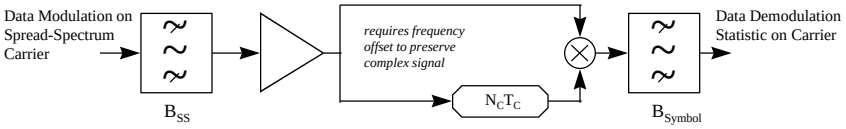
Transmission Security (TRANSEC)

John H. Cafarella
MICRILOR, Inc.
Wakefield, MA

TRANSEC vs. Data Encryption

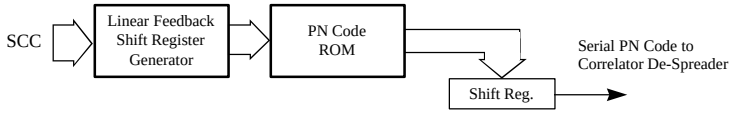
TRANSEC	Data Encryption
– Waveform-Domain	– Data-Domain
– Protection Against Jamming, Spoofing and Traffic Analysis	– Protection Against Disclosure of Data to Any Unauthorized Party
– Protection for Seconds	– Protection for Decades
– Local Coordination	– Net-Wide Coordination
Needed by All Users for Most Transmissions	Needed by Few Users for Some Data

Example Repeated Code Attack



- Little A Priori Information
  - know that code is repeated, and its length
  - don't need code pattern
- ~ 3 dB less than full Processing Gain
- No SSDS Protection; Must Add Encryption

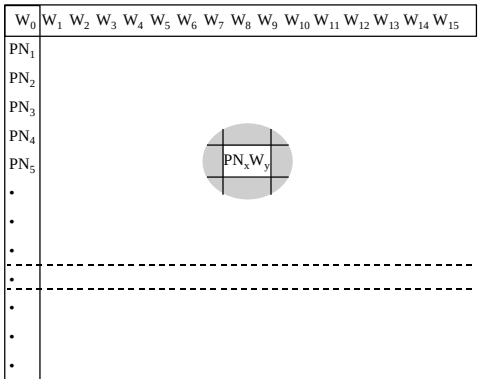
DUWL/M10 TRANSEC



- Security Code Channel (SCC) Seeds LFSR
- Initial Acquisition Uses Non-Changing Code
- Data "Frame Sync" Provides Time Alignment
- PN Code Sequence Does Not Reveal LFSR States
- PN Codes Selected for Best Multipath Performance

PN Code Selection

- 16 bits: 32K Codes
  (plus compliments)
- Functions W_0-W_{15}
  - Proper Subgroup
  - Coset Decomposition
  - PN Code Coset Leaders
  - 2048 Cosets
- Pick Cosets Having Low Near-In Crosscorrelation Side Lobes



TRANSEC Summary

- Change PN Codes Symbol-to-Symbol
- Synchronize in Repeated-Code Header
- Code Channel = PN Code Sequence
- Use Only “Good” PN Codes (Multipath)
- Still Use Encryption for Select Data