Vienna University of Technology
Distributed Systems Group
Information Systems Institute
A-1040 Vienna, Argentinierstrasse 8
http:/ / www.infosys.tuwien.ac.at/

TRADE

Trustworthy adaptive quality balancing through temporal decoupling

Motivation:

Auctioning of bonds is one of the finance systems with the highest volume in a single transaction. Therefore, these systems have to be highly dependable facing the following threats:

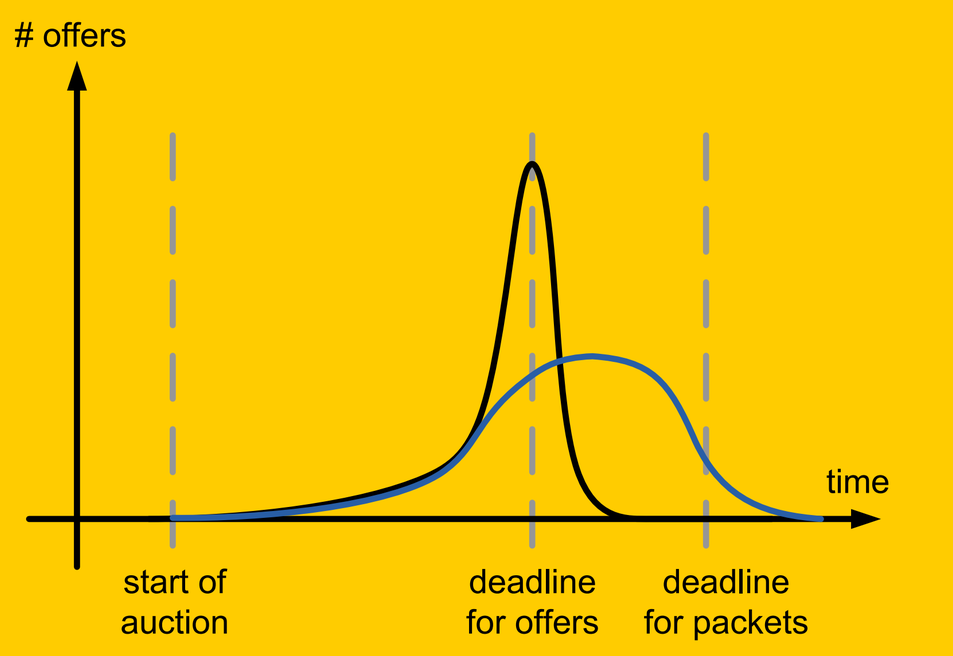
- Excessive load
- Node or link failure
- Security attacks

Solution approach:

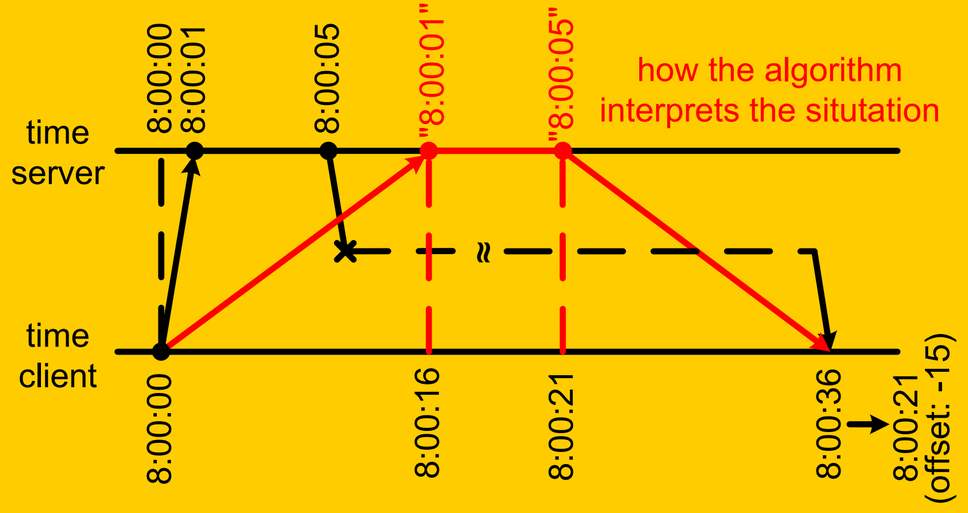
- Temporal decoupling
- Tamper-proof timestamps
- Secure client
- Secure clock synchronization protocol

Clock Synchronization:

- Typically, NTP is used.
- Middleman could arbitrarily delay messages and thereby delay (or advance) the clock.
- Probalistic clock synchronization algorithms guarantee better bounds with some probability.
- TRADE will contribute to new randomized approaches.



Clients deliver a vast amount of bids in the last seconds of an auction. Temporal decoupling allows for adaptive load balancing and fault tolerance—at the price of new security demands.



An adversary cheats the time synchronization algorithm.

Research Contributions:

- Optimal software partitioning between smart card and untrusted client.
- Secure time synchronization.
- Adaptive run-time balancing of dependability.
- Integration of dependability and security.

TRADE is supported by the FIT-IT – Trust in IT systems research programme under contract number 816143.

Duration: 1.02.2008-31.01.2010
Person months: 109

Website: http://www.dedisys.org/trade/