

---

# Experimental Evaluation of the Performance Costs of Different IKEv2 Authentication Methods

Zoltán Faigl, Stefan Lindskog, and Anna Brunstrom

---

Mobile Innovation Center, Budapest University of Technology and  
Economics, Budapest, Hungary, [zfaigl@mik.bme.hu](mailto:zfaigl@mik.bme.hu)

Centre for Quantifiable Quality of Service in Communication  
Systems, Norwegian University of Science and Technology,  
Trondheim, Norway, [stefan.lindskog@q2s.ntnu.no](mailto:stefan.lindskog@q2s.ntnu.no)

Department of Computer Science, Karlstad University, Karlstad,  
Sweden, [anna.brunstrom@kau.se](mailto:anna.brunstrom@kau.se)

---

# Outline

- Motivation
  - Background
  - Reference scenario
  - Considered authentication methods
  - Experimental setup
  - Results
  - Conclusions
-

---

# Motivation

- Next generation networks
    - Openness: more third party providers, more complex administration
    - Authentication, Authorization and Accounting (AAA) is a major issue
  - AAA services:
    - AAA architecture composed of many protocols
    - Internet Key Exchange version 2 protocol is one candidate to enforce authentication, and security association negotiation
  - AAA services should be aware of performance overheads (QoS)
  - Very few papers on IKEv2 deal with performance costs:
    - Simulations of IKEv1 and IKEv2 in limited scenarios
    - Theoretical analysis: performance analysis of IKEv2 in an AAA scenario
    - None of them include the costs of the security application framework
  - Lack of research analyzing the performance costs of using IKEv2 for AAA services in real environments
-

---

# What is Internet Key Exchange version 2 (IKEv2) protocol?

- Negotiates security associations for IPsec
  - Authenticates the peers
  - Supports Extensible Authentication Protocol (EAP) methods
  - Supports other services, e.g.
    - Bootstrapping
      - addressing and naming
    - MOBIKE
      - avoid reauthentication in case of IP address changes
      - dynamic update of security associations
  - Candidate technology in future AAA frameworks
-

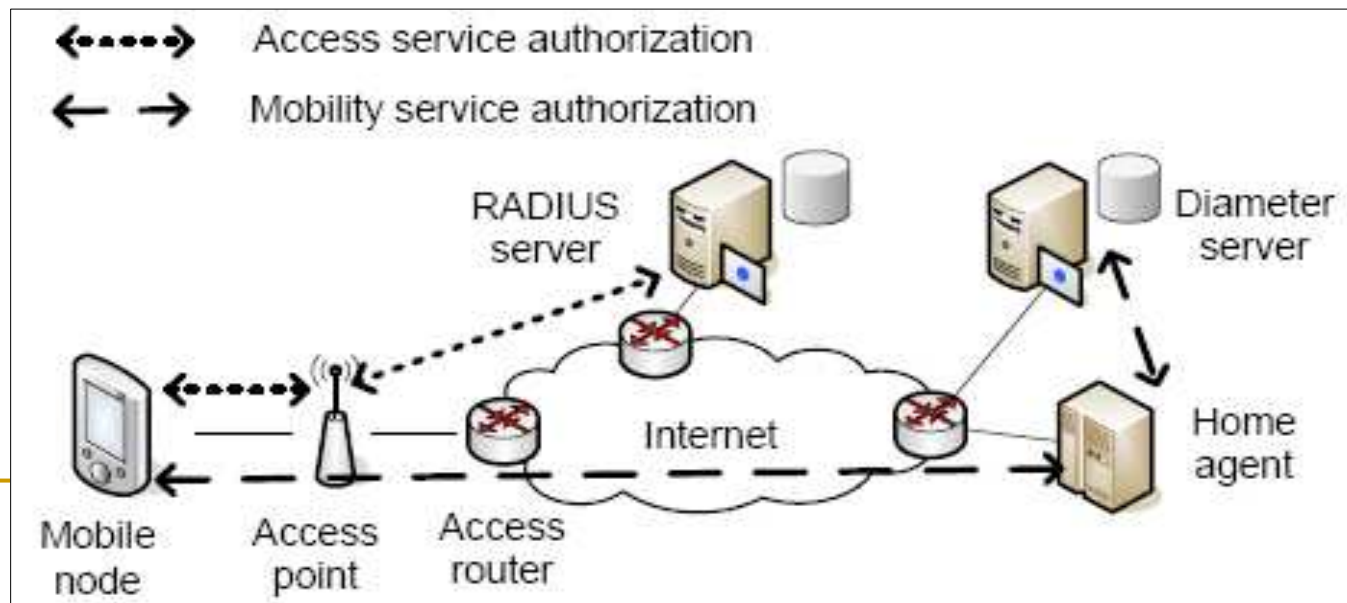
---

# AAA services in future wireless networks

- AAA is an important part of most services
    - Network access service (3G, WiFi, WiMAX, DSL, cable)
    - Mobility service
    - IMS services (voice, video)
    - M-banking
  - Many providers of the services, but the users are common (same device)
  - Many AAA framework concepts
-

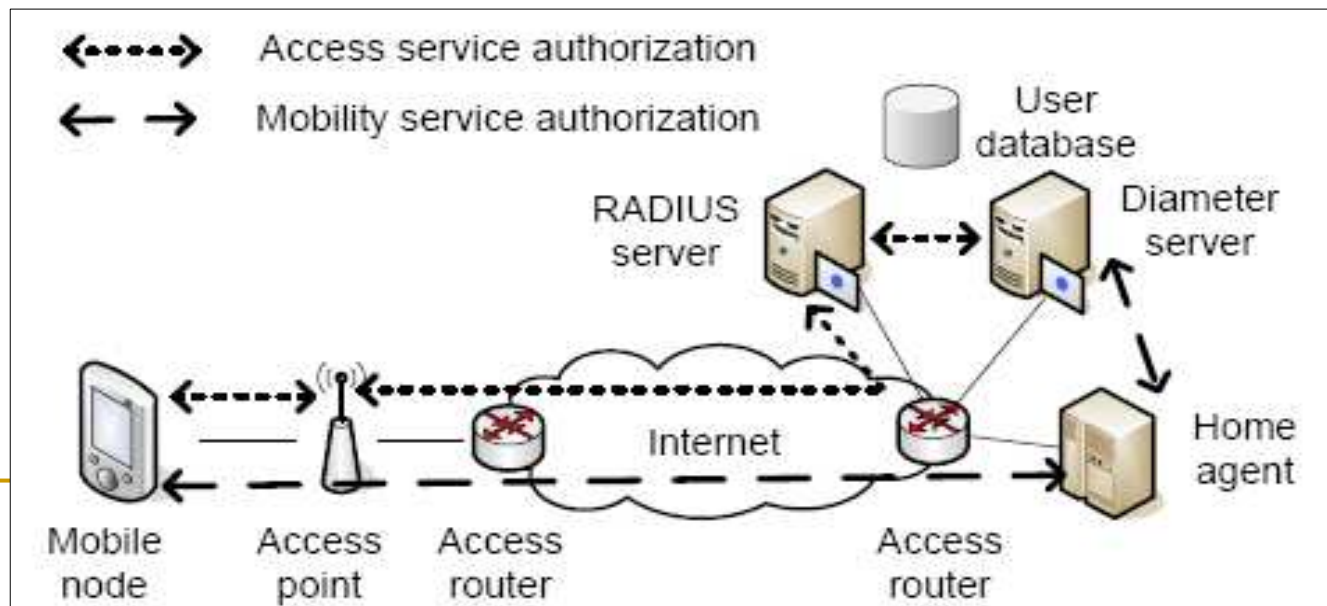
# AAA services in future wireless networks

- AAA is an important part of most services
  - Network access service (3G, WiFi, WiMAX, DSL, cable)
  - Mobility service
  - IMS services (voice, video)
  - M-banking
- Many providers of the services, but the users are common (same device)
- Many AAA framework concepts
  - Split AAA services



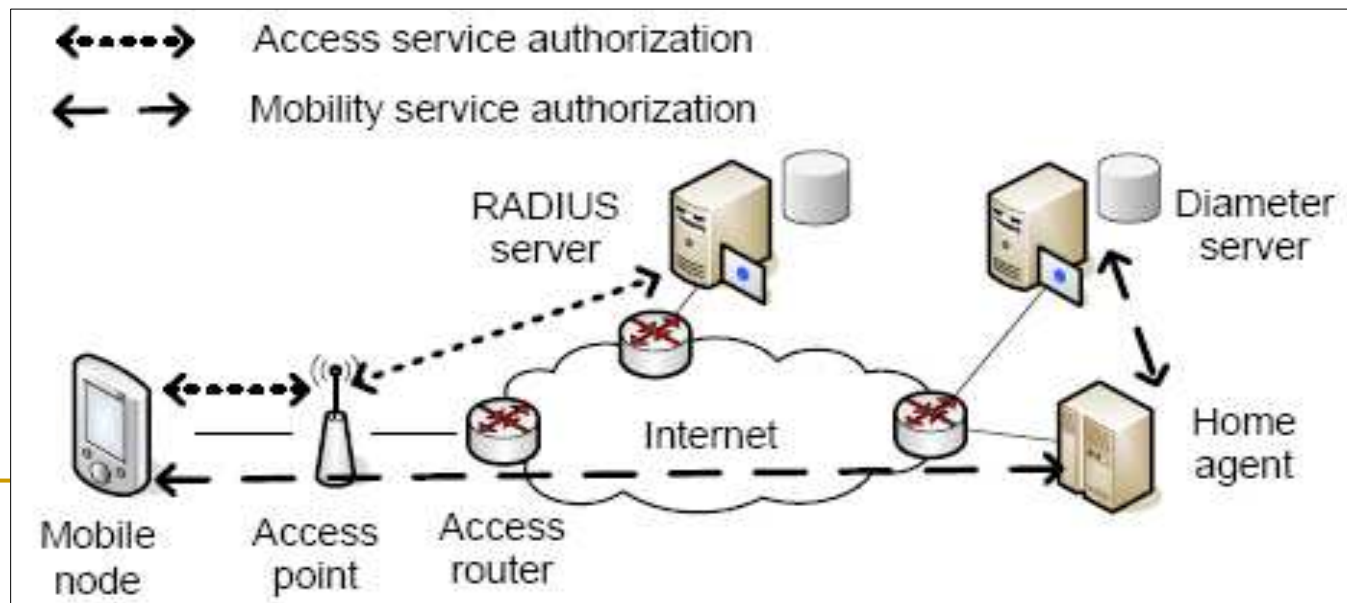
# AAA services in future wireless networks

- AAA is an important part of most services
  - Network access service (3G, WiFi, WiMAX, DSL, cable)
  - Mobility service
  - IMS services (voice, video)
  - M-banking
- Many providers of the services, but the users are common (same device)
- Many AAA framework concepts
  - Integrated AAA services



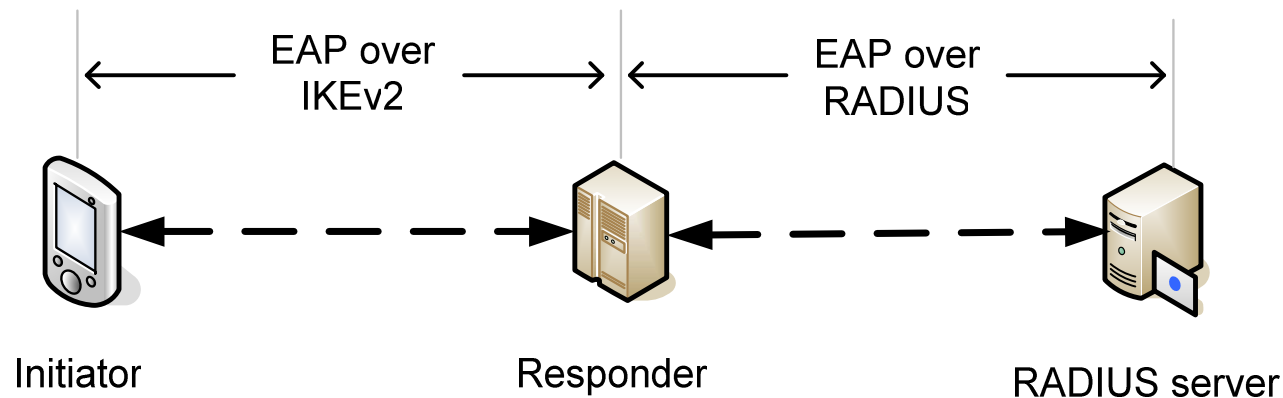
# AAA services in future wireless networks

- AAA is an important part of most services
  - Network access service (3G, WiFi, WiMAX, DSL, cable)
  - Mobility service (changing IP address )
  - IMS services (voice, video)
  - M-banking
- Many providers of the services, but the users are common (same device)
- Many AAA framework concepts
  - Split AAA services



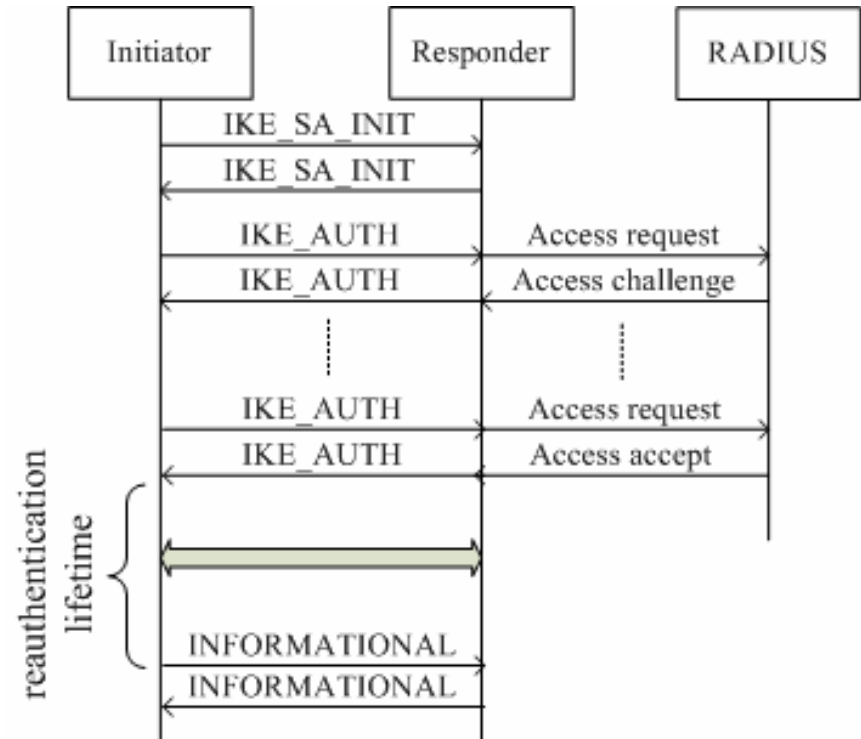
## Reference scenario

- We look at mobility service authentication and authorization at the IP layer
- Protocols enforcing AAA services
  - IKEv2 (pre-shared key (PSK) authentication, creation of protected environment, bootstrap)
  - RADIUS (AAA server and messaging protocol)
  - Extensible Authentication Protocol (EAP-MD5, EAP-TLS authentication method)
  - IPsec (enforce cryptographically strengthened service access, security services)



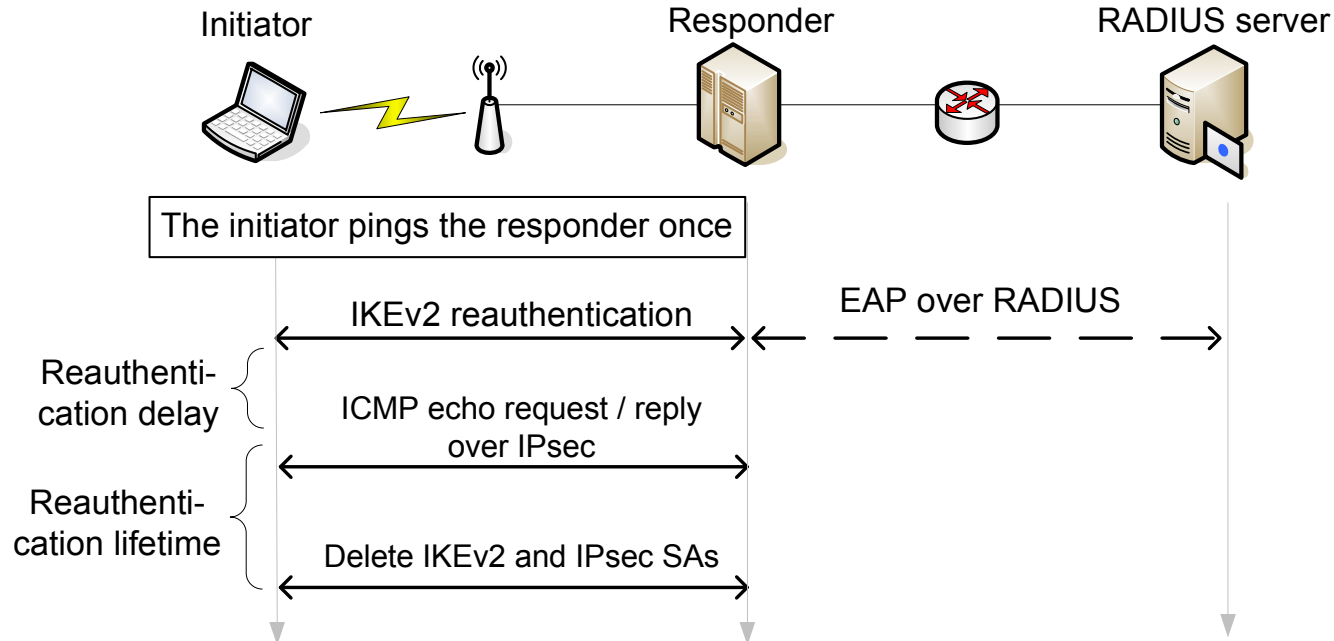
# Measurement goals

- Determine the performance costs of different IKEv2 authentication methods in a real environment
  - Network delay
  - Computational cost
- Considered methods
  - IKEv2 with PSK auth.
    - PSK between initiator and responder
  - IKEv2 with EAP-MD5
    - PSK between initiator and AAA server
  - IKEv2 with EAP-TLS
    - EAP-TLS authentication using RSA signing certificates
    - 1, 2 and 3-tier certificate chains

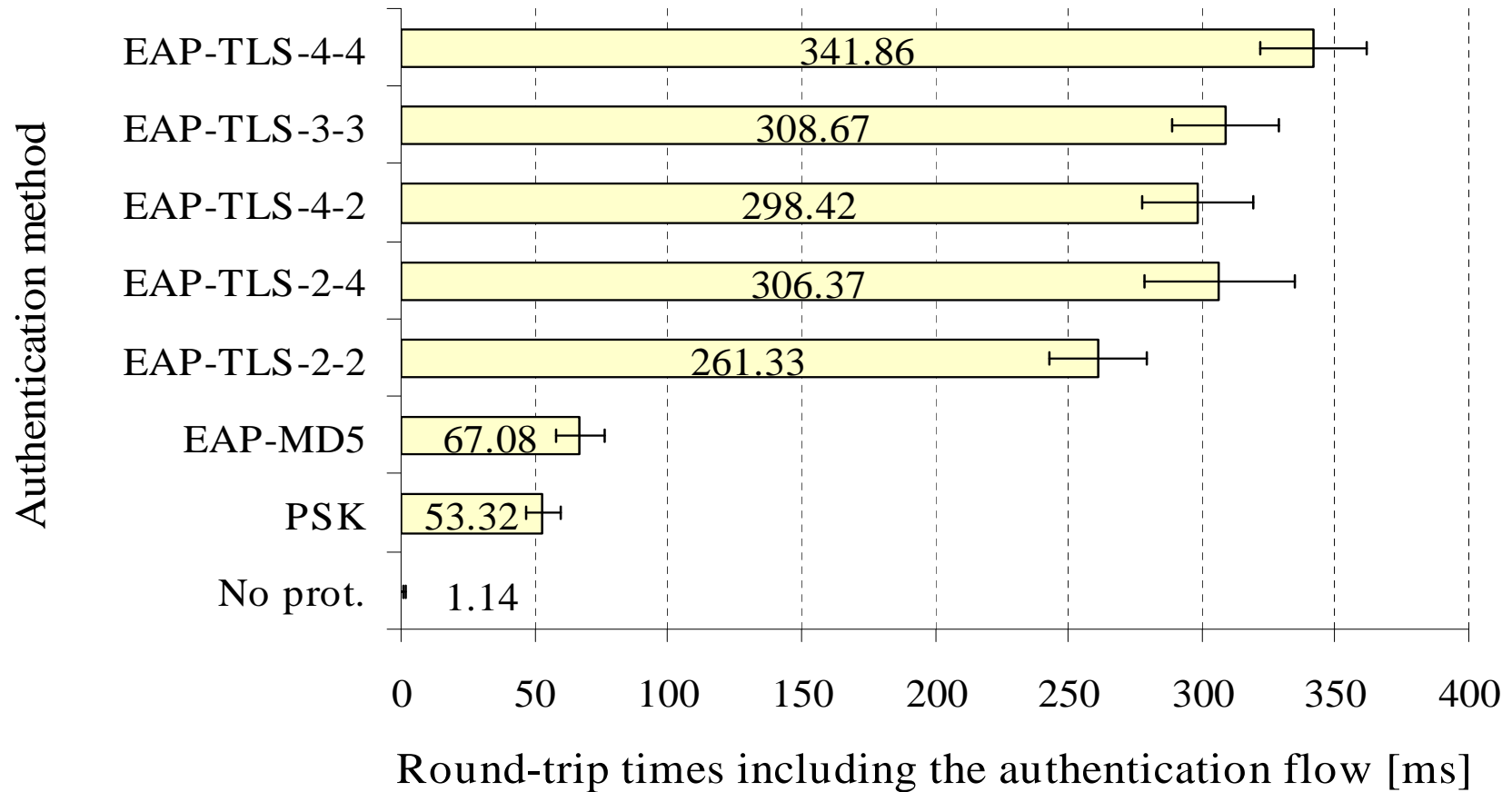


# Experimental setup

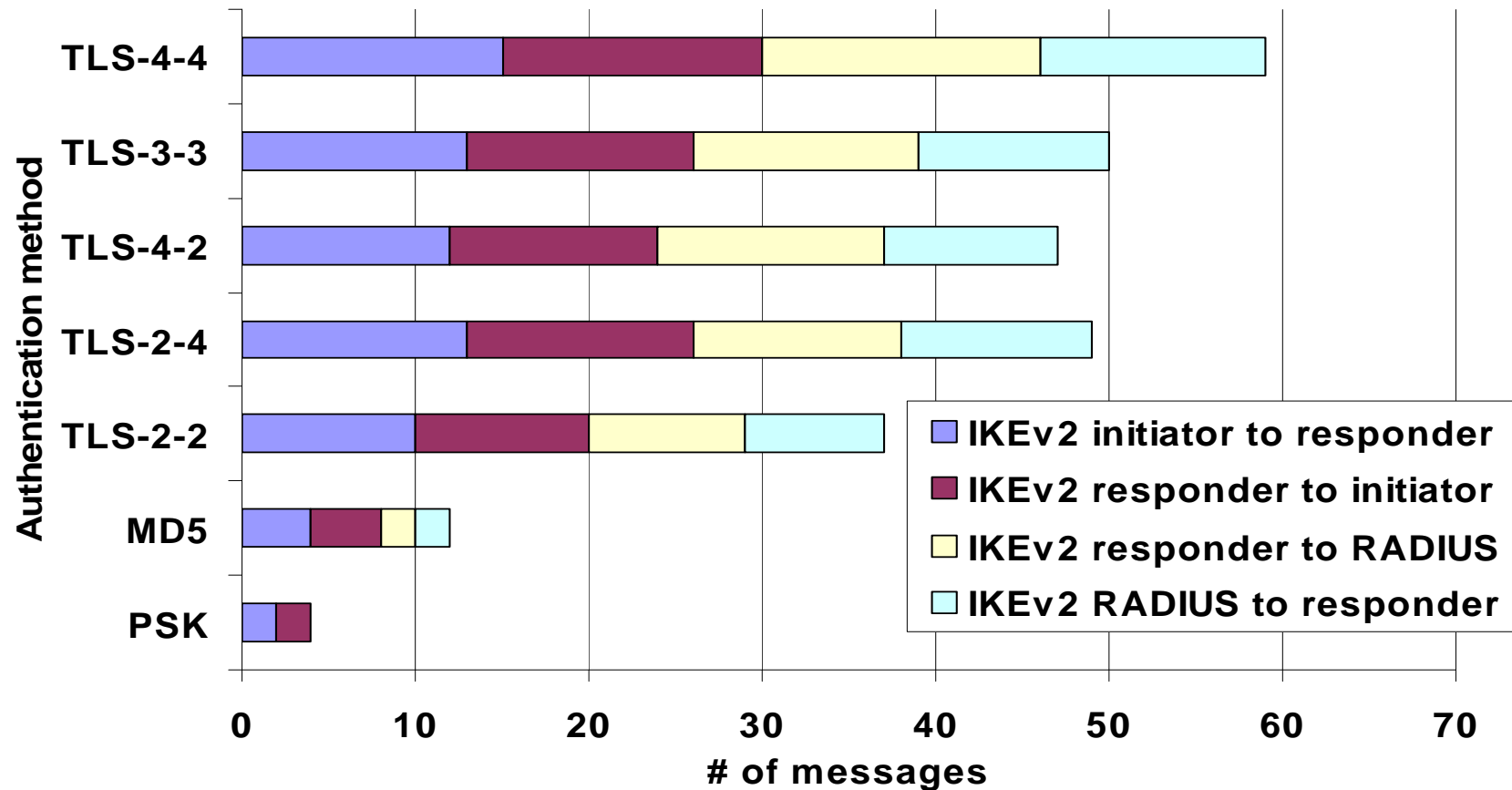
- Measurement method
  - ❑ Configure the system to protect ICMP echo request and reply between the initiator and responder with IPsec
  - ❑ ICMP echo request triggers IKEv2 negotiation if IPsec SA does not exist
  - ❑ Responder sets the reauthentication lifetime to 6 seconds, initiator pings each 12 seconds
- Measurement tools:
  - ❑ Authentication delay: ping round-trip time
  - ❑ Computational cost: OProfile profiler tool collects information on running processes at given time intervals



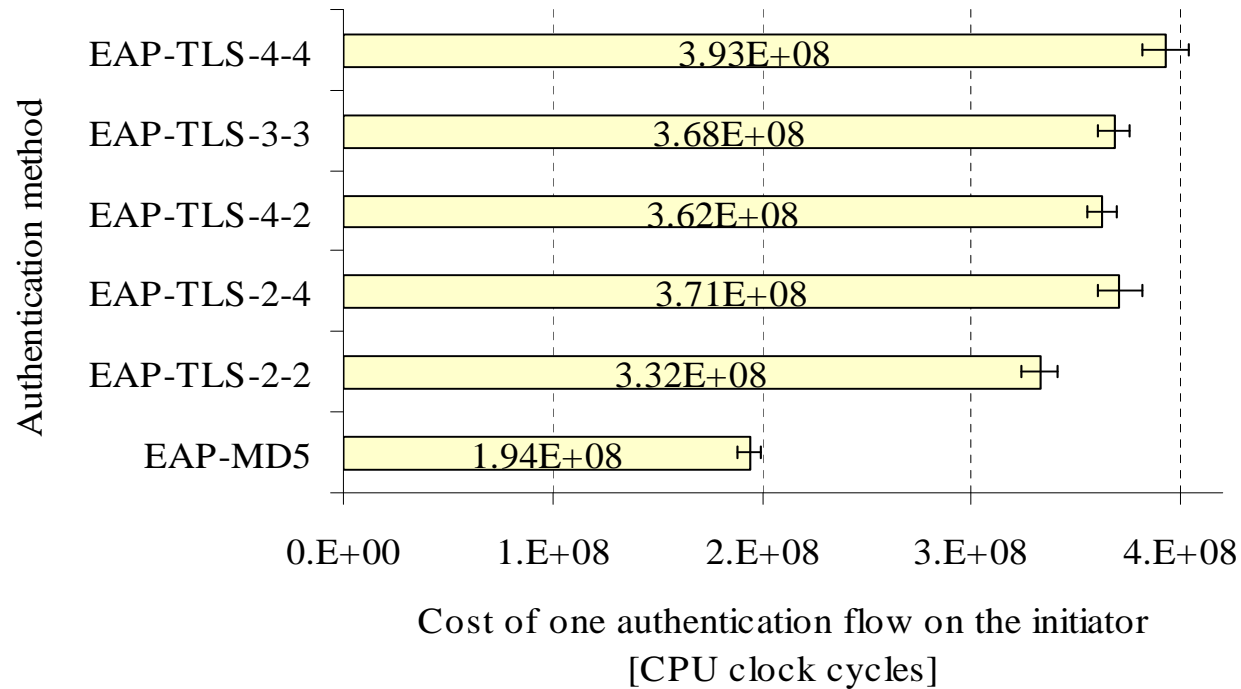
# Measurement results - authentication delay



# Measurement results - message complexity



# Measurement results - computational overhead



MEAN NUMBER OF SAMPLES BELONGING TO THE CONSIDERED LIBRARIES AND THE OS ON THE INITIATOR SIDE.

$$C_{\text{init}} = \frac{Sf_{\text{CPU}}}{nf_{\text{timer interrupt}}}$$

Name	libcrypto	libc	vmlinux	yenta
TLS-4-4	1387	1620	1266	641
TLS-3-3	1392	1397	1185	629
TLS-4-2	1440	1282	1161	647
TLS-2-4	1422	1440	1225	627
TLS-2-2	1371	1083	1060	644
MD5	615	377	807	626

---

# Concluding remarks

- Experimental performance evaluation of IKEv2 authentication methods was provided
  - Real measurements are an important complement to theoretical analysis or simulation environments, and captures all the overhead involved in the system
  - Main results
    - The authentication delays of the considered methods show large differences
      - EAP-TLS is several times slower than both PSK and EAP-MD5.
    - Authentication delay of EAP-TLS configurations (>150 ms) may impact some applications even in a small scenario
    - For EAP-TLS, the lengths of the certificate chains are also shown to be important for performance
      - The increase of the certificate chain lengths from two to four led to an increase in delay of roughly 30%.
    - EAP-TLS is significantly more computationally demanding than EAP-MD5
  - The results can also be used as input parameters for analytical modeling of authentication processes
-

---

## Future Work

- Complete our measurements with more EAP-methods
- Larger network scenario
- Apply the obtained cost values in a proof-of-concept example of a security design method

In general

- Device miniaturization → symmetric key algorithms
  - Large-scale network → decentralize AAA functions, localize re-authentications (e.g. RFC 5296: EAP Re-authentication Protocol)
  - Environment can be more complicated (e.g. mesh, hybrid networks with multi-hop communication, and un-trusted relays)
  - New AAA enforcing solutions are needed
-

---

Thank you for your attention!  
Any questions

---

---

# Concluding Remarks

- Authentication delay
    - We have measured reauthentication delays on the application level in a system where each participant is located on the same small internet site
    - Still, the differences between the considered authentication methods are large, with EAP-TLS being several times slower than both PSK and EAP-MD5.
    - For EAP-TLS, the lengths of the certificate chains are also shown to be important for performance. In the ping measurements, increasing the certificate chain lengths from two to four at the initiator and the AAA server led to an increase in delay of roughly 30%.
    - Authentication delay of EAP-TLS configurations (>150 ms) may impact some applications even in a small scenario
  
  - Utilization measurements
    - EAP-TLS is significantly more computationally demanding than EAP-MD5 both at the initiator and the AAA server
    - In case of TLS configurations the certificate-chain length to be verified seems to influence the computational cost.
-

# Measurement results - computational overhead

MEAN NUMBER OF SAMPLES BELONGING TO THE CONSIDERED LIBRARIES AND THE OS ON THE INITIATOR SIDE.

Name	libcrypto	libc	vmlinux	yenta
TLS-4-4	1387	1620	1266	641
TLS-3-3	1392	1397	1185	629
TLS-4-2	1440	1282	1161	647
TLS-2-4	1422	1440	1225	627
TLS-2-2	1371	1083	1060	644
MD5	615	377	807	626

$$C_{\text{init}} = \frac{S f_{\text{CPU}}}{n f_{\text{timer interrupt}}}$$

$$f_{\text{timer interrupt}} = 1000 \text{ Hz}$$

$$f_{\text{CPU}} = 1.6 \text{ GHz (init.)}, 3\text{GHz (AAA)}$$

n: # authentication flows

S: # collected samples

