Improved lethality and survivability through advanced networking

Toby Prescott
Northrop Grumman Technical Fellow
Avionics and Tactical Networks
Chief Engineer
Wave of the Future - Robust and Secure Networking

- Networking of modern weapons systems is essential to produce the full capability inherent in modern weapon systems.
- Vulnerabilities arise when these networking capabilities can be detected by an adversary or diminished through an adversary’s electronic attacks.
- Multiple techniques can be employed to counter these tactics but requires the application of all available techniques to combat a sophisticated adversary’s attempt to exploit the communication network.
Wave of the Future – Protecting Our Communications

• The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  – Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications

• The primary techniques employed to add robustness to the communication are
  – Directionality
  – Frequency Of Operation
  – Frequency Hopping
  – Direct spreading
  – Amplitude Control
  – Modulation/time dithering
Wave of the Future – Protecting Our Communications

• The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  – Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications

• The primary techniques employed to add robustness to the communication are
  – Directionality
  – Frequency Of Operation
  – Frequency Hopping
  – Direct spreading
  – Amplitude Control
  – Modulation/time dithering

1. Even the simplest of antenna apertures provides an improvement in range performance of at least a factor of four when the adversary is not in the main beam
2. Improves performance from detectability and jamming equally
3. Array design can be optimized for improved RCS
Wave of the Future – Protecting Our Communications

• The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  – Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications

• The primary techniques employed to add robustness to the communication are
  – Directionality
  – Frequency Of Operation
  – Frequency Hopping
  – Direct spreading
  – Amplitude Control
  – Modulation/time dithering

1. Choice of frequencies can have profound propagation effects for signal penetration to the ground
2. Available bandwidth is directly proportional to selected operating frequency
3. Availability of adversary equipment for jamming and/or signal detection
Wave of the Future – Protecting Our Communications

• The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  – Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications

• The primary techniques employed to add robustness to the communication are
  – Directionality
  – Frequency Of Operation
  – Frequency Hopping
  – Direct spreading
  – Amplitude Control
  – Modulation/time dithering

1. Hopping between frequencies limits the amount of integration time available to an adversary’s detection process and increases the complexity of the receive operation
2. Larger number of hops increases the number of hypotheses required for evaluation to determine signal presence
3. Jamming is more complicated (typically invoking follower jammers) requiring agility
4. Fast hopping greatly complicates both the jamming and detection processes
Wave of the Future – Protecting Our Communications

• The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  – Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications

• The primary techniques employed to add robustness to the communication are
  – Directionality
  – Frequency Of Operation
  – Frequency Hopping
  – Direct spreading
  – Amplitude Control
  – Modulation/time dithering

1. Direct spreading is useful to create a trade between transmit power and bandwidth
2. Exclusive use of direct spreading is effectively countered by allowing larger integration times afforded to the adversary’s receiver – any gains obtained via spreading can be offset with increased integration times.
3. Narrow band jamming is perhaps most effective requiring good amplifier linearity to avoid capturing of the RF front end
Wave of the Future – Protecting Our Communications

- The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  - Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications
- The primary techniques employed to add robustness to the communication are
  - Directionality
  - Frequency Of Operation
  - Frequency Hopping
  - Direct spreading
  - Amplitude Control
  - Modulation/time dithering

1. Amplitude control to adjust the transmit power to achieve minimum acceptable performance to the communicant can greatly reduce signal detectability for communicants close to the transmitting entity
2. Amplitude control does have the deleterious effect of making the radio more susceptible to jamming
Wave of the Future – Protecting Our Communications

- The measure of goodness of a robust communication system is a direct measure of its effectivity against an adversary’s bad intentions
  - Evaluated in terms of the range of communication effectiveness to the range at which an adversary can exploit those communications
- The primary techniques employed to add robustness to the communication are
  - Directionality
  - Frequency Of Operation
  - Frequency Hopping
  - Direct spreading
  - Amplitude Control
  - Modulation/time dithering

1. Modulation and/or time jitter is designed to remove predictable signal structures that an adversary can exploit
2. For example for a fixed modulation and chipping rate, an adversary can implement the equivalent of a simple delay line discriminator for demodulation of the signal
3. Jitter of the basic signal structure requires the adversary to evaluate a larger set of hypotheses for signal detection
Wave of the Future – Spectral Reuse In Directional Network

• Aside from the effects of increased robustness, directional networking can provide increased network capacity through spectral reuse

• Given the directional nature of transmissions, multiple entities within the network can transmit at the same time occupying the same spectral bandwidth without disrupting each others communications

• When coupled with power control, even more users can occupy the same bandwidth
Wave of the Future – Comprehensive Solution

• For the greatest effectivity, all the techniques available to our design team should be employed to enhance the performance of our radio links in the face of a determined and sophisticated adversary

• Integrating a communications network to collaboratively enable our warfighters to prosecute their mission effectively is much more complicated and expensive than the counter measures to be employed by our adversaries

• A high valued network capability that improves our warfighter lethality and survivability will surely garner the attention of our adversaries creating an incentive to develop counter measures to exploit the weaknesses in our system

• Therefore it is only logical that we make our system as robust as possible making the adversary’s task more complicated