Time-Awareness in the Internet of Things

NUIG, October 2014
Marc Weiss, NIST Consultant
mweiss@nist.gov  ++1-303-497-3261
Outline: Time-Aware Systems in the Internet of Things

• Motivation
  – Anticipated large growth
  – Timing and computing don’t mix!
  – What is Timing?

• Who is Developing Systems that Need Timing
  – Government science foundations
  – Industrial Internet
  – Cyber Physical Systems

• Time-Aware Systems – TAACCS group
  – Oscillators
  – Time transfer
  – Time in networks
  – Hardware/software support
  – Development Environments
  – Applications

• Timing Security
  – General issues
  – Jamming and Spoofing in GPS

• Conclusions
Main Points of this Talk

• Huge growth is expected in the Internet of Everything
• A few groups are addressing timing
• New Paradigms for timing will be needed to wed IT to OT: Time-Aware Systems
  – Example of “Correctness by Design”
  – Timing security leads to different requirements than cybersecurity
• One Area: Cyber-Physical Systems
  – Requirements on time intervals between events
  – Time network management
  – Timing security and resilience
• Timing Security: Protect Both **Signal Plus Data**
  – Jamming and Spoofing in GPS
  – Similar (yet different!) vulnerabilities in networks
Embracing the Internet of Everything
To Capture Your Share of $14.4 Trillion
More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience

Executive Summary
- The Internet of Everything (IoE) creates $14.4 trillion in Value at Stake — the combination of increased revenues and lower costs that is created or will migrate among companies and industries from 2013 to 2022.
- The five main factors that fuel IoE Value at Stake are: 1) asset utilization (reduced costs) of $2.5 trillion; 2) employee productivity (greater labor efficiencies) of $2.5 trillion; 3) supply chain and logistics (eliminating waste) of $2.7 trillion; 4) customer experience (addition of more customers) of $3.7 trillion; and 5) innovation (reducing time to market) of $3.0 trillion.
- Technology trends (including cloud and mobile computing, Big Data, increased...
A Broad Set of Applications

Enable New Knowledge

Predictive maintenance

Energy Saving (I2E)

Enhance Safety & Security

Defence

Industrial Automation

Intelligent Buildings

Transportation and Connected Vehicles

Agriculture

Healthcare

Smart Grid

Smart City

Smart Home

Source: Cisco (flavio@cisco.com)
Systems that Benefit from Precise Time

- Audio-visual transmission
- Time stamping of events
  - Correlation for analysis
  - Data aggregation
- Telecom systems
  - Multiplexing
  - Wireless access
- Optimal use of wireless spectrum
- Cyber-Physical Systems (CPS)
  - Local systems
  - Global systems
- Temporal determinism in software
  - Optimizes energy usage and resource allocation
  - Supports CPS timing (sensing to actuation)
  - Allows increased regulation in trades
- Location-based services
  - 1 ns = 1 foot
- Many, many more...
Time and Frequency Sources

- A clock is a frequency device based on physics

- Electronic systems count cycles for time interval

- Time is steered to UTC
Three Types of Sync

• Frequency
  – Match the rate only – syntonization
  – Usually inexpensive oscillator locked to a reference
  – Used e.g. for multiplexing

• Phase
  – Match epochs
  – Ensure simultaneity of control or logging

• Time
  – Same year-month-day, hour-minute-second
  – Refer to external time scale, e.g. UTC
  – Used e.g. for synchrophasors in electrical network
The Generation of UTC: Time Accuracy
Any Real Time UTC is only a Prediction
A PLL with a one-month delay

Accuracy: Laboratory Frequency Standards

Stability: Labs provide clock data

Labs collect data from labs, computes and outputs TAI and UTC

Labs Output UTC(lab) Based on Predictions of UTC
Time and Frequency Needs **Signals**!

• Signals are *Physical* with data
  – Accuracy and stability are no better than the physical layer
  – Data layers disrupt the T & F signals
  – Interference to the physical signal blocks access to T & F
  – Data modifies the signal, but does not require sync

• Communications systems are layered with devices only connected to the neighboring layers
  – Sync gets worse farther from the physical layer
Time Signal Plus Data

Time Distribution

Asynch time msg:
05:00:00.000000 10/31/2014 Z

Physical Time Marker

CPS Node

CPS Node knows it is
05:00:00.000000 10/31/2014 Z
Upon receipt of time marker
Two Issues Here

- Since a **clock is a frequency device**, the best clock exhibits only white noise on frequency, hence a random walk in phase. Even the best clocks will walk off unboundedly in time.

- Since the **time standard is artificial**, time MUST be transferred from the relevant time standard
  - There is often confusion with the human experience of time vs. metrological time. Standard time is a signal plus data
  - Often what is needed is synchronization among locations, not UTC per se, though that is often the most efficient way to achieve sync
The IoT Will Need Synchronization

• Since optimal data techniques obstruct synchronization

• Internet of Things requires New Paradigms for combining Time and Data
  – Need to be able to design time correctness independent of hardware
  – Need determinism and security in networks
One-Way Dissemination or Comparison System

Clock 1 Systematics and Noise

Delay, Perturbations, and Measurement Noise

Clock 2 Systematics and Noise

One-way Time Transfer requires determining and removing the Delay
One-Way Time Transfer: GPS

Problems at Receiver:
• Coordinates
• Multi-path interference
• Delays in cables
• Delay through receiver
• Receiver software
Clock Hierarchies

Clock 1

Clock 1 Systematics and Noise

Lock Loop Systematics and Noise: Contributions from Measurement Noise and Path Perturbations

Clock 2

Clock 2 Systematics and Noise
GNSS-aided Time and Frequency Systems: Lock Local Oscillator to GPS

- Quartz Crystal Oscillator
- Rubidium Vapor Atomic Oscillator

- GNSS Rcvr
- Compare
- Qz Osc.
- Output Freq.
- Rb Vapor Phy Pkg

- Or

- Rb oscillator 100 to 1000 times better Holdover Performance

Courtesy H. Fruehauf, ViaLogy LLC
Two-Way Comparison System

Two-way transfer depends on the Path being Reciprocal: $d_{21} = d_{12}$
Two-Way Time Transfer

• Via communications satellite

• In networks
  – NTP
  – PTP
We need a new network

Physical Networks

Timing Networks

Virtual Networks

Timing Network is both Physical and Virtual!
Outline: Time-Aware Systems in the Internet of Things

• Motivation
  – Anticipated large growth
  – Timing and computing don’t mix!
  – What is Timing?

• Who is Developing Systems that Need Timing
  – Government science foundations
  – Industrial Internet
  – Cyber Physical Systems

• Time-Aware Systems – TAACCS group
  – Oscillators
  – Time transfer
  – Time in networks
  – Hardware/software support
  – Development Environments
  – Applications

• Timing Security
  – General issues
  – Jamming and Spoofing in GPS

• Conclusions
New five-year, $4 million Frontier award aims to improve the coordination of time in networked physical systems

NSF announces five-year, $4 million award to tackle the challenge of time in cyber-physical systems.

Credit and Larger Version

June 13, 2014

The National Science Foundation (NSF) today announced a five-year, $4 million award to tackle the challenge of synchronizing time in cyber-physical systems (CPS)—systems that integrate sensing, computation, control and networking into physical objects and infrastructure.
The Industrial Internet Consortium (IIC)

• Mission: To accelerate growth of the Industrial Internet by coordinating ecosystem initiatives to connect and integrate objects with people, processes and data using common architectures, interoperability and open standards that lead to transformational business outcomes.
• Open membership, global, nonprofit
• Founded by AT&T, Cisco, GE, IBM and Intel
• Governed by the IIC Steering Committee
  – 10 members
    • 5 permanent seats by Founding companies; 2 members from large enterprise; 1 member from small enterprise; 1 from academia; 1 seat for Executive Director, ex officio
    • Any company can run for an open seat in its category
IIC Announcement – March 27, 2014

Announcement highlights

• 150+ articles to date
  – Business, technology and industry publications
  – Press release viewed over 24,000 times
• Hundreds of social media posts
  – Estimated audience of 3.6 million within first 24 hours
• 93% neutral-positive sentiment
Cyber Physical Systems

- **Business & User Goals**: Specific, measurable, action-oriented, realistic, and timely goals for lines of business and users to reach organizational mission objectives.

- **Data Analytics**: Develops and maintains dynamic, performance-based, computational models. These models use decisions on diagnosis and prognosis from the data analytics as input and determine whether business goals are met.

- **Monitor & Control System(s)**: Assimilates, filters, and processes data from different components for pattern recognition (normal or abnormal), predictive analytics and intelligent decision-making, and visual analytics for use by controller, users, where can the study and other environments.

- **Sensors & Actuators**: Control system(s), which may be distributed, acquire data from sensors, perform local processing, and control actuators to produce a prescribed state of the physical system in the physical environment.

- **Physical System**: Sensors acquire data from the physical system and transmit the information to storage, measurement and/or control devices. Actuators receive signals from a control device and act on the physical system. Sensors and actuators may be smart and/or distributed.

- **Physical Environment**: The engineered physical system that interacts with sensors and actuators and operates in the physical environment. The physical system is ideally co-designed along with the cyber-system to optimize the overall system. In some cases, the physical system is an existing legacy system into which cyber elements are added.

- **Interoperability**: Provides a means to securely transport data and information across the architecture layers. It may be composed of several sublayers.

- **Networking & Communications**: Resource for data storage, access, integration, cleansing and preprocessing, knowledge base/repository, data computation and service-based delivery, including time and synchronization services.

- **Human-System Interaction**: Interactions between humans (e.g., end user, operator, human-in-the-loop) and the CPS.

- **Security & Cybersecurity**: Applying physical security, cybersecurity, safety and resilience processes and protective measures to mitigate organizational risk to an acceptable level that allows the organization to perform its business and user goals (or critical functions).

- **Data & Data Services**: The capability of two or more networks, systems, devices, applications, or components to exchange and readily use information without the need for configuration or user intervention.
NIST CPS Public Working Group

Public Collaboration of Government, Academia, and Industry
NIST CPS Public Working Group

- The CPS PWG is composed of five initial sub-working groups, each with Government, Academic, and Industrial Co-Chairs
  - Vocabulary and Reference Architecture
  - Use Cases
  - Timing and Synchronization
    - Co-Chairs: Marc Weiss, NIST—Government, Hugh Melvin, NUIG—Academic, Sundeep Chandhoke, NI—Industrial
  - Cybersecurity and Privacy
  - Data Interoperability
Outline: Time-Aware Systems in the Internet of Things

• Motivation
  – Anticipated large growth
  – Timing and computing don’t mix!
  – What is Timing?

• Who is Developing Systems that Need Timing
  – Government science foundations
  – Industrial Internet
  – Cyber Physical Systems

• Time-Aware Systems – TAACCS group
  – Oscillators
  – Time transfer
  – Time in networks
  – Hardware/software support
  – Development Environments
  – Applications

• Timing Security
  – General issues
  – Jamming and Spoofing in GPS

• Conclusions
TAACCS Initiative

• A new initiative started with a face-to-face meeting in June 2014
• 50+ experts in timing focused on needed research
Critical Research Needs: New Paradigms

1. **Oscillators** in the network will require a range of performance and cost, as well as ensembling methods, that challenge the state-of-the-art.

2. **Time Transfer Systems** will need to deliver signals to orders of magnitude more endpoints than currently, with both specified accuracy and integrity, and by traversing both wired and wireless systems.

3. **Time Aware Networks** will need development in a number of areas:
   1. **Network equipment** hardware and software will need designs that support and utilize time awareness.
   2. Development of time aware and controlled networks requires research in both propagating and using timing signals.
   3. Time awareness is a critical factor in controlling latency in networks, which is crucial to tele-surgery, online gaming, the financial industry and other areas.
   4. Timing and analysis for performance monitoring is a challenge for maintenance.
   5. **Spectrum bandwidth utilization** can be optimized with precision timing.
Critical Research Needs: New Paradigms

4. **Timing support** for applications will need cross-discipline research in the following areas:

1. Hardware and software support of **predictable execution** will need to balance the depth of change in systems with cost and implementation.

2. Timing across **interfaces** will require standards and latency control both between CPU and in crossing network domains.

3. **Scale** issues in supplying time to large numbers of systems.

5. **Development environments** will need the ability to specify timing accuracy independent of the hardware that systems are running on.

6. **Applications** can make innovative use of time, and will further stimulate the development of these other items.
An example of a system with critical timing requirements - The “Flying Paster”

(next 2 slides from “Using Ptides and Synchronized Clocks to Design Distributed Systems with Deterministic System-wide Timing”, Derler et al., ISPCS 2013-Lemgo)

1. When feed roll B is nearly empty
2. Reserve roll A is brought to matching surface velocity
3. The position of the tape is observed and angles are calculated
4. When B is at a critical radius and the tape is at the “contact” angle, E forces the two feeds together
5. A short time later D cuts the B feed leaving A as the primary feed

This slide due to John Eidson
Embedded systems—especially distributed systems. Designers should be able to design, simulate, and code generate for multiple targets with guaranteed timing!
Comments on the Flying Paster example

The Ptides implementation shown demonstrates:

• Physical time vs. Model time with correspondence enforced only at key points, e.g. sensors and actuators

• Same design compiled to two different platforms => identical timing to within clock resolution (8ns)

The “You Tube” video no doubt used a time-triggered architecture where a strict: sense, compute, actuate cycle is enforced with hardware supported sense and actuation timing.

This slide due to John Eidson
Cyber Physical Systems Node and Environment, Currently

- No semantics of accurate time neither in design, nor languages
- Possibly bounded TIs
- Almost never stable (deterministic)
- Hence robust, correct by construction solutions cannot be done here!

- Precise TIs
- Can be accurate (traceable to SI second or TAI)
- Hence robust, correct by construction is possible (but not very flexible)

This slide based ones by John Eidson
Cyber Physical Systems Node and Environment with Correct by Construction

- Time can be specified as abstraction in model
- Code is Bounded and Time explicit
- I/O is Time sensitive, explicit, and precise
- CPU clock is precise and if needed accurate
- Hence robust, correct by construction solutions can be done here!

- Precise TIs
- Can be accurate (traceable to SI second or TAI)
- Hence robust, correct by construction is possible (but not very flexible)

This slide based ones by John Eidson
Outline: Time-Aware Systems in the Internet of Things

• Motivation
  – Anticipated large growth
  – Timing and computing don’t mix!
  – What is Timing?
• Who is Developing Systems that Need Timing
  – Government science foundations
  – Industrial Internet
  – Cyber Physical Systems
• Time-Aware Systems – TAACCS group
  – Oscillators
  – Time transfer
  – Time in networks
  – Hardware/software support
  – Development Environments
  – Applications
• Timing Security
  – General issues
  – Jamming and Spoofing in GPS
• Conclusions
CPS Security and Resilience

• Since timing is both signal and data
  – Security of data is like cybersecurity
  – Security of timing signal is new

• Resilience generally means redundancy

• Time accuracy, UTC, generally comes from GNSS, which is vulnerable to interference
  – We focus on jamming and spoofing in GPS
  – Similar (yet Different!) vulnerabilities appear in networks
Spectra of GNSS’s

Slide 41
GNSS Vulnerability

• GNSS best feature and worst problem: it is extremely reliable

• Jamming Power Required at GPS Antenna
  – On order of a Picowatt (10^-12 watt)

• Many Jammer Models Exist
  – Watt to MWatt Output – Worldwide Militaries
  – Lower Power (<100 watts); “Hams” Can Make
Jamming Events Each Hour, Feb – Oct 2013: London Financial District

Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project
GNSS Spoofing

Slide courtesy of Kyle D. Wesson, The University of Texas at Austin
Civil GPS Spoofing Threat Continuum*

Simplistic
- Commercial signal simulator

Intermediate
- Portable software radio

Sophisticated
- Coordinated attack by multiple phase-locked spoofers

* Courtesy of Coherent Navigation, Inc
Conclusions

• Huge growth expected in the IoT will require new paradigms for timing
• Many different groups are working on timing
• New timing paradigms
  – Time Awareness is key
  – Correct-by-design is necessary to support large growth and change
  – Designs for control in CPS
  – Timing Security requires securing both the signal and data
And that’s all

- Thank you for your interest
Extra Slides
Collaborative Research Needed:

• Industry-Government-Academia
  – Broad range of goals
  – Different priorities and resources

• Communications Systems need Sync research
  – NIST group has expertise in time transfer issues
  – NIST WSTS has a basis for collaboration with industry
Time in networks: CPS Schedule Generation and Distribution

Centralized Network Controller computes topology for network

CNM determines bandwidth requirements for each stream

CNM provides bandwidth and stream linkage information to Centralized Network Controller

Centralized Network Controller computes path for stream and gathers performance metrics based on path selected
- Propagation Delay
- Bridge Delay

Centralized Network Controller provides path information and metrics to CNM to compute schedule

Centralized Network Controller provides bridge schedules to Centralized Network Controller for distribution

Centralized Network Controller calculates the Schedule

Centralized Network Controller provides End-Station transmission schedule to CNM

Centralized Network Controller distributes Schedule to Bridges

Stream Configuration Failed

Schedule Distribution Successful?

Yes

CNM distributes Transmission Schedule to CPS Nodes

Schedule Distribution Successful?

Yes

Stream Configuration Successful

No

Schedule Distribution Successful?

No

Schedule Distribution Successful?

Yes

Stream Configuration Successful

(Source: Sundeep Chandhoke, National Instruments)
Time in networks: Time-Aware CPS Device Model

- **Time Stamp Unit (e.g. IEEE 802.1AS/1588)**
- **Converged Data Management**
- **Best Effort Applications** (HTML, Web Services, etc.)
- **Time Based Application**
- **Time-Sensitive Stream data mapping**

**Layers:**
- **Application Layer**
- **Data Link Layer**
- **Physical Layer**

**Protocols:**
- Timing and Sync Protocols (802.1AS, etc.)
- HTTP, etc.
- TCP/UDP
- IP

**Components:**
- **Rx/Tx**
- **MAC**
- **TSU** (Time Stamp Unit)
- **PHY** (Physical Layer)

**Data Flow:**
- Time Stamping
- I/O Functions
- Best Effort Applications (HTML, Web Services, etc.)
- Time Based Application
- Time-Sensitive Stream data mapping

**Network Functions:**
- **I/O Functions**
- **Converged Data Management**
- **Time Stamping**
- **Rx/Tx**
- **HTTP, etc.**
- **TCP/UDP**
- **IP**

**Network Protocols:**
- Physical Layer
- Data Link Layer
- Application Layer

**Network Devices:**
- NIC/Bridge

**Network Applications:**
- Time-Sensitive Stream
- Best Effort Applications
- Time Based Application
Jamming Events Day of Week, Feb – Oct 2013: London Financial District

Data and image courtesy of Charles Curry, Chronos Technology Ltd and the SENTINEL Research Project
Disruption Mechanisms - Spoofing/Meaconing

- Spoof – Counterfeit GNSS Signal
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- Meaconing – Delay & Rebroadcast
- Possible Effects
  - Long Range Jamming
  - Injection of Misleading PVT Information
- No “Off-the-Shelf” Mitigation
Conclusions

• GNSS provide all three types of sync: Time and Frequency and Phase

• GNSS accuracy meets PRTC and PRC specs

• GNSS are growing internationally

• GNSS are Vulnerable, best feature and worst problem: extremely reliable
## Secure Timing

<table>
<thead>
<tr>
<th>Source channel assurance</th>
<th>Opportunities to verify that the timing information is coming from a legitimate source. Verification may include unpredictable bits of a digital signature, or a symmetrically encrypted channel.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source data assurance</strong></td>
<td>Verification mechanisms to prove timing data are not forged. These may include digital signatures or symmetrically encrypted packets.</td>
</tr>
<tr>
<td><strong>User provided assurance</strong></td>
<td>User implemented security to verify unassured timing information. This may include anti-spoof GNSS receiver techniques or additional layers of network security.</td>
</tr>
<tr>
<td><strong>Predictable failure</strong></td>
<td>Known CPS failure modes that account for timing denial and detected timing spoofing.</td>
</tr>
<tr>
<td><strong>Diversity &amp; Redundancy</strong></td>
<td>Multiple sources and paths of secure time are available to a CPS. Where possible, sources are verified against each other, and in the event of a denial or spoofing attack on one source, a mechanism to switch to a redundant source is available.</td>
</tr>
</tbody>
</table>
## Resilience in Timing: Multiple Timing Sources

<table>
<thead>
<tr>
<th>Source Channel</th>
<th>Order of Timing</th>
<th>Source Channel Assurance Provided Today</th>
<th>Source Data Assurance Provided Today</th>
<th>Source Channel Assurance Possible via Enhancement</th>
<th>Source Data Assurance Possible via Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>GPS L1 C/A</td>
<td>nanoseconds</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>GPS L2C/L5</td>
<td>nanoseconds</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Galileo</td>
<td>nanoseconds</td>
<td>No</td>
<td>No</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>PTP</td>
<td>nanoseconds</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NTP</td>
<td>milliseconds</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Low Frequency Signals (eLORAN, WWVB, DCF77, ...)</td>
<td>nanoseconds</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Galileo is not yet a fully operational GNSS constellation, but has indicated strong support for source channel and data assurance.
### Principal attack vectors in an unsecured time network

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Attack Characteristics</th>
<th>Impact</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Manipulation</td>
<td>Modification (Man in the Middle (MitM))</td>
<td>False time</td>
<td>In-flight manipulation of time protocol packets</td>
</tr>
<tr>
<td>Replay Attack</td>
<td>Insertion / Modification (MitM or injector)</td>
<td>False time</td>
<td>Insertion of previously recorded time protocol packets</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Insertion (MitM or injector)</td>
<td>False time</td>
<td>Impersonation of legitimate master or clock</td>
</tr>
<tr>
<td>Rogue Master (or Byzantine Master) Attack</td>
<td>Insertion (MitM or injector)</td>
<td>False time</td>
<td>Rogue master manipulates the master clock election process using malicious control packets, i.e. manipulates the best master clock algorithm</td>
</tr>
<tr>
<td>Interception and Removal</td>
<td>Interruption (MitM)</td>
<td>Reduced accuracy, depending on precision of local clock</td>
<td>Time control packets are selectively filtered by attacker</td>
</tr>
<tr>
<td>Packet Delay Manipulation</td>
<td>Modification (in widest sense) (MitM)</td>
<td>Reduced accuracy, depending on precision of local clock</td>
<td>Intermediate: transparent clock relays packets with non-deterministic delay</td>
</tr>
<tr>
<td>Flooding-based general DoS or Time Protocol DoS</td>
<td>Insertion (MitM or injector)</td>
<td></td>
<td>Rogue node floods 802.15.4 network with packets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rogue node overwhelms single victim with time protocol packets</td>
</tr>
<tr>
<td>Interruption-based general DoS or Time Protocol DoS</td>
<td>Interruption (MitM or possibly injector)</td>
<td></td>
<td>Rogue node jams network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Rogue node jams selectively certain time protocol packets</td>
</tr>
<tr>
<td>Master Time Source Attack</td>
<td>Interruption (MitM or injector)</td>
<td>Reduced accuracy</td>
<td>GPS jamming</td>
</tr>
<tr>
<td>Cryptographic Performance Attack</td>
<td>Insertion (MitM or injector)</td>
<td>Limited or no availability of target</td>
<td>GPS spoofing</td>
</tr>
</tbody>
</table>