



The Coming Threat of Sensor Networks

Simon Lewis and Michael Inggs

Radar Remote Sensing Group, UCT
Mini AOC Conference Simon's Town

Introduction

1. Sensor Networks
 - a. What are they?
 - b. Taxonomy of Sensors
 - c. PNT + D
2. Countermeasures
3. Examples
 - a. Active multistatic radar
 - b. Commensal radar
4. Conclusion



ASSOCIATION
OF OLD CROWS

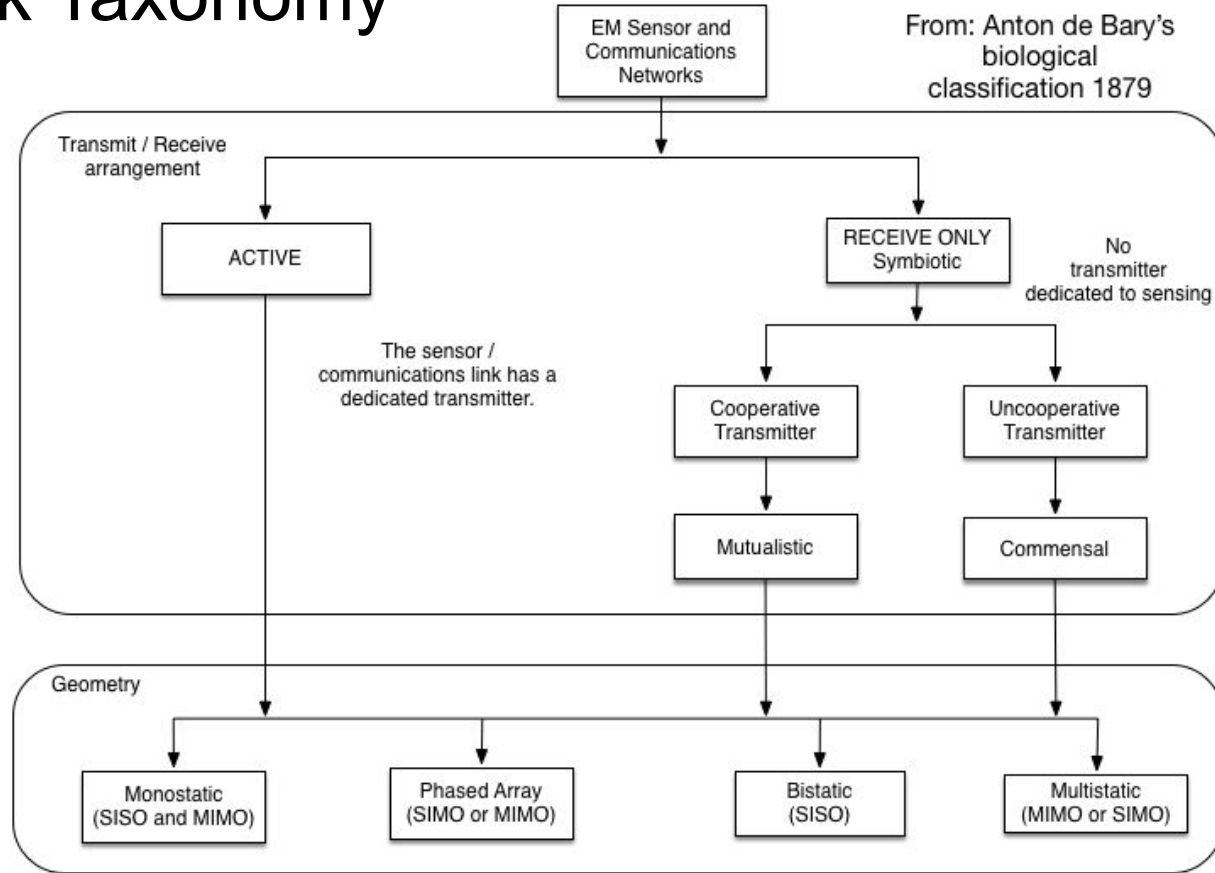


What are Sensor Networks?

Sensor Networks

- *Sensors*: any device that gathers environmental information
 - EM sensors particularly important in EW (Radar, Lidar, Optics)
- *Sensor Networks*: Spatially (geographically) dispersed coordinated sensors
 - Data fusion at different levels of abstraction
 - Radio - coherent and centralised
 - Video - incoherent and centralised
 - Plot - local processing - decentralised fusion
- Spatial and temporal coherence is the goal (especially in MIMO)
 - Coherence - Receiver phase is constant w.r.t transmitter

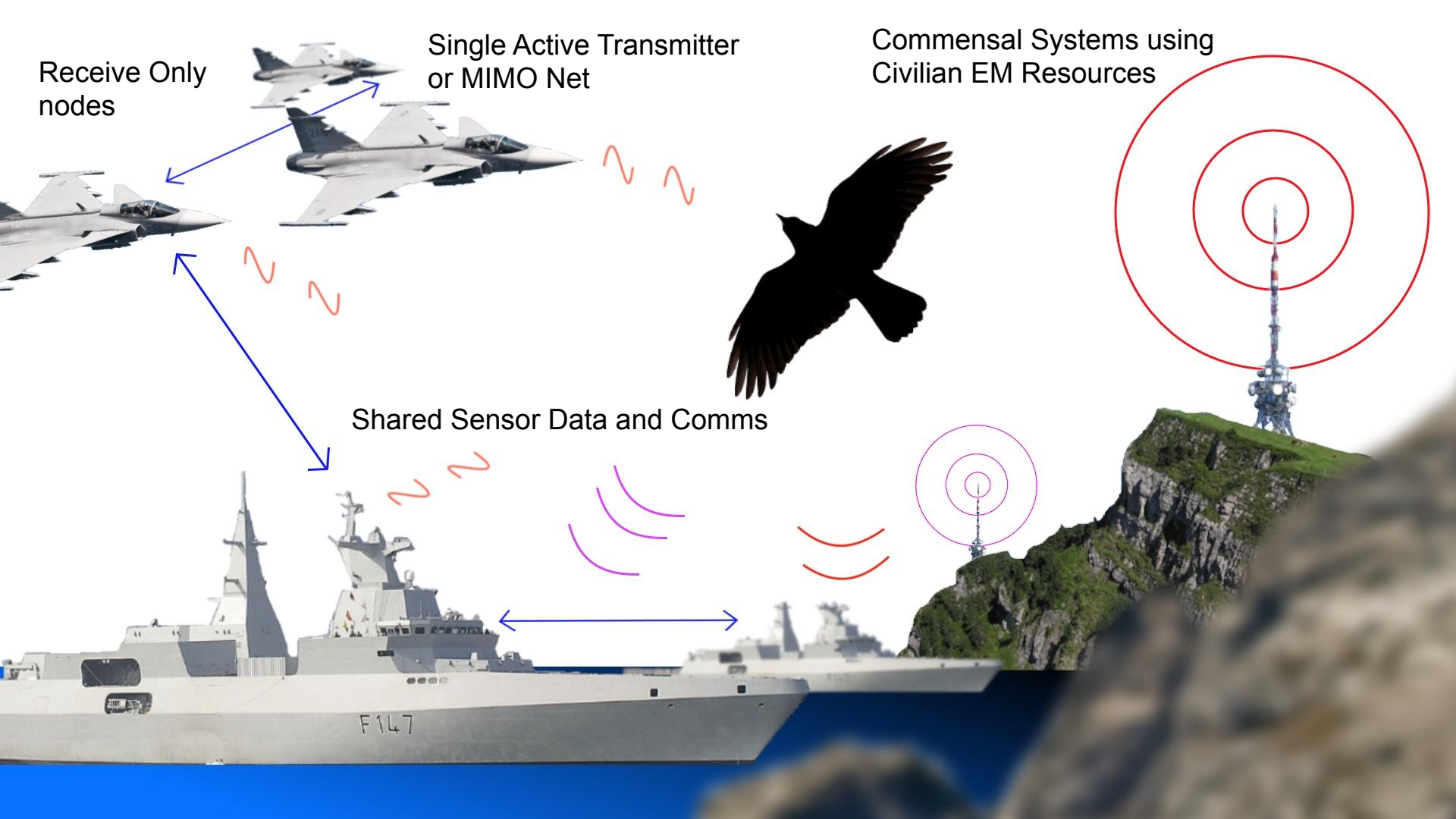
Network Taxonomy



Receive Only
nodes

Single Active Transmitter
or MIMO Net

Commensal Systems using
Civilian EM Resources



Shared Sensor Data and Comms

PNT + D

- **Position, Navigation and Timing (PNT)** required for coherence
- **Position and Navigation**
 - Simplest case: stationary nodes (can have *a priori* position)
 - Portable nodes require a spatial reference
 - Predominantly GNSS (GPS, GLONASS, Galileo, Beidou)
 - eLORAN or similar system
 - Custom PNTs and ePelorus (drive towards Resilient PNT)
- **Data Links (often required)**
 - Type of data fusion and command & control determine bandwidth
 - Communications

Temporal Coherence

- Time Synchronisation
 - Nodes need to know relative time
 - Care about time **accuracy**
 - Primarily affects bistatic range accuracy
- Frequency Syntonisation
 - Radars typically use low frequency stable Master Oscillators (OCXO)
 - Distributed Oscillators will diverge in phase/frequency
 - Care about frequency/phase **stability**
 - Short term - Phase noise (no correlation improvement in bistatic)
 - Long term - Drift
 - Affects range drift, CPI, clutter suppression, Doppler accuracy
- Phase synchronisation important in MIMO and distributed phased arrays

Time and Frequency Transfer

1. Fibre (ps)

- RFoF and White Rabbit
- Stable and RFI immune, but require fixed infrastructure

2. GNSS all-in-view (ns)

- Prevalent and cheap, includes GNSS spatial reference
- Prone to GNSS Denial

3. Low loss Coax (ns)

- Cheap and simple, but bulky and requires fixed infrastructure

4. Microwave and Optical links (ns- μ s)

- Expensive, RFI and multipath

5. RF direct/scattered path (μ s)

- RFI and multipath, not suitable to high resolution radar

Countermeasures

Defense Against Hostile Networks


- Passive nodes inherently difficult to detect and jam
 - Require visual reconnaissance
- Potential Countermeasures
 - GNSS Jamming and Spoofing
 - Easy and Cheap
 - ... but will jam own GNSS
 - Active Sensors
 - Locate and remove transmitter
 - Wide area jamming
 - Distribute power isotropically over assumed volume - Large power required

To protect Putin, Russia is spoofing GPS signals on a massive scale

GPS spoofing technology linked to Russia has been used almost 10,000 times, tricking ships into being off-grid. It's also used to protect Vladimir Putin and secretive Russian areas


<https://www.wired.co.uk/article/russia-gps-spoofing>

Pages: 1 2 3 4 5 6 Next »




[Handheld Powerful 8 Antennas Selectable 2G 3G 4G Worldwide Phone Jammer & WIFI GPS Jammer](#)

US\$302.99
★★★★★



[Handheld Selectable 8 band All Cell Phone Signal Jammer & WIFI GPS L1 All in one Jammer High-capacity \(USA Version\)](#)

US\$282.99
★★★★★



[Mini Handheld Mobile Phone and GPS Signal Jammer](#)

US\$79.99
★★★★☆

Russia jammed GPS during major NATO exercise with US troops

<https://edition.cnn.com/2018/11/14/politics/russia-nato-jamming/index.html>

Security

Sad Nav: How a cheap GPS spoofer gizmo can tell drivers to get lost

Eggheads reveal designs for causing navigation mischief for folks unsure of surroundings

By [Shaun Nichols in San Francisco](#) 16 Jul 2018 at 20:25

96 SHARE ▼

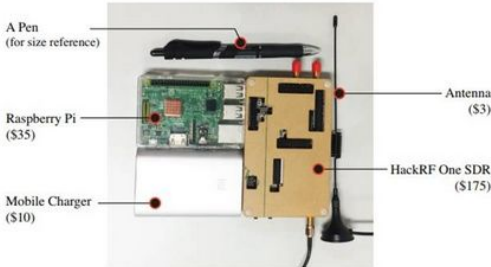


Figure 1: A low-cost portable GPS spoofer.

https://www.theregister.co.uk/2018/07/16/researchers_hack_gps/

HK\$1 million in damage caused by GPS jamming that caused 46 drones to plummet during Hong Kong show

- Expert says powerful device must have been used given how far machines were from land
- Online search shows large range of drone jamming and hacking electronics available for sale

<https://www.scmp.com/news/hong-kong/law-and-crime/article/2170669/hk-13-million-damage-caused-gps-jamming-caused-46-drones>

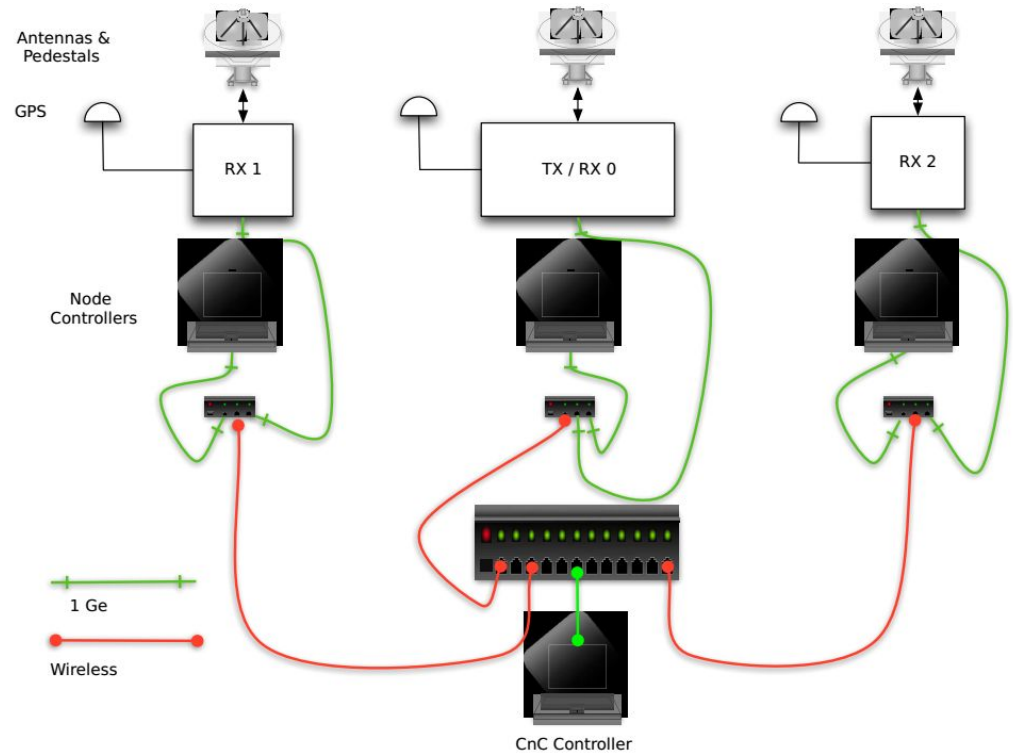
Examples

Example: Nextrad¹

Parameter	Value
X Band freq range	8.5 to 9.2 GHz
L Band	1.2 to 1.4 GHz
Polarimetry X Band	co- and cross-polar
Polarimetry L Band	co- or cross-polar alt PRI
Instantaneous BW	50 MHz
Peak power X Band	400 W
Peak power L Band	1.6 kW
X Band NF	3.5 dB
L Band NF	6.3 dB
Max PRF	Depends on blind range and
Max Pulse length	amplifier duty cycle



Example: Nextrad

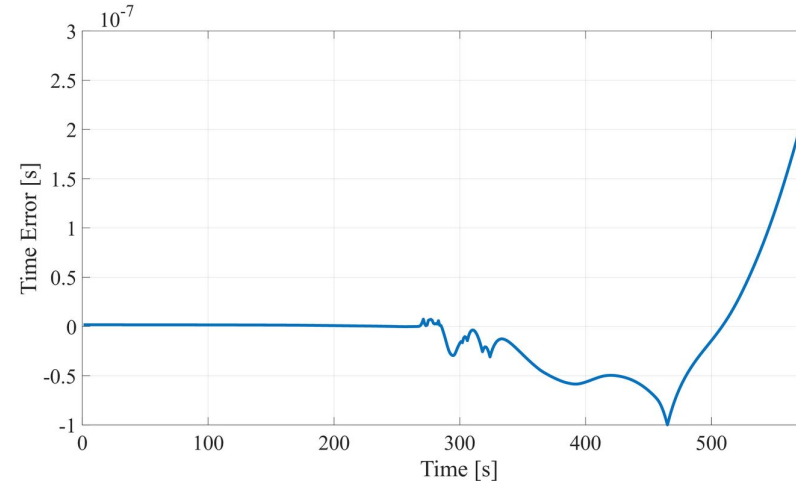
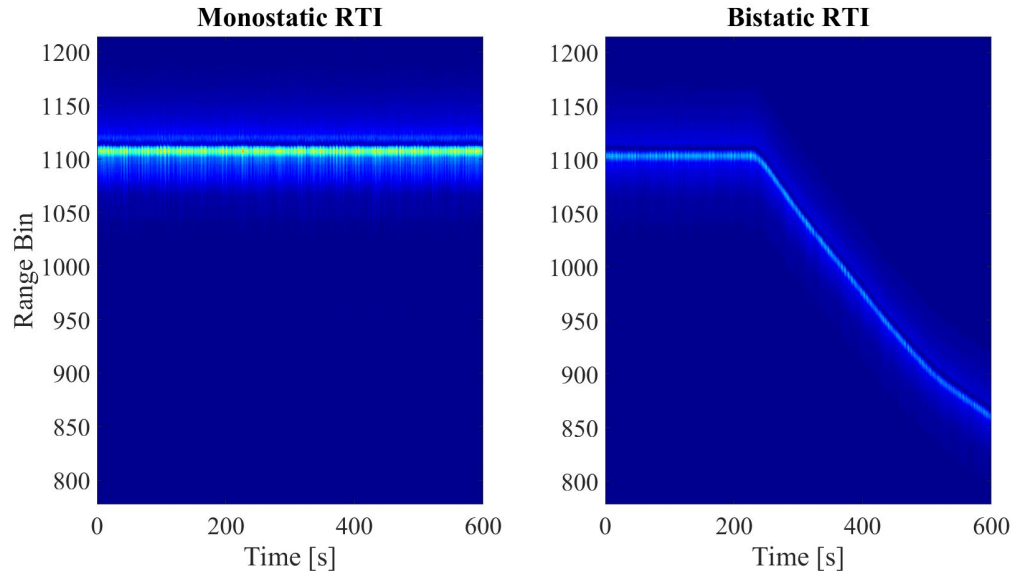


GPS Denial

- Roof of IMT recording Roman Rock lighthouse
- No Jammer used (pretty bad idea near military assets!)
- ‘Simulated’ GNSS denial by removing Transceiver GPS cable
- **Disclaimer:** Old GPS receivers (>15 years), No holdover.

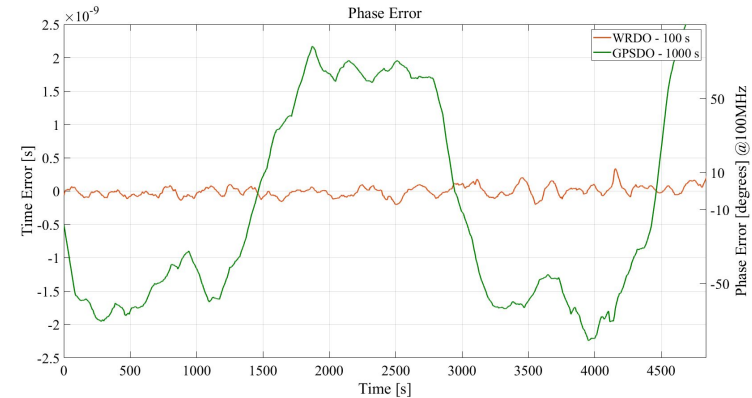
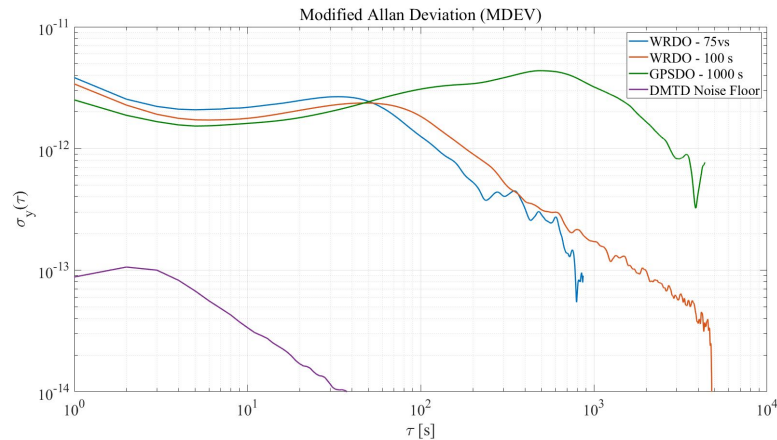


Roman Rock (The fastest lighthouse)

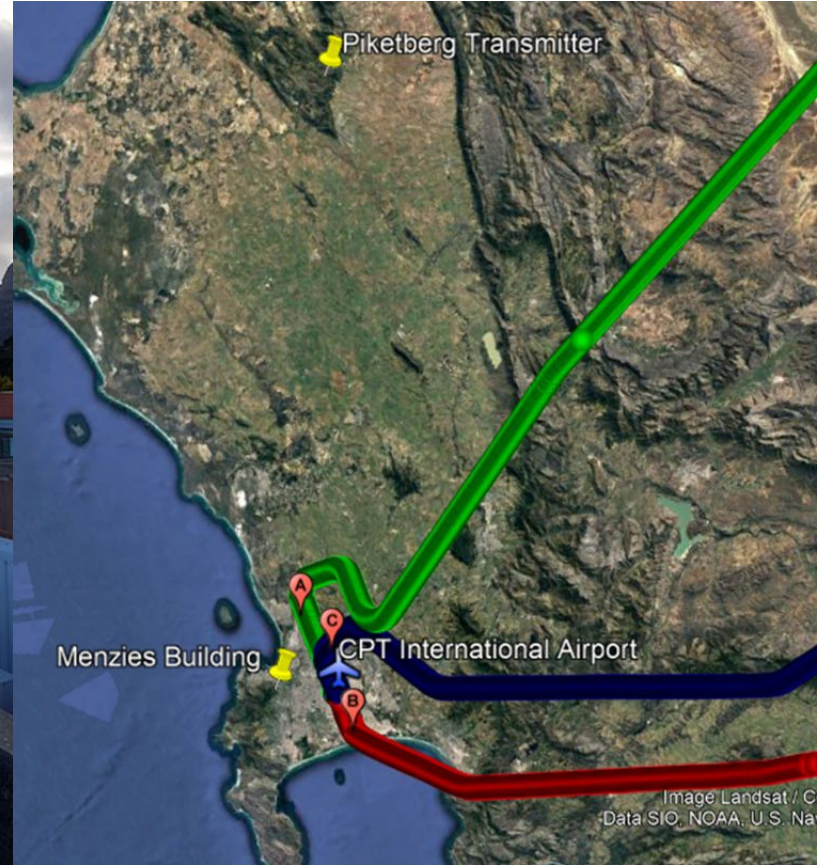


Fibre Optics and WR²

- White Rabbit is a fibre optic Ethernet network with sub-nanosecond synchronisation
- Modified to discipline GPSDOs



Example: Commensal at UCT³



FM Commensal Parameters

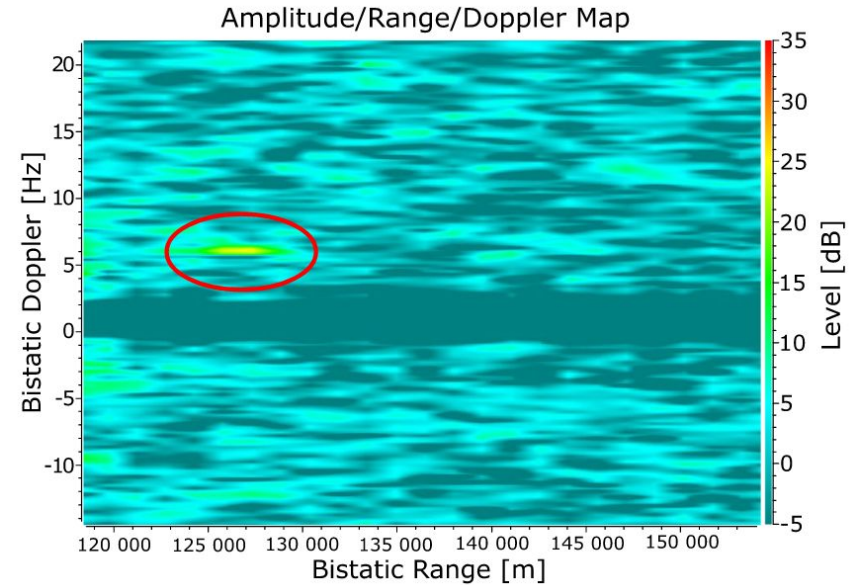
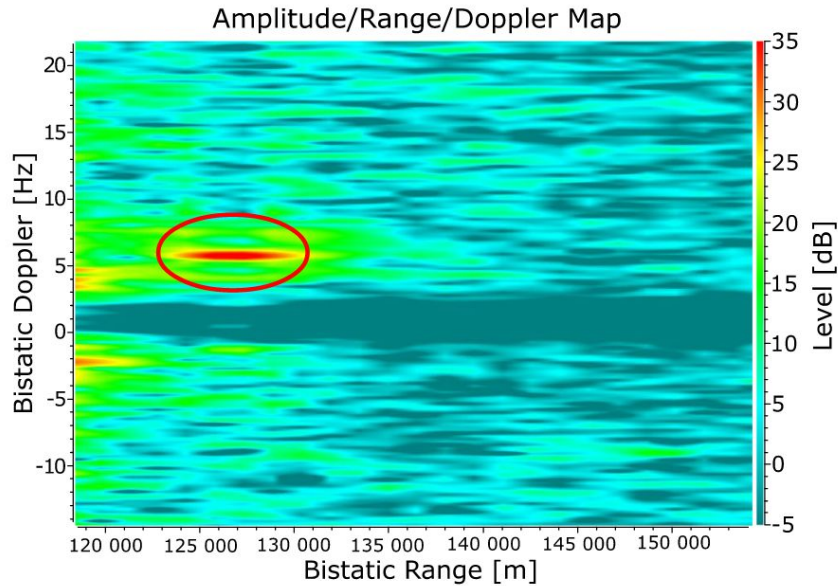
Transmitter (Tx)	
Antenna Beam Pattern	Isotropic
Antenna Gain	2.15 dBi
Antenna Altitude	850 m
Carrier Frequency	91.1 MHz
EIRP	16.4 kW
Waveform	Commercial FM radio

Receiver (Rx)	
Antenna Beam Pattern	Sinc
Antenna Gain	7.2 dBi
Antenna Altitude	140 m
LO Error	50 ppb (std. dev. of 0.01 Hz @ 204.8 kSps)
Noise Figure	4 dB
Digitisation	204.8 kSps complex, 16 bit quantisation
Tx to Rx Baseline	118 500 m

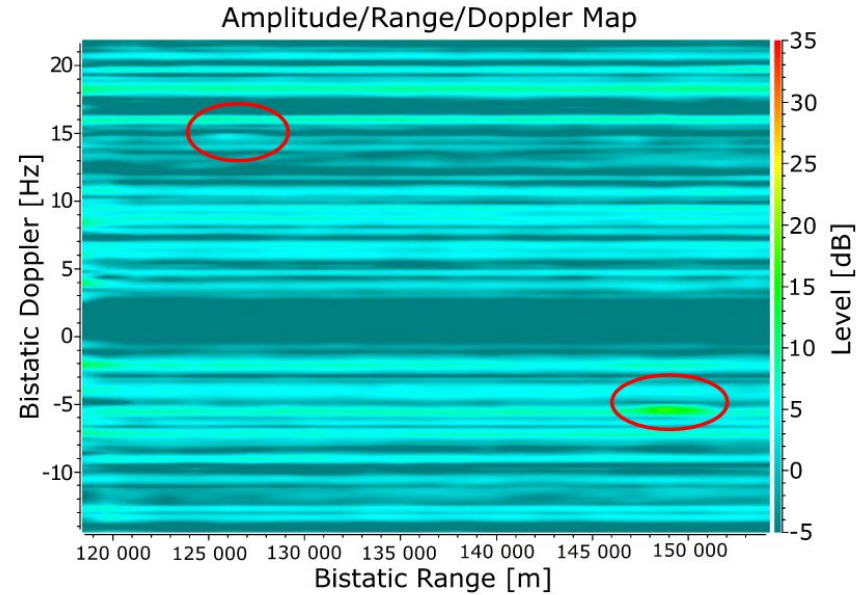
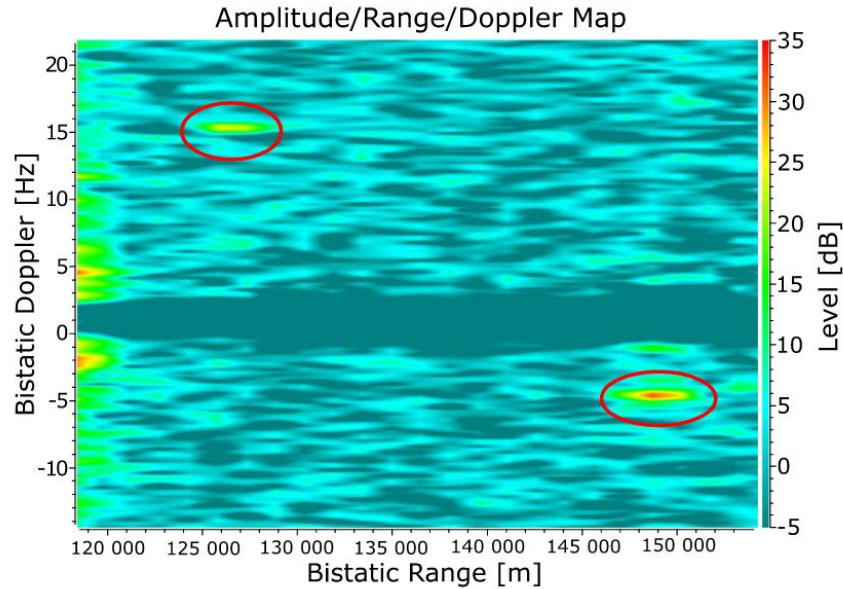
Jammer	
Antenna Beam Pattern	isotropic
Antenna Gain	2.15 dBi
Transmit Power	-35 dBm before antenna gain
Carrier Frequency	91.1 MHz
Waveform	204.8 kSps complex, random Gaussian white noise, sine wave on carrier

Processing Parameters	
DSI Cancellation	120 range, 5 Doppler bins
DSI Cancellation CPI	102400 samples (0.5s)
Range/Doppler Processing	120 range, 1601 Doppler bins
Range/Doppler CPI	819200 samples (4s)
CFAR Algorithm	GOCA-CFAR
CFAR Window	4 guard cells, 8 reference cells (either side of CUT)
CFAR Dimension	Doppler (Robust against bandwidth fluctuations)
CFAR Threshold	$P_{fa} = 10^{-5}$ (exponential noise model)

Broadband Noise Jamming

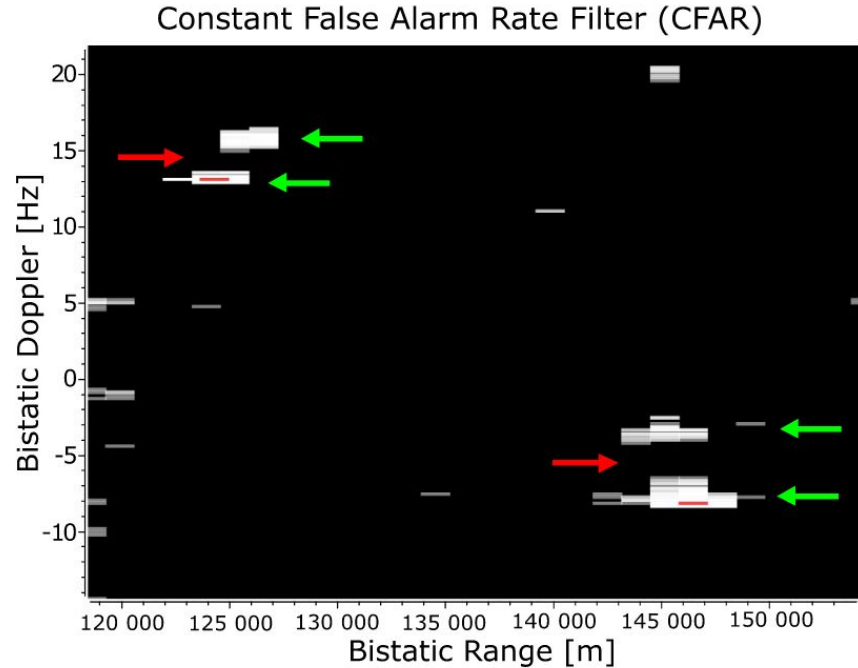


Single Tone Jamming



CFAR Single Tone

- Green = No Jamming
 - Red = Jamming On
-
- CFAR no detection during jamming



Conclusion

Conclusion

- Sensor networks pose a threat to homeland security
 - They are difficult to locate
 - Jamming power spread over a large volume
- Future of NeXtRAD
 - Operated in cooperation with IMT
 - Testbed for :
 - Combined communications
 - MIMO radar
 - Time and frequency references

Acknowledgements

- A list of capable engineers too long to list here ...
- ONR-G, FFI, IMT, IET AF Harvey Prize, Thales Nederland and UK, SANDF, NRF
- Reutech, Peralex
- armasuisse, Pentek

References

- 1** NextRAD: M. Inggs, H. Griffiths, S. Lewis, R. Palama, M. Ritchie, “Report on the 2018 Trials of the Multistatic NeXtRAD Dual Band Polarimetric Radar”, IEEE Radar Conference, Boston, 2019.
- 2** WRDO: S. Lewis, M. Inggs, S. Sandenbergh, “Evaluating an off-the-shelf white rabbit system to synchronise network radar via optic fibre”, IEEE Radar Conference, Seattle, 2017.
- 3** PCL Jamming: S. Paine, D. O’Hagan, M. Inggs, C. Shupbach, U. Boniger, “Evaluating the Performance of FM-Based PCL Radar in the Presence of Jamming”, IEEE Transactions on Aerospace and Electronic Systems, 2018.