ERICSSON

ACTUATORS AND CYBERPHYSICAL SYSTEMS

DRAFT-MATTSSON-CORE-COAP-ACTUATORS

MATTSSON, FORNEHED, SELANDER, PALOMBINI

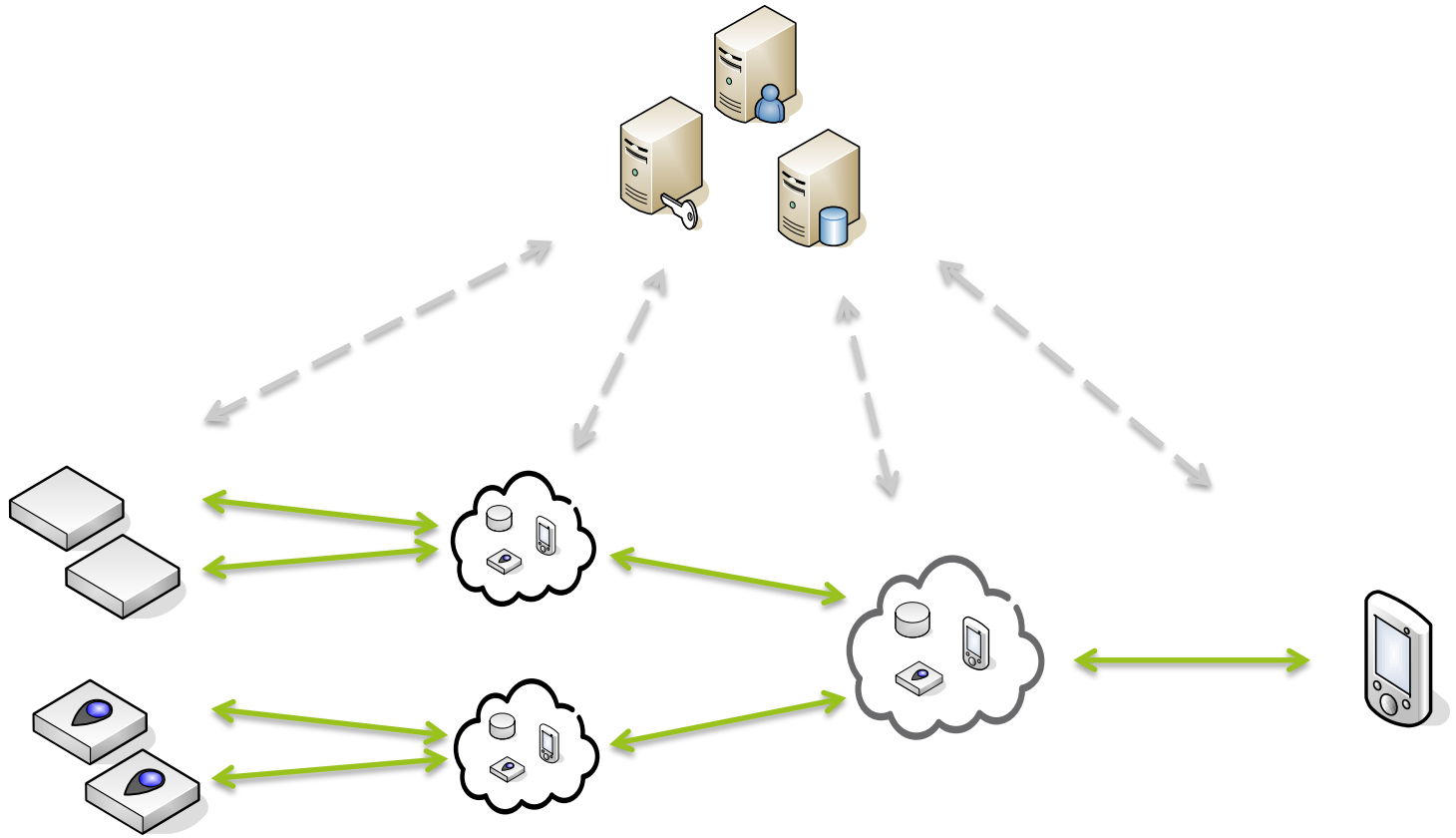
IRTF T2TPRG, OCT 31 2015

ERICSSON

BACKGROUND

SECURITY AND PRIVACY FOR IOT SENSORS IS COMPLEX

- The *store-and-forward* and *publish-subscribe* architectures rely on middle boxes.
- As DTLS only offers hop-by-hop security, fully trusted intermediaries are necessary.
- e2e security mechanisms needed.

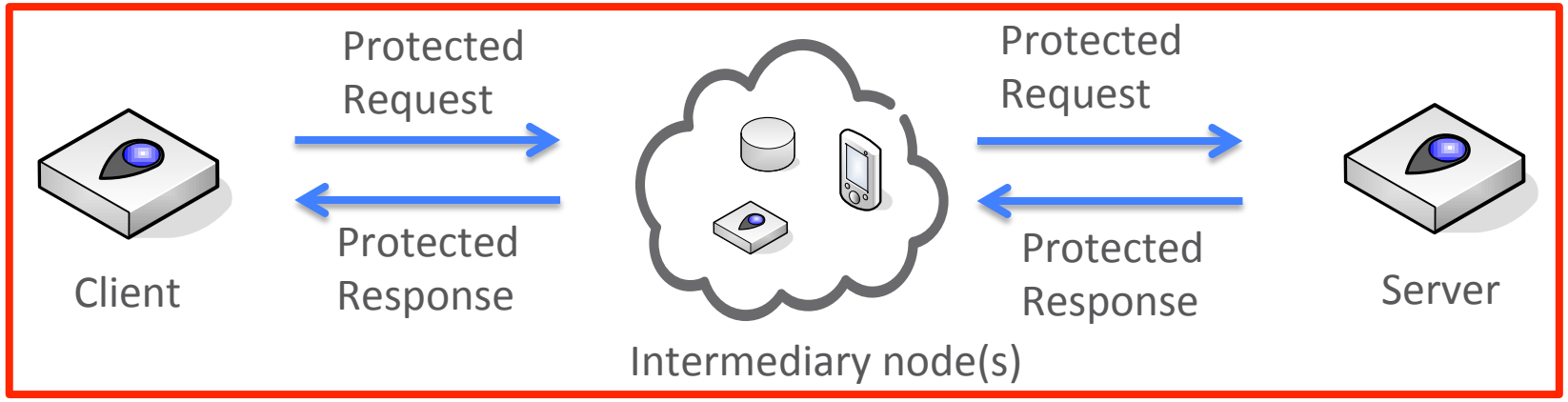


E2E SECURITY OVER MIDDLEBOXES

Object Security: More details in draft-selander-ace-object-security.

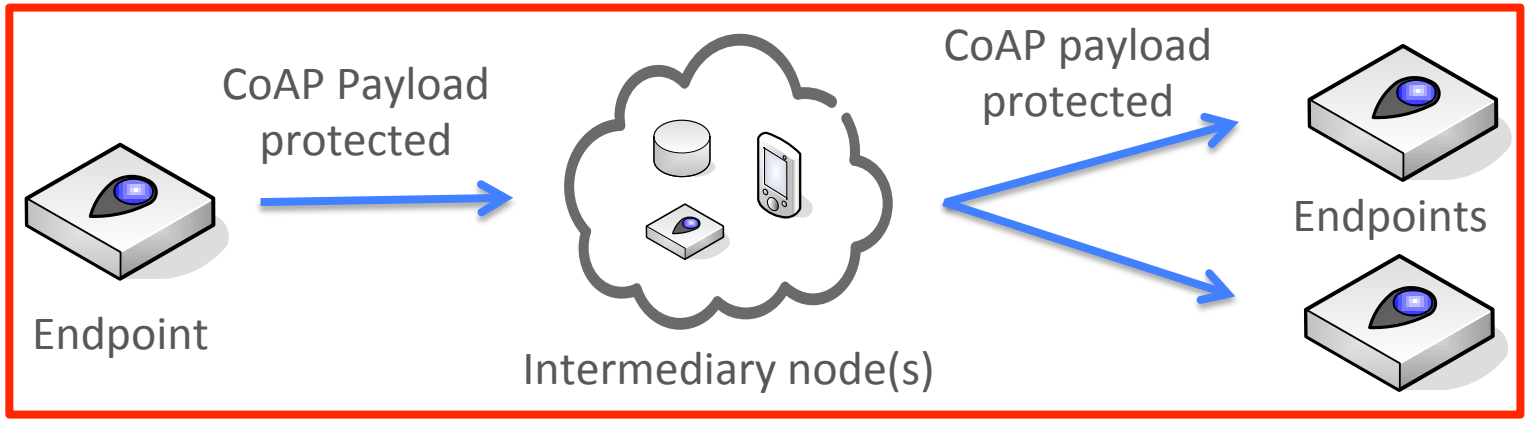
OSCOAP

- CoAP Option that protects CoAP request-response
- Supports store-and-forward



OSCON (COSE)

- Protects CoAP Payload only
- Supports publish-subscribe



REQUEST-RESPONSE MATCHING IN COAP, DTLS, AND OSCOAP

CoAP

› Response-request matching is done with hbh token

DTLS

› "Independent" sender and receiver contexts.
No binding between request and response.
Responses can typically be **delivered out-of-order**.

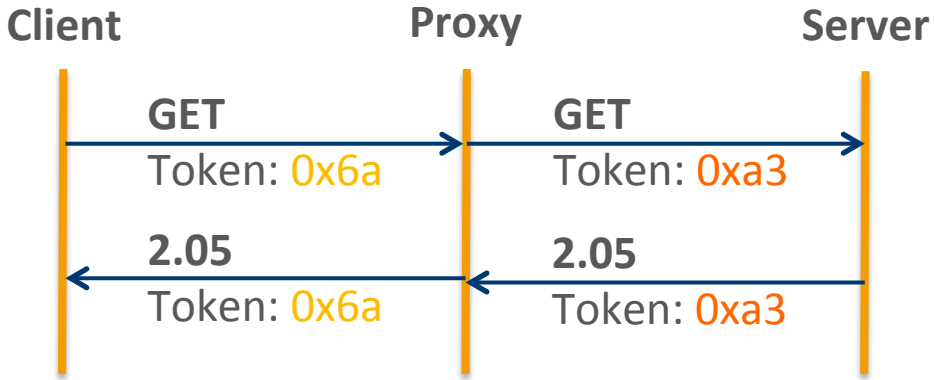
CoAP over DTLS

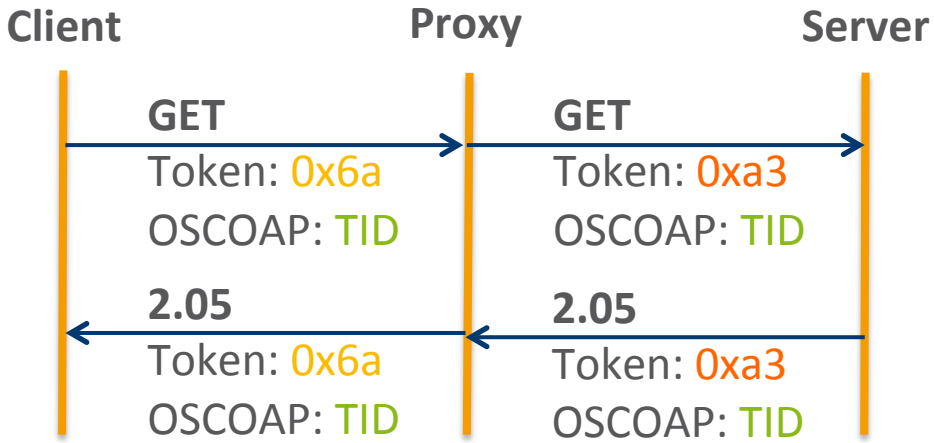
› CoAP RFC says that tokens currently "in use" SHOULD (not SHALL) be unique.

› **Less strict** profiling of token when used with DTLS.
  – **This leads to serious attacks**.

CoAP with OSCOAP

› e2e Transaction ID (TID) provides request-response binding.





ERICSSON

ATTACKS

Assumptions:

- Attacks are performed by an on-path attacker, not a “trusted” middle box.
- CoAP is protected with a security protocol such as DTLS or OSCOAP.

BLOCK ATTACK

- Blocking sensor messages is just DoS.
- Blocking actuator messages results in the client losing information.
- Is the door locked or unlocked?
- Remedy: Inform user.

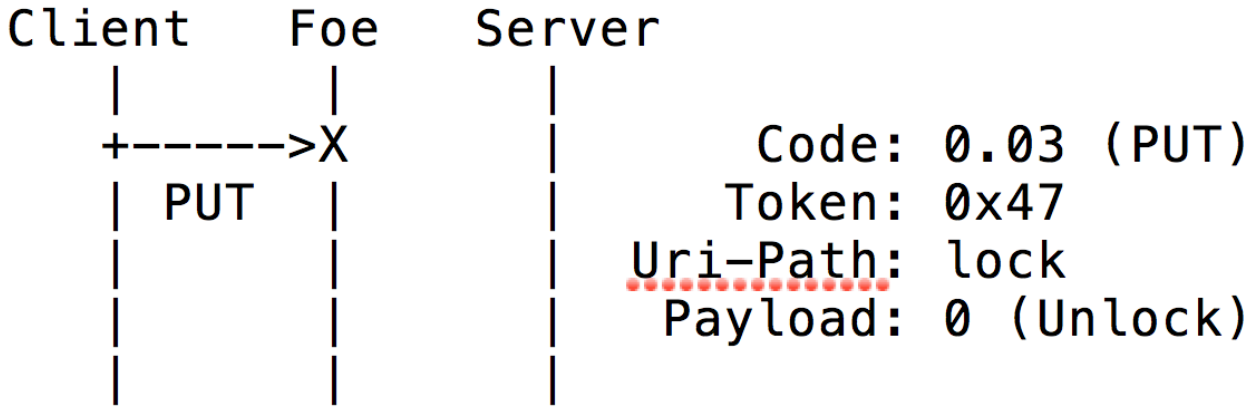


Figure 1: Blocking a Request

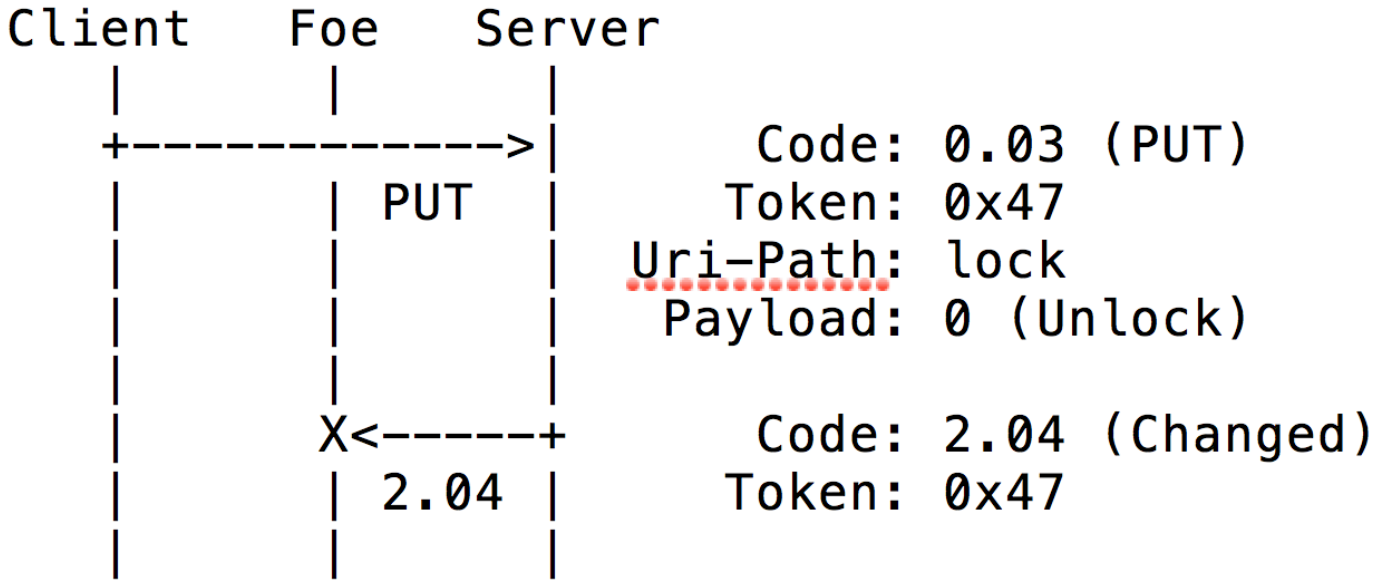


Figure 2: Blocking a Response

DELAY ATTACK (1/2)

- An attacker can delay the delivery of any packet (request or response) by a chosen amount of time.
- The attacker can control the replay window.
- Attacker can e.g. unlock a door at a given time.

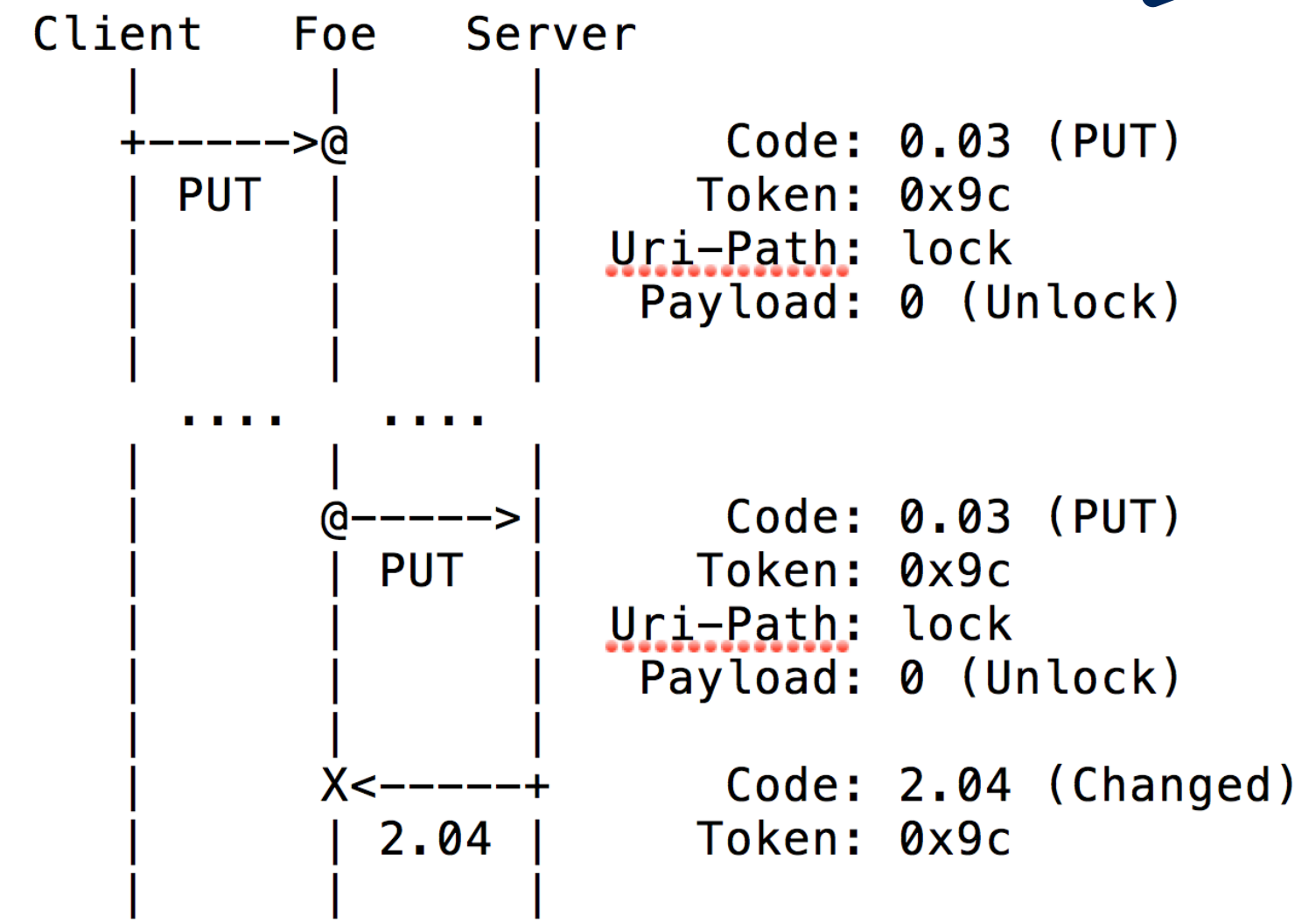


Figure 3: Delaying a Request

DELAY ATTACK (2/2)

- **Reordering**: If a non-zero replay window is used, the attacker can let the client interact with the actuator before delivering the delayed request.

- Remedy: New CoAP option: The Repeat Option

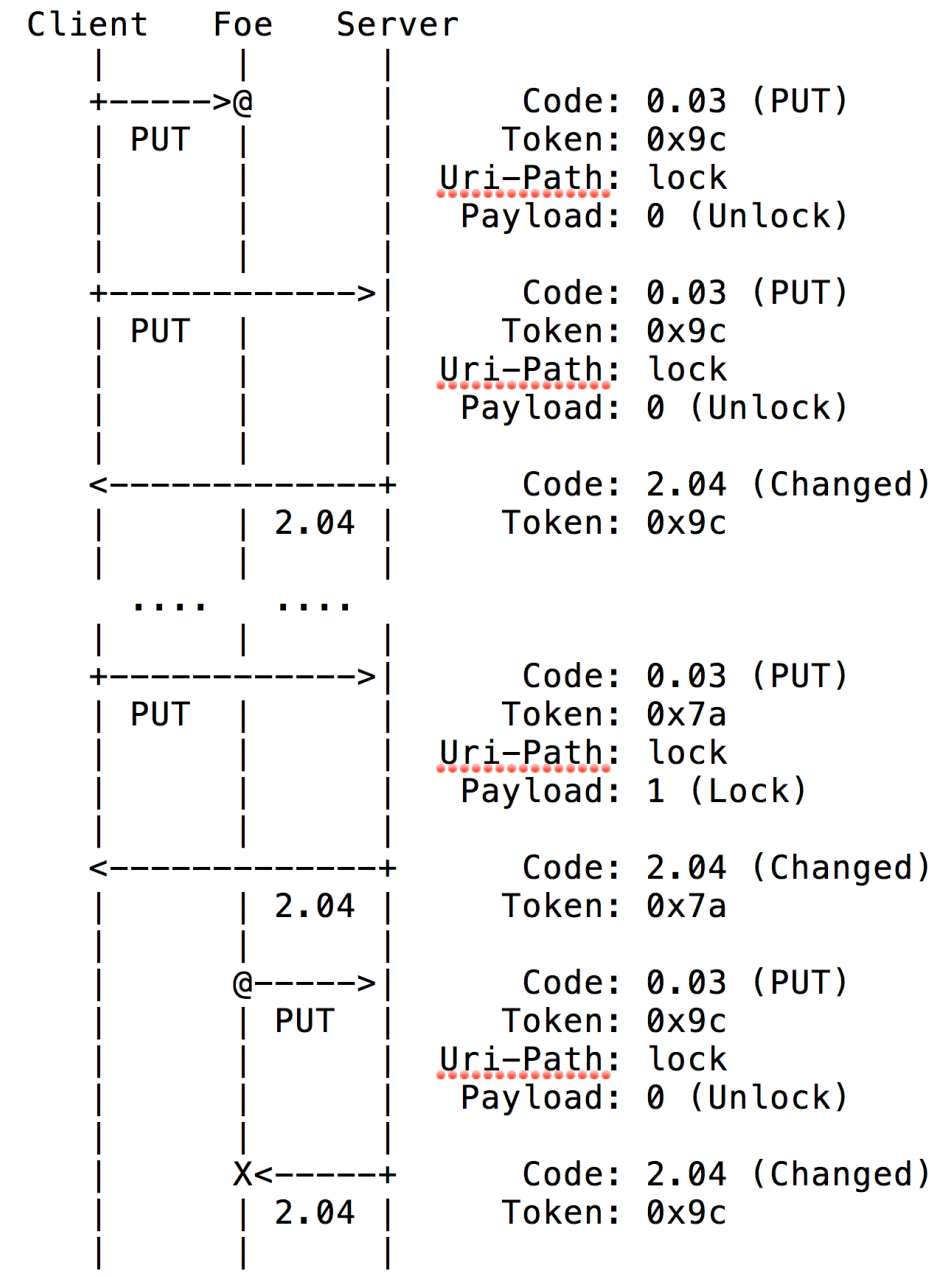


Figure 4: Delaying Request with Reordering

MISMATCH ATTACK (1/3)

- Possible if CoAP is protected with DTLS (but not OSCOAP).
- The client needs to reuse the same token.
- The attacker can still control the replay windows.
- Attacker can e.g. fool client to believe a door has been locked.

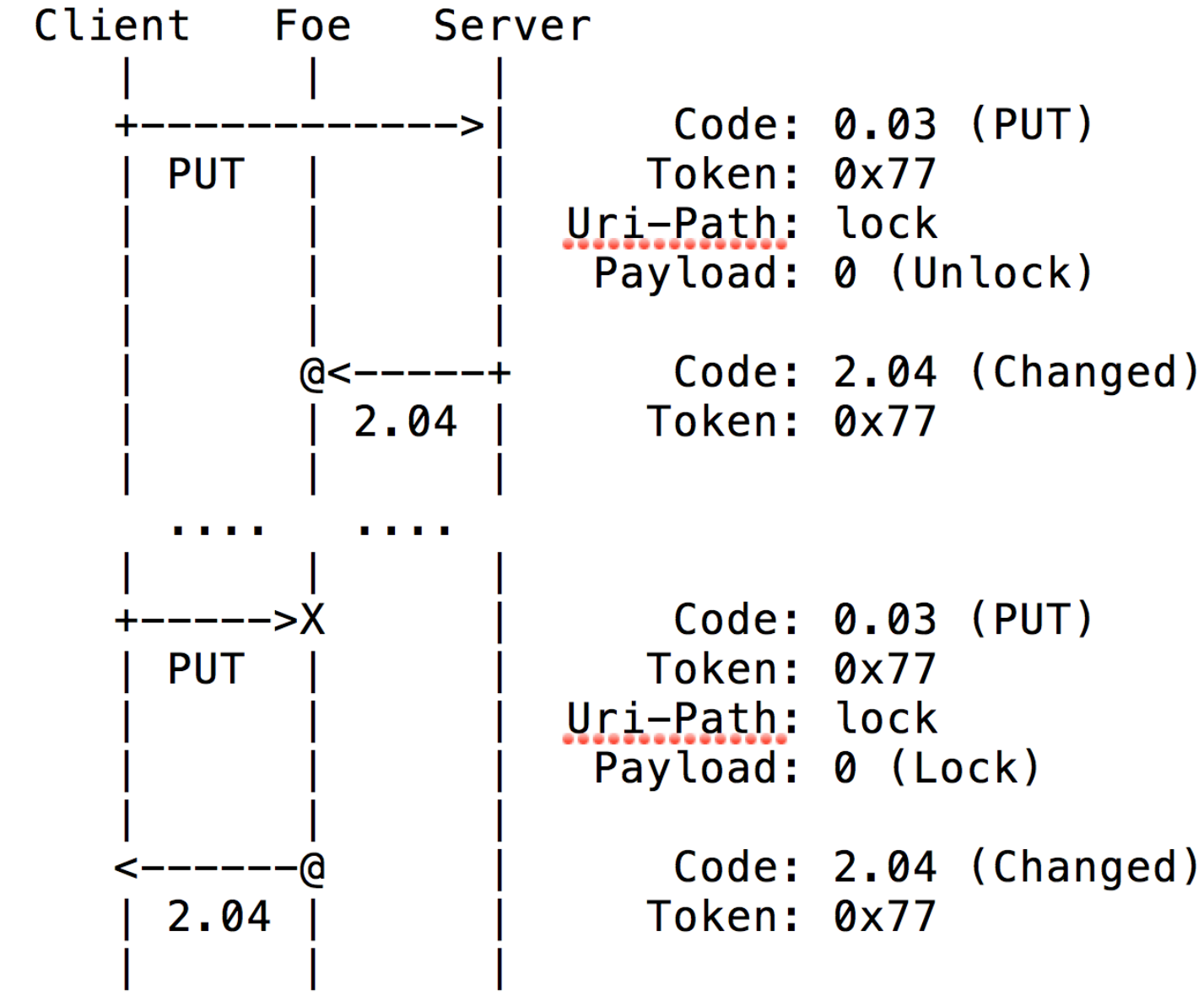


Figure 5: Mismatching Response to PUT

MISMATCH ATTACK (2/3)

- Attack is also valid for sensors. Also here with serious consequences.

- Attacker can e.g. fool client to believe a door is locked.

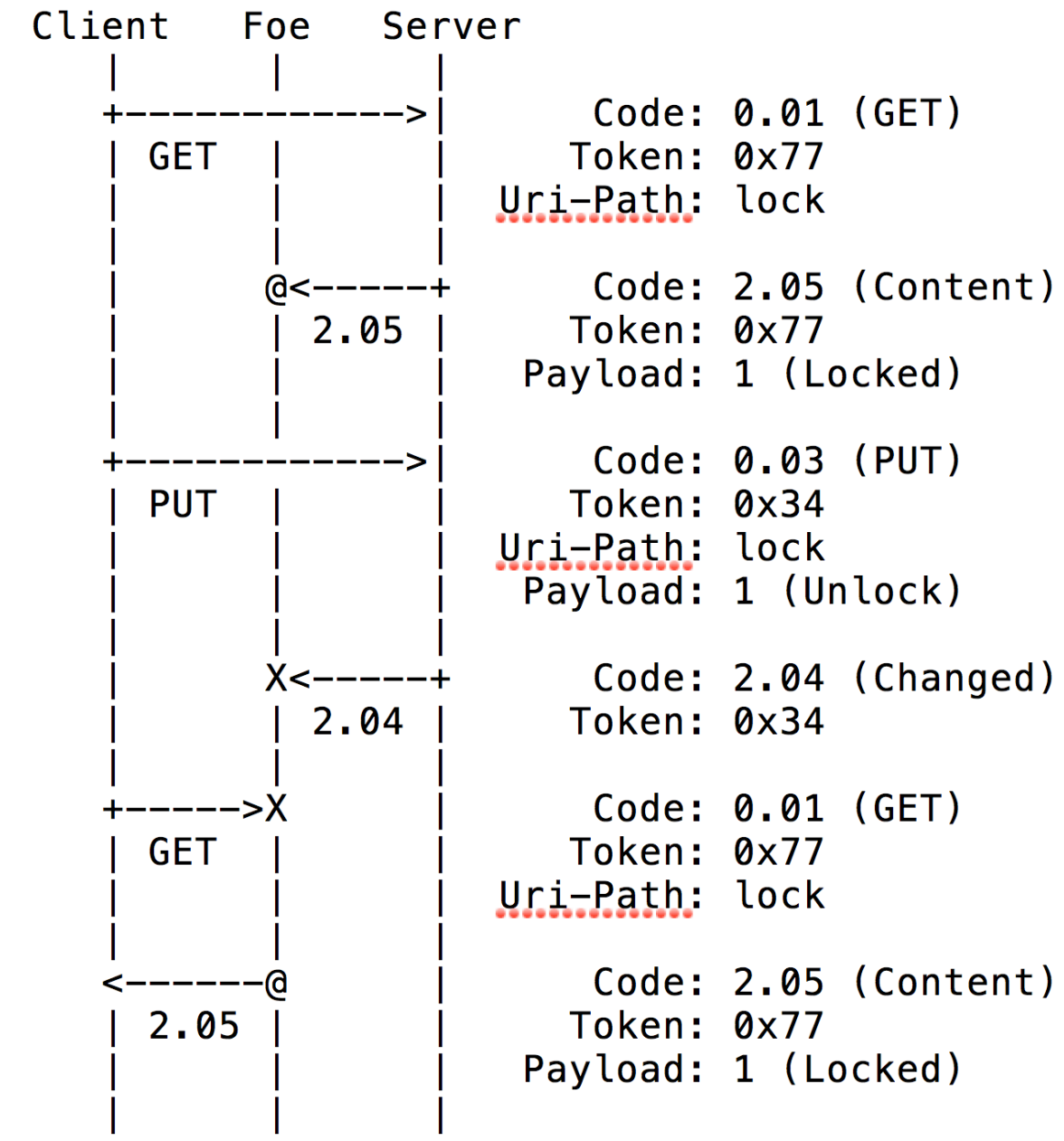


Figure 6: Mismatching Response to GET

MISMATCH ATTACK (3/3)

- Attacker can even mix responses from different resources if the resources share the same DTLS connection **on some part of the path.**
  - Located behind a common gateway
  - Served by the same CoAP proxy.
- Example: Attacker makes client believe the house is on fire.
- Remedy: Never reuse tokens (which the client has not received responses to).

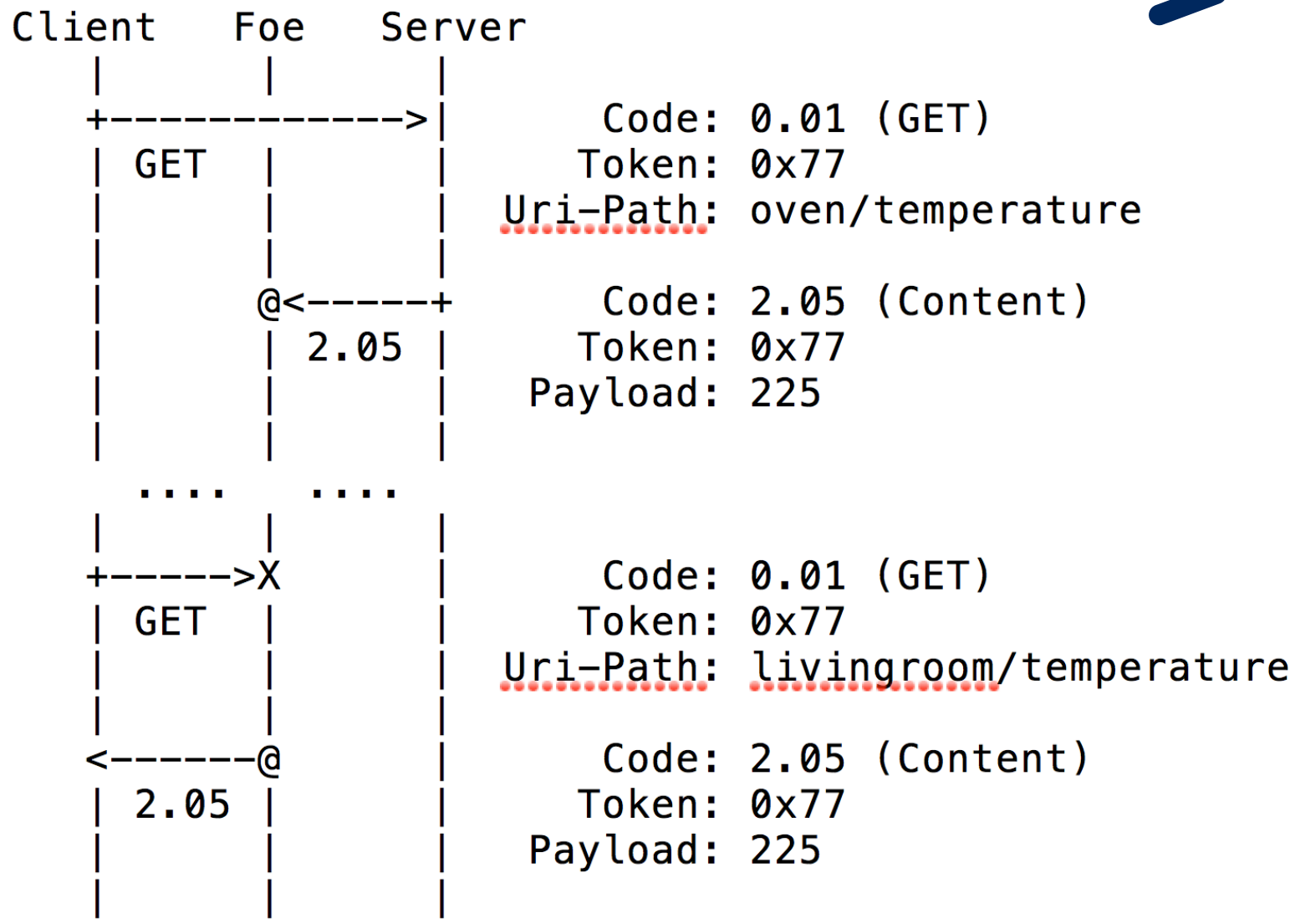


Figure 7: Mismatching Response from other resource

RELAY ATTACK

- Common with deployments where actuator actions are triggered automatically based on proximity.
- E.g. a car (the client) constantly polling for the car key (the server) and unlocking both doors and engine as soon as the car key responds.

- An attacker relaying the CoAP messages out-of-band, completely breaks the security.
- Unfortunately already happening in practice.
- Remedy: Don't use automatic car locks.

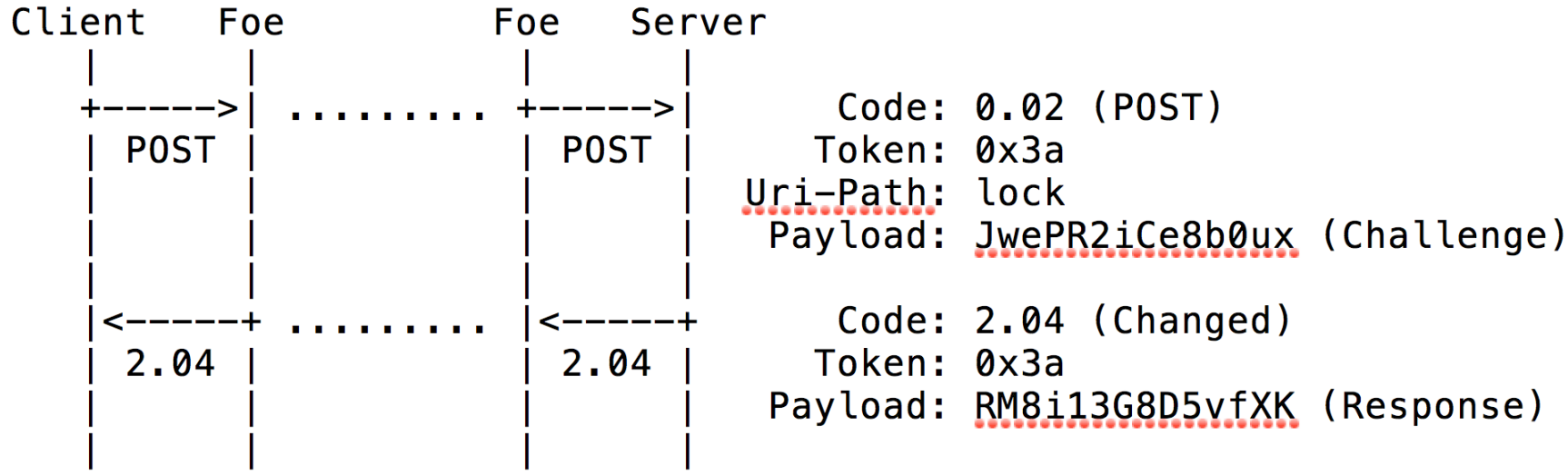


Figure 8: Relay Attack (the client is the actuator)

ERICSSON

THE REPEAT OPTION

REPEAT OPTION

- New e2e challenge-response mechanism for CoAP, binding a request to an earlier response.
- The challenge (for the client) is simply to echo the value.
- Enables the server to verify the freshness of a request:
  (t1 - t0) = RTT < Threshold,
  thus mitigating delay attacks.

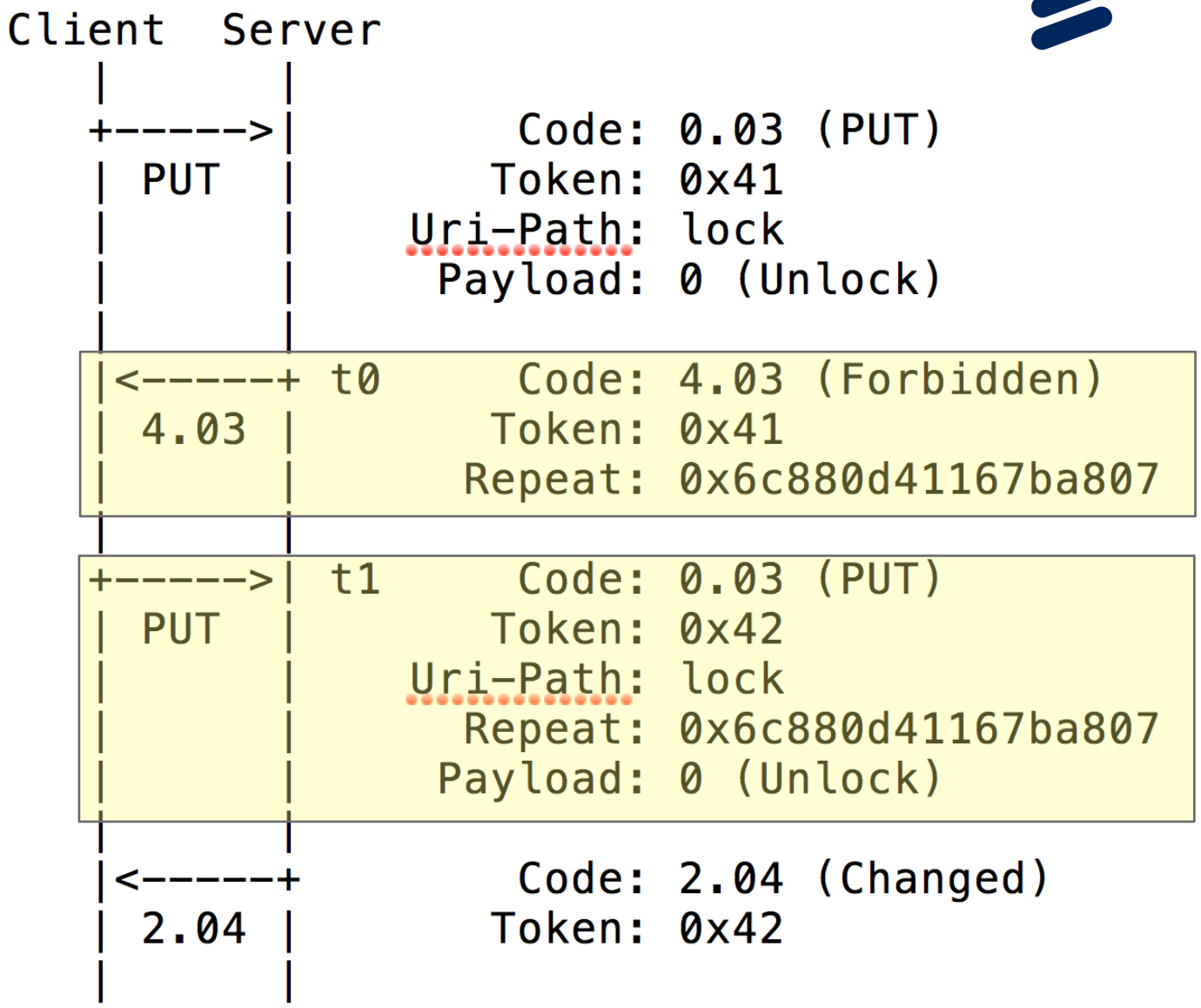


Figure 9: The Repeat Option

REPEAT OPTION

- Gives the server freshness guarantee independently of what the client does. But takes two round-trips and server has to save the option value and time t0.

- The server may simply send the current time t0. The client may then estimate the current time in the servers timescale when sending future requests (i.e. not echoing). This reduces round-trips and server state, but has security problems.

- The server may instead of a pseudorandom value send an CCM-encrypted timestamp:

  option value = AEAD(key, t0, NULL)
  or AEAD(key, t0, parts of request)

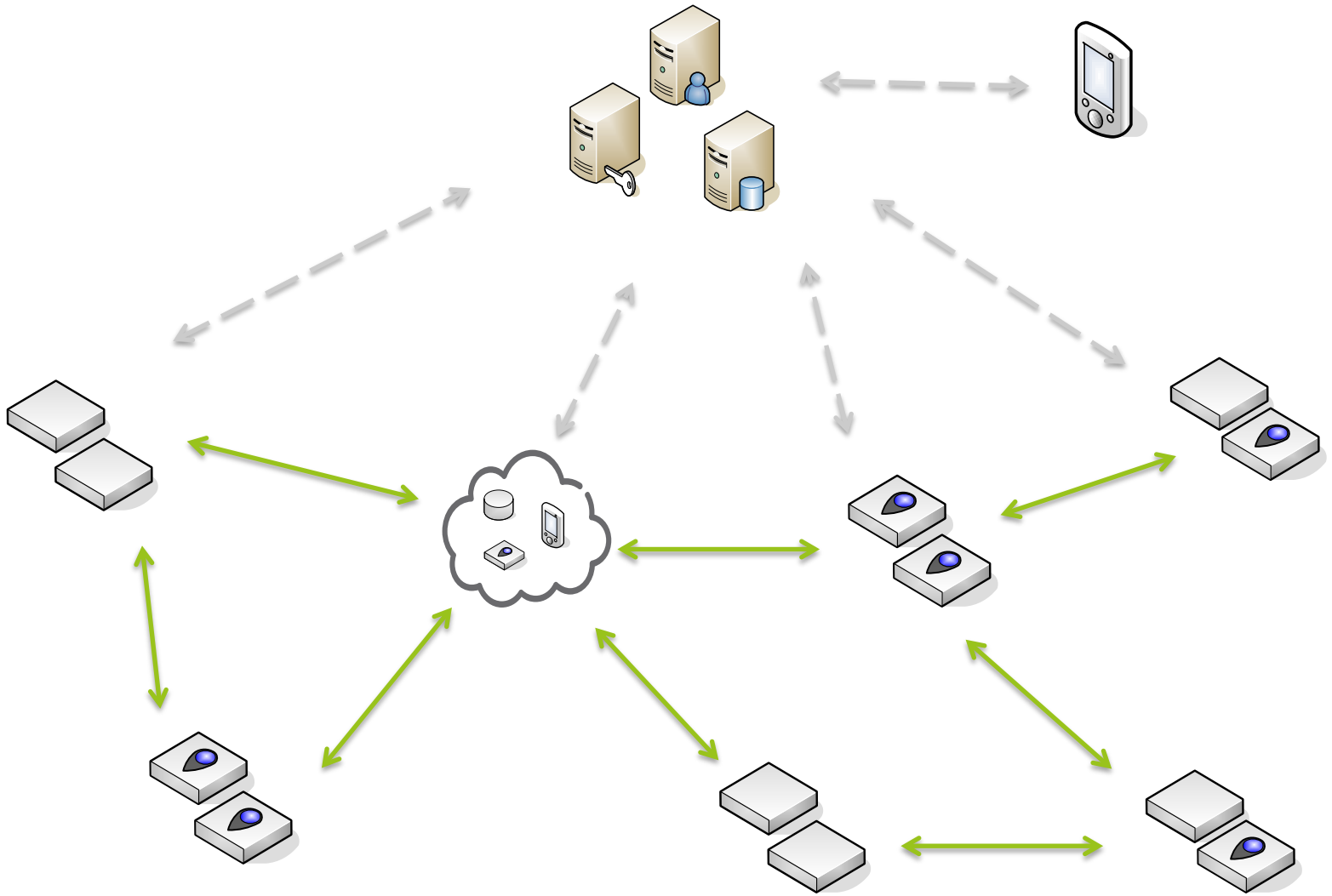
  This does not reduce the number of round-trips but eliminates server state.

ERICSSON

CYBERPHYSICAL

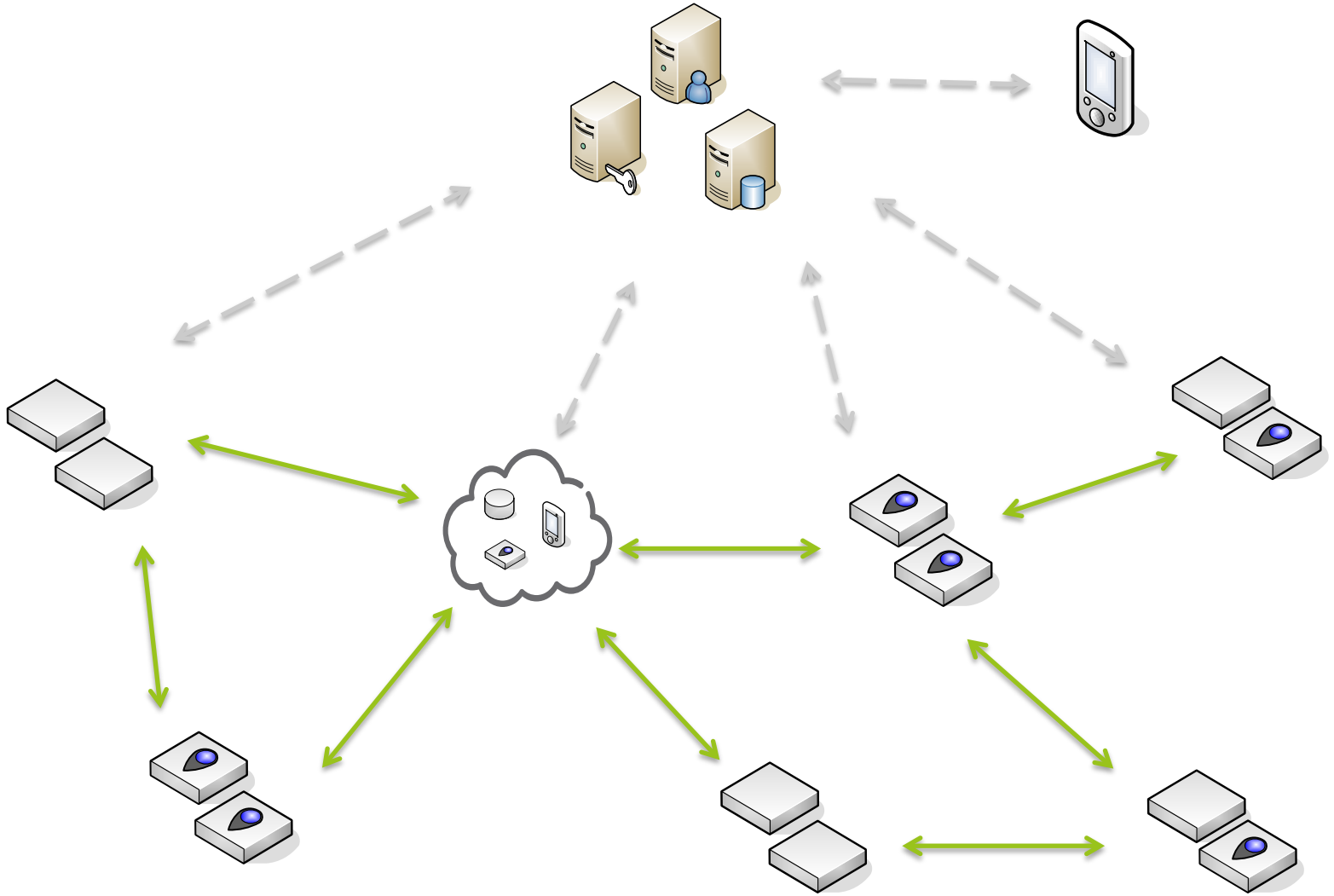
CYBERPHYSICAL SYSTEMS

- Security and privacy for sensors is complex
- Security for actuators is worse
- Security for privacy for cyberphysical systems where actuators are controlled by sensors is much worse.



CYBERPHYSICAL SYSTEMS

- Attackers can as before compromise nodes, block, delay, and relay messages.
- Attackers can also break sensors or actuators, influence sensors, move sensors, change time, and selectively block, delay or relay new programming…
- How to get general such systems secure and reliable?
- Which layers?
- A job for T2TRG?



ERICSSON

CONCLUSIONS

CONCLUSIONS

IoT systems needs more then integrity for individual messages:

- **Message bundle integrity.** Binding for example a response to a request, or an authentication handshake together. Lack of this has led to various attacks on e.g. TLS. Responses should always be bound to requests.
- **Time integrity,** binding a message or a bundle to a particular time. Standard to do in authentication protocols using timestamps or challenge-response, but missed when sending things over security protocols.
- **Space integrity**, binding a message or a message flow to a particular location. Is done in for e.g. HDCP 2.0 but needed also for cyberphysical systems.

Adding TLS or DTLS is not enough. Security analysis needed.

ERICSSON