Northeastern University

Reproducibility in Wireless Experimentation: Need, Challenges, and Approaches

Guevara Noubir

College of Computer and Information Science
Northeastern University, Boston, MA
noubir@ccs.neu.edu

Motivation for Reproducibility

- Scientific approach
  - Reproducibility is an important principle of the scientific method
  - “There is no scientific knowledge of the individual (isolated)” Aristotle
  - Modern scientific method “the foundations of knowledge should be constituted by experimentally produced facts, which can be made believable to a scientific community by their reproducibility” Robert Boyle -- wikipedia
- Credit motivates solid and far reaching research
  - “standing on the shoulders of giants” from Bernard de Chartres to Isaac Newton
- Healthy research eco-system
- Reduces waste of research resources
- Personal satisfaction

Outline

- Reproducibility in the theory community
- Biological fields
- Reproducibility in Computer Science
- Challenges in Mobile and Wireless
- Approaches including some research projects
- Conclusions

Theory

- Reproducibility is driven by providing a proof
  - Output: papers, theorems supported by proofs
- The proof enables reproducibility

Multiplication Algorithms

- From Brahmagupta to modern computer algorithms

- Trivial way: n^2
- Karatsuba O($n^{\log 3}$) [1962]
- Multiplication using Fast Fourier Transform
  - Strassen-Schonhage O($n \log(n) \operatorname{loglog}(n)$) [1971]
  - Furer $n \log(n)\, 2^{O(\log^* n)}$ [2007]
  - Harvey-van der Hoeven-Lecerf O($n \log(n)\, 2^{2 \log^* n}$) [2014]
  - …

Theoretical Computer Science

- Proofs

- Reductions of hardness
  - Complexity classes: NP-hard, polynomial hierarchy
- Approximation algorithms for optimization
  - Polynomial Time Approximation Algorithms (PTAS): 1+ ϵ within optimum
  - Constant approximation
  - Lower bounds

Examples in Theoretical Computer Science

- Traveling Salesman Problem
- Minimum Steiner Tree
- Matrix Multiplication

Biological Sciences

- A messy science
- Heavily relies on experiments
- Developed protocols for sharing and reporting results

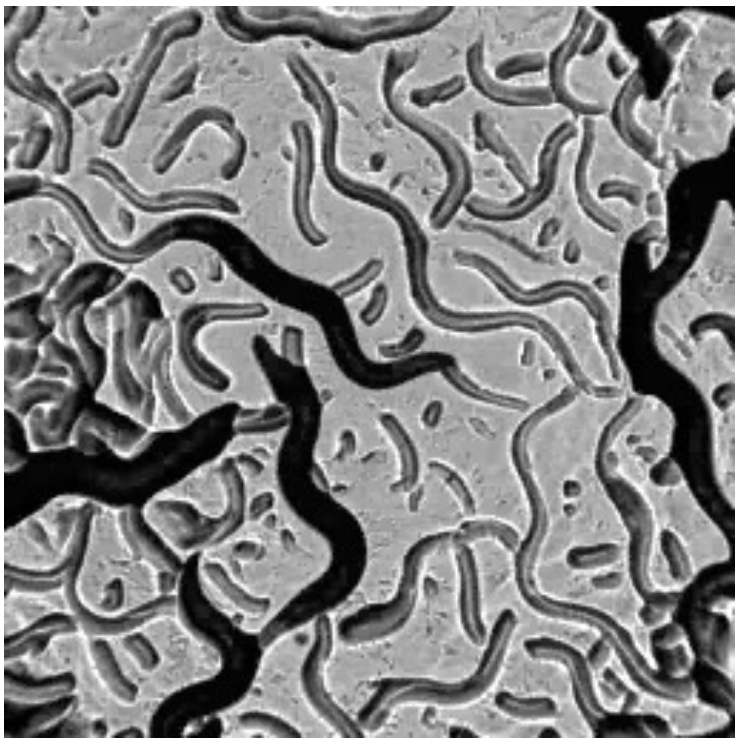
nature nanotechnology

LETTERS

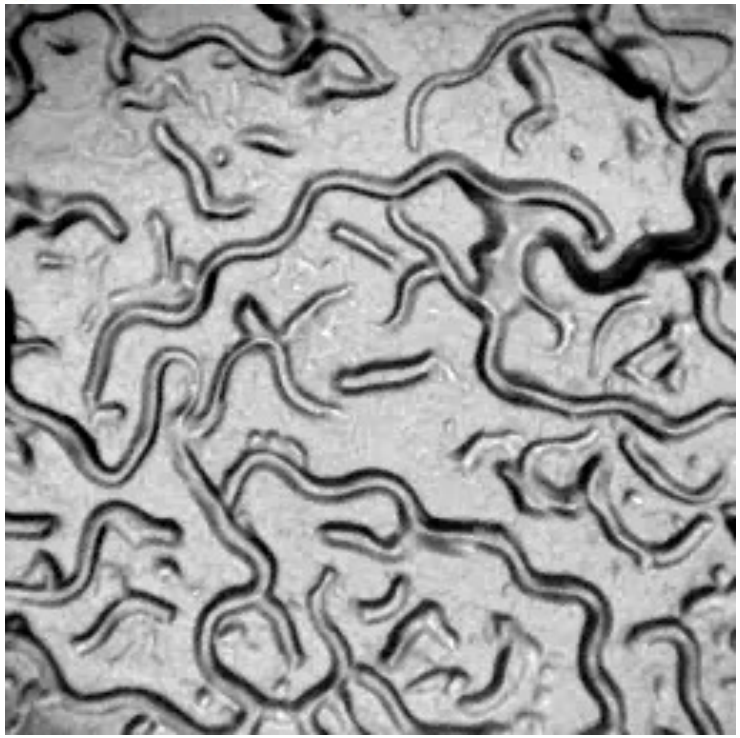
PUBLISHED ONLINE: 27 JUNE 2010 | DOI: 10.1038/NNANO.2010.125

Remote control of ion channels and neurons through magnetic-field heating of nanoparticles

Heng Huang[1], Savas Delikanli[1], Hao Zeng[1], Denise M. Ferkey[2] and Arnd Pralle[1]*



Surface labeled with PEG NPs



Negative control without NPs

- Two-step response of *C. elegans*
  - Halting of forward motion then Retraction

c. elegans freely crawling on e.coli on agarose pad, AC magnetic indicated by gray square , 5fps

Methods

Cell and *C. elegans* culture and imaging. HEK 293 cells, rat hippocampal neurons and *C. elegans* were maintained, transfected and imaged according to standard procedures (for details see Supplementary Information).

Nanoparticle synthesis and functionalization. Manganese ferrite ($MnFe_2O_4$) nanoparticles (6 nm) were synthesized according to published procedures[12]. See Supplementary Information and references[12,13] for details of synthesis. They were made water-dispersible by surface ligand exchange and coated with 2,3-dimercaptosuccinic acid (DMSA) following modified procedures by Jun and Lee[14]. $MnFe_2O_4$ nanoparticle dispersion (200 μl) in hexane was washed with methanol to remove excess surfactant oleylamine. The precipitants were redissolved in hexane and added dropwise into a DMSA solution (9 mg ml^{-1}) in methanol. The precipitated nanoparticles were washed with acetone, dried, and dissolved in 200 μl of 2.5% NH_4OH solution. The pH value of the nanoparticle aqueous solution was adjusted to 8.0 by flowing nitrogen gas above the solution to accelerate reduction of NH_4^+ to NH_3.

For further stabilization, and to provide a means for specific targeting, the nanoparticles were conjugated with streptavidin[15]. The nanoparticles were conjugated with streptavidin–DyLight-549 (Pierce) using succinimidyl-4-[*N*-maleimidomethyl]-cyclohexane-1-carboxylate (SMCC, Pierce) as cross-linker. The final hydrodynamic radius of the nanoparticles was expected to be 6 to 8 nm.

Nanoparticle targeting to cell membrane and amphid of *C. elegans*. The cells of interest were genetically labelled by expressing the engineered membrane marker protein AP-CFP-TM, which contains a transmembrane domain (TM) of the platelet-derived growth factor, an extracellular cyan fluorescent protein (CFP) and a biotin acceptor peptide (AP)[19,20]. The biotin acceptor peptide was enzymatically biotinylated by the co-expressed BirA protein, forming specific binding sites for the streptavidin-conjugated nanoparticles.

For experiments with *C. elegans*, the nanoparticles were PEG-phospholipid coated following procedures similar to those of Grancharov and colleagues[26], in which 60 μl of $MnFe_2O_4$ nanoparticle solution in hexane was washed with methanol to remove the surfactant oleylamine. The precipitants were dissolved in 650 μl of chloroform, and 60 μl of DSPE-methoxy PEG (2000) (10 mg ml^{-1}), 60 μl of maleimide-PEG (2000) (10 mg ml^{-1}) and 30 μl of DSPE-PEG (2000)-carboxy fluorescein (0.5 mg ml^{-1}) (all from Avanti Polar Lipids) were then added to the chloroform solution and mixed for 1 h in the dark. After evaporating the chloroform, the phospholipid-coated nanoparticles were dissolved in 600 μl of distilled water and incubated at 80 °C for 12 h before removing excess PEG-phospholipids.

RF magnetic-field and bulk solution heating. A 40 MHz sinusoidal signal was provided by a signal generator (Marconi Instruments), amplified by a 100 W amplifier (Amplifier Research), and applied to a 25-turn solenoid coil with a diameter of 7 mm. The magnetic field strength was adjusted between 0.67 and 1 kA m^{-1} (8.4 to 13 G). The coil was insulated with a 500-μm coating and positioned directly above the sample using a micromanipulator.

When subjected to a RF magnetic field (40 MHz, 8.4 G), the temperature in an aqueous dispersion of the DMSA-coated nanoparticles (20 mg ml^{-1}) increased at an initial rate of 0.62 °C s^{-1}, as measured with a thermocouple. This heating corresponds to a specific absorption rate (SAR) of 2.51 J g^{-1} s^{-1} (Supplementary Fig. S1).

Local heat quantification. Local temperature changes were measured by recording the changes in fluorescence intensity of fluorophores (DyLight549, YFP or ANNINE6), subtracting the bleach rate, and converting it into a temperature change based on the measured temperature dependence of the fluorescence intensity. The $\Delta F(T)/F(T_0)$ of these fluorophores are −1.5% for DyLight549, −1.3% for YFP, −0.81% for ANNINE6 and −1.2% for fluorescein (Supplementary Fig. S3).

Received 7 March 2010; accepted 19 May 2010;
published online 27 June 2010

Supplementary

- 10 pages making every step explicit

nature nanotechnology
SUPPLEMENTARY INFORMATION
DOI: 10.1038/NNANO.2010.125

"Remote control of ion-channels and neurons through magnetic field heating of nanoparticles"

Heng Huang, Savas Delikanli, Hao Zeng, Denise M. Ferkey, Arnd Pralle

SUPPLEMENTARY INFORMATION

Supplementary Methods

Nanoparticle Synthesis and Functionalization

A mixture of 2 mM of $Fe(acac)_3$, 1 mM of $Mn(acac)_2$, 10 mM of 1,2-hexadecandiol, 6 mM of oleic acid, 6 mM of oleylamine and 25 ml of benzyl ether was heated and maintained at 110° C for 1 hr under N_2 flow. The temperature was then raised to 210° C for 2 hrs. Under N_2 blanketing, the mixture was heated to a reflux temperature of about 295° C, and kept refluxing for 1 hr. The solution mixture was cooled to room temperature, and the nanoparticles were precipitated by adding ethanol, before being dissolved in hexane (More details in [1,2]).

Cell Culture

Human embryonic kidney (HEK 293) cells were cultured in Dulbecco's modified Eagle's medium (DMEM) supplemented with 10% fetal bovine serum and 1% penicillin-streptomycin (Invitrogen) at 37°C under 5% CO_2. For imaging, the cells were plated sparsely on 35-mm glass coverslips. Transfections were performed 24 h after plating using Lipofectamine 2000 (Invitrogen). For calcium imaging, cells were co-transfected with equal amount of plasmids encoding TRPV1 (in pcDNA vector), TN-XL (pcDNA) [23] and AP-CFP-TM (pDISPLAY)[3] (0.4 μg each). 24 h after transfection, a mixture of BirA enzyme (2 μM) and biotin (5 μM) was added to the cell culture media[4,5]. After incubation at 37°C for 30 min, the cells were washed 3 times with Phosphate Buffered Saline (PBS) solution and incubated with Streptavidin-DyLight

[1] Zeng, H., Rice, P. M., Wang, S. X. & Sun, S. Shape-controlled synthesis and shape-induced texture of MnFe2O4 nanoparticles. *J Am Chem Soc* 126, 11458-11459 (2004).
[2] Sun, S. *et al.* Monodisperse MFe2O4 (M = Fe, Co, Mn) nanoparticles. *J Am Chem Soc* 126, 273-279 (2004).
[3] Howarth, M. *et al.* A monovalent streptavidin with a single femtomolar biotin binding site. *Nat Methods* 3, 267-273 (2006)
[4] Howarth, M., Takao, K., Hayashi, Y. & Ting, A. Y. Targeting quantum dots to surface proteins in living cells with biotin ligase. *Proc Natl Acad Sci U S A* 102, 7583-7588 (2005).
[5] Howarth, M. & Ting, A. Y. Imaging proteins in live mammalian cells with biotin ligase and monovalent streptavidin. *Nat Protoc* 3, 534-545 (2008).

Reproducibility in Applied CS

- Databases
- Computer Vision
- Artifacts Evaluations

ACM SIGMOD 2016 Reproducibility

What is SIGMOD Reproducibility?

SIGMOD Reproducibility has three goals:

- Highlight the impact of database research papers.
- Enable easy dissemination of research results.
- Enable easy sharing of code and experimentation set-ups.

Reproducible Label

The experimental results of the paper were reproduced by the committee and were found to support the central results reported in the paper. The experiments (data,code,scripts) are made available to the community.

> The "Reproducible label" will be visible in the **ACM digital library**.

- Process takes 1.5 months

ACM SIGMOD 2016 Reproducibility

Readme for reproducibility submission of paper

A) Source code info

Repository: [url]
Programming Language: [C/C++/java/...]
Additional Programming Language info: [optional, e.g., java version]
Compiler Info: [full details of compiler and version]
Packages/Libraries Needed: [an as thorough as possible list of software packages needed]

B) Datasets info

Repository: [url]
Data generators: [url]

C) Hardware Info[Here you should include any details and comments about the used hardware in order to be able to accommodate the reproducibility effort. Any information about non-standard hardware should also be included. You should also include at least the following info:]

C1) Processor (architecture, type, and number of processors/sockets)
C2) Caches (number of levels, and size of each level)
C3) Memory (size and speed)
C4) Secondary Storage (type: SSD/HDD/other, size, performance: random read/sequnetial read/random write/sequnetial write)
C5) Network (if applicable: type and bandwidth)

D) Experimentation Info

D1) Scripts and how-tos to generate all necessary data or locate datasets[Ideally, there is a script called: ./prepareData.sh]
D2) Scripts and how-tos to prepare the software for system[Ideally, there is a script called: ./prepareSoftware.sh]
D3) Scripts and how-tos for all experiments executed for the paper[Ideally, there is a script called: ./runExperiments.sh]

Computer Vision: Face Detection

Face detection without bells and whistles

ECCV'2014

Markus Mathias [1] Rodrigo Benenson [2] Marco Pedersoli [1] Luc Van Gool [1,3]

- "Due to the lack of a commonly accepted annotation guidelines and evaluation protocols, a fair evaluation of face detectors on various data sets is still missing"

– We point out that the evaluation of existing face datasets is biased due to different guidelines for the annotation. We provide improved annotations and a new evaluation criteria that copes better with these problems (section 2).

– We show that (despite common belief) face detection has not saturated, and there are still relevant open questions to explore (section 6).

Artifacts Evaluation

- ACM terminology inspired by (Metrology)
  - Repeatability (Same team, same experimental setup)
  - Replicability (Different team, same experimental setup)
  - Reproducibility (Different team, different experimental setup)
- Artifacts Evaluation Committee
  - Still optional for accepted papers
  - Few weeks
- Several conferences
  - CAV, PLDI

Challenges in Mobile and Wireless

- Much harder problem

- The propagation channel is difficult to control and reproduce
  - Surrounding objects, their mobility, temperature, rain, wind, other communications

Some of the Approaches

- Theory approach
  - Assume a model and prove properties
  - UDG, AWGN, or random gains matrix
  - Do not provide much insight into real world performance
  - Models should derive from experimental measurements
- Simulations
  - Physical layer
  - All stack discrete event simulator
  - Limitations: scale and accuracy
- Emulation
- Live experimental measurements

Simulations

- Communications/standardisation community had procedures for evaluating performance

- Recommendation ITU-R M.1225 [1997]
  - Guidelines for evaluation of radio transmission technologies for imt-2000
  - 60 pages document

RECOMMENDATION ITU-R M.1225

GUIDELINES FOR EVALUATION OF RADIO TRANSMISSION TECHNOLOGIES FOR IMT-2000

(Question ITU-R 39/8)

(1997)

CONTENTS

1 Introduction

International Mobile Telecommunications-2000 (IMT-2000) are third generation mobile systems which are scheduled to start service around the year 2000 subject to market considerations. They will provide access, by means of one or more radio links, to a wide range of telecommunication services supported by the fixed telecommunication networks (e.g. PSTN/ISDN), and to other services which are specific to mobile users.

A range of mobile terminal types is encompassed, linking to terrestrial and/or satellite based networks, and the terminals may be designed for mobile or fixed use.

Key features of IMT-2000 are:

– high degree of commonality of design worldwide,

– compatibility of services within IMT-2000 and with the fixed networks,

– high quality,

– use of a small pocket terminal with worldwide roaming capability.

IMT-2000 will operate worldwide in bands identified by Radio Regulations provision No. S5.388 (1 885-2 025 and 2 110-2 200 MHz, with the satellite component limited to 1 980-2 010 and 2 170-2 200 MHz). IMT-2000 are defined by a set of interdependent ITU Recommendations, of which this Recommendation is a member.

It is a design objective of IMT-2000 that the number of radio interfaces should be minimal and, if more than one interface is required, that there should be a high degree of commonality between them. These radio interfaces will serve the radio operating environments as nominated in Recommendation ITU-R M.1034. A number of sets of radio transmission technologies (SRTTs) may meet the requirements for the radio interfaces. This Recommendation contains the procedure and criteria that will be used to evaluate candidate radio transmission technologies (RTTs).

The subject matter of IMT-2000 is complex and its representation in the form of Recommendations is evolving. To maintain the pace of progress on the subject it is necessary to produce a sequence of Recommendations on a variety of aspects. The recommendations strive to avoid apparent conflicts between themselves. Nevertheless, future Recommendations, or revisions, will be used to resolve any discrepancies.

2 Scope

This Recommendation provides guidelines for both the procedure and the criteria to be used in evaluating RTTs for a number of test environments. These test environments, defined herein, are chosen to simulate closely the more stringent radio operating environments. The evaluation procedure is designed in such a way that the impact of the candidate RTTs on the overall performance and economics of IMT-2000 may be fairly and equally assessed on a technical basis. It ensures that the overall IMT-2000 objectives are met.

The Recommendation provides, for proponents and developers of RTTs, the common bases for the submission and evaluation of RTTs and system aspects impacting the radio performance.

ITU-R M.1225 [1997]

7 Selected test environments for evaluation

The test environments for evaluation are discussed in Annex 2. The selected test operating environments are the following:

- indoor office,
- outdoor to indoor and pedestrian,
- vehicular,
- mixed-cell pedestrian/vehicular,
- satellite.

The key parameters to describe each propagation model would include:

- time delay-spread, its structure, and its statistical variability (e.g. probability distribution of time delay spread);
- geometrical path loss rule (e.g. R^{-4}) and excess path loss;
- shadow fading;
- multipath fading characteristics (e.g. Doppler spectrum, Rician vs. Rayleigh) for the envelope of channels;
- operating radio frequency.

1.2.1.1 Path loss model for indoor office test environment

The indoor path loss model (dB) is in the following simplified form, which is derived from the COST 231 indoor model presented in Appendix 1. This low increase of path loss versus distance is a worst-case from the interference point of view:

$$L = 37 + 30 \log_{10} R + 18.3\, n^{\left(\frac{n+2}{n+1} - 0.46\right)}$$

where:

R: transmitter-receiver separation (m)

n: number of floors in the path.

NOTE 1 – L shall in no circumstances be less than free space loss. A log-normal shadow fading standard deviation of 12 dB can be expected.

1.2.1.2 Path loss model for outdoor to indoor and pedestrian test environment

The following model should be used for the outdoor to indoor and pedestrian test environment:

$$L = 40 \log_{10} R + 30 \log_{10} f + 49$$

where:

R: base station – mobile station separation (km)

f: carrier frequency of 2 000 MHz for IMT-2000 band application.

NOTE 1– L shall in no circumstances be less than free space loss. This model is valid for non-line-of-sight (NLOS) case only and describes worse case propagation. Log-normal shadow fading with a standard deviation of 10 dB for outdoor users and 12 dB for indoor users is assumed. The average building penetration loss is 12 dB with a standard deviation of 8 dB.

1.2.1.3 Path loss model for vehicular test environment

This model, based on the same general format as in § 1.2.1.2, is applicable for the test scenarios in urban and suburban areas outside the high rise core where the buildings are of nearly uniform height:

$$L = 40\,(1 - 4 \times 10^{-3}\, \Delta h_b) \log_{10} R - 18 \log_{10} \Delta h_b + 21 \log_{10} f + 80 \quad \text{dB}$$

where:

R: base station – mobile station separation (km)

f: carrier frequency of 2 000 MHz

Δh_b: base station antenna height (m), measured from the average rooftop level.

To quantitatively evaluate each RTT, the base station antenna height is fixed at 15 m above the average rooftop (Δh_b = 15 m). Each proponent has an option to specify an alternate base station antenna height to optimize coverage and spectrum efficiency in their proposal.

NOTE 1 – L shall in no circumstances be less than free space loss. This model is valid for NLOS case only and describes worse case propagation. Log-normal shadow fading with 10 dB standard deviation are assumed in both urban and suburban areas.

NOTE 2 – The path loss model is valid for a range of Δh_b from 0 to 50 m.

1.2.1.4 Decorrelation length of the long-term fading

The long-term (log-normal) fading in the logarithmic scale around the mean path loss L (dB) is characterized by a Gaussian distribution with zero mean and standard deviation. Due to the slow fading process versus distance Δx, adjacent fading values are correlated. Its normalized autocorrelation function $R(\Delta x)$ can be described with sufficient accuracy by an exponential function (Gudmundson, M. [7 November, 1991] Correlation Model for Shadow Fading in Mobile Radio Systems. *Electron. Lett.*, Vol. 27, **23**, 2145-2146):

$$R(\Delta x) = e^{-\frac{|\Delta x|}{d_{cor}} \ln 2}$$

with the decorrelation length d_{cor}, which is dependent on the environment. This concept can be applied in the vehicular test environment with a decorrelation length of 20 m.

1.2.2 Channel impulse response model

For each terrestrial test environment, a channel impulse response model based on a tapped-delay line model is given. The model is characterized by the number of taps, the time delay relative to the first tap, the average power relative to the strongest tap, and the Doppler spectrum of each tap. A majority of the time, r.m.s. delay spreads are relatively small, but occasionally, there are "worst case" multipath characteristics that lead to much larger r.m.s. delay spreads. Measurements in outdoor environments show that r.m.s. delay spread can vary over an order of magnitude, within the same environment. Although large delay spreads occur relatively infrequently, they can have a major impact on system performance. To accurately evaluate the relative performance of candidate RTTs, it is desirable to model the variability of delay spread as well as the "worst case" locations where delay spread is relatively large.

As this delay spread variability cannot be captured using a single tapped delay line, up to two multipath channels are defined for each test environment. Within one test environment channel A is the low delay spread case that occurs frequently, channel B is the median delay spread case that also occurs frequently. Each of these two channels is expected to be encountered for some percentage of time in a given test environment. Table 2 gives percentage of time the particular channel may be encountered with the associated r.m.s. average delay spread for channel A and channel B for each terrestrial test environment.

TABLE 2

Parameters for channel impulse response model

Test environment	Channel A		Channel B	
	r.m.s. (ns)	*P* (%)	r.m.s. (ns)	*P* (%)
Indoor office	35	50	100	45
Outdoor to indoor and pedestrian	45	40	750	55
Vehicular – high antenna	370	40	4 000	55

Tables 3 to 5 describe the tapped-delay-line parameters for each of the terrestrial test environments. For each tap of the channels three parameters are given: the time delay relative to the first tap, the average power relative to the strongest tap, and the Doppler spectrum of each tap. A small variation, ±3%, in the relative time delay is allowed so that the channel sampling rate can be made to match some multiple of the link simulation sample rate.

Simulations in Wireless Networking

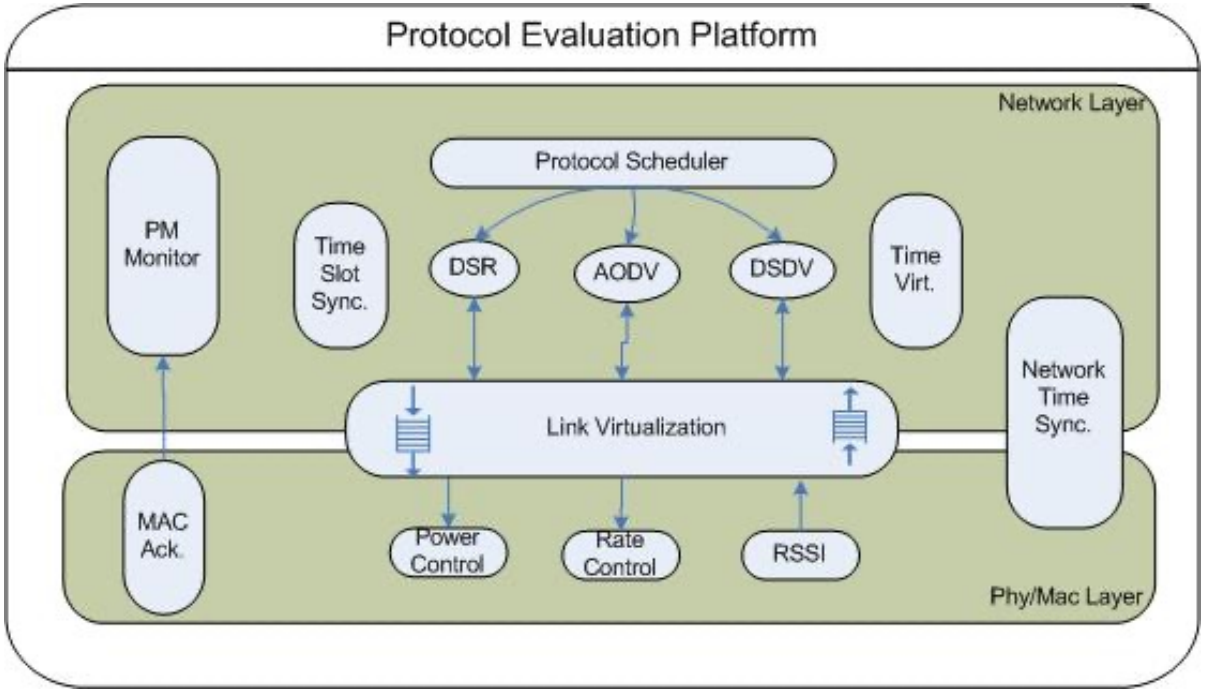
- Networking community
  - Expertise in simulating data networks (discrete event simulator)
- Issues with simulators for wireless networks
  - Accuracy of physical/link layer models
- Results cannot be always reproduced across simulators
  - Even for a simple flooding protocol
  - Opnet, Glomosim, NS-2 [Cavin, Sasson, Schiper 2002]

Comparing in Fairness

- Even if we give-up on reproducibility can we at least compare the performance
  - Realistic environments
  - Similar conditions

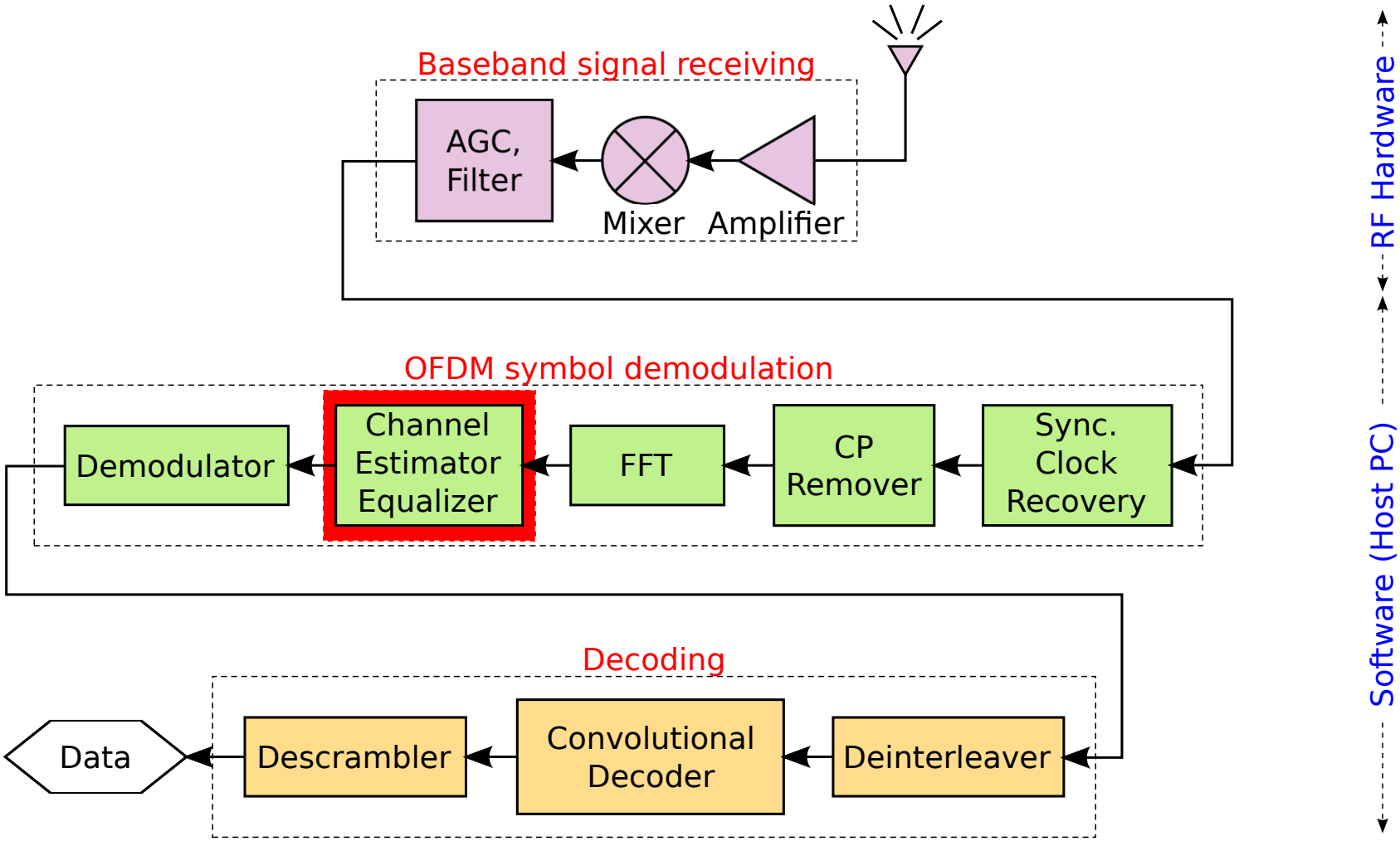
Wireless Network Virtualization [2007]

- Enable cross-layer protocols
  - Phy/MAC parameters control & channel assessment
- Protocols switching for performance comparison under similar environment conditions
- SPREAD at MAC and Routing layers



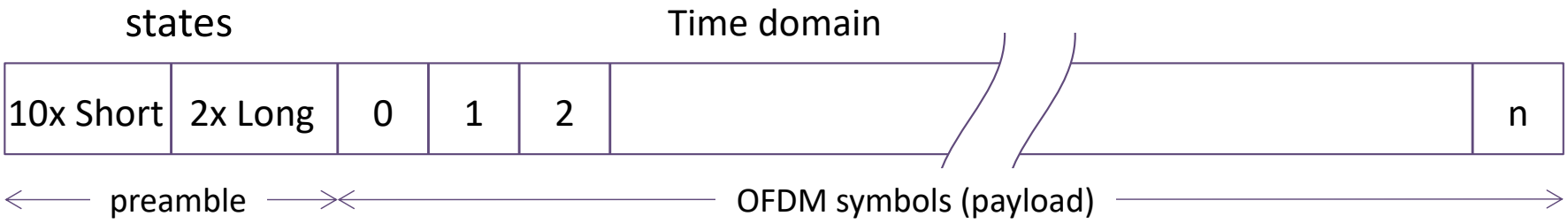
SWiFi: an SDR IEEE 802.11agb

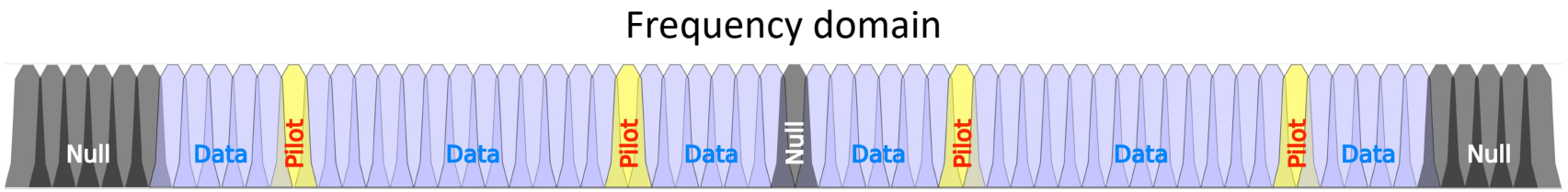
SWiFi Receiver Design



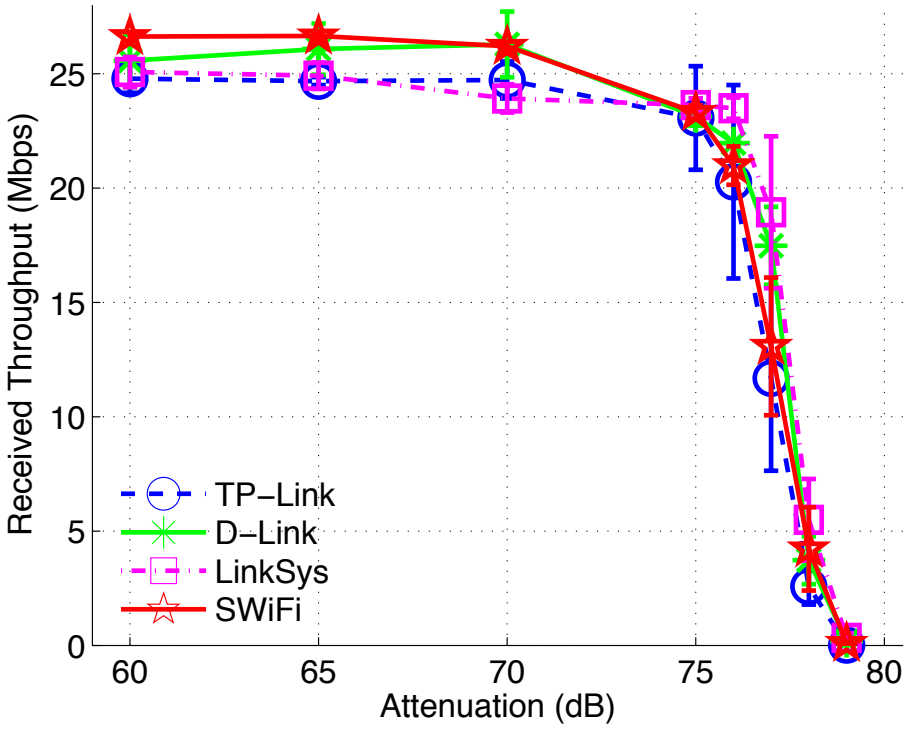
Channel Estimation and Equalization

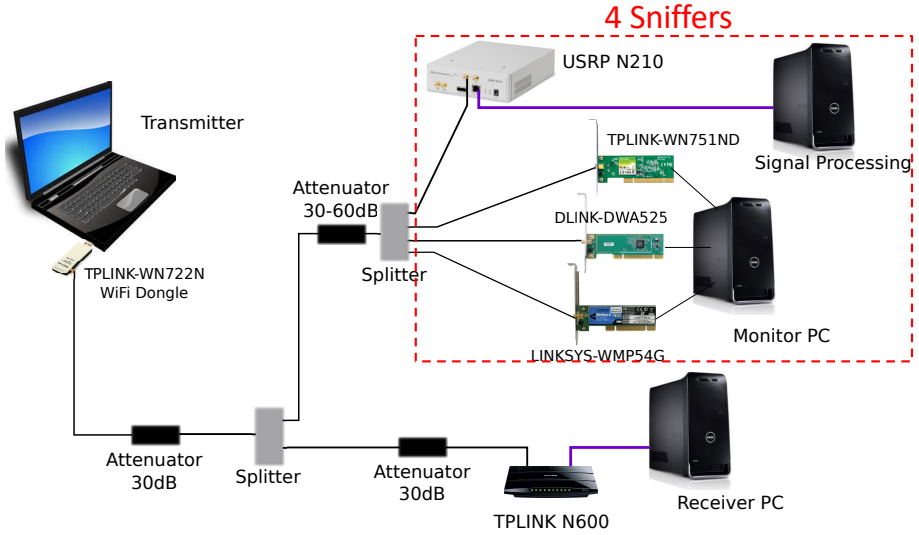
- Preambled-based frequency offset correction
  - Coarse estimation: using short preamble symbols
  - Fine estimation: using long preamble symbols
- Initial channel estimation: using long preamble symbols
- Update channel:
  - Phase correction using pilot subcarriers
  - Decision-directed update: demodulate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



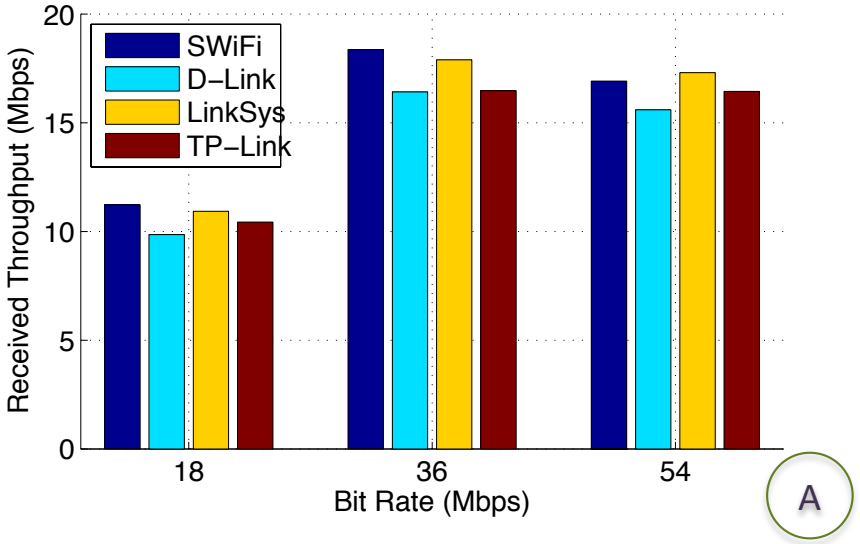


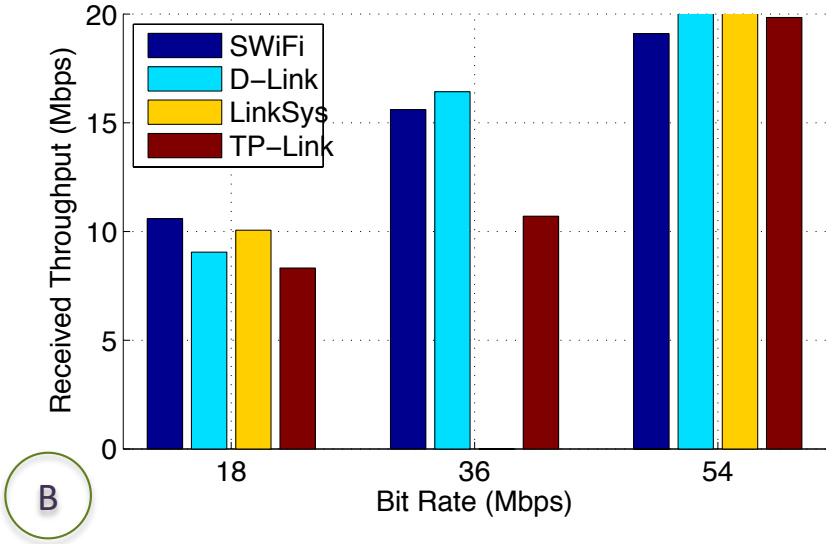
Throughput Comparison (Controlled Attenuation)

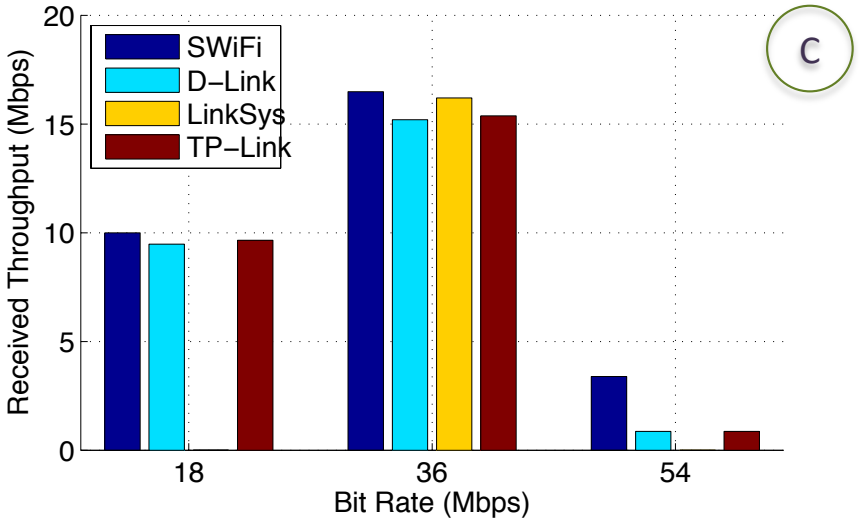


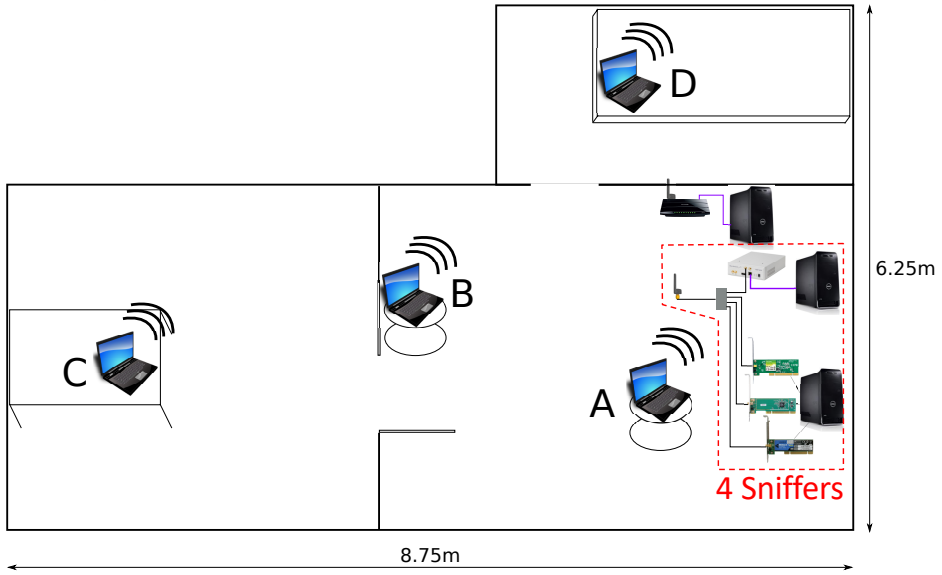


Throughput Comparison (Wireless Setup)







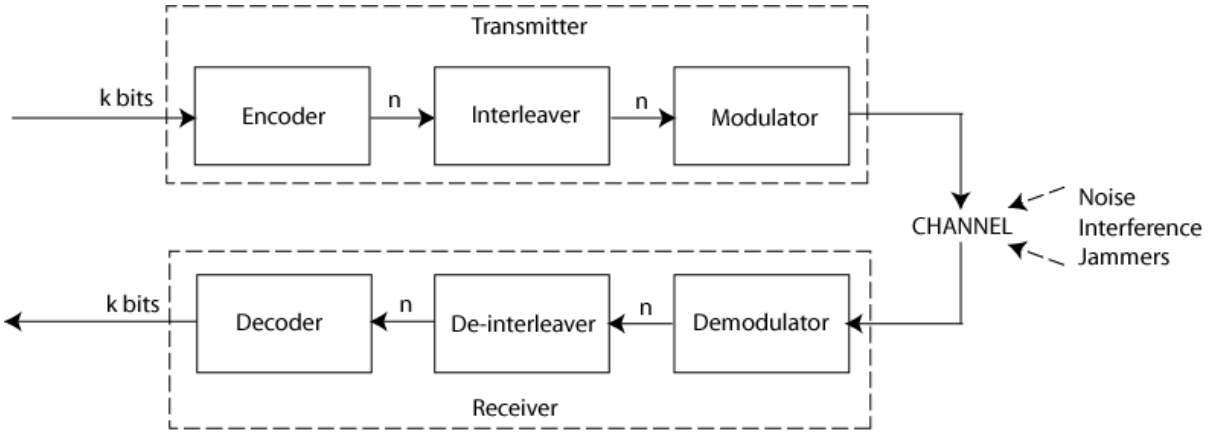


Analyzing Smart-Jamming in 802.11

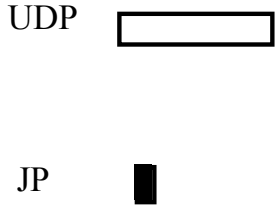
[ACM WiSec'16]

Jamming Generic Data Packets [Noubir & Lin 2003]

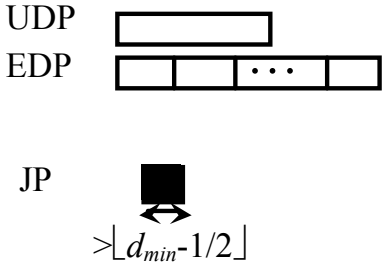
Link Architecture



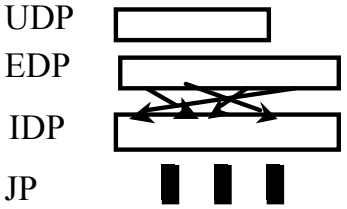
Jamming Unreliable Communication



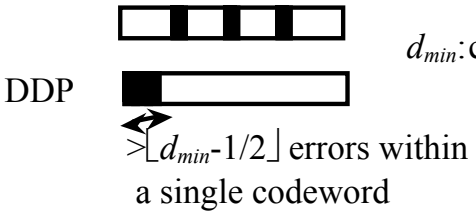
Jamming ECC Protected Communication



Jamming Interleaved ECC Protected Communication



UDP: Uncoded Data Packet
JP: Jamming Packet
EDP: Encoded Data Packet in l codewords
RP: Received Packet
IDP: Interleaved Data Packet
DDP: De-Interleaved Packet

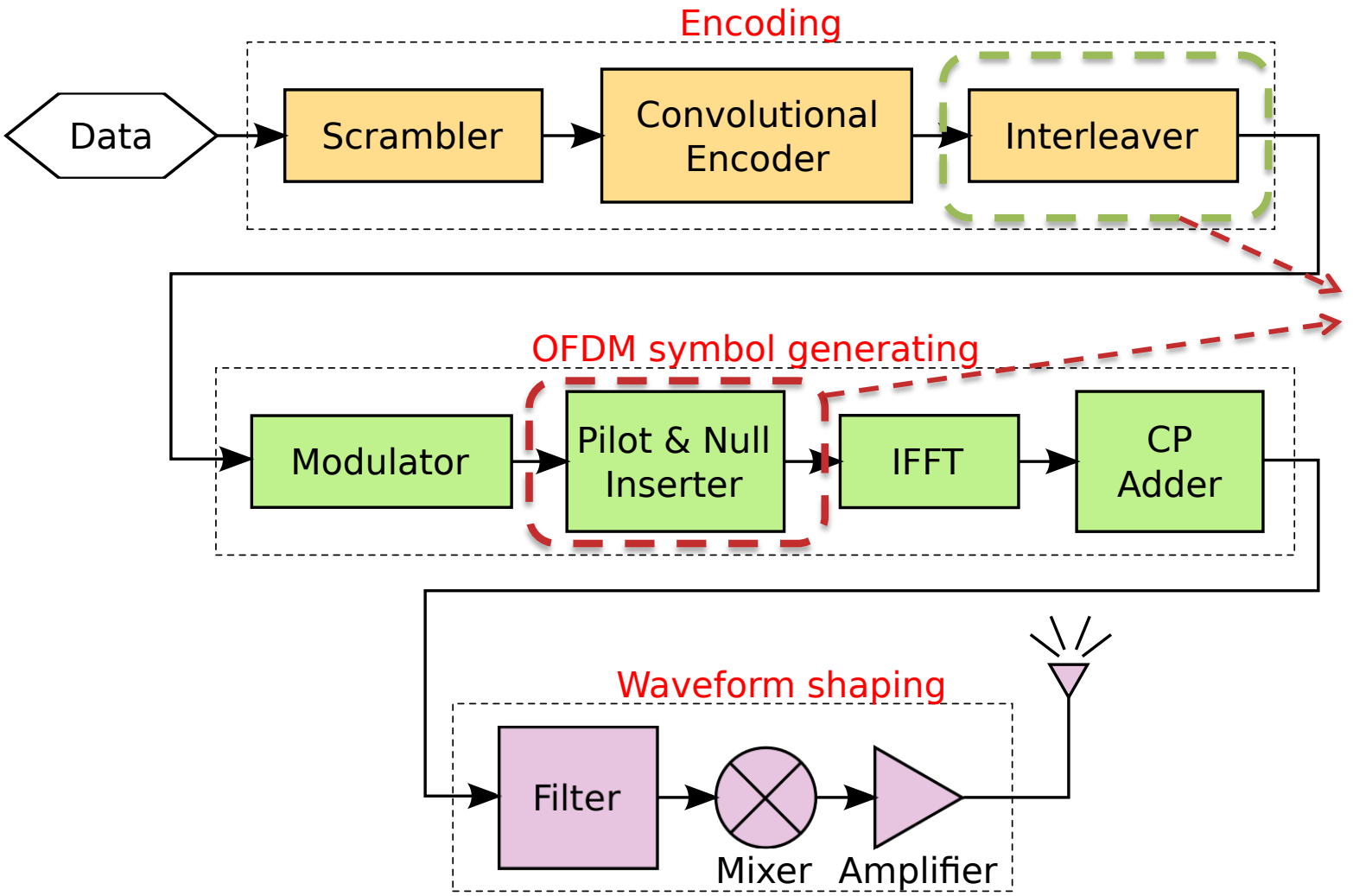


d_{min}: code minimum Hamming distance

Challenge: time synchronization

Solution: use cryptographic interleaving

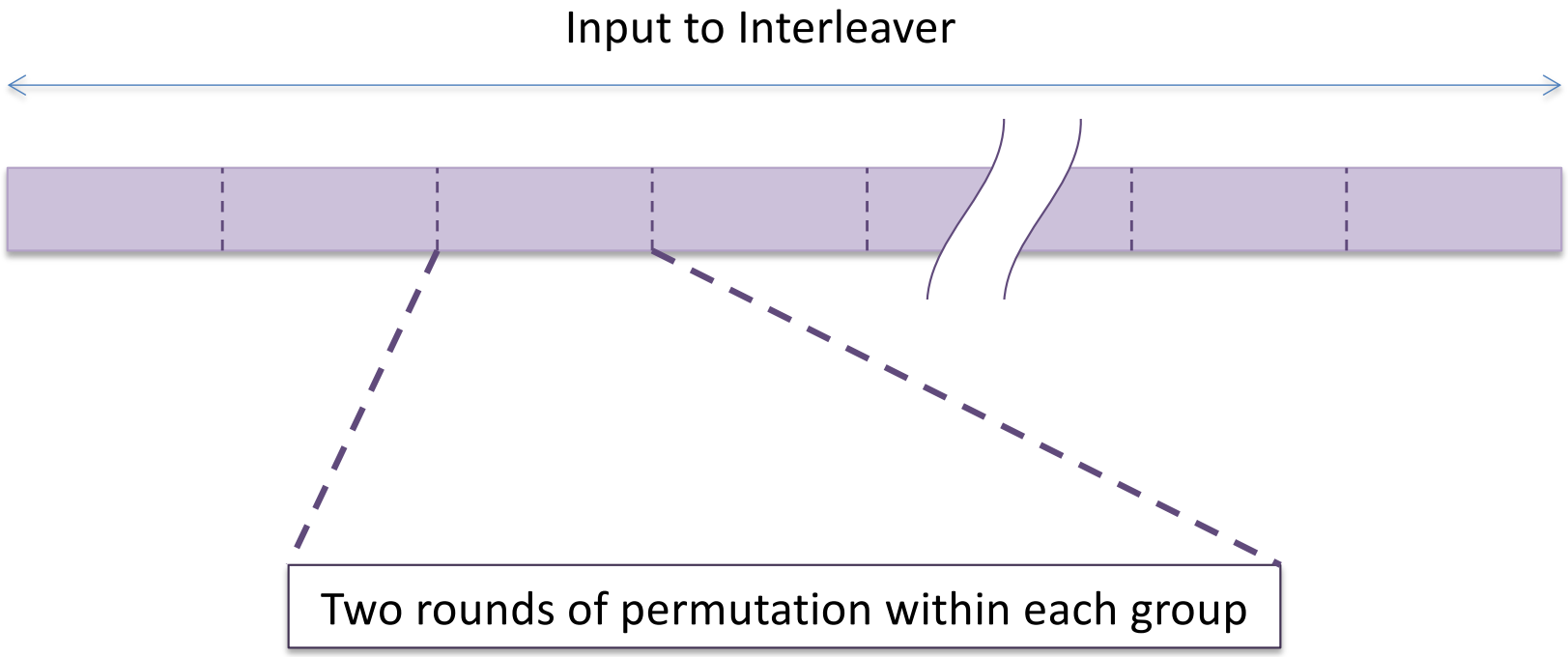
Wi-Fi Transmit Chain



Focus of This Jamming Study

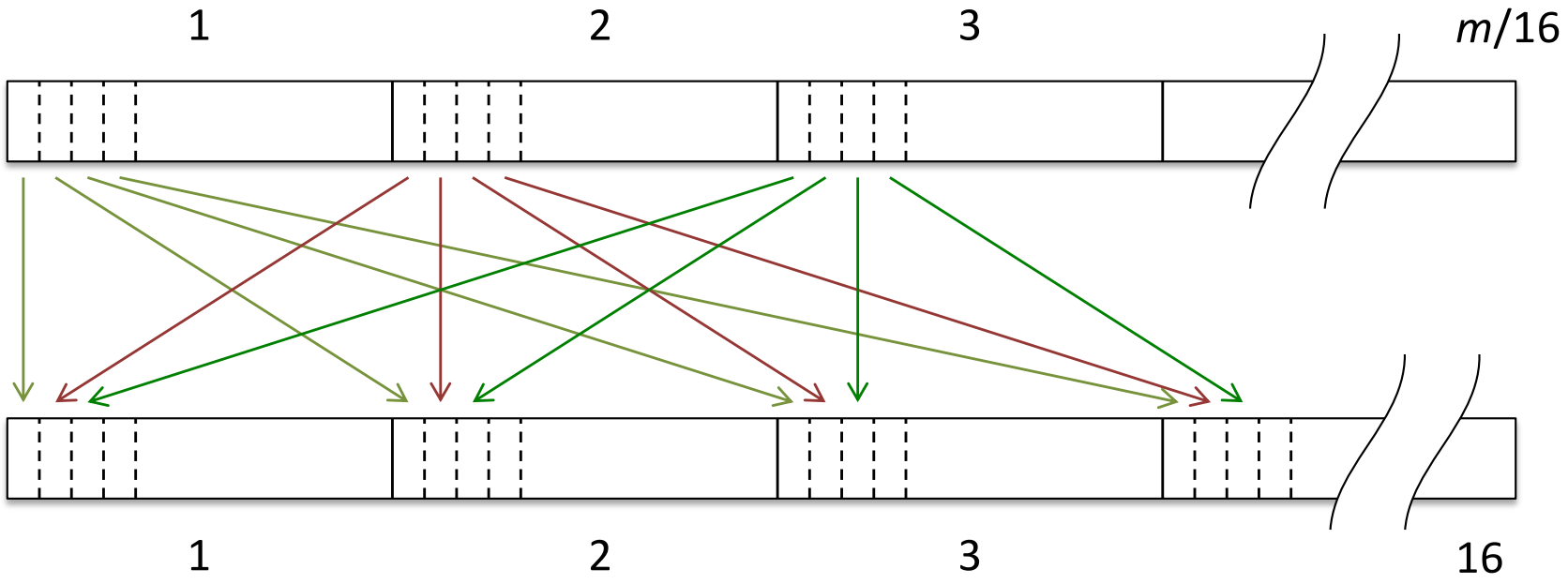
Interleaving Mechanism

- Dividing coded bit sequence (Convolutional Encoder's output) into multiple same-size groups $m = 48b$
  - *b* is number of bits per subcarrier (e.g., BPSK: *b* = 1)



Interleaving Mechanism – First Round

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



$$K' = (K \bmod 16)\frac{m}{16} + \lfloor K/16 \rfloor$$

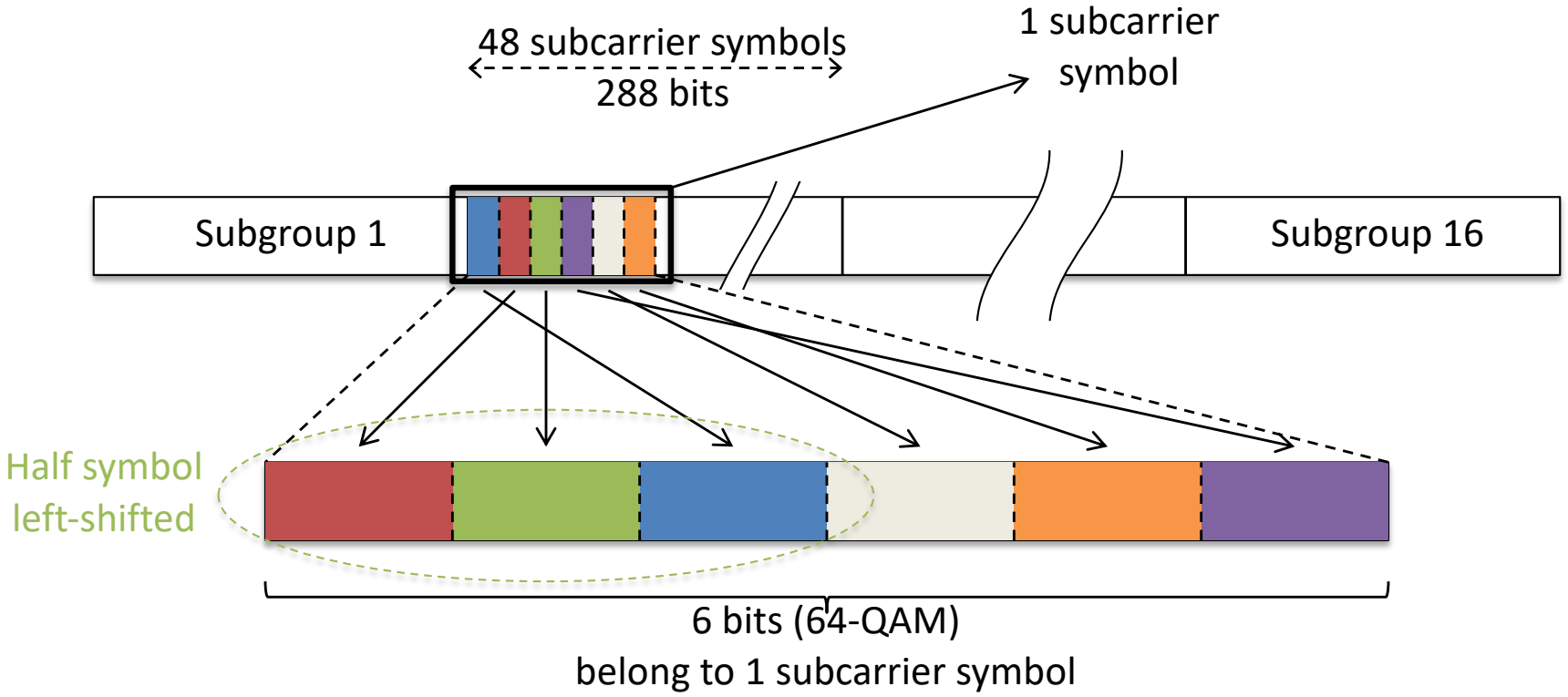
Interleaving Mechanism – Second Round

- Goal: permuting adjacent bits within every subcarrier symbol
  - Rule: cyclically shifting each half symbol

$$K'' = s\lfloor \frac{K'}{s} \rfloor + (K' + m - \lfloor 16\frac{K'}{m} \rfloor) \bmod s$$

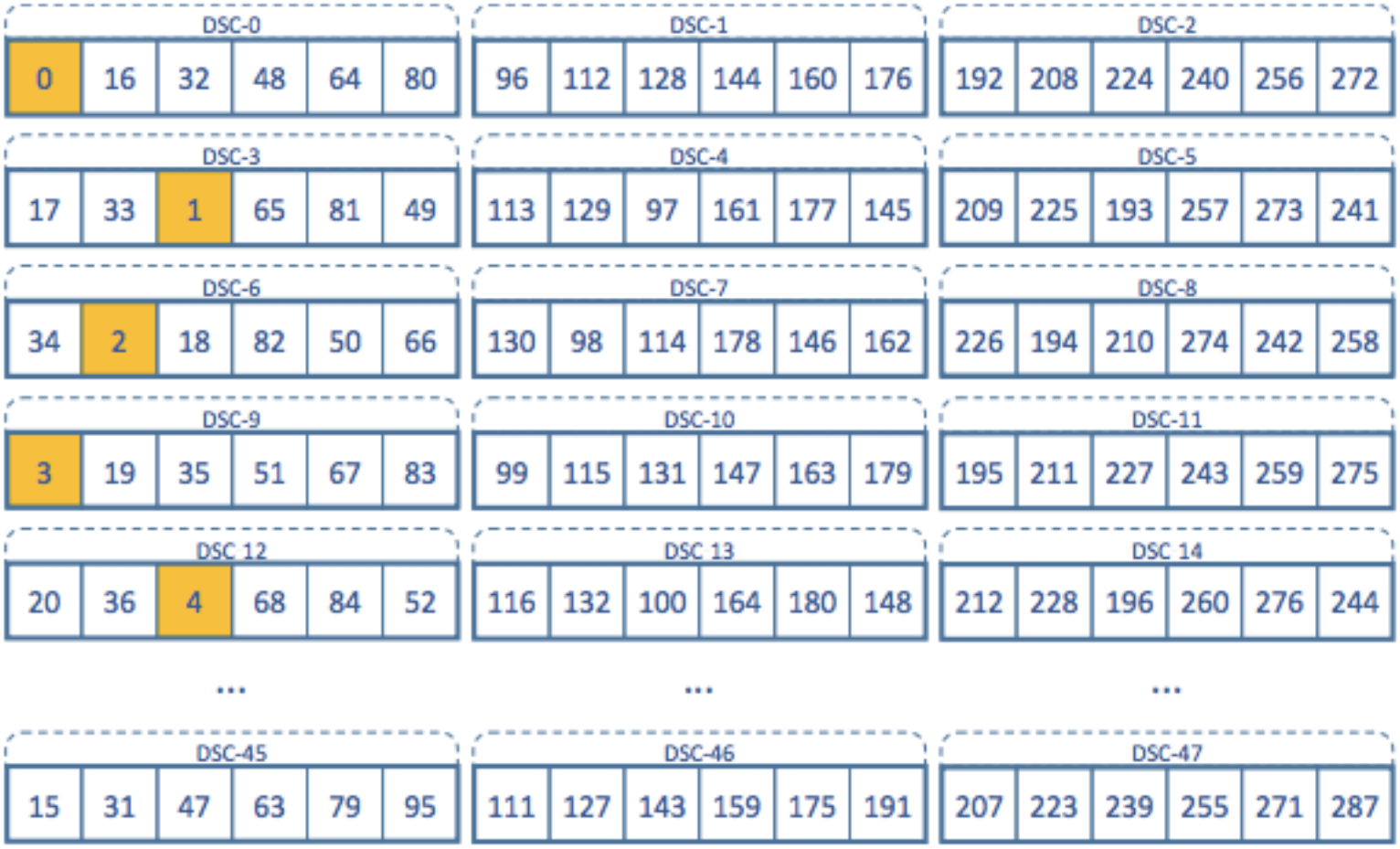
$s = \max(b/2, 1)$

- Example: 64-QAM, 1-bit left shift for each half of a symbol



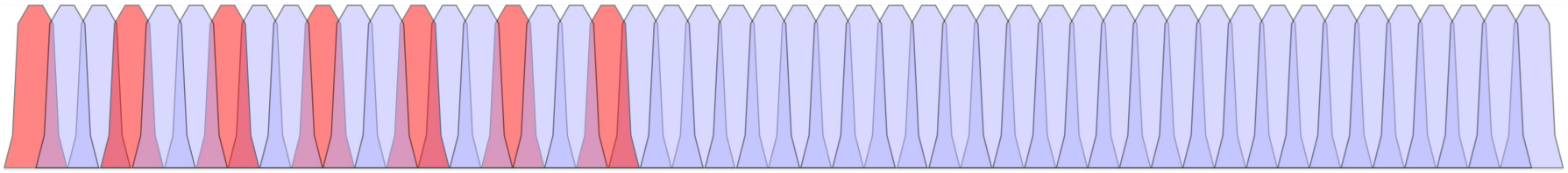
Example of Interleaving Pattern

- 64-QAM Modulation



IEEE 802.11 Interleaving

- Theorem: In IEEE 802.11, any two data subcarriers, whose distance is either 3 or 45, always consist of at least two bits originally located adjacently in the coded data sequence.



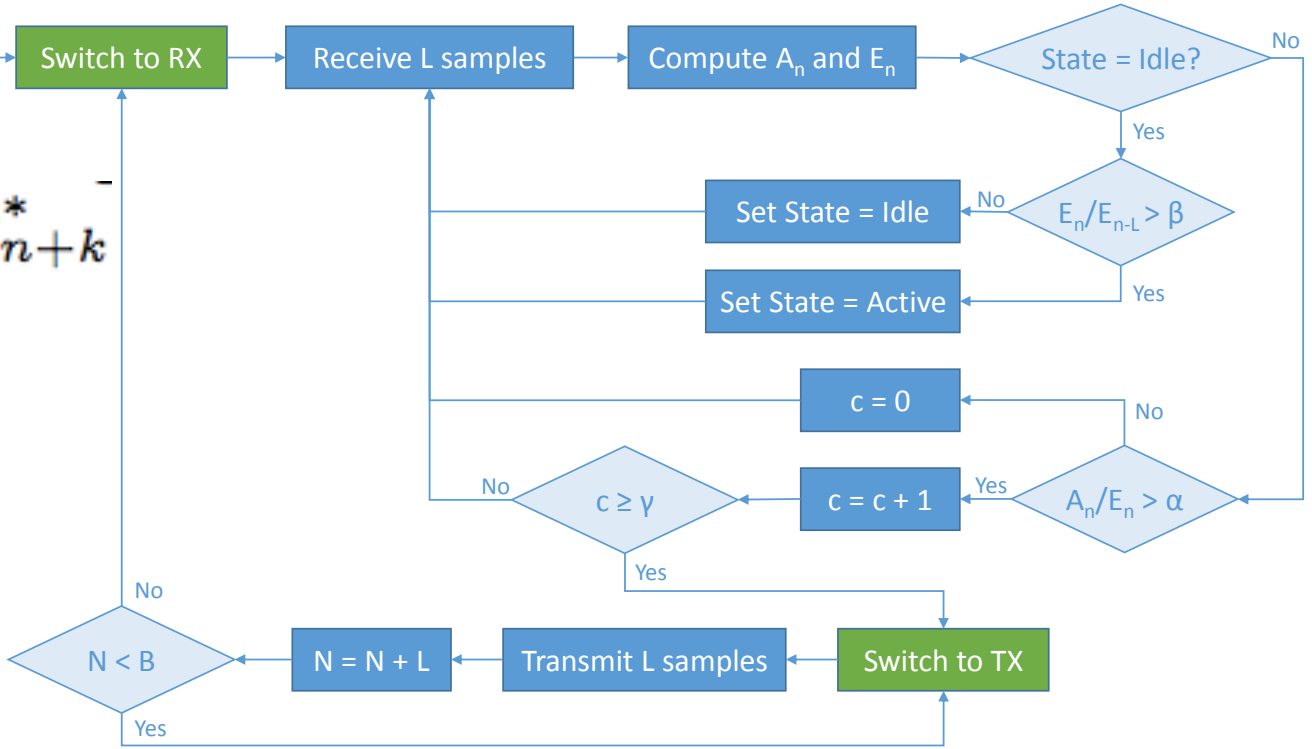
Real-time Jammer

- Built on HackRF One (NXP LPC4320 with Cortex M4 204MHz processor)
- Efficient frame detection and jamming burst using SIMD

$$\{r_n\} = \underbrace{\ldots\ldots\ldots\ldots}_{\text{inter-frame spacing}}, \underbrace{\hat{p}_1, \ldots, \hat{p}_L, \hat{p}_{L+1}, \ldots, \hat{p}_{2L}, \ldots}_{\text{preamble starting with 10 short patterns}}, \underbrace{\ldots, \hat{x}_k, \ldots}_{\text{data}}$$

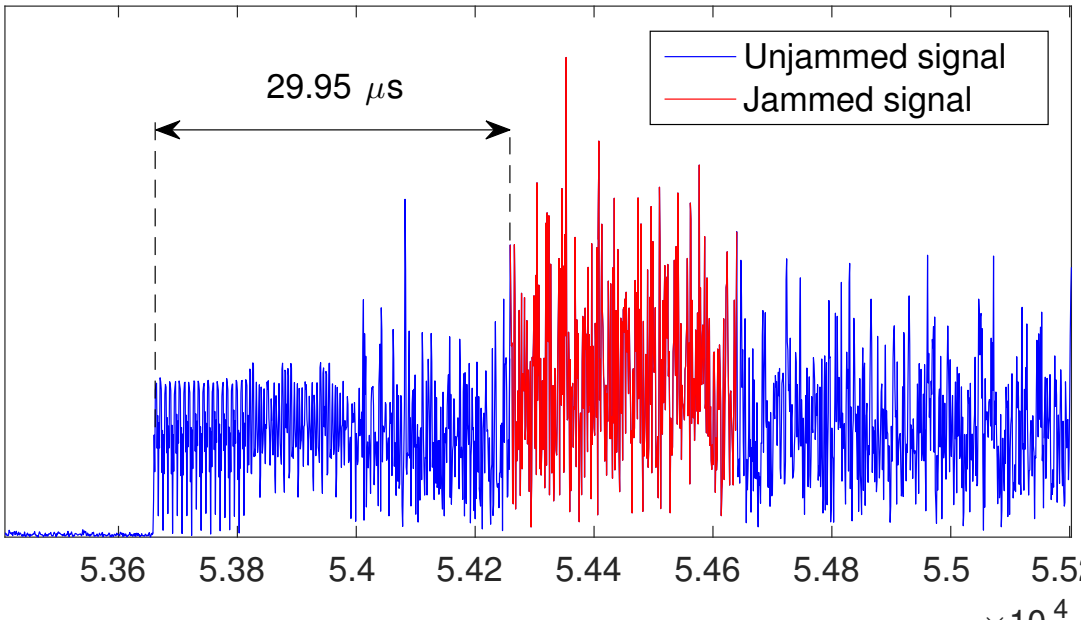
$$A_n = \sum_{k=0}^{L-1} r_{n+k+L} r_{n+k}^{*}$$

$$E_n = \sum_{k=0}^{L-1} |r_{n+k}|^2$$



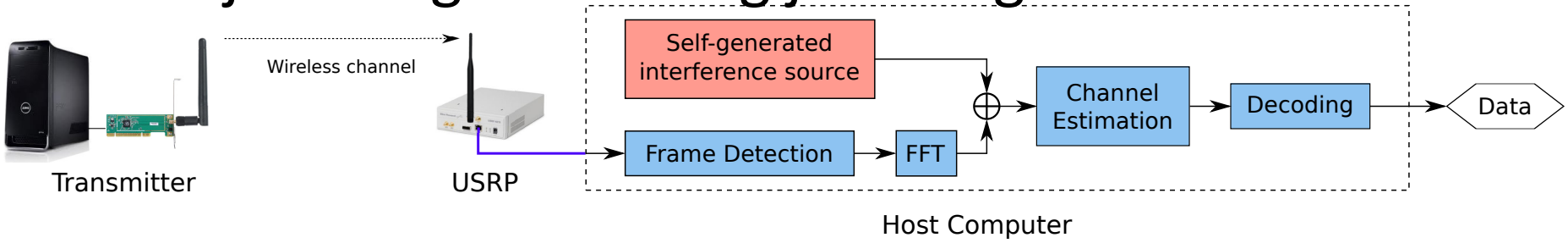
Real-time Jammer

- Speed:
  - 128 CPU cycles for frame detecting on every 16 received samples → 0.04us/sample
  - → able to operate in 20MHz
  - Switching and Jamming: less than 0. 16us
- Response time: <30us
  - Can jam a MAC frame > 3 OFDM symbols
  - 6 bytes of payload + 64bytes of header (UDP, IP, LLC, MAC)

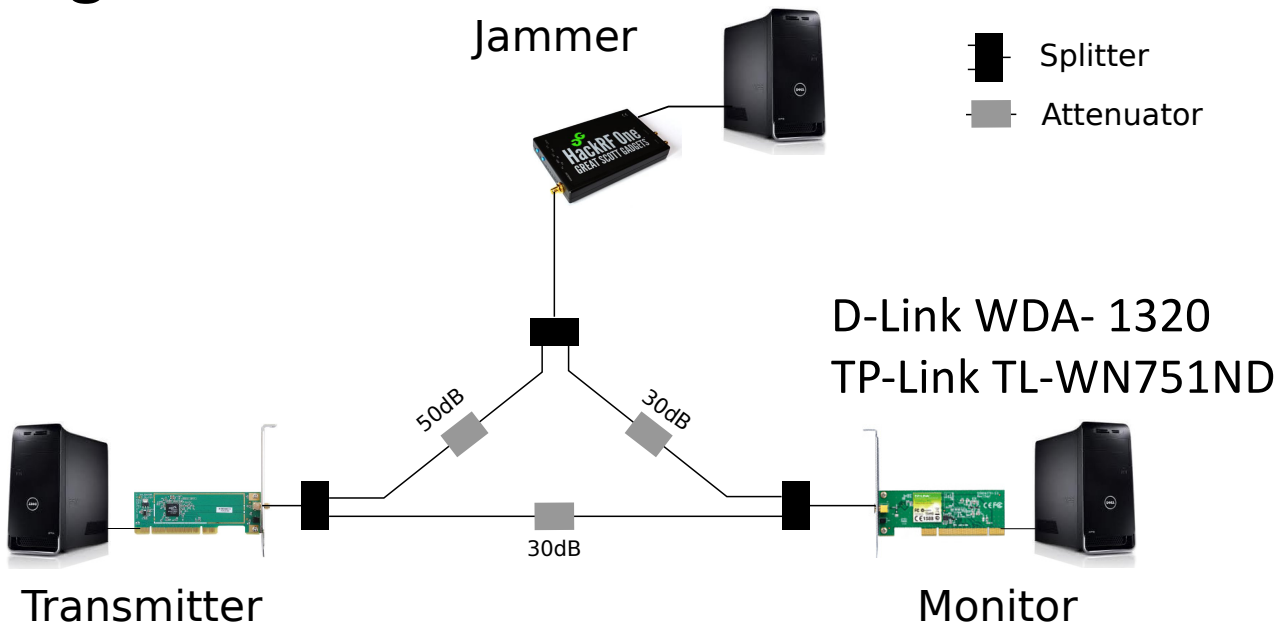


Experimental Evaluation

- Self-jamming: emulating jamming on SWi-Fi



- Jamming commercial Wi-Fi cards

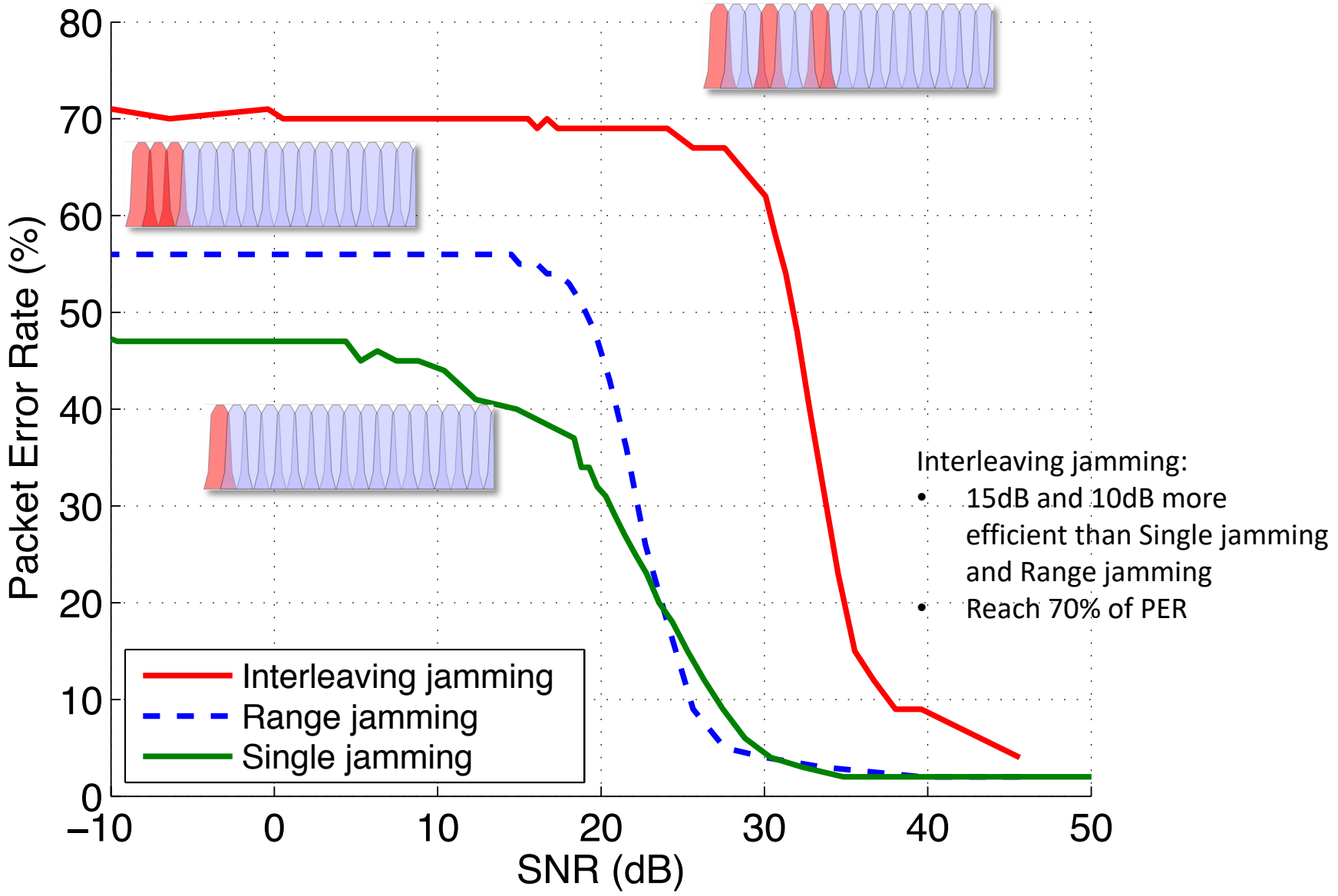


Parameters and Metrics

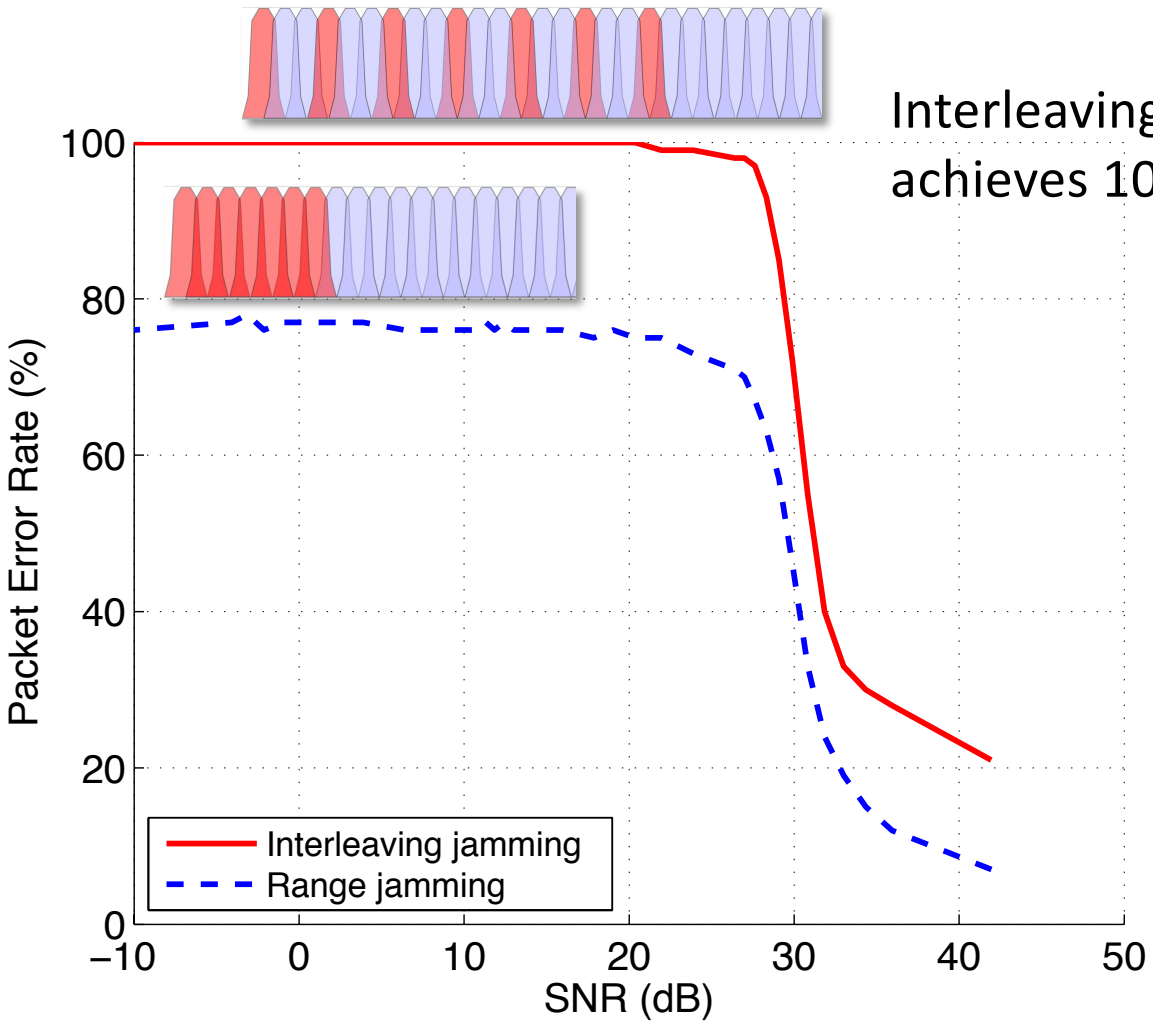
- Parameters:
  - Packet size: UDP 1500 bytes
  - Channel 11 (2.462GHz), bandwidth 20MHz
  - Rate adaptation disabled
  - Broadcast transmissions

- Metrics:
  - PER (packet error rate) vs. SJR (signal to jamming ratio)
  - Measured using a Wi-Fi Monitor node

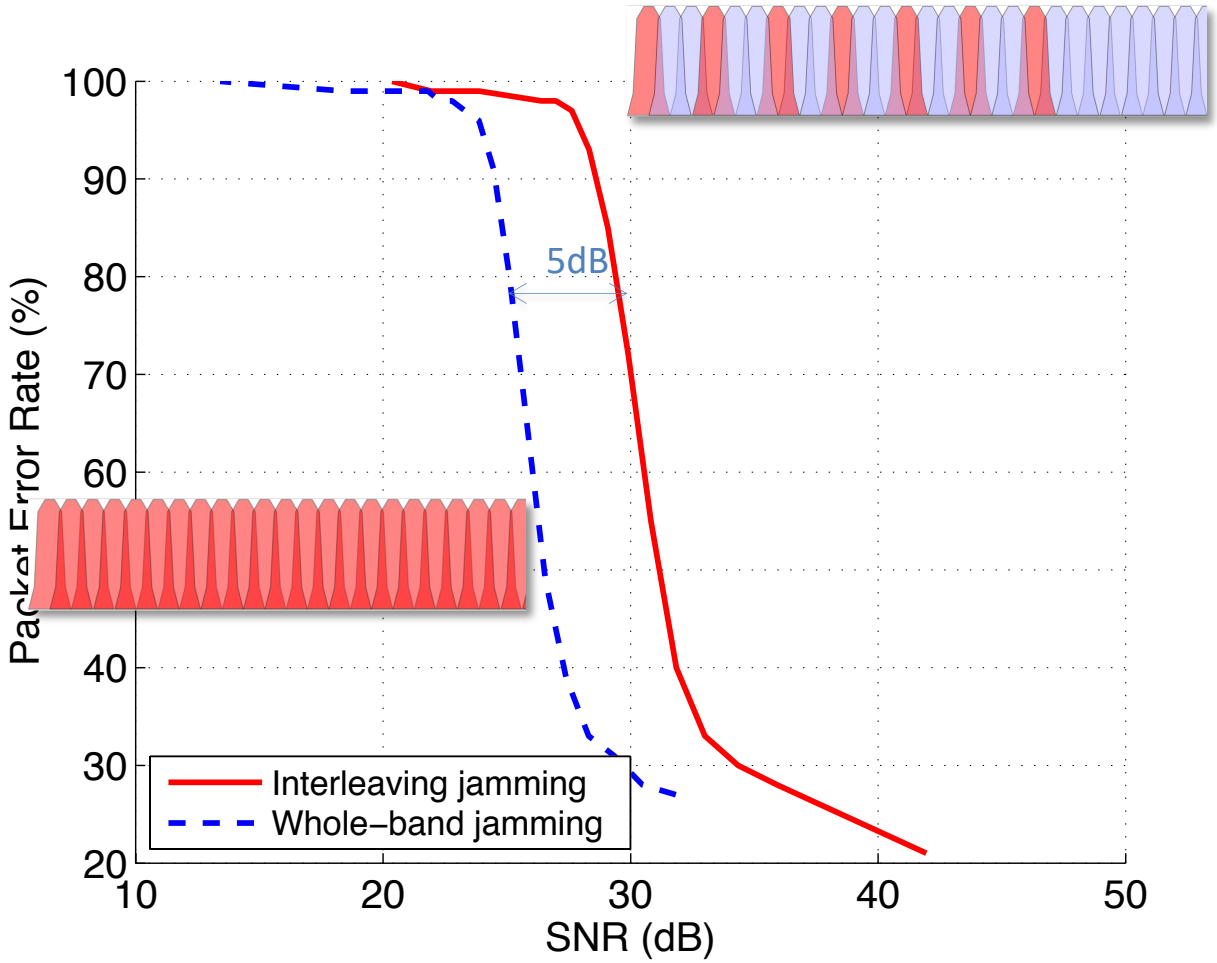
Preliminary Results with Emulated-Jamming: Continuous-time Narrow-band Jamming



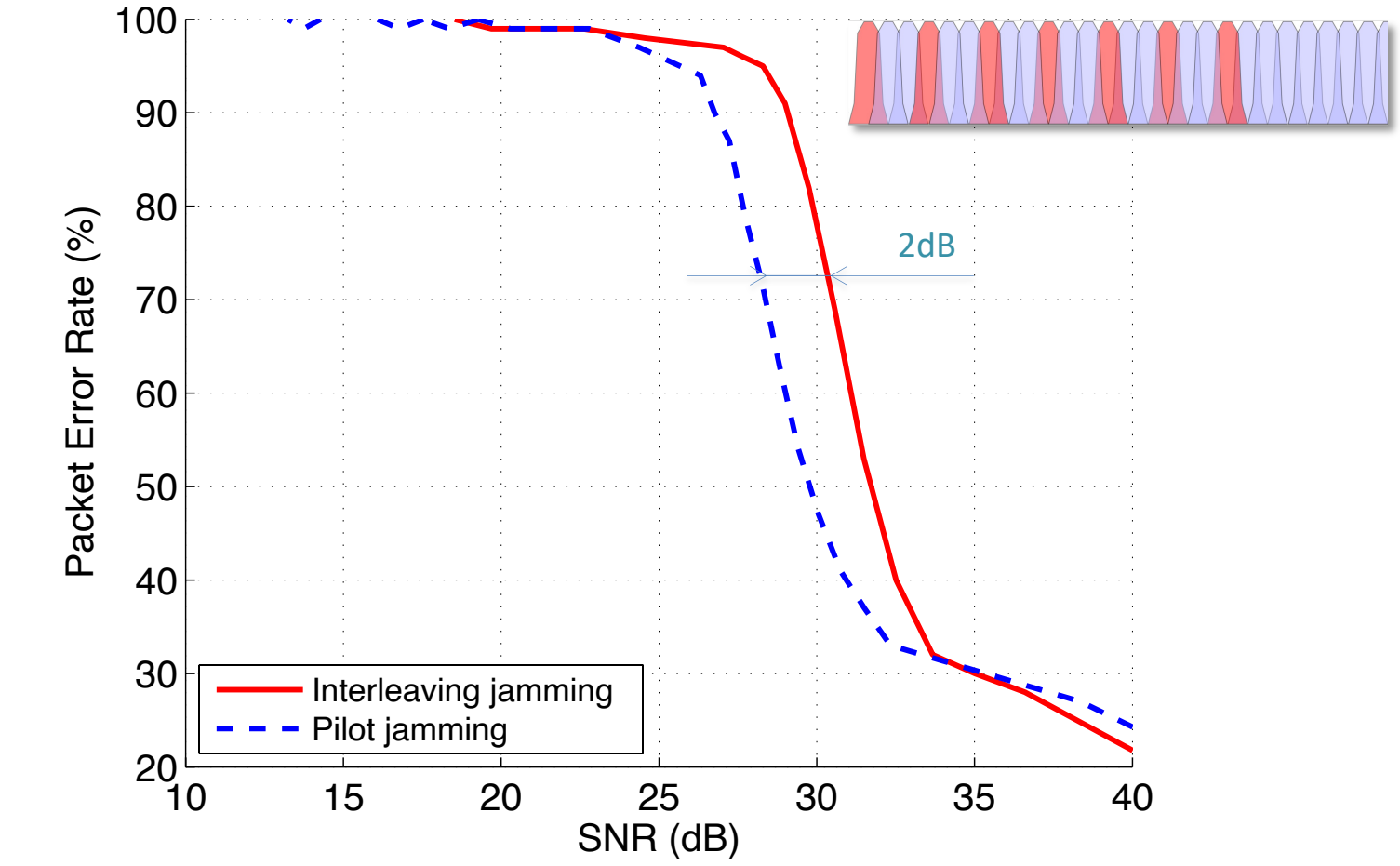
Preliminary Results with Emulated-jamming: Continuous-time Wide-band Jamming



Preliminary Results with Self-jamming: Continuous-time Whole-band Jamming

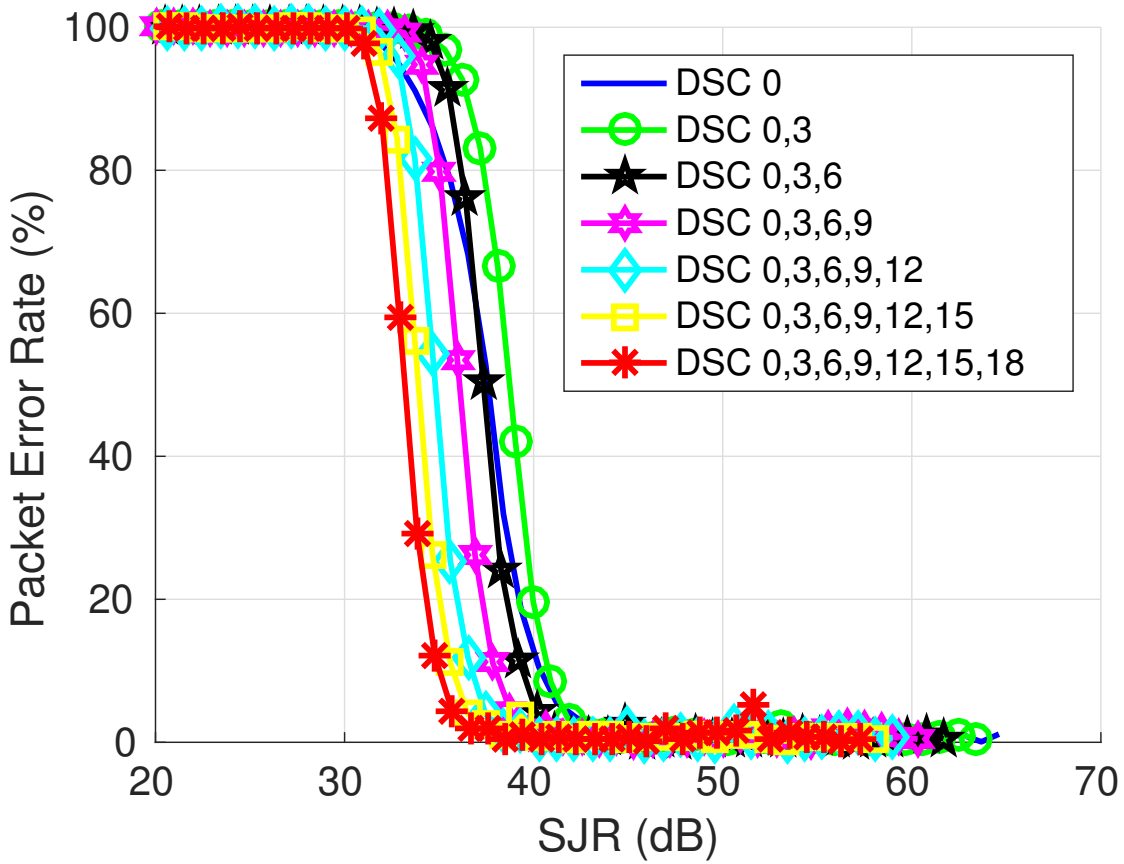


Preliminary Results with Emulated-Jamming: Continuous-time Pilot Subcarriers Jamming

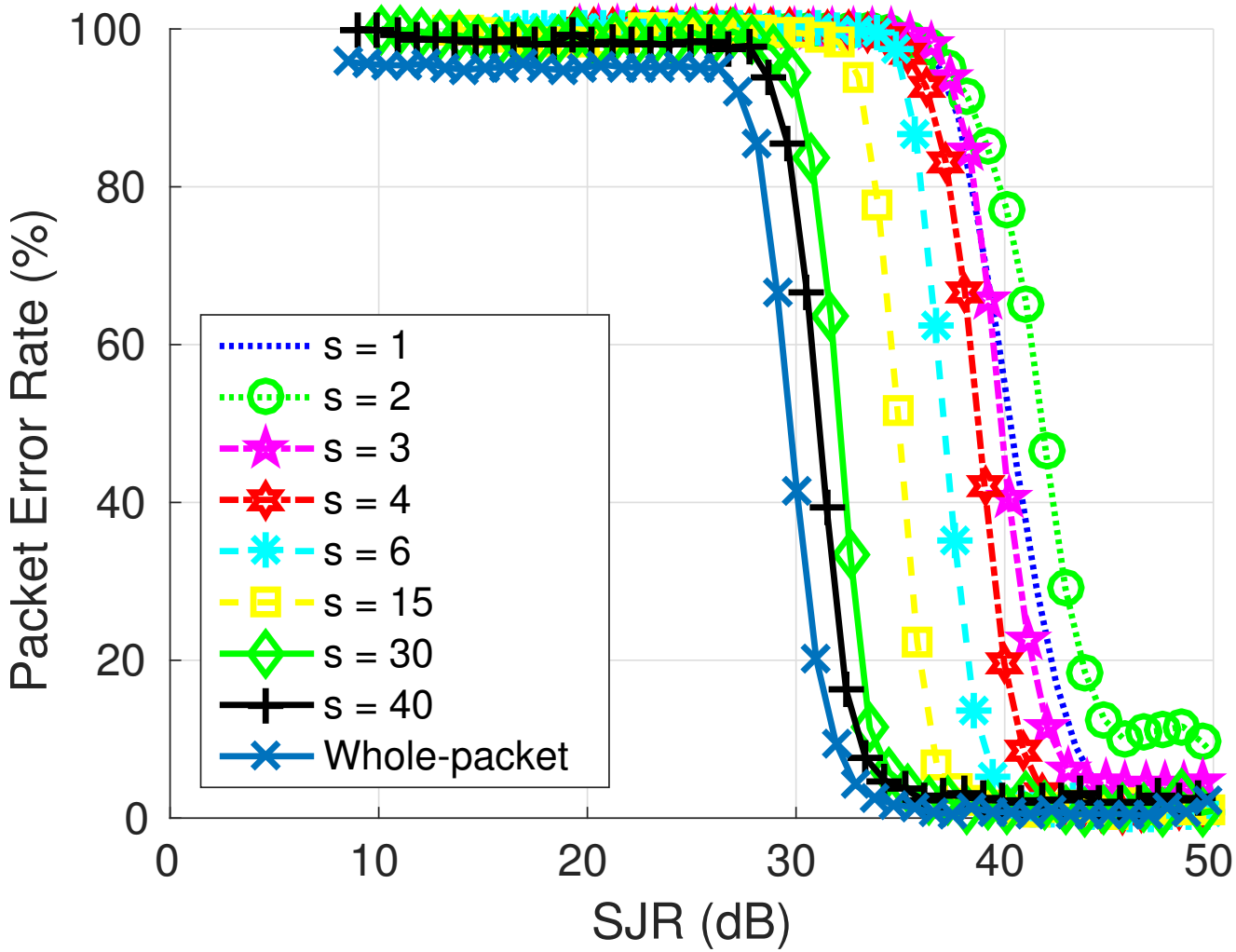


Impact on Commercial Wi-Fi Cards: Effect of Number of Subcarriers

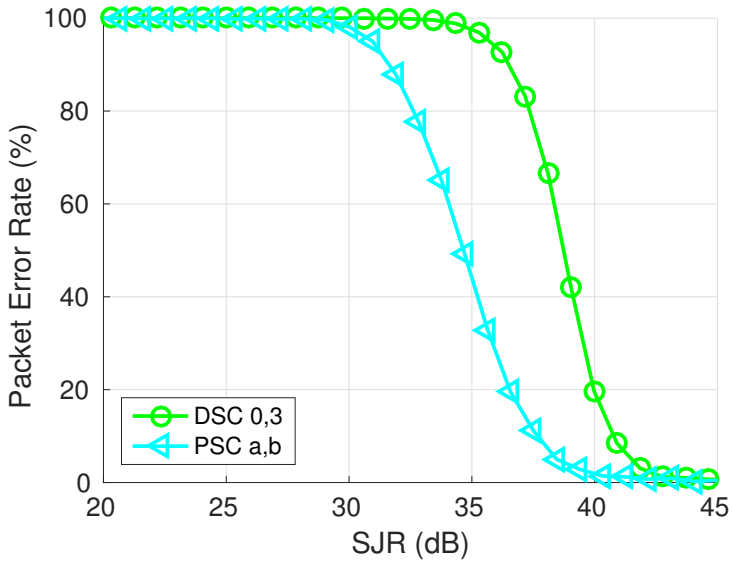
D-Link WDA- 1320
TP-Link TL-WN751ND

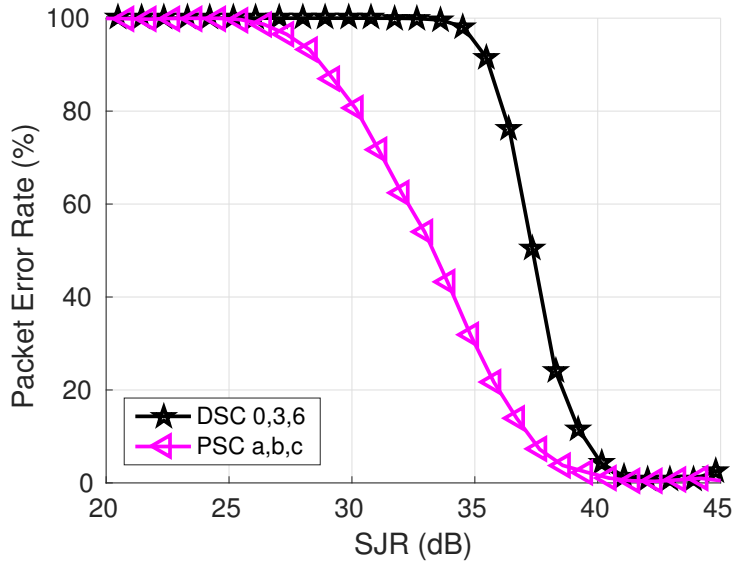


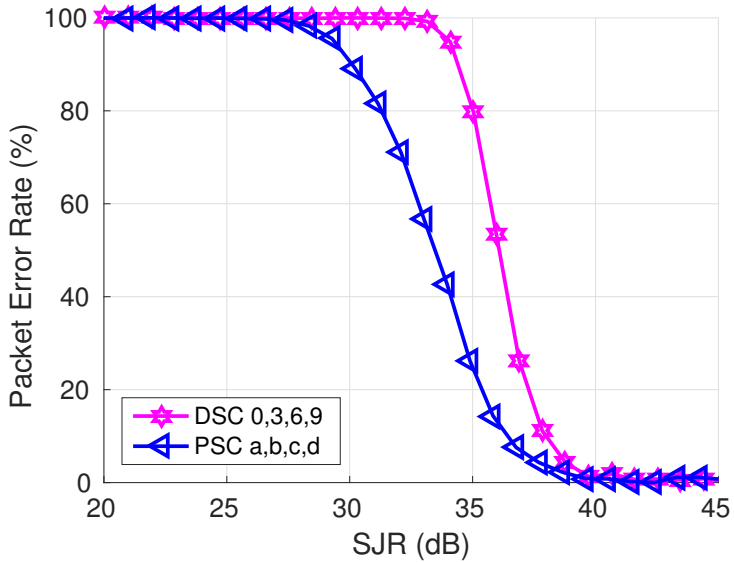
Impact on Commercial Wi-Fi Cards: Effect of Burst Length



Impact on Commercial Wi-Fi Cards: Short-burst Pilot Jamming vs. Interleaving Jamming

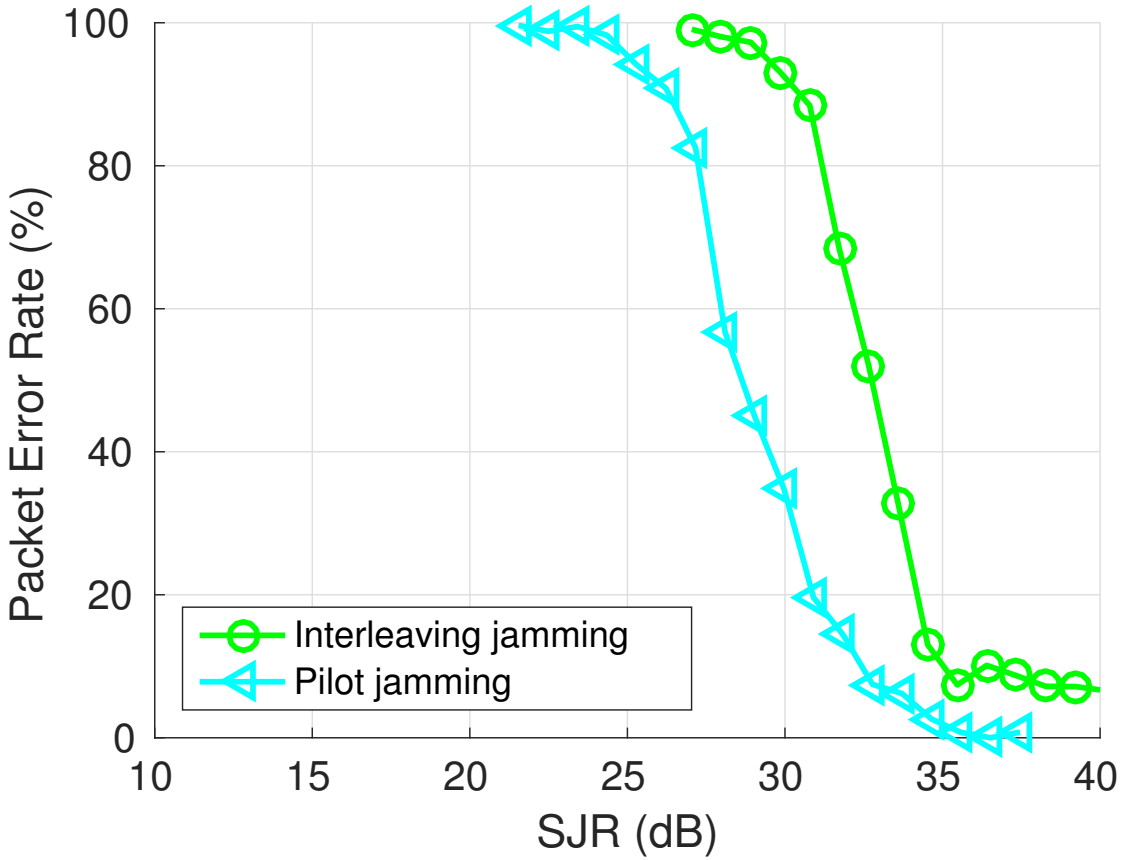






Burst s = 4

Impact on Commercial Wi-Fi Cards: Interleaving vs. Pilot Jamming in Wireless Environment



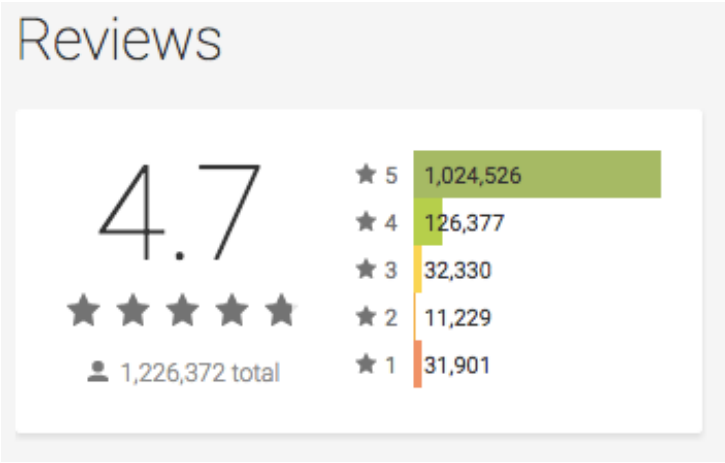
Conclusion on Interleaving Jamming

- Interleaving jamming is effective against Wi-Fi:
  - Blocks 95%-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
- Interleaving jamming is at least 5dB and up to 15dB more power efficient than other multicarrier jamming strategies
- Interleaving jamming is practical enough for implementation on low-cost SDR platform
- Further improvements
  - Low power packets detection
- Mitigation
  - Crypto-interleaving

Inferring User Routes and Locations w/ Zero-Permission Mobile Sensors

IEEE Security and Privacy 2016

How malicious can a Flashlight App be?



FTC Approves Final Order Settling Charges Against Flashlight App Creator

https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app

Brightest Flashlight Free ®

GoldenShores Technologies, LLC

Free

Version 2.4.2 can access:

Location
- approximate location (network-based)
- precise location (GPS and network-based)

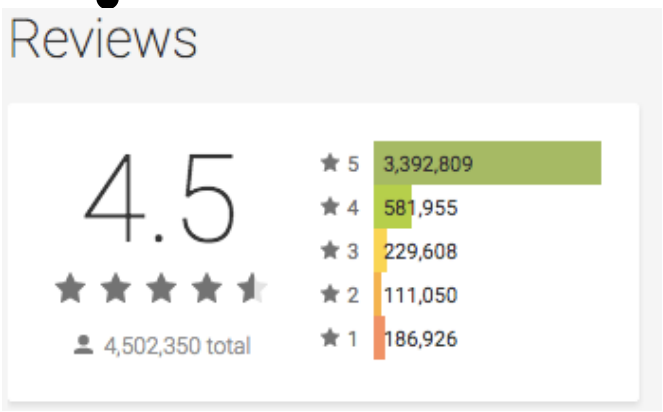
Photos/Media/Files
- modify or delete the contents of your USB storage
- read the contents of your USB storage

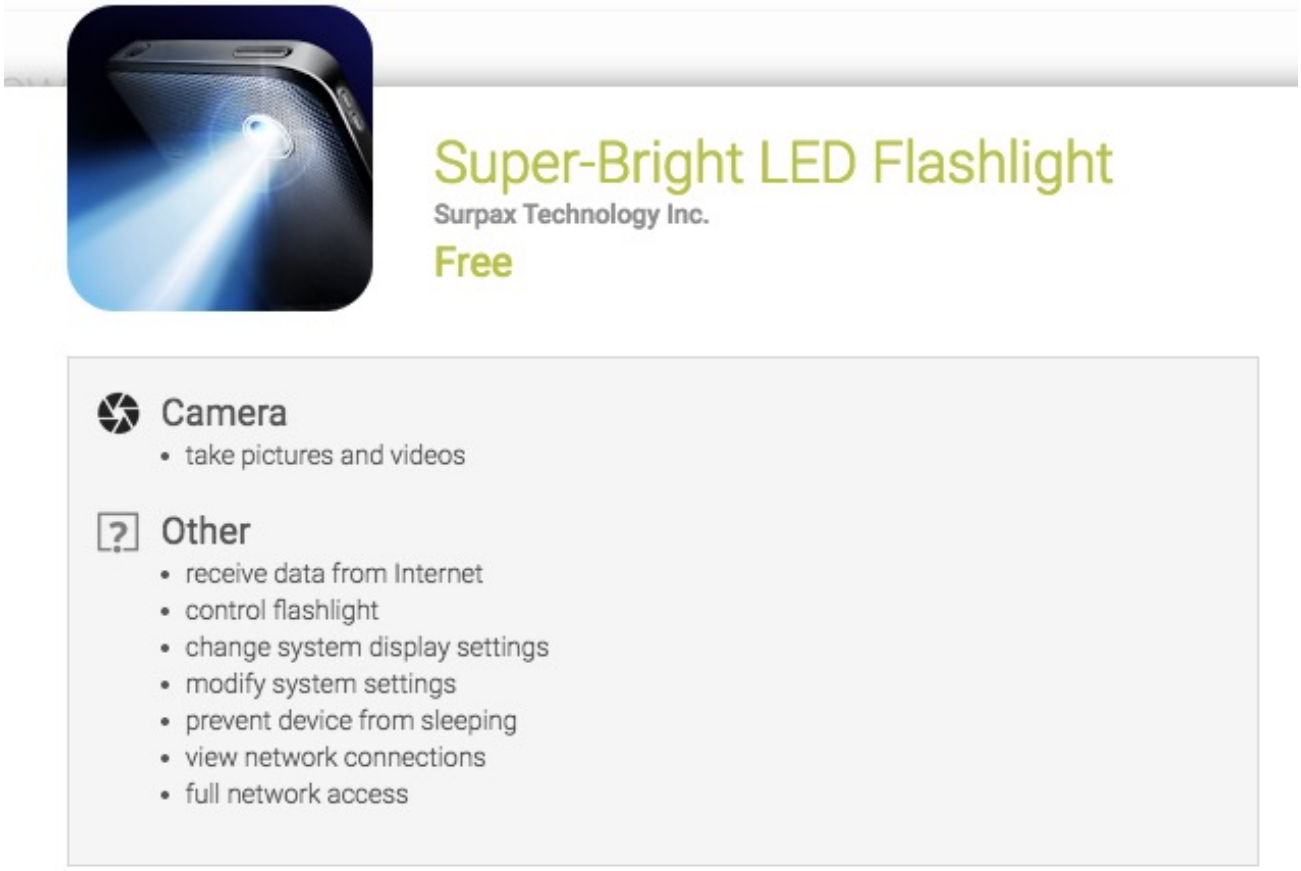
Camera
- take pictures and videos

Device ID & call information
- read phone status and identity

Other
- disable or modify status bar
- read Home settings and shortcuts
- control flashlight
- prevent device from sleeping
- view network connections
- full network access
- install shortcuts
- uninstall shortcuts

Less Intrusive Flashlight App



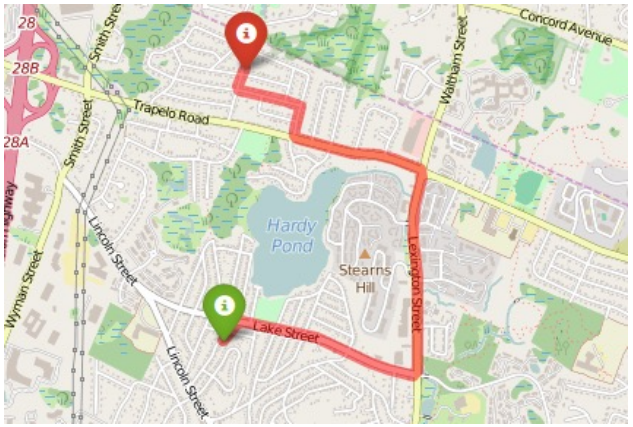


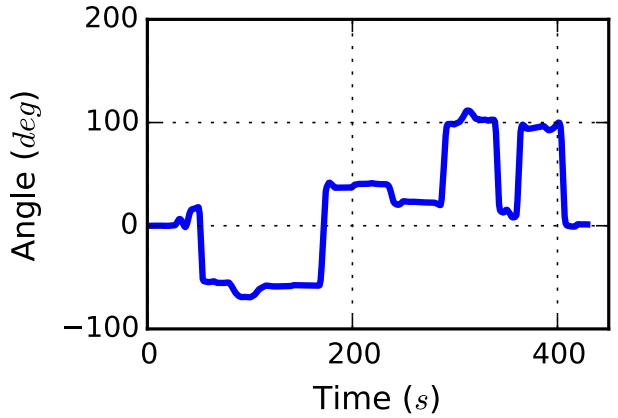
Zero Permissions Malicious App

- Observation
  - No need to request permission for accelerometer, gyroscope, compass, barometer
  - Most Apps obtain Internet access
  - GPS/Location can be viewed as suspicious
- Can we infer?
  - Gender? Age? Health information?
  - Work location, home? Identity? Social circle?

Inferring Location Information

- Goal is not to build an Inertial Navigation System
  - Gyroscope is fairly accurate
  - Accelerometers and compass are noisy

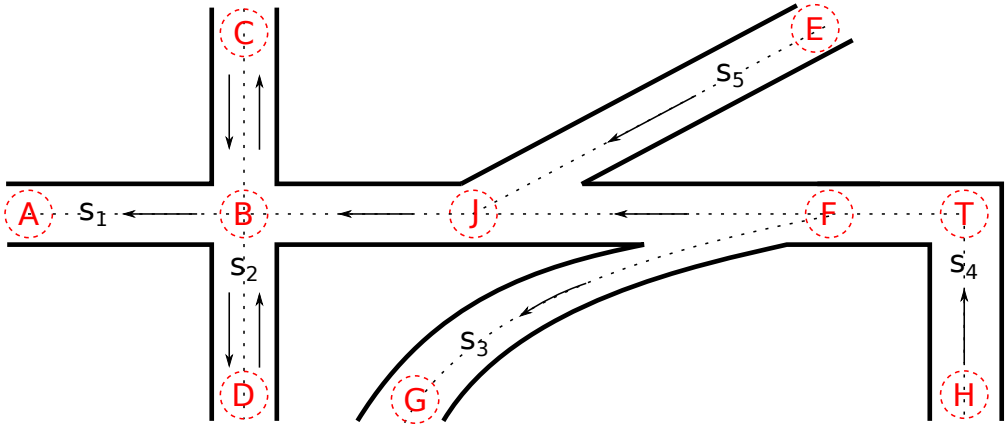


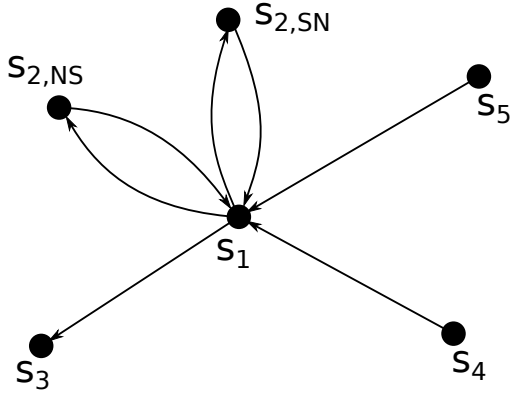


- Collect sequence of turns
- Infer most likely trajectory

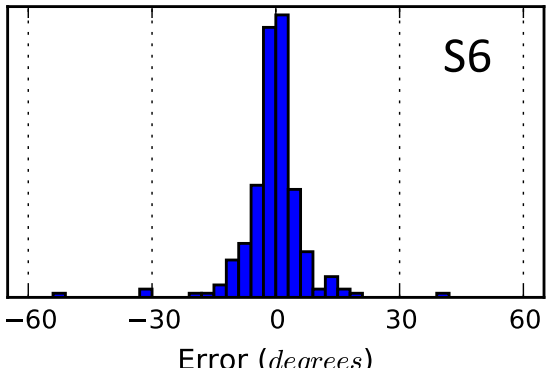
Inferring Location Information

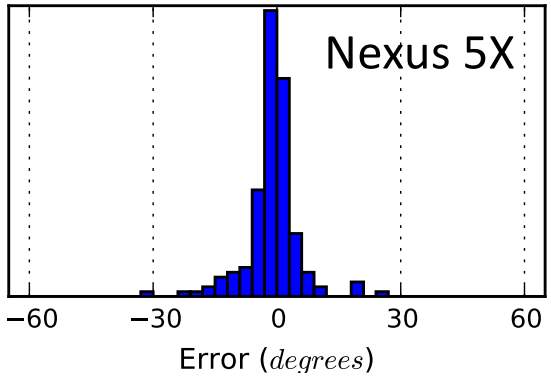
- Open Street Maps data => build a directed graph
  - enhance with road signature (curvature, compass headings, speed limit, potholes)





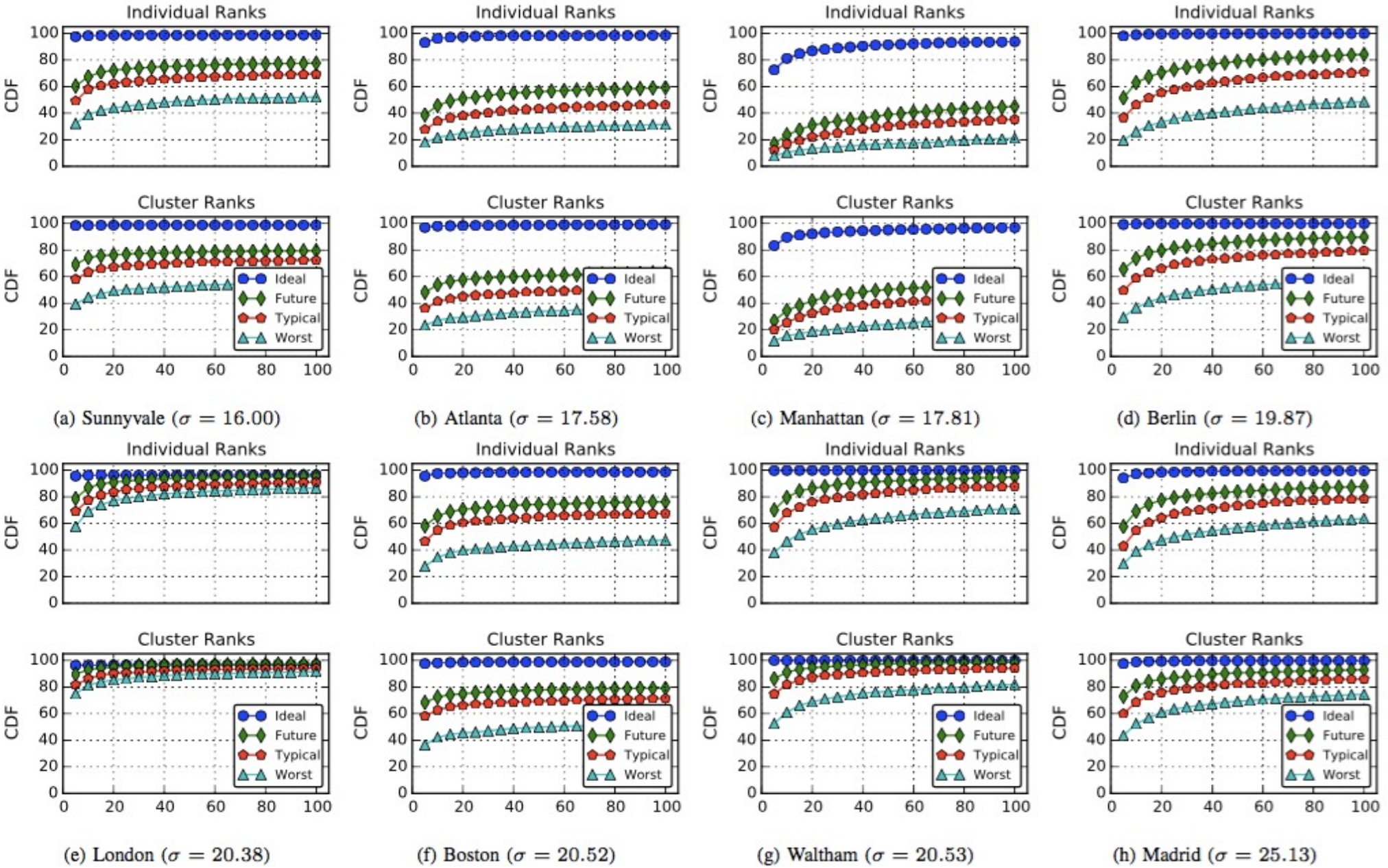
- Problem: finding maximum likelihood path
  - Error approx.
    by Gaussian
    but deletions





Techniques and Evaluation

- Developed several techniques
  - Processing data (compensating gyroscope bias, eliminating idle time)
  - Maximum likelihood path incorporating gyroscope & compass, curvature, speed limit with simple assumption on turns distribution
- Evaluation
  - Simulation on 11 cities: prob > 50% to output path in top 10
  - Real experiments in Boston (30%) and Waltham (60%) in top 5
  - Better results for longer lists, longer paths

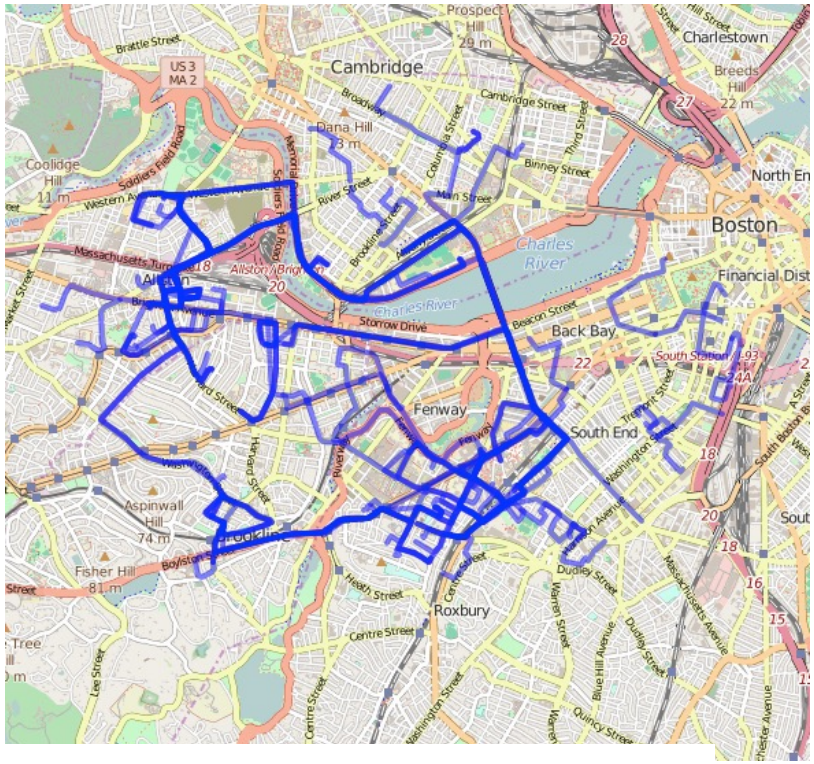


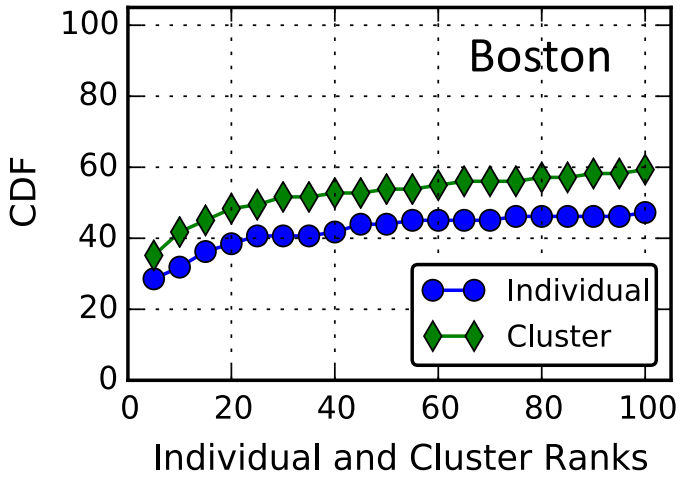
(a) Sunnyvale ($\sigma = 16.00$) (b) Atlanta ($\sigma = 17.58$) (c) Manhattan ($\sigma = 17.81$) (d) Berlin ($\sigma = 19.87$)

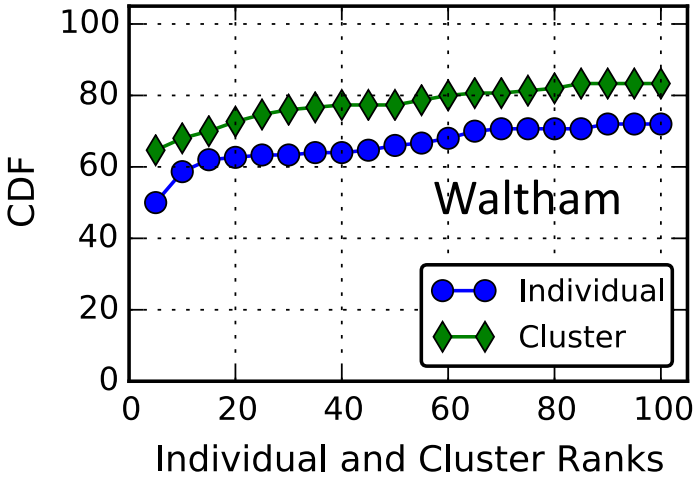
(e) London ($\sigma = 20.38$) (f) Boston ($\sigma = 20.52$) (g) Waltham ($\sigma = 20.53$) (h) Madrid ($\sigma = 25.13$)

Results on Real Experiments

- Boston & Waltham
  - 4 drivers, 70 + 70 paths, 980 Km
  - Boston
    - ~ 30-35% in top 5 (13% ranked 1)
  - Waltham
    - ~ 50-60% in top 5 (38% ranked 1)







Inferring Location Information

- Code + Dataset accessible

  https://ares.ccs.neu.edu/location_tracking/sensors

Conclusion

- Reproducibility in wireless research is challenging but critical and feasible for wireless networking community impact
- Need for community defined methods, templates, formats, annotations
- Open source repositories for RF signals
- Large scale network emulators & testbeds
  - (Emulating real radio channels)
- Community validated wireless artifacts
  - Artifact evaluation committees in major conferences and journals
  - Methods for wireless artifacts evaluations
  - Orbit validated experiments?