CS 925

Lecture 23

Time Synchronization Security

Thursday, April 25, 2024

Time transfer protocols

- Software-only solution:

  Network Time Protocol (NTP)

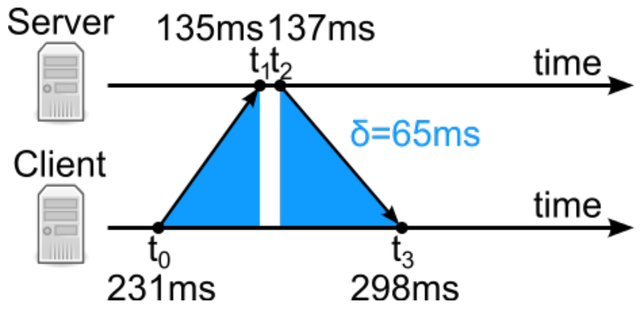
- Hardware-assisted solutions:

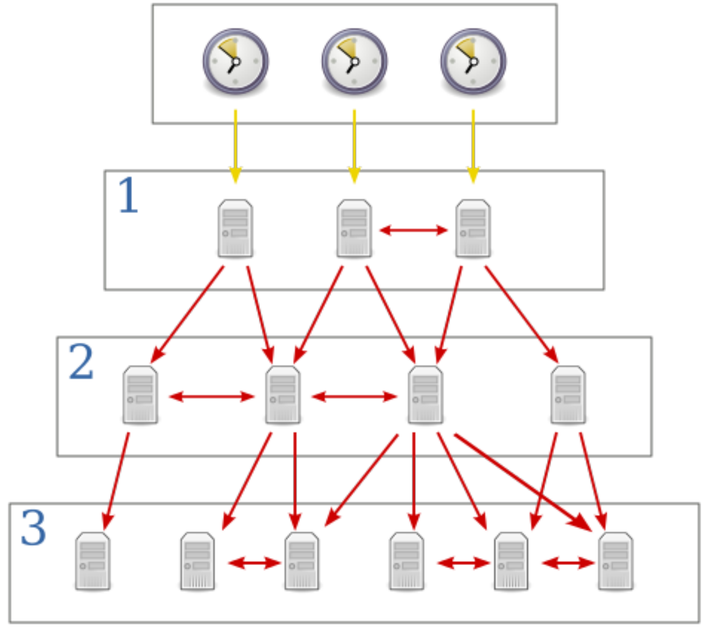
  IEEE 1588 Precision Time Protocol (PTP)

  White Rabbit

NTP

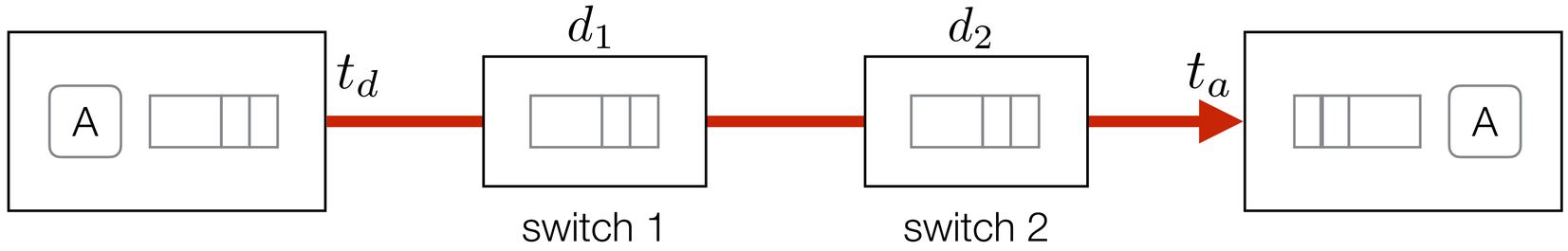
- Network Time Protocol (NTP)
- One of the fundamental Internet protocols
- Current version (NTPv4): RFC 5905 is from 2010
- Clock strata
- Implemented and enabled by default by most operating systems



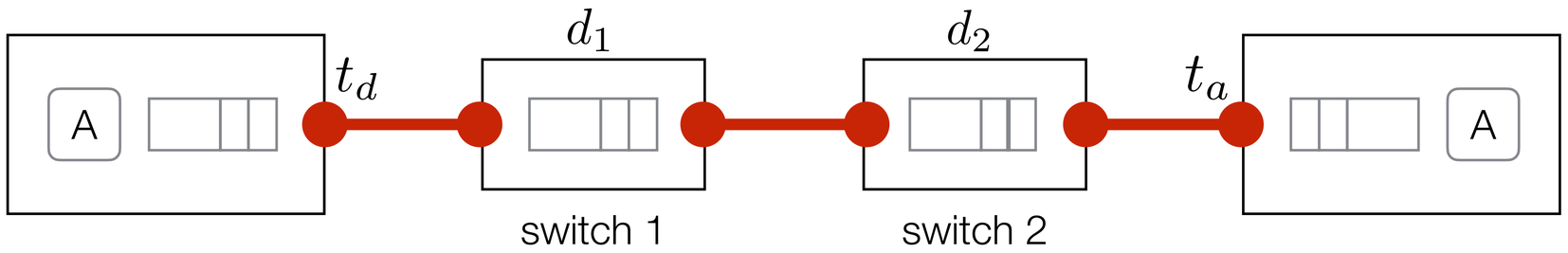


IEEE Std 1588

- Precision Time Protocol (PTP)
  - initial version: IEEE Std 1588™-2002
  - “current” version: IEEE Std 1588™-2008 (a.k.a. v2)
  - new version: IEEE Std 1588™-2019 (a.k.a. v2.1)
- Takes advantage of hardware support
  - precise packet arrival and departure timestamp
  - allows for compensation of delay encountered within a switch



IEEE Std 1588



- Link latency:
  - "constant" on links
  - variable at endpoints and switches due to queueing
- Variable components can be eliminated:

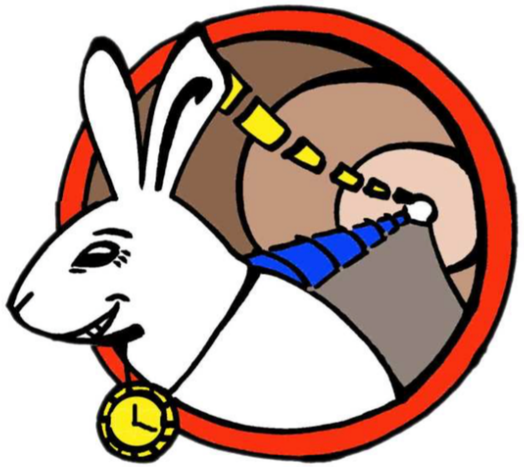
$$t_a - t_d - \sum_{i=1}^{N} d_i$$

Key Components

- Node types (“clock” = IEEE Std 1588 aware node)
  - ordinary clocks (OC)
  - boundary clocks (BC)
  - transparent clocks (TC)
- End to End (e2e) and Peer to Peer (p2p) modes
- Use of multicasting
- MAC or IP as underlying protocols
- Best Master Clock (BMC) algorithm
- Application domain specific profiles

White Rabbit

- A project from CERN, supported in the latest version of IEEE Std 1588
- Goals: sub-nanosecond accuracy, flexibility, predictability and reliability, robustness, open source hardware and software
- Means:
  - Synchronous Ethernet for syntonization
  - IEEE 1588 Precision Time Protocol



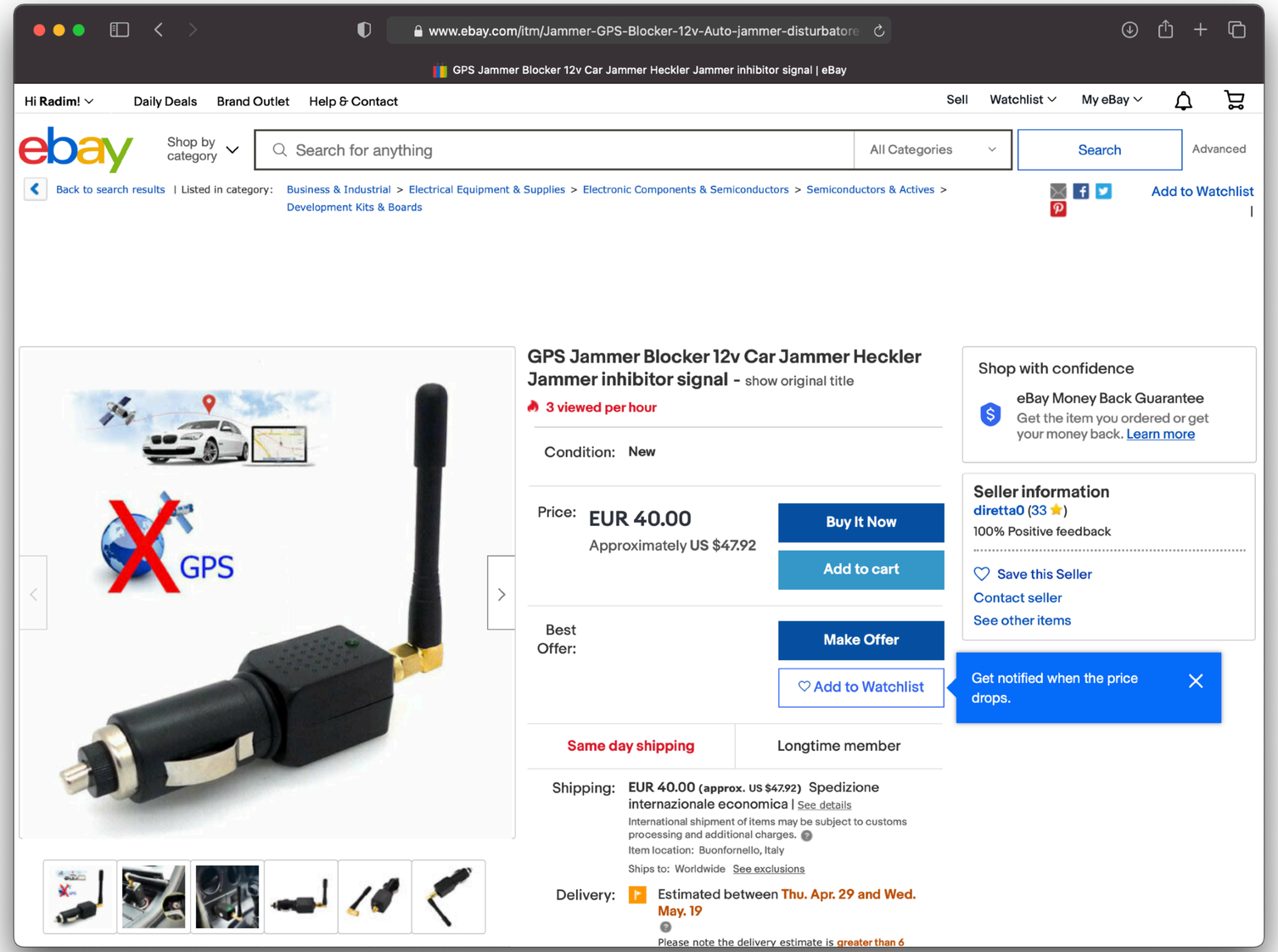
Achievable accuracy

- Continental distances:
  - GNSS (GPS, Glonass, BeiDou, Galileo): 1 µs is easy, 50 ns is possible, <10 ns very hard
  - NTP (Network Time Protocol): milliseconds
- Within a LAN:
  - IEEE1588: 1 µs easy, 50 ns with care, few ns hard
  - White Rabbit: 100 ps accuracy, 10 ps jitter

Timing Security

- Loss of precise time synchronization can have serious consequences:
  - disruption of the power grid, including physical damage
  - disruption of mobile networks
  - halted high-frequency securities trading
- Much of these systems depend on functioning GNSS (GPS):
  - bad idea: GPS signal is weak and can be jammed or even spoofed

From eBay…


www.ebay.com/itm/Jammer-GPS-Blocker-12v-Auto-jammer-disturbatore
GPS Jammer Blocker 12v Car Jammer Heckler Jammer inhibitor signal | eBay
Hi Radim!
Daily Deals
Brand Outlet
Help & Contact
Sell
Watchlist
My eBay
ebay
Shop by category
Search for anything
All Categories
Search
Advanced
Back to search results | Listed in category:
Business & Industrial > Electrical Equipment & Supplies > Electronic Components & Semiconductors > Semiconductors & Actives > Development Kits & Boards
Add to Watchlist
GPS
GPS Jammer Blocker 12v Car Jammer Heckler Jammer inhibitor signal - show original title
3 viewed per hour
Condition: New
Price: EUR 40.00
Approximately US $47.92
Buy It Now
Add to cart
Best Offer:
Make Offer
Add to Watchlist
Get notified when the price drops.
Same day shipping
Longtime member
Shipping: EUR 40.00 (approx. US $47.92) Spedizione internazionale economica | See details
International shipment of items may be subject to customs processing and additional charges.
Item location: Buonfornello, Italy
Ships to: Worldwide See exclusions
Delivery: Estimated between Thu. Apr. 29 and Wed. May. 19
Please note the delivery estimate is greater than 6
Shop with confidence
eBay Money Back Guarantee
Get the item you ordered or get your money back. Learn more
Seller information
diretta0 (33)
100% Positive feedback
Save this Seller
Contact seller
See other items

Timing Security - Solutions

- Fancy antennas and smart GNSS receivers
  - How about swarms of autonomous aerial GPS spoofers?
- Combine GNSS and network-based solutions
  - this is a good idea for other reasons…
  - but now we need to protect the protocol!

Securing Timing Protocols

- Attacks:
  - Packet manipulation
  - Spoofing
  - Replay attack
  - Rogue master attack
  - Interception and removal
  - Packet delay manipulation
  - L2/L3 DoS attacks
  - Crypto performance attacks
  - Time protocol DoS attacks

Securing Timing Protocols

- PTP-Integrated Security Mechanisms
  - adding security features to the timing protocols
- External Transport Security Mechanisms
  - using existing transport security (IPsec and MACsec)
- Architecture Guidance
  - robust and resilient deployment
- Monitoring and Management Guidance
  - mechanisms to detect problems