# GPS Vulnerabilities and Implications for Telecom

**Moderator**

**Dr. James Armstrong**

*Chief Technology Officer, Symmetricom*

**Panelists**

**Todd Humphreys**

*Assistant Professor,*

*University of Texas at Austin*

**Martin Nuss, Ph.D.**

*Vice President, Technology and*

*Strategy and CTO,*

*Vitesse Semiconductor*

# About the Speakers

## Moderator:

**Dr. James Armstrong**
*Chief Technology Officer*
*Symmetricom*

## Panelists:

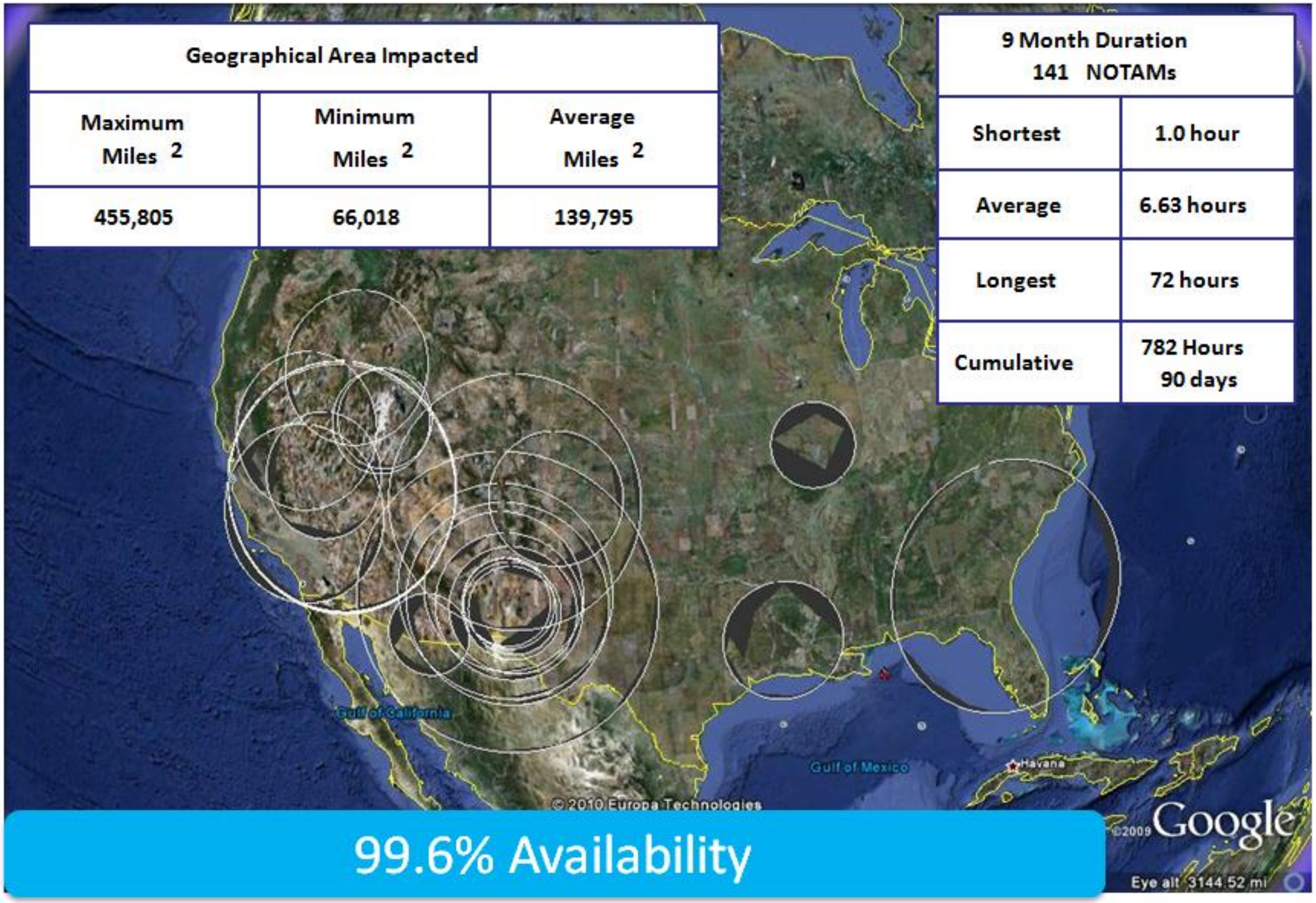
**Todd Humphreys**
*Assistant Professor*
*Aerospace Engineering and Engineering Mechanics*
*University of Texas at Austin*

**Martin Nuss, Ph.D.**
*Vice President,*
*Technology and Strategy and Chief Technology Officer*
*Vitesse Semiconductor*

# GNSS


Communications
Emergency Services
Power Utility
Defense Industrial Base
Government Facilities
GNSS
Information Technology
Water Treatment
Transportation Systems
Healthcare & Public Health
Commercial Facilities

# GNSS Challenges: GPS Tested by DOD



| Geographical Area Impacted | | |
|---|---|---|
| Maximum Miles 2 | Minimum Miles 2 | Average Miles 2 |
| 455,805 | 66,018 | 139,795 |

| 9 Month Duration<br>141 NOTAMs | |
|---|---|
| Shortest | 1.0 hour |
| Average | 6.63 hours |
| Longest | 72 hours |
| Cumulative | 782 Hours<br>90 days |

99.6% Availability

# Everyday Localized GNSS Outages

GPS jammers and spoofing

Mechanical / antenna failures

Environmental / lightning storms

# Frequency and Phase Specifications

| Application | Frequency: Physical / Air Interface | Phase |
|---|---|---|
| UMTS/LTE FDD Residential Small Cell | NA / 250 ppb | NA |
| UMTS Metro Small Cell | NA / 100 ppb | NA |
| GSM / UMTS / W-CDMA | 16 ppb / 50 ppb | NA |
| CDMA2000 | | ± 3 to 10 µs |
| TD-SCDMA | | ± 1.5 µs |
| LTE -FDD | | NA |
| LTE-TDD | | ± 1.5 µs |
| LTE-A MBSFN | | ± 1 µs |
| LTE-A CoMP (Network MIMO) * | | ± 0.5 to ± 1.5 µs |
| HetNet Coordination (eICIC) | | ± 5 µs |

*Multiple proposals under consideration

# LTE Synchronization

| Application | Frequency / Air Interfaces | Time /Phase | Why You Need to Comply | Impact of Non-compliance |
|---|---|---|---|---|
| LTE (FDD) | 16 / 50 ppb | N/A | Call Initiation | Call Interference<br>Dropped calls |
| LTE (TDD) | 16 / 50 ppb | +/- 1.5 µs | Time slot alignment | Packet loss/collisions<br>Spectral efficiency |
| LTE MBSFN | 16 / 50 ppb | +/- 32 µs | Proper time alignment of video signal decoding from multiple BTSs | Video broadcast interruption |
| LTE-A MIMO/COMP | 16 / 50 ppb | +/- 500 ns | Coordination of signals to/from multiple base stations | Poor signal quality at edge of cells, LBS accuracy |

# Timing Technology Options

| | |
|---|---|
| Satellite based | GNSS |
| Network based | IEEE 1588 (Frequency and phase)<br>Synchronous Ethernet (SyncE) |
| Holdover Protection | Rubidium |

**Resilient Networks Needs 2 Out of 3**

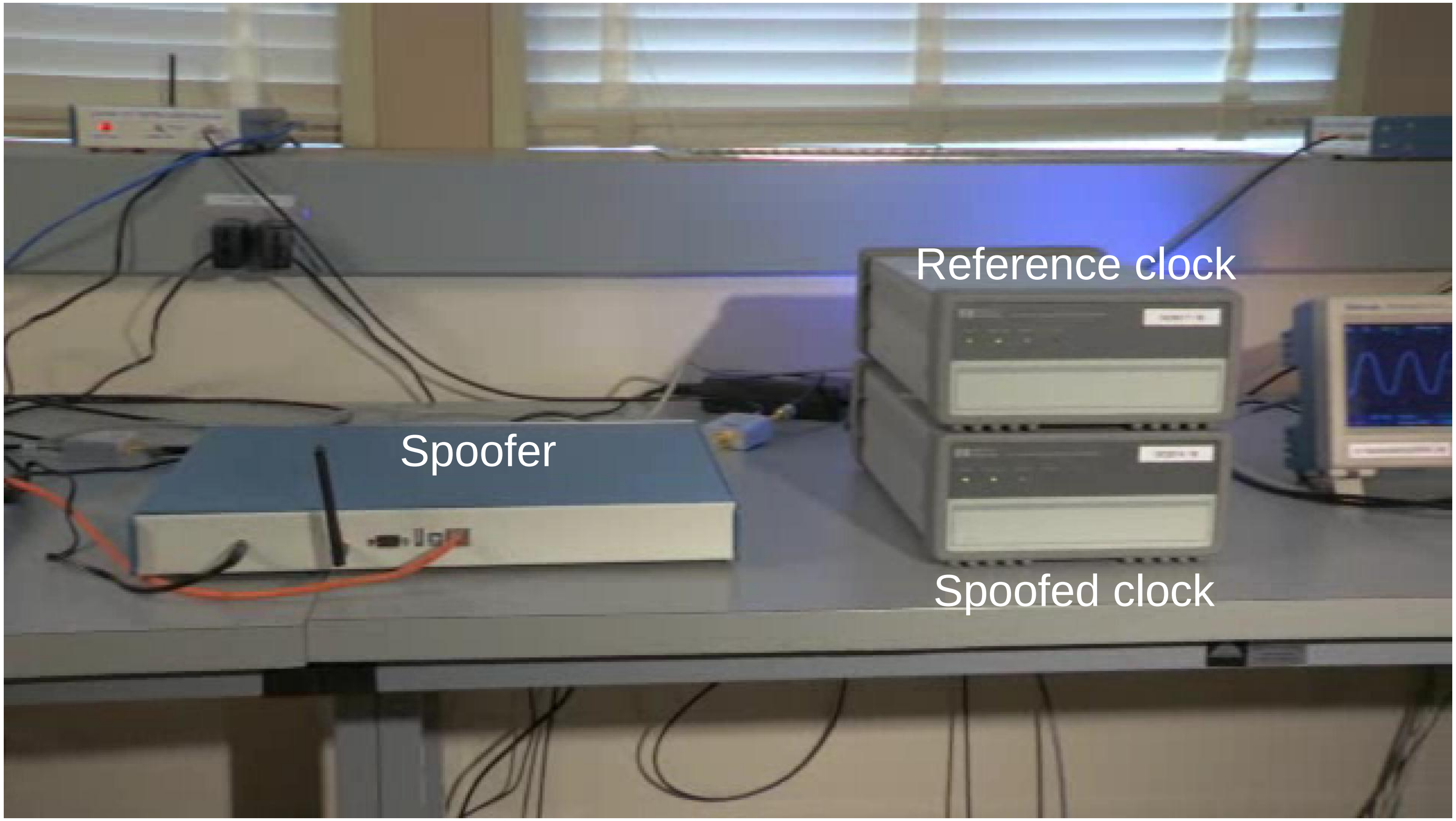
# Secure Time

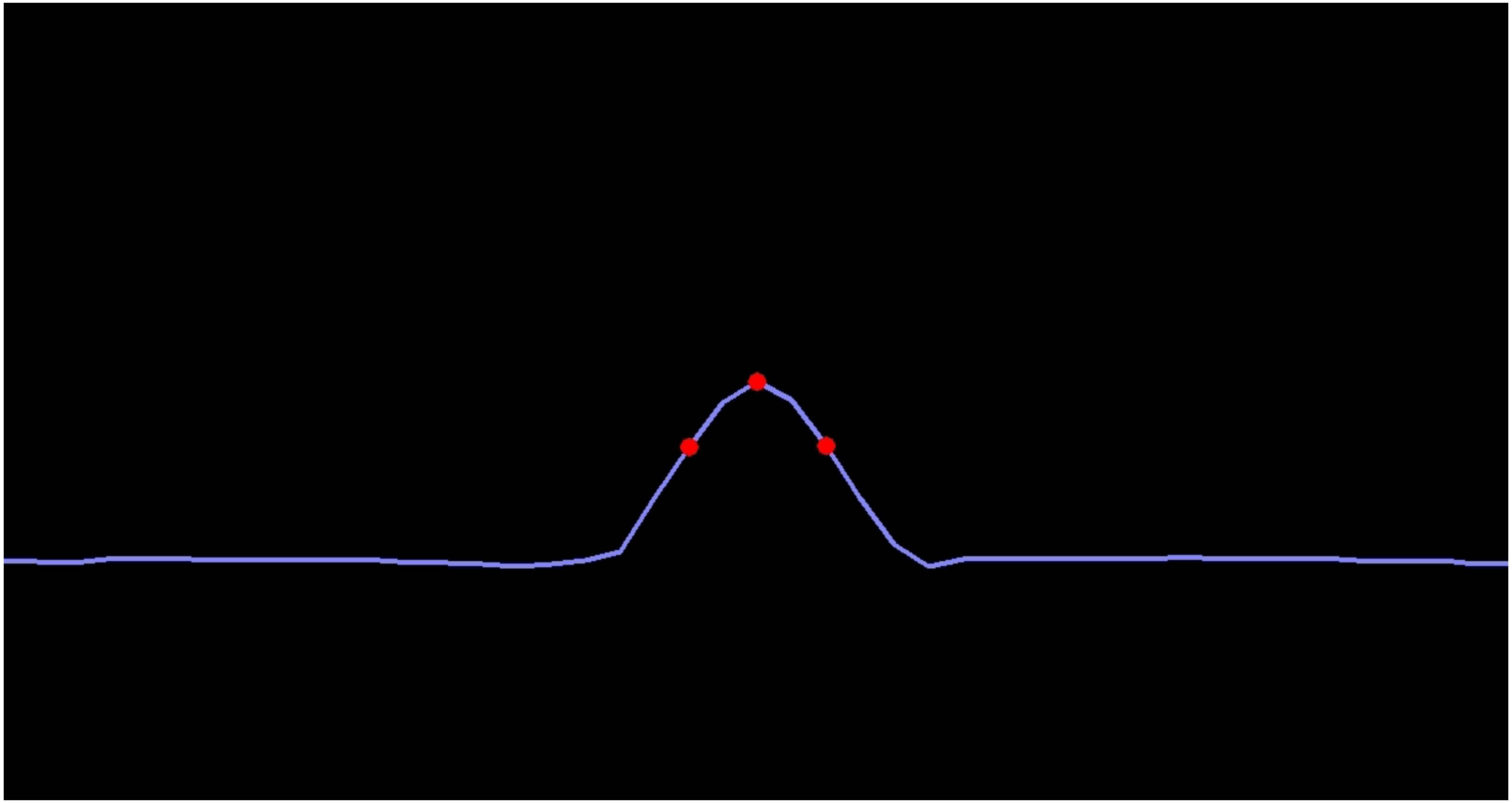
**Todd Humphreys**
*Assistant Professor*
*University of Texas at Austin*

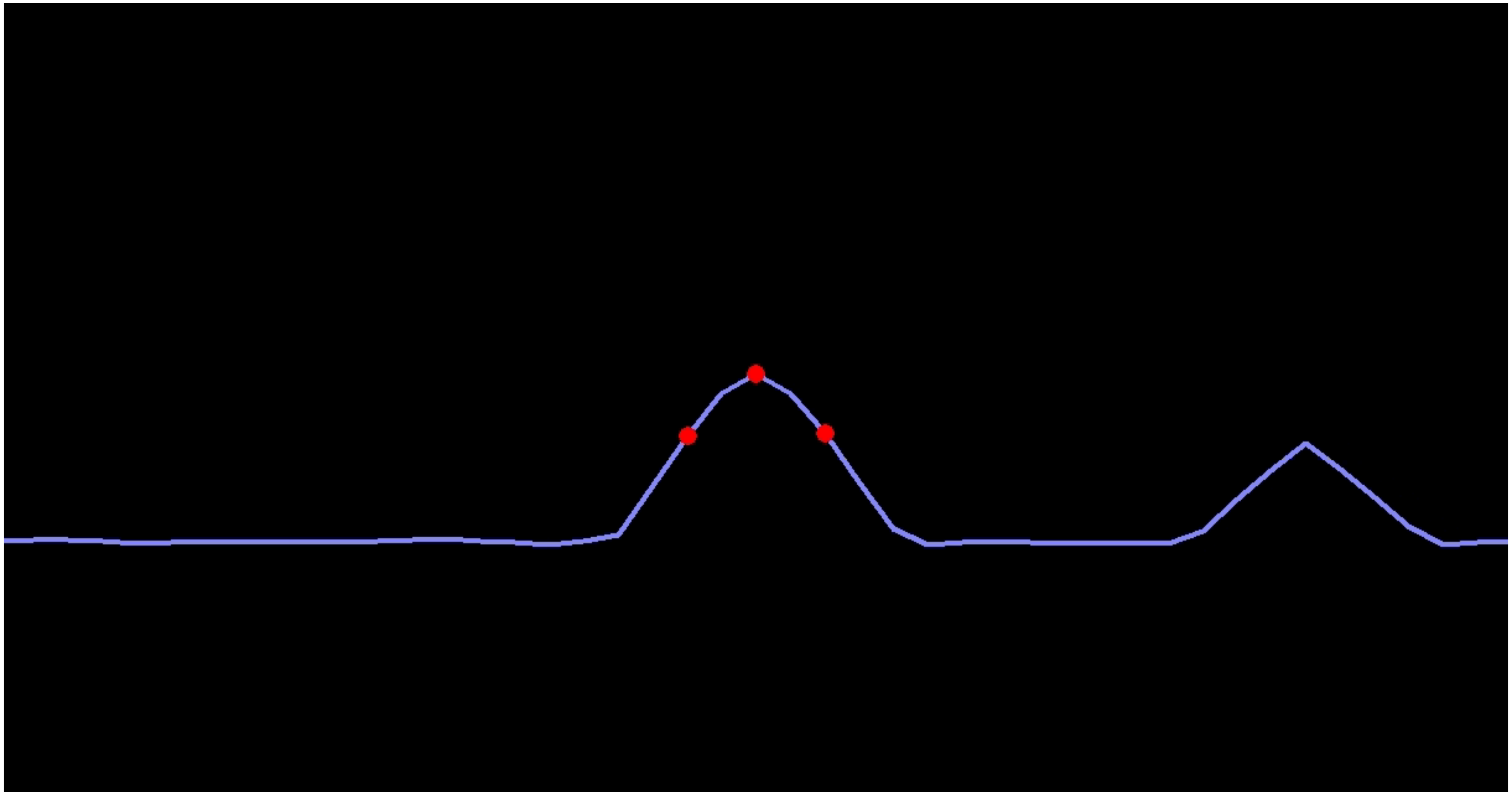
# Outline

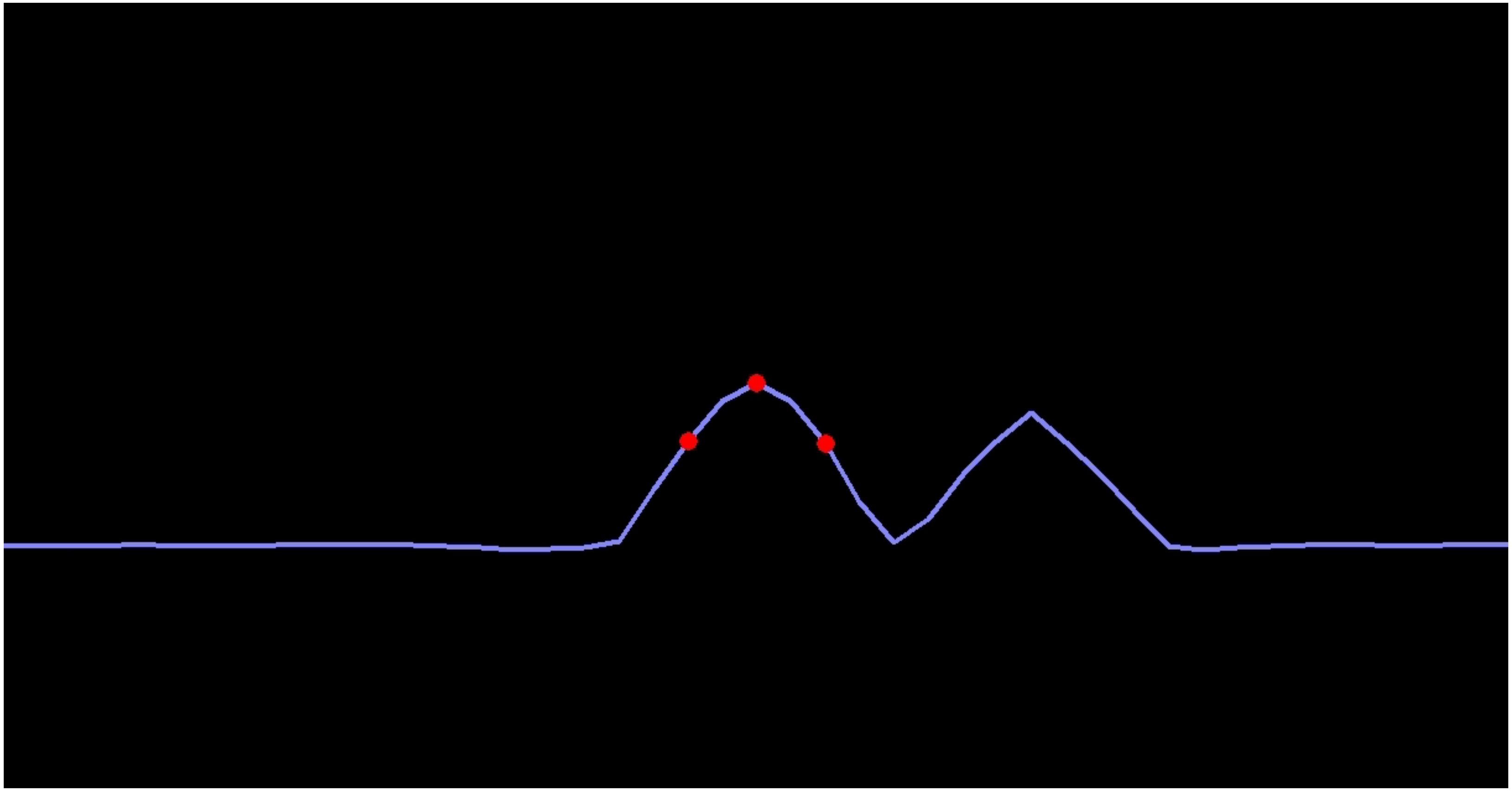
- Inside a GPS spoofing attack
- Example effects of time manipulation on communications, finance, and energy sectors
- Misconceptions about timing security
- Options for secure ns-accurate timing

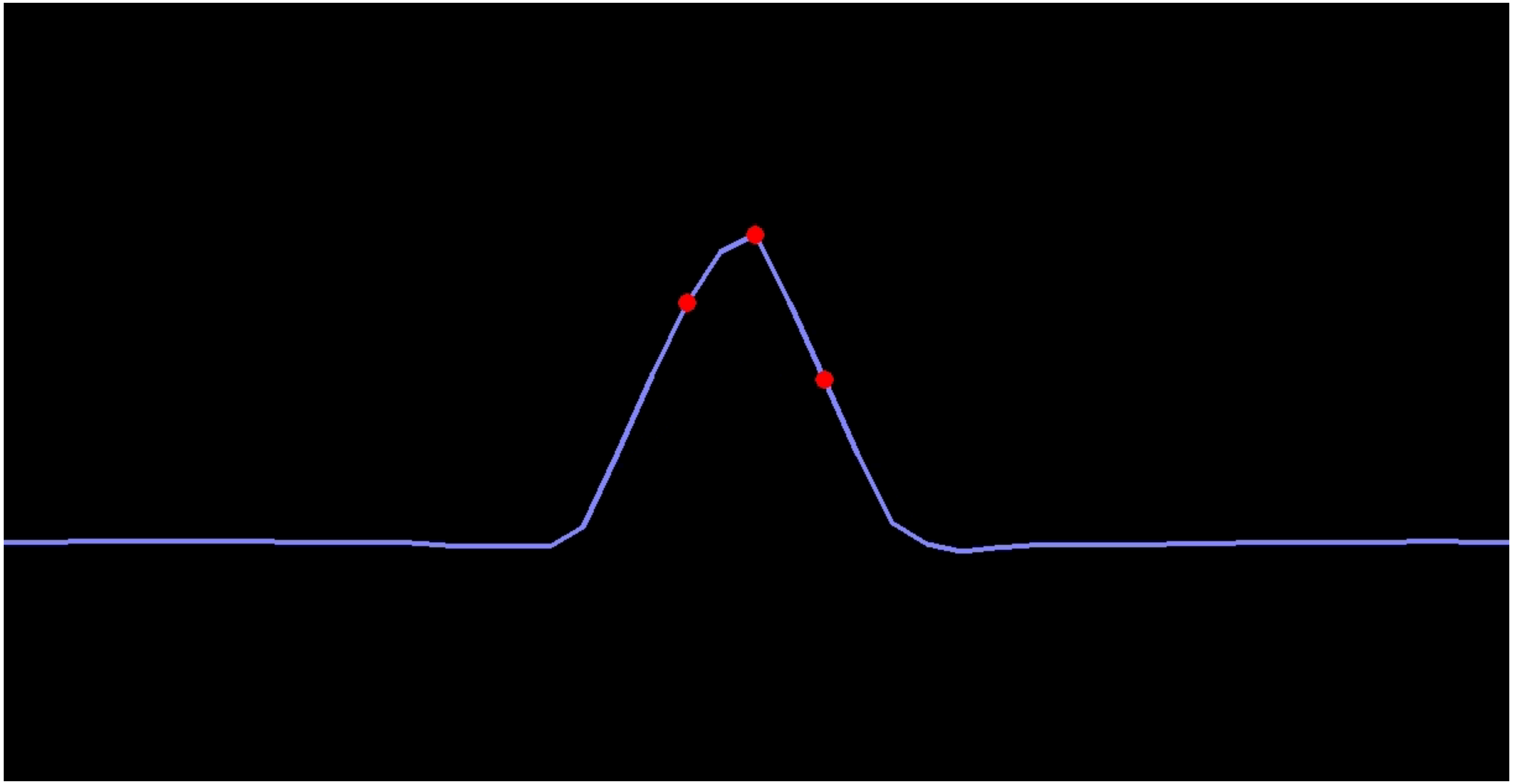
# Example Attack

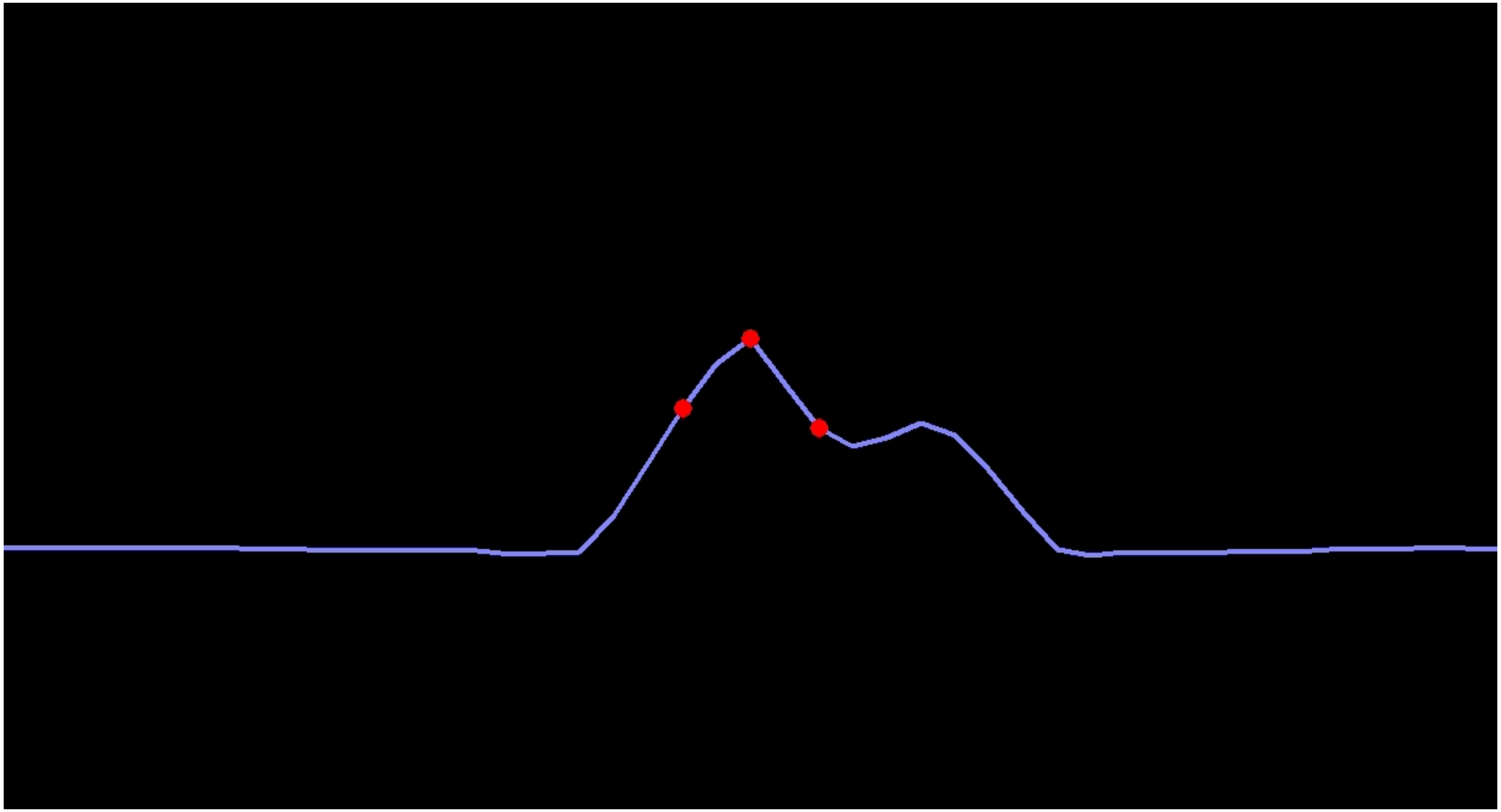


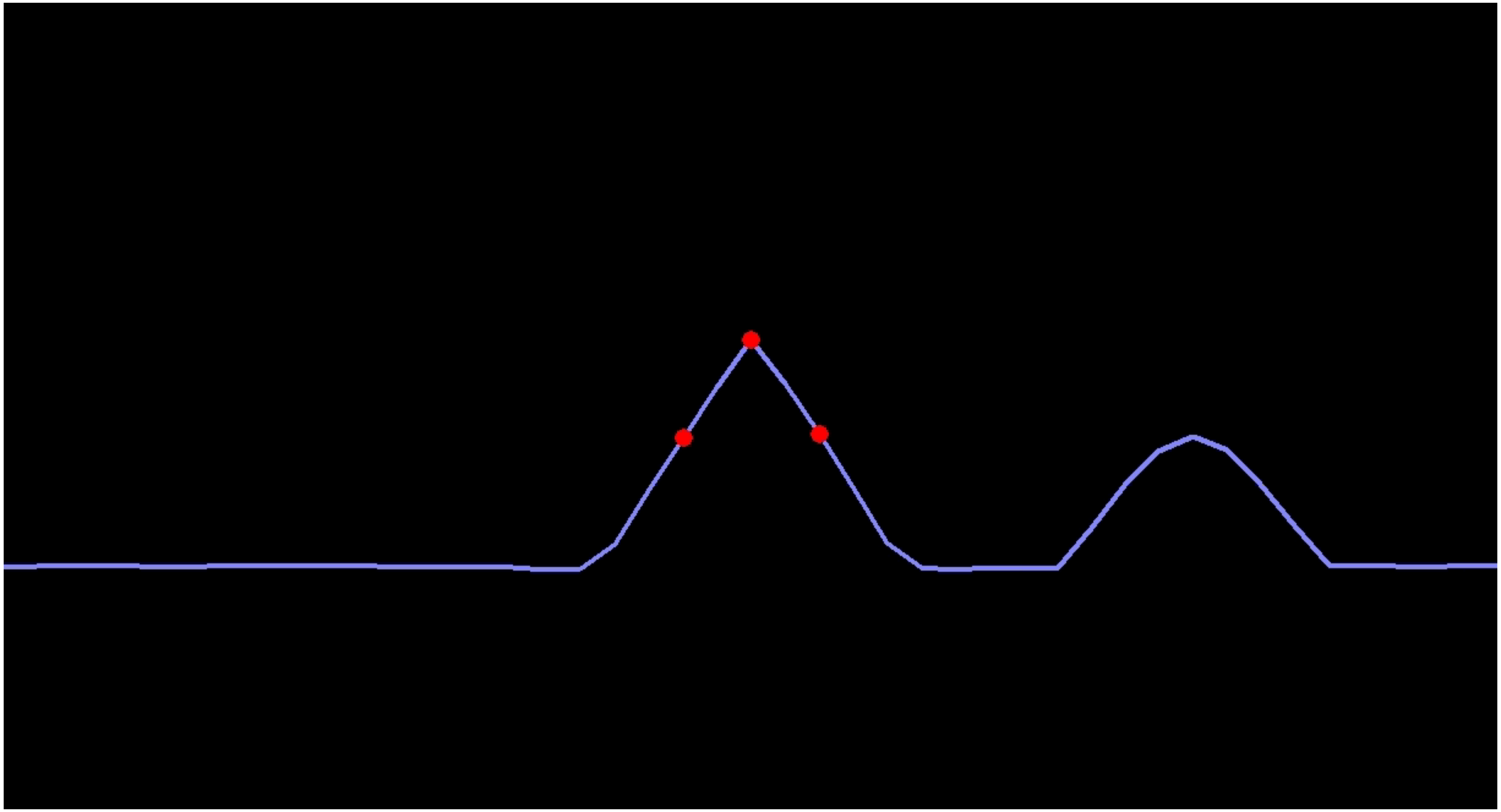












# Spoofer’s Effect on PPS Phase

Reference

Spoofed

# Example Effects: CDMA Cellular Systems

- CDMA 2000 standard requires towers to be synchronized to within 10 us of GPS time
- Synchronization has many benefits: soft handoff, more efficient acquisition, better power efficiency in handset
- Towers all use same spreading code; they distinguish themselves by the phase of this code in 52-us increments
- A spoofer could induce a 10-us error in a tower in less than 30 mins; thereafter, handoff to nearby towers would become unreliable
- Worse yet, a coordinated spoofing attack could bring multiple towers into spreading code phase alignment: Handsets near cell edges may not be able to connect calls

# Example Effects: Smart Energy Distribution

- Phasor Measurement Units (PMUs) are a key enabling technology for the next-generation power grid
- PMUs require synchronization to better than 26 us
- All PMUs rely on GPS for synchronization
- Latest PMUs have been built with control in mind:  can be configured to take immediate control action (e.g., trip a generator) if PMU data indicate a fault condition
- A spoofing attack against a PMU can simulate a fault condition

D.P. Shepard, T.E. Humphreys, A.A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks Evaluation of the Vulnerabilityof Phasor Measurement Units to GPS Spoofing Attacks," International Journal of Critical Infrastructure Protection, Vol. 5, December, 2012.

# Example Effects: Smart Order Routing

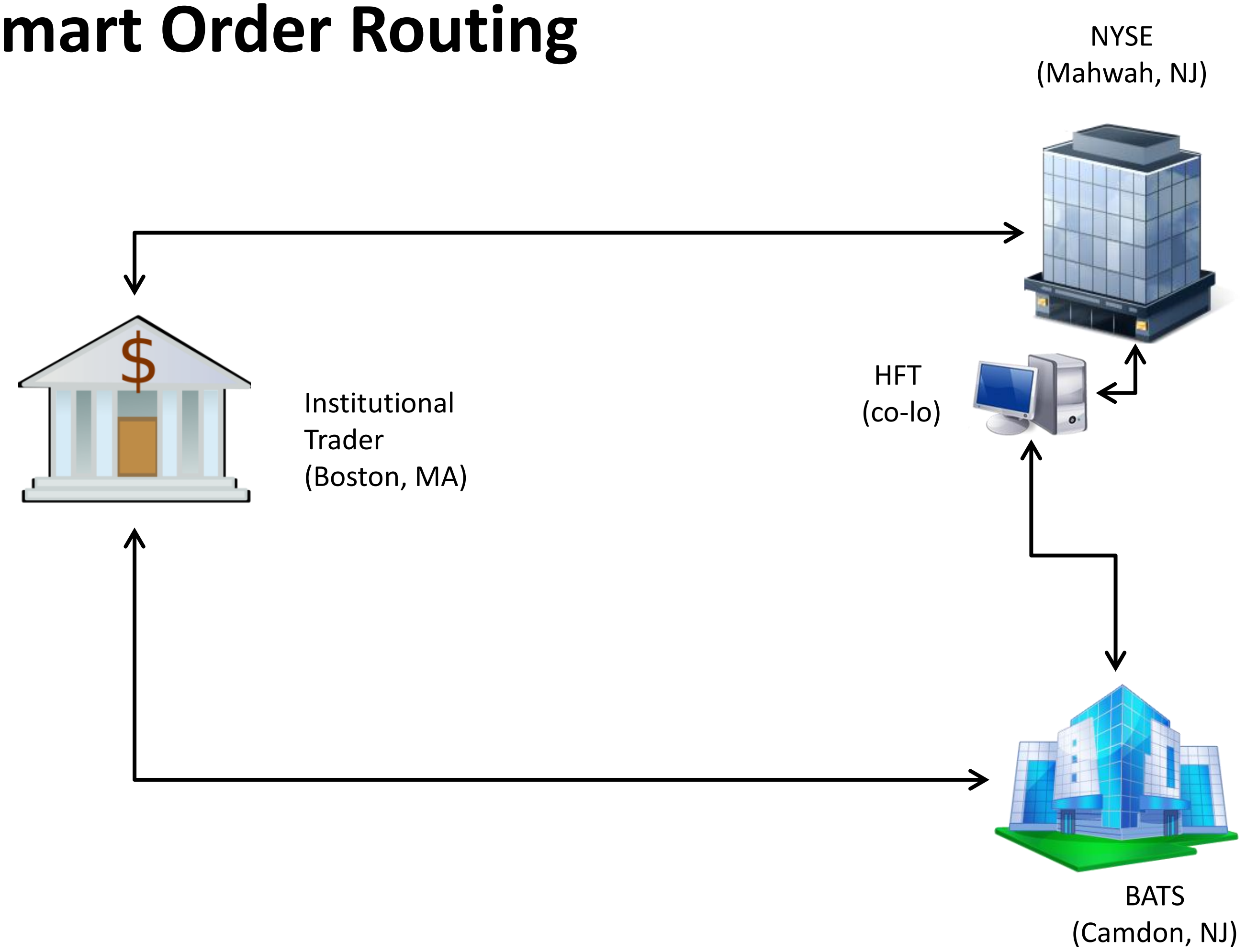
**Background:** Post-2007 "REG NMS" regulations have fragmented US markets, forcing large investors to "vacuum up" liquidity from multiple trading venues

**Problem**: Liquidity vanishes as high-frequency traders (HFTs) sense the presence of a large institutional trader (IT) (a "whale") in one venue and then alter orders in other venues before the IT can complete its orders there.

**Whales Strike Back:** In response to the HFT's (entirely legal) game of bait-and-switch, ITs have developed a powerful weapon: smart order routing (SOR).

**SOR's Timing Component:** SORs continuously monitor round-trip times to various exchanges (and possibly monitor time stamps). They then break up large orders and launch them so that they arrive at multiple exchanges *simultaneously.*

# Smart Order Routing

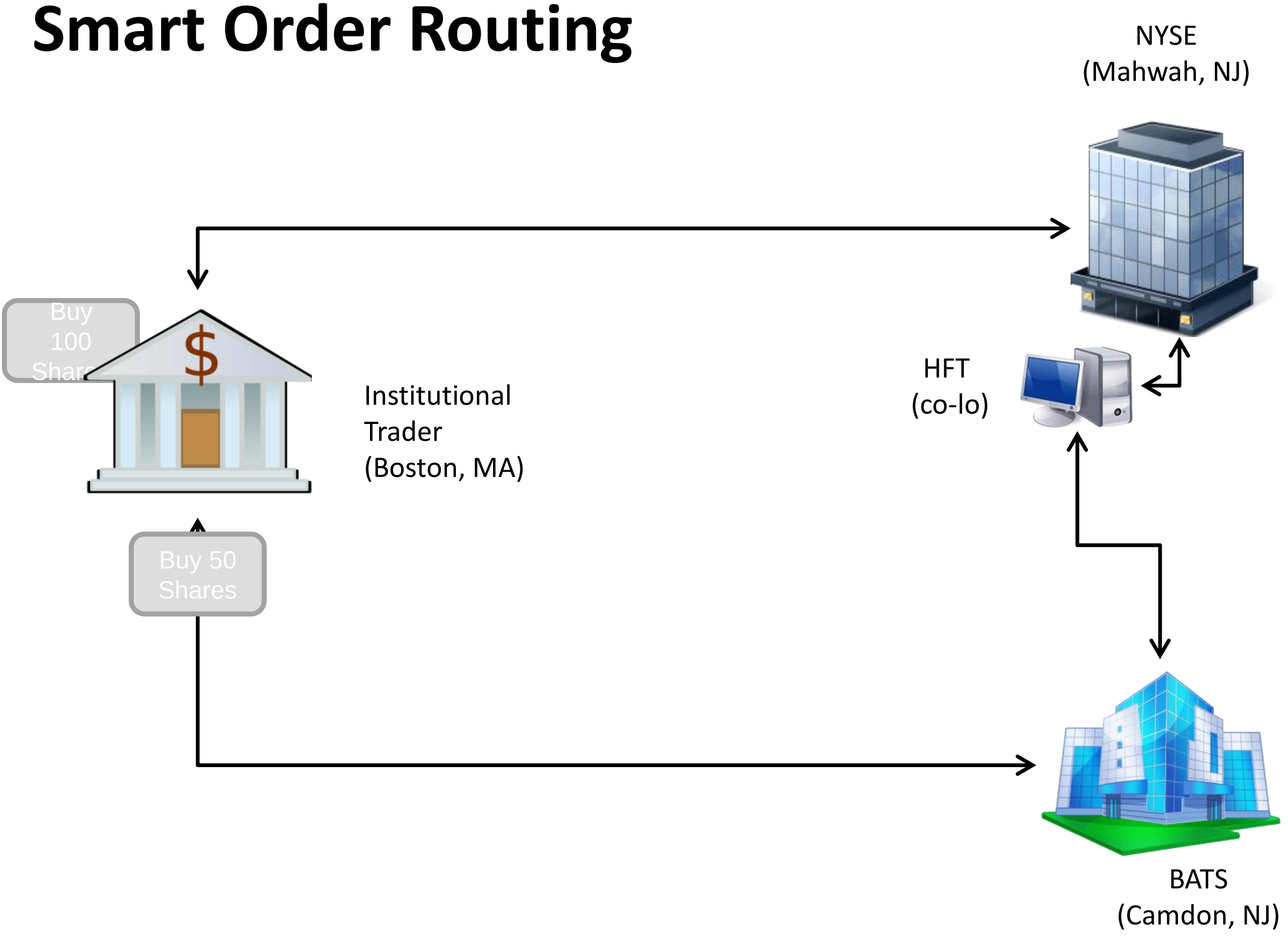


| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 100 | $55 |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | 50 | $55 |
| | | 175 | $57 |

Suppose, due to geometrical distance and networking delays, the route to NYSE is 2 ms shorter than route to BATS

# Smart Order Routing

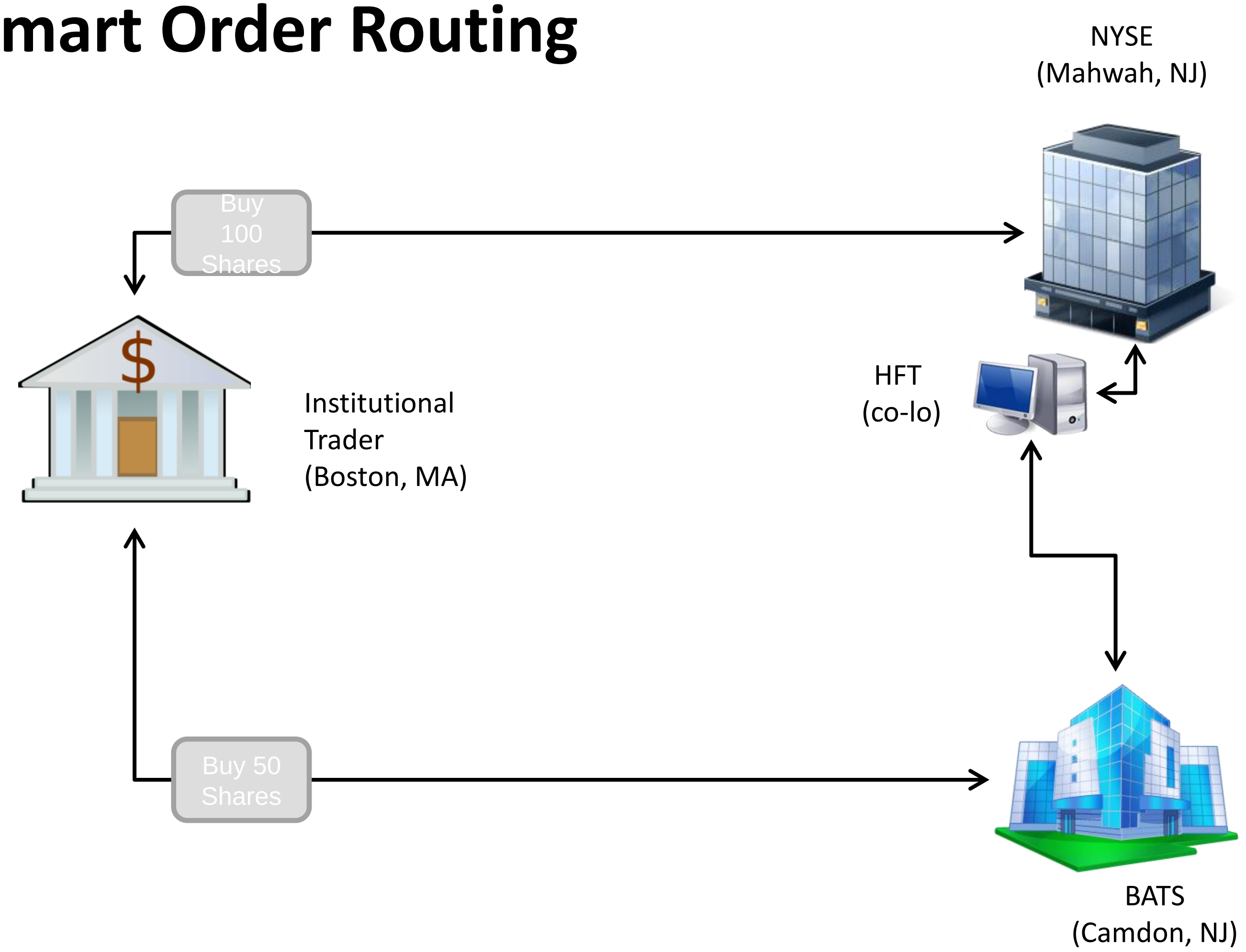


| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | **100** | **$55** |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$55** |
| | | 175 | $57 |

SOR delays NYSE order by 2 ms so that both orders arrive simultaneously

# Smart Order Routing



NYSE
(Mahwah, NJ)

Buy 100 Shares

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

Buy 50 Shares

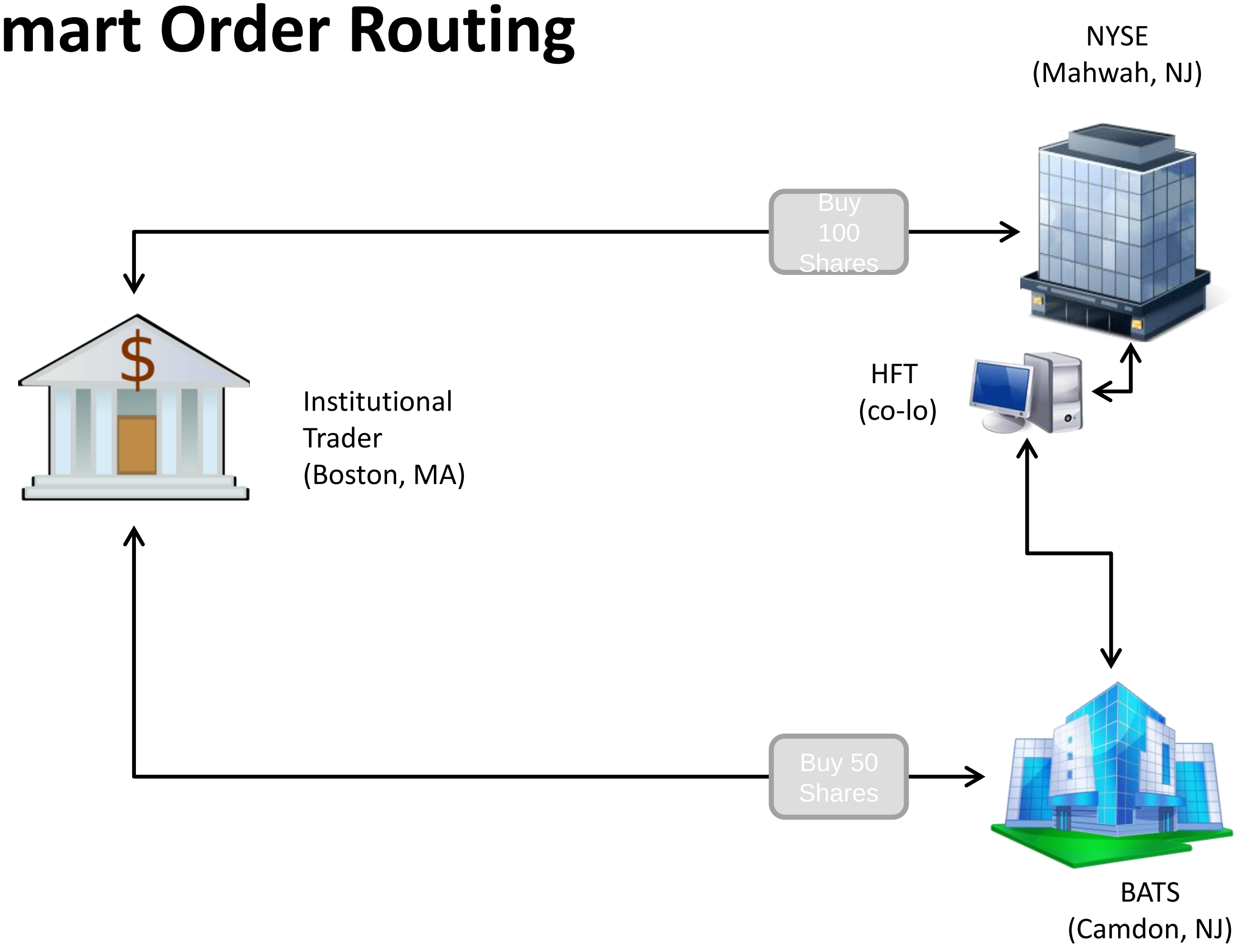
BATS
(Camdon, NJ)

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | **100** | **$55** |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$55** |
| | | 175 | $57 |

SOR delays NYSE order by 2 ms so that both orders arrive simultaneously

# Smart Order Routing



NYSE
(Mahwah, NJ)

Buy 100 Shares

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

Buy 50 Shares

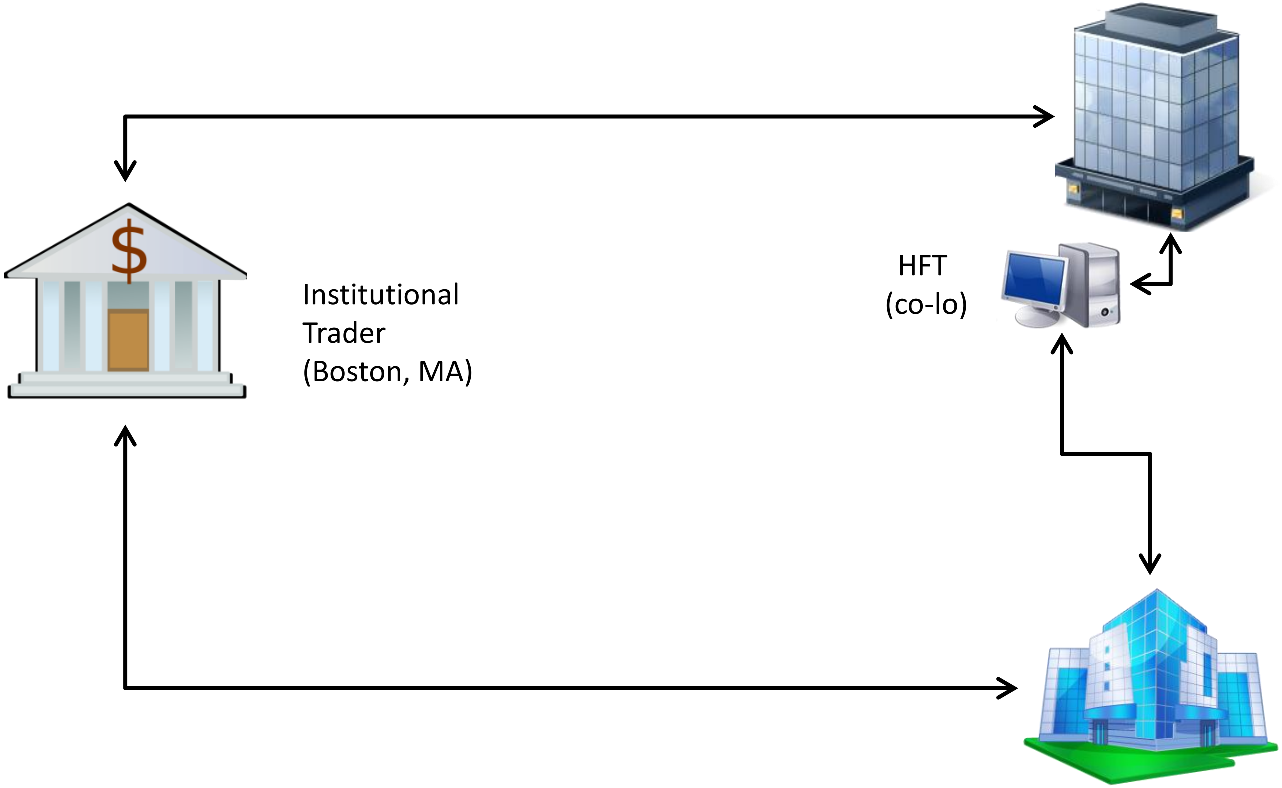
BATS
(Camdon, NJ)

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | **100** | **$55** |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$55** |
| | | 175 | $57 |

SOR delays NYSE order by 2 ms so that both orders arrive simultaneously

# Smart Order Routing



NYSE
(Mahwah, NJ)

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

BATS
(Camdon, NJ)

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 50 | $56 |
| | | | |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | 175 | $57 |
| | | | |

Trade executed at best price: The HFT could not alter orders at either exchange because the orders from the IT arrived simultaneously

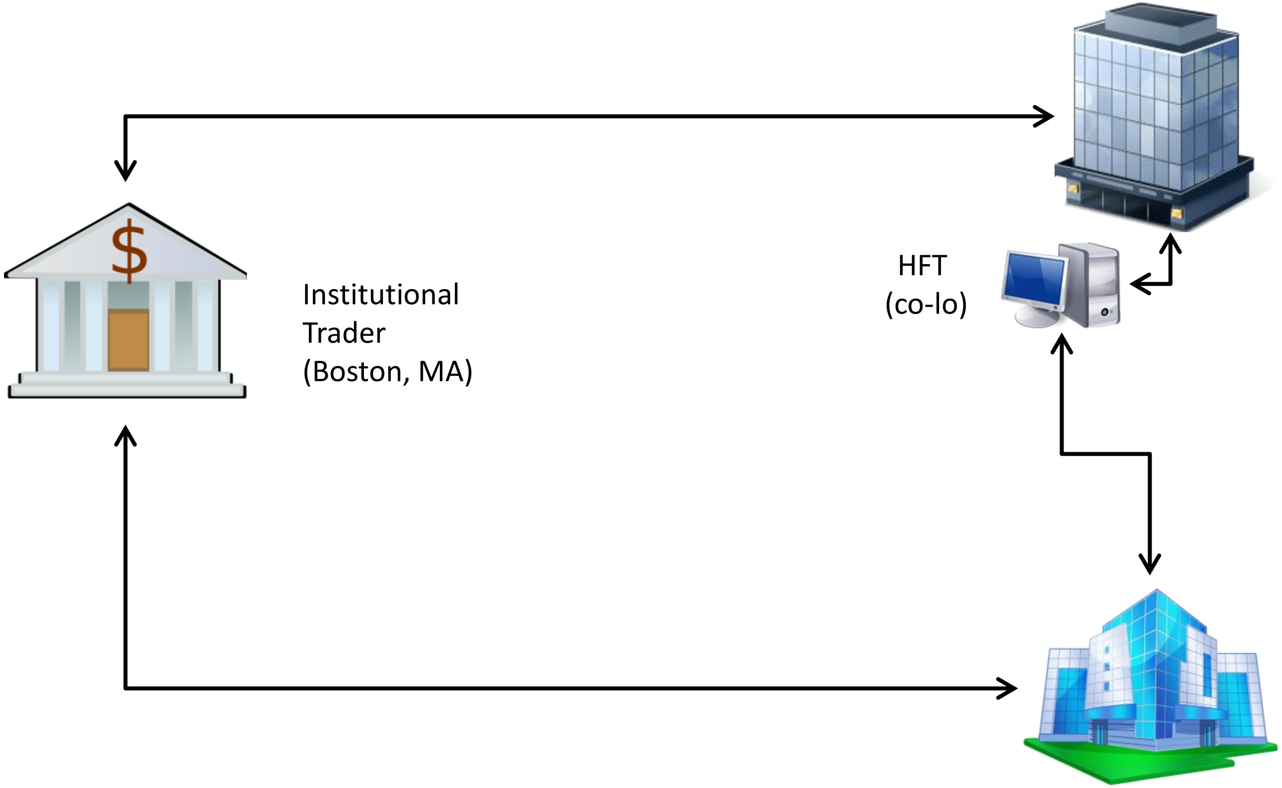
# An Absolute Time Component to Smart Order Routing

If SORs only use round-trip time (RTT) to measure delays to each exchange, then they have no dependence on absolute time.  But there can be many 100s of microseconds of error in the estimated forward-path delay when only RTT measurements are used:  HFTs can exploit this error!  Consequently, there is increasing pressure on the exchanges to timestamp order arrivals with (absolute) microsecond accuracy.  Such timestamps would likely allow the forward-path delay to each exchange to be estimated accurately enough (e.g., < 100 us) that HFTs could not exploit the remaining errors.

***But market reliance on absolute time stamps opens up a vulnerability to time manipulation …***

# Smart Order Routing

## GPS-Spoofing-Assisted Frontrunning



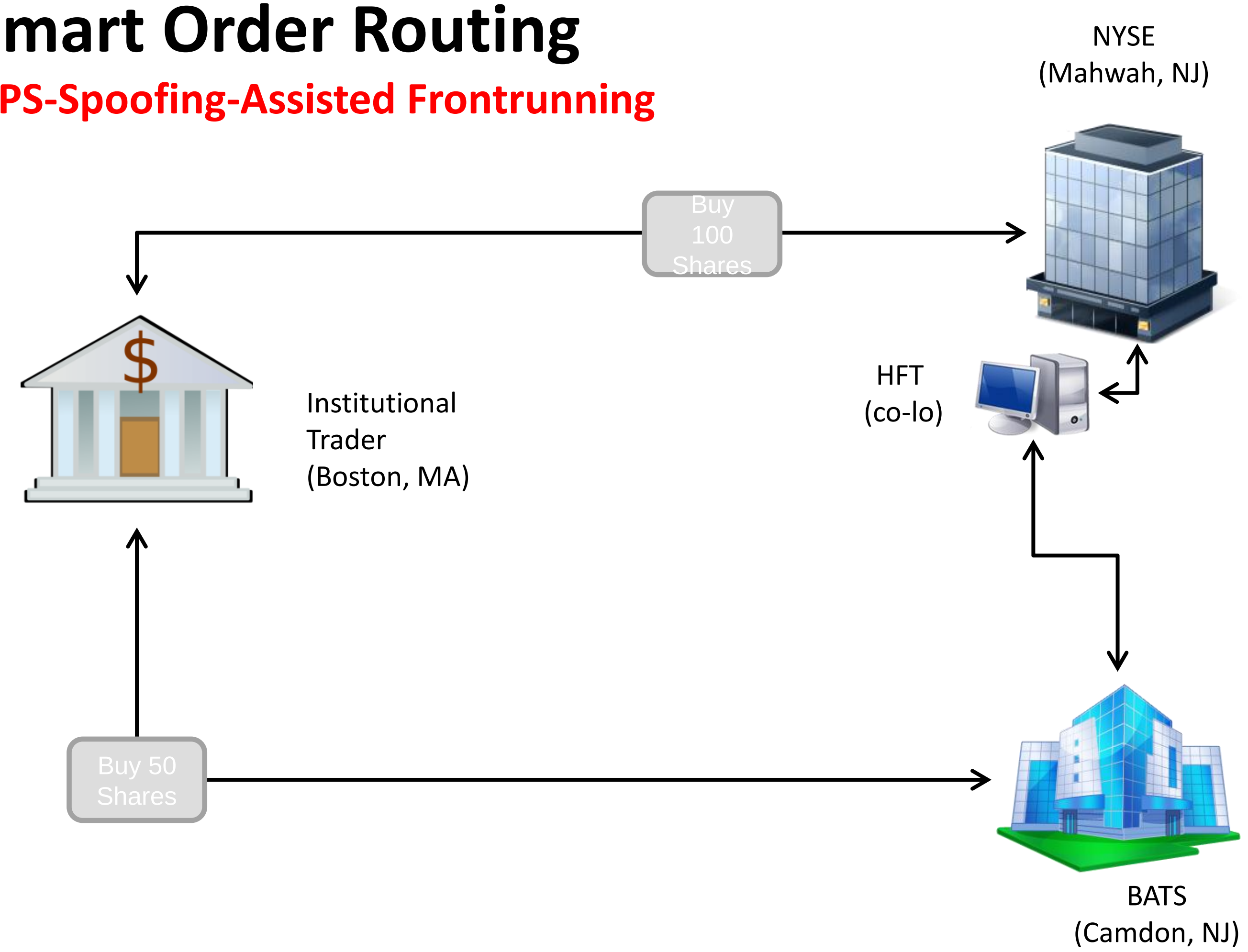
| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 100 | $55 |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | 50 | $55 |
| | | 175 | $57 |

**Action:** Spoofer advances time at NYSE by 2 ms.
**Result**: An SOP reliant on absolute time stamps now sees equivalent-time routes to NYSE and BATS

# Smart Order Routing

## GPS-Spoofing-Assisted Frontrunning



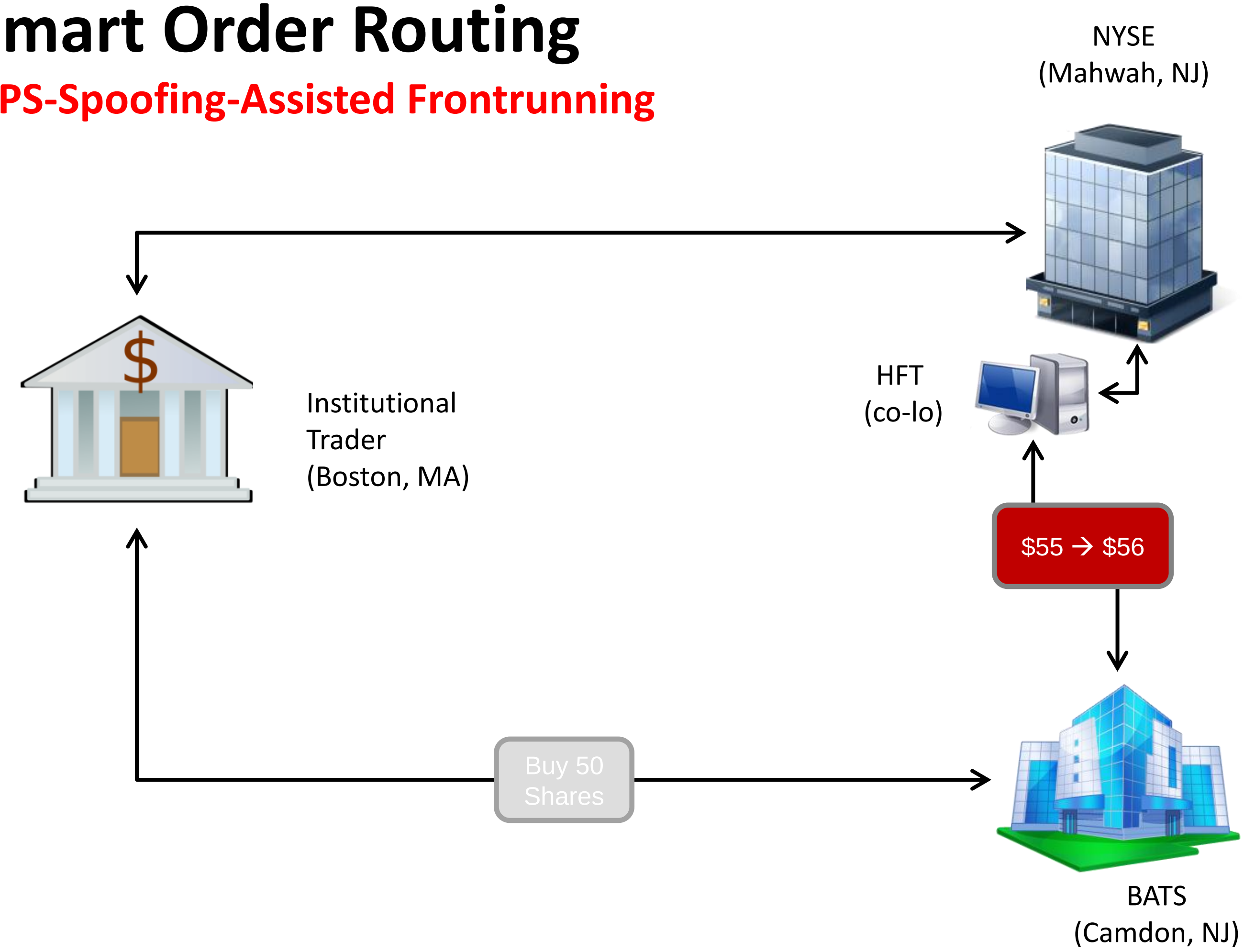
| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | **100** | **$55** |
| | | 50 | $56 |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$55** |
| | | 175 | $57 |

SOR issues both market orders simultaneously

# Smart Order Routing

## GPS-Spoofing-Assisted Frontrunning



NYSE
(Mahwah, NJ)

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

$55 → $56

Buy 50
Shares

BATS
(Camdon, NJ)

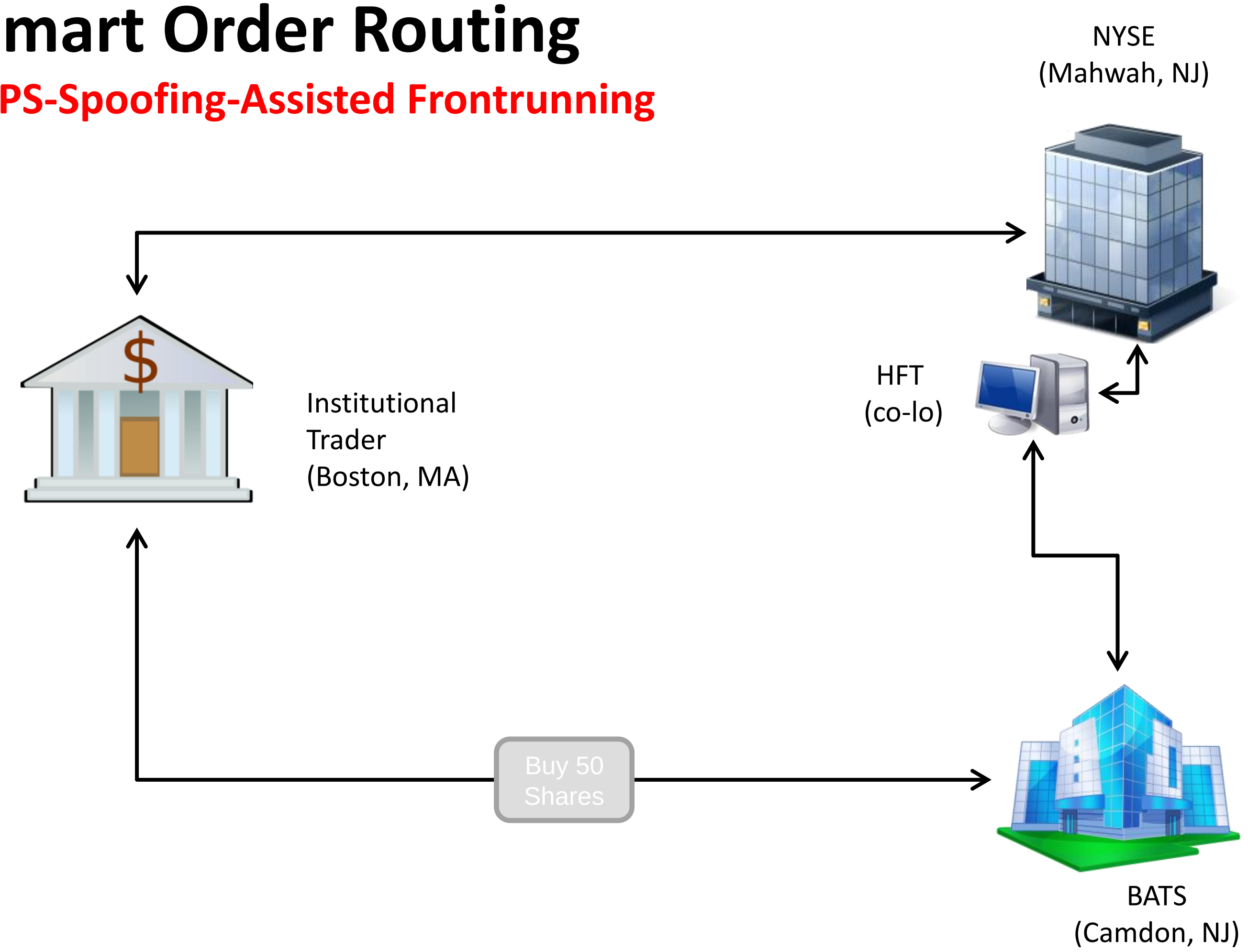
| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 50 | $56 |
| | | | |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$55** |
| | | 175 | $57 |

Trade executed at best price at NYSE.
HFT detects “whale” at NYSE and quickly changes ask price at BATS; HFT’s alteration arrives *before* the IT’s order.

# Smart Order Routing

## GPS-Spoofing-Assisted Frontrunning



NYSE
(Mahwah, NJ)

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

Buy 50
Shares

BATS
(Camdon, NJ)

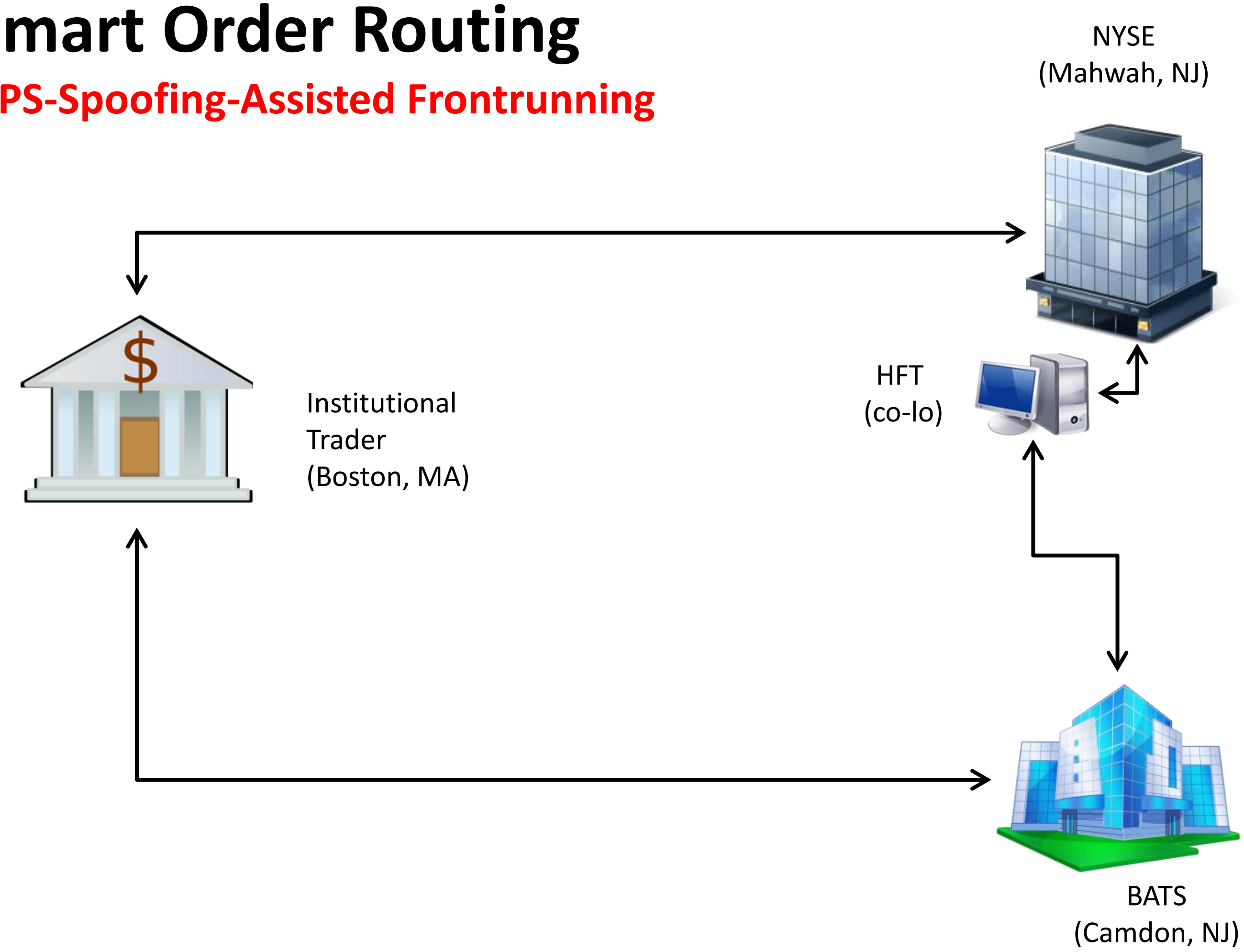
| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 50 | $56 |
| | | | |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | **50** | **$56** |
| | | 175 | $57 |

New price at BATS

# Smart Order Routing

## GPS-Spoofing-Assisted Frontrunning



NYSE
(Mahwah, NJ)

Institutional
Trader
(Boston, MA)

HFT
(co-lo)

BATS
(Camdon, NJ)

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 70 | $45 | 50 | $56 |
| | | | |

| Buyers (Bid) | | Sellers (Ask) | |
|---|---|---|---|
| Shares | Price | Shares | Price |
| 20 | $45 | 175 | $57 |
| | | | |

Trade executed at HFT price at BATS.

HFT makes profit at $1/share.

# Misconceptions About Timing Security (1/2)

- “Holdover” capability of GPS-disciplined oscillator (GPSDO) protects against spoofing
  - Holdover will not be triggered by a sophisticated spoofing attack
- The reference oscillator’s drift rate is the upper limit of speed at which a GPSDO can be spoofed (e.g., 1 us per day)
  - Drift rate only matters if GPSDO is configured to alarm on a mismatch between GPS rate and internal clock rate
  - Even then, spoofer can push GPS timing at ~5x the calibrated clock drift rate because of need to keep false alarm rate low

# Misconceptions About Timing Security (2/2)

- Timing errors only become a problem at the level of seconds, or maybe milliseconds.
  - Microseconds matter for comms, finance, and energy sectors
- Cross-checking against an atomic clock affords foolproof timing security
  - Rubidium clock with stability of 10^(-12) can be pushed off by ~100 ns per day
- PTP/NTP are the solution to GPS spoofing problem
  - These are getting better, but, due to network asymmetry, they still not accurate enough for most demanding applications non-dedicated networks

# Options for Secure ns-Accurate Timing (1/2)

- Obtain required permissions to purchase SAASM-equipped GPSDO
  - Lots of paperwork, special handling
  - Expensive
  - Fairly secure against spoofing
  - Not secure against replay attack
- Wait for GPS Directorate to insert digital signatures into modernized GPS signals
  - They’re making progress! (The University of Texas is helping.)
  - Not so strong as SAASM for timing security, but quite effective
  - Eventually inexpensive, but will require new GPSRO

# Options for Secure ns-Accurate Timing (1/2)

- Cross-check GPS timing against redundant high-quality (e.g., atomic) clocks
  - Self-contained
  - Expensive
  - Absolutely secure to within about 5x the drift rate of ensemble
- “All Signals” Approach: Develop a GPSDO that pulls in signals from GPS + Glonass + Galileo and rigorously cross-checks these
  - None on market yet (so far as I’m aware)
  - Potentially inexpensive: uBlox LEA-7 runs ~$50
  - Spoofer’s job gets much harder with each new signal
- PTP/NTP over a dedicated network

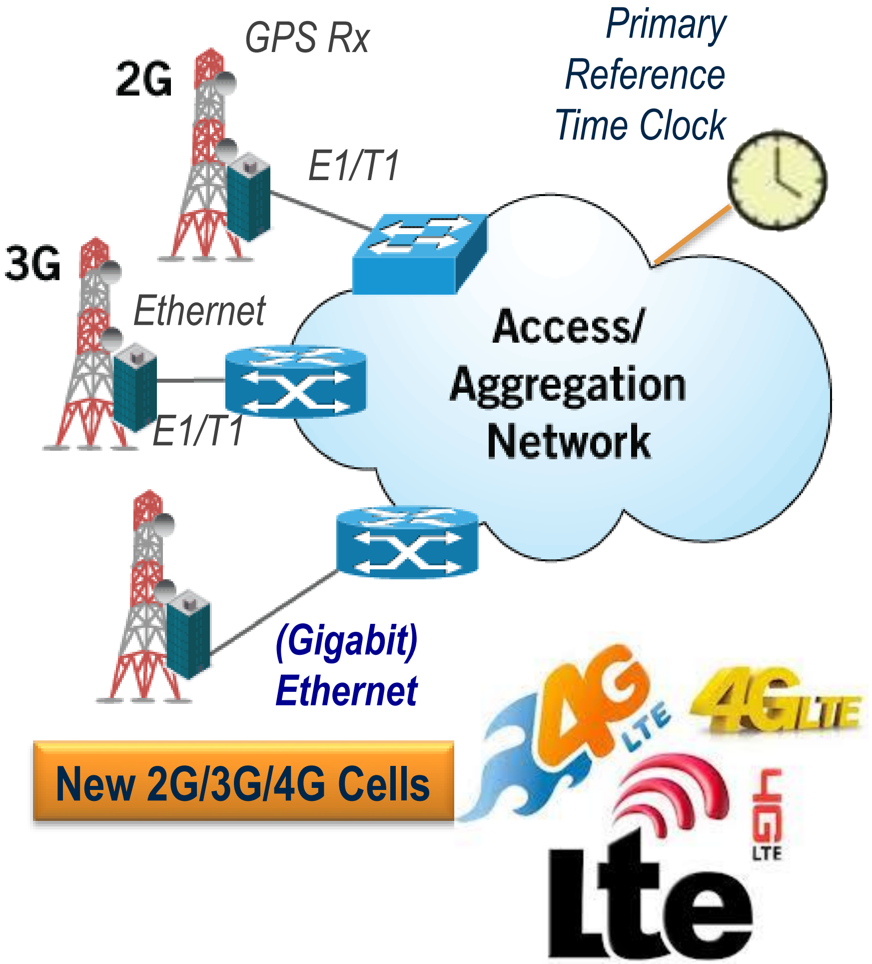
# Reliable Network-Based Timing

**Martin Nuss, Ph.D.**
*Vice President, Technology and Strategy and CTO*
*Vitesse Semiconductor*

# Overview

- We need a backup for GPS to provide timing
- Packet-based network timing using IEEE1588 Precision Time Protocol is the solution
- Even stringent TD-LTE and LTE-A timing requirements can be met

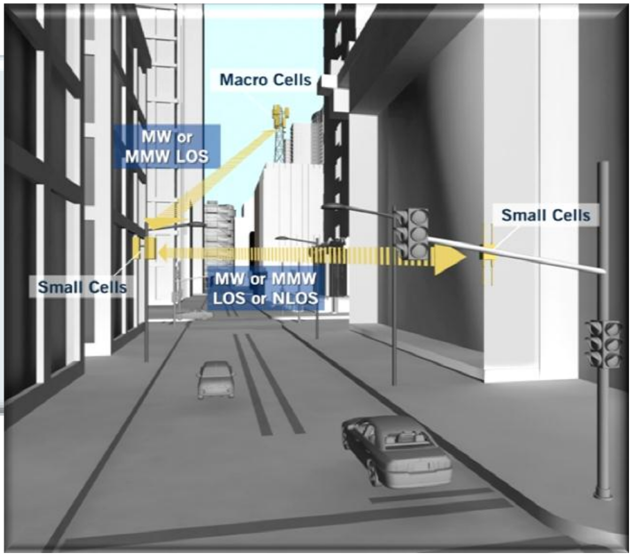
# New Base Stations Require New Timing Models



- For 2G/3G, E1/T1 backhaul also provided (frequency) synchronization

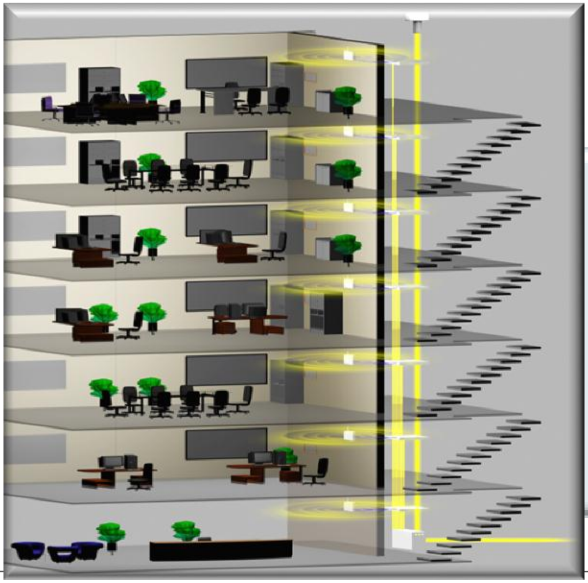
- New base stations use Gigabit Ethernet for backhaul
- TD-LTE and LTE-A need phase in addition to frequency synch

# GPS Not Viable in Many New LTE Deployments



## Outdoor Small Cells

- Small Cells to deliver LTE capacity
- Often no line of sight to GPS satellites
- More vulnerable to attacks at street level



## Indoor Picocells

- Picocells or Enterprise Femtocells for LTE indoor coverage & capacity
- Can't get timing to Femtocells using GPS

# The Solution: Timing Over IP/Ethernet

**Two new methods for carrying timing and synchronization over Ethernet networks have emerged**

G.8262 SyncE

- Line timing of the each Ethernet interface
- Can deliver **only frequency**, not phase

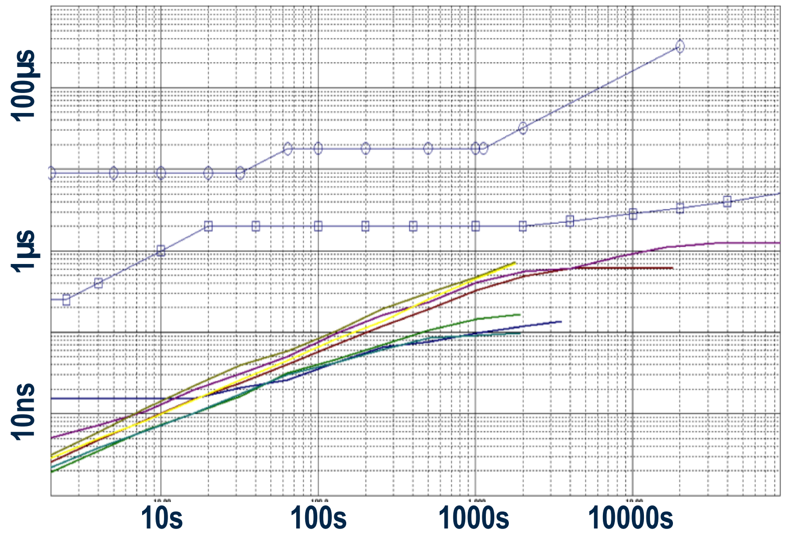
IEEE1588-2008

Precision Time Protocol

- Time stamped Sync packets & protocol exchange
- Over 1M Base Stations support 1588 PTP today
- 1588 can deliver frequency **AND** phase

# Frequency Delivery Over PTP-Unaware Networks

- **ITU-T G.8261.1 completed work on 1588 FREQUENCY delivery**
- **Packet delay variations (PDV) need to be within bounds**
- **Software algorithms (“servos”) are key to filter out effect of PDV**
- **Key servo performance usually long-term wander**



*ITU-T G.8261.1 test cases compared against G.823 Traf & SEC  MTIE masks*

# LTE Can Require Very High Phase/Time Accuracy

- Many wireless standards require PHASE synchronization in addition to frequency
- LTE-Advanced in particular requires very tight phase synch
- Standards are in the process of defining time and phase delivery via IEEE1588 to these specs

**Air Interface Phase Accuracy Specs**

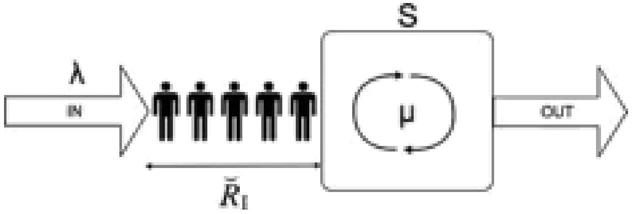
| | |
|---|---|
| CDMA2000 | 3-10 µs |
| TD-SCDMA | 1.5 µs |
| LTE Hetnet | 5 µs |
| TD-LTE | 1.5 µs |
| LTE-A | 500 ns |

# Factors That Impair PTP Time & Phase Accuracy

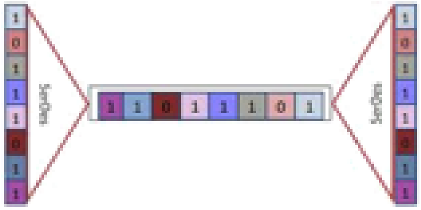
- Upstream/downstream packet delay asymmetries translate directly into time & phase errors
- Packet switching inherently has unpredictable queuing and forwarding delays
- Additional mechanisms become important when getting into the 100ns accuracy range

*Link Asymmetries (10-100ns)*

*Queuing & Forwarding (10-100µs)*

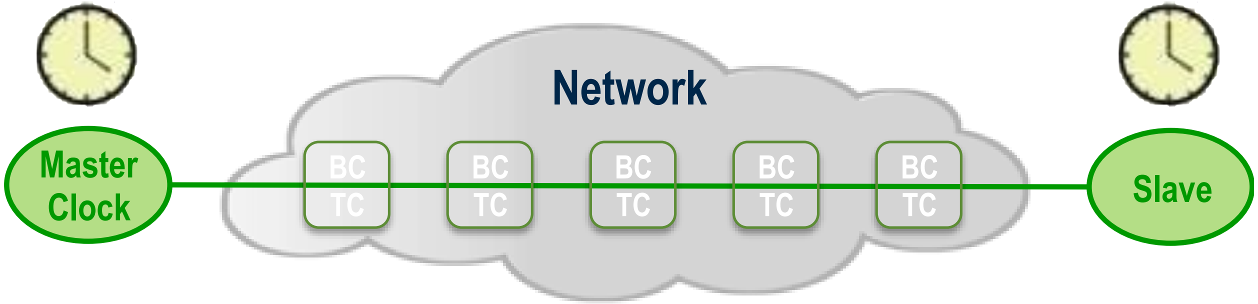


*I/O Serialization (10-100ns)*



**Queuing and forwarding delay asymmetries alone can be >100µs, blowing LTE phase accuracy requirements by 2 orders of magnitude**

# Boundary and Transparent Clocks to the Rescue



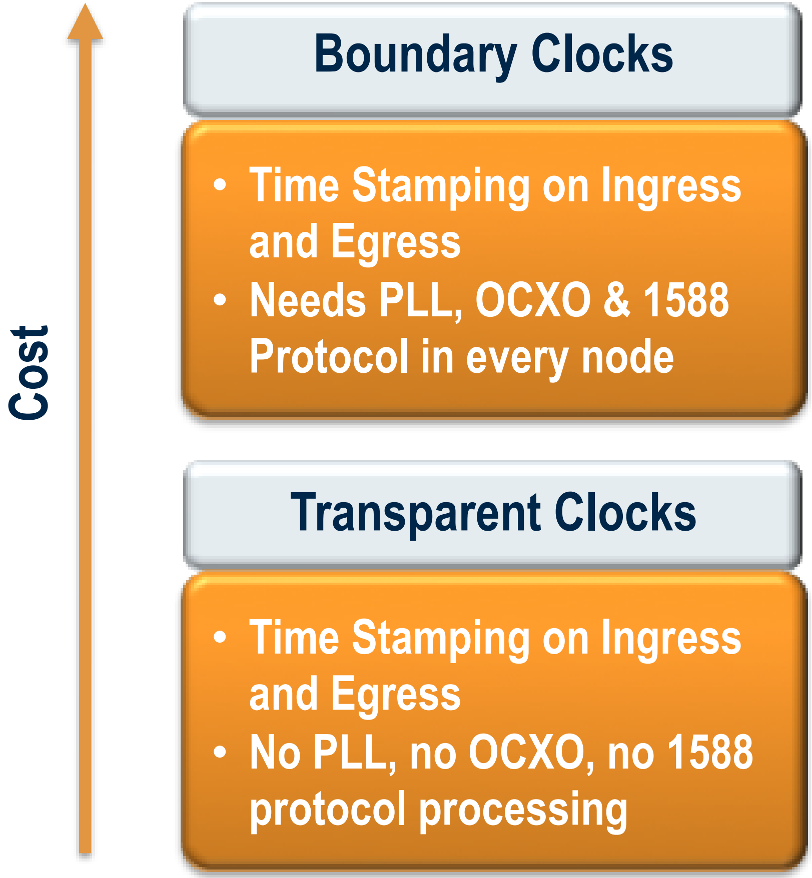
## Boundary Clock (BC)

- Recovers clock from the master, and regenerates clock towards next node
- Can be combined with Time Stamping at the PHY level to eliminate I/O serialization PDV

## Transparent Clock (TC)

- Simply corrects the Sync packet time stamp for residence time in the node
- Can be implemented solely at the PHY level if desired

# Network Timing Cost Comparison



Cost

**Boundary Clocks**

- Time Stamping on Ingress and Egress
- Needs PLL, OCXO & 1588 Protocol in every node

**Transparent Clocks**

- Time Stamping on Ingress and Egress
- No PLL, no OCXO, no 1588 protocol processing

- Boundary Clocks more expensive than Transparent Clocks
- Switches and Routers typically implement both
- TC can lower cost of clock recovery at slave
- Could be important for cost sensitive Small Cells

# Performance of a BC/TC Network

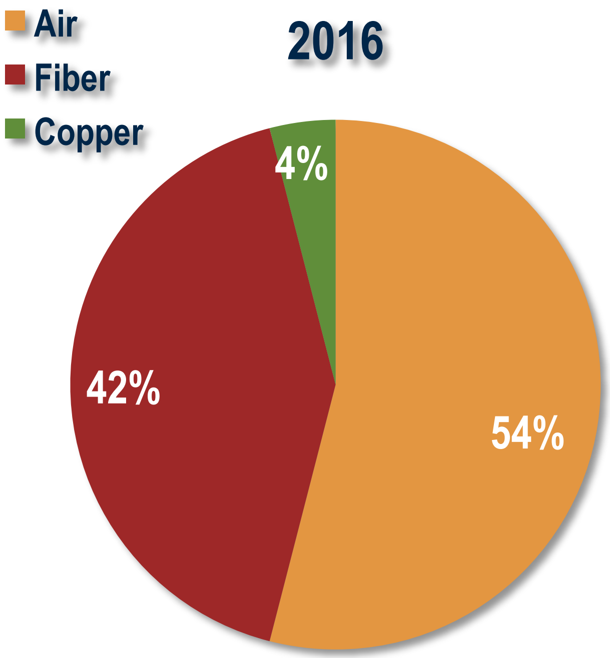
| Configuration | Frequency Support | 1PPS MTIE (5000 s) | 1 PPS Max TE |
|---|---|---|---|
| **Master - 9 x TC - Slave** | PTP | 24 ns | 25 ns |
| | SyncE | 17 ns | 11 ns |
| **Master - 9 x T-BC - Slave** | PTP | 75 ns | 51 ns |
| | SyncE | 30 ns | 17 ns |

*Select ITU-T G.8261.1 test cases; for details see WD17, June 2012 ITU-T SG15 Meeting*

- Nanosecond-level MTIE and Max Time Errors for both BC and TC
- No dependence on traffic load
- PHY-based time stamping removes queuing as well as I/O serialization PDV

**For Fiber or 1000Base-T connected nodes,
sub-10ns maximum time errors can easily be achieved**

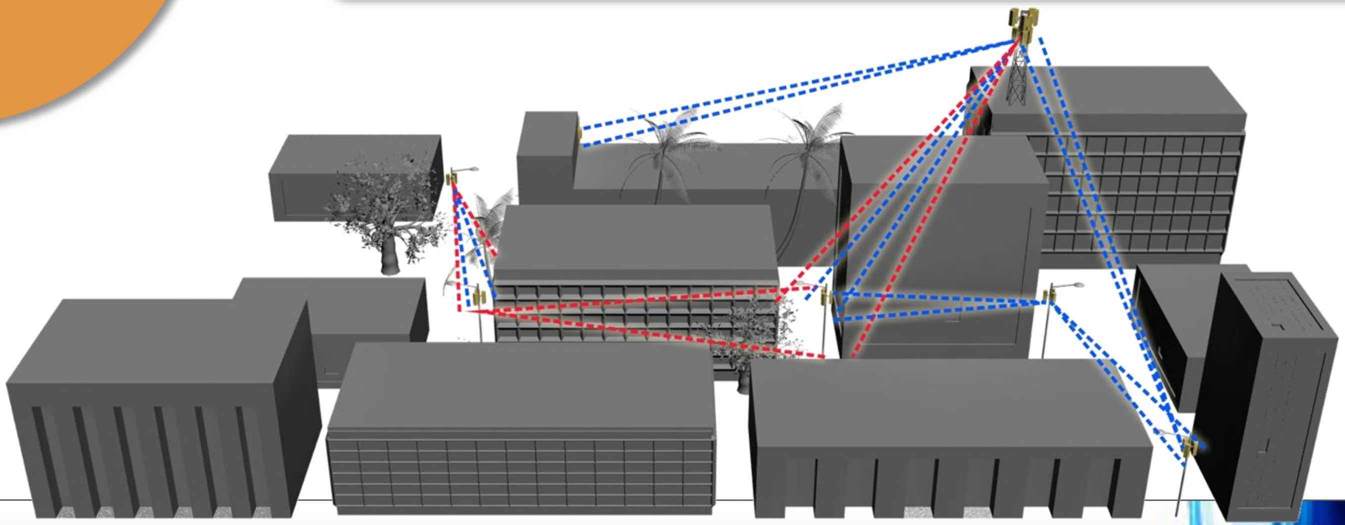
# Not all Backhaul Networks are Alike



Source:  Infonetics

- Backhaul can be fiber, microwave, or copper
- >85% of Small Cells will be connected by Microwave or Millimeter-wave (Infonetics)

**Network Timing over Microwave more difficult than over Fiber**



# Time Error Budgets for Various Link Types

| Equipment Type | Time Error Budget |
|---|---|
| Switch/Router (1000BT or Fiber) | 10-20ns |
| Microwave Link | 100ns |
| GPON | 100ns |
| DSL | ? |

BC/TC can control Time Errors to <10ns;

Distributed TC can keep MW & PON to <100ns

# Calculating Maximum Network Time Errors

- Operators need an easy way to calculate maximum time error
- This is possible if standards specify maximum time errors per equipment class

| Equipment | Max Time Error | Hop Count |
|---|---|---|
| Small Cell | 20 ns | 3 |
| MW/MMW Link | 100 ns | 2 |
| Cell-site Gateway | 20 ns | 1 |
| Pre-Aggregation Router/Switch | 20 ns | 1 |
| Aggregation Router | 20 ns | 10 |
| **Total Network Time Error** | | **500 ns** |

**1588 network timing will be possible even with multiple Microwave links in the last mile**

# Summary and Conclusions

- GPS cannot be the only source of timing – we need a backup!

- IEEE1588 PTP with Boundary and Transparent Clock support can provide networks based timing even for TD-LTE & LTE-Advanced

- Standards should allocate time error budgets per equipment class so operators can easily calculate maximum network time errors for heterogeneous backhaul networks

**Thank you for attending**

***GPS Vulnerabilities and Implications for Telecom***

**All registered attendees will receive a follow up email containing links to a recording and the slides from this presentation.**

**For information on upcoming ATIS events, visit**

**www.atis.org/events**