Access Control on Multiprotocol Networks

T2TRG - IETF 93
18 July 2015

Pablo Puñal Pereira
pablo.punal@ltu.se

Department of Computer Science, Electrical and Space Engineering
EISLAB

Luleå University of Technology

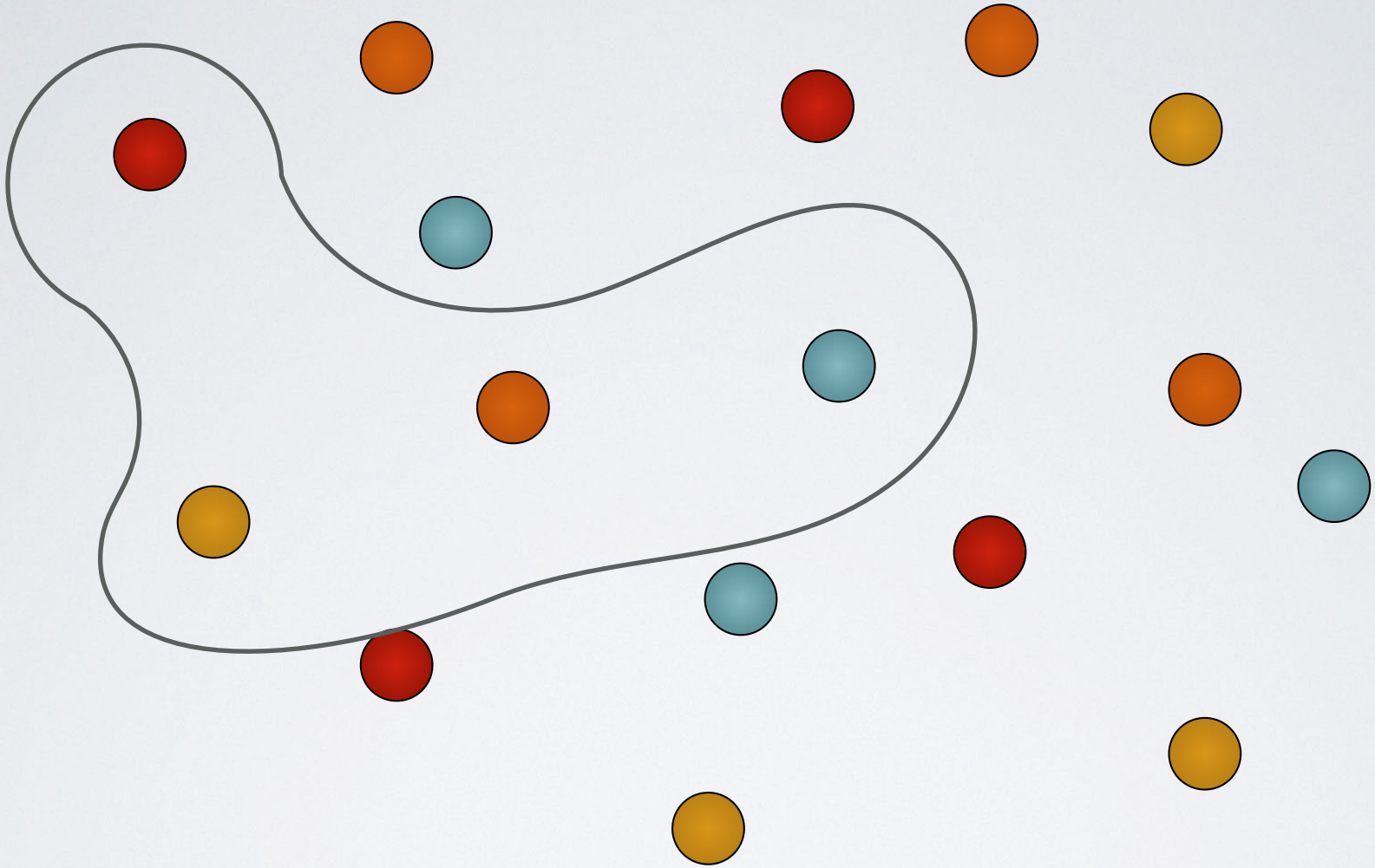
Arrowhead project

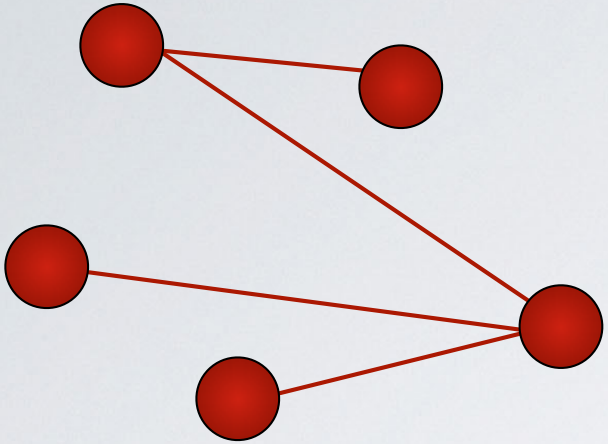
Outline

- Why
  - Arrowhead Introduction
    - Translation Service
  - Multiprotocol communication issues
- Requirements
- Current Solution
  - Architecture
  - How it works
- Results (demo with CoAP protocol)
- Limitations
- Future Work

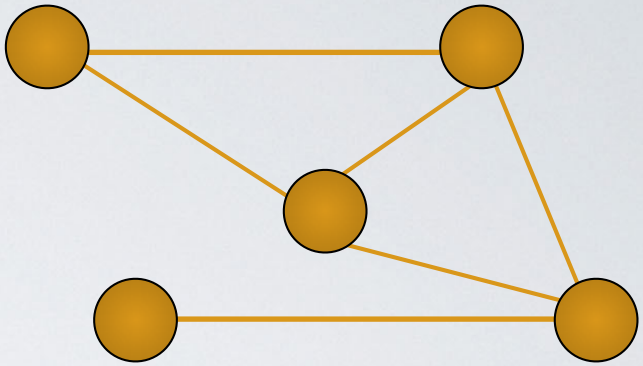
Arrowhead project

www.arrowhead.eu





Translator

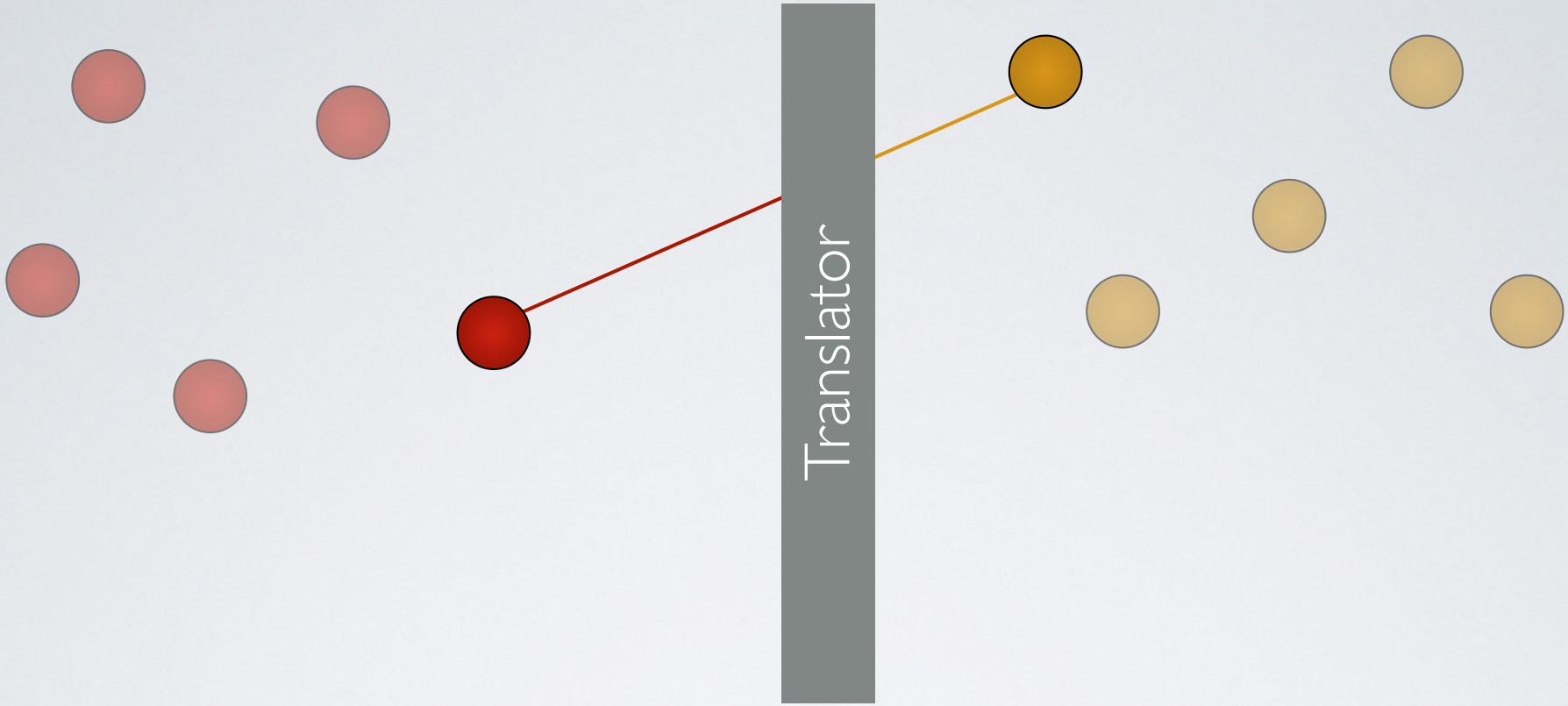


Network A

- Protocol A
- Security Type A
- Access Control A

Network B

- Protocol B
- Security Type B
- Access Control B



Interoperability

- Protocol Level
- Semantic Level
- Coding Level

Problems

- Man in the Middle
- No end to end Security
- How to fit ticket on each protocol
- Encrypted Payload

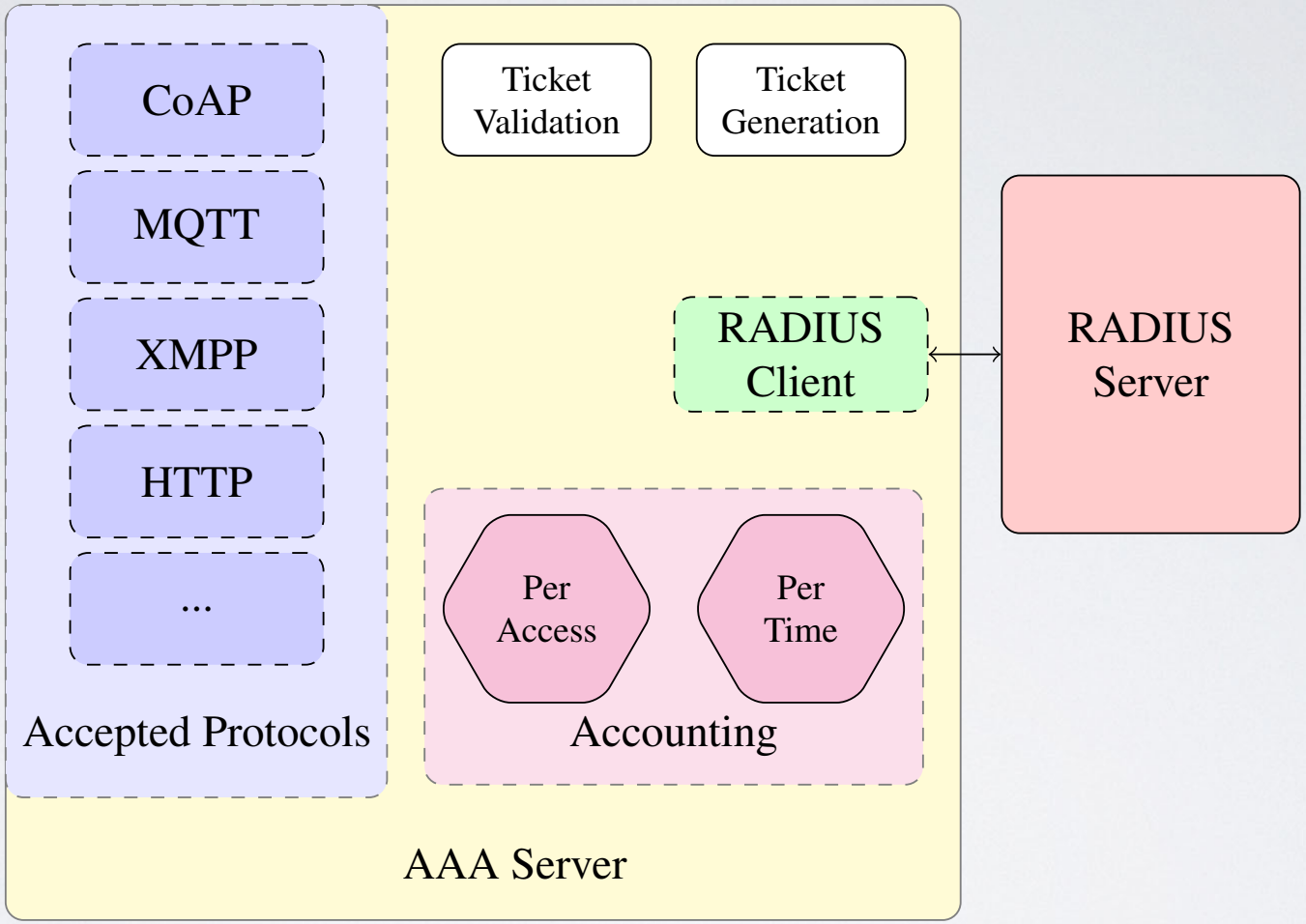
Requirements for Access Control

- Supported by all involved devices
- Devices with different performance
  - Special care of low power constrained devices
    - No complex processing
      - ✓ Compromising the low power criteria
      - ✓ Introducing latencies during the communication
    - Mitigate additional overhead
      - ✓ Increasing the communication usage
      - ✓ Increasing the computation
    - Reduce extra communication
      - ✓ Keeping the low power criteria
      - ✓ Keeping the network performance

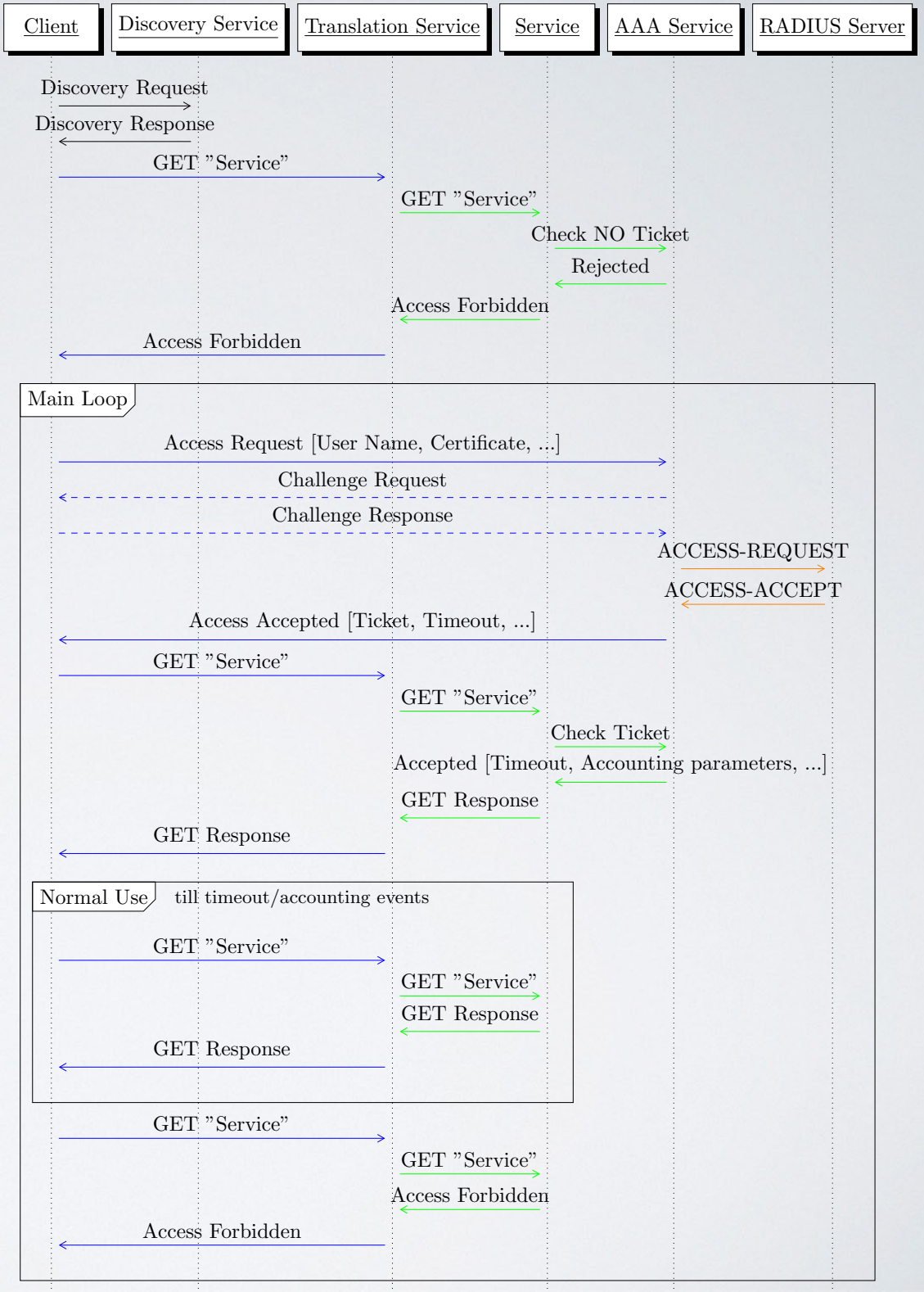
Proposed Solution: Tickets

- Ticket just as an ID, no extra information inside
- Add it to each protocol
- Flexible size
- Static / Dynamic
- Timeout validation
- Supports Accounting
- Supports Network Monitoring

AAA Server Architecture



How it works?


Client
Discovery Service
Translation Service
Service
AAA Service
RADIUS Server
Discovery Request
Discovery Response
GET "Service"
GET "Service"
Check NO Ticket
Rejected
Access Forbidden
Access Forbidden
Main Loop
Access Request [User Name, Certificate, ...]
Challenge Request
Challenge Response
ACCESS-REQUEST
ACCESS-ACCEPT
Access Accepted [Ticket, Timeout, ...]
GET "Service"
GET "Service"
Check Ticket
Accepted [Timeout, Accounting parameters, ...]
GET Response
GET Response
Normal Use
till timeout/accounting events
GET "Service"
GET "Service"
GET Response
GET Response
GET "Service"
GET "Service"
Access Forbidden
Access Forbidden

Demo

InfoCoAP Server

- "info" resource

coap://projects.punyal.com

AAA Server

Modified Cupper Client

Network Monitor

http://security.punyal.com

Limitations

Future Work

Thanks for your attention