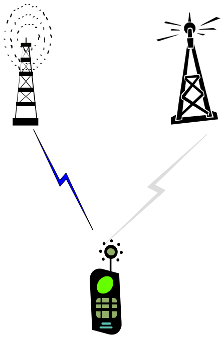
Mobility Protection

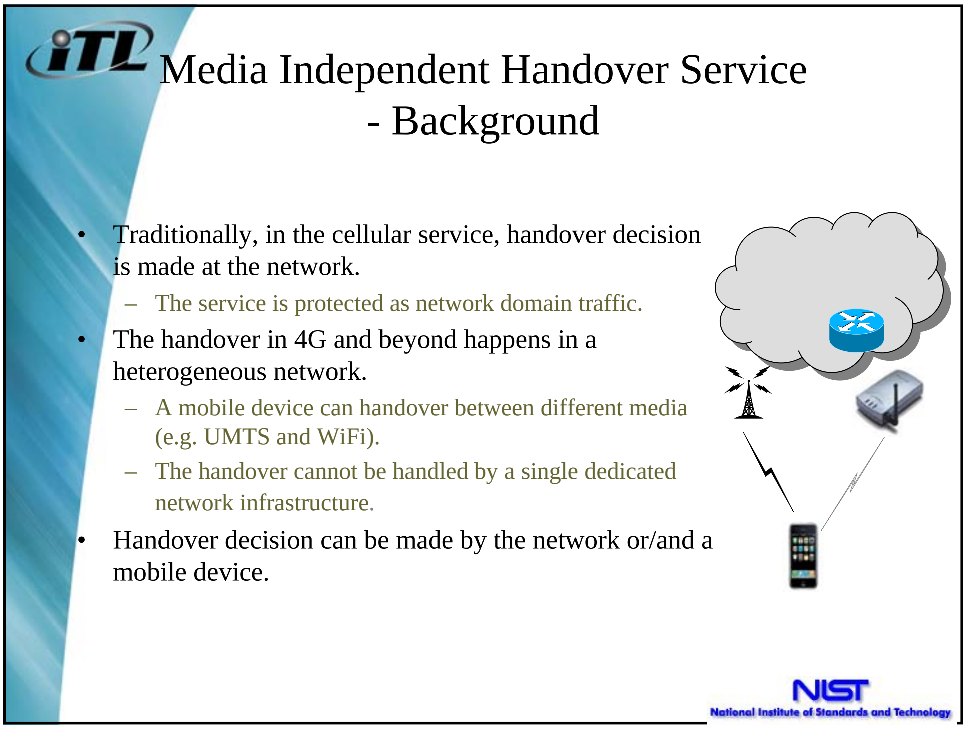
ISPAB
February 2012

Lily Chen
Computer Security Division
Cryptographic Technology Group

Mobility Protection (3 aspects)

1. Communication Protection (Link layer)
   - Protect data traffic over radio interface;
   - When a mobile device moves, establish new protections.
2. Mobility information protection (IP layer)
   - Authenticated IP address update in Mobile IP
3. (Focus on)Mobility service protection (application layer)
   - Media independent handover (MIH) service.

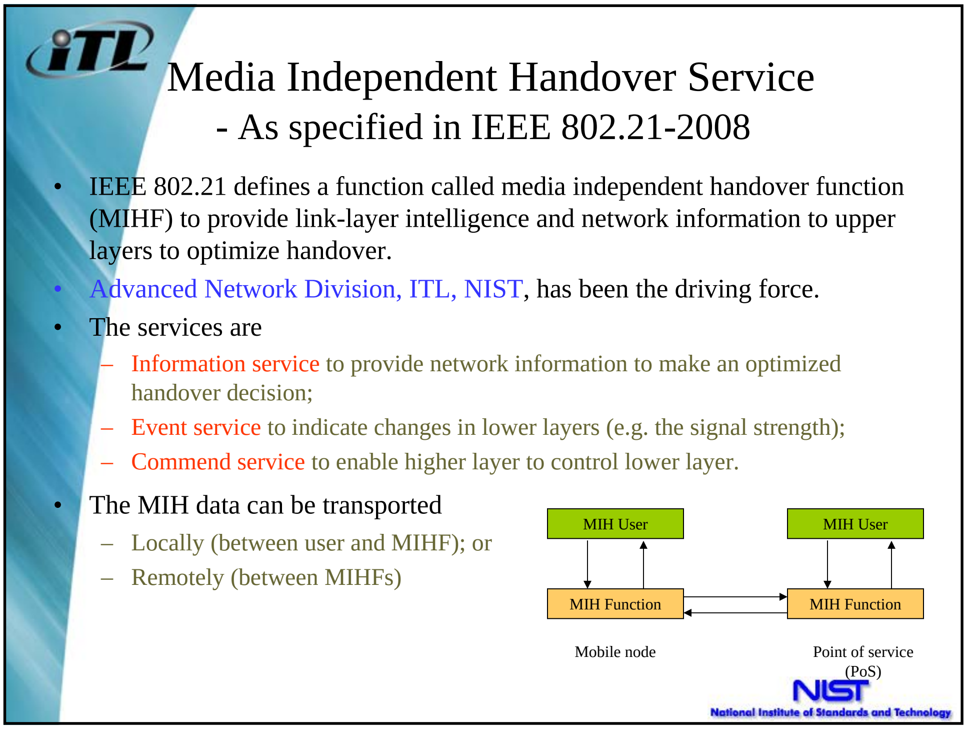




Media Independent Handover Service - Background

- Traditionally, in the cellular service, handover decision is made at the network.
  - The service is protected as network domain traffic.
- The handover in 4G and beyond happens in a heterogeneous network.
  - A mobile device can handover between different media (e.g. UMTS and WiFi).
  - The handover cannot be handled by a single dedicated network infrastructure.
- Handover decision can be made by the network or/and a mobile device.

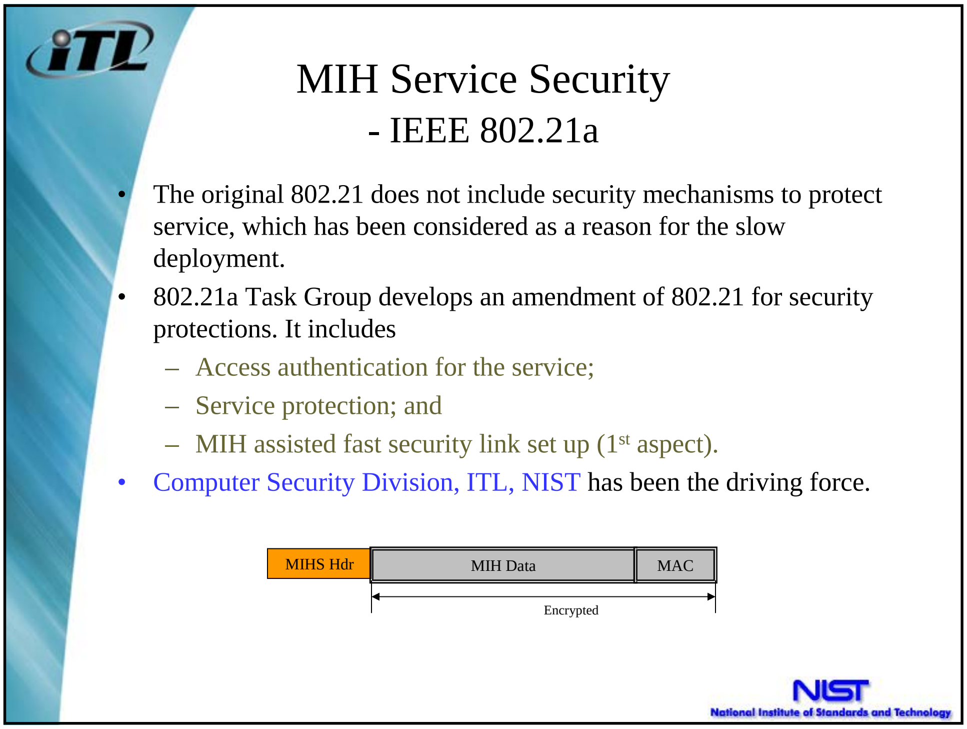
NIST
National Institute of Standards and Technology



Media Independent Handover Service - As specified in IEEE 802.21-2008

- IEEE 802.21 defines a function called media independent handover function (MIHF) to provide link-layer intelligence and network information to upper layers to optimize handover.
- Advanced Network Division, ITL, NIST, has been the driving force.
- The services are
  - Information service to provide network information to make an optimized handover decision;
  - Event service to indicate changes in lower layers (e.g. the signal strength);
  - Commend service to enable higher layer to control lower layer.
- The MIH data can be transported
  - Locally (between user and MIHF); or
  - Remotely (between MIHFs)

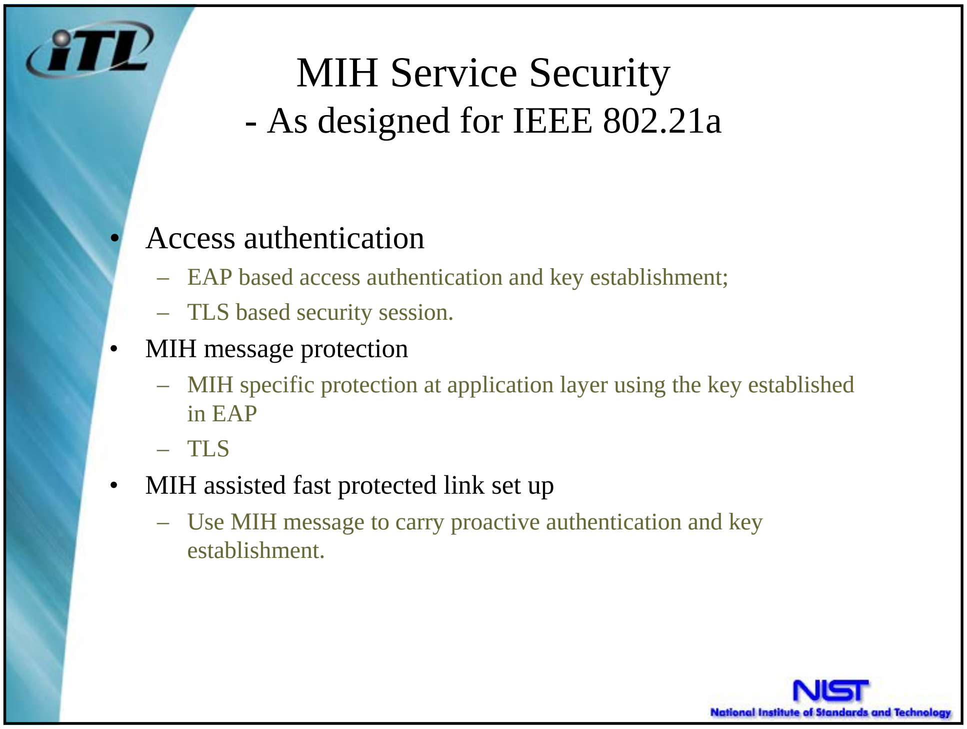
NIST
National Institute of Standards and Technology



MIH Service Security
- IEEE 802.21a

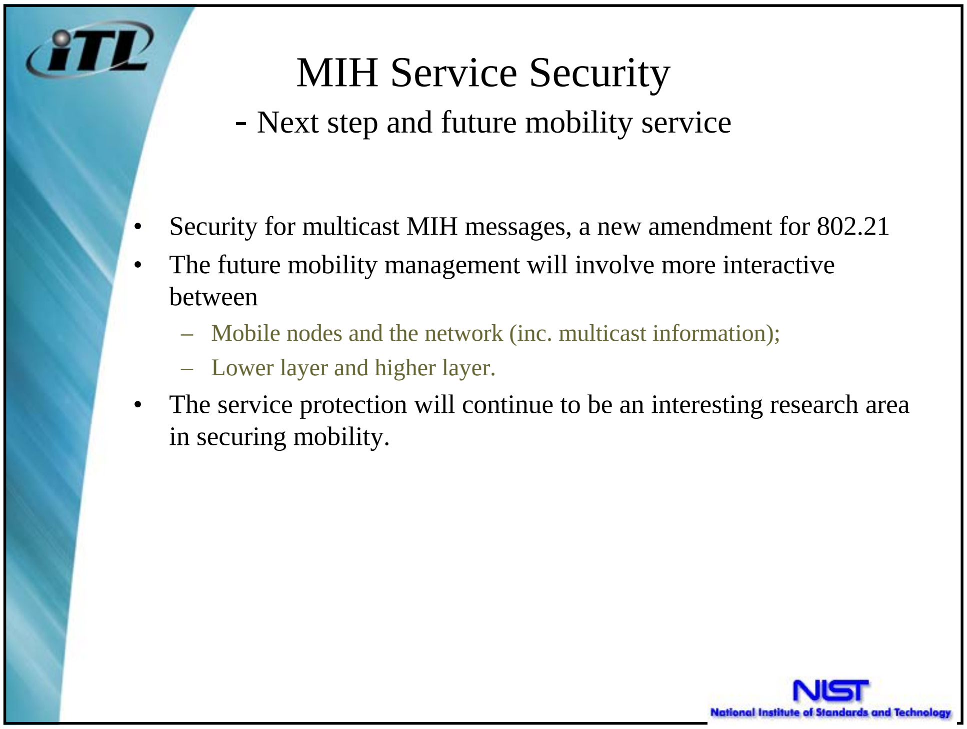
- The original 802.21 does not include security mechanisms to protect service, which has been considered as a reason for the slow deployment.
- 802.21a Task Group develops an amendment of 802.21 for security protections. It includes
  - Access authentication for the service;
  - Service protection; and
  - MIH assisted fast security link set up (1st aspect).
- Computer Security Division, ITL, NIST has been the driving force.

MIHS Hdr
MIH Data
MAC
Encrypted



MIH Service Security
- As designed for IEEE 802.21a

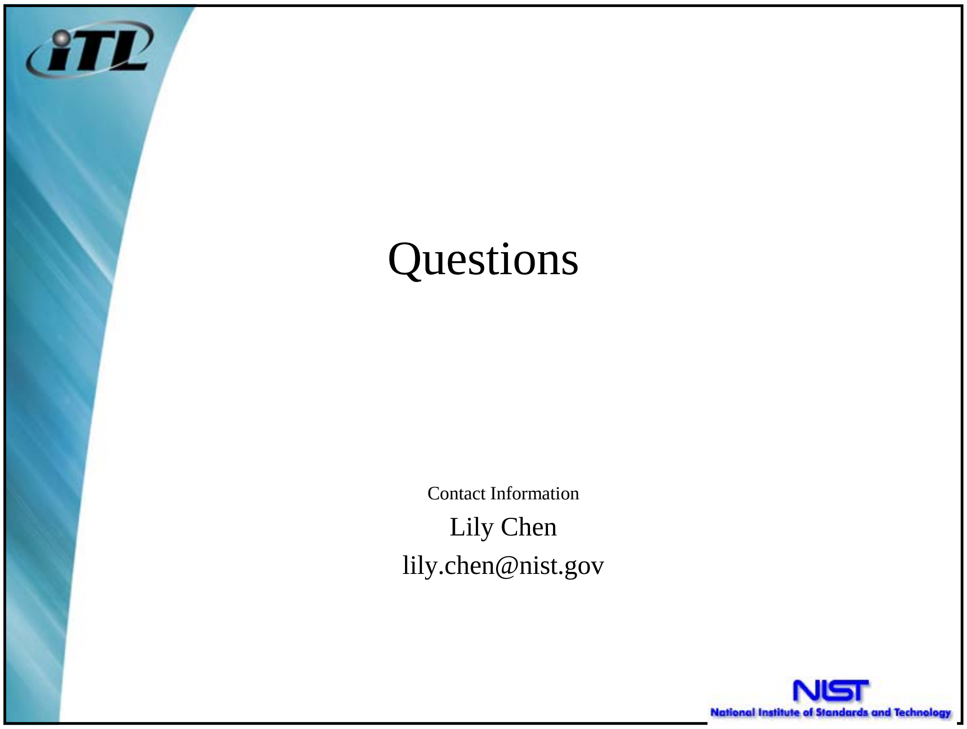
- Access authentication
  - EAP based access authentication and key establishment;
  - TLS based security session.
- MIH message protection
  - MIH specific protection at application layer using the key established in EAP
  - TLS
- MIH assisted fast protected link set up
  - Use MIH message to carry proactive authentication and key establishment.



MIH Service Security

- Next step and future mobility service

- Security for multicast MIH messages, a new amendment for 802.21
- The future mobility management will involve more interactive between
  - Mobile nodes and the network (inc. multicast information);
  - Lower layer and higher layer.
- The service protection will continue to be an interesting research area in securing mobility.



Questions

Contact Information

Lily Chen

lily.chen@nist.gov