A Look at Project 25 (P25) Digital Radio

Aaron Rossetto

Principal Architect, NI

Agenda

- What is Project 25?
- A brief introduction to trunked radio
- The P25 protocol
- GNU Radio and P25 decoding experiments

About the presenter

- 21-year veteran of NI*
  - August 2019: Joined SDR team to work on UHD 4.0 and RFNoC
- Long-time SDR enthusiast
  - 2003: Ten-Tec RX320D
  - FunCube, AirSpy, RTL-SDR dongles
- Long-time interest in public safety communications monitoring
  - 1988: PRO-2013 (my first scanner!)
  - 1997-present: Various Uniden scanners

* NOTE: Not speaking for my employer in this presentation

What is Project 25?

- In an emergency, communication is often the key to survival
- Many agencies must collaborate and coordinate in a disaster scenario
  - First responders: Police, fire, EMS (city, county, state)
  - Federal agencies (e.g. FEMA, military reserves, NTSB, ATF, etc.)
  - Relief agencies, local government resources, etc.
- Challenge: Lack of interoperability between public safety comms systems
  - Technical: Spectrum used, system features
  - Political: Isolated or lack of planning, lack of coordination, funding disparities, jurisdictional issues, etc.

What is Project 25?

- 1988: U.S. Congress directs the Federal Communications Commission to study recommendations for improving existing public safety communications systems
- 1989: APCO Project 25 coalition formed
  - Association of Public Safety Communications Officials (APCO)
  - National Association of State Telecommunications Directors (NASTD)
  - National Telecommunications and Information Administration (NTIA)
  - National Communications System (NCS)
  - National Security Agency (NSA)
  - Department of Defense (DoD)

What is Project 25?

- Set of standards for land mobile radio systems enabling public safety responders to communicate with each other and, thus, achieve enhanced coordination, timely response, and efficient and effective use of communications equipment
- Codified in TIA-102 series of documents
  - Defines open interfaces between components of LMR systems

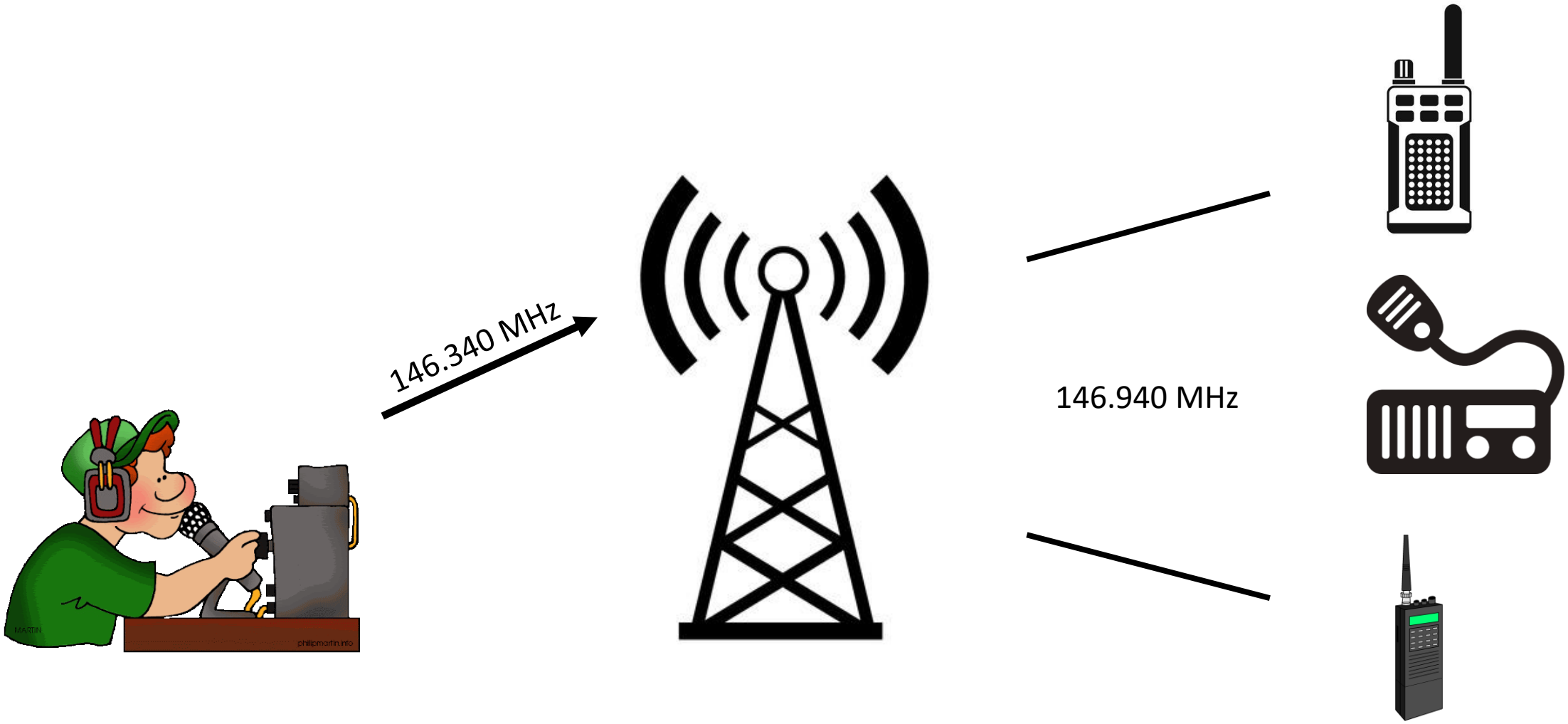
What is Project 25?

- Common Air Interface (CAI)
  - Specifies the type and content of signals transmitted by compliant radios
- Subscriber Data Peripheral Interface
- Fixed Stations Interface
- Console Subsystem Interface
- Network Management Interface
- Data Network Interface
- Telephone Interconnect Interface
- Inter-RF Subsystem Interface

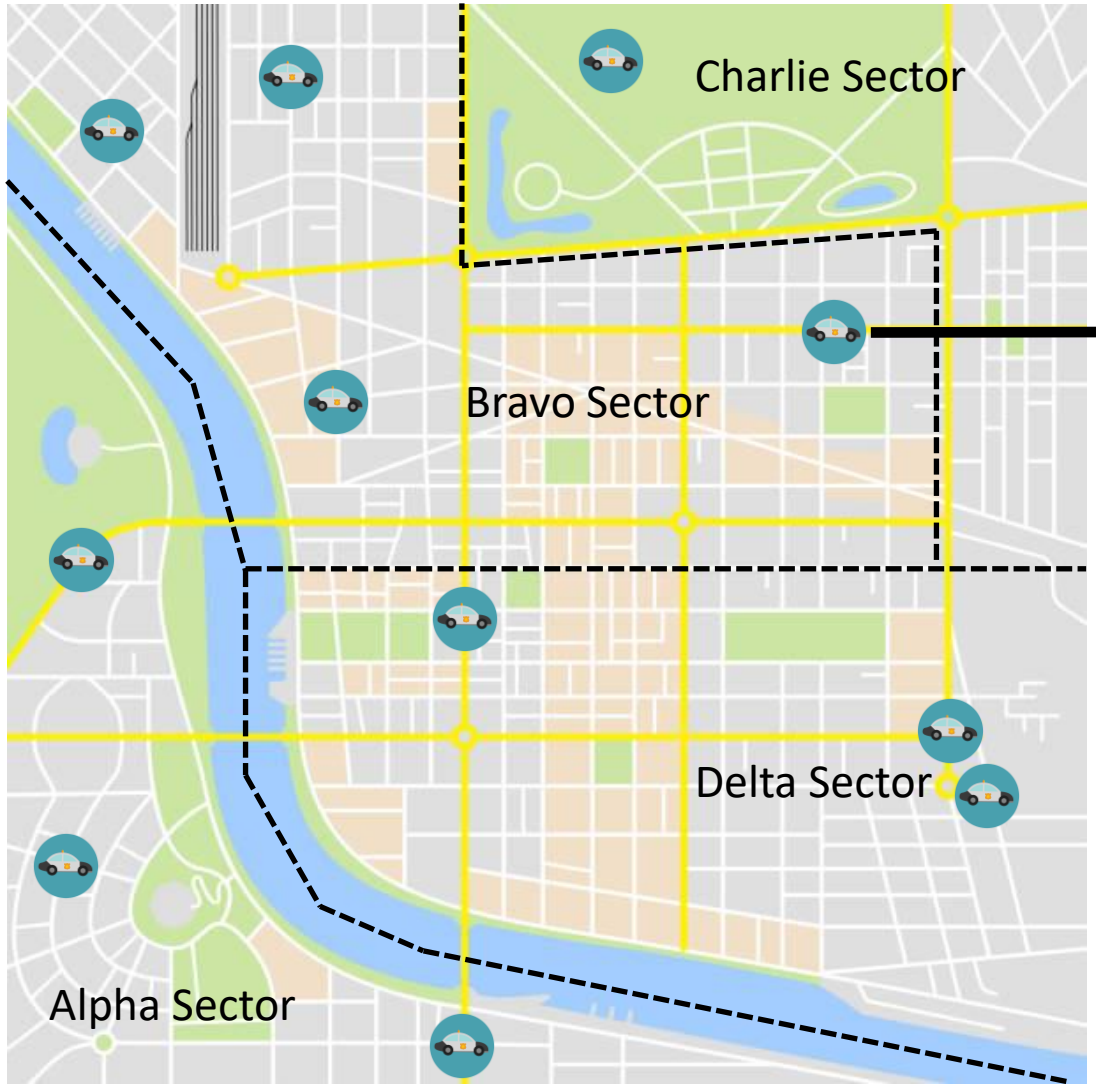
What is Project 25?

- **Common Air Interface (CAI)**
  - **Specifies the type and content of signals transmitted by compliant radios**
- Subscriber Data Peripheral Interface
- Fixed Stations Interface
- Console Subsystem Interface
- Network Management Interface
- Data Network Interface
- Telephone Interconnect Interface
- Inter-RF Subsystem Interface

A brief introduction to trunked radio



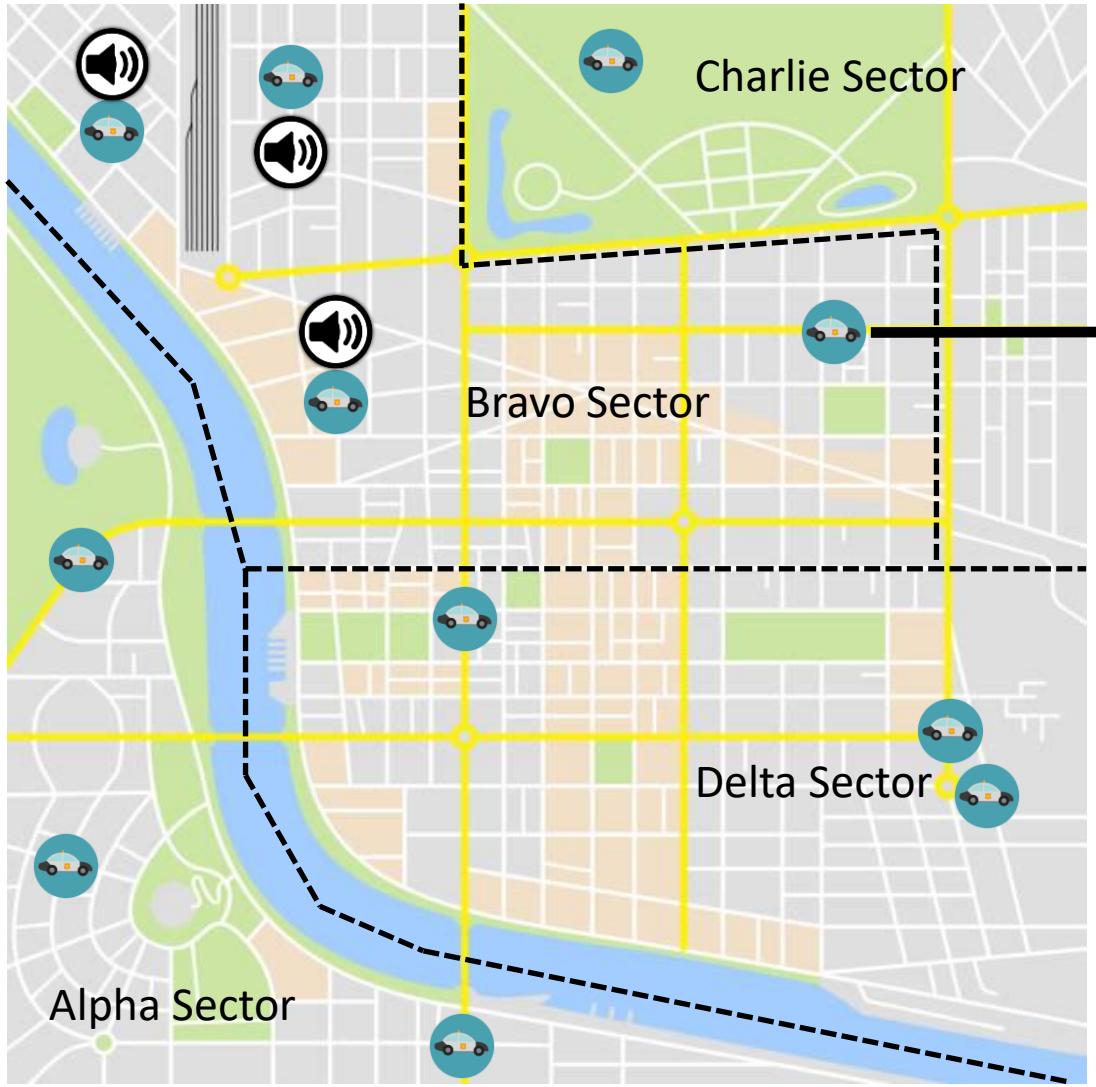
A brief introduction to trunked radio



input frequency
voice traffic

output frequency
voice traffic

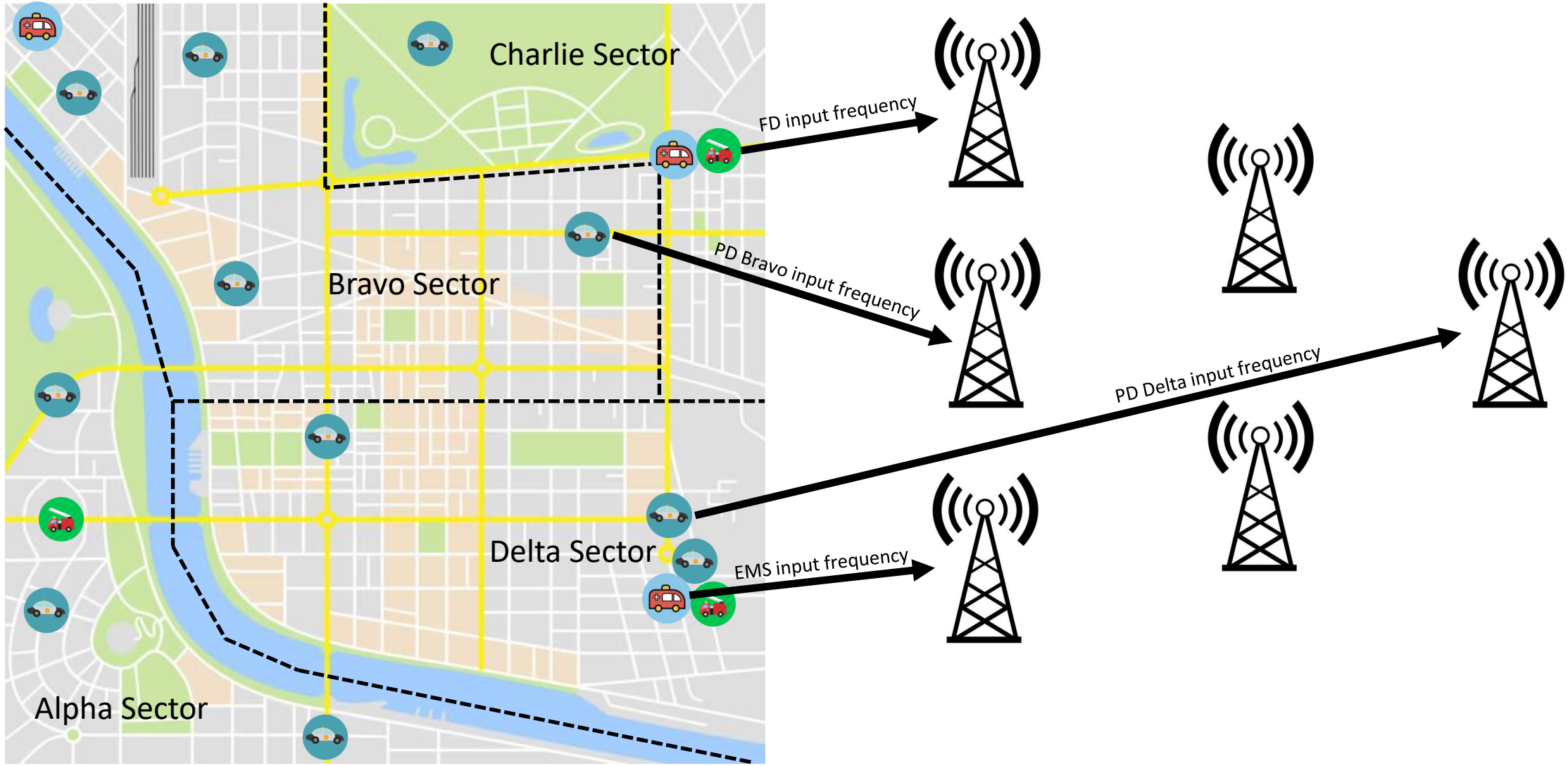
A brief introduction to trunked radio



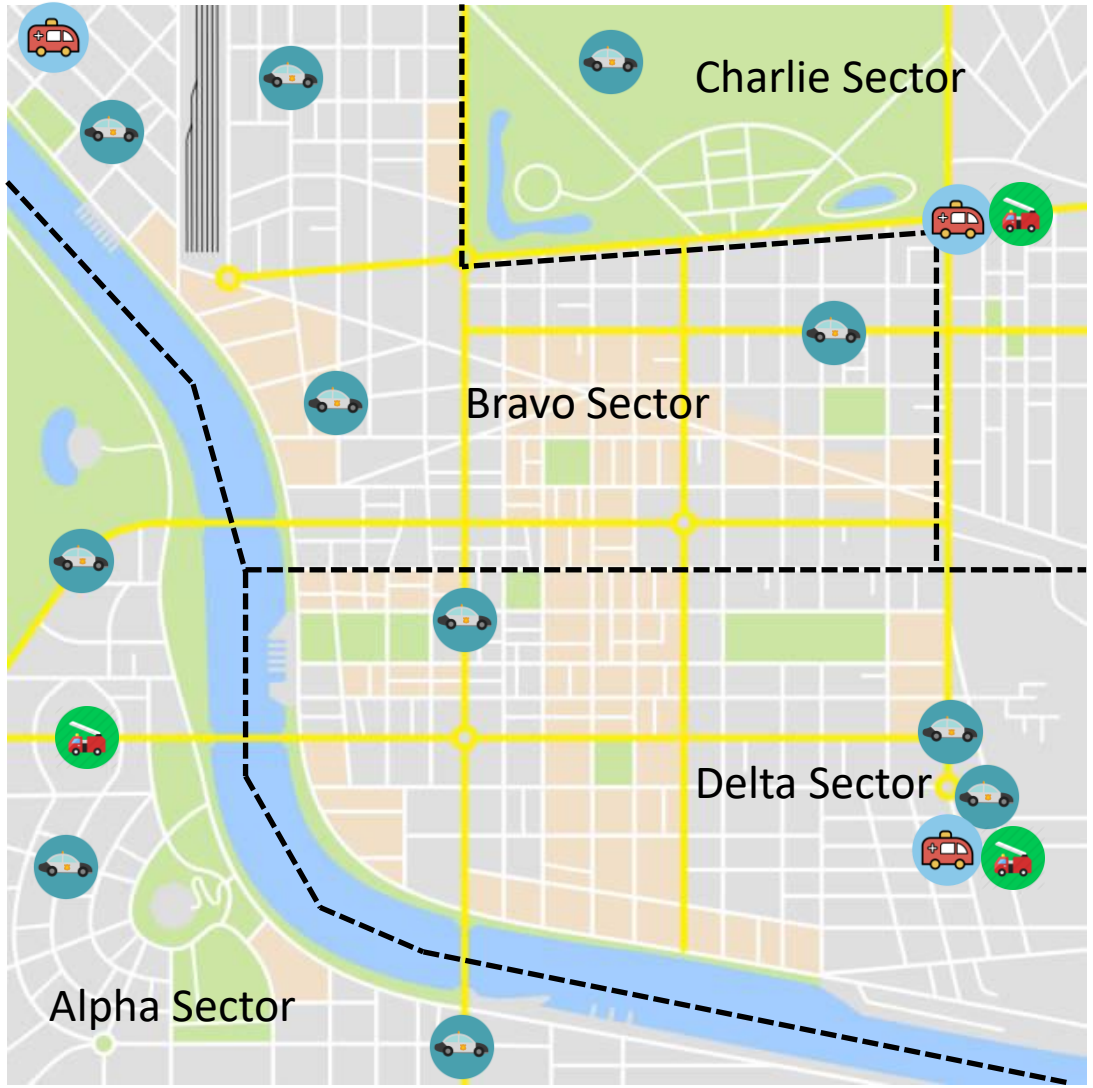
input frequency
voice traffic + CTCSS tone

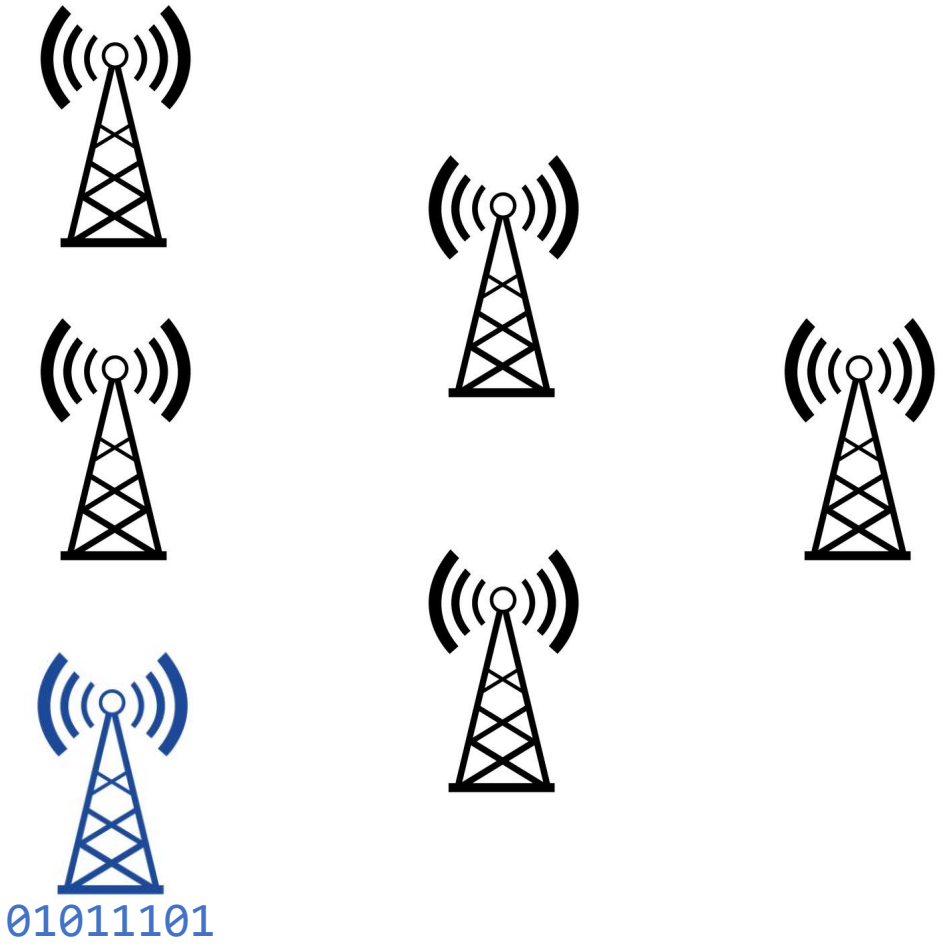
output frequency
voice traffic + CTCSS tone

A brief introduction to trunked radio

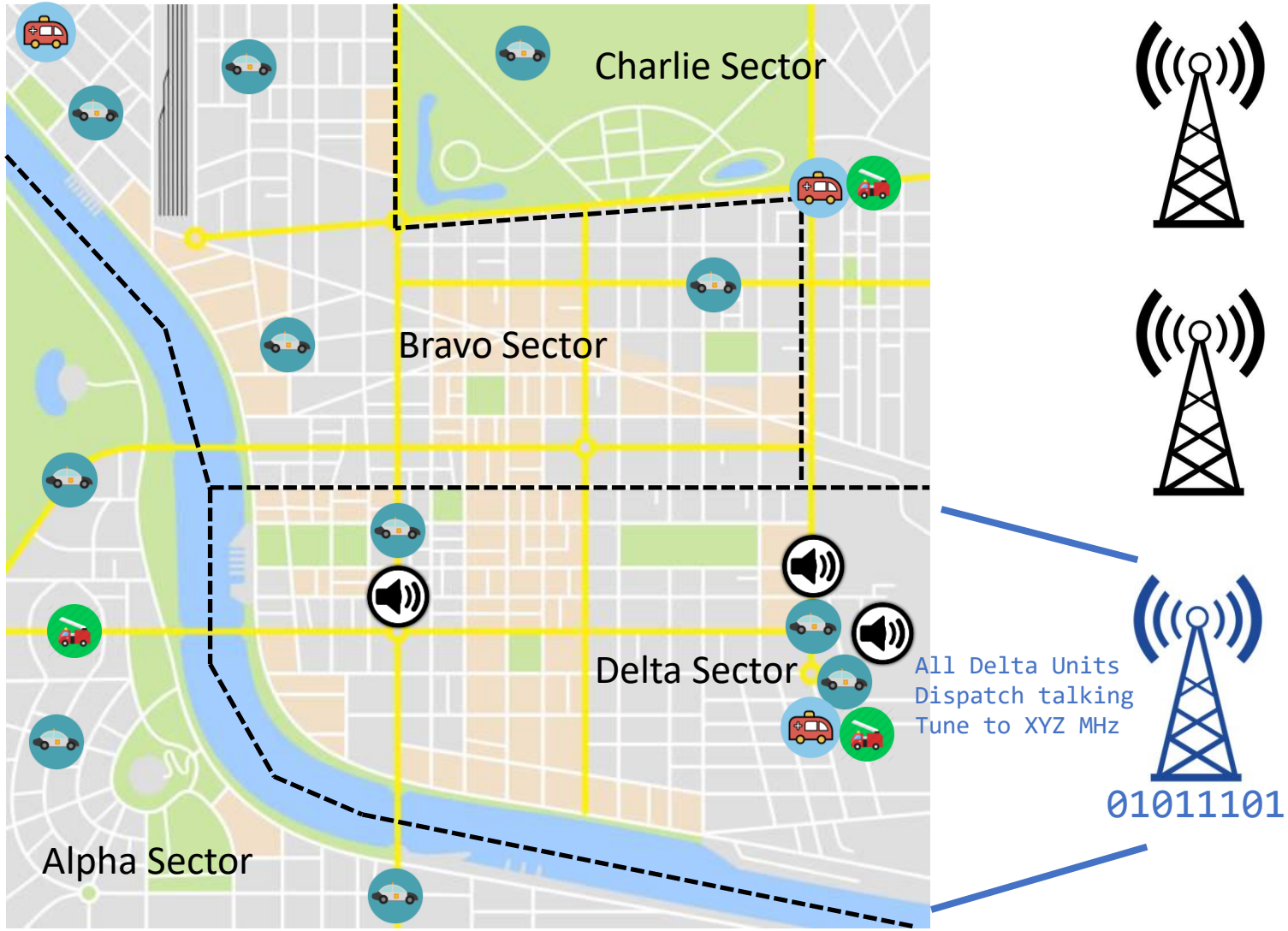


A brief introduction to trunked radio



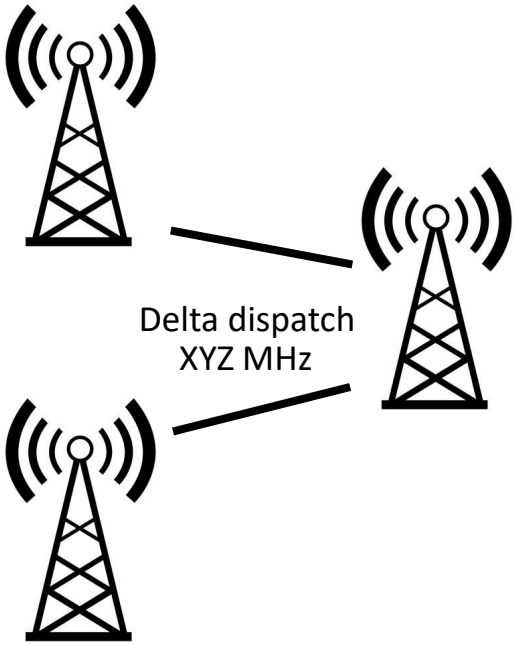


A brief introduction to trunked radio

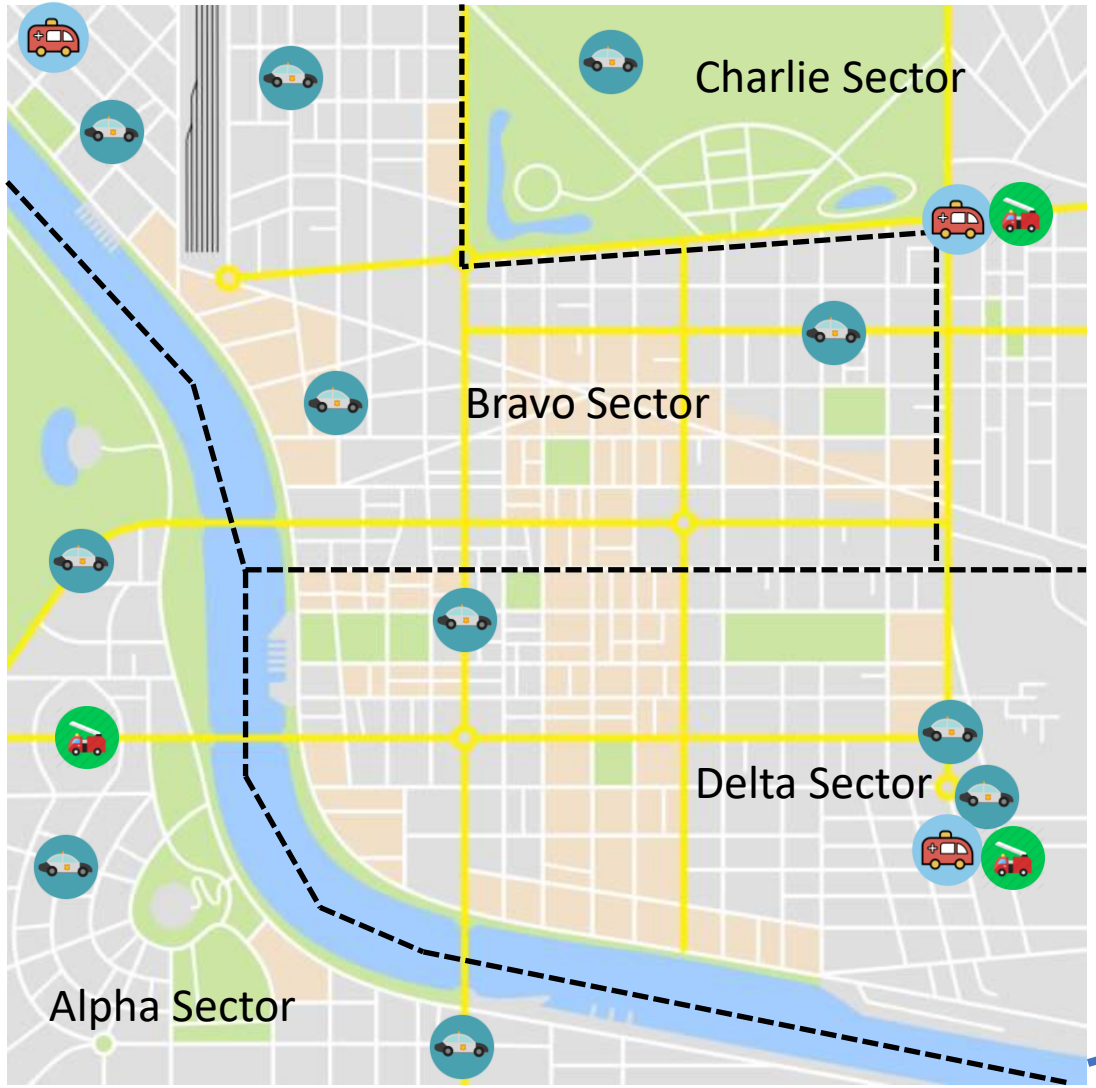


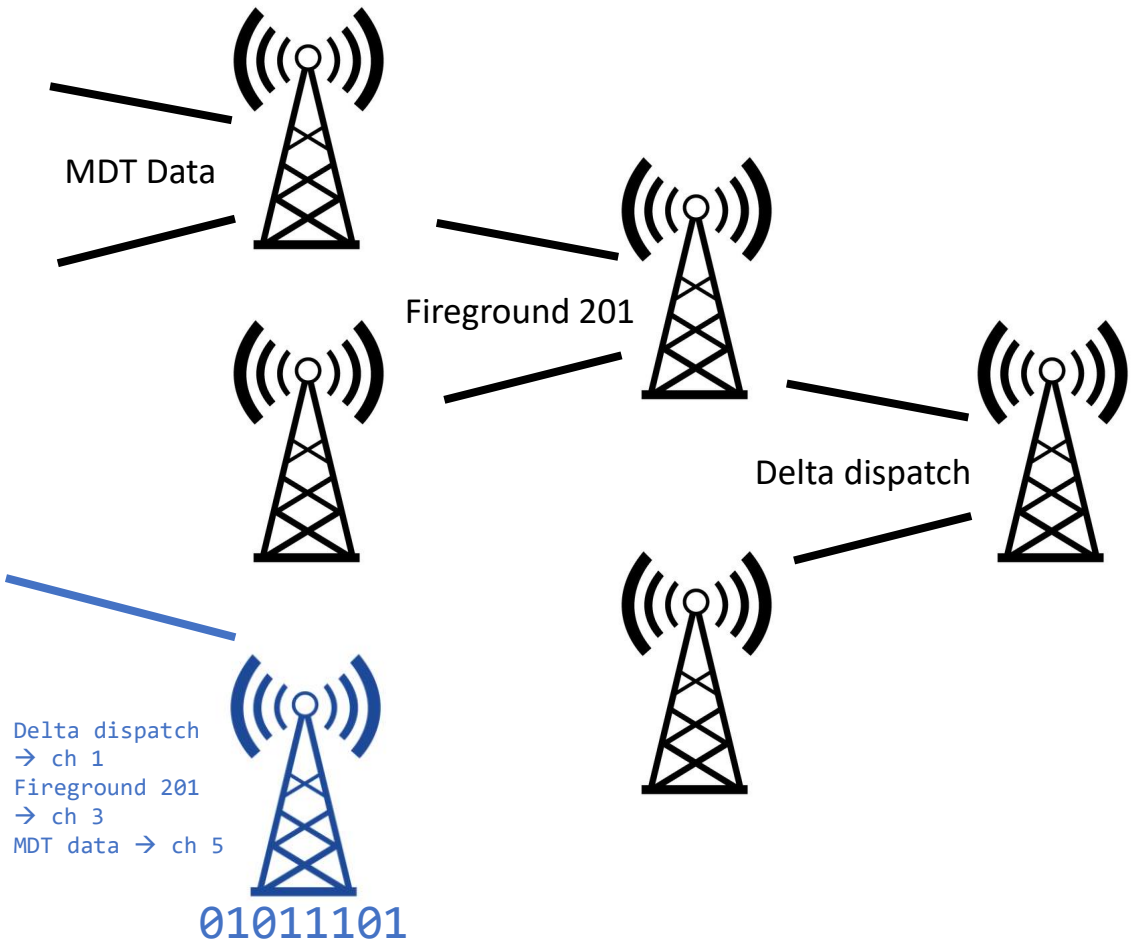
All Delta Units
Dispatch talking
Tune to XYZ MHz

01011101

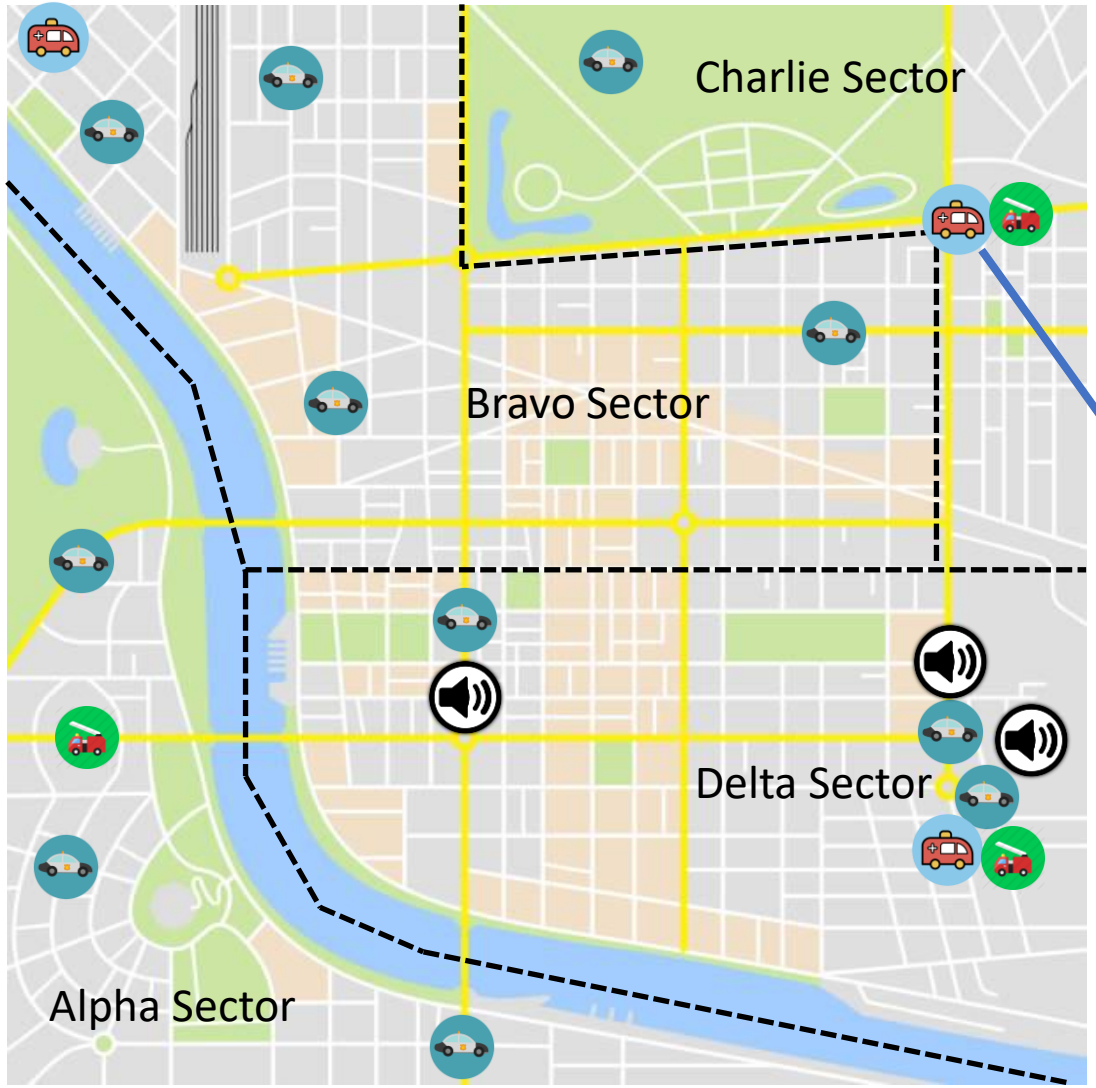


A brief introduction to trunked radio

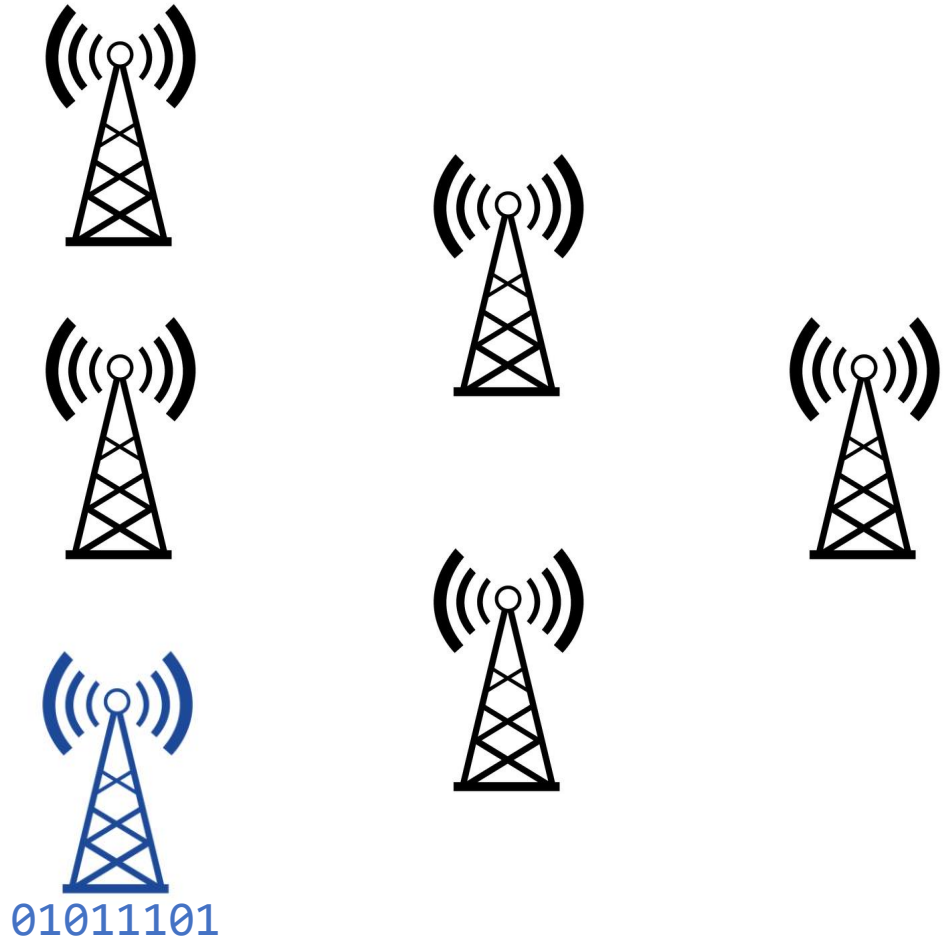




A brief introduction to trunked radio



Engine 17
Emergency



A brief introduction to trunked radio

- Greater Austin/Travis County Regional Radio System (GATRRS)
  - Project 25 Phase I system
  - 66 sites covering 40 counties

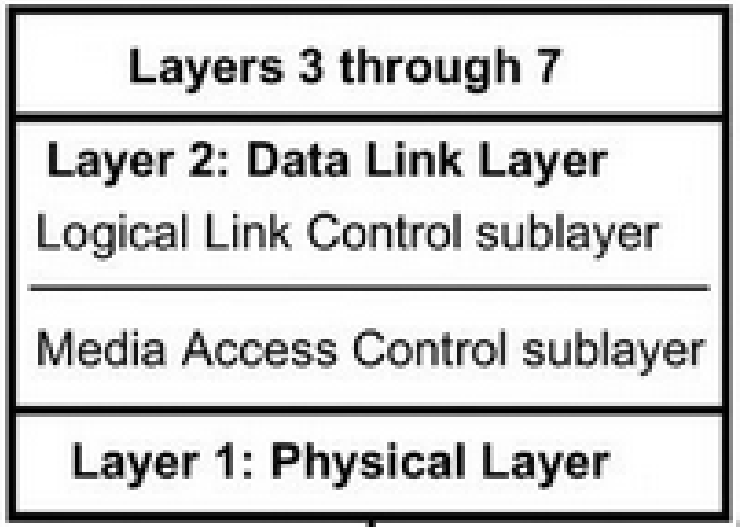
RFSS	Site	Name	County	Freqs						
1 (1)	001 (1)	Simulcast 1	Travis	851.0375	851.1625a	851.2875c	851.4125a	851.5625a	851.7125	851.8125
				851.925	852.0875	852.1125	852.3125	852.3375	852.575	852.600
				852.825	852.850	853.100	853.125	853.3625	853.425	853.625
				853.6875	853.875	853.950				
1 (1)	002 (2)	Simulcast 2	Travis	851.0625	851.1375c	851.3125a	851.3875a	851.5875a	851.7375	851.8375
				852.1625	852.4125	852.6375	852.6875	852.950	853.050	853.275
				853.325	853.550	853.575	853.825	853.850		
1 (1)	003 (3)	Marble Falls IR	Travis	852.800c	853.150a	853.750				
1 (1)	004 (4)	Honeycomb IR	Travis	852.2625	852.725c	853.175a	853.775a			
1 (1)	005 (5)	Burleson Manor IR	Travis	851.8875	852.2875	853.225c	853.525a	853.925a		
1 (1)	006 (6)	USGS Shingle IR	Travis	852.6625	852.925c	853.400a	853.800a			
1 (1)	008 (8)	Fayette County	Fayette	851.7875	852.050c	852.475	852.975			
1 (1)	009 (9)	Creedmoor IR	Travis	851.8625	852.2125c	852.900a	853.250a	853.500a		
1 (1)	010 (A)	Central Austin	Travis	769.21875c	769.45625a	769.68125	769.91875a	770.14375	770.40625	
1 (1)	011 (B)	Del Rio	Val Verde	151.040c	154.370	155.3175a	156.180			
1 (1)	012 (C)	Eagle Pass	Maverick	151.4375	154.0175a	155.2575c	156.1875			
1 (1)	013 (D)	Bracketville	Kinney	151.010c	154.2575	155.6775				
1 (1)	014 (E)	Uvalde	Uvalde	151.115	154.8825c	155.670a	156.2025			
1 (1)	015 (F)	Crystal City	Zavala	151.0625	154.8825	155.145c	156.1425a			
1 (1)	016 (10)	Carrizo Springs	Dimmit	151.0475c	154.1075a	155.2425	155.7675			
1 (1)	017 (11)	Barksdale	Real	154.415	154.9275a	155.2725c				
1 (1)	018 (12)	El Indio	Webb	156.0825c	156.210	158.9475a				
1 (1)	019 (13)	Utopia	Uvalde	158.8275a	159.120	159.1575c				
1 (1)	020 (14)	Williamson Simulcast	Williamson	854.9625	854.9875	855.2125	855.7125	855.9875	856.6875	856.9625
				856.9875	857.9625c	857.9875	858.9625a	858.9875	859.5875a	859.9625a
				859.9875						
1 (1)	023 (17)	Loma Alta	Val Verde	153.8225c	154.0325a	154.100	154.2125			

Austin Fire Department Talkgroups

DEC	HEX	Mode	Alpha Tag	Description
1121	461	D	AFD FCOM N	Firecom North
1122	462	D	AFD FCOM E	Firecom East (ESD's East of I35)
1123	463	D	AFD FCOM S	Firecom South
1124	464	D	AFD 1124	TG 1124
1142	476	D	AFD FCOM W	Firecom West (ESD's West of I35)
1403	57b	D	TC FIRENET	Firenet-linked to 153.950
1127	467	D	AFD ARSON 1	Arson Com 1
1159	487	DE	AFD BC	Battalion Chief
1155	483	D	AFD SPECOP	Special Operations
1146	47a	D	EM AFD	Emergency
1147	47b	D	AFD LOCUTION	City Locution Dispatch (with 154.965 MHz paging)
1162	48a	D	TCFD LOCUTION	County Locution Dispatch (with 154.205 MHz paging)
1371	55b	D	AFD FTAC201	Fire Tac 201
1372	55c	D	AFD FTAC202	Fire Tac 202
1373	55d	D	AFD FTAC203	Fire Tac 203
1374	55e	D	AFD FTAC204	Fire Tac 204
1375	55f	D	AFD FTAC205	Fire Tac 205
1376	560	D	AFD FTAC206	Fire Tac 206
1377	561	D	AFD FTAC207	Fire Tac 207
1378	562	D	AFD FTAC208	Fire Tac 208
1379	563	D	AFD FTAC209	Fire Tac 209
1380	564	D	AFD FTAC210	Fire Tac 210
1381	565	D	AFD FTAC211	Fire Tac 211
1382	566	D	AFD FTAC212	Fire Tac 212
1383	567	D	AFD FTAC213	Fire Tac 213
1384	568	D	AFD FTAC214	Fire Tac 214
1385	569	D	AFD FTAC215	Fire Tac 215
1386	56a	D	AFD FTAC315	Fire Tac 315
1139	473	D	AFD ARFF Tac 301	Aircraft Rescue and Fire Fighting Tactical 301
1140	474	D	AFD ARFF Tac 302	Aircraft Rescue and Fire Fighting Tactical 302
1141	475	D	AFD ARFF Tac 303	Aircraft Rescue and Fire Fighting Tactical 303
1163	48b	D	AFD FTAC303	Fire Tac 303

P25 Common Air Interface

- Standard specific for digital voice modulation and the digital signals transmitted by compliant radios
  - Access method, modulation, data rate and message format for P25 radios
  - Codified in TIA-102-BAAA-A standard document

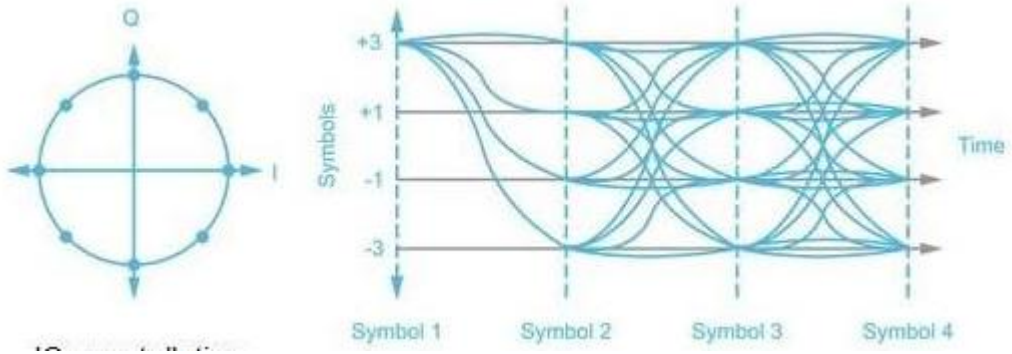


Physical layer

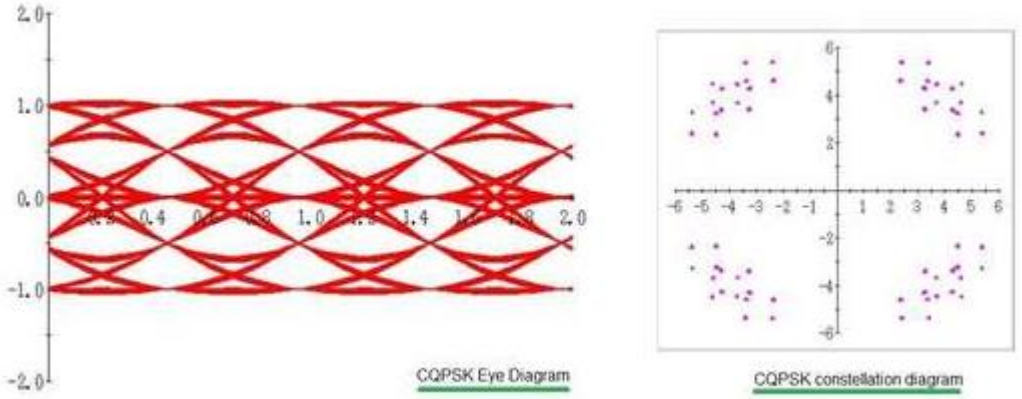
- Phase 1: Modulation is a form of π/4 differential QPSK
  - 4800 symbols (‘dibits’)/sec * 2 bits/symbol = 9600 bits/sec

Information Bits	Symbol	CQPSK Phase Change	C4FM Deviation
01	+3	+135 degrees	+1.80 kHz
00	+1	+45 degrees	+0.60 kHz
10	-1	-45 degrees	-0.60 kHz
11	-3	-135 degrees	-1.80 kHz

C4FM: Continuous 4-level FM
Constant amplitude carrier



CQPSK: Compatible/Continuous QPSK
Variable amplitude carrier



a.k.a. LSM (Linear Simulcast Modulation)

Physical layer

- Phase 2: 2-slot TDMA in 12.5 kHz channel
  - Provides two 6.25 kHz-equivalent channels
  - 30 ms slots
- H-DQPSK modulation (Harmonized – Differential QPSK) outbound
  - Essentially π/4 DQPSK with different filtering
- H-CPN (Harmonized – Continuous Phase Modulation) inbound

Physical layer

- 24-dibit frame synchronization
- Dibits are interleaved in data blocks to spread burst errors across the block
- Trellis encoding for error correction
  - Rate ½ code: 48 dibits in, 98 dibits out
    - Unconfirmed data blocks, including TSDUs
  - Rate ¾ code: 48 tribits in, 98 dibits out
    - Confirmed data blocks

transmitted first ↓ transmitted last ↓

```
0000    0100    1100    1111    0101    1111
  0       4       C       F       5       F
```

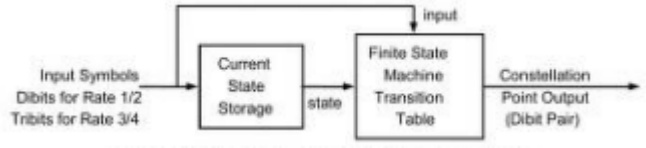
where "1" = di-bit (11) and "0" = di-bit (01)
The expanded vector is:

```
01010101  01110101  11110101  11111111  01110111  11111111
  5   5     7   5     F   5     F   F     7   7     F   F
```

111113113311333313133333

INTERLEAVE TABLE

Output Index	Input Index	Output Index	Input Index	Output Index	Input Index	Output Index	Input Index
0	0	26	2	50	4	74	6
1	1	27	3	51	5	75	7
2	8	28	10	52	12	76	14
3	9	29	11	53	13	77	15
4	16	30	18	54	20	78	22
5	17	31	19	55	21	79	23
18	72	44	74	68	76	92	78
19	73	45	75	69	77	93	79
20	80	46	82	70	84	94	86
21	81	47	83	71	85	95	87
22	88	48	90	72	92	96	94
23	89	49	91	73	93	97	95
24	96						
25	97						



Media access layer

- Voice and data messages are sent over the air as data units
- Voice-related data units
  - HDU – Header Data Unit
  - LDU1/LDU2 – Logical Link Data Unit
  - TDU – Terminator Data Unit
  - TDULC – Terminator Data Unit with Link Control
- Data-related data units
  - PDU – Packet Data Unit (variable length data unit)
  - TSDU (a.k.a. TSBK) – Trunked Signalling Data Unit (Block)
    - Not part of CAI
- Heavy use of error correction and detection codes (Golay, Hamming, Reed-Solomon, CRC)

Media access layer/Channel access

- Data units begins with frame sync and network identification (NID)
  - NAC: Uniquely describes the system
  - DUID: Indicates the type of data unit to follow
- Status symbols
  - Injected periodically within data units to indicate status of channel
- Data packets include protection flag for encrypted payloads

↓ transmitted first — transmitted last ↓

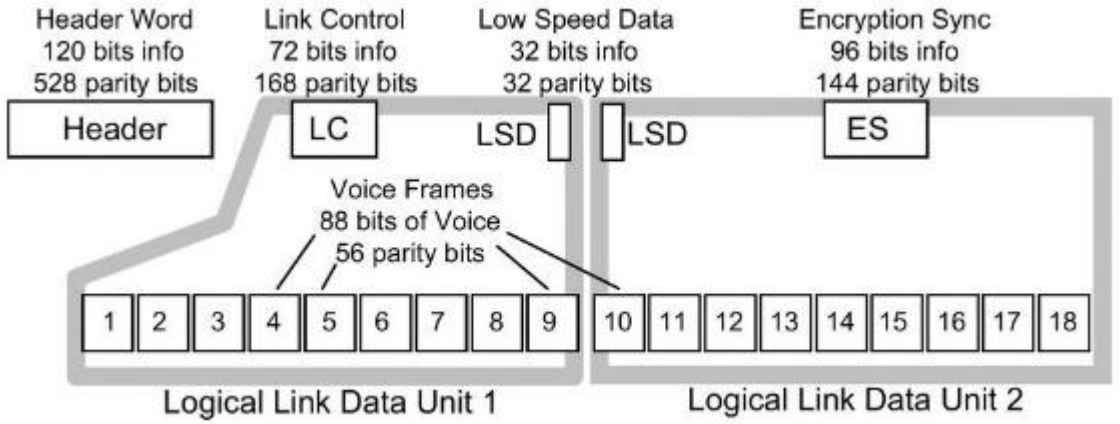
Network Access Code												Data Unit ID			
A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1	A0	S3	S2	S1	S0
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

Data Unit ID	P	Data Unit Usage
%0000	0	Header Data Unit
%0011	0	Terminator without subsequent Link Control
%0101	1	Logical Link Data Unit 1
%1010	1	Logical Link Data Unit 2
%1100	0	Packet Data Unit
%1111	0	Terminator with subsequent Link Control

Status Symbol	Meaning	Usage
01	Inbound Channel is Busy	Repeater
00	Unknown, use for talk-around	Subscriber
10	Unknown, use for inbound or outbound	Repeater or subscriber
11	Inbound Channel is Idle	Repeater

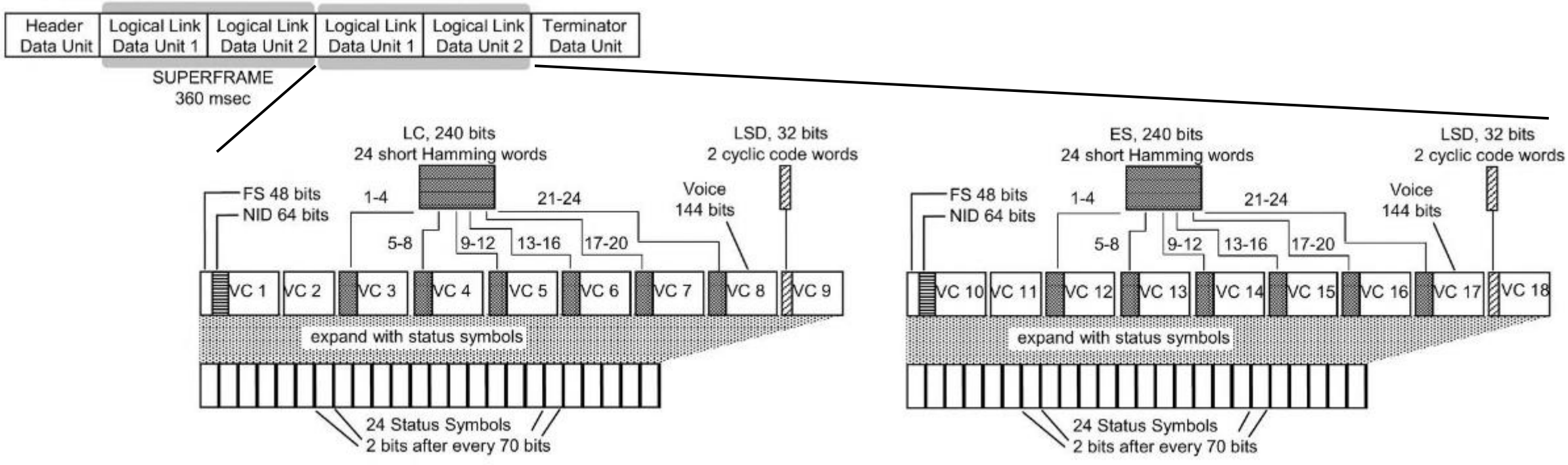
P25 voice traffic

- Voice traffic encoded as Improved Multi-Band Excitation (IMBE)
  - IMBE frames encode 20 ms of speech into 88 bits of information
    - Pitch, voicing, quantized gain for each audio band
  - Continuous average of 4.4 kbps



P25 voice traffic

- Voice traffic begins with HDU, then alternating LDUs, then a TDU/TDULC
  - LDU1/2 pair comprise 360 ms of audio data
  - Link control, encryption sync, and low speed data embedded within LDUs



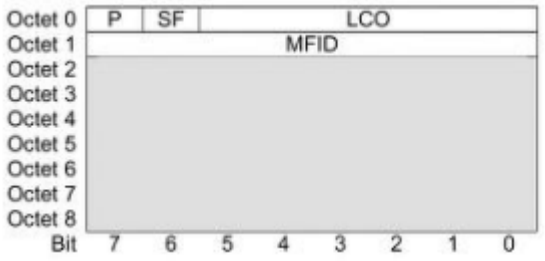
P25 voice traffic

- IMBE frame contents
  - Quantized pitch (8 bits)
  - Voicing vector information (3-12 bits, one bit per band)
  - Quantized average frame gain level (6 bits)
  - Quantized gain vector and DCT coefficients (remainder)
  - Sync (1 bit)
- TIA-102.BABA document describes the vocoder implementation
  - NOTE: IMBE is a patented technology of Digital Voice Systems, Inc. (DVSI)

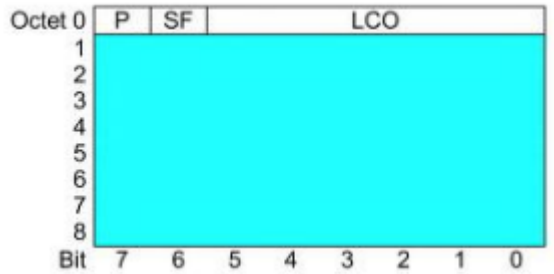
P25 voice traffic link control information

- Link control information embedded within voice messages or in TDULC packet
  - Identification information and control information for notifying listeners on a voice call of system events and status
- Used in conventional and trunked system
- Messages and formats described in TIA-102-AABF-A

Explicit MFID (SF==0)



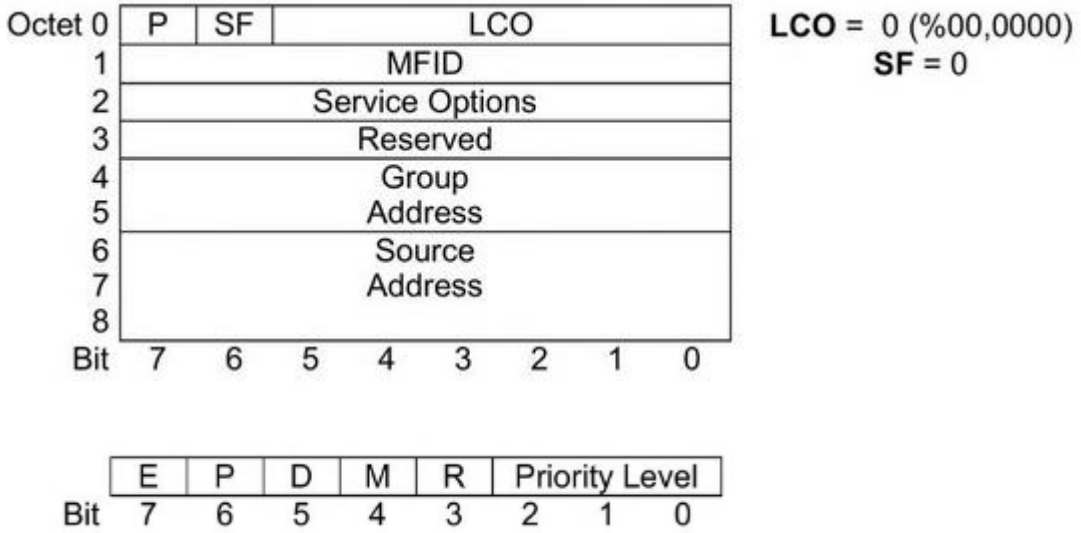
Implicit MFID (SF==1)



Link control information example

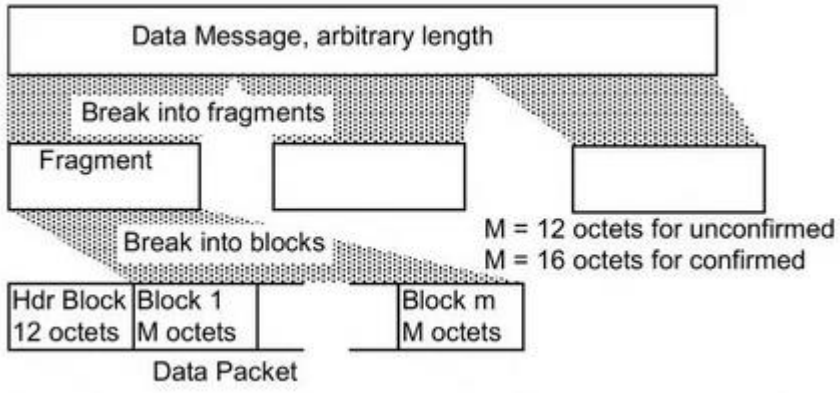
- Group Voice Channel User LC message
  - Indicates user of this channel for group voice traffic

- Group address defines whom the user is addressing
- Source address is the user of the channel
- Service options indicate type of service being requested (E==emergency)



P25 data traffic

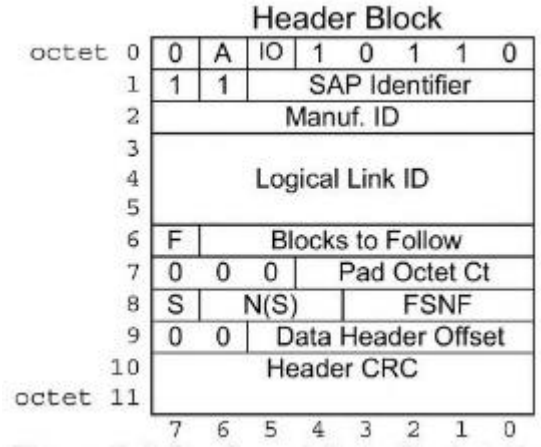
- PDU – Packet Data Unit
  - Data is split into packets beginning with a header and then blocks of 12 or 16 bytes
- Packet data can be confirmed or unconfirmed
  - Confirmed: Receiver can request retransmission of individual blocks
  - Unconfirmed: Single CRC over entire payload; no retry



P25 data traffic

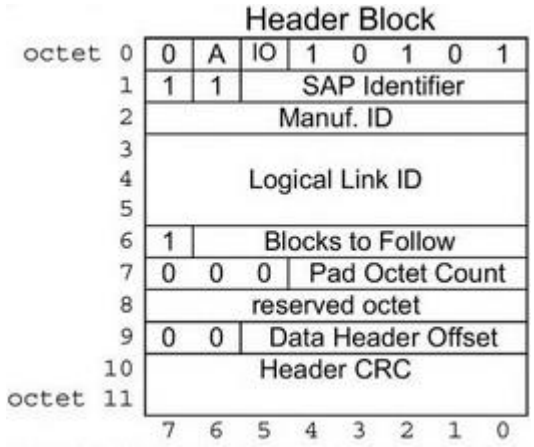
- PDU header is 12 bytes
  - IO indicates inbound or outbound message
  - Logical Link ID indicates subscriber unit source or destination
  - Confirmed header has additional sequence number synchronization fields

Confirmed (A==1)



S – Sequence # resync flag
N(S) – Sequence # of packet
FSNF – Fragment sequence #

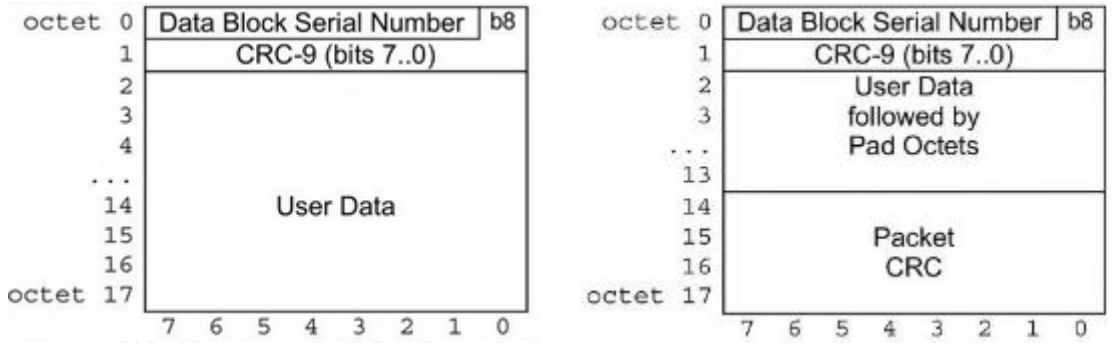
Unconfirmed (A==0)



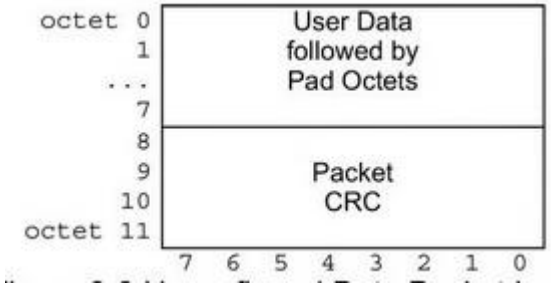
P25 data traffic

- Confirmed packet blocks contain serial number and per-block CRC
  - Last block has packet-wide CRC
- Unconfirmed packet blocks message-wide CRC on last block

Confirmed data blocks (1..N-1, N)



Unconfirmed data blocks



P25 data traffic

- Confirmed data receiver sends an acknowledge response
  - Class, type, and status specify the meaning of the response
- Selective retry encoded in following blocks
  - 1 or 2 blocks can follow to selectively resend up to 127 blocks

Acknowledgment

octet		7	6	5	4	3	2	1	0
	0	0	0	IO	0	0	0	1	1
	1	Class		Type				Status	
	2	Manuf. ID							
	3	Logical Link ID							
	4								
	5								
	6	X	Blocks To Follow						
	7	Source Logical Link ID (when X = 0)							
	8								
	9								
	10	Header CRC							
octet	11								

Class	Type	Status	Meaning
%00	%001	N(R)	ACK -- All blocks successfully received
%01	%000	N(R)*	NACK -- Illegal Format
%01	%001	N(R)	NACK -- Packet CRC (32-bit) parity check failure
%01	%010	N(R)	NACK -- Memory Full
%01	%011	FSN	NACK -- Out of logical sequence FSN
%01	%100	N(R)	NACK -- Undeliverable
%01	%101	V(R)	NACK -- Out of sequence, N(S) ≠ V(R) or V(R)+1
%01	%110	N(R)	NACK -- Invalid User disallowed by the system
%10	%000	N(R)	ACK -- Selective Retry for some blocks

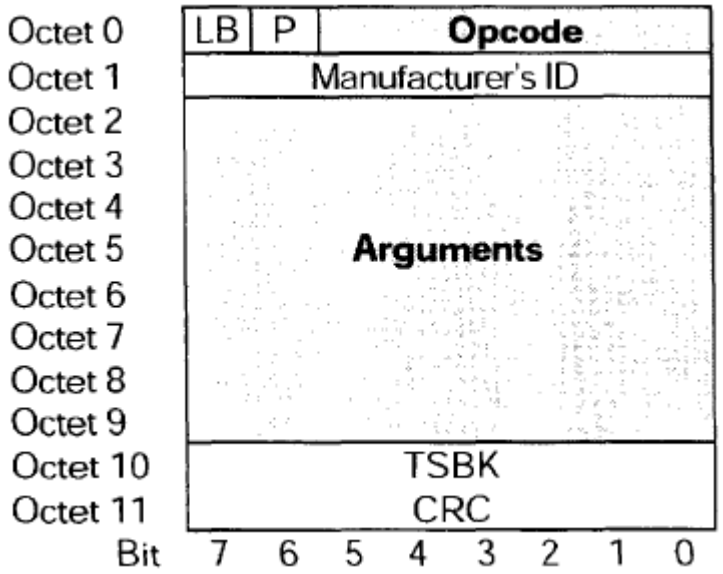
octet		f7	f6	f5	f4	f3	f2	f1	f0
	1	15		.	.	.		f9	f8
	2	23		.	.	.			16
	3	31		.	.	.			24
	4							33	32
	5								
	6								
	7								
	8	CRC							
	9								
	10								
octet	11								
		7	6	5	4	3	2	1	0

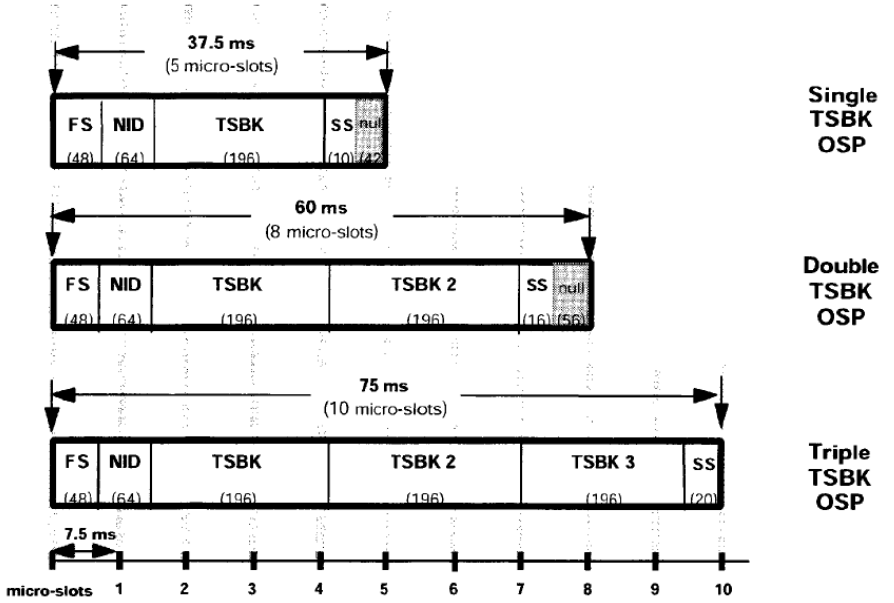
P25 trunking control

- Defined in TIA-102.AABB – but not part of the P25 CAI
- Allows trunked radio control channels to be transmitted on P25-compliant systems
- Two forms of trunk control channel message
  - Single and multiple block packet
- System independent and manufacturer-specific messages supported
  - TIA-102.AABC defines system independent common messages
- Micro-slots of 7.5 ms allow for consistent response time potential

P25 trunking control

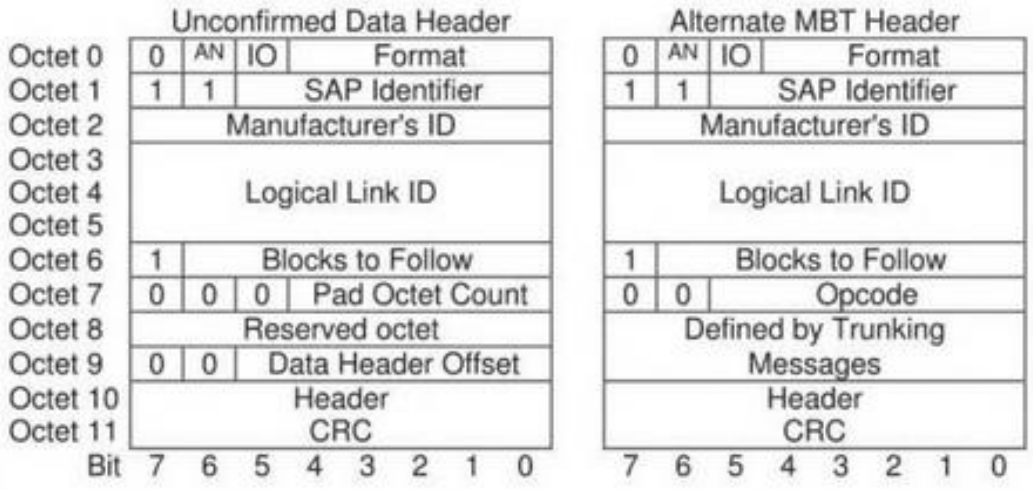
- Single block packet format
  - DUID of 7
- Single, double, and triple TSBKs supported



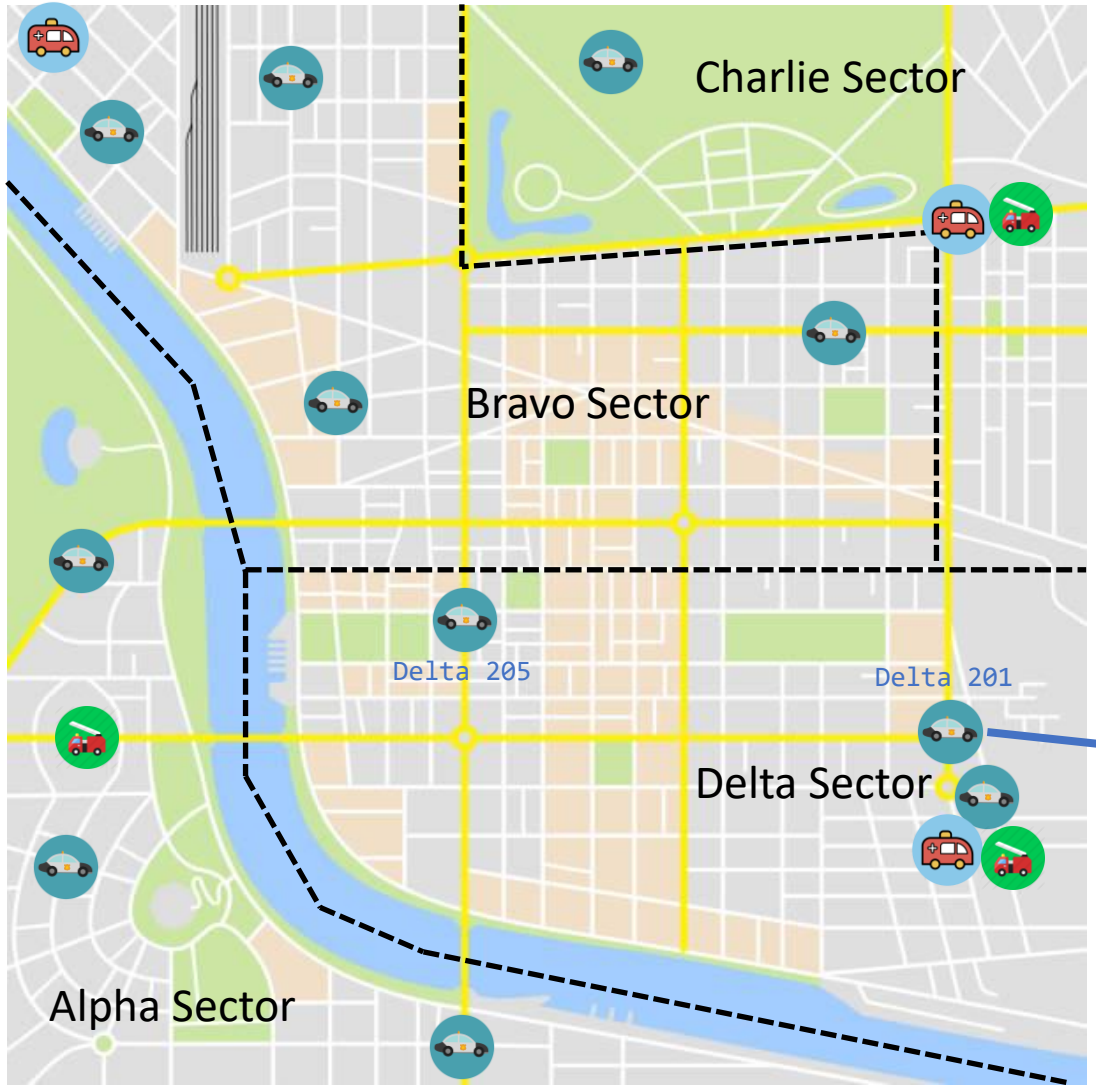


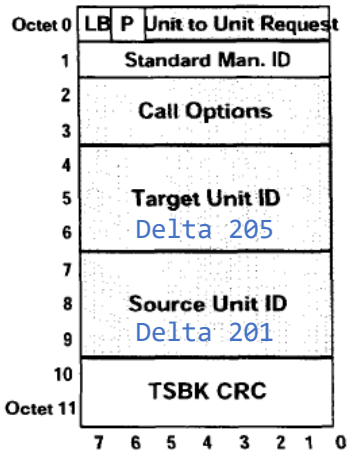
P25 trunking control

- Multiple block packet format
  - Same DUID and format as PDU



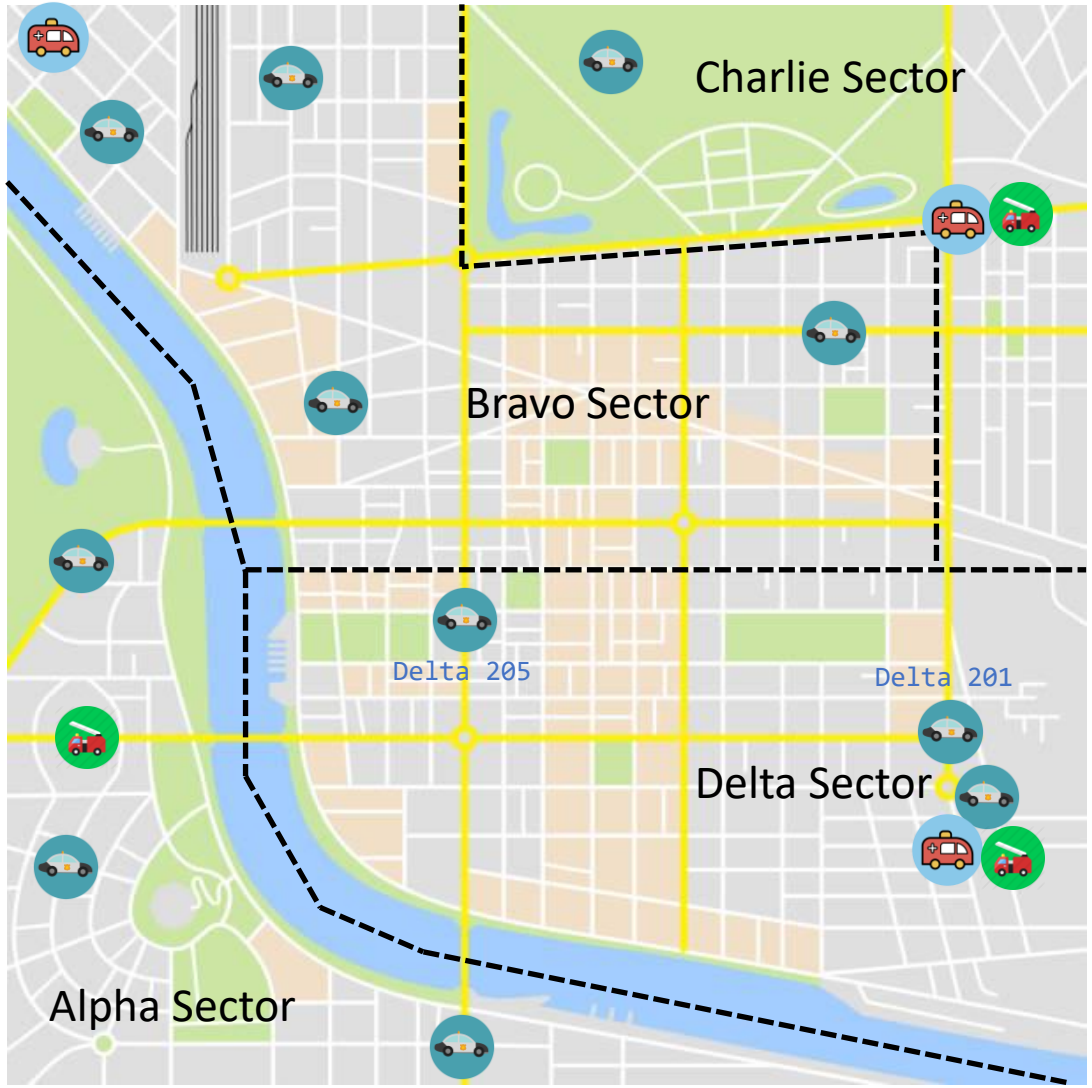
P25 trunking control example

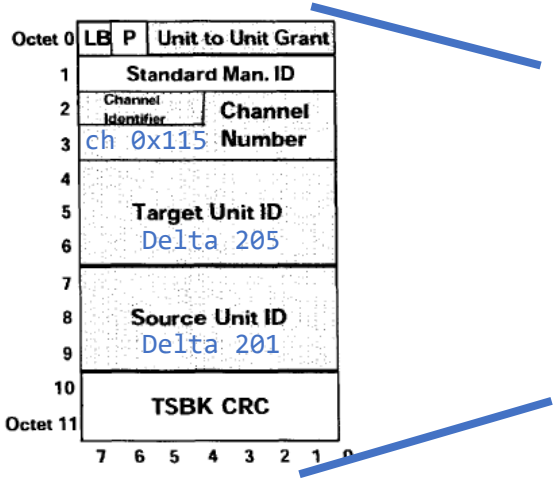




01011101

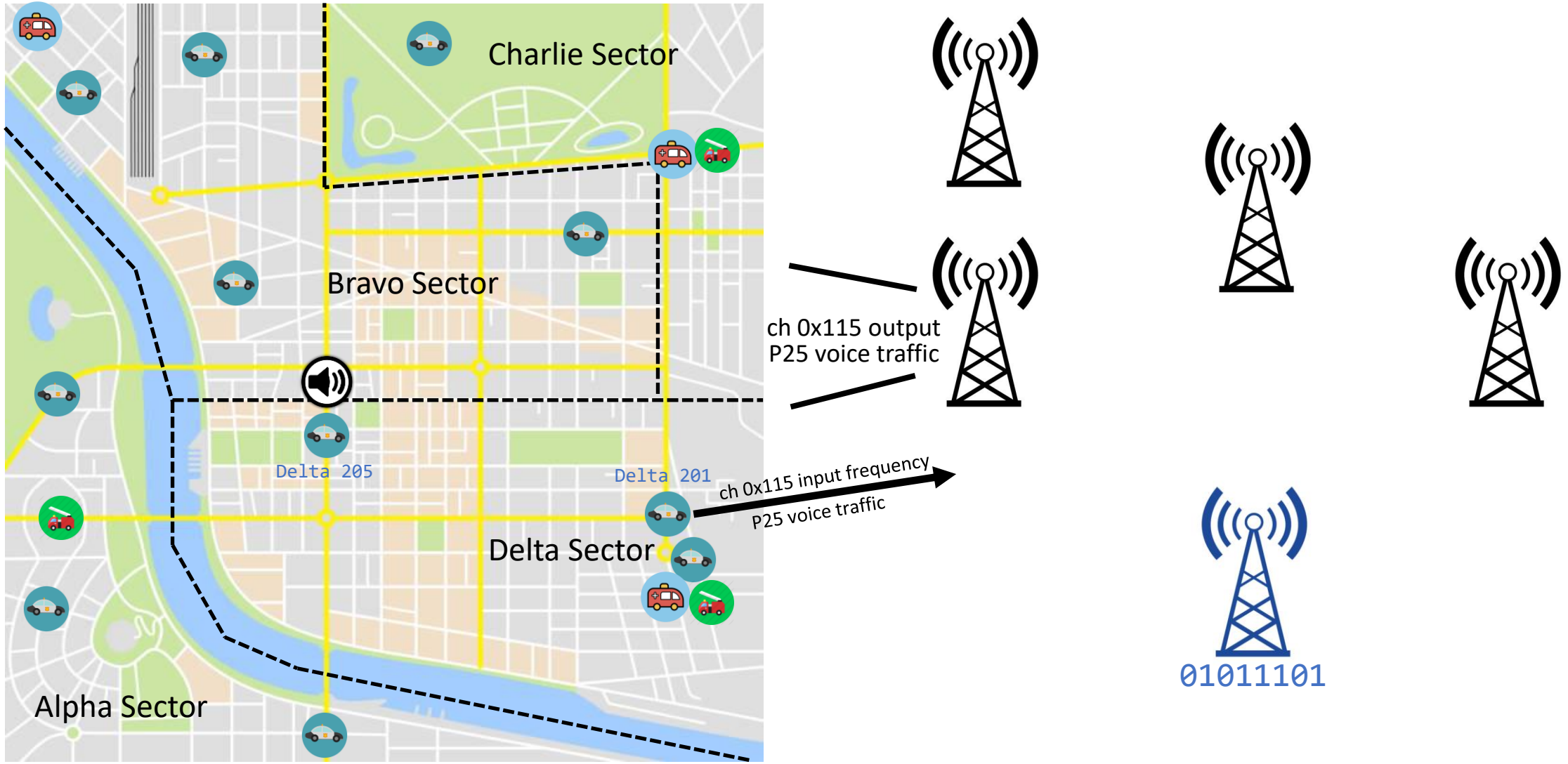
P25 trunking control example





01011101

P25 trunking control example



P25 GNU Radio experiments

CAVEAT PROGRAMMATOR!

- There are likely FAR better ways to do all of this
  - They've probably already been implemented
- My signal processing knowledge is very basic
- Code is >3 years old

P25 GNU Radio experiments

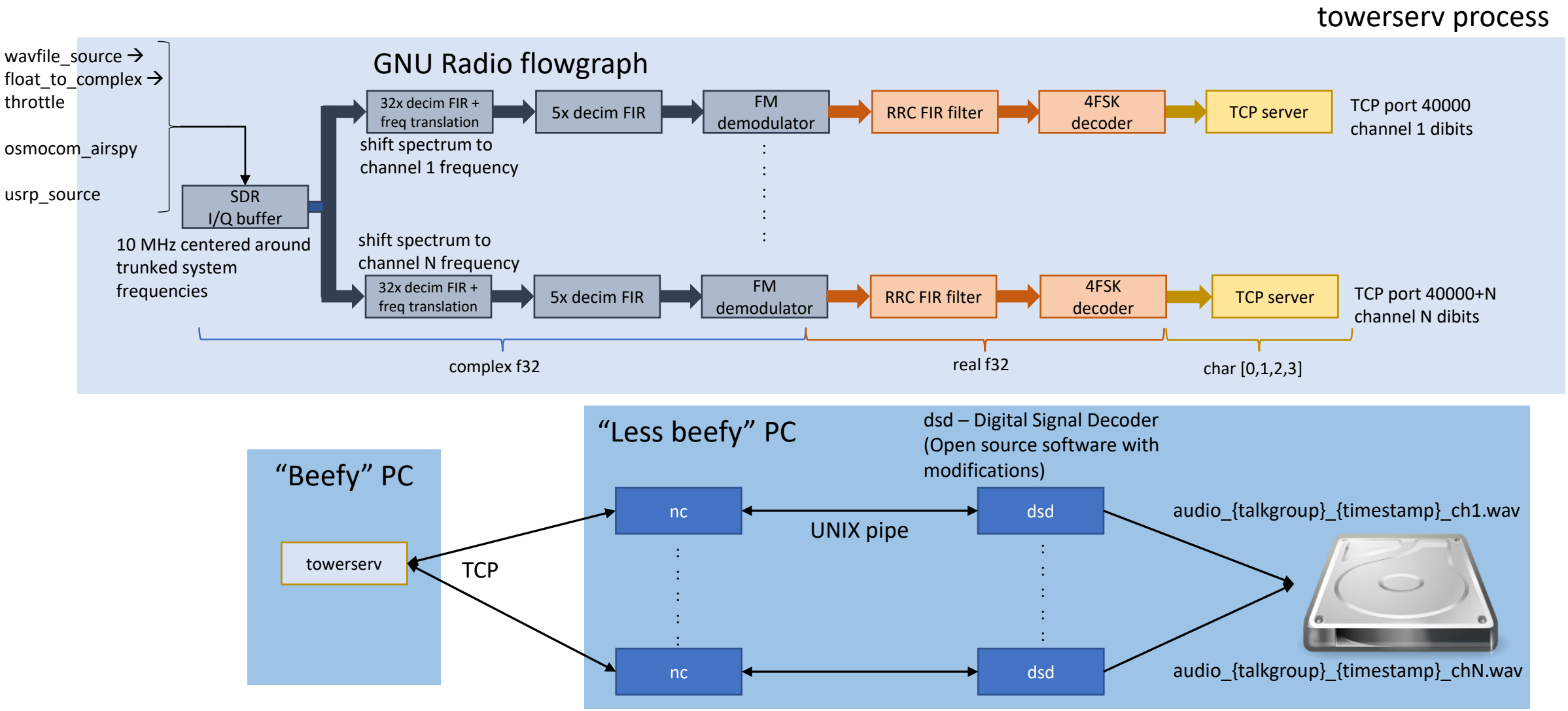
- “The Scanopticon”
  - Record all voice traffic on a trunked radio system to disk
  - Long-term: Web accessible audio with graphical per-talkgroup timelines

P25 GNU Radio experiments

- “The Scanopticon”
  - Record all voice traffic on a trunked radio system to disk
  - Long-term: Web accessible audio with graphical per-talkgroup timelines

“What is the most UNIXy way in which I could go about this?”

Scanopticon architecture



4FSK decoder

- Derived from gr-fsk4 OOT module
  - https://github.com/JohandeGraaf/gr-fsk4 (not original author)
- Small modifications
  - Removed message queue for fine frequency adjustments
  - Output ‘3’, ‘2’, ‘0’, ‘1’ based on slicing decision
- Also version that outputs packed bytes (4 dibits/byte) for a different experiment

dsd

- Digital Speech Decoder
  - https://github.com/szechyjs/dsd
- Major modifications
  - Accept pre-sliced dibits as input from file
    - Previously only accepted discriminator input from sound card/serial slicer
  - Remove all live audio playback functionality (disable PortAudio)
  - Write separate .wav files per transmission
    - Previously one huge .wav file per dsd instance
    - Uses link control information in LDU1/2 packets to determine channel user
  - Fix various bugs in the code
- NOTE: There is a gr-dsd block!

cc_mon

- Control channel message monitor (very basic)
  - Early research work for trunk scanner architecture
- Reads control channel dibits from socket
- Outputs group channel grant information
  - Which users are on which channels

```
patch grp ch upd     0-093 (851925000 Hz) tg  1122              [AFD Firecom East ESDs East of I35]
grp ch grant upd     0-0ff (852600000 Hz) tg   971              [APD Dispatch Adam Northwest]
grp ch grant upd     0-0d5 (852337500 Hz) tg   990              [APD Dispatch Ida North Central]
grp ch grant upd     0-019 (851162500 Hz) tg  3076              [AISD Police Primary]
grp ch grant upd     0-1ad (853687500 Hz) tg  2443              [TCSO Jail Ops]
grp ch grant upd     0-081 (851812500 Hz) tg   101              [Austin Energy Electric Dispatch]
patch grp ch upd     0-093 (851925000 Hz) tg  1122              [AFD Firecom East ESDs East of I35]
```

Demo

- Start up towerserv process
- Show TCP traffic on channel 16 (control channel)
- Run cc_mon utility
- Show nc/dsd pipe script
- Start nc/dsd pipe script
  - Explain output
- Show and play audio files

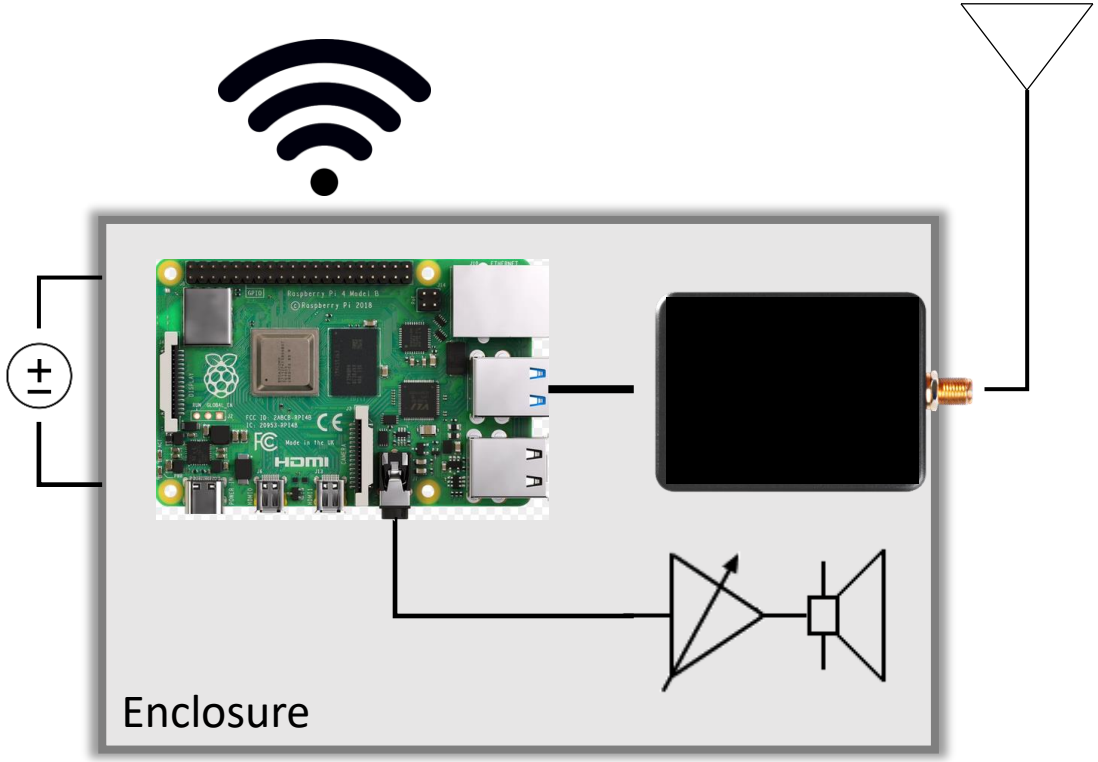
Other OSS libraries

- libmbe: Open source decoder for IMBE/AMBE packets
  - https://github.com/szechyjs/mbelib
  - Required by dsd to convert LDU packet data to audio
  - NOTE! Encumbered by DVSI patents
    - “For educational purposes only”
- it++ (itpp): C++ library of math, signal processing, and communications classes or functions
  - http://itpp.sourceforge.net/4.3.1/
  - Required by dsd for error detecting and correcting of P25 packet data

My dream

"DIY OSS Trunked Radio Scanner"

- RPi, SDR module, and audio amp/speaker in an enclosure
- Headless (web-based mobile friendly UI for interactive control)
- Wi-Fi enabled for updating, configuration, audio streaming, and cloud audio backup
- GNU Radio support, of course :)
  - Maybe even implemented in GR



Additional Resources

- https://archive.org/details/TIA-102_Series_Documents
  - Subset of TIA-102 documents
- https://www.radioreference.com/
  - Comprehensive radio systems database