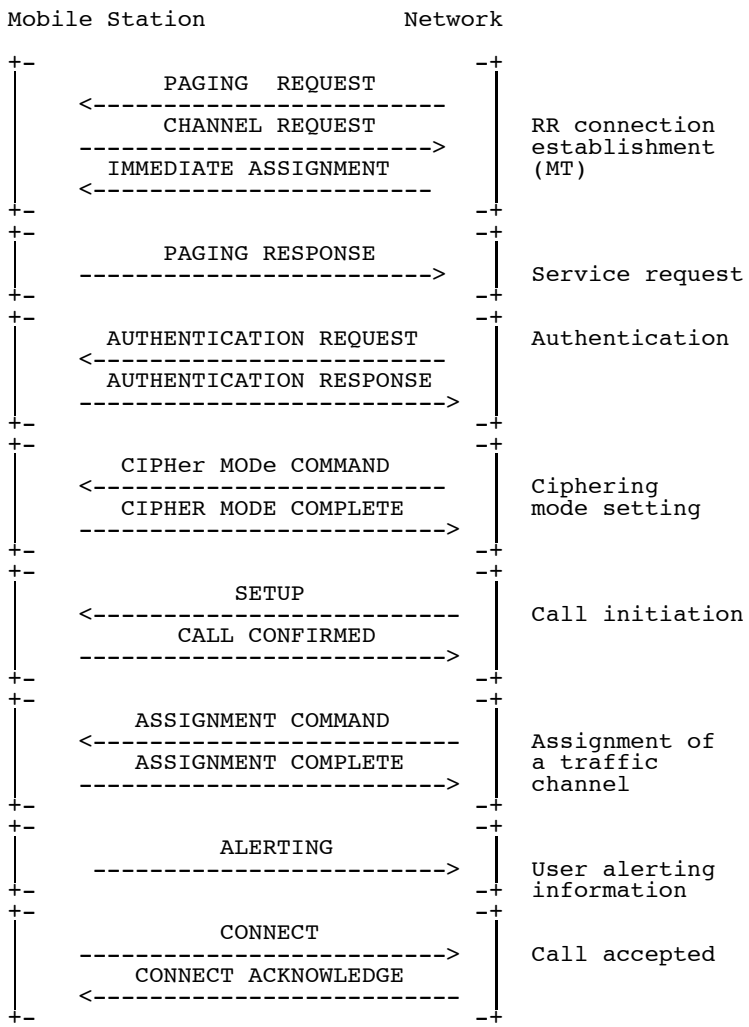
Example Transaction – Location Update



Example Transaction – MO Call Setup



Example Transaction – MT Call Setup



SMS – Layers

GSM TS 04.11 and 03.40 define SMS in five layers:

- L1 is taken from the Dm channel type used, either SDCCH or SACCH. This layer terminates in the BTS.
- L2 is normally LAPDm, but can be LLC in GPRS devices. In LAPDm SMS uses SAPI 3. This layer terminates in the BTS.
- L3 the connection layer, defined in GSM 04.11 5. This layer terminates in the MSC.
- L4 the relay layer, defined in GSM 04.11 6. This layer terminates in the MSC.
- L5 the transfer layer, defined in GSM 03.40. This layer terminates in the SMSC.

As a general rule, every PDU transferred in L(n) requires both a transfer and an acknowledgment on L(n-1).

SMS Connection Layer (L3)

- Terminates in the MSC.
- No addressing. Just peers on Dm link.

CP-DATA	carries an RPDU.
CP-ACK	acks CP-DATA.
CP-ERROR	nacks CP-DATA with cause code.

SMS Relay Layer (L4)

- Terminates in MSC.
- Addresses are SMSC E.164s.

RP-DATA	carries a TDPU to submit/deliver SMS between the MS and network.
RP-SMMA	polls network for SMS.
RP-ACK	acks RP-DATA. May carry TPDU.
RP-ERROR	nacks RP-DATA with cause code. May carry TPDU.

SMS Transfer Layer (L5)

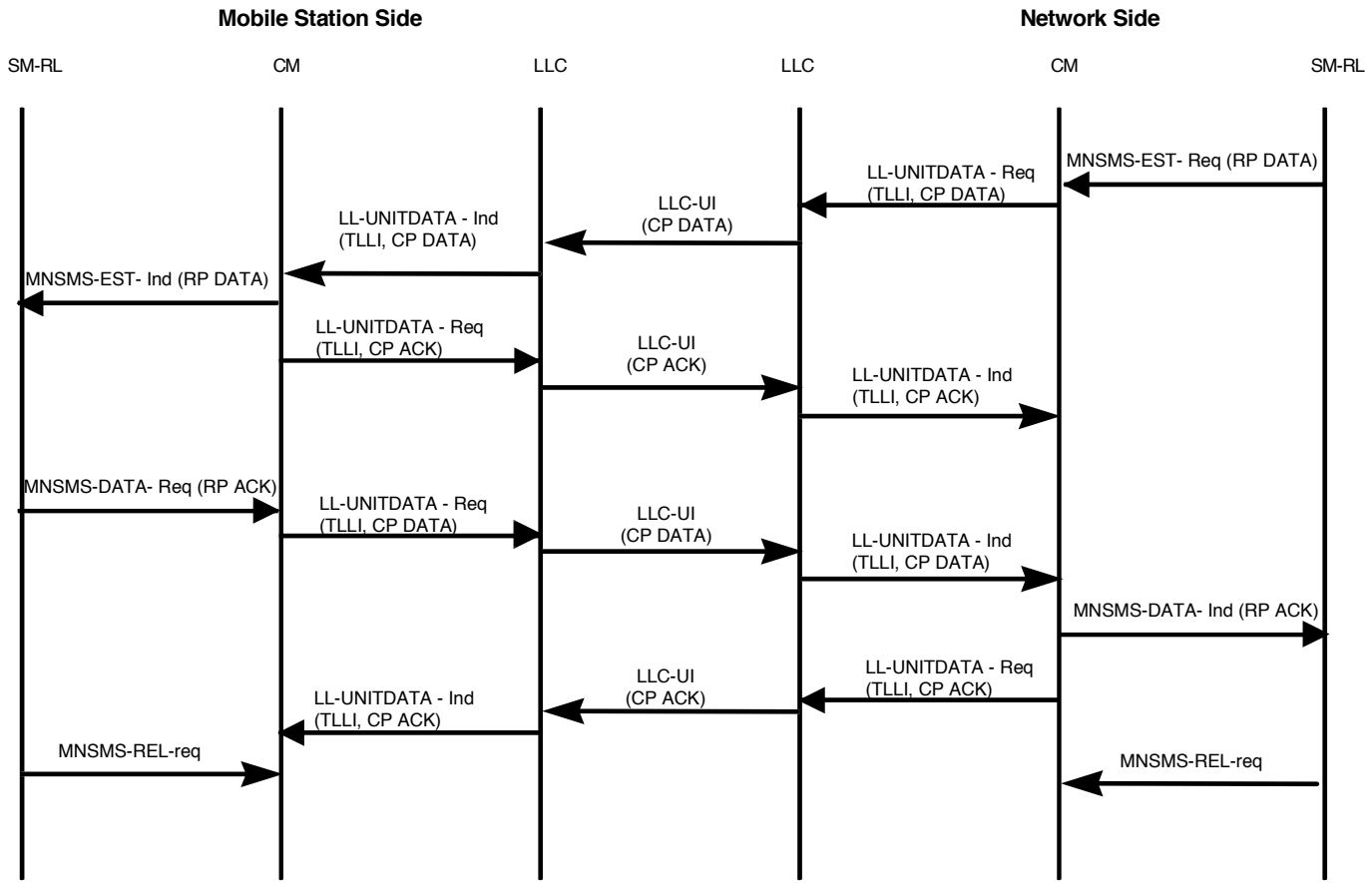
- Terminates in the SMSC.
- Addresses are user E.164s.

SMS-DELIVER	carries user data to MS.
SMS-DELIVER-REPORT	acks/nacks SMS-DELIVER
SMS-SUMBIT	carrier user data from MS.
SMS-SUBMIT-REPORT	acks/nacks SMS-SUBMIT.
SMS-STATUS-REPORT	reports status of previously submitted SMS.
SMS-COMMAND	can delete or cancel status report for a previously submitted SMS.

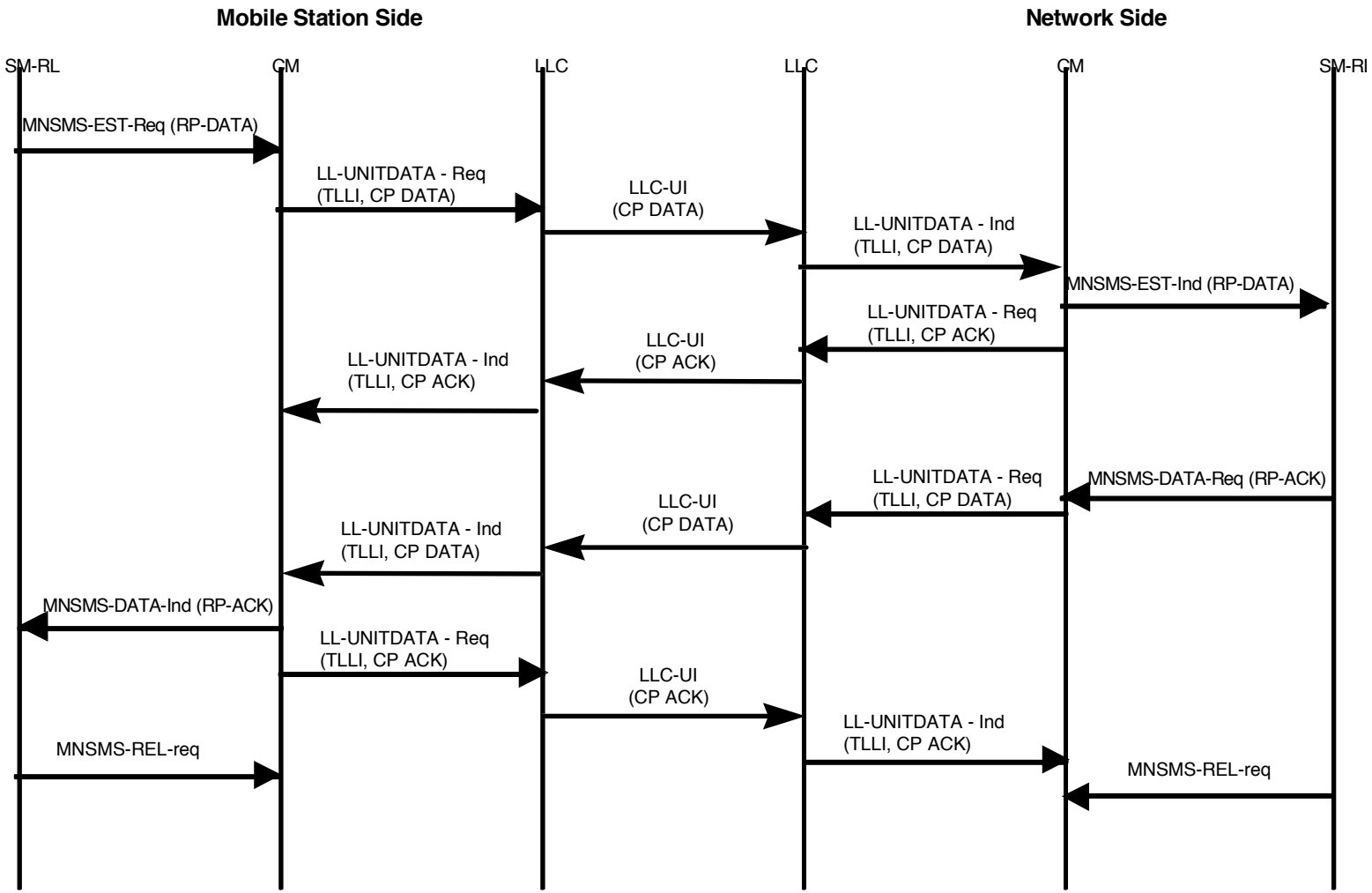
SMS User Data Header (L6)

- Endpoints are user devices.
- The User Data part of the TPU has an optional header, the UDH, described in GSM 03.40 9.2.3.24.
  - Segmentation for long messages.
  - Message waiting indications.
  - SIM Toolkit Security Header, wraps STK APDU.
  - WCMP, for WAP transport

MT-SMS in L3 & L4



MO-SMS in L3 & L4



Um Testing Tools – Nokia DCT-3

- Nokia DCT-3 handsets (1998-2003) include testing features in their firmware. These features can be enabled to covert these phones into useful test equipment.
- “Field Test Mode” can be enabled in many models through keypad sequences, serial port or IR ports.
- Some models (3310, for example) can provide full L2 traces through the serial port. These traces can be decoded with gammu and wireshark.

Um Testing Tools – Other Trace Tools

- Many Motorola handsets have a “Netmonitor” feature, similar to Nokia’s Field Test Mode.
- Other tools can give functionality similar to 3310 trace feature, but with more convenience and at 10× to 50× the cost.
  - Sagem OT-series engineering handsets.
  - Ericsson TEMS handsets.

Um Testing Tools – Example

(TEMS system, from Ericsson brochure. Watch the road, buddy.)

Um Testing Tools – Emulators/Testers

- Handset emulators to exercise BTS units:
  - Verify beacon content and modulation, measure RACH response, run standard transactions. Some include Abis support for end-to-end testing.
  - Rohde & Schwarz CMD57, used for US$4.5k-6k, for example.
- Network emulators to exercise handsets:
  - Generate beacon, verify modulation, answer RACH, run standard transactions.
  - Hewlett Packard 8922, used for US$10k-20k, for example.

Open Source GSM Tools
OpenBSC

What is OpenBSC

- A *GSM network in a box* software
- Implements minimal subset of BSC, MSC, HLR, SMSC
- Is Free and Open Source Software licensed under GNU GPLv2+
- Supports Siemens BS-11 BTS (E1) and ip.access nanoBTS (IP based)
- Has classic 2G signalling, voice and SMS support
- Implements various GSM protocols like
  - A-bis RSL (TS 08.58) and OML (TS 12.21)
  - TS 04.08 Radio Resource, Mobility Management, Call Control
  - TS 04.11 Short Message Service

OpenBSC software architecture

- Implemented in pure C, similarities to Linux kernel
  - Linked List handling, Timer API, coding style
- Single-threaded event-loop / state machine design
- Telnet based command line interface *Cisco-style*
- Input driver abstraction (mISDN, Abis-over-IP)

OpenBSC: GSM network protocols

The A-bis interface

Layer 1	Typically E1 line, TS 08.54
Layer 2	A variant of ISDN LAPD with fixed TEI's, TS 08.56
Layer 3	OML (Organization and Maintenance Layer, TS 12.21)
Layer 3	RSL (Radio Signalling Link, TS 08.58)
Layer 4+	transparent messages that are sent to the MS via Um

OpenBSC: How it all started

- In 2006, I bought a Siemens BS-11 microBTS on eBay
  - This is GSM900 BTS with 2 TRX at 2W output power (each)
  - A 48kg monster with attached antenna
  - 200W power consumption, passive cooling
  - E1 physical interface
- I didn't have much time at the time (day job at Openmoko)
- Started to read up on GSM specs whenever I could
- Bought a HFC-E1 based PCI E1 controller, has mISDN kernel support
- Found somebody in the GSM industry who provided protocol traces

OpenBSC: Timeline

- In November 2008, I started the development of OpenBSC
- In December 2008, we did a first demo at 25C3
- In January 2009, we had full voice call support
- In June 2009, I started with actual security related stuff
- In August 2009, we had the first field test with 2BTS and > 860 phones

OpenBSC: Field Test at HAR2009

Open Source GSM Tools: OpenBTS

- Open implementation of Um L1 & L2, an all-software BTS.
- L1/L2 design based on an object-oriented dataflow approach.
- Includes L3 RR functions normally found in BSC.
- Uses SIP PBX for MM and CC functions, eliminating the conventional GSM network. L3 is like an ISDN/SIP gateway.
- Intended for use in low-cost and rapidly-deployed communications networks, but can be used for experiments.

Open Source GSM Tools: OpenBTS

- Started work in August 2007, first call in January 2008, first SMS in December 2008.
- First public release in September 2008, assigned to FSF in October 2008.
- Tested 3-sector system with 10,000-20,000 handsets at September 2009 Burning Man event in Nevada.
- Latest release (2.5) is about 13k lines of C++.
- Now part of GNU Raido project, distributed under GPLv3

OpenBTS – “Nevada Test Site” & 21m Mast

Open Source GSM Tools: Airprobe

- *airprobe* is a collection of Um protocol analyzer tools using the USRP software defined radio
- A number of different Um receiver implementations

gssm	One of the two early Um receiver implementations (M&M clock recovery)
gsmsp	The other early Um receiver implementation
gsm-tvoid	For a long time the Um receiver with best performance
gsm-receiver	The latest generation of Um receiver

- Today, gsm-receiver seems to be the most popular choice

Open Source GSM Tools: Airprobe

- Some other airprobe tools

  gsmdecode A standalone text-mode Um L2 frame parser

  wireshark Dissector code for feeding Um frames into wireshark

  gsmstack An unfinished more modular implementation of a Rx-only L1

  viterbi_gen Generate C++ implementations of a viterbi decoder

- Still under development, no user friendly solution
  - gsmtap frame format needs to be added as clean wireshark interface
  - receivers need automatic frequency scanning
  - full solution needs proper UI

Part II - Um Security Features

- Theory
- The Baseband
- Observations

8 GSM Security Features
- TMSI – Anonymization
- A3/A8 – Authentication
- A5 – Ciphering
- Frequency Hopping

9 GSM Security – Design Flaws
- Oversights
- Intentional Weaknesses
- Handset Bugs

10 GSM Best Practises
- General
- TMSI's
- Frequency Hopping

11 Lawful Intercept

Known GSM security problems

Scientific papers, etc

- No mutual authentication between phone and network
  - leads to rogue network attacks
  - leads to man-in-the-middle attacks
  - is what enables IMSI-catchers
- Weak encryption algorithms
- Encryption is optional, user never knows when it's active or not
- DoS of the RACH by means of channel request flooding
- RRLP (Radio Resource Location Protocol)
  - the network can obtain GPS fix or even raw GPS data from the phone
  - combine that with the network not needing to authenticate itself

Known GSM security problems

The Baseband side

- GSM protocol stack always runs in a so-called baseband processor (BP)
- What is the baseband processor
  - Typically ARM7 (2G/2.5G phones) or ARM9 (3G/3.5G phones)
    - Runs some RTOS (often Nucleus, sometimes L4)
    - No memory protection between tasks
  - Some kind of DSP, model depends on vendor
    - Runs the digital signal processing for the RF Layer 1
    - Has hardware peripherals for A5 encryption
- The software stack on the baseband processor
  - is written in C and assembly
  - lacks any modern security features (stack protection, non-executable pages, address space randomization, ..)

Interesting observations

Learned from implementing the stack

While developing OpenBSC, we observed a number of interesting

- Many phones use their TMSI from the old network when they roam to a new network
- Various phones crash when confronted with incorrect messages. We didn't even start to intentionally send incorrect messages (!)
- There are tons of obscure options on the GSM spec which no real network uses. Potential attack vector by using rarely tested code paths.

OpenBTS developers observed the same.

GSM Security Overview

- Anonymization – The TMSI is assigned on a temporary basis and is substituted for the IMSI whenever possible.
- Authentication – Challenge-response dialog based on 128-bit secret key K_i and A3 & A8 algorithms.
- Ciphering – Authentication produces a 64-bit ciphering key K_C as a byproduct that is used to encrypt Dm and Bm channels with one of the A5 algorithms.
- Hopping – Not intended as a security feature, but makes interception considerably more difficult.

GSM Security: TMSI – Anonymity

- For anonymity, transmitting the IMSI in cleartext is avoided
- However, we still need to identify the MS that has requested a channel activation
- TMSI is a 32bit number and used as substitute for IMSI
- MS identifies itself the first time by IMSI, then the network allocates a TMSI.
  - MS stores allocated TMSI in SIM, even across reboots
  - network stores TMSI in HLR
- Network can reallocate TMSI at will
  - e.g. during location update
  - e.g. every 4 transactions (call, sms, ...)
- TMSI reallocation can happen after A5 encryption is started

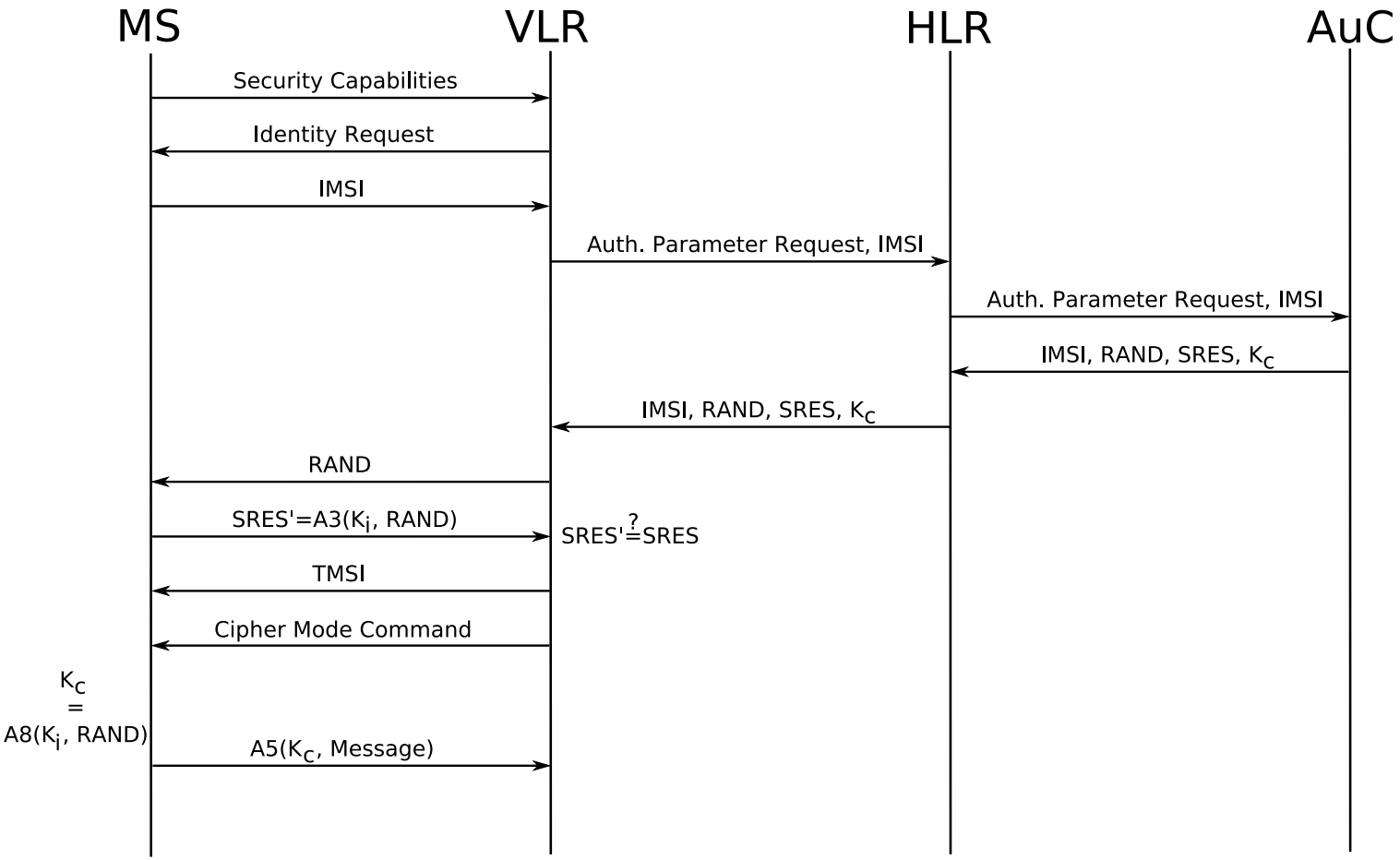
GSM Security: A3/A8 – Keys involved

- Much of GSM security is based on a 128-bit shared secret, K_i.
- There is one copy of K_i inside in the SIM.
  - regular SIM cards do not permit reading it back
  - of course, SIM card maker or operator might have a special key for that
- There is another copy of K_i in the AUC (Auth Center)
- K_i is never exposed directly anywhere.

GSM Security: A3/A8 – Authentication

1. Network generates 128 bit random value (RAND)
2. Network sends RAND to the MS in the MM Authentication Request message
3. MS forms a 32-bit hash (SRES) by encrypting RAND with A3 algorithm, using K_i as a key. Network performs identical SRES calculation
4. MS sends back its SRES value in the RR Authentication Response message
5. Network compares its calculated SRES value to the value provided by MS. If they match, the MS is authenticated.
6. Both the MS and the network also compute a 64-bit ciphering key (K_C) from RAND and K_i using the A8 algorithm. Both parties save this value for later use when ciphering is enabled.

GSM Security: A3/A8 – Authentication



GSM Security: A5 – Ciphering

- A5 is a family of symmetric ciphers inside the GSM Um Layer 1
  - A5/0 means no encryption
  - A5/1 is the *secure* cipher variant
  - A5/2 is the *weak* cipher variant
  - A5/3 is the UMTS replacement; can be used on GSM, too
  - A5/4..8 mentioned in protocol spec but never defined
- MS indicates A5 capabilities in classmark procedure
  - Compromised MS software could indicate no A5/1 capability to the network
  - Network can decide to use A5/0 even if the phone supports A5/1,2,3

GSM Security: A5 – Ciphering

- Encryption Key K_C is produced as result to A3/A8 authentication
- Re-keying can be initiated by the network at any given time by means of the authentication procedure
- K_C as a result of authentication is stored on SIM
- K_C can be read and written by the phone itself
  - OS on Baseband Processor typically has some kind of API to access SIM
  - However, quite often direct access to K_C is not permitted
  - Still, baseband processor software exploits do exist!

GPRS Security

- GPRS uses same A3/A8 Authentication as GSM
- GPRS uses its own GEA family of ciphers
  - Algorithm spec as secret as A5
  - However, no leaked / reverse engineered implementation yet
  - No academic or practical attacks known (yet?)
- GEA is used on Layer 2 (LLC), not Layer 1 as in GSM
  - Encryption between MS and SGSN, does not terminate at BTS
  - Not possible to capture unencrypted data on backhaul anymore

GSM Security: Frequency Hopping

- Requires that an interceptor support hopping or have sufficient bandwidth to capture the entire carrier allocation.
- Complicates decryption for a hopping interceptor, since you may have to decrypt a channel assignment before you even know where to tune next. (Wideband interceptors do not have this problem.)
- Hopping parameters can be reverse engineered from the spectrum if call activity is low.
- But you may not need to reverse engineer much:
  - The CA is global and usually divided into a small number (1 or 2) of non-overlapping MAs.
  - The HSN is usually the same for every assignment in the cell
  - In networks with synchronized cells, the HSN is the same even accross cells

GSM Security – Bad Assumption

Bad Assumption

No rogue actors in L3

- Any entity that can implement L1 and L2 correctly is assumed to be legitimate until a challenge fails
- This was a common telco security assumption in the 1980's, back when equipment was big and expensive and all of the networks were run by governments and quasi-governmental monopolies
- It is an assumption inherited from wireline telcos, and is even weaker in the wireless world

GSM Security – Oversights

Oversight

No authentication of the network

- GSM allows the network to authenticate a handset, but provides no means for the handset to authenticate the network
- Authentication is based on challenge-response, but the only comparison happens in the network end
- Any entity that can present a network-side Um interface is assumed to the legitimate, making it easy to create the GSM equivalent of a rogue access point.

GSM Security – Oversights

Oversight

Handset cannot release in L3 RR

- The channel release operation must always be initiated by the network
- As long as the handset sees a valid idle pattern in L2, it can be made to hold an active channel indefinitely

GSM Security – Oversights

Oversight

The network controls privacy

- GSM privacy controls are in the network, not in the handset
- Ciphering indications controlled by carrier.
- Any entity that assumes the role of the network takes control of the privacy features as well.
- Once camped, the MS is essentially a slave of the BTS.

GSM Security – Oversights

Oversight

Ciphering was an afterthought

- Ciphering was added to the system low in L1, below FEC
- L2 idle frames generate a lot of known plaintext
- FEC lowers the entropy of the plaintext stream
- The A5 ciphering algorithms were not subject to adequate review by cryptographic experts prior to standardization
- Encryption at L1 cannot be end-to-end since L1 terminates in the BTS, *so microwave backhaul can still be fully exposed*

GPRS Security – Oversights

Oversight

GPRS uses same K_C key generation (A3/A8) as GSM

- Even if GPRS has stronger crypto algorithm, K_C is generated the same way as in GSM
- K_C key recovery attack using A5/2 can be performed using same random challenge
- GPRS traffic can thus be recorded and later reviewed if MS with same SIM enters IMSI-Catcher and is presented with challenge from the recording

GSM Security – Oversights

Oversight

UMTS handsets also support GSM

- Many GSM security problems are fixed in UMTS, but all UMTS handsets fall back to 2.5G GSM operation when UMTS is not available.
- UMTS handsets can be ordered to fall back to GSM by a rogue 3G Node B before mutual authentication even happens.
- UMTS handsets can be forced into the GSM mode by jamming the UMTS service.

GSM Security – Anachronism

Anachronism

Predates public key encryption

- Network cannot authenticate the initial access attempt
- Any transaction must begin with the revelation of some subscriber ID over an unencrypted channel
- All security depends on the protection of K_i
- Once K_i is broken, the SIM is permanently compromised

GSM Security – Intentional Weaknesses

Intentional Weakness

A5/1 & A5/2

- Western governments were reluctant to export “strong” encryption to other parts of the world, so they defined two ciphering algorithms, A5/1 for the US and Europe and A5/2 for everywhere else
- The specification requires that any handset support both of these algorithms, so the cryptosystem is exported anyway and determined party can reverse-engineer either A5 from a standard handset.

GSM Security – Intentional Weaknesses

Intentional Weakness

Carriers do not use the full range of K_i, K_C.

- The spec allows 128 bits for K_i, but most carriers use only 64.
- The spec allow 64 bits for K_C, but most carriers use only 54.

GSM Security – Intentional Weaknesses

Intentional Weakness

Security features are optional

- Authentication is optional
- A5/0 means no ciphering at all and all handsets support it
- TMSIs are optional
- A3/A8 is selected by the operator, used to be COMP128

GSM Security – Handset Bugs

- TMSI exposure bugs compromise anonymization
- Many handsets crash or hang when presented with erroneous message formats or sequences
- Many features of the protocol are not widely used and therefore probably not well tested
- Many handsets vendor specific OTA and SIM support features not subject to outside review

GSM Best Practices – General

- Perform authentication and start ciphering as early as possible in a transaction, on the Dm channel.
- Never send subscriber E.164 over Um. E.164's are the easiest kind of subscriber ID to find in public records and there's no need to tell a handset its own phone number.

GSM Best Practices – TMSIs

- Never expose IMSI and TMSI in cleartext during the same transaction. Once the IMSI/TMSI pairing is exposed, the TMSI is useless.
- Reassign TMSIs frequently. If the user has the same TMSI for more than a few days, it is just as traceable as the IMSI. TMSI reassignment policies are operator-dependent and vary widely.

GSM Best Practices – Hopping

- Use hopping for Dm channels whenever possible. The start of a Dm transaction is never encrypted, so you use hopping to obscure it.
- Choose cell allocation ARFCNs with wide frequency separation, if possible given your licensed frequencies. This makes whole-cell interception much more expensive.
- Use uplink and downlink DTX and power control. This makes it more difficult to reverse-engineer hopping parameters through statistical analysis.

Typical GSM Security Configurations

- Developed world – best practices, for the most part. These networks are about as secure as possible given the limitations of the spec.
- Police state – no ciphering, often no hopping. Many countries outlaw ciphering to make life easier for their domestic intelligence services. Some have two networks, one for officials and one for everyone else.
- In Between – ciphering traffic, but not control.

"Best Practice" Example – Aaaaa in the US

Aaaaa follows security procedures typical of large GSM carriers in the US & EU.

- Immediate assignment is to a hopping SDCCH
- Immediate authentication, then ciphering
- Second assignment is to encrypted, hopping TCH
- TMSIs are typically reassigned several times each day.

"Worst Practices" Example – Bbbbb Mobile in the US

Bbbbb is a US iDEN network, not GSM but with very similar L2 & L3 protocols. These same procedures are used by GSM carriers an many parts of the world.

- Immediate assignment is to a non-hopping SDCCH.
- No authentication or encryption.
- Second assignment is to a non-hopping TCH, often on C0.
- TMSIs are stable for days or even weeks at a time.

Lawful Intercept

- Security flaw deliberately designed into all carrier-grade telecom systems.
- Required by law in most markets (US CELEA, UK RIPA, EU 17 Jan 1995 resolution).
- Allows intercepting party to access call traffic at the switching center.
- In principle, a law enforcement agency petitions a court for an order to get access to specific traffic.
- Lawful intercept features have been exploited by attackers to eavesdrop on high-profile individuals (Athens 2004-2005).

With lawful intercept, why bother with Um?

Why not just get a warrant and tap the core network?

- Maybe you are operating in *someone else's* country
- Maybe you cannot trust the telco or its employees
- Maybe you need tactical flexibility
- Maybe you just forgot all about the rule of law

Part III – Passive Interception and Geolocation

Example – Smith-Myers

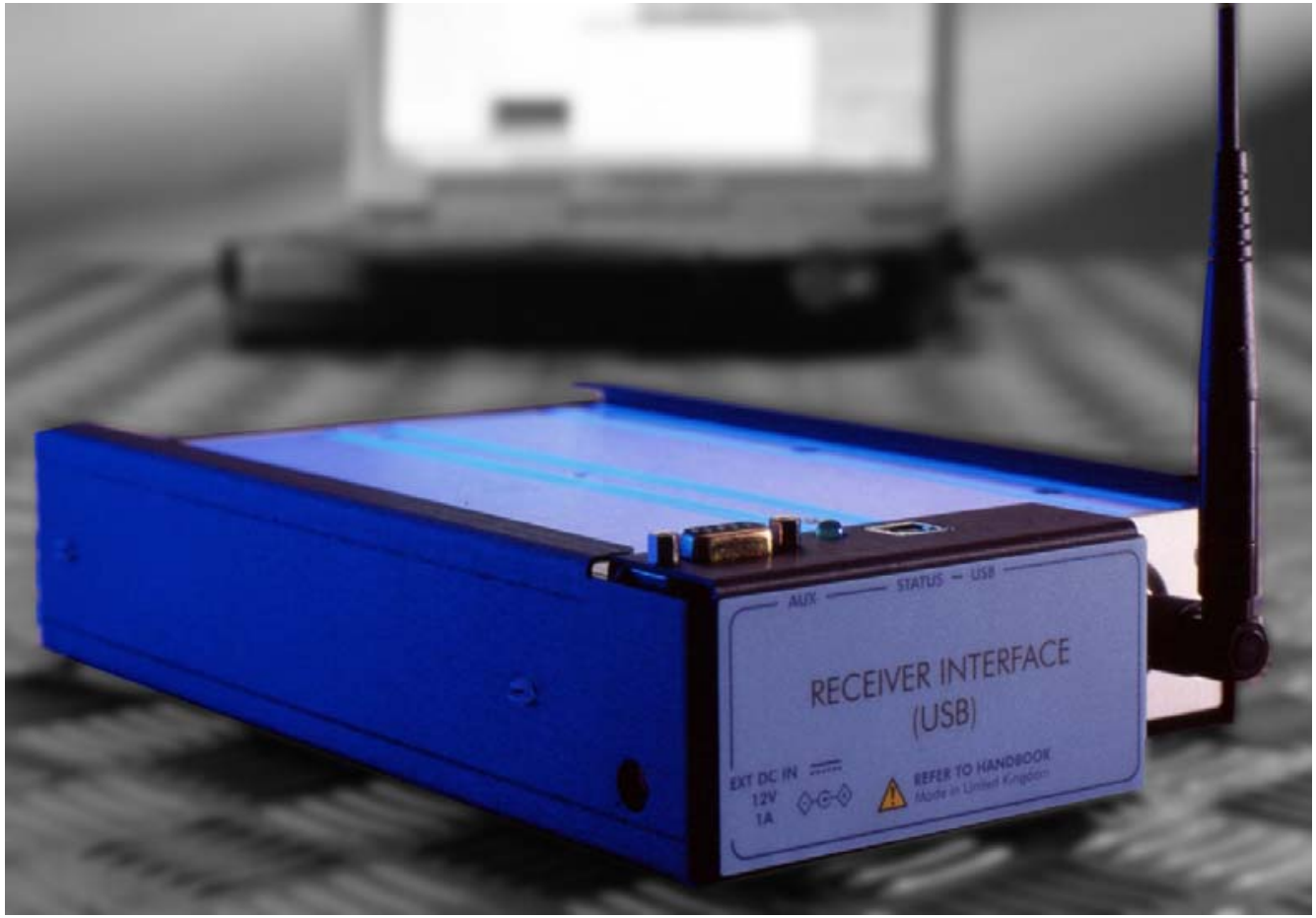


Figure: A typical passive intercept radio

The A5 Obsession

- Many discussions of passive intercept quickly devolve to A5 tutorials and not much else.
- In the many applications, A5 is a non-issue.
  - Maybe telco doesn't use ciphering.
  - Maybe the attacker knows K_i
  - Maybe the attacker can obtain K_C from the SIM
  - Recording the encrypted data and later providing the same challenge to the phone by means of an IMSI-Catcher can also recover the K_C
- Just decoding speech is of little practical value without the control messages.

Publicized A5 Attacks

- Academic cryptoanalysis of A5/1 cipher: EC1997, FSE2000, Crypto 2003, SAC 2005, ...
- Commercial A5/1 crackers exist in intelligence agencies
- Attacks based on a code book attack, mapping from known output to secret state
- First community project to compute rainbow tables in 2007/2008 but never released
- New distributed project now working with CUDA graphics cards and FPGA's

Uplink Intercept is Hard

- MS uplink transmission is 10-30 dB below downlink.
- MS is in the ground clutter, not on a tower.
- Big antennas improve performance but draw attention.
- Uplink intercept range is usually $<$1 km, even with good equipment, unless you have a high vantage point.
- Uplink strongest at the edges of the BTS coverage, but then reselection and handover are problems.

Good Demod Gives Flexibility

- Multi-antenna, vector-channel.
  - Doubling number of antennas gives 3-6 dB improvement, expanding range 30%-70%.
  - Greatly improves performance against multipath.
  - Improves performance against CCI.
- Soft demodulation. GSM's rate-1/2 FEC means that you can lose 1/2 of the radio bursts and still recover data, *as long as you know which half is lost*.

Timing, Power and Location

Geoobservables

- A geoobservable is any physical measurement that places a constraint on the geographic location of an object.
- The GSM TA value is a geoobservable. So is the TDOA of the MS and BTS signals at the interceptor. So is an AOA estimate from a DF antenna.
- Measurement reports of power levels from neighboring BTS units are also geoobservables, if you know their coverage areas.
- Given enough independent geoobservables, you can estimate the location of the MS.

Direct Measurement of Geoobservables

- GSM midamble can be used as a marker for parameter estimation on Um. (*That's why it's there.*)
- Cross correlation with a reference training sequence can yield a TOA estimate.
- Cross correlation between antennas in an array can yield an AOA estimate.
- Frequency estimation can yield Doppler offset estimate, a useful geooservable for a moving receiver.

Power-Scanning DF

- The operator waves it around watching a power meter, like something out of a wildlife program.
- It is a crude device, but useful at very close ranges.

Doppler AOA Estimation

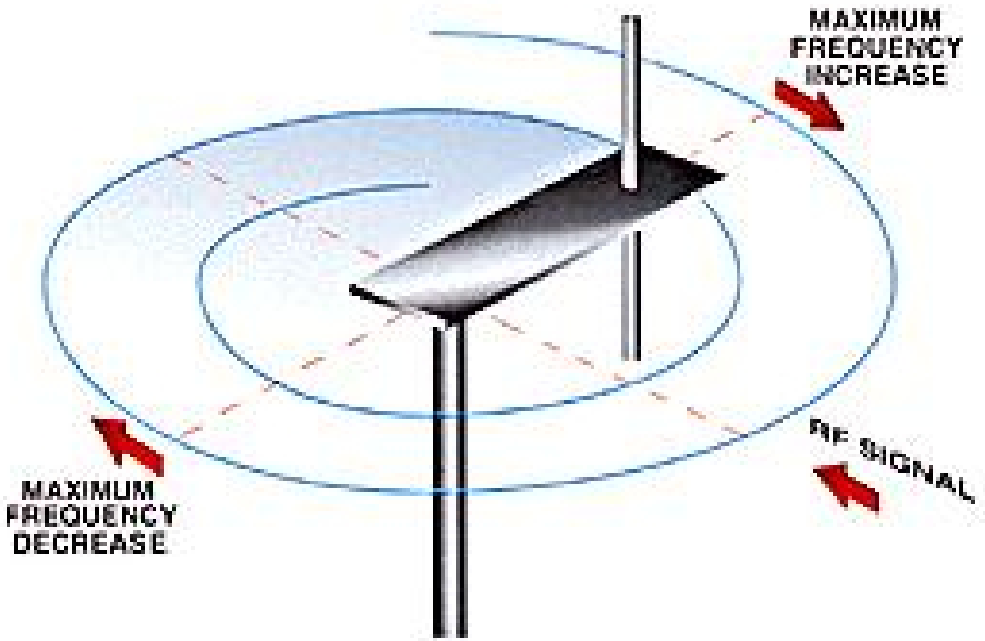


Figure: Imagine a spinning antenna

Doppler AOA Estimation

- For the spinning antenna, Doppler effect produces a frequency offset that varies with the angle relative to the target. Estimate Doppler offsets and you can estimate the AOA.
- The spinning antenna can be simulated by switching rapidly among antennas in a circular array, usually 4.
- Accuracy is on the order of $\pm 10°$, so many estimates are require to average out the errors.

Doppler AOA Estimation

Figure: Classic Datong DF1, from datongarchive.googlepages.com

MUSIC AOA Estimation

- Signal is received by a compact array of many precisely-placed elements. Array response is measured at many angles in a calibration procedure.
- AOA estimated by comparing array response to calibration data with MUSIC algorithm.
- Calibration is sensitive to vehicle shape and antenna array mounting location. May require calibration specific to vehicle type.
- High gain from multiple antenna elements allows estimation on very weak signals. Total processing gain of a 16-element array on a single GSM midamble is 20-23 dB.
- Accuracy at the Cramér-Rao bound, generally sub-degree, even for negative SNR.

MUSIC AOA Estimation

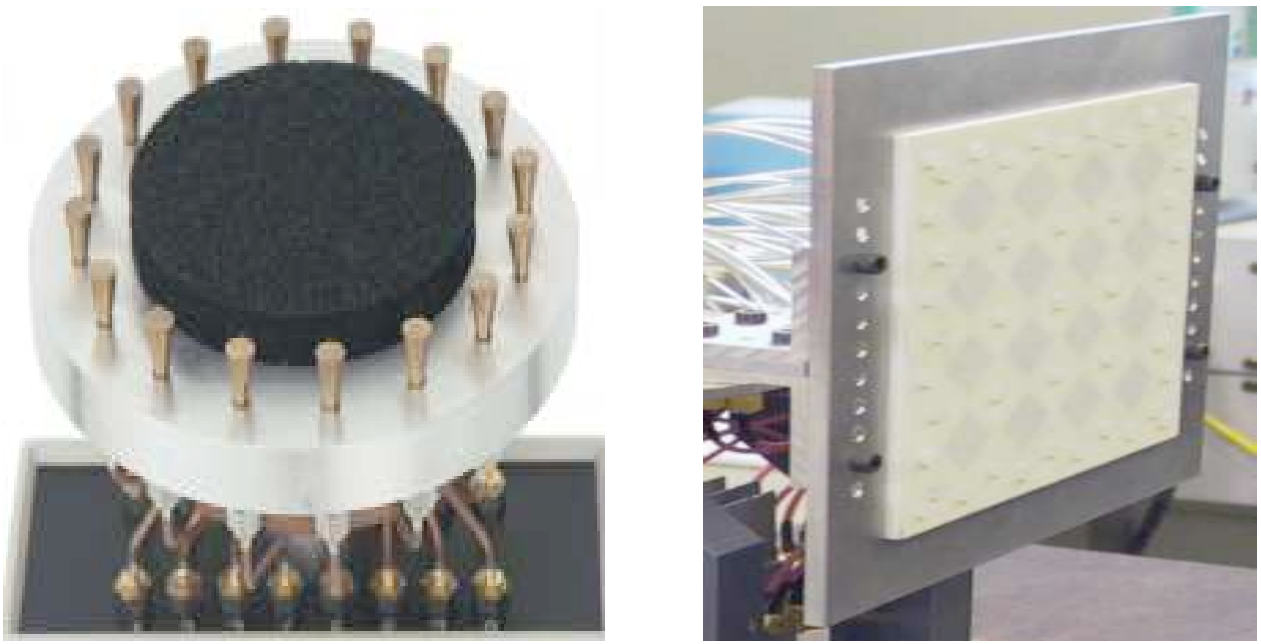


Figure 5: On the LHS, Uniform Circular Array (UCA) with $N = 16$ conical sensors (TU-Ilmenau). On the RHS, Uniform Rectangular Polarimetric Array (URPA) with $N = 16$ patch elements (HUT).

Figure: (From "PERFORMANCE OF ROOT-MUSIC ALGORITHM USING REAL-WORLD ARRAYS", Fabio Belloni, Andreas Richter, and Visa Koivunen.)

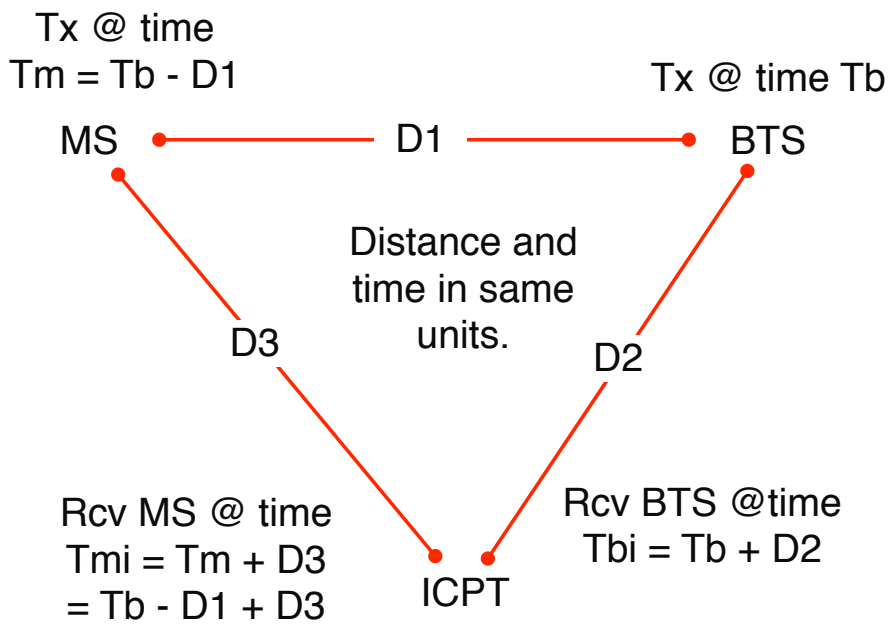
Typical AOA Geolocation Tool

Figure: Display from UI-DF application

SACCH Data as Geoobservables

- MS reports its current TA and tx power level on every SACCH message and BTS sends commanded values on downlink.
- The MS-BTS distance is c times $1/2$ the TA, or 553 m/sym.
- Knowing the true locations of interceptor and BTS you can also estimate interceptor-MS distance from MS-BTS TOA.
- Watch TAs from multiple BTSs during handover for more geooservables.

SACCH Data as Geoobservables



D1 is known from TA.
D2 is known from map.
We measure Tmi & Tbi.

Tmi - Tbi = Tm + D3 - Tb - D2
Tmi - Tbi = Tb - D1 + D3 - Tb - D2
Tmi - Tbi = D3 - D1 - D2

So D3 = (Tmi - Tbi) + D1 + D2.

And now we can estimate MS location on the map.

Caveat: This is accurate +/- 200 m.

Geolocation Pitfall – Multipath

- Creates false images for MUSIC systems
- Breaks Doppler systems entirely
- Adds unknown offsets to TOA estimates
- A serious challenge to tracking in urban areas
- Errors often have one-sided distributions that break classical linear estimators
- Can be mitigated with non-linear statistical techniques

Downlink-Only Intecept

- LAPDm always echos back the first message in a transaction, which always contains an unencrypted IMSI or TMSI.
- Calling party E.164s and MT SMS.
- DTMF echoed back in downlink acks.
- SACCH timing and power data gives some MS location information, even in downlink.
- BCCH/CCCH useful for network mapping.

The Identity Problem

- Intercept is useless if you cannot identify the parties.
- 3 IDs that matter:

  IMSI most stable on Um
  TMSI most likely to see on Um
  E.164 in public records, but rarely on Um
- Knowing a target's *friend's* E.164 is actually more useful, since *that* might appear in the downlink.

Getting IMSI/TMSI from E.164

- “Silent paging”
  1. Call E.164 and hang up before alerting starts.
  2. Watch PCH for paging activity.
  3. Repeat 1, 2 and watch for correlated IMSI or TMSI.
- “Silent SMS” – Send type 0 SMS TPDU and watch downlink activity.
- Wait for an MT call from a known associate’s E.164 and unwind the transaction from a log.

Small Scale Systems

- For intercepting a single target.
- Ideally, at least two receivers:
  1. One to always watch the beacon.
  2. One to follow the target, hopping if needed.
- Portable, usually in a vehicle.
- Interactive GUI, usually on a laptop.

Forcing Traffic

- Q: How do you intercept a multi-ARFCN BTS on a single-ARFCN interceptor?
- A: If there's a non-hopping C0, DOS the other ARFCNs.
  - Get a pile of cheap phones and place calls until you occupy all of the channels you can't intercept. (Be sure to use prepaid SIMs!)
  - Use narrowband jamming to block ARFCNs you can't intercept.

Large Scale Systems

- Intercepting many cells at once.
- Single wide-band radio intercepts whole carrier spectrum.
- Many software receivers running in parallel.
- Spews data. Output bandwidth is the sum of the backhauls.
- Fixed installation or dedicated vehicle.
- GUI is mostly through database tools.

Organizing Intercept Data

- Intercept system vs. test tool. Different applications and goals. Legal distinction of “primary purpose”.
- Wireshark vs. databases. Wireshark is a great diagnostic tool, but serious interceptors uses SQL.
- Live audio vs. traffic “corpus”. Log *every* vocoder frame with the time, frame number and BTS identity.
- Good interceptors never discard data. Field work is dangerous and expensive. Squeeze every bit and never throw anything away.

Intercept Data Mining

- Save every message, even if you can't decode it.
- Merge databases from multiple collectors and missions.
- Map social networks from control channel data.
- Identify talkers by tracing call establishment.
- Reconstruct user movements by merging databases and searching location updating operations.

Part IV – IMSI-Catchers

False BTS Basis #1

Problem

The handset does not authenticate the network.

- Any device that can generate the network-side Um interface can be used to spoof a cellular carrier.
- All you need to do is terminate L3 locally and run a partial simulation of the carrier's core network.
- Once you overcome the technical hurdle of generating Um, the rest is depressingly easy.

False BTS Basis #2

Problem

Ciphering is optional.

- If ciphering were mandatory, it would allow the handset a means of authenticating the network Oh well...

False BTS IP History

- Patents are public records:
  - Early Nokia work
  - R&S EP 1051053 – the first real IMSI-catcher patent
- Litigation produces public records:
  - MMI v CellXion – lots of discussion of IMSI-catcher history, identified several IMSI-catcher developers
  - Martone v Burgess – public identification of IMSI-catcher developers working for the US gov't

R&S "Virtual Basestation"

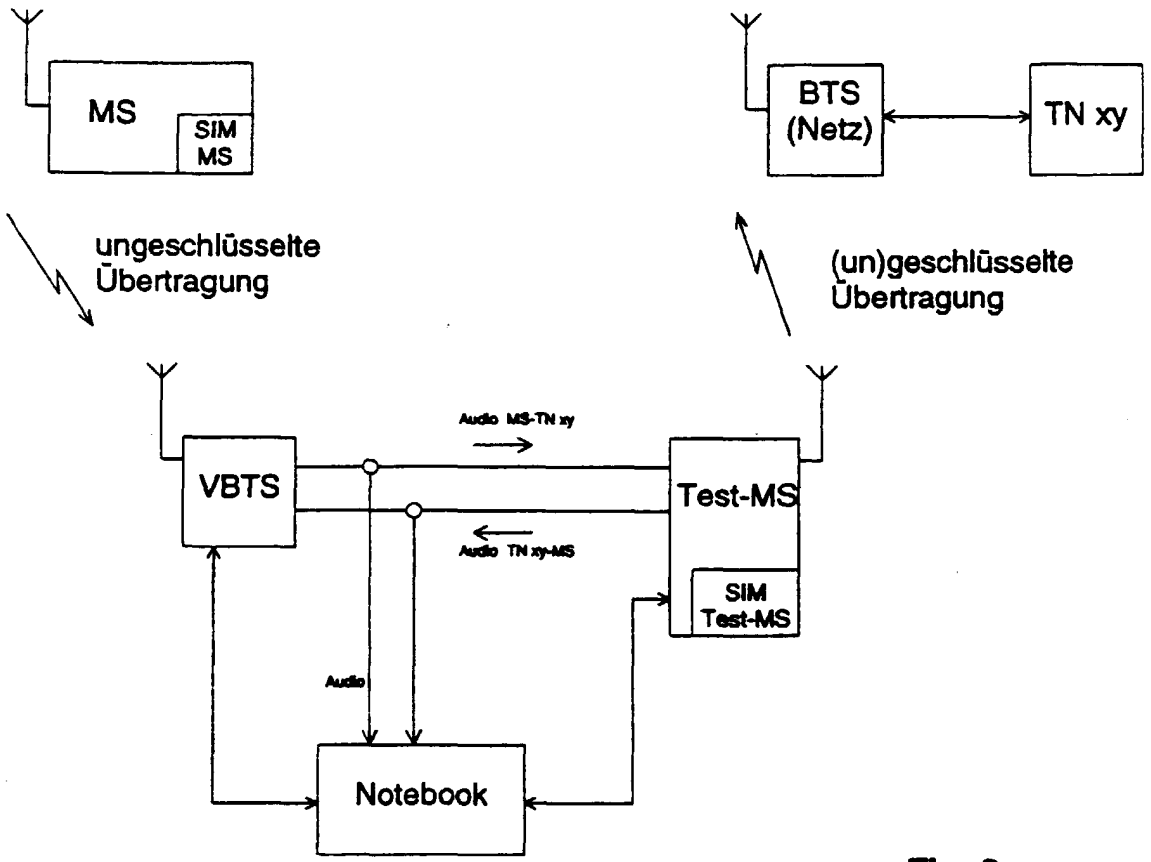


Figure: From EP 1051053

False BTS Design Approaches

- Early R&S designs (GA 090) based on BTS emulators.
- Standard approach: mini-BTS and laptop with T1/E1 card. Hardware similar to OpenBSC w/BS11.
- Abis-over-IP quickly replacing T1/E1 systems (CellXion/Datong DX series). Hardware same as OpenBSC w/NanoBTS.
- All-software BTS units with tighter L3 integration starting to appear (MRT-BTS). Software approach more similar to OpenBTS.

False BTS Example – Datong

The Datong series of DX products are primarily designed to provide Law Enforcement and the Military with a comprehensive toolkit of functionality in the increasing battle against mobile communications technology.
The DX series is primarily intended for

- Hard identification of mobiles in a given area
- A mechanism to enable a tracking signal from a “target” mobile
- Providing an interface for monitoring target mobile originated calls and SMS’s
- The protection of personnel and real estate from injury, harm or damage where mobile communications equipment have been known to be used to remotely trigger incendiary devices.

Figure: From Datong brochure

False BTS Example – MRT

Figure: From MRT, Inc. public web pages

False BTS Example – Tecore

WHAT IS IT AND HOW DOES IT WORK?

IntelliJAM is comprised of a control unit and a mini base station. It is deployed within the area of interest and emits a signal to compel handsets within its range to lock on to it. This stronger signal forces users within the controlled coverage area to register onto the IntelliJAM network while appearing to still be on the commercial network. Based on the IntelliJAM settings, wireless phone users in the controlled coverage area will either be approved and redirected to the commercial network for normal service, or they will be denied and will be unable to place or receive calls or text messages.

Facility coverage within the mobile network

Figure: From Tecore public web pages

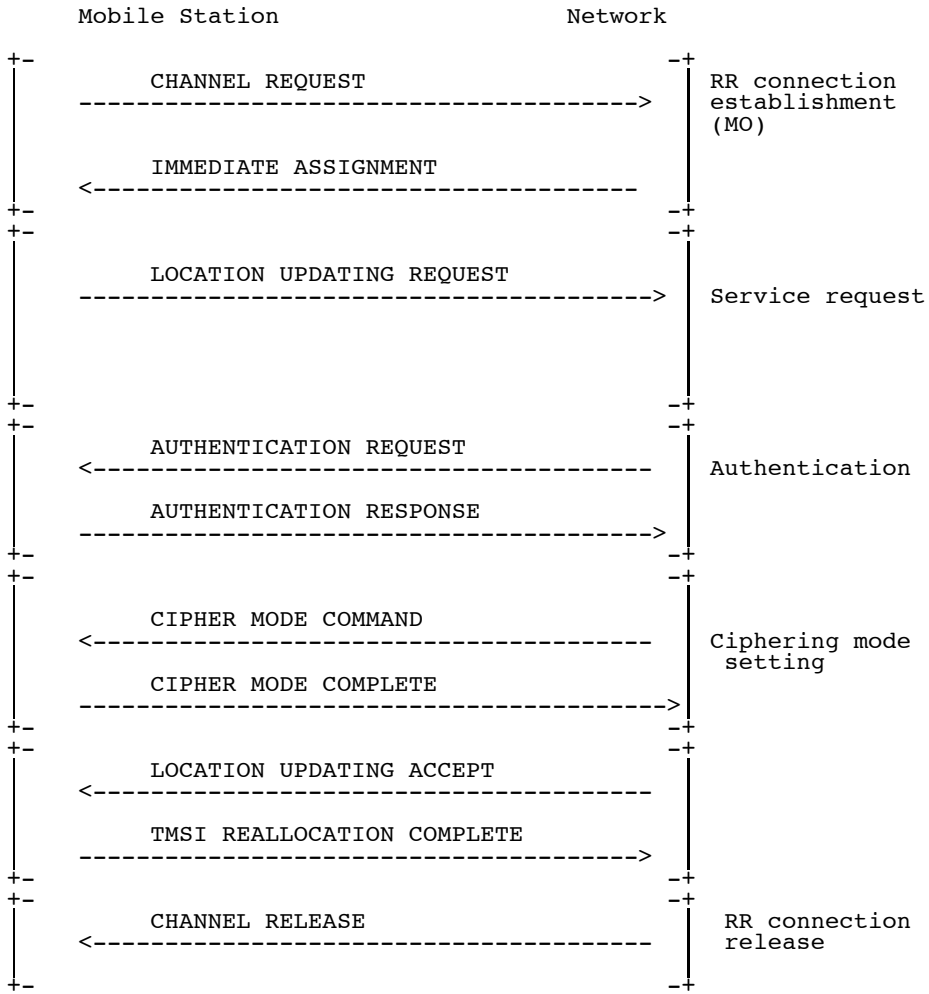
Cell Selection Behavior

- “Capture” technique based on handset’s BTS selection rules, GSM 03.22 4 and GSM 04.08 4.2.
- Use the same MCC/MNC/NCC as the local GSM carrier.
- Choose an ARFCN from the serving cell’s neighbor list.
- Ramp up power gradually to avoid congestion.
- Can also use CRO to increase effective power advantage.

Mobility Behavior

- Based on rules of GSM 04.08 4.
- When the handset enters a new “location area” it will attempt to register.
- So the IMSI-catcher advertises LAC different from any of the other cells in the area.
- Set timer T3212 for registrations on 6-minute intervals or change LAC to induce registration, like a broadcast ping to all camped handsets.

Key Transaction – Location Update



Location Update Options

- Location update request includes IMSI or TMSI of MS, plus MCC/MNC/LAC of previous serving cell.
- Authentication and ciphering are optional, so don't use them.
- Can request IMSI, TMSI or IMEI during update operation.
- Can assign a new TMSI.
- Can accept or refuse location update attempt *based on inspection of ID*.

Accept/Reject Tricks

- If IMSI-catcher accepts registration, the handset remains camped to IMSI-catcher and ignores real network. DOS.
- Reject cause codes matter:

illegal MS	locks handset until SIM is removed.
no roaming in LA	denies service *in any cell with the same LAC* until next time phone power-cycles.
IMSI not in VLR	kicks the phone back to the carrier with little or no disruption.

More Accept/Reject Tricks

- Send an “MM Information” message.
  - Set network name on the display.
  - Set the handset clock. (May allow smartphones to accept expired security certs, BTW.)
- Query the handset GPS receiver. (More on that later.)

Location Updating Demos

- Query and reject.
- Accept and DOS.
- Reject and lock.

Boy-In-the-Middle

- Accept target handset registrations.
- Allow MO call attempts, using A5/0.
- Connect call with wireline phone or another GSM handset, as in EP1051053 figure.
- Suppress CLID in the PSTN.
- Collect both sides of the conversation.

Man-In-the-Middle

- Accept target handset registrations.
- Allow MO call attempts, using A5/0.
- Connect call with VoIP carrier or ISDN.
- *Spoof* CLID in the PSTN.
- Collect both sides of the conversation.

Covert Call – Technique

- Starts like a normal MT call setup, but user is never alerted.
- Connection in RR and MM, but no CC/Q.931 steps.
- Phone goes to an active TCH and transmits an idle pattern.
- Phone is assigned a known training sequence, unique on its ARFCN, to make tracking easier.
- BTS controls power and channel release, tracks timing advance for distance estimate.

Covert Call – Applications

- Battery drain, by pushing tx power to maximum.
- Handset tracking via geoobservables.
  - Timing advance and measurement reports.
  - Midamble and idle pattern as markers for TOA & AOA estimation.

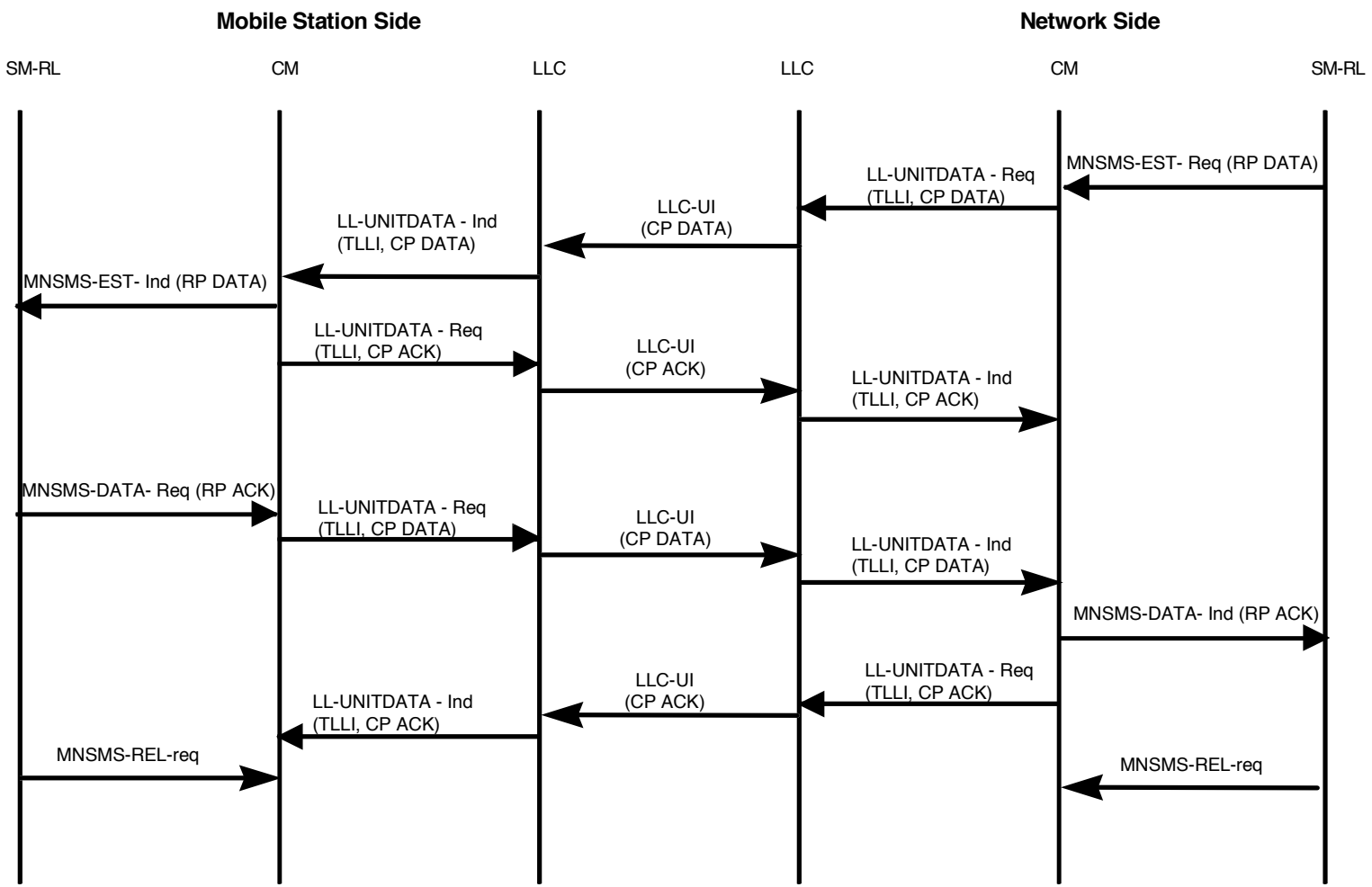
IMSI-Catcher with Integrated Geolocation

BTSGeo, an integrated BTS with Geolocation

BTSGeo enables **unique** capabilities and supersedes the accuracy and speed provided by Artemis. Proprietary and sensitive signal processing techniques empower the user with unsurpassed geolocation capabilities.

Figure: From MRT, Inc. public web pages

MT-SMS


Mobile Station Side
Network Side
SM-RL
CM
LLC
LLC
CM
SM-RL
MNSMS-EST- Req (RP DATA)
LL-UNITDATA - Req
(TLLI, CP DATA)
LLC-UI
(CP DATA)
LL-UNITDATA - Ind
(TLLI, CP DATA)
MNSMS-EST- Ind (RP DATA)
LL-UNITDATA - Req
(TLLI, CP ACK)
LLC-UI
(CP ACK)
LL-UNITDATA - Ind
(TLLI, CP ACK)
MNSMS-DATA- Req (RP ACK)
LL-UNITDATA - Req
(TLLI, CP DATA)
LLC-UI
(CP DATA)
LL-UNITDATA - Ind
(TLLI, CP DATA)
MNSMS-DATA- Ind (RP ACK)
LL-UNITDATA - Req
(TLLI, CP ACK)
LLC-UI
(CP ACK)
LL-UNITDATA - Ind
(TLLI, CP ACK)
MNSMS-REL-req
MNSMS-REL-req

MT-SMS Attacks

Source spoofing

- A false BTS can control any header field, L3-L5, including the originating addresses (user & SMSC) and timestamps
- Source address spoofing eliminates another security mechanism that a carrier or SIM application might use
- Plenty of other SMS attacks, especially for smartphones, do not require a false basesation. See “Attcking SMS” talk later this week

MT-SMS Attacks – TL-PID Types

As described in GSM 03.40 Section 9.2.3.9

Type 0 like a ping for SMS. Acked, then discarded silently.

Types 1-7 *replace* previously stored SMS from this OA.

Type 31 Page. Informs user to return call to OA.

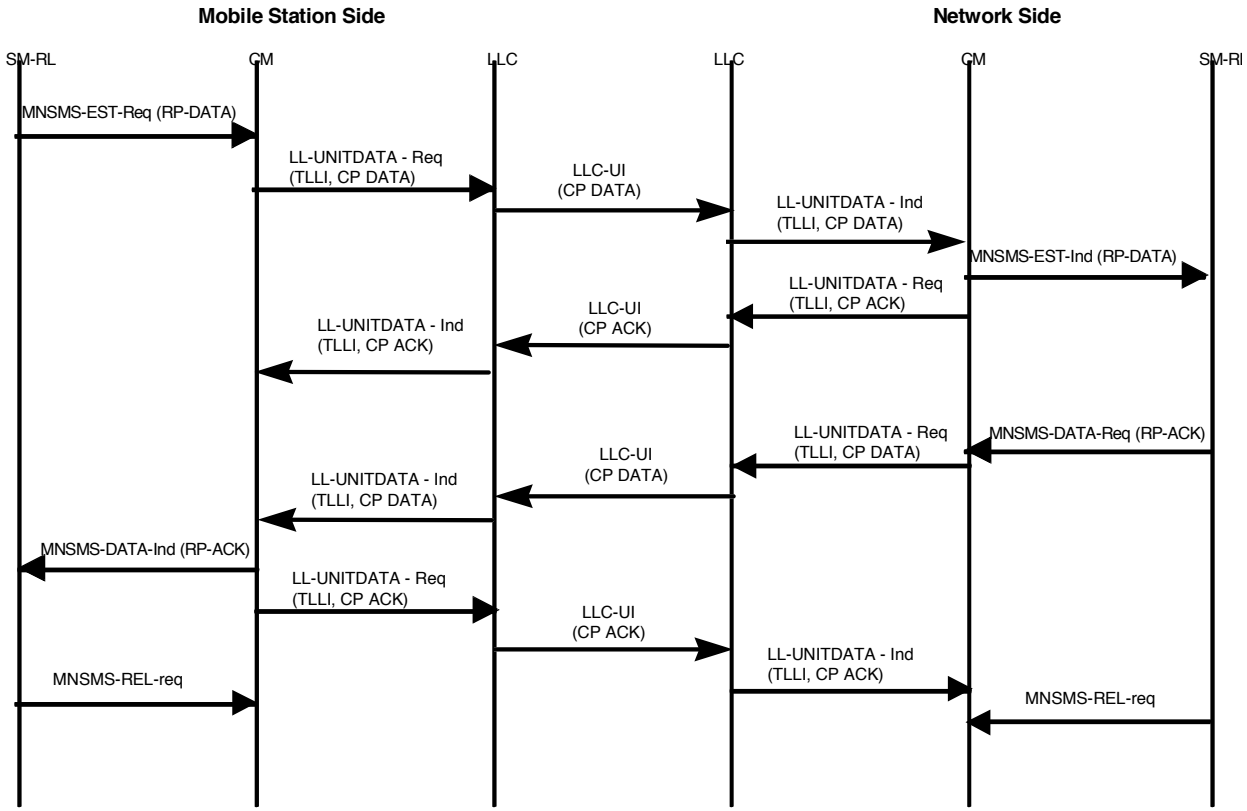
Type 61 ME Data download. Vendor-specific data, including OTA.

Type 62 “Depersonalization”, GSM 02.22 9, requires SIM keys.

Type 63 SIM Data download. Carries an ENVELOPE for a SIM Toolkit application. Security is application-specific.

MT-SMS Demos

MO-SMS


Mobile Station Side
Network Side
SM-RL
CM
LLC
LLC
CM
SM-RL
MNSMS-EST-Req (RP-DATA)
LL-UNITDATA - Req
(TLLI, CP DATA)
LLC-UI
(CP DATA)
LL-UNITDATA - Ind
(TLLI, CP DATA)
MNSMS-EST-Ind (RP-DATA)
LL-UNITDATA - Req
(TLLI, CP ACK)
LLC-UI
(CP ACK)
LL-UNITDATA - Ind
(TLLI, CP ACK)
LL-UNITDATA - Req
(TLLI, CP DATA)
MNSMS-DATA-Req (RP-ACK)
LLC-UI
(CP DATA)
LL-UNITDATA - Ind
(TLLI, CP DATA)
MNSMS-DATA-Ind (RP-ACK)
LL-UNITDATA - Req
(TLLI, CP ACK)
LLC-UI
(CP ACK)
LL-UNITDATA - Ind
(TLLI, CP ACK)
MNSMS-REL-req
MNSMS-REL-req

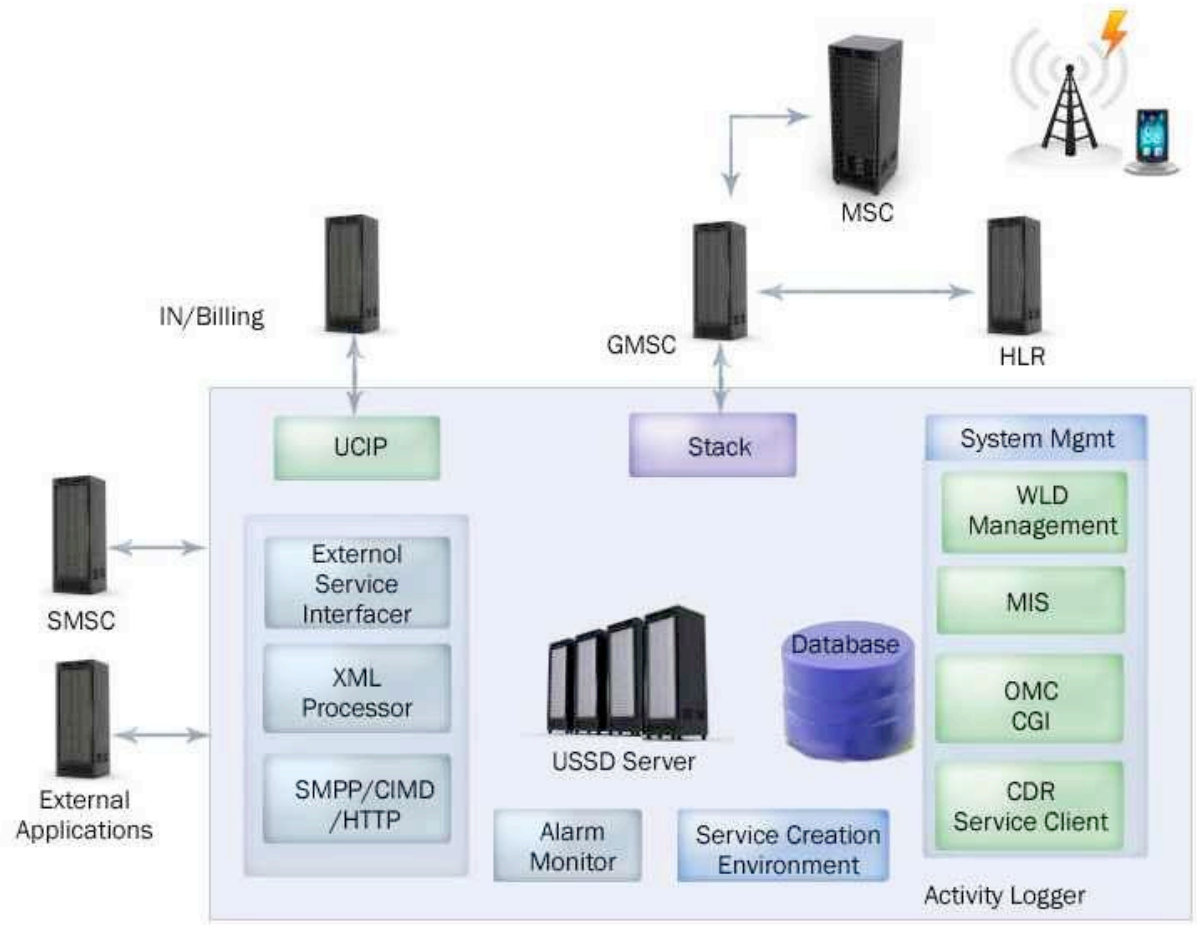
MO-SMS Intercept

- Accept CP-DATA from MS with RP-DATA / TP-DATA payload.
- Respond with CP-ACK success.
- Send CP-DATA with RP-ACK payload reporting a success or a network failure.
- Get CP-ACK success from handset.
- Release channel.

USSD

- Unstructured Supplementary Service Data, GSM 02.90.
- Similar to SMS, but session-oriented and faster.
- Used for interacting with core network applications & “value-added services”:
  - Calling feature access and configuration.
  - Payment systems and banking.
- Can also be used as WAP transport.

USSD


MSC
IN/Billing
GMSC
HLR
UCIP
Stack
System Mgmt
WLD Management
MIS
OMC CGI
CDR Service Client
SMSC
External Applications
Externol Service Interfacer
XML Processor
SMPP/CIMD /HTTP
USSD Server
Database
Alarm Monitor
Service Creation Environment
Activity Logger

RRLP
Radio Resource Location Protocol

- Radio Resource Location Protocol, GSM 04.31
- Protocol for accessing GPS receiver in a handset.
- Required for emergency call support in some markets.
- Can be queried whenever there is an active Dm channel. Handset can be paged just to do RRLP. No notification to the user.
- All privacy controls are on the network side, so if someone spoofs the network the subscriber has no privacy.

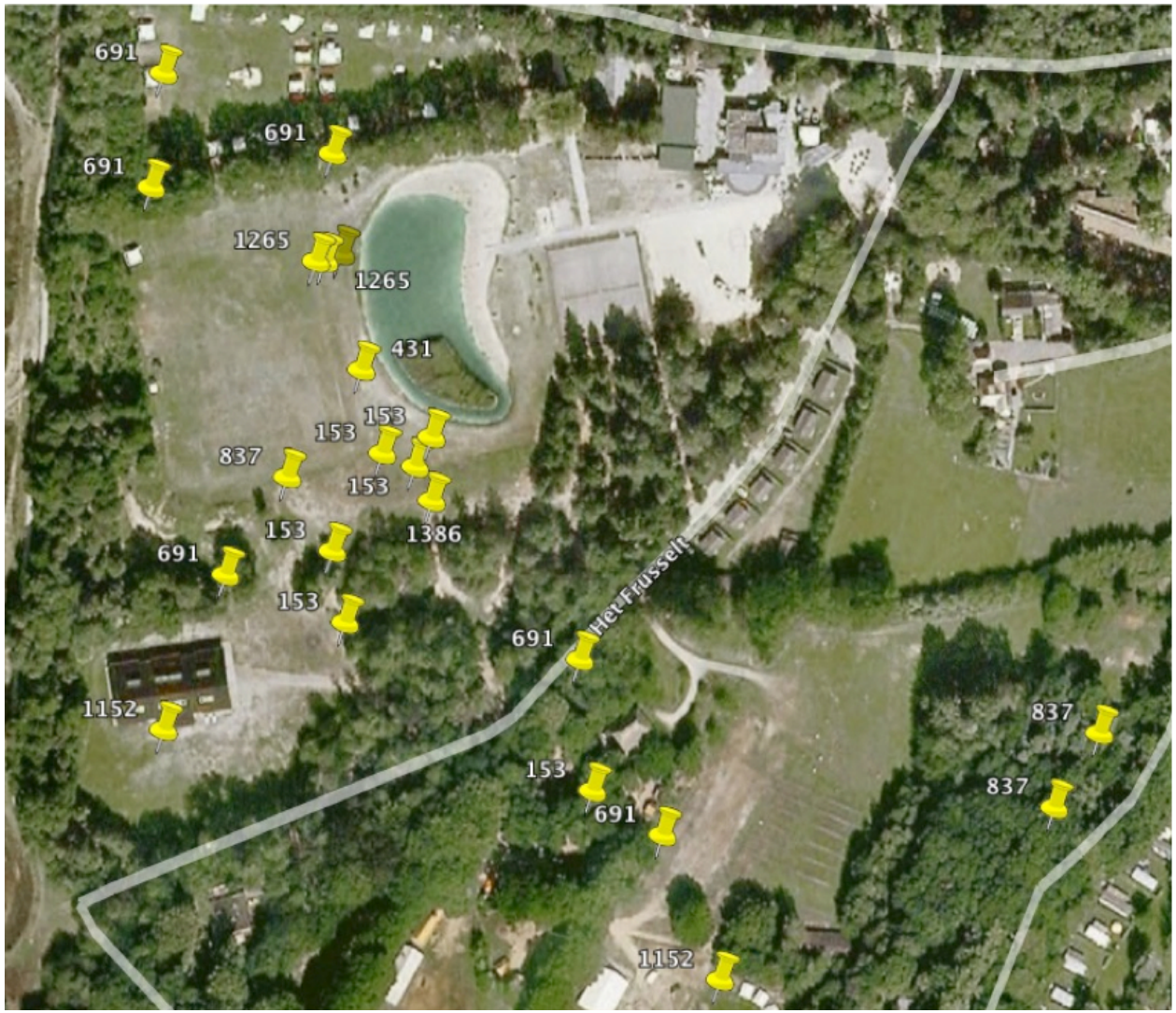
Some GPS Background

- GPS signal has 1.024 MHz bandwidth, transmitted synchronously from a fleet of MEO SVs.
- Positioning based on TOA measurements, but you need exact SV positions, clock deviations and atmospheric data to do the calculation.
- That information is modulated onto the GPS signal in the *ephemeris* and *almanac* messages.
- However, it is possible to measure TOA even if a signal is 20 dB too weak to allow demodulation.

RRLP

- Most RRLP attempts require GPS assistance information (almanac and ephemeris) because MS GPS antennas are tiny and the MS is usually poorly placed.
- Some experiments with non-assisted RRLP:
  - OpenBSC @ HAR 2009, Netherlands, 1% success
  - OpenBTS @ Burning Man 2009, US, 0.1% success
- *BUT* in both tests $>$ 90% of handsets *did* support the protocol and most failures were due to lack of assistance data. (Obviously, we need to try this again...)

RRLP results at HAR 2009



Part V – Jammers

Jammers

- Radio interface DoS attack.
- Useful to disrupt local communication or to disable remote-contol weapons.
- Useful for forcing traffic though vulnerable points.
  - Jam UMTS to force handsets to GSM.
  - Jam specific BTS units to control handovers or force traffic to compromised sites.

Downlink Jammers

- Downlink jamming overpowers the BTS signal at the handset. GMSK is a robust modulation, so you must really overpower, not just interfere.
- Downlink power levels are typically -70 to -100 dBm for normal service so you need at least -70 dBm to jam reliably.
- A 20 W vehicle-mounted wideband jammer has a reliable range of 100-200 m in an urban area.
- Most jammers are wideband, but single-ARFCN jamming of C0 affords much greater range at the same power levels.

Example Jammer

Figure: Typical generic quadband downlink jammer, probably about 10 W/band, probably made in China, probably jams a lot more than GSM.

Uplink Jammers

- Uplink jamming overpowers the handset signal at the BTS.
- Narrowband jamming does not require much more power than a standard handset, just 2 W to jam from the edge of a cell.
- Jamming the C0 makes the RACH/AGCH unusable. Also disrupts Dm channels on many BTS configurations.
- Jams the entire serving cell. Most in-progress calls are unaffected, but no new calls can be established.

RACH Flood DoS

- A more sophisticated uplink jamming attack.
- Mimics RACH bursts from a normal handset, but more rapidly, inducing resource exhaustion in the network.
- Requires very little power. Peak power up to 1 W but low duty cycle.
- See Dieter Spaar “A Practical DOS Attack to the GSM Network” later this week.

Part VI – Countermeasures

Operating Signature of an IMSI-Catcher

The network operator will see:

- Non-existent or distant LACs and invalid TMSIs in the location updates of handsets returning to the real network.
- Waves of heavy registration activity, especially if the IMSI-catcher is mobile or the operator is sloppy with power control.

With proper software in the BSC, a carrier might detect these symptoms automatically.

IMSI-Catcher Counter-counter-measures

To minimize the signature, the IMSI-catcher operator can:

- Ramp power up and down slowly at the start and end of a operating session.
  - Slow ramp-up prevents congestion in the IMSI-catcher.
  - Slow ramp-down prevents congestion in the carrier network.
- Accept all handsets and save reported TMSIs as the phones are captured.
- Set LAC to match local network prior to shutdown; reassign original TMSIs in last wave of location updates.

Moving handsets still produce a signature, but a much more subtle one and none of these techniques can hide a mobile IMSI-catcher.

Operating Signature of an IMSI-Catcher

On most handsets, the user might notice:

- Short battery life
- Encryption disabled on MO calls
- Failed MO attempts (if there's no man-in-the-middle support)
- Lack of MT calls
- Frequent visits to the AGCH

...and by the time you notice any of these it is probably too late.

Operating Signature of an IMSI-Catcher

On a field test handset, the user will see:

- Frequent LAC change, even if you are stationary.
- Active traffic channel with no active call.

It may not be hard to write a smartphone application to detect these conditions.

IMSI-Catcher Counter-measures

- Turn off your handset if you are not using it.
- Have people call you back, with their caller ID blocked.
- Use a field test handset and pay attention.
- Change SIMs frequently.
- Avoid handsets known to have TMSI retention bugs.

Countermeasures against A5/1 cracking

- Rolling change-over to A5/3 even in GSM networks
  - All modern 3G phones indicate A5/3 availability even on GSM
  - So far, no networks known that use it
- Re-keying intervals as short as possible
  - Ensures one cracked session key will not last for long

True Secure GSM

- Application-layer encryption over CSD.
  - Uses normal Q.931-style call control for a point-to-point raw link, then runs encrypted vocoder frames over the link.
  - Can call other like phones or a gateway service.
- Application layer encryption with VoIP over GPRS. Lie to the VoIP network about the media type and avoid transcoding.

Example Secure GSM Handset

Cryptophone G10i+

The GSMK CryptoPhone G10i+ is a lightweight quad-band GSM mobile phone that comes with full source code available for independent review.

- Voice & SMS encryption
- Fully encrypted storage system for secure contacts, messages and keys
- Encrypted storage system protects confidential data against unauthorized access in case the device is lost or stolen
- Strongest and most secure algorithms available today: AES256 and Twofish
- 4096 bit Diffie-Hellman key exchange with SHA256 hash function
- Readout-hash based key authentication
- 256 bit effective key length
- Encryption key is destroyed as soon as the call ends
- Source code available online for independent security assessments
- Also supports unencrypted calls, unencrypted SMS, address book, calendar etc.
- Works with any GSM 850/900/1800/1900 network that supports circuit-switched data calls
- Standby: up to 150 hours
- Talk time: Secure up to 5 hours

CryptoPhone G10i+
Dimensions:
98.5 x 51.4 x 15.8 mm
Weight: 99g incl. battery
Standby time: up to 150 hours
Talk time: up to 5 hours

Order now

Download the CryptoPhone video: **MPG** or **WMF**

An Open Source MS-side GSM stack

And how this would help us with many of our problems

- Enables user to deactivate unwanted features
  - No support for RRLP, SIM Toolkit, Network-initiated MO call or other abominations
  - Do not answer arbitrary IMEI or IMSI inquiries without user approval
- Enables us to implement important features
  - Make silent SMS non-silent
  - Reliable indication when phone is transmitting or not (silent call)
  - Reliable indication if and which GSM and GPRS encryption is used
  - IMSI-Catcher detection based on statistical analysis
  - Defend against TOA/TDOA based geolocation by artificial TA increase/decrease

An Open Source MS-side GSM stack

- Unfortunately, the stack alone is not sufficient
  - The stack needs to run on a baseband processor
  - The baseband processor needs to run in an actual phone
  - Cooperation from the industry unlikely, thus problem of deploying this stack much harder than it should be
- Even the stack itself is a fair amount of work
  - However, who would have thought of OpenBTS and OpenBSC coming along so quickly?
  - It clearly can be done, even with very few dedicated people
- Don't you too want a phone that you *own*, not the manufacturer or operator?

Summary
What we've learned

- The GSM industry is making security analysis very difficult
- It is well-known that the security level of the GSM stacks is very low
- We now have multiple solutions for sending arbitrary protocol data
  - From a rogue network to phones (OpenBSC, OpenBTS)
  - From an A-bis proxy to the network or the phones
- There is ongoing work for an accessible phone-side GSM L1/L2/L3 implementation

TODO
Where we go from here

- The basic protocol-level tools for security analysis of the GSM protocols exist
- It is up to the security community to make use of those tools (!)
- Don't you agree that TCP/IP security is boring?
- Join the GSM protocol security research projects today
- Boldly go where no man has gone before

Future plans

- Packet data (GPRS/EDGE) support in OpenBSC
  - GPRS is used extensively on modern smartphones
  - Enables us to play with those phones without a heavily filtered operator network
- UMTS(3G) support in OpenBSC
- CSD support in OpenBTS
- Access to MS side layer 1
- Higher-level attacks based on existing lowe layers
  - Playing with SIM Toolkit from the operator side
  - Playing with MMS
  - More exploration of RRLP

Further Reading

- Open source Software on a GSM protocol level

  OpenBSC `http://openbsc.gnumonks.org/`
  OpenBTS `htto://openbts.sourceforge.net/`
  airprobe `http://airprobe.org/`

- References to GSM protocol documentation

  Joachim G"oller `http://www.informatik.hu-berlin.de/~goeller/`
  nobbi `http://www.nobbi.com/`
  THC wiki `http://wiki.thc.org/gsm`

- A5 security related publications

  A5 public `http://groups.google.com/group/uk.telecom/msg/ba76615fef32ba32`
  Biham2003 `http://cryptome.org/gsm-crack-bbk.pdf`
  Biham2006 `http://www.cs.technion.ac.il/users/wwwb/cgi-bin/tr-get.cgi/2006/CS/CS-2006-07.pdf`
  HAR2009 `https://har2009.org/program/attachments/119_GSM.A51.Cracking.Nohl.pdf`
  rainbow tables `http://reflextor.com/trac/a51/wiki`