Mobility in Heterogeneous 4G networks using Mobile IP

Charles E. Perkins
charliep@computer.org
Miracle: November 10, 2011

tellabs®

Where is Mobile IP in 4G?

- LTE design loses the simplicity and power of IP mobility
  - Per-application handovers
  - Per-radio technology handovers

➔ Complicated heterogeneous handovers within LTE

- additional operational expense
- more difficult interoperability testing (IOT)
- more expensive and longer development cycles
- reduced functionality
- difficulty for future extensibility
- poorer user experience.

Future Internet is "all mobile". Will IETF be relevant?

Modular view of Mobile IP design

- Address space mgmt
  - Home agent intercepts / manages home address
  - assignment / acquisition of care-of address
  - → very efficient instance of a "locator / ID" style solution
- Tunnel management
  - IPv*-within-IPv*, GRE, "minimal", routing header
  - reverse tunnel control
- Authentication / authorization services
  - IPv4 authentication extensions
  - IPsec
  - AAA interface

These modular components are crucial for LTE

Possible defects of Mobile IP (from the point of view of 3GPP)

- Wrong tunnel protocol
- Wrong security
- Wrong home agent architecture
- Client-controlled approach disfavored
- AAA interface favorable to IP-address based bookkeeping, not session-based
- No desire for statistical multiplexing?
- Why enable seamless handovers to competitor's networks?
- Misunderstanding the power of layer-3 approach
- Mobile context types of interest to 3GPP not defined

Wrong tunnel protocol

- **Operators have a huge investment in GTP. GTP has been refined for many years, with numerous extensions (Information Elements) added over time**
- **Tunnel setup in Mobile IP appears oversimplified; many more traffic controls are specified for GTP.**
  - **Operations for optimizing data-plane are missing (never explicitly part of any Mobile IP design criteria)**
  - **Accounting controls missing from Mobile IP tunneling**
  - **Many other controls not present in Mobile IP (needed or not?)**

Wrong tunnel protocol: Solutions

- **part 1: Enable home agent to utilize alternative encapsulations, make extensible by protocol number (e.g., GTP == NNNN)**
  - draft-perkins-mext-gtpdata needs update
- **part 2 (alternative 1): Identify modular classification of the accounting and traffic management controls existing within GTP-C, duplicate within BU/PBU**
- **part 2 (alternative 2): Enable GTP-C as a control interface to the data-plane features of the home agent (more on this later)**

Incompatible security design

- Mobile IPv4 specifies relatively simple extensions to basic control signaling to assure authentication
- Mobile IPv6 specifies IPsec
- Problem: mobile devices rarely implement IPsec or MIP
- Problem: 3GPP security architecture has evolved along a certain path over time, and Mobile IPv6 does not make that available, requiring IPsec / IKE instead
- Problem for non-LTE handover: access authentication is done separately from authentication for signaling tunnel management from the home network

Incompatible security design: Solutions

1. **Allow home agent to invoke alternative security mechanisms, using SPI of authentication data header**
   - draft-patil-mext-mip6issueswithipsec
2. **Enable integration of access authentication with authentication used for tunnel retargeting. Note: in some cases, same AAA is used for both anyway.**
   - draft-perkins-netext-eapbu, for example
3. **Show Mobile IP authentication satisfies 4G req's**
   - **mobile can verify authenticity of the network**
   - **network can verify the authenticity of the mobile**
   - **additional crypto parameters do not improve**

Wrong home agent architecture

- **4G network designed to separate mobility management control plane from data-plane tunneling through the packet core.**
- **Needed: separation of home agent into control plane and data plane modules.**
- **Solution part 1: enable alternative HA tunnel address so the mobile receives incoming tunneled packets from expected IP address, and delivers encapsulated outgoing packets to desired gateway address.**
  - draft-perkins-mext-hatunaddr, for example
- **Solution part 2: control plane ←→ data plane interface**

Client-controlled approach disfavored

- Solution: PMIP for network-controlled operation
  - but see next slide
- Solution not in use: DSMIPv6 in LTE specifications
  - operator policy? perceived as redundant?
- Analysis needed to precisely characterize trade-offs for client-based versus network-based approach
  - Windows Mobile IP client “rare”
  - Network-based policy enforcement
  - Loss of operator control

Session-based accounting

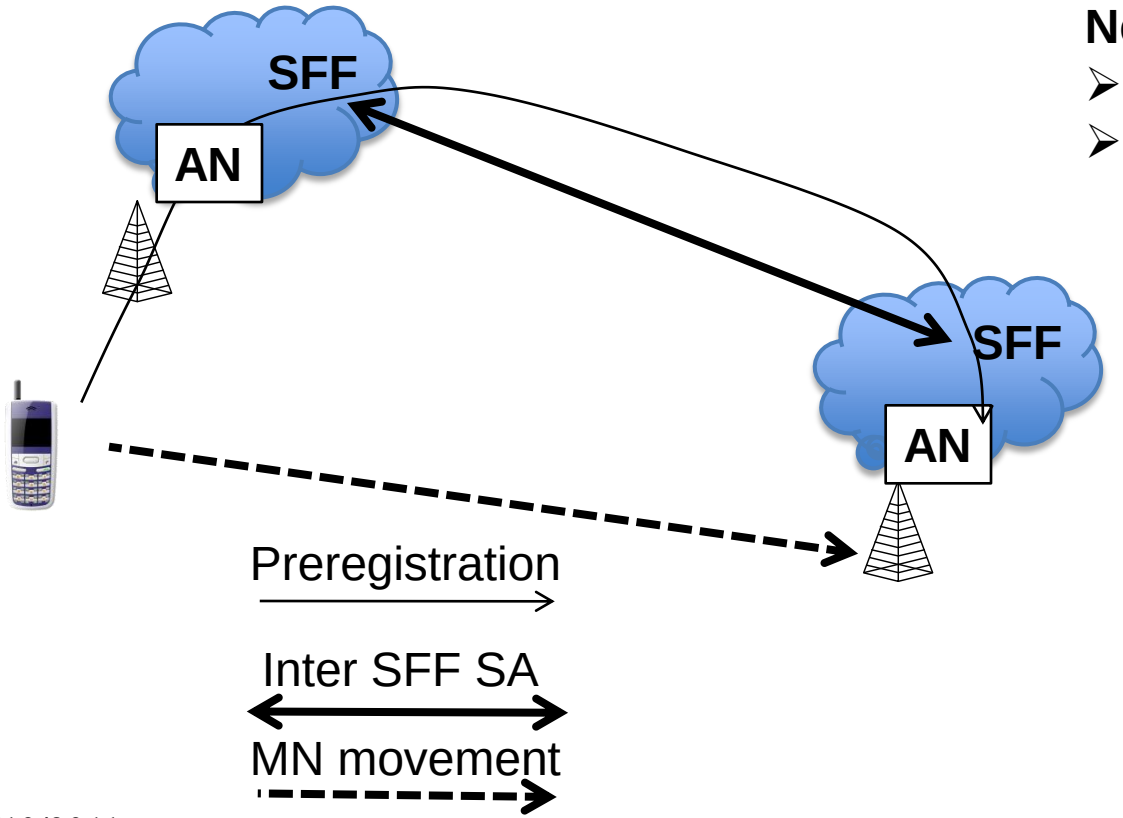
- GTP has features to enable per-session accounting, which have not been specifically enabled for PMIP.
- Solution: Use GRE key as tunnel endpoint identifier (TEID), and specify new mechanisms to tie GRE/TEIDs into existing accounting mechanisms for 3GPP.
  - Including new session controls a la GTP-C?
- Analysis needed for understanding trade-off between added complexity of session-based signaling versus simple connectionless model of operation.
  - Can current session management handle shorter sessions, huge growth, WiFi offload, …?

Heterogeneous handovers

- Characterize need for IP-address continuity
  - real-time applications
  - lengthy transactions
- Identify specific RATs/use cases
  - Needed for WiFi “offload”
- Compare user experience
  - Users are now trained to expect bad performance [URP]
- Future need for vehicular
- Single-radio advantage
- SFF-based approach (described next) versus PAR/NAR
- high-speed WLANs versus 4G speeds

SFF-oriented roaming agreement

- SFF (Signal Forwarding Function) enables pre-registration and pre-authentication of mobile node in target Access Network
- Especially valuable for single-radio devices
- Specified in IEEE 802.21c -- e.g., for WiMAX, WiFi, potentially LTE



Needed / useful:

- Security
- Location Assist

Access Information Database

- Assistance for heterogeneous network handovers
- Per-operator database authoritative for network
- Mobile to access information on demand
  - 3GPP has ANDSF
  - IEEE 802.21 has MIIS
  - IETF has PAWS
  - Seamoby CARD not used; should have been revisited?
- Commercial access-point information database – useful for WiFi, for example

Access model for roaming partners

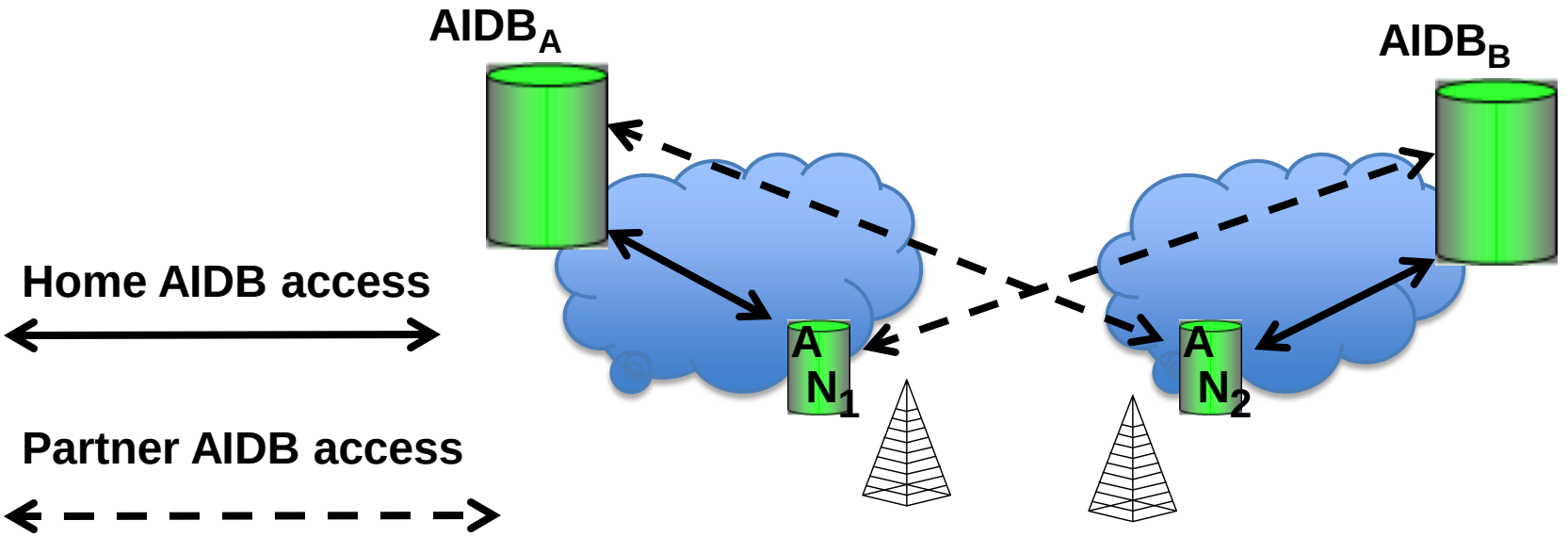
How does one operator provide all the information useful to its customers that have heterogeneous radios?

- **May be authoritative for only one radio technology (RAT)**
- **Access needed to authoritative data from roaming partners (at least)**
- **Partner information should be cached by operator to avoid frequent cross-network access**
- **Even more important for “single-radio” solutions**
- **Needed: cross-network database access – so that each operator can fetch and provide to UEs authoritative data**

Proposal: local caching

- For fastest response, UE should receive local access information from a local cache agent
- Only information about local neighborhood(s) kept
- Basestations often have overlapping neighborhoods
- Same database access mechanism can be used by roaming partners and local cache agents
  - But, likely restricted to specific neighborhood only
  - Access formats, triggers to be defined
  - Publish/subscribe model a good choice
  - Caching policy restrictions for per-UE information

AIDB per operator network useful for handovers



- Operators A and B are roaming partners
- Access network AN_1 overlaps access network AN_2
- AIDB cache AN_1 subscribes to small part of $AIDB_A$ (Operator A)
- AIDB cache AN_1 subscribes to small part of $AIDB_B$ (Operator B)