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

Global traces, global time

\[
RTT = \delta_j = (t_4^j - t_1^j) - (t_3^j - t_2^j), j = 1, \ldots, n
\]
\[
t_2^j = t_1^j + T_f^j - \theta_j, j = 1, \ldots, n
\]
\[
t_4^j = t_3^j + T_b^j + \theta_j, j = 1, \ldots, n
\]

**Symmetry:** if \( T_f^j = T_b^j \),

\[
Offset = \theta_j = \frac{(t_4^j - t_1^j) - (t_3^j - t_2^j)}{2}, j = 1, \ldots, n
\]

**Asymmetry:** if \( T_f^j \neq T_b^j \),

\[
Offset = \theta_j = \frac{(t_4^j - t_1^j) - (t_3^j - t_2^j)}{2} + \frac{T_b^j - T_f^j}{2}, j = 1, \ldots, n
\]

- Accuracy depends on asymmetry!
Calibrating NTP

One way delays

Histograms of $T_f$

Histograms of $T_b$

Histograms of $d_f^{\text{min}}$

Histograms of $d_b^{\text{min}}$

Faten MKACHER and Andrzej DUDA (LIG)

Calibrating NTP
Compensate the systematic offset

Histograms of $O$ set for standard NTP (left) and calibrated NTP (right) at 9AM.

- Standard NTP: $\mu = 1744, 7\mu s$, $\sigma = 336, 9\mu s$
- Calibrated NTP: $\mu = 108, 7\mu s$, $\sigma = 299, 7\mu s$
Secure Time Synchronization

Secure Time Synchronization

- Time Client (TC)
- Authorization Server (AS)
- Time Server (TS)

TLS Session

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

Send me block headers from Block 9000

Block headers from Block 9000 to the end of the Blockchain

SPV Client

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

$$C_1(t) = a_{12}C_2(t) + b_{12}$$
SVM - Support Vector Machines

- H3 separates two classes with the maximum margin

Here H1 does not separate the classes. H2 does, but only with a small margin. H3 separates them 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

<table>
<thead>
<tr>
<th></th>
<th>NTP (with NIC timestamps)</th>
<th>Huygens</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mean abs. error</td>
<td>99th percentile abs. error</td>
<td>Mean abs. error</td>
</tr>
<tr>
<td>0% load</td>
<td>177.7 ns</td>
<td>558.8 ns</td>
<td>10.2 ns</td>
</tr>
<tr>
<td>40% load</td>
<td>77,975 ns</td>
<td>347,638 ns</td>
<td>11.2 ns</td>
</tr>
<tr>
<td>80% load</td>
<td>211,011 ns</td>
<td>778,070 ns</td>
<td>14.3 ns</td>
</tr>
</tbody>
</table>
802.11 Performance Anomaly
802.11 Performance Anomaly

### Performance anomaly

<table>
<thead>
<tr>
<th>nominal rate (Mb/s)</th>
<th>throughput (Mb/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 11</td>
<td>B 11</td>
</tr>
<tr>
<td>A 1</td>
<td>B 11</td>
</tr>
</tbody>
</table>

- LAN Access Point
- 802.11b: 11 Mb/s rate

1 Mb/s rate
One slow host, one fast

DCF - CSMA/CA
- equal access probability, not equal share
- same packet/s rate, not b/s

Throughput when \( R = 11 \text{ Mb/s}, r = 1 \text{ Mb/s} \)
- Fast: \( \frac{1}{11} / \left( \frac{1}{11} + 1 \right) \times 0.7 \times 11 \text{ Mb/s} = 0.64 \text{ Mb/s} \)
- Slow: \( \frac{1}{11} / \left( \frac{1}{11} + 1 \right) \times 0.7 \times 1 \text{ Mb/s} = 0.64 \text{ Mb/s} \)
Performance anomaly

\[ X_f = X_s = X = \frac{s}{T_f + T_s}, \]

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

- \( R, r \) – lower data rate, higher data rate
- \( s \) – frame size
- \( T_f, T_s \) – time on air, \( T_f = \frac{s}{R} + t_{ov}^R \)
- \( t_{ov} \) – 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

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

![Markov Chain model for the backoff window size.](image)

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

from which we get

\[
M = \frac{1 - p}{p \cdot \text{Total}_{\text{Idle},p}}.
\]  

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

---

538 IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 18, NO. 3, MARCH 2000
Optimal CW

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

CW proportional to \( N \)

\( \bar{n}_i \): average number of idle slots between transmission attempts

\( \bar{n}_i \) converges quickly

\( n_i \) target
Idle Sense

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

\[ \alpha = 1/1.2, \quad \epsilon = 0.01, \quad n_{\text{trans}} = 3, \quad \hat{n}_i^{\text{target}} = 5.7 \]
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:`

<table>
<thead>
<tr>
<th>Initial probabilities</th>
<th>Transition probabilities</th>
<th>Termination probabilities</th>
<th>Final probability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PayPal</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22:2</td>
<td>4.3% 20:,22:</td>
<td>99.93%</td>
<td>20:,22: 23.5%</td>
</tr>
<tr>
<td>22:11,22:14</td>
<td>99.93% 23:</td>
<td>100%</td>
<td>23: 61.6%</td>
</tr>
<tr>
<td>22:</td>
<td>100% 21:</td>
<td></td>
<td>21: 8.1%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>P1 = 70.7% * 94.4% * 99.6% * 99.5% * 10% * 8.1% = 0.54%</strong></td>
</tr>
</tbody>
</table>

| **Twitter**            |                          |                           |                   |
| 22:2                   | 42.7% 22:11,22:14        | 99.79%                    | 22:11,22:14 28%  |
| 22:20,22:             | 78.09% 20:,22:           | 96.1%                     | 20:,22: 96.1%    |
| 22:                     | 91.9% 23:                 | 40.3%                     | 23: 40.3%        |
|                         |                          |                           | **P2 = 42.7% * 97.9% * 70.9% * 91.9% * 58.6% * 91.8% = 14.7%** |
| 22:2,20:,22:          | 98.5%                    |                           |                   |
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**
  \[ A = \text{ripemd160(sha256}(K_p)) \]
- A is encoded with **base32** (20 characters) giving the DNS name
- 8 byte EUI64 identifier from A with
  \[ \text{DevEUI} = \text{SHA-3}(A) \]
- Several other domain names (aliases):
  - CNAME records
Examples - Semantic Description

- **W3C Thing Description** - complex, hierarchical attributes

  ```json
  "@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`.

- The 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

<table>
<thead>
<tr>
<th>Context</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
<td>5 bits</td>
</tr>
</tbody>
</table>

Encoded semantic properties
Examples - Semantic Description

- W3C Thing Description:
  
  ```json
  "@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>
<thead>
<tr>
<th>Context</th>
<th>geohash, geoprefix, or Plus Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 bits</td>
<td>59 bits</td>
</tr>
</tbody>
</table>

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

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

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

<table>
<thead>
<tr>
<th>geohash</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr5r7p4rx6kz</td>
<td>40.689167</td>
<td>-74.044444</td>
</tr>
<tr>
<td>dr5r7p4</td>
<td>40.69</td>
<td>-74.04</td>
</tr>
<tr>
<td>dr5r111</td>
<td>40.61</td>
<td>-74.13</td>
</tr>
</tbody>
</table>

- **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
- Decalogue/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?