Protecting a Federated Database Infrastructure Against Denial-of-Service Attacks

Arne Ansper, Ahto Buldas,
Margus Freudenthal, Jan Willemson

Cybernetica, ELIKO

This research has been supported by EU through European Regional Development Fund

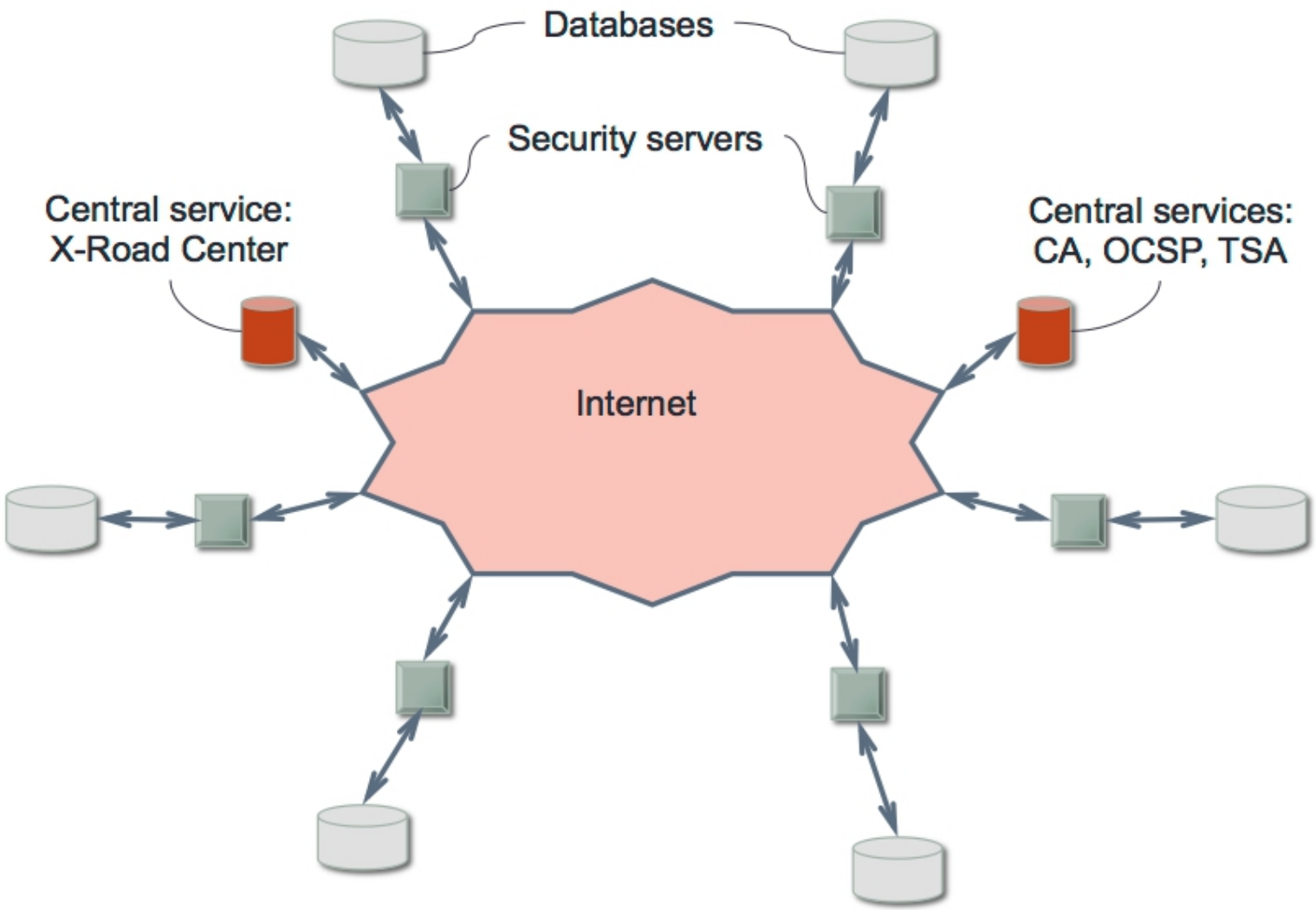
Federated Database Systems

- Federated Database System is a type of meta-database management system, which transparently maps multiple autonomous database systems into a single federated database
- The main security issues considered:
  - Integrity
  - Confidentiality
  - Access control
- Availability has typically lower priority
- However, as more and more services rely on federated databases, this issue can not be ignored any more

X-Road

- Developed in early 2000s as a common access layer for Estonian state databases
- Today, connects over 600 registers and mediates more than 300 million queries per year
- Was originally not meant to ensure high availability, but now provides access to several time-critical databases (law enforcement, medical, etc.)
- The goal of this paper is to propose availability enhancements for X-Road

X-Road Architecture

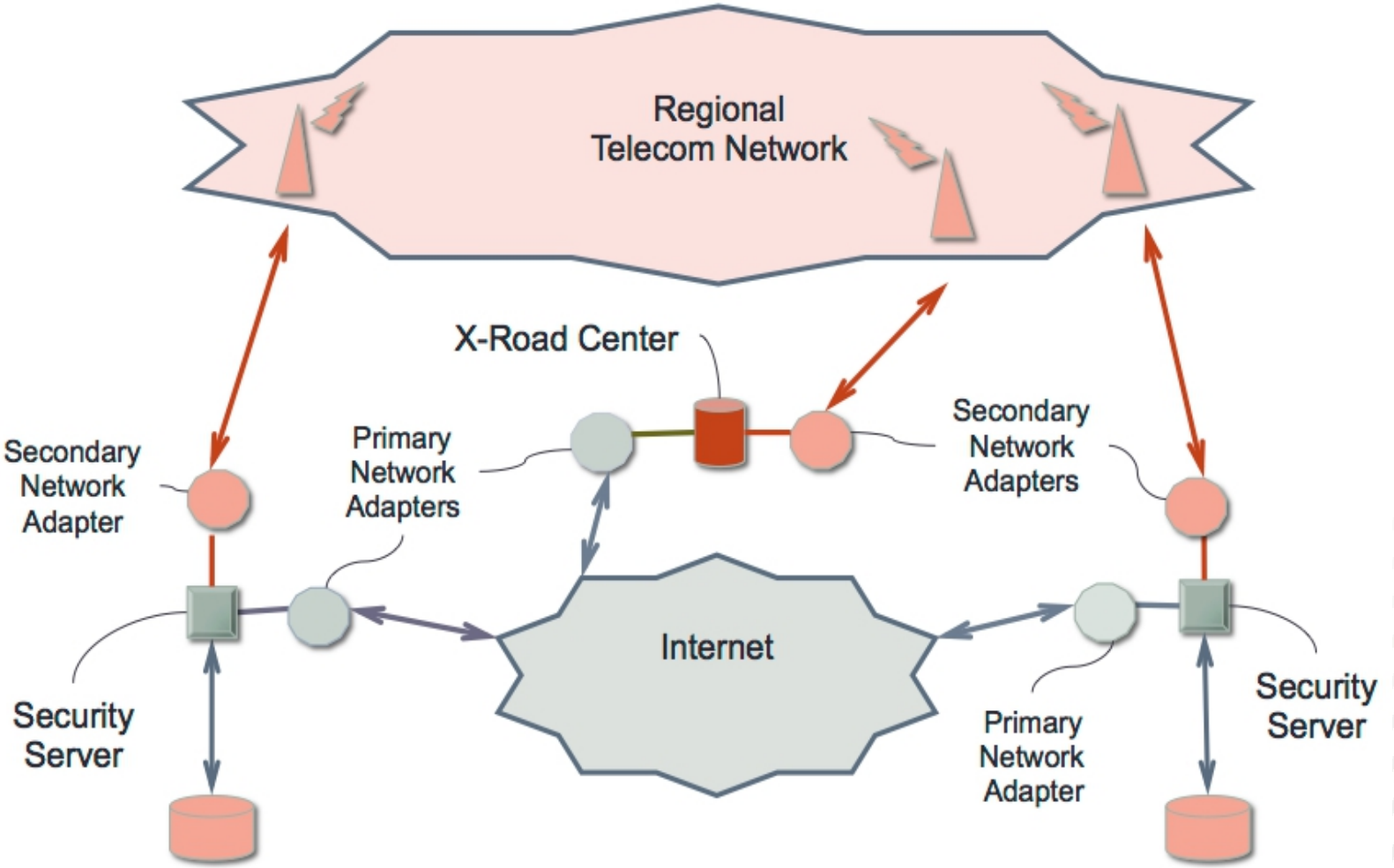


CYBERNETICA

Center-Independent Work

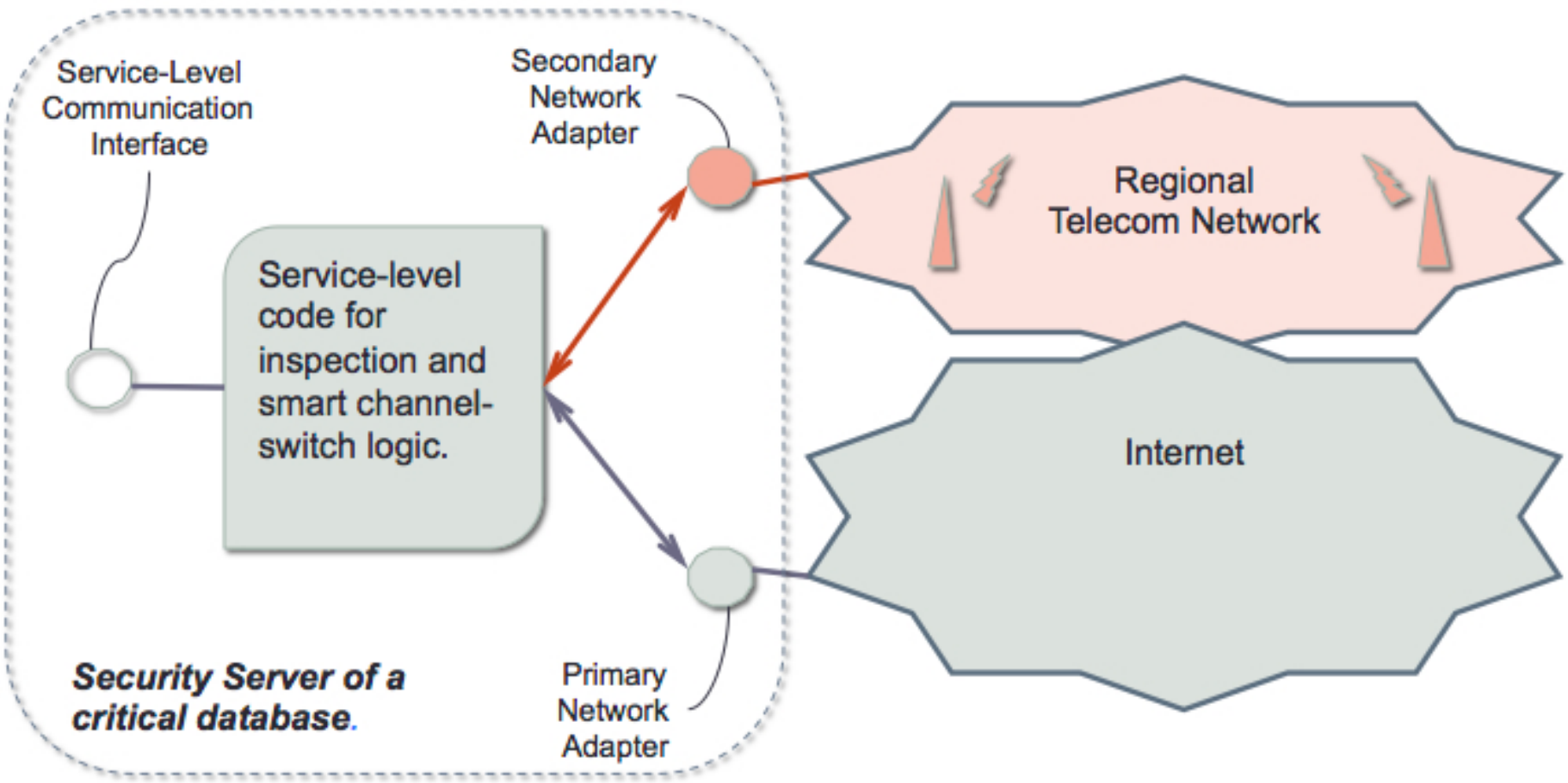
- The problem: currently, DNSSEC is used to propagate configuration and certificate validity information of X-Road servers
  - If the Internet access is blocked, the caches will expire, all the communication becomes untrusted and gets blocked
- Solution: Use OCSP responses and time-stamps instead
  - The responses can be cached on the client side
  - In case of the Internet failure, the time-stamping service becomes temporarily inaccessible, but time-stamps can also be taken later

Alternative Channels



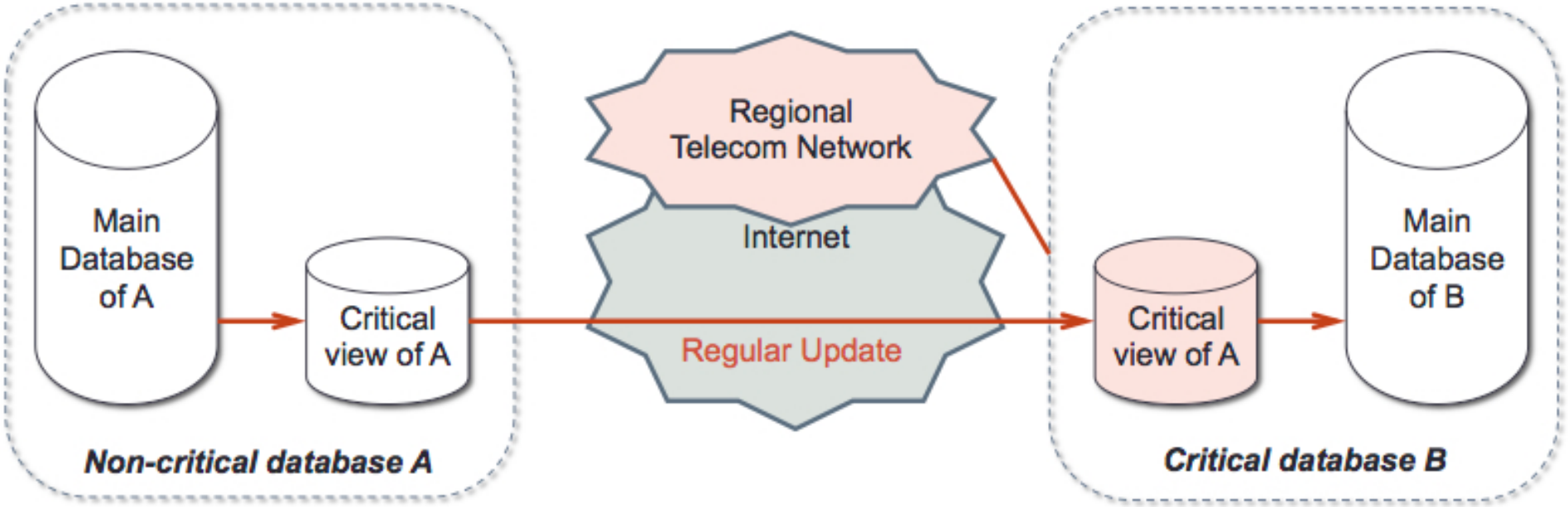
CYBERNETICA

Security Server Enhancement



CYBERNETICA

Database Replication



CYBERNETICA

Channel Switching Logic

- The servers have to ping each other regularly over all the channels between them
  - Check the health of channels
  - Determine whether a temporarily blocked channel has been freed
- The ping has to be replied via the same channel where it came from
- If a server determines a DoS attack on the main channel, it has to switch to the secondary one
- If a server does not detect a DoS attack itself, but the other server does not reply to the main channel pings,the server has to switch to the secondary channel
- When while using the secondary channel the other server starts replying to the main channel pings, switch back

CYBERNETICA

CYBERNETICA