Intrinsic adversary detection in Cyber-physical systems:

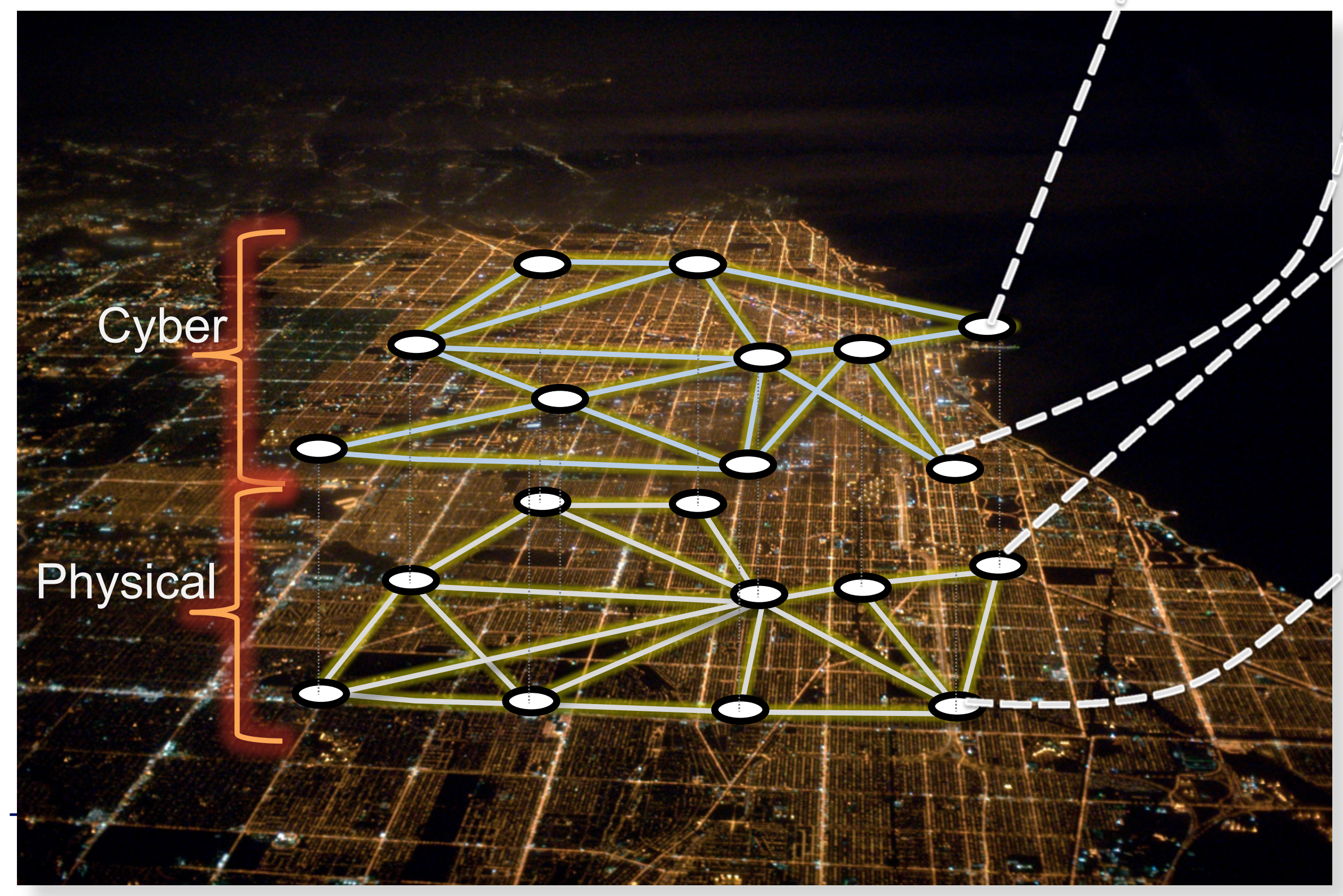
Precise network synchronized clocks enable detection and isolation of adversarial attacks.

Dhananjay Anand NIST | ITL | SSD

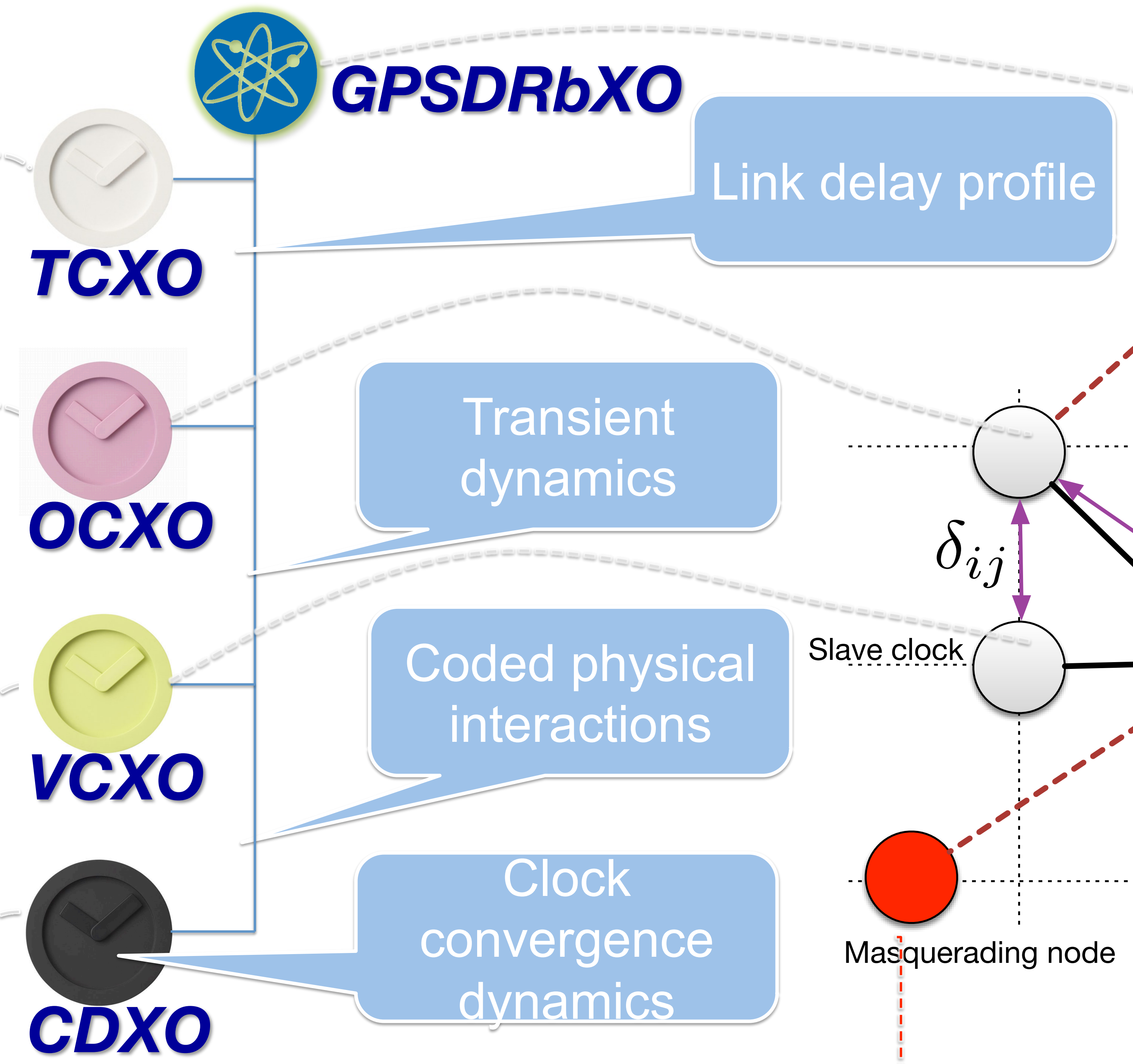
Main Idea

Networks of the future are purportedly more vulnerable given their eventual evolution to large, amorphous, cyber-physical systems (CPSs).
The focus of our research is to leverage a precisely synchronized network of clocks embedded within a CPS to design implicit security features, identify network intrusion, adversarial proxies and unauthorized reconfiguration.

Our premise is that while network topology, data content and size may change unpredictably in a CPS, the use of precise clocks to profile the physics of individual nodes and to accurately model the relative timing differences between nodes offers a unique structure-semantic oracle for node authentication and link validation.



A Cy-phy network of clocks



Link delay profile

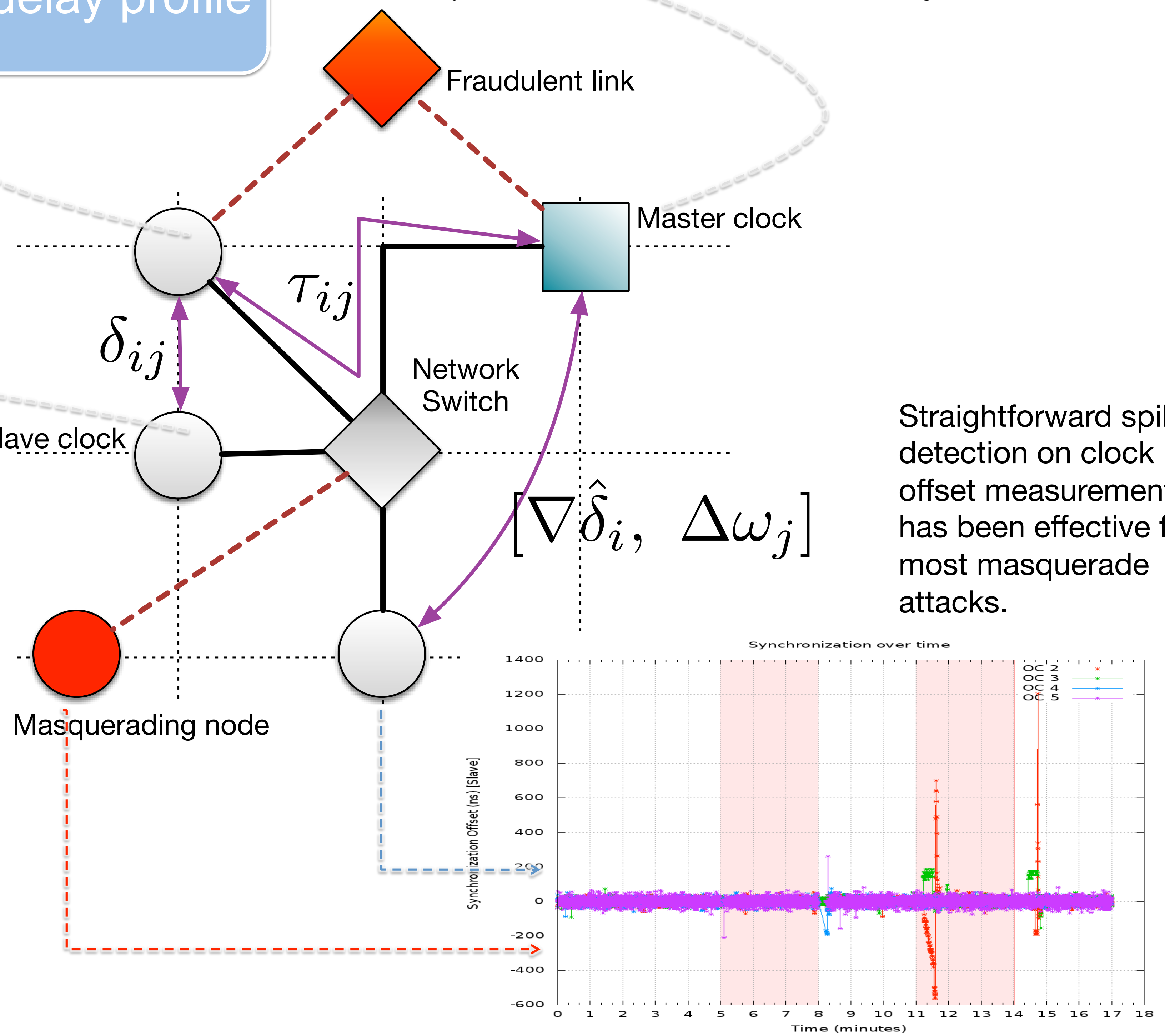
Transient dynamics

Coded physical interactions

Clock convergence dynamics

Chronometric fingerprinting

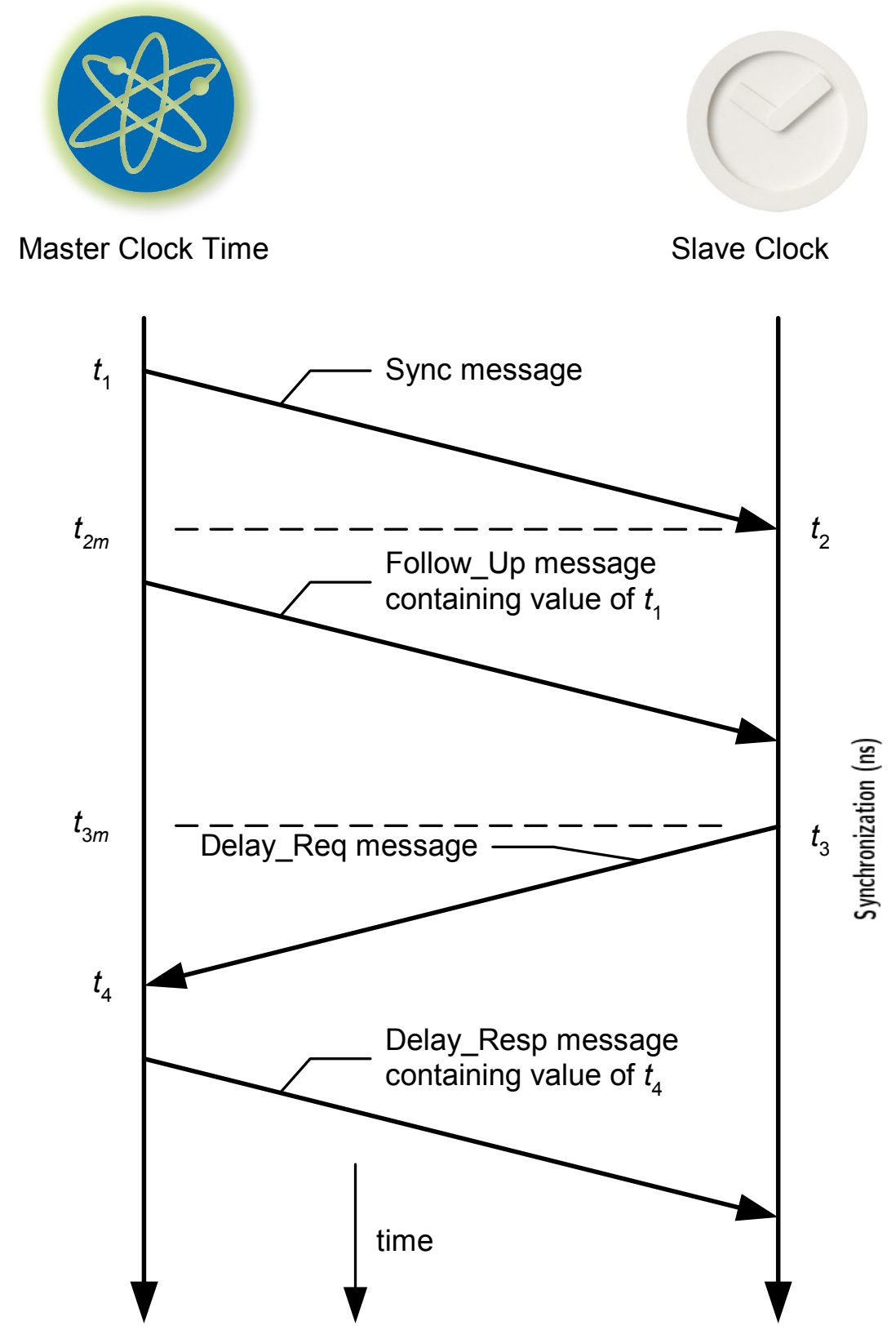
When a reference feature set is available, Bayes classifiers, the K-means algorithm or a neural network may be used to identify anomalous time signatures.
“Hidden change point” unsupervised anomaly detection, using the Shiryaev-Roberts statistic, is also being considered



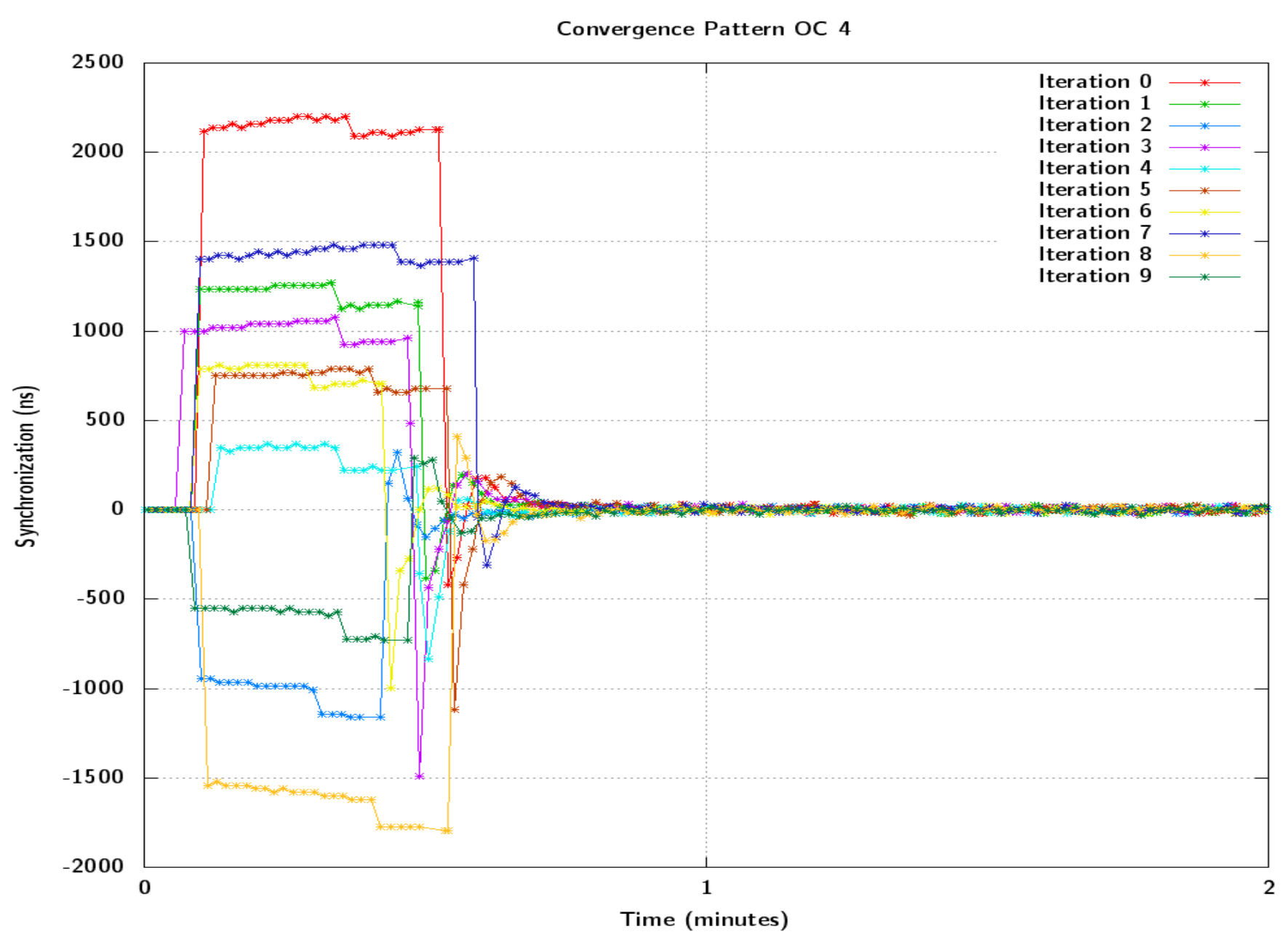
Straightforward spike detection on clock offset measurements has been effective for most masquerade attacks.

Clock synchronization

Clocks on devices connected over an Ethernet link may be synchronized very precisely using the IEEE 1588 Precision Time Protocol.
The protocol uses a temporally coded packet exchange to compensate for network delay and to compute clock offset to a reference Master clock.



Sub-microsecond accuracy is achievable across typical local area networks.



Discrete clock offset correction:

$$\delta_{ij} = \frac{1}{2}(t_2 - t_1 - t_3 + t_4)$$

Dynamic Syntonization:

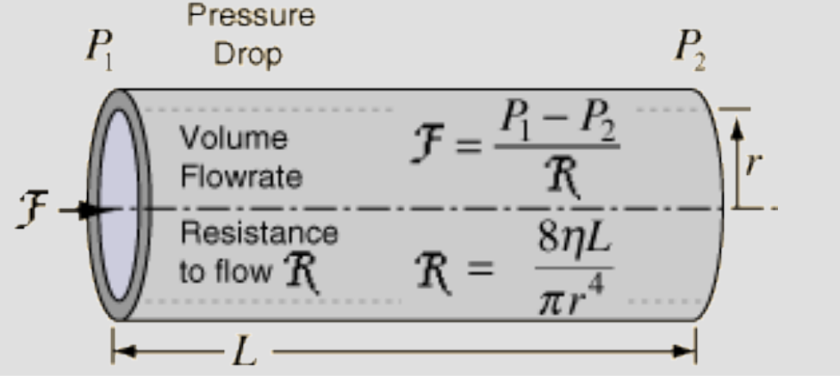
$$\omega(t)_j = \underbrace{\alpha_{ij}\Delta\omega(t)_j}_{\text{Bias}} + \underbrace{\gamma_j \cdot t}_{\text{Drift}} + \underbrace{\psi_j \cdot t^2/2 + \phi(t)}_{\text{Dilution}}$$

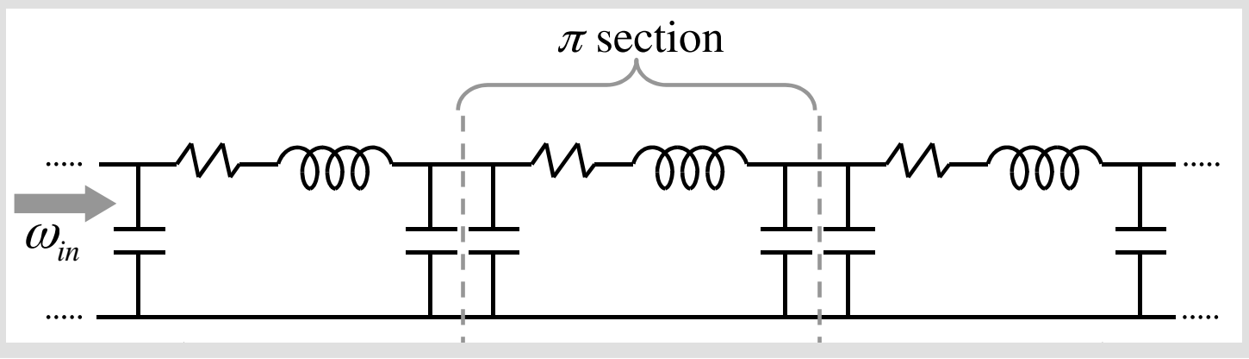
Link characteristics

Physical

Physical networks used to distribute electricity or natural gas tend to be particularly vulnerable to attack given the high asset value, pervasive presence and wide geographic footprint.

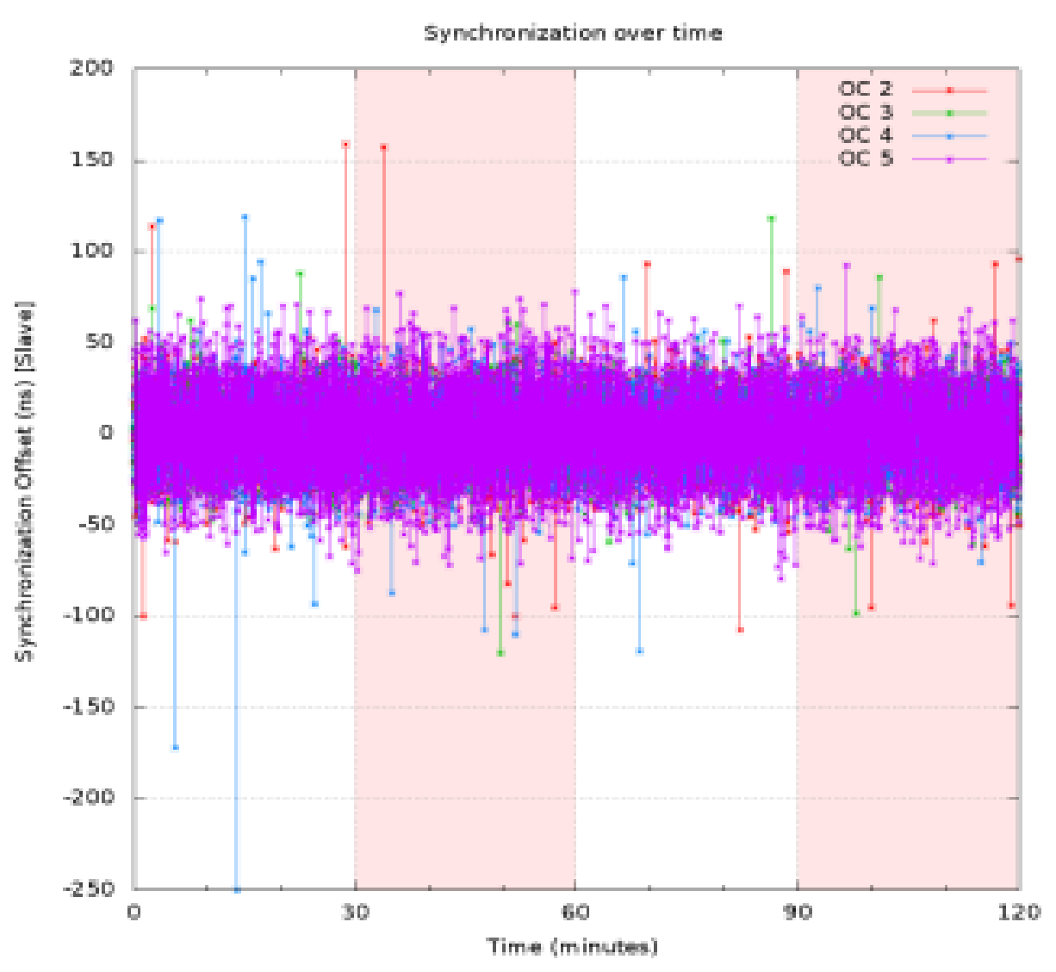
However, the physical dynamics associated with a system comprised of interconnected pipes or cables also provides us a method to characterize the topology of the physical network.

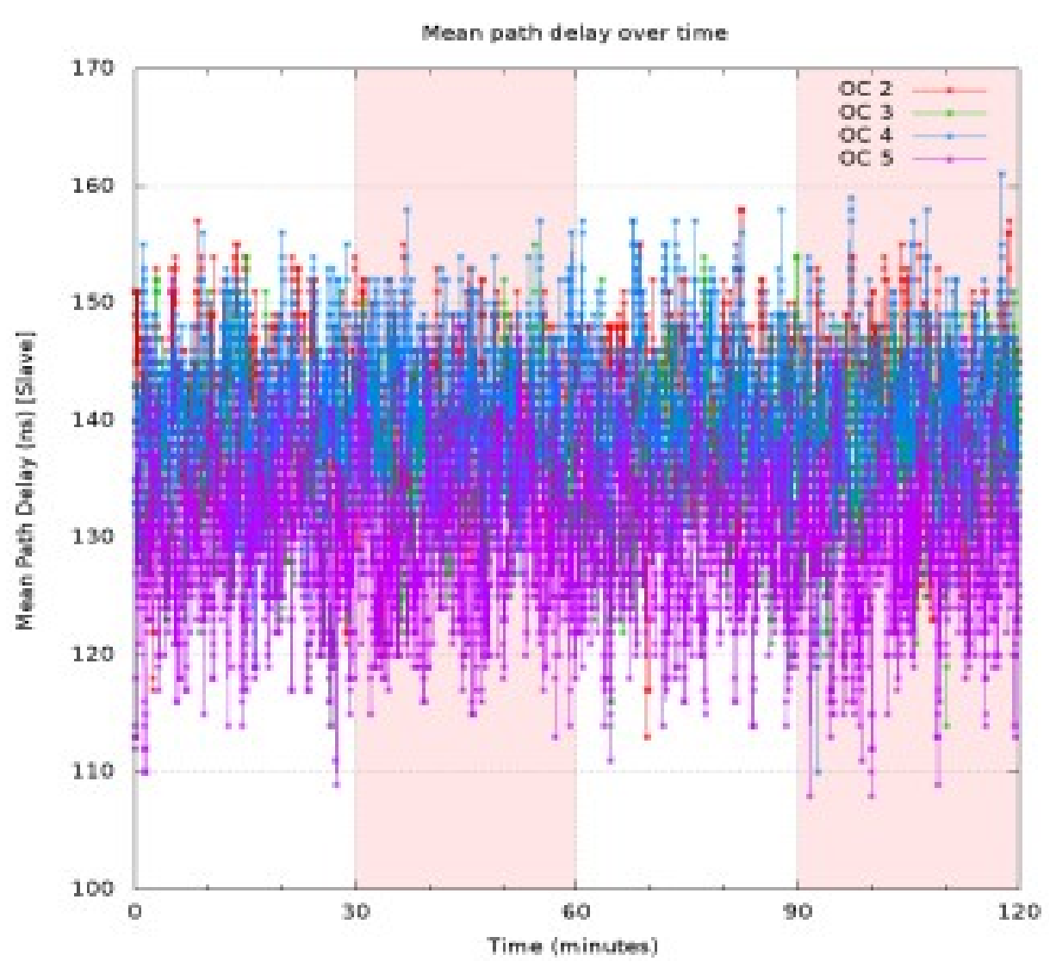

P_1
Pressure Drop
P_2
Volume Flowrate
$\mathcal{F} = \frac{P_1 - P_2}{\mathcal{R}}$
$\mathcal{F}$
Resistance to flow $\mathcal{R}$
$\mathcal{R} = \frac{8\eta L}{\pi r^4}$
r
L



Cyber

Cyber links may be characterized as information channels subject to classical information theory /security assessments.
In our study we consider that links in the cyber domain pertain packetized digital networks (i.e., Ethernet) subject to packet delay and jitter.
We are able to characterize the network based on packet propagation delay and peer clock offsets.





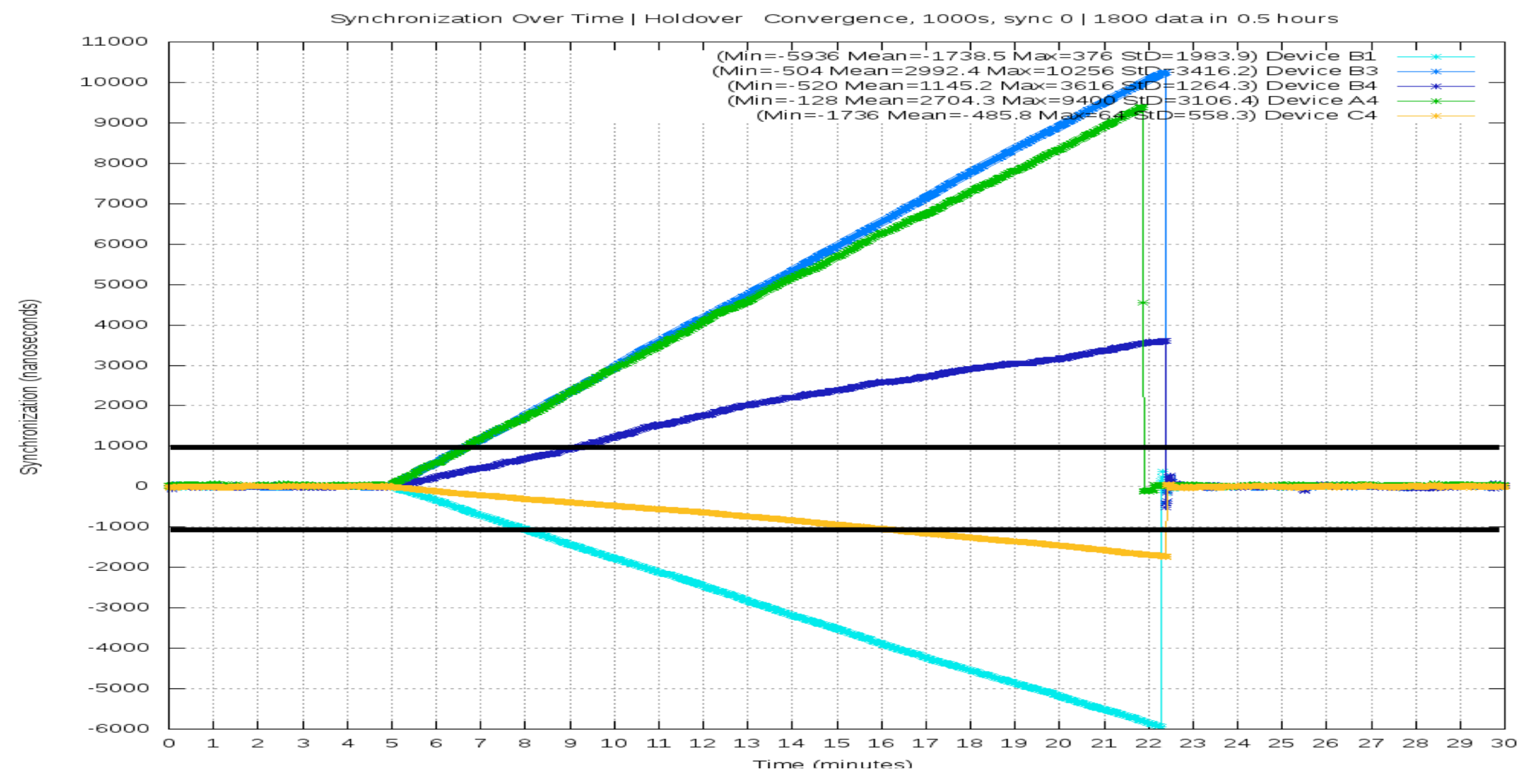
Node characteristics

Nodes in a power network may include generators, loads, transformers, etc. Gas networks utilize pumps, pressure reducers and manifolds, etc.

Accurate clocks within physical sensors improve the quality and rate of sampled observations of physical nodes. The improvement in data quality has a direct impact on anomaly detection and currently is the primary driver for improved clock accuracy.

Assuming that each node (physical and cyber) uses a precise clock, the dynamics associated with clock convergence (e.g., PLL transients) provide a powerful oracle to assess node fidelity.

Clock drift characteristics are unique to the crystal resonator being used and show significant pattern differentiation between manufacturing runs.



NIST National Institute of Standards and Technology • U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY