A framework towards adaptable and delegated end-to-end transport-layer security for Internet-integrated Wireless Sensor Networks

Jorge Granjal
Edmundo Monteiro
Jorge Sá Silva

Centre for Informatics and Systems
University of Coimbra, Portugal

Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions

Outline

1) **Motivation and goals**
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions

Motivation and goals

We may currently observe that:

- Sensing applications on the IoT will require appropriate security mechanisms, including to protect end-to-end communications.
- Security should be quantifiable and adaptable.

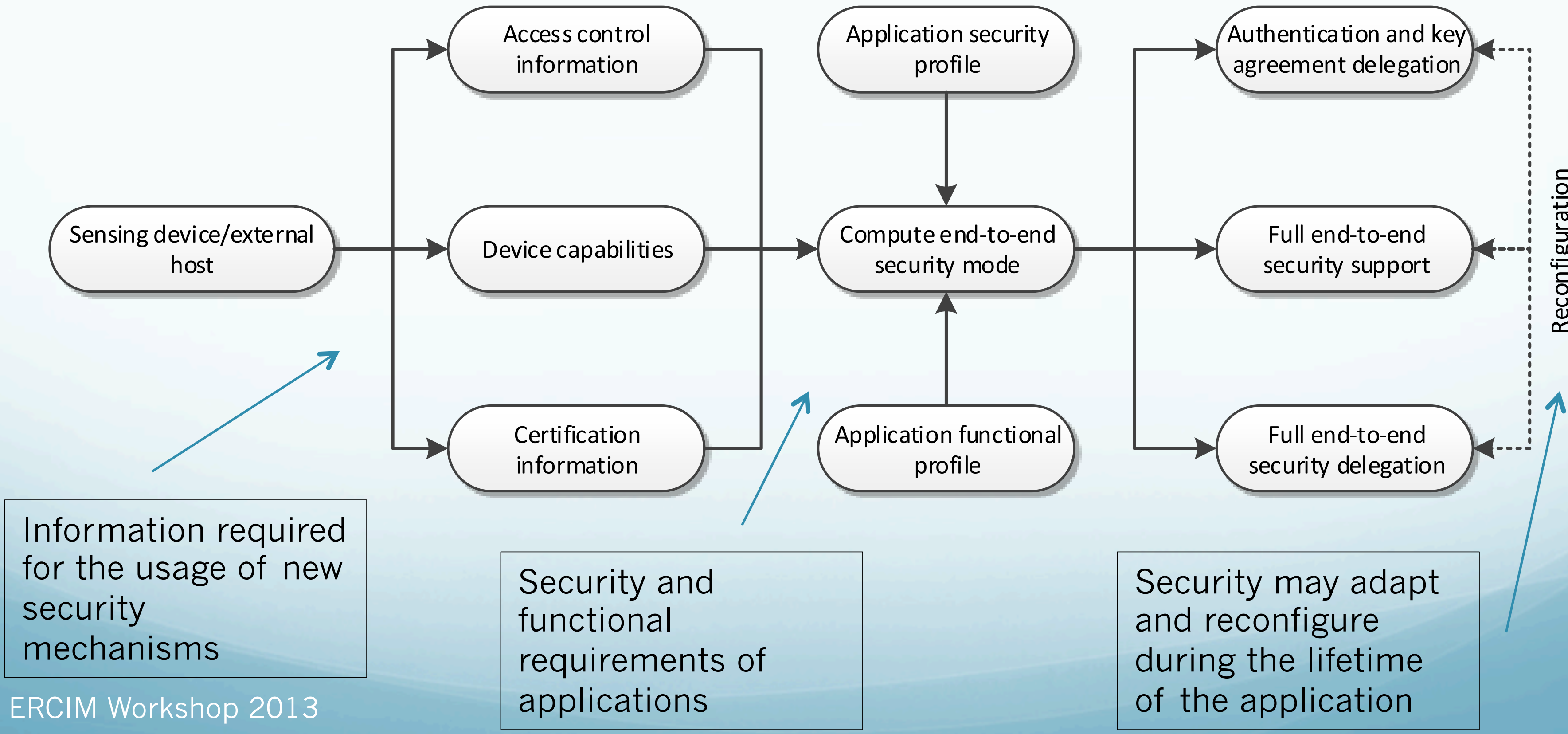
Main goals:

- Propose a framework supporting adaptable end-to-end security in the context of Internet-interconnected WSN.
- Address end-to-end transport-layer security with delegated ECC public-key authentication.
- Evaluate experimentally the proposed mechanisms in the context of the proposed framework.

Outline

Proposed framework

- A framework for the usage of secure end-to-end transport-layer communications with Internet-integrated sensing applications:



Outline

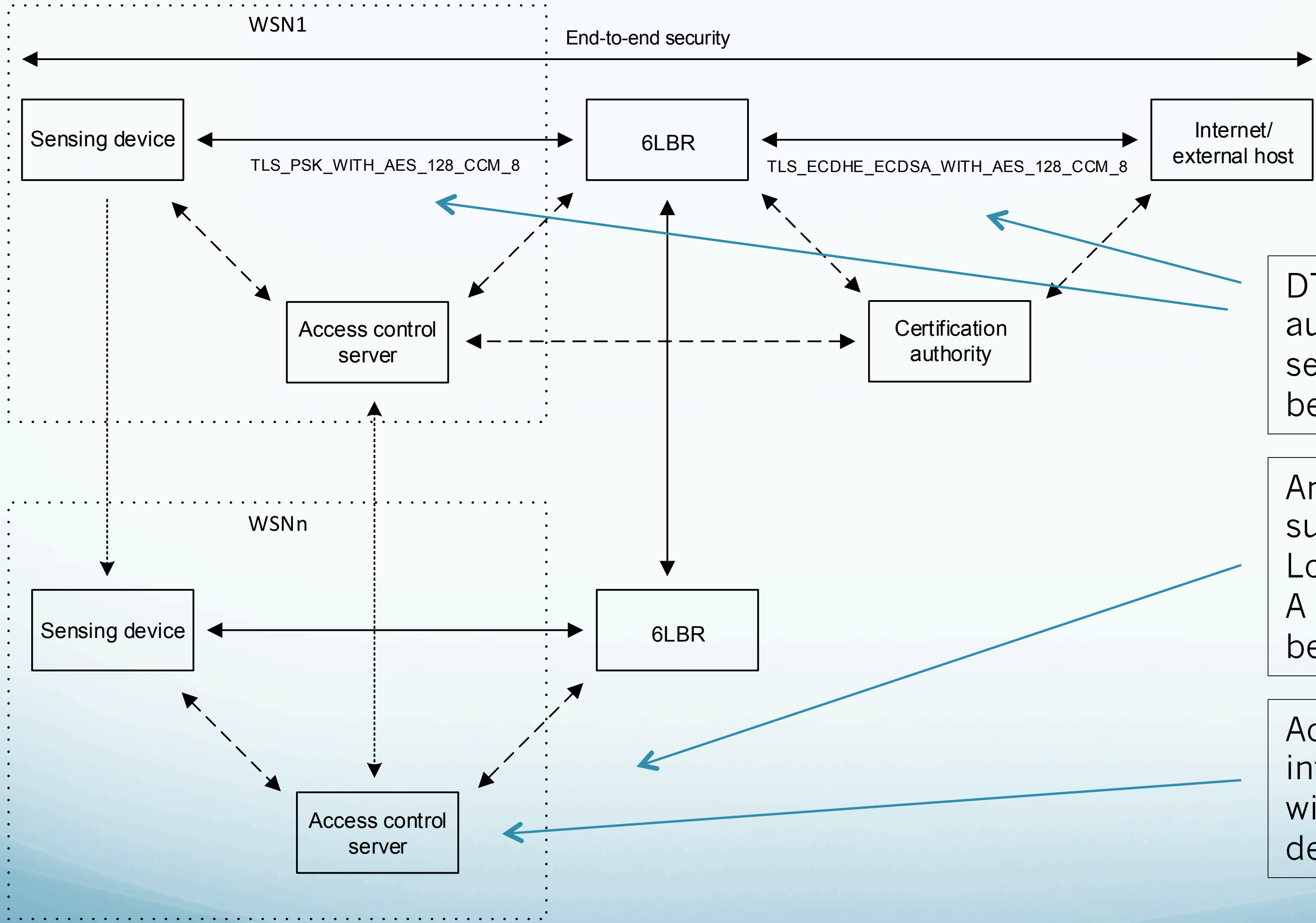
1) Motivation and goals
2) Proposed framework
3) **Proposed system architecture**
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) Conclusions

Proposed system architecture

Main goals:

- Support of end-to-end transport-layer security in three usage modes: full DTLS security, DTLS with delegated handshake, DTLS with fully delegated handshake.
- Support of future security mechanisms in the context of Internet-integrated WSN.
- Full compatibility with application-layer CoAP and 6LoWPAN security

Proposed system architecture



DTLS delegated authentication, other security suites may be supported

An application may support multiple LoWPAN domains
A device may move between domains

Access control information related with LoWPAN devices

Outline

Delegated ECC public-key authentication

Regarding CoAP security:

- CoAP supports three security modes :
  - *PreSharedKey* (TLS_PSK_WITH_AES_128_CCM_8)
  - *RawPublicKey* and *Certificates* (TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8)
- Encryption may use AES (CCM,CBC)
- AES/CCM is available in sensing platforms such as the TelosB implementing IEEE 802.15.4

Delegated ECC public-key authentication

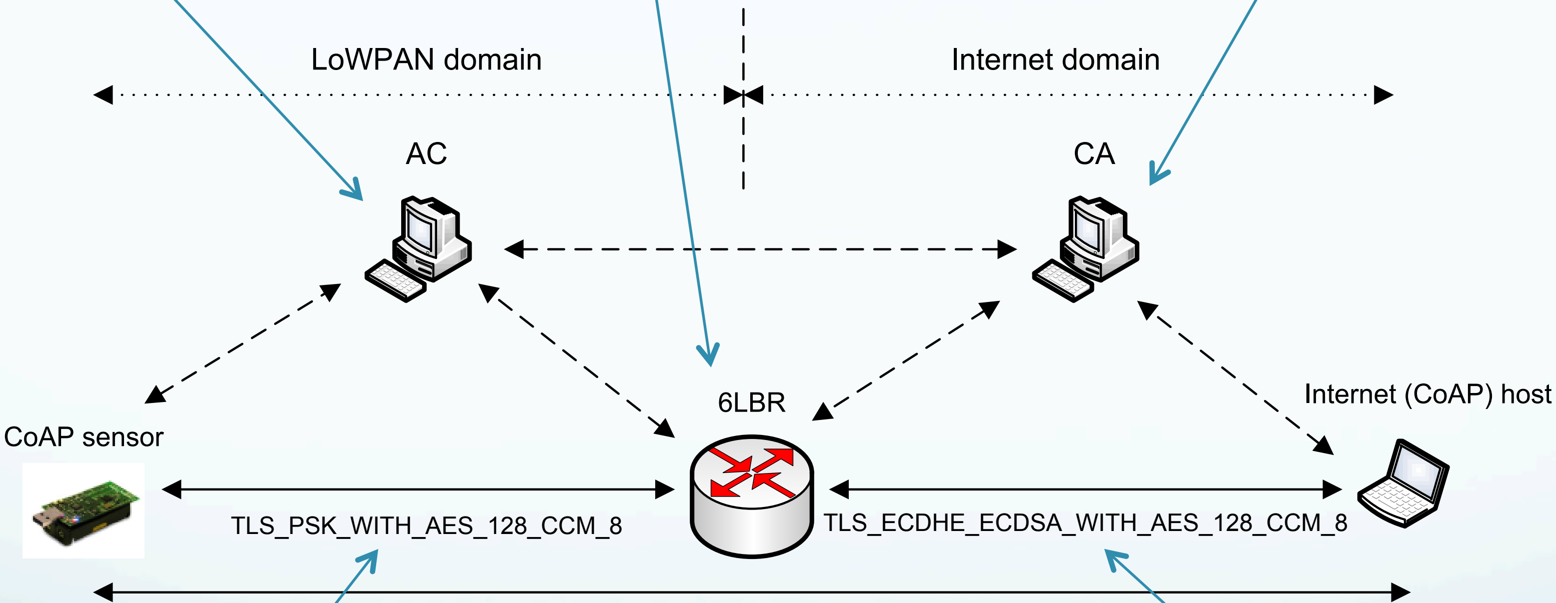
- A secure DTLS session requires the two parties to agree on:
  - The cipher suite
  - The encryption keys
- The DTLS handshake transports the information required for both parties to obtain encryption keys:
  - A shared master key is obtained from a pair of client and server random values plus a pre-shared master secret key (PMSK)
  - Final encryption keys are obtained from the shared master secret.
- PMSK generation depends on the cipher employed:
  - With public-key suites the client generates the PMSK and sends it to the server
  - Pre-shared keys suites don't support this, but we may **modify** TLS_PSK_WITH_AES_128_CCM_8 as long as we maintain appropriate security on the LoWPAN

Delegated ECC public-key authentication

Trust and security between 6LBR and 6LoWPAN devices

Intercepts and forwards packets at the transport-layer

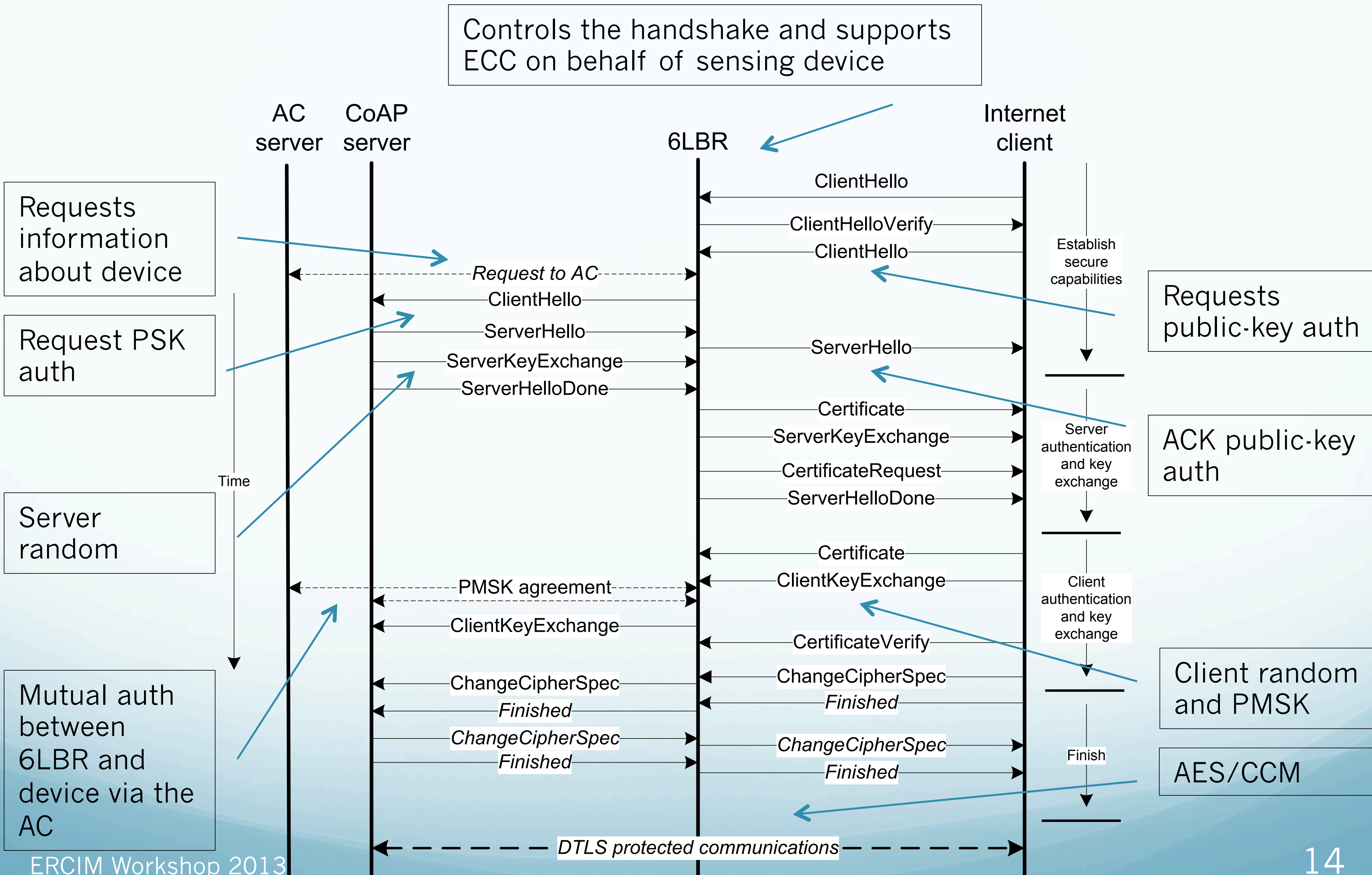
Public-key certification of communicating entities



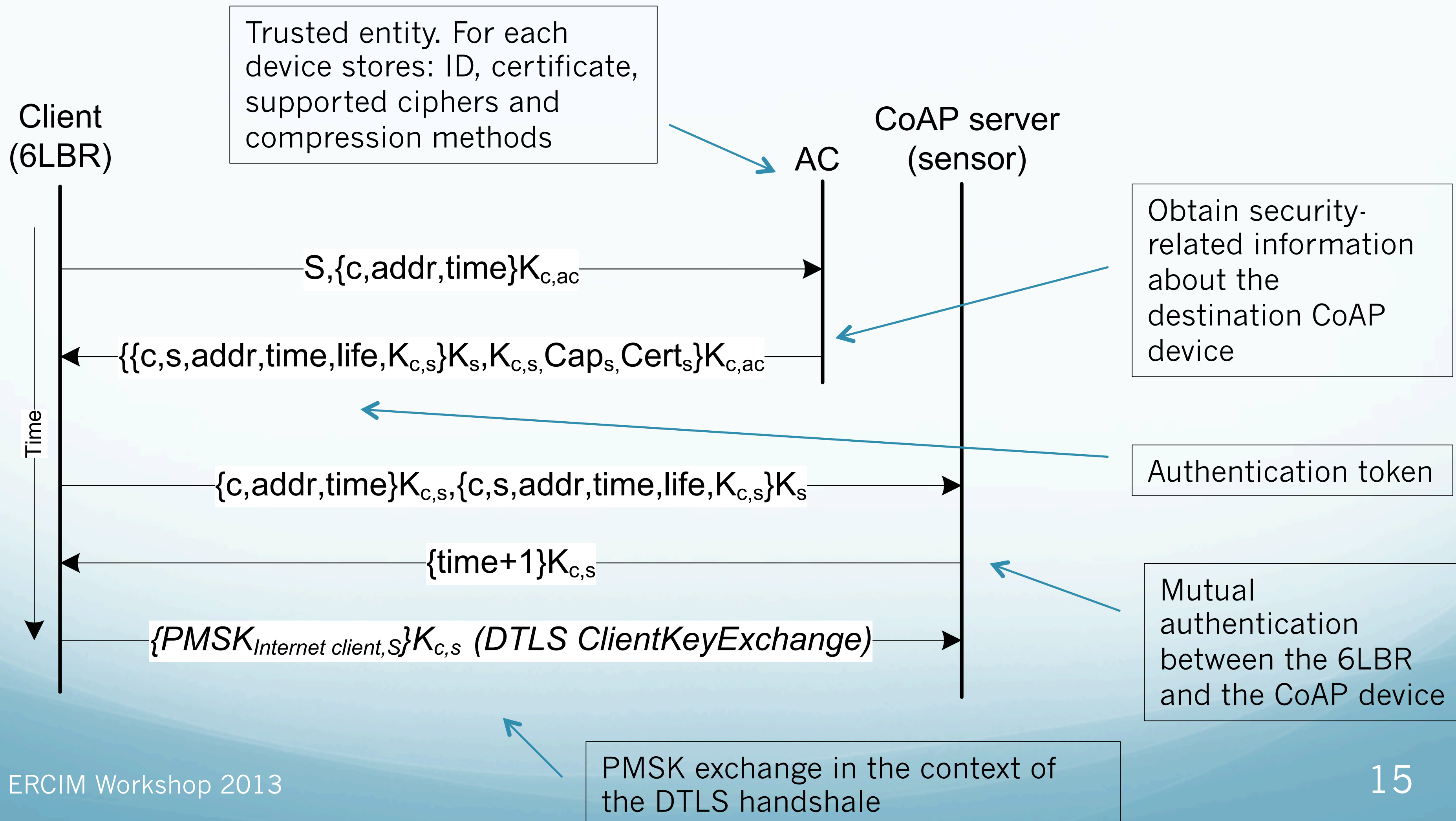
PreSharedKey CoAP security mode (modified)

Certificates CoAP security mode

Mediated DTLS handshake



6LBR and CoAP server mutual authentication



Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) **Experimental evaluation**
6) Conclusions

Experimental evaluation

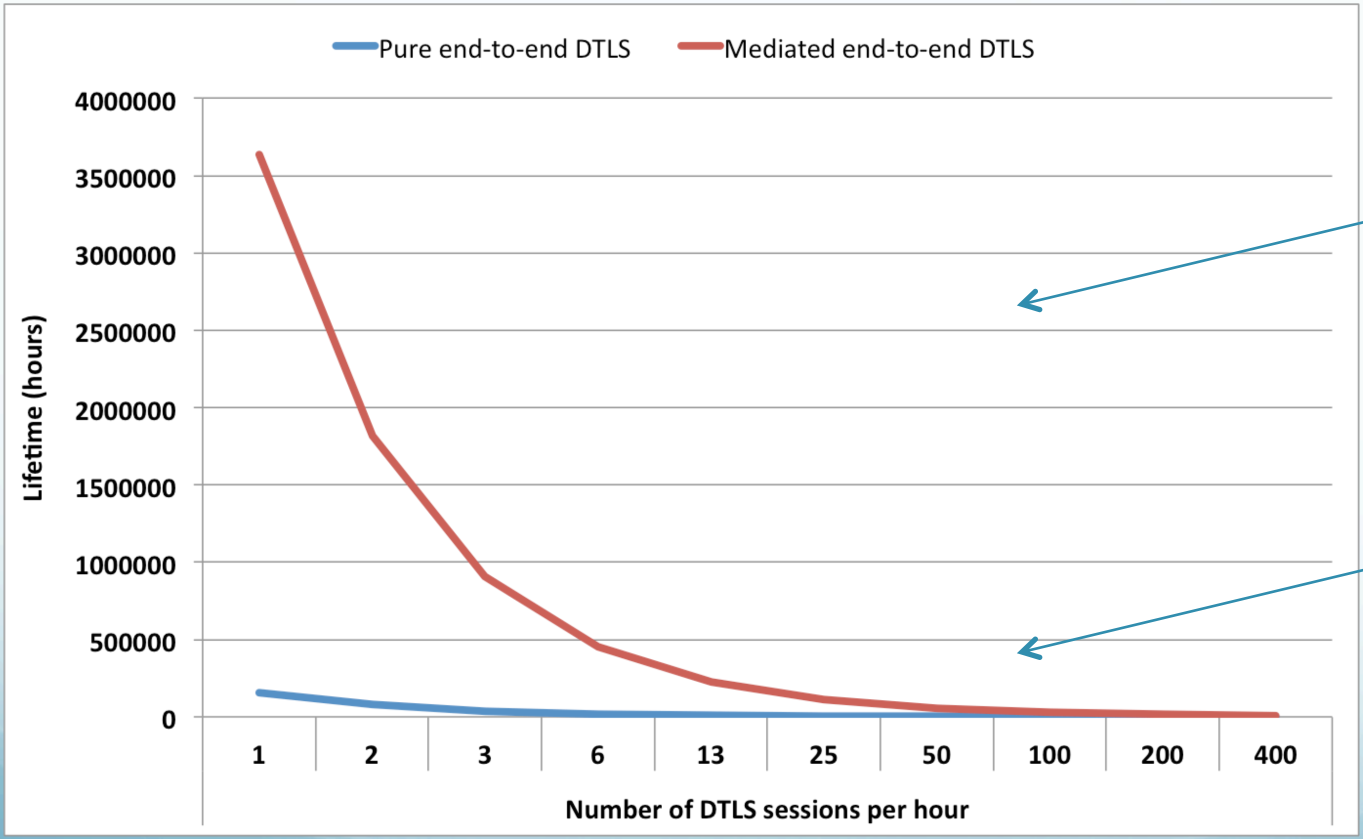
- Experimental evaluation setup using Linux and TelosB devices
- TelosB: 16-bit MSP430, 48KB ROM, 10KB RAM, IEEE 802.15.4
- Support of TinyOS, BLIP, CoAP, DTLS (ECDSA, ECDHE), SHA-256 and LoWPAN authentication
- Standalone AES/CCM hardware encryption
- LibCoAP with DTLS support

Experimental evaluation

- Two application profiles:
  - Moderate number of DTLS sessions/hour (1 to 400) and of CoAP requests per DTLS session (2).
  - Higher number of DTLS sessions/hour (14 to 7200) and of CoAP requests per DTLS session (10).
- Evaluate end-to-end security in two usage modes:
  - Support of full end-to-end DTLS security.
  - Delegated DTLS authentication using the proposed mediated handshake.

Experimental evaluation

- Impact on the lifetime of sensing applications (moderate usage profile):

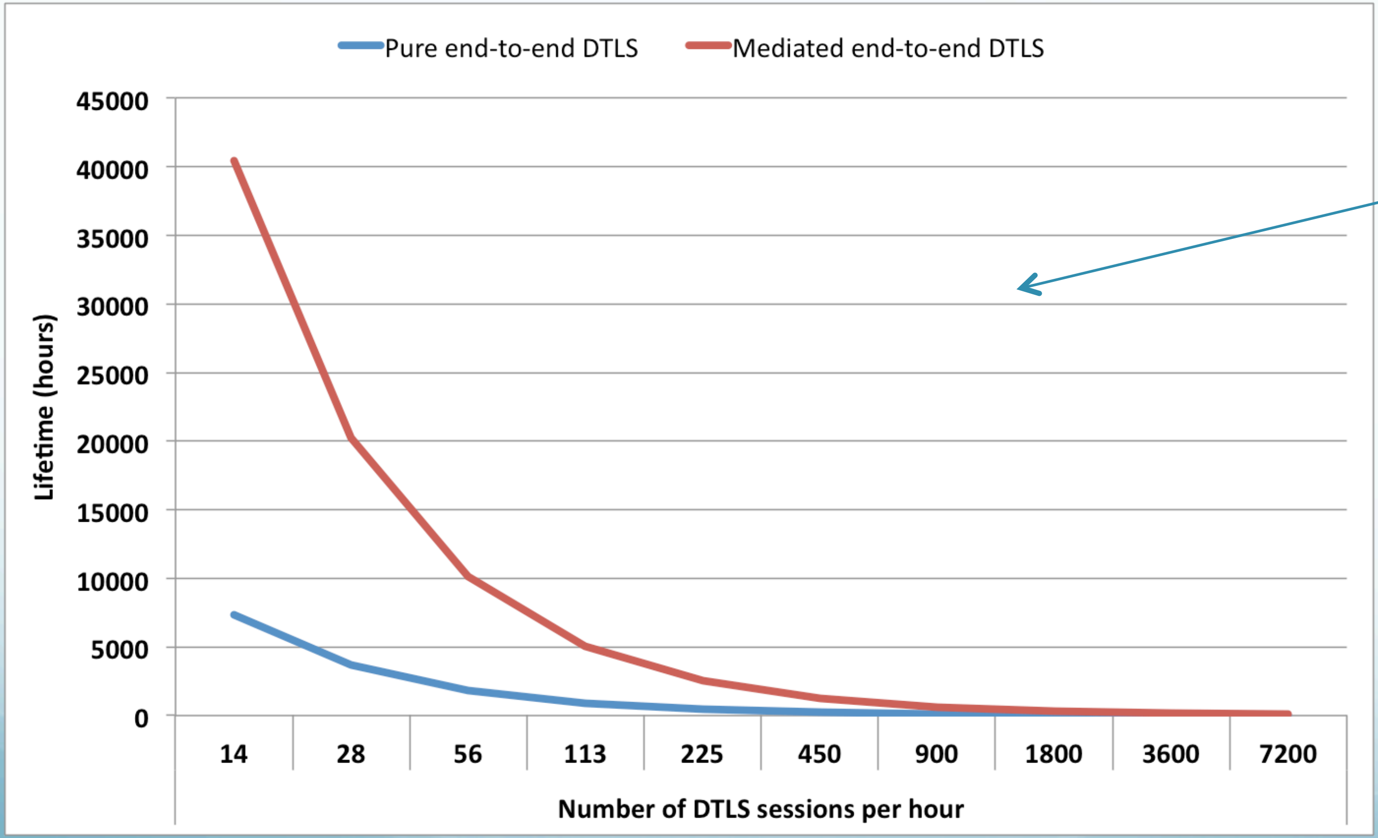


Clear advantage of delegated DTLS authentication, particularly for a lower number of DTLS sessions per hour

Advantage is less expressive for higher values, due to the higher impact of AES/CCM encryption in comparison with the DTLS handshake

Experimental evaluation

- Impact on the lifetime of sensing applications (higher usage profile):



Similar conclusions regarding the advantages of delegated DTLS authentication

Outline

1) Motivation and goals
2) Proposed framework
3) Proposed system architecture
4) Delegated ECC public-key authentication
5) Experimental evaluation
6) **Conclusions**

Conclusions

- Efficient support of end-to-end security using delegated mutual authentication.
- Compatibility with standardized CoAP security.
- Other security mechanisms based on a security gateway may be adopted in the future (application-layer message analysis and filtering, 6LoWPAN security).
- Future work:
  - Transparent end-to-end security for mobile devices.
  - Mechanisms to configure security according to application profiles and characteristics of devices.
  - Adoption of other security suites on the LoWPAN domain.