Wireless Network Security

Spring 2015

Patrick Tague

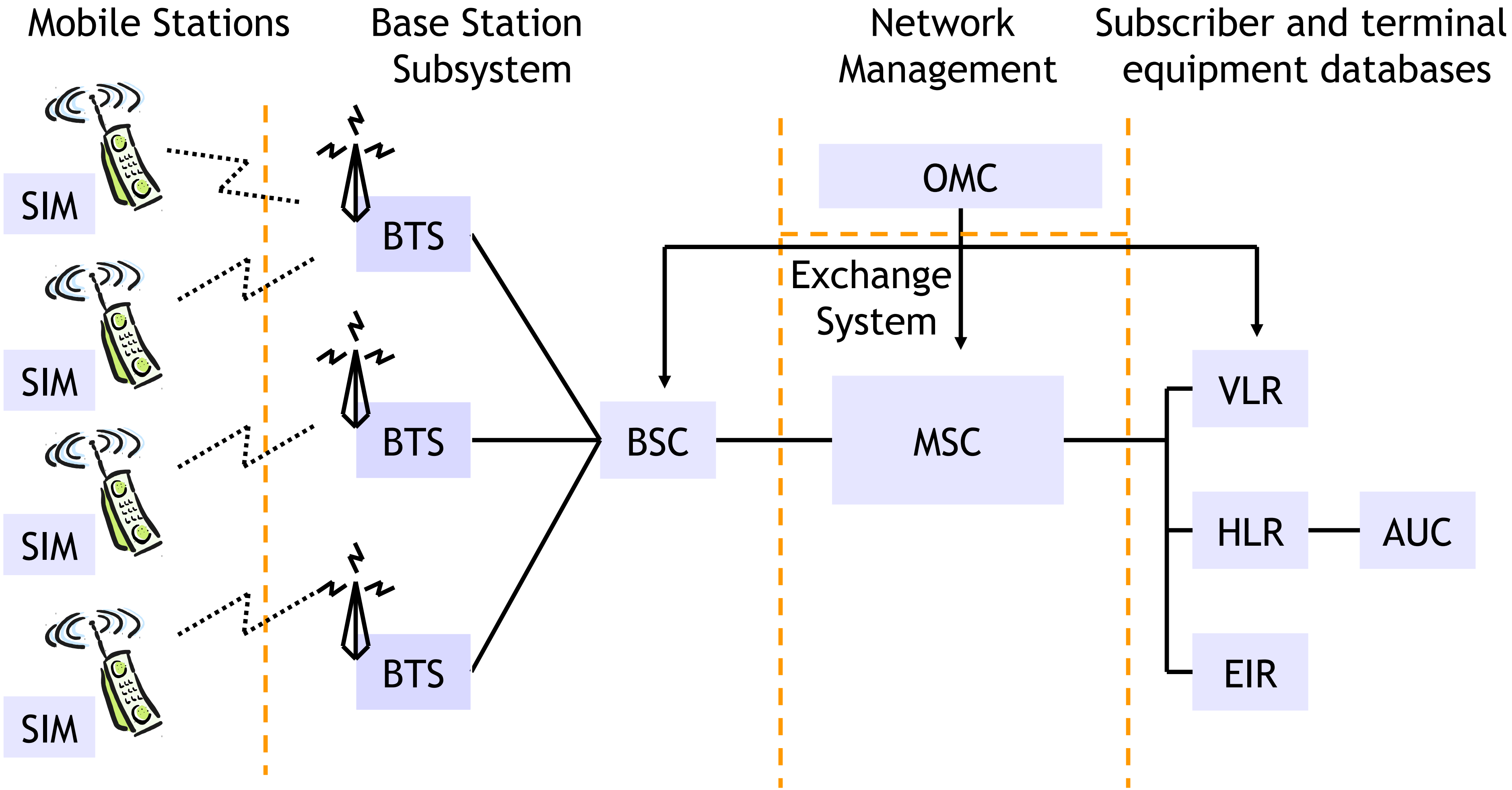
Class #21 – Telecom Security & Privacy

Class #21

- Past and current S&P concerns in mobile networks
- Possible future S&P issues in mobile networks
- Several open research areas

Let's talk about mobile networks

2G GSM/CDMA Architecture



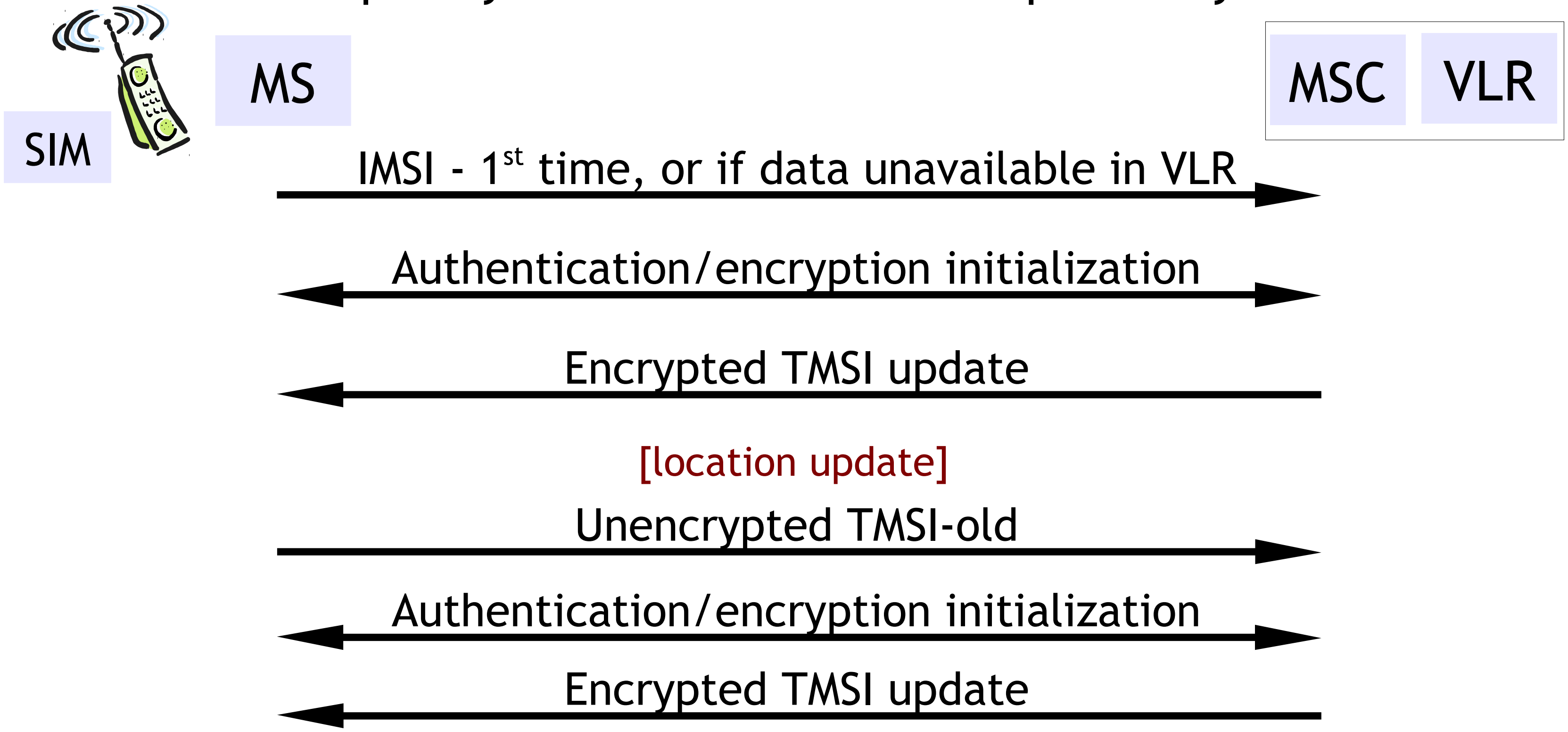
adapted from [M. Stepanov; http://www.gsm-security.net/]

2G GSM Security

- Secure access
  - User authentication for billing and fraud prevention
  - Uses a challenge/response protocol based on a subscriber-specific authentication key (at HLR)
- Control and data signal confidentiality
  - Protect voice, data, and control (e.g., dialed telephone numbers) from eavesdropping via radio link encryption (key establishment is part of auth)
- Anonymity
  - Uses temporary identifiers instead of subscriber ID (IMSI) to prevent tracking users or identifying calls

Temporary ID Management

- User and device identity:
  - IMEI: Int'l Mobile Equipment ID - device
  - IMSI: Int'l Mobile Subscriber ID - user
  - TMSI: Temporary Mobile Subscriber ID – pseudonym



IMSI - 1st time, or if data unavailable in VLR

Authentication/encryption initialization

Encrypted TMSI update

[location update]

Unencrypted TMSI-old

Authentication/encryption initialization

Encrypted TMSI update

3G Evolution

- The move from 2G to 3G primarily included:
  - Support for mobile data at (near-)broadband rates
    - UMTS, TD-CDMA, WCDMA, CDMA-3xRTT, TD-SCDMA, HSDPA, HSUPA, HSPA, HSPA+
  - Improved security protocols
    - Because everything in 2G was broken several ways

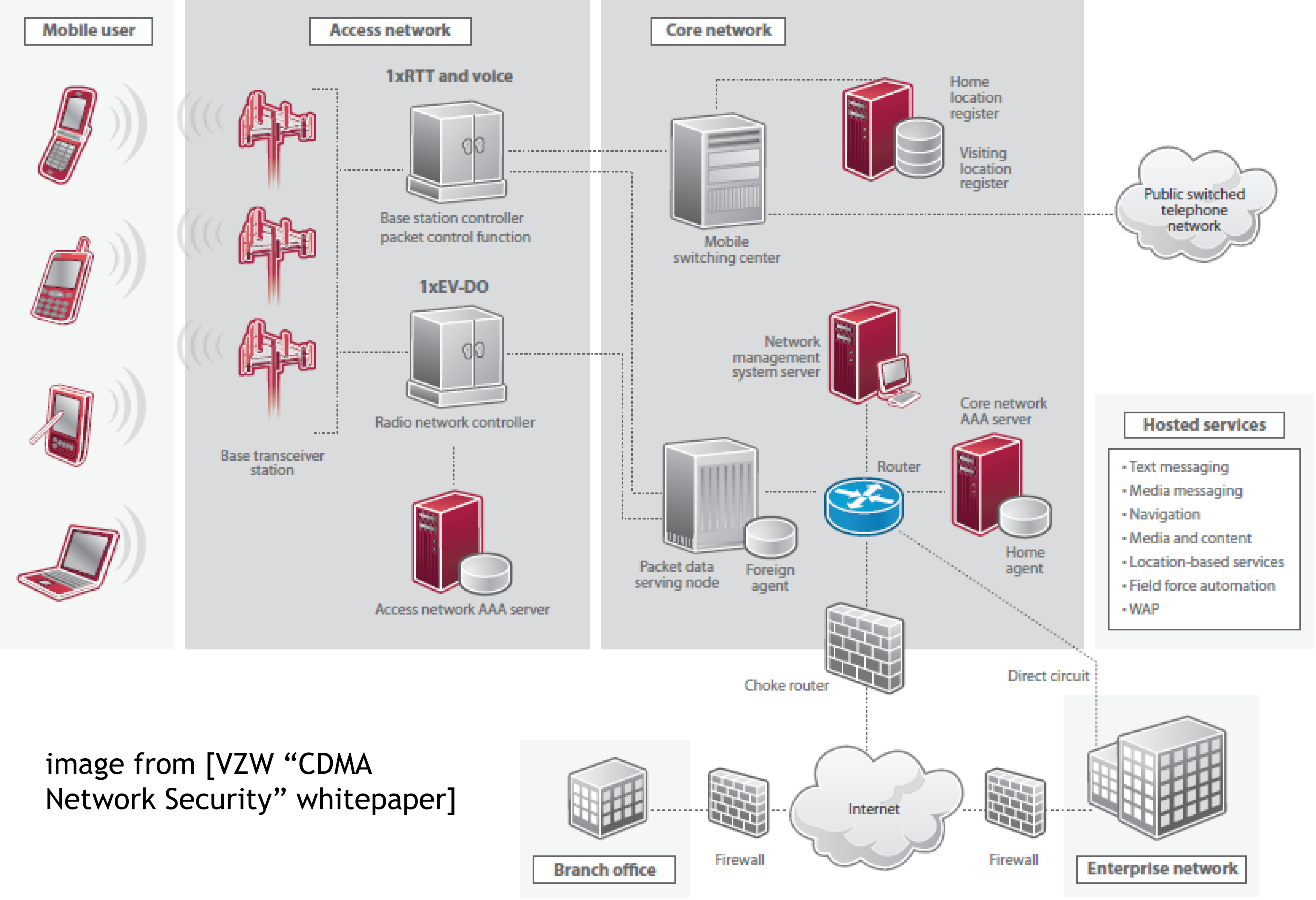
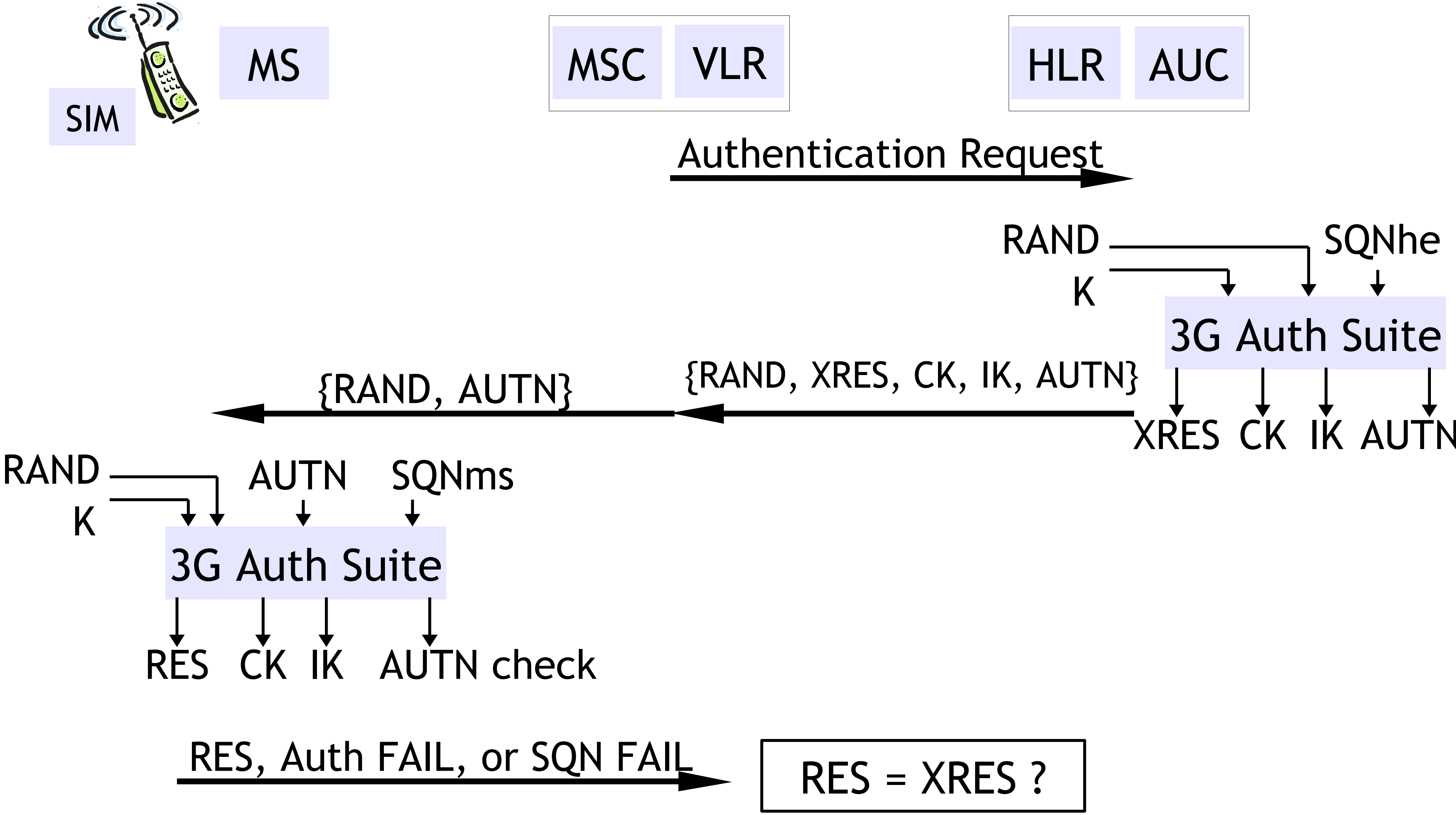


image from [VZW "CDMA Network Security" whitepaper]

Re-Design in 3G

- 3G security model builds on GSM
- Protection against active attacks
  - Integrity mechanisms to protect critical signaling
  - Enhanced (mutual) authentication w/ key freshness
- Enhanced encryption
  - Stronger (public) algorithm, longer keys
  - Encryption deeper into the network
- Core security – signaling protection
- Potential for secure global roaming (3GPP auth)

Authentication & Key Gen.



SIM

MS

MSC VLR

HLR AUC

Authentication Request

RAND

K

SQNhe

3G Auth Suite

XRES CK IK AUTN

{RAND, XRES, CK, IK, AUTN}

{RAND, AUTN}

RAND

K

AUTN

SQNms

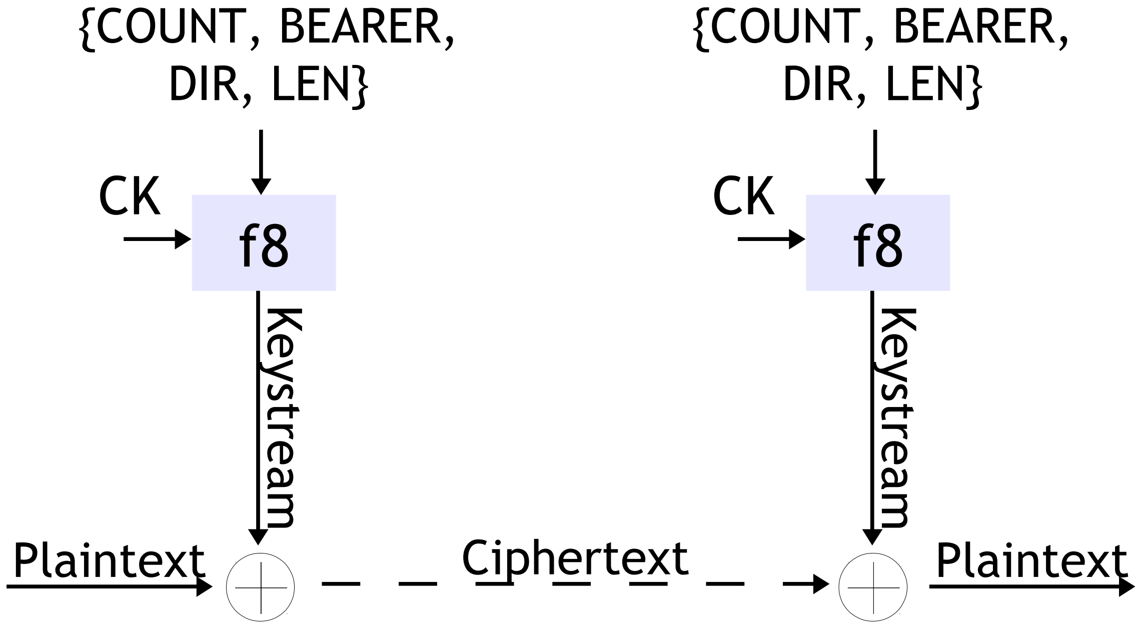
3G Auth Suite

RES CK IK AUTN check

RES, Auth FAIL, or SQN FAIL

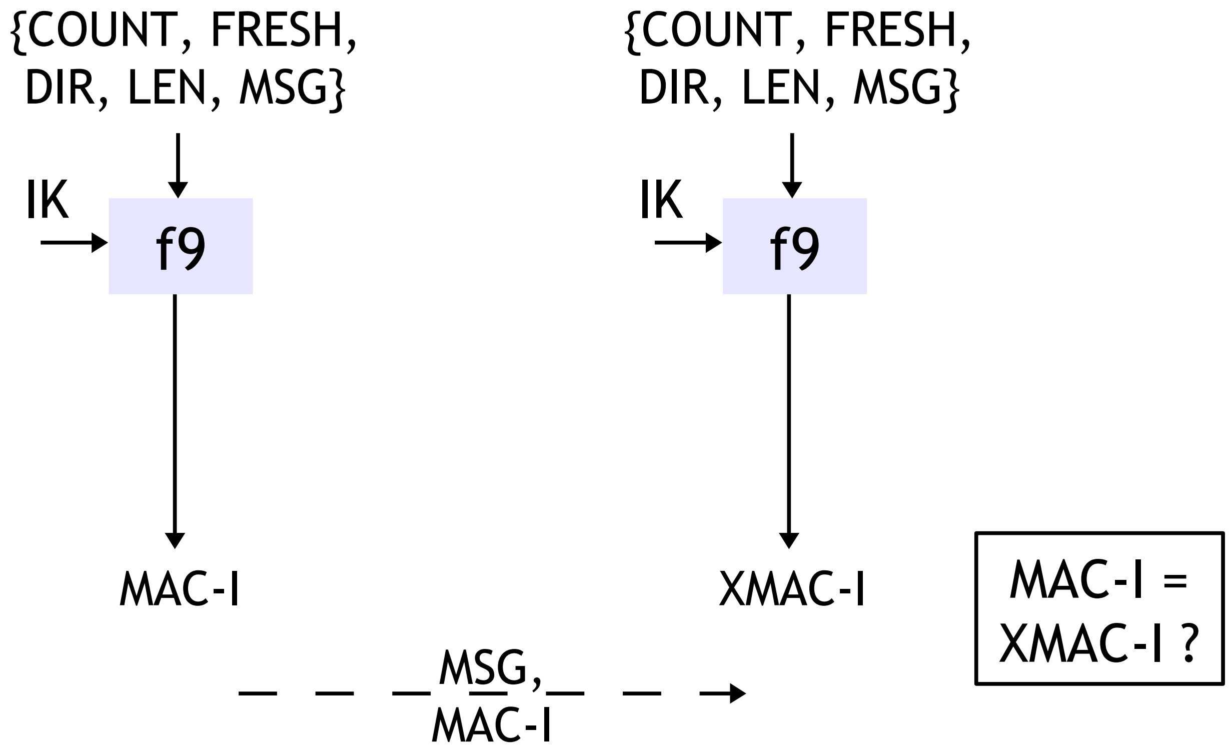
RES = XRES ?

Enhanced Confidentiality



- f8 is one mode of KASUMI, based on MISTY cipher
  - Externally reviewed (positively), published, broken

Enhanced Integrity



- f9 is another mode of KASUMI

Toward 4G

- 4G represents the next generation in cellular communication
  - ITU-R standard: 1Gbps fixed, 100Mbps @ 100kph
  - WiMAX Release 2, LTE-Advanced
    - WiMAX and LTE are not really 4G
    - Verizon, Sprint, AT&T use LTE; T-Mobile, AT&T use HSPA+
    - Most provide ~20Mbps fixed
- "4G is a combination of marketing speak and future tech" [Warren, Mashable 02/2011]
  - Current "4G" systems are actually 3.75G or 3.9G, but they'll be upgraded to real 4G in the future

4G Security Issues

- All-IP network → all IP-based threats apply
- Verification of users
- Heterogeneous network access
  - User-preferred connection methods
  - Multiple available connections:
    - Attacker has more opportunity for exploit/attack
    - Device is exposed to attacks on each connection
      - Exploits based on driver code, comm protocols, transport / signaling, file-sharing, update, etc.
  - Complex management systems are required
- ?

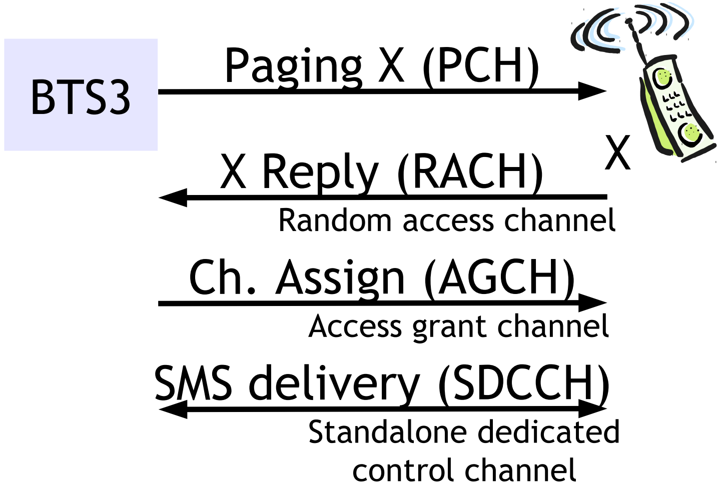
Some other attacks on mobile networks

SMS Flooding

- Flooding a user with SMS messages:
  1. Buffer (@ MS or SMSC) overflow
     - With enough flooding, SMSC will drop valid messages
     - Some devices auto-delete previously read messages when they run out of storage
  2. Valid messages are delayed beyond useful lifetime
     - Ex: meeting reminders are useless after the meeting
  3. Valid messages are buried in the SMS flood

- Also a battery-depletion attack...

SMS Flooding → Voice DoS



BTS3

Paging X (PCH)

X

X Reply (RACH)

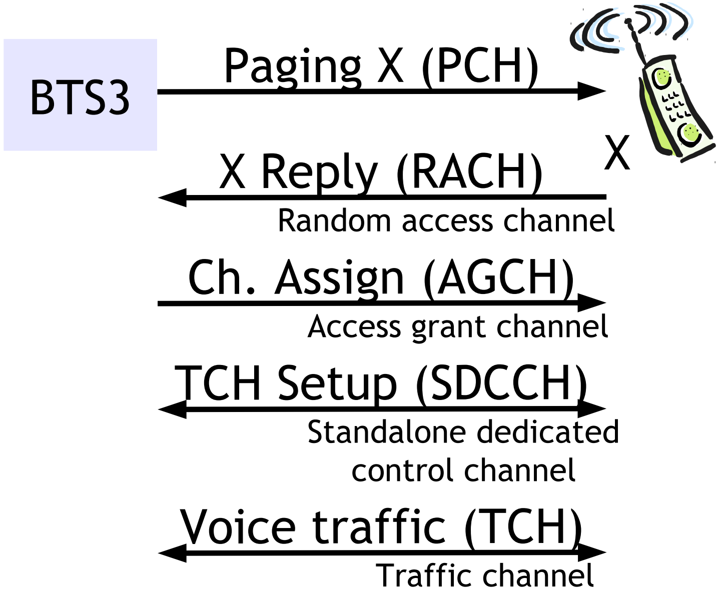
Random access channel

Ch. Assign (AGCH)

Access grant channel

SMS delivery (SDCCH)

Standalone dedicated control channel



BTS3

Paging X (PCH)

X

X Reply (RACH)

Random access channel

Ch. Assign (AGCH)

Access grant channel

TCH Setup (SDCCH)

Standalone dedicated control channel

Voice traffic (TCH)

Traffic channel

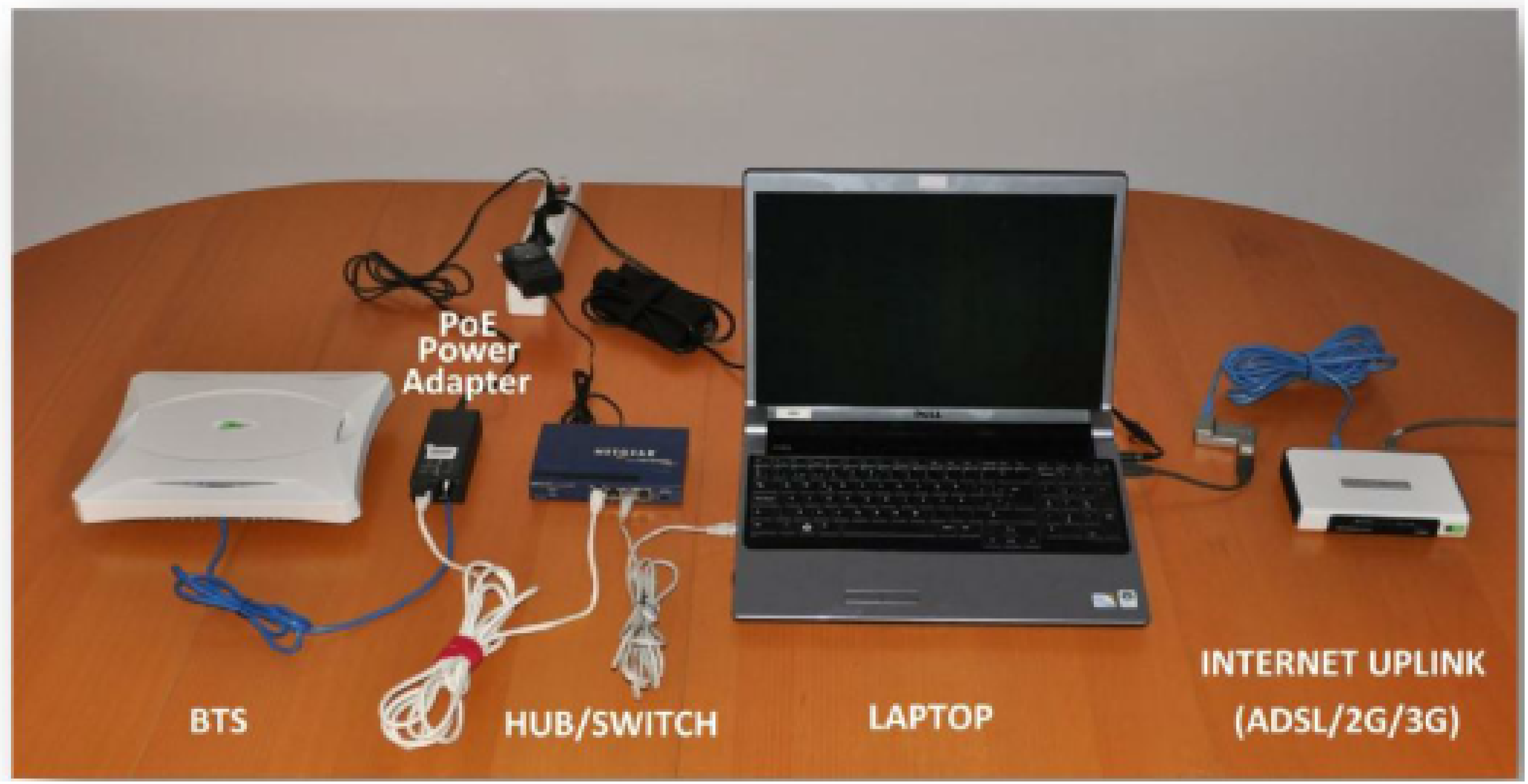
- Voice & SMS Resources
  - TCH is not used for SMS
  - Both SMS and voice init. use RACH, AGCH, and SDCCH

SMS flooding also works as DoS against voice calls!

Rogue BTS

- An adversary can deploy a rogue BTS that attempts to spoof the service provided by a valid BTS, attracting users for various reasons
- Possible to launch a MitM attack on 2G/3G mobile connections
- Applies to GPRS, EDGE, UMTS, and HSPA capable devices
- Cheap

Setting up a Rogue BTS

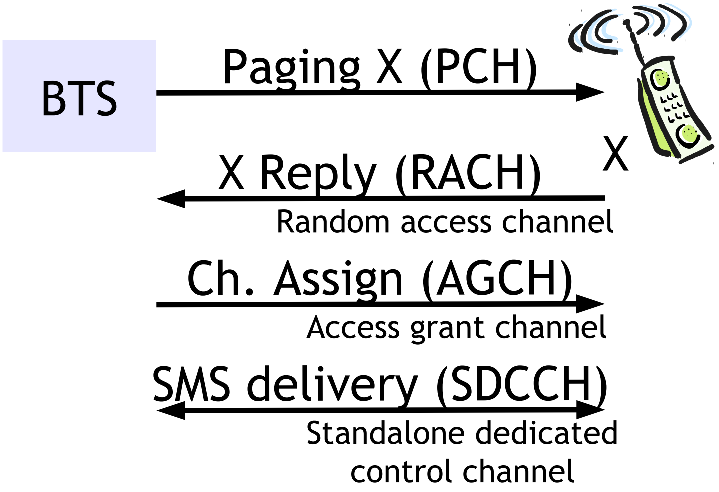


[Perez & Pico, BlackHat 2011]

But, what's coming next is going to get a lot more interesting

Spectrum Management

- Most current mobile networks use multiple dedicated channels for voice, data, text, etc.



BTS

Paging X (PCH)

X

X Reply (RACH)

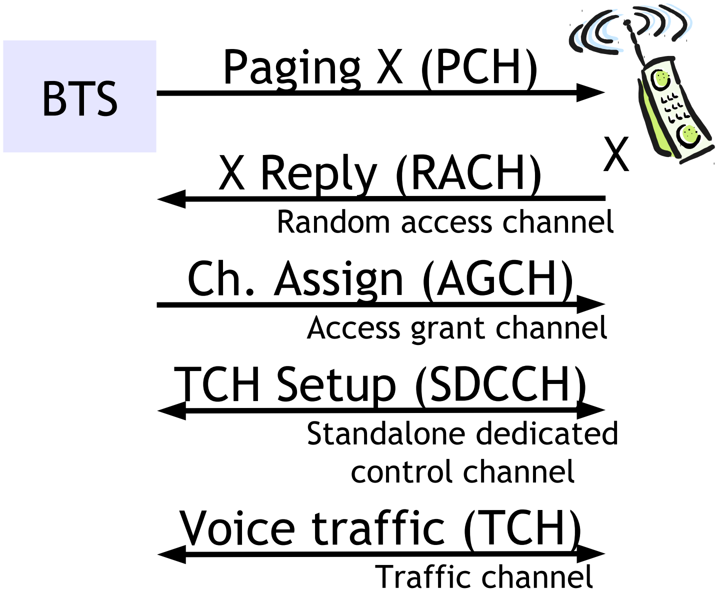
Random access channel

Ch. Assign (AGCH)

Access grant channel

SMS delivery (SDCCH)

Standalone dedicated control channel



BTS

Paging X (PCH)

X

X Reply (RACH)

Random access channel

Ch. Assign (AGCH)

Access grant channel

TCH Setup (SDCCH)

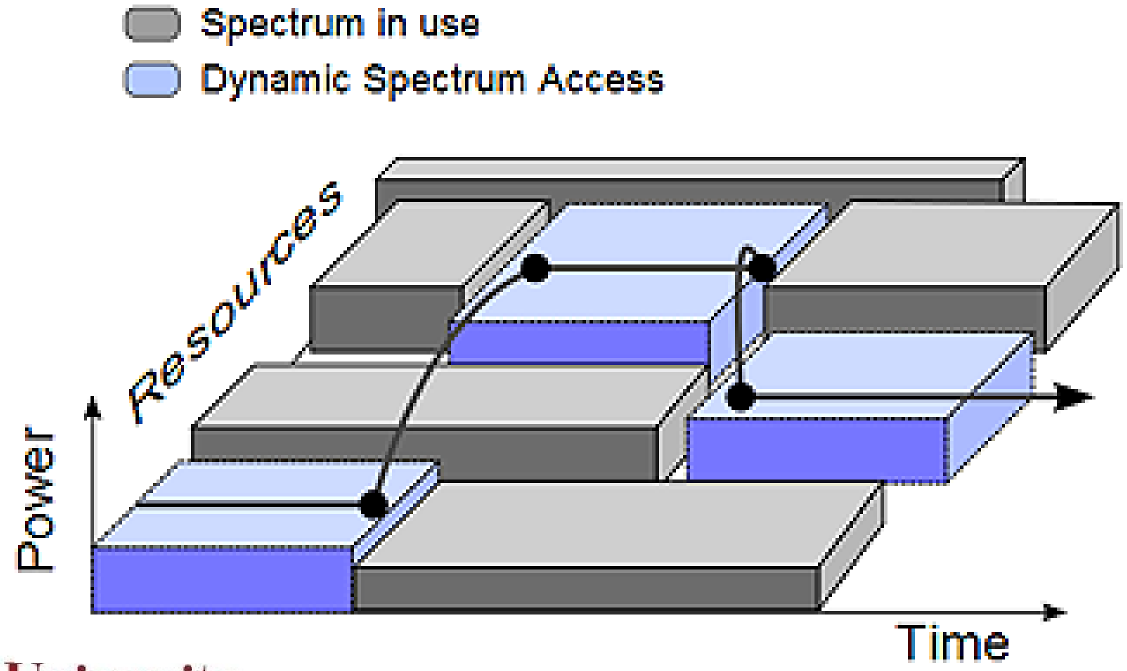
Standalone dedicated control channel

Voice traffic (TCH)

Traffic channel

Spectrum Agility

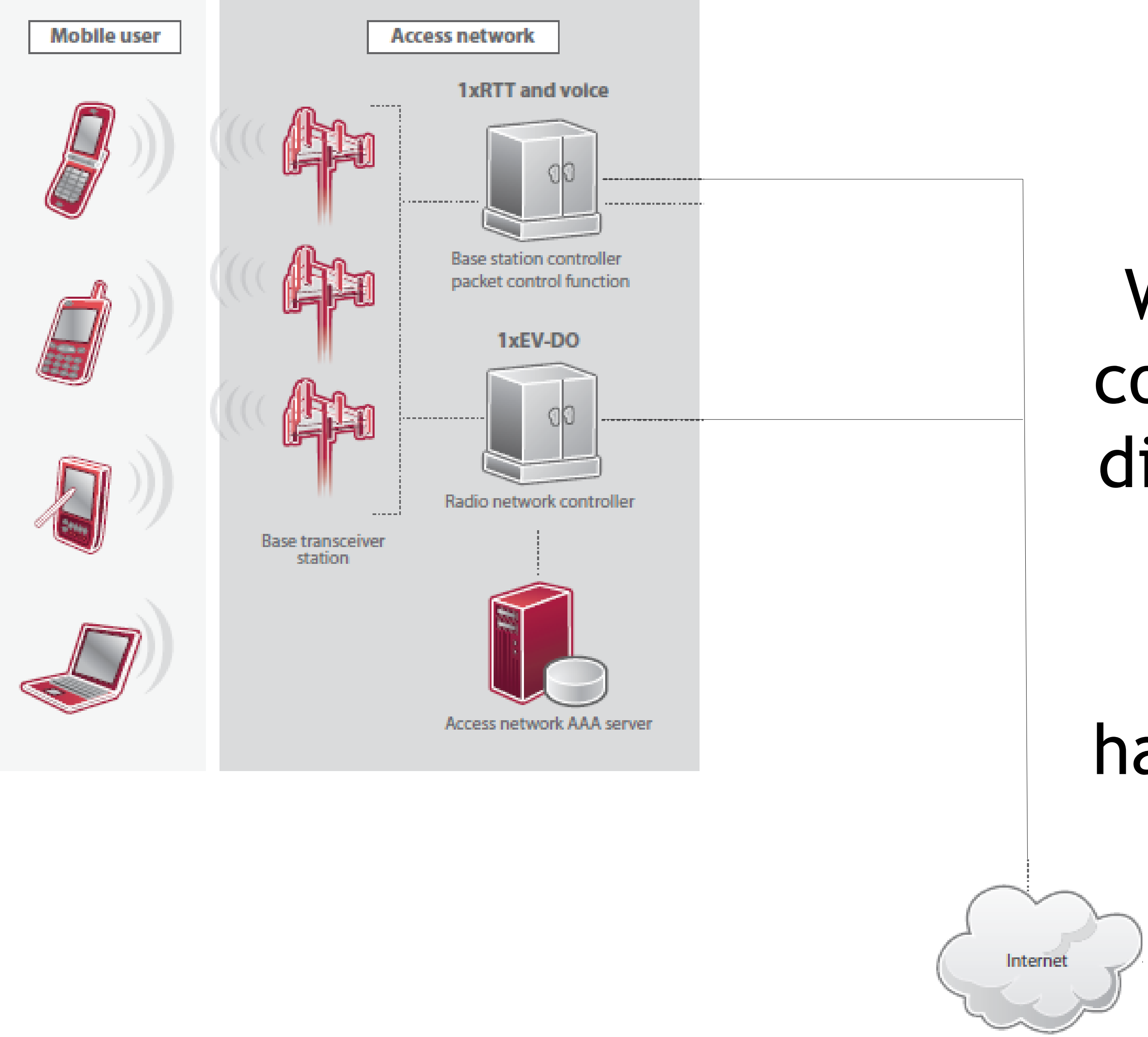
- Base stations and handsets can learn how spectrum is being used, so they can find gaps that are available between used “channels”
  - This is the basic idea of “cognitive radio” and “whitespace radio”



How can radios coordinate to find available spectrum resources?

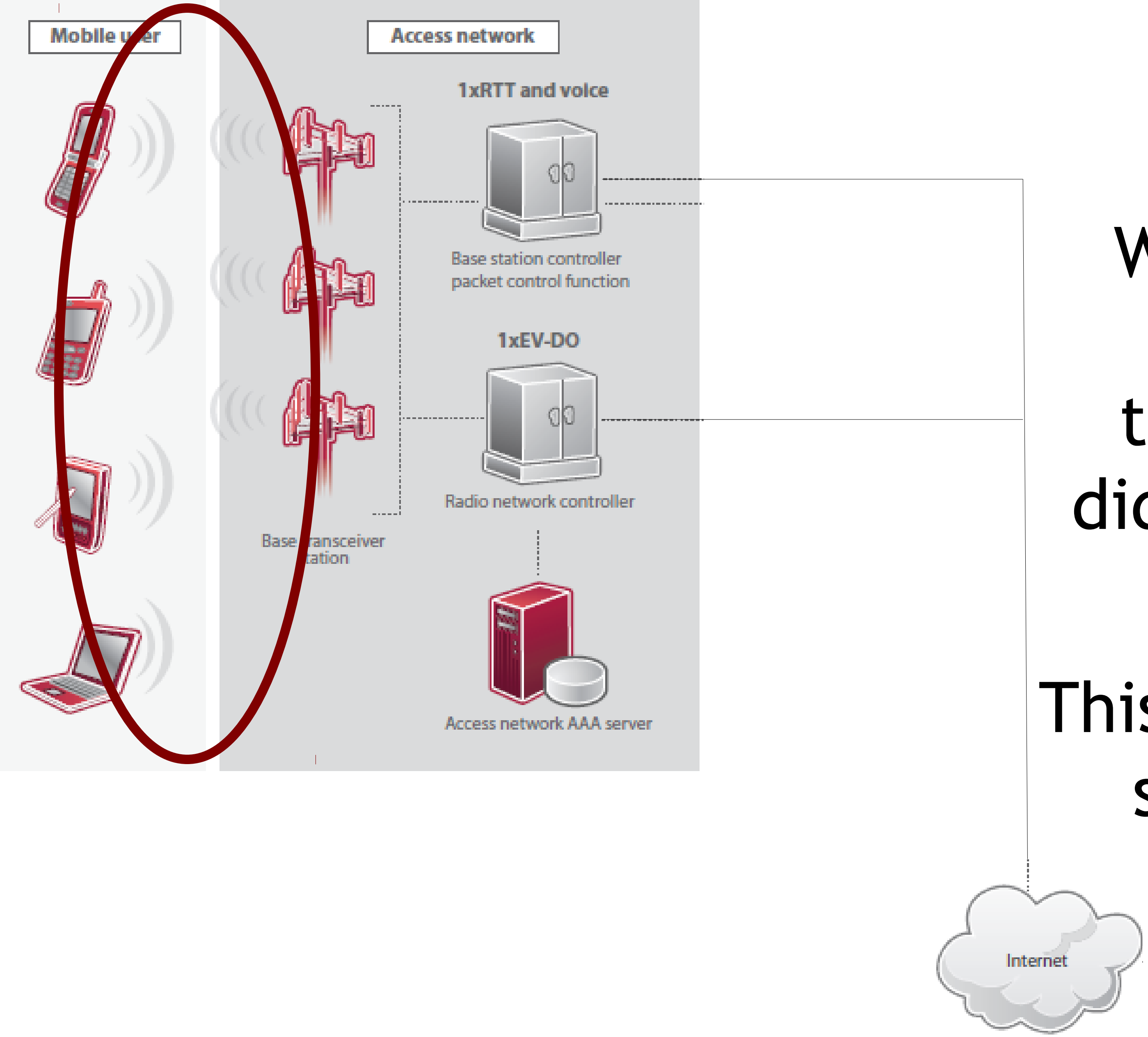
Opportunities for misbehavior? Cheating?

Risks of flexibility?



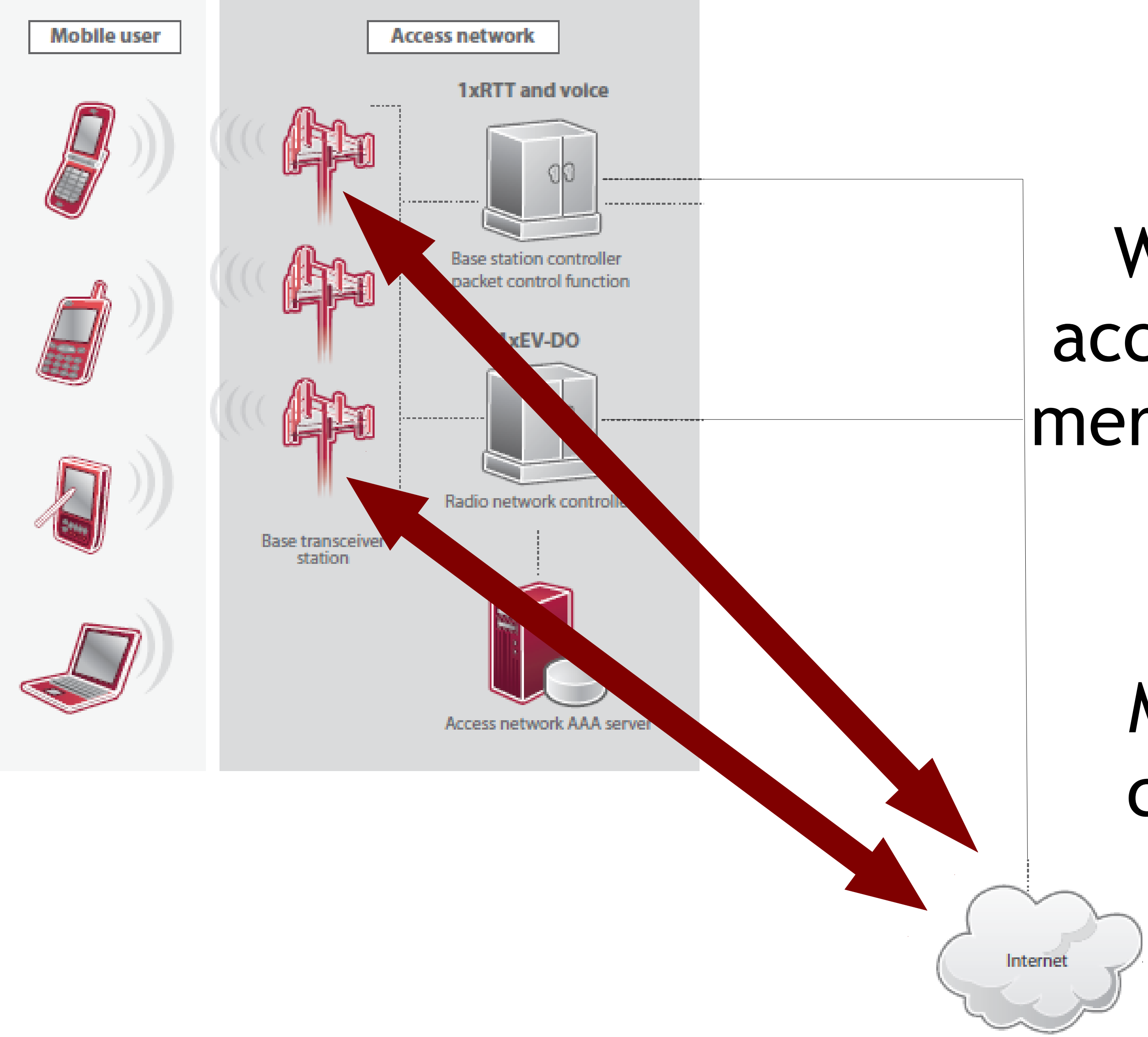
What if the core network disappeared?

This will happen soon.



What if the access technology didn't matter?

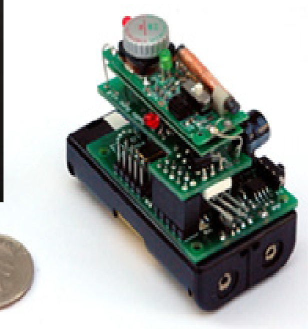
This will change soon, too.

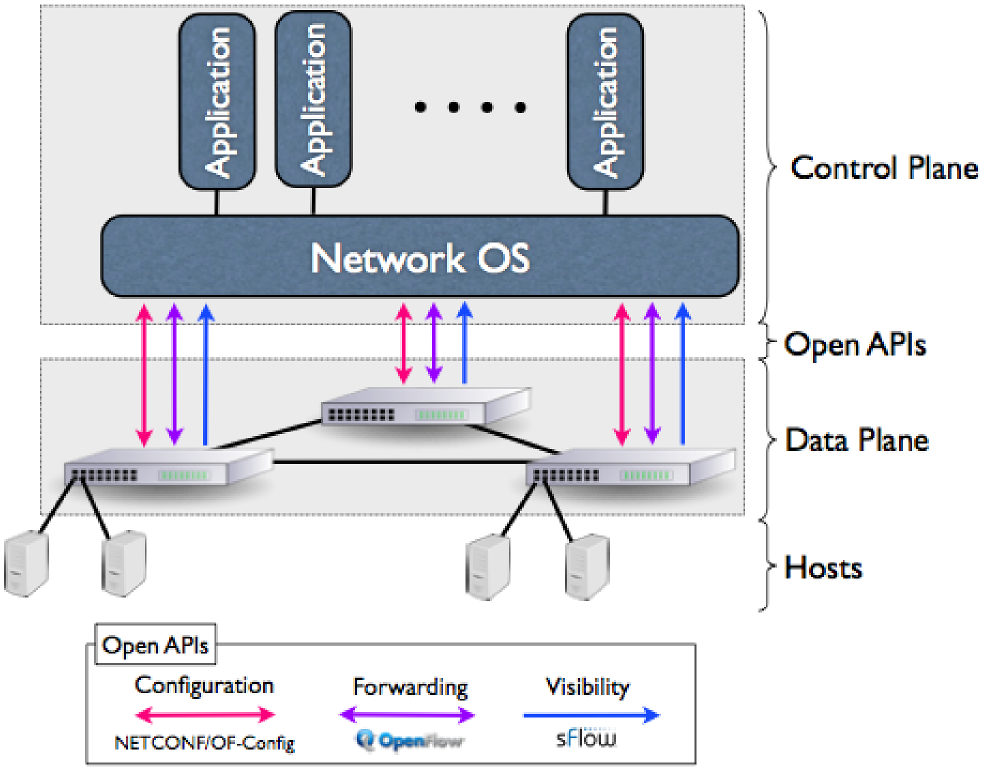


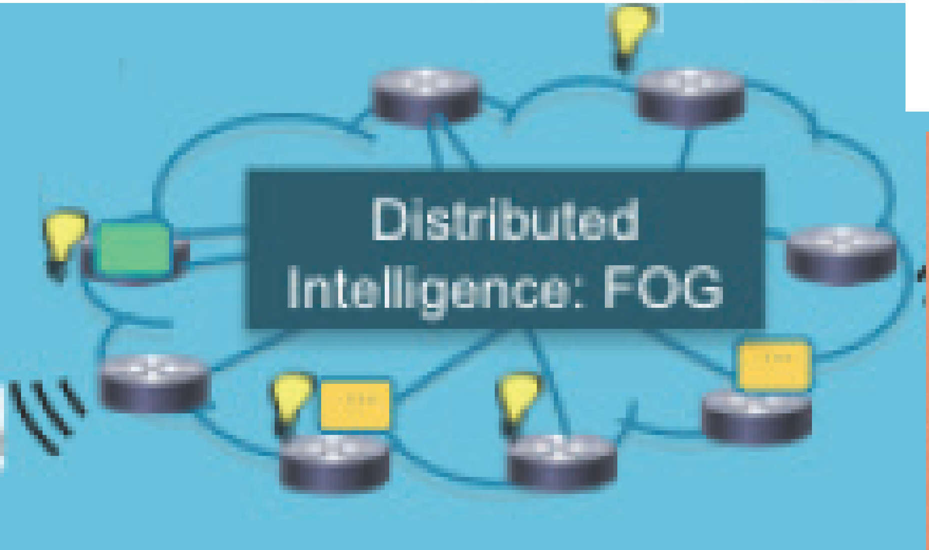
What if the access network merged with the cloud?

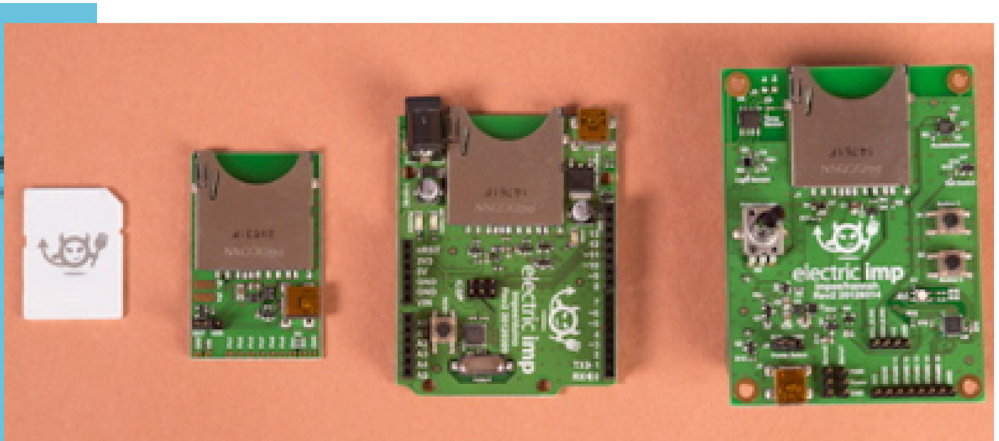
Mobile fog computing

Modern Computing





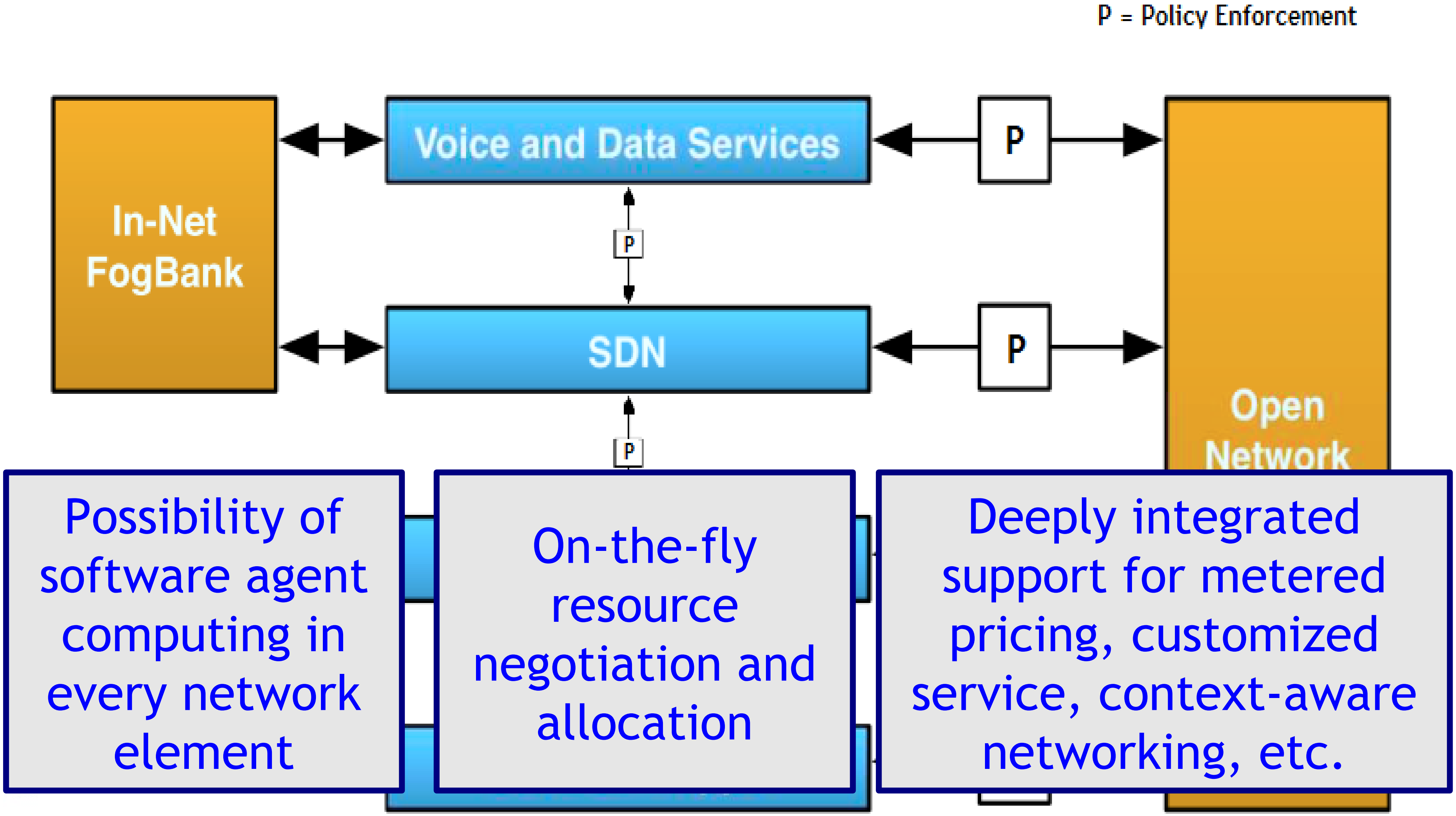

Distributed Intelligence: FOG



What if we incorporate computation into every element of the mobile network?

What if we allow network elements to collaborate and share info?

CROSSMobile: a radical agent-based approach to mobile networking that deeply integrates computing capabilities and proactive resource provisioning

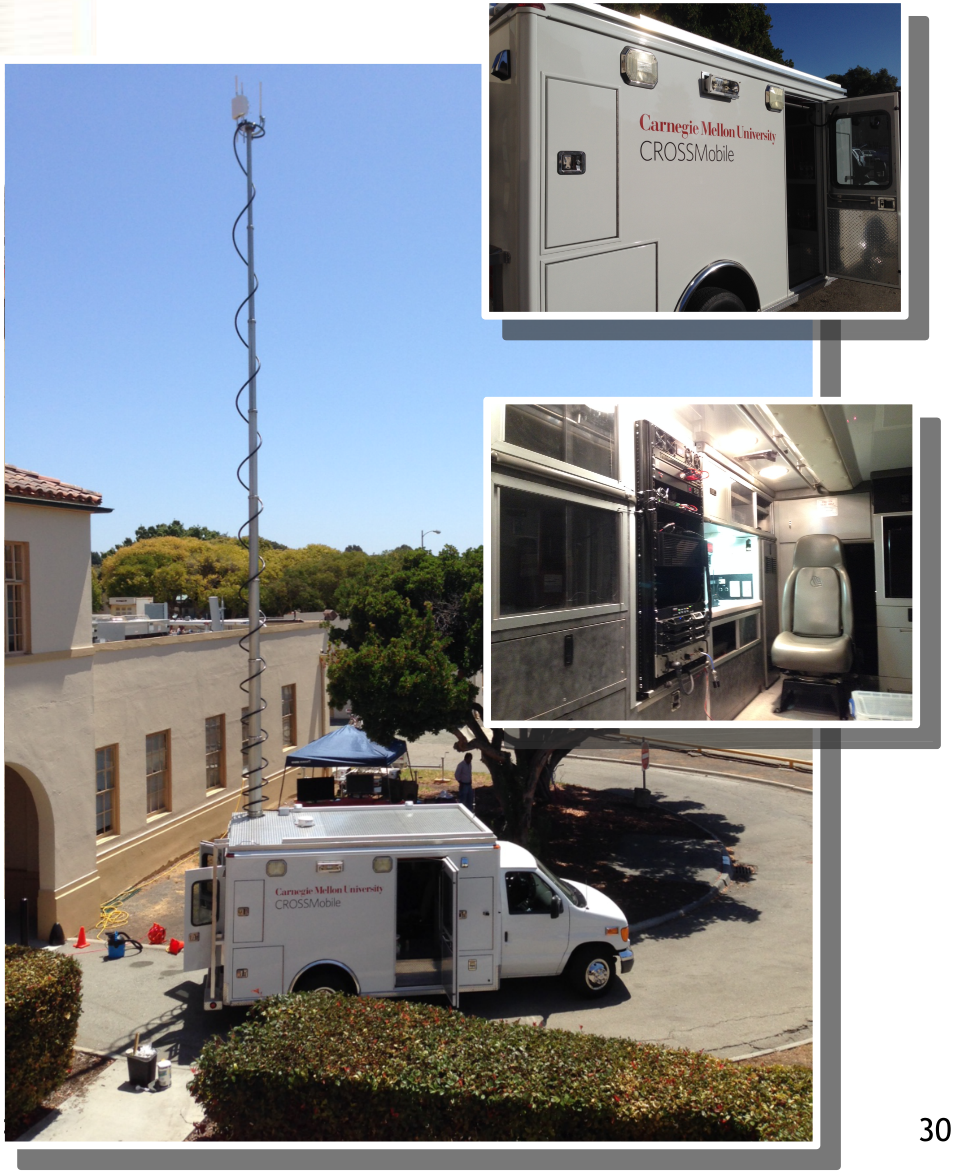


Possibility of software agent computing in every network element

On-the-fly resource negotiation and allocation

Deeply integrated support for metered pricing, customized service, context-aware networking, etc.

CROSSMobile Network



CROSSMobile Network

Fully operational (FCC-licensed) mobile network based on open-source tools

What are the risks of broad (though controlled) information sharing across devices, domains, layers, etc.?

Additional risk of software-defined everything?

Apr 14 & 16:

No class – work on projects

Apr 21 & 23:

Discussion of projects

Apr 28 & 30:

Final presentations