Characterization of Radar and EW Systems

Andy Stove

26th June 2023

Characterization of Radar and EW Systems

Radar and EW systems are characterized in very different ways

- The tools available make it easy to characterize a new radar concept in ways which are robust against changes in the details of its implementation and its targets
- This is very valuable in research work
- Few such powerful 'general' tools are available for EW

- Radar Electronic Support Measures
- Active Jamming of Radar (Electronic Attack)
  - Electronic Counter-Counter Measures

Radar Analysis Techniques

- Matched Filter
  - Defines sensitivity in noise
    - Can specify/measure to better than 1 dB (with care)
  - Defines potential resolution / measurement accuracy in range
    - Seldom need full accuracy in range
- Cramér-Rao lower band
  - For example for angular measurement accuracy, where maximum accuracy is needed
- Tracker designs
  - Given input data accuracies (see above) the performance of these are statistically deterministic

Radar Performance Prediction

- In practice uncertainty and variability in clutter and noise levels limits accuracy of performance assessment
  - And makes excessive precision in prediction redundant
- But good quantitative match with predictions is possible
  - Say 3 dB with care over the long run
- Quantitive prediction of the performance of hypothetical systems is therefore useful.

Radar Performance Prediction

- Small, but significant/persistent, interest in the theory and practice of "The Specification and Measurement of Radar Performance"

EW System Specification (1)

- Effectiveness of EW is less closely tied to low-level metrics than for radar
- Receiver processing chain:
  - RF signal conditioning and detection → pulse descriptor
  - Pulse train analysis → emitter descriptor
  - Library matching → emitter type → platform type, possible countermeasures

EW System Specification (II)

- Platform type → situational awareness → higher level tactical actions
- Possible countermeasures → disrupt radar operations → reduce platform effectiveness.
- Four non-deterministic stages between detection and military effect

Generic ECCM Improvement Factor?

- Seeking for a general way to measure ECCM resistance
- Analogy with MTI Improvement Factor
  - Although that is also (arguably) an over-simplification
- Balance:
  - MTI (constant PRF/constant frequency) to suppress chaff
  - Frequency/PRF agility to avoid jammers
- Creating a single definition of ECCM Improvement Factor is generally reckoned to be not possible

ECM As 'Cheating the Rules' (1)

- Essence of warfare is to do the unexpected – 'break the accepted rules'
- Therefore, there can be no 'general' rules to estimate effects of ECCM techniques
  - Except for the limits imposed by the laws of physics
    - Except to the extent that these cannot be evaded

Estimating the Effectiveness of ECM

- Once a technique is found, the effectiveness of the ECM can be estimated because the performance of the radar is well-characterised
- However, the effectiveness of ECCM cannot be so well characterised because the behaviour of the ECM is not so tightly characterised [?]
- (Cannot use game theory as that assumes the players play by the rules instead of trying to break them) [?]

The Questions We Want to be Able to Answer:

- How should I design a radar to protect it from ECM?
- How should I design the ECM to degrade the usefulness of radars?
- These are 'Inverse Problems'
  - Must try various solutions and see how well they work
- Is my ECM or ECCM idea of sufficiently general application to be worth developing?

The Questions We Want to be Able to Answer:

- The above are essentially "researchers' " questions.
- Developers can be more specific in specifying the 'opponent'
- But taking that approach too far will risk making the system vulnerable to countermeasures which the customer hasn't thought to specify

Approach (I)

- Simulate scenarios, radars, ESMs, ECMs in software
- Run many versions and try to extract general rules
  - Ideally:
    - Doing "this" to the radar reduces ECM effectiveness by *X* (dB, %, ??)
    - This changes tactical outcome by *Y*

Approach (II)

- Ideally use representative, unclassified, inputs
- May need classified inputs
  - But results will average results of many different ‘experiments’
  - ‘Averaged’ conclusions may still be able to be unclassified

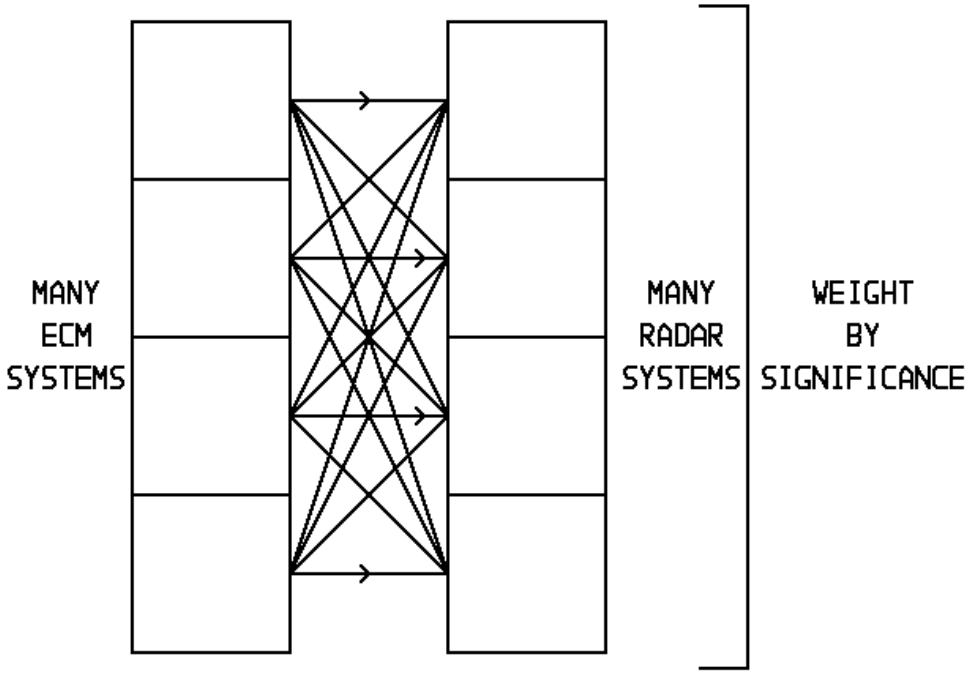
Prior Art

e.g. Bachmann, D. J., Evans, R. J. and Moran, B., "Game Theory of Analysis of Adaptive Radar Jammer" IEEE Proc AeES **47**, pp1081-1100 (2) April 2011

- but only considers 'detection' not the tactical outcome.

Many Radars / Many ECMs

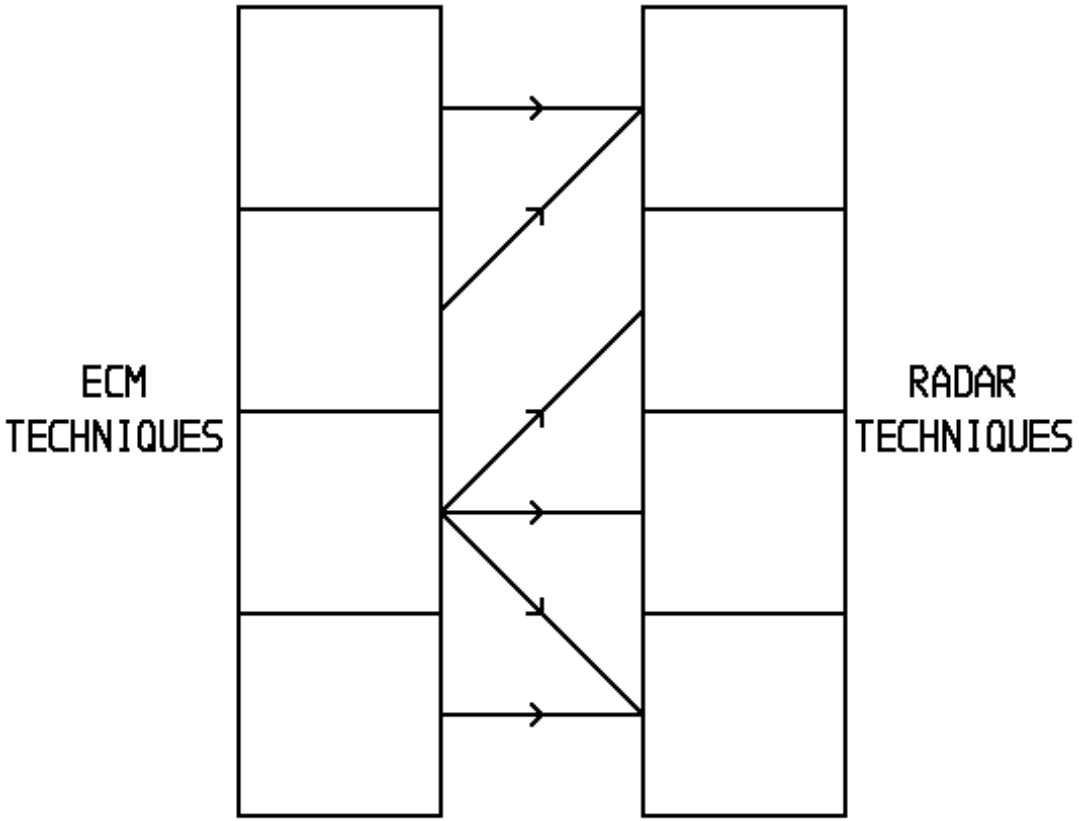
- Umpteen Interactions
- Need to 'average' results
- Similar Issue for ECCM



Look Instead at Techniques

- Simplify by assumeingthat the radar has been properly designed: e.g.
  - Noise jamming only affects detection
  - False target jamming only affects plot extractor & tracker but not detection
- No need to ‘average’ results

Looking at Techniques



Conclusions (1)

- Mathematical models can characterise radar behaviour well, but this is not the case for EW
- EW techniques are essentially opportunistic, often responding to inadvertent features of the radars
  - But they are still subject to the laws of physics

Conclusions (II)

- For research we aspire to be able to answer general questions:
  - How should I design a radar to protect it from ECM?
  - How should I design the ECM to degrade the usefulness of radars?
  - Is my ECM or ECCM idea of sufficiently general application to be worth developing?

Conclusions (III)

- Possible approach
  - Simulate effect of technique on tactical outcomes
  - Extract unclassified parametric performance
- Not sure this will work
- Other suggestions?