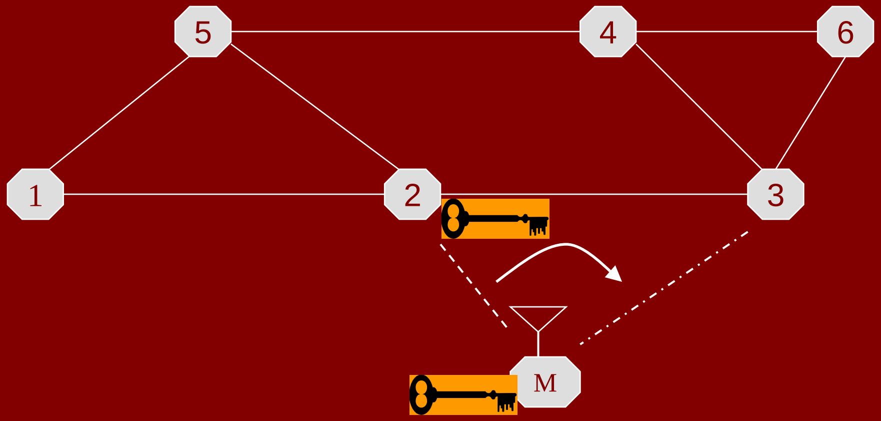
Key Management Challenges and Approaches in Mobility Applications

Lily Chen,

CSD, NIST

September 11, 2012

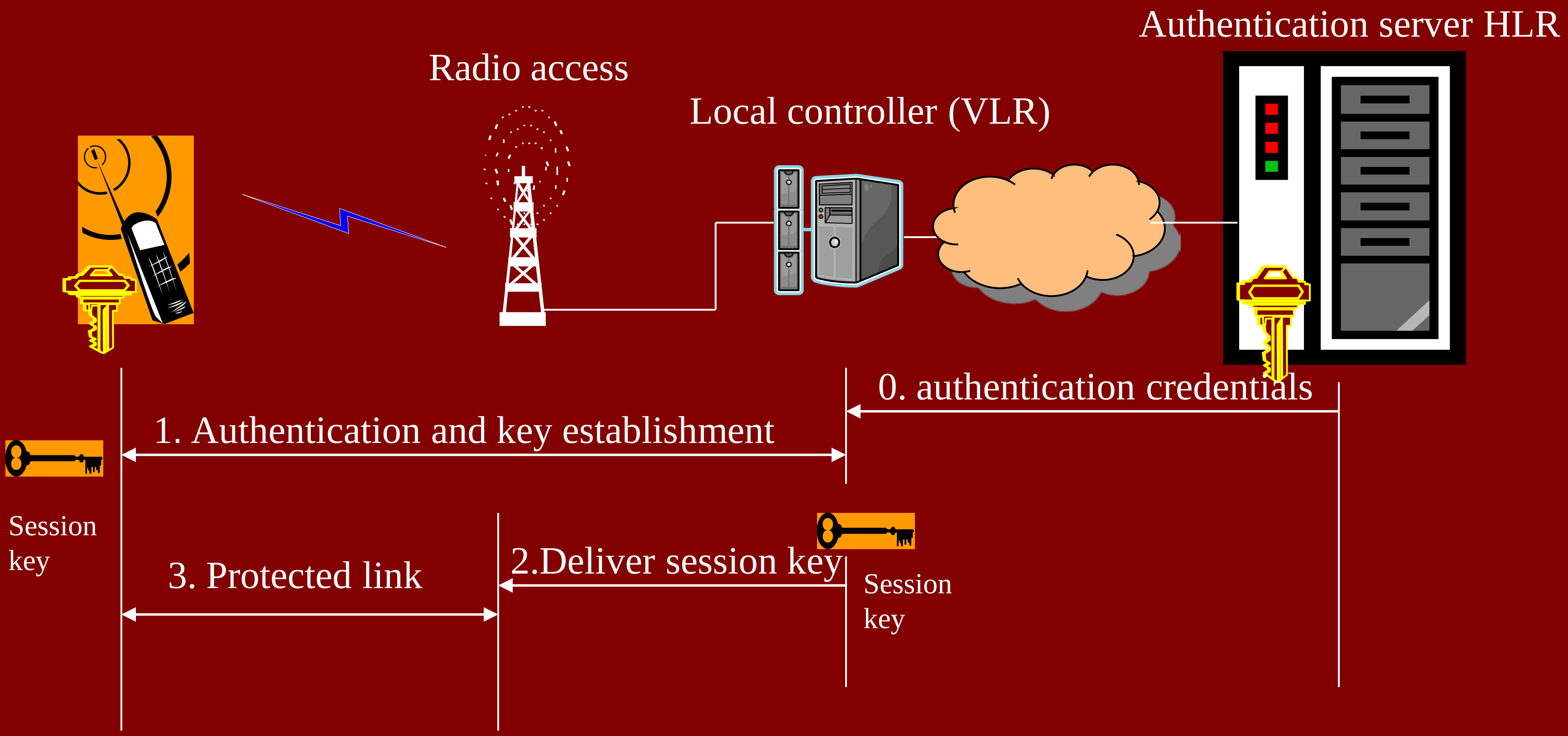


Outline

- How security link is set up in a handover
- Challenges in heterogeneous networks
- Approaches for fast security link set up
- Summary, trends and future directions

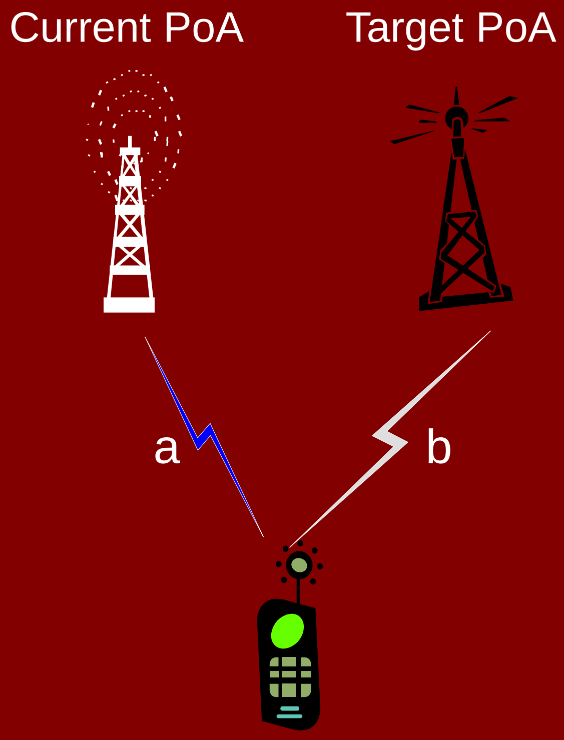
Keys for protecting communications

- Access authentication and key establishment



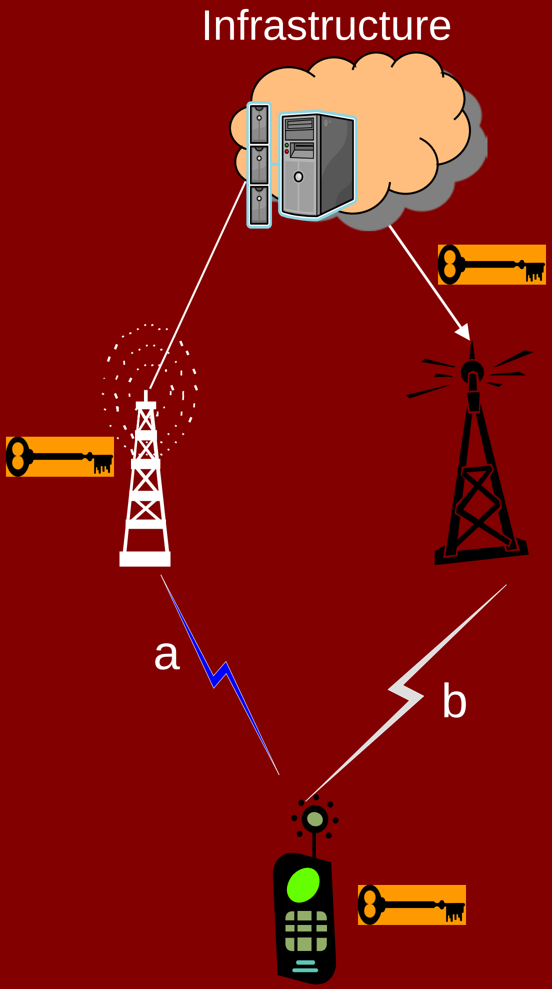
A key word – handover

- The term “handover” comes from cellular networks.
- It implies a mobile node directly switches its connection from one base station to another without executing an access authentication and key establishment.
- It requires to be
  - Fast – No interruption;
  - Secure – New link (b) is protected.
- If the term “handover” is used as a verb, then it is the network that handovers a mobile node from the current point of attachment (PoA) to a target PoA.



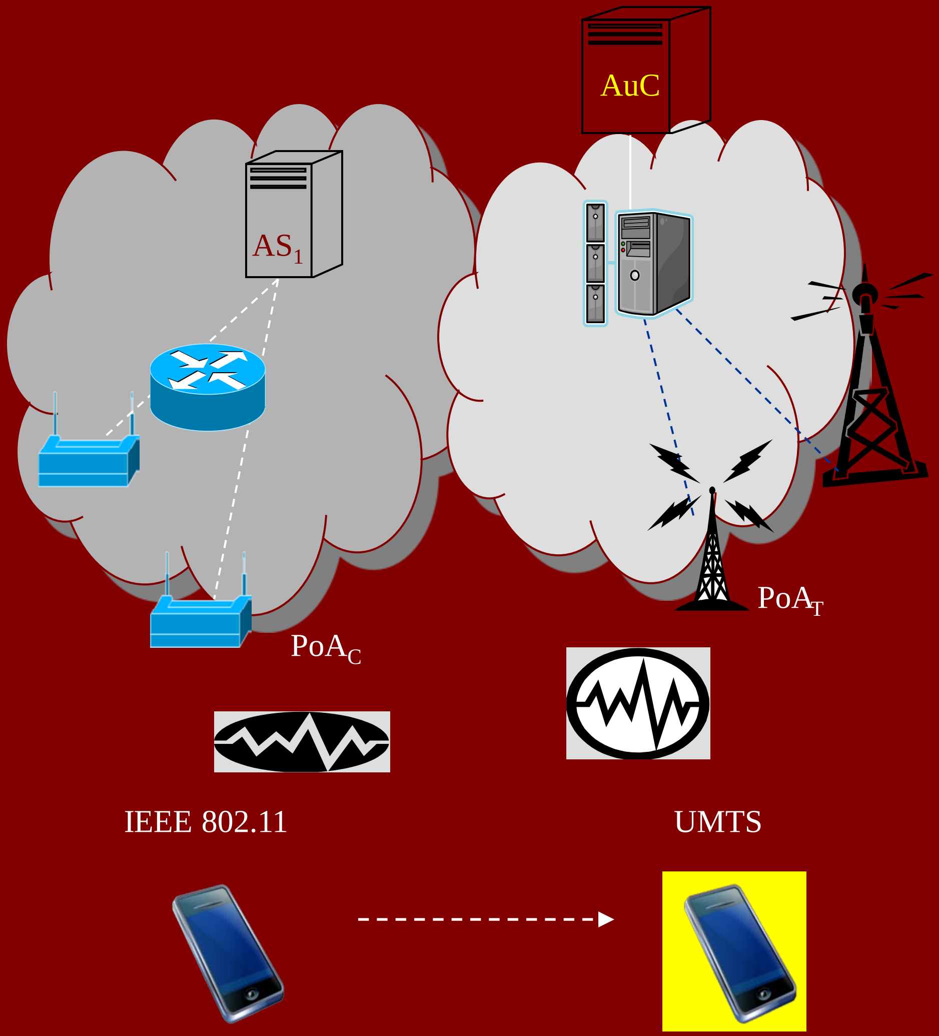
Handover keys for new security link

- In a (≤) 3G cellular network, when a handover happens, the key(s) used for protecting link “a” is handed over to the new base station to protect link “b”.
- Security link handover means key handover.
- The “infrastructure” is aware a mobile node’s where about and handles key establishment, distribution, update, and revocation.



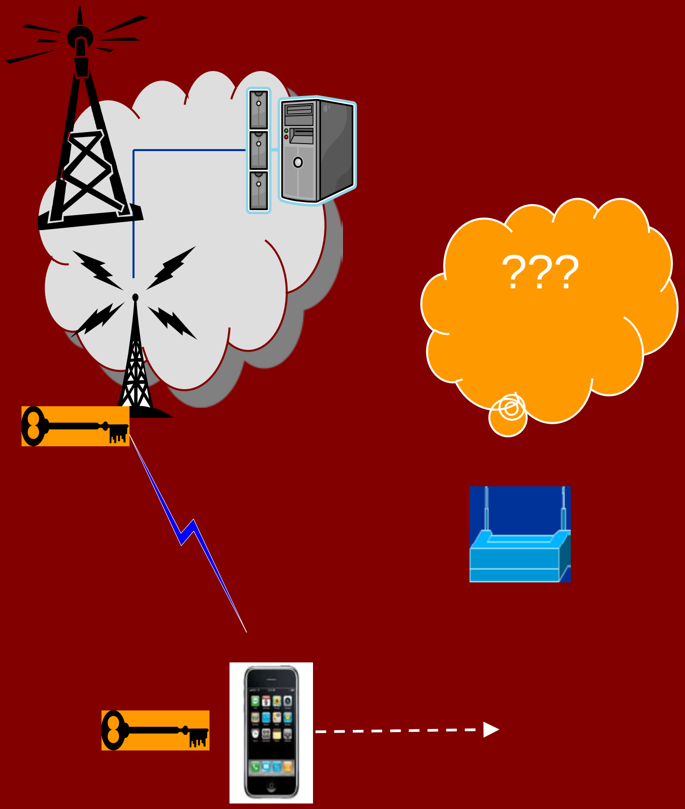
4G and beyond – heterogeneous networks

- The current and future wireless networks employ different radio access technologies.
  - Handover can happen between cellular network and other wireless networks.
- The handover may not be anticipated by the network but initiated by the mobile device.
  - The cross-media infrastructure may not exist to support the handover.
  - The target network may not authorize the connection unless a new authentication is executed. It may have to be a "re-entry" not a handover.



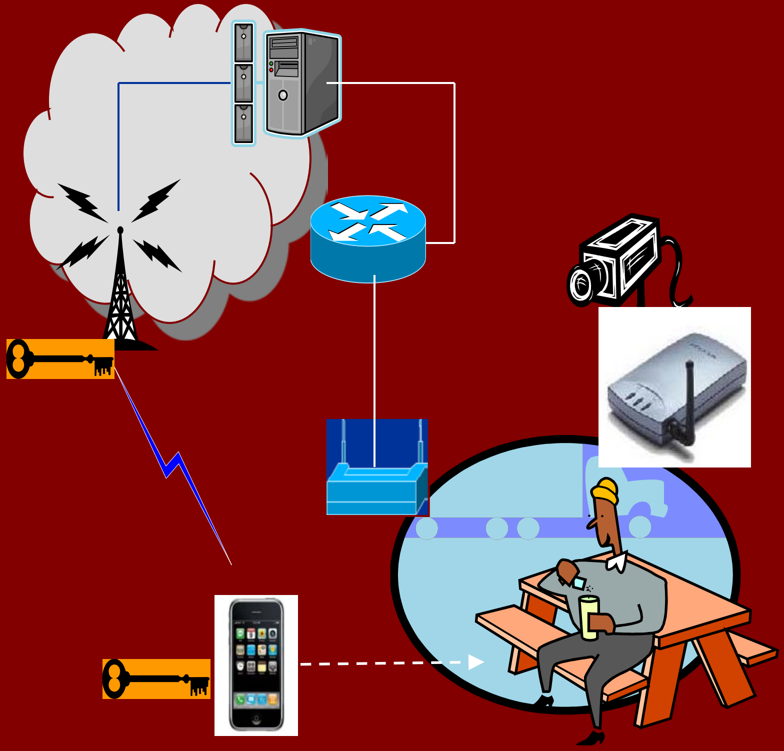
Challenge I – Lack of "Infrastructure"

- The newly emerged wireless technologies may not have the infrastructure to support all the mobility domains.
  - The network such as specified by IEEE 802.11 (WLAN) was not designed to support mobility.
  - The fast transition was an add-on to resolve from one basic service set to another (IEEE 11r). It does not support "handover" in general.
  - The so called "roaming agreement" for cellular operators can hardly apply to a network without an "operator" per se.
- Without infrastructure support, security status cannot be handed over.



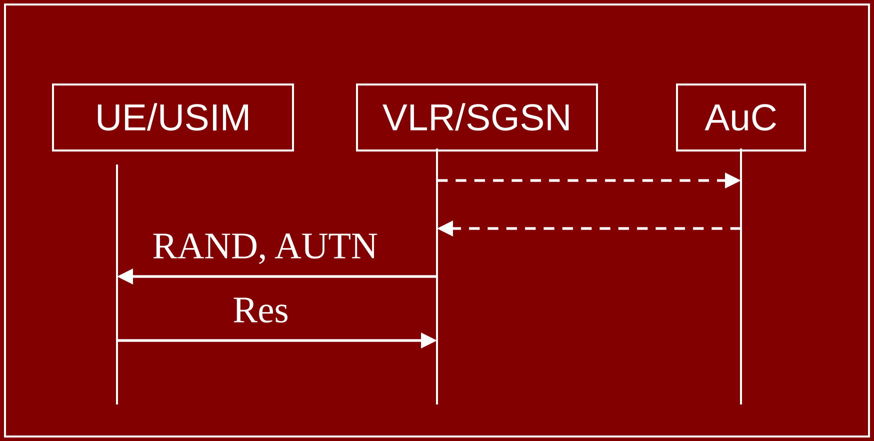
Challenge II – Trust/threat model

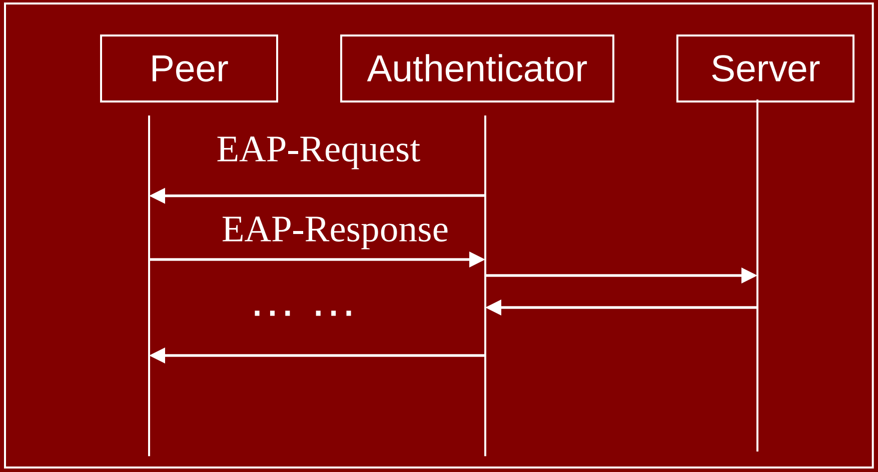
- Different wireless technologies employ different trust models.
  - Cellular network tends to consider a base station physically secure and expensive to clone. As a result, for example, in UMTS, the same session keys are used by different base stations and valid for a long time.
  - The newly emerged wireless technology such as specified by IEEE 802.11 (WLAN) considers an access point (AP) at a high risk to be physically attacked.
    - The session keys used for different APs must be separate.



Challenge III – Access authentication

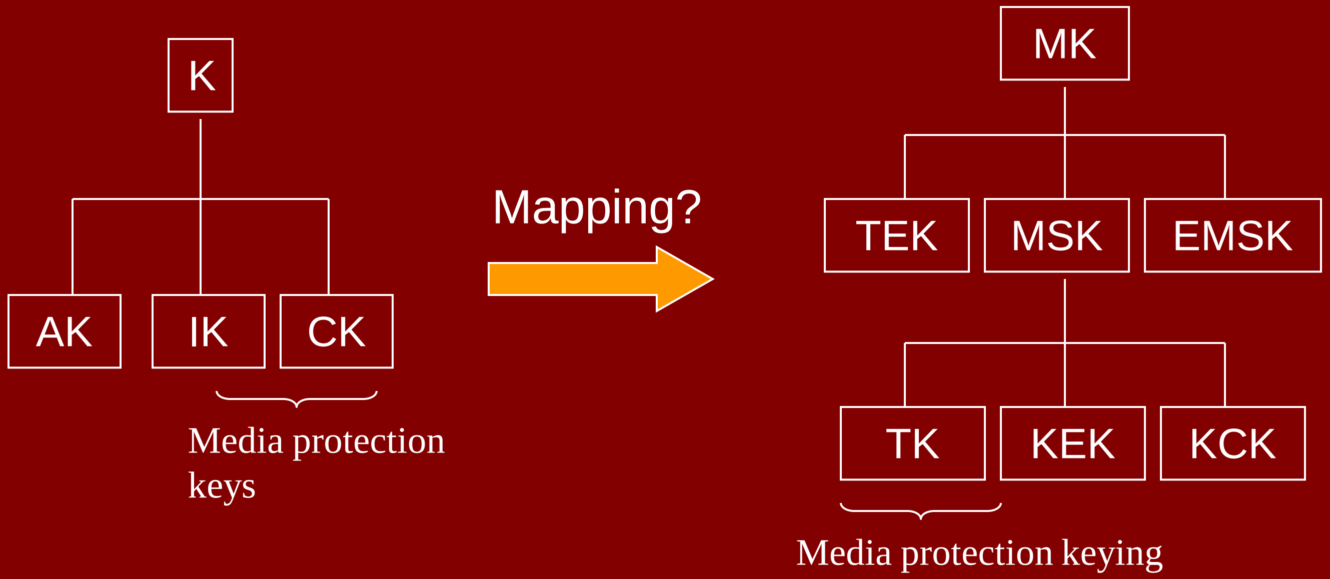
- Different access networks may use different authentication methods with, possibly, different credentials.
  - UMTS/LTE uses USIM card (symmetric key) and AKA for subscriber authentication.
  - IEEE 802.11 uses EAP, which can be, for example, EAP-TLS (public key certificates).
- When a handover happens from one network authenticated with AKA to a network authenticated with EAP, the authenticated status may not be handed over as well.
- Even with the same authentication method, roaming from one domain to another may not be covered under any roaming agreement.





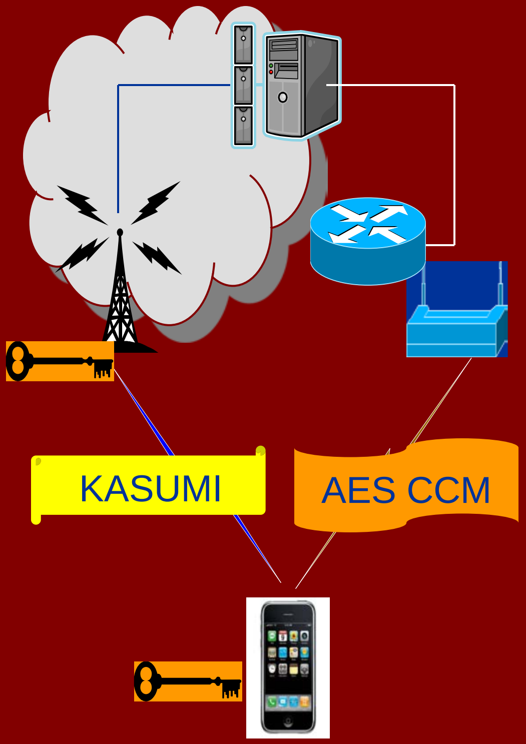
Challenge IV – Key hierarchy

- Different authentication protocols will end up with different key hierarchies.
  - UMTS AKA derives a two tier key hierarchy.
  - EAP derives a MSK from master-secret, which will be used to generate session keys.
- Regardless trust model and authentication method, when a handover happens from one network to another, it is impossible to handover keys unless a mapping exists to match two key hierarchies.



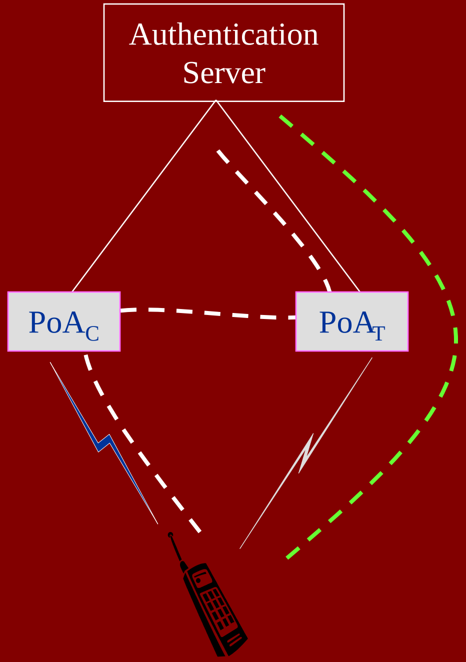
Challenge V – Protection mechanisms

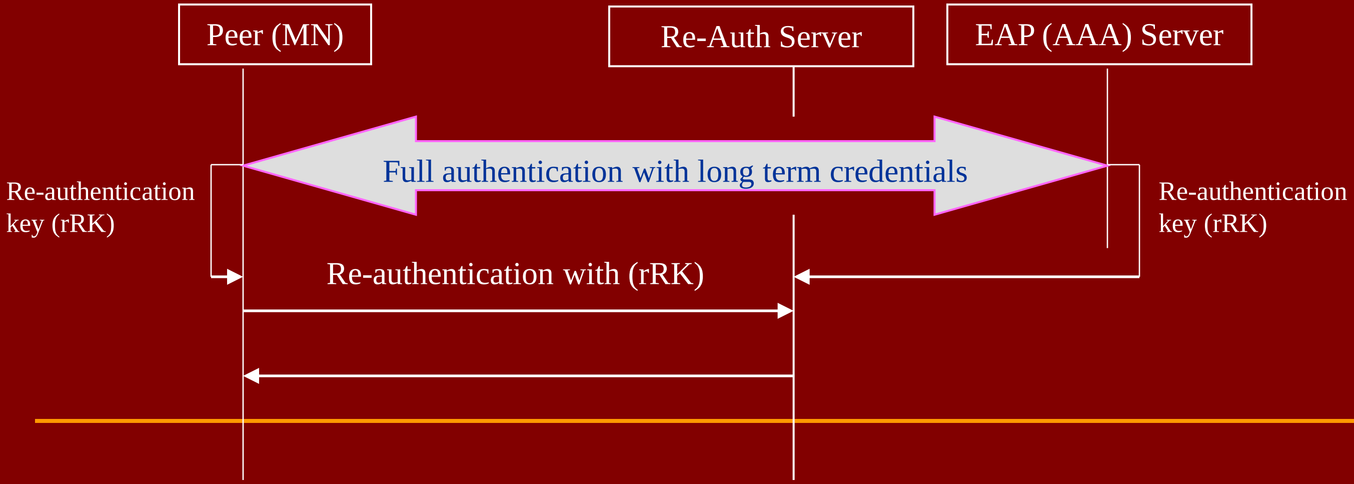
- Different radio access technologies use different protection mechanisms.
  - Cellular network traditionally uses algorithms specified in a specific standard, e.g. KASUMI and SNOW 3G for UMTS
  - IEEE 802.11 uses WEP, TKIP, or AES CCM.
- Even though key handover is possible, the same key shall not be used in different algorithms.



Approach I – Fast authentication and session key establishment

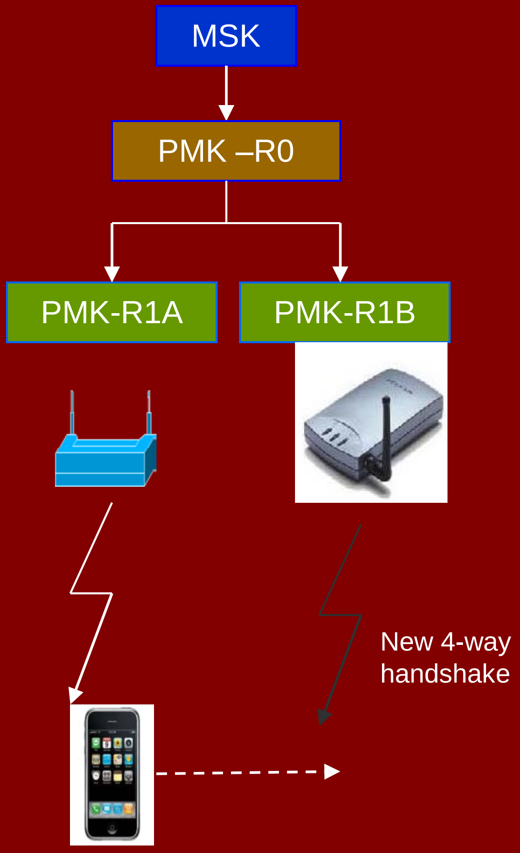
- Pre-authentication
  - Execute authentication before handover.
    - Use the current link;
    - Use the new link.
- Re-authentication
  - Establish keys in a full authentication for different local servers;
    - A re-authentication uses a local key with less message round trips.

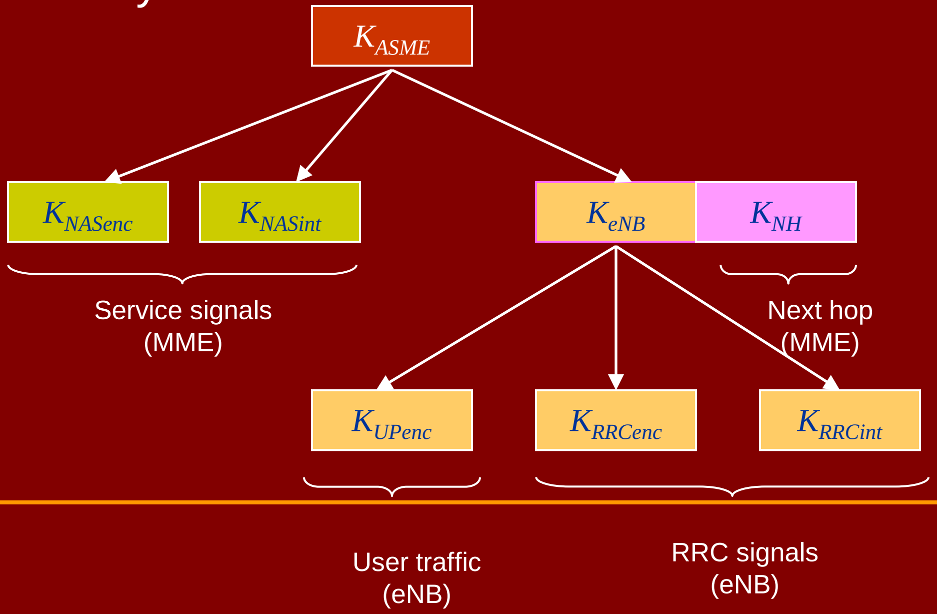



Peer (MN)
Re-Auth Server
EAP (AAA) Server
Full authentication with long term credentials
Re-authentication key (rRK)
Re-authentication key (rRK)
Re-authentication with (rRK)

Approach II – Key separation

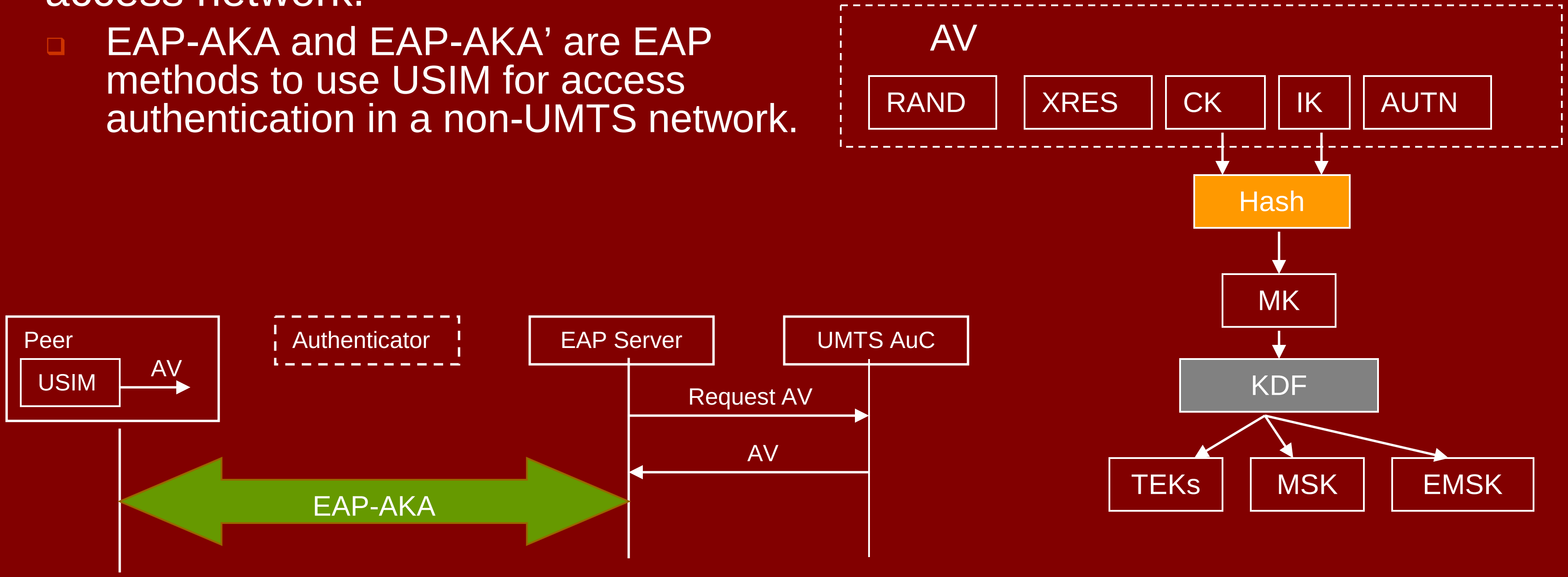
- LTE introduces a new key hierarchy to separate keys for
  - Service signals, user traffic, and radio resource control;
  - Different eNBs (base stations) using next hop key.
    - Not directly handover keys.
- IEEE 802.11 developed new key hierarchy for fast BSS transition.
  - Each AP obtains a key to be used to derive session keys.





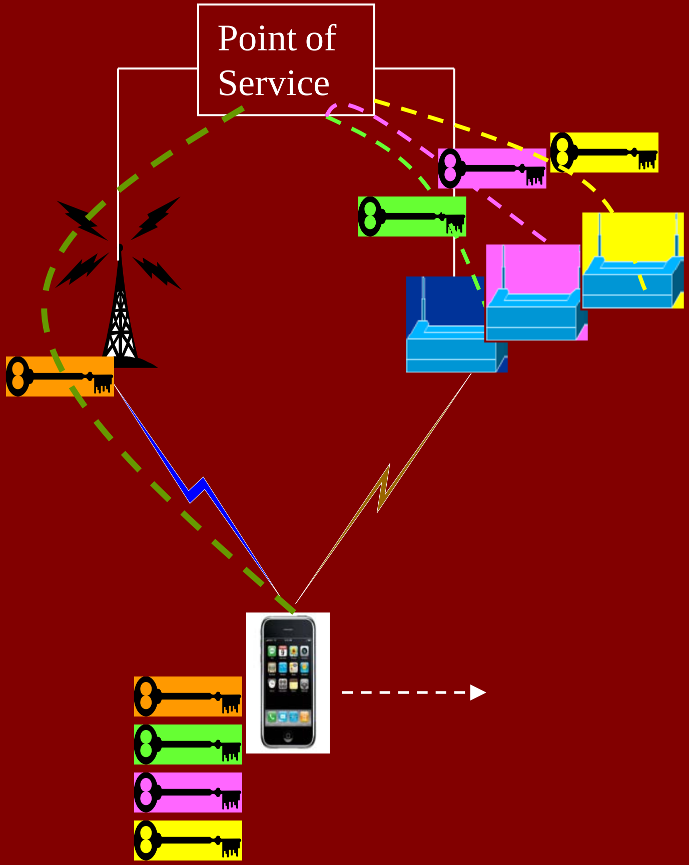
Approach III – Same credentials for different access networks

- For the services through one provider or a enterprise domain, same credentials are used for different access network.
  - EAP-AKA and EAP-AKA’ are EAP methods to use USIM for access authentication in a non-UMTS network.



Approach IV – Media independent handover service for key distribution

- Media independent handover services are specified in IEEE 802.21.
- The security services enable proactive authentication and media independent key distribution.
  - Push key distribution;
  - Reactive pull key distribution;
  - Optimized proactive pull key distribution.



Summary and future directions

- Heterogeneous networks challenged traditional key management method for mobile applications.
- The main idea for all the approaches is to use less trust assumptions and replace the session keys more frequently.
- The approaches have been developed piece by piece and a more general framework is needed for service providers (operators) to manage cryptographic keys for inter-domain and inter-technology mobility.
- Media and service independent key management is a right direction but will take a long time to launch.