Cell Broadcast 101

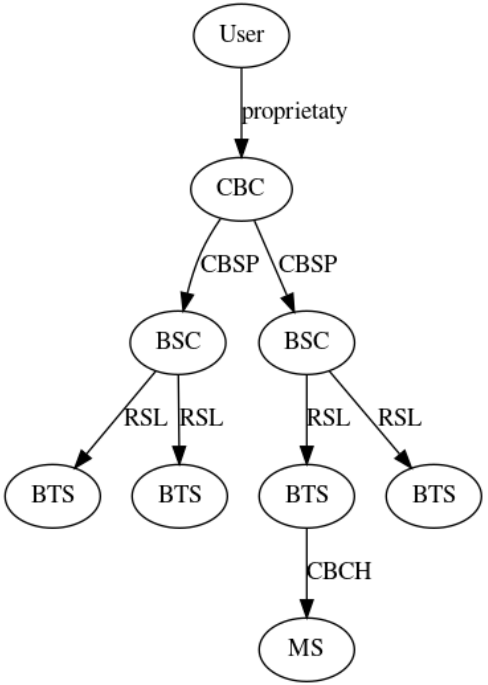
Akademy 2025 BoF

Shinjo Park

Agenda

- Over-the-air transmission of cell broadcast
- Possible methods of testing cell broadcast
- Questions?

Cell Broadcast Architecture



https://osmocom.org/projects/cellular-infrastructure/wiki/Cell_Broadcast

- From the Plasma Mobile's perspective, only over-the-air transmission is important
- Can't wait for test cell broadcast, how can we easily reproduce?
- Let's dig into cellular specifications and software implementations

How Cell Broadcasts are Carried

- Each generation has its own over-the-air transmission format

- 2G: SMS-CB
  - 3GPP TS 44.012 (GSM 04.12)
- 4G: SIB10, SIB11 (ETWS), SIB12 (CMAS)
  - 3GPP TS 36.331, “6.3.1 System information blocks”
- 5G: SIB6, SIB7 (ETWS), SIB8 (CMAS)
  - 3GPP TS 38.331, “6.3.1 System information blocks”

Regional Specifics

- Japanese ETWS has two message types, while the rest of world has only one message type
  - Intended to deliver early warning as fast as possible
- Every country/region has different meaning of message identifier (channel number)
  - 3GPP TS 23.041, Section 9.4.1.2.2 “Message Identifier”
  - To be covered later with a real example
  - cellbroadcastd and mobile-broadband-data has provision of this
- Two types of encoding: GSM 7-bit and UCS2

Encoding of Text Data

- 3GPP TS 23.041, Section 9.4.2.2.5 “CB Data”
  - Each GSM 7bit or UCS2 encoded data is divided into 82 octets – consisting individual page
  - [Number of pages] ([Page content] [Page length])*
- Example
  - “KDE Linux Alpha is available! https://kde.org/linux” could be encoded in a single page with GSM 7-bit encoding
  - “KDE Linux Alpha is available! 🍌 https://kde.org/linux” needs to be UCS2 encoded due to banana, also takes 2 pages

Example Cell Broadcast

- Test cell broadcast in Germany
- COVID-19 related cell broadcast in South Korea
- All carried over 4G and 5G
  - Tried to capture real world 2G example, but was not available
  - 2G/3G shutdown is going on, different architecture from 4G/5G
- Message segmentation is in use
  - Hope Plasma Mobile don’t have to reassemble the segments

Example Cell Broadcast

```
▾ sib12-v920
    messageIdentifier-r9: CMAS Identifier for CMAS Presidential Level Alerts (4370)
  ▾ serialNumber-r9: 41a0 [bit length 16, 0100 0001  1010 0000 decimal value 16800]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..00 0001 1010 .... = Message Code: 26
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType-r9: notLastSegment (0)
    warningMessageSegmentNumber-r9: 0
  ▾ warningMessageSegment-r9 [truncated]: 0450e95358bc06a5ceaaf3c80209ab4e62717a2d26a94529e81a943a
      [Reassembled In: 8303]
  ▾ dataCodingScheme-r9: 00
      0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)
      .... 0000 = Language: German (0)
```

Example Cell Broadcast

```
▾ sib12-v920
    messageIdentifier-r9: CMAS Identifier for CMAS Presidential Level Alerts (4370)
  ▾ serialNumber-r9: 41a0 [bit length 16, 0100 0001  1010 0000 decimal value 16800]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..00 0001 1010 .... = Message Code: 26
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType-r9: lastSegment (1)
    warningMessageSegmentNumber-r9: 1
  ▾ warningMessageSegment-r9: 1a8d46a3d168341a8d46a3d168341a8d46a3d168341a8d46a3d168341a8d46a3d168341a8d46a3d168341a8c
    ▾ [3 Fragments (333 bytes): #8301(263), #8302(263), #8303(70)]
        [Frame: 8301, payload: 0-262 (263 bytes)]
      ▸ [Frame: 8302, payload: 0-262 (263 bytes)]
        [Frame: 8303, payload: 263-332 (70 bytes)]
        [Fragment Count: 3]
        [Reassembled Length: 333]
        [Reassembled Data [truncated]: 0450e95358bc06a5ceaaf3c80209ab4e62717a2d26a94529e81a943aa9c123480693cd14c4b70
      Number of Pages: 4
      Decoded Page 1: PROBEWARNUNG, BUNDESWEITER WARNTAG 2023\nDo. 14.09.2023 - 10:59 Uhr - Probewarnung - für Deuts
      Decoded Page 2: chland - Es besteht keine Gefahr. - Weitere Infos auf https://warnung.bund.de/m/S_jcy037ETGT
      Decoded Page 3: - Herausgegeben von: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Nationale Warnze
      Decoded Page 4: ntrale 1 Bonn
```

Example Cell Broadcast?

```
▾ sib12-v920
    messageIdentifier-r9: Unknown (919)
  ▾ serialNumber-r9: 41a0 [bit length 16, 0100 0001  1010 0000 decimal value 16800]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..00 0001 1010 .... = Message Code: 26
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType-r9: lastSegment (1)
    warningMessageSegmentNumber-r9: 25
  ▾ warningMessageSegment-r9: 68341a8d46a3d1000c
    ▸ [ [truncated]68 Fragments (333 bytes): #8318(12), #8319(13), #8320(13), #8325(13), #8326(13), #8327(13), #8328(
      Number of Pages: 4
      Decoded Page 1: PROBEWARNUNG, BUNDESWEITER WARNTAG 2023\nDo. 14.09.2023 - 10:59 Uhr - Probewarnung - für Deuts
      Decoded Page 2: chland - Es besteht keine Gefahr. - Weitere Infos auf https://warnung.bund.de/m/S_jcy037ETGT
      Decoded Page 3: - Herausgegeben von: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Nationale Warnze
      Decoded Page 4: ntrale 1 Bonn
```

Differences

- So-called “channel number” is “messageIdentifier-r9”
  - First example was 4370, second was 919
- Even though these two messages carry the same content, if the mobile OS did not recognize the difference it may be flagged with invalid message type

More Examples

```
▾ sib12-v920
    messageIdentifier-r9: CMAS Identifier for CMAS Presidential Level Alerts for additional languages (4383)
  ▾ serialNumber-r9: 41a0 [bit length 16, 0100 0001  1010 0000 decimal value 16800]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..00 0001 1010 .... = Message Code: 26
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType-r9: lastSegment (1)
    warningMessageSegmentNumber-r9: 0
  ▾ warningMessageSegment-r9 [truncated]: 03d4e2940a0a328b522a0be40c52934fe735492c8282cca2940a2206b320194c3653
      [Reassembled In: 10196]
  ▾ dataCodingScheme-r9: 01
      0000 .... = Coding Group: Coding Group 0(Language using the GSM 7 bit default alphabet) (0)
      .... 0001 = Language: English (1)
```

Differences

- Message identifier denotes the usage of additional language
  - Example: English is additionally used along with German
  - Different ID: 4370 (0x1112) vs 4383 (0x111F)
- dataCodingScheme-r9 has language hint
  - 3GPP TS 23.038, Section 5 “CBS Data Coding Scheme”
  - Original GSM 7-bit encoding and UCS2 will be useful

Even More Examples (5G)

```
▾ sib8
    messageIdentifier: CMAS Identifier for CMAS Extreme Alerts with Severity of Extreme, Urgency of Immediate, and Certainty of Likely (4372)
  ▾ serialNumber: 7c40 [bit length 16, 0111 1100  0100 0000 decimal value 31808]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..11 1100 0100 .... = Message Code: 964
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType: notLastSegment (0)
    warningMessageSegmentNumber: 0
  ▾ warningMessageSegment [truncated]: 03005bbd80c0b0c2dc005d00310031002e00320035002e0028ae08002c00200030c2dcae30c90000290020cf54b85cb0980031
      [Reassembled In: 321]
  ▾ dataCodingScheme: 58
      0101 .... = Coding Group: General Data Coding indication (5)
      ..0. .... = Compressed indicator: The text is uncompressed
      ...1 .... = Message Class present: Bits 1 to 0 have a message class meaning
      .... 10.. = Character set being used: UCS2 (16 bit) (2)
      .... ..00 = Message Class: Class 0 (0)
```

Even More Examples (5G)

```
▾ sib8
    messageIdentifier: CMAS Identifier for CMAS Extreme Alerts with Severity of Extreme, Urgency of Immediate, and Certainty of Likely (4372)
  ▾ serialNumber: 7c40 [bit length 16, 0111 1100  0100 0000 decimal value 31808]
      01.. .... .... .... = Geographical Scope: Display mode normal, PLMN wide (1)
      ..11 1100 0100 .... = Message Code: 964
      .... .... .... 0000 = Update Number: 0
    warningMessageSegmentType: lastSegment (1)
    warningMessageSegmentNumber: 1
  ▾ warningMessageSegment: c5c6c7740020c811c88552ac00b2a50020260e00310033003300390d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d0d
    ▸ [2 Fragments (250 bytes): #313(156), #321(94)]
      Number of Pages: 3
      Decoded Page 1: [부산시]11.25.(금, 0시기준) 코로나19 확진자 3,172명. 60
      Decoded Page 2: 세이상 동절기 2가백신 집중접종기간(11.21~12.18), 예약없이 접종
      Decoded Page 3: 가능 ☎1339
```

Differences

- Different meaning of message identifier
  - 4372 (0x1114) means extreme alert by default, public safety alert in South Korea
  - The difference was not properly documented; generated a lot of false alarms during COVID-19 times
- UCS2 and GSM 7-bit encoding is differentiated in the network
  - How does ModemManager abstract the encoding difference?

How to Test?

- Free software implementation of cellular radio is available
  - 2G GSM: Osmocom suite
  - 3G: OpenBTS-UMTS (not so mature in this moment)
  - 4G: srsRAN 4G (a.k.a. srsLTE)
  - 5G: srsRAN 5G, OpenAirInterface, free5GC, Open5GS
- Software defined radio (SDR) hardware
  - USRP is the most expensive (~1900 EUR), used by most universities
  - LimeSDR could be a cheaper alternative (~450 EUR)

Disclaimer

- Cellular network typically uses **licensed** frequency spectrum
  - Notable exception: USA CBRS (4G, 5G)
- Get your frequency license from regulators or a faraday cage
  - Germany: Bundesnetzagentur (BNetzA), France: ARCEP
  - Can interfere with commercial mobile networks
  - Usage of frequency may be monitored by regulators

Preparing srsRAN for Cell Broadcast

- Provision some test SIM cards with custom network code
- Vanilla srsRAN does not support cell broadcast out-of-box
  - Patches available!
  - https://github.com/nakolos/srsRAN/commit/07a9ae01c8bb6da4209a19c94de63c83ba7c00a1
- Connect the SDR hardware and configure srsRAN
- Plug in the provisioned SIM card and let it connect
- Enjoy

Spoofing Cell Broadcast

- “This is Your President Speaking: Spoofing Alerts in 4G LTE Networks” – Gyuhong Lee et al., MobiSys 2019
  - https://doi.org/10.1145/3307334.3326082
- Cell broadcasts are not authenticated, anyone with required hardware can fire up a 4G base station
  - Just like the pirate radio
  - URLs in cell broadcast could not be always trusted
- There should be an option to opt-out from the cell broadcast

THANK YOU