Wireless Networking Projects

Ashok K. Agrawala
Udaya Shankar
University of Maryland

The Maryland Information and Network Dynamics Lab

Participants

- Ashok Agrawala
- Udaya Shankar
- Moustafa Youssef
- Students
  - Adel
  - Jihwang
  - Tamer
  - Andre
  - Arun
  - Bao
  - …

Activities

- Location Determination
  - Adhoc
    - PinPoint and Extensions
  - Infrastructure Based
    - Horus Technology
    - Nuzzer Technology for passive determination of location
- Energy Efficient On-Demand Routing
- Enhancements to DCF
  - BEB in 802.11 in Noisy Environment
  - Location Aware Enhancements
- WiFi Traffic Characterization

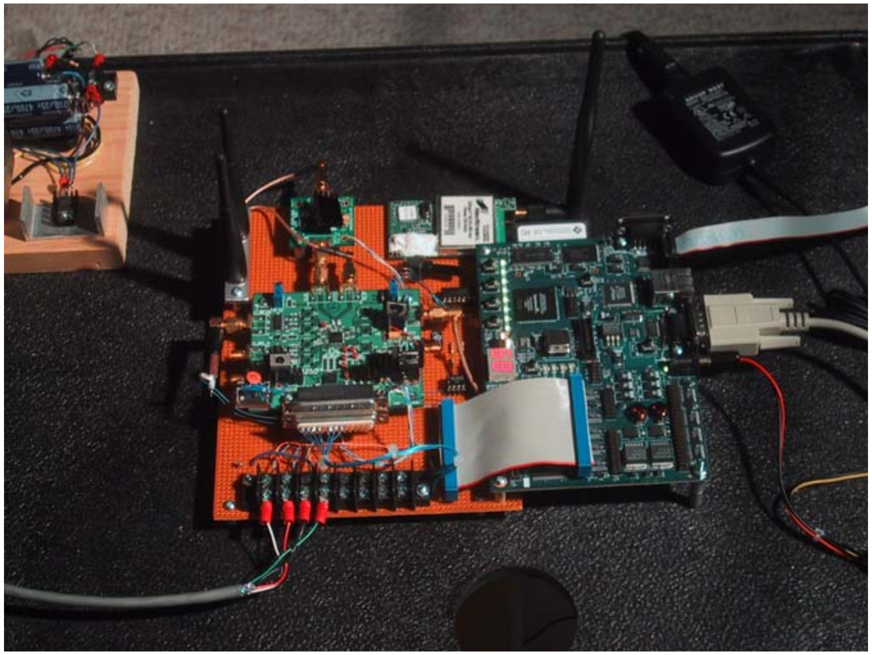
Location Determination in AdHoc Environments

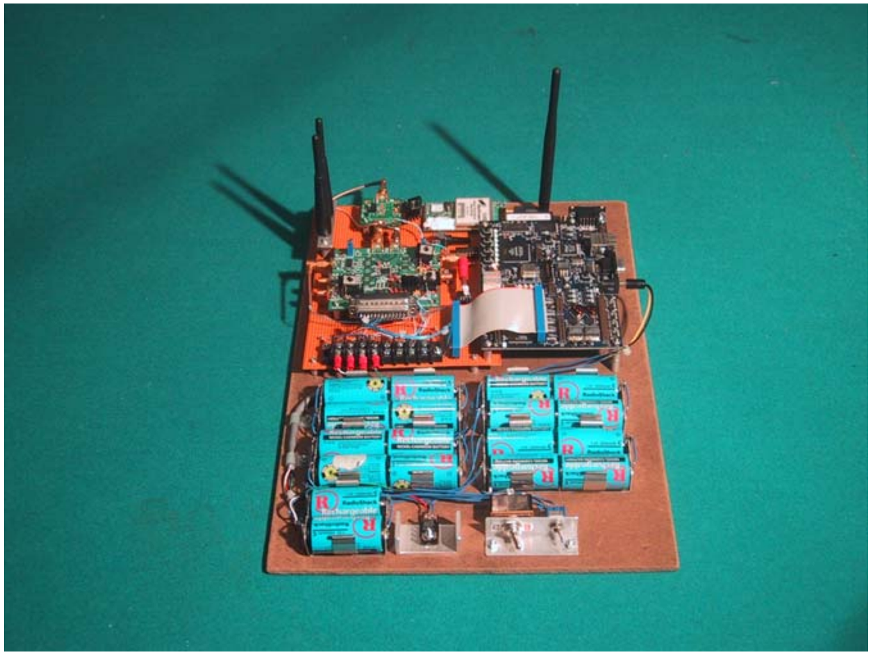
- There is no infrastructure
- There are no anchors – nodes with known locations

- Need to determine the range – distance between two nodes
  - PinPoint Technology
- Integrated view
  - SALAM – A Scalable Anchor-free Location Algorithm for a heterogeneous Network

PinPoint

Current Hardware – Client node





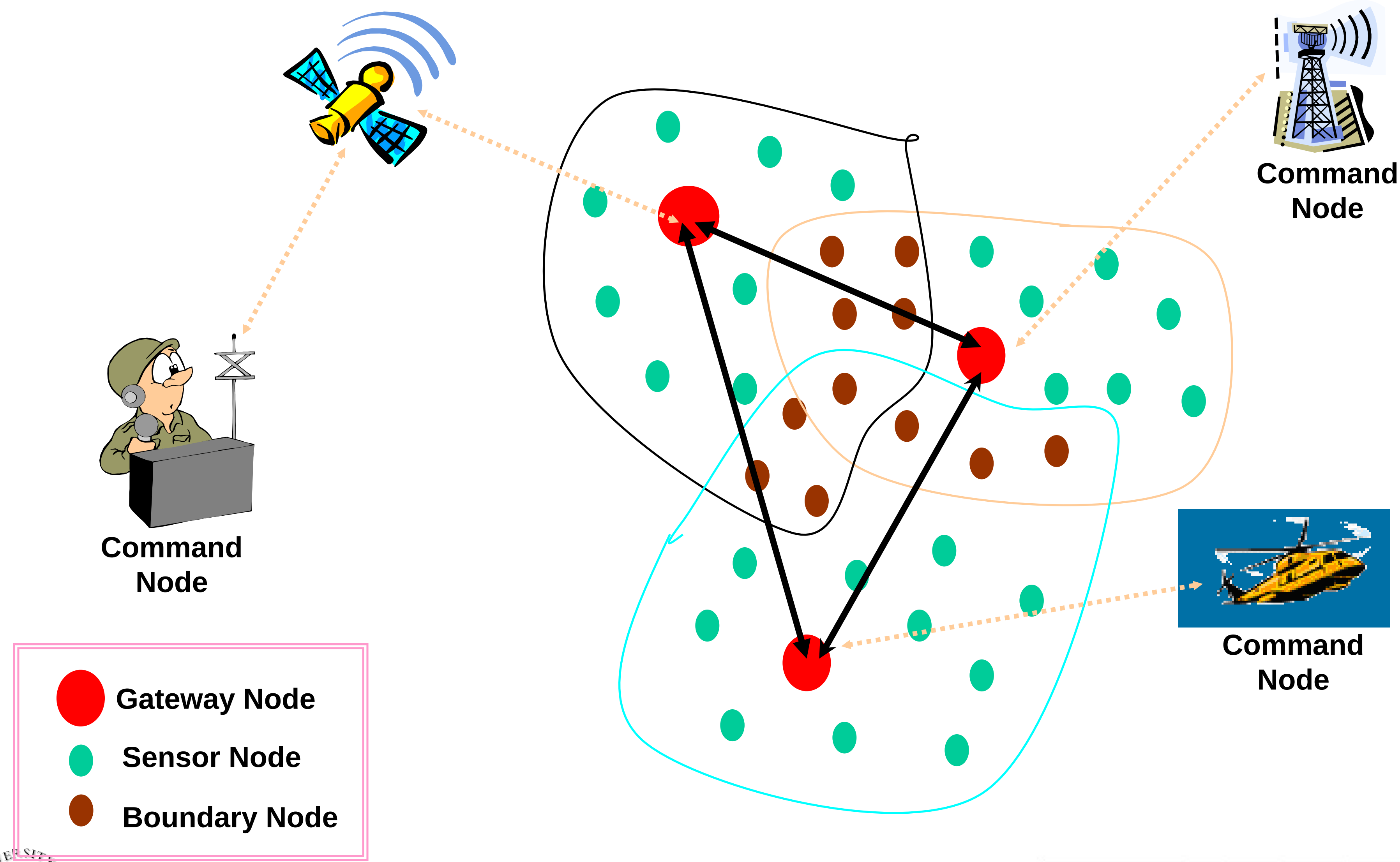
SALAM

Motivation

- **Locally centralized algorithms scale well with increased network size**
- **They are robust to network partitioning and node failure.**
- **They can achieve acceptable accuracy compared to a centralized approach.**

A locally centralized algorithm should be a good compromise between accuracy, communication overhead, depending on the size of the cluster and the location of the cluster head.

System Architecture



The Maryland Information and Network Dynamics Lab

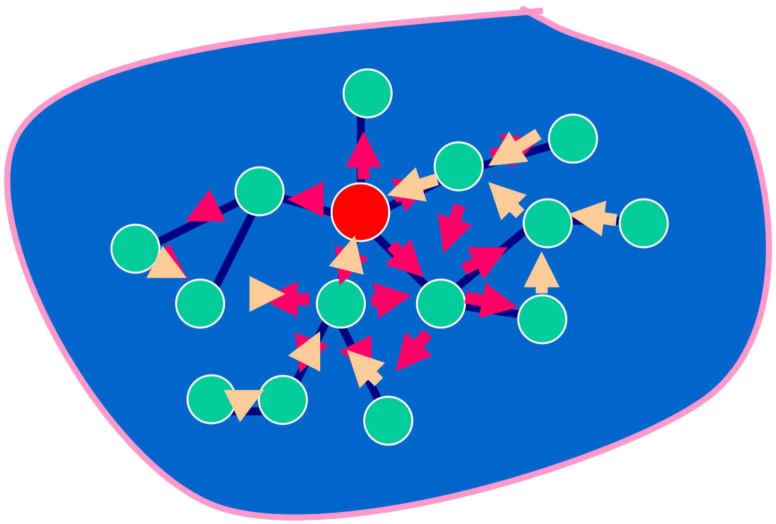
SALAM

Phase I: Network Bootstrapping

- Range Estimation - PinPoint

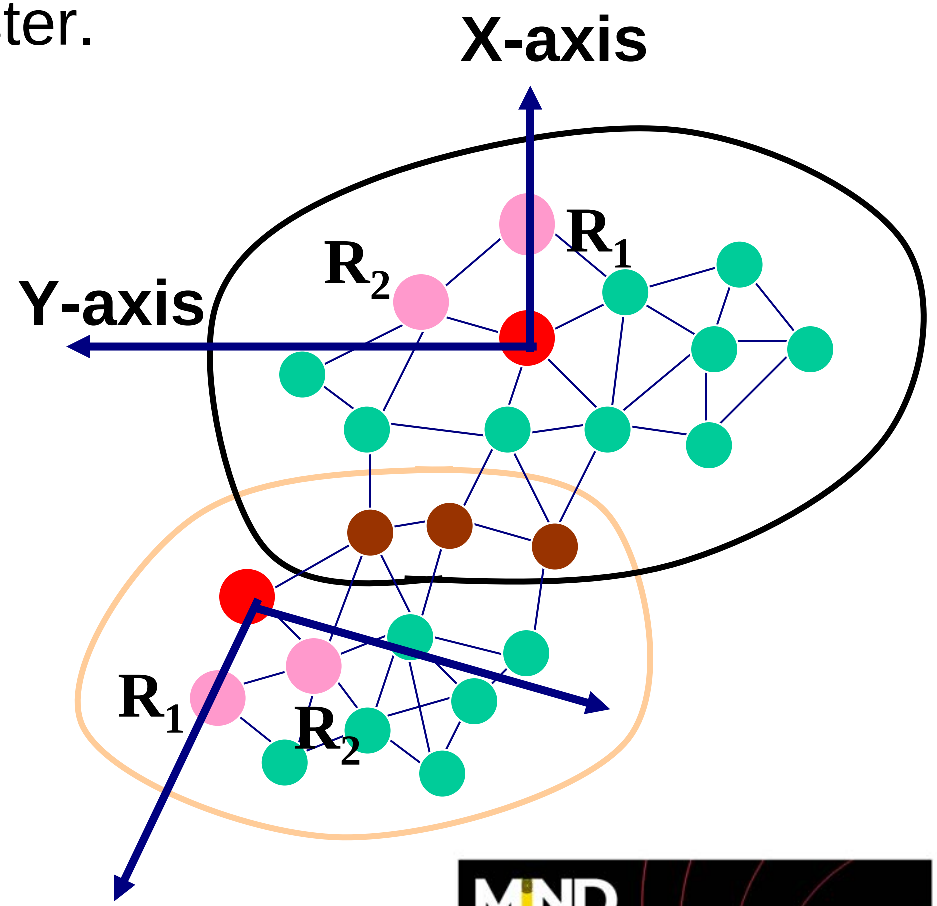
- **Node Discovery**
  - **Discover nodes that are *K*-hops (cluster radius) away from gateway node.**
  - **Build a breadth first spanning tree rooted at the gateway node.**

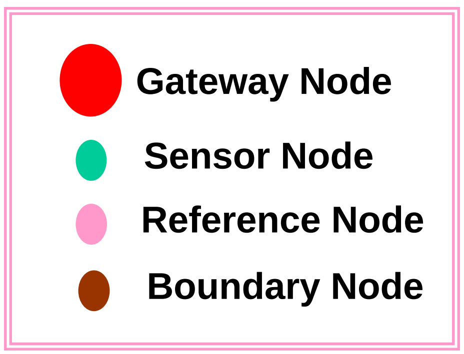
- Cluster Formation



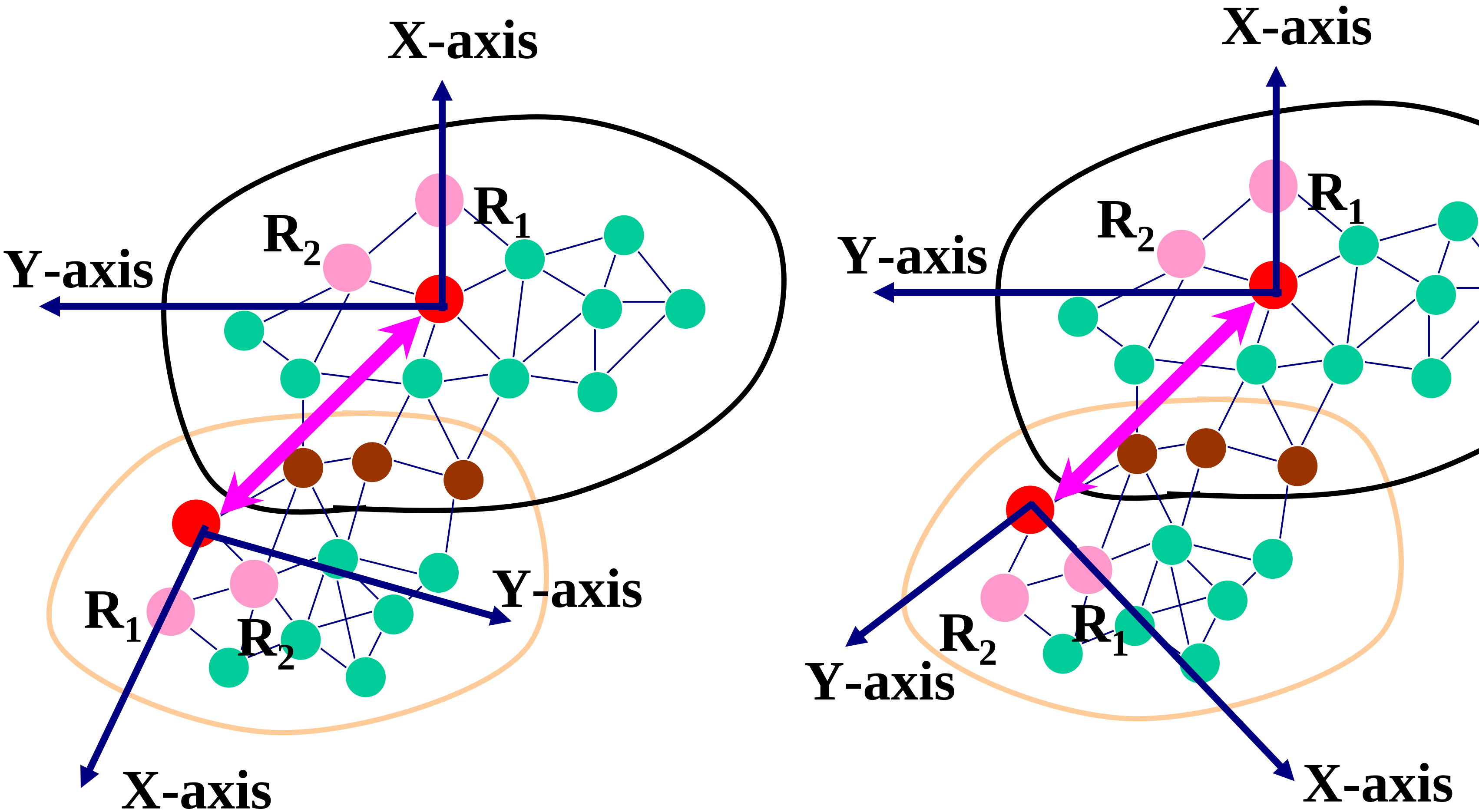
SALAM Phase II: Local Location Discovery

- Each gateway node has inter-node distance matrix D for the nodes that are within K-hops.
- Build a local map for the cluster.





Phase III: Integrated View



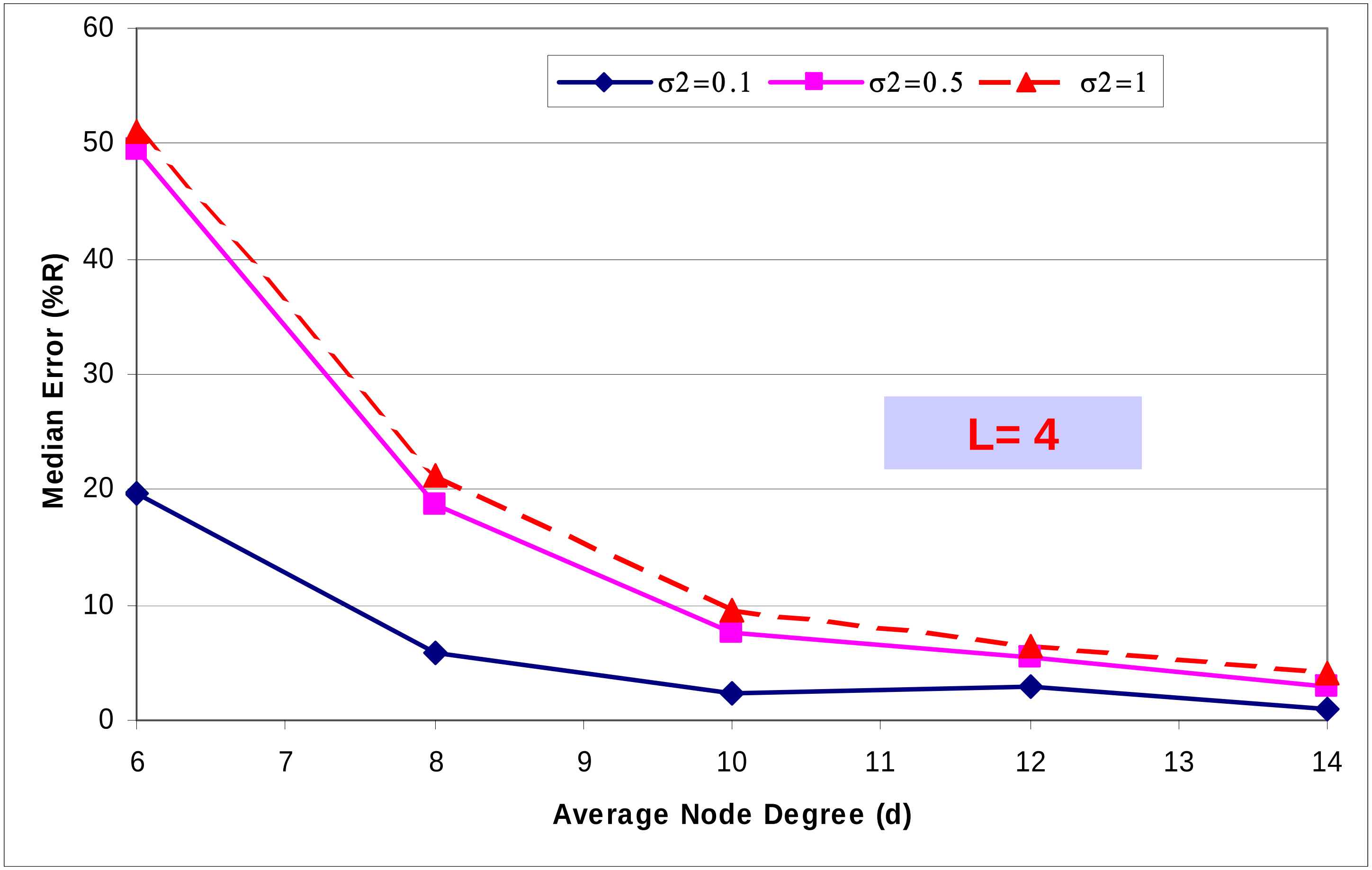
SALAM

Experimental Setup

- 1000 different topologies, different cluster size ranging from 20-60 nodes per cluster
- Nodes are randomly placed according to a uniform distribution on a 100x100 area
- Varying transmission range to achieve different node degree (6-14)
- Different coordinate system radius (1-4)
- Range Error: N(0, σ2), where σ2 ranges from 0.1-1

SALAM

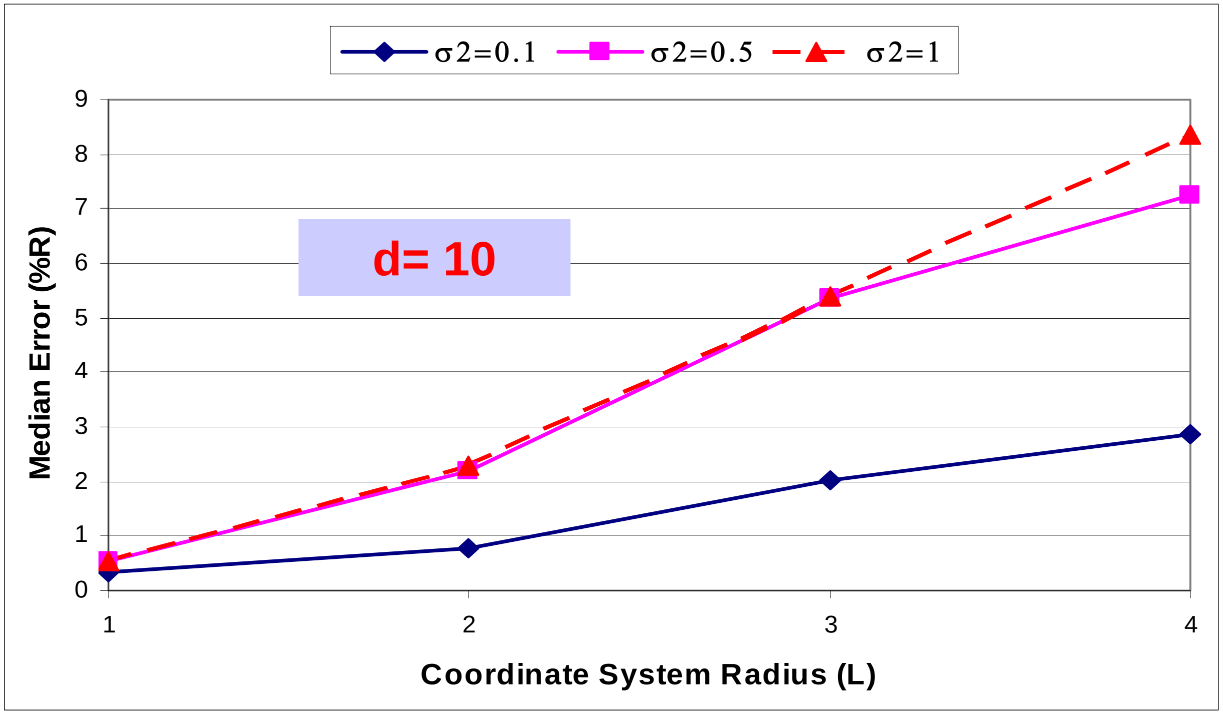
The Effect of Connectivity on Accuracy



As node degree increases, range errors become very insignificant.

The Maryland Information and Network Dynamics Lab

SALAM The Effect of Coordinate System Radius on Accuracy

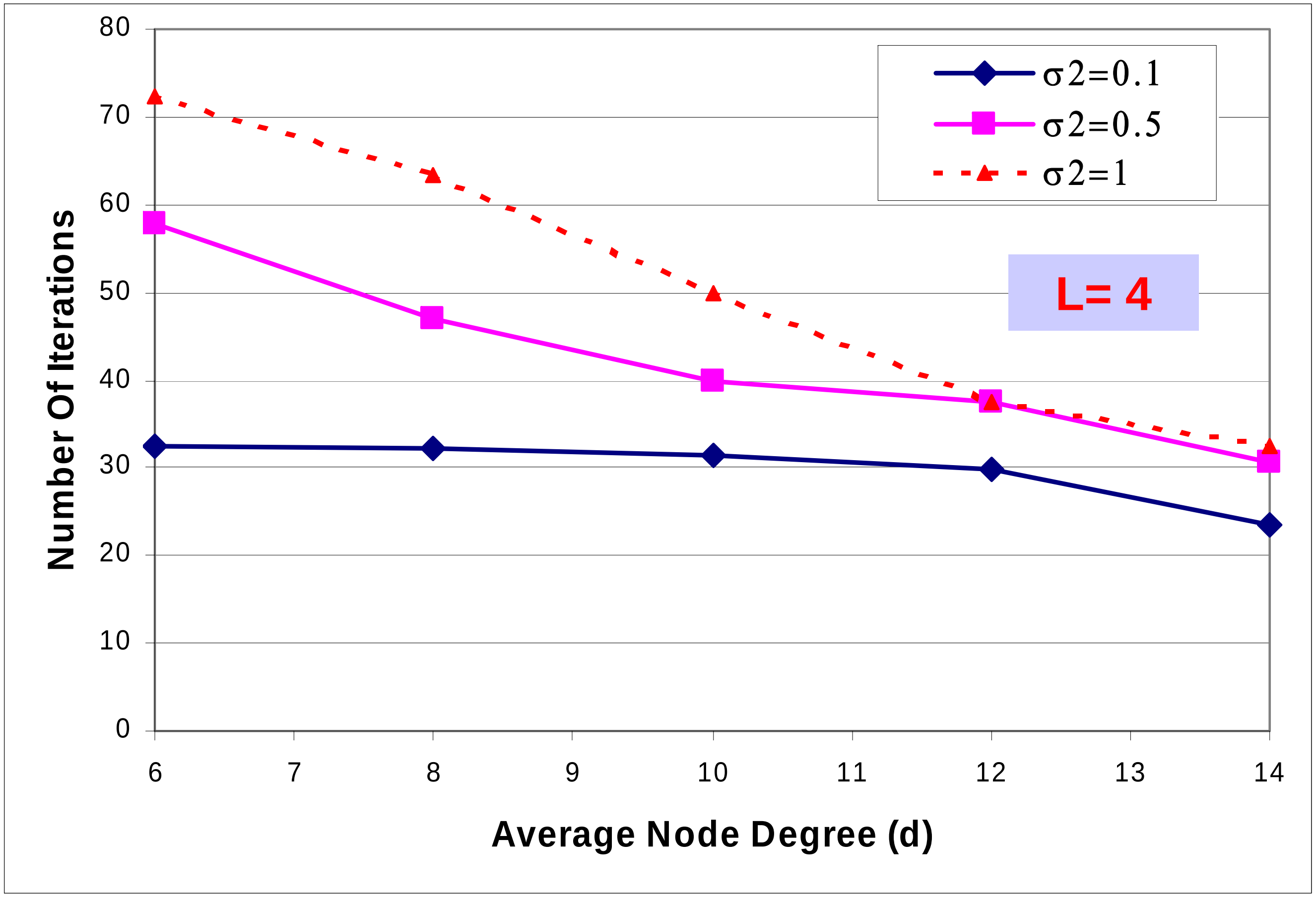


- Decrease in accuracy is *linear* in "*L*".
- A jump in the range error variance from .5 to 1 caused little impact compared to the increase for .1 to .5. Such observation stresses the importance of employing a good range measurements technology.

The Maryland Information and Network Dynamics Lab

SALAM

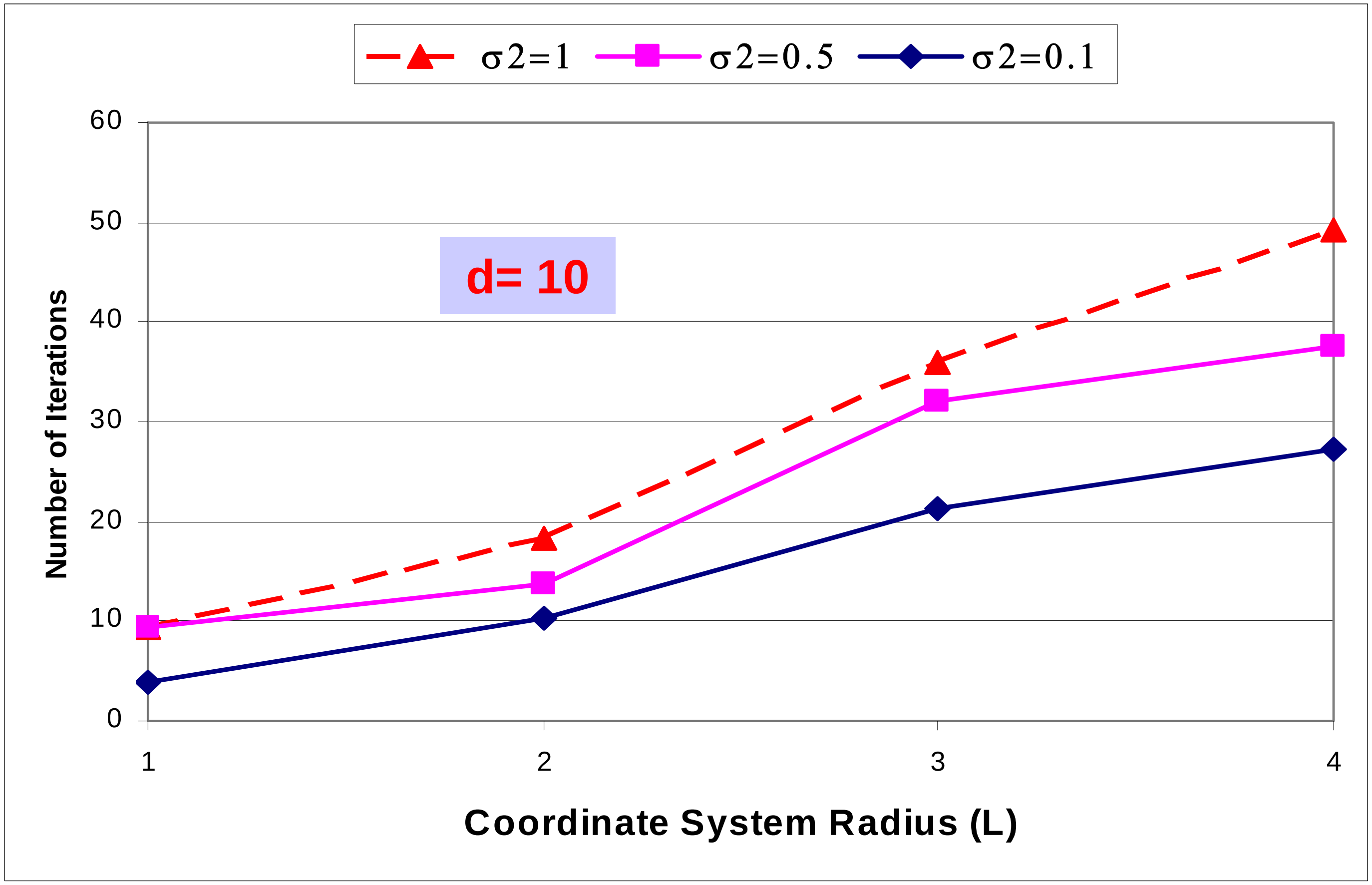
The Effect of Connectivity on Convergence Latency



The Maryland Information and Network Dynamics Lab

SALAM

The Effect of Coordinate System Radius on Convergence Latency



UNIVERSITY OF MARYLAND 1856

The MIND Lab
The Maryland Information and Network Dynamics Lab

SALAM

Conclusion

- Developing a cluster-based anchor-free localization algorithm for as hoc sensor networks:
  - Network bootstrapping (the OK clustering algorithm)
  - Local location discovery (formulating a LSE model to minimize the intra-cluster cumulative errors)
  - Global location discovery (finding the best order of transformations)
- Analyzing the effect of different parameters on the performance of the system.
- Analyzing error accumulation (inter-/intra-cluster).
- Compare the performance of the proposed system with other anchor-free systems.

Location Determination
Horus Technology

- Signal-Strength (RSSI) Based Approach

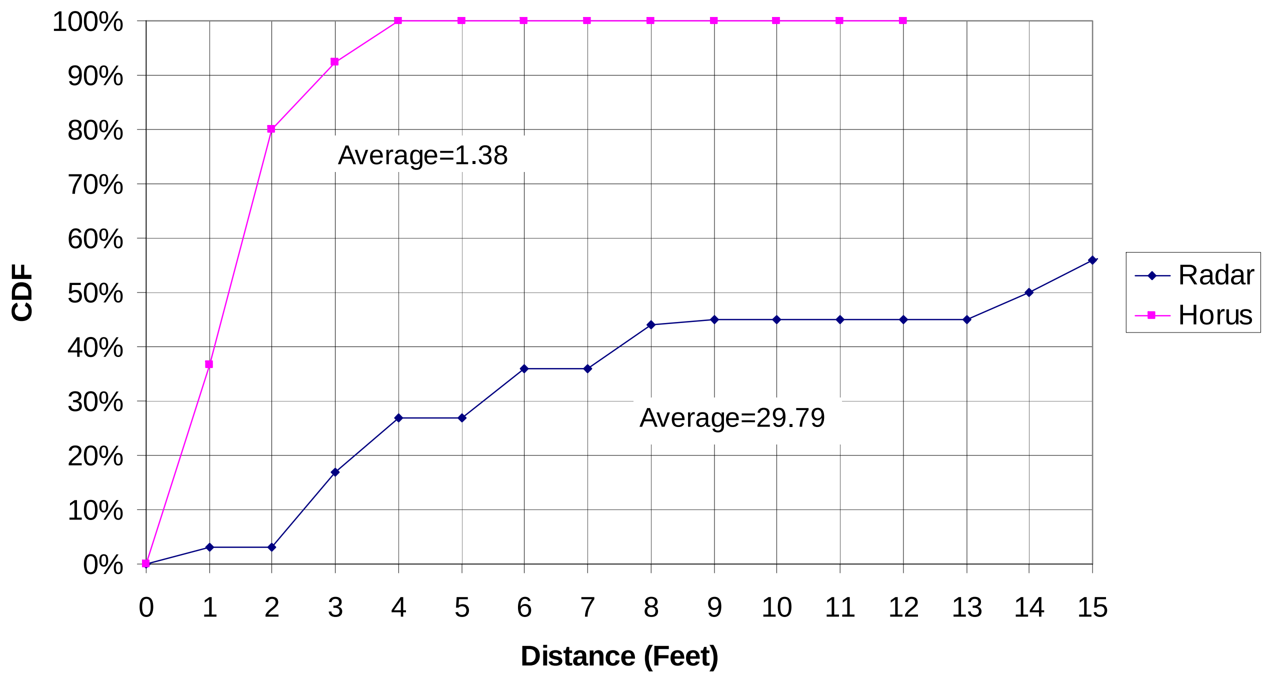
- A few commercially available, e.g. Ekahau, PanGo
- A few research groups working on it

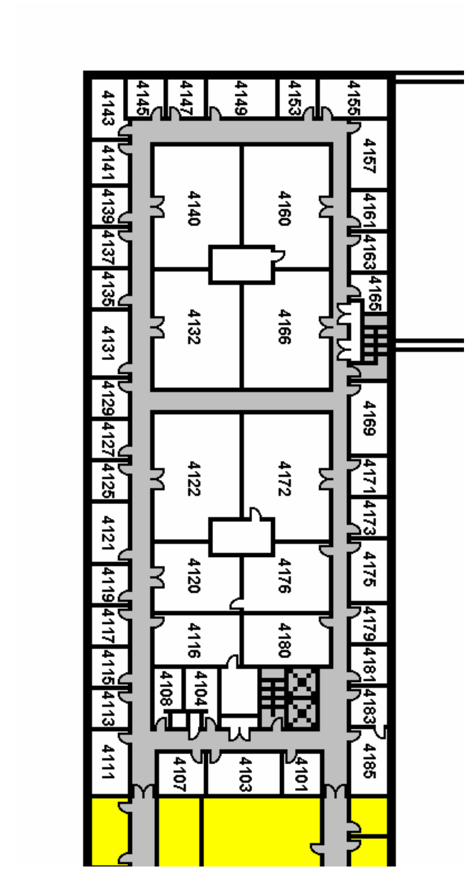
- Horus results significantly better than all

- Licensed by Fujitsu and deployed in a shopping center application

Horus

Comparison With Other Systems: RADAR

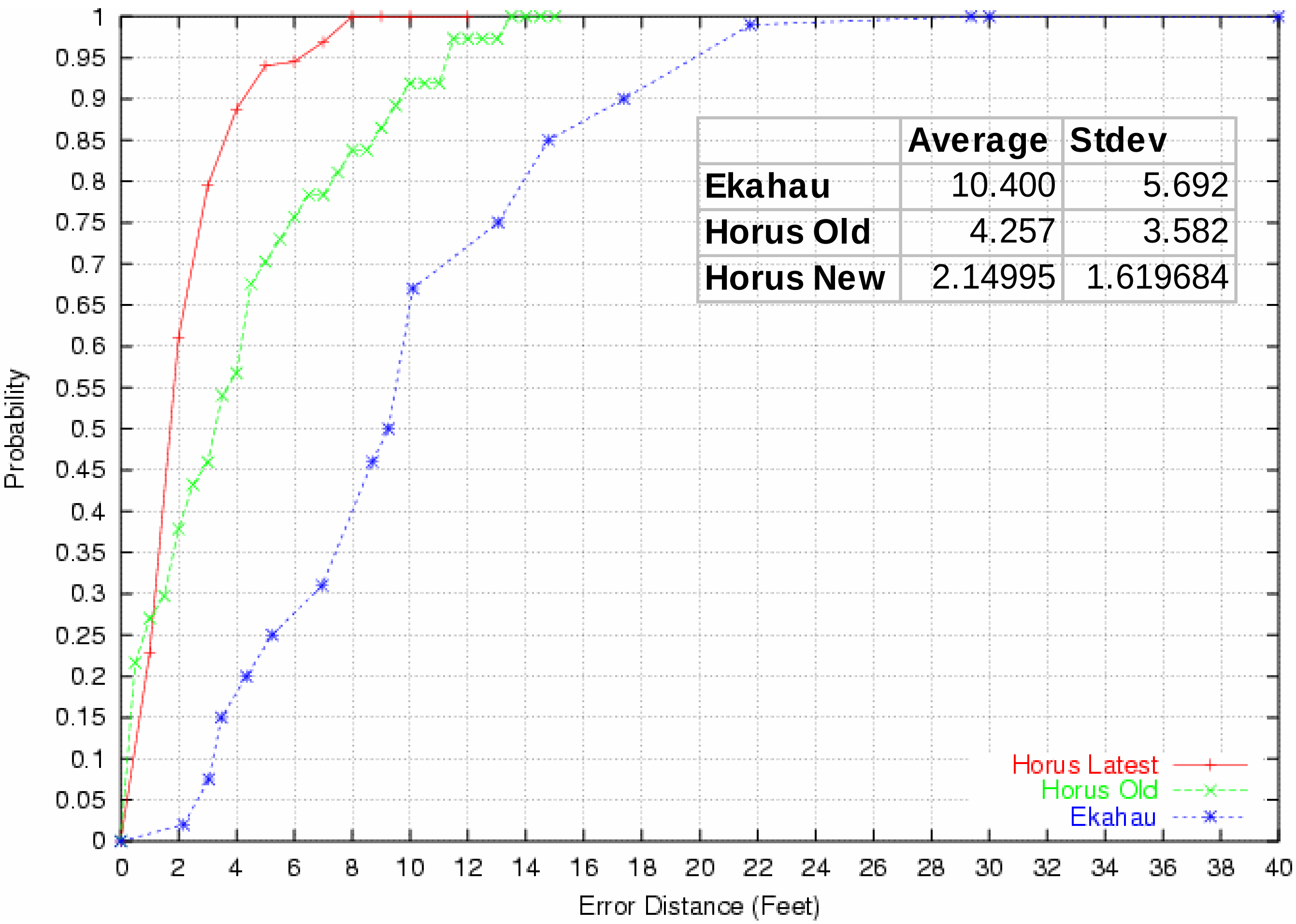




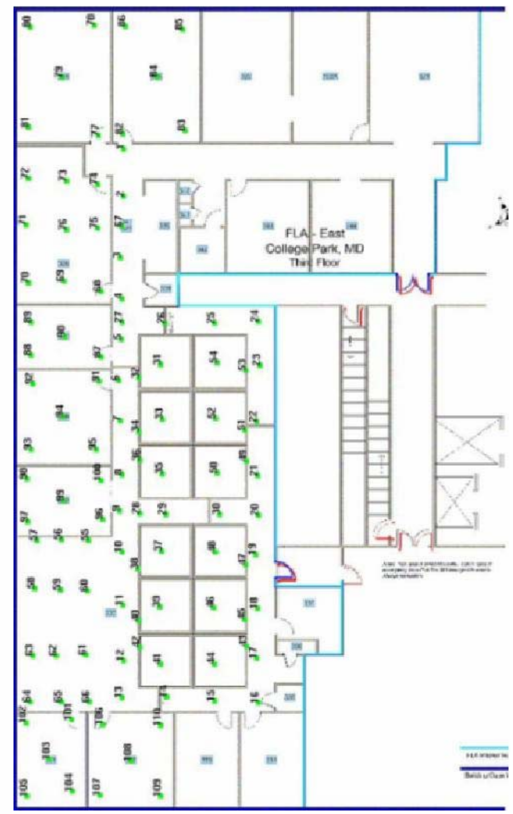
The Maryland Information and Network Dynamics Lab

Horus

Comparison With Other Systems: Ekahau



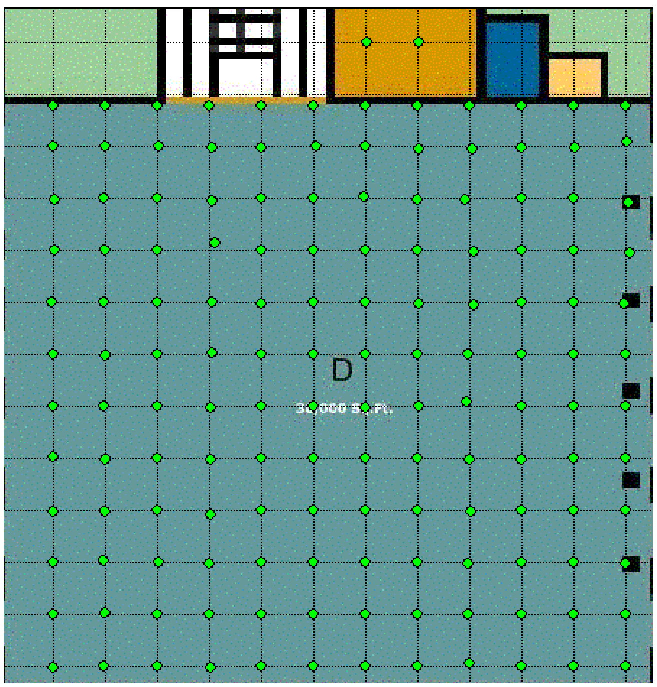
	Average	Stdev
Ekahau	10.400	5.692
Horus Old	4.257	3.582
Horus New	2.14995	1.619684

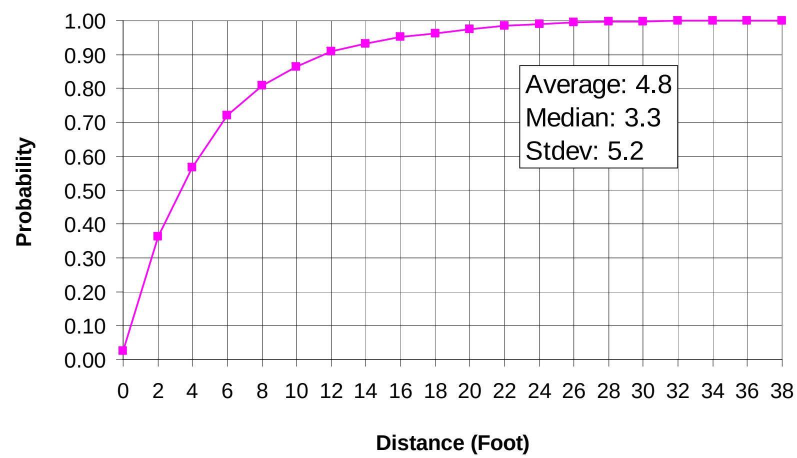


Horus

Baltimore Convention Center Test

- Large Open Hall 150’ by 150’





The Maryland Information and Network Dynamics Lab

Horus

Recent Enhancements

- Speed and Direction Estimation
- Latency Reduction
- Barrier Detection

- “Click and Connect”

- DEMO!!

Passive Determination of Location
Nuzzer Technology

Ashok K. Agrawala
Moustafa Youssef

University of Maryland

The Maryland Information and Network Dynamics Lab

Passive Object Recognition Problem

- Can the location of a person/object be determined without the person carrying an active device, e.g. a NIC or an RFID ?
- Are the changes in RSSI sufficient for this purpose ??
- Nuzzer Technology

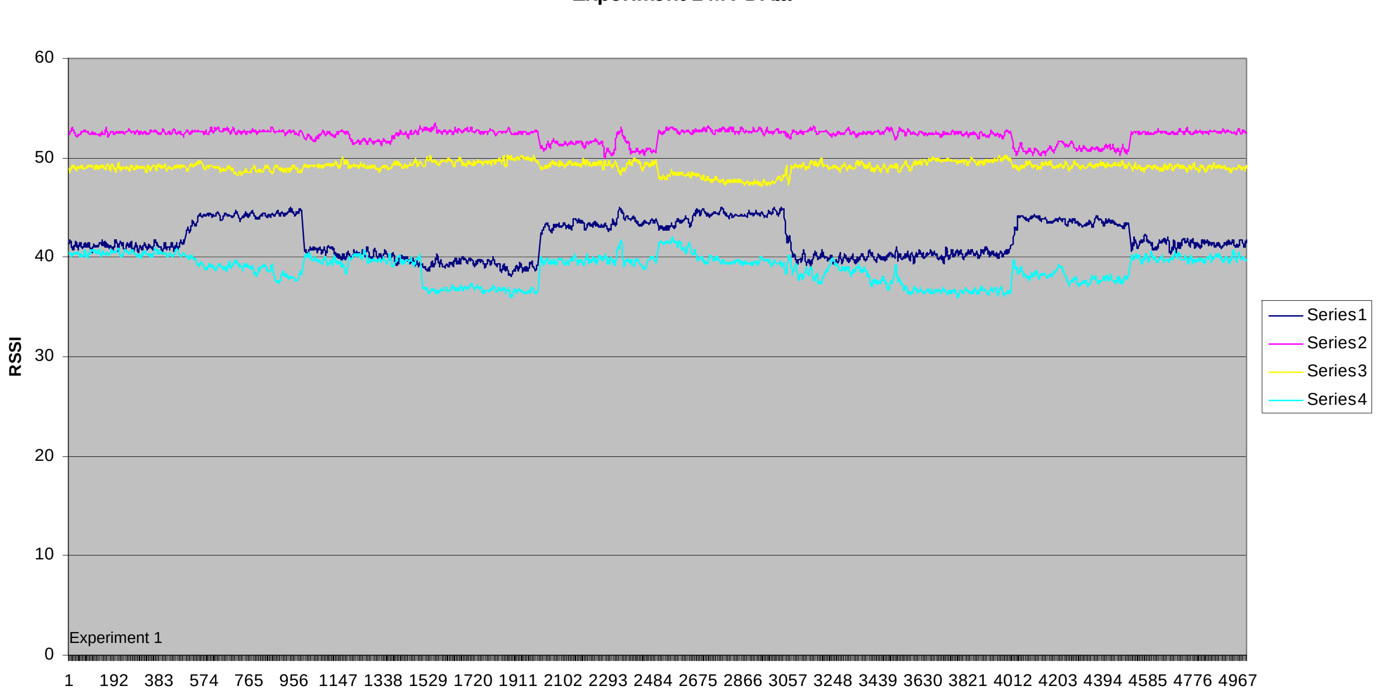
Nuzzer

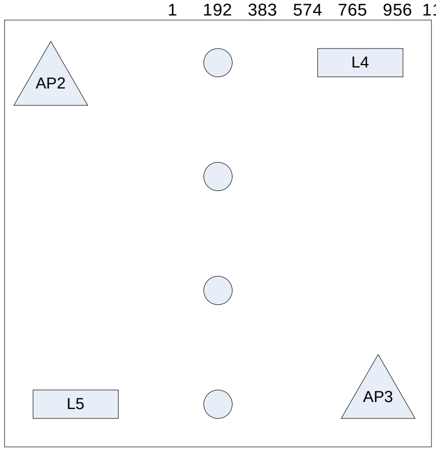
Initial Experiments

- Conducted controlled experiments in a bank vault
  - “no” outside RF interference
- Placed two APs and two laptops with NICs at selected locations
- Initially nobody in the room
- Then a person stands at 4 locations which are 3 feet apart.

Nuzzer

Experimental Setup and Results





Training set = SET1		Training set = SET2	
total	4920	total	4920
correct	4410	correct	4243
err	510	err	677
%err	10.36585	%err	13.76016

The Maryland Information and Network Dynamics Lab

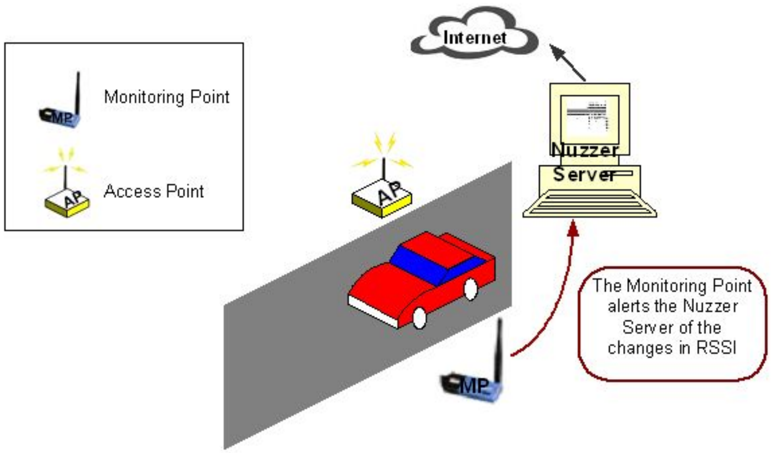
Nuzzer

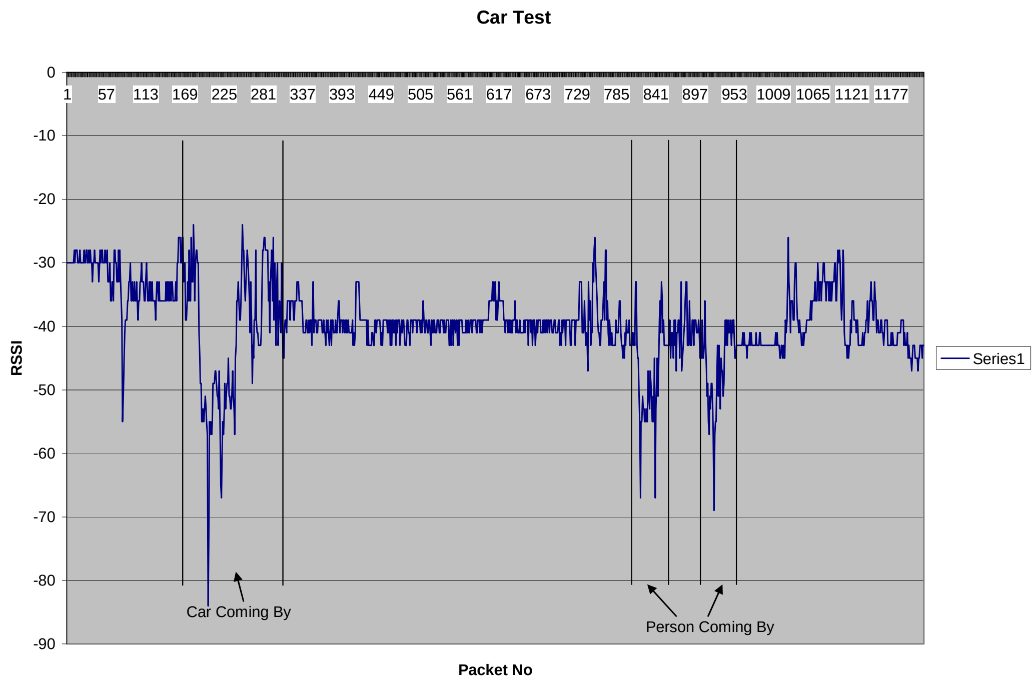
Nuzzer Indoors

- Initial results
  - > 85% accuracy
  - Can improve by using better techniques
- Performance limited by the accuracy/repeatability of RSSI measurements

- Can we use this approach outdoors to detect objects
  - Vehicles in a protected zone – Railroad track, Pipeline,…

Nuzzer Outdoors





The Maryland Information and Network Dynamics Lab

Nuzzer

Characteristics of RF Fields

- Need to understand the characteristics of RF fields
  - Multipath effects
    - Reflection
    - Refraction
    - Scattering
    - Diffusion
  - How are they affected by the presence of objects
    - Humans
    - Metal Objects
- Need a good model

The Maryland Information and Network Dynamics Lab

Nuzzer

Radio Wave Propagation

- Signal Intensity

$$J(x) = (J_0 x^{-D}) e^{i(2\pi f x c)}$$

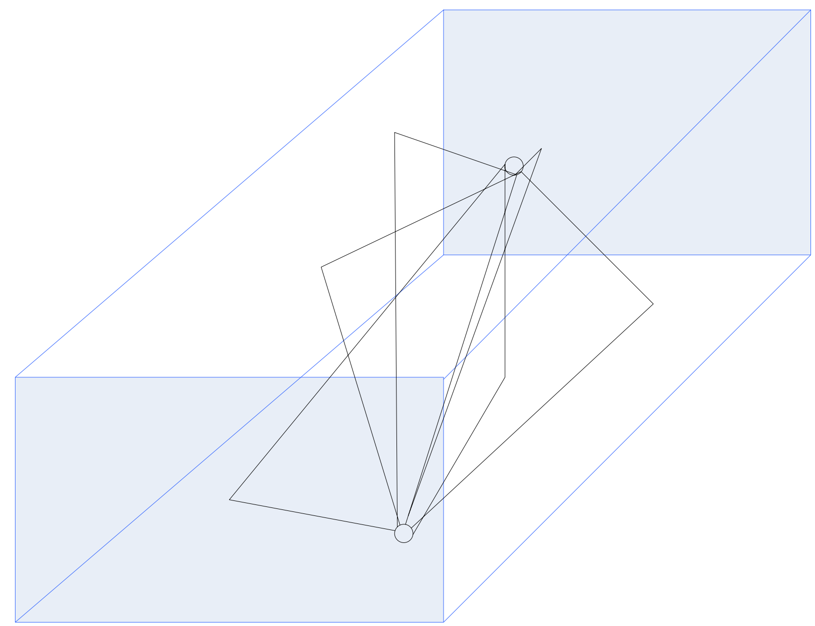
- *x = distance from source*
- J_0 *= signal amplitude at source*
- *f= frequency(2.4 GHz)*
- *D=Exponent value contributing to decay of signal as a function of distance x*
- *c= speed of light in free space*

The Maryland Information and Network Dynamics Lab

Nuzzer

Wave Propagation Model

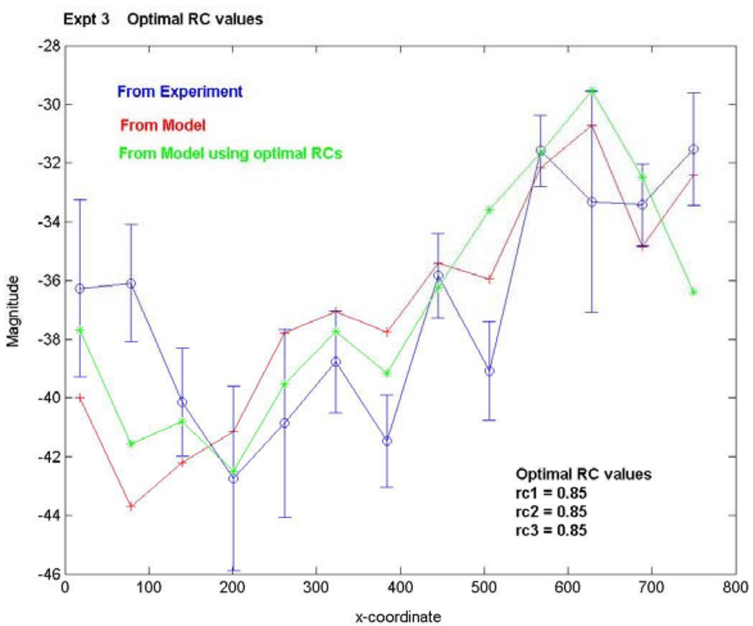
- Consider a 3D rectangular box
- One transmitter
- One receiver
- Take into account
  - Direct line of Sight
  - Six reflected Waves
- Validate the model with empirical measurements

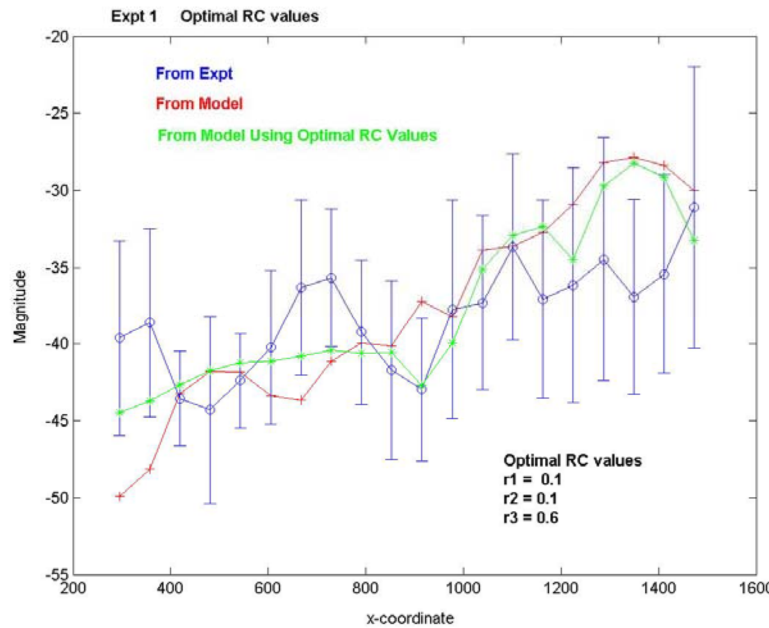


Nuzzer

Model Validation

- Measurements along one corridor
- Optimal Model values mostly within one sigma of the measured values

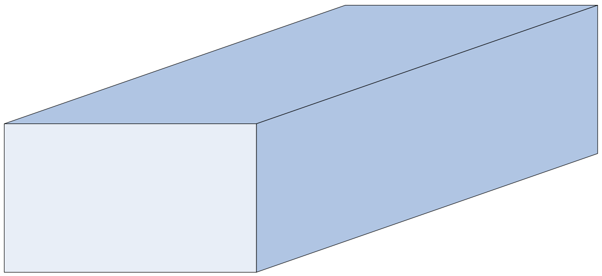


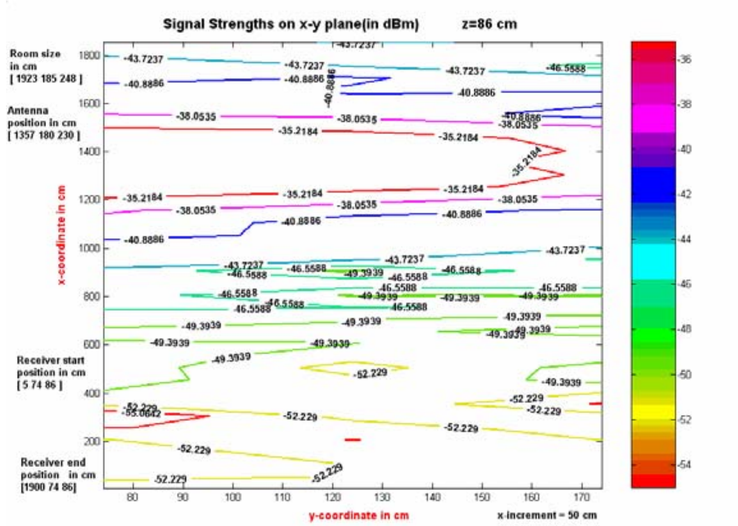


The Maryland Information and Network Dynamics Lab

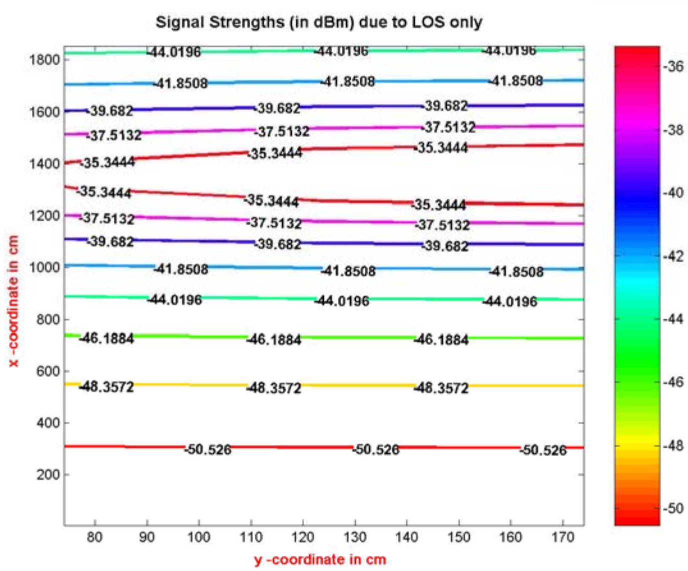
Nuzzer

2D Signal Plots – Corridor – XY Plane

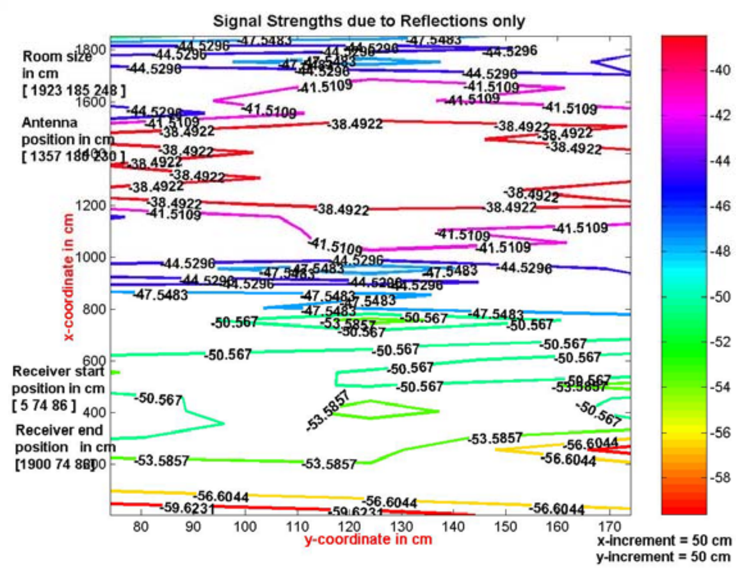




Combined



LOS Only

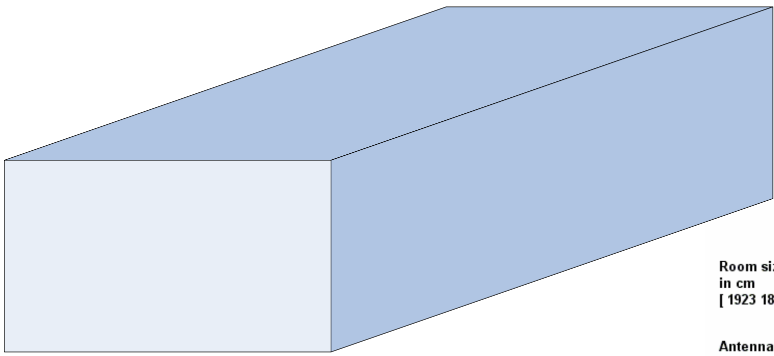


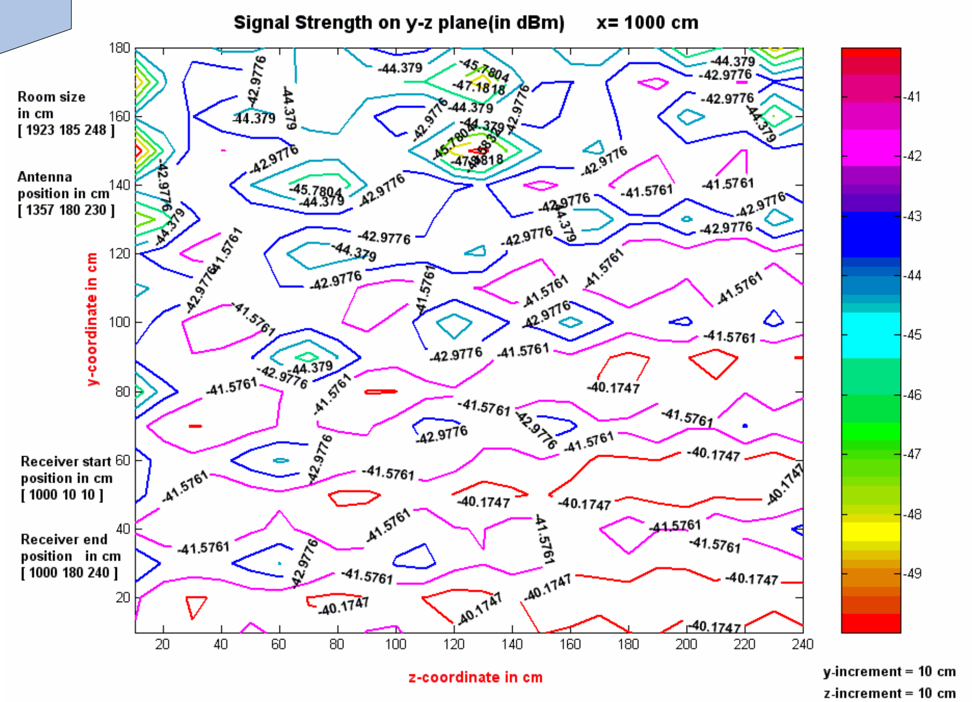
Reflections Only

The Maryland Information and Network Dynamics Lab

Nuzzer

2D Signal plots – YZ Plane





The Maryland Information and Network Dynamics Lab

Nuzzer

Effect of an Object on RF Field

- Initial model of an object
  - Block
    - Rectangular
    - Spherical
  - Empirical
    - Measurements with a person at a known location
    - Conducted measurements in the corridor

Estimated		Measured
-45.3929		-44.7
-42.2258	Front	-41.2
-38.7981	left	-36.7
-41.9157	behind	-40.8
-45.3929	right	-44.6

Model of Signal Strength

- Account for variabilities
  - Temporal
    - Due to noise in receive circuits
    - Movement of objects
  - Spatial
    - Variability due to multipath affects
- Use the results to improve Horus and Nuzzer
- Placement of Transmitters and Receivers
  - Avoid “holes”
  - Assess effectiveness of the locations

Applications

- Home
  - Security
    - Location of intruder
    - Internet intimation
- Office
  - Monitoring in the night at no additional costs
- Outdoors
  - Pipelines
  - Railroad tracks
  - Parking lots
  - …

Energy Efficient Routing

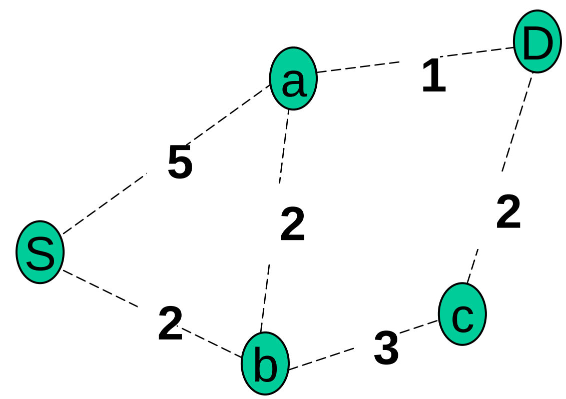
EER

Introduction

- Motivation
  - Energy is a scarce resource
  - Transmissions consumes large portion of node energy
  - Noise → Error Rate → Retransmission → Energy Consumption

- To reduce energy consumption, we need reduce the number of retransmissions.

- In ad hoc networks, paths with low number of retransmissions along the hops minimize the end-to-end energy consumption.

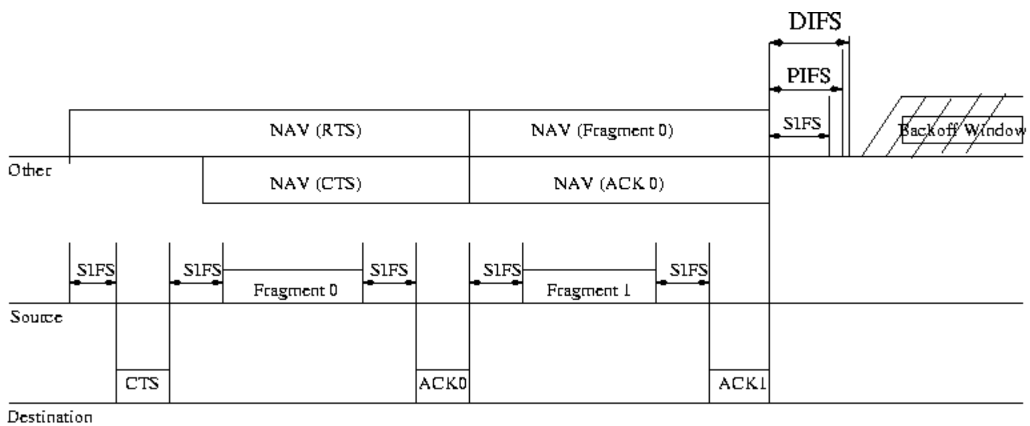


- Develop mechanism for AODV protocol using IEEE 802.11 as MAC layer to construct energy-efficient paths.

The Maryland Information and Network Dynamics Lab

IEEE 802.11 Fragmentation

- Fragmentation mechanism:
  - A Frame will be fragmented to frames with length no longer that *aFragmentThreshold*.
  - Each fragmented frame is sent as independent transmission.



  - Each is separately acknowledged.
  - Retransmissions occur per fragment.

- Fragmentation bits overhead:
  - o_1 bits: transmitted separately with each fragment and are not considered as a part of the fragment bits (e.g. PLCP preamble bits, PLCP header, ACK frame).
  - o_2 bits: transmitted within each fragment (e.g., frame header, frame CRC).

EER

Link Cost with 802.11 Fragmentation

- Cost of transmitting L bits using fragments of k bits:

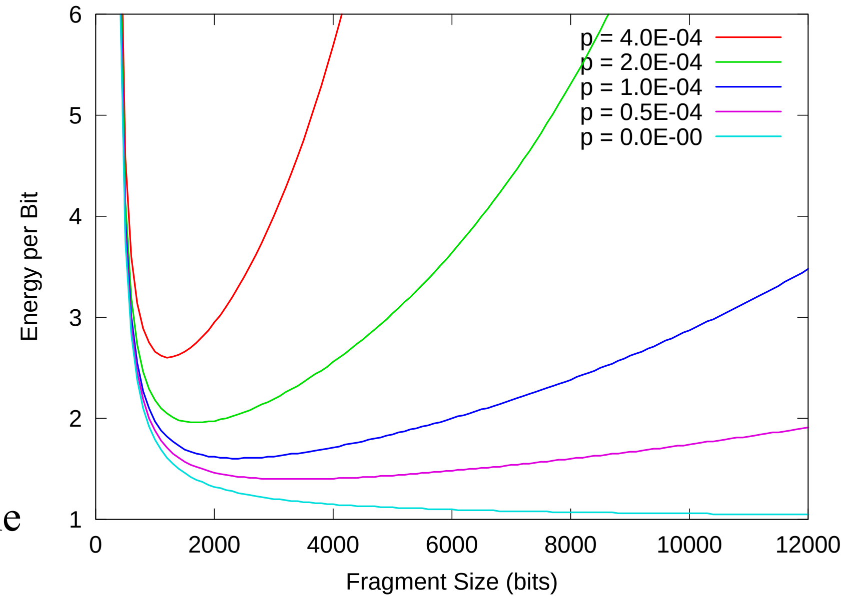
$$C = v \times (o_1 + k) \times \frac{L}{k - o_2} \times \frac{1}{(1-p)^k}$$

v: transmission energy per bit

p: bit error rate over the link

o_1: bits: transmitted separately with each fragment and are not considered as a part of the fragment bits (e.g. PLCP preamble bits, PLCP header, ACK frame).

o_2: transmitted within each fragment (e.g., frame header, frame CRC).



Energy consumption for each transmitted bit where o_1=250bits, o_2=300bits, and v=1unit

- Optimum fragment size is:

$$k^* = \frac{(o_2 - o_1)\beta - \sqrt{(o_2 - o_1)^2\beta^2 - 4\beta(o_1 + o_2 - o_1 o_2 \beta)}}{2\beta}$$

where β is $\ln(1-p)$

EER

Bit Error Rate Estimation in AODV

- Link cost is calculated at the receiver side only
  → Link bit error rate needs to be estimated at the receiver side only.
- Estimation mechanisms:
  – Probe Packets
    - Each node broadcasts a probe packet periodically.
    - Each probe has a sequence number.
    - Receiver can track the number of dropped packets
      → estimate the bit error rare
  – Signal-to-Noise Ratio (SNR = 10*log(Pr/N))
    - Bit error modeled as function of SNR of the link

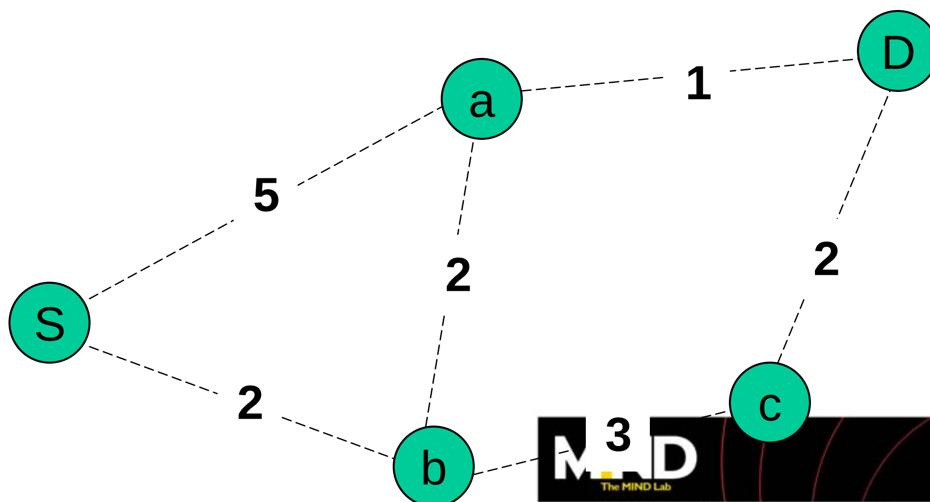
$$p \propto erfc(\sqrt{constant \times SNR})$$

    - Each node is capable of measuring the SNR for each received packet.
  – AODV uses periodic *Hello* packets each *t* sec jittered by up to ±*0.25t*.

The Maryland Information and Network Dynamics Lab

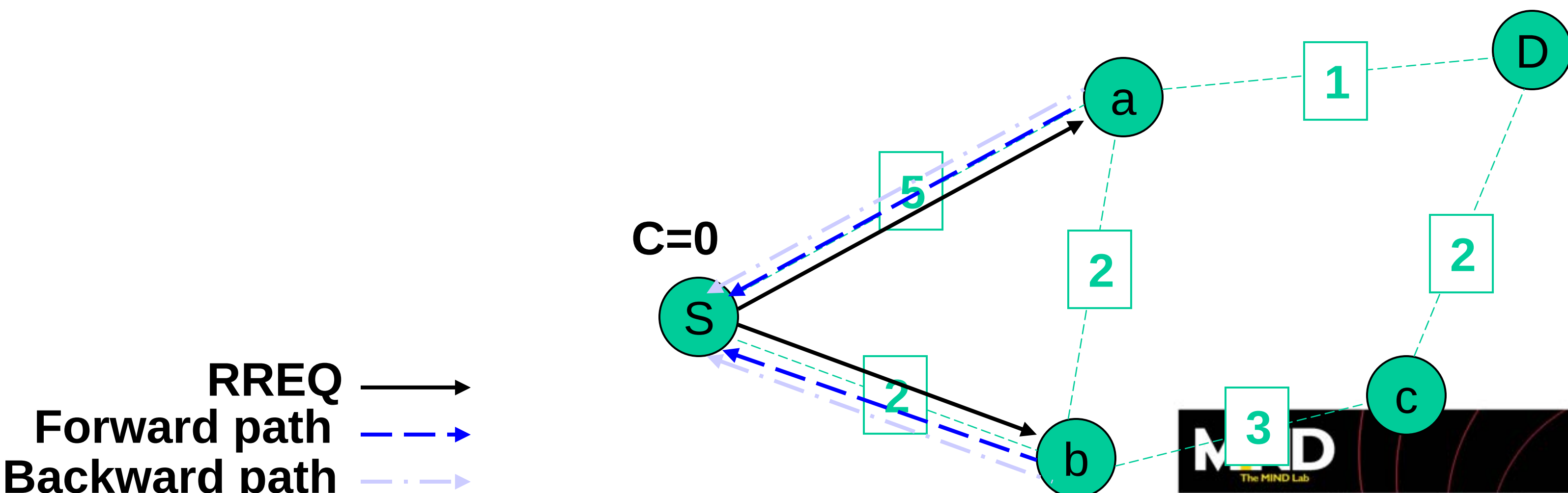
AODV in Noisy Environments

- Construct forward path from S to D



AODV in Noisy Environments

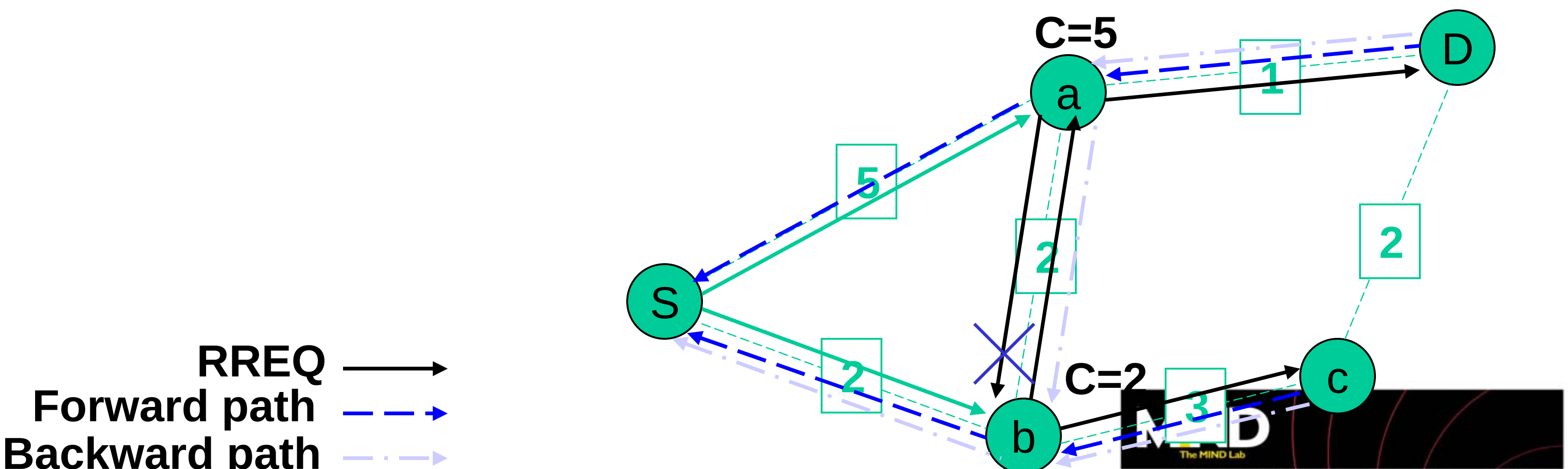
- Construct forward path from S to D
  - S broadcasts RREQ augmented with a cost field, C, initialized to Zero
  - Each node receives RREQ
    - Updates the cost filed by the link cost
    - Stores the backward path to S



The Maryland Information and Network Dynamics Lab

AODV in Noisy Environments

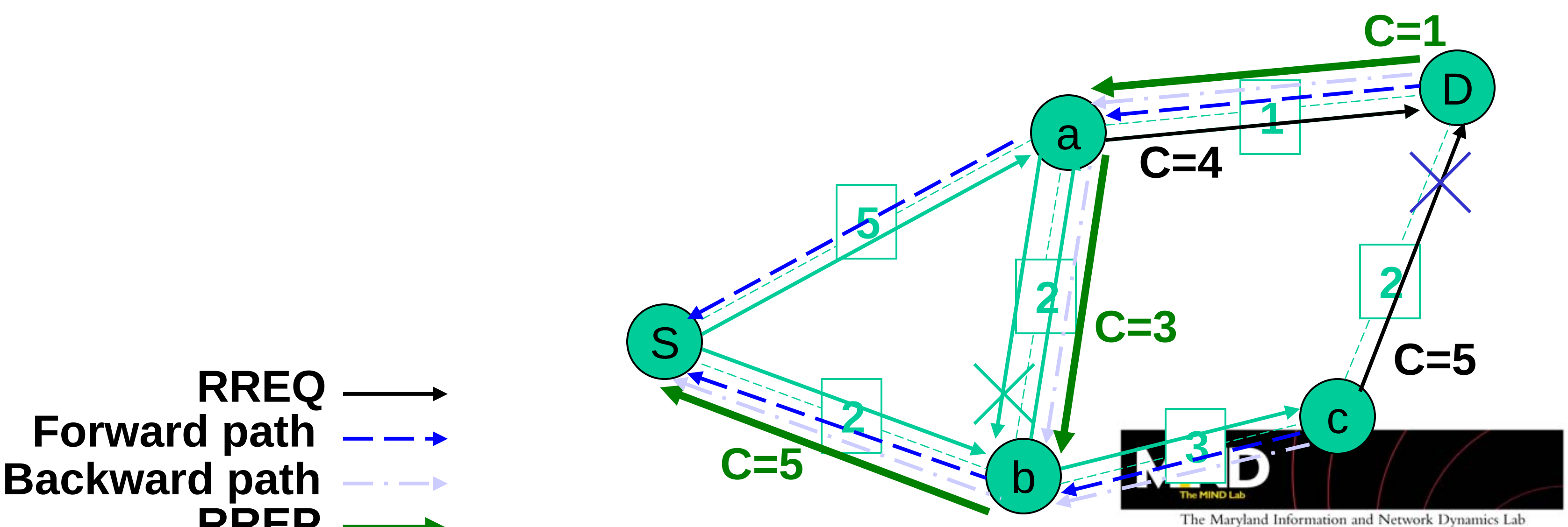
- Construct forward path from S to D
  - S broadcasts RREQ augmented with a cost field, C, initialized to Zero
  - Each node receives RREQ
    - Updates the cost filed by the link cost
    - Stores the backward path to S
  - Each node accepts RREQ with lower cost and rebroadcasts it



The Maryland Information and Network Dynamics Lab

AODV in Noisy Environments

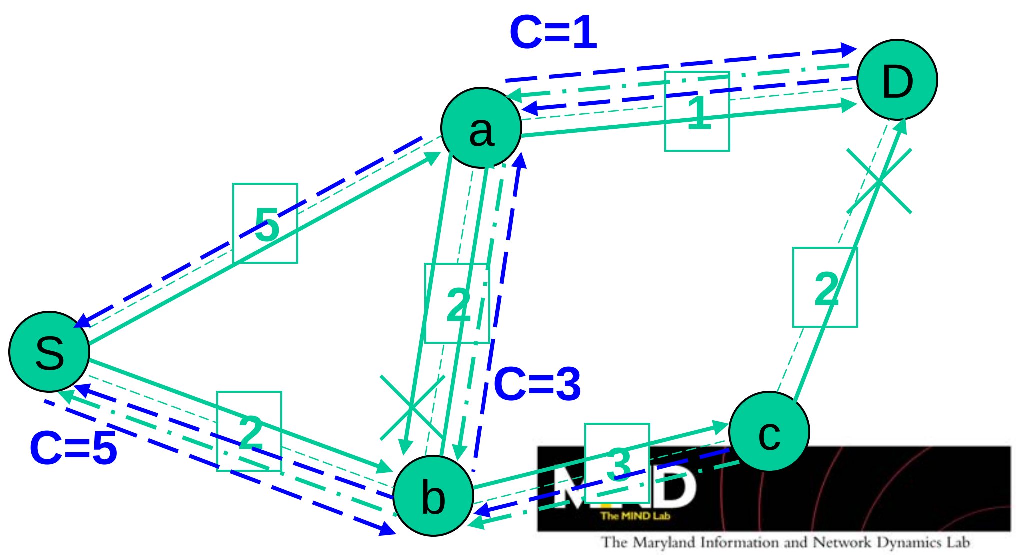
- Construct forward path from S to D
  - S broadcasts RREQ augmented with a cost field, C, initialized to Zero
  - Each node receives RREQ
    - Updates the cost filed by the link cost
    - Stores the backward path to Each node accepts RREQ with lower cost and rebroadcasts it
  - RREP follow the backward path, contains
    - Partial cost to D
    - Optimum fragment over the transmitted link



The Maryland Information and Network Dynamics Lab

AODV in Noisy Environments

- Construct forward path from S to D
  - S broadcasts RREQ augmented with a cost field, C, initialized to Zero
  - Each node receives RREQ
    - Updates the cost filed by the link cost
    - Stores the backward path to Each node accepts RREQ with lower cost and rebroadcasts it
  - RREP follow the backward path, contains
    - Partial cost to D
    - Optimum fragment over the transmitted link



EER

Performance Evaluation

- NS-2, simulation parameters
  - 49 nodes
  - Area of 700mX700m
  - 12 UDP flows, 1500 bytes each 0.2 sec
- Routing schemes
  - AODV Standard (SD_fix, SD_var)
  - Energy-Aware (EA_fix, EA_var)
  - Retransmission-Aware (RA_fix, RA_var)
- 250 seconds simulation 50 seconds warm up
- Flows start in serial with gap of 5 seconds.
- Each point in the results is the average of 10 runs.
- Cost of single bit transmission over a link is 60μJ.

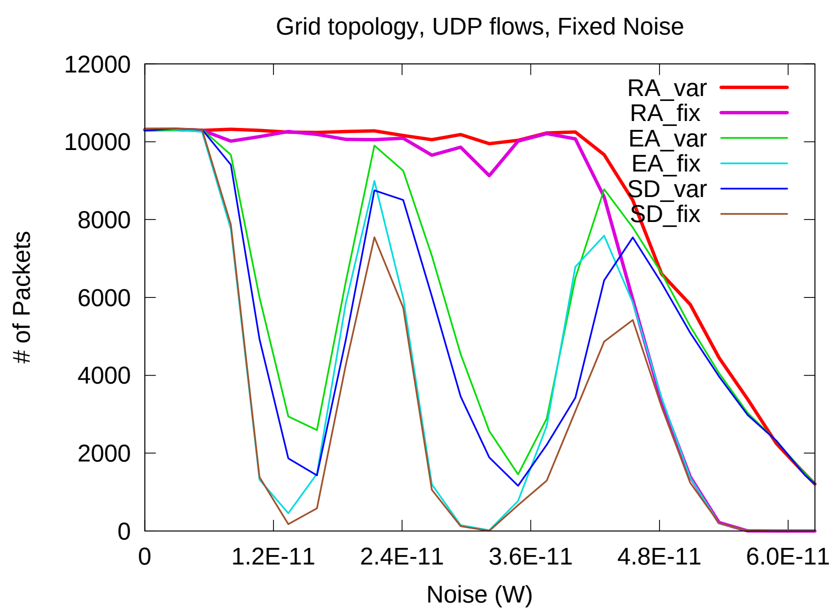
EER

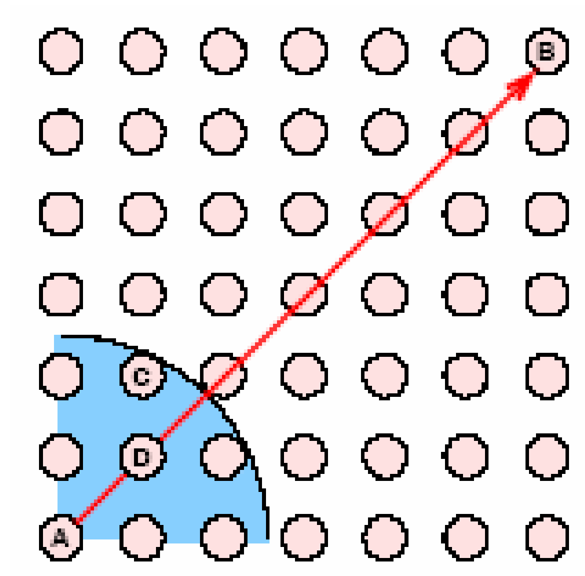
Performance Evaluation

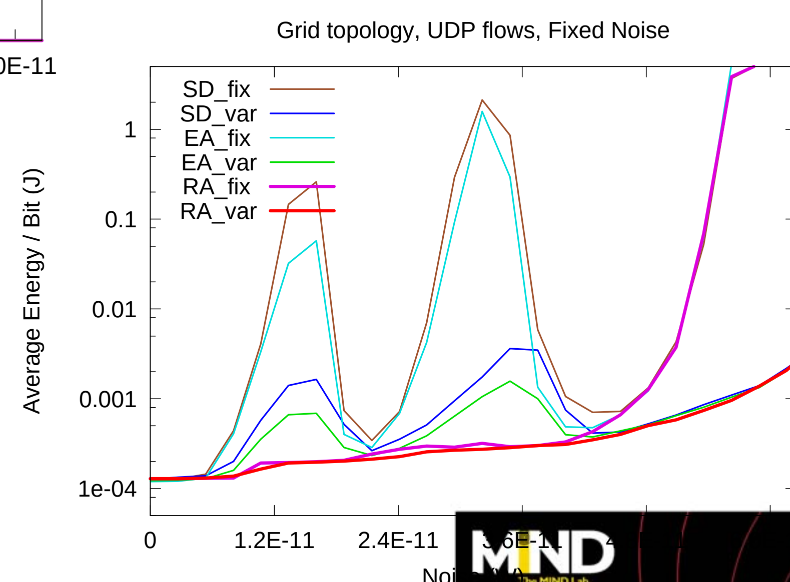
- Noise Models
  - Region partitioned into small square grids (50 *x* 50 each).
  - Grid's noise is Gaussian noise with μ and σ
  - μ is chosen to vary between *Nmin* and *Nmax*
    - Fixed noise environment*: Nmin* is equal to *Nmax* [0.0, 20.0×10^{-11}] *W*.
    - Random noise Environment*: Nmin*=0.0*W Nmax* between [0.0, 20.0×10^{-11}] *W*.
  - σ is chosen to be equal to (0.1x μ)*W*.

EER

Grid Topologies



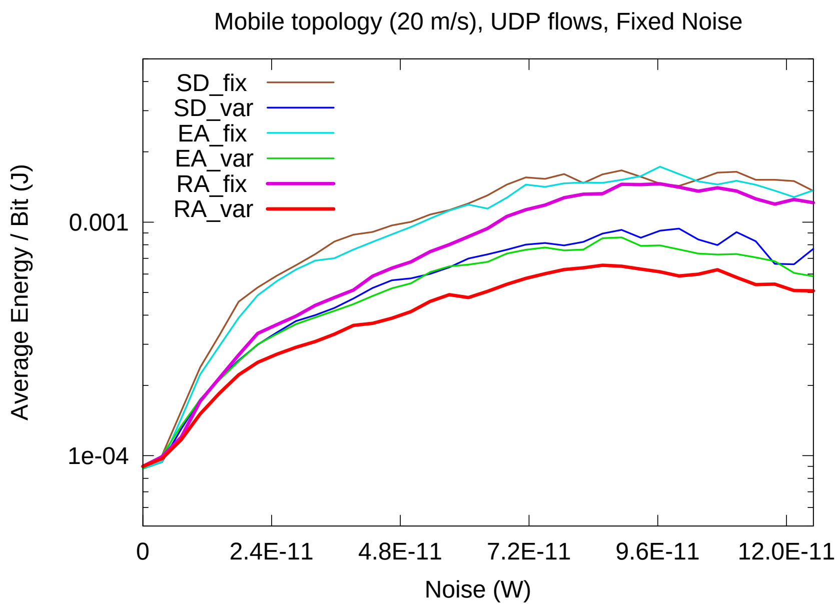


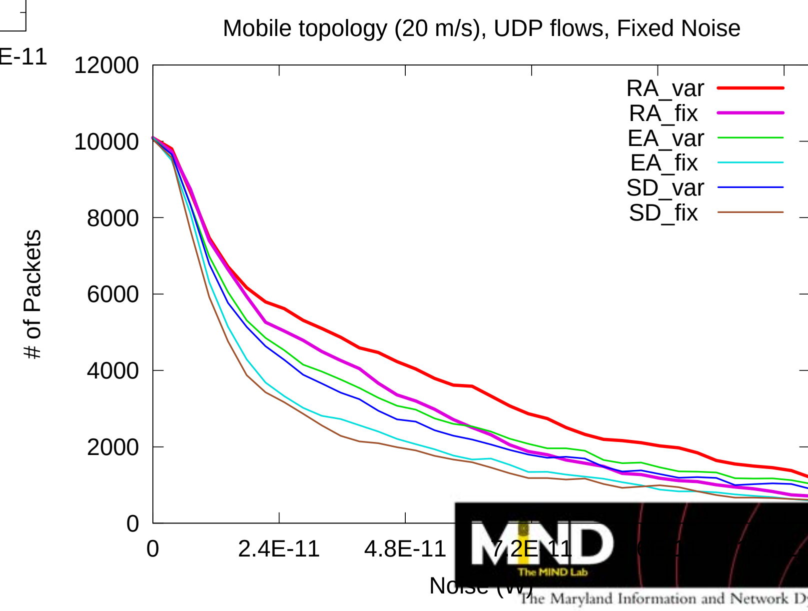


The Maryland Information and Network Dynamics Lab

EER

Mobile Topologies





The Maryland Information and Network Dynamics Lab

EER

Conclusion

- Our modifications and techniques can be ported and easily implemented on other routing protocols.
- Performance gains of our schemes will be magnified as the average path length becomes large, in large scale networks (hundreds or thousands of nodes).
- Other estimation mechanisms
- We assumed that the network noises characteristics are fixed during the network life time. Such assumption may not be true in some environments. Therefore, we need to develop mechanisms that discover and redirect the current flow to a new optimum path as soon as it changes.

ENE

Enhancing 802.11 for Noisy Environments

The Maryland Information and Network Dynamics Lab

ENE

Enhancement of IEEE 802.11 DCF in Noisy Environments

- In noisy environments, large number of unsuccessful transmissions are due to noise corruption
- IEEE 802.11 doesn't differentiate between packet loss due to *packet collision* or *packet error*.

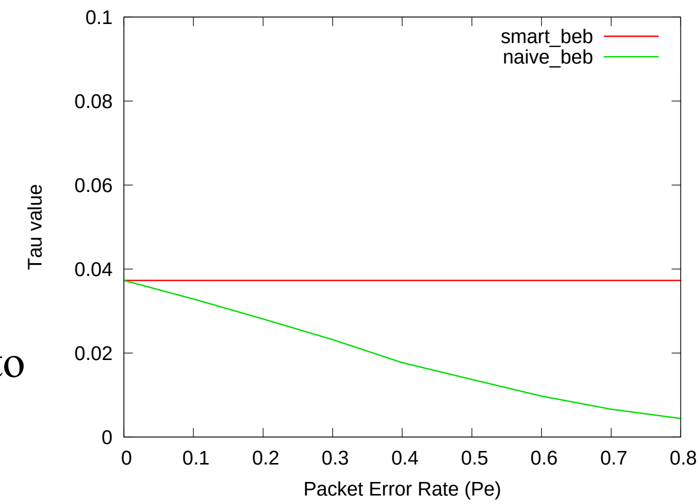
  →BEB doubles CW range in the cases of packet errors → unnecessary large idle slots → performance degradation

- Propose a new mechanism to enhance the standard 802.11 BEB mechanism (BEB_{naive}) capable of differentiating between the collision loss and the error loss

  → BEB will double the contention window ***only*** for the case of the collision (BEB_{smart}).

BEB_{smart} Implementation (Basic access)

- Using a Markov chain model to model BEB, we calculate the probability a node transmits in a randomly chosen time slot, τ.
- Mechanism:
  - Each node calculates τ_{ideal}
  - Each node maintains a parameter *p*, initially set to zero.



  - When ACK is missing, node doubles the contention window with probability (1 – *p*) and resets its *CW* to W_0 with probability *p.*
  - Each node measures its τ every T time slots.
  - If $\tau > \tau_{ideal}$ → too *frequent* transmissions → few idle slots → *Decrease p* by δ
  - If $\tau < \tau_{ideal}$ → too *few* transmissions → large idle slots → *Increase p* by δ

Simulation Results

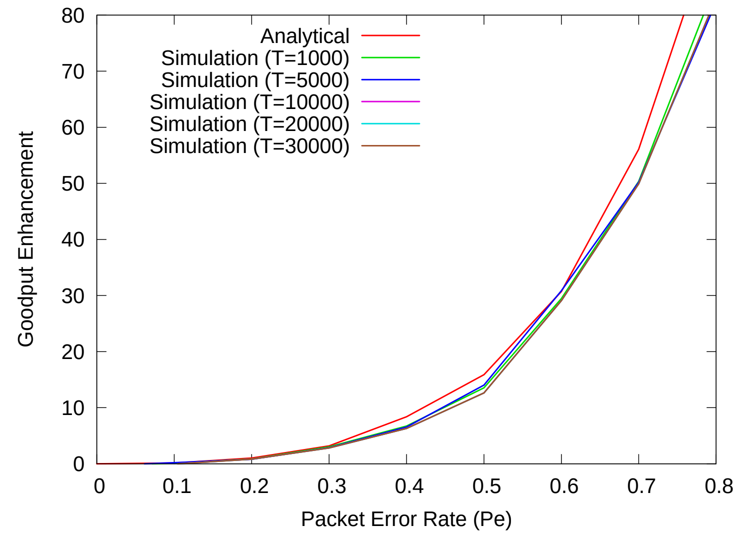
ENE

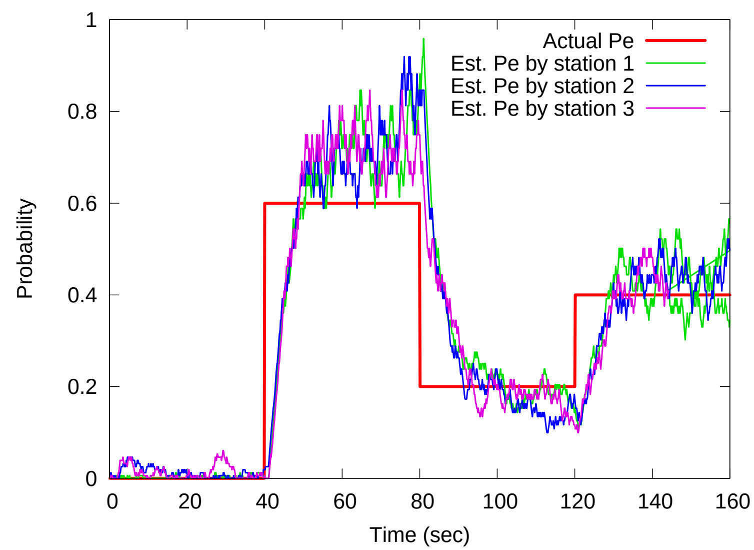
- 10 nodes transmitting data packets of size 500 bytes at data rate 22Mbps where $\delta = 0.01$.

- p is the percentage of the dropped packet assigned to the noise corruptions only.

$$p = \frac{(1 - p_c)p_e}{p_c + p_e - p_c p_e}$$

  - From the maintained parameter p, a node can estimate its packet error rate p_e





The Maryland Information and Network Dynamics Lab

Location-aware Enhanced DCF (LED)

LED

Introduction

- IEEE 802.11 DCF is based on Carrier Sense Multiple Access (CSMA) mechanism
  - a station may transmit if and only if the medium is sensed to be idle.
  - not efficient in shared channel use due to its overcautious approach.

- Capture Effect:
  - When two transmissions are received by the same receiver, the signals of stronger transmission will capture the receiver modem, and signals of the weaker transmission will be rejected as noise.

- Capture Model:
  - Captures a particular transmission if the received energy *Pr* sufficiently exceeds all *n* other combined received energy. This ratio α is called the *capture ratio*.

$$P_r > \alpha \sum_{i=1, i \neq r}^{n} P_i$$

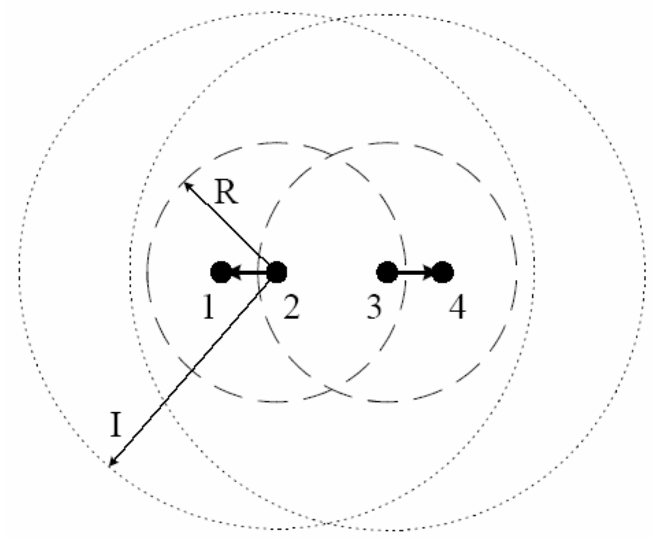
The Maryland Information and Network Dynamics Lab

LED

Introduction (contd')

EXAMPLE

- Two concurrent connections share the same wireless communication channel. The first from station 2 to station 1 and the second is from station 3 to station 4
- In IEEE 802.11 DCF, once a connection seizes the channel, the other connection would have detected the carrier signals of this connection and remain blocked.

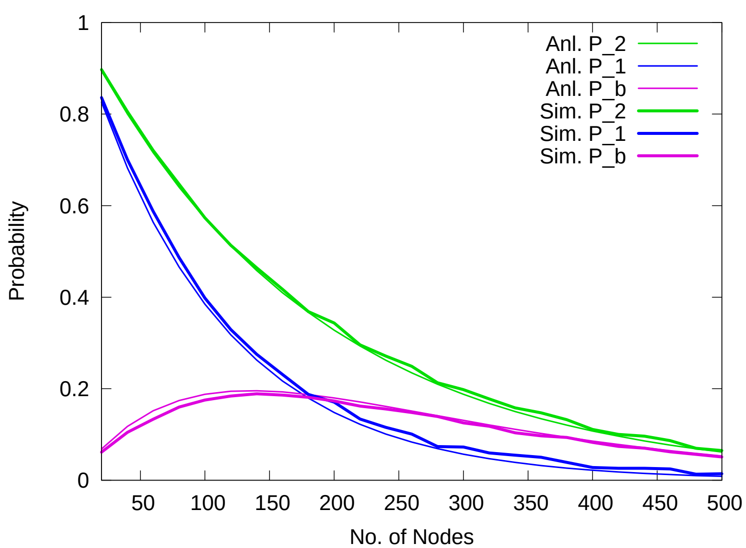


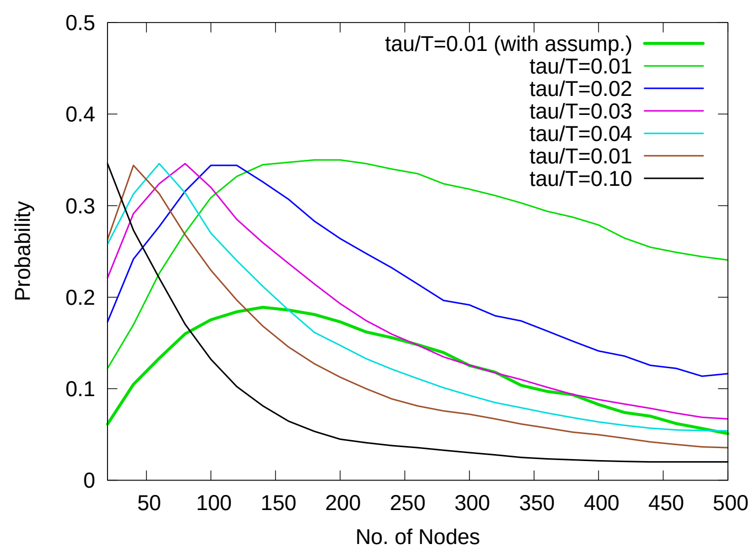
- However, if stations are positioned in such a way that the energy levels of stations 3 and 4's transmissions as measured at stations 1 and 2 are not strong enough that stations 1 and 2 can still capture each other's transmissions → both connections can go simultaneously

LED

Analysis of Blocking Probabilities with Capture Effect

- Using a conservative model, we analytically studied the probability a node, detecting on going transmissions, can transmit without corrupting others.
- Verified the analytical results using simulation.
- Studied a realistic model using simulation.





The Maryland Information and Network Dynamics Lab

LED Mechanism

- Physical Layer Design
  - Unlike regular IEEE 802.11 PHY designs, a receiver is able to correctly detect and capture a strong frame regardless of the current state of the receiver, for example, “Message-In-A-Message” (MIM) support.

- MAC Layer Design
  - insert a block of information called ENH (“Enhanced”) as part of the PLCP header to provide the additional information needed for the LED.
  - When other stations overhearing ENH information, they are able to better assess whether their own transmissions may harm this ongoing delivery or not.

LED

LED Mechanism

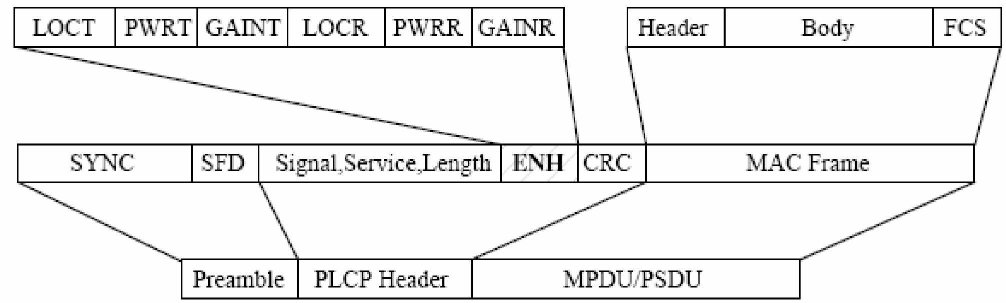


Fig. 9. Frame structure

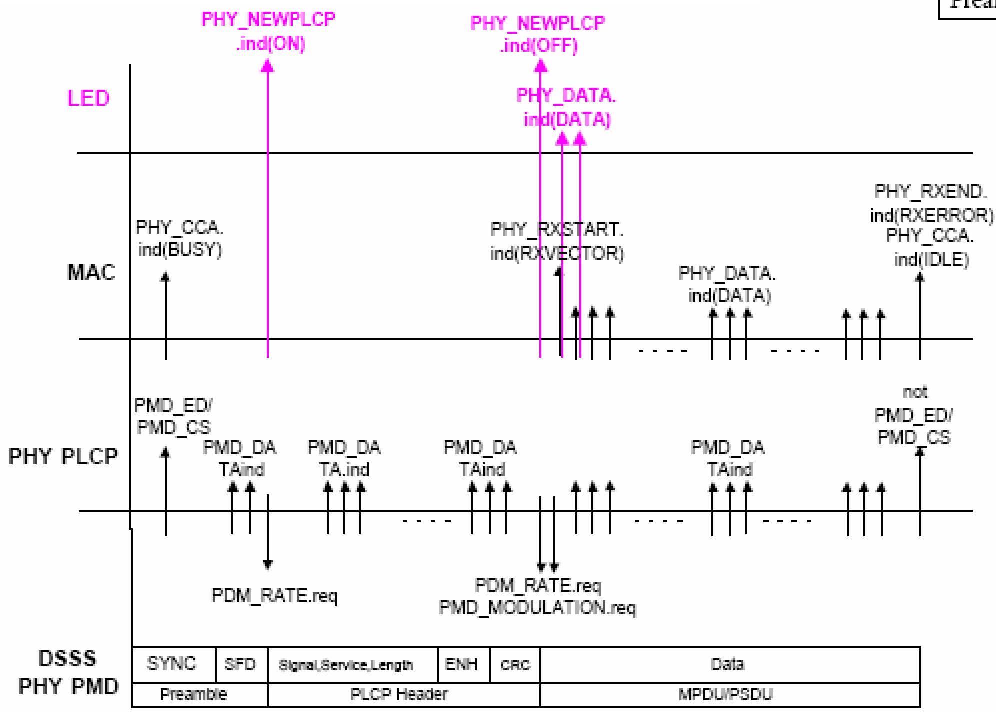


Fig. 10. PHY-MAC interactions

The Maryland Information and Network Dynamics Lab

LED

Performance Evaluation

- NS-2, simulation parameters
  - Variable number of nodes.
  - Area of 1000x1000m^2
  - UDP connections, 1000 bytes with different rate
  - Data rate is 11Mbps
- Schemes
  - Original IEEE 802.11
  - MACAW
  - LED_CS: a station receiving a frame it cannot decode, assumes its transmission will not interfere with that ongoing delivery.
  - LED_RX: a station assumes its transmission will interfere with the ongoing delivery under receiving a frame it cannot decode.
- Capture ratio α is set to 5, Transmission Radius=250m, Interference Radius=550m
- Simulation time is 50 seconds.
- Each point in the results is the average of 10 runs.

LED

Performance Evaluation (contd')

- Various number of connections, each with UDP rate of 20 packets per second.

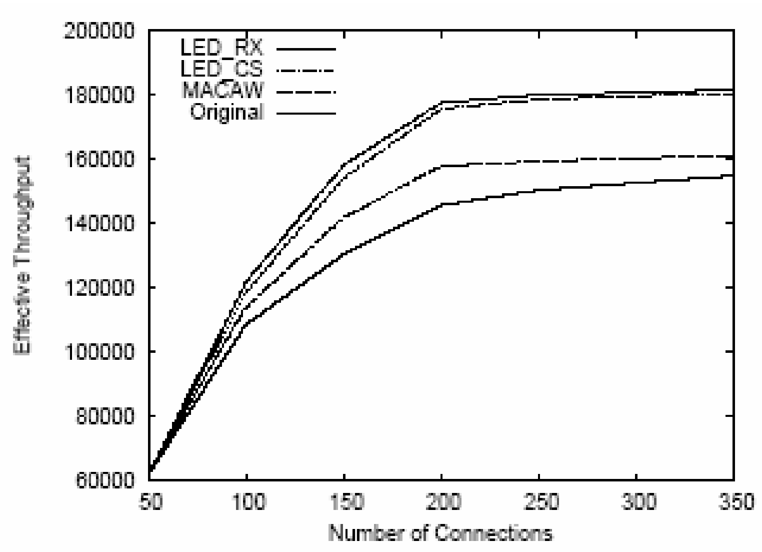


Fig. 12. Effective throughput versus node density

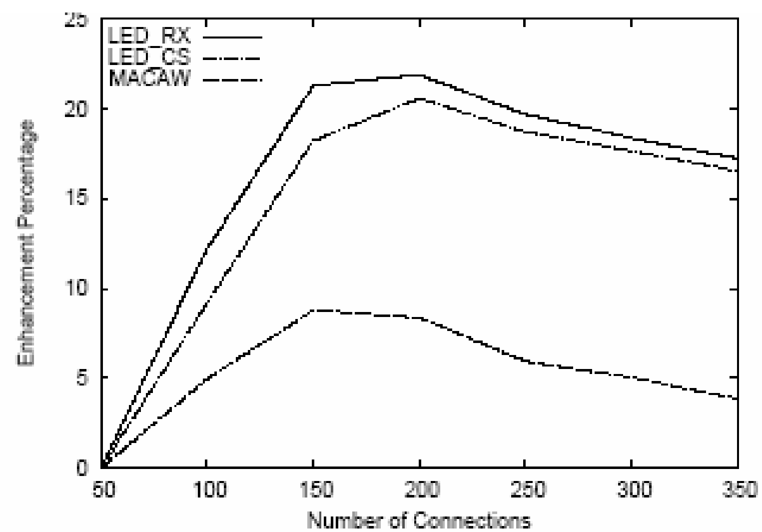


Fig. 13. Throughput enhancement over Original mechanism versus node density using RTS/CTS access mode

The MIND Lab
The Maryland Information and Network Dynamics Lab

LED

Performance Evaluation (contd')

- 50 UDP connections, each with various packet rates.

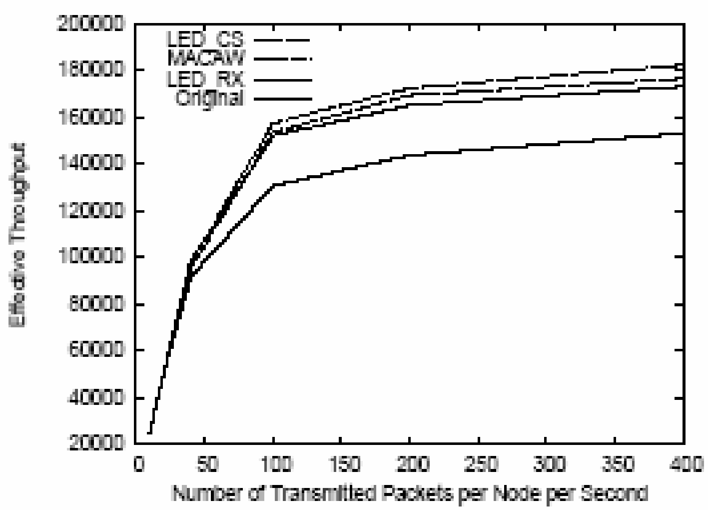


Fig. 16. Effective throughput versus network load using RTS/CTS access mode

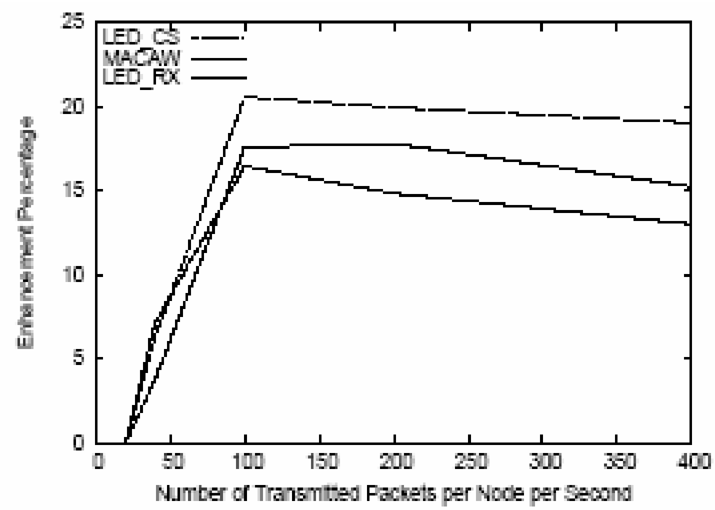


Fig. 17. Throughput enhancement over Original mechanism versus network load using RTS/CTS access mode

The Maryland Information and Network Dynamics Lab

WiFiTC

WiFi Traffic Characterization

The Maryland Information and Network Dynamics Lab

WiFiTC

Measurement Setup

- Location: 4th floor, A.V.Williams Bldg
- Duration: Feb 9 (Monday) 0 am – Feb 22 (Sunday) 12 pm (2 weeks)
- Target traffic: Wireless LAN traffic of one umd AP (at Rm. 4149) on Channel 6
- Methodology:
  - Three wireless sniffers at Rm. 4140 (closest to the AP), Rm. 4166, and Rm. 4132
  - Wireless sniffers capture MAC traffics
  - Merging three sniffers to reduce the measurement losses

WiFiTC

802.11 Traffic Characterization

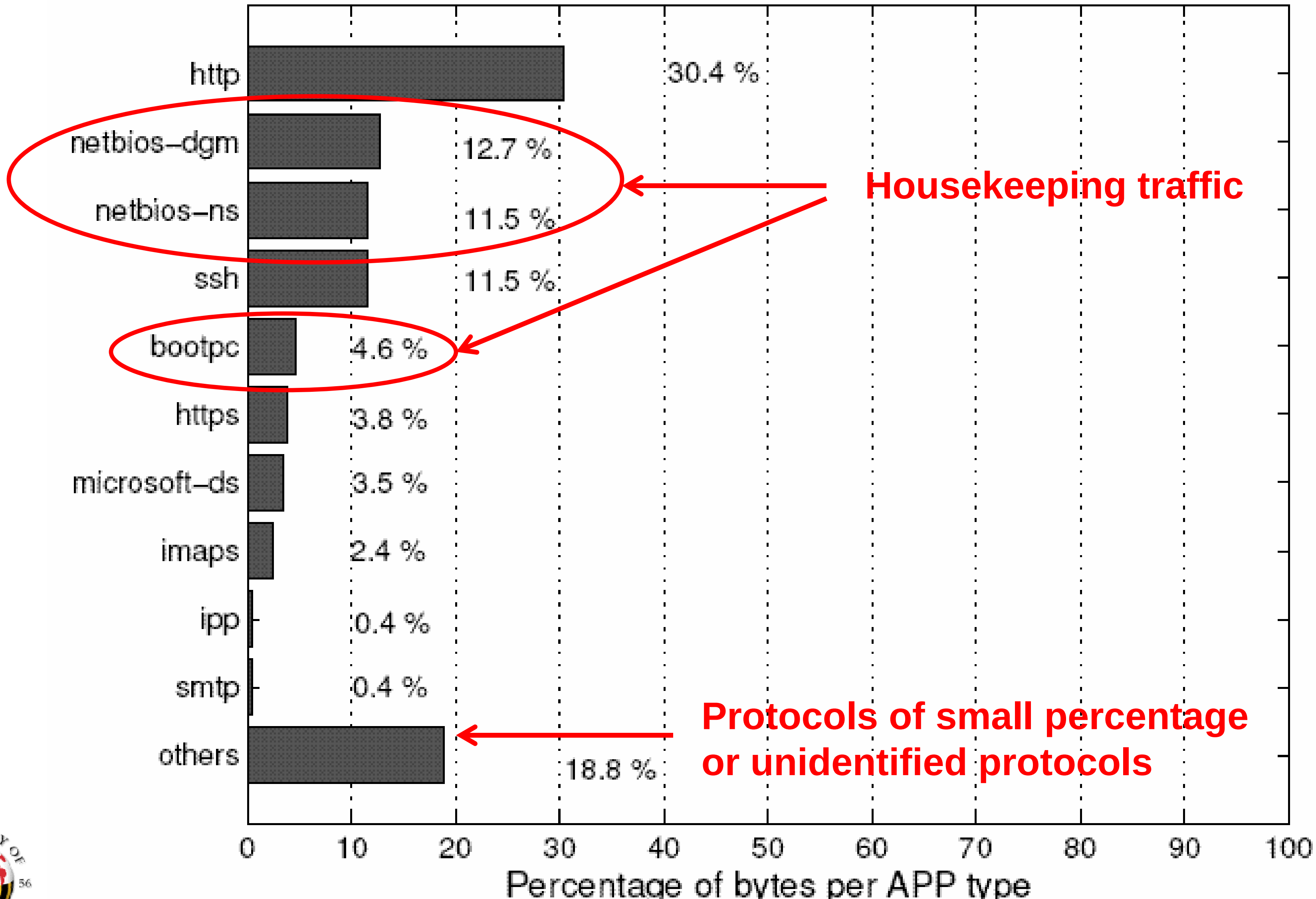
- Previous results: characterization of traffic, error, types, frame size, and data rate on only MAC layer
- New results:
  1. Above-MAC Layer Characterization
     - APP, IP, and LLC (Logical Link Control) Layer
  2. Session Analysis
     - Session: A traffic duration of a wireless STA sending/receiving, which is expired when the STA not send/receive for some time threshold (e.g. 30 minutes)

Above-MAC Traffic Characterization

- APP protocol mix
  - About 40% in bytes are housekeeping traffic (NetBios, boot protocol, etc) for windows name/browse service and bootstrap, etc.
  - About 50% in bytes are used for well-known user applications (http, ssh, email, file share, etc)
  - 76% of wireless STAs run Windows OS.
- IP protocol mix
  - 16% in number are used for VPN connection.
- LLC type mix
  - ARP (Address Resolution Protocol) traffic amounts to 19% in number, 6% in bytes.
  - IP frame size: From-AP has larger than To-AP due to (small) request/ (large) response.

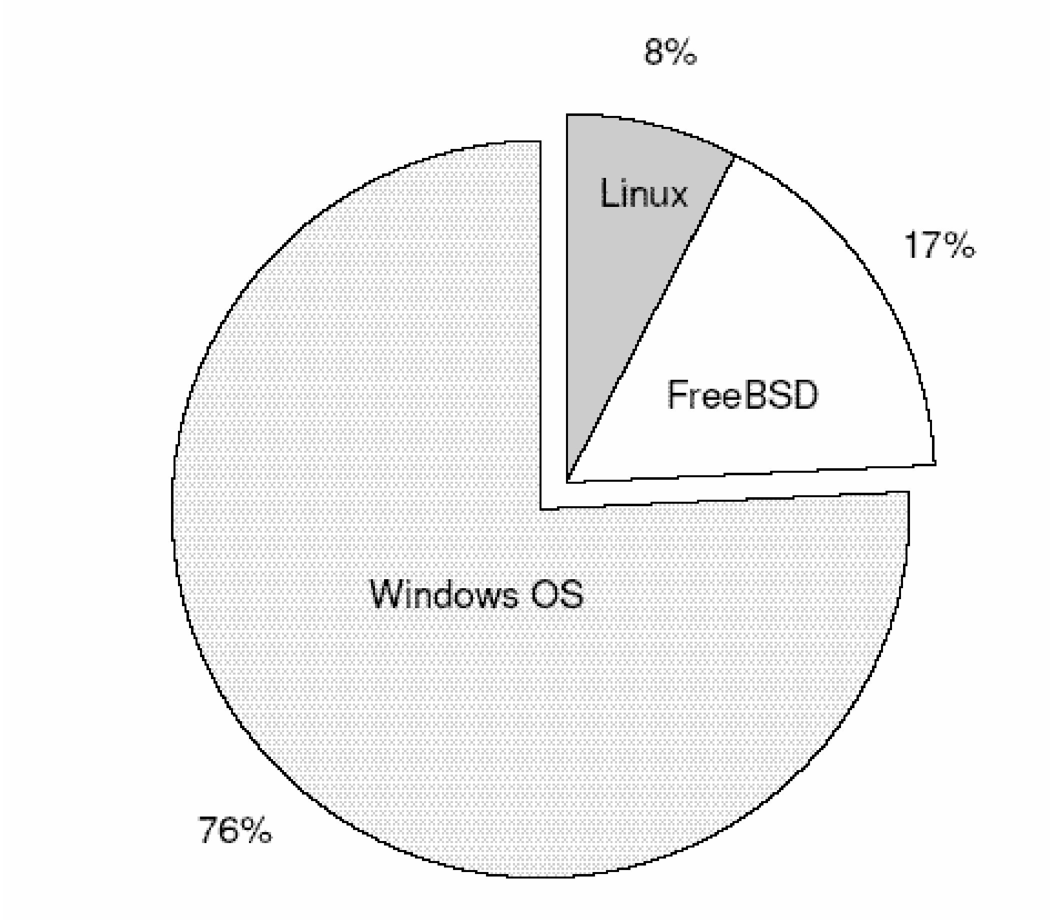
WiFiTC

APP Protocol Histogram



WiFiTC

OS Distribution

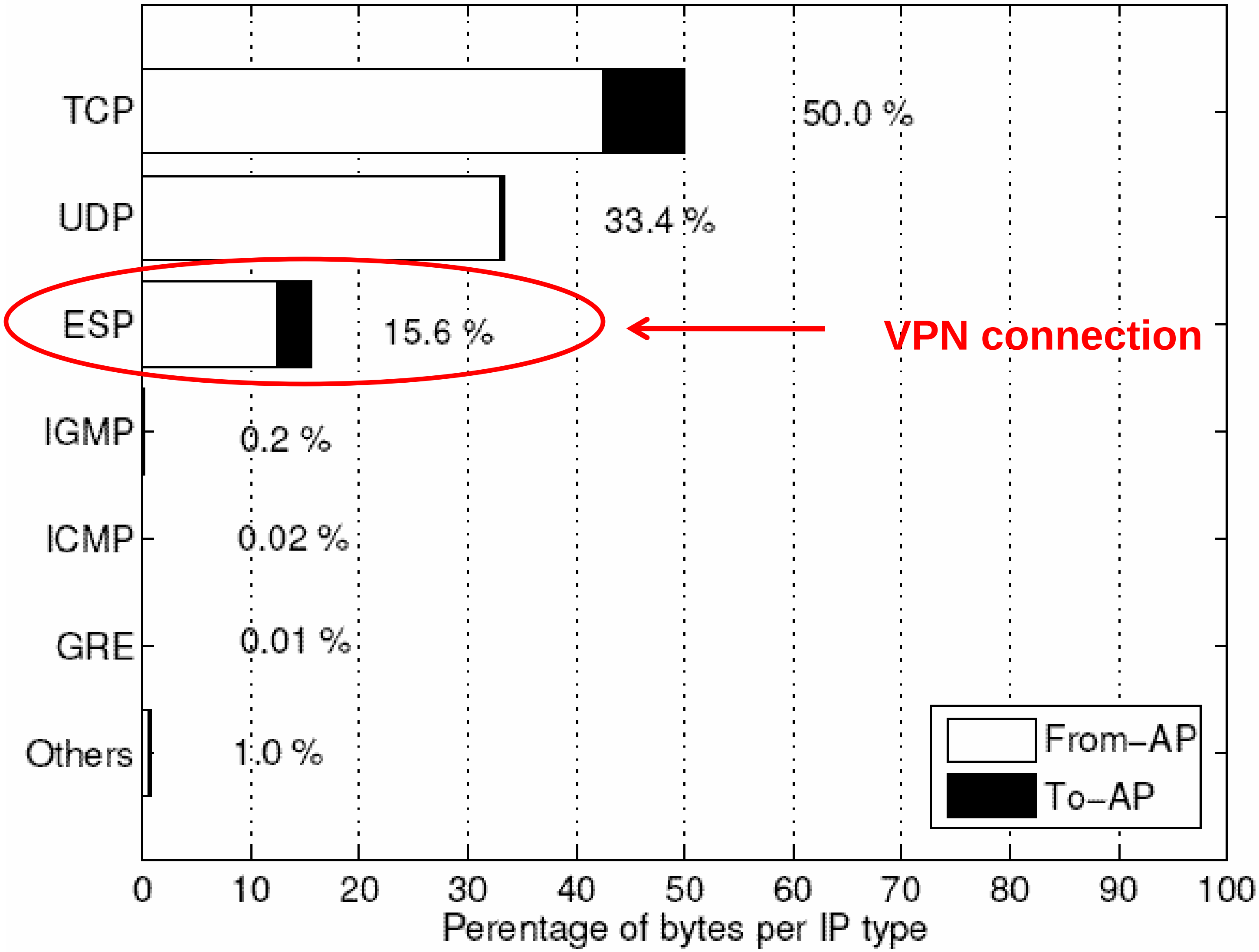


- **Identified by analyzing TCP traffic with OS fingerprinting tool (p0f)**

The Maryland Information and Network Dynamics Lab

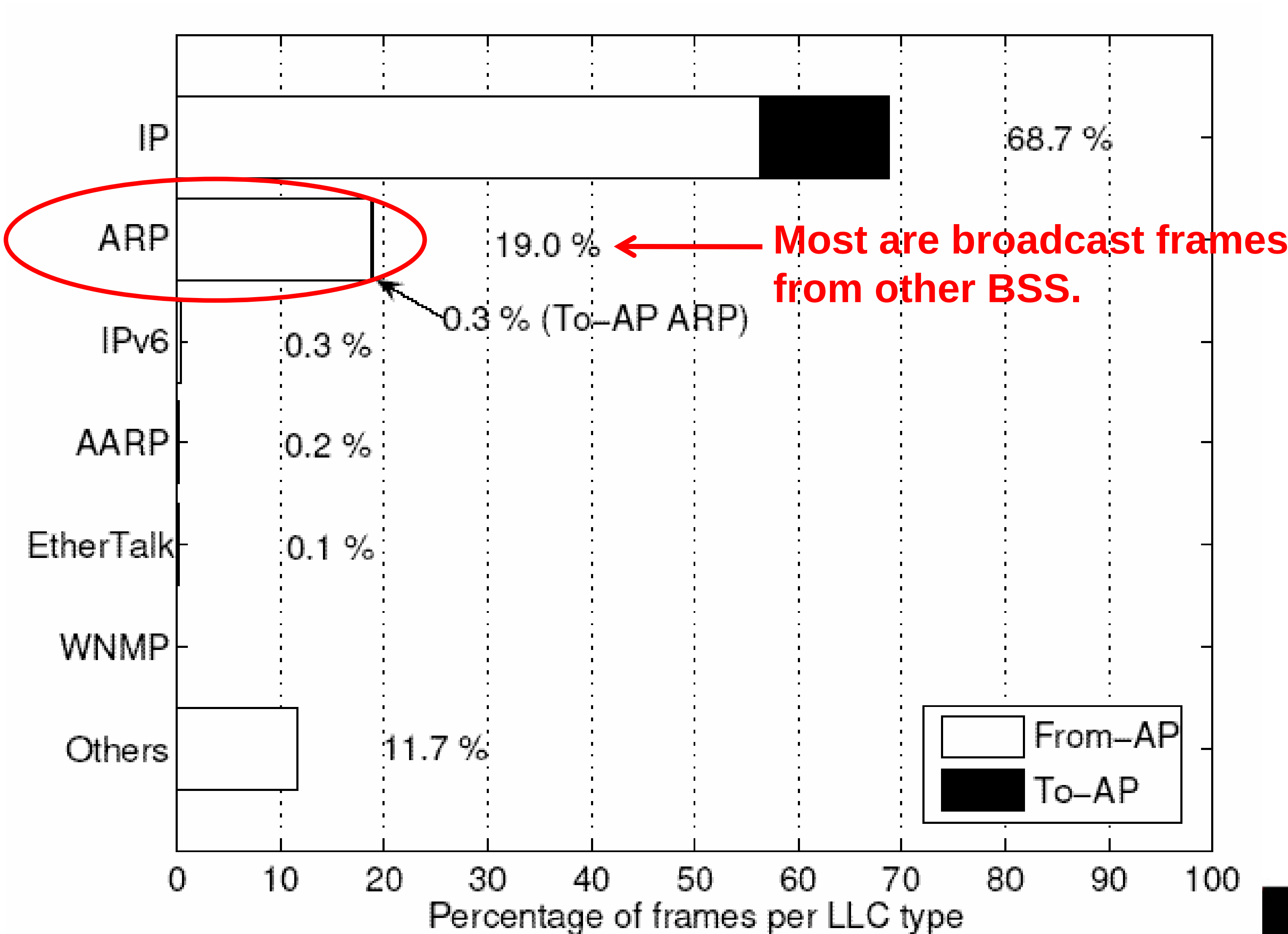
WiFiTC

IP Protocol Histogram



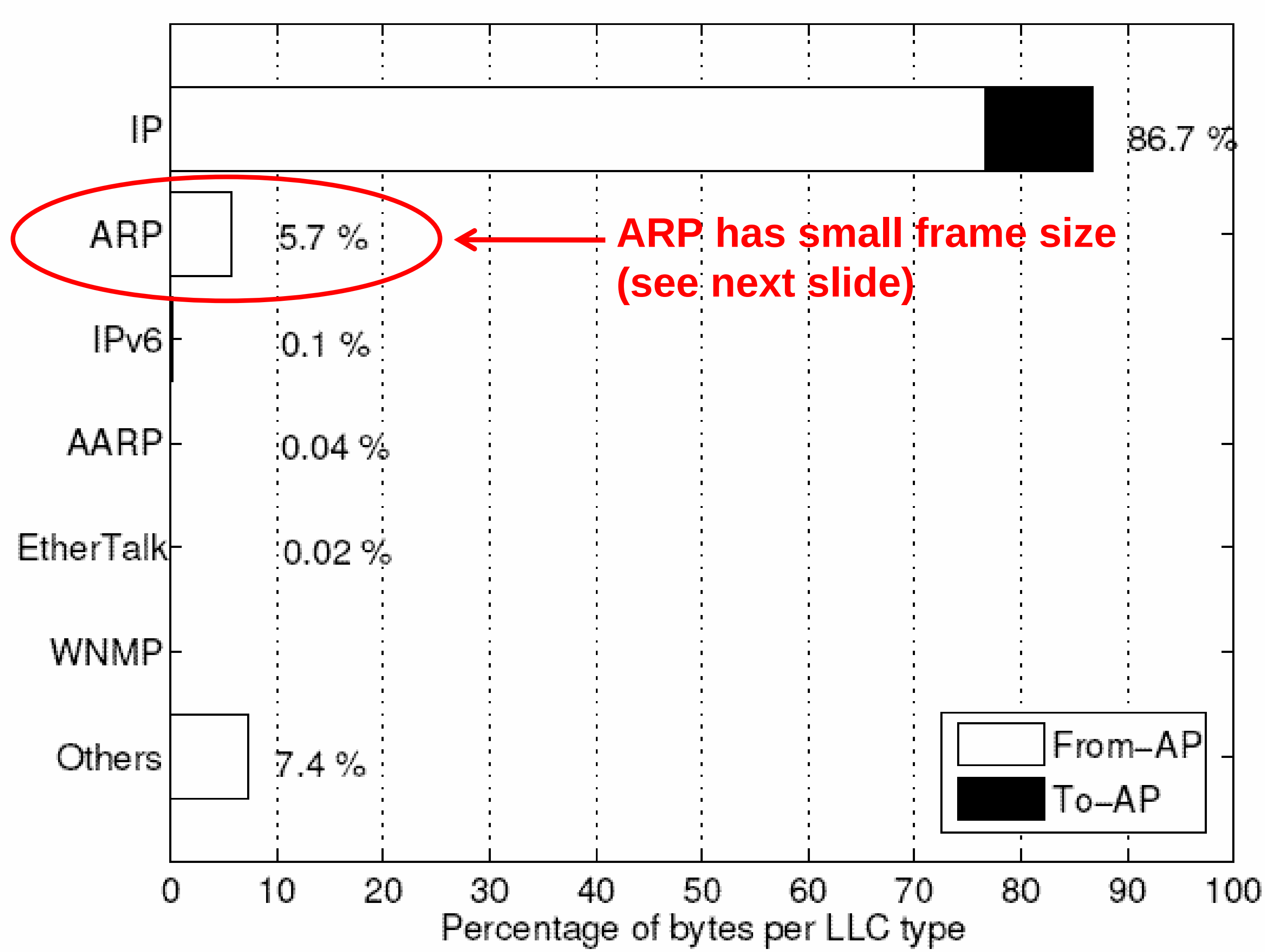
WiFiTC

LLC Type Histogram



WiFiTC

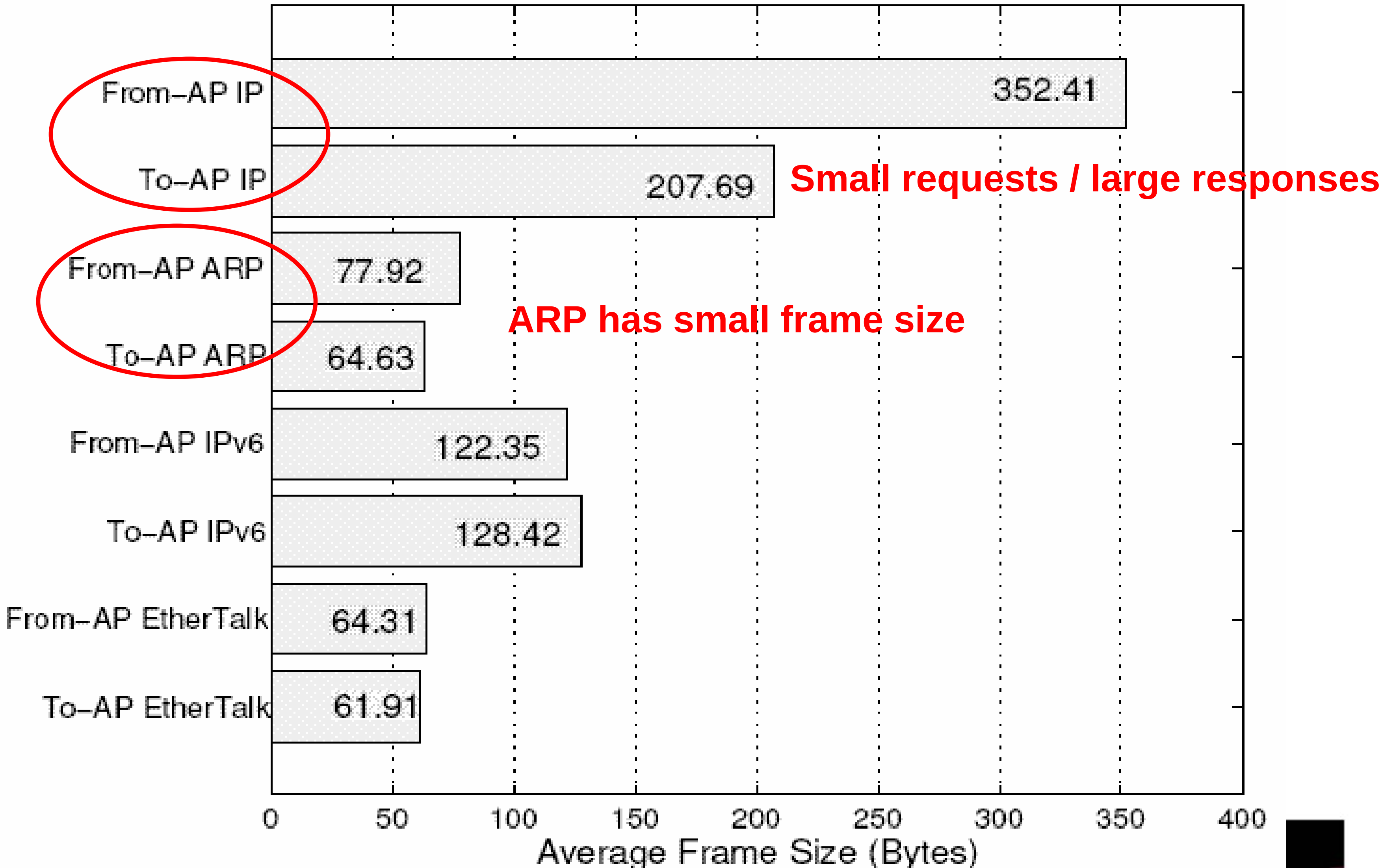
LLC Type Histogram (in Bytes)



The Maryland Information and Network Dynamics Lab

WiFiTC

LLC Average Frame Size



WiFiTC

Session Analysis

- Session: A traffic duration of a wireless STA sending/receiving, which is expired when the STA does not send/receive for some time threshold (e.g. 30 minutes)
- Advantages: grouping into homogeneous traffic units helps characterization.
- Session Analysis
  - Per-protocol session analysis : aim to characterize each protocol traffic in wireless LAN.
  - Session clustering analysis (on-going work) : aim to characterize a typical one-AP wireless LAN traffic.

WiFiTC

Per-Protocol Analysis

- Traffics in wireless LAN consists of
  - **User** traffic (34% in number of frames): generated by human users, e.g. HTTP, SSH, IMAPS (email), ESP (vpn), etc.
  - **Broadcast** traffic (53% in number of frames): generated by machines for requests to **all,** responses from any, e.g. NetBios (windows name/browse **service**), ARP (address resolution), MAC Probe, etc.
  - **Multicast** traffic (13% in number of frames): generated by machines for requests to **some**, responses from them, e.g. Srvloc (service location), IGMP (group mgmt), ICMP (network discovery), etc.

UNIVERSITY OF MARYLAND 18 56

MIND The MIND Lab
The Maryland Information and Network Dynamics Lab

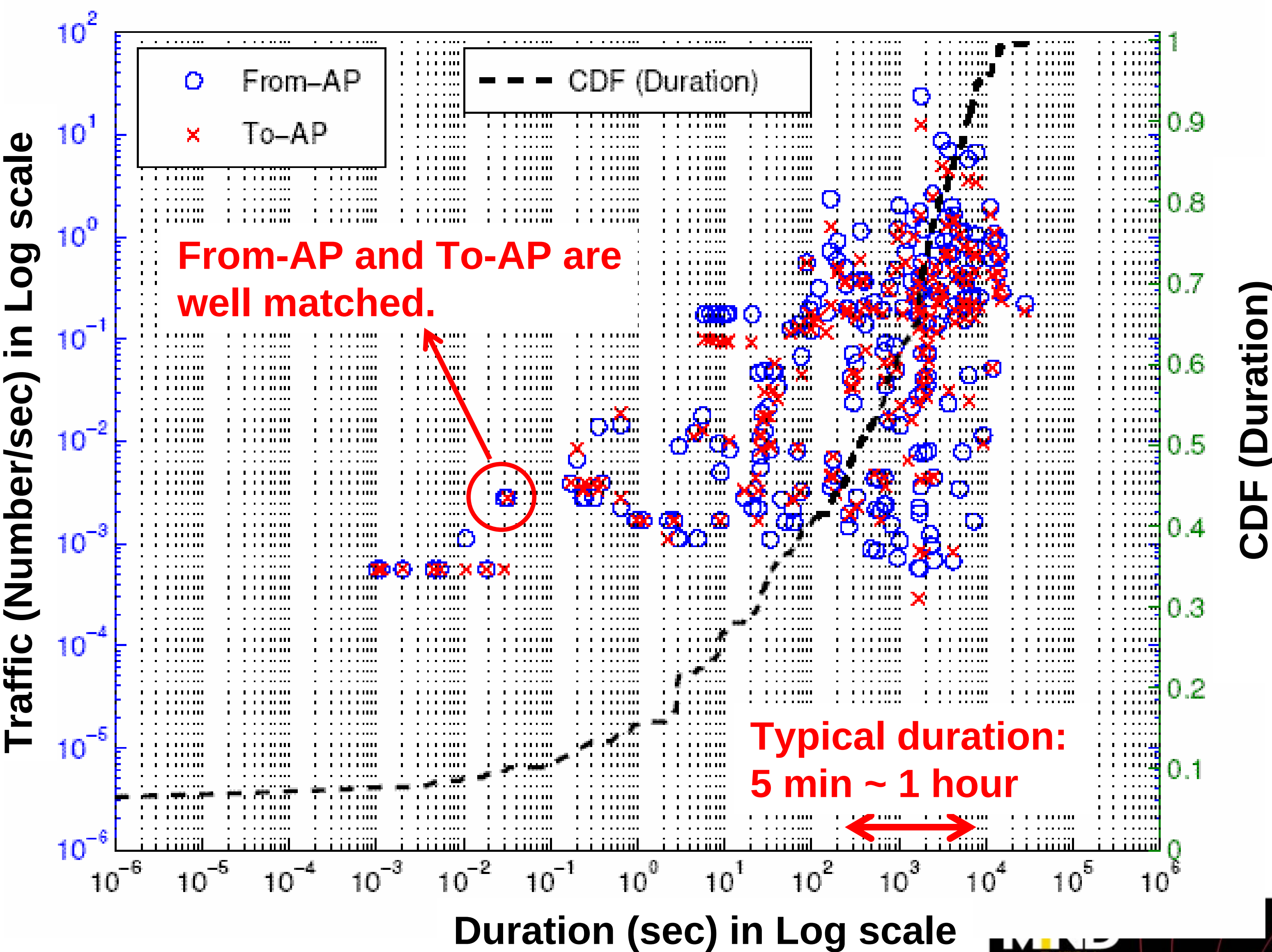
WiFiTC

User Protocol Session Characteristics

- 34% in number of frames.
  - http/https, ssh, imaps (email), esp (for vpn), etc.
- Typical Characteristics
  - High traffic
  - From-AP/To-AP traffics are well matched for unicast request/response.
  - Session duration: around 1 hour
- Other observations
  - IMAP spike
    - Some IMAP sessions have as large traffic as order of 2.
    - Inferred to be email worm (W32.Netsky.B@mm)

WiFiTC

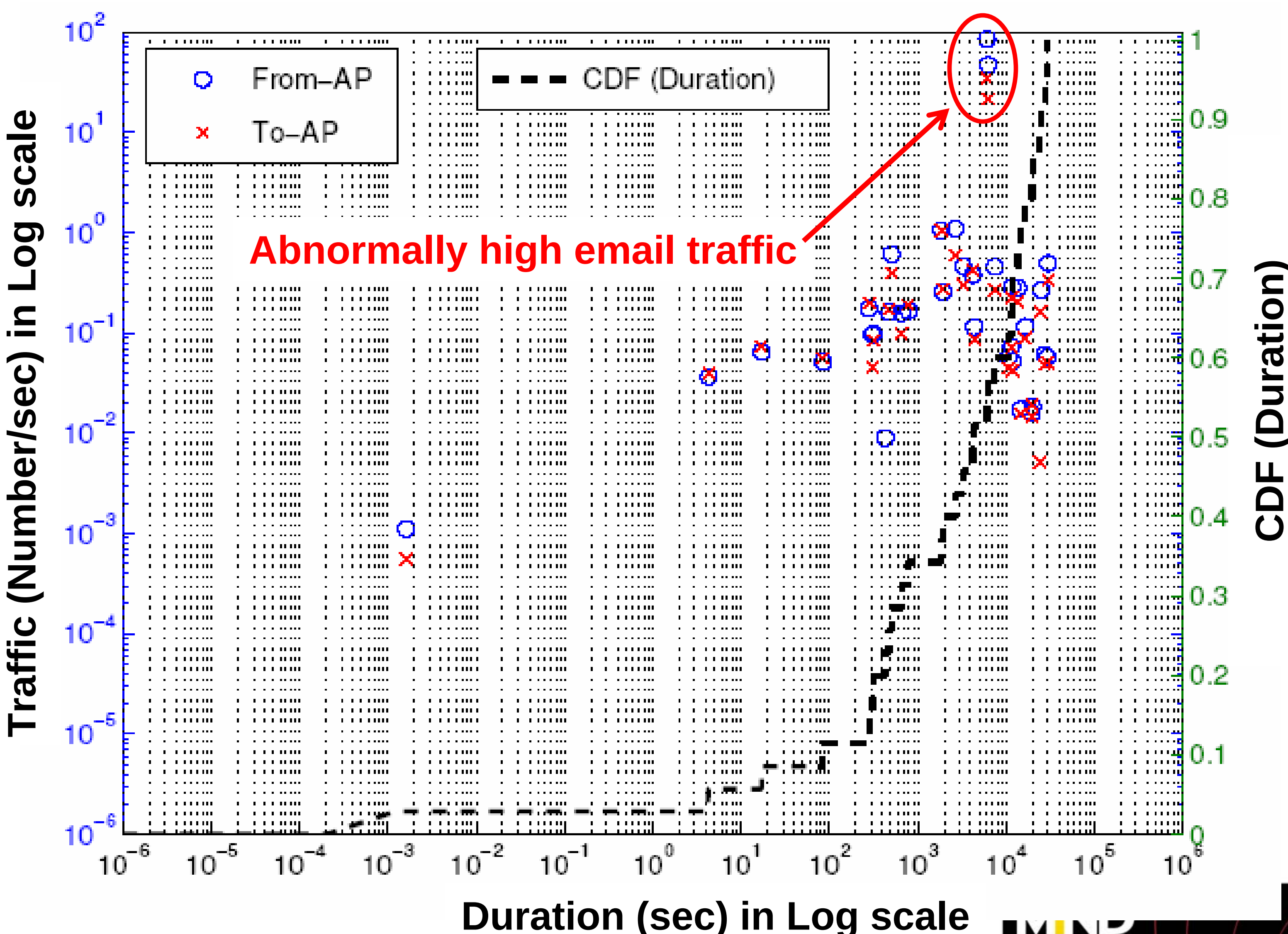
User Protocol Sessions (HTTP)



The MIND Lab
The Maryland Information and Network Dynamics Lab

WiFiTC

User Protocol Sessions (IMAPS)



The Maryland Information and Network Dynamics Lab

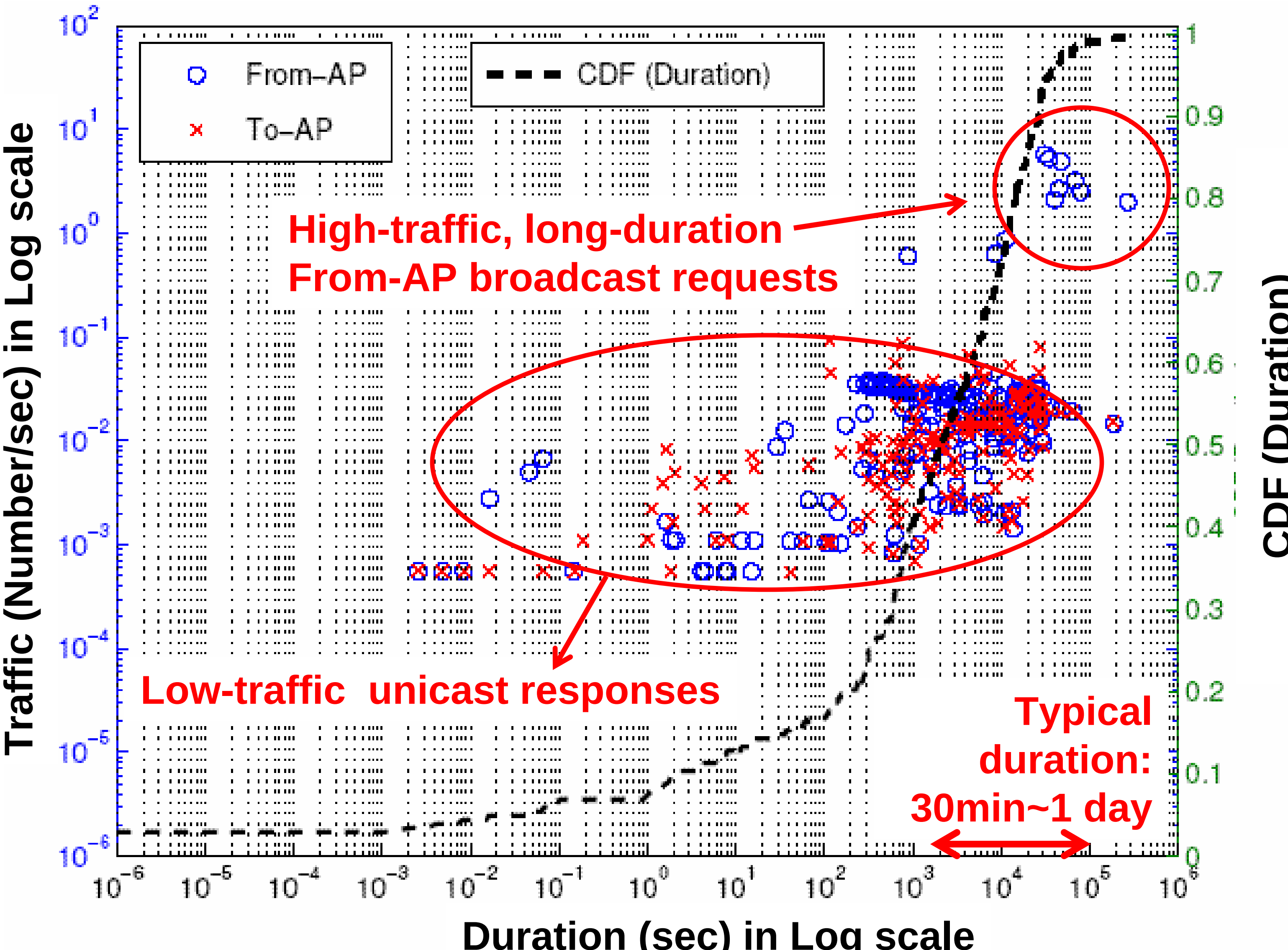
WiFiTC

Broadcast Session Characteristics

- 53 % in number of frames.
  - Netbios, bootp, arp, probe, etc.
- Typical Characteristics
  - Medium traffic
  - Most traffic are From-AP, due to broadcast request/ unicast response.
  - Long session duration: longer than 2 hours
- Other observations
  - Long Probe sessions
    - Some STAs in border of APs frequently and continuously (as long as **3 days**!) send Probe Requests
    - AP can hear Probe Request messages from even far-away STAs, sending Probe Responses.

WiFiTC

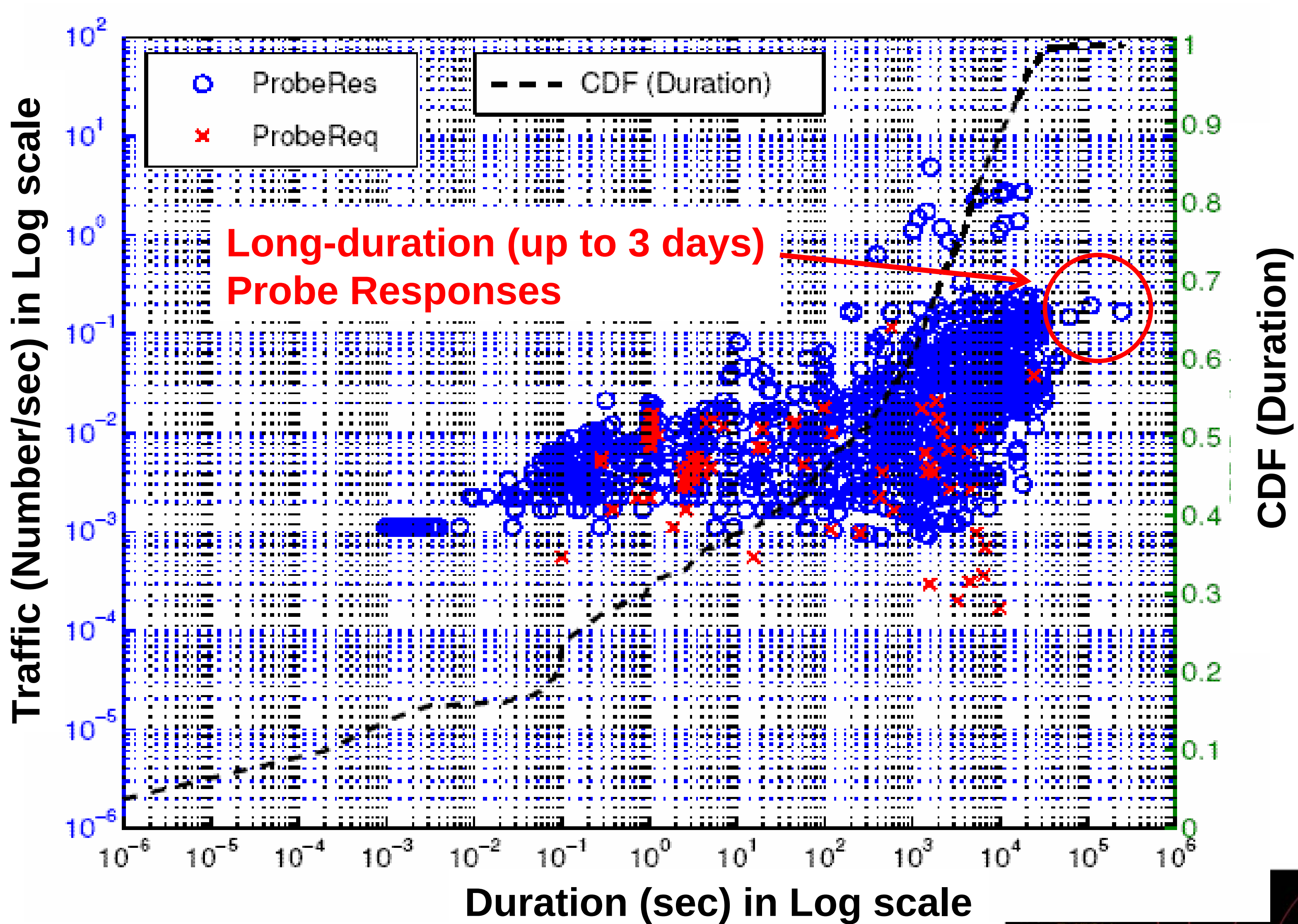
Broadcast Sessions (ARP)



The Maryland Information and Network Dynamics Lab

WiFiTC

Broadcast Sessions (Probe)



The MIND Lab
The Maryland Information and Network Dynamics Lab

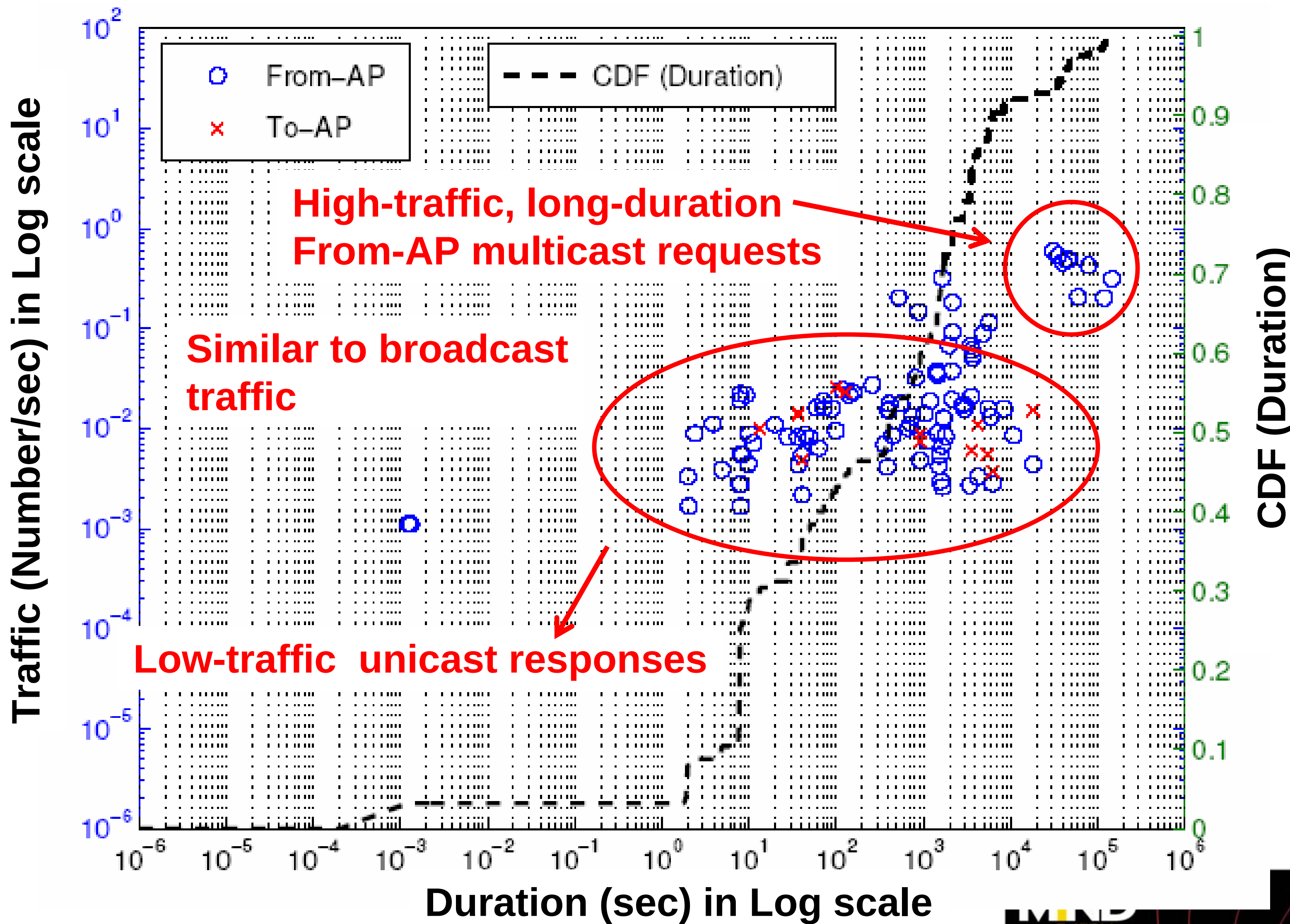
WiFiTC

Multicast Session Characteristics

- 13% in number of traffics.
  - srvloc, igmp, icmp, ipv6, etc.
- Typical Characteristics
  - Small traffic
  - Multicast traffic using well-known addresses: similar to broadcast – long duration From-AP sessions.
  - Multicast traffic for network discovery: instant-lived sessions.
- Other observations
  - ICMP (ping) scans
    - Some STA outside the target BSS sends ping messages to arbitrary, synthetic (multicast) addresses.
    - Generate significant number of short (2-second) sessions.
    - Potentially malicious.

WiFiTC

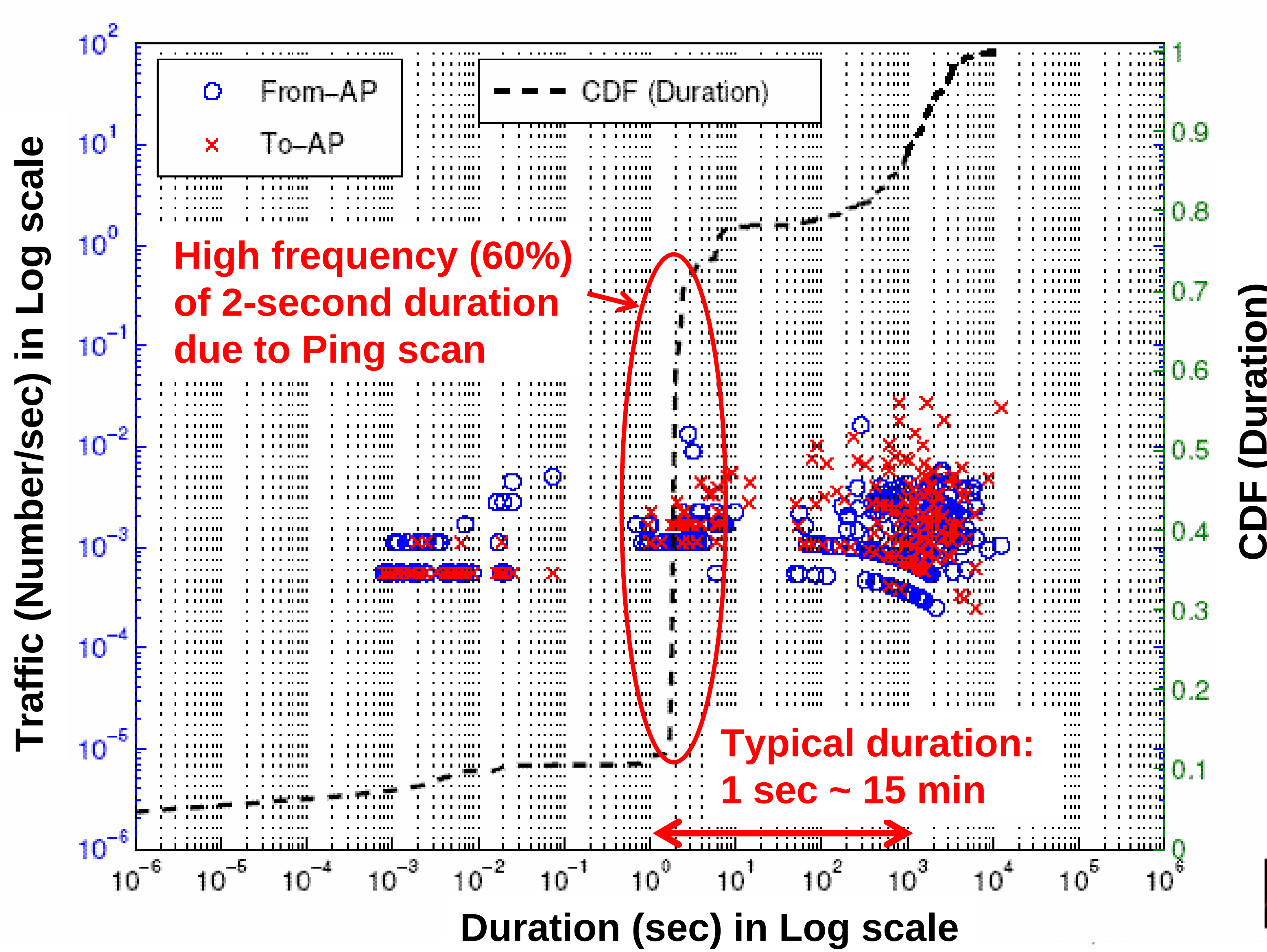
Multicast Sessions (srvloc) : when well-known multicast addresses used



The Maryland Information and Network Dynamics Lab

WiFiTC

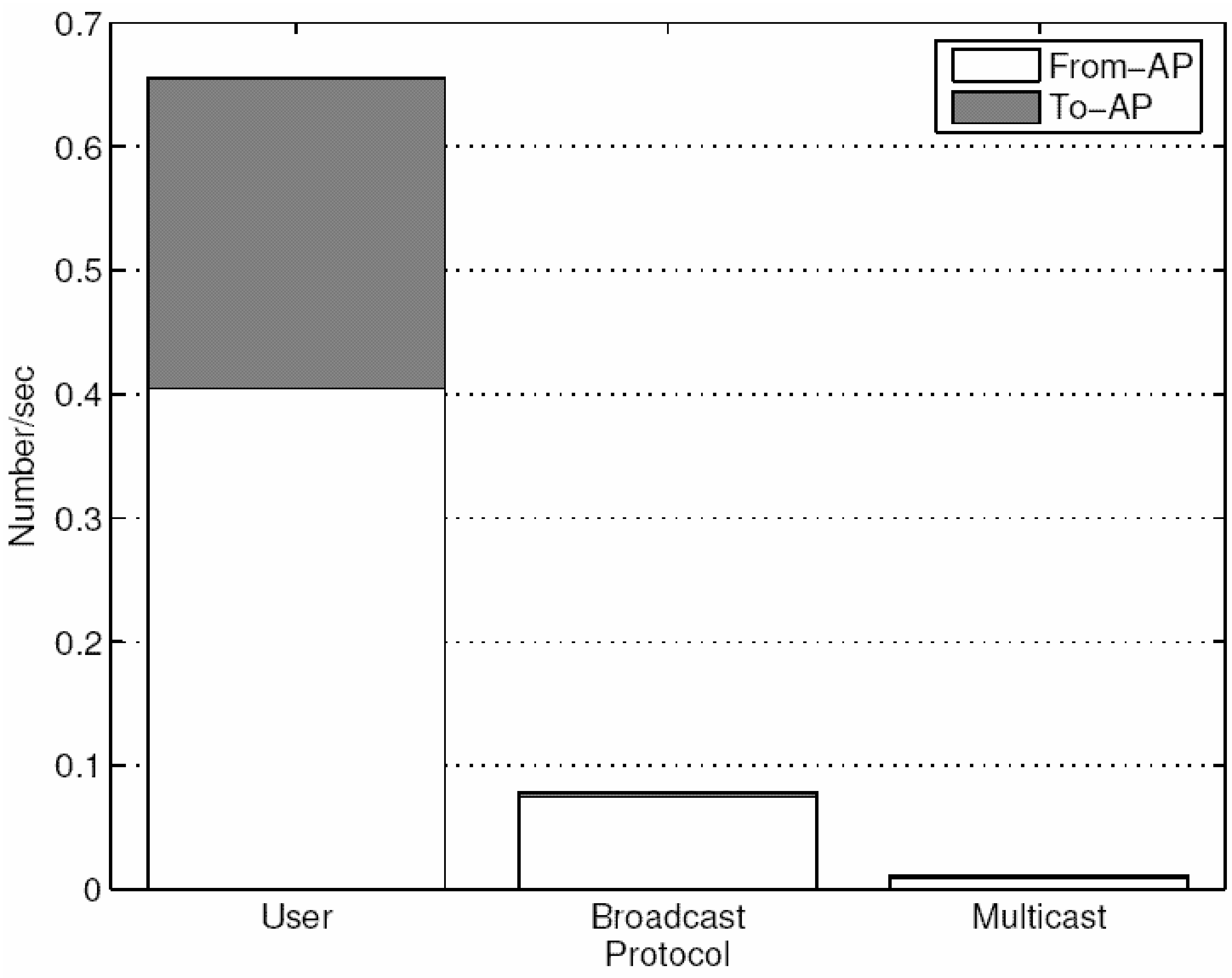
Multicast Sessions (ICMP): for network discovery purpose



Dynamics Lab

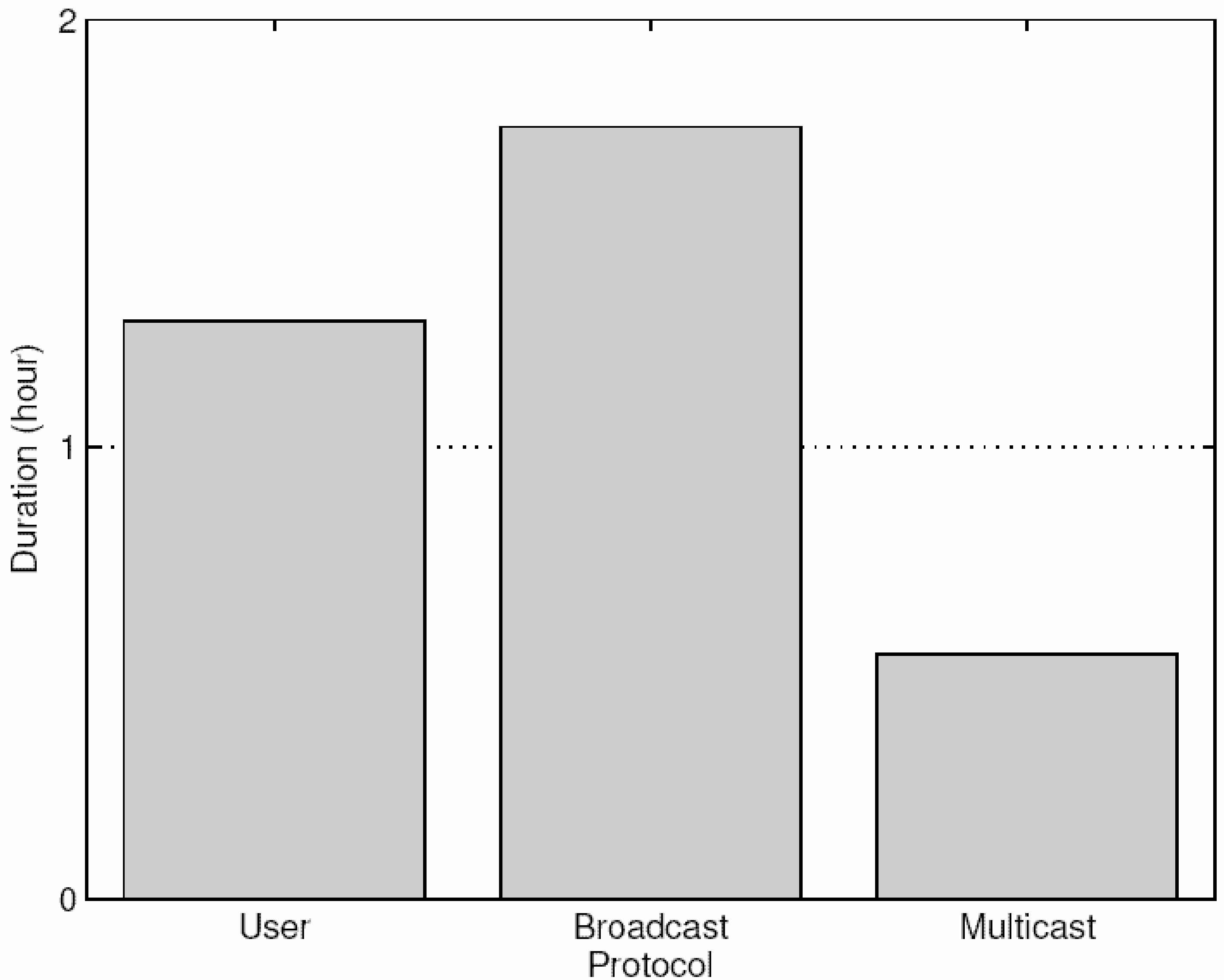
WiFiTC

Mean Session Traffic (number/sec)



WiFiTC

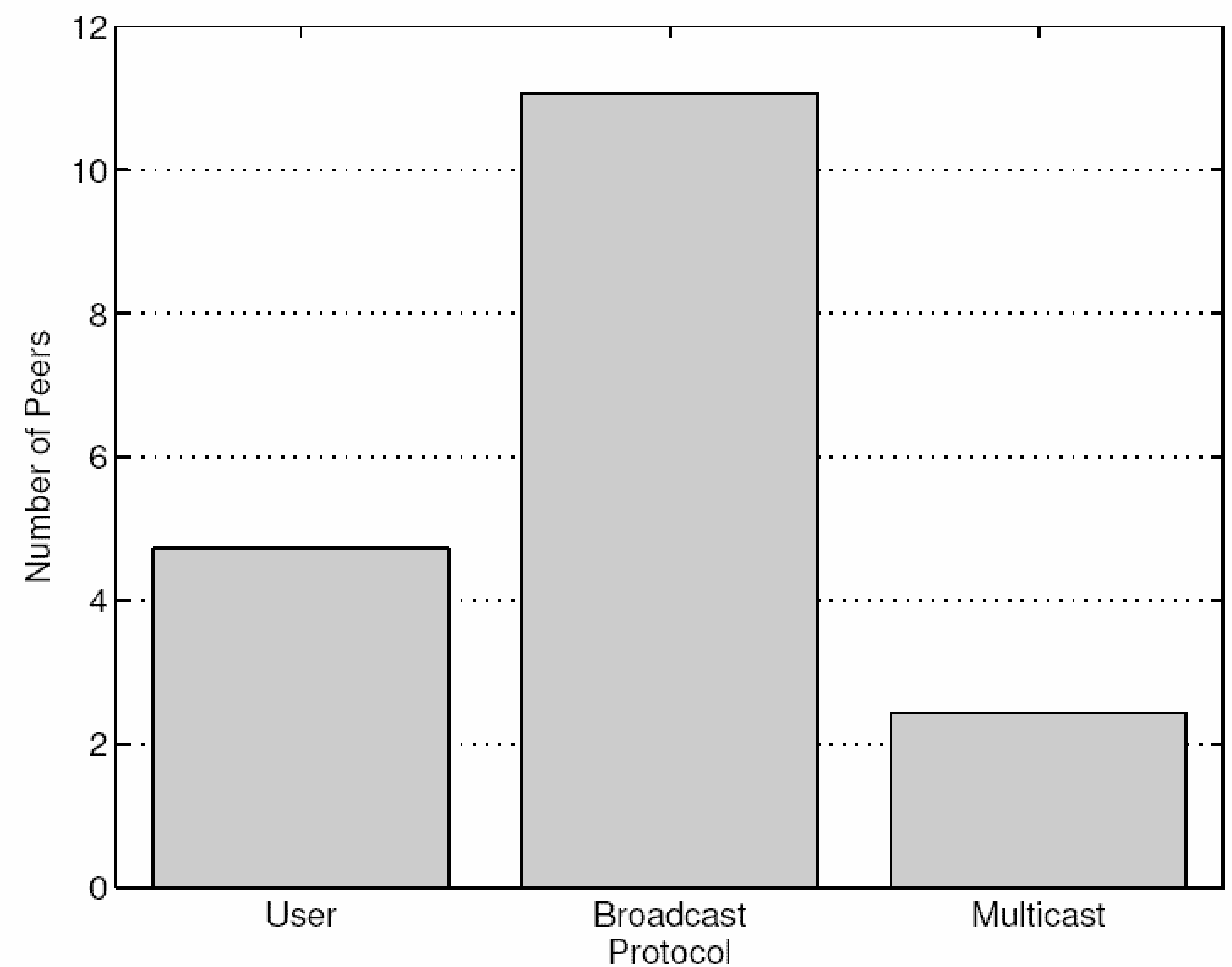
Mean Session Duration (hour)



The Maryland Information and Network Dynamics Lab

WiFiTC

Mean Number of Peers



rk Dynamics Lab

WiFiTC

Session Clustering Analysis

- Generate sessions on all (protocol-mixed) traffic
- Apply adaptive clustering algorithm with 4 features:
  - From-AP number of frames/sec
  - To-AP number of frames/sec
  - Number of distinct peers
  - Session duration (sec)
- Successfully classify wireless LAN traffic into a small number of characteristic sets (clusters).

WiFiTC

Conclusion

- We characterize 2-week long WLAN traffics on:
  - MAC and above-MAC Characteristics
  - Session Characteristics
- Actual WLAN has
  - Significant volumes of broadcast/multicast traffic
  - Some potentially malicious traffic (e.g. IMAPS (email) spike, ICMP (ping) scans)
  - Long-duration (as long as 3 days) Probe Response traffic