Ph.D. Thesis Proposal

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

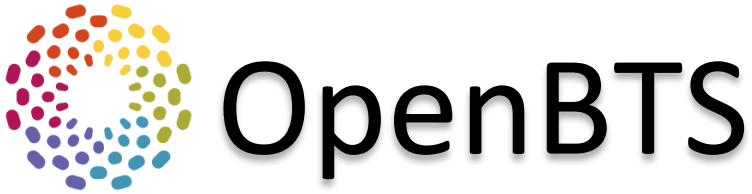
October 27, 2014

Pervasiveness of Wireless Systems

- Beyond providing user information and data services:
  - Air-traffic control
  - Power grids
  - Transportation systems
  - Human body implantable devices

Trend of Software Radio

- Radio devices migrating from hardware to software



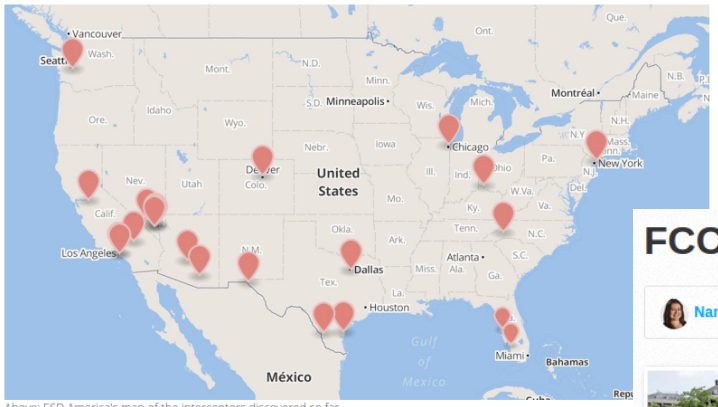
Jamming Threats

GPS Jammer

CDMA/GSM/3G/
WiFi Jammer

Software-defined radio

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

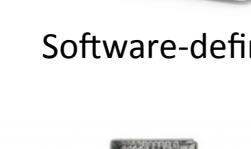


Above: ESD America's map of the interceptors discovered so far
Image Credit: ESD America

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 Age



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

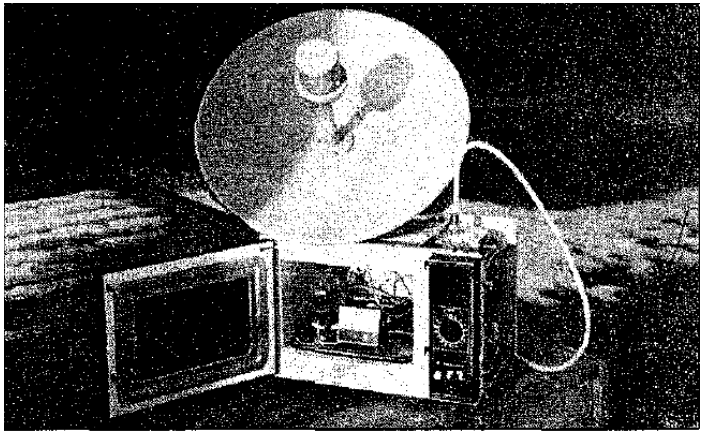
Marriott International will pay $600,000 to resolve a Federal Communications Commission investigation into whether a hotel's employees blocked customers from using their personal Wi-Fi networks and then charged them to use the hotel network.

Focus

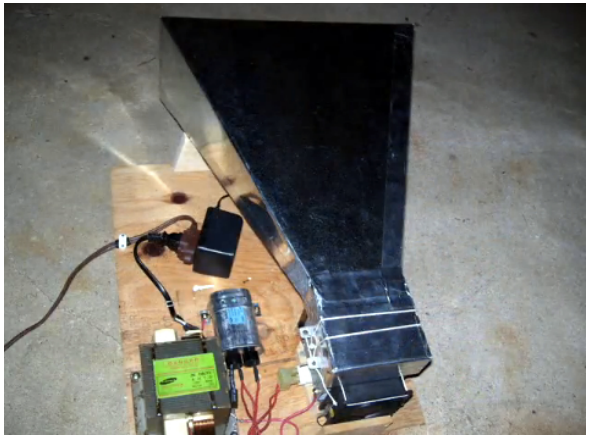
- High-Power Jamming
- Crippling Jamming
- Multi-Carrier Jamming

High-Power Jamming

- Powerful interference source (High Energy RF gun)
  - Magnetron
  - Directional antenna
- High coverage (hundreds of meters)
- Strong (1KW >> WiFi signal ≈ max. 20mW)
- Low cost



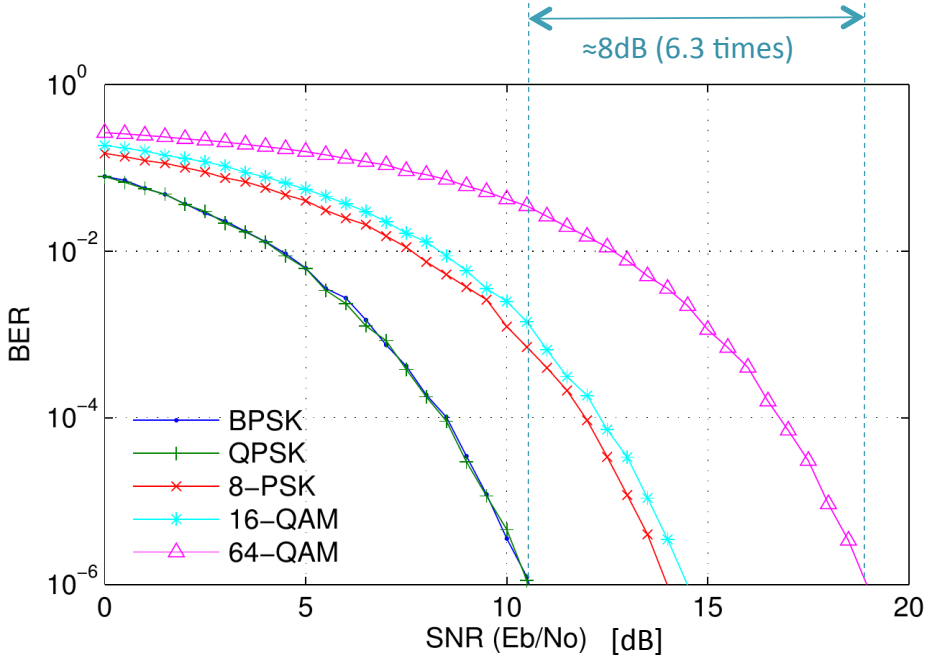
[Pacholok89]



[hacknmod.com]

Crippling Jamming

- Degrade system performance
- Hard to detect jammers
- 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

- Jamming on control channels
  - GSM: Jamming on BCCH channels is four order of magnitude more efficient [CLNT'07]
  - LTE: Attack on PCFICH with jamming rate of 0.4% [KMGLMR'14]

- Jamming on synchronization mechanisms

Research Goal

- Develop efficient and practical solutions to mitigate impacts of attacks from
  - High-Power Jamming
    - ➢ Steerable-separable Antenna for Interference Mitigation (SAIM) System [VBN'13]
  - Crippling jamming (rate/link attacks)
    - ➢ Conceal and Boost Modulation (CBM) System [VN'15]
  - Multi-Carrier jamming
    - ➢ Enhancing Multi-Carrier Multi-Antenna System

Focus of the rest of work

Data link layer

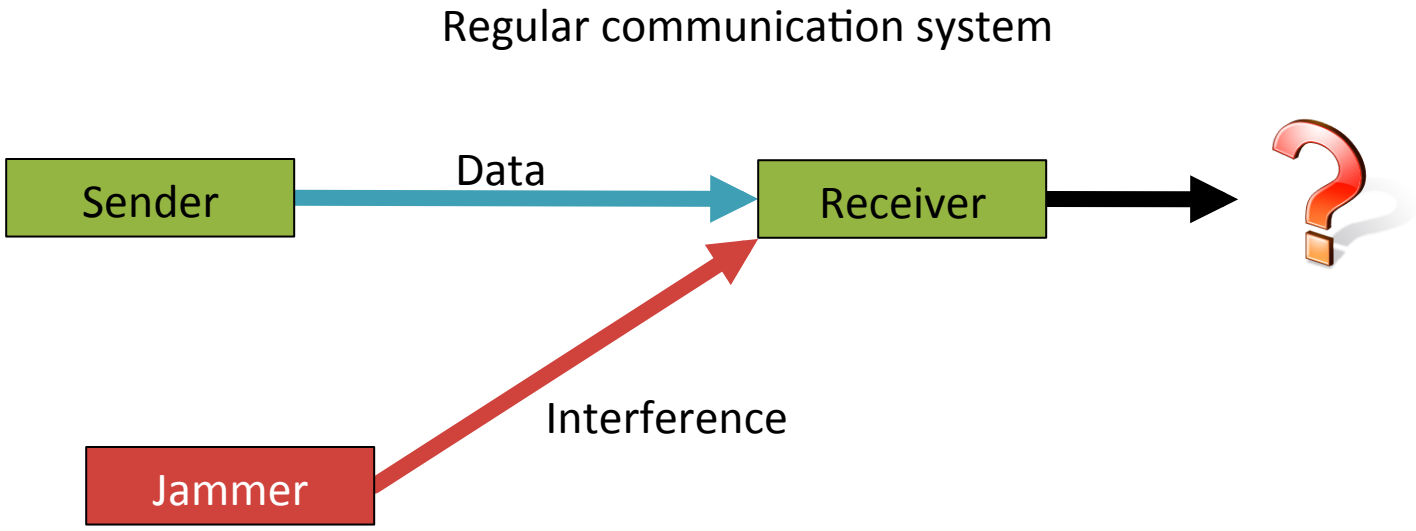
Physical layer

Agenda

1. Counter High-power Jamming
2. Conceal Rate Information and Boost Resiliency
3. Enhancing Multi-Carrier Multi-Antenna Systems
4. Future work

Countering High-Power Jamming

High-power Jamming Attack



- Jamming is effective because:
  - Jammer's power much stronger than sender's signal
  - Sender stops transmitting because of interference

Previous Work

- Directional antennas, phase array antennas: high cost, more appropriate for radar systems


PAVE PAWS

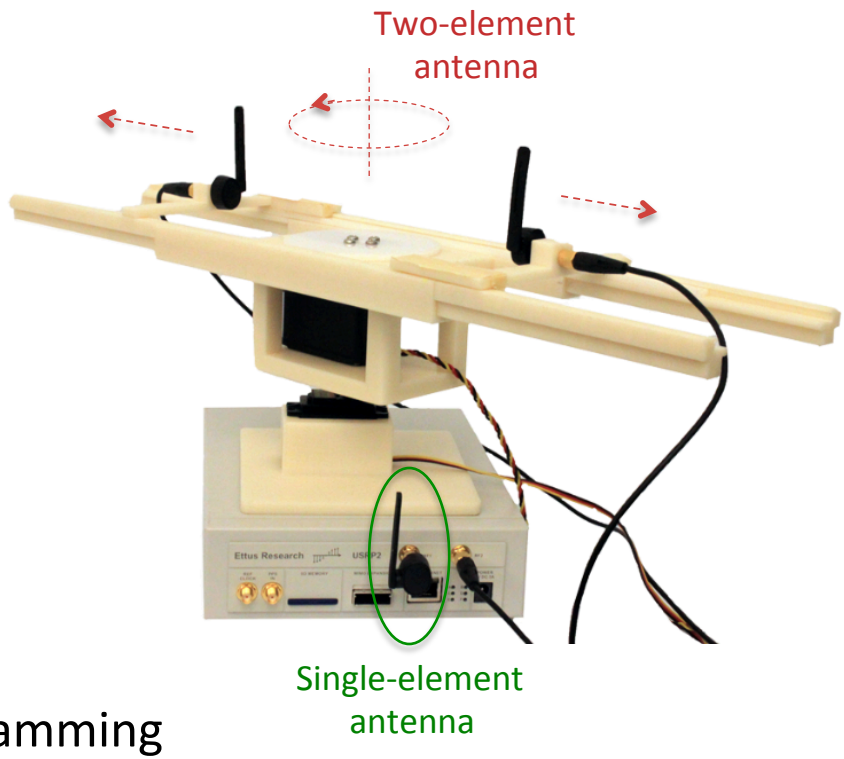
- MIMO: cooperative settings, require training sequences

- Spread spectrum: lowers the transmission rate

- Full-duplex wireless communications, Ally friendly jamming are designed for extracting known signal rather than unknown jammers

Our Approach: Steerable-separable Antenna for Interference Mitigation (SAIM)

- **Steerable** and **separable two-element** receive antenna (28dB)
  - Increase user signal's power
  - Decrease jamming signal's power
  - Fast configurations (5-18 seconds)

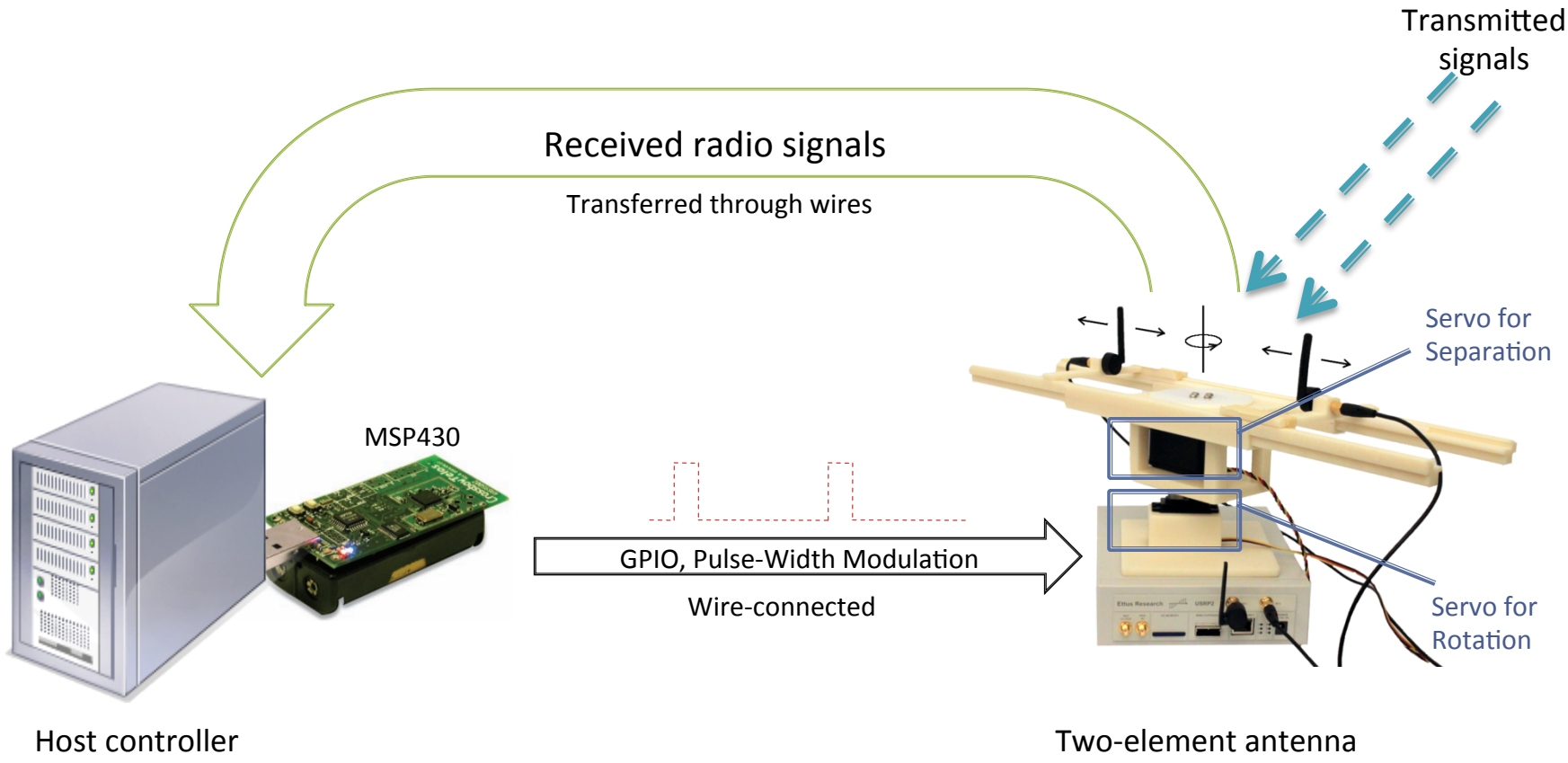


- **Digital Jamming Cancellation** (48dB)
  - Additional single-element antenna
  - Requires no training sequences
  - Removes unknown and powerful jamming

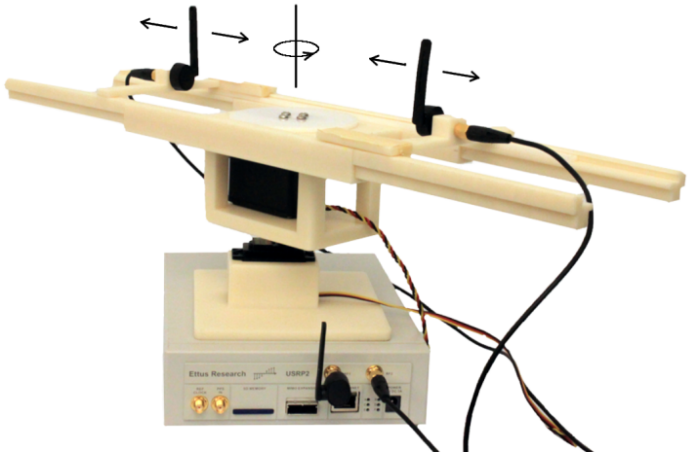
Model

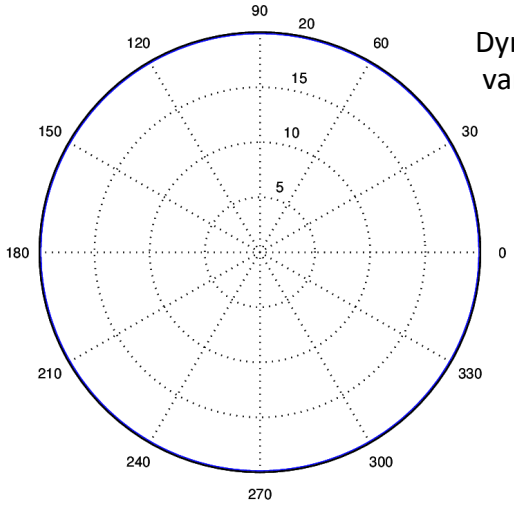
- Communication nodes:
  - Flat fading channel (5 MHz)
  - Pre-agreed modulation scheme (DBPSK, DQPSK)
  - Constant transmitting power
- Locations:
  - All nodes are not aware of locations of each other nor themselves
  - Fixed (stationary)
- Jammer is allowed to have:
  - High and variable power

Antenna Control Diagram

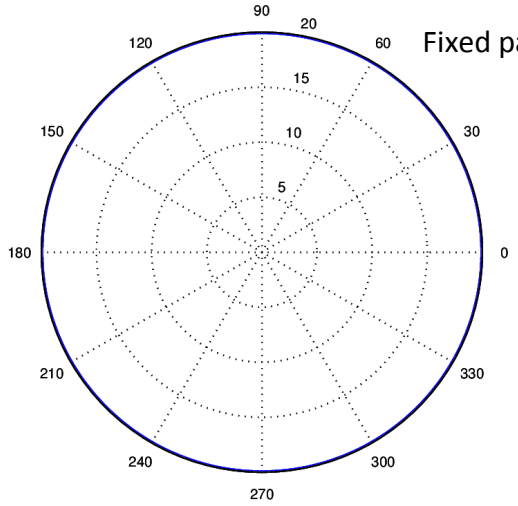


Outdoor Receive Pattern





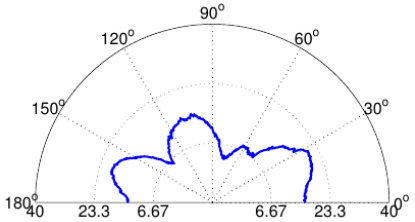
Dynamic pattern by varying separation



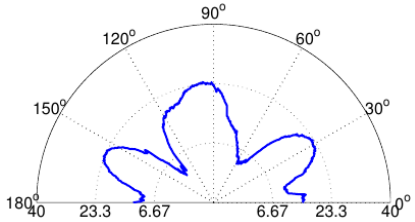
Fixed pattern

Receive pattern indicates signal power (in dB) received at the antenna corresponding to directions where the signal come from

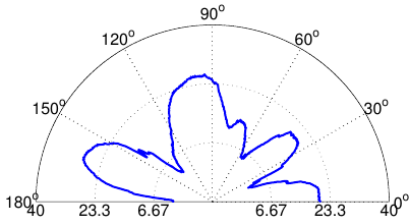
Indoor Receive Pattern



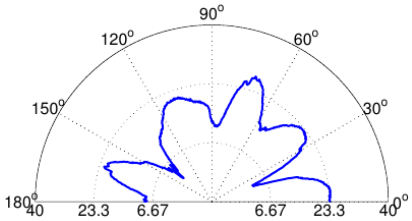
L = 3 λ/2



L = 2 λ



L = 5 λ/2



L = 3 λ

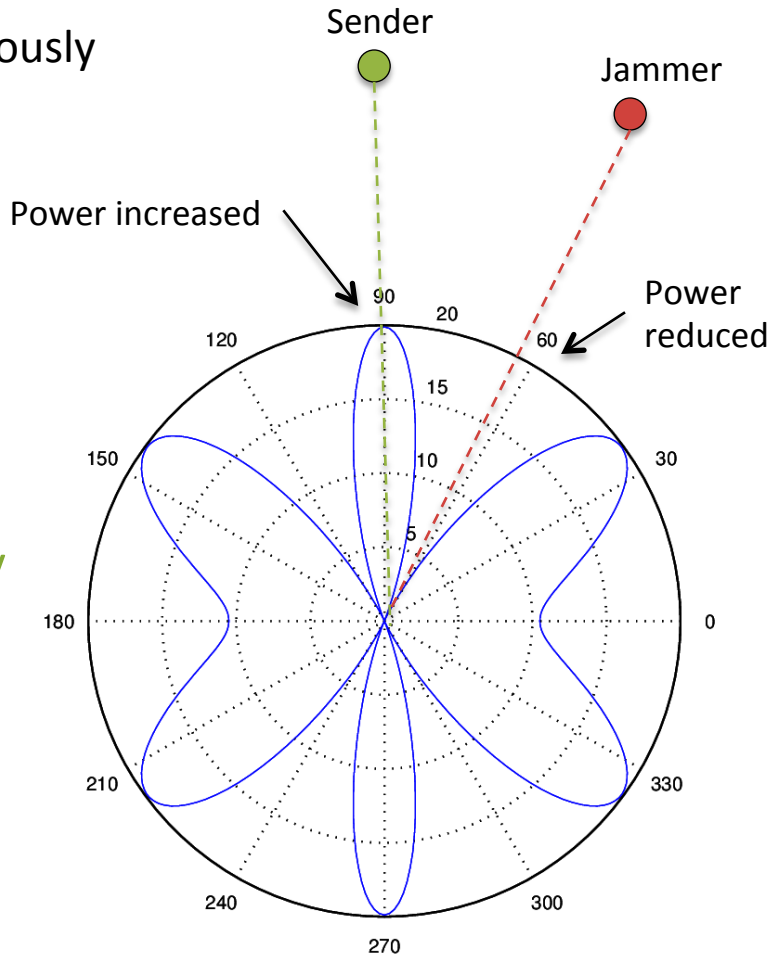
- Hard to predict
- Depends on environments

Antenna Control

- Goal:
  - Put jammer into the nulls
  - Put sender into the lobes

  } simultaneously

- How:
  - Rotate pattern by rotating antenna
  - Change pattern by adjusting separation
  - Locations of lobes and nulls deviate slightly when separation changes slightly
  - ➢ New lobes and nulls by trying nearby locations (local search)



Fast Antenna Control Algorithm Outline

1. Rotate antenna within a range $[\Phi_1,\Phi_2]$ (while fixing separation), measure received power for each angle

2. Change element separation within a range $[L_1,L_2]$ (while fixing orientation), measure received power for each separation value

3. Update $[\Phi_1,\Phi_2]=[\Phi^*-\theta, \Phi^*+\theta]$, $[L_1,L_2]=[L^*-\Delta L,L^*+\Delta L]$

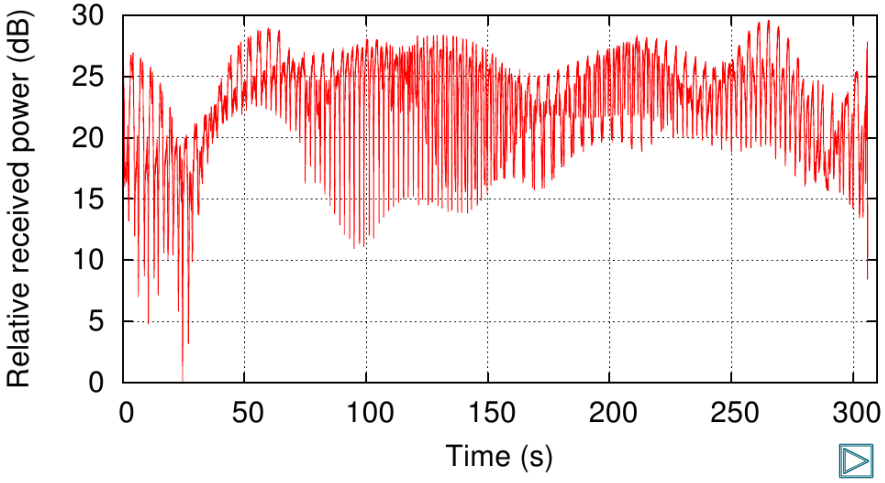
4. Repeat step 1-3 until Φ^*, L^* unchanged

5. Return (Φ^*, L^*)

Fast vs. Brute-force

Fast

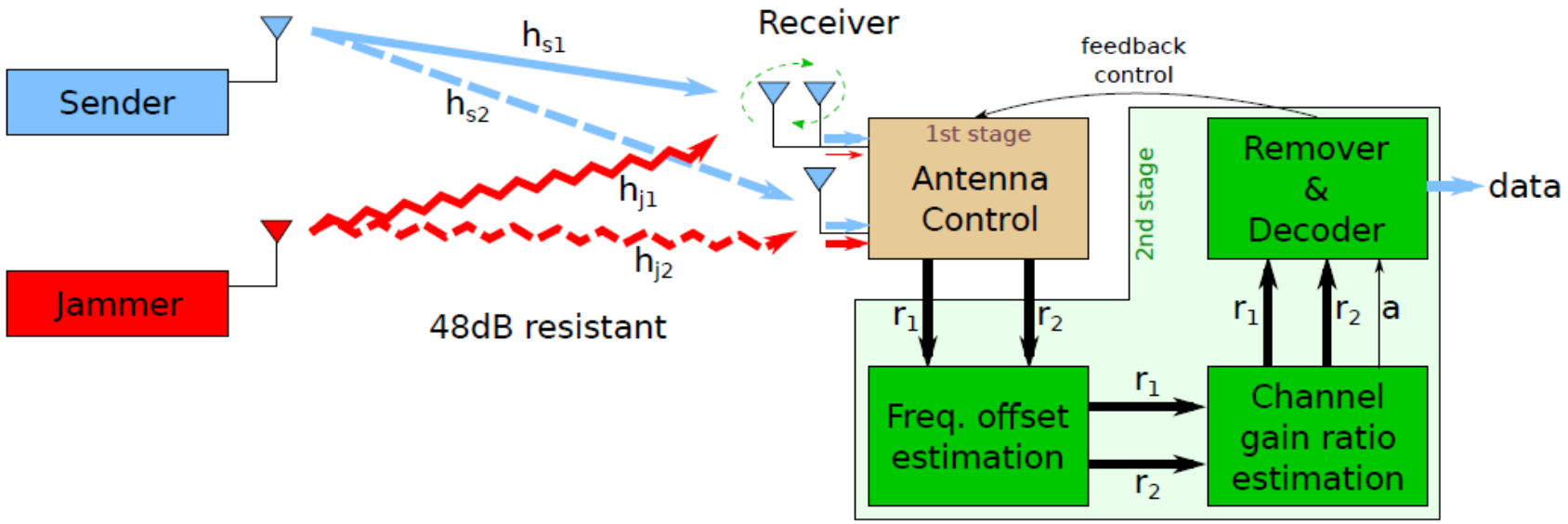
Brute-force



	Fast	Brute-force
Performance	15 – 28 dB	15 – 30 dB
Running time	5 – 18 seconds Environment-dependent	> 5 minutes Environment-independent

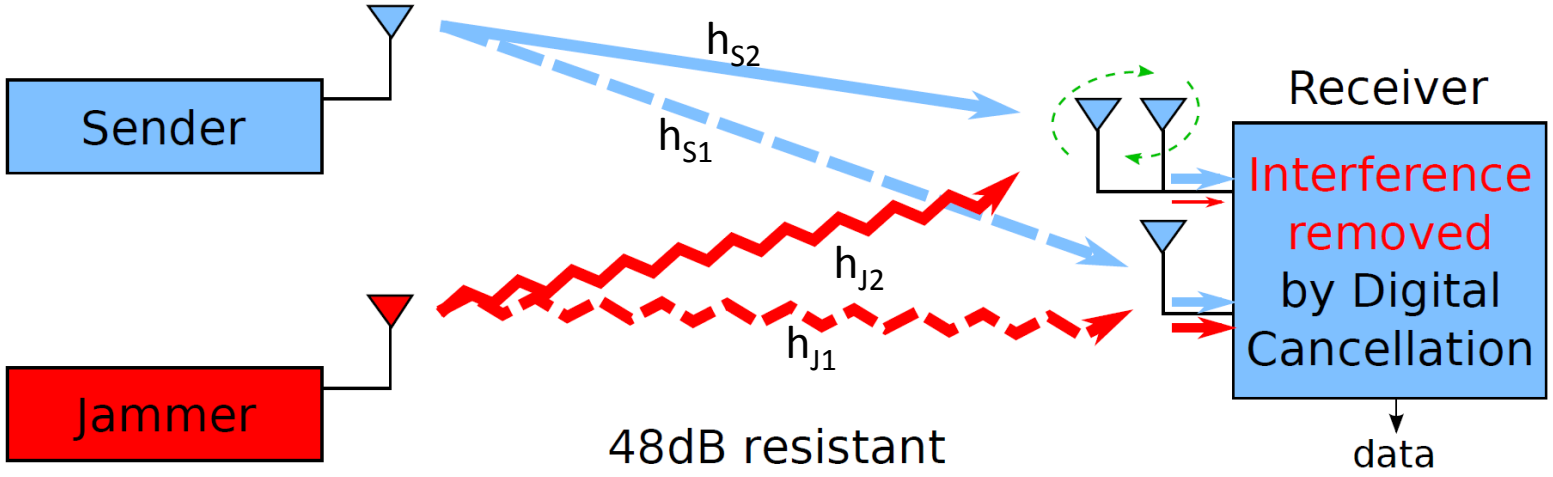
Digital Jamming Cancellation

- Goal: increase anti-jamming capability from 28dB to 48dB
- Approach:
  - Use an additional single-element antenna
  - Extract original data signal from 2 received signals



Extracting Original Data

- Received signal at single-element antenna:
  - $R_1 = h_{S1} S + h_{J1} J$
- Received signal at two-element antenna:
  - $R_2 = h_{S2} S + h_{J2} J$
- Problem: 2 equations, 6 variables (S, J, h_{S1}, h_{S2}, h_{J1}, h_{J2})



Principle of Digital Jamming Cancellation

- If we knew
  - $a = h_{J2} / h_{J1}$: channel gain ratio
  - $b = a h_{S1} - h_{S2}$: residual gain
  - We could extract: $S = (aR_1 - R_2) / b$

$$R_1 = h_{S1} S + h_{J1} J$$
$$R_2 = h_{S2} S + h_{J2} J$$

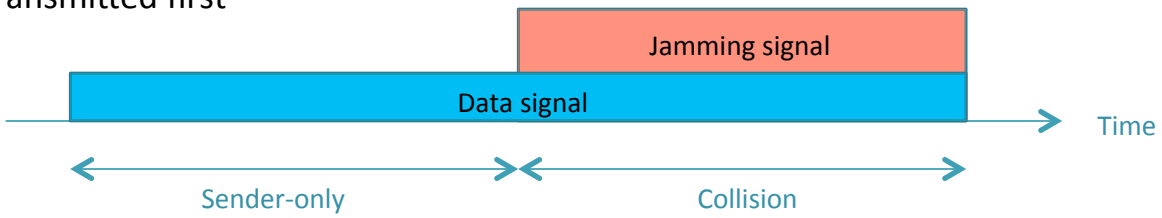
- Estimating a does not require estimating h_{J1}, h_{J2} separately
  - Our technique is energy-based estimation
- Estimating b is similar to equalizing and demodulating techniques in traditional communication systems
  - $bS = aR_1 - R_2$: b is just a new gain of signal resulted from jam removing
- Different from traditional MIMO techniques:
  - No training sequences are required
  - Deal with unknown and strong jammer

Estimating Channel Gain Ratio

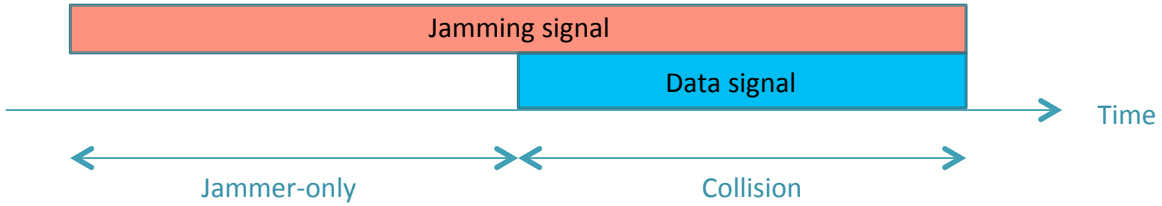
- Measure signal's average power at both single-element and two-element antennas during a short period right before collision and during the collision
  - Running average power over a period of 100 samples

- Distinguish 2 cases:

Sender transmitted first



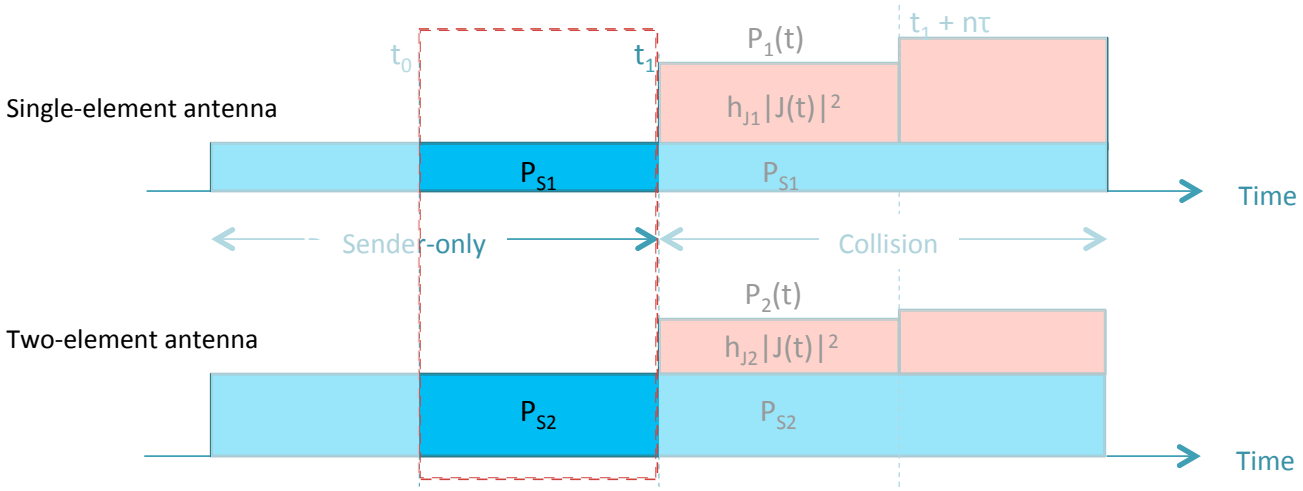
Jammer transmitted first



Sender Transmitted First

- Step 1: Measure signal power before collision (in period $[t_0, t_0+n\tau]$)

$$P_1(t_0) = \frac{1}{n}\sum_{t=t_0}^{t_0+n\tau} \left|h_{S1}(t)S(t)\right|^2 = \frac{1}{n}\left|h_{S1}\right|^2 \sum_{t_0} \left|S(t)\right|^2 = P_{S1} \qquad P_2(t_0) = \frac{1}{n}\left|h_{S2}\right|^2 \sum_{t_0} \left|S(t)\right|^2 = P_{S2}$$



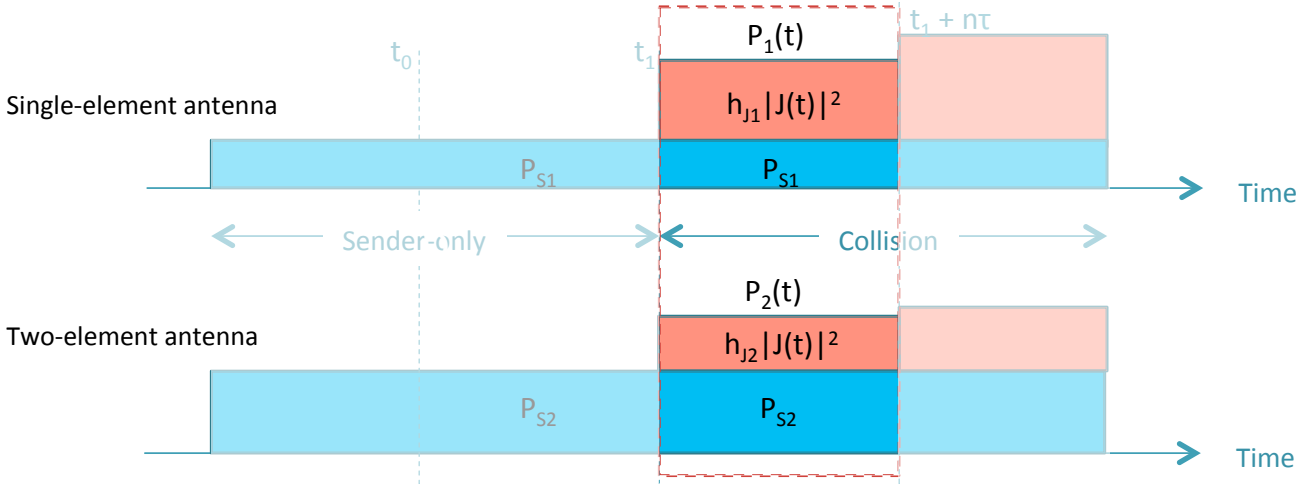
Sender Transmitted First

- Step 2: Measure signal power during collision (in period $[t_1, t_1+n\tau]$)

$$P_1(t_1) = \frac{1}{n}\sum_{t=t_1}^{t_1+n\tau}\left|h_{S1}(t)S(t) + h_{J1}(t)J(t)\right|^2 \approx \frac{1}{n}\left(\left|h_{S1}\right|^2\sum_{t_1}\left|S(t)\right|^2 + \left|h_{J1}\right|^2\sum_{t_1}\left|J(t)\right|^2\right) = \frac{1}{n}\left(P_{S1} + \left|h_{J1}\right|^2\sum_{t_1}\left|J(t)\right|^2\right)$$

$$P_2(t_1) = \frac{1}{n}\sum_{t=t_1}^{t_1+n\tau}\left|h_{S2}(t)S(t) + h_{J2}(t)J(t)\right|^2 \approx \frac{1}{n}\left(\left|h_{S2}\right|^2\sum_{t_1}\left|S(t)\right|^2 + \left|h_{J2}\right|^2\sum_{t_1}\left|J(t)\right|^2\right) = \frac{1}{n}\left(P_{S2} + \left|h_{J2}\right|^2\sum_{t_1}\left|J(t)\right|^2\right)$$

sender's and jammer's signal are independent

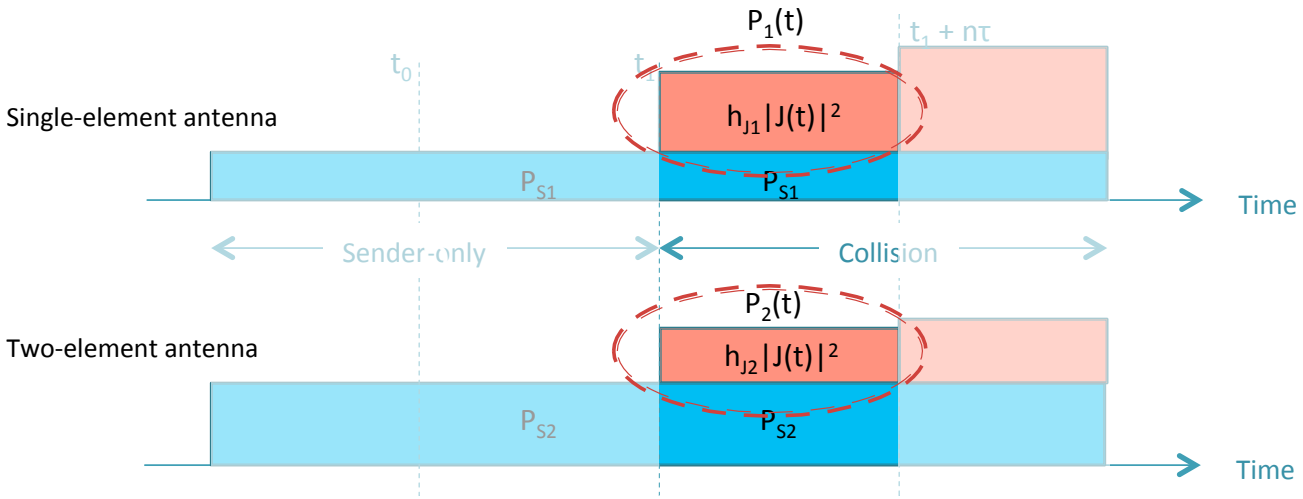


Sender Transmitted First

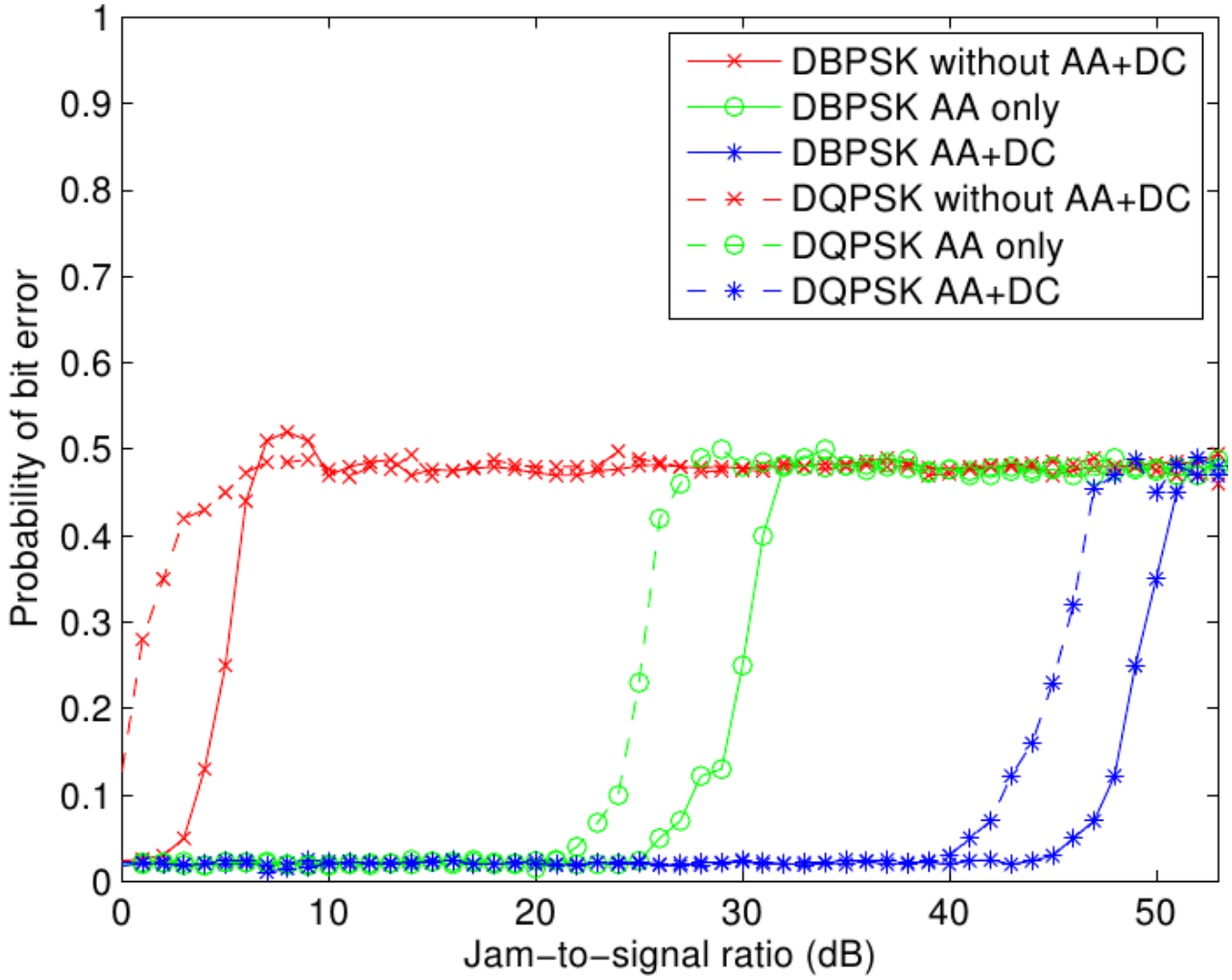
- Step 3: Estimate channel gain ratio a:

Magnitude: $|a| = \left|\frac{h_{J2}}{h_{J1}}\right| = \sqrt{\frac{P_2(t) - P_{S2}}{P_1(t) - P_{S1}}}$

Phase: $\angle a = \tan^{-1}\left(-\frac{\sum[I_1(t)Q_2(t) - I_2(t)Q_1(t)]}{\sum[I_1(t)I_2(t) + Q_1(t)Q_2(t)]}\right)$



Anti-jamming Performance: DBPSK and DQPSK



AA: Antenna Auto-configuration
DC: Digital Cancellation

Summary

- Low-cost hybrid system
- Counter adversaries with significantly more power than transmitting node: up to 48dB
  - First stage: custom-designed antenna allows a large number of receive patterns for eliminating jamming signal
  - Second stage: digital module removes jamming signal using two received signal from both antennas
- Zero-knowledge anti-jamming: unknown locations, variable jamming power, no preamble/training sequence
- Environment adaptivity: outdoor and indoor anti-jamming

Conceal Rate Information and Boost Resiliency

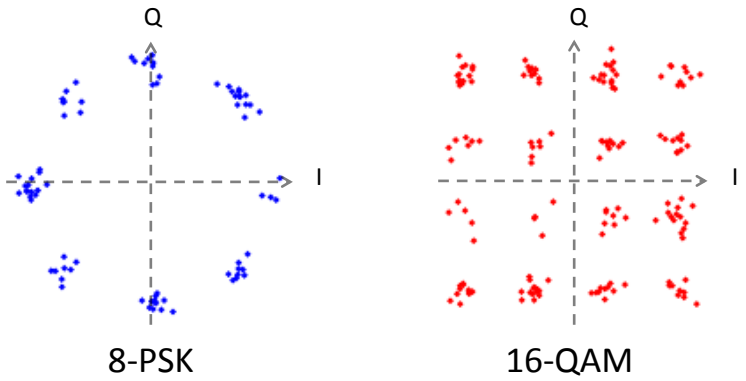
Why Need to Hide Rate

- Crippling jamming attack on rate adaptation:
  - Destroy high-rate packets
  - Low-rate transmission links block other communications
  - Degrade whole system's performance

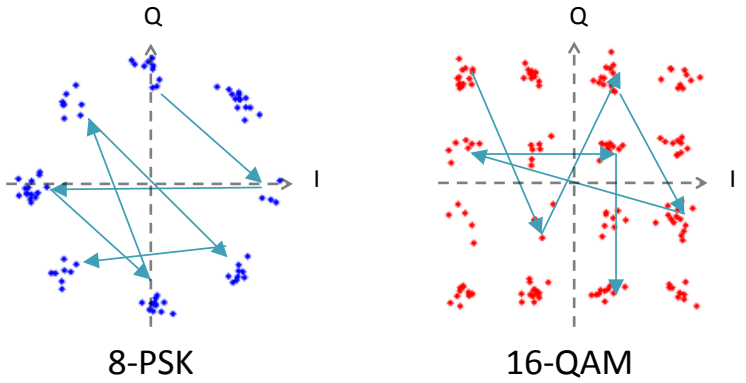
- Reason: Adversary knows the rate information (rate exposed in WiFi SIGNAL field, LTE MCS field)

Rate Detection

- Explicit:
  - Rate exposed in protocol's public header (WiFi, LTE, …)
- Implicit:
  - Not require parsing of protocol's frame structure
  - Modulation guessing: by analysis of received complex samples (in-phase and quadrature components)
  - Code guessing: by analysis of received complex samples and tracking maximum likelihood symbol sequences



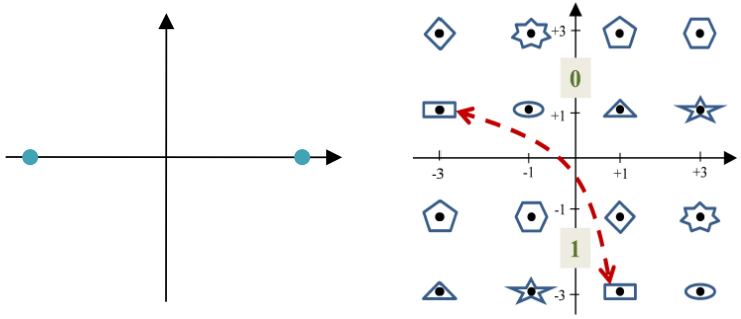
Modulation guessing



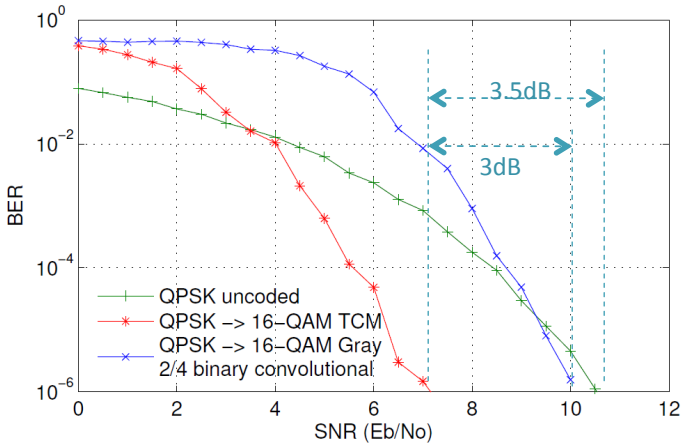
Code guessing
(code transitions can be traced)

Challenges of Rate Hiding

- Encrypting Header:
  - ☺ No explicit rate exposing
  - ☹ Suffer from implicit rate detection
- Use only one rate:
  - ☺ No rate information lost
  - ☹ Lost 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



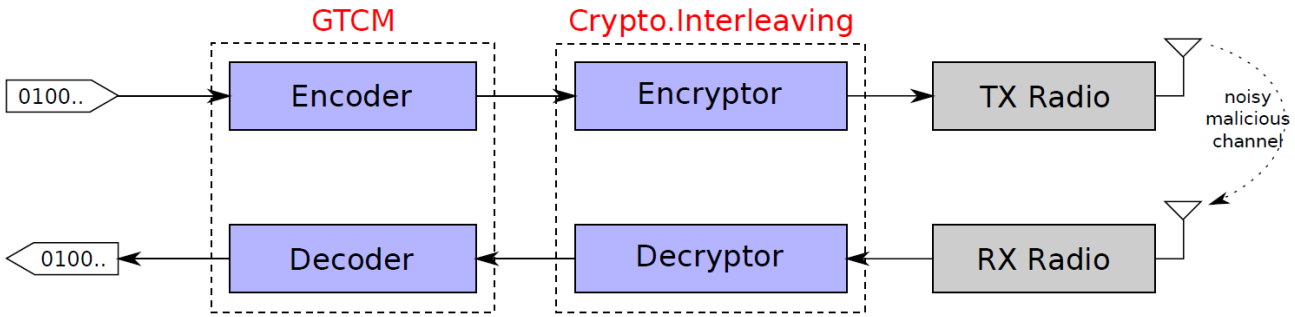
Modulation Unification



Binary codes (blue line)
do not increase resiliency for 16-QAM

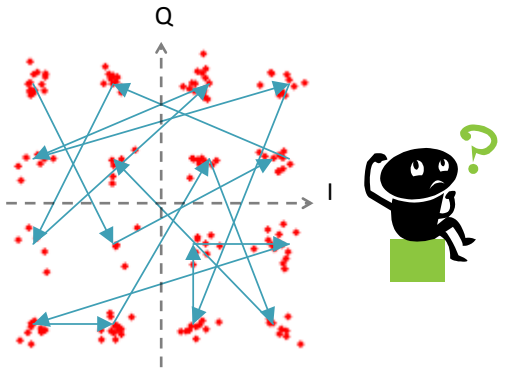
Goal and Approach

- 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:
    - No rate exposing
    - Counter modulation guessing

    } Always use highest order modulation
    - Boost resiliency: Generalize TCM codes
  - Cryptographic Interleaving:
    - Counter code guessing: cryptographic permutation of transmitted symbols



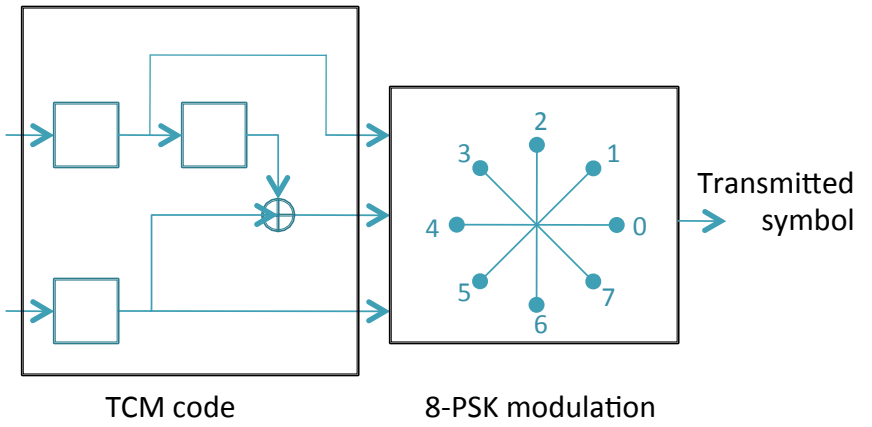
(a) Modulation hidden inside higher-order modulation, and (b) Symbol sequence transitions are randomized

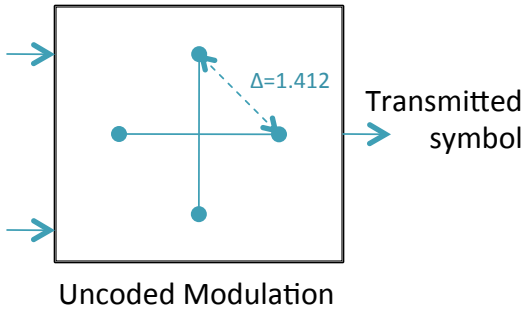
Trellis Coded Modulation

- TCM is a convolutional code (n,k,v) designed specifically to higher-order modulation

- Maximize Euclidean distance between coded symbol sequences
  - Binary codes are designed to maximize Hamming distance

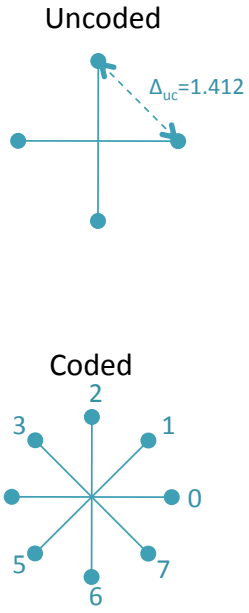
- Parameters:
  - Input: k bits
  - Output: n bits (n>k)
  - Constraints (cells per input): $v_0,\ldots v_{k-1}$
  - Constraint length (total cells): $v=\Sigma v_i$
  - Number of states: 2^v

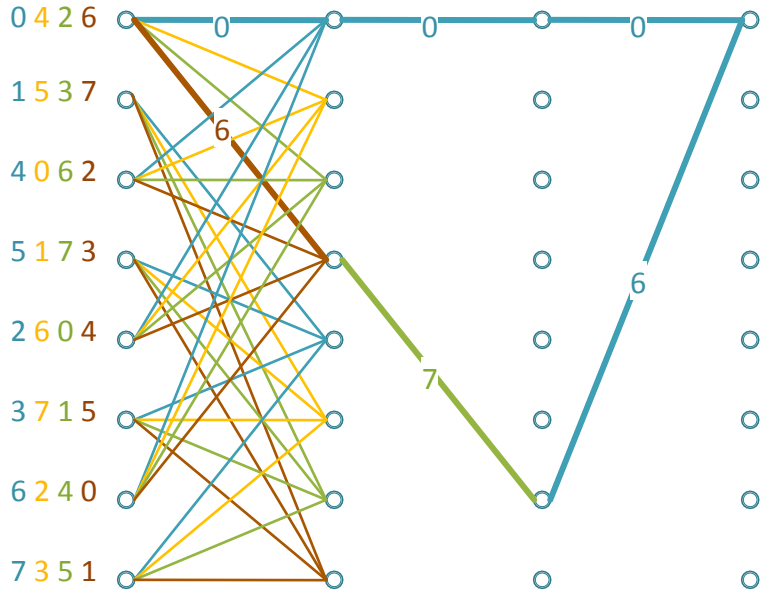




Performance Metrics

- Coding gain $G = d^2_{free}/\Delta^2_{uc}$
- d_{free} : TCM code's free distance
  - Shortest distance between any two paths diverging from the same starting state and remerging into the same ending state
- Δ_{uc}: Uncoded modulation symbol distance

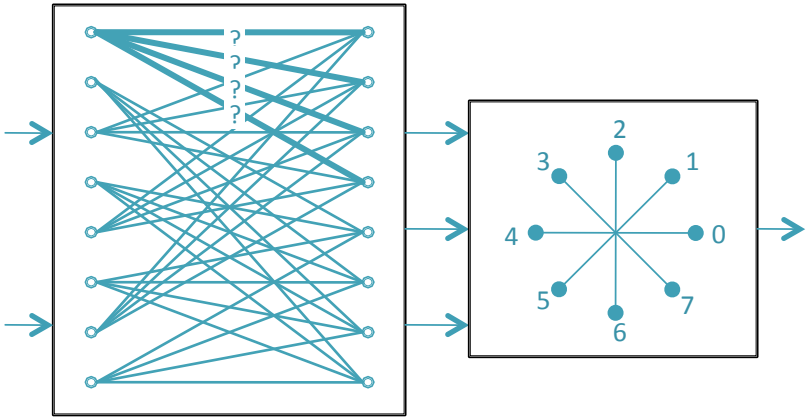




d_{free}= Δ(0,6)+ Δ(0,7)+ Δ(0,6)=2.141 → G=3.6dB

TCM Codes vs. Generalized TCM Codes

- Finding traditional TCM codes:
  - Set partitioning and design rules
    → regular/uniform mapping
  - Only for rate k/(k+1)
  - Heuristic (no theoretical proof)



TCM Search: determine trellis mapping

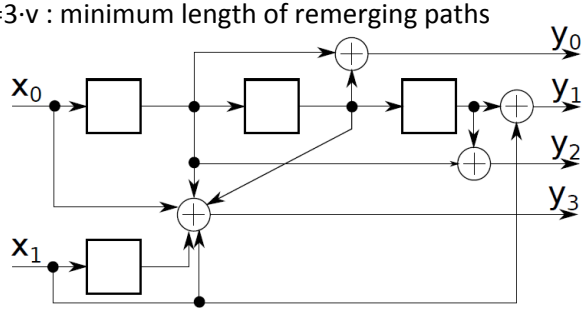
- We generalize TCM codes:
  - General rate k/n
    → conceal any modulation into any higher-order modulation
  - Relax uniformity
    → larger class of codes. We found some better codes
  - Heuristic: but not based on set partitioning and design rules

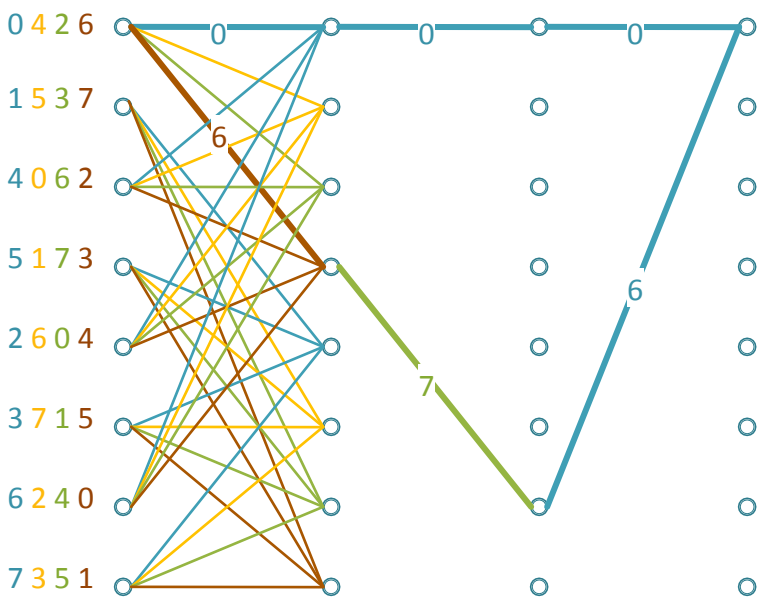
Search Algorithm for Generalized TCM Codes

1. Generate a random code mapping
   - Time: O(logV+logK)
2. Check validity of generated code: if invalid, repeat step 1
   - Time: O(V+N)
3. Compute free distance of generated code:
   - Involves distances between every pair of paths that diverge and remerge
   - Time: $O(K^2V^2L)$. Practice: < 2ms
   - Compare to naïve algorithm: $O(K^LKVL)$

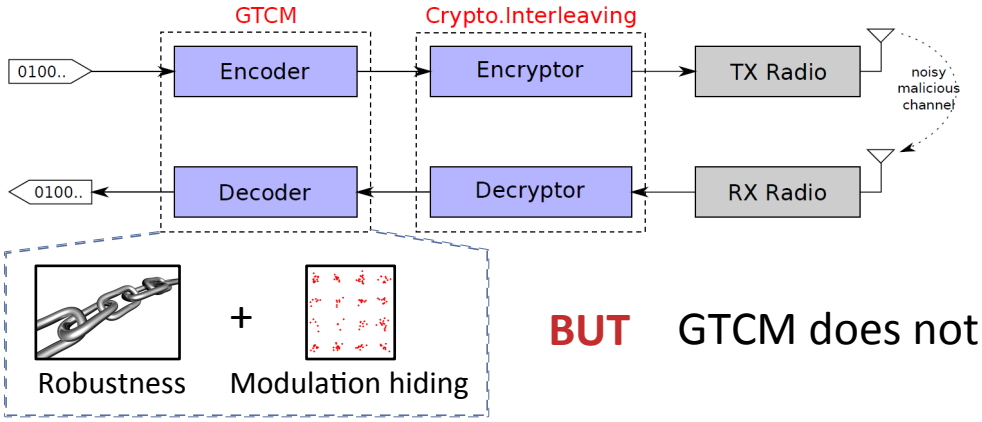
To justify the algorithm, let

- $K=2^k$: number of code's input symbols
- $N=2^n$: number of code's output symbols
- $V=2^v$: number of code's states
- $L=3 \cdot v$: minimum length of remerging paths



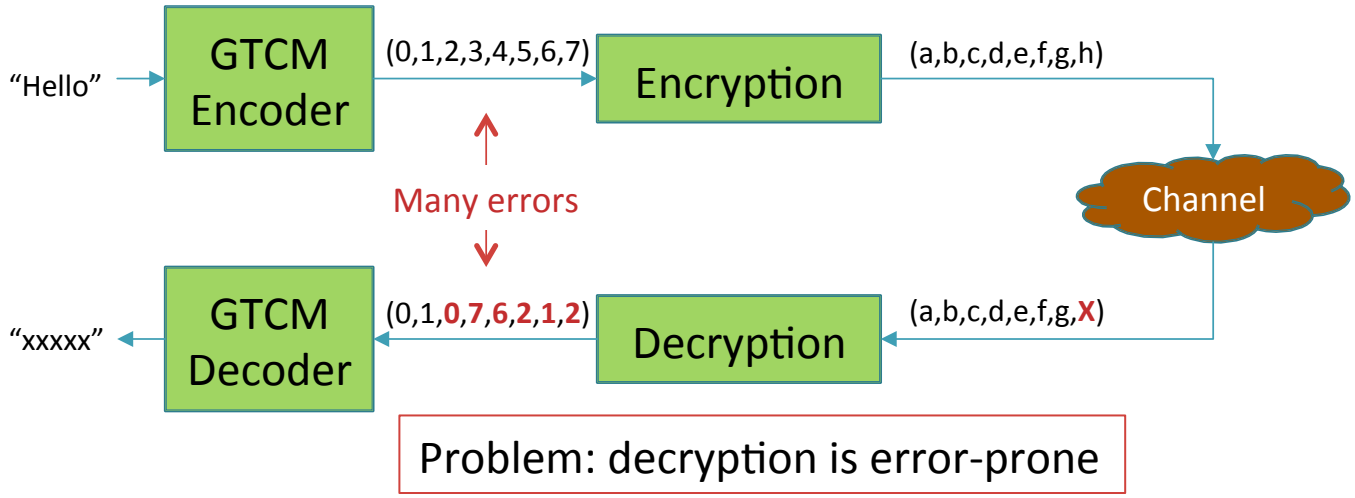


Why Cryptographic Interleaving?



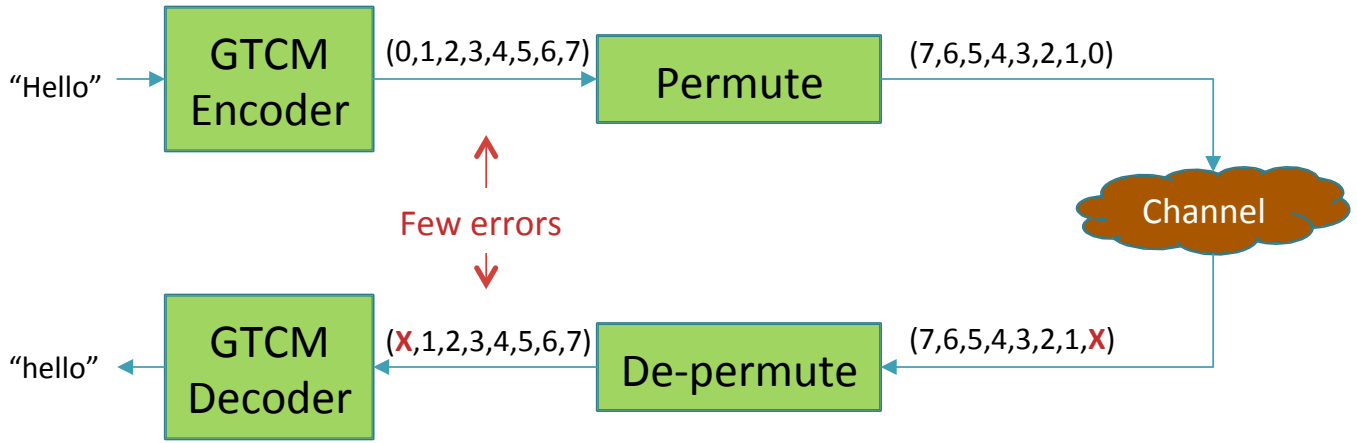
BUT GTCM does not conceal codes

- Can we encrypt coded symbol sequence? Answer: No

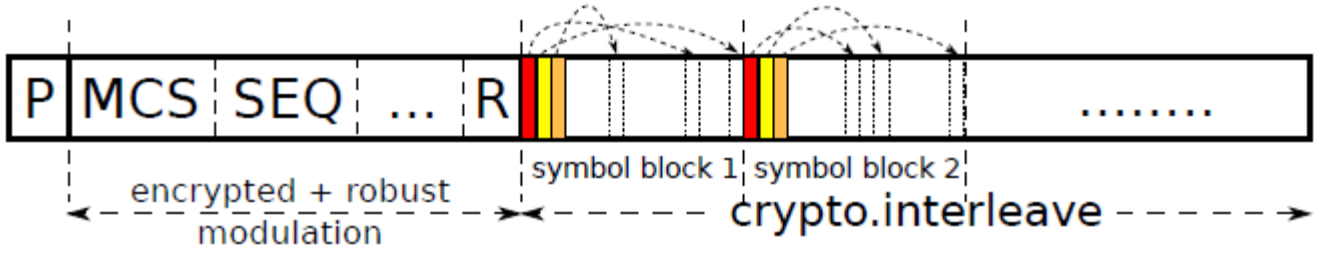


Our Approach

- Permuting (interleaving) coded symbols



Interleaving Process

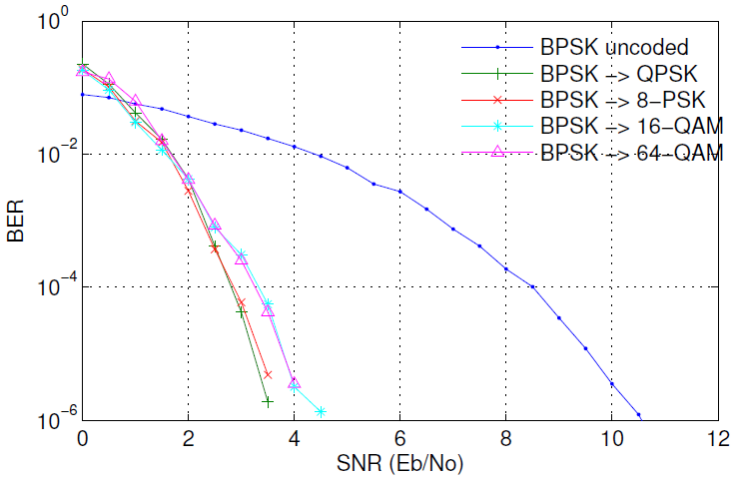


- Interleaving:
  - Designed based on cryptographic hash functions
  - Blocks of interleaved symbols are indistinguishable

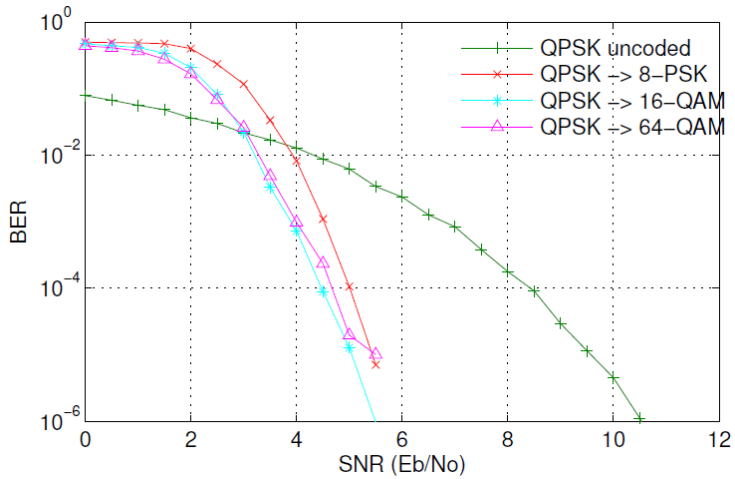
- Concealing Header:
  - Encoded with fixed robust coding scheme
  - Encrypted using AES-CBC: $\text{AES-CBC}_K(\text{MCS}|\text{SEQ}|\ldots|\text{R})$

Evaluation of CBM

- MatLab simulation:
  - From any modulation to any higher-order modulation
  - Transmission of 1Gbits
  - Channel: Additive White Gaussian Noise
  - Signal-to-noise ratio: 0dB → 15dB (0.5dB step)
  - Codes constraint length: v=10

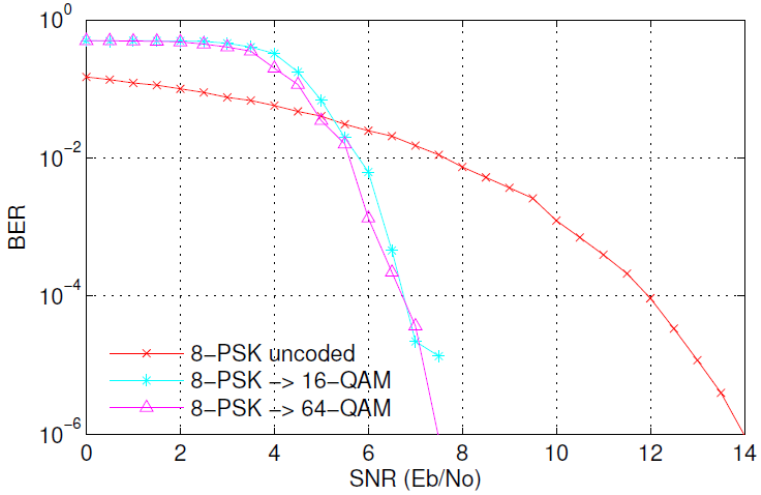


Concealing BPSK

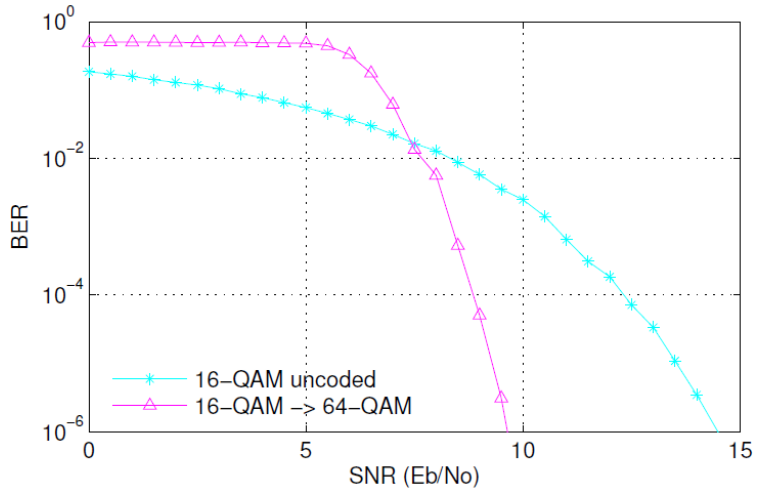


Concealing QPSK

Evaluation of CBM



Concealing 8-PSK



Concealing 16-QAM

- Resiliency boost between 5dB to 6.5dB when 64-QAM is used for rate concealing → up to 8dB compared to [RK'14]
- Performance boost is similar across different target modulations
  - Future wireless systems can always use the highest modulation
  - Adapt to channel conditions by only changing codes

Summary

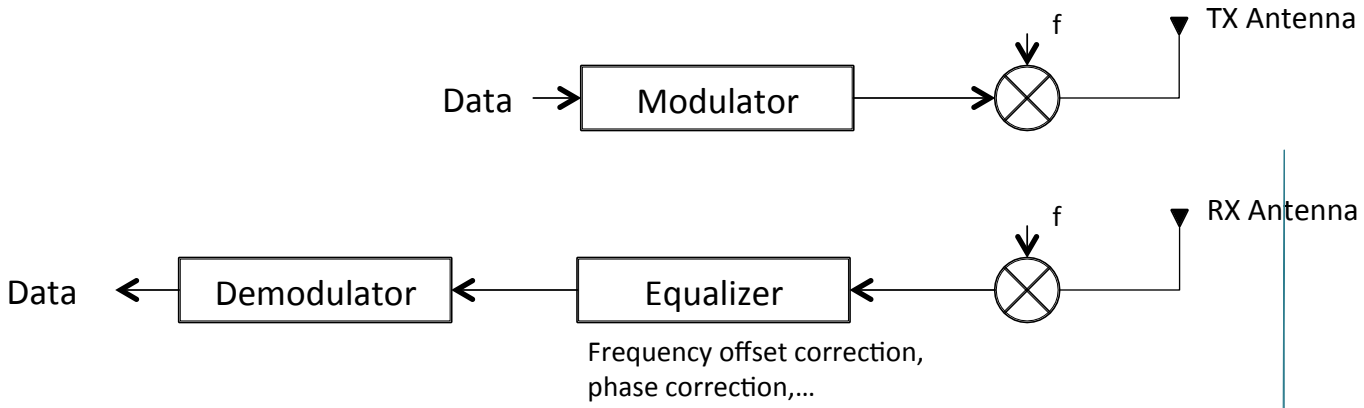
- Hiding rate and increasing robustness at the same time
- Discovering new Generalized TCM codes
  - New efficient free distance computation algorithm for GTCM codes
  - Explicitly derive 85 codes for upgrading {BPSK, QPSK, 8-PSK, 16-QAM, 64-QAM} to any higher-order modulation
- Cryptographic interleaving technique for completely concealing modulation and code schemes

Enhancing Multi-Carrier Multi-Antenna Systems

Focus of Rest of Work

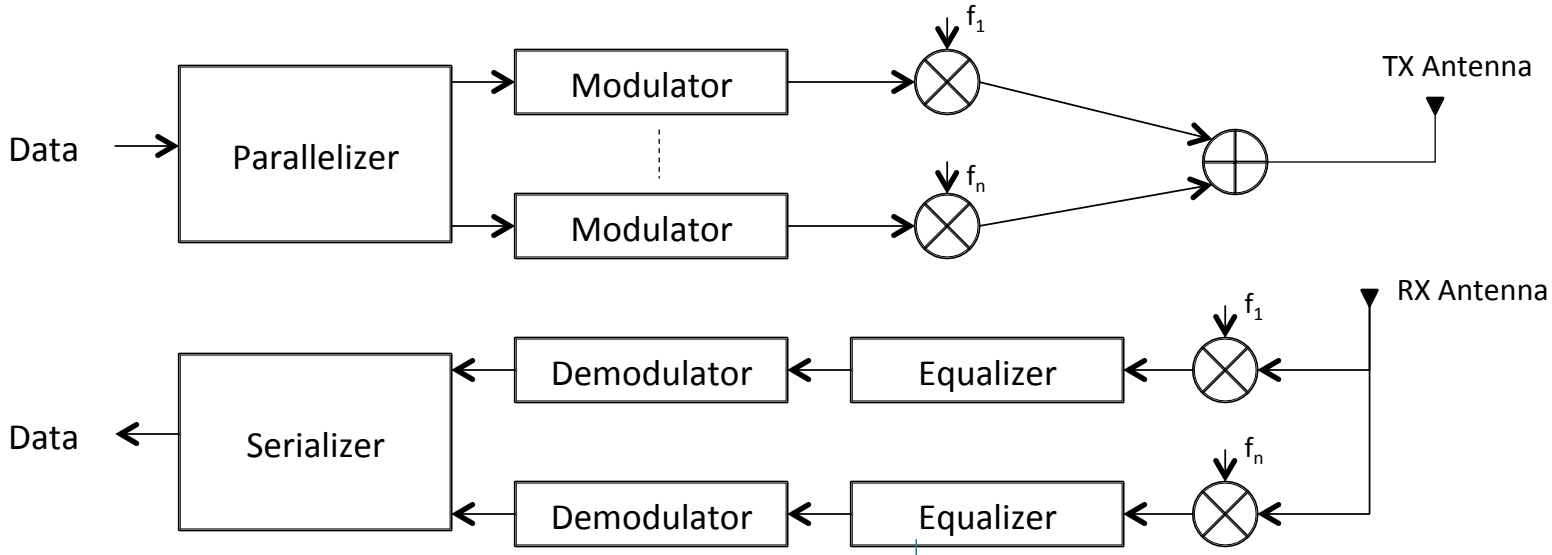
Single-Carrier Communication

- Use one frequency band for transmission



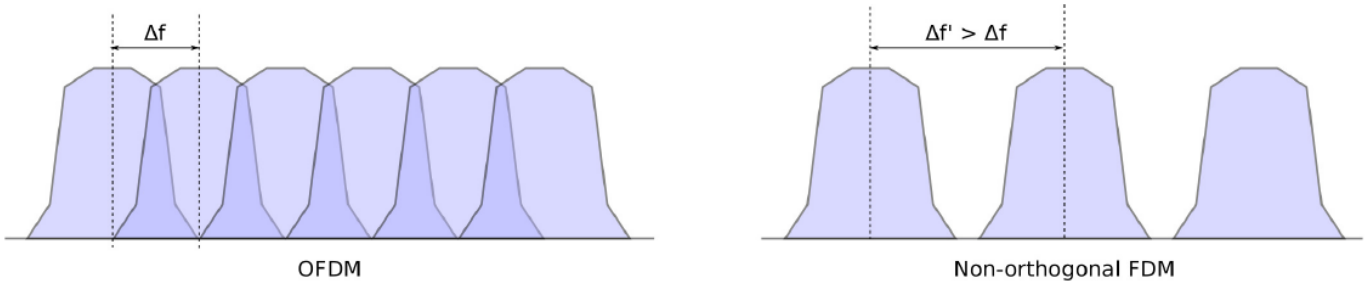
- Issues in wide band:
  - Frequency-selective fading channel
  - Short symbol period → Inter-symbol interference (ISI)
  - Requires complex equalizer

Multi-Carrier Communication



- Parallel streams: each on a single narrowband carrier
- Flat fading in each carrier → simpler equalizer
- Longer symbol period → less severe ISI

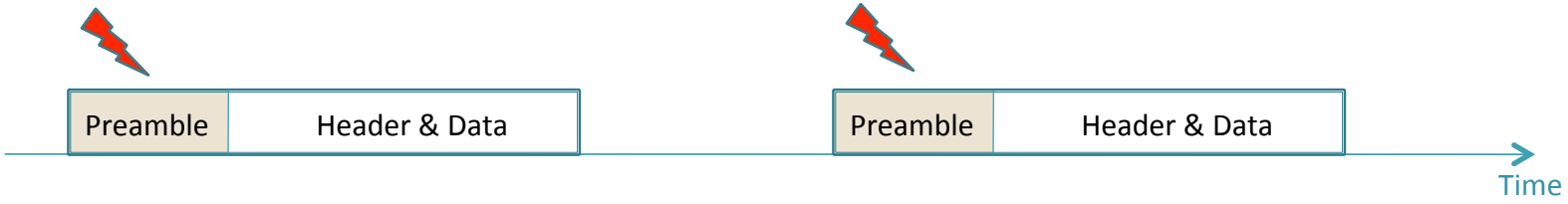
Orthogonal vs. Non-orthogonal



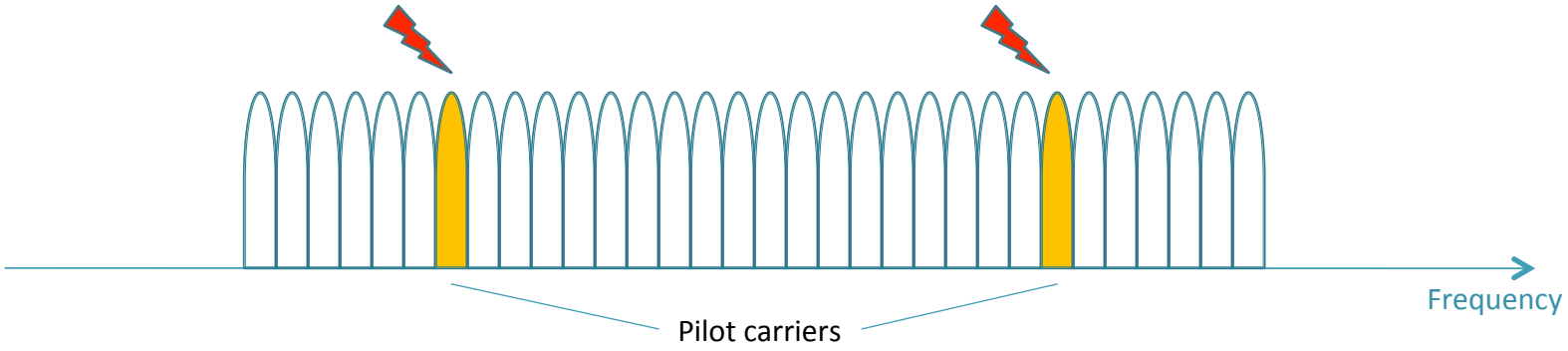
- Orthogonal Frequency Division Multiplexing:
  - Bandwidth efficiency
  - Require carriers' orthogonality
- Non-orthogonal Frequency Division Multiplexing:
  - Less bandwidth efficiency
  - Not require carriers' orthogonality

Ongoing Work

- Jamming on multi-carrier systems:
  - Attacks on time synchronization



  - Attacks on frequency synchronization



Multi-Carrier System

- Our Northeastern team's multi-carrier system won the DARPA Spectrum Challenge 2013

Summary of Future Work

- Investigate jamming techniques for multi-carrier systems
  - Analysis of weaknesses of multi-carrier systems (WiFi, LTE)
  - Practical feasibility of attacks
- Investigate protection mechanisms for multi-carrier systems
  - Based on our DSC work
- Investigate MIMO system under jamming
- Complete our CBM work

Timeline

Task	Completion date
Complete IEEE 802.11a/b/g receiver on SDR	November 2014
Investigate reactive jamming technique	December 2014
Investigate protection mechanism	January 2015
Complete CBM work	February 2015
Thesis writing and defense	April 2015

THANK YOU!

QUESTIONS?