LTE Recon and Tracking with RTLSDR

An SDR SIGINT Primer

whoami

Ian Kline

Wolf Den Associates

ian@wolfdenassociates.com

PGP Public Key

Lead: “Emissions Inspection”, Red Teams, Web App Pentests, Forensic Analyst, Hacker for Hire

Why should you listen

Fast

Need a PoC quickly

- start with open source research
- integrate with commodity tools
- you can be up and running an hour from now

Cheap

Build PoCs without major $$$ investment

- Start with RTLSDR-E4000 ~$50
- No need for other fancy LTE gear

Enough about me, let’s track some phones

Radio Used To Be Hard

http://www.k4ro.net/k4ro/station_tour/images/station10.jpg

Now for $50...

RTLSDR - E4000

Either RTLSDR will do, but the E4000 can hit one more LTE band than the newer R820T

Quick RTLSDR Demos

1 - Planes with ADS-B

Hex	Mode	Sqwk	Flight	Alt	Spd	Hdg	Lat	Long	Sig	Msgs	Ti\
ACA5DD	S								6	1	40
A482FC	S			37000					8	11	30
A57F04	S			36975					9	26	1
A6982F	S			8775	295	019			8	11	36
A6AB93	S	1346	NKS936	28450	451	265	39.163	-76.770	23	569	0
AD72C6	S	2423		34000					8	224	1
A5F581	S	7270		34975					8	387	2
A2CA5D	S	2470	UAL97	39000	492	044	38.684	-76.486	9	177	0
ACE96D	S	6640		5050					178	1004	0
A968F8	S			2800					20	269	2
A6A3C2	S	7163	JBU1201	34000	458	224	39.373	-76.518	16	650	0
A0A9D1	S			2525					10	296	51

Quick RTLSDR Demos

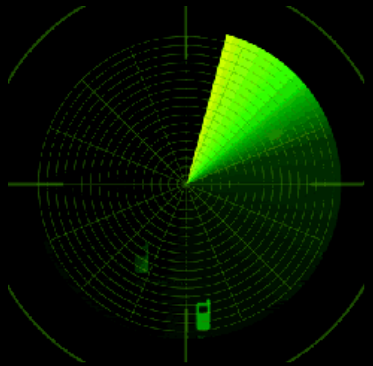
2 - Cars by their TPMS output

[Shove live TPMS feed from parking lot here]

Data vs Positional

All this is great, but reading data != positional tracking.

I want a tool with a big green arrow



HF/DF

HF/DF

1 - Field testing during WW2

2 - Measure signal strength and time of arrival

3 - Sink u-boats

4 - Required massive infrastructure

TDOA DF

"Time Difference of Arrival"

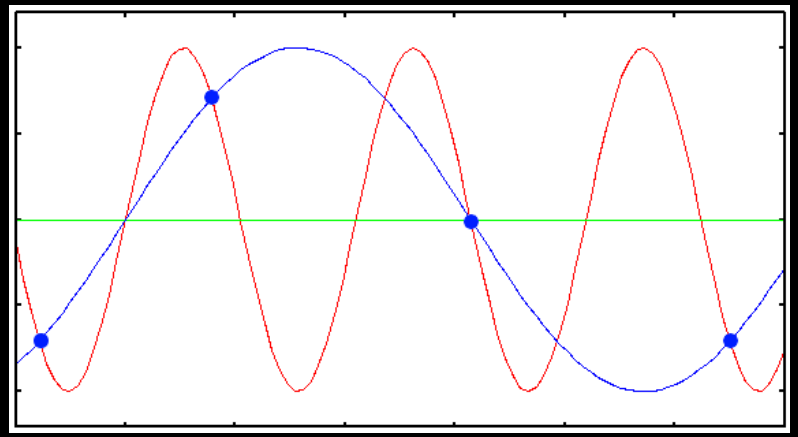
1. Measure time of arrival of a signal at two different points
2. Take the difference
3. Draw a bearing

TDOA DF - Challenges

1. Requires extremely accurate clocking between radios

TDOA DF - Challenges

2. High frequency signals exceed sampling rate of RTL-SDR platform



Pseudo Doppler DF

- Doppler DF requires a high speed moving antenna
- 50,000+ RPMs for GSM
- Use hardware antenna switch to simulate doppler effect to determine bearing

Commercial PD DF System

Quick and Dirty LTE Tracker

1 - DF sync data when phones connect to towers

2 - Save it

3 - Plot it all with Kibana because that’s easy

Quick RTLSDR Demos

3 - Tracking individuals by their LTE/GSM devices

[Emissions Inspection Demo]