Aspects of mobile live tracking over low coverage zones

CIVL Plenary 2025

Budva, Montenegro

Intro

- Live Tracking has moved from a “nice to have” option for some competitions to a critical safety tool, as well as being a key piece of the scoring and spectator viewing system.
- New applications and uses for tracking data open up new possibilities and are welcome, but come with additional usage of the cell network.
- In remote areas where many of our competitions are held, these new applications can consume more bandwidth than the network in some areas can provide.
- Until the cell service is upgraded in these remote areas, which is still several years in the future, we need to have a well designed and coordinated approach to live tracking to ensure that the potentially life saving data is not compromised by network saturation.
- **This document explains the basics of mobile communications for the purpose of live tracking.**

Basic parameters

- **Bandwidth** how wide is the transmission channel in KHz or MHz
- **Latency** (delay between data packages) in milliseconds, ms
- **Packet** size (Maximum transmission unit, **MTU**) in bytes, B

Comparison by bandwidth and packet size

Technology	Typical Bandwidth	Speed: Practical/ Theoretical	Notes	Packet Size Limit (MTU/PDU)	Latency	Notes
2G (GPRS)	200 kHz per channel	40-114 kbps	Uses GPRS for data. Very slow.	~500-1500 bytes	500 - 1,000 ms	Small packets due to narrow bandwidth and latency issues.
2.5G (EDGE/E)	200 kHz per channel	200-400 kbps	Enhanced version of GPRS, but still very limited.	~1500 bytes	~300-500 ms	Slightly improved due to better modulation.
3G (UMTS/WCDMA)	5 MHz per channel	384 kbps - 2 Mbps	First true mobile broadband.	~3000 bytes	~100-200 ms	Larger packets allow for more efficient data transmission.
3.5G (HSPA/HSPA+)	5 MHz per channel	Up to 42 Mbps	High-speed upgrade of 3G.	~3000-4000 bytes	~100 ms	Better data rates reduce fragmentation.
4G (LTE)	1.4 - 20 MHz per channel	100 Mbps - 1 Gbps	Much higher speeds with OFDM.	~9000 bytes (Jumbo Frames supported)	30-50 ms	Higher MTU improves performance for large data transfers.
5G (NR)	10 MHz - 400 MHz per channel	1 - 10 Gbps	Uses mmWave for extreme speeds.	~9000 bytes (or higher in some cases)	<10ms	Ultra-low latency and high-speed data allow efficient large packets.

Kbps – kilobit per second, b – bit, B – byte, 1B=8b (bit), ms – millisecond.

High latency in **2G (GPRS/EDGE)** is mainly caused by these factors:

1. **Circuit-Switched Network Design** – 2G was originally built for voice calls, not for fast data. Data transmission happens in small bursts, making it slow.

2. **Low Data Throughput** – GPRS (up to **114 kbps, but 40-50 in reality**) and EDGE (up to **384 kbps**) transmit small data packets, which take longer to be processed and reassembled.

3. **High Network Congestion** – 2G networks have **limited bandwidth**, meaning more users sharing the network increases delays.

4. **Multiple Time Slots for Data** – 2G splits connections into **timeslots** (TDMA), so **each user gets a small window to send data**, increasing waiting time.

5. **Longer Signal Processing Times** – Data compression and error correction in **2G radio channels** take longer compared to newer technologies.

6. **Long Distance to Towers** – 2G signals can travel farther than higher-frequency networks.

What if a packet is larger than network MTU?

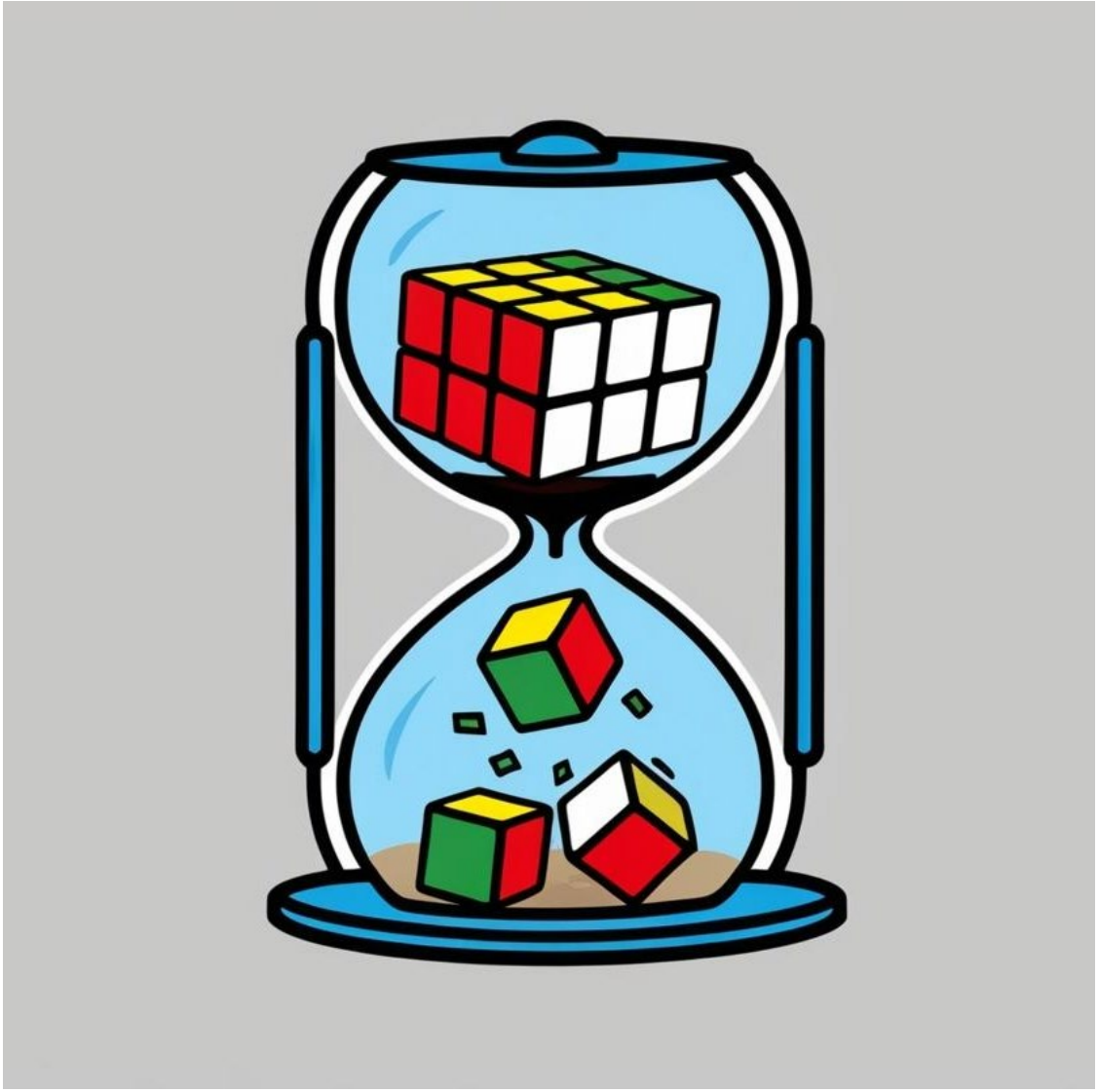
The packet will be split into packets that fit MTU.

E.g.3064B packet will be split into:

3 parts for 1500B MTU (EDGE)

Or

7 parts for 500 MTU (2G)



When Does MTU and Packet Count Matter?

- While **MTU and packet splitting do not change the raw transmission time**, they **do impact overall end-to-end delay** due to:

1. Acknowledgments (ACKs) & Latency

1. In **2G networks, latency is high (500-1000 ms per packet)**.
2. More packets = More ACKs delays. ACK delay is equal to latency

2. Overhead from Headers

1. Each packet has extra header data (IP, TCP/UDP), reducing actual data throughput.
2. More packets = More overhead = Less efficiency.

3. Retransmissions

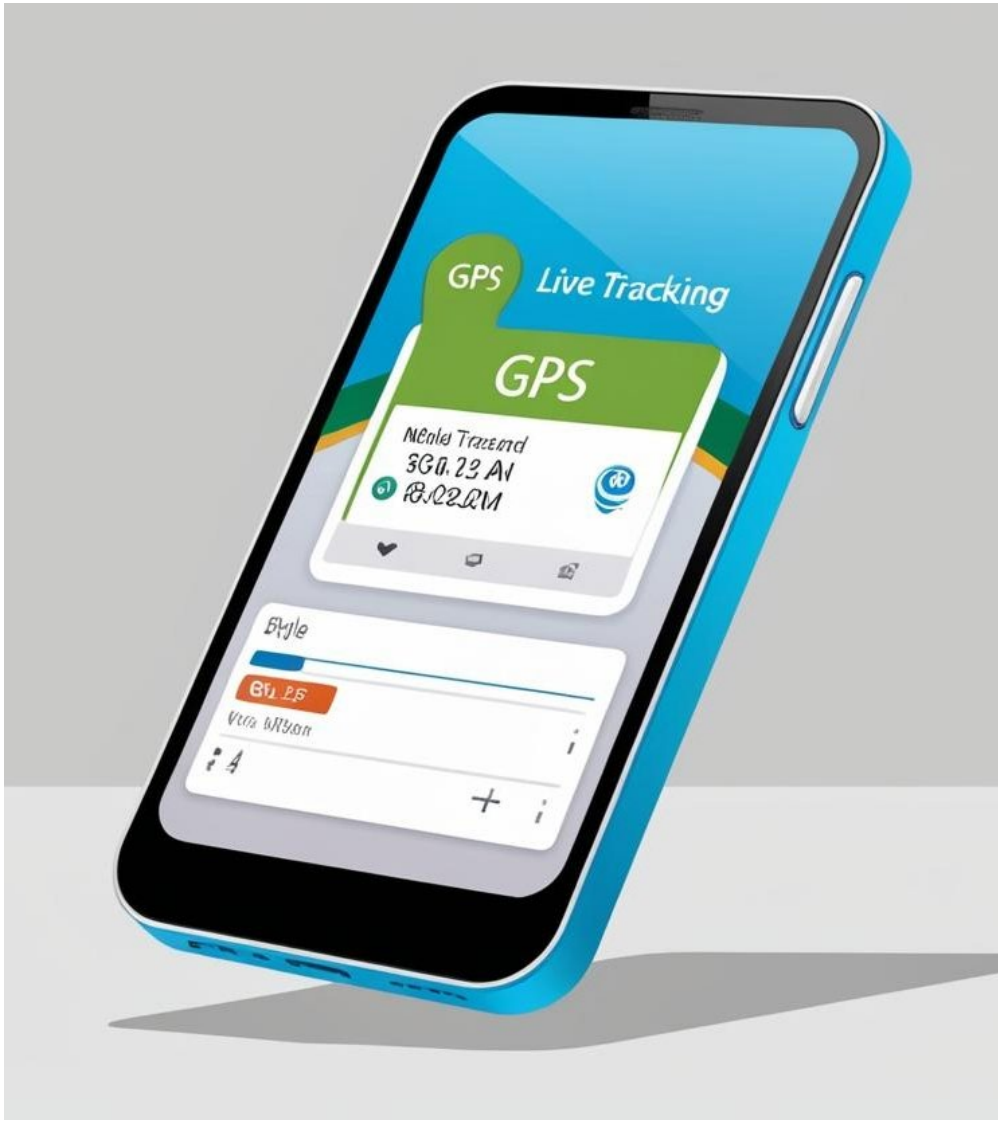
1. If a single packet is lost, it must be resent.
2. More packets = Higher risk of packet loss = More retransmissions.

Comparison in time of sending same 3064B via 2G, EDGE, LTE and NB-IoT

	MTU 1500 (3 Packets)	**MTU 500 (7 Packets)**	**MTU 9000 (less than 0,5 packet)**
GPRS (50 kbps, 600ms latency)	4.09 sec	8.89 sec	
EDGE (200 kbps, 200ms latency)	1.32 sec	2.92 sec	
LTE (~10 Mbps, 40ms latency)			42.45 **ms**
4G LTE-M, IoT /NB-IoT (~200 kbps, 600ms latency)			722.56 **ms**

Test of 2 well known mobile tracking apps data transmission

1. XCguide with sending to Pure track and Livetrack 24 (2s tracking, tracklog sending)
2. Volandoo (1 sec tracking, tracklog sending).



1 XC guide with sending to Puretrack and Livetrack 24
(position sending, 2 sec tracklog both on phone and server)

367698 bytes were sent during **10 min** of flight

1028 packets Min **40B** Max **3064B**

Network limitations

- **2G (EDGE) is highly vulnerable**, with **41 working apps*** needed to cause congestion**.
- **3G can handle significantly more**, requiring **612 apps** to cause issues.
- **4G is resistant**, needing **2,041 apps** to clog the network.

*App means literary 1 application working. Any mobile phone usually has several applications working (Google, Gmail, What's app, etc)

** Assuming there are no other uses of the cell towers.

1

Packets on wire

No.	Time	Source	Destination	Protocol	Length	Info
276	2025-02-18 10:19:46.829722	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
277	2025-02-18 10:19:46.831368	10.215.173.1	45.76.11.84	TCP	552	47002 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 278]
278	2025-02-18 10:19:46.831579	10.215.173.1	45.76.11.84	TLSv1.2	45	Client Hello (SNI=puretrack.io)
279	2025-02-18 10:19:46.831862	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=1 Ack=518 Win=523264 Len=0
280	2025-02-18 10:19:46.840505	188.40.246.133	10.215.173.1	TLSv1.2	298	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
281	2025-02-18 10:19:46.846828	188.40.246.133	10.215.173.1	TLSv1.2	875	Application Data
282	2025-02-18 10:19:46.849461	10.215.173.1	188.40.246.133	TCP	40	42350 → 443 [ACK] Seq=964 Ack=4118 Win=112128 Len=0
283	2025-02-18 10:19:46.849494	10.215.173.1	188.40.246.133	TLSv1.2	71	Encrypted Alert
284	2025-02-18 10:19:46.849683	188.40.246.133	10.215.173.1	TCP	40	443 → 42342 [ACK] Seq=4593 Ack=578 Win=523776 Len=0
285	2025-02-18 10:19:46.849809	10.215.173.1	188.40.246.133	TCP	40	42342 → 443 [FIN, ACK] Seq=578 Ack=4593 Win=125952 Len=0
286	2025-02-18 10:19:46.849882	188.40.246.133	10.215.173.1	TCP	40	443 → 42342 [ACK] Seq=4593 Ack=579 Win=523776 Len=0
287	2025-02-18 10:19:46.898536	188.40.246.133	10.215.173.1	TCP	40	443 → 42342 [FIN, ACK] Seq=4593 Ack=579 Win=524288 Len=0
288	2025-02-18 10:19:46.960839	45.76.11.84	10.215.173.1	TLSv1.2	196	Server Hello, Change Cipher Spec, Encrypted Handshake Message
289	2025-02-18 10:19:46.961642	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=518 Ack=157 Win=80896 Len=0
290	2025-02-18 10:19:46.965336	10.215.173.1	45.76.11.84	TLSv1.2	91	Change Cipher Spec, Encrypted Handshake Message
291	2025-02-18 10:19:46.965765	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=157 Ack=569 Win=523776 Len=0
292	2025-02-18 10:19:46.966048	10.215.173.1	45.76.11.84	TLSv1.2	510	Application Data
293	2025-02-18 10:19:46.966102	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=157 Ack=1039 Win=523264 Len=0
294	2025-02-18 10:19:47.161818	45.76.11.84	10.215.173.1	TLSv1.2	564	Application Data
295	2025-02-18 10:19:47.166925	10.215.173.1	188.40.246.133	TLSv1.2	71	Encrypted Alert
296	2025-02-18 10:19:47.167008	10.215.173.1	188.40.246.133	TCP	40	42334 → 443 [FIN, ACK] Seq=578 Ack=4593 Win=125952 Len=0
297	2025-02-18 10:19:47.167953	188.40.246.133	10.215.173.1	TCP	40	443 → 42334 [ACK] Seq=4593 Ack=548 Win=523776 Len=0
298	2025-02-18 10:19:47.168710	188.40.246.133	10.215.173.1	TCP	40	443 → 42334 [RST, ACK] Seq=4593 Ack=548 Win=65024 Len=0
299	2025-02-18 10:19:47.198309	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=1039 Ack=681 Win=81920 Len=0
300	2025-02-18 10:19:56.673237	10.215.173.1	188.40.246.133	TLSv1.2	360	Application Data
301	2025-02-18 10:19:56.674273	188.40.246.133	10.215.173.1	TCP	40	443 → 42350 [ACK] Seq=4118 Ack=1284 Win=523776 Len=0
302	2025-02-18 10:19:56.689131	10.215.173.1	37.128.187.9	UDP	68	43150 → 5555 Len=40
303	2025-02-18 10:19:56.735941	10.215.173.1	45.76.11.84	TLSv1.2	511	Application Data
304	2025-02-18 10:19:56.736087	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=681 Ack=1510 Win=523776 Len=0
305	2025-02-18 10:19:56.738460	10.215.173.1	34.140.25.176	UDP	130	37605 → 52010 Len=102
306	2025-02-18 10:19:56.783956	188.40.246.133	10.215.173.1	TLSv1.2	875	Application Data

```
> Internet Protocol Version 4, Src: 188.40.246.133, Dst: 10.215.173.1
v Transmission Control Protocol, Src Port: 443, Dst Port: 42350, Seq: 3283, Ack: 964, Len: 835
    Source Port: 443
    Destination Port: 42350
    [Stream index: 11]
    [Stream Packet Number: 14]
  > [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 835]
    Sequence Number: 3283    (relative sequence number)
    Sequence Number (raw): 2011923646
    [Next Sequence Number: 4118    (relative sequence number)]
```

```
0000  45 00 03 6b 00 00 40 00  40 06 cd 06 bc 28 f6 85   E··k··@· @····(··
0010  0a d7 ad 01 01 bb a5 6e  77 eb 84 be e7 12 5e b7   ·······n w·····^·
0020  50 18 04 00 94 59 00 00  17 03 03 03 3e 91 92 5f   P····Y·· ····>··_
0030  19 ef f5 40 b5 49 06 25  ef 84 b2 d5 1c 74 fe 97   ···@·I·% ·····t··
0040  6b 32 48 d4 6d 5a c4 0f  fe 62 e0 78 6d da 2a 6e   k2H·mZ·· ·b·xm·*n
0050  6f cb 1d 11 a8 82 ed 2c  fb 27 5e 05 c7 30 dc b7   o·····, ·'^··0··
0060  18 09 91 88 d2 d5 a9 4f  46 5b 86 b0 4a 6a 31 57   ·······O F[··Jj1W
0070  49 3c fe 4a 07 05 1d 4d  12 ac 0d 7a e9 00 e1 52   I<·J···M ···z···R
0080  d7 25 eb a4 b1 da f9 c3  d7 d3 ed 00 2f f2 13 c4   ·%····· ····/···
0090  15 fe 78 4f ab 92 c8 ae  30 0d 01 59 12 c2 a9 cb   ··xO···· 0··Y····
00a0  d0 d9 27 f8 3a 2c 4e 58  24 ad b1 67 1d 85 0e 4c   ··':,NX $··g···L
00b0  03 f5 15 1e 55 93 83 b8  9e d8 40 57 5d 91 c0 79   ····U··· ··@W]··y
00c0  ef b4 e4 df 8b 08 fe 43  ee f6 52 fc e1 89 38 32   ·······C ··R···82
```

No.	Time	Source	Destination	Protocol	Length	Info
361	2025-02-18 10:20:36.801645	34.140.25.176	10.215.173.1	UDP	898	52010 → 38168 Len=870
362	2025-02-18 10:20:36.836657	188.40.246.133	10.215.173.1	TCP	48	443 → 42366 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=9960 WS=512
363	2025-02-18 10:20:36.837325	10.215.173.1	188.40.246.133	TCP	40	42366 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
364	2025-02-18 10:20:36.838871	10.215.173.1	188.40.246.133	TCP	552	42366 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 365]
365	2025-02-18 10:20:36.839081	10.215.173.1	188.40.246.133	TLSv1.2	45	Client Hello (SNI=api.livetrack24.com)
366	2025-02-18 10:20:36.839395	188.40.246.133	10.215.173.1	TCP	40	443 → 42366 [ACK] Seq=1 Ack=518 Win=523264 Len=0
367	2025-02-18 10:20:36.883111	45.76.11.84	10.215.173.1	TLSv1.2	565	Application Data
368	2025-02-18 10:20:36.883480	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=3390 Ack=3301 Win=87040 Len=0
369	2025-02-18 10:20:36.895304	188.40.246.133	10.215.173.1	TLSv1.2	3064	Server Hello, Certificate, Server Key Exchange, Server Hello Done
370	2025-02-18 10:20:36.896270	10.215.173.1	188.40.246.133	TCP	40	42366 → 443 [ACK] Seq=518 Ack=3025 Win=99840 Len=0
371	2025-02-18 10:20:36.909489	10.215.173.1	188.40.246.133	TLSv1.2	166	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
372	2025-02-18 10:20:36.909720	188.40.246.133	10.215.173.1	TCP	40	443 → 42366 [ACK] Seq=3025 Ack=644 Win=523776 Len=0
373	2025-02-18 10:20:36.909860	10.215.173.1	188.40.246.133	TLSv1.2	334	Application Data
374	2025-02-18 10:20:36.909935	188.40.246.133	10.215.173.1	TCP	40	443 → 42366 [ACK] Seq=3025 Ack=938 Win=523776 Len=0
375	2025-02-18 10:20:36.964078	188.40.246.133	10.215.173.1	TLSv1.2	298	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
376	2025-02-18 10:20:36.998140	10.215.173.1	188.40.246.133	TCP	40	42366 → 443 [ACK] Seq=938 Ack=3283 Win=105984 Len=0
377	2025-02-18 10:20:39.165542	188.40.246.133	10.215.173.1	TLSv1.2	1769	Application Data
378	2025-02-18 10:20:39.166790	10.215.173.1	188.40.246.133	TCP	40	42366 → 443 [ACK] Seq=938 Ack=5012 Win=112128 Len=0
379	2025-02-18 10:20:39.169972	10.215.173.1	188.40.246.133	TLSv1.2	71	Encrypted Alert
380	2025-02-18 10:20:39.170361	188.40.246.133	10.215.173.1	TCP	40	443 → 42328 [ACK] Seq=6047 Ack=577 Win=523776 Len=0
381	2025-02-18 10:20:39.171976	10.215.173.1	188.40.246.133	TCP	40	42328 → 443 [FIN, ACK] Seq=577 Ack=6047 Win=126464 Len=0
382	2025-02-18 10:20:39.172444	188.40.246.133	10.215.173.1	TCP	40	443 → 42328 [ACK] Seq=6047 Ack=578 Win=523776 Len=0
383	2025-02-18 10:20:39.234297	188.40.246.133	10.215.173.1	TCP	40	443 → 42328 [FIN, ACK] Seq=6047 Ack=578 Win=524288 Len=0
384	2025-02-18 10:20:42.493159	188.40.246.133	10.215.173.1	TCP	40	443 → 42326 [RST, ACK] Seq=4593 Ack=545 Win=65024 Len=0
385	2025-02-18 10:20:42.494619	188.40.246.133	10.215.173.1	TCP	40	443 → 42332 [RST, ACK] Seq=4593 Ack=547 Win=65024 Len=0
386	2025-02-18 10:20:46.699863	10.215.173.1	188.40.246.133	TLSv1.2	360	Application Data
387	2025-02-18 10:20:46.700765	188.40.246.133	10.215.173.1	TCP	40	443 → 42350 [ACK] Seq=8293 Ack=2884 Win=523776 Len=0
388	2025-02-18 10:20:46.711236	10.215.173.1	37.128.187.9	UDP	68	45806 → 5555 Len=40
389	2025-02-18 10:20:46.744717	10.215.173.1	45.76.11.84	TLSv1.2	510	Application Data
390	2025-02-18 10:20:46.744848	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=3301 Ack=3860 Win=523776 Len=0
391	2025-02-18 10:20:46.746810	10.215.173.1	34.140.25.176	UDP	130	38628 → 52010 Len=102

```
> Internet Protocol Version 4, Src: 188.40.246.133, Dst: 10.215.173.1
v Transmission Control Protocol, Src Port: 443, Dst Port: 42366, Seq: 1, Ack: 518, Len: 3024
    Source Port: 443
    Destination Port: 42366
    [Stream index: 13]
    [Stream Packet Number: 7]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 3024]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2011920364
    [Next Sequence Number: 3025    (relative sequence number)]
```

```
0000  45 00 0b f8 00 00 40 00  40 06 c4 79 bc 28 f6 85   E·····@· @··y·(··
0010  0a d7 ad 01 01 bb a5 7e  77 eb 77 ec 3f a5 4c 08   ·······~ w·w·?·L·
0020  50 18 04 00 99 11 00 00  16 03 03 00 50 02 00 00   P·······  ····P···
0030  4c 03 03 14 b6 35 1f 32  28 98 26 8e 6c 66 7f bc   L····5·2 (·&·lf··
0040  dd cd b0 eb 9c 15 67 ea  d3 05 79 e8 5c ef 77 fe   ······g·  ··y·\·w·
0050  e5 6a 63 00 c0 30 00 00  24 00 00 00 00 ff 01 00   ·jc··0··  $·······
0060  01 00 00 0b 00 04 03 00  01 02 00 23 00 00 00 10   ········  ···#····
0070  00 0b 00 09 08 68 74 74  70 2f 31 2e 31 16 03 03   ·····htt  p/1.1···
0080  0a 1b 0b 00 0a 17 00 0a  14 00 05 04 30 82 05 00   ········  ····0···
0090  30 82 03 e8 a0 03 02 01  02 02 12 03 08 ff dd ba   0·······  ········
00a0  a5 3e cc 26 9a 68 d0 78  09 50 a1 ef d3 30 0d 06   ·>·&·h·x  ·P···0··
00b0  09 2a 86 48 86 f7 0d 01  01 0b 05 00 30 33 31 0b   ·*·H····  ····031·
00c0  30 09 06 03 55 04 06 13  02 55 53 31 16 30 14 06   0···U···  ·US1·0··
```

No.	Time	Source	Destination	Protocol	Length	Info
994	2025-02-18 10:28:17.246335	45.76.11.84	10.215.173.1	TLSv1.2	566	Application Data
995	2025-02-18 10:28:17.246695	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=25020 Ack=27430 Win=135680 Len=0
996	2025-02-18 10:28:27.053801	10.215.173.1	188.40.246.133	TLSv1.2	358	Application Data
997	2025-02-18 10:28:27.054547	188.40.246.133	10.215.173.1	TCP	40	443 → 42350 [ACK] Seq=46703 Ack=17637 Win=523776 Len=0
998	2025-02-18 10:28:27.062896	10.215.173.1	37.128.187.9	UDP	65	43433 → 5555 Len=37
999	2025-02-18 10:28:27.101484	10.215.173.1	45.76.11.84	TLSv1.2	503	Application Data
1000	2025-02-18 10:28:27.101623	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=27430 Ack=25483 Win=523776 Len=0
1001	2025-02-18 10:28:27.104518	10.215.173.1	34.140.25.176	UDP	128	48777 → 52010 Len=100
1002	2025-02-18 10:28:27.130740	188.40.246.133	10.215.173.1	TLSv1.2	875	Application Data
1003	2025-02-18 10:28:27.131159	10.215.173.1	188.40.246.133	TCP	40	42350 → 443 [ACK] Seq=17637 Ack=47538 Win=198656 Len=0
1004	2025-02-18 10:28:27.240600	34.140.25.176	10.215.173.1	UDP	893	52010 → 48777 Len=865
1005	2025-02-18 10:28:27.241226	34.140.25.176	10.215.173.1	UDP	890	52010 → 48777 Len=862
1006	2025-02-18 10:28:27.241470	34.140.25.176	10.215.173.1	UDP	207	52010 → 48777 Len=179
1007	2025-02-18 10:28:27.252713	45.76.11.84	10.215.173.1	TLSv1.2	566	Application Data
1008	2025-02-18 10:28:27.253136	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=25483 Ack=27956 Win=136704 Len=0
1009	2025-02-18 10:28:37.064281	10.215.173.1	188.40.246.133	TLSv1.2	334	Application Data
1010	2025-02-18 10:28:37.065282	188.40.246.133	10.215.173.1	TCP	40	443 → 42366 [ACK] Seq=17114 Ack=3290 Win=523776 Len=0
1011	2025-02-18 10:28:37.066634	10.215.173.1	188.40.246.133	TLSv1.2	359	Application Data
1012	2025-02-18 10:28:37.066909	188.40.246.133	10.215.173.1	TCP	40	443 → 42350 [ACK] Seq=47538 Ack=17956 Win=523776 Len=0
1013	2025-02-18 10:28:37.077605	10.215.173.1	37.128.187.9	UDP	66	41974 → 5555 Len=38
1014	2025-02-18 10:28:37.102702	10.215.173.1	45.76.11.84	TLSv1.2	510	Application Data
1015	2025-02-18 10:28:37.102832	45.76.11.84	10.215.173.1	TCP	40	443 → 47002 [ACK] Seq=27956 Ack=25953 Win=523776 Len=0
1016	2025-02-18 10:28:37.106925	10.215.173.1	34.140.25.176	UDP	129	49025 → 52010 Len=101
1017	2025-02-18 10:28:37.141885	188.40.246.133	10.215.173.1	TLSv1.2	875	Application Data
1018	2025-02-18 10:28:37.142456	10.215.173.1	188.40.246.133	TCP	40	42350 → 443 [ACK] Seq=17956 Ack=48373 Win=200704 Len=0
1019	2025-02-18 10:28:37.161589	34.140.25.176	10.215.173.1	UDP	208	52010 → 49025 Len=180
1020	2025-02-18 10:28:37.167374	34.140.25.176	10.215.173.1	UDP	891	52010 → 49025 Len=863
1021	2025-02-18 10:28:37.168310	34.140.25.176	10.215.173.1	UDP	893	52010 → 49025 Len=865
1022	2025-02-18 10:28:37.240701	45.76.11.84	10.215.173.1	TLSv1.2	566	Application Data
1023	2025-02-18 10:28:37.241086	10.215.173.1	45.76.11.84	TCP	40	47002 → 443 [ACK] Seq=25953 Ack=28482 Win=137728 Len=0
1024	2025-02-18 10:28:39.330792	188.40.246.133	10.215.173.1	TLSv1.2	1770	Application Data
1025	2025-02-18 10:28:39.331657	10.215.173.1	188.40.246.133	TCP	40	42366 → 443 [ACK] Seq=3290 Ack=18844 Win=204800 Len=0
1026	2025-02-18 10:28:47.077251	10.215.173.1	188.40.246.133	TLSv1.2	358	Application Data

```
[Time delta from previous captured frame: 0.011243000 seconds]
[Time delta from previous displayed frame: 0.011243000 seconds]
[Time since reference or first frame: 1010.788958000 seconds]
Frame Number: 1007
Frame Length: 566 bytes (4528 bits)
Capture Length: 566 bytes (4528 bits)
[Frame is marked: False]
[Frame is ignored: False]
```

```
0000  45 00 02 36 00 00 40 00  40 06 48 4a 2d 4c 0b 54   E··6··@· @·HJ-L·T
0010  0a d7 ad 01 01 bb b7 9a  77 eb e3 11 05 27 66 a3   ········ w····'f·
0020  50 18 04 00 a0 2d 00 00  17 03 03 02 09 46 53 af   P····-·· ·····FS·
0030  81 43 88 47 75 57 c3 b6  7d 77 c8 48 c3 ce 36 99   ·C·GuW·· }w·H··6·
0040  28 9d 01 4f 94 3e 88 14  8d 81 7c a6 cd c5 cf 39   (··O·>·· ··|····9
0050  31 e7 6b 4f 23 d3 04 21  e8 b4 b2 d6 cf 24 5f 7b   1·kO#··! ·····$_{
0060  2a 24 cf e0 64 16 d0 ef  6e 98 b9 b1 dd 54 9b a0   *$··d··· n····T··
0070  69 e8 6f 0b 75 cf d4 b3  20 86 fc cf 87 42 75 8e   i·o·u···  ····Bu·
0080  14 91 d4 f3 25 84 6c 46  aa 67 81 35 cb 75 8f 3a   ····%·lF ·g·5·u·:
```

2 Volandoo sending to its server

(1 sec tracking, position sending and tracklog on server)

424458 bytes were sent during **10 min** of flight

2870 packets Min **40B**, Max **10000B**

Network limitations

- **2G (EDGE) is highly vulnerable**, with just **35 apps working** will cause congestion*.
- **3G can handle more**, requiring **530 apps** to cause issues.
- **4G is very resistant**, needing **1,767 apps** to clog the network.

* Assuming there are no other uses of the cell towers.

2 Packets on wire

No.	Time	Source	Destination	Protocol	Length	Info
8465	2025-01-30 12:43:03.787649	10.215.173.1	76.76.21.21	TCP	40	49794 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
8466	2025-01-30 12:43:03.787665	10.215.173.1	76.76.21.21	TCP	40	49798 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
8467	2025-01-30 12:43:03.787679	10.215.173.1	76.76.21.21	TCP	40	49802 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
8468	2025-01-30 12:43:03.790868	10.215.173.1	76.76.21.21	TCP	552	49798 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 8478]
8469	2025-01-30 12:43:03.791094	10.215.173.1	76.76.21.21	TCP	552	49790 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 8472]
8470	2025-01-30 12:43:03.791133	10.215.173.1	76.76.21.21	TCP	552	49802 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 8471]
8471	2025-01-30 12:43:03.791159	10.215.173.1	76.76.21.21	TLSv1.2	45	Client Hello (SNI=volandoo.com)
8472	2025-01-30 12:43:03.791216	10.215.173.1	76.76.21.21	TLSv1.2	45	Client Hello (SNI=volandoo.com)
8473	2025-01-30 12:43:03.791309	76.76.21.21	10.215.173.1	TCP	40	443 → 49790 [ACK] Seq=1 Ack=518 Win=523264 Len=0
8474	2025-01-30 12:43:03.791357	76.76.21.21	10.215.173.1	TCP	40	443 → 49798 [ACK] Seq=1 Ack=513 Win=523776 Len=0
8475	2025-01-30 12:43:03.791393	76.76.21.21	10.215.173.1	TCP	40	443 → 49802 [ACK] Seq=1 Ack=518 Win=523264 Len=0
8476	2025-01-30 12:43:03.791991	10.215.173.1	76.76.21.21	TCP	552	49794 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 8480]
8477	2025-01-30 12:43:03.792107	76.76.21.21	10.215.173.1	TCP	40	443 → 49794 [ACK] Seq=1 Ack=513 Win=523776 Len=0
8478	2025-01-30 12:43:03.792235	10.215.173.1	76.76.21.21	TLSv1.2	45	Client Hello (SNI=volandoo.com)
8479	2025-01-30 12:43:03.792364	76.76.21.21	10.215.173.1	TCP	40	443 → 49798 [ACK] Seq=1 Ack=518 Win=523264 Len=0
8480	2025-01-30 12:43:03.792485	10.215.173.1	76.76.21.21	TLSv1.2	45	Client Hello (SNI=volandoo.com)
8481	2025-01-30 12:43:03.792568	76.76.21.21	10.215.173.1	TCP	40	443 → 49794 [ACK] Seq=1 Ack=518 Win=523264 Len=0
8482	2025-01-30 12:43:03.792683	10.215.173.1	76.76.21.21	TCP	552	49788 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=512 [TCP PDU reassembled in 8484]
8483	2025-01-30 12:43:03.792777	76.76.21.21	10.215.173.1	TCP	40	443 → 49788 [ACK] Seq=1 Ack=513 Win=523776 Len=0
8484	2025-01-30 12:43:03.792855	10.215.173.1	76.76.21.21	TLSv1.2	45	Client Hello (SNI=volandoo.com)
8485	2025-01-30 12:43:03.792950	76.76.21.21	10.215.173.1	TCP	40	443 → 49788 [ACK] Seq=1 Ack=518 Win=523264 Len=0
8486	2025-01-30 12:43:03.843292	76.76.21.21	10.215.173.1	TLSv1.2	342	Server Hello, New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
8487	2025-01-30 12:43:03.843649	10.215.173.1	76.76.21.21	TCP	40	49802 → 443 [ACK] Seq=518 Ack=303 Win=80896 Len=0
8488	2025-01-30 12:43:03.844380	10.215.173.1	76.76.21.21	TLSv1.2	91	Change Cipher Spec, Encrypted Handshake Message
8489	2025-01-30 12:43:03.844436	76.76.21.21	10.215.173.1	TCP	40	443 → 49802 [ACK] Seq=303 Ack=569 Win=523776 Len=0
8490	2025-01-30 12:43:03.847616	10.215.173.1	76.76.21.21	TCP	1064	49802 → 443 [ACK] Seq=569 Ack=303 Win=80896 Len=1024 [TCP PDU reassembled in 8491]
8491	2025-01-30 12:43:03.847630	10.215.173.1	76.76.21.21	TLSv1.2	449	Application Data
8492	2025-01-30 12:43:03.847747	76.76.21.21	10.215.173.1	TCP	40	443 → 49802 [ACK] Seq=303 Ack=2002 Win=522752 Len=0
8493	2025-01-30 12:43:03.849467	76.76.21.21	10.215.173.1	TLSv1.2	342	Server Hello, New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
8494	2025-01-30 12:43:03.849962	76.76.21.21	10.215.173.1	TLSv1.2	342	Server Hello, New Session Ticket, Change Cipher Spec, Encrypted Handshake Message

```
    Identification: 0xfbab (64427)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x25e6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.215.173.1
    Destination Address: 76.76.21.21
    [Stream index: 6]
> Transmission Control Protocol, Src Port: 49802, Dst Port: 443, Seq: 513, Ack: 1, Len: 5
```

```
0000  45 00 00 2d fb ab 40 00  40 06 25 e6 0a d7 ad 01   E··-··@· @·%·····
0010  4c 4c 15 15 c2 8a 01 bb  83 4d a6 c5 77 eb 77 ec   LL····· ·M··w·w·
0020  50 18 00 9c b7 c1 00 00  00 00 00 00 00           P····· ·····
```

No.	Time	Source	Destination	Protocol	Length	Info
11228	2025-01-30 12:54:19.721902	10.215.173.1	170.253.18.130	TCP	40	42538 → 3003 [ACK] Seq=44154 Ack=2905 Win=79872 Len=0
11229	2025-01-30 12:54:20.638803	10.215.173.1	170.253.18.130	TCP	102	42538 → 3003 [PSH, ACK] Seq=44154 Ack=2905 Win=79872 Len=62
11230	2025-01-30 12:54:20.639312	170.253.18.130	10.215.173.1	TCP	40	3003 → 42538 [ACK] Seq=2905 Ack=44216 Win=523776 Len=0
11231	2025-01-30 12:54:20.757702	170.253.18.130	10.215.173.1	TCP	44	3003 → 42538 [PSH, ACK] Seq=2905 Ack=44216 Win=524288 Len=4
11232	2025-01-30 12:54:20.758011	10.215.173.1	170.253.18.130	TCP	40	42538 → 3003 [ACK] Seq=44216 Ack=2909 Win=79872 Len=0
11233	2025-01-30 12:54:21.639772	10.215.173.1	170.253.18.130	TCP	102	42538 → 3003 [PSH, ACK] Seq=44216 Ack=2909 Win=79872 Len=62
11234	2025-01-30 12:54:21.640248	170.253.18.130	10.215.173.1	TCP	40	3003 → 42538 [ACK] Seq=2909 Ack=44278 Win=523776 Len=0
11235	2025-01-30 12:54:21.704610	170.253.18.130	10.215.173.1	TCP	44	3003 → 42538 [PSH, ACK] Seq=2909 Ack=44278 Win=524288 Len=4
11236	2025-01-30 12:54:21.704857	10.215.173.1	170.253.18.130	TCP	40	42538 → 3003 [ACK] Seq=44278 Ack=2913 Win=79872 Len=0
11237	2025-01-30 12:54:22.254357	10.215.173.1	157.240.203.14	TLSv1.2	459	Application Data
11238	2025-01-30 12:54:22.254779	157.240.203.14	10.215.173.1	TCP	40	443 → 47996 [ACK] Seq=4194 Ack=1106 Win=523776 Len=0
11239	2025-01-30 12:54:22.270208	10.215.173.1	157.240.203.14	TCP	60	48048 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM TSval=2360125012 TSecr=0 WS=512
11240	2025-01-30 12:54:22.315805	157.240.203.14	10.215.173.1	TCP	48	443 → 48048 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=9960 WS=512
11241	2025-01-30 12:54:22.318789	10.215.173.1	157.240.203.14	TCP	40	48048 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
11242	2025-01-30 12:54:22.318837	10.215.173.1	157.240.203.14	TLSv1.2	256	Client Hello (SNI=graph.facebook.com)
11243	2025-01-30 12:54:22.319228	157.240.203.14	10.215.173.1	TCP	40	443 → 48048 [ACK] Seq=1 Ack=217 Win=523776 Len=0
11244	2025-01-30 12:54:22.357486	157.240.203.14	10.215.173.1	TLSv1.2	196	Server Hello, Change Cipher Spec, Encrypted Handshake Message
11245	2025-01-30 12:54:22.357806	10.215.173.1	157.240.203.14	TCP	40	48048 → 443 [ACK] Seq=217 Ack=157 Win=80896 Len=0
11246	2025-01-30 12:54:22.361130	10.215.173.1	157.240.203.14	TLSv1.2	91	Change Cipher Spec, Encrypted Handshake Message
11247	2025-01-30 12:54:22.361431	157.240.203.14	10.215.173.1	TCP	40	443 → 48048 [ACK] Seq=157 Ack=268 Win=523776 Len=0
11248	2025-01-30 12:54:22.362075	10.215.173.1	157.240.203.14	TLSv1.2	912	Application Data
11249	2025-01-30 12:54:22.362133	157.240.203.14	10.215.173.1	TCP	40	443 → 48048 [ACK] Seq=157 Ack=1140 Win=523264 Len=0
11250	2025-01-30 12:54:22.362251	10.215.173.1	157.240.203.14	TLSv1.2	74	Application Data
11251	2025-01-30 12:54:22.362394	157.240.203.14	10.215.173.1	TCP	40	443 → 48048 [ACK] Seq=157 Ack=1174 Win=523264 Len=0
11252	2025-01-30 12:54:22.412170	157.240.203.14	10.215.173.1	TCP	1388	443 → 47996 [PSH, ACK] Seq=4194 Ack=1106 Win=524288 Len=1348 [TCP PDU reassembled in 11253]
11253	2025-01-30 12:54:22.443982	157.240.203.14	10.215.173.1	TLSv1.2	2728	Application Data, Application Data, Application Data
11254	2025-01-30 12:54:22.444287	10.215.173.1	157.240.203.14	TCP	40	47996 → 443 [ACK] Seq=1106 Ack=8230 Win=160768 Len=0
11255	2025-01-30 12:54:22.450115	157.240.203.14	10.215.173.1	TLSv1.2	900	Application Data
11256	2025-01-30 12:54:22.481648	10.215.173.1	157.240.203.14	TCP	40	48048 → 443 [ACK] Seq=1174 Ack=1017 Win=82432 Len=0
11257	2025-01-30 12:54:22.640774	10.215.173.1	170.253.18.130	TCP	102	42538 → 3003 [PSH, ACK] Seq=44278 Ack=2913 Win=79872 Len=62
11258	2025-01-30 12:54:22.641349	170.253.18.130	10.215.173.1	TCP	40	3003 → 42538 [ACK] Seq=2913 Ack=44340 Win=523776 Len=0
11259	2025-01-30 12:54:22.758718	170.253.18.130	10.215.173.1	TCP	44	3003 → 42538 [PSH, ACK] Seq=2913 Ack=44340 Win=524288 Len=4
11260	2025-01-30 12:54:22.759147	10.215.173.1	170.253.18.130	TCP	40	42538 → 3003 [ACK] Seq=44340 Ack=2917 Win=79872 Len=0
11261	2025-01-30 12:54:23.642314	10.215.173.1	170.253.18.130	TCP	101	42538 → 3003 [PSH, ACK] Seq=44340 Ack=2917 Win=79872 Len=61

```
Epoch Arrival Time: 1738238062.450115000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.005828000 seconds]
[Time delta from previous displayed frame: 0.005828000 seconds]
[Time since reference or first frame: 1100.952512000 seconds]
Frame Number: 11255
Frame Length: 900 bytes (7200 bits)
```

```
0000  45 00 03 84 00 00 40 00  40 06 16 9d 9d f0 cb 0e   E·····@· @······
0010  0a d7 ad 01 01 bb bb b0  77 eb 78 88 4b 54 36 24   ······ w·x·KT6$
0020  50 18 04 00 a8 10 00 00  17 03 03 03 57 66 4c c4   P····· ····WfL·
0030  ec 2b 0e f6 3a 7a 02 3a  1a 97 91 f3 b9 95 e1 63   ·+··:z·: ·····c
0040  70 84 75 05 0d 92 6d a6  71 0d 61 d6 5d 01 e0 82   p·u···m· q·a·]···
0050  ed f9 02 42 20 68 25 a0  91 31 77 01 10 a5 53 1f   ···B h%· ·1w···S·
0060  cb 2c 8c e8 ec a2 5d 07  6f 4c 43 9b 26 d9 ff 86   ·,····]· oLC·&···
0070  dd de 24 b2 0b 21 f9 3a  65 2f 9c 9a e2 c5 76 50   ··$··!·: e/····vP
```

No.	Time	Source	Destination	Protocol	Length	Info
13440	2025-01-30 13:02:50.597882	10.215.173.2	10.215.173.1	DNS	167	Standard query response 0xec4c A ik.imagekit.io CNAME d28h3jm4r3crf8.cloudfront.net A 18.66.218.120
13441	2025-01-30 13:02:50.601418	10.215.173.1	18.66.218.120	TCP	60	46650 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=9960 SACK_PERM TSval=533336038 TSecr=0 WS=512
13442	2025-01-30 13:02:50.622213	18.66.218.120	10.215.173.1	TCP	48	443 → 46650 [SYN, ACK] Seq=0 Ack=1 Win=1024 Len=0 MSS=9960 WS=512
13443	2025-01-30 13:02:50.622423	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=1 Ack=1 Win=79872 Len=0
13444	2025-01-30 13:02:50.624713	10.215.173.1	18.66.218.120	TLSv1.2	220	Client Hello (SNI=ik.imagekit.io)
13445	2025-01-30 13:02:50.625011	18.66.218.120	10.215.173.1	TCP	40	443 → 46650 [ACK] Seq=1 Ack=181 Win=523776 Len=0
13446	2025-01-30 13:02:50.647770	18.66.218.120	10.215.173.1	TLSv1.2	4084	Server Hello, Certificate
13447	2025-01-30 13:02:50.648386	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=181 Ack=4045 Win=88064 Len=0
13448	2025-01-30 13:02:50.653248	18.66.218.120	10.215.173.1	TLSv1.2	729	Certificate Status, Server Key Exchange, Server Hello Done
13449	2025-01-30 13:02:50.653368	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=181 Ack=4734 Win=96256 Len=0
13450	2025-01-30 13:02:50.661858	10.215.173.1	18.66.218.120	TLSv1.2	133	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13451	2025-01-30 13:02:50.662003	18.66.218.120	10.215.173.1	TCP	40	443 → 46650 [ACK] Seq=4734 Ack=274 Win=523776 Len=0
13452	2025-01-30 13:02:50.662820	10.215.173.1	18.66.218.120	TLSv1.2	288	Application Data
13453	2025-01-30 13:02:50.662875	18.66.218.120	10.215.173.1	TCP	40	443 → 46650 [ACK] Seq=4734 Ack=522 Win=523776 Len=0
13454	2025-01-30 13:02:50.683880	18.66.218.120	10.215.173.1	TLSv1.2	244	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
13455	2025-01-30 13:02:50.716835	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=4938 Win=104448 Len=0
13456	2025-01-30 13:02:50.767984	18.66.218.120	10.215.173.1	TLSv1.2	6207	Application Data
13457	2025-01-30 13:02:50.768121	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=11105 Win=123904 Len=0
13458	2025-01-30 13:02:50.774214	18.66.218.120	10.215.173.1	TCP	10000	443 → 46650 [ACK] Seq=11105 Ack=522 Win=524288 Len=9960 [TCP PDU reassembled in 13460]
13459	2025-01-30 13:02:50.774359	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=21065 Win=143872 Len=0
13460	2025-01-30 13:02:50.774390	18.66.218.120	10.215.173.1	TLSv1.2	6256	Application Data
13461	2025-01-30 13:02:50.774477	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=27281 Win=163840 Len=0
13462	2025-01-30 13:02:50.781048	18.66.218.120	10.215.173.1	TCP	10000	443 → 46650 [ACK] Seq=27281 Ack=522 Win=524288 Len=9960 [TCP PDU reassembled in 13464]
13463	2025-01-30 13:02:50.781306	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=37241 Win=183808 Len=0
13464	2025-01-30 13:02:50.781340	18.66.218.120	10.215.173.1	TLSv1.2	3560	Application Data
13465	2025-01-30 13:02:50.781433	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=40761 Win=203776 Len=0
13466	2025-01-30 13:02:50.786353	18.66.218.120	10.215.173.1	TCP	4084	443 → 46650 [PSH, ACK] Seq=40761 Ack=522 Win=524288 Len=4044 [TCP PDU reassembled in 13470]
13467	2025-01-30 13:02:50.786495	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=44805 Win=223744 Len=0
13468	2025-01-30 13:02:50.792614	18.66.218.120	10.215.173.1	TCP	5432	443 → 46650 [PSH, ACK] Seq=44805 Ack=522 Win=524288 Len=5392 [TCP PDU reassembled in 13470]
13469	2025-01-30 13:02:50.792795	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=50197 Win=243712 Len=0
13470	2025-01-30 13:02:50.808011	18.66.218.120	10.215.173.1	TLSv1.2	6780	Application Data
13471	2025-01-30 13:02:50.808171	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=56937 Win=263680 Len=0
13472	2025-01-30 13:02:50.814095	18.66.218.120	10.215.173.1	TCP	10000	443 → 46650 [ACK] Seq=56937 Ack=522 Win=524288 Len=9960 [TCP PDU reassembled in 13476]
13473	2025-01-30 13:02:50.814326	10.215.173.1	18.66.218.120	TCP	40	46650 → 443 [ACK] Seq=522 Ack=66897 Win=283648 Len=0

```
UTC Arrival Time: Jan 30, 2025 12:02:50.781340000 UTC
Epoch Arrival Time: 1738238570.781340000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000034000 seconds]
[Time delta from previous displayed frame: 0.000034000 seconds]
[Time since reference or first frame: 1609.283737000 seconds]
Frame Number: 13464
```

```
0000  45 00 0d e8 00 00 40 00  40 06 88 7d 12 42 da 78   E·····@· @··}·B·x
0010  0a d7 ad 01 01 bb b6 3a  77 ec 09 64 d1 06 a1 a8   ·······: w··d····
0020  50 18 04 00 1e 93 00 00  db 1c 0b e6 08 24 f7 cc   P········ ·····$··
0030  b0 15 bf 9d 7b a1 ec 89  49 1a eb 7a 8e b0 ff a3   ····{··· I··z····
0040  f3 3f 13 fc 96 be bc 18  9d 4b 8a 28 f6 63 3a f9   ·?····· ·K·(·c:·
0050  40 c7 36 14 77 5d fd 9e  a0 4e 09 dd 1c f3 61 60   @·6·w]·· ·N····a`
0060  d7 40 7d 26 de c4 a7 f1  bb 6e 3a a9 08 6d b3 30   ·@}&···· ·n:··m·0
```

Frame (3560 bytes) | Reassembled TCP (16413 bytes)

2G sunset and 3G, LTE-M coming

- The decision to switch off 3G and 2G has been announced. They will be replaced by LTE-M but the replacement is gradual.
- On the web there are many resources for example this where you can get “so far promised” years for technology replacement.
- Currently we are in the situation that even if we have 4G, 5G or LTE-M available, they are not widely spread.
- If the 5G signal is too weak, your phone may drop back to 4G LTE for a more stable connection and if 4G LTE is not available it will fall back to EDGE (since 3G has been mostly switched off)

How 5G Works (Simple Explanation)

- Imagine a flashlight instead of a light bulb. A light bulb spreads light in all directions, while a flashlight focuses light into a beam. 5G beamforming works like a flashlight—instead of sending signals everywhere, the 5G tower directs a focused "beam" of signal toward your phone.
- When your phone is at the farthest edge of a 5G antenna's range The beam becomes stretched and less focused, like the dim edge of a flashlight’s beam. The signal is weak and your phone may struggle to maintain a strong connection.
- Besides there is EMF noise that delutes or blocks the signal more
- Slower Speed. Data transmission slows down because your phone has to work harder to send and receive signals.
- More Power Consumption – Your phone increases its transmission power to "shout" back to the tower, draining the battery faster.
- Switching to 4G (Fallback) – If the 5G signal is too weak, your phone may drop back to 4G LTE for a more stable connection.

What happens if no 4G or 3G Available or 4G is signal is not strong enough?

1. If the 5G signal is too weak and there is no **4G LTE or 3G coverage**, the phone may fall back to **2G (GSM/EDGE)** if the network still supports it.
2. **Network Operator Settings –** Some carriers **no longer support 2G** and have shut it down. In that case, the phone would simply lose connection instead of falling back.
3. **Phone Settings & Compatibility –** Some modern phones **disable 2G fallback** to save battery or for security reasons (since 2G is less secure). Again the phone would simply lose connection instead of falling back.
4. **Data vs. Voice –** If you're on a voice call and **VoLTE (4G Calling) is unavailable**, the phone may fall back to **2G for voice-only service** while data is lost or slowed down drastically.

If the phone is on the limit of 5G or 4G how can it drop to H/EDGE?

1. **Network Congestion – When many users (like 100 people) started sending data, the 4G LTE network may also get overloaded.**
    - **If the network couldn't handle the traffic, some devices were forced to switch to lower-generation networks (4G, 3G, or even 2G).**
2. **Tower Load Balancing – The mobile network dynamically manages connections by shifting some devices to less congested networks.**
    - **If 5G and 4G were overloaded, the system moved some phones down to HSPA (H) or EDGE (E) to maintain connectivity.**
    - **This is called load balancing—ensuring that everyone gets at least some connection, even if it's slower.**
3. **Limited 5G Backhaul – In remote areas like mountains, the fiber or microwave link that connects the 5G tower to the core network may have limited capacity.**
    - **When too many users consume bandwidth, the tower struggles to process all the data, forcing devices to downgrade.**
4. **Signal Interference & Weakening – As more people connected, the tower's radio resources were stretched, which can cause a weaker 5G signal for some users.**
    - **The phone may have automatically switched to a more stable (but slower) 3G or 2G signal.**

Why do I see "H" or "E" instead of 4G on the phone when I just was on 5G

- **4G LTE was also likely congested, so your phone skipped it and went to HSPA (H) or EDGE (E) instead.**
- **Some network providers prioritize voice and emergency services on 4G, pushing data-heavy users down to HSPA or EDGE.**
- **This is a common issue in crowded events, concerts, and remote areas with limited network capacity.**
- **The network prioritizes essential connections (like calls, SMS) and shifts data users to older technologies to prevent total network failure.**
- **If you were closer to the tower or using a higher-priority SIM (like business or emergency services), you might have stayed on 5G or 4G longer.**

CIVL competitions live tracking sources

- OLD
  - GSM tracker
  - GSM mobile app on smartphone
  - Satellite tracker
  - OGN device (FLARM, FANET, ADSL, ADSL-M, GSM/GPRS)
  - FANET device
- NEW
  - GSM+FLARM device
  - GSM+ADSL device
  - GSM+FANET device

  But only GSM connection can be used for the purpose of live scoring

GSM

In GSM every device competes with every other device for the time slot to transfer its packet. So the smaller the packet the easier it goes through. **But the number of packets sent counts as well.**

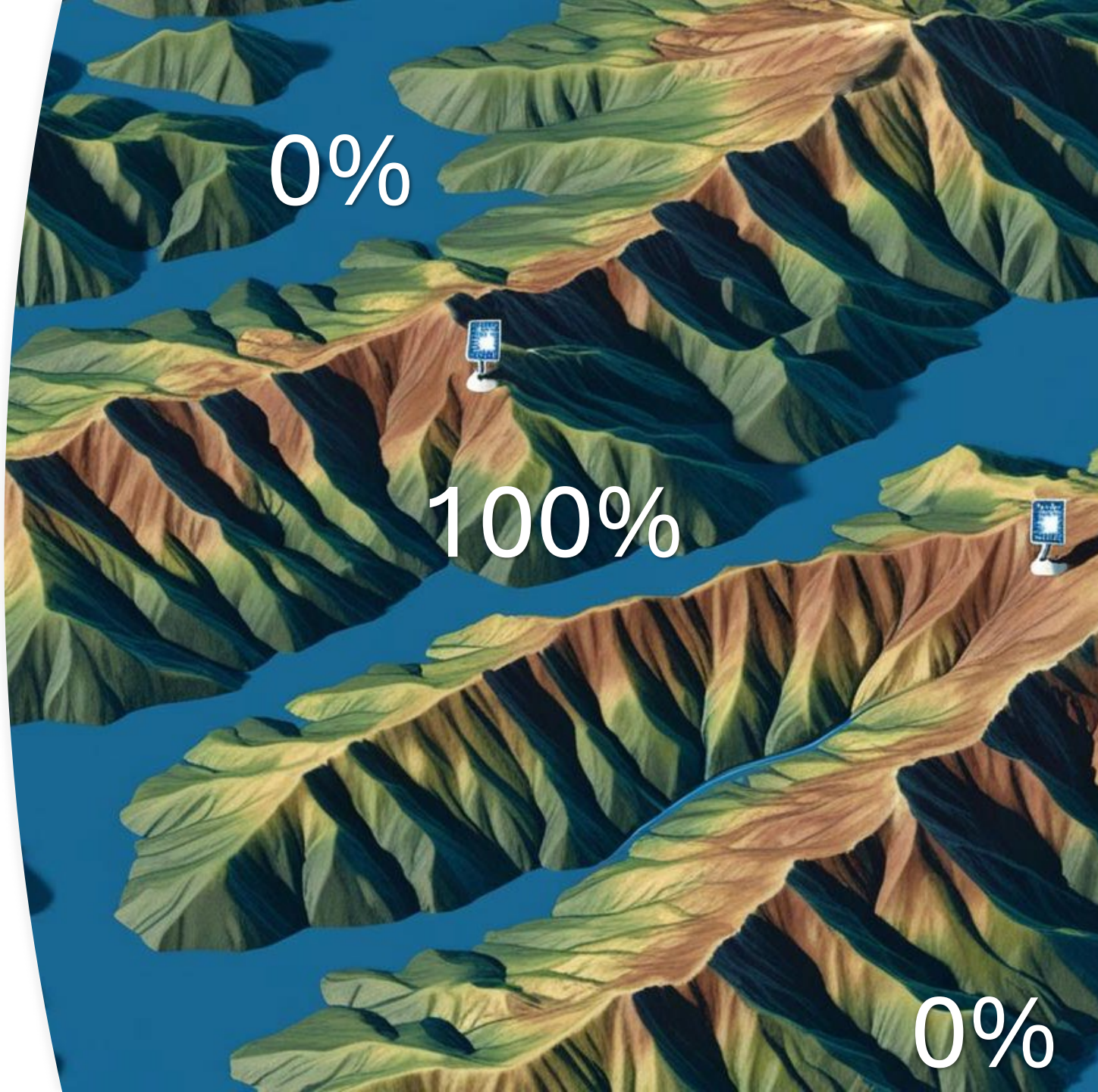
- Mobile apps packets vary from 40 bytes to 10000 bytes.
  - 40 B of mobile app is a header or ACK* packet.
  - From 94 B of mobile app is PSH* packet.
  - From 3000B for Server Hello, Certificate, Encryption, etc
  - Position packets from mobile apps starts from 100B. But they are always sent together with Server Hello, ACK, PSH packets that increate the total amount of data sent.
- Tracker can send up to 10 times less data but it has to wait for a vacant time slot in between mobile app packets.

*ACK means that the machine sending the packet with ACK is acknowledging data that it had received from the other machine. In TCP, once the connection is established, *all* packets sent by either side will contain an ACK, even if it's just re-acknowledging data that it's already acknowledged.

PSH is an indication by the sender that, if the receiving machine's TCP implementation has not yet provided the data it's received to the code that's reading the data (program, or library used by a program), it should do so at that point. To quote RFC 793, the official specification for TCP:

OGN/FANET/ADSL

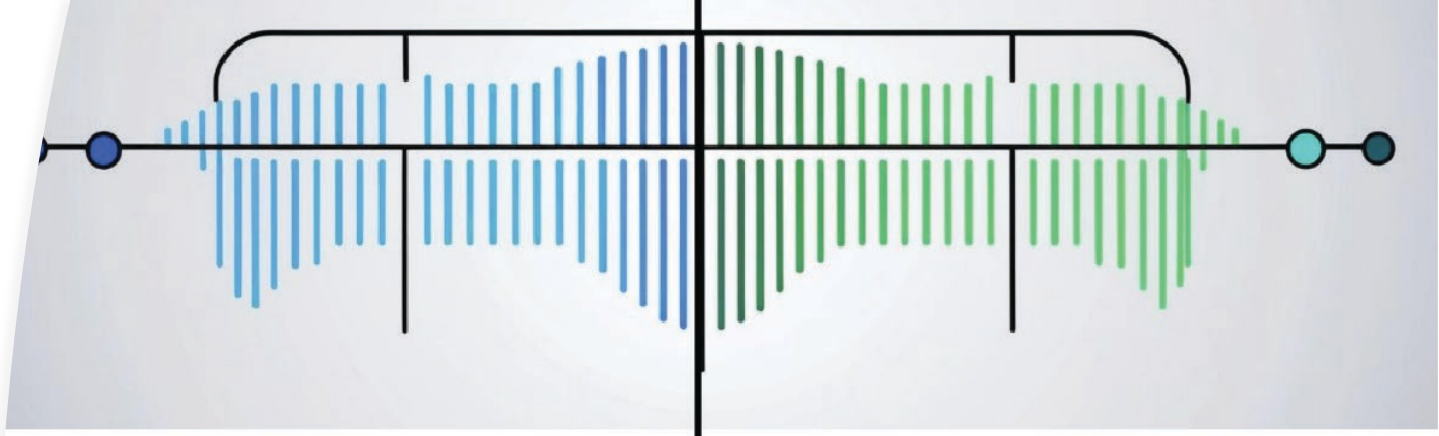
- Devices that transmit positions via RF have the advantage of not overloading GSM network as they operate via separate base stations that retransmit RF signal into internet (OGN or SafeSky)
- On the other hand, they have disadvantage that they depend on the number of these base stations existing in the area.
- On the picture you can see that the valley in the middle is well covered but the valleys on top and bottom are not covered at all.

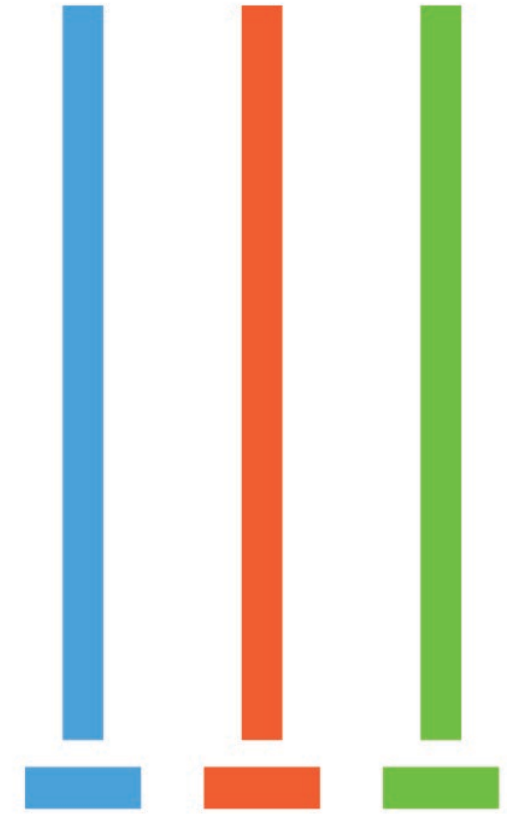


FANET VS FLARM

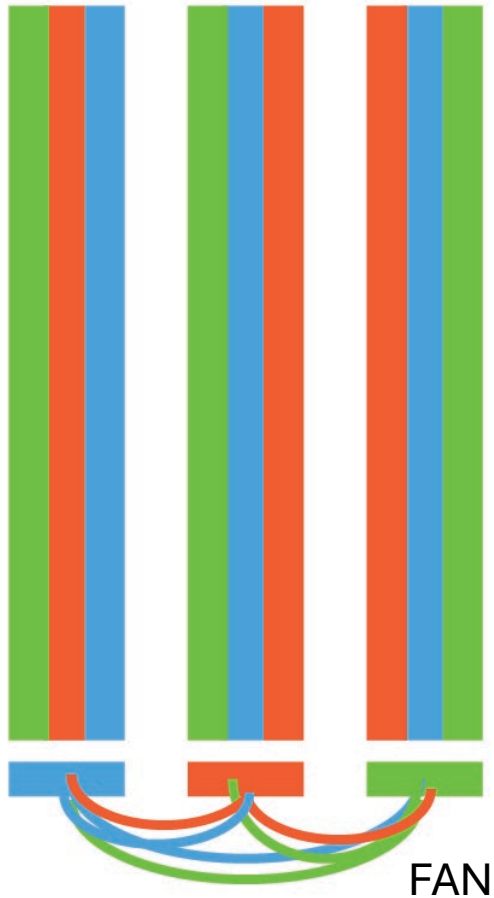
- FANET: each device retransmits all (!) the received positions of others that allows the signal travel farther but can saturate RF channel.
- FANET: good for limited number of devices.

- FLARM collision awareness for fast moving aviation: helicopters, gliders, private planes, etc.
- FLARM each device sends only its own position, excluding channel saturation.
- FLARM good for considerable number devices located in one area, as the load on band is much less

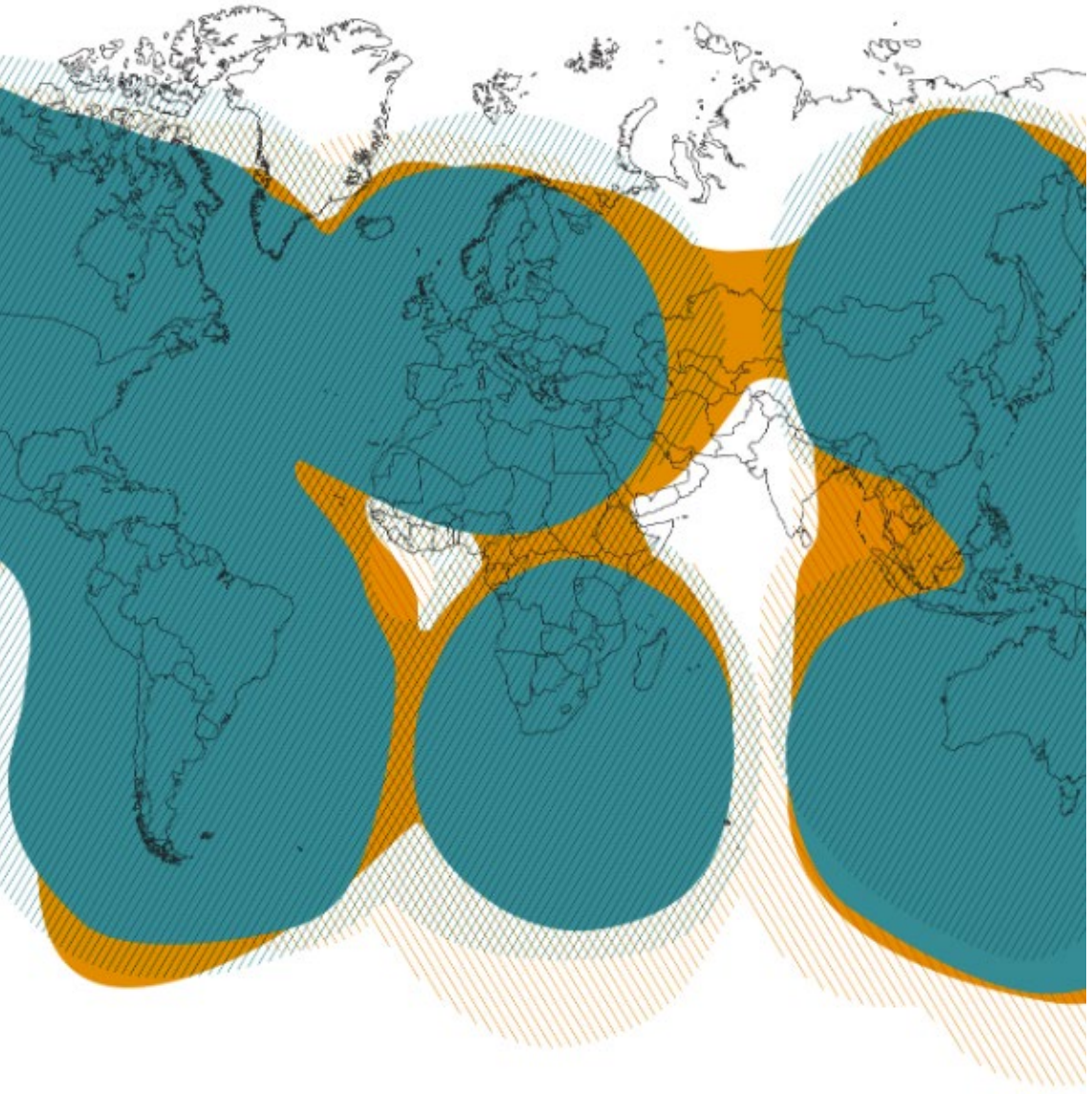




FLARM



FANET



Satellite tracking

- Global coverage including no-GSM areas (e.g SPOT on picture).
- But expensive, and can work only as emergency beacon.

GSM to Satellite

- iPhone and Google pixel have announced connection to satellites for emergency SMS, but you need to be out GSM coverage to get it.
- Currently some GSM devices can connect to some satellite operators but they are extremely expensive.
- The satellite operators that do provide connection for phones still have very sporadic and inconsistent coverage.

Conclusion

- New solutions and research in the field of combining RF transmission with GSM can significantly improve the quality of competition live tracking.
- Currently as we are in technology transition period. So, things are already not good as they were and not yet good as they should be.
- Remember band is finite. Our advice is to act responsively and knowledgeable.
- **Quantity in our case does not mean quality.** Organizers are advised not to overload GSM network or RF band of the competition.

Summary

- Live Tracking is now a critical safety tool for safety at Paragliding XC Competitions.
- Use of high-bandwidth apps can clog the cell network in remote areas if not planned carefully.
- In order to embrace innovation and open the market up to new applications without overwhelming the network, a well-considered and managed approach is needed.