A Secure Civil GNSS:

Satellite signal authentication and location & time verification using hidden signatures

David De Lorenzo, Sherman Lo, Per Enge

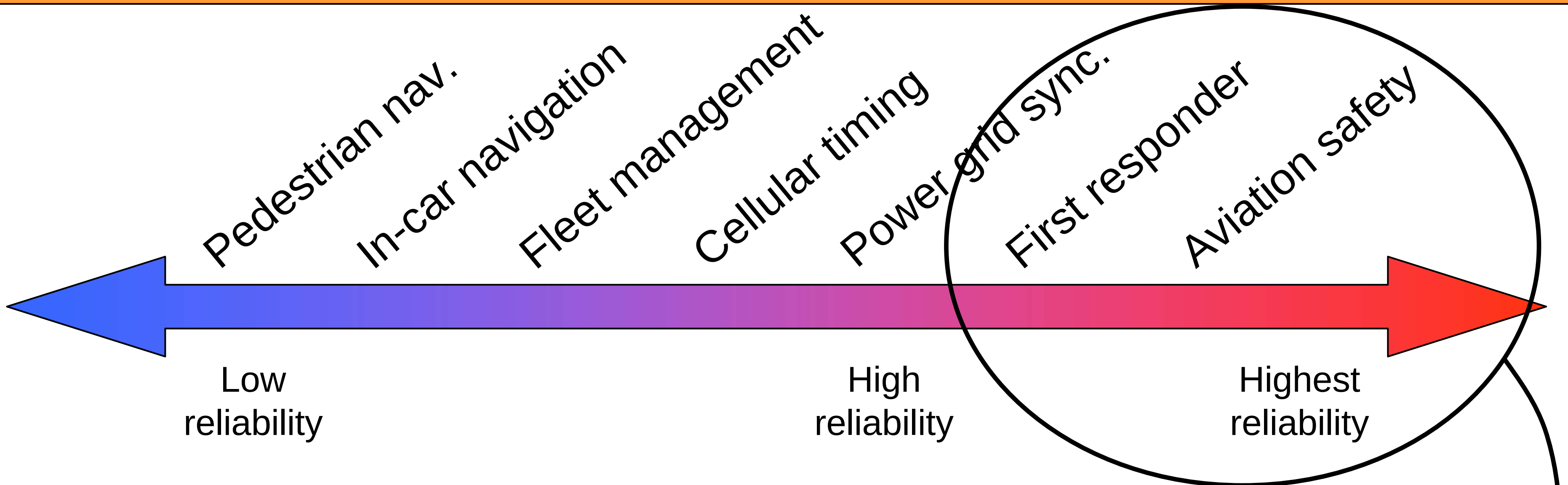
Trusted Navigation for Aviation

- GNSS augmentation for aviation safety-of-life
- SBAS & GBAS protect against:
  - Environmental faults
    - Iono, tropo, multipath
  - System faults
    - Clock, ephemeris
  - Off-nominal yet fault-free conditions

"GPS navigation guidance places you on glide slope and on runway centerline."

→ Rich history evaluating GPS reliability

A Continuum of Civilian GNSS Reliability



- Our reliance on satellite-derived ***position, navigation, and time*** is profound and pervasive
- Applications requiring the highest reliability are specifically concerned with GPS/GNSS degradation

➡ A new class of location-enabled transactions will test the resilience of civilian GNSS

Location Verification & Security

- When processing signals I receive myself, how do I ensure their authenticity?

  ➡ Signal authentication via hidden markers

- When receiving an assertion from another party about the signals they receive, how do I ensure the validity of their assertion?

  ➡ Location verification by digital watermarks

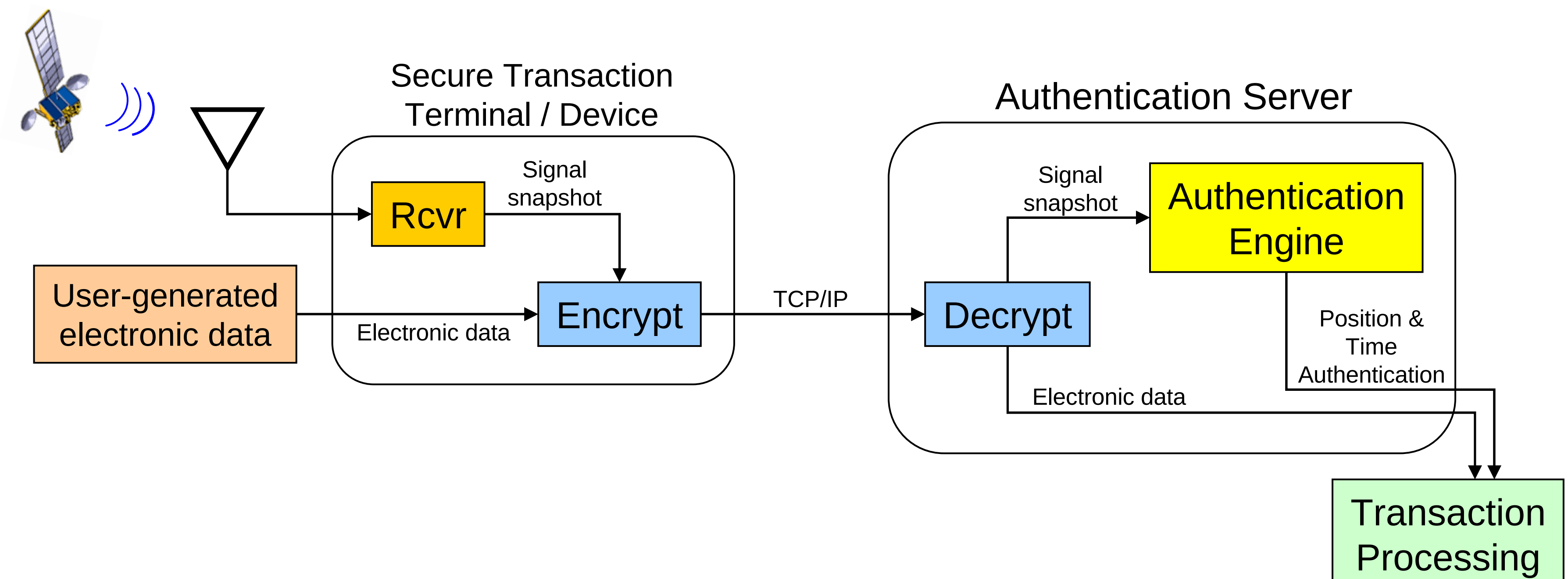
How does one use location verification to improve transaction security?

Location/Time Authentication Increases the Security of Electronic Transactions

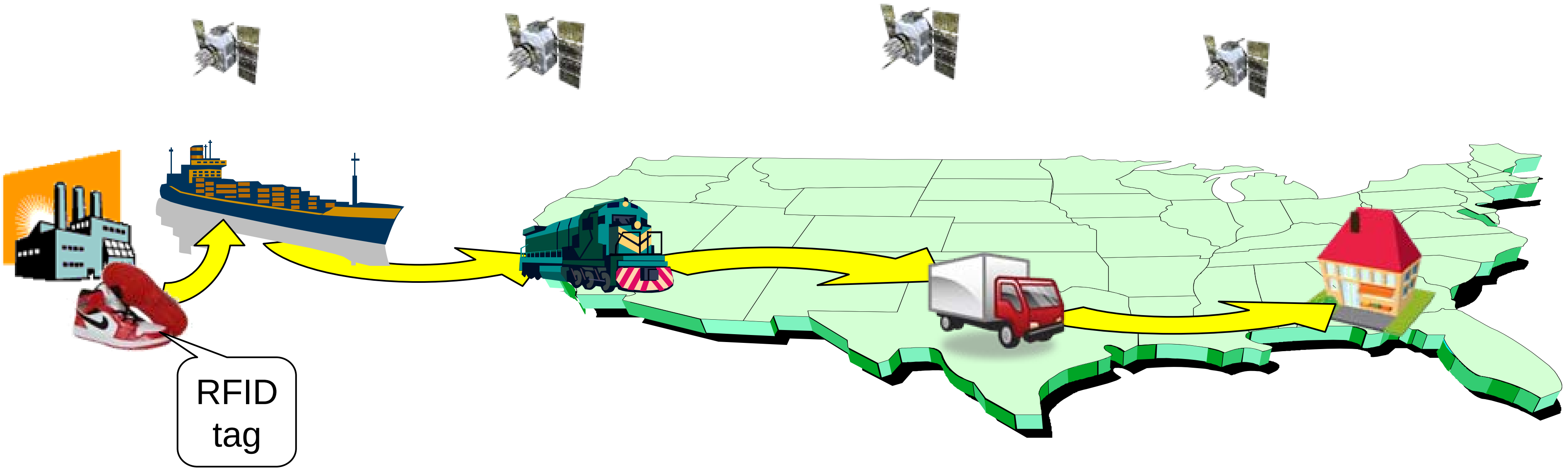
Please transfer $100,000 from Chase account 123456 to Fidelity account 987654, and then buy 1000 shares of Microsoft and 500 shares of Apple.

Sir, your location and password have been confirmed, and your transactions are authorized.

Report: User authentication successful.

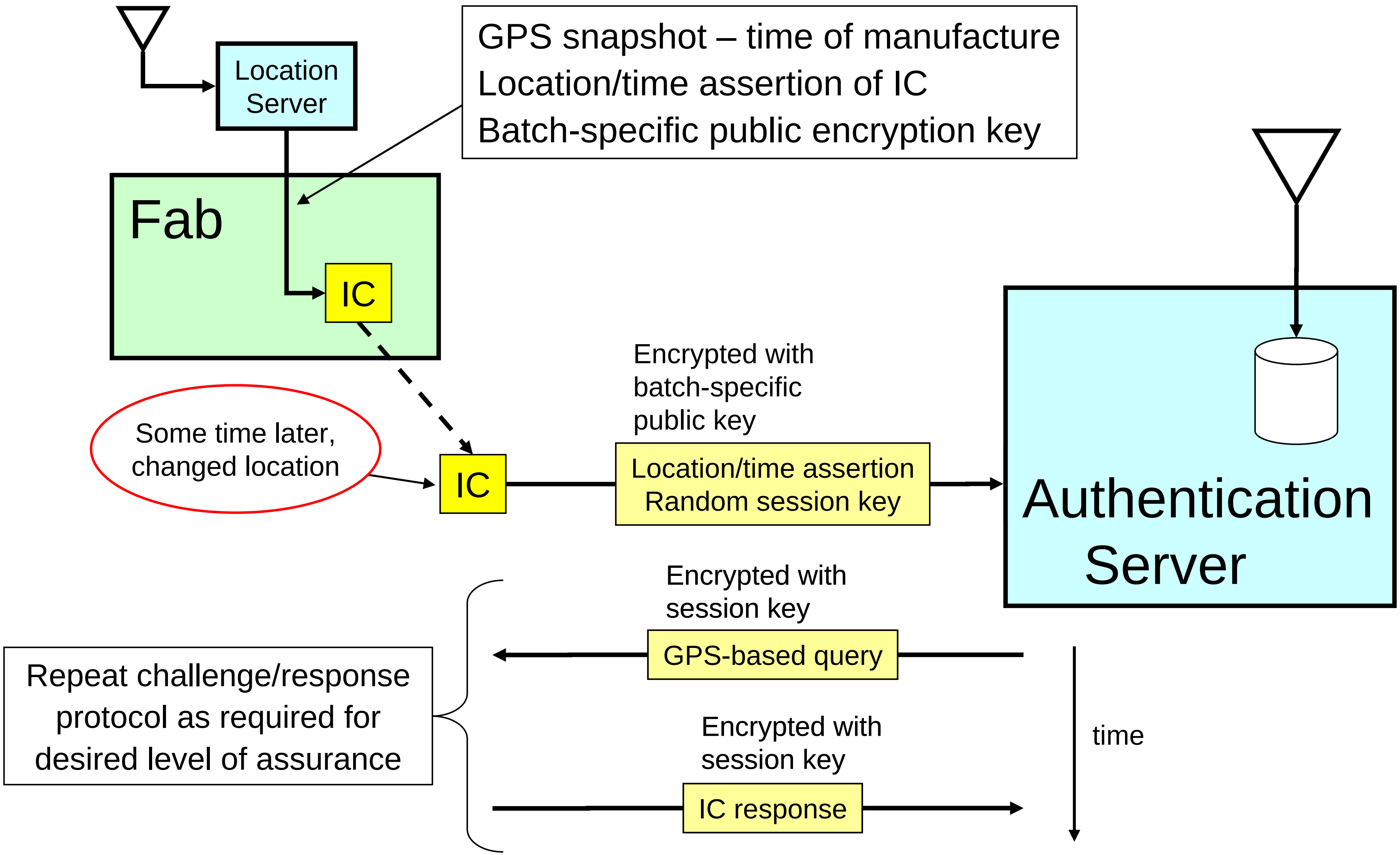


Anti-counterfeiting and Supply Chain Management

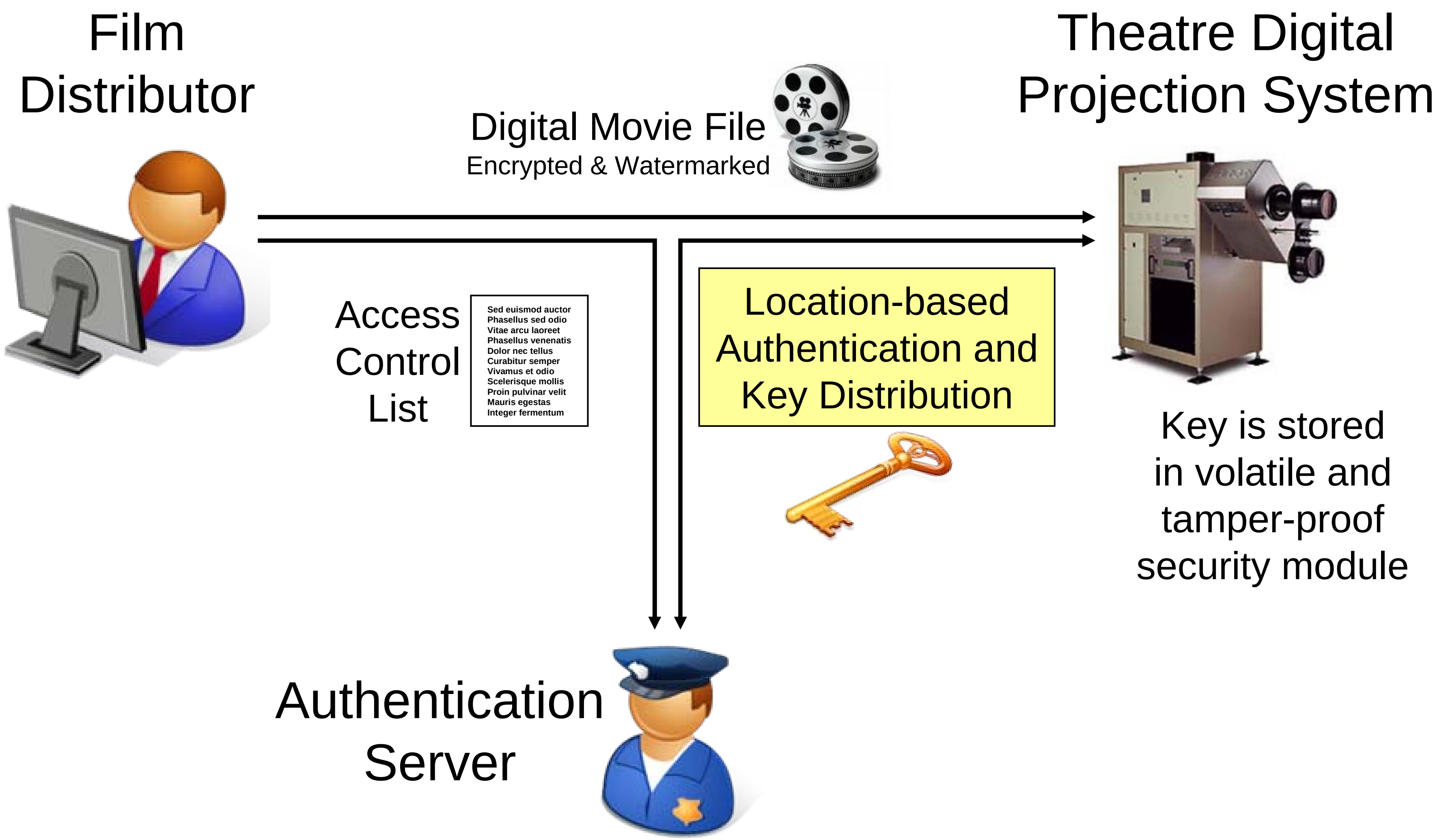


- The manufacturing attributes of ***"where"*** and ***"when"*** can distinguish counterfeit from *bona fide* goods.
- The security tag carries a ***"location & time watermark"*** which provides a secure, inexpensive, and highly-reliable guarantee of authenticity throughout the supply chain.

Location-based Security for Integrated Circuit Trust & Assurance



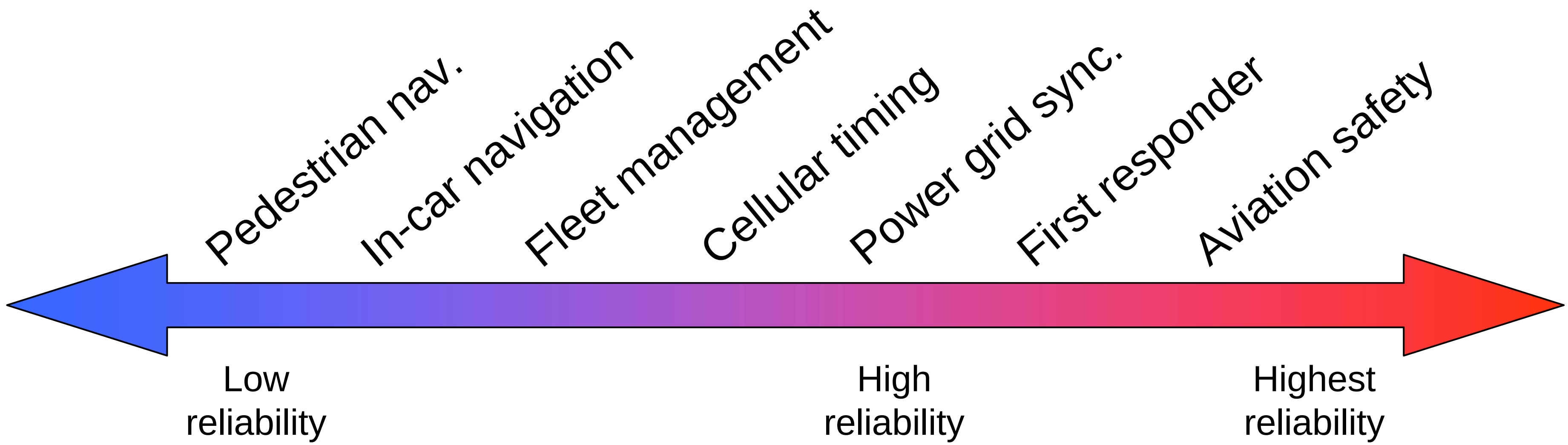
Film Distribution and High-Security Digital Rights Management

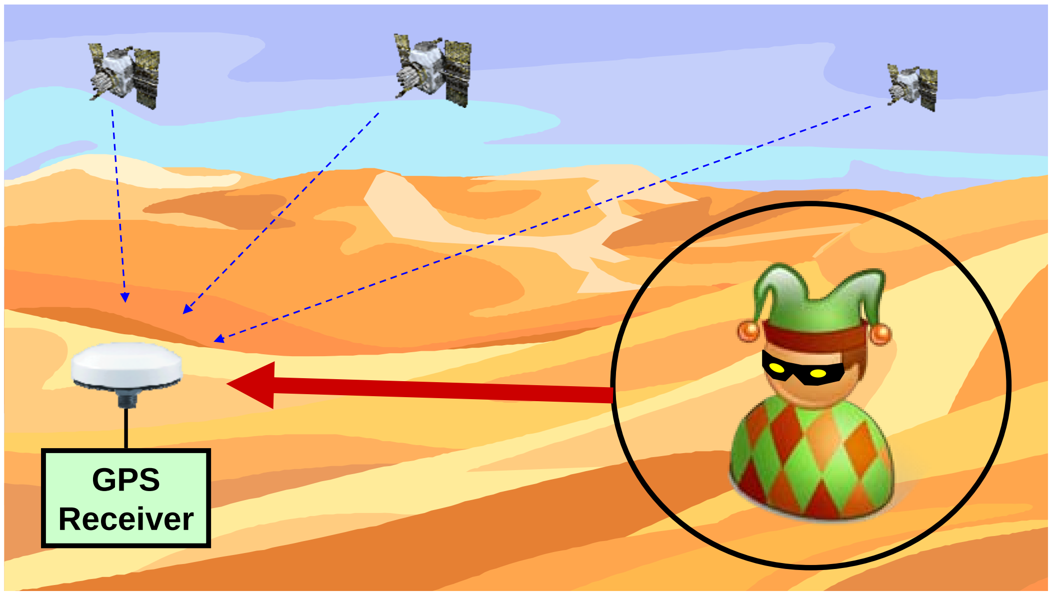


Location Security for Nonproliferation or Arms Control Inspections

- Inspections seek to document physical infrastructure and materiel inventories
- Unfamiliar or remote inspection sites
- Significant incentive for host to mislead inspection teams
- Location, time, and ***verification***

Malicious Attacks Against the GPS Utility





- But what happens when faults are perpetrated by a malicious agent?
  - Denial of service
  - Signal spoofing

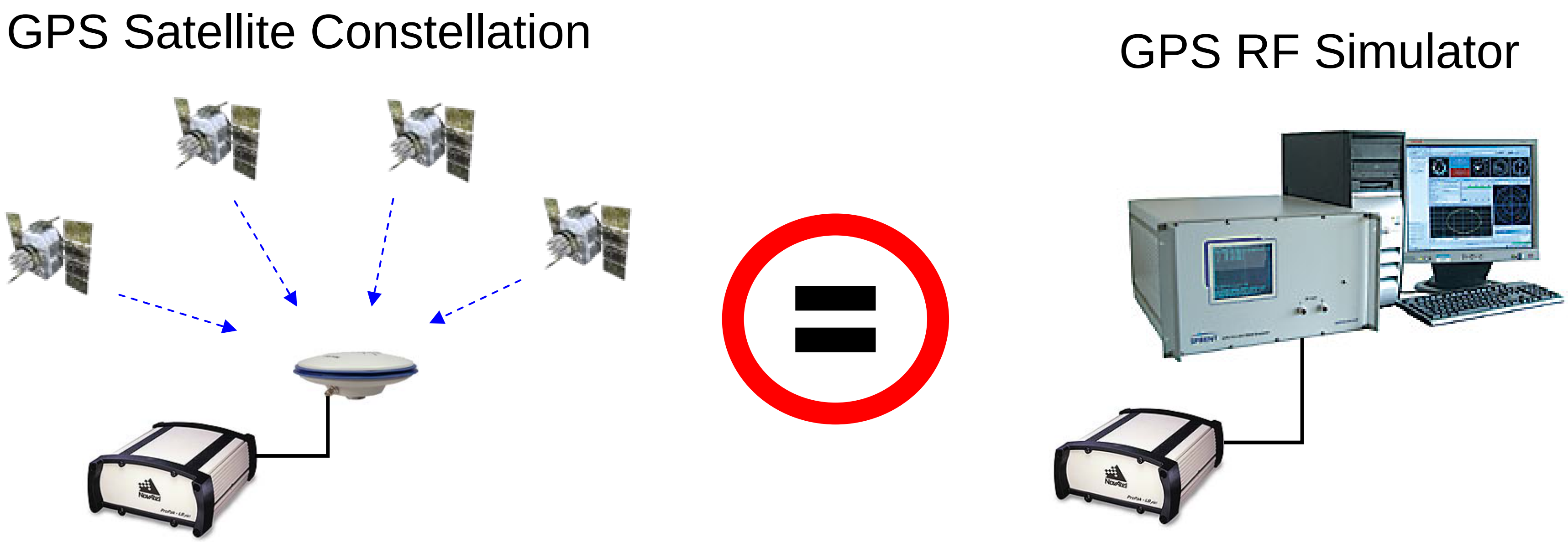
Location Verification & Security

- We seek a marker irrefutably tied to a location
  - For example, a picture establishes these climbers at the summit of Mt. Kilimanjaro (at least before PhotoShop!!)
- One possibility: a trusted (or bonded) navigation module w/ encryption and digital signatures
- Is there an RF signature that is location and time unique ***and*** unspoofable?

– from Frank van Diggelen @ Mt. Kilimanjaro

➡ Yes – GPS-based digital watermarks

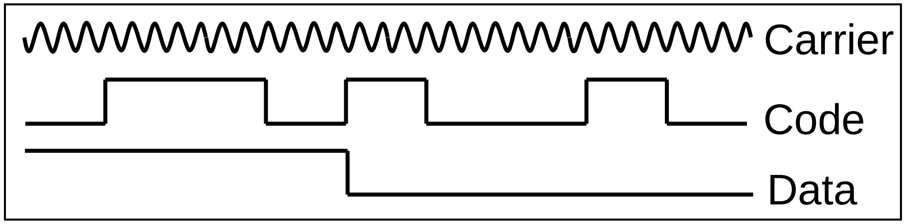
Trusted Navigation: Problem Statement



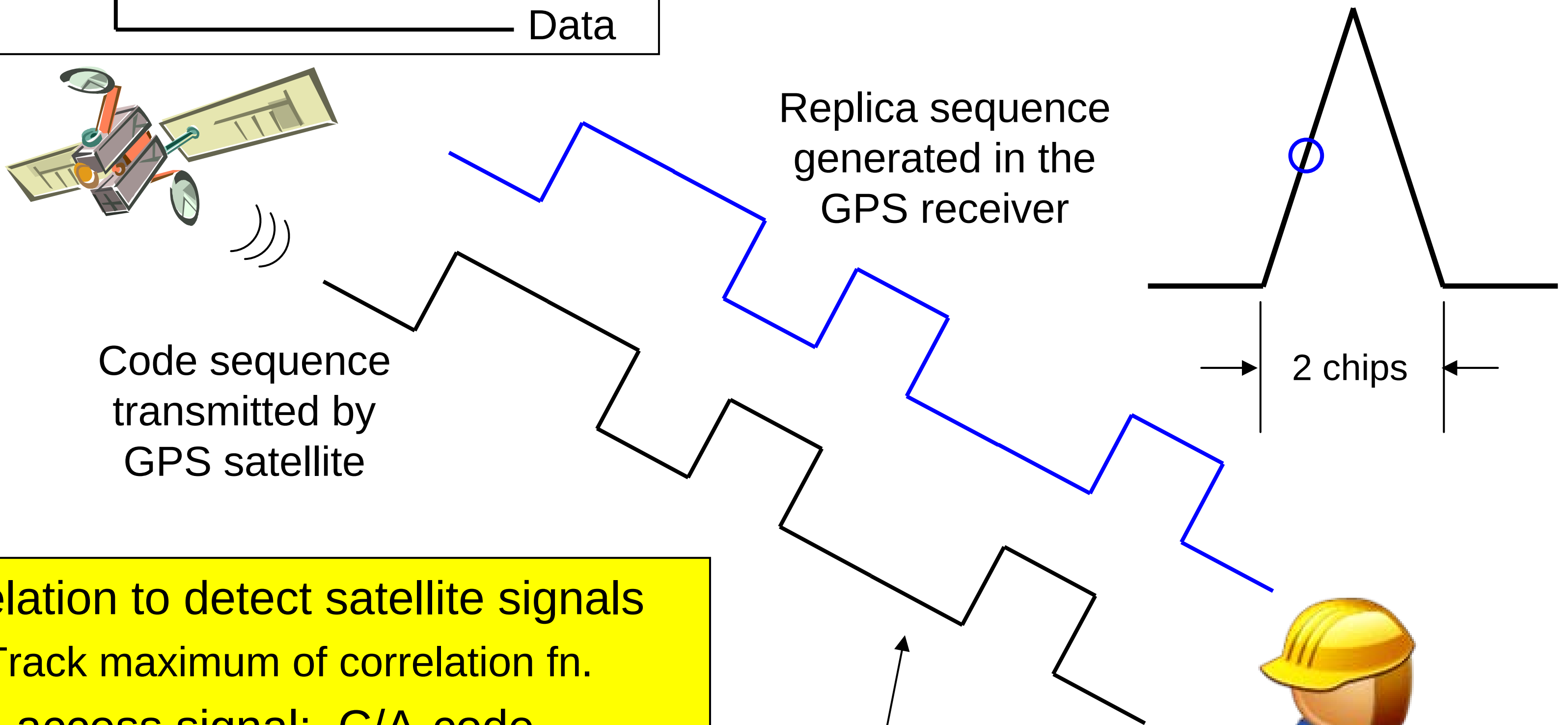
- GPS/GNSS reliability is only as strong as the trust in the underlying navigation signals

- Intra-system consistency checks: RAIM, GBAS/SBAS, DOA, etc.
- Inter-system consistency checks: GPS/INS/Wi-Fi/TV/eLoran/etc.
- Digital signatures and encryption: P(Y), M-code, Galileo PRS

GPS 101: Signal Correlation with Locally Generated Code Replica



GPS Signal Structure

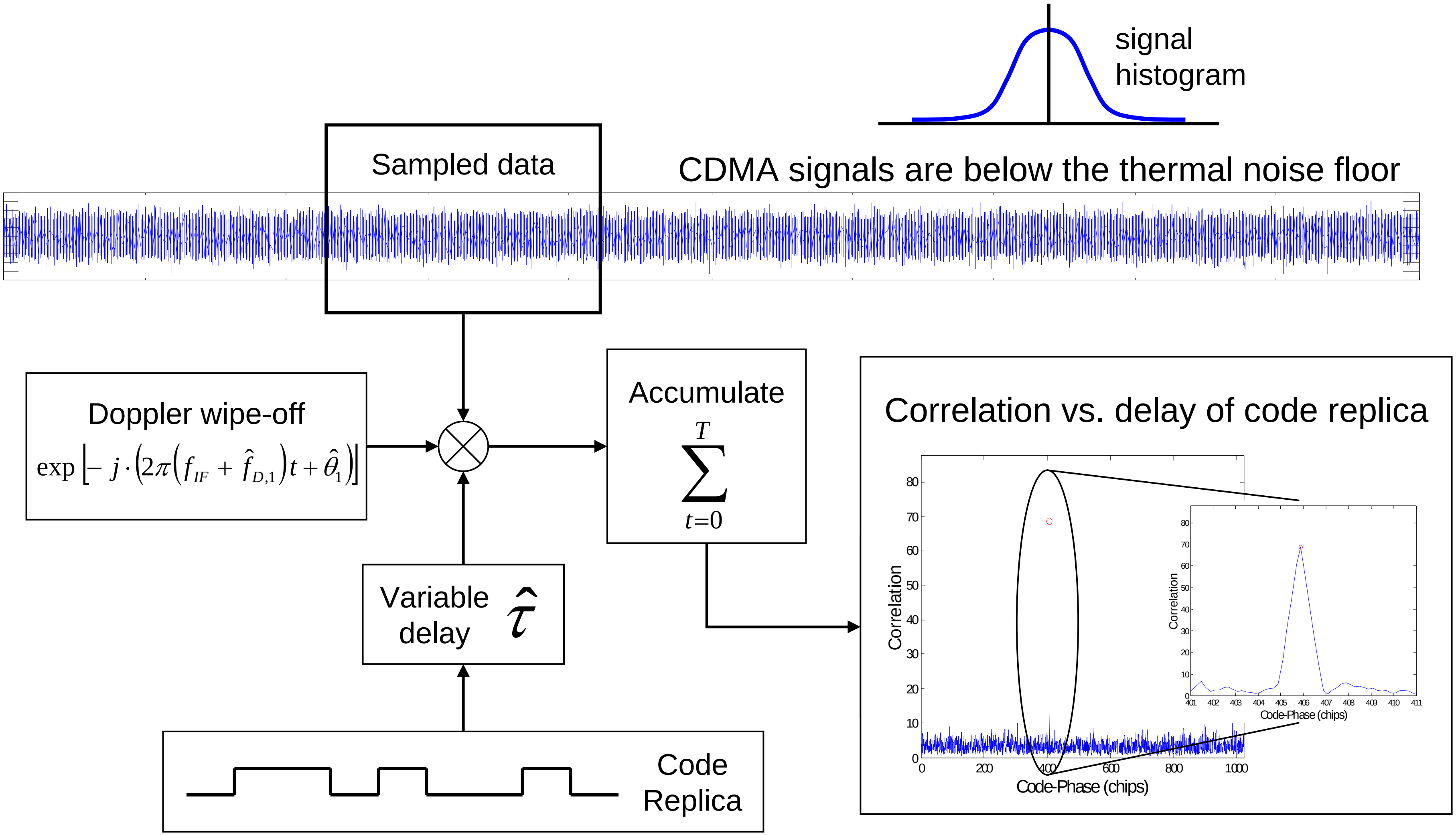


300m C/A-code
30m P-code

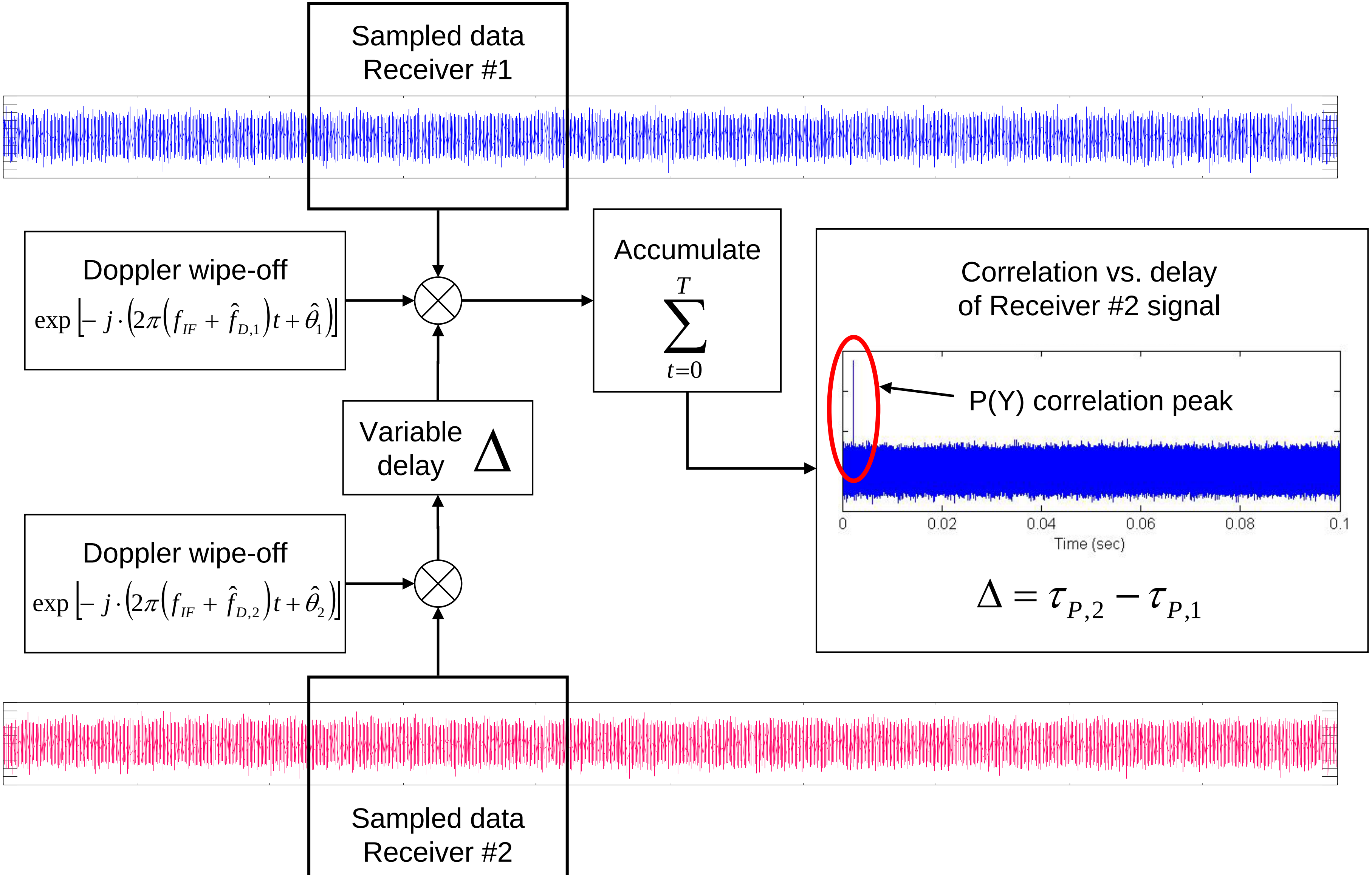
- Correlation to detect satellite signals
  - Track maximum of correlation fn.
- Open access signal: C/A-code
- Encrypted military signal: P(Y)-code
  - Denies access to unauthorized users
  - Authenticates signal broadcast source

Note: C/A and P(Y) are transmitted in phase quadrature

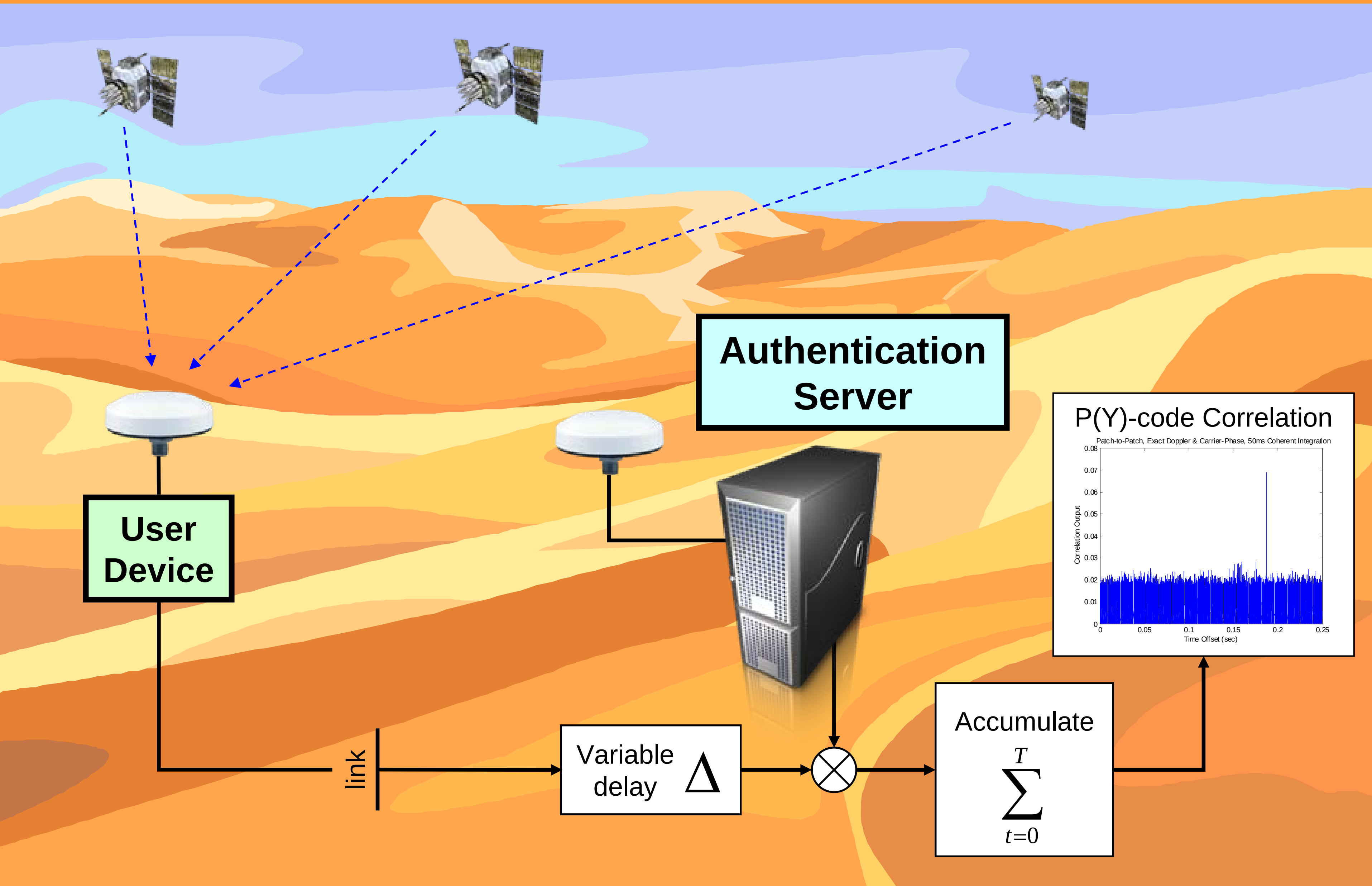
GPS Receiver Signal Processing:
Known CDMA Spreading Code Sequence



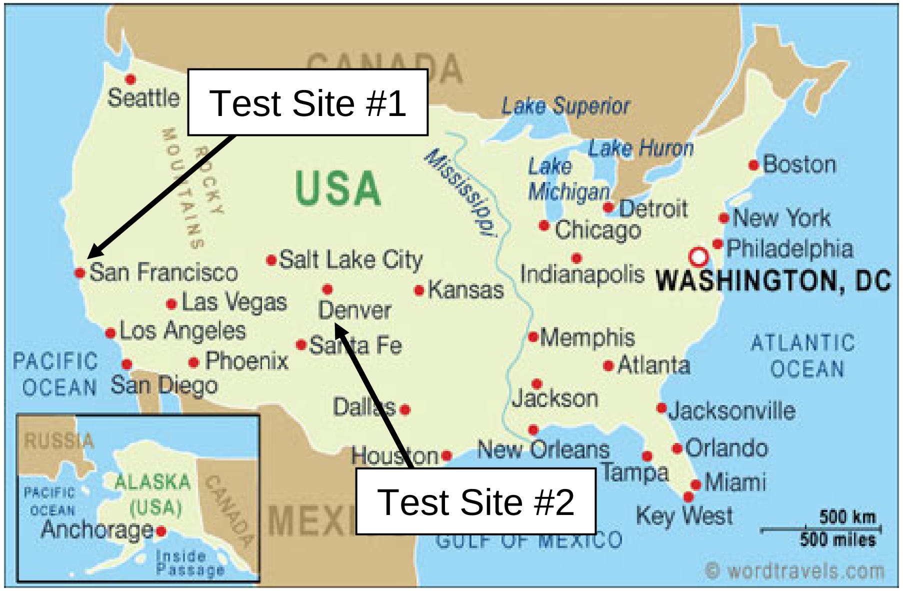
GPS Signal Authentication:
Unknown CDMA Code w/ 2-Receiver Correlation



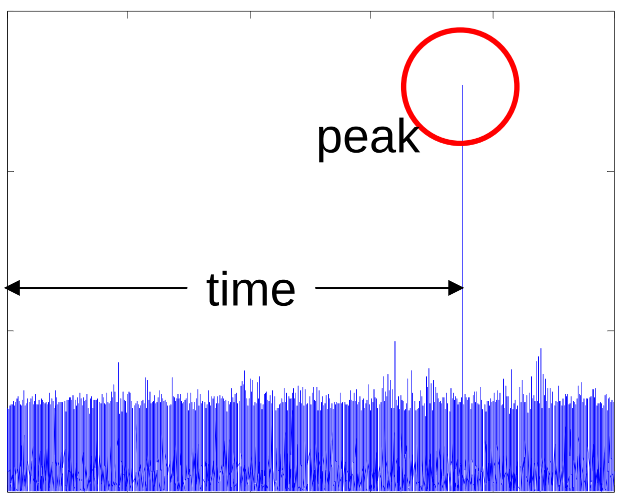
GPS Signal Authentication: Overview

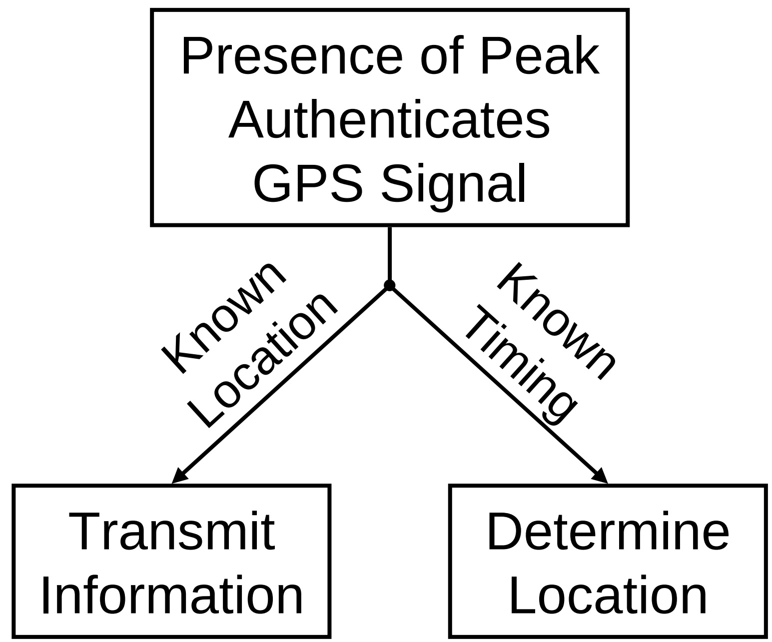


GPS Signal Authentication: Demonstration w/ Live Satellite Signals



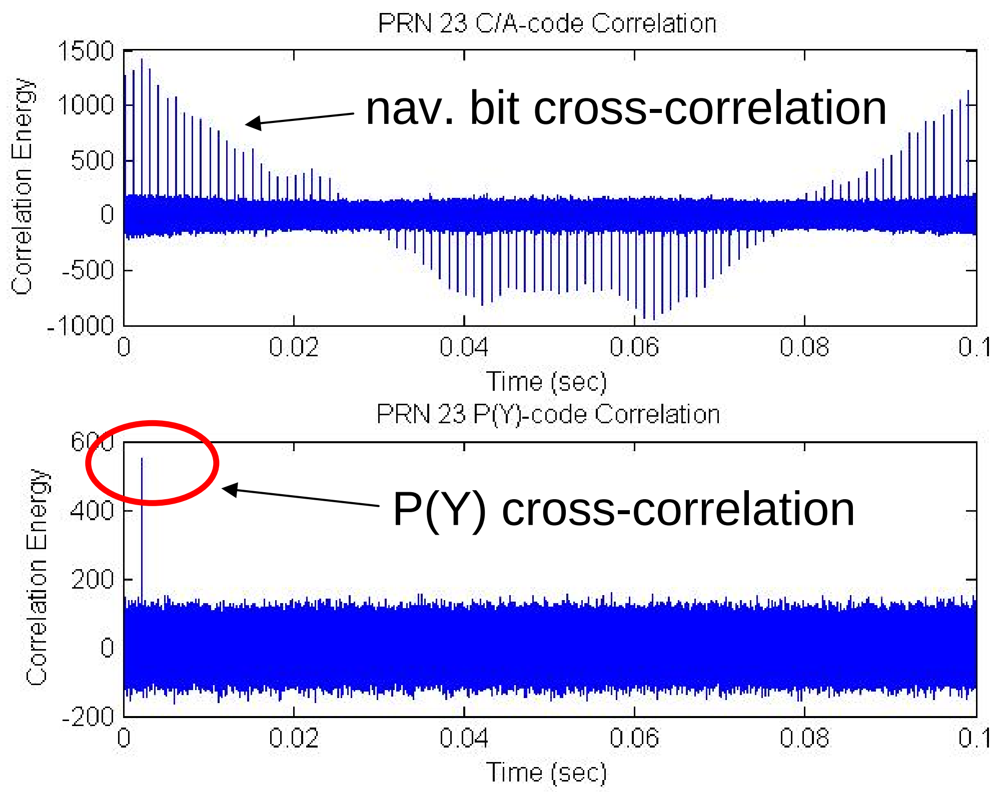
- <u>Reduction to practice:</u>
  - Signal authentication and secure positioning
  - Verified at two sites





GPS Signal Authentication: Proof-of-Concept Verification

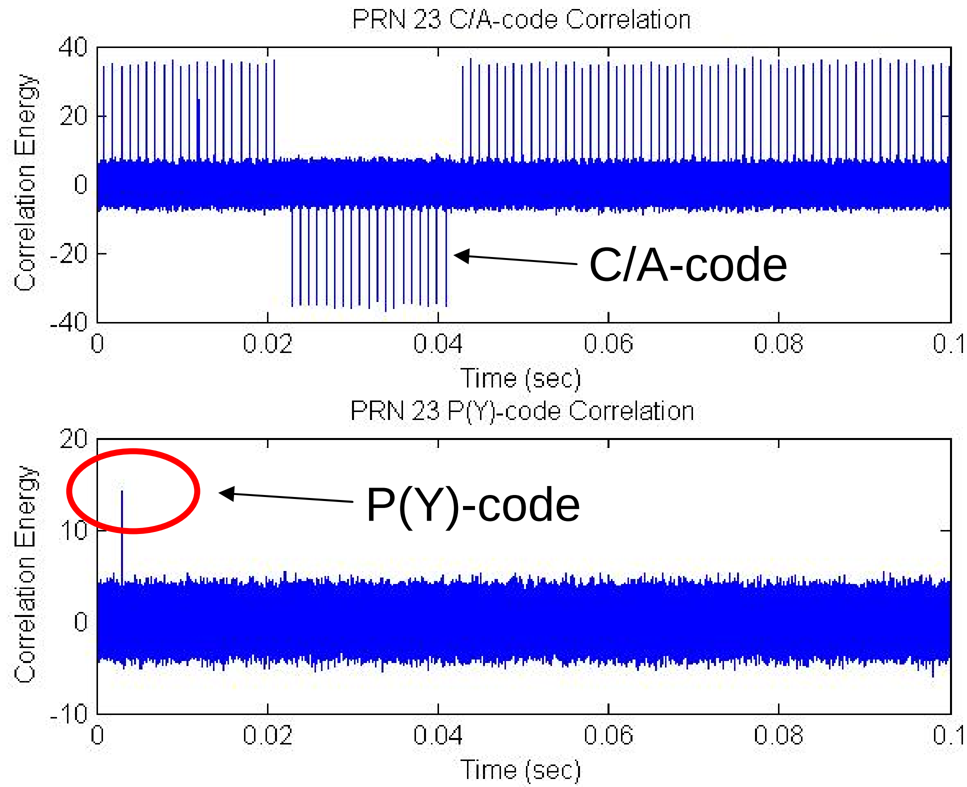
- Initial test with 100ms correlation window
  - 23.68 MHz sampling
  - Signal processing with a GNSS software receiver
  - Correlation peaks for several satellites in the common set
  - PRN-23 (shown here) is the strongest in the common set



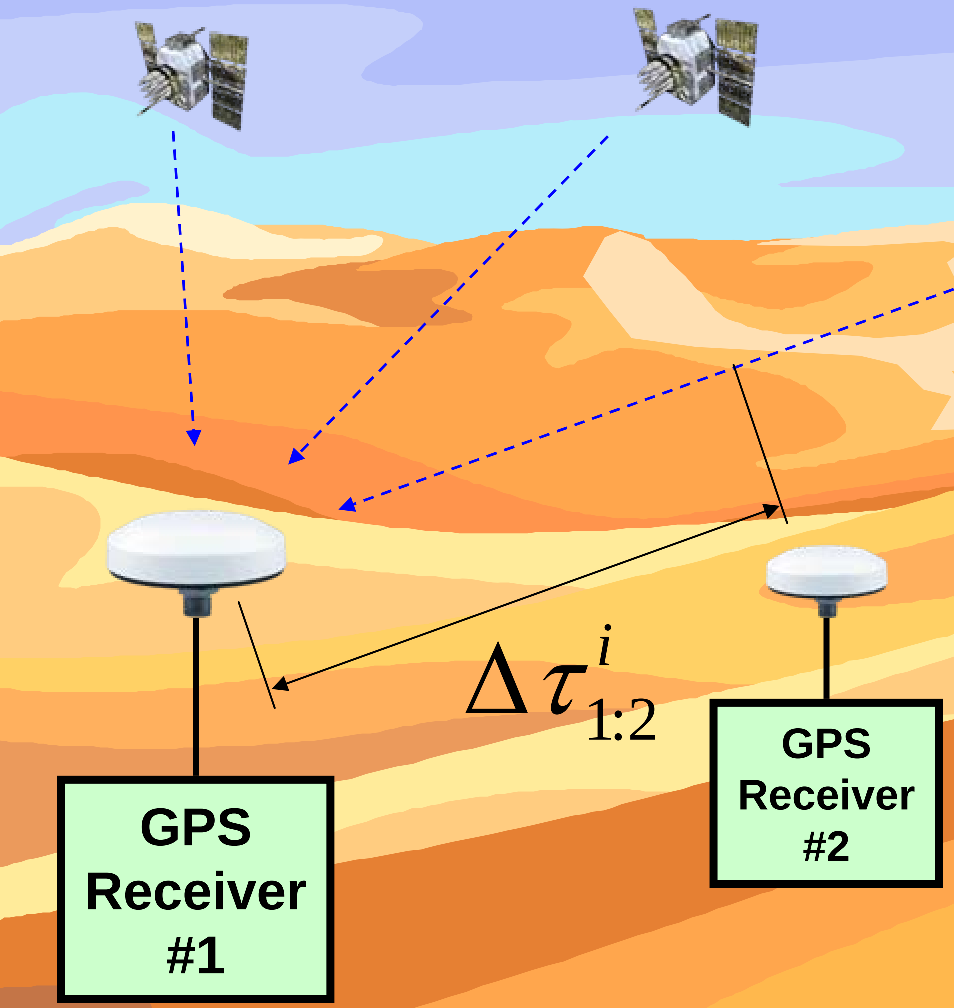
- Hemispherical patch at Remote Station and at Authentication Server

GPS Signal Authentication: Minimum Signature Payload Size

- Shown here: 4800 bits
  - 23.68 MHz sampling
- Projected: 3000 bits
  - 15 MHz sampling will not lose much P(Y) spectral energy
  - 1ms correlation client-to-server
  - 1-bit I/Q samples
  - 15 MHz * 0.001 sec * 1-bit/word * 2 IQ words/sample = 3000 bits
- Hemispherical patch at Remote Station
- 1.8m dish at Authentication Server



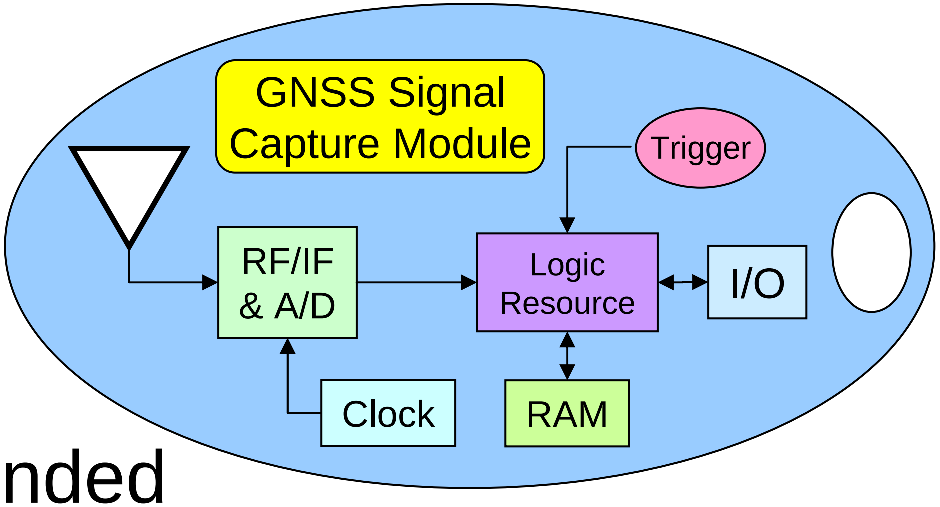
Authenticated GPS Signals for Location Verification



- Correlation peak from a single satellite identifies time to <1second
  - P(Y)-code is non-repeating
- Time differences for several satellites allows irrefutable position computation
  - Analogous to carrier-phase differential positioning

- The GPS RF signature is a location & time specific digital watermark

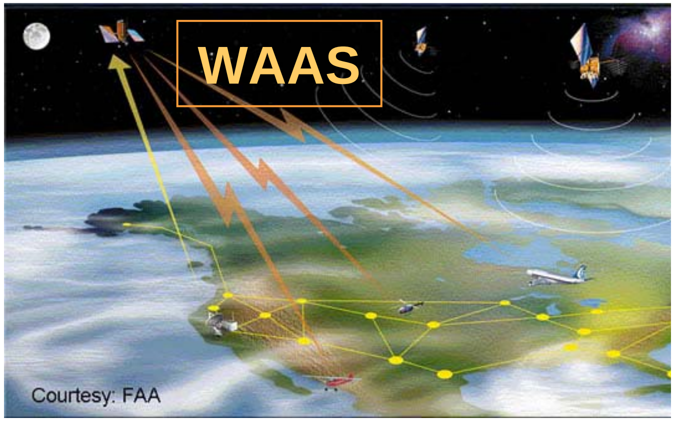
GPS Authentication & Security: Reference Architecture for User Device



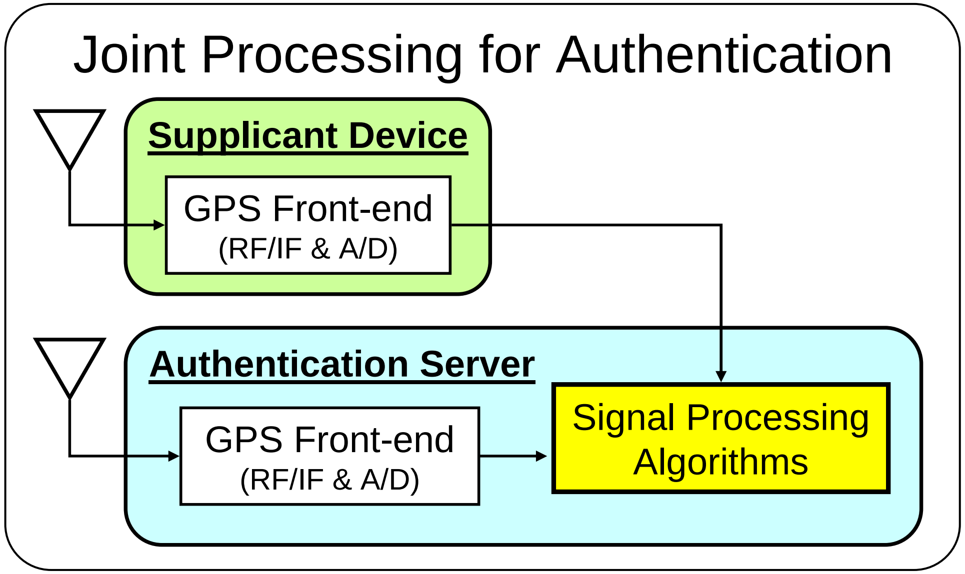
- Signal authentication and location verification for civil GNSS users
- Open architecture does not rely on trusted or bonded navigation and security module
- Server-based computation means seamless migration to modernized GNSS signals
- Minimizing hardware and processing in the User Device improves cost, size, and power consumption

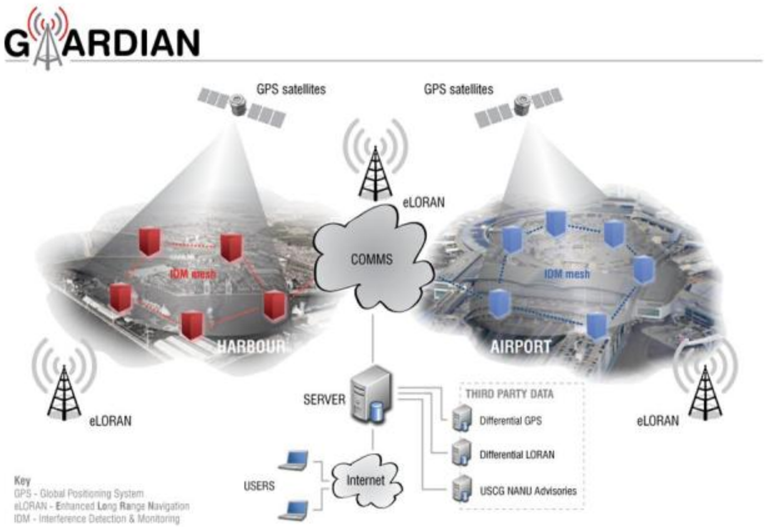
Trusted Navigation: Several Strategies to Verify the Utility

- Intra-system consistency checks
  - RAIM, GBAS/SBAS, DOA, etc.
- Inter-system consistency checks
  - GPS, INS, Wi-Fi, TV, eLoran, etc.
- Digital signatures and encryption
  - P(Y), M-code, Galileo PRS



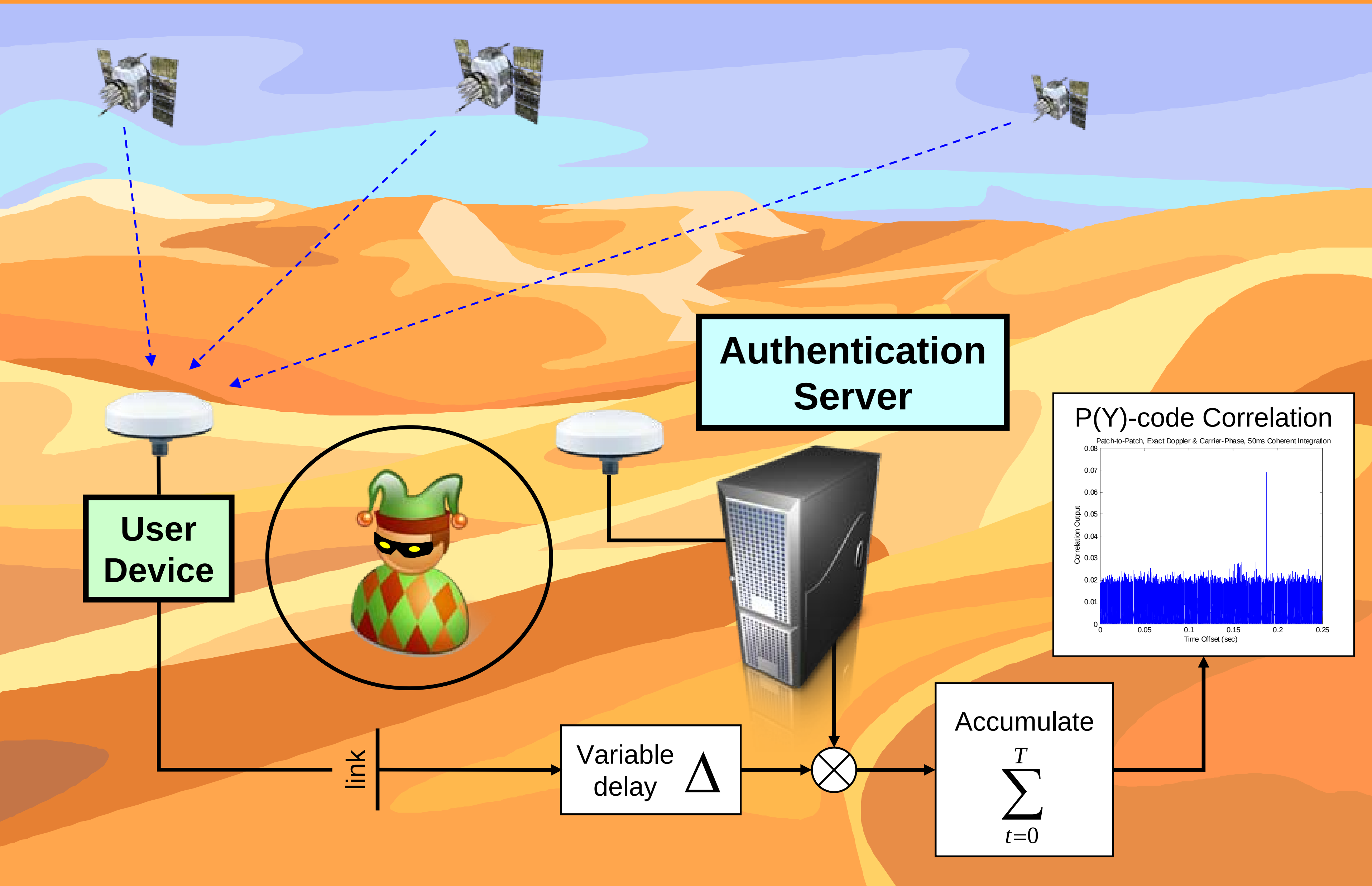
– image courtesy FAA





– image courtesy GPS World

GPS Signal Authentication:
How Might an Attacker Operate?



Attack #1 – Denial of Service

- RF jamming that denies GPS navigation & time service to all users in a region
  - As GNSS becomes a critical infrastructure asset, deliberate denial-of-service attacks *will* occur
  - We are researching other mitigation options – smart antennas, robust tracking loops, aiding techniques …
  - Signal authentication *per se* is not focused on anti-jam
- RF jamming that specifically targets the Authentication Server
  - Robust anti-jam measures can be employed here
  - This high-value service justifies extensive (and expensive) facility hardening

Attack #2 – Proximity or Replay

- Get "close enough" to authorized location for attacker to observe *bona fide* GPS signatures
  - Physical security, access control, and surveillance
- Collect valid GPS signatures, replay at later date
  - P(Y)-code signature is essentially non-repeating (*we have not analyzed the P(Y) sequences or encryption*)
- Several attacking stations observe satellites and then synthesize a valid P(Y)-code signature
  - Attacker is using noisy synthesized signals
  - Authentication Server shortens the correlation window

Attack #3 – Sequencing of W-code

- Attacker employs a collection of high-gain directional antennas or a beamsteering array, allows direct observation of P(Y)-code signals
  - Requires more gain than a simple 2m dish provides
  - If the attacker seeks only a noisy estimate of P(Y), then the Authentication Server can counter with its own beamsteering array and shorten the correlation window (reducing processing gain)
  - If the attacker seeks a reliable estimate of P(Y), then they are expending significant $$ – security practice teaches us that the resource being secured should be cheaper than the cost to compromise it

Attack #3 – Sequencing of W-code

- Attacker employs a collection of high-gain directional antennas or a beamsteering array allows direct observation of P(Y)
  - Requi…

The attack vectors against this authentication technology are boxed into methods that can be studied analytically and countered via signal processing

…seeks a reliable estimate of P(Y), then they are expending significant $$ – security practice teaches us that the resource being secured should be cheaper than the cost to compromise it

GNSS Security Architecture: Summary of Method

- Processes signals received simultaneously at two locations
  - The presence of a P(Y)-code correlation peak authenticates the signal, since an adversary cannot replicate the encrypted CDMA sequence.
  - Correlation peak timing for several satellites verifies the location
  - Works with other signal structures – especially those specifically designed for security and communications
- The GPS signature is an *irrefutable digital watermark*
- Available and demonstrated now with today's GPS signals; improves as GNSS constellations continue to evolve
  - Simple low-cost user hardware needs no refresh for new signals
  - Bulk of heavy processing occurs at hardened security stations

Conclusion

- Methods of signal authentication and location verification give us:

  ➡ *Security for navigation*

  ➡ *Security from navigation*

An Enabling Architecture for High-Security Applications