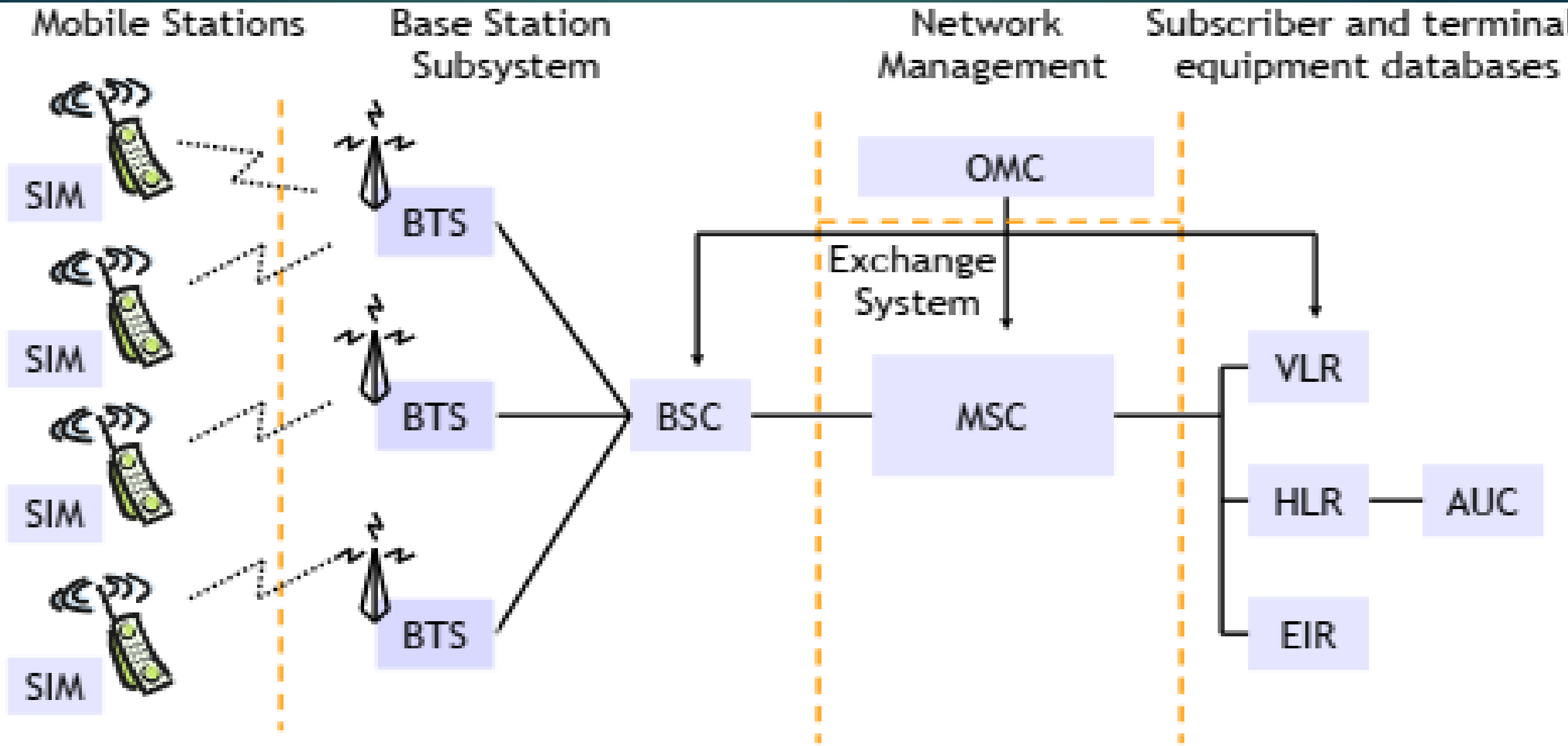
BÀI #21 - BẢO MẬT & QUYỀN RIÊNG TƯ TRONG MẠNG VIỄN THÔNG

- MỐI QUAN TÂM VỀ S&P TRONG QUÁ KHỨ VÀ HIỆN TẠI ĐỐI VỚI MẠNG DI ĐỘNG
- CÁC SỰ CỐ S&P CÓ THỂ XẢY RA TRONG TƯƠNG LAI TRONG MẠNG DI ĐỘNG
- MỘT SỐ LĨNH VỰC NGHIÊN CỨU MỞ

TS. HOÀNG SỸ TƯƠNG

Let's talk about mobile networks

KIẾN TRÚC 2G GSM/CDMA



BẢO MẬT 2G GSM

- Truy cập an toàn

  Xác thực người dùng để thanh toán và phòng chống gian lận

  Sử dụng giao thức thách thức/phản hồi dựa trên khóa xác thực dành riêng cho thuê bao (tại HLR)

- Kiểm soát và bảo mật tín hiệu dữ liệu

  Bảo vệ giọng nói, dữ liệu và điều khiển (ví dụ: số điện thoại đã gọi) khỏi bị nghe lén thông qua mã hóa liên kết vô tuyến (thiết lập khóa là một phần của xác thực)

- Ẩn danh

  Sử dụng số nhận dạng tạm thời thay vì ID thuê bao (IMSI) để ngăn người dùng theo dõi hoặc xác định cuộc gọi

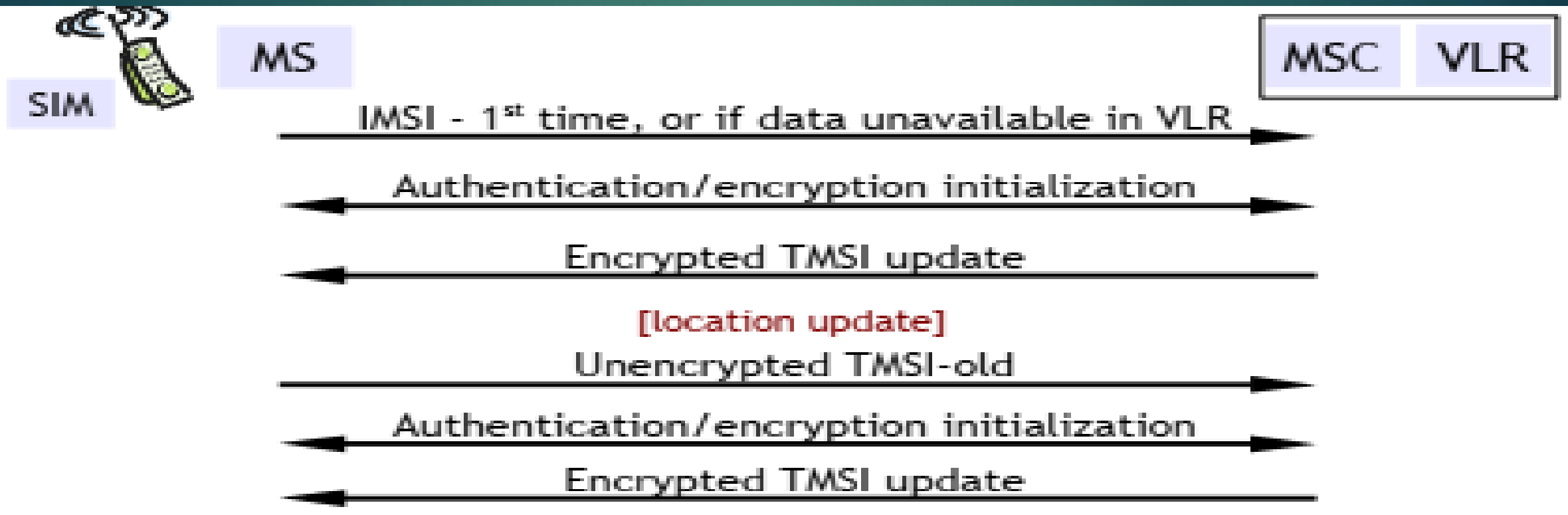
QUẢN LÝ ID TẠM THỜI

- Nhận dạng người dùng và thiết bị:

IMEI: ID thiết bị di động quốc tế - thiết bị

-IMSI: ID thuê bao di động quốc tế - người dùng

TMSI: ID thuê bao di động tạm thời - bút danh



TIẾN HÓA CỦA MẠNG 3G

- Việc chuyển từ 2G sang 3G chủ yếu bao gồm:
  - Hỗ trợ dữ liệu di động ở (gần) tốc độ băng thông rộng

    UMTS, TD-CDMA, WCDMA, CDMA-3xRTT, TD-SCDMA, HSDPA, HSUPA, HSPA, HSPA+
  - Cải thiện các giao thức bảo mật
    - Bởi vì mọi thứ trong 2G đã bị phá vỡ theo nhiều cách

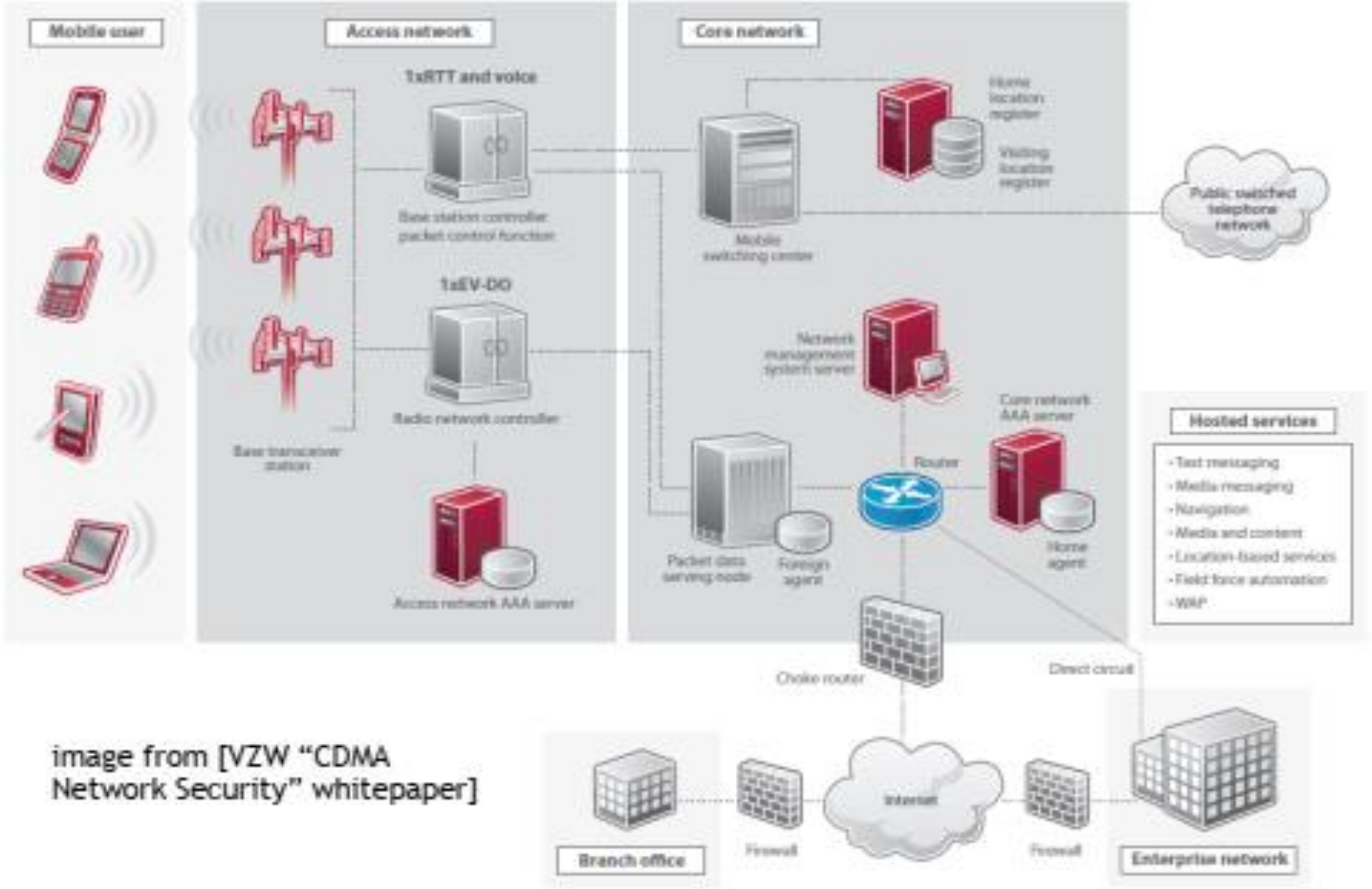


image from [VZW "CDMA Network Security" whitepaper]

THIẾT KẾ LẠI TRONG MẠNG 3G

- Mô hình bảo mật 3G xây dựng trên GSM
- Bảo vệ chống lại các cuộc tấn công chủ động

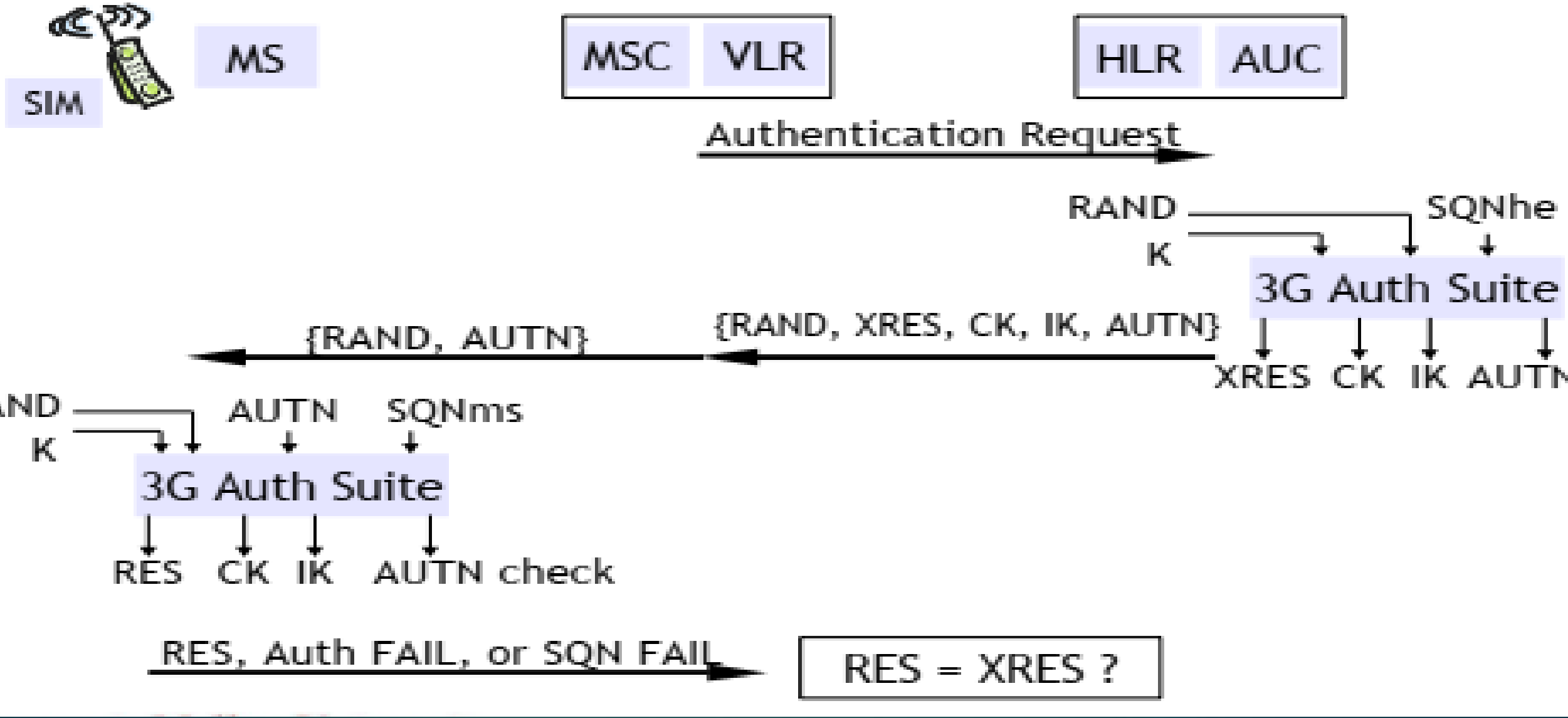
  Cơ chế toàn vẹn để bảo vệ tín hiệu quan trọng

  Xác thực nâng cao (tương hỗ) với độ mới của khóa
- Mã hóa nâng cao

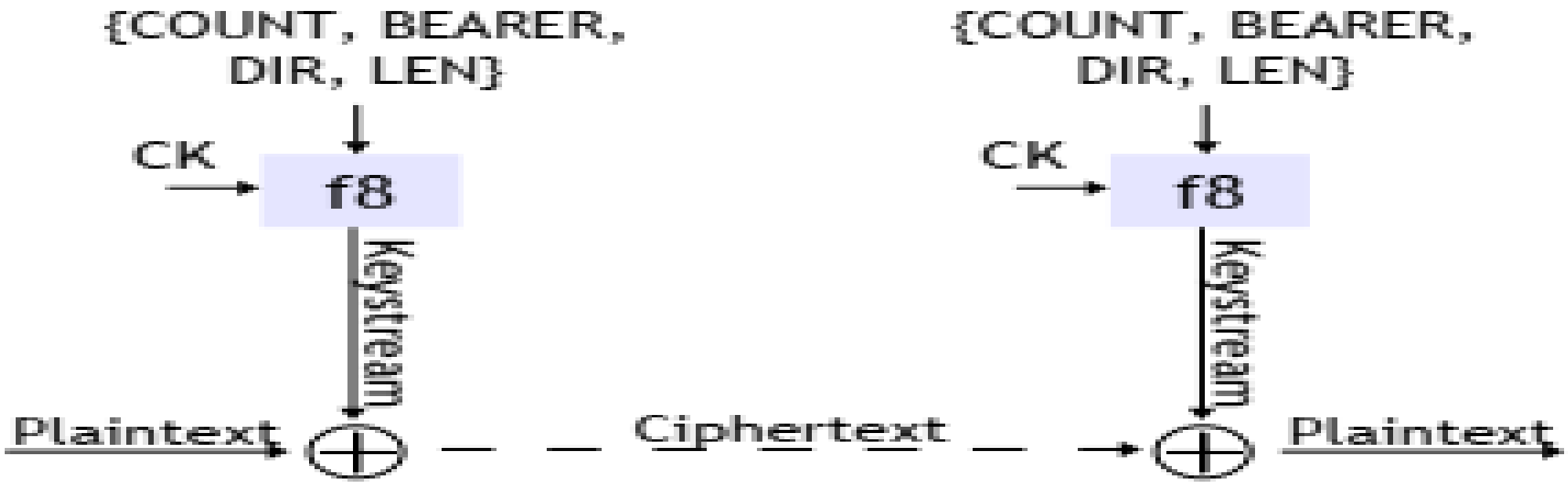
  Thuật toán (công khai) mạnh hơn, khóa dài hơn

  Mã hóa sâu hơn vào mạng
- Bảo mật cốt lõi - bảo vệ báo hiệu
- Khả năng chuyển vùng toàn cầu an toàn (3GPP auth)

XÁC THỰC & SINH KHÓA



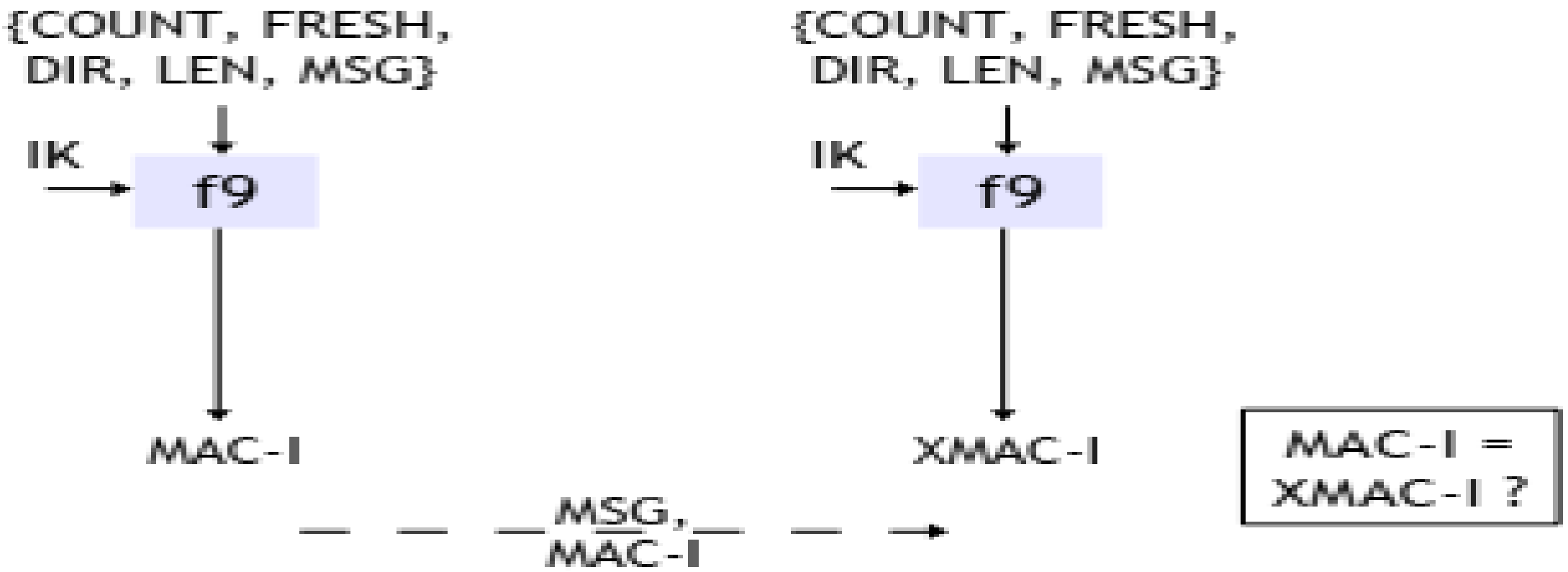
TĂNG CƯỜNG TÍNH BÍ MẬT



- f8 là một chế độ của KASUMI, dựa trên mã MISTY

Đánh giá bên ngoài (tích cực), xuất bản, bị phá vỡ

TĂNG CƯỜNG TÍNH TOÀN VẸN



f9 là một chế độ khác của KASUMI

HƯỚNG TỚI MẠNG 4G

- 4G đại diện cho thế hệ tiếp theo trong truyền thông di động
  - Chuẩn ITU-R: IGbps cố định, 100Mbps @ 100kph
  - Phiên bản WiMAX 2, LTE-Nâng cao

    WiMAX và LTE không thực sự là 4G

    Verizon, Sprint, AT&T sử dụng LTE; T-Mobile, AT&T sử dụng HSPA+

    Hầu hết cung cấp ~20Mbps cố định
- "4G là sự kết hợp giữa ngôn ngữ tiếp thị và công nghệ tương lai" [Warren, Mashable 02/2011]

  Các hệ thống "4G" hiện tại thực sự là 3,75G hoặc 3,9G, nhưng chúng sẽ được nâng cấp lên 4G thực trong tương lai

VẤN ĐỀ BẢO MẬT 4G

- Mạng All-IP áp dụng tất cả các mối đe dọa dựa trên IP
- Xác minh người dùng
- Truy cập mạng không đồng nhất
  - Phương pháp kết nối ưa thích của người dùng
  - Nhiều kết nối có sẵn:

    Kẻ tấn công có nhiều cơ hội khai thác/tấn công hơn

    Thiết bị dễ bị tấn công trên mỗi kết nối

    Khai thác dựa trên mã trình điều khiển, giao thức comm, vận chuyển/tín hiệu, chia sẻ tệp, cập nhật, v.v.
  - Cần có hệ thống quản lý phức tạp

MỘT SỐ TẤN CÔNG KHÁC TRÊN MẠNG DI ĐỘNG

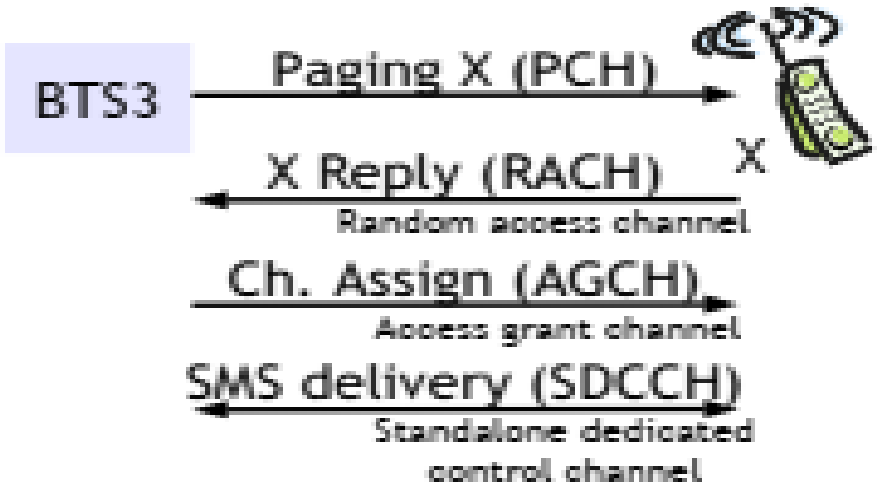
SMS FLOODING

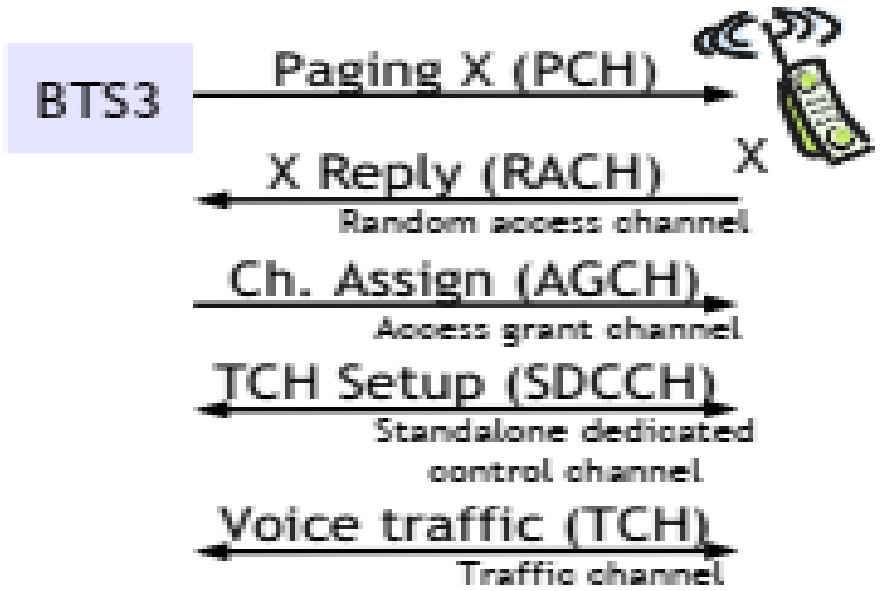
- Làm ngập người dùng bằng tin nhắn SMS:

1. Tràn bộ đệm (@ MS hoặc SMSC)
    - Khi đủ ngập, SMSC sẽ loại bỏ các tin nhắn hợp lệ
    - Một số thiết bị tự động xóa tin nhắn đã đọc trước đó khi hết bộ nhớ
2. Tin nhắn hợp lệ bị trì hoãn ngoài thời gian hữu ích
    - Ví dụ: lời nhắc cuộc họp là vô ích sau cuộc họp
3. Tin nhắn hợp lệ bị chôn vùi trong cơn lũ SMS

- Cũng là một cuộc tấn công cạn kiệt pin...

SMS Flooding → Voice DoS





- Tài nguyên thoại & SMS
  - TCH không dùng cho tin nhắn SMS
  - Cả SMS và giọng nói init. Sử dụng RACH, AGCH và SDCCH

Tràn ngập tin nhắn SMS cũng hoạt động như DoS đối với các cuộc gọi thoại!

GIẢ MẠO TRẠM BTS

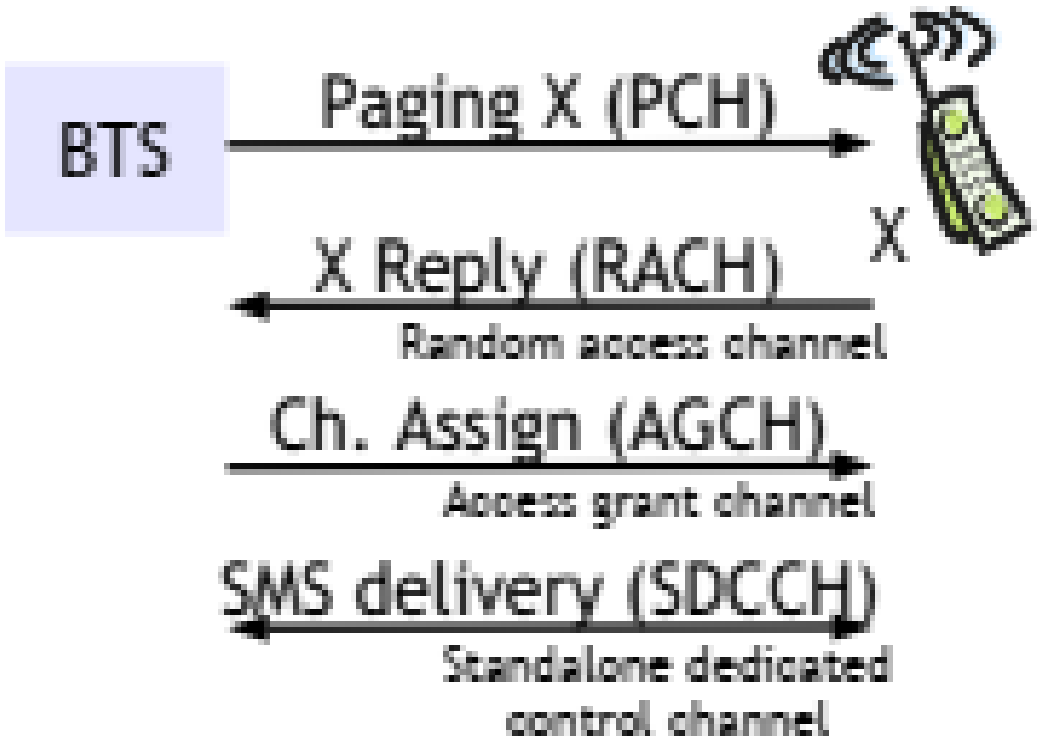
- Đối thủ có thể triển khai một BTS lừa đảo cố gắng giả mạo dịch vụ do một BTS hợp lệ cung cấp, thu hút người dùng vì nhiều lý do
- Có thể khởi động một cuộc tấn công MitM trên các kết nối di động 2G/3G
- Áp dụng cho các thiết bị hỗ trợ GPRS, EDGE, UMTS và HSPA
- Rẻ

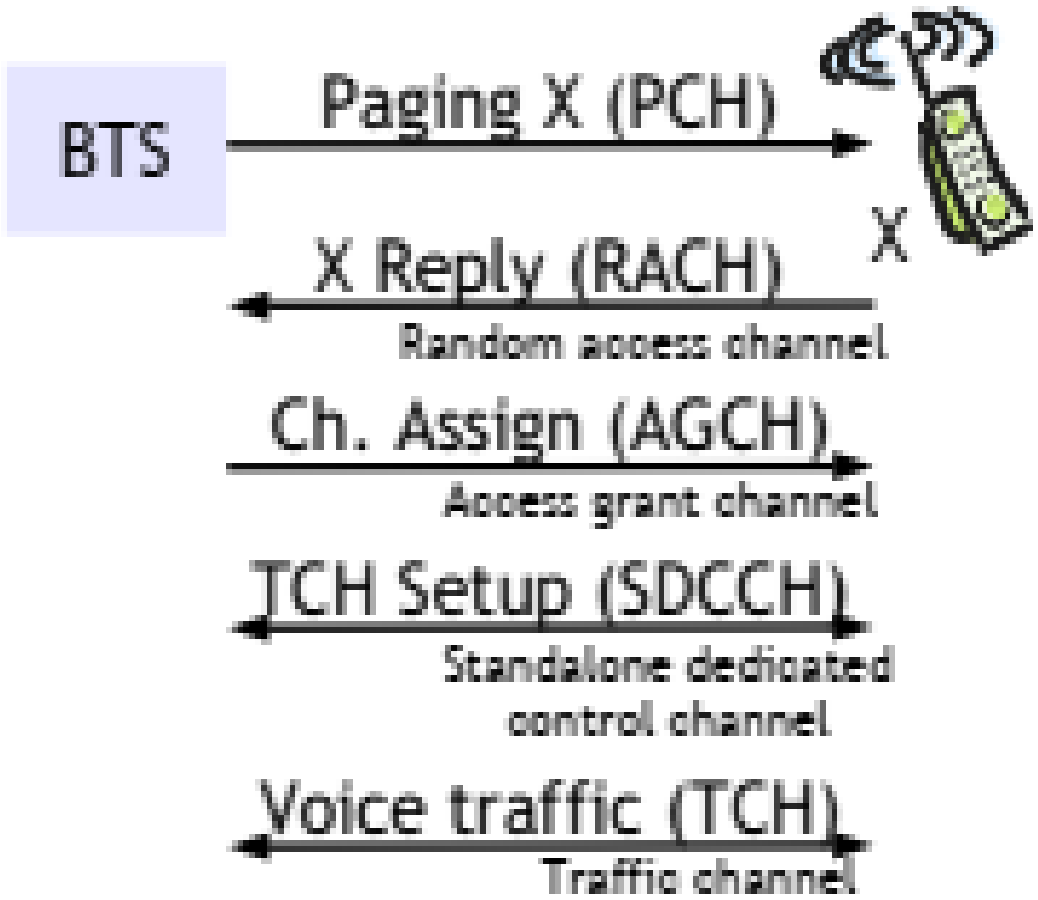
THIẾT LẬP BTS ROGUE

NHƯNG, NHỮNG GÌ SẮP TỚI SẼ THÚ VỊ HƠN RẤT NHIỀU

QUẢN LÝ PHỔ

Hầu hết các mạng di động hiện nay đều sử dụng nhiều kênh dành riêng cho thoại, dữ liệu, văn bản, v.v.

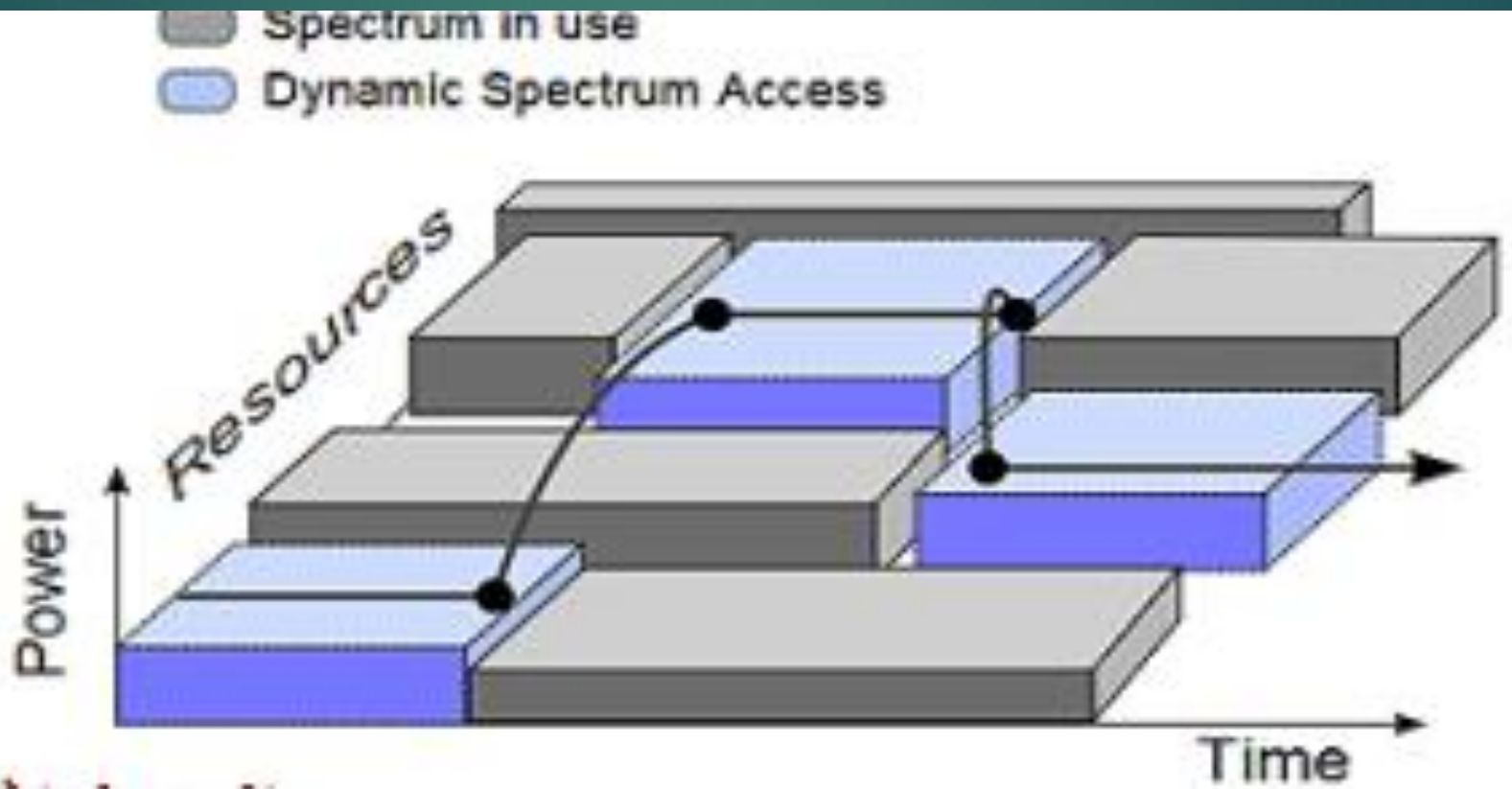




QUANG PHỔ NHANH

- Các trạm cơ sở và thiết bị cầm tay có thể tìm hiểu cách sử dụng phổ tần, vì vậy chúng có thể tìm thấy các khoảng trống có sẵn giữa các "kênh" đã sử dụng

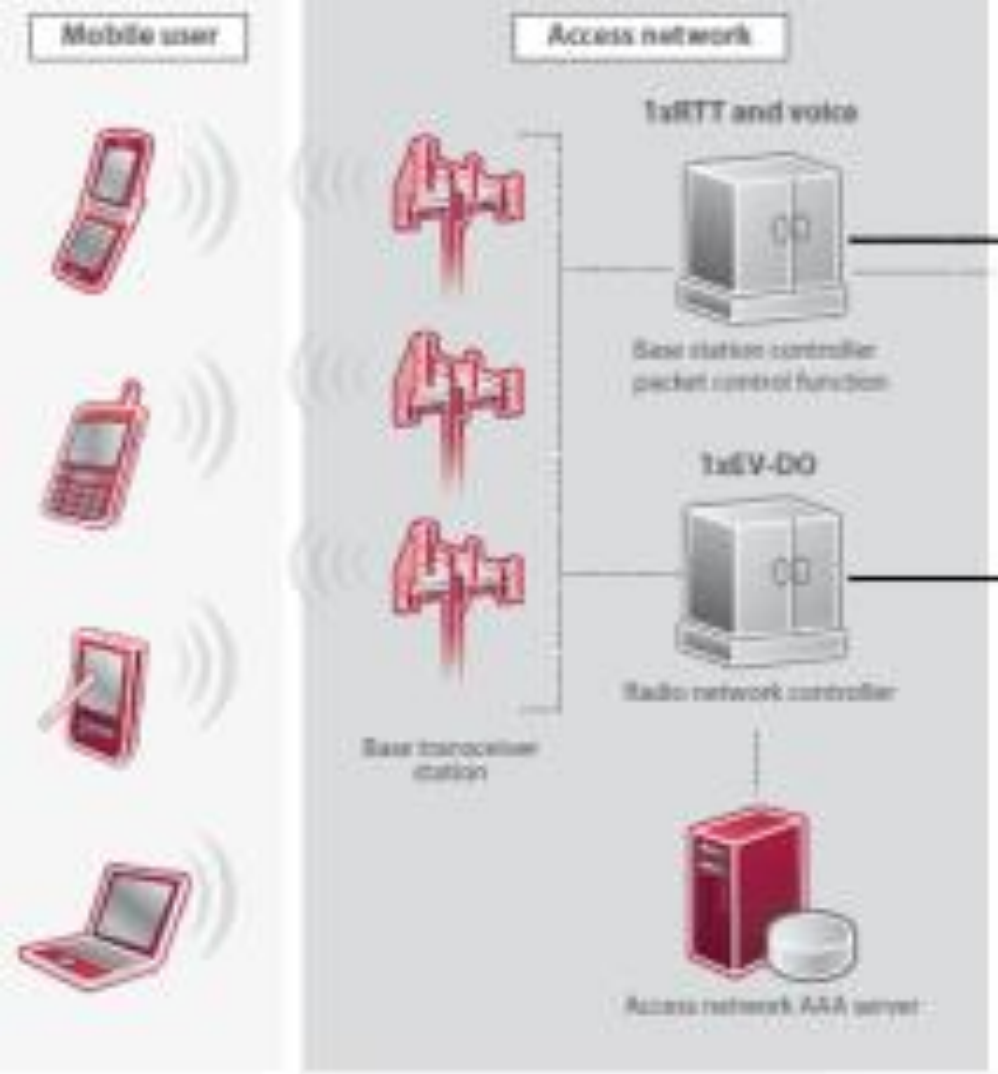
Đây là ý tưởng cơ bản của "radio nhận thức" và "radio khoảng trắng"



LÀM THẾ NÀO CÁC ĐÀI CÓ THỂ PHỐI HỢP ĐỂ TÌM TÀI NGUYÊN PHỔ CÓ SẴN?

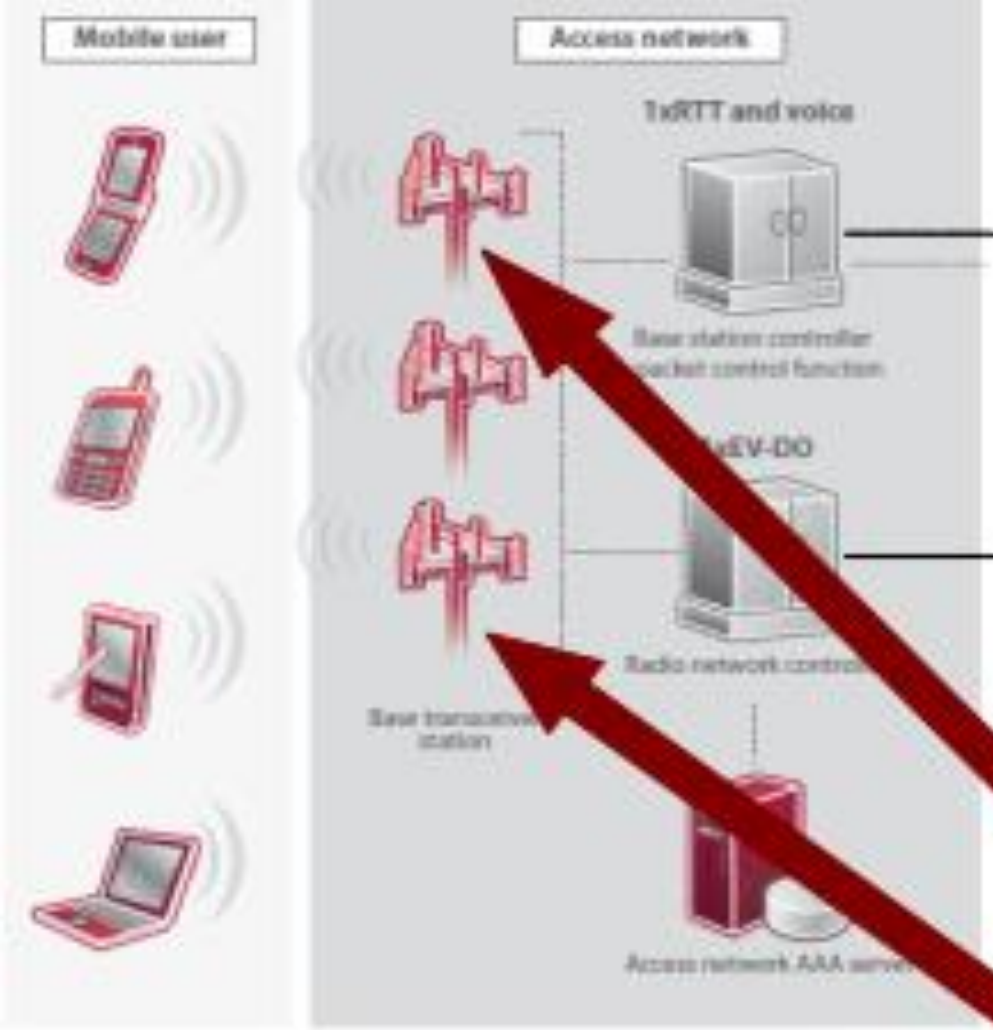
CƠ HỘI CHO HÀNH VI SAI TRÁI? GIAN LẬN?

RỦI RO VỀ TÍNH LINH HOẠT?



What if the core network disappeared?

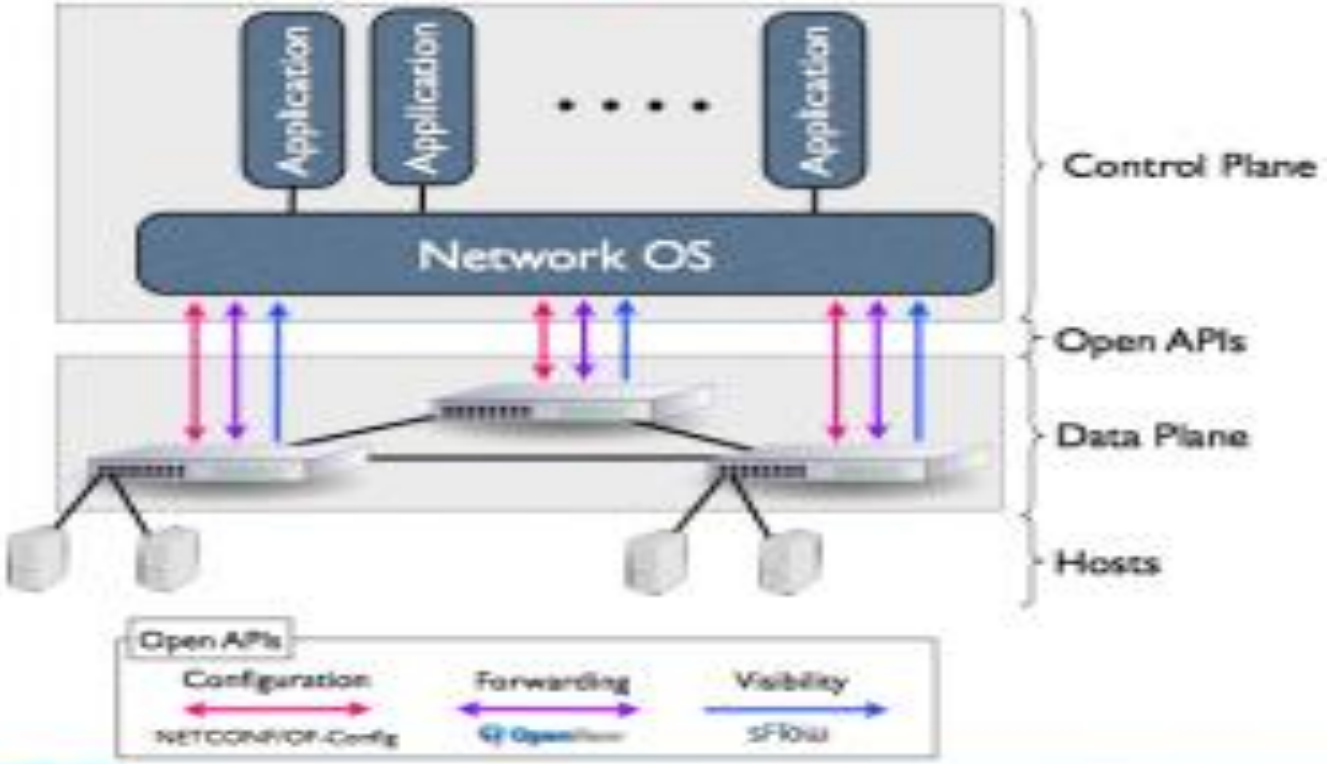
This will happen soon.

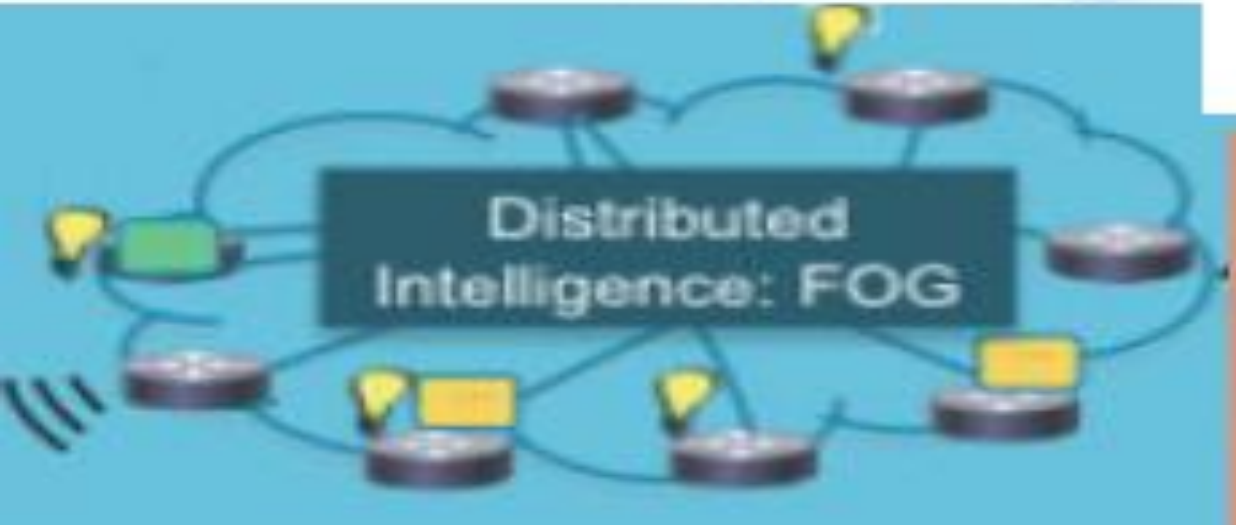


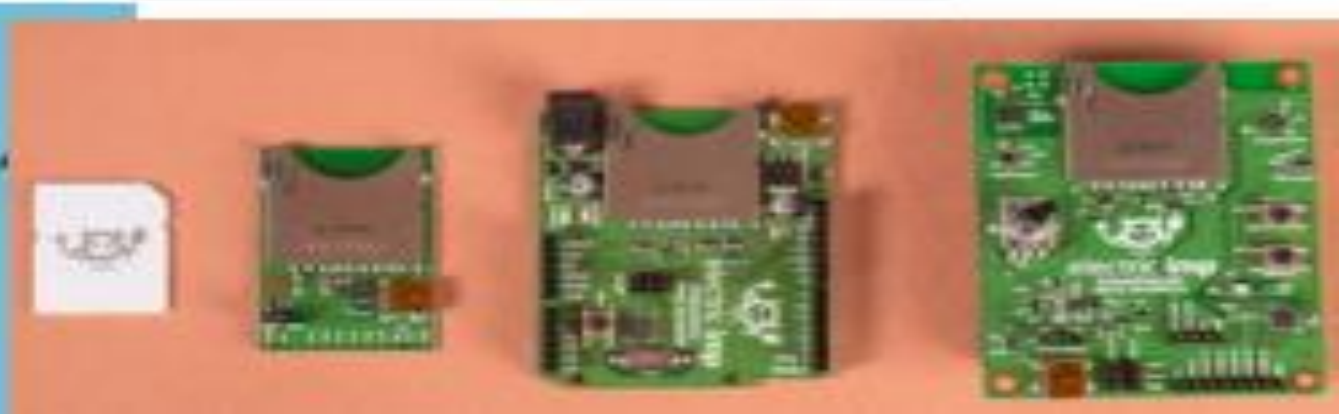
What if the access network merged with the cloud?

Mobile fog computing

TÍNH TOÁN HIỆN ĐẠI



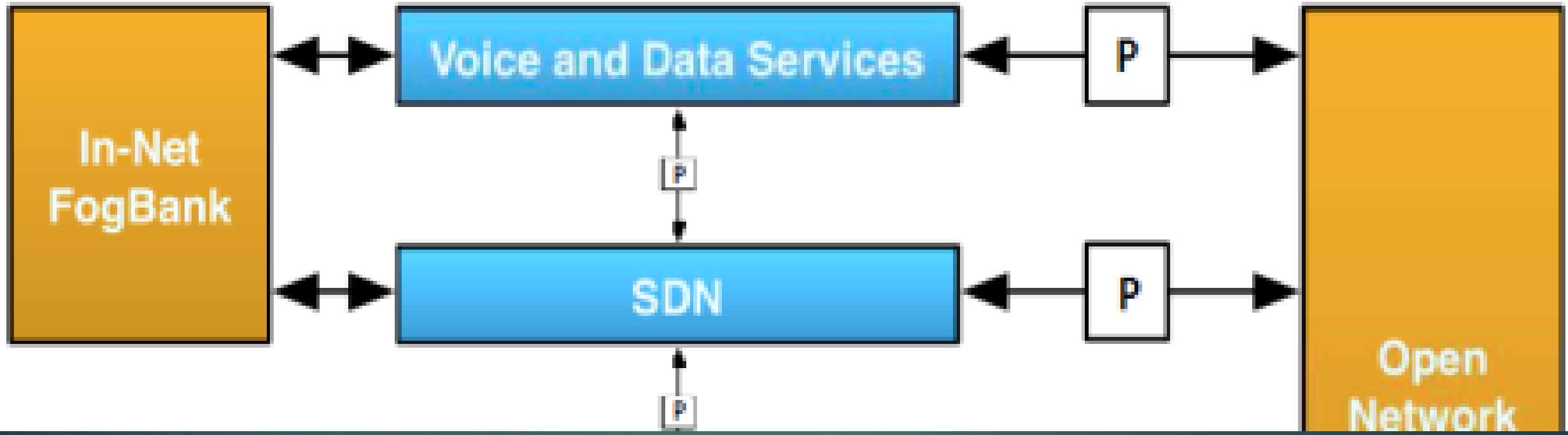




ĐIỀU GÌ SẼ XẢY RA NẾU CHÚNG TA KẾT HỢP TÍNH TOÁN VÀO MỌI THÀNH PHẦN CỦA MẠNG DI ĐỘNG?

ĐIỀU GÌ SẼ XẢY RA NẾU CHÚNG TA CHO PHÉP CÁC PHẦN TỬ MẠNG CỘNG TÁC VÀ CHIA SẺ THÔNG TIN?

crossmobile: một cách tiếp cận triệt để dựa trên tác nhân đối với mạng di động tích hợp sâu các khả năng tính toán và cung cấp tài nguyên chủ động



KHẢ NĂNG TÍNH TOÁN TÁC NHÂN PHẦN MỀM TRONG MỌI PHẦN TỬ MẠNG

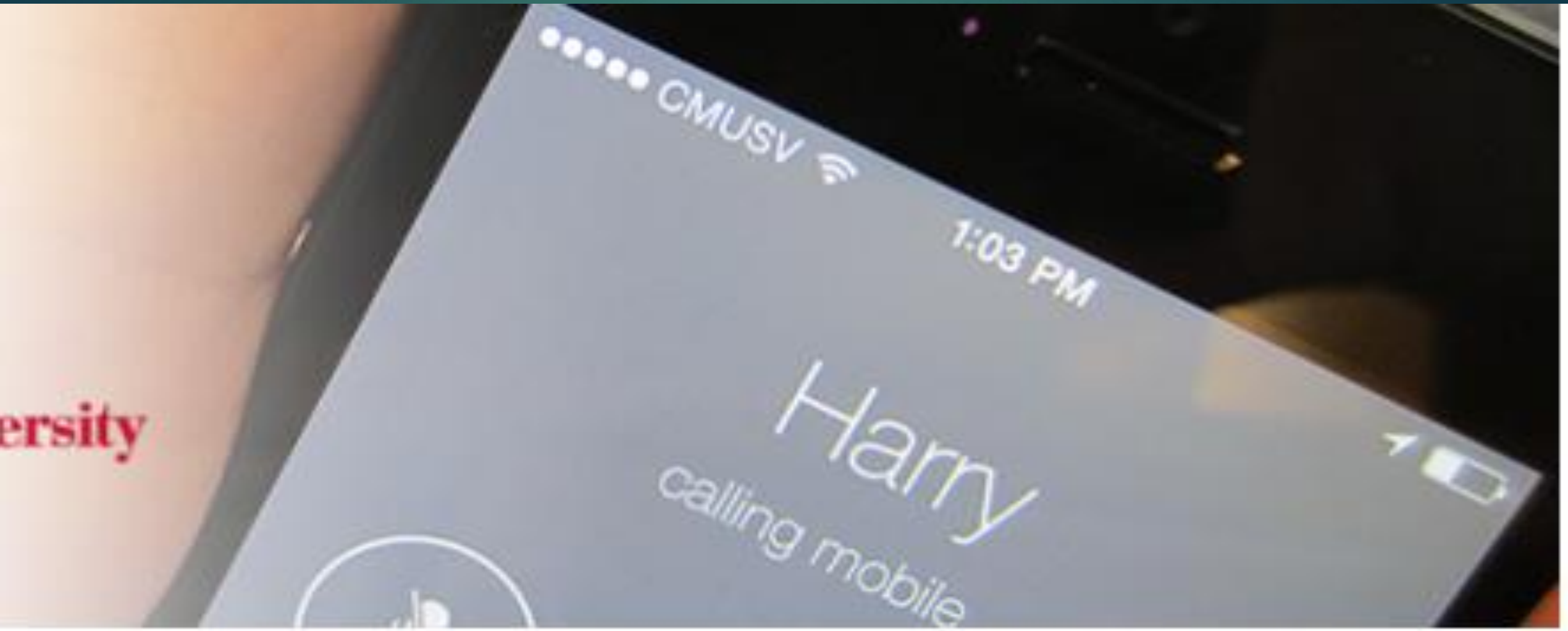
ĐÀM PHÁN VÀ PHÂN BỔ NGUỒN LỰC NHANH CHÓNG

HỖ TRỢ TÍCH HỢP SÂU CHO ĐỊNH GIÁ THEO ĐỒNG HỒ ĐO, DỊCH VỤ TÙY CHỈNH, MẠNG NHẬN BIẾT NGỮ CẢNH, V.V.

MẠNG COSSMobile

MẠNG COSSMobile

Mạng di động hoạt động đầy đủ (được FCC cấp phép) dựa trên các công cụ nguồn mở



RỦI RO CỦA VIỆC CHIA SẺ THÔNG TIN RỘNG RÃI (MẶC DÙ ĐƯỢC KIỂM SOÁT) TRÊN CÁC THIẾT BỊ, MIỀN, LỚP, V.V. LÀ GÌ?

RỦI RO BỔ SUNG CỦA MỌI THỨ DO PHẦN MỀM XÁC ĐỊNH?

KẾT THÚC HỌC PHẦN