NDN-BMS Security: Requirements and Solution

Wentao Shang (UCLA)

Application scenario

- NDN-BMS collects sensor data from UCLA campus and publishes the data into an NDN repo
- Multiple users have access to the data
- Different users have different access privileges

Security requirements

- Authenticity & Integrity: each data packet is verifiable

- Confidentiality: only authorized user can access BMS data

- Scalability: security mechanism need to scale to a large number of users

Current solution

- Authenticity & Integrity:
  - Every data packet is signed by the data publisher (a gateway connected to sensors)
  - Gateway's public key is certified by some higher-level authority (e.g., building manager), which is certified by the top manager (using the root key)
  - Every entity in the system trusts the root key

Current solution

- Confidentiality: encryption-based access control
  - All BMS data is encrypted with a symmetric key
  - Users gain access to the data by acquiring the encryption key

Encryption key distribution

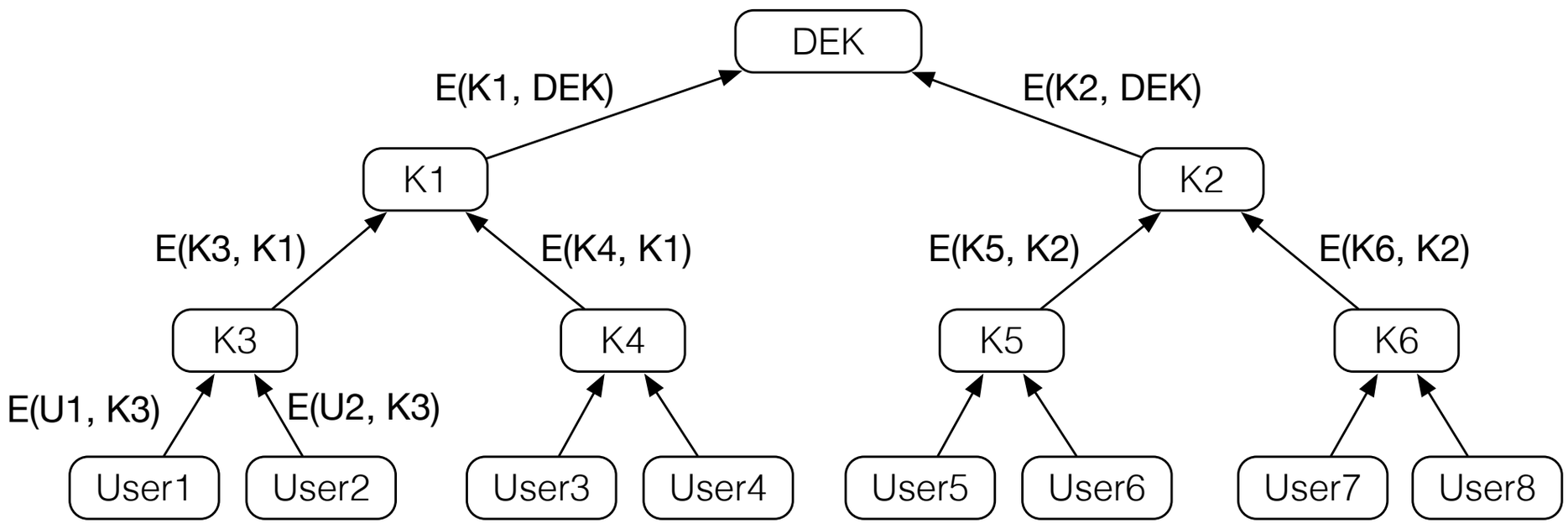
- Users are identified by their public keys
- The data encryption key (DEK) is encrypted by the authorized user' public key and published as normal NDN data
- DEK is updated periodically, or whenever a user changes privilege (e.g., adding or dropping access to some data)

Scalability issue in DEK management

- The first prototype publishes DEK for each user as a separate data packet
  - O(n) RSA encryption and O(n) RSA signing
- A simple optimization: pack all encrypted DEKs into a single data packet
  - O(n) RSA encryption and O(1) RSA signing

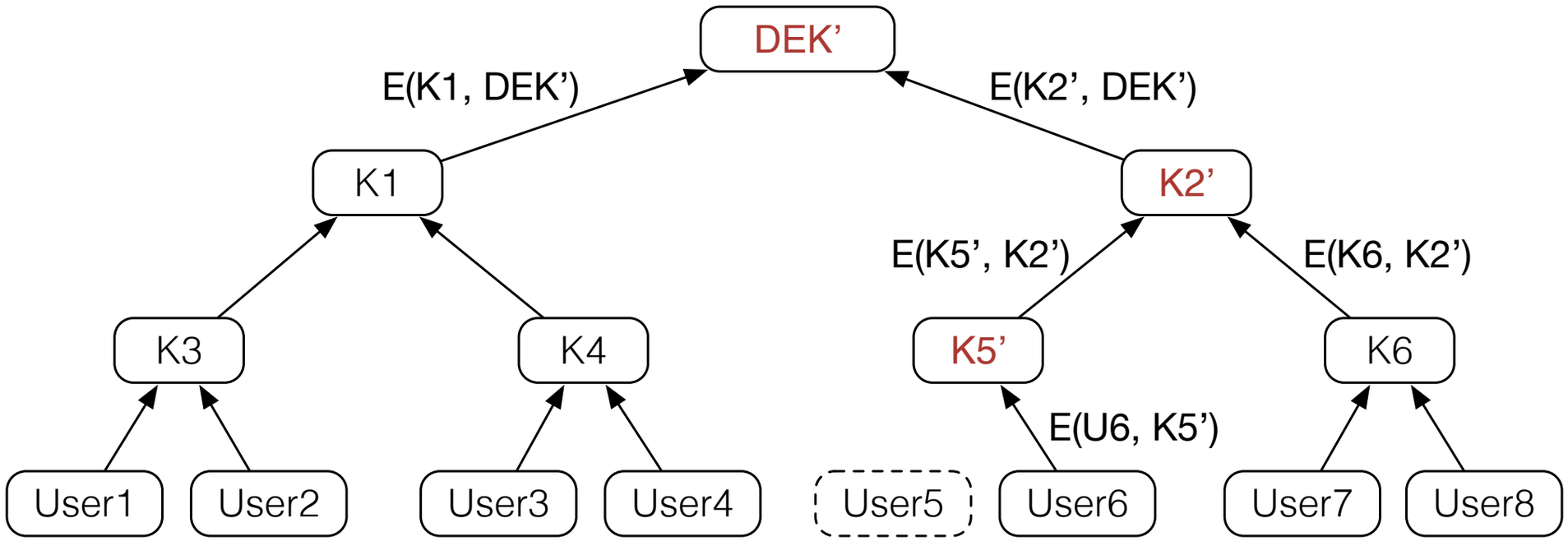
A better(?) solution

- Recommended by RFC 2627: hierarchical key management (designed for secure multicast)



Scalable user deletion

- O(log(n)) updates vs. O(n) updates in old scheme
  - Cost: more keys to manage & transmit



Other issues

- Selection of cryptography
  - Symmetric vs. asymmetric encryption
  - HMAC vs. RSA signing
- Hierarchical access control

Summary

- Encryption is the most effective access control for NDN applications
- Multicast security may be a useful reference
- Hierarchical access control is a new challenge