School of Computer Science
University of Manchester

New Security Protocol for M-Learning

Lirong He
Lisha He
Ian Rogers

M-Learning and Security

- Mobile Learning (M-Learning)

  → the next generation of e-learning

  → based on mobile devices

- Security is a significant challenge for M-Learning

  → authentication, confidentiality, integrity, privacy, etc

- Authentication is essential

  → to ensure that someone or something is whom it claims to be

Related Work

- Some protocols with only two entities normally require heavy operational load at the mobile side.

- Some solutions (with three entities) allow a server to get access to the session key establishment and therefore subsequent confidential transactions.

- Though the solutions by [Yeh and Sun 2004, Alsan 2003] are secure and more efficient than other proposals, they remain computationally expensive.

Our Objectives

- To present a secure and efficient authentication protocol for M-Learning applications

- Achieve mutual authentication and key establishment between a mobile learner and an online education organisation

- Place less operational cost at the mobile side

Network Assisted Authentication Protocol (NAAP)

- Network operators can:
  - easily implement new platforms and protocols for secure mobile transactions
  - use existing Internet-based protocols to communicate with the education organisation on the Internet
  - reuse this security sensitive information
  - be always online and provide ample resource

Authentication Requirements

- (S1) Authentication of the online education organisation to the mobile learner.

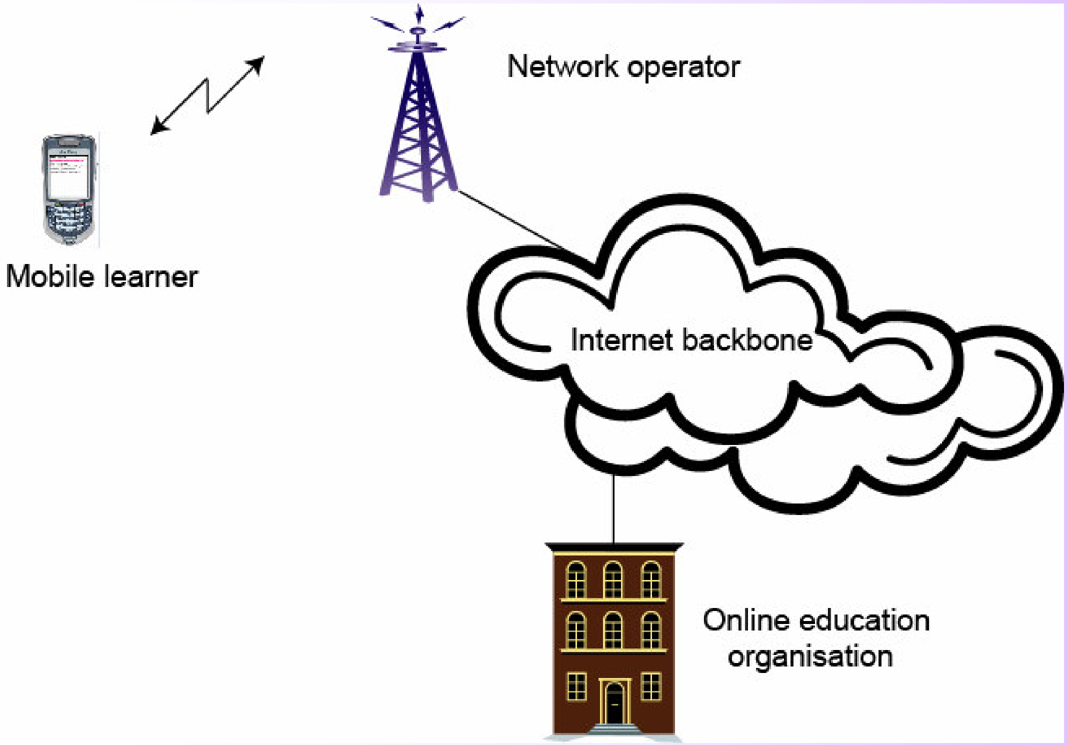
- (S2) Authentication of the mobile learner to the online education organisation.

- (S3) End-to-end session key establishment.

- (S4) Session key confirmation.

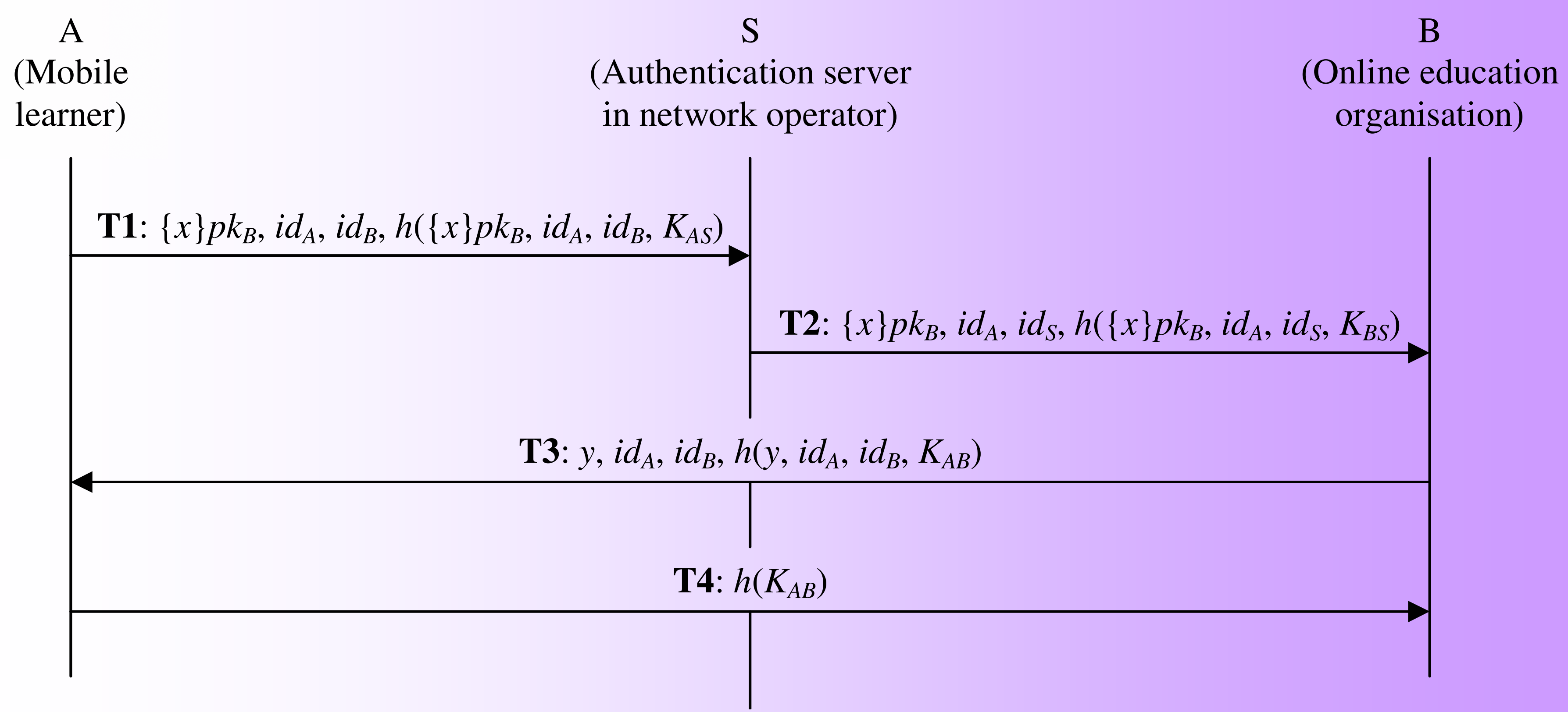
- (S5) Freshness of the session key.

Network Infrastructure



- a mobile learner
- an online education organisation
- a trusted authentication server inside the network operator

NAAP Description



NAAP Protocol Analysis (1)
- Against requirements

- Use of the authentication challenge $\{x\}pk_B$ meets the requirement S1.

- Use of K_{AS} meets the requirement S2.

- The session key K_{AB} (= $h(x, y)$) is not transmitted in clear text in any transaction, and x is always inaccessible to the public. These together meet S3.

- $h(y, id_A, id_B, K_{AB})$ in T3 confirms B's knowledge to A, and $h(K_{AB})$ in T5 demonstrates A's knowledge of K_{AB} to B. S4 is met.

- K_{AB} is computed by using two random numbers, x and y, generated by A and B. Therefore K_{AB} is fresh.

NAAP Protocol Analysis (2)
- Comparison with KAAP and AUTHMAC_DH

- All three protocol meet all security requirements.
- Each protocol requires the mobile learner to send two transactions (same communication cost).
- NAAP requires least computational cost.

Heavy cryptographic operations at mobile	**KAAP**	**AUTHMAC_DH**	**NAAP**
Number of public key encryption	1	0	1
Number of exponential operation	2	2	0

Conclusions

- Authentication requirements have been addressed.

- The current state-of-the-art work of authentication services have been investigated and evaluated.

- An novel network-assisted approach for authentication services has been proposed.

- This asymmetrical authentication protocol has been analysed with regard to the requirements and been compared with related work.

Thank you