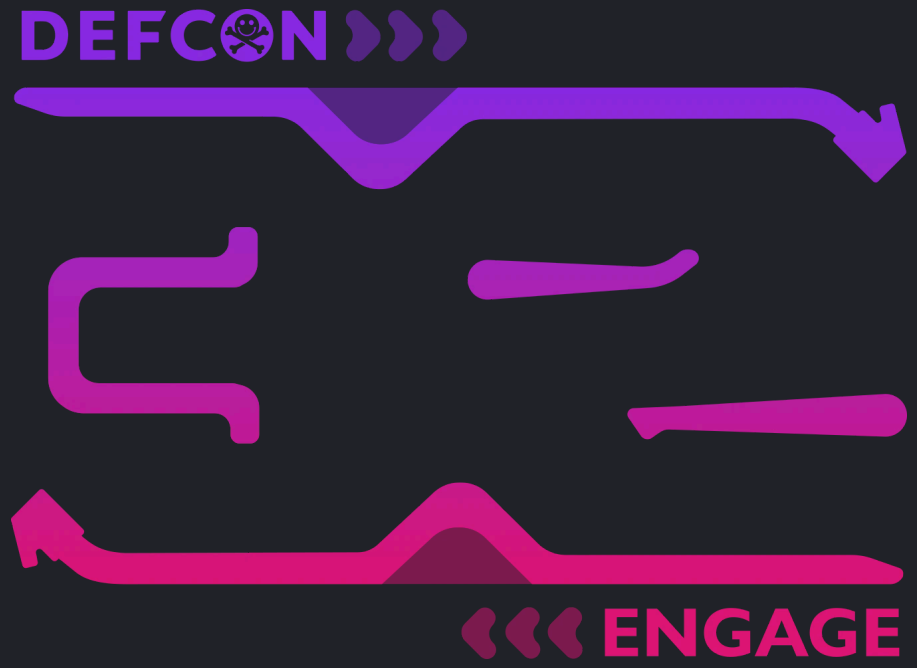
DEFCONtastic

du mesh, des flags,
du fun 😎



/me

- Hardware/Software Reverser
- Joue avec les protos wireless (des fois)
- Aime aussi coder (beaucoup)

DEF CON 32

- Ça se passe à Las Vegas 🤮
- C'est **très grand**
- C'est **blindé** de monde (35k pers.)

r/meshtastic • il y a 27 j
AutoModerator

🚀 DEFCON 32 Hackers: Level Up Your Mesh Game! 🔐

Get ready to join the exclusive Meshtastic network at #DEFCON2024!

✅ Scan our special DEFCON 32 QR code for a custom network config.
➡️ Stay tuned for more DEFCON-specific updates, including a special firmware release soon!

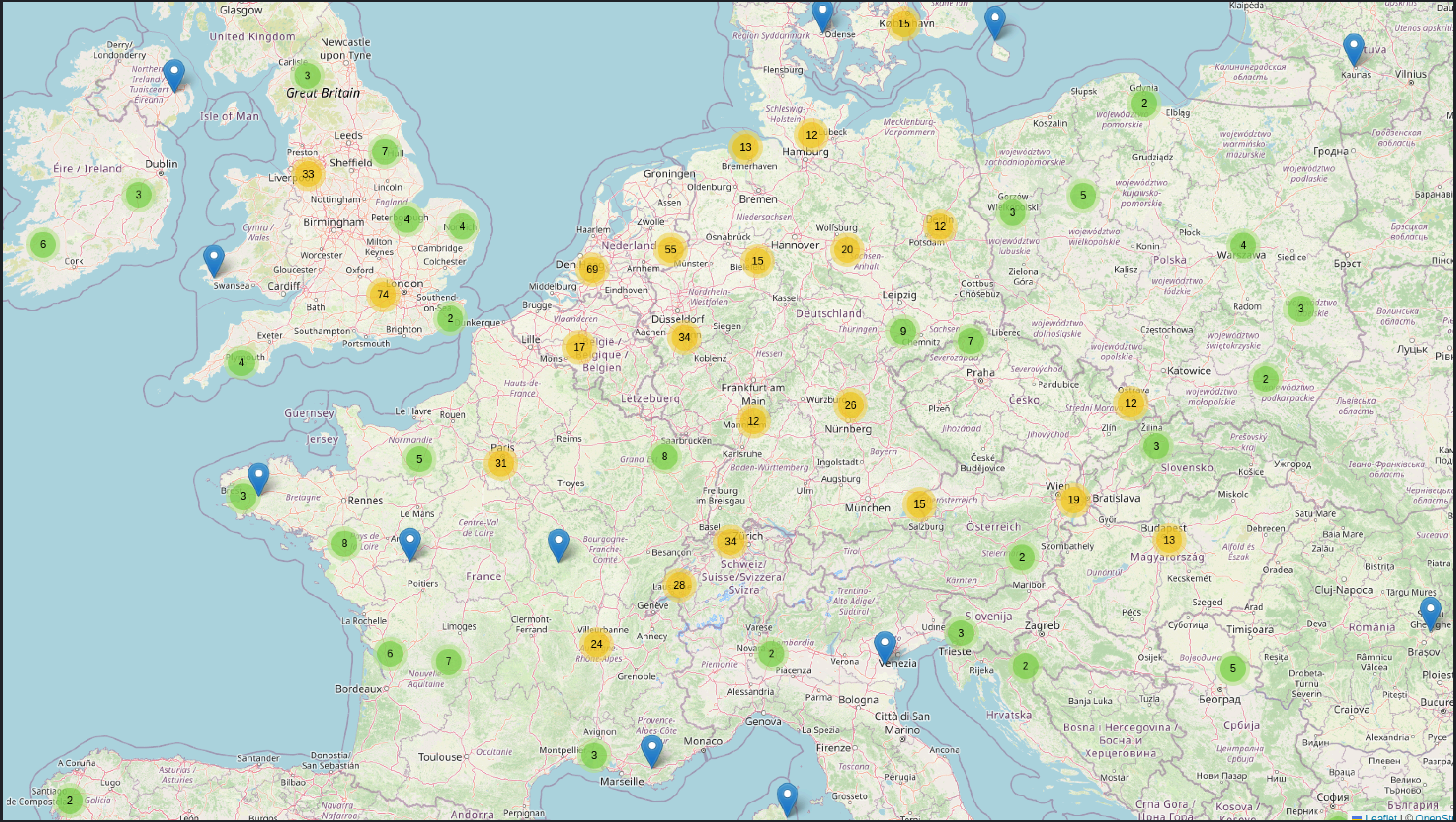
Gear up and stay tuned! #Meshtastic #MeshNetwork #defcon #defcon32 #dc32

Suivre
les talks à
DEFCON

Jouer
avec
Meshtastic

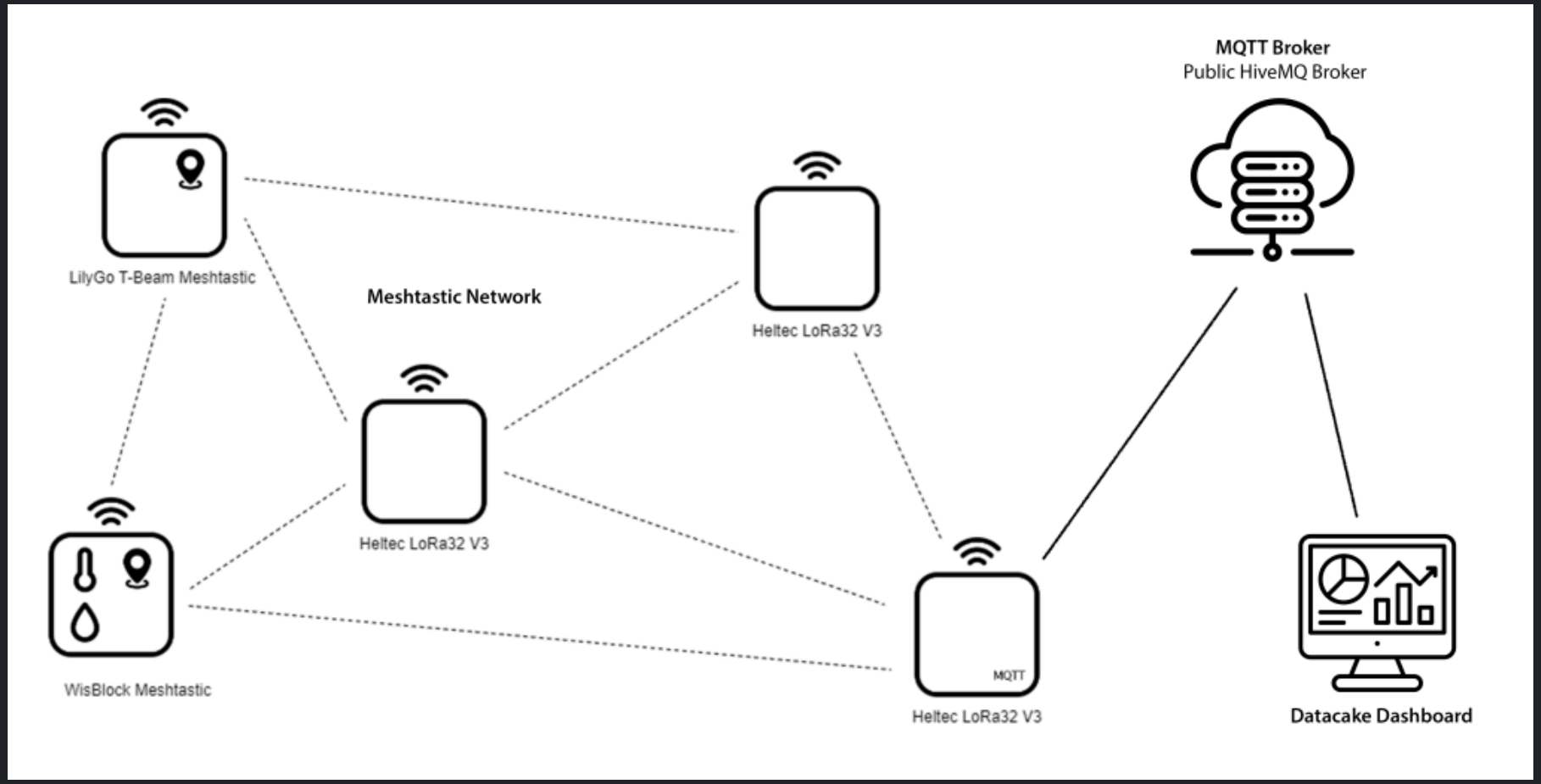
Meshtastic ?

- Réseau maillé (mesh) de communication
- Utilise **LoRa** !
- *"Relativement"* répandu

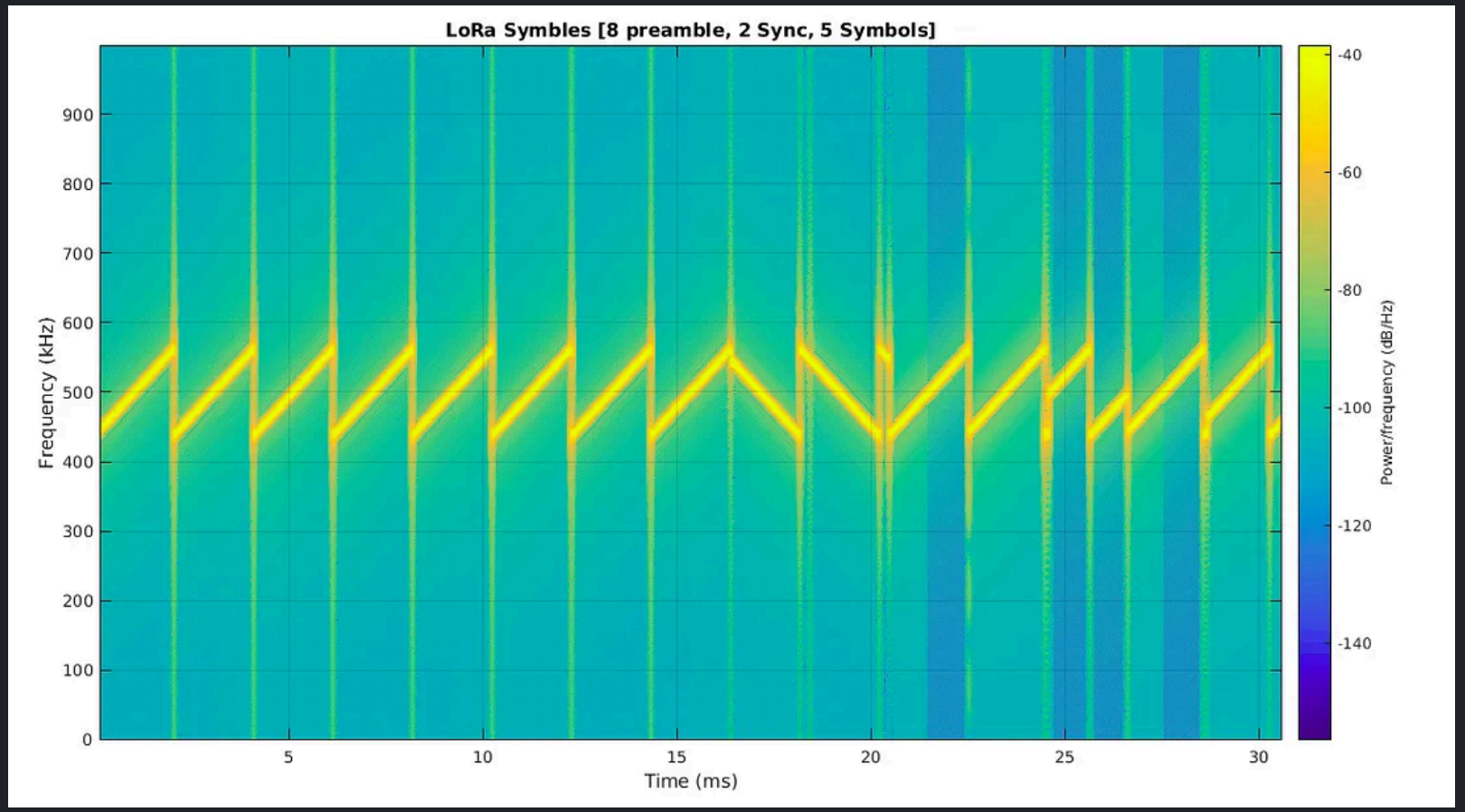


Glasgow
United Kingdom
Newcastle upon Tyne
Derry/ Londonderry
Carlisle
Great Britain
Isle of Man
Leeds
Preston
Sheffield
Éire / Ireland
Dublin
Liverpool
Lincoln
Nottingham
England
Birmingham
Peterborough
Cymru / Wales
Cork
Swansea
Cardiff
Gloucester
Oxford
Milton Keynes
Cambridge
Colchester
Worcester
London
Southend-on-Sea
Bath
Exeter
Southampton
Brighton
Portsmouth
Plymouth
Guernsey
Jersey
Le Havre
Rouen
Normandie
Bretagne
Rennes
Le Mans
Pays de la Loire
Poitiers
La Rochelle
Limoges
Bordeaux
Nouvelle-Aquitaine
Toulouse
Occitanie
Montpellier
Marseille
Avignon
Provence-Alpes-Côte d'Azur
Monaco
Andorra
Perpignan
Santander
Donostia/ San Sebastián
Bilbao
A Coruña
Lugo
Galicia
Asturias / Asturies
Navarra
Paris
Reims
Troyes
Centre-Val de Loire
France
Bourgogne-Franche-Comté
Besançon
Clermont-Ferrand
Villeurbanne
Annecy
Genève
Grenoble
Lille
Dunkerque
Mons
Hauts-de-France
Brugge
Vlaanderen
Middelburg
Haarlem
Den Haag
Nederland
Zwolle
Arnhem
Eindhoven
Groningen
Assen
Oldenburg
Bremen
Bremerhaven
Hamburg
Lübeck
Schleswig-Holstein
Flensburg
Odense
København
Region Syddanmark
Niedersachsen
Osnabrück
Münster
Bielefeld
Hannover
Wolfsburg
Nordrhein-Westfalen
Düsseldorf
Aachen
Siegen
Koblenz
Kassel
Hessen
Deutschland
Leipzig
Thüringen
Sachsen
Chemnitz
Potsdam
Berlin
Cottbus - Chóśebuz
Frankfurt am Main
Mannheim
Würzburg
Nürnberg
Saarbrücken
Karlsruhe
Baden-Württemberg
Bayern
Ingolstadt
Augsburg
Ulm
Freiburg im Breisgau
München
Basel
Zürich
Schweiz/ Suisse/Svizzera/ Svizra
Lausanne
Letzebuerg
Tirol
Salzburg
Österreich
Wien
Bratislava
Steiermark
Kärnten
Trentino-Alto Adige/ Südtirol
Varese
Novara
Piemonte
Lombardia
Piacenza
Alessandria
Verona
Venezia
Parma
Bologna
Genova
La Spezia
Firenze
Toscana
Città di San Marino
Perugia
Ancona
Grosseto
Udine
Trieste
Slovenija
Zagreb
Rijeka
Hrvatska
Maribor
Banja Luka
Tuzla
Bosna i Hercegovina / Босна и Херцеговина
Mostar
Crna Gora / Црна Гора
Kosova / Косово
Praha
Česko
Plzeň
České Budějovice
Liberec
Pardubice
Jihočeský
Jihomoravský
Zlín
Ostrava
Žilina
Slovensko
Košice
Miskolc
Győr
Szombathely
Budapest
Magyarország
Dunántúl
Kecskemét
Szeged
Pécs
Osijek
Debrecen
Oradea
Cluj-Napoca
Târgu Mureș
Arad
Deva
Timișoara
România
Brașov
Ploiești
București
Craiova
Drobeta-Turnu Severin
Râmnicu Vâlcea
Pitești
Reșița
Београд
Србија
Ниш
Видин
Плевен
София
България
Szczecin
Słupsk
Gdynia
Elbląg
Koszalin
Grudziądz
Gorzów Wielkopolski
Zielona Góra
Płock
Konin
Kalisz
Polska
Warszawa
Siedlce
Radom
Częstochowa
Katowice
Kaunas
Vilnius
Калининградская область
Гродна
Брэст
Луцьк
Ужгород
Leaflet

Off-grid mesh network



LoRa en 30 secondes



LoRa en 15 secondes

- **LPWAN**: communication *longue portée* et *low power*
- **envoyer loin**: étalement **étroit** et balayage **lent**
- **envoyer vite**: étalement **large** et balayage **rapide**

L'idée du siècle (ou pas)

- On a release **WHAD** à DEFCON (https://whad.io) 😈
- **WHAD** supporte **LoRa** !
- Et si on essayait d'avoir du fun avec Meshtastic ?

Meshtastic Layer 0

Offset	Length	Type	Usage
0x00	4	Integer	Destination NodeId
0x04	4	Integer	Sender NodeId
0x08	4	Integer	Packet ID (unique)
0x0C	1	Bits	Packet flags
0x0D	1	Bits	Channel Hash
0x0E	2	Bytes	RFU
0x10	<=237	Bytes	Data payload

Meshtastic Layer 0

- Le header est toujours **envoyé en clair**
- Les nodes peuvent **répéter** tous les messages
- ... et nous on peut tout monitorer 😈

Goto Scapy

```
# Define our Meshtastic message in scapy
class MeshtasticHdr(Packet):
    name = "MeshtasticHdr "
    fields_desc=[
        XLEIntField("dest_addr", 0xffffffff),
        XLEIntField("sender_addr", 0xffffffff),
        XLEIntField("packet_id", 0),
        BitField("hop_limit", 3, 3),
        BitField("want_ack", 0, 1),
        BitField("via_mqtt", 0, 1),
        BitField("hop_start", 0, 3),
        ByteField("channel_hash", 0),
        ShortField("rfu", 0),
    ]
```

Packets RX

```
# Import WHAD LoRa connector
from whad.device import WhadDevice
from whad.phy.connector.lora import LoRa

class Meshtastic(LoRa):
    """Meshtastic Connector
    """
    # ...

    def on_packet(self, packet):
        try:
            frame = MeshtasticHdr(bytes(packet))
            frame.show()
        except Exception:
            pass
```

Chiffrement

- **AES-CTR** avec *Nonce* public
- Clé de 128 ou 256 bits
- La clé chiffre **tous les échanges** !
- La clé du channel DEFCON est publique 😄

Sniffons, mes bons !

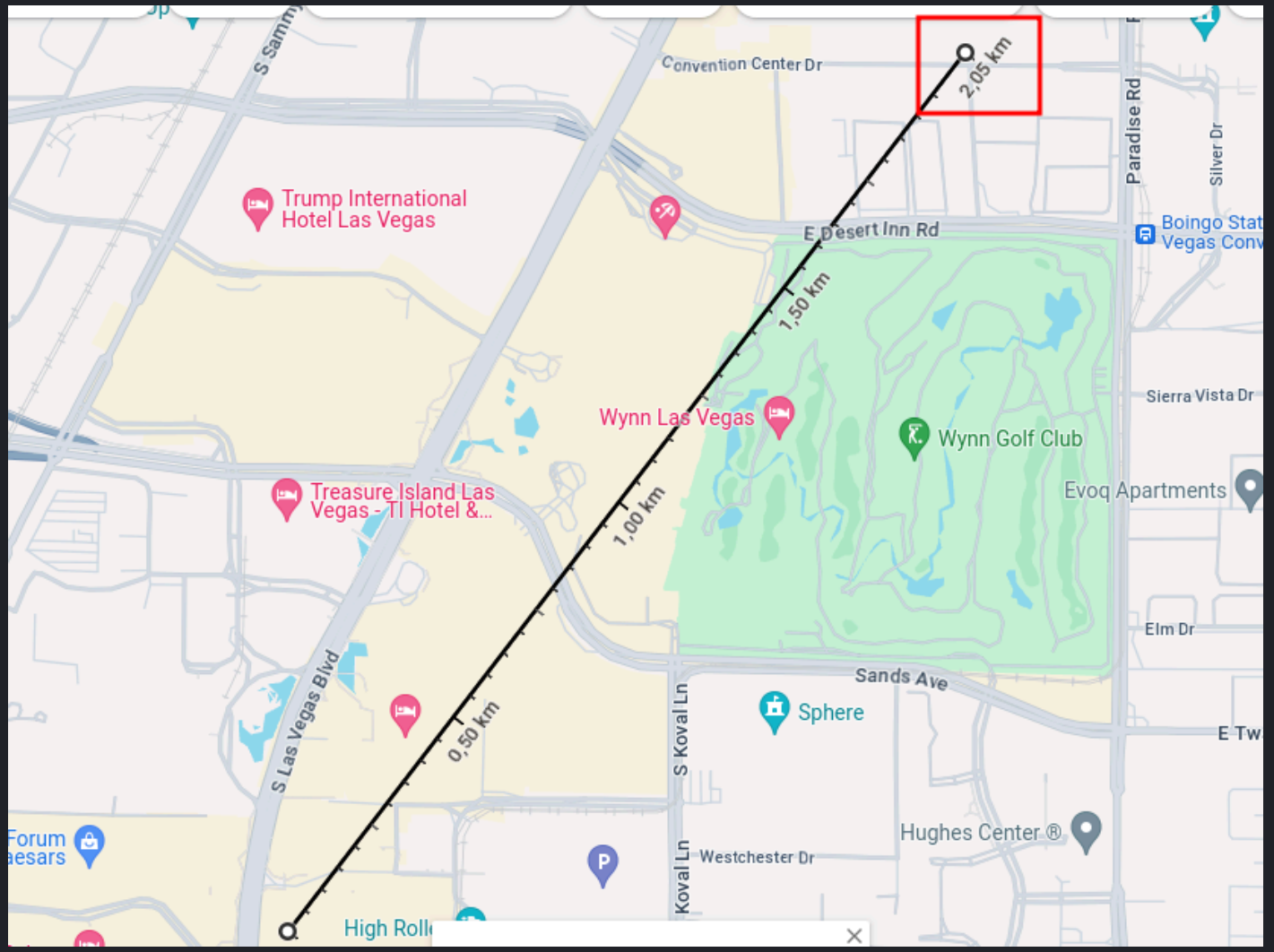
```
dda1843b -> ffffffff Challenge 6: wiX/<f=``N0co7*Zh2C
dda1843b -> ffffffff And dont forget to send a message to our bot, flags everywhere!
dda1843b -> ffffffff Challenge 4: IZGECRZNIQZUMQZQJYZTETCIIMZDAMRU
1930a15b -> 336908ec Q
dda1843b -> ffffffff Its another day at DEF CON, our CTF is still going. Post your solves at ctf.lone
lyhackers.lol, get prizes!
```

Client Meshtastic maison

```
(venv)  ✘ virtualabs@virtubox  ~/perso/defcon32/meshtastic  python3 mesh.py
my address: bfacf80e
MeshChannelConfiguration(freq=905625000, cr=45, sf=7, bw=250000, psk=384bbcc01dc022d181bf36b86
21e1fb96b72e55bf74227e9d6afb48d64cb1a1, chan_hash=209)
encryption key: 384bbcc01dc022d181bf36b86121e1fb96b72e55bf74227e9d6afb48d64cb1a1
> someone can read me ?
[bfacf80e] someone can read me ?
[33681cf8] Yep
> cool :D
[bfacf80e] cool :D
```

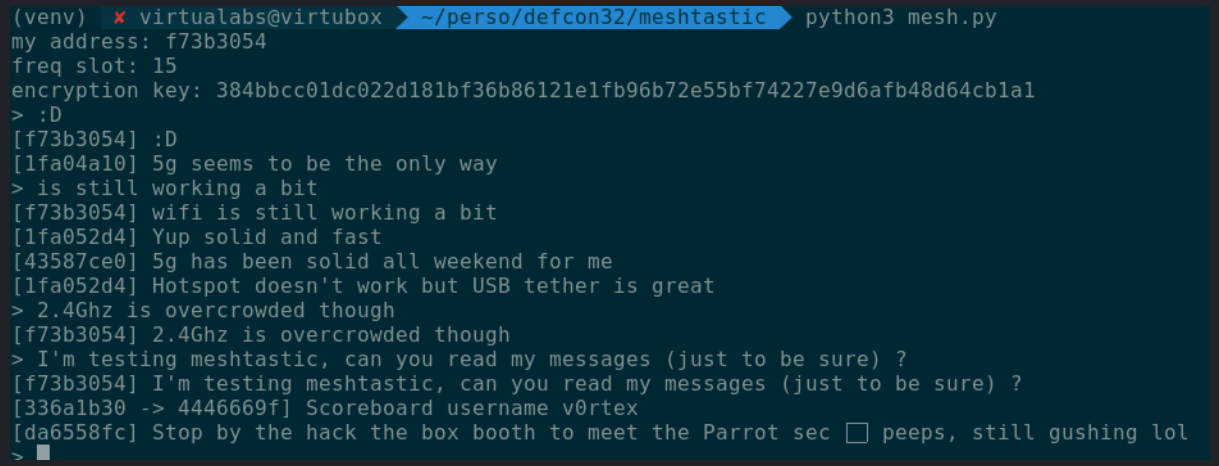
- Je peux spoofer n'importe quelle *NodeId* 🤣
- Envoi et réception de messages supportés
- **Aucune** info annoncée sur ma node 😈

Ça porte assez loin 🤯

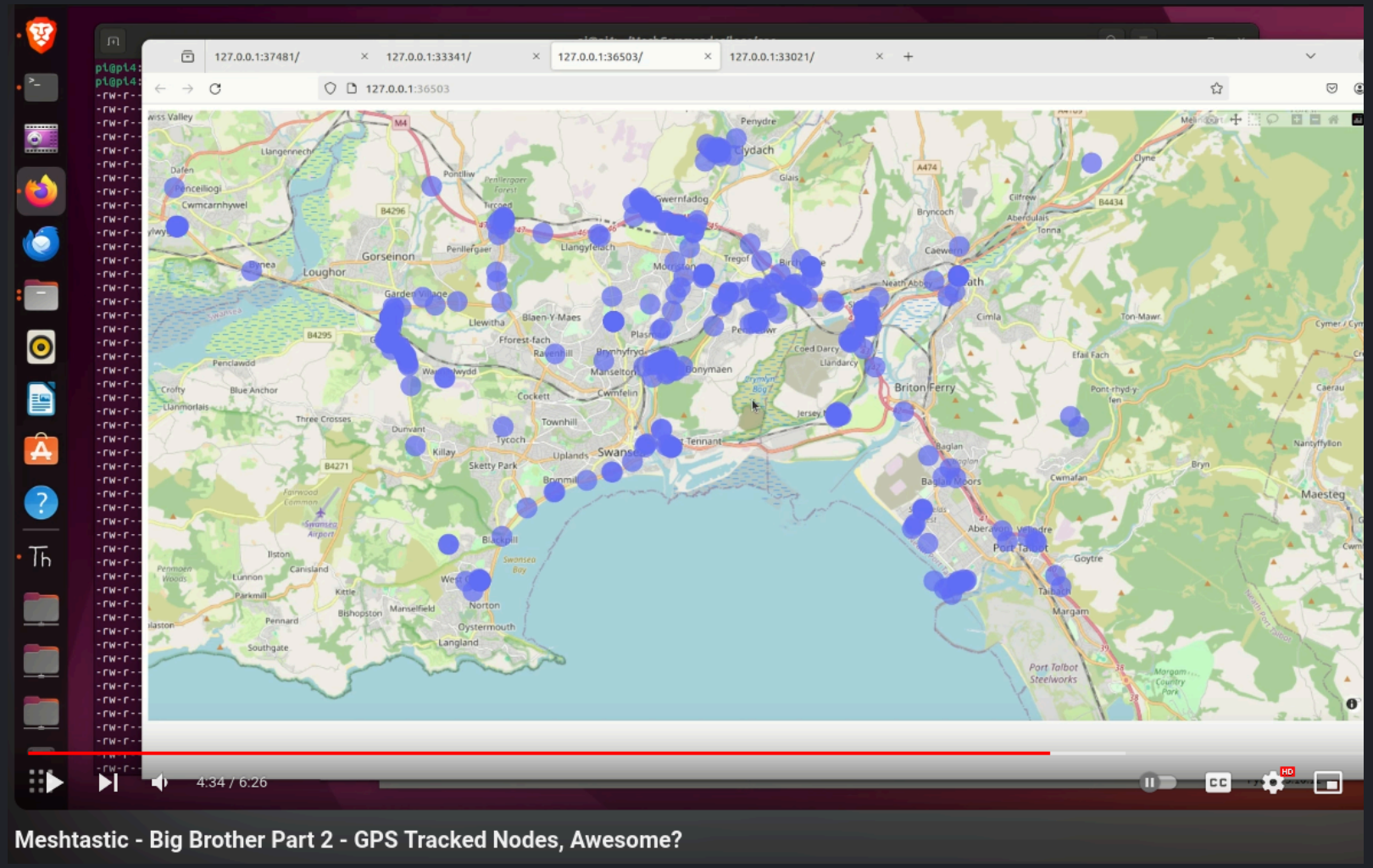


Privacy ?

- Pas mal de messages directs sur le chan public 🤣
- Quelques flags partagés
- Beaucoup de discussions privées (logistique, rdv, etc.)

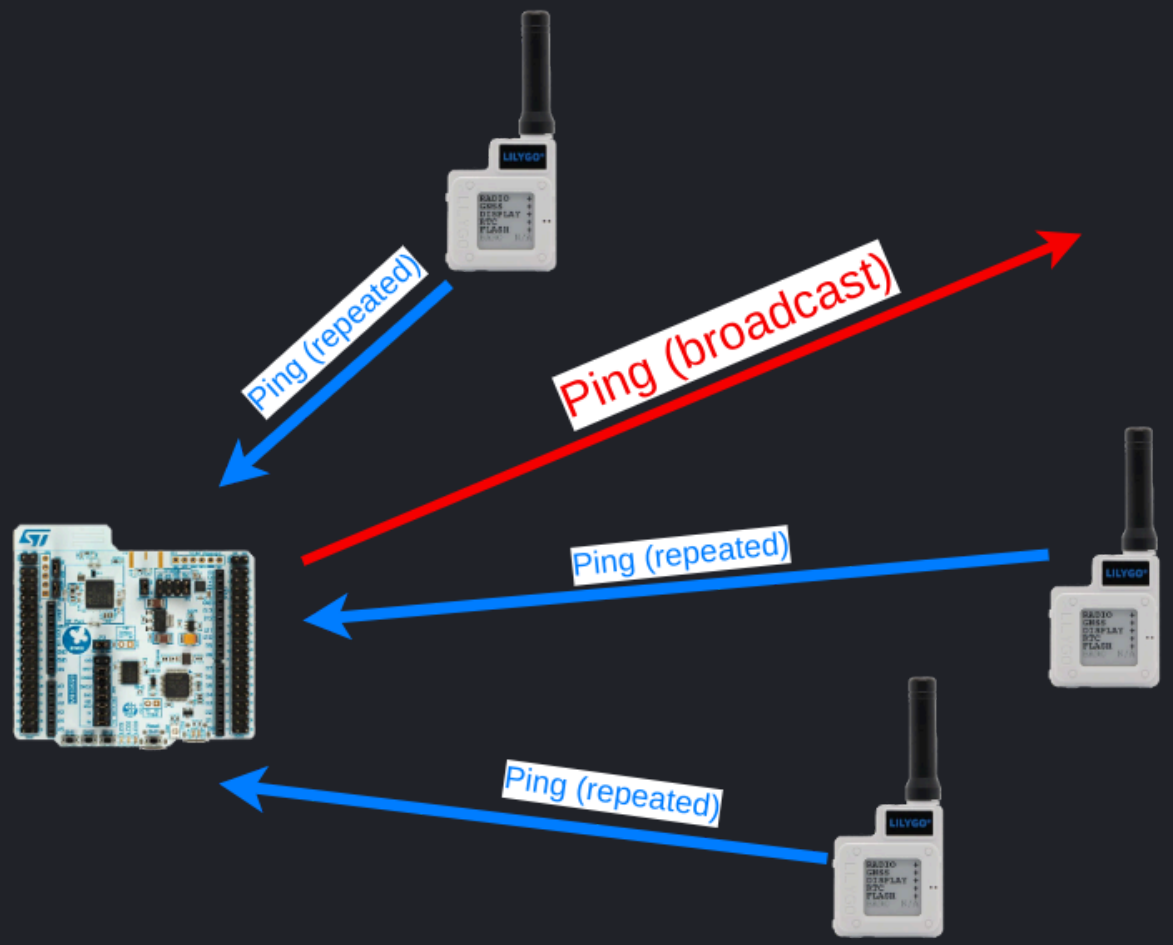


Tracking nodes



https://www.youtube.com/watch?v=5BpvEzeijYU

Scanning



mesh-scanner.py

Conclusion

Meshtastic vs. security

- C'est chiffré, **mais** ...
  - Pas de chiffrement authentifié (*AEAD*)
  - Méta-données non-chiffrées et non-signées
  - Pas de clés de sessions
  - La sécurité repose sur l'**unique clé de chiffrement**

Meshtastic vs. privacy

- C'est chiffré, **mais** ...
  - ID émetteur et destinataire en clair (*by design*)
  - les utilisateurs semblent **faire confiance au réseau**

- **L'absence d'outil(s) offensif(s)**: *illusion* de sécurité

Si vous souhaitez creuser

- https://whad.io + Nucleo STM32WL55 😎
- Getting started with Meshtastic
- Du LoRa avec des boards à 4$ (hack inside)
- gr-lora pour ceux qui préfèrent la SDR

Cocorico

We have created a public France-wide channel to connect users over MQTT until we have a good enough mesh to cover large areas.

Nous avons crée un canal public France pour connecter les utilisateurs via MQTT en attendant d'avoir un maillage suffisant pour avoir une meilleure couverture.

Pour nous rejoindre, rajouter le canal avec l'une des méthodes suivantes:

- **QR Code**:

- **URL**: Copiez ce lien 410
- **Manuellement**: Créez un canal **France** avec la clé **AQ==** et activez **Uplink** et **Downlink** par MQTT.

Source code

https://github.com/virtualabs/defcontastic

Merci 😊

- 🐘 @virtualabs@mamot.fr
- 🌍 virtualabs.fr
- 📧 virtualabs@gmail.com