Cool Ideas and How to Find Them

Andrzej Duda
Grenoble INP – LIG Lab

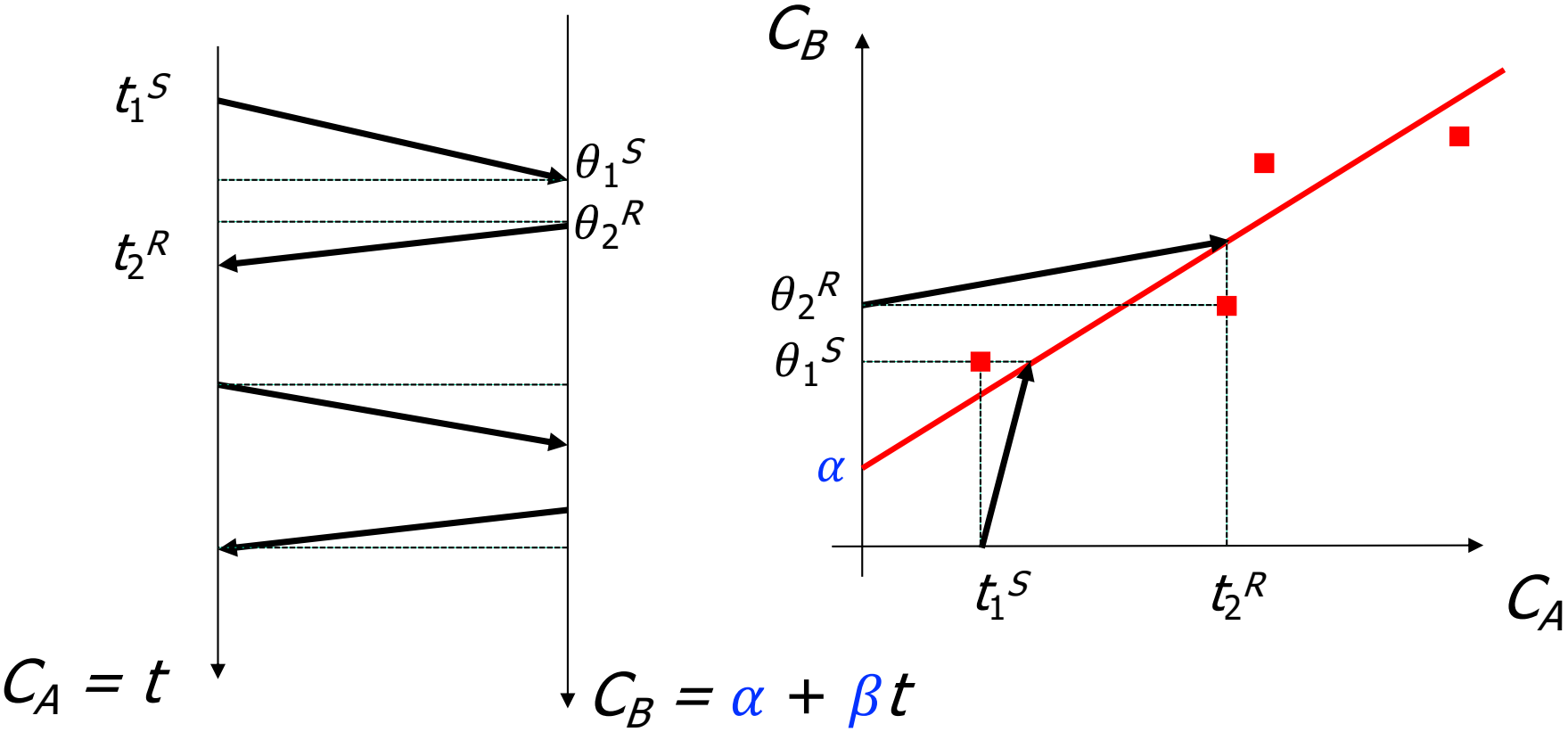
Content

- From Global Time to Calibrated NTP
- 802.11 Performance Anomaly
- Interarrival Intervals
- Idle Sense
- Classifying Encrypted Flows
- Semantic Names for IoT

- Some final thoughts

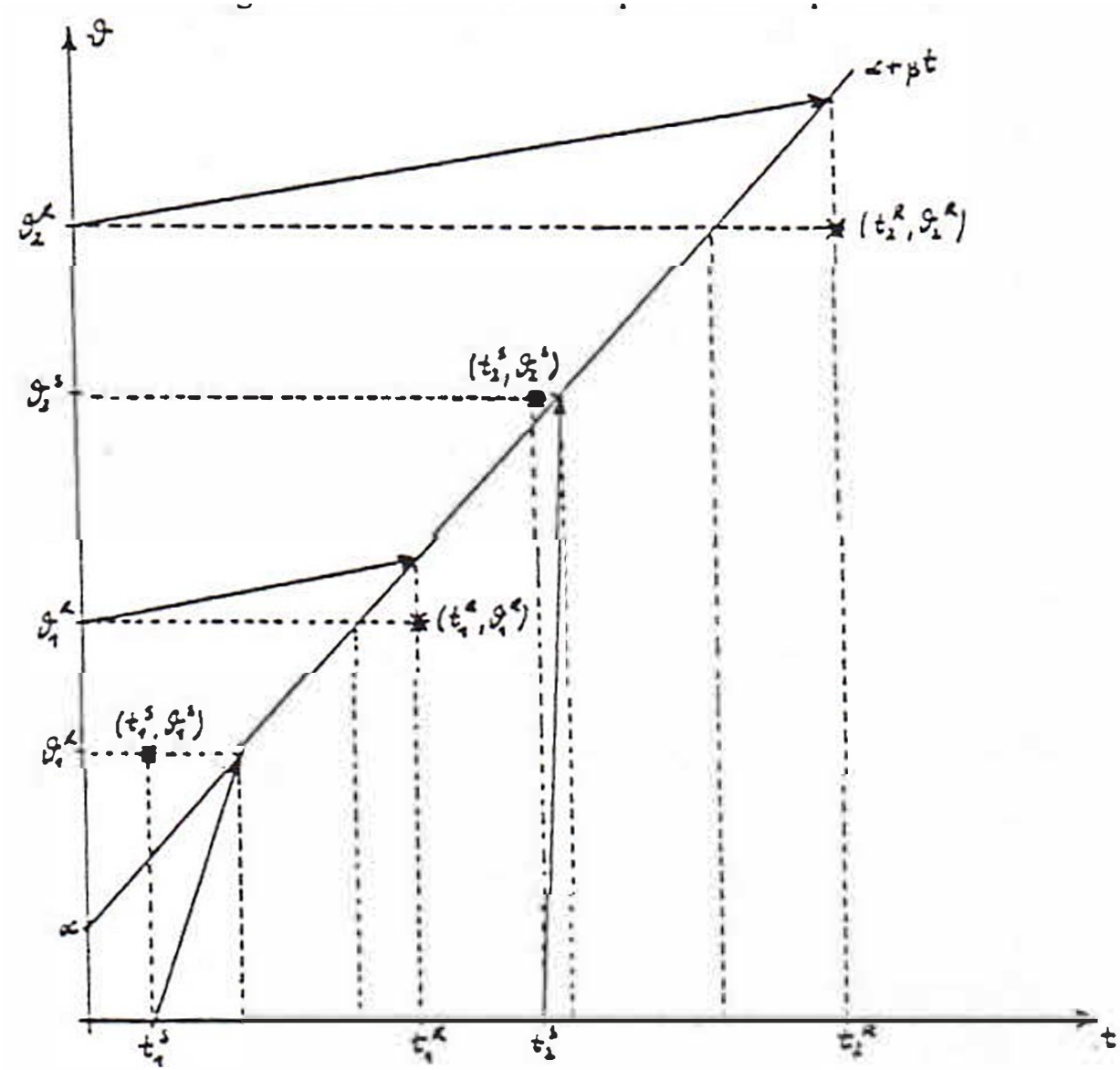
Global Time

Global traces, global time

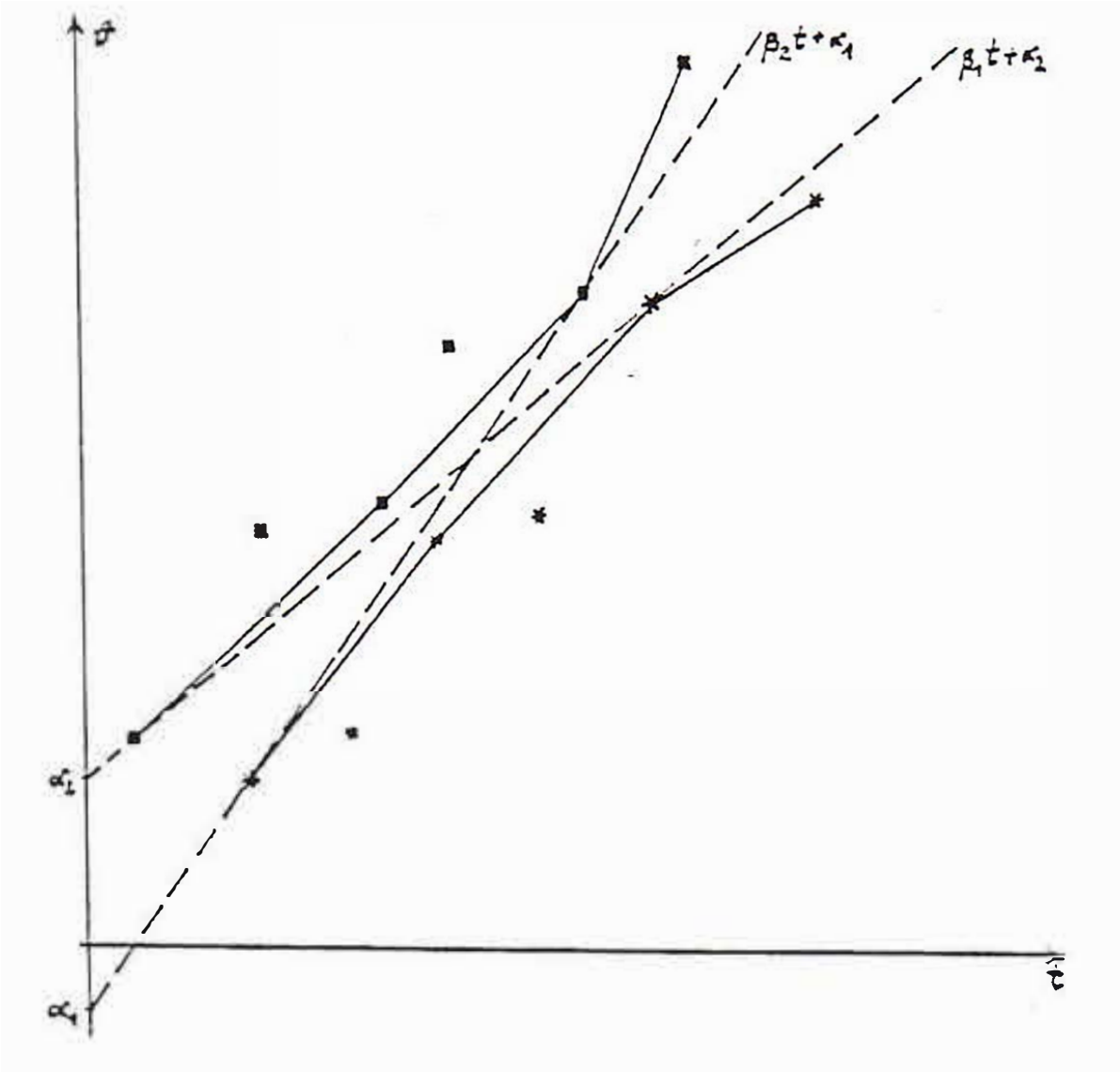


- Distributed system
- Gather local traces of sending and receiving events
- ICDCS 1987

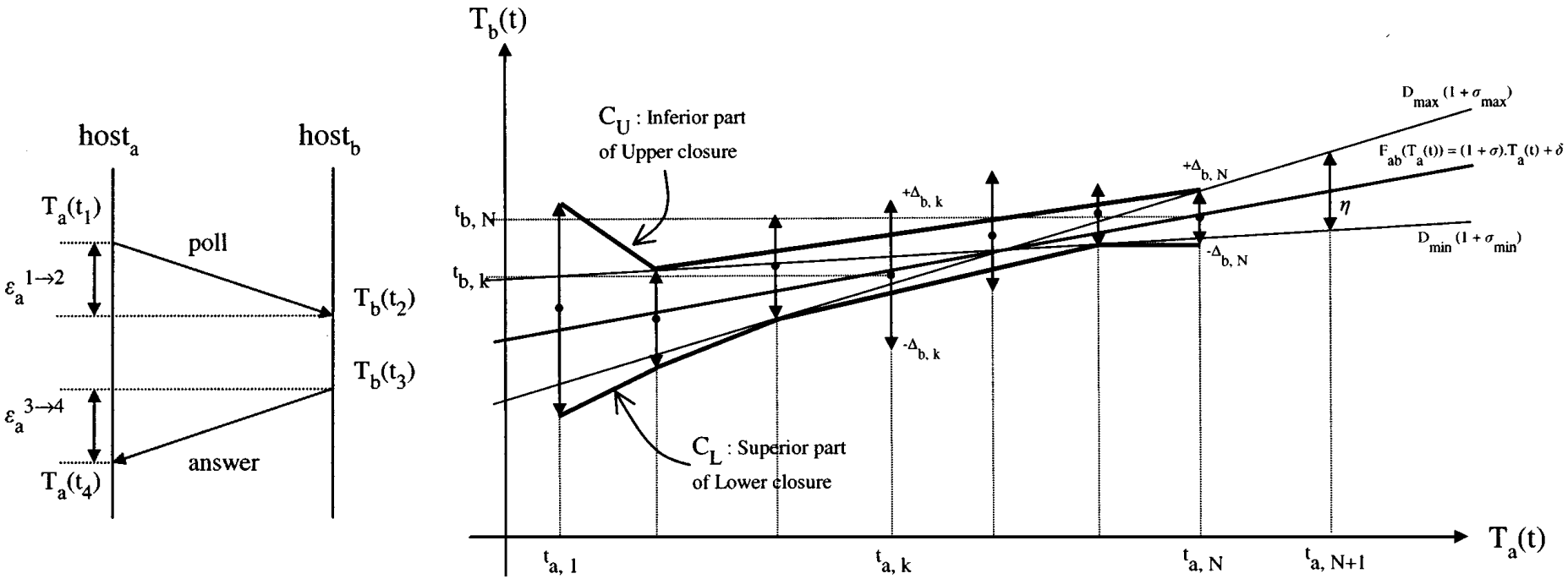
Global traces, global time



Global traces, global time

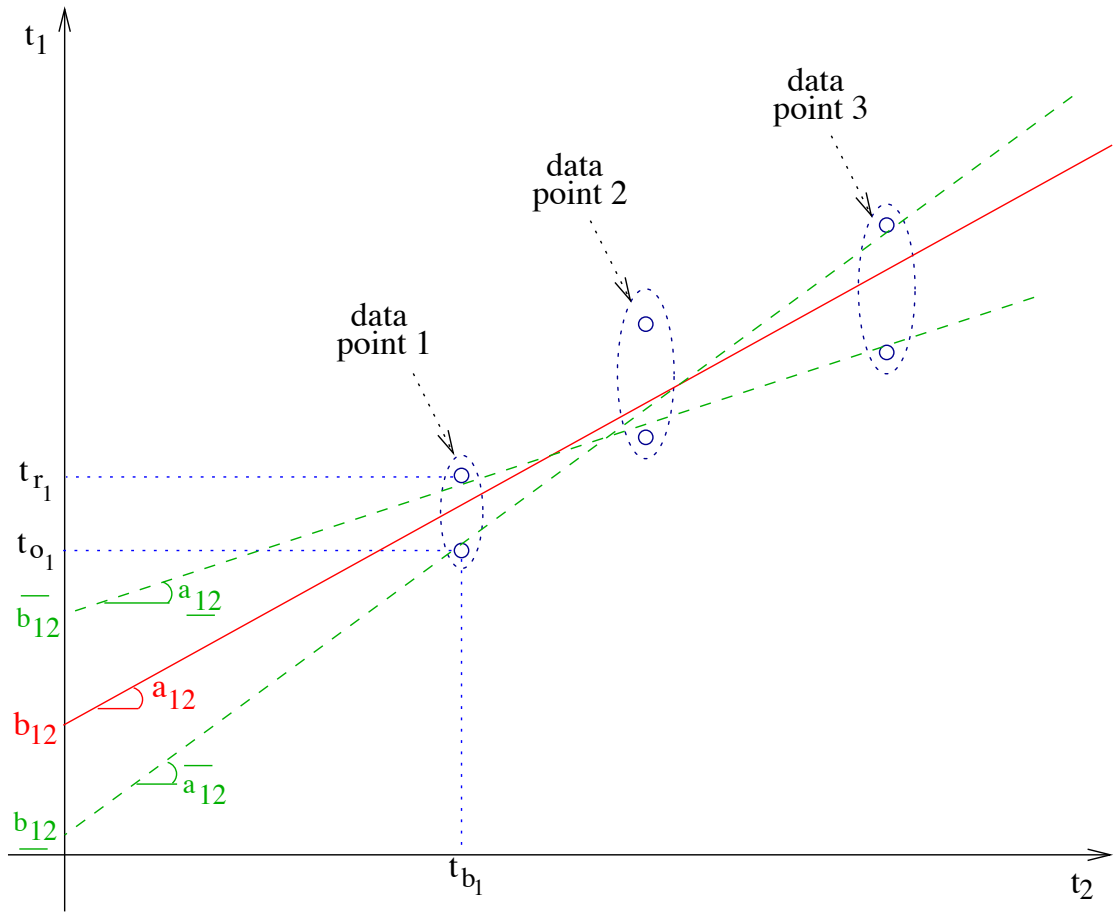


Global traces, global time



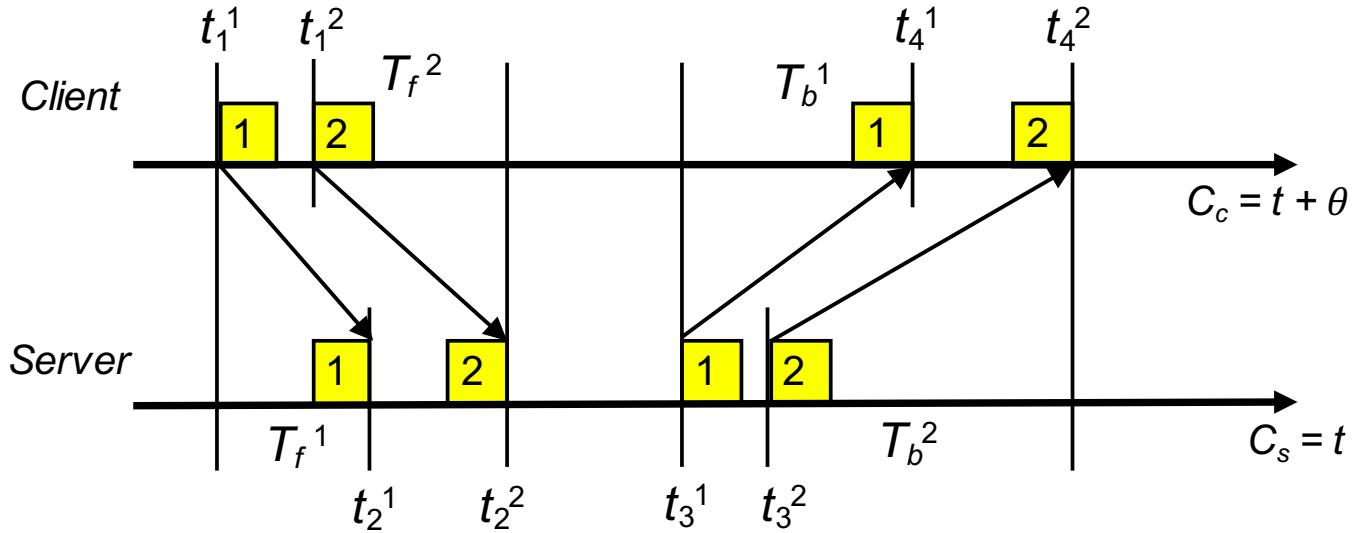
- Berthaud J. *Time Synchronization Over Networks Using Convex Closures,* IEEE/ACM Trans. on Networking 2000

Global traces, global time



- S. Yoon, C. Veerarittiphan, and M. L. Sichitiu *"Tiny-Sync: Tight Time Synchronization for Wireless Sensor Networks"*, ACM Transactions on Wireless Sensor Networks, 2007

NTP



$$RTT = \delta^j = (t_4^j - t_1^j) - (t_3^j - t_2^j), j = 1, \dots, n$$

$$t_2^j = t_1^j + T_f^j - \theta^j, j = 1, \dots, n$$

$$t_4^j = t_3^j + T_b^j + \theta^j, j = 1, \dots, n$$

Symmetry: $if\ T_f^j = T_b^j,$

$$Offset = \theta^j = \frac{(t_4^j - t_1^j) - (t_3^j - t_2^j)}{2}, j = 1, \dots, n$$

$Asymmetry$: $if\ T_f^j \neq T_b^j,$

$$Offset = \theta^j = \frac{(t_4^j - t_1^j) - (t_3^j - t_2^j)}{2} + \boxed{\frac{T_b^j - T_f^j}{2}}, j = 1, \dots, n$$

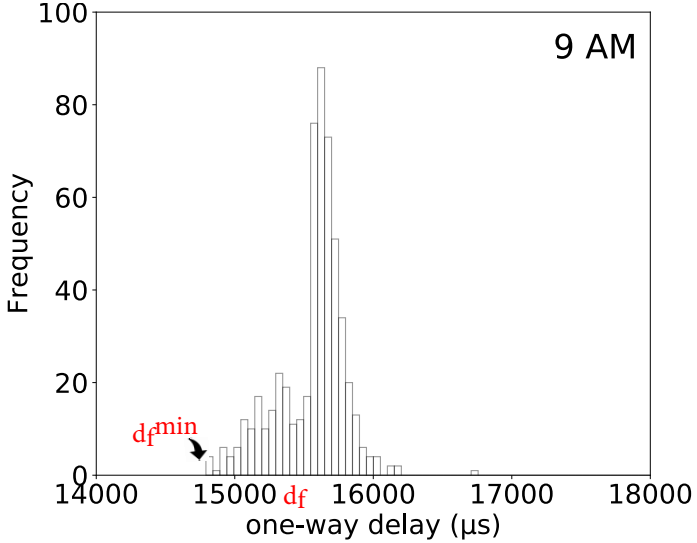
- Accuracy depends on asymmetry!

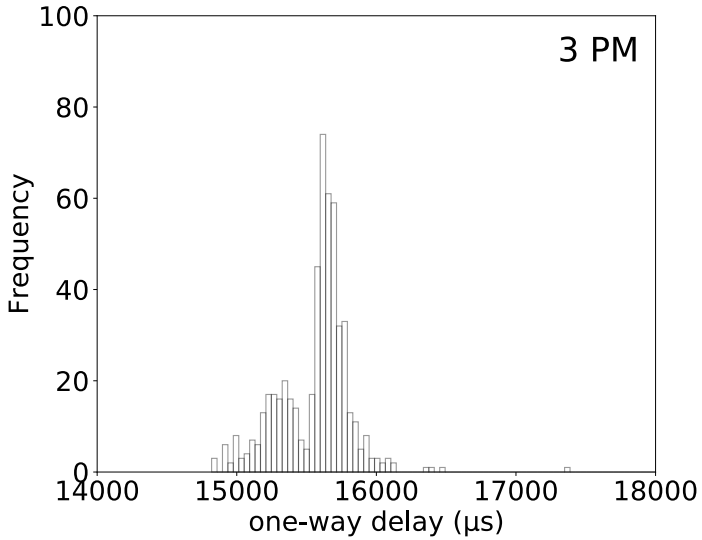
Calibrating NTP

- F. Mkacher and A. Duda, *"Calibrating NTP", 2019 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, 2019.

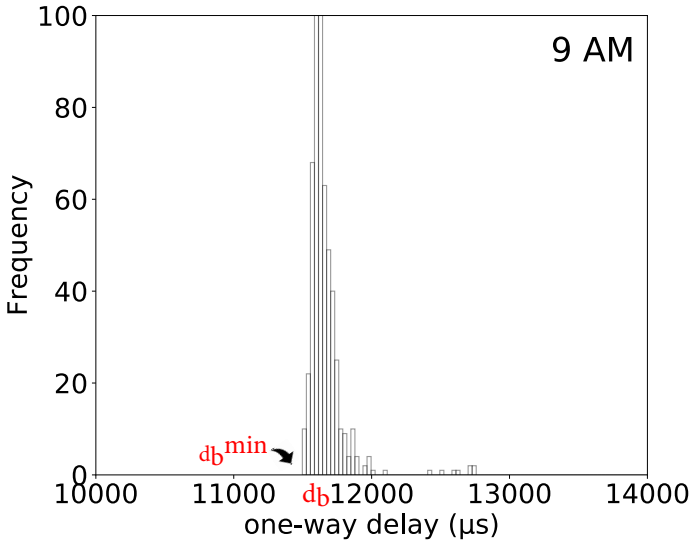
One way delays

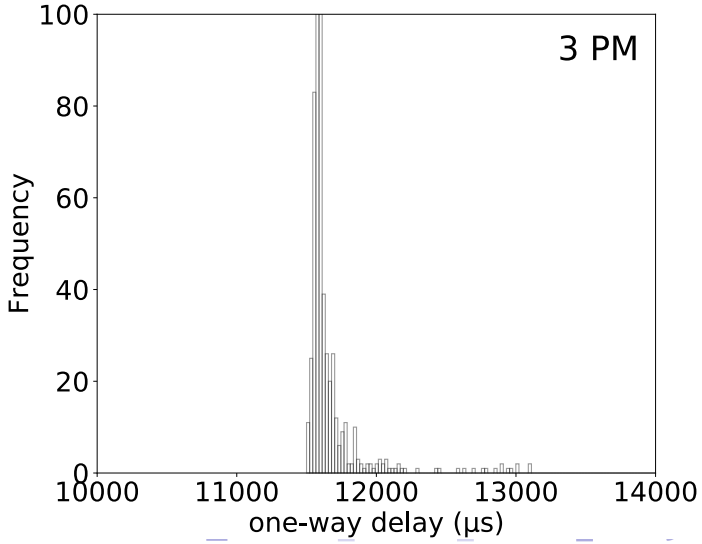
Histograms of T_f



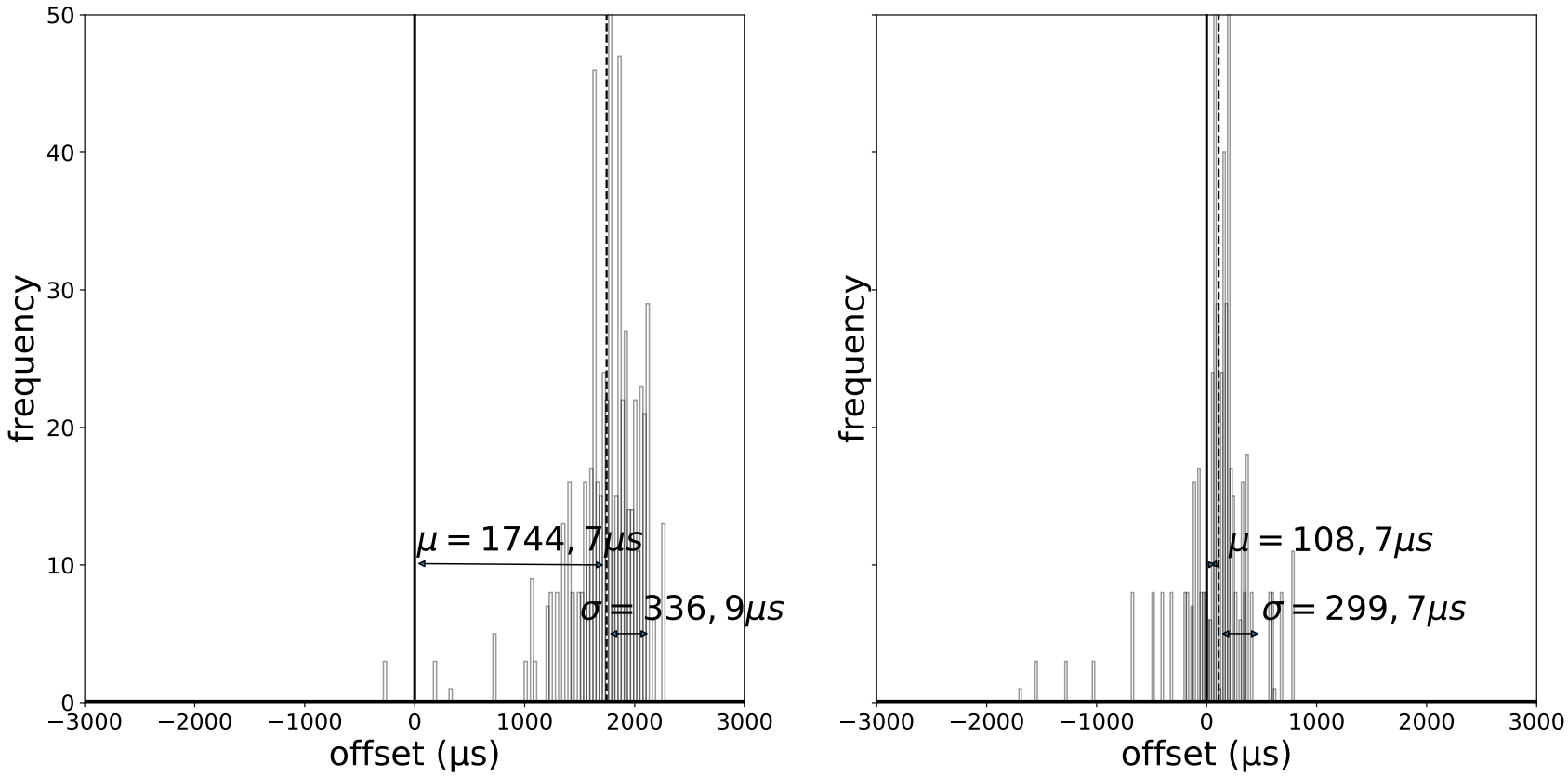


Histograms of T_b





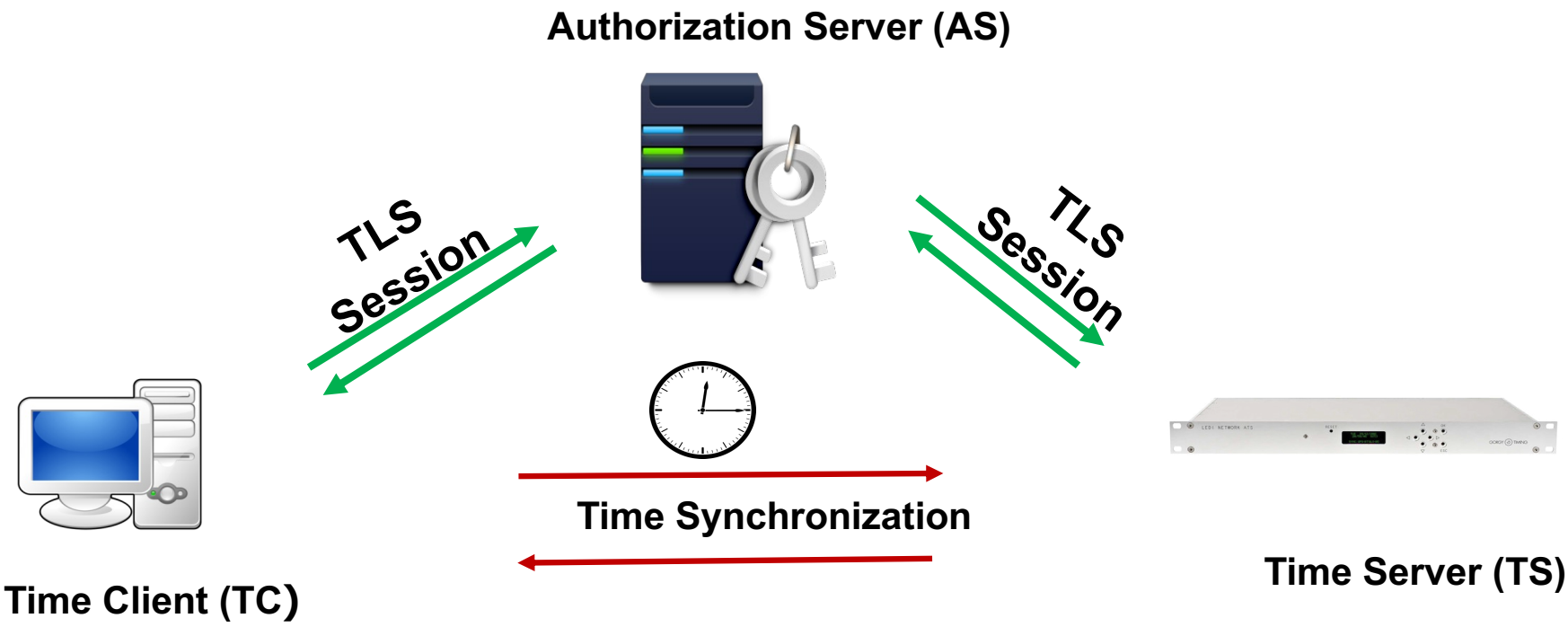
Compensate the systematic offset



Secure Time Synchronization

- F. Mkacher, X. Bestel and A. Duda, *"Secure Time Synchronization Protocol"*, *2018 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS)*, 2018

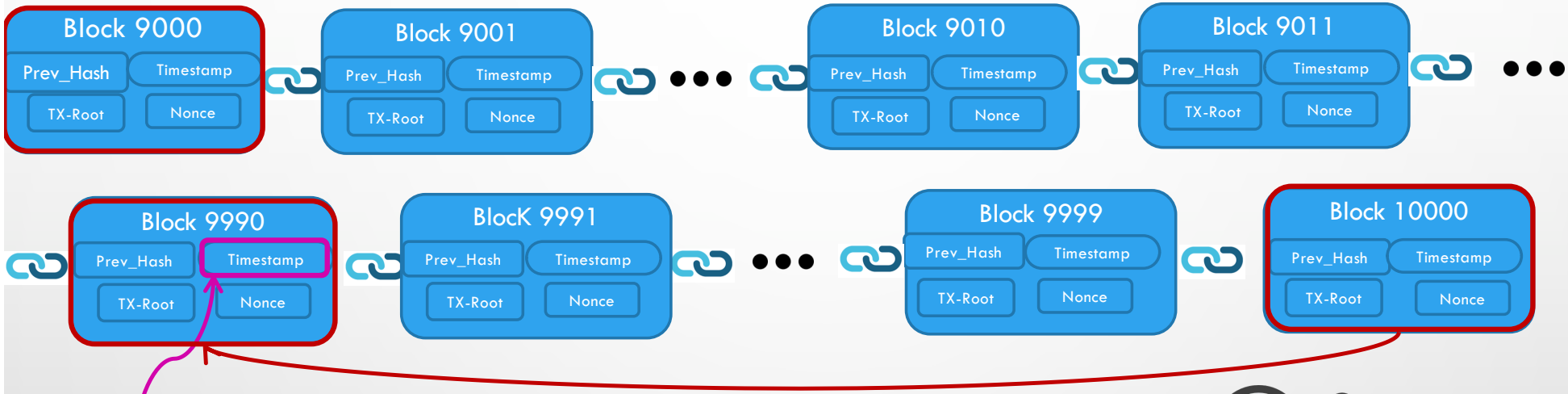
Secure Time Synchronization



TLS => Certificates => Time

- Device wants to synchronize its clock
- Uses TLS, needs time to validate AS certificate
- Need rough estimate of time
- Use Bitcoin!

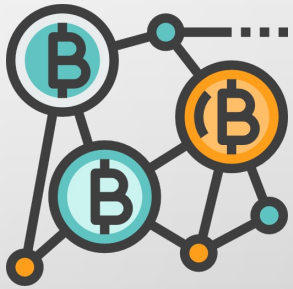
Get last headers from Bitcoin



SPV Client

Send me block headers from Block 9000

Block headers from Block 9000 to the end of the Blockchain



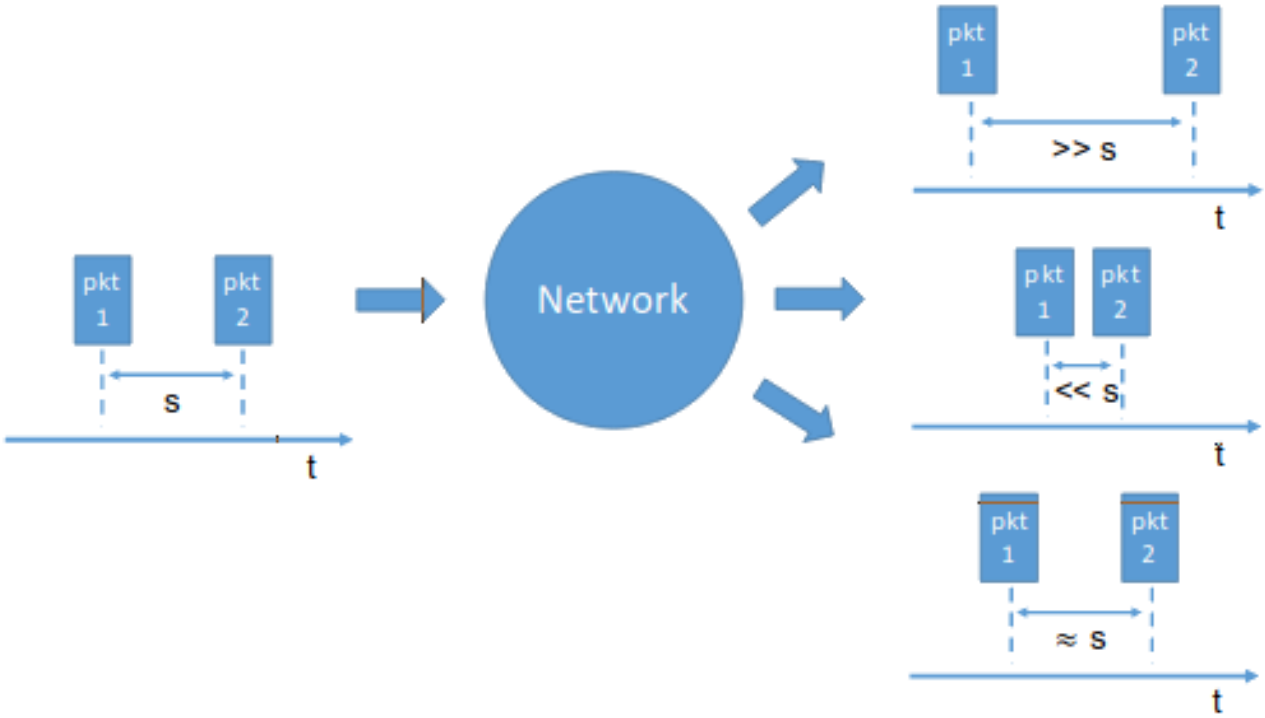
Bitcoin Blockchain

Huygens (Stanford/Google, NSDI ’18)

- Coded probes
- Linear relationship between clocks – estimation via Support Vector Machines
- Network effect - intersection of several estimations

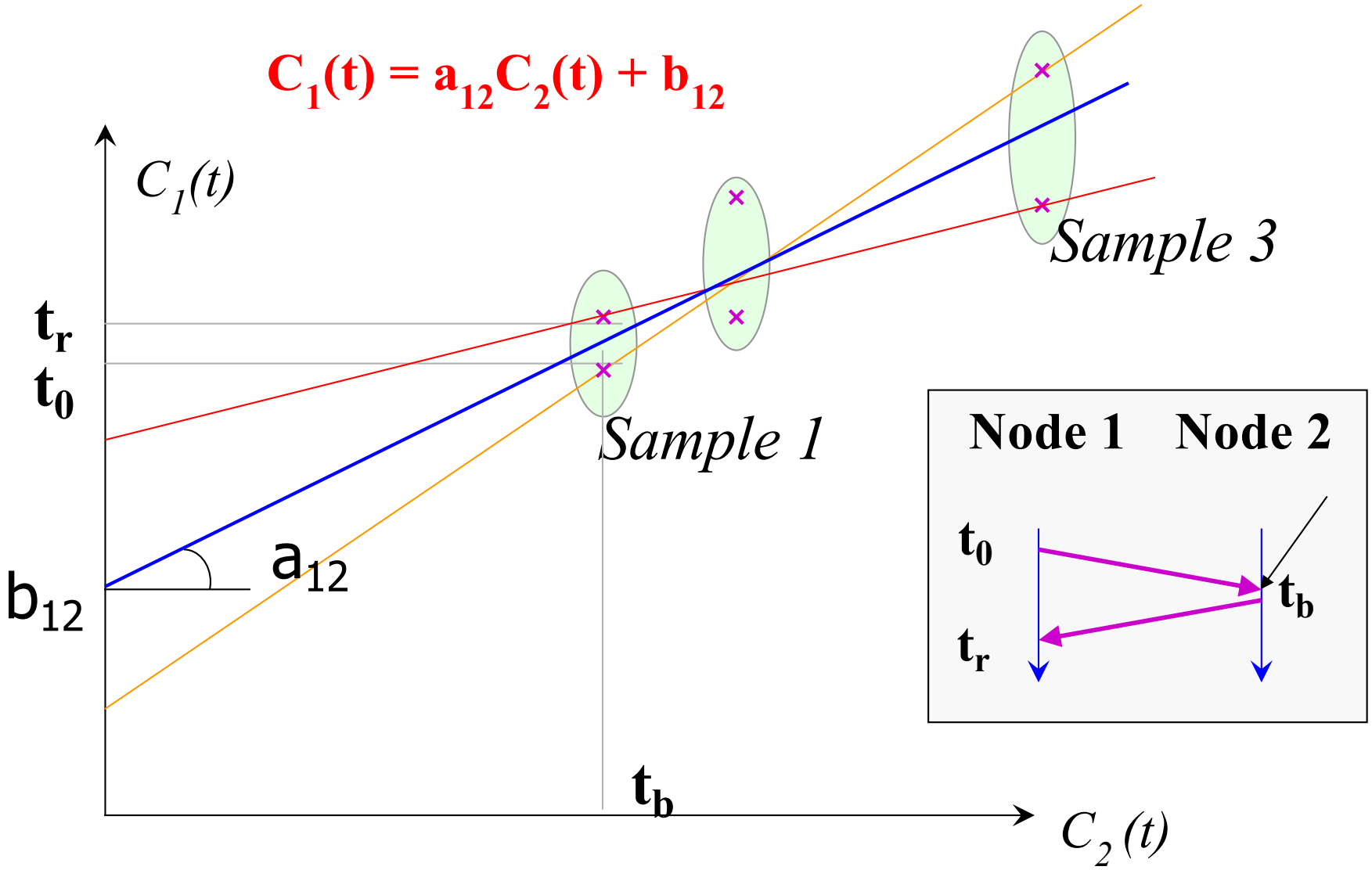
- Performance:
  - On 40 Gb/s 2-stage Clos data center network (3 switches, short distance)
  - Less than 15 ns average error

Coded probes

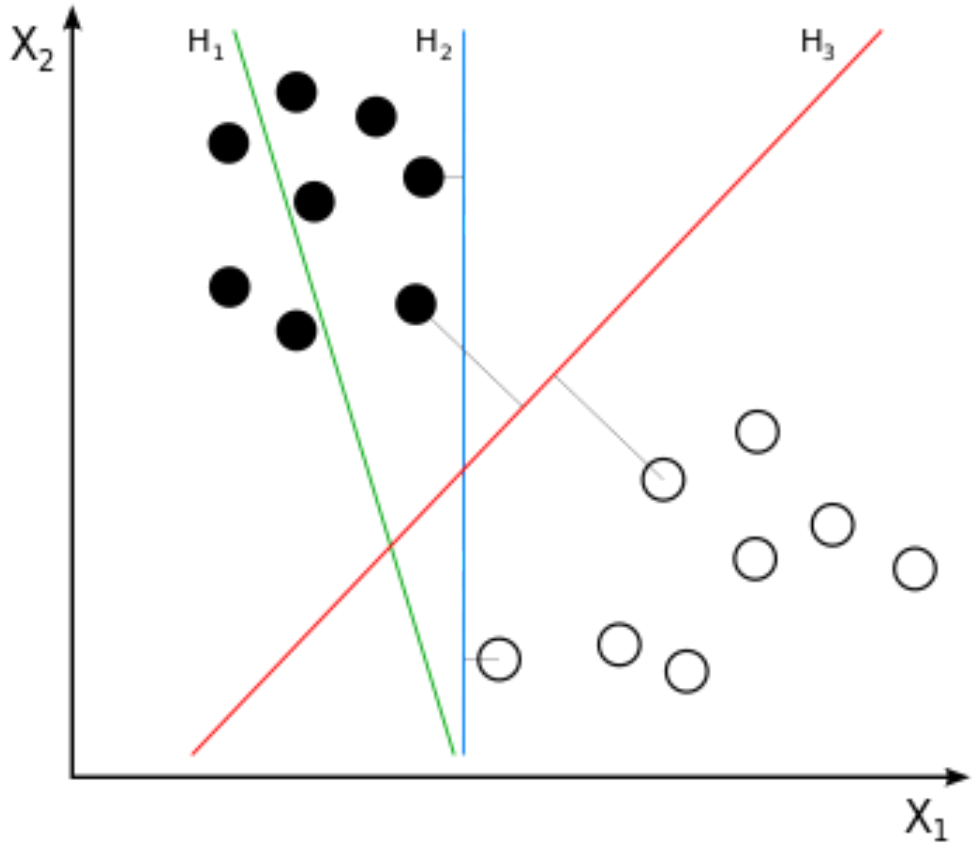


- Consider only the last one measurement

Linear relation between clocks

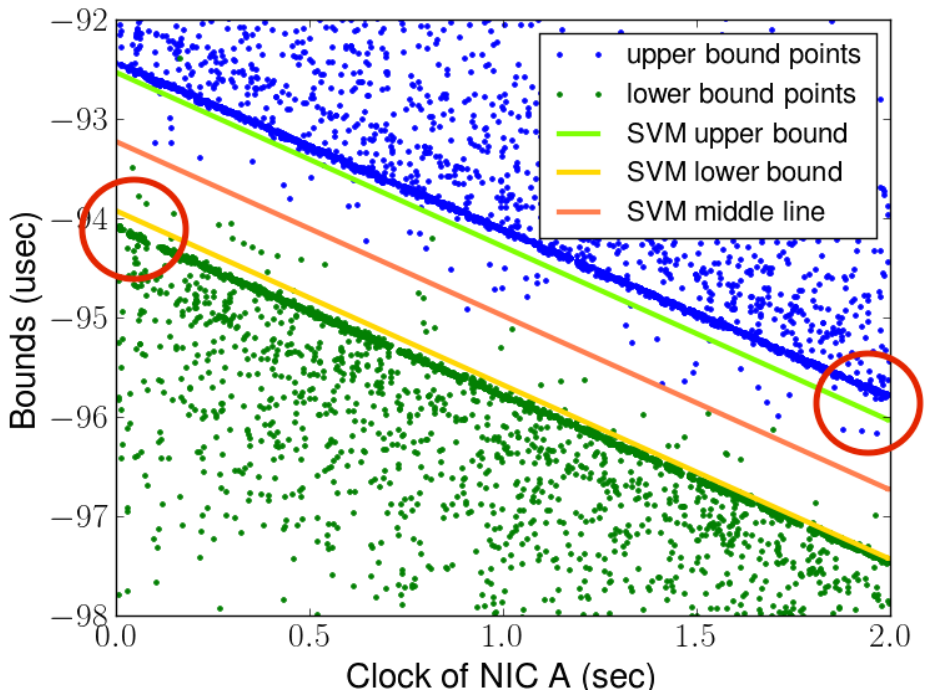


SVM - Support Vector Machines

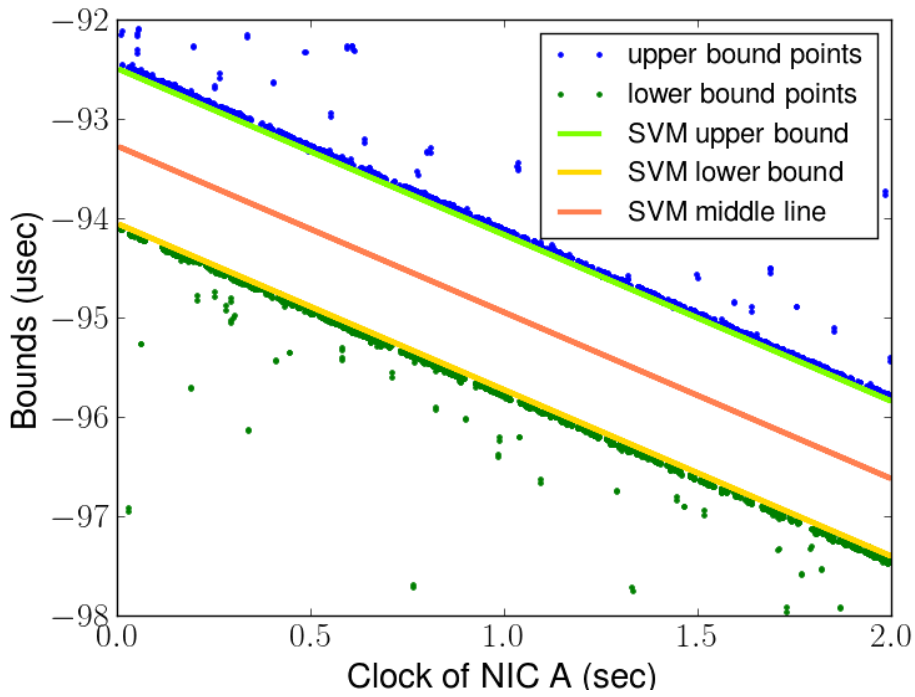


- H3 separates two classes with the maximum margin

Estimating error between two clocks

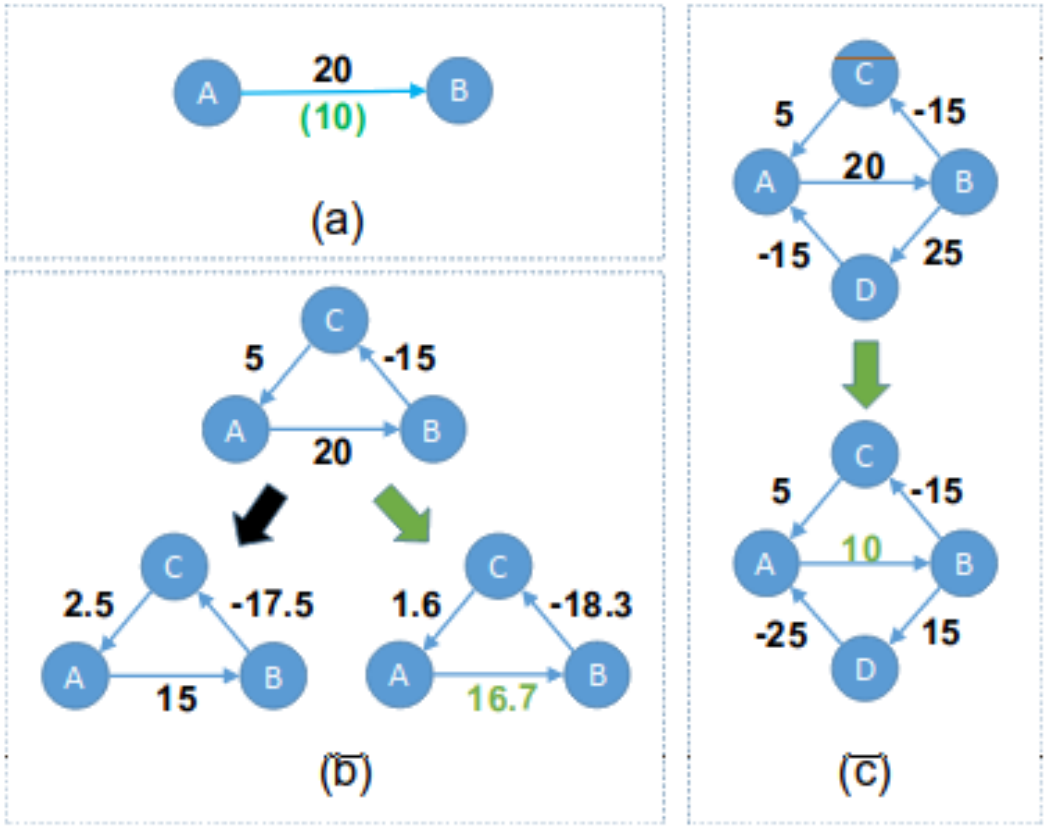


(a) All coded probes



(b) “Pure” coded probes

Correcting clocks of several nodes



- Here A & B alone can't guess they have a wrong sync (20 instead of 10); with C it's getting closer, with D the correct sync is found.

Comparison with NTP

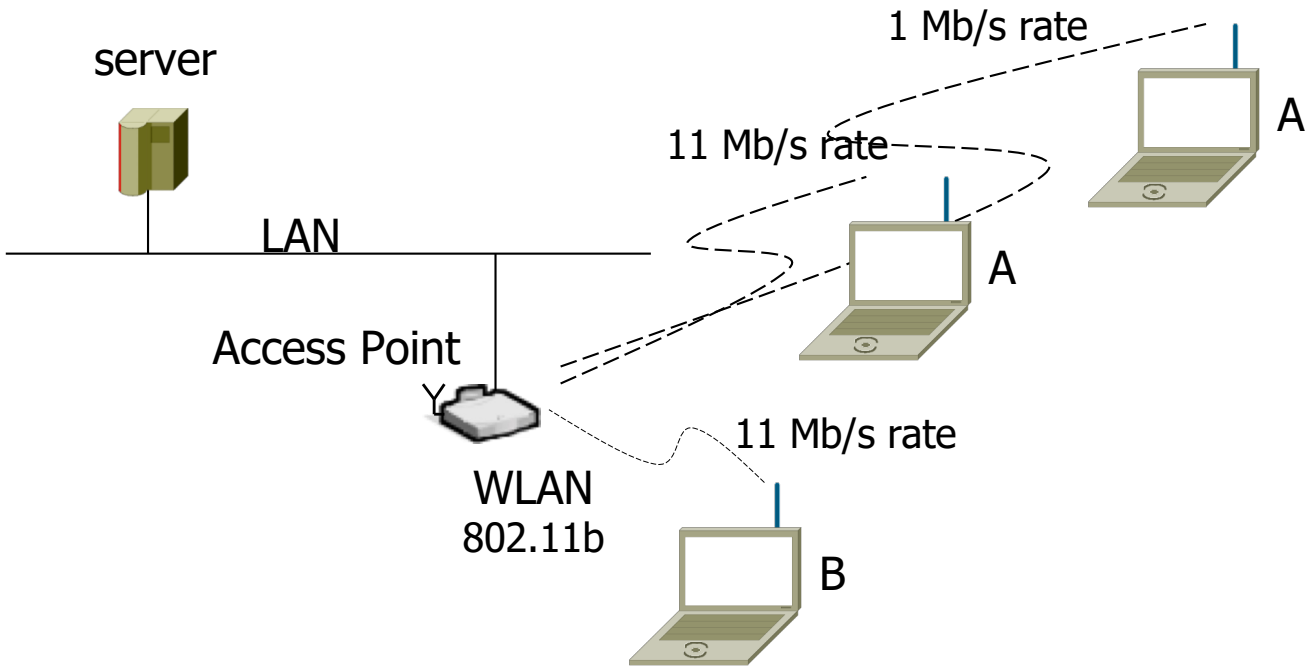
	NTP (with NIC timestamps)		Huygens	
	Mean abs. error	99th percentile abs. error	Mean abs. error	99th percentile abs. error
0% load	177.7 ns	558.8 ns	10.2 ns	18.5 ns
40% load	77,975 ns	347,638 ns	11.2 ns	22.0 ns
80% load	211,011 ns	778,070 ns	14.3 ns	32.7 ns

802.11 Performance Anomaly

802.11 Performance Anomaly

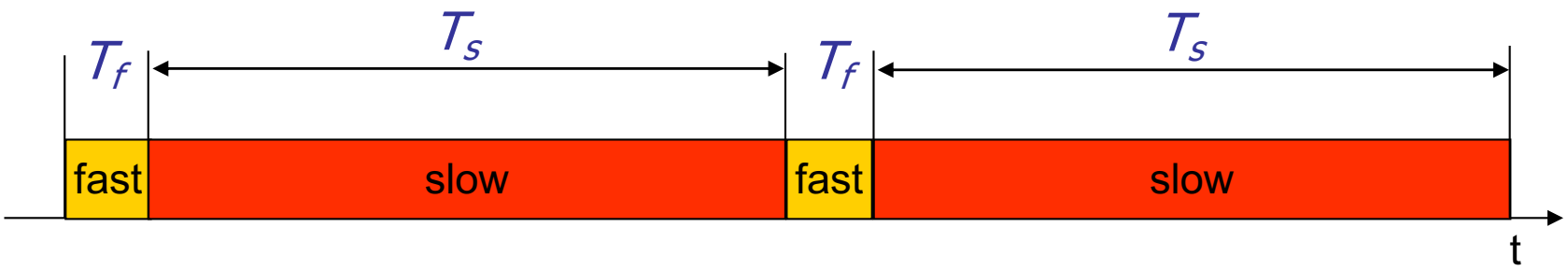
- G. Berger-Sabbatel, F. Rousseau, M. Heusse, A. Duda: *Performance anomaly of 802.11b,* INFOCOM 2003

Performance anomaly



nominal rate (Mb/s)		throughput (Mb/s)	
A	B	A	B
11	11	3.09	3.36
1	11	0.76	0.76

One slow host, one fast



- DCF - CSMA/CA
  - equal access probability, not equal share
  - same packet/s rate, not b/s
- Throughput when R = 11 Mb/s, r = 1 Mb/s
  - Fast: (1/11)/(1/11 + 1) * 0.7 * 11 Mb/s = 0.64 Mb/s
  - Slow: (1)/(1/11 + 1) * 0.7 * 1 Mb/s = 0.64 Mb/s

Performance anomaly

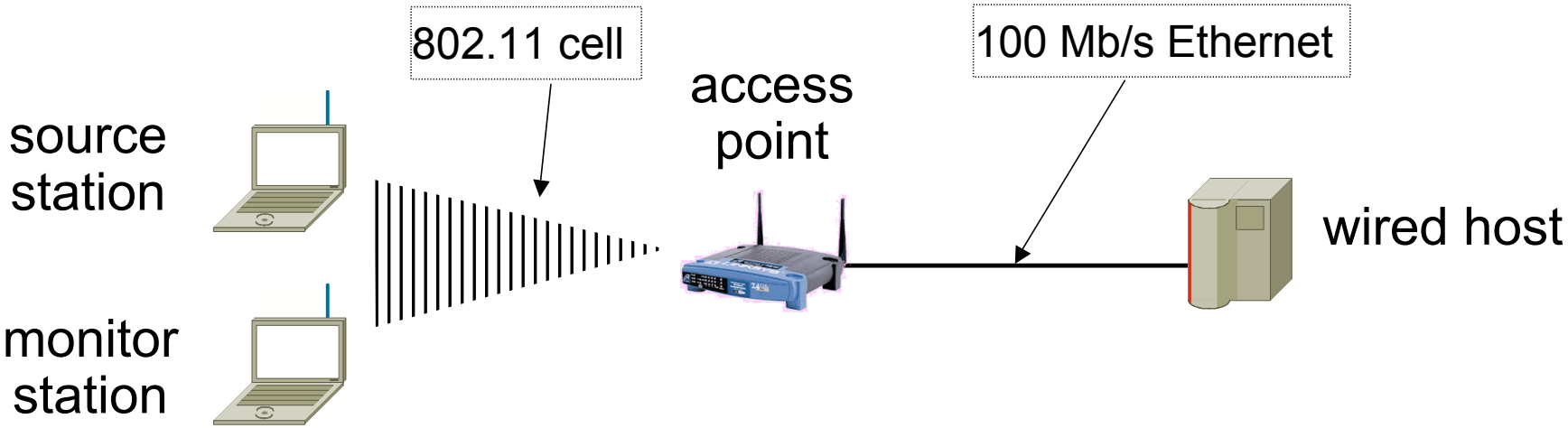
$$X_{\mathrm{f}} = X_{\mathrm{s}} = X = \frac{s}{T_{\mathrm{f}} + T_{\mathrm{s}}},$$

$$\frac{1}{X} = \frac{1}{R} + \frac{1}{r} + s(t_{\mathrm{ov}}^{R} + t_{\mathrm{ov}}^{r}),$$

- R, r – lower data rate, higher data rate
- s – frame size
- T_f, T_s – time on air, $T_f = s/R + t_{ov}^{R}$
- t_{ov} – overhead
- Throughput
  - Geometric mean of bit rates
  - Max-min fairness of throughputs X_f, X_s

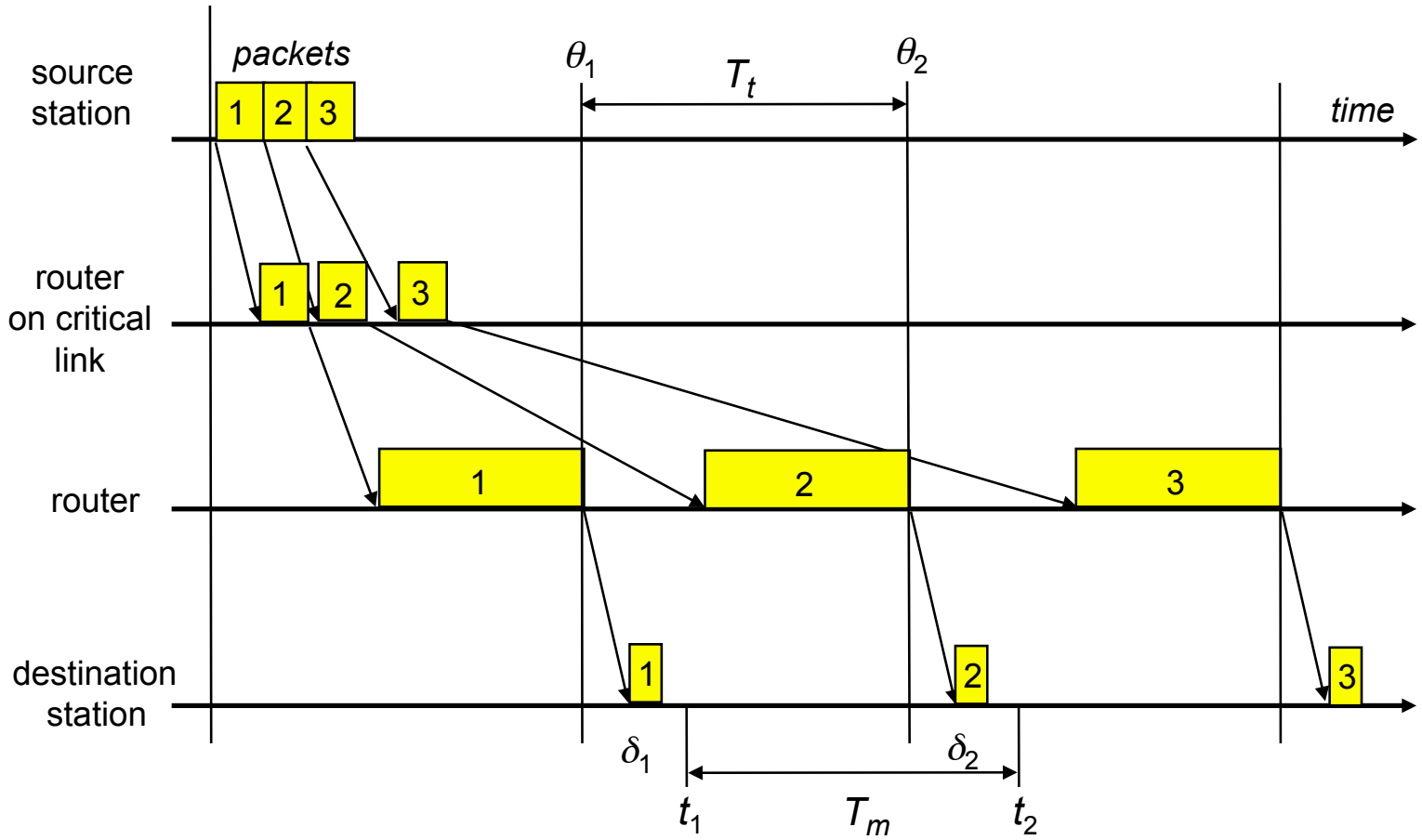
Interarrival Histograms: Measuring One-Way Variable Transmission Delays without Synchronized Clocks

Interarrival Histograms



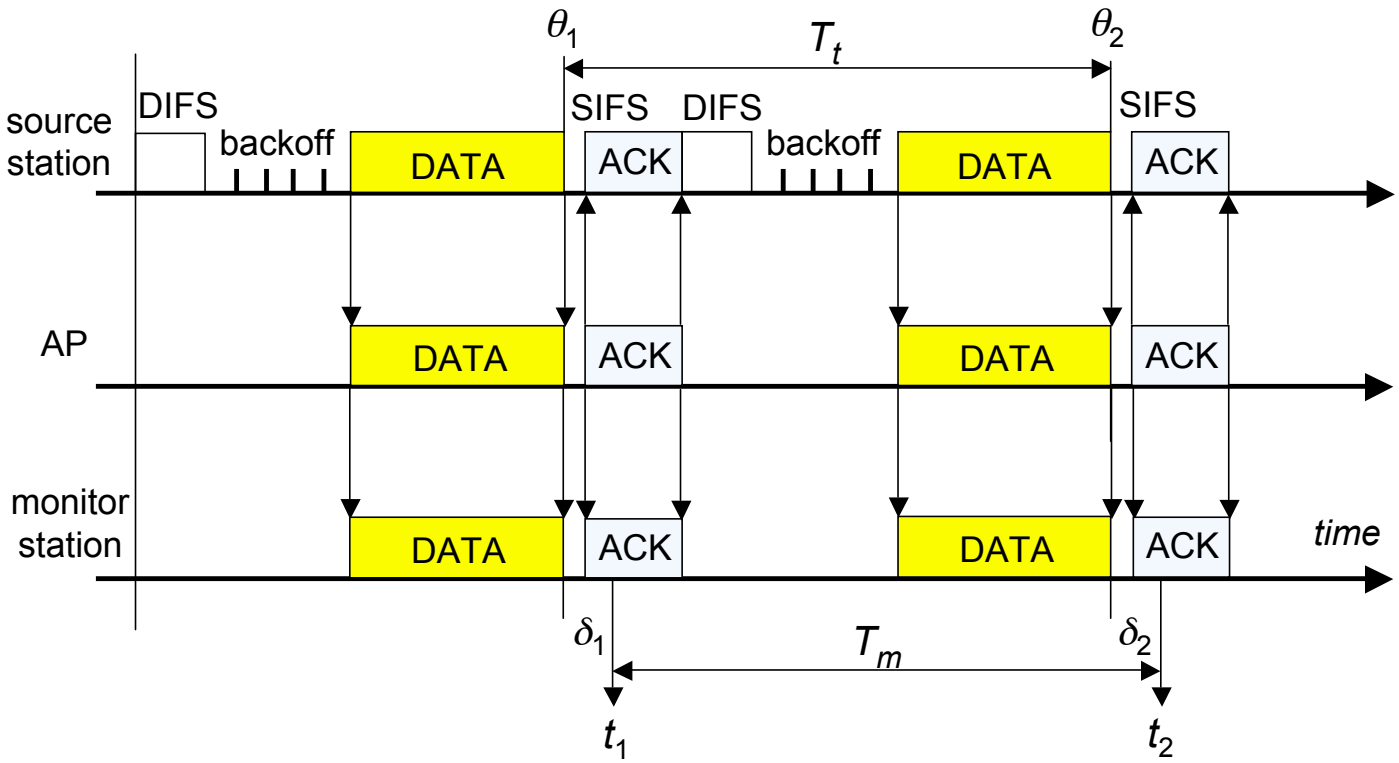
- Measurement configuration of the 802.11 WLAN

Interarrival Histograms



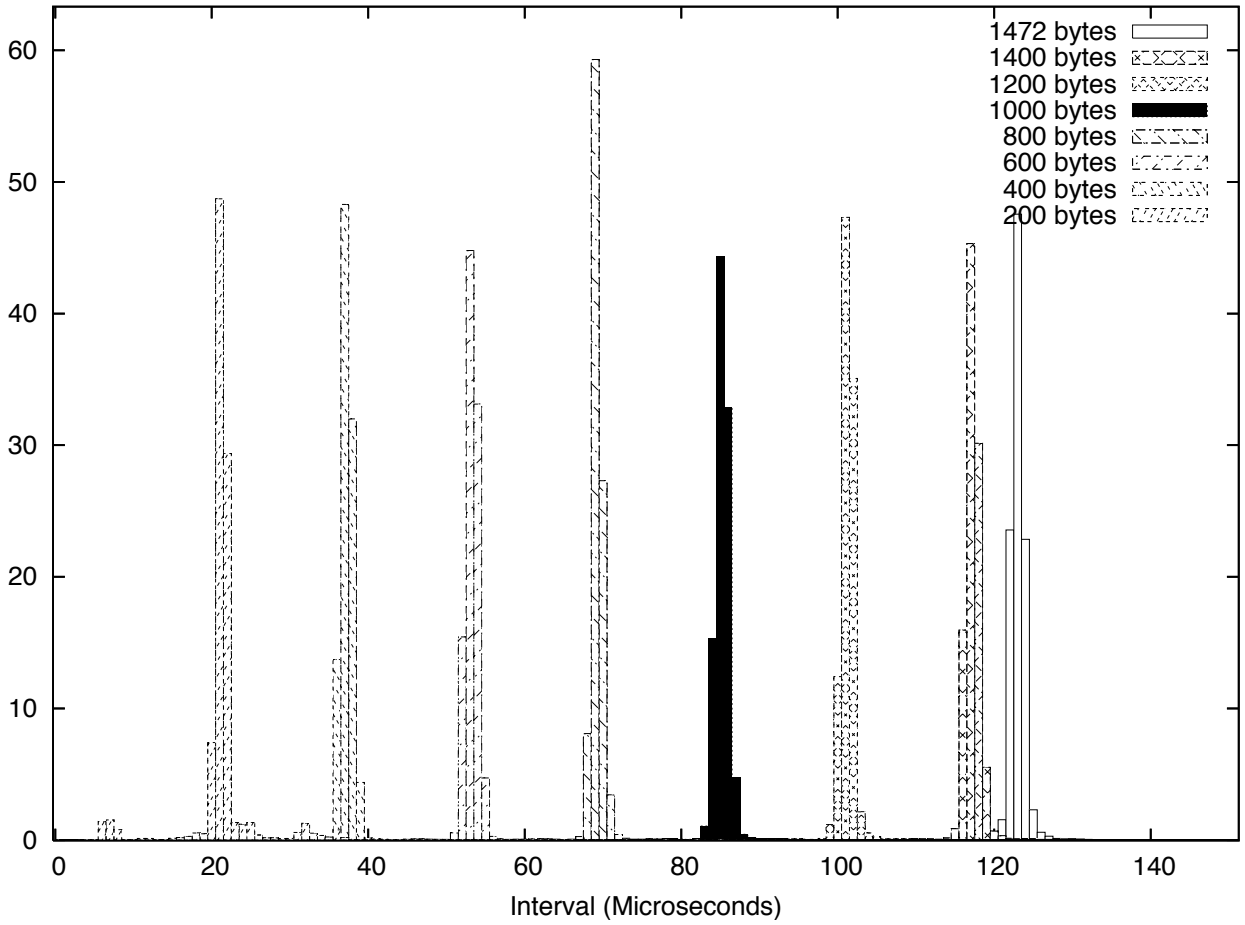
- Principle of measurements – extension of Packet Pair

Interarrival Histograms



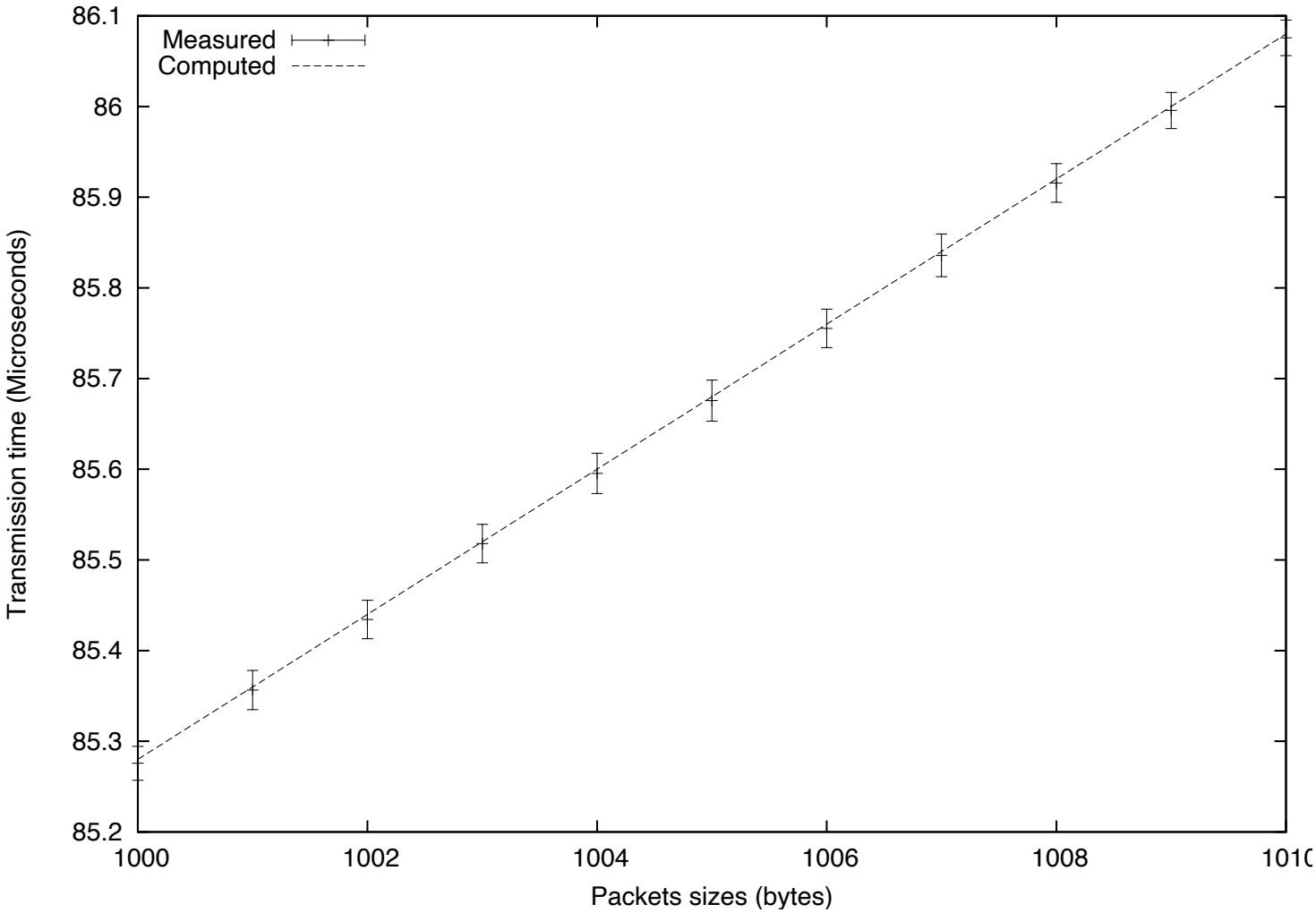
- Principle of measurements of the 802.11 WLAN

Interarrival Histograms



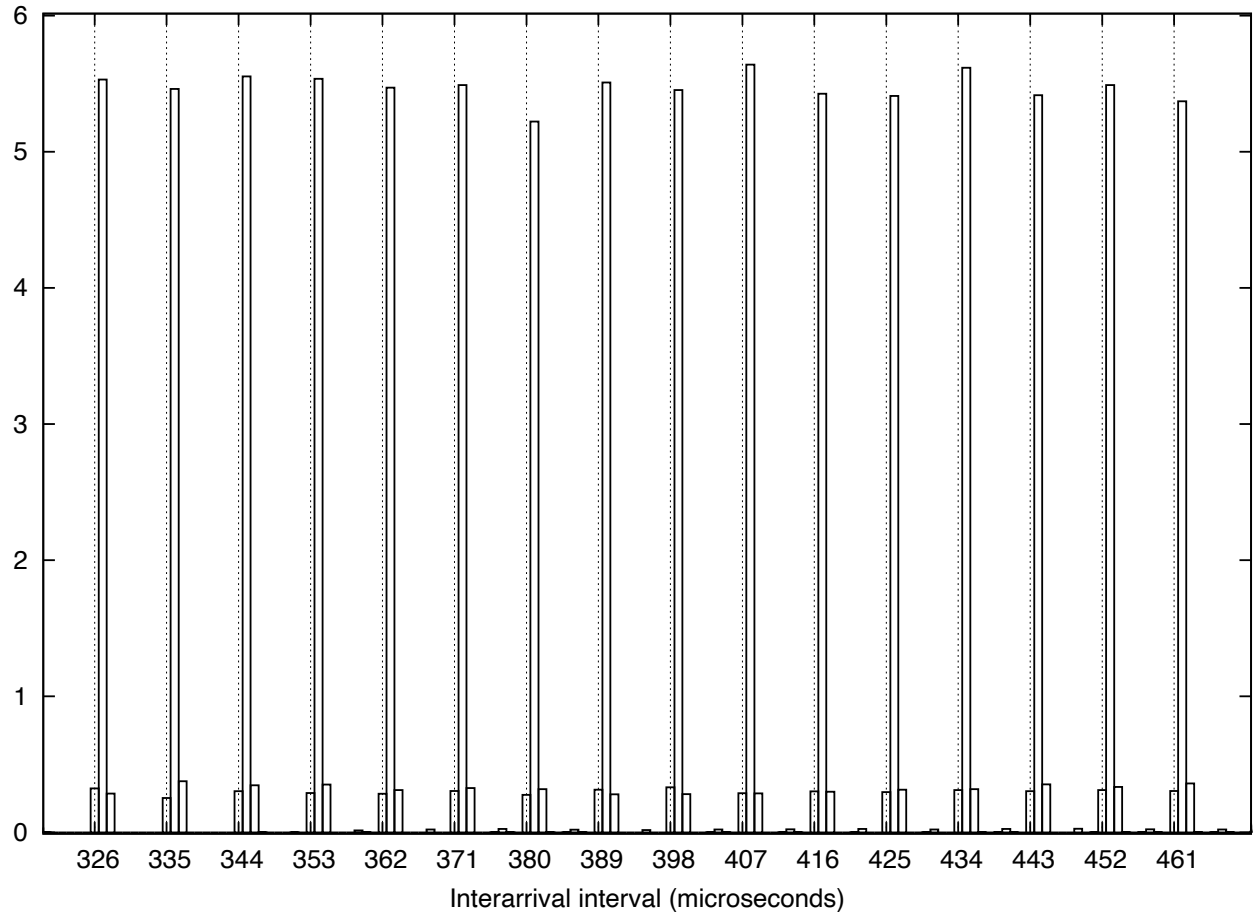
- Histograms of transmission times for the 100 Mb/s Ethernet

Interarrival Histograms



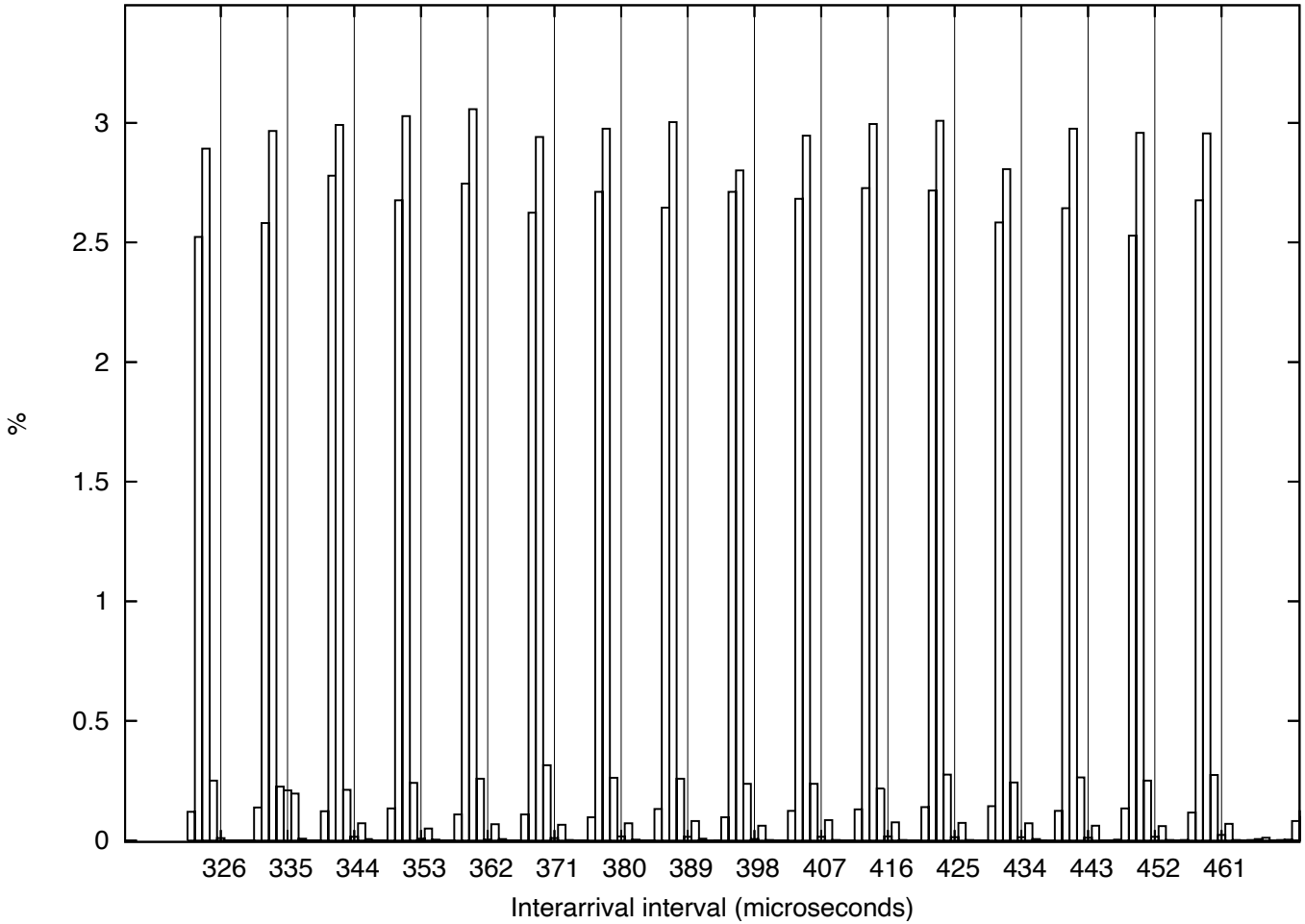
- Transmission delay vs. frame size

Interarrival Histograms



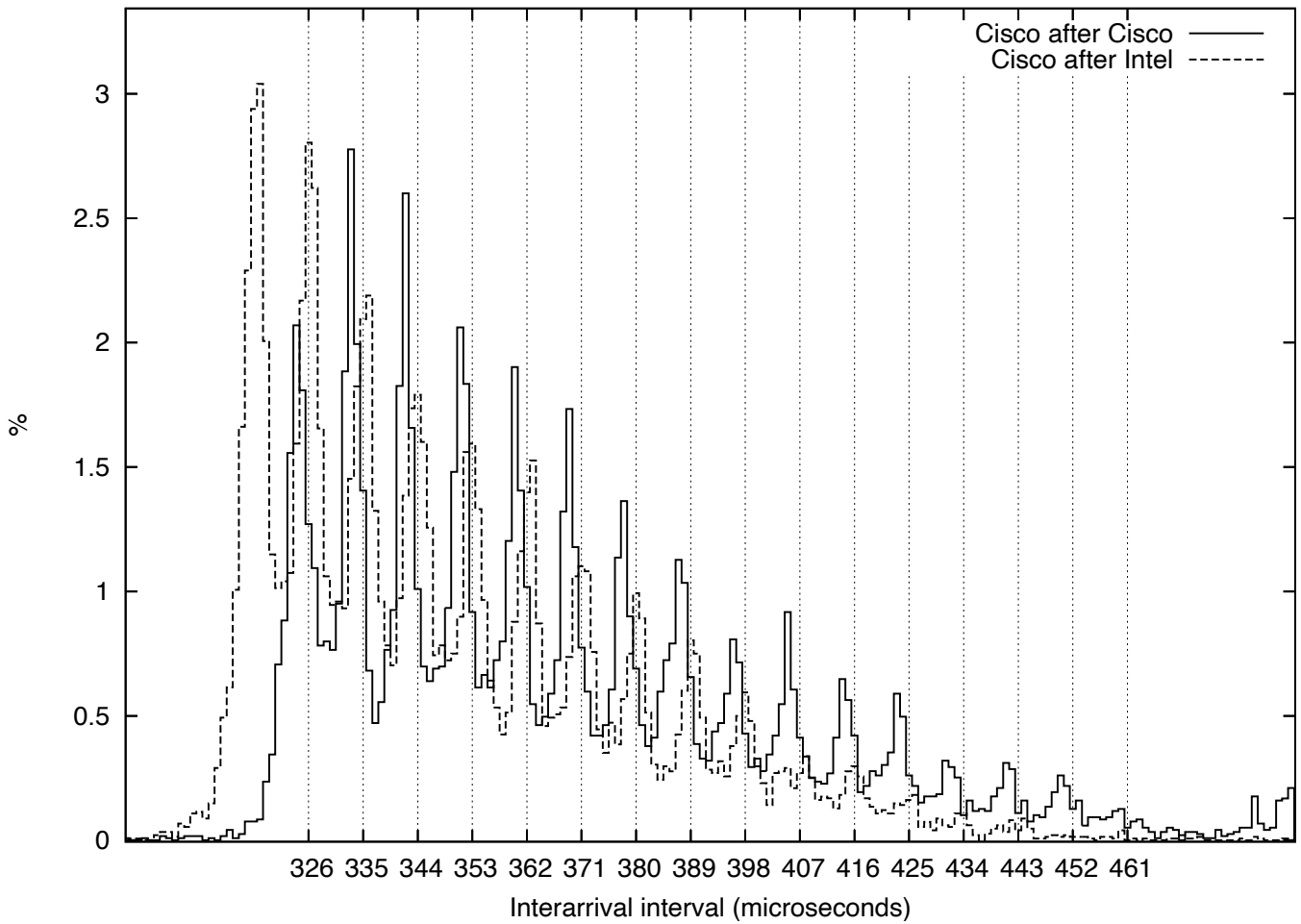
- Measured Linksys WRT 54GL access point, hardware timestamping on the Netgear-Prism GT card

Interarrival Histograms



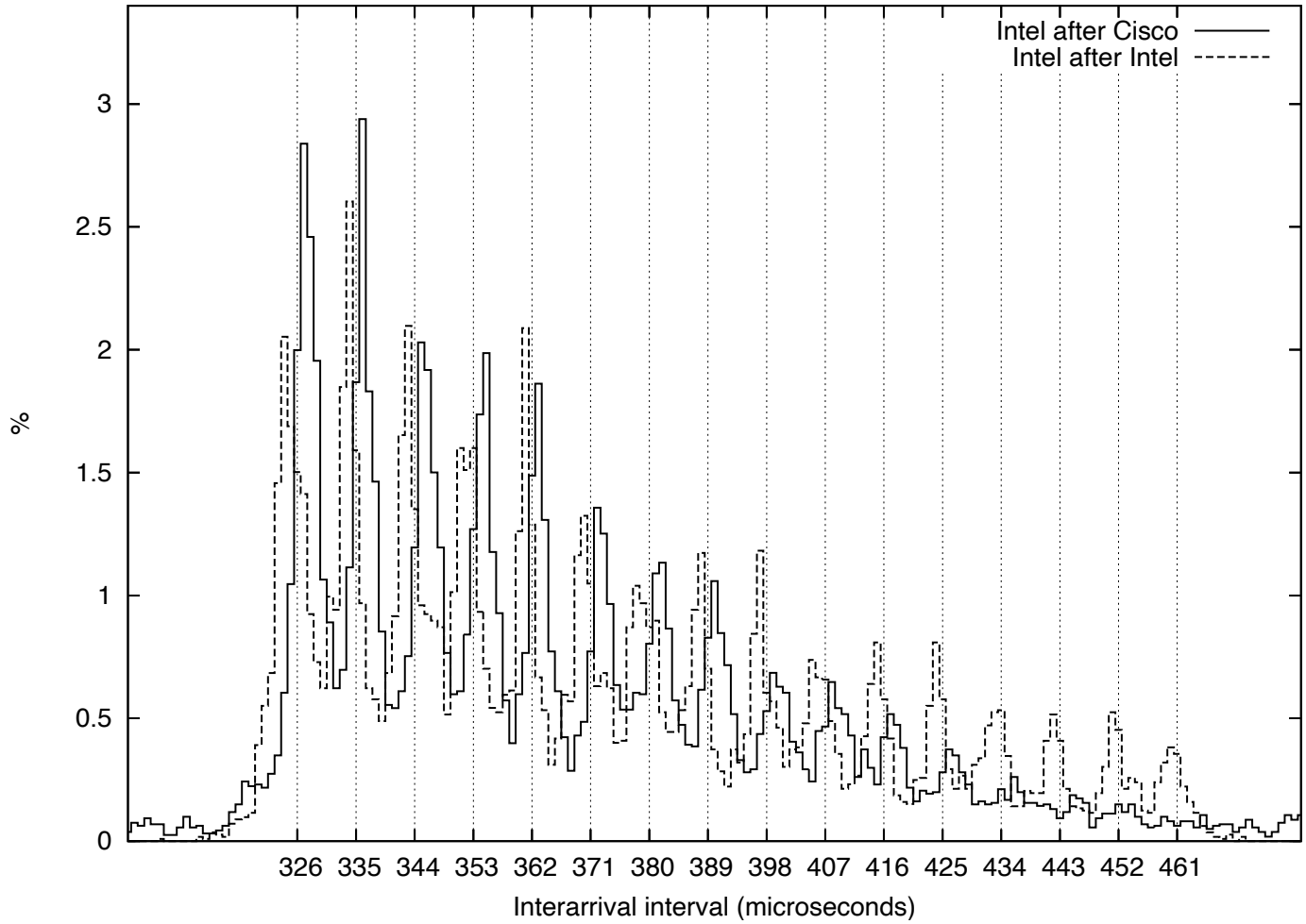
- Histogram of Cisco Aironet AP 1132 AG
- Peaks appear too early compared to the standard values by 4 μs, the first peak appearing at 322 μs.

Interarrival Histograms



- Cisco Aironet AP 1132 AG vs. Intel Centrino-IPW2200
- Cisco after Cisco - access point after its previous transmission, Cisco after Intel - access point after a transmission by the test station with the Intel card

Interarrival Histograms



- Cisco Aironet AP 1132 AG vs. Intel Centrino-IPW2200
- Intel after Cisco - test station after a transmission by the access point, Intel after Intel - test station after its previous transmission

Idle Sense for 802.11

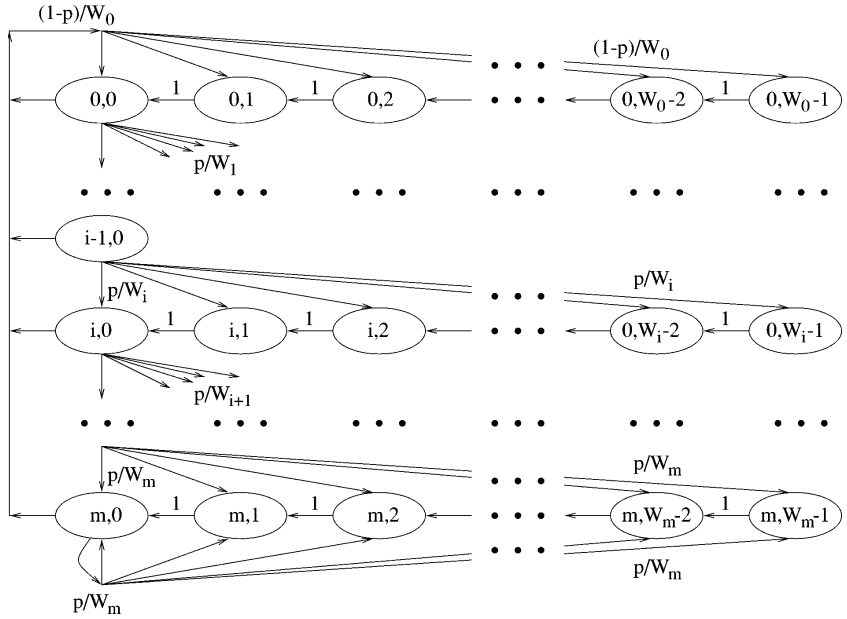
Idle Sense for 802.11

- M. Heusse, F. Rousseau, R. Guillier, A. Duda: *Idle sense: an optimal access method for high throughput and fairness in rate diverse wireless LANs,* SIGCOMM 2005

Optimal Access Method for 802.11

- Observe the number of idle slots before transmission
  - Channel load indicator
- Control CW (Contention Window)
  - Adjust CW to the current state
  - Optimal operation in all conditions
    - What is the optimal CW?
    - How it relates to the number of idle slots?

Number of idle slots



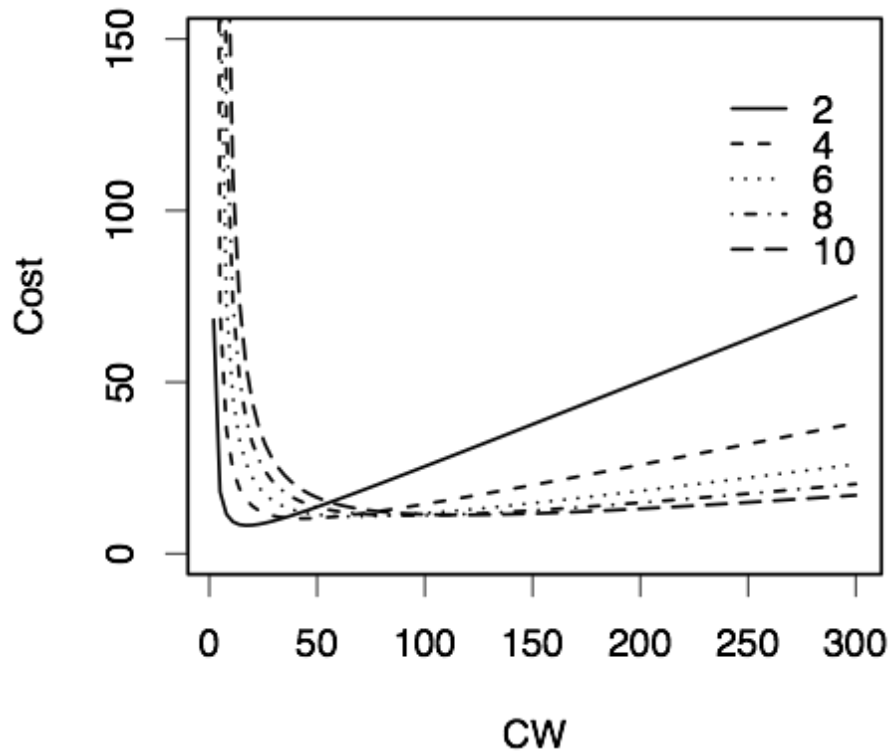
$$\text{Total\_Idle\_}p = (E[N_c]+1)\cdot E[\text{Idle\_}p] = \frac{1-p}{M\cdot p}$$

from which we get

$$M = \frac{1-p}{p\cdot \text{Total\_Idle\_}p}. \qquad (11)$$

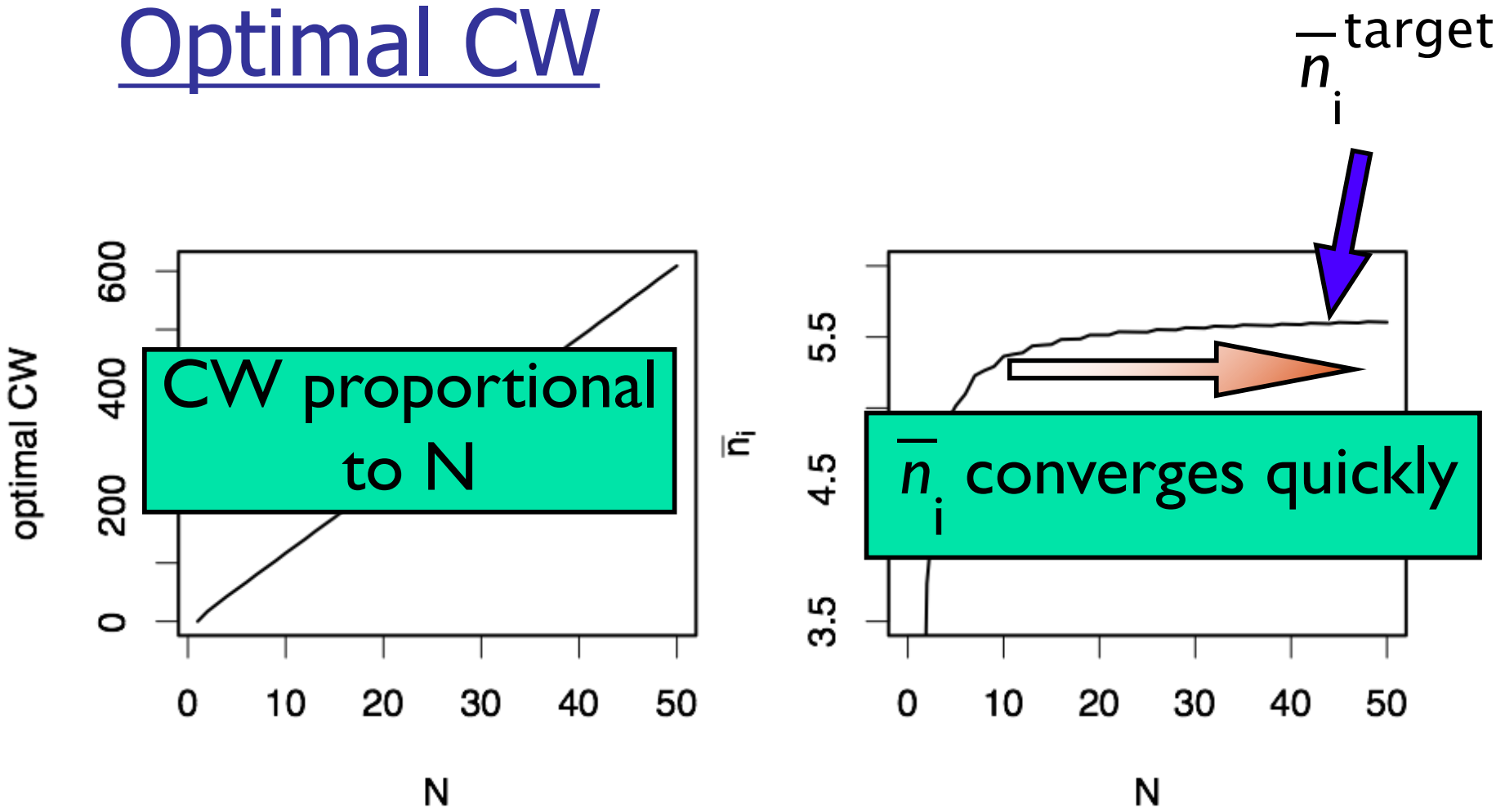
- Related work
  - optimizing DCF – optimal CW size
  - estimating the number of contending stations

Optimal CW



- Cost function: Proportion of time spent in collisions or contention
- Minimizing the cost ⇒ Maximizing throughput

Optimal CW

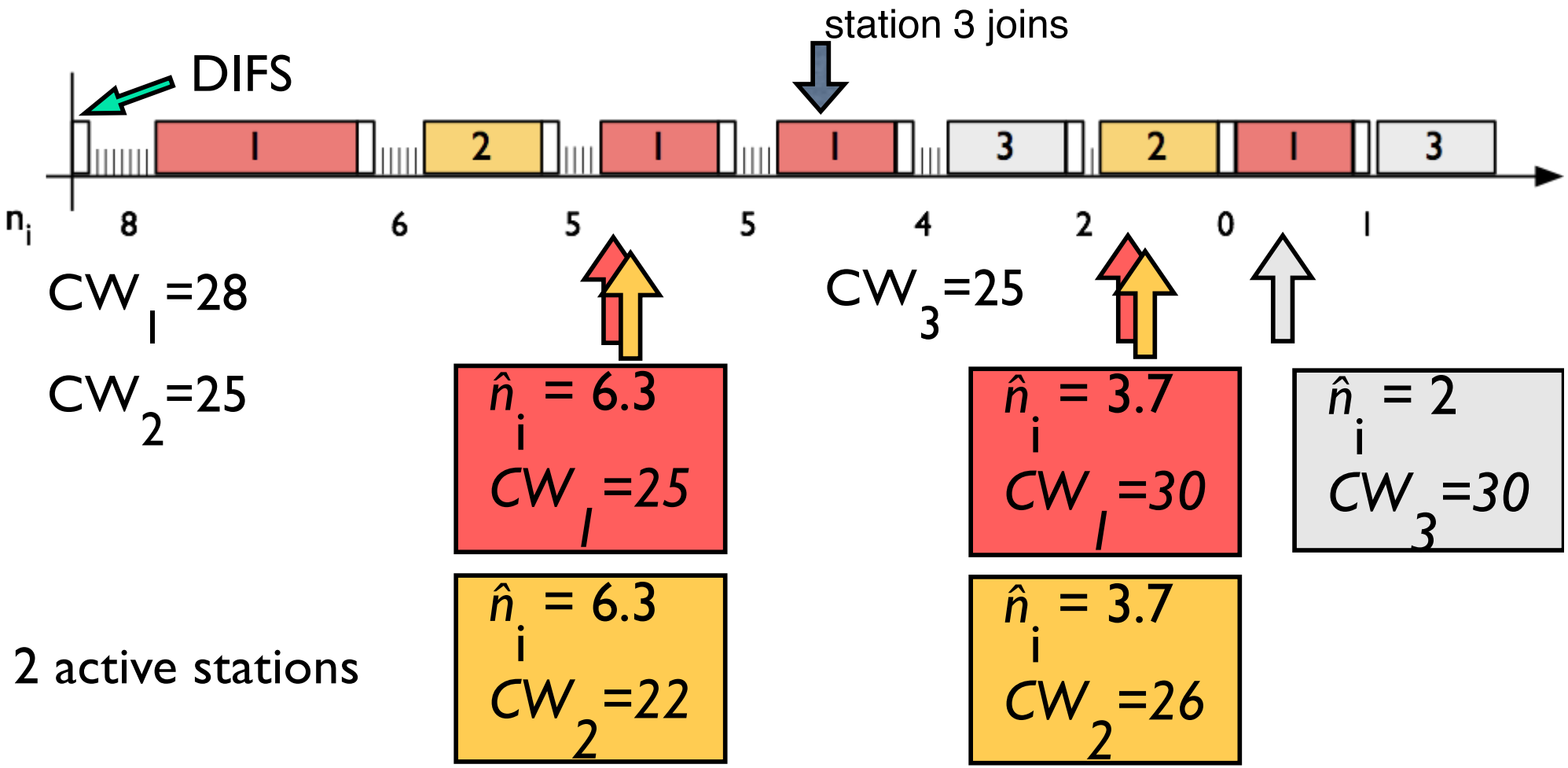


$\overline{n}_i$: average number of idle slots between transmission attempts

Idle Sense

- Stations track $\overline{n}_i$ and make it converge to the target value
  - Each station estimates $\overline{n}_i$
  - Rises/Lowers CW when $\overline{n}_i$ too small/big compared to $\overline{n}_i^{\text{target}}$
- Adjusting CW is done according to AIMD
  - all stations converge to a similar value of CW

Example



2 active stations

(α= 1/1.2, ε=0.01, ntrans=3, $\bar{n}_i^{target}$ = 5.7)

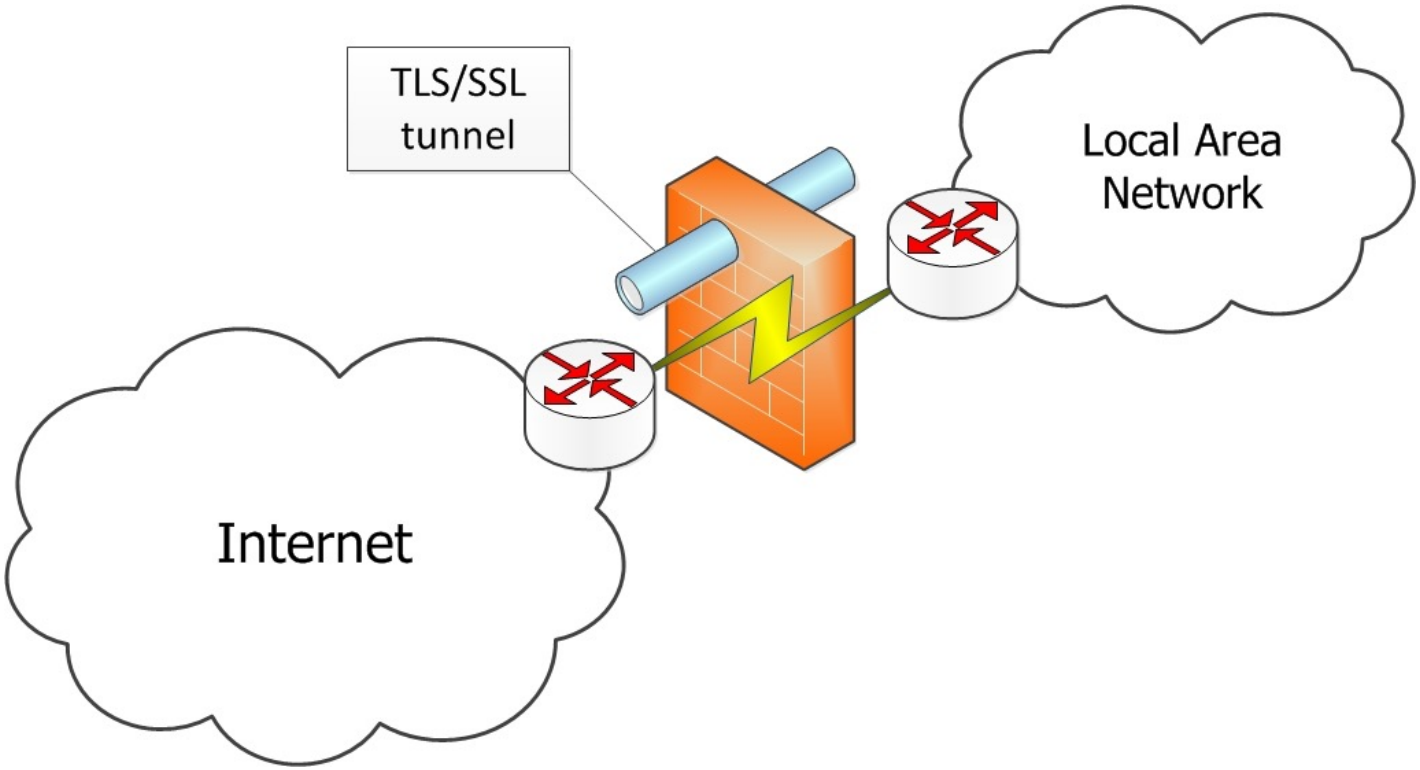
Classifying TLS/SSL Encrypted Application Flows

Classifying TLS/SSL Encrypted Application Flows

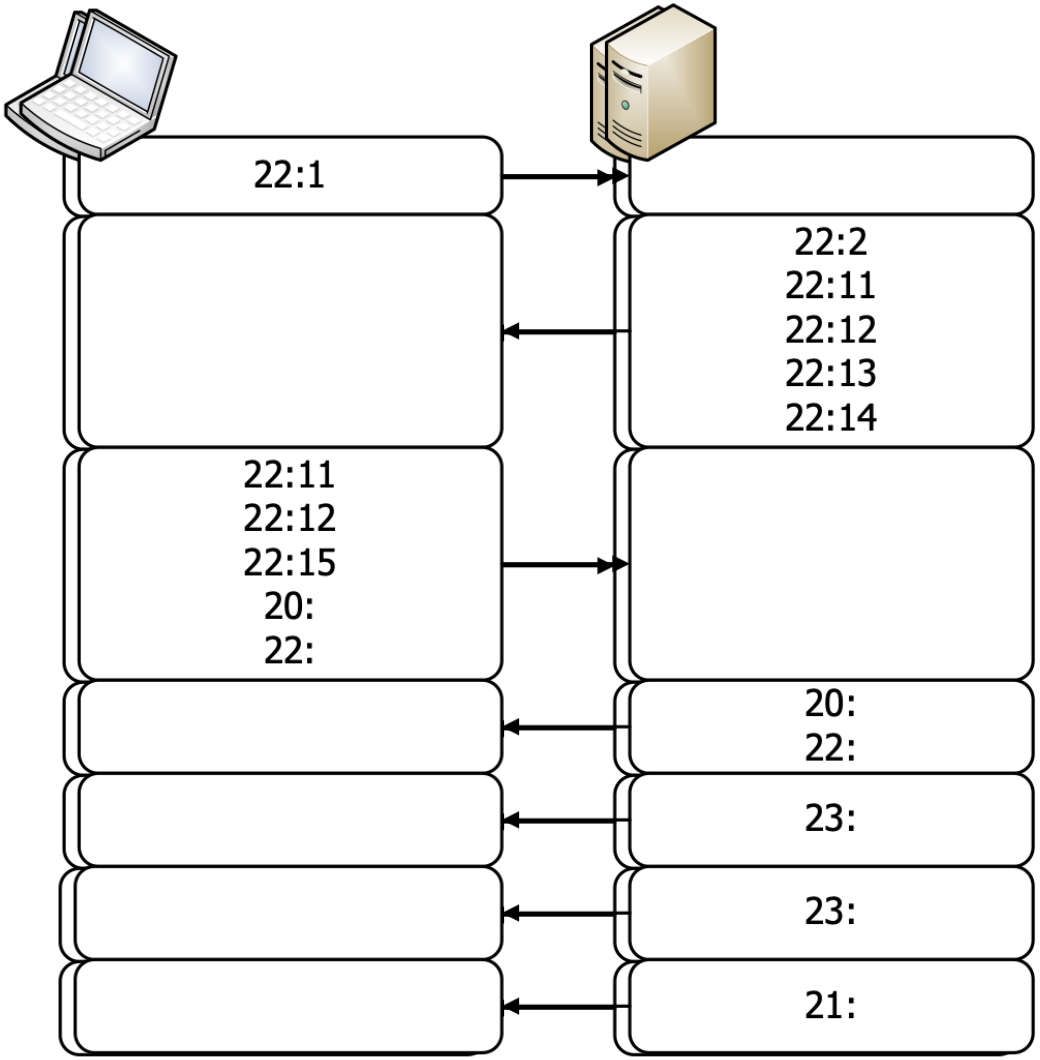
- M. Korczynski, A. Duda: *Markov chain fingerprinting to classify encrypted traffic*, INFOCOM 2014

Objectives

- Classifying TLS/SSL encrypted/tunneled application flows



Client-Server communication

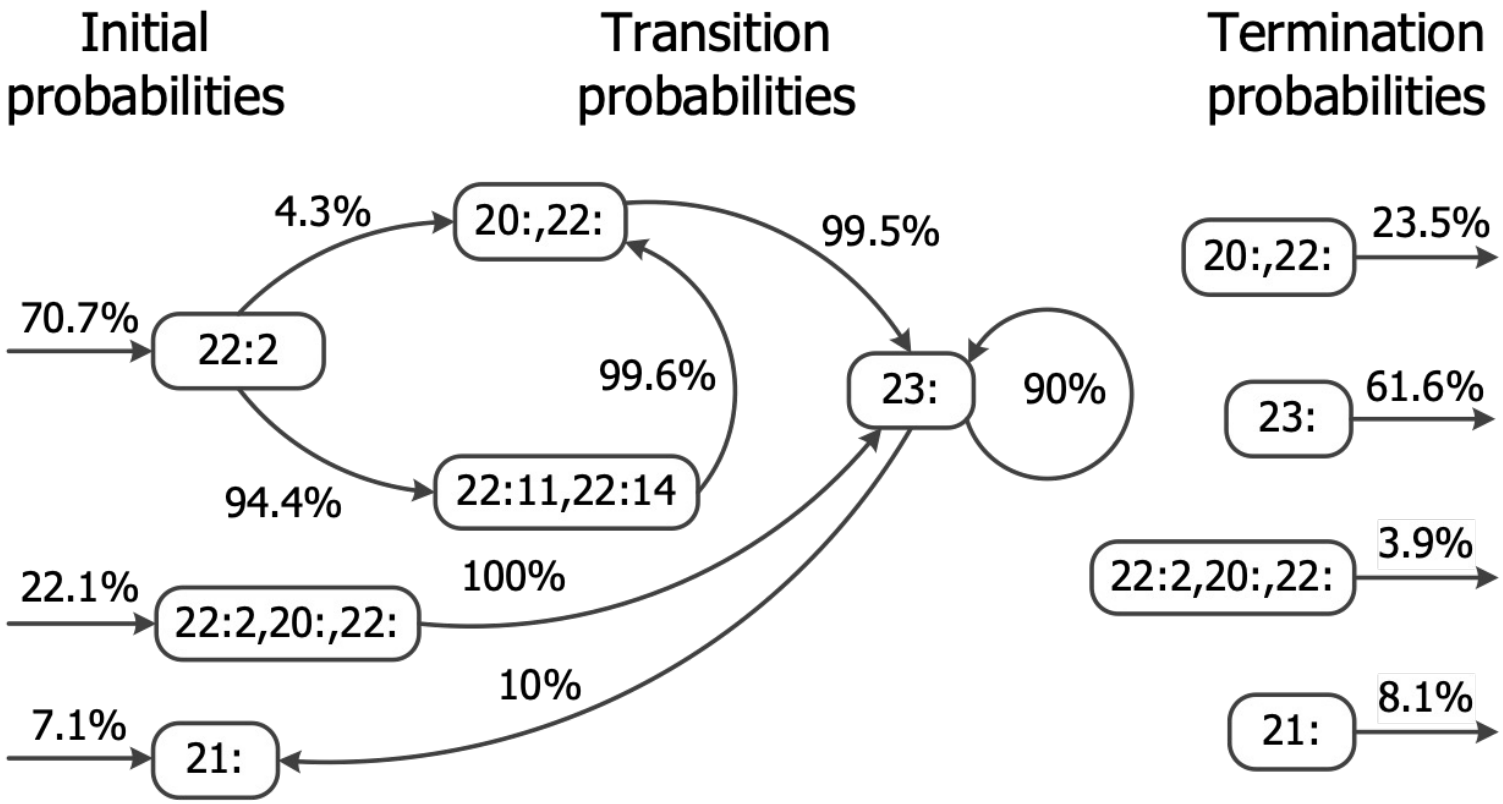


Decimal Code	Protocol Type
20	Change Cipher Spec
21	Alert
22	Handshake
23	Application Data

Decimal Code	Handshake Message Type
0	Hello Request
1	Client Hello
2	Server Hello
11	Certificate
12	Server Key Exchange
13	Certificate Request
14	Server Hello Done
15	Certificate Verify
16	Client Key Exchange
20	Finished

Methodology: Markov classifier

- Client-server communication represented as Markov states (e.g., PayPal)

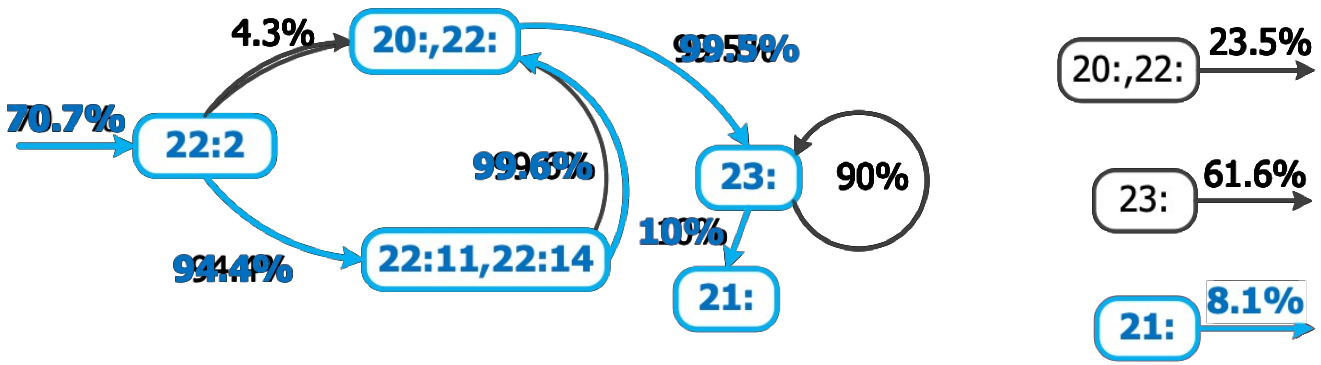


Classification phase: Markov classifier

- **Flow to classify:** 22:2; 22:11,22:14; 20:,22:; 23:; 21:.

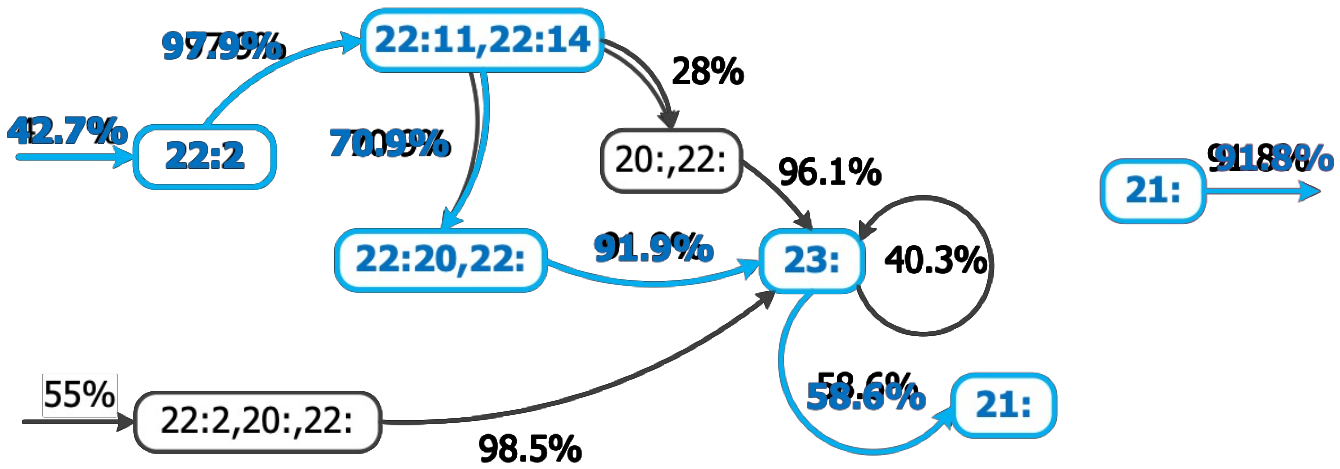
Initial probabilities | Transition probabilities | Termination probabilities | Final probability

PayPal



P1 = 70.7% * 94.4% * 99.6% * 99.5% * 10% * 8.1% = 0.54%

Twitter



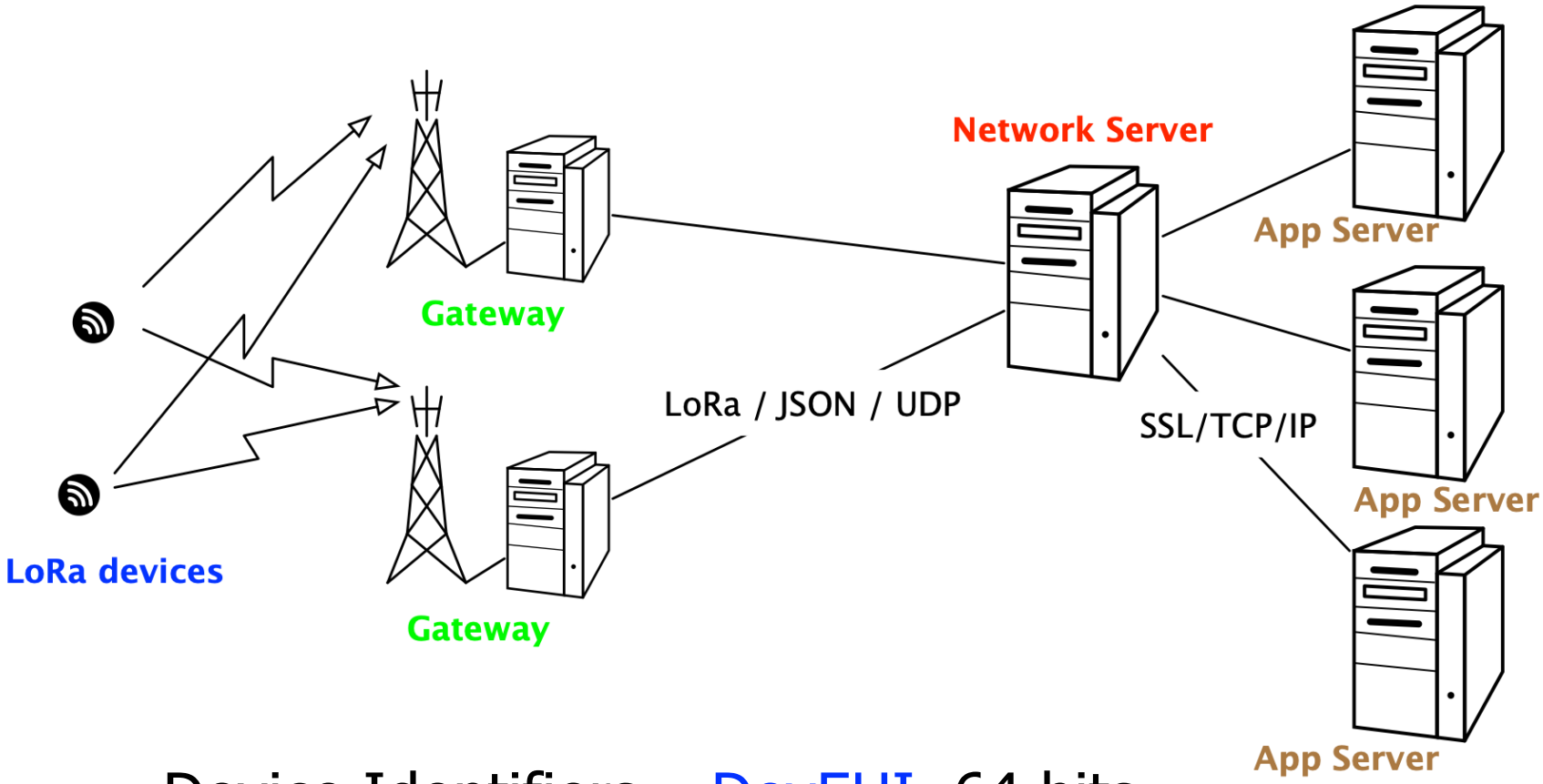
P2 = 42.7% * 97.9% * 70.9% * 91.9% * 58.6% * 91.8% = 14.7%

LoRa and Semantic Names

Semantic Names

- S. Fernandez, M. Amoretti, F. Restori, M. Korczynski, A. Duda: *Semantic Identifiers and DNS Names for IoT*, ICCCN 2021

LoRa and Semantic Names



- Device Identifiers – DevEUI, 64 bits
- Encoded as a compact domain name
- Support queries on semantic names

Semantic Names

- Self-certifying name for IoT devices - name derives from a public key

  $$A = \mathbf{ripemd160}(\mathbf{sha256}(\mathbf{K_p}))$$

- A is encoded with **`base32`** (20 characters) giving the DNS name
- 8 byte EUI64 identifier from A with

  DevEUI = SHA-3(A)

- Several other domain names (aliases):
  - CNAME records

Examples - Semantic Description

- W3C Thing Description - complex, hierarchial attributes

```
"@context": [
    "https://www.w3.org/2019/wot/td/v1",
...],
"@type": "saref:TemperatureSensor",
...
"properties": {
    "temperature": {
        "description": "Weather Station Temperature",
        "type": "number",
        "minimum": -32.5,
        "maximum": 55.2,
        "unit": "om:degree_Celsius",
        "forms": [...]
    },
    ...
},
...
```

- **1d152**: properties, temperature, unit – degrees Celsius, value 2

Examples – Logical Location

- Logical Location, e.g., COAP: send a packet to a group

`all.bu036.floor1.west.bldg6.example.com.`

- group corresponds to ”all nodes in office bu036, floor 1, west wing, building 6”.

- assume that we have up to 32 buildings, 32 floors, and 1024 rooms

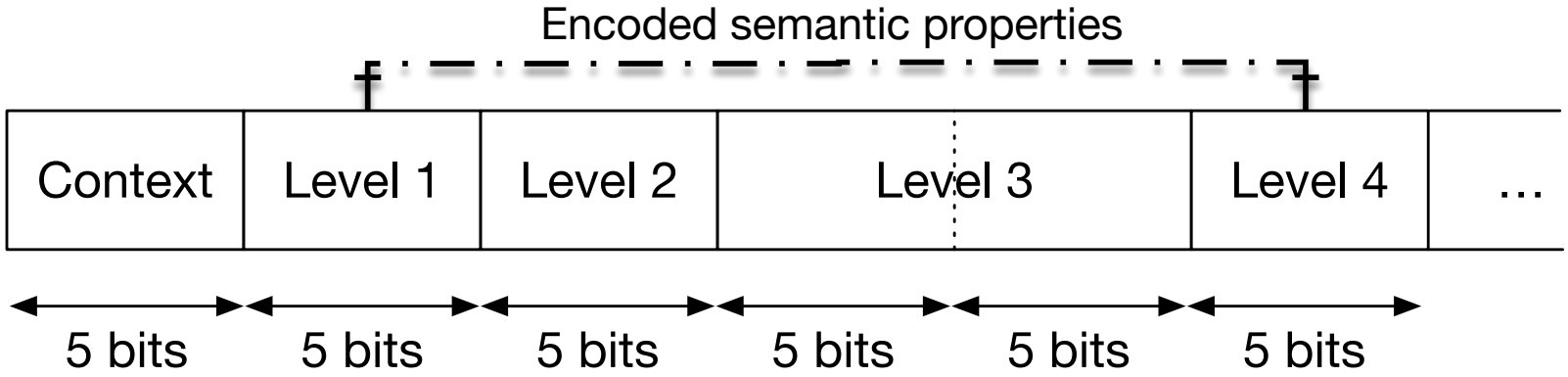
- **`27mcs`**: Room 214 on Floor 19 in Building 7

Examples – Physical Location

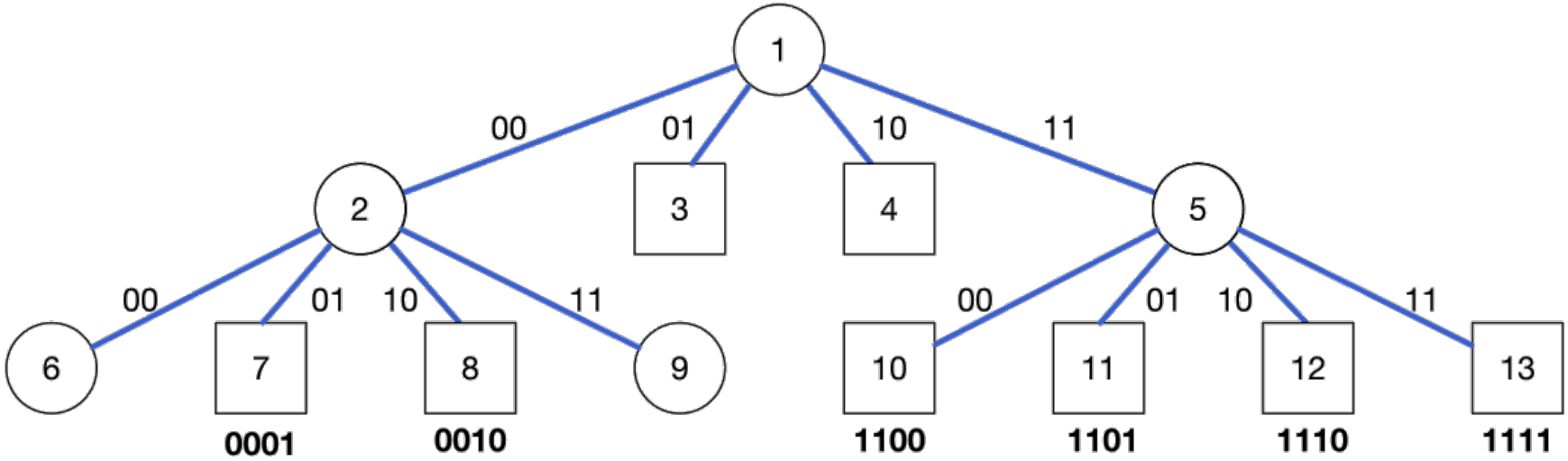
- Physical Location - the Statue of Liberty at coordinates (40.689167,−74.044444)

- **`dr5r7p4rx6kz`** – (40.689167,−74.044444)

Quad trees



- Context – defines the quad tree or type of geo-hash
- Leaves – encoding of properties



Examples - Semantic Description

- W3C Thing Description:

```
"@context": [
    "https://www.w3.org/2019/wot/td/v1",
...],
"@type": "saref:TemperatureSensor",
...
"properties": {
    "temperature": {
        "description": "Weather Station Temperature",
        "type": "number",
        "minimum": -32.5,
        "maximum": 55.2,
        "unit": "om:degree_Celsius",
        "forms": [...]
    },
    ...
},
...
```

- **1d152**: properties, temperature
  - **00001** — Context-1 (**1**)
  - **01100** — properties, 12th property in the description (**d**)
  - **00001** — temperature, 1st attribute (**1**)
  - **00101** — unit, 5th attribute (**5**)
  - **00010** — degree Celsius (**2**)

Examples – Logical Location

- Logical Location, e.g., COAP - send a packet to a group:

`all.bu036.floor1.west.bldg6.example.com.`

- group corresponds to ”all nodes in office bu036, floor 1, west wing, building 6”.

- Assume that we have up to 32 buildings, 32 floors, and 1024 rooms

- **`27mcs`**: Room 214 on Floor 19 in Building 7
  - **`00010`** - Context-2 (**`2`**)
  - **`00111`** - Building 7 (**`7`**)
  - **`10011`** - Floor 19 (**`m`**)
  - **`01011`** - Room 376 - first part (**`c`**)
  - **`11000`** - Room 376 - second part (**`s`**)

Physical Location

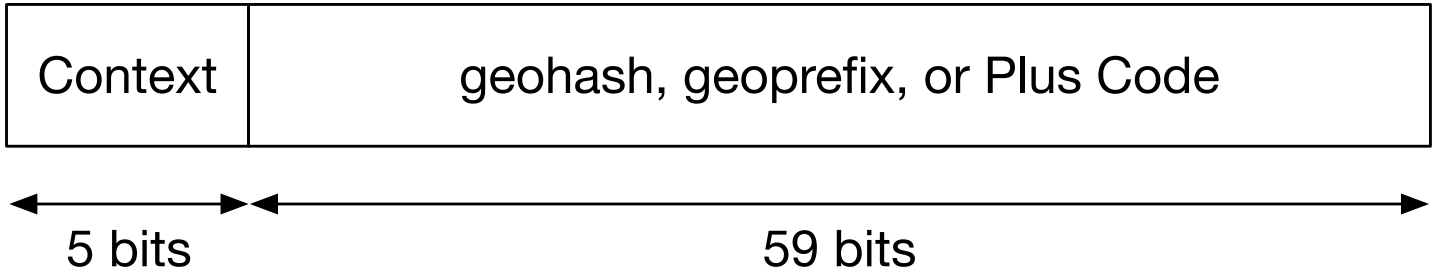


TABLE III
LONGITUDINAL DECIMAL DEGREE PRECISION AND THE SIZE OF A GEOHASH

length	lat bits	lng bits	lat error	lng error	error
1	2	3	± 23°	± 23°	± 2500 km
2	5	5	± 2.8°	± 5.6°	± 630 km
3	7	8	± 0.70°	± 0.70°	± 78 km
4	10	10	± 0.087°	± 0.18°	± 20 km
5	12	13	± 0.022°	± 0.022°	± 2.4 km
6	15	15	± 0.0027°	± 0.0055°	± 610 m
7	17	18	± 0.00068°	± 0.00068°	± 76 m
8	20	20	± 0.000085°	± 0.00017°	± 19 m
9	22	23			
10	25	25			± 59 cm
11	27	28			
12	30	30			± 1.84 cm

Semantic Names

- Physical Location - the Statue of Liberty at coordinates (40.689167,−74.044444)

TABLE IV
PRACTICAL EXAMPLE OF A GEOHASH

geohash	Latitude	Longitude
dr5r7p4rx6kz	40.689167	-74.044444
dr5r7p4	40.69	-74.04
dr5r111	40.61	-74.13

- **dr5r7p4rx6kz** – (40.689167,−74.044444)
- **dr5r**: resolution of 20 km
- **dr5r7p**: resolution of 600 m
- **dr5r7p4r**: resolution of 20 m

Semantic Names

```
<Instance>.<Service>.<Domain> IN SRV <data>
```

- Query for a PTR record:

```
<Service>.<Dom> IN PTR <Instance>.<Service>.<Dom>
```

- Example:

```
_dr5r7p4r._iot._udp.iot.org IN PTR
```

- look for IoT devices near the Statue of Liberty

Lessons Learnt

Nice paper – one cool idea

- Global Time – linear relation between clocks
- Anomaly – surprising performance
- Idle Sense – load estimator and AIMD
- Encrypted SSL – modeling establishment of secure session
- Histograms – extension of Packet Pair
- LoRa – compact representation of complex information

Experimental work is important

- Simulators?
- You can only simulate what you know!

- Theory?
- Nice if it gives you a basis for a cool algorithm
- Need to confront with reality

Team is important

- Stimulating discussions
- Fruitful amplification
- Mode "commando"

Writing is important

- The best idea gets rejected if not understood
- Decalog/Writing Tips
  - simple, direct language (active voice) – one thing=one phrase
  - write for others, not for you (putting the reader first)
  - reviewer may be not a specialist in your narrow problem
    - if not understood, it's your fault, not the reviewer
  - reread by somebody not involved
  - giving intuition, examples

"Writing is thinking. To write well is to think clearly. That's why it's so hard."

Writing is important

- Get a well-written paper, try to imitate the style
- Common errors
  - complex phrases
  - clash of variables, missing definitions
  - ~~works, performances, interactions~~
- Spell check – your best friend

Easy reading is damn hard writing.

The introduction (1 page)

1. What is the problem?
2. Why is it interesting and important?
3. Why is it hard? (e.g., why do naive approaches fail?)
4. Why has not it been solved before? (Or, what's wrong with previous proposed solutions? How does mine differ?)
5. What are the key components of my approach and results? (Any specific limitations?)
6. State your contributions

Your real best friend - Thesaurus

- Look up for a synonym
  - accurate meaning
  - use different words
- Roget's Thesaurus
- ChatGPT?

A synonym is a word you use when you can't spell the other one.

As a conclusion: Ideal environment - MIT

- Small research group (5)
- Assistant asked me if I have some requests for her
- Needed to buy a device, 24h delivered
- No Lab/Univ reporting
- Funding – spent one afternoon to write 10 pages for 6 M$ DARPA funding
- Managing previous proposals
  - deliverables = parts of papers

Questions? Comments?