Ph.D. Thesis Defense

Robust Wireless Communication for Multi-Antenna, Multi-Rate, Multi-Carrier Systems

Triet Dang Vo-Huu

College of Computer and Information Science
Northeastern University

Committee members

Guevara Noubir	Advisor, Northeastern University
Erik-Oliver Blass	Airbus Group Innovations / Northeastern University
Rajmohan Rajaraman	Northeastern University
Srdjan Capkun	Ext. member, ETH Zurich
David Starobinski	Ext. member, Boston University

June 9, 2015

Pervasiveness of Wireless Systems

- Beyond providing user information and data services:
  - Air-traffic control
  - Power grids
  - Transportation systems
  - Human body implantable devices
- Trend: Radio devices migrating from hardware to software

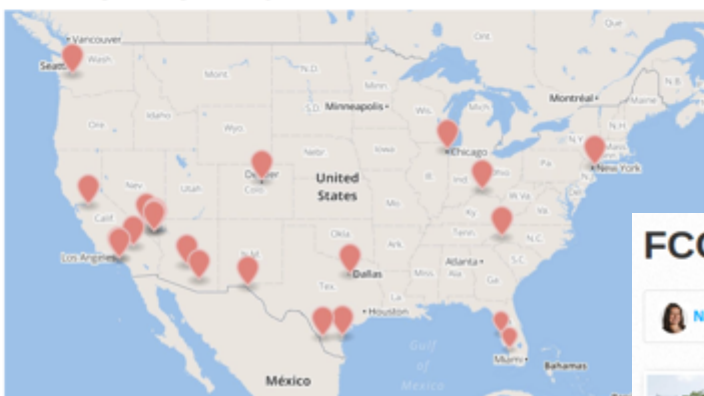
Jamming Threats

GPS Jammer

CDMA/GSM/3G/
WiFi Jammer

Software-defined radio

Who is putting up 'interceptor' cell towers? The mystery deepens



Above: ESD America's map of the interceptors discovered so far
Image Credit: ESD America

September 2, 2014 2:58 PM
Barry Levine

2.1k 11.6k 438 716 189 884

Mysterious "interceptor" cell towers in the USA are
phone calls — but they're not part of the phone ne
And, two experts told VentureBeat today, the towe
appear to be projects of the National Security Ager

Magnetron

FCC fines Marriott $600,000 for Wi-Fi blocking

Nancy Trejos, USA TODAY 2:39 p.m. EDT October 3, 2014

(Photo: Mark Humphrey, AP)

216 CONNECT | 58 TWEET | 9 LINKEDIN | 17 COMMENT | EMAIL | MORE

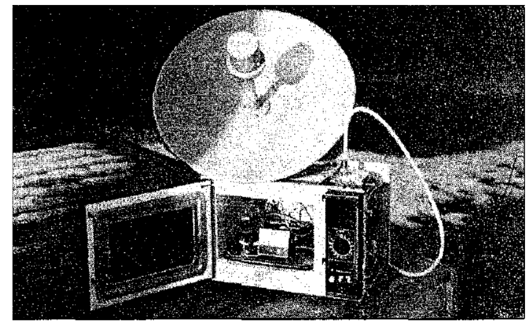
Marriott International will pay $600,000 to resolve a Federal Communications Commission investigation into whether a hotel's employees blocked customers from using their personal Wi-Fi networks and then charged them to use the hotel network.

Focus

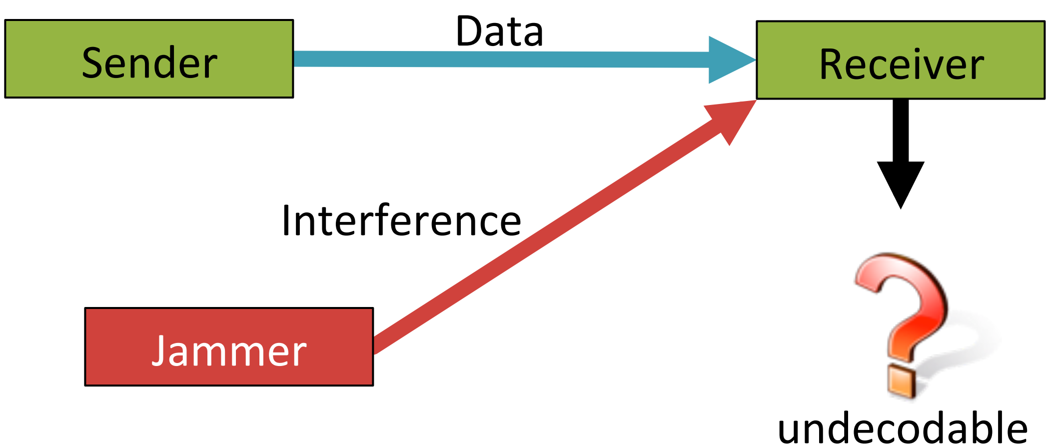
- High-Power Jamming
- Crippling Jamming
- Multi-Carrier Jamming

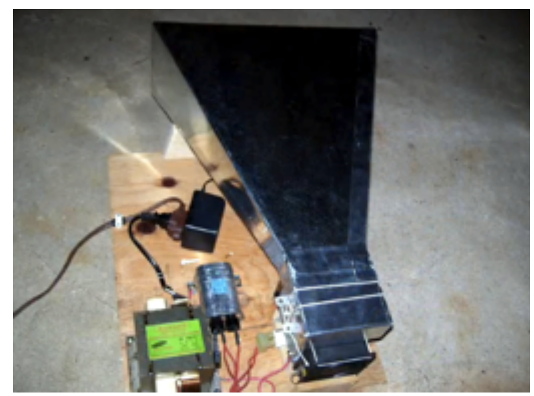
High-Power Jamming

- Powerful interference
- High coverage (hundreds of meters)
- Strong (1KW >> WiFi signal ≈ max. 20mW)
- Low cost



[Pacholok89]

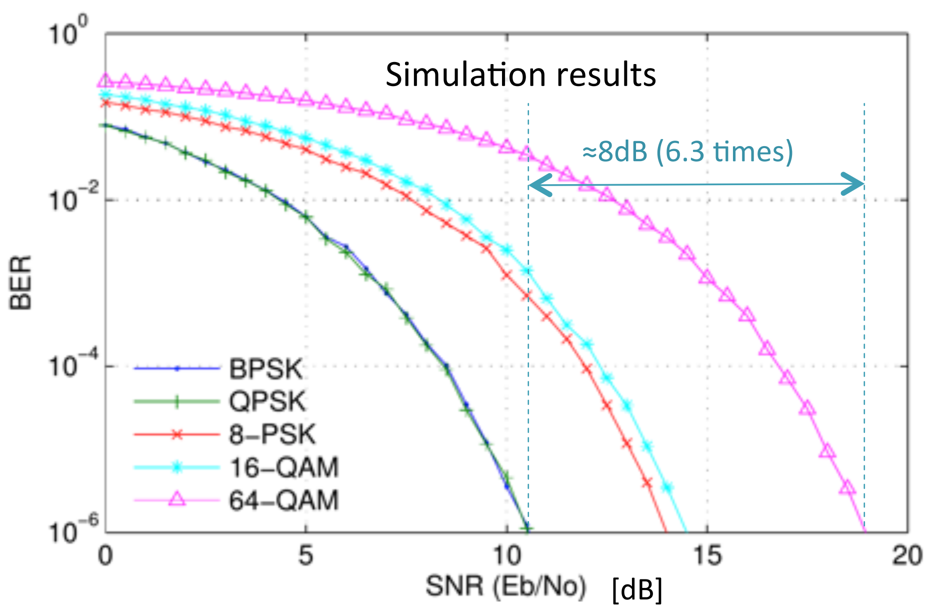


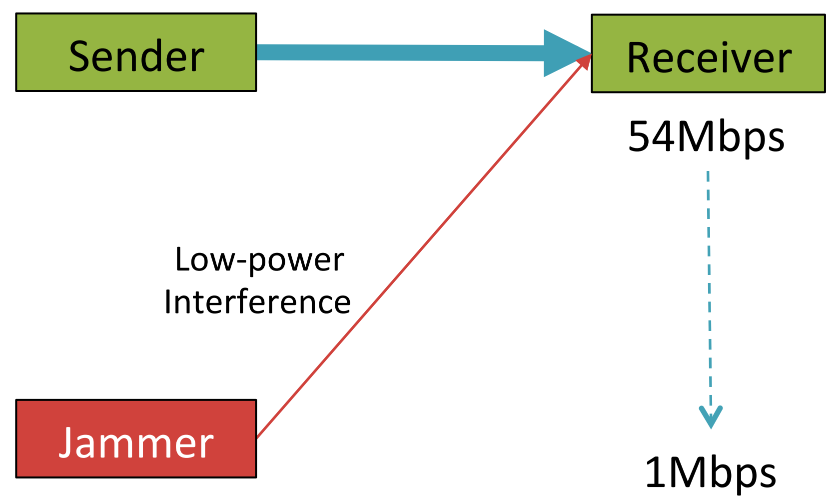


[hacknmod.com]

Crippling Jamming

- Degrade system performance with low jamming power
- Hard to be detected
- Attack on link rate adaptation:
  - Higher bit rate, higher probability of error → higher jamming efficiency
  - Low-rate transmission link → network congestion
  - Attack [NRST'11] causes rate adaptation algorithms to use basic rate (1Mbps)
  - Theoretical analysis [OS'12] shows an effective jamming rate as low as 5%





Jamming in Multi-Carrier Communication Systems

- Multi-carrier communication systems are popular today

- Previous work: Jamming on
  - Preamble (frequency offset attacks)
  - Pilot subcarriers
  - Control channels (LTE, GSM)

- Our study: Jamming on Wi-Fi communications

Agenda

1. Counter High-power Jamming

2. Conceal Rate Information and Boost Resiliency

3. SDR for High-Rate Wi-Fi Analysis

4. Multi-Carrier Jamming on Wi-Fi Communications

5. Conclusion

Agenda

1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. SDR for High-Rate Wi-Fi Analysis
4. Multi-Carrier Jamming on Wi-Fi Communications
5. Conclusion

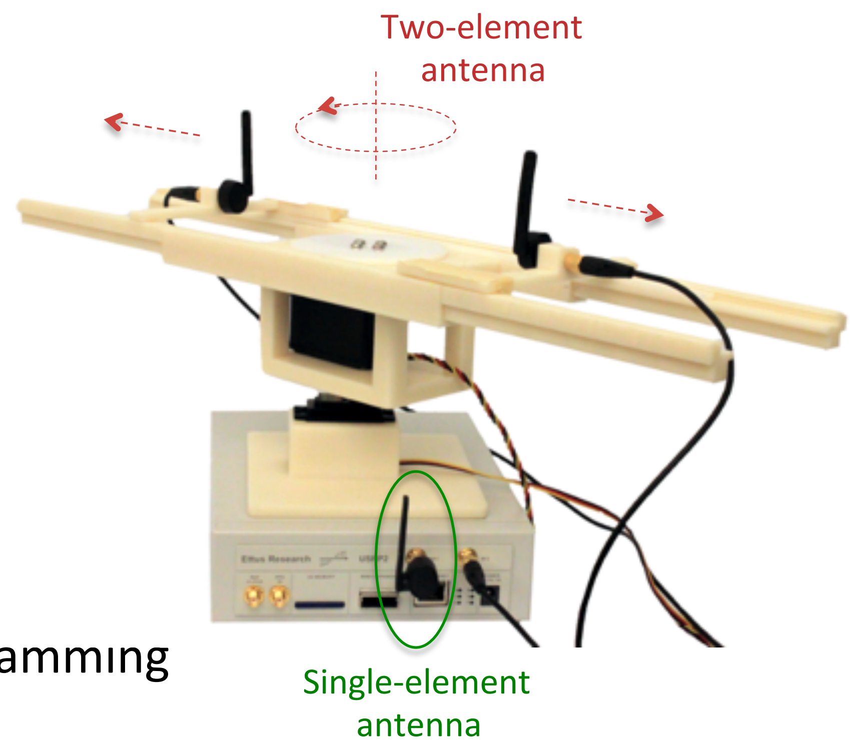
Previous Work

- Directional antennas, phase array antennas: high cost, more appropriate for radar systems
- Uncoordinated spread spectrum [PSC'10]: lower transmission rate
- MIMO: require training sequences (cooperative)
- Full-duplex wireless communications, Ally friendly jamming are designed for extracting known signal rather than unknown jammers

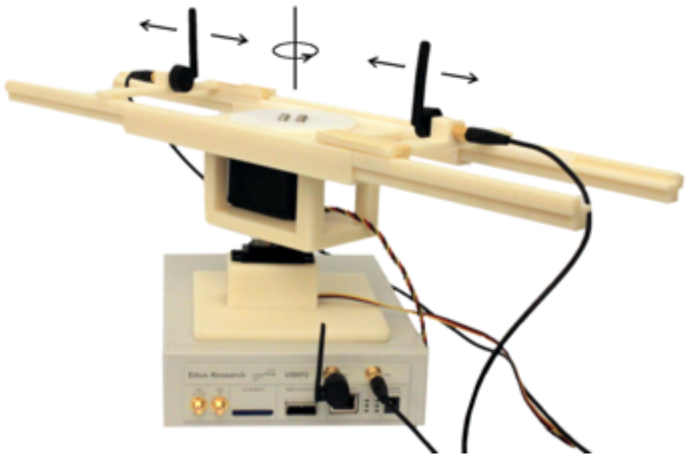

PAVE PAWS

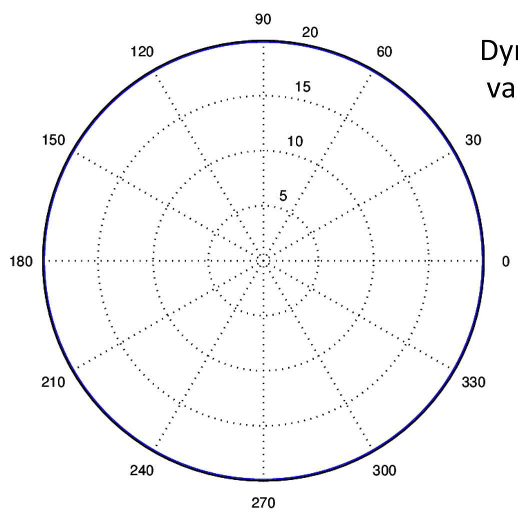
Our Approach

- **Steerable** and **separable two-element** receive antenna (28dB)
  - Increase user signal's power
  - Decrease jamming signal's power
  - Antenna auto-control
  - Location awareness not required
- **Digital Jamming Cancellation** (20dB)
  - Additional single-element antenna
  - Requires no training sequences
  - Removes unknown and powerful jamming
- Two stages: 48dB

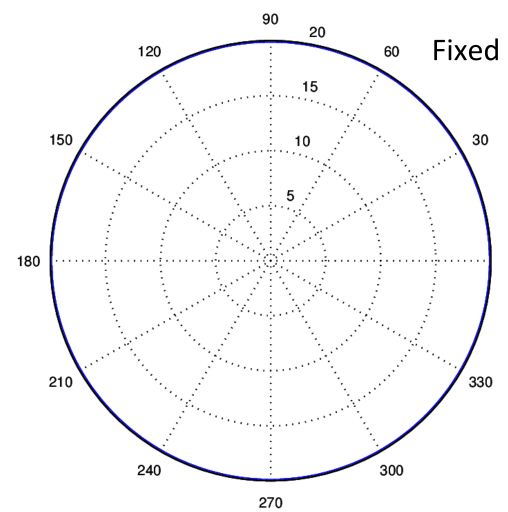


Receive Pattern





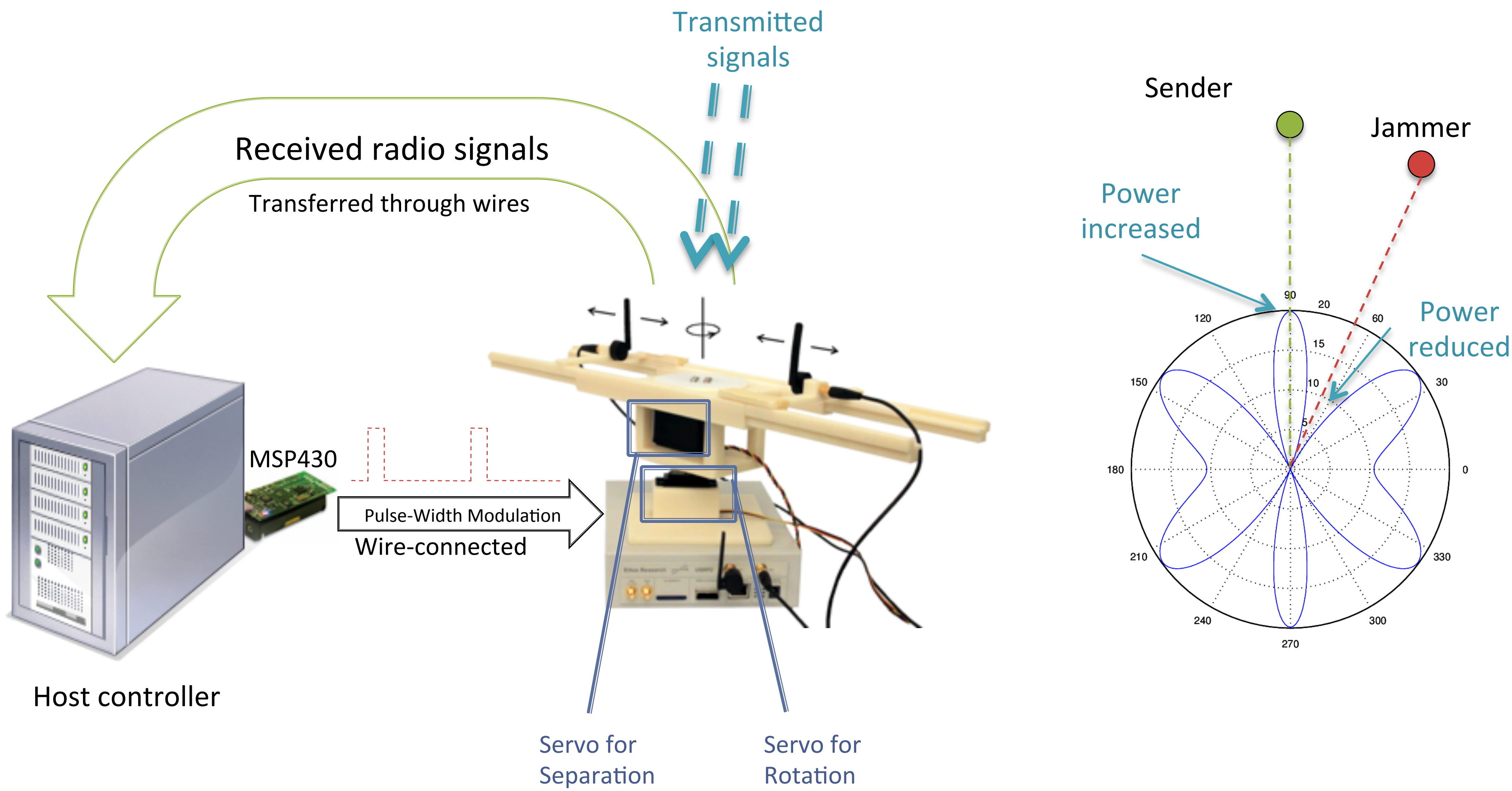
Dynamic pattern by varying separation



Fixed pattern

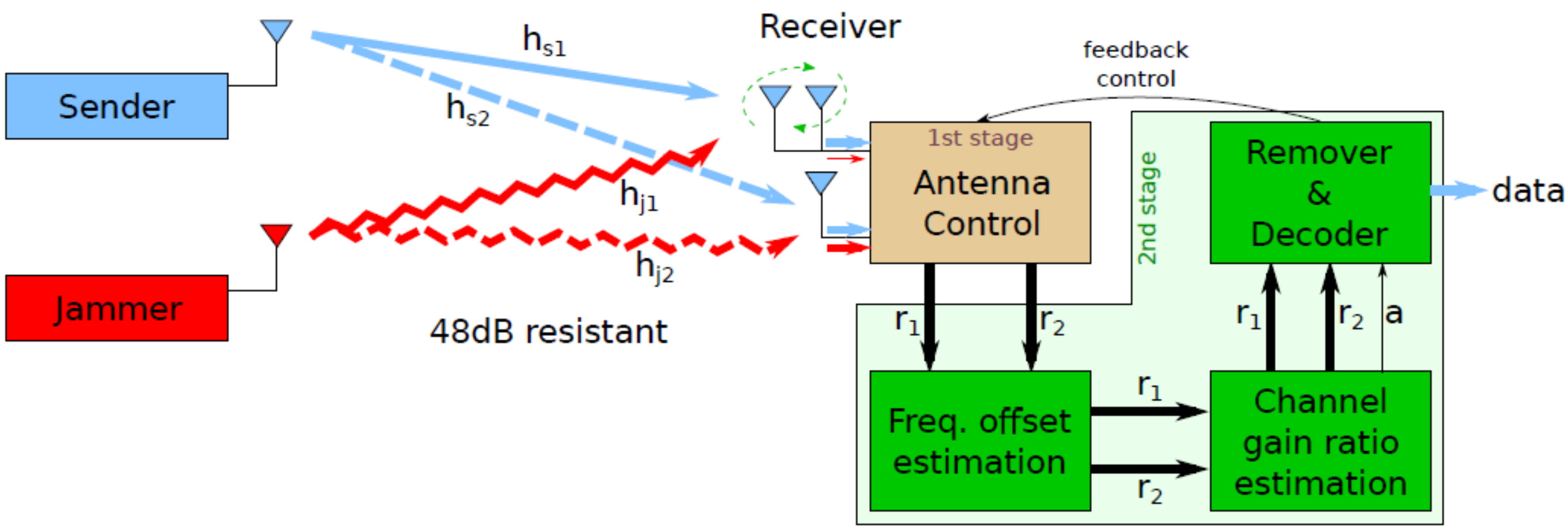
Number of lobes (or nulls)
≈ 4 (separation / wavelength)

Antenna Control Diagram

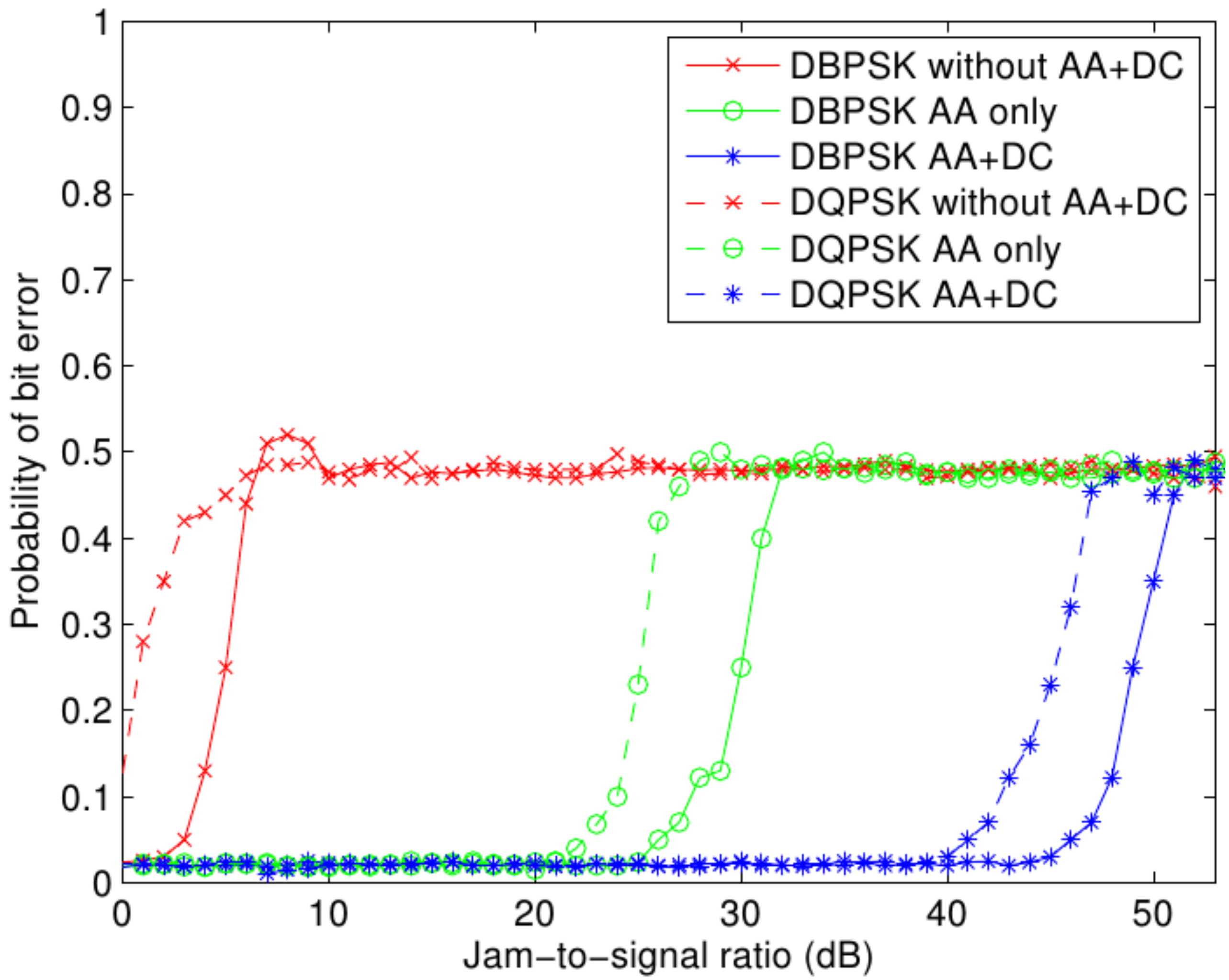


Digital Jamming Cancellation

- Goal: increase anti-jamming capability beyond 28dB
- Approach:
  - Use an additional single-element antenna
  - Extract original data signal from 2 received signals



Anti-jamming Performance: DBPSK and DQPSK



AA: Antenna Auto-configuration
DC: Digital Cancellation

Agenda

1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. SDR for High-Rate Wi-Fi Analysis
4. Multi-Carrier Jamming on Wi-Fi Communications
5. Conclusion

Rate Attacks

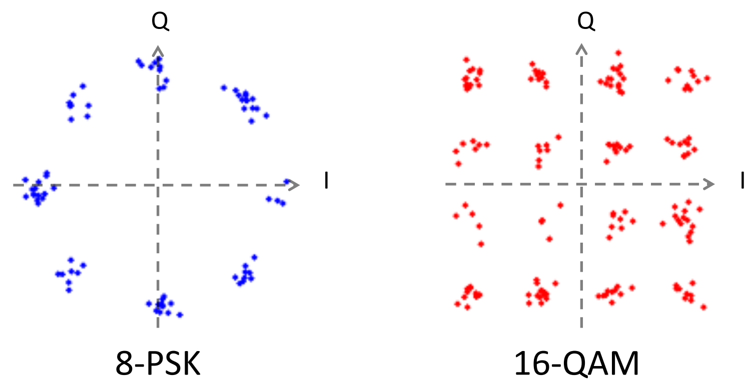
- Jamming attack on rate adaptation:
  - Target to high-rate packets
  - Low-rate transmission links block other communications
  - Degrade whole system's performance

- Reason: Adversary knows the rate information

→ needs to hide the rate

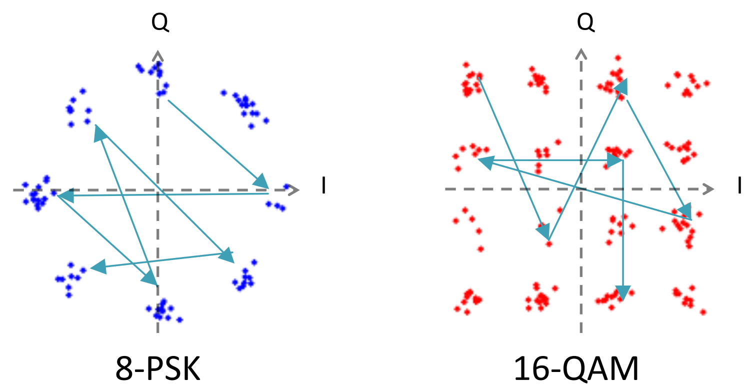
Rate Detection

- Explicit:
  - Rate exposed in protocol's public header (Wi-Fi, LTE, …)
- Implicit:
  - Modulation guessing: by analysis of received complex samples (in-phase and quadrature components)



Modulation guessing

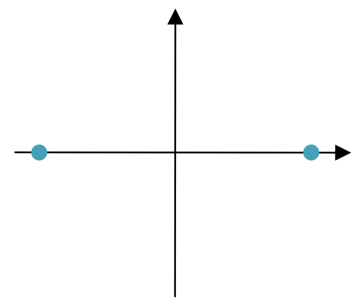
  - Code guessing: by analysis of received complex samples and tracking maximum likelihood symbol sequences



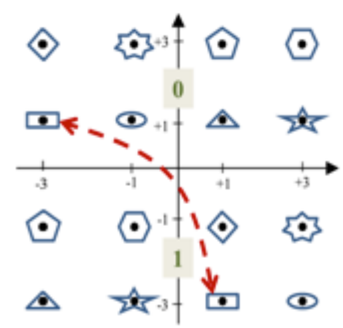
Code guessing
(code transitions can be traced)

Challenges of Rate Hiding

- Encrypting Header:
  - No explicit rate exposing
  - Suffer from implicit rate detection
- Use only one rate:
  - No rate information lost
  - Loss of efficiency (always lowest rate)
- Modulation Unification [RK'14]:
  - Conceal modulation
  - Sacrifice of resiliency due to shorter symbol distance
- Applying Binary Error Correction Codes:
  - Good for BPSK and QPSK
  - Robustness not guaranteed for higher-order modulations
  - No protection against code guessing



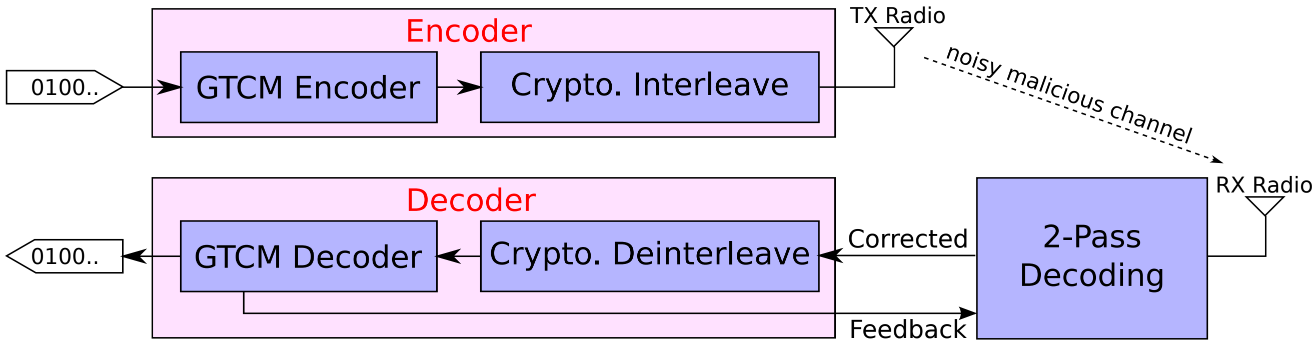
Original Modulation



Modulation Unification

Goal and Approach

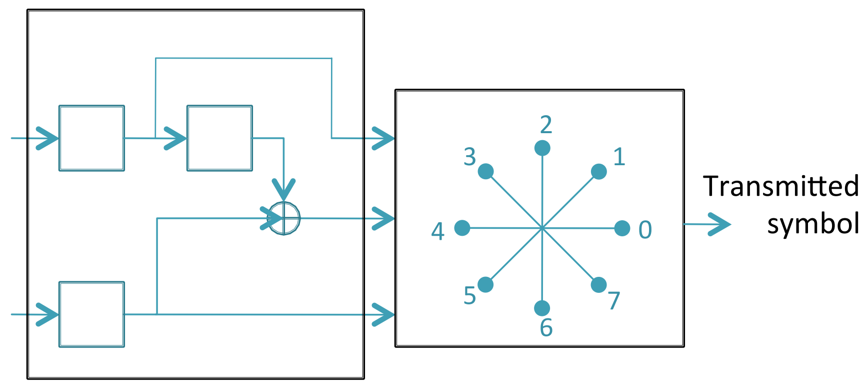
- Goal:
  - Prevent explicit exposing rate, modulation guessing, and code guessing attacks
  - Boost resiliency at the same time with rate concealing
- Approach: We develop:

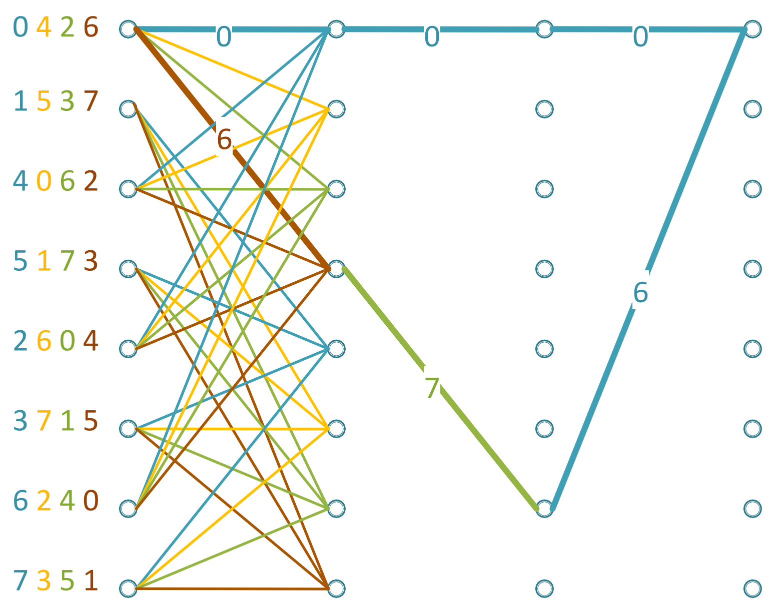


  - Generalized Trellis Coded Modulation:
    - Counter modulation guessing: use highest-order modulation
    - Boost resiliency: Generalize TCM codes
  - Cryptographic Interleaving:
    - Rate is not explicitly exposed
    - Counter code guessing
  - Two-Pass Decoding: soft pre-decoding re-encoding for improved phase correction

Trellis Coded Modulation

- TCM is a convolutional code of rate k/(k +1) designed specifically to higher-order modulation
- Maximize Euclidean distance between coded symbol sequences
  - Binary codes are designed to maximize Hamming distance
- Coding gain depends on minimum distance between sequences of coded symbols
  - Uncoded modulation: minimum distance between individual symbols
- Heuristic code search: Set partitioning and design rules → regular/uniform mapping





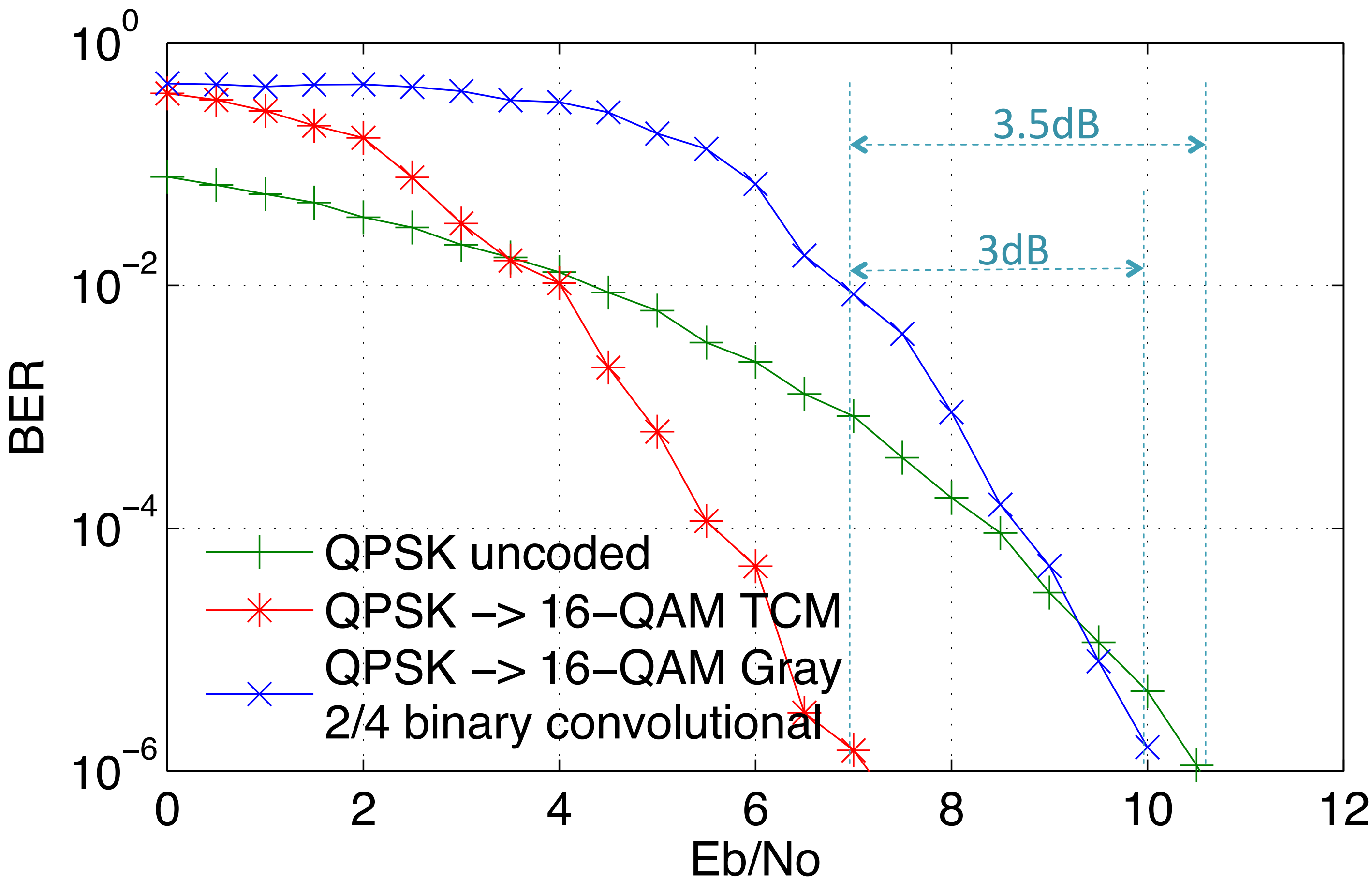
Generalized TCM Codes

- General rate k/n
  → conceal any modulation into any higher-order modulation

- Relax uniformity
  → larger class of codes. We found some better codes

- Heuristic: but not based on set partitioning and design rules
  1. Generate a random code mapping
  2. Check validity of generated code
  3. Check coding gain: Compute free distance of code
     - Involves distances between every pair of paths that diverge and remerge
     - Running time: < 2ms per code

GTCM vs. Binary codes

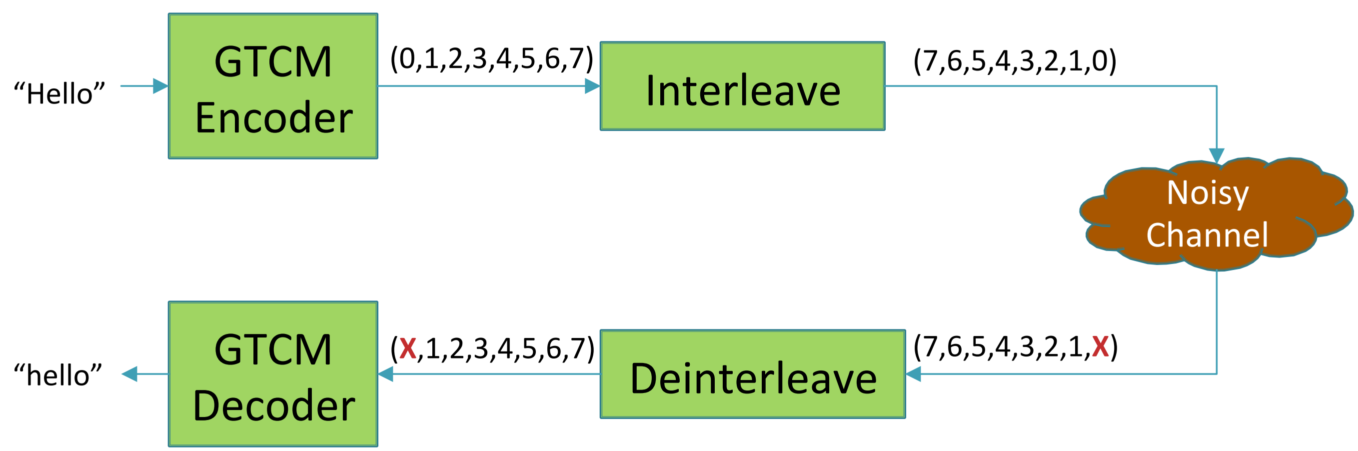


Applying binary codes can result in less resiliency than uncoded modulation

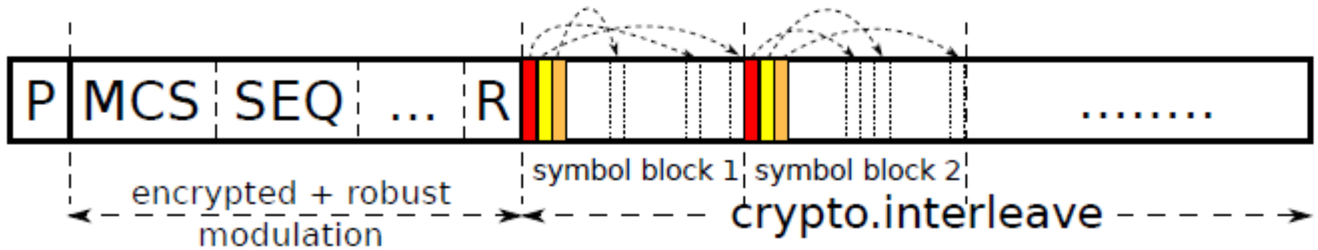
Cryptographic Interleaving

- Why Cryptographic Interleaving?
  - GTCM does not conceal codes
  - Encryption baseband symbols amplifies errors exceeding decoding capability

- Our approach: Cryptographic Interleaving



Interleaving Process



- Indistinguishable interleaving function:

  y = Ax + B mod m
  A = h(K|s|i|0) mod (m-1) + 1
  B = h(K|s|i|1) mod m

  x: index of symbol before interleaving
  y: index of symbol after interleaving
  m: block size, i: block index
  s: packet sequence number
  K: shared secret

  - Requires 2 hash operations per block
- Concealing Header:
  - Encoded with fixed robust coding scheme
  - Encrypted using AES-CBC: AES-CBC$_K$(MCS|SEQ|…|R)

System Impairments in Low SNR

- Performance drop with practical implementation and evaluation

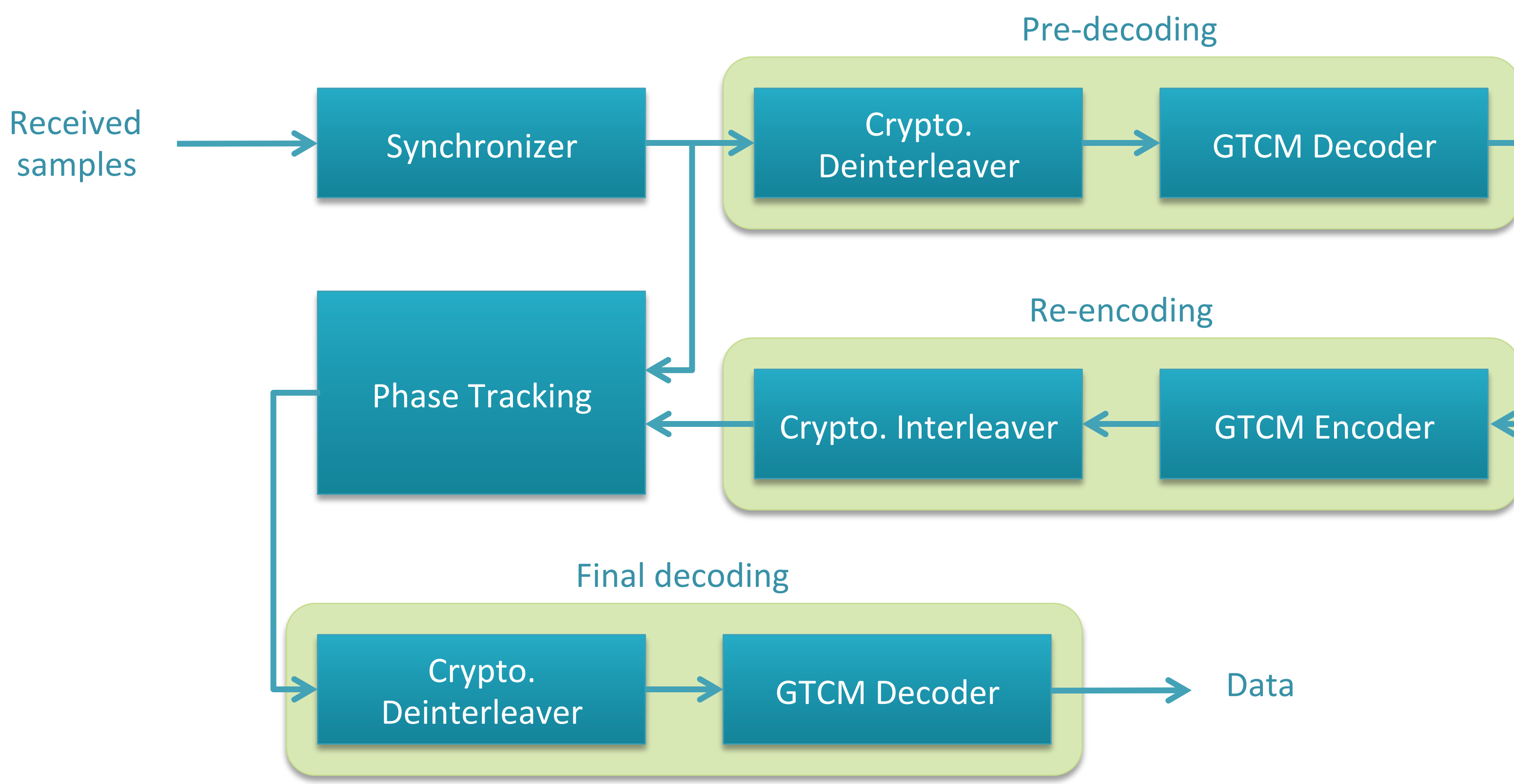
- Reason: regular synchronization and correction techniques for frequency and phase offsets perform poorly in low SNR:

  → introduce more errors than decoder's correction capability

- This is also a reason communication systems today still use low-order modulations (eg. BPSK) as a fallback mode to adapt to the environment

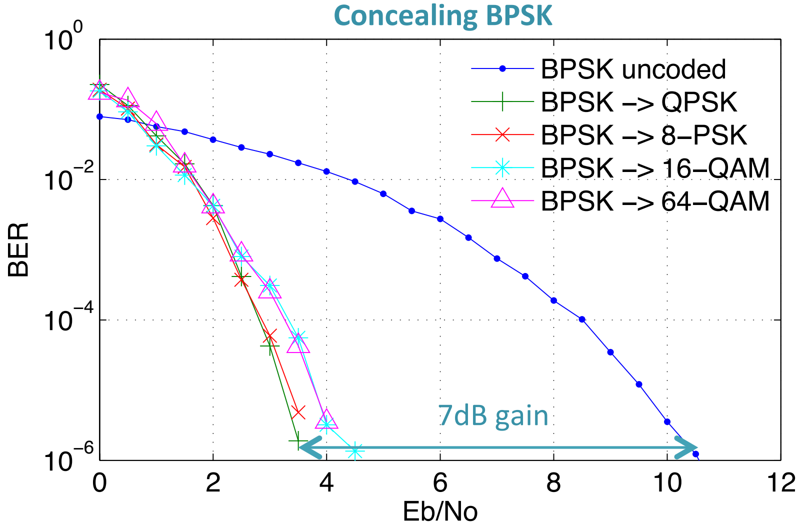
2-Pass Decoding

- Soft pre-decoding re-encoding
- Phase tracking: correction based on re-encoded symbols (skip wrong symbols)

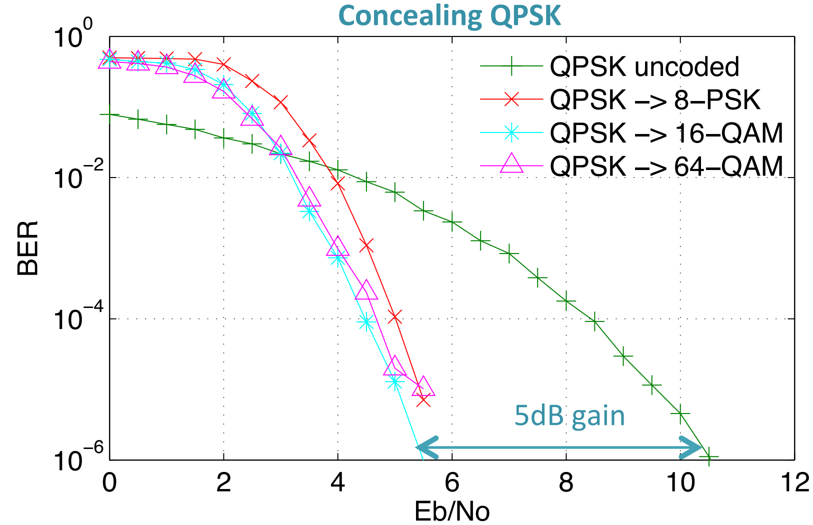


Simulation Results

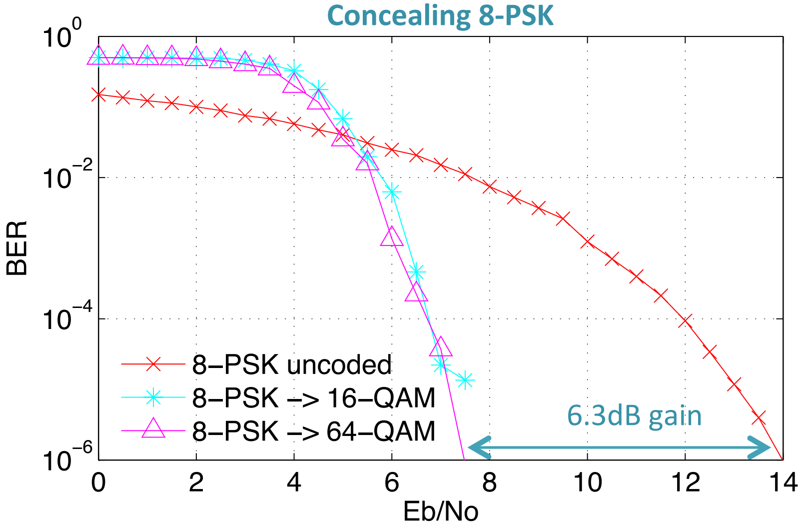
Concealing BPSK



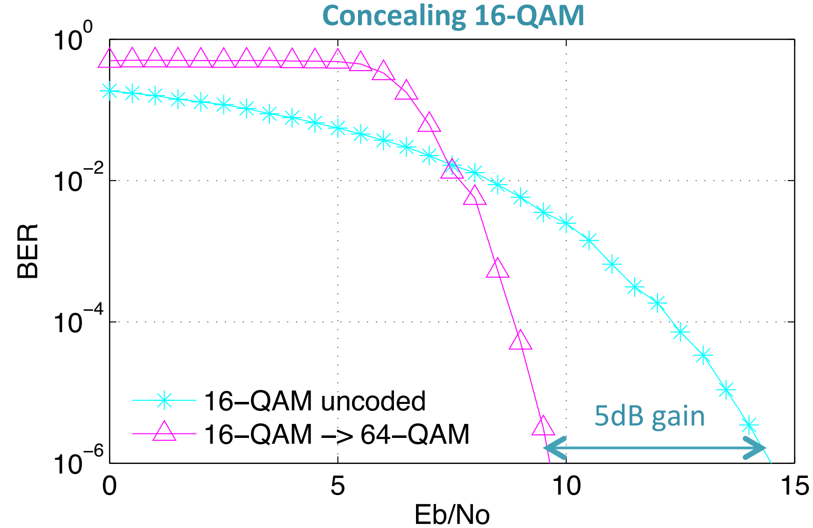
Concealing QPSK



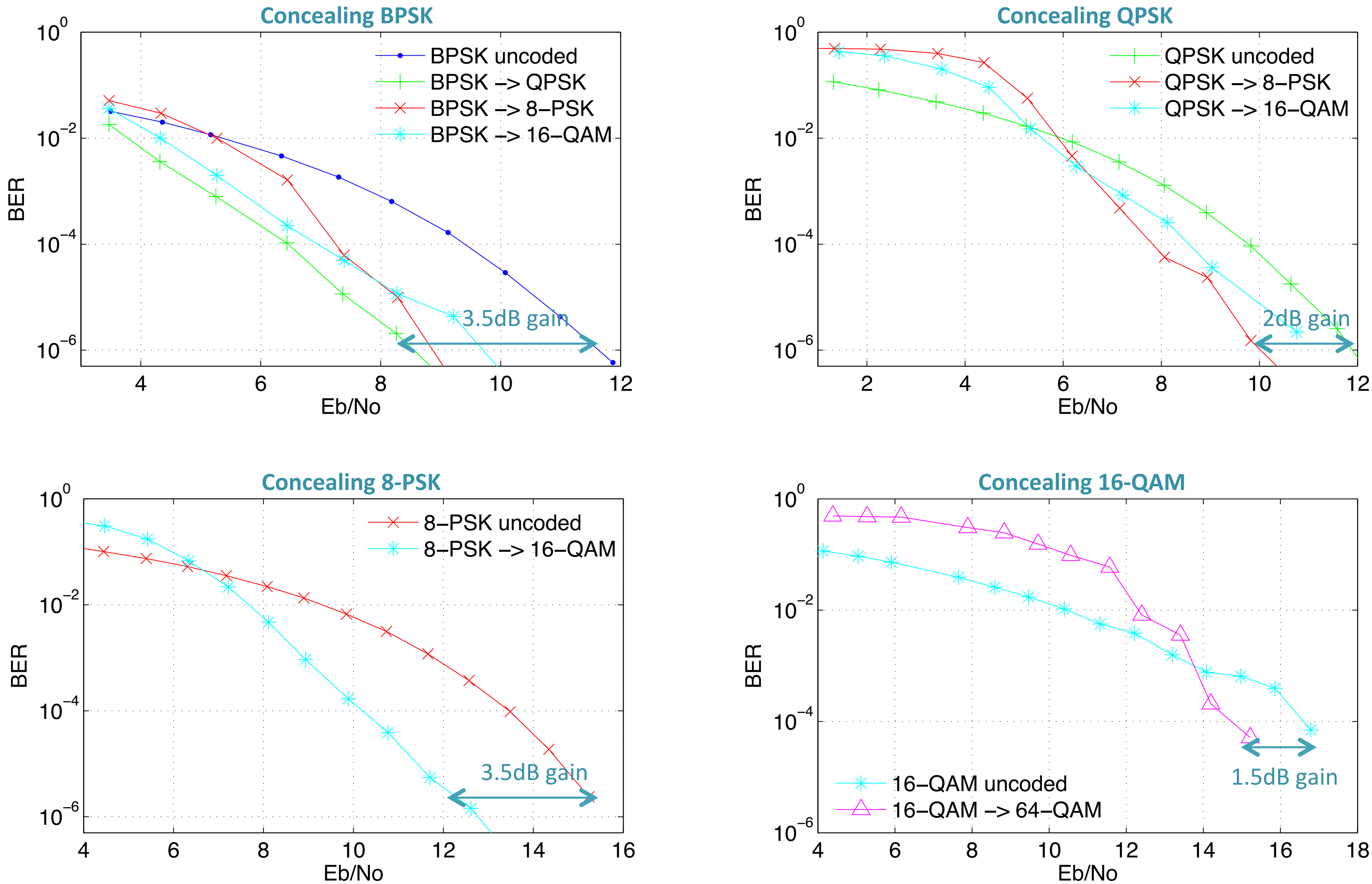
Concealing 8-PSK



Concealing 16-QAM



Experimental Results



Agenda

1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. SDR for High-Rate Wi-Fi Analysis
4. Multi-Carrier Jamming on Wi-Fi Communications
5. Conclusion

Motivation

- GNU Radio is currently the most popular Software Defined Radio (SDR) platform, but:
    - Still lacks good Wi-Fi implementation
    - Some previous efforts (gr-ieee802-11) do not support full rate (only PSK modulations)

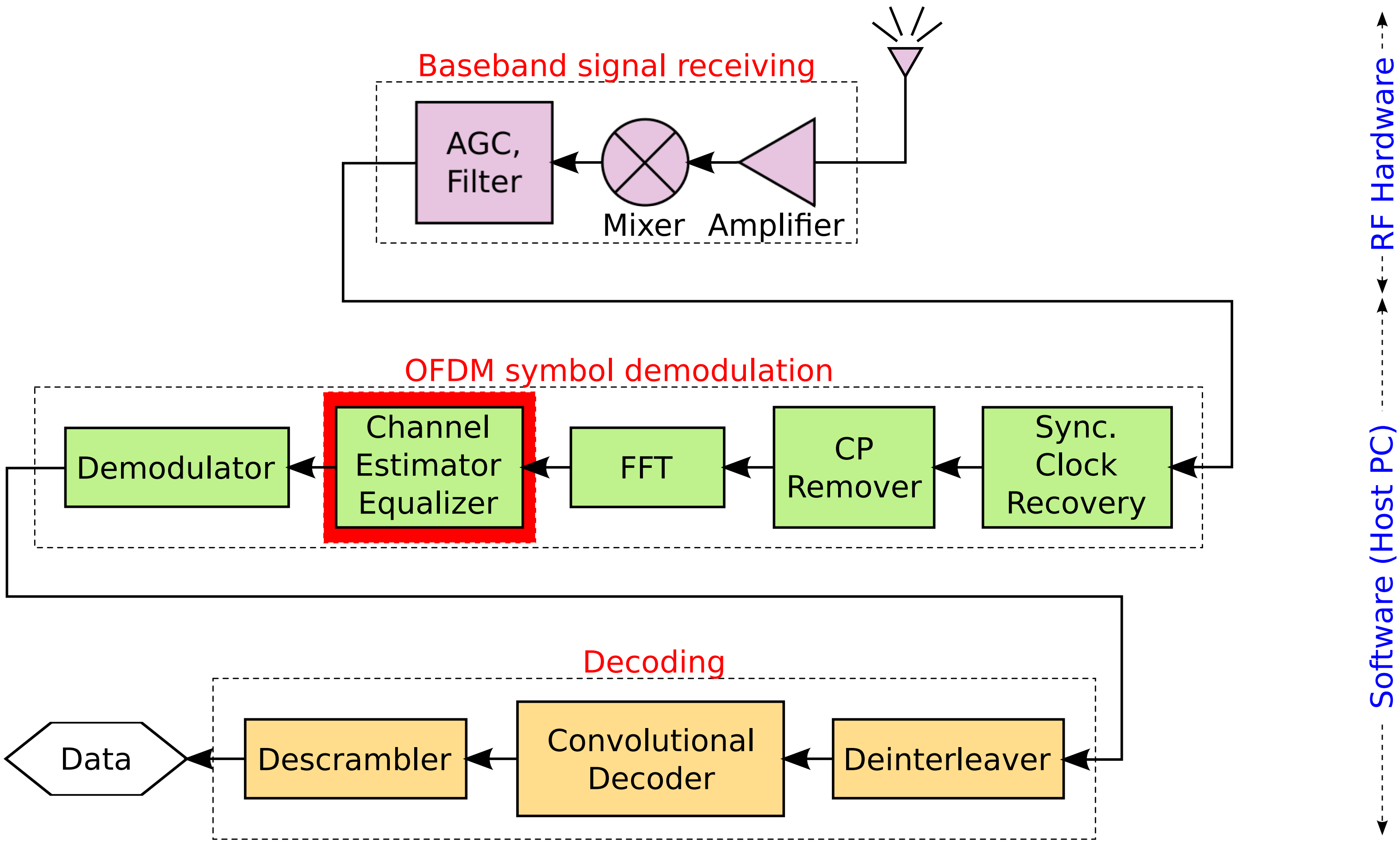
- Other existing platforms (WARP, Sora):
    - More expensive (WARP: $4,900+, Sora: $3000+)
    - WARP: custom development is more dependent on specific hardware and architecture (constrained to the FPGA capabilities)
    - Sora: still at pre-mature stage

SWiFi - Our goal

- Develop Wi-Fi radio on GNU Radio
  - Compatible with general RF front-ends (e.g., USRP)
  - Re-use as much as possible GNU Radio supports

- Current status:
  - Broadcast transmitter and receiver with support for IEEE 802.11a/g full rates (up to 54Mbps)
  - At every point in the transmit and receive chain, allows information extraction (e.g., for fingerprinting, etc.) or injection (e.g., covert channel)
  - All signal processing functions are written in purely C++

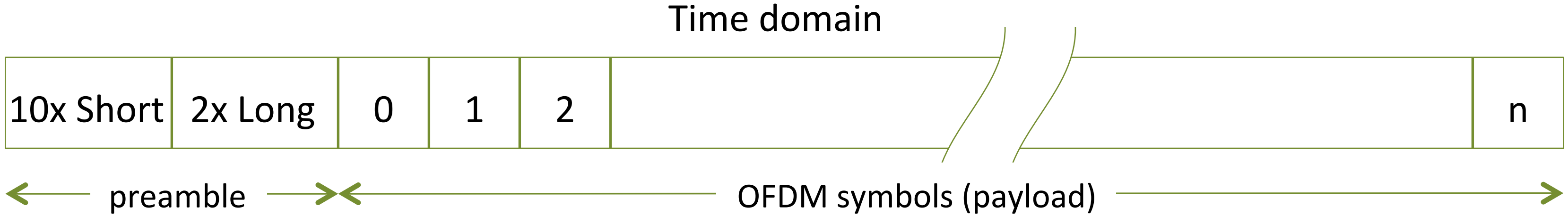
SWiFi Receiver Design



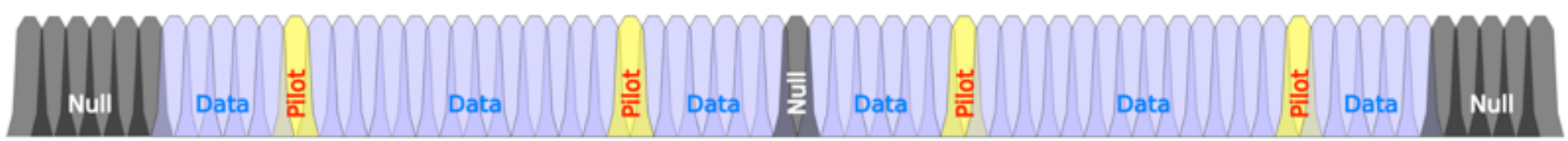
Channel Estimation and Equalization

- Preambled-based frequency offset correction
  - Coarse estimation: using short preamble symbols
  - Fine estimation: using long preamble symbols
- Initial channel estimation: using long preamble symbols
- Update channel:
  - Phase correction using pilot subcarriers
  - Decision-directed update: demodulate symbol → compute mean squared errors → remove large errors → update by averaging over previous channel states

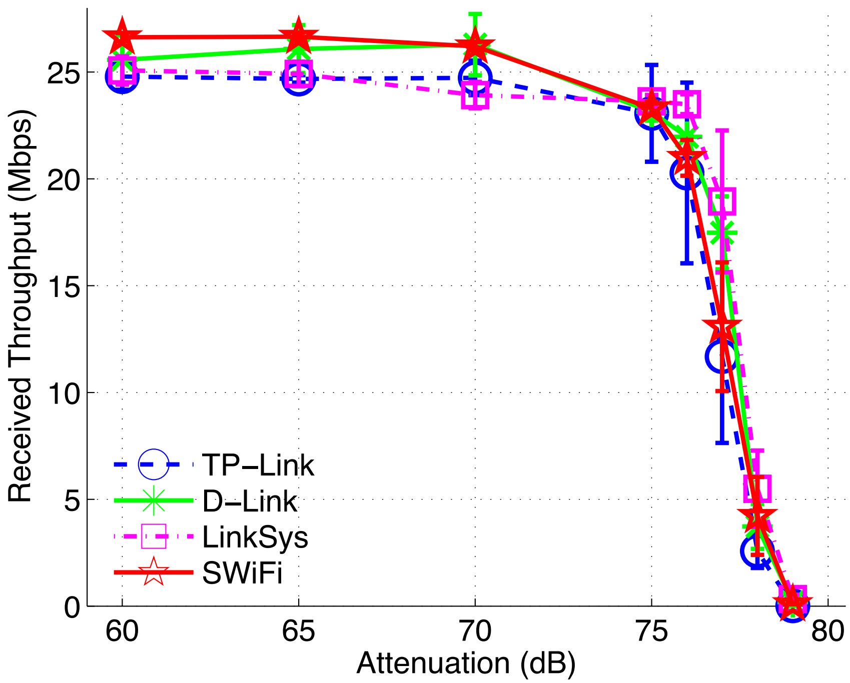
Time domain

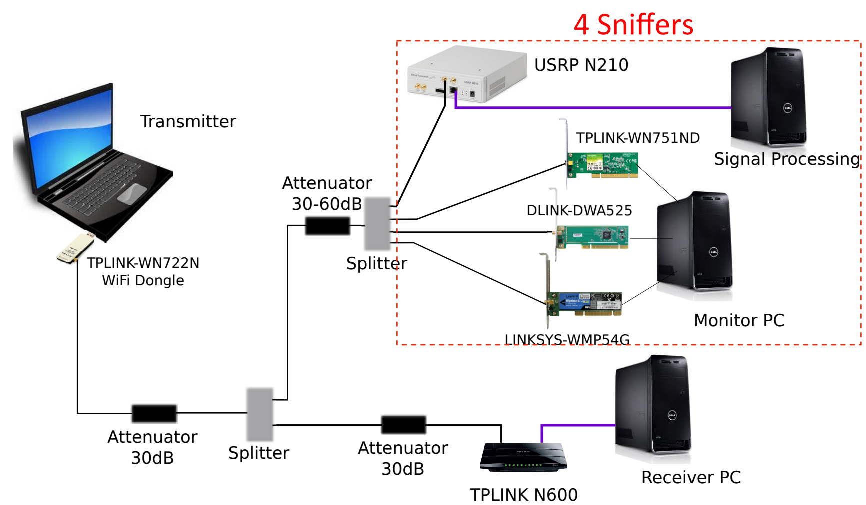


Frequency domain

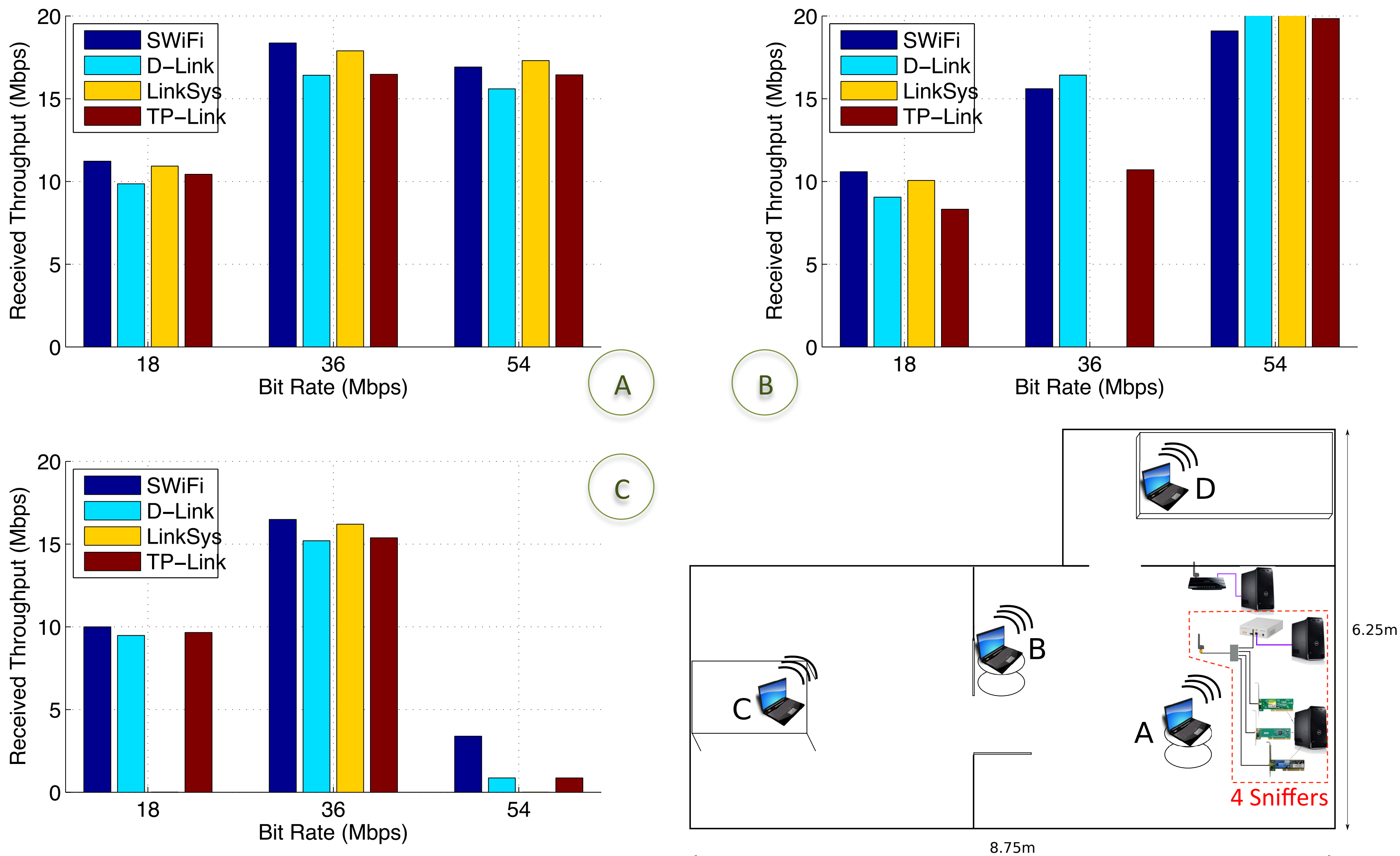


Throughput Comparison (Controlled Attenuation)





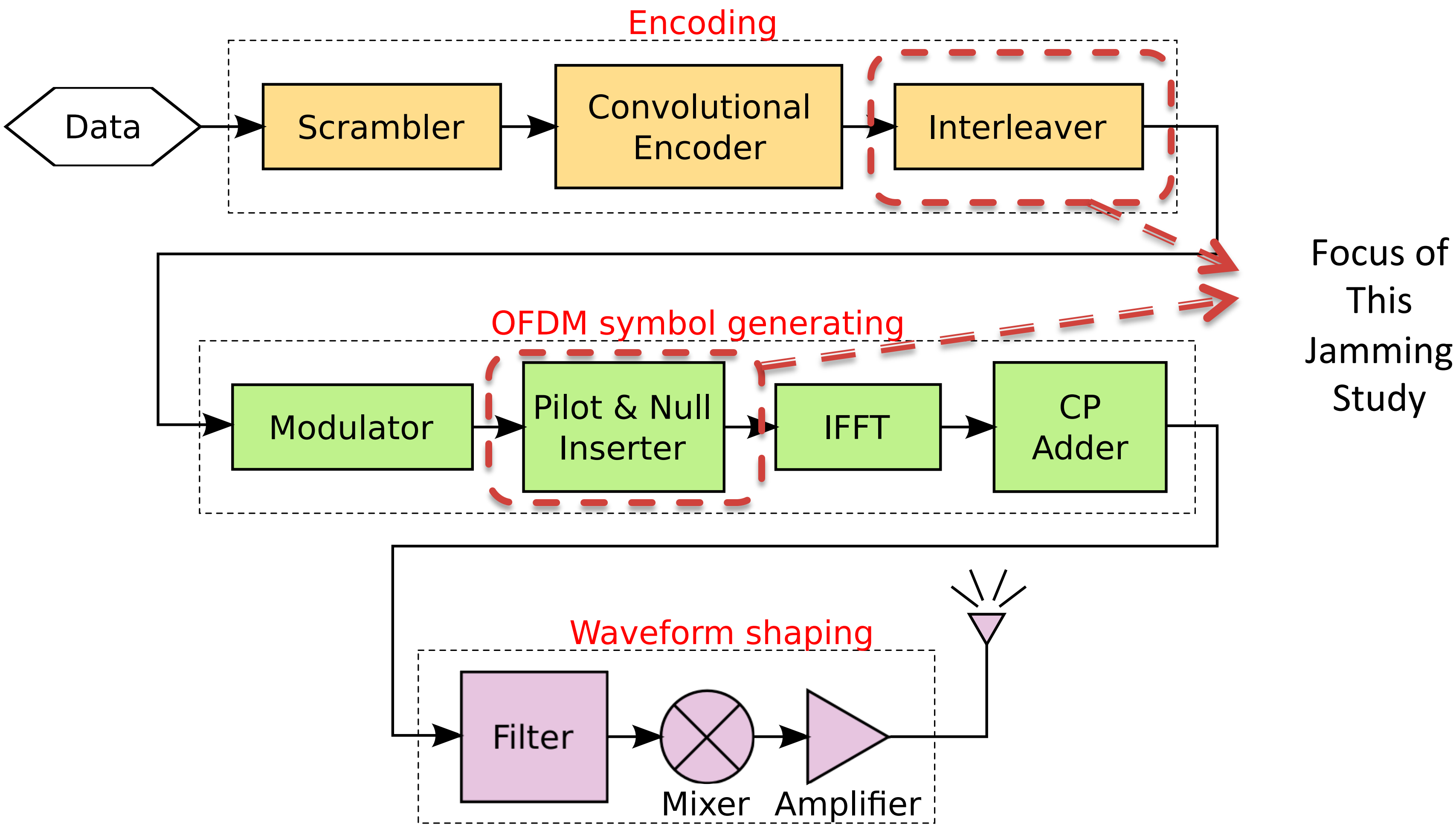
Throughput Comparison (Wireless Setup)



Agenda

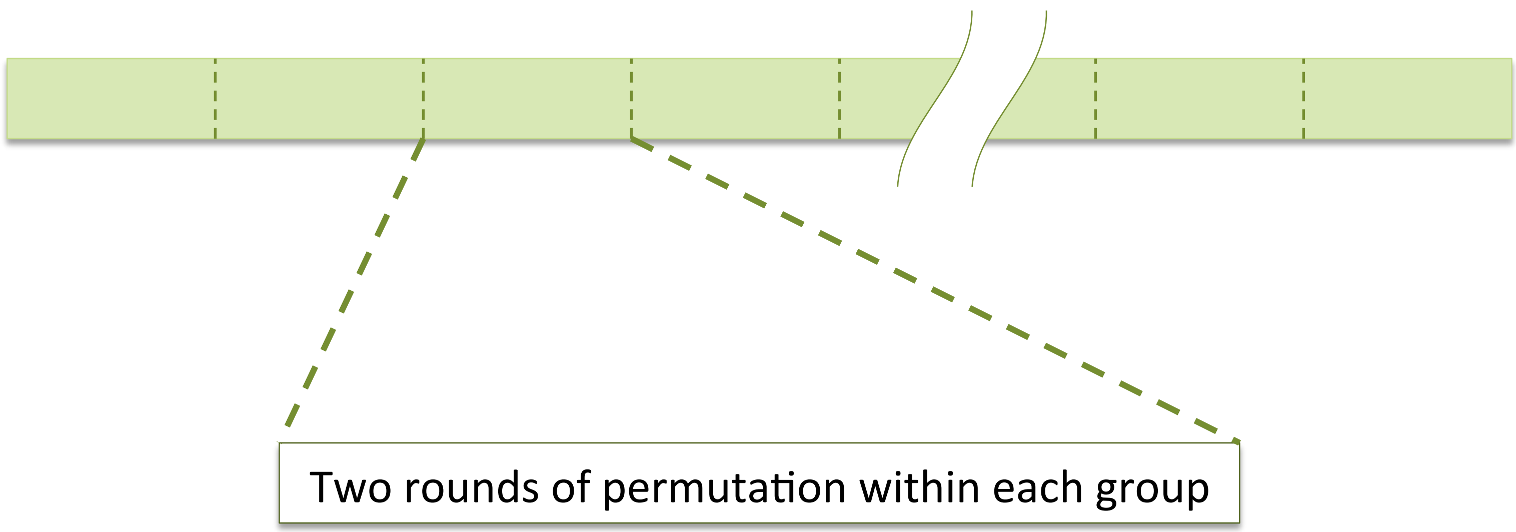
1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. SDR for High-Rate Wi-Fi Analysis
4. Multi-Carrier Jamming on Wi-Fi Communications
5. Conclusion

Wi-Fi Transmit Chain



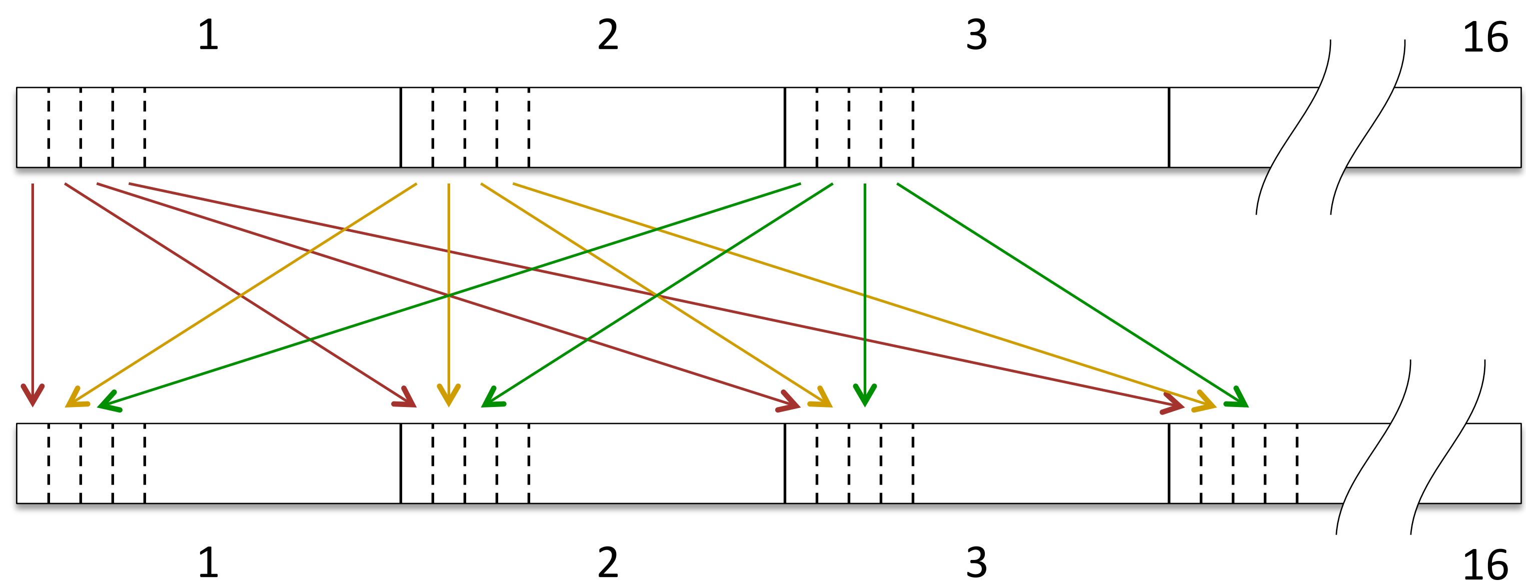
Interleaving Mechanism

- Dividing coded bit sequence (Convolutional Encoder’s output) into multiple same-size groups



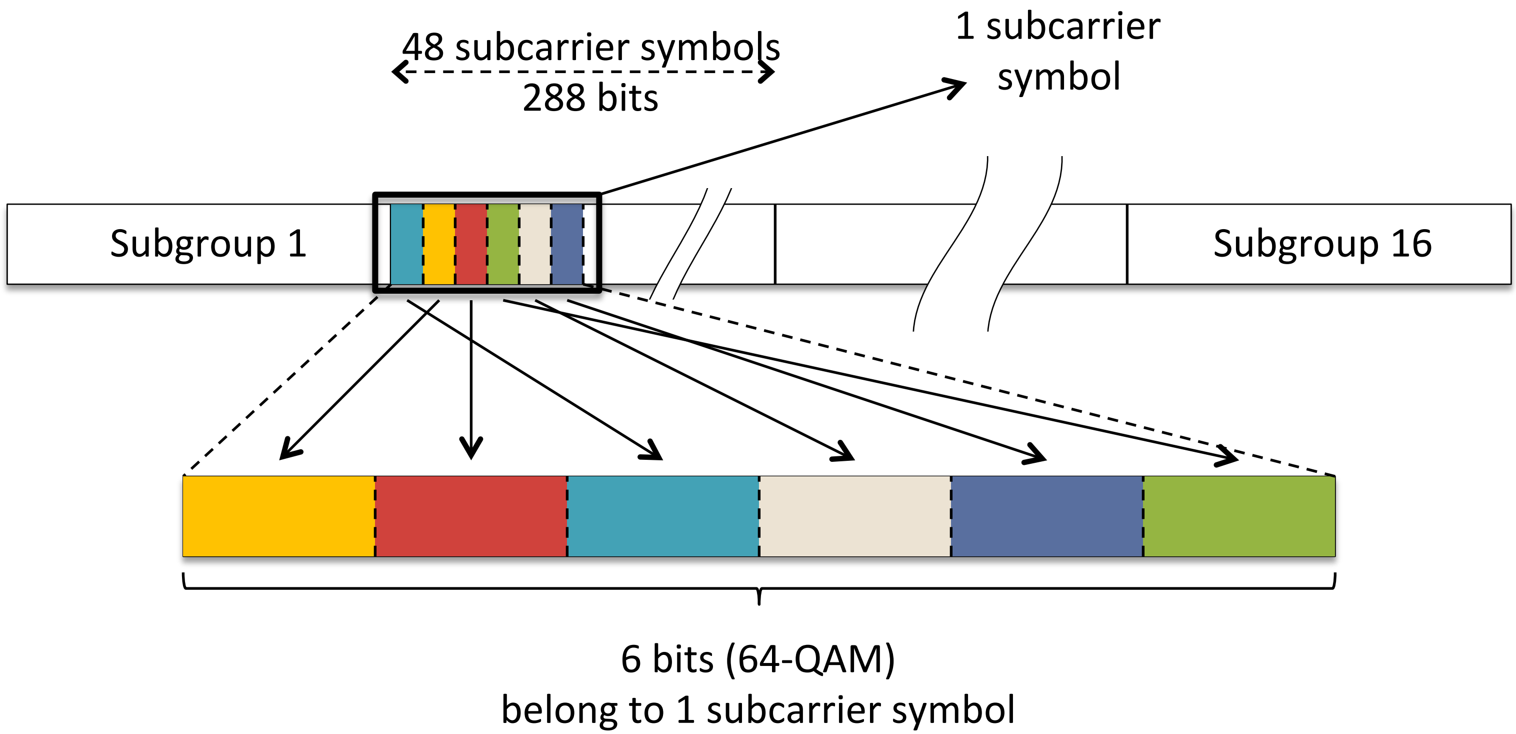
Interleaving Mechanism

- First-round permutation: scatter adjacent coded bits
  - Each group divided into 16 subgroups
  - Bit j of subgroup i moved to bit i of subgroup j



Interleaving Mechanism

- Second-round permutation: switch adjacent bits within every subcarrier symbol



Jamming Strategy

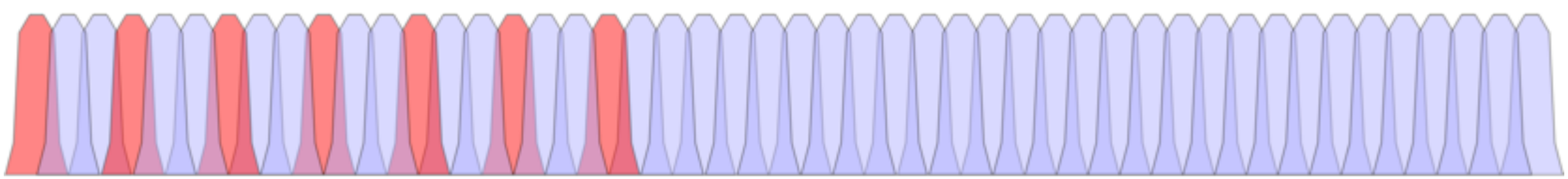
Rate-independent interleaving pattern:

- Each subgroup consists of exactly 3 subcarrier symbols
- Two adjacent bits in the same subgroup are interleaved into two adjacent subgroups

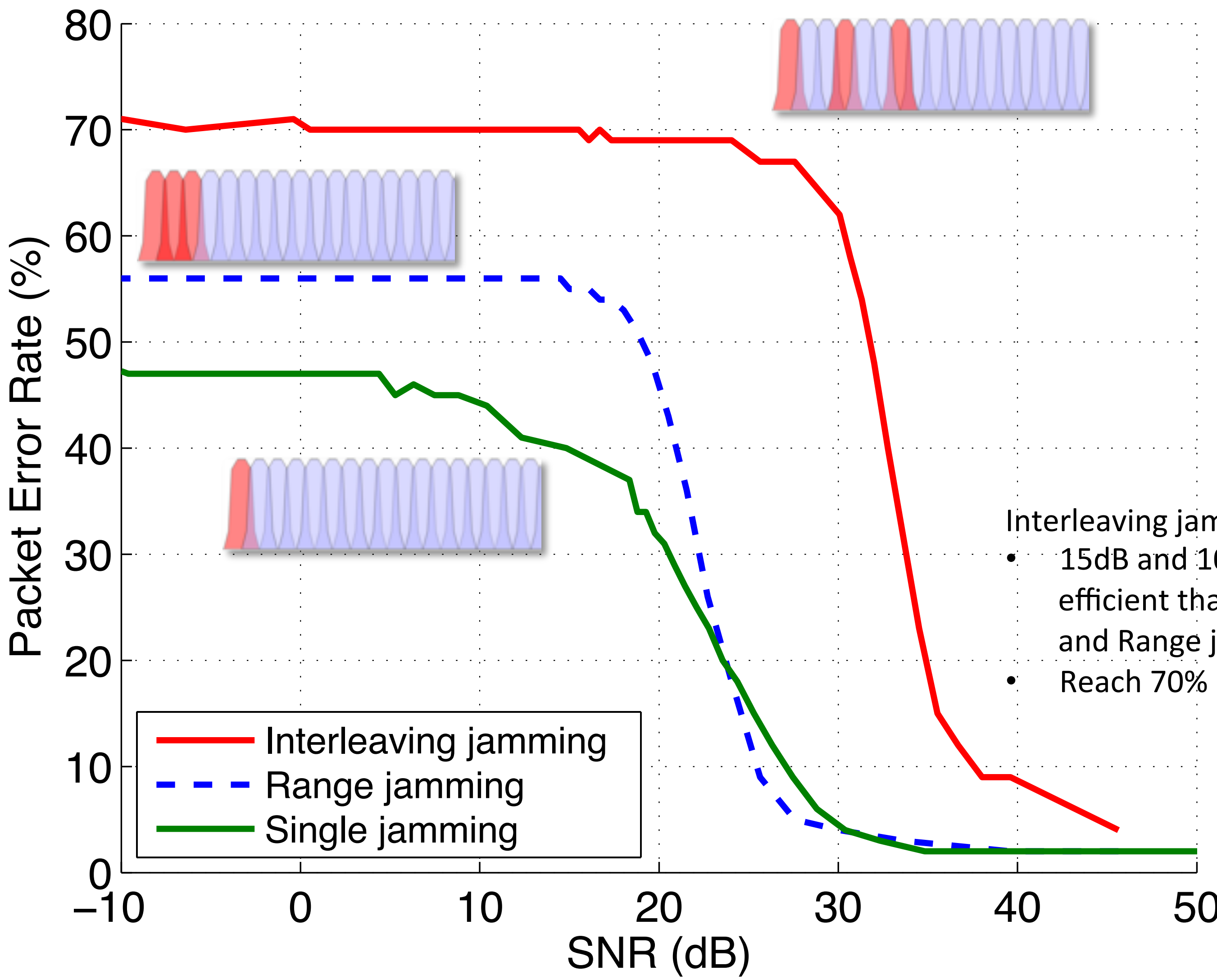
→ Two adjacent bits interleaved into subcarriers of distance 3

Interleaving Jamming

To jam n+1 subcarriers, select subcarriers i+0, i+3, i+6, …, i+3n for arbitrary i



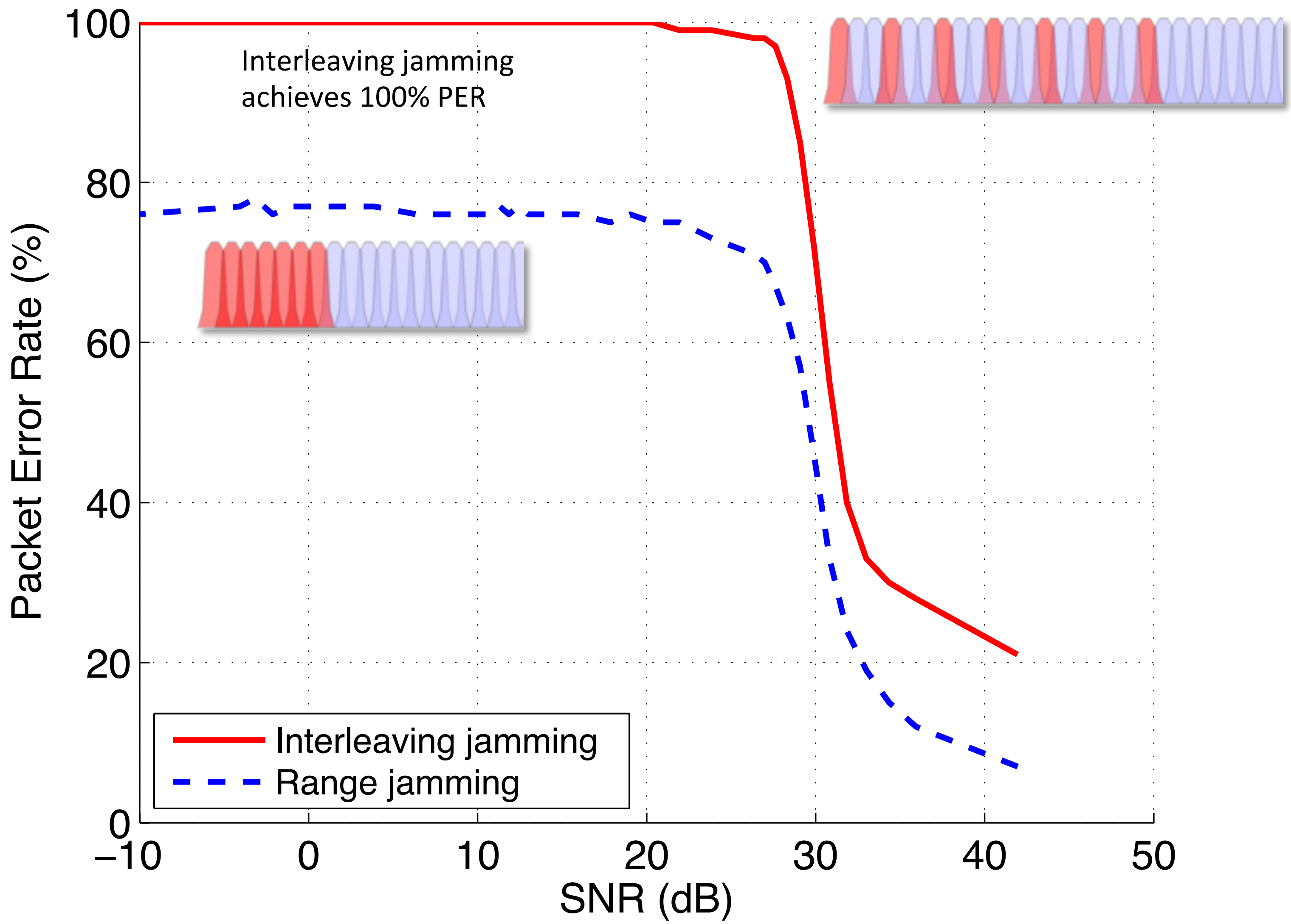
Continuous-time Narrow-band Jamming



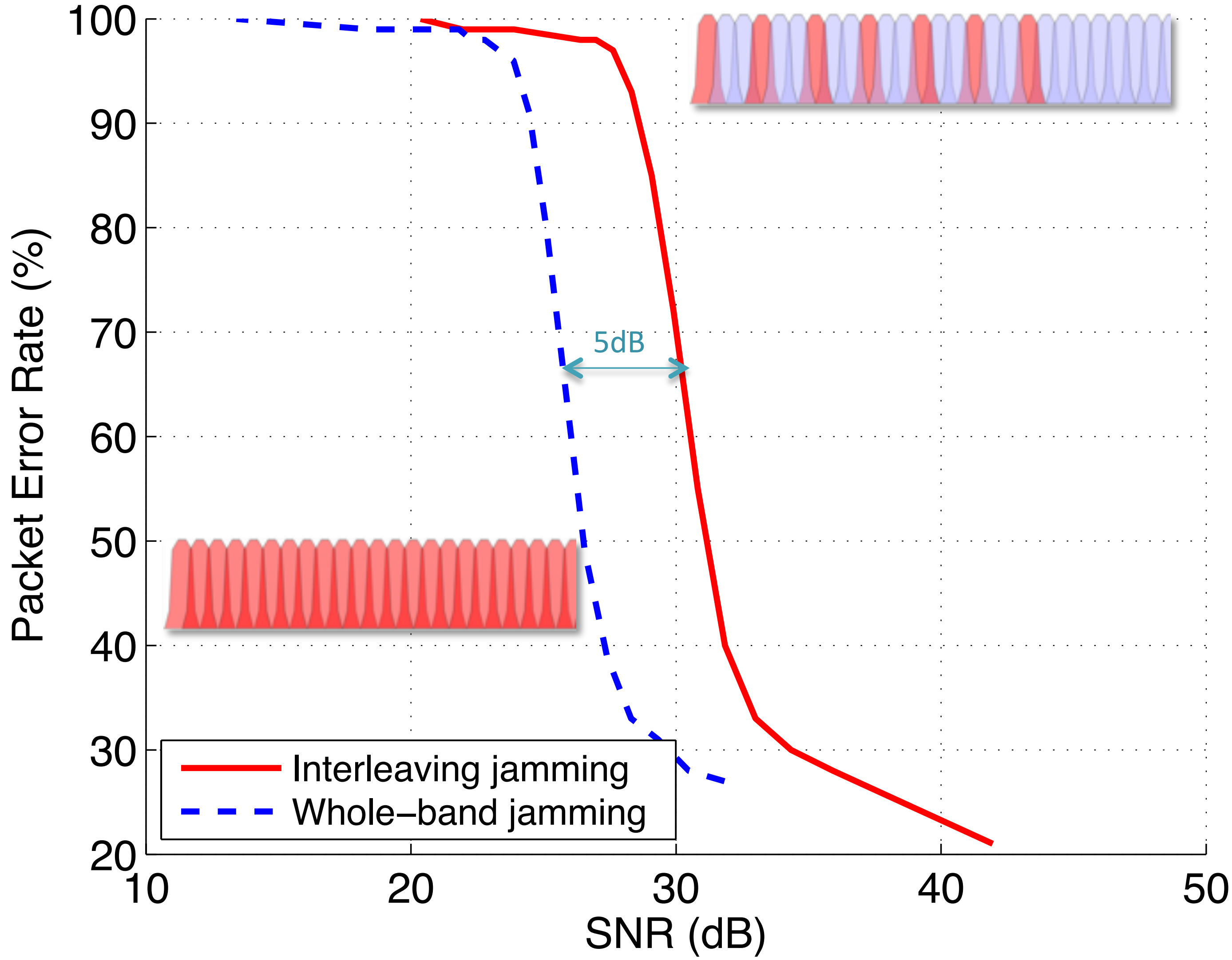
Interleaving jamming:

- 15dB and 10dB more efficient than Single jamming and Range jamming
- Reach 70% of PER

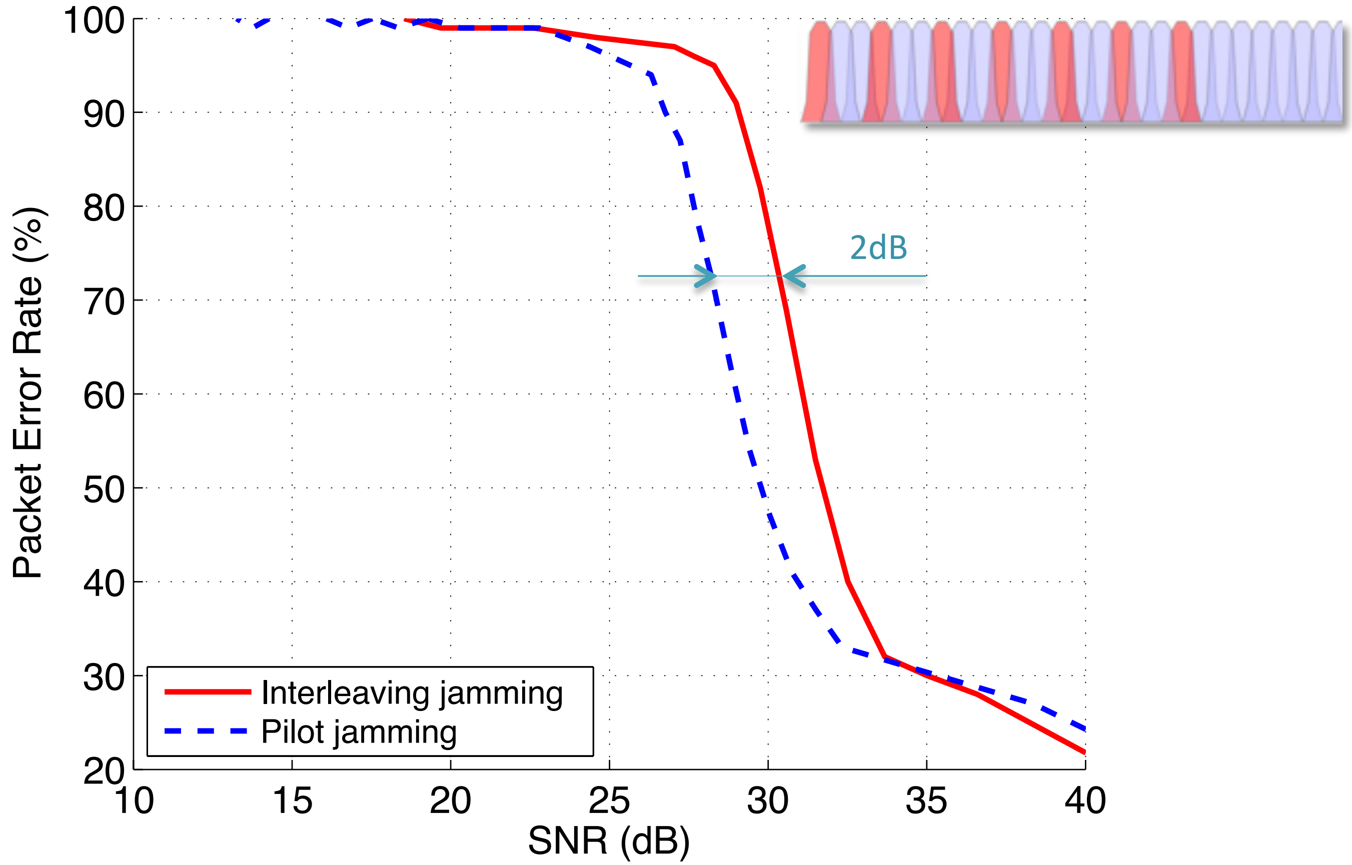
Continuous-time Wide-band Jamming

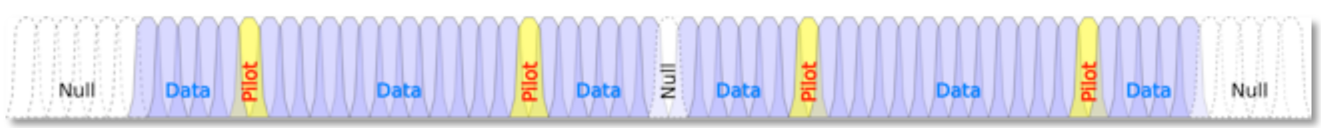


Continuous-time Whole-band Jamming

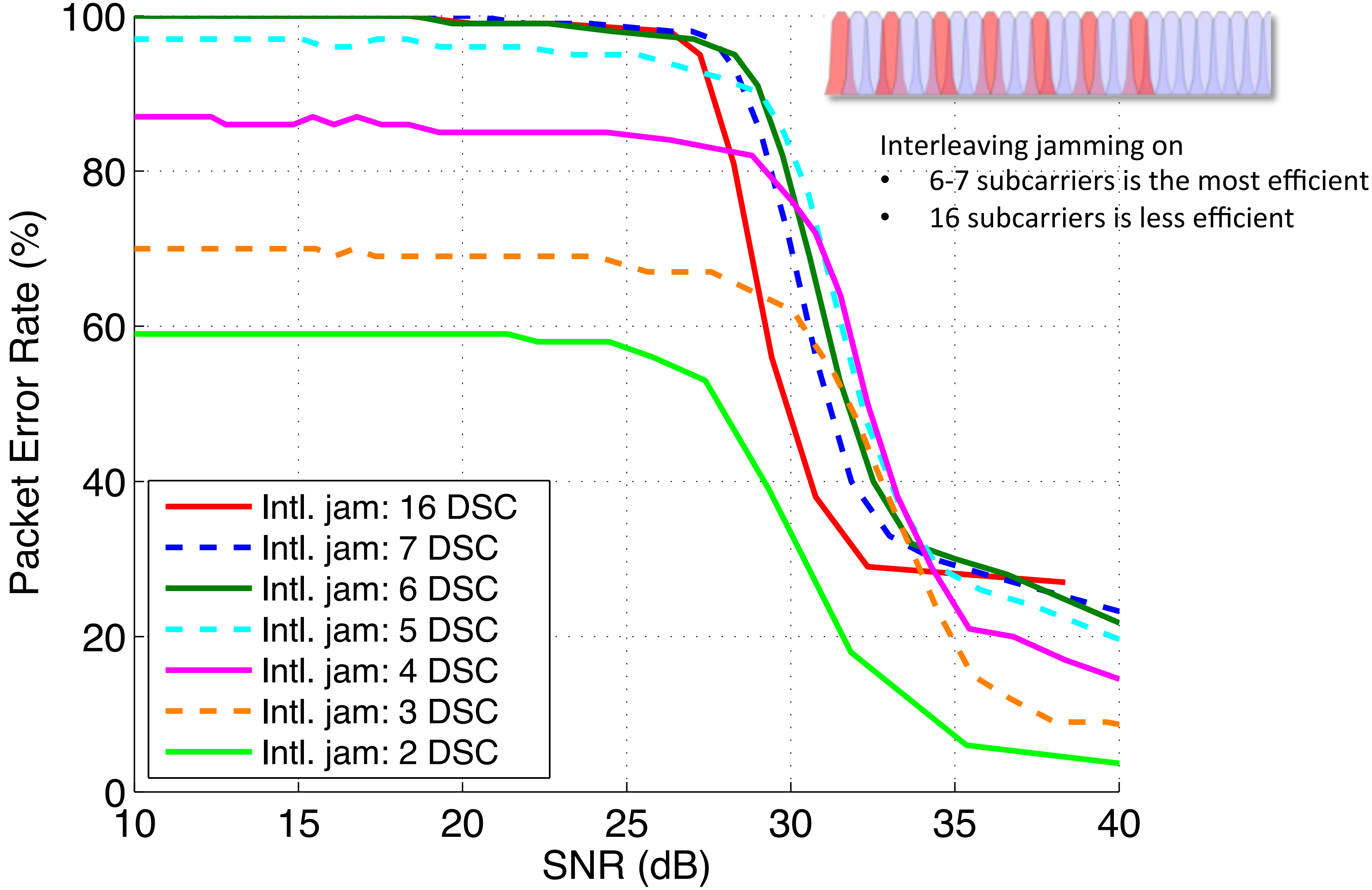


Continous-time Pilot Subcarriers Jamming

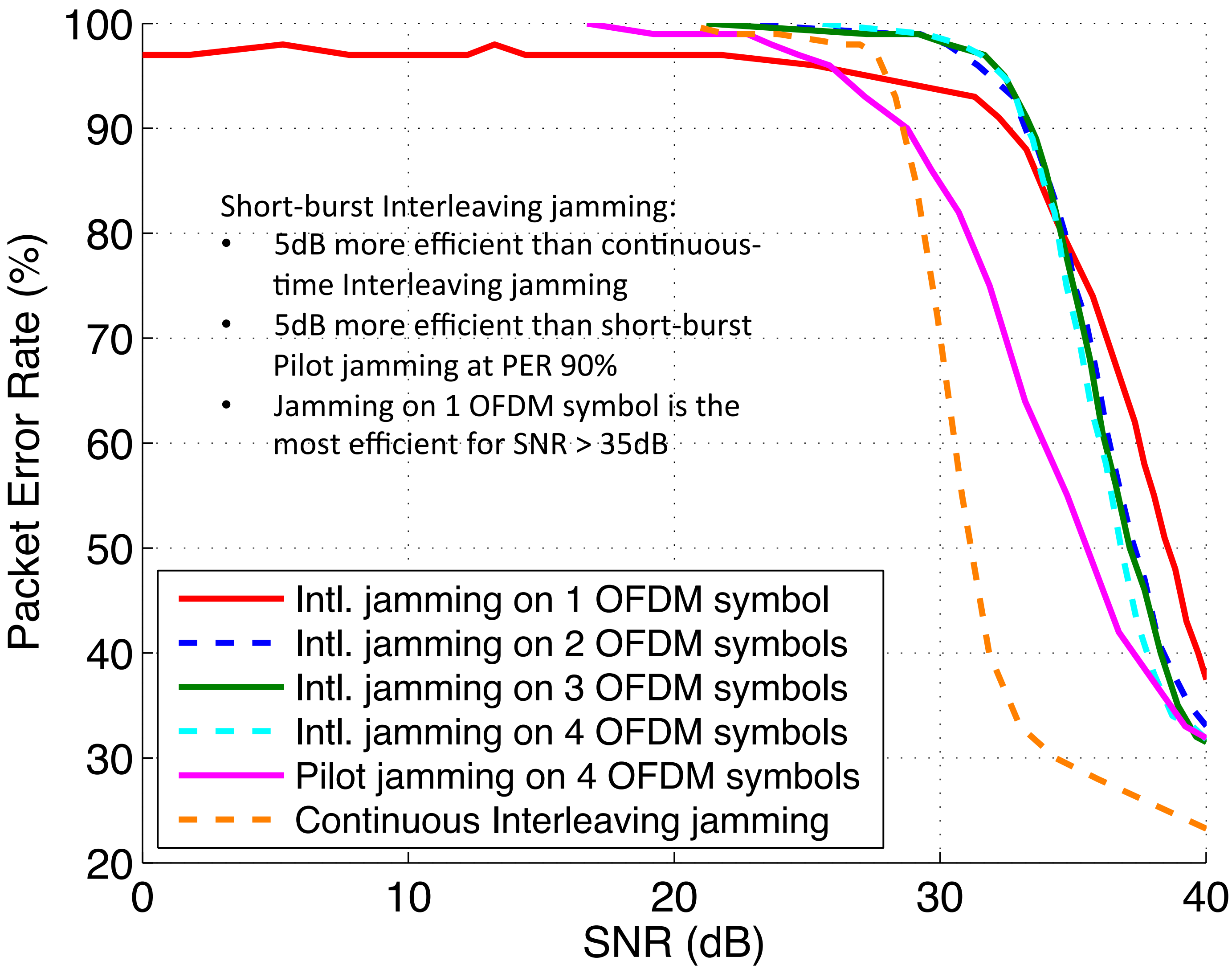




Continuous-time Interleaving Jamming with Different Number of Subcarriers



Short-burst Pilot Jamming vs. Interleaving Jamming



Agenda

1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. SDR for High-Rate Wi-Fi Analysis
4. Multi-Carrier Jamming on Wi-Fi Communications
5. Conclusion

Conclusion - 1

- Counter high-power jamming:
  - Low-cost hybrid system: special antenna design and control combined with digital cancellation technique
  - Reduce up to 48dB of jamming power
  - Zero-knowledge anti-jamming: unknown locations, variable jamming power, no preamble/training sequence
  - Environment adaptivity: outdoor and indoor anti-jamming

Conclusion - 2

- Mitigate rate attacks:
  - Hiding rate and increasing robustness at the same time
  - Discovering new Generalized TCM codes: derive 85 codes for upgrading {BPSK, QPSK, 8-PSK, 16-QAM, 64-QAM} to any higher-order modulation
  - Cryptographic interleaving technique for completely concealing modulation and code schemes
  - 2-pass decoding mechanism improves the system performance more than 3.5dB

Conclusion - 3

- Interleaving jamming strategy:
  - Efficient against IEEE 802.11 interleaving mechanism
    - Blocks 99% of packets by using jamming power 1/1000 of regular transmit power
    - Block all packets by jamming power 1/100 of regular transmit power
  - At least 5dB and up to 15dB more efficient than other multicarrier jamming strategies

THANK YOU!

QUESTIONS?