BÀI #4 – GIỚI THIỆU OMNET++; CÁC MỐI ĐE DỌA LỚP VẬT LÝ

- GIỚI THIỆU OMNET++
- THÔNG TIN CƠ BẢN VỀ LỚP PHY VÀ CÁC MỐI ĐE DỌA

TS. HOÀNG SỸ TƯƠNG

GIỚI THIỆU VỀ OMNET++/INET?

OMNET++ LÀ GÌ?

• Đó là một bộ mô phỏng sự kiện riêng biệt cung cấp cơ sở cho mô phỏng "mạng"

– Mạng truyền thông

– Mạng xếp hàng

– Mạng logic kỹ thuật số

– '…' mạng

• Hai thành phần

– Nhân mô phỏng hướng sự kiện

– Các lớp tiện ích

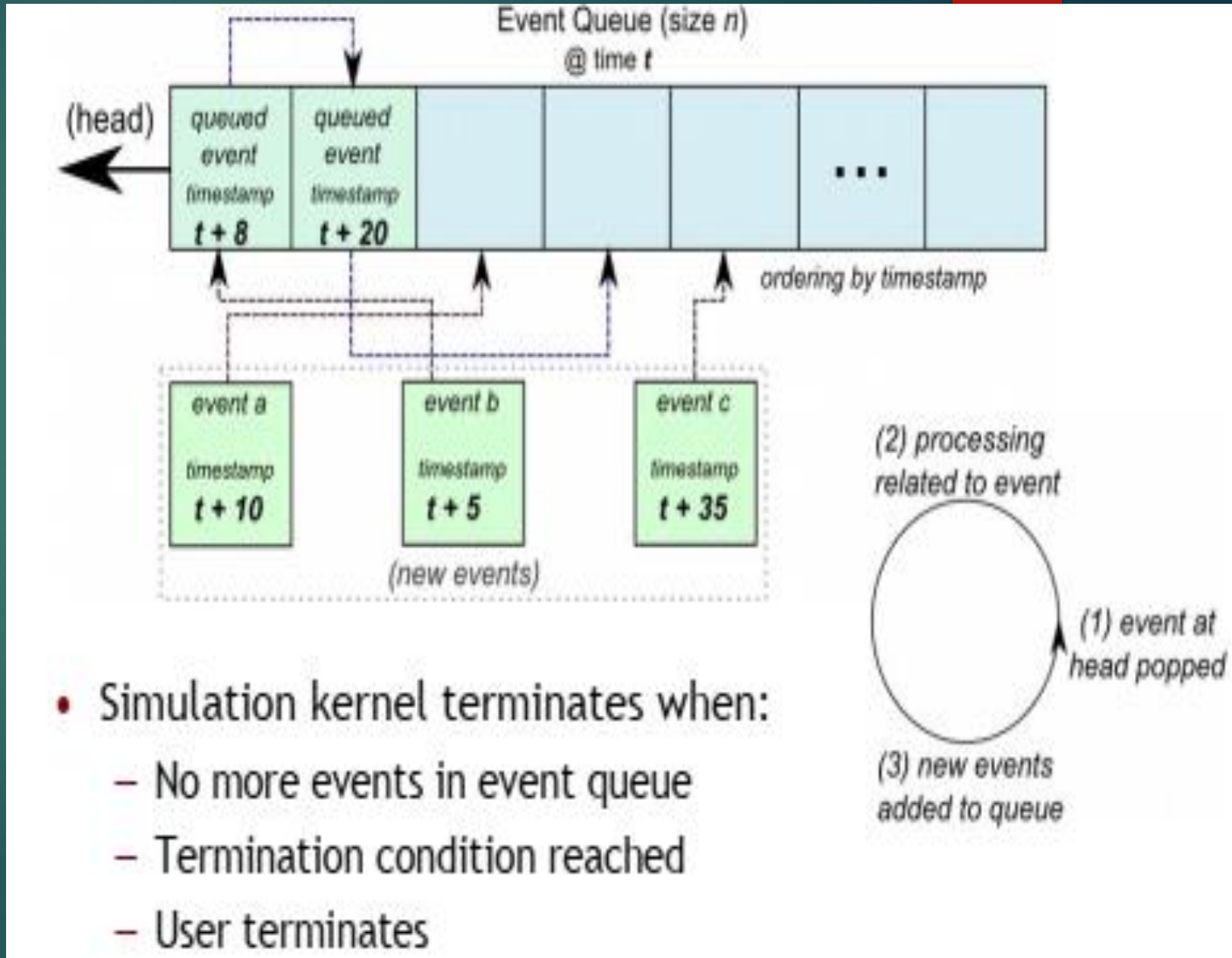
- Triển khai chức năng chung cho mô phỏng mạng
- Các hàm toán học
- Số liệu thống kê
- Các lớp trợ giúp các đặc trưng mạng vật lý
- – …

Nhân mô phỏng kết thúc khi:

- Không còn sự kiện nào trong hàng đợi sự kiện

– Đã đạt đến điều kiện chấm dứt

– Người dùng chấm dứt



MÔ HÌNH MÔ PHỎNG - SIMULATION MODELS

- Một mô hình mô phỏng bao gồm các mô-đun được nhóm lại/kết nối với nhau.
  - Các mô-đun được nhóm lại cùng với nhau
  - Cung cấp một hệ thống phân cấp mô-đun
- Trong OMNeT++, mô hình mô phỏng còn được gọi là *mạng*
  - Một mạng (mô hình mô phỏng) bản thân nó là một module

CÁC LOẠI MÔ-ĐUN - MODULE TYPES

Điều gì xảy ra bên trong một mô hình mô phỏng?

– Tất cả được bắt đầu với các *Mô-đun đơn giản*

- Khối xây dựng cơ sở
- Khai báo bằng ngôn ngữ NED
- Được hỗ trợ bởi các lớp C++ xác định hành vi của chúng
- Xác định các tham số để chuyển sang triển khai (C++)

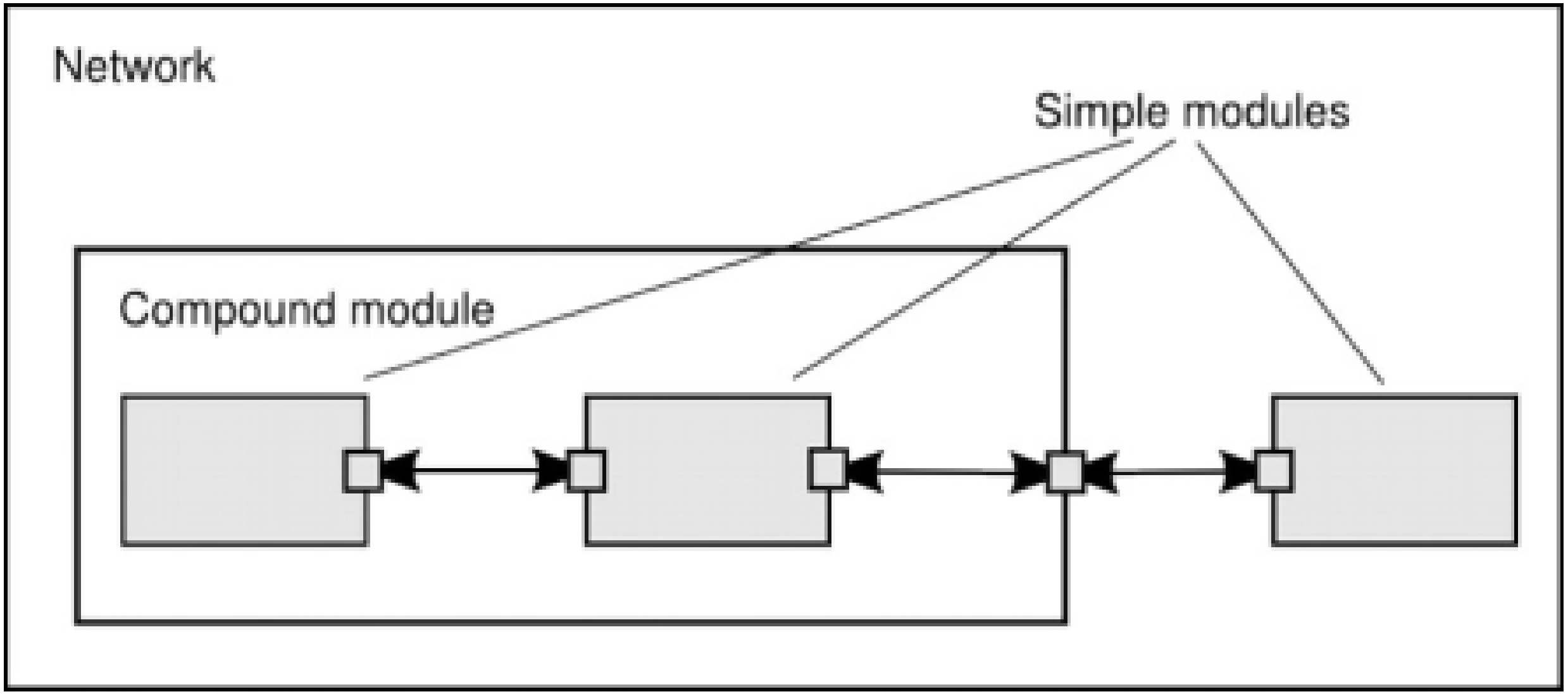
– Các mô-đun đơn giản nhóm lại với nhau để tạo thành Mô-đun phức hợp

- Khai báo bằng ngôn ngữ NED
- Xác định các tham số để chuyển đến các mô-đun đơn giản

MÔ HÌNH MÔ PHỎNG - CỔNG SIMULATION MODELS - GATES

- Cổng cho phép gửi tin nhắn
  - Tin nhắn chuyển giữa các cổng sử dụng các kết nối
    - Hai cổng có thể được liên kết trực tiếp thông qua một kết nối
      - Hãy nghĩ đến mạng truyền thông có dây
    - Các kết nối cũng có thể được sử dụng để chuyển trực tiếp một thông báo tới một cổng không được liên kết
      - Hãy nghĩ đến mạng truyền thông không dây
  - Các kết nối có thể được xác định và sử dụng lại
    - Các Kênh được gọi

MÔ HÌNH MÔ PHỎNG - SIMULATION MODELS



INET

- Gói mô phỏng mạng truyền thông cho OMNeT++
  - Cung cấp các mô hình cho nhiều giao thức mạng có dây/không dây
  - Các mô hình này xây dựng cùng nhau để tạo ra các mô hình mô phỏng các nút giao tiếp và mạng
  - Cung cấp hỗ trợ mạng truyền thông OMNeT++ mà chúng ta không cần phải viết các giao thức của riêng mình
- Dễ cài đặt – đi kèm với OMNET++
  - Đã có phiên bản dành cho nhà phát triển dev

LỰA CHỌN THỐNG KÊ

- Vectơ đầu ra

  - Dữ liệu chuỗi thời gian (Time-series data)

  – Nội dung được ghi lại trong quá trình mô phỏng

- Đầu ra vô hướng

  – Nội dung tổng hợp được ghi lại ở cuối mô phỏng

  – Mean of something, std dev of something,…

BỘ SƯU TẬP THỐNG KÊ

- Khai báo thống kê
  - Trong NED:
    - @statistic[stat_name](properties)
      - stat_name = biến được phát ra từ lớp C++
      - thuộc tính = nội dung cần ghi và ở dạng nào (vô hướng, vectơ)
    - @statistic[received_pkt](record=sum,vector?)
      - got_pkt là một biến được phát ra mỗi khi nhận được gói
      - Chúng tôi đang ghi lại vô hướng tổng số gói nhận được
      - Chúng tôi đang ghi vào một vectơ mỗi khi nhận được gói
      - Lưu ý dấu '?' - điều này có nghĩa là nó là tùy chọn

BỘ SƯU TẬP THỐNG KÊ

- Phát ra các biến (tín hiệu)
  - http://omnetpp.org/doc/omnetpp/manual/usman.html#s ec193
  - Đăng ký tín hiệu theo tên
    - registerSignal(“stat_name”)
      - stat_name phải khớp với tên được đưa ra trong khai báo NED
      - Hàm trả về id cho tín hiệu
  - Phát ra tín hiệu khi thích hợp
    - emit(signal_id, value)
      - signal_id = id của tín hiệu (được ánh xạ tới stat_name)
        - » simsignal_t signal_id = registerSignal("stat_name")

Ví dụ Thời gian

inet/examples/wireless/hosttohost/

TẦNG VẬT LÝ KHÔNG DÂY

PHY

PHY KHÔNG DÂY

• PHY không dây chịu trách nhiệm phân phát luồng bit từ bộ phát đến một hoặc nhiều bộ thu.

- Tx/Rx là viết tắt của "transmitter/receiver" trong lĩnh vực truyền thông và mạng máy tính. Nó thường được sử dụng để chỉ hai chức năng hoặc thiết bị riêng biệt: bộ truyền (transmitter) và bộ thu (receiver).

• Tx/Rxs cần được phối hợp về thời gian, không gian, tần số, pha, mã hóa/ngôn ngữ

• Không dây có nghĩa là có nhiều nguồn lỗi, lý do lỗi, v.v.

CHUẨN PHY

• Trong mạng WiFi, IEEE 802.11 xác định một số phiên bản của PHY, bao gồm các phần mở rộng cho lưới, phương tiện, v.v.

• Trong lĩnh vực viễn thông, dòng GSM 05. xx xác định lớp vật lý Um và các tiêu chuẩn khác được xây dựng trên đó, bao gồm các tiêu chuẩn ITU-T như 4G.

• Trong PAN, các tiêu chuẩn như 802.15.1 (Bluetooth), .3 (tốc độ cao, ví dụ: UWB) và .4 (tốc độ thấp, ví dụ: Zigbee) đều xác định các mô hình PHY của riêng chúng.

DỊCH VỤ PHY KHÔNG DÂY

- Các phần khác nhau của hoạt động PHY:
  - – Giao diện vô tuyến: phân bổ phổ, cường độ tín hiệu, băng thông, cảm biến sóng mang, đồng bộ pha,…
  - – Xử lý tín hiệu: cân bằng, lọc, huấn luyện, định dạng xung, báo hiệu,…
  - – Mã hóa: mã hóa kênh, xen kẽ bit, sửa lỗi fwd,…
  - – Điều chế (ánh xạ bit thành tín hiệu)
  - – Cấu trúc liên kết, ăng-ten, song công/đơn công, ghép kênh, v.v.
- PHY thường là phần phức tạp nhất của mạng không dây

CÁC MỐI ĐE DỌA LỚP PHY LÀ GÌ?

TRỞ LẠI VỚI VÍ DỤ VỀ BỮA TIỆC

HOẠT ĐỘNG SAI Ở TẦNG VẬT LÝ

- Phương tiện mở, chia sẻ dễ bị tấn công

– Bất cứ ai cũng có thể "nói chuyện" → tấn công greedy (tham lam) hoặc tấn công sử dụng mã độc có thể dễ dàng can thiệp

- *Ngăn chặn/làm suy giảm truyền thông thông qua gây nhiễu*
- *Việc cắt giảm các tài nguyên có sẵn ảnh hưởng đến việc kiểm soát, vận hành và hiệu suất của mạng*

– Ai cũng có thể "nghe" ⟶ các nút tò mò hoặc độc hại có thể dễ dàng nghe trộm thông tin liên lạc

- *Khôi phục thông tin được trao đổi bởi hàng xóm (vi phạm dữ liệu, danh tính, hoạt động/ý định riêng tư)*
- *Suy luận/học hỏi, theo dõi, quan sát*

THÁCH THỨC

• Làm cách nào chúng ta có thể ngăn chặn một bên tò mò hoặc có ý đồ xấu nghe lén đường truyền không dây ở lớp vật lý?

• Làm cách nào chúng ta có thể ngăn chặn một bên tham lam hoặc độc hại can thiệp vào quá trình truyền và nhận PHY?

• Cho cả hai trường hợp:

– *Câu trả lời ngắn gọn, chúng ta không thể*

– *Câu trả lời dài, chúng ta có thể làm cho nó khó khăn hơn*

TRẢI PHỔ - SPREAD SPECTRUM

• Trải phổ là một phần mở rộng của ghép kênh sử dụng ngẫu nhiên để tăng tính đa dạng và cải thiện hiệu suất theo nhiều cách khác nhau

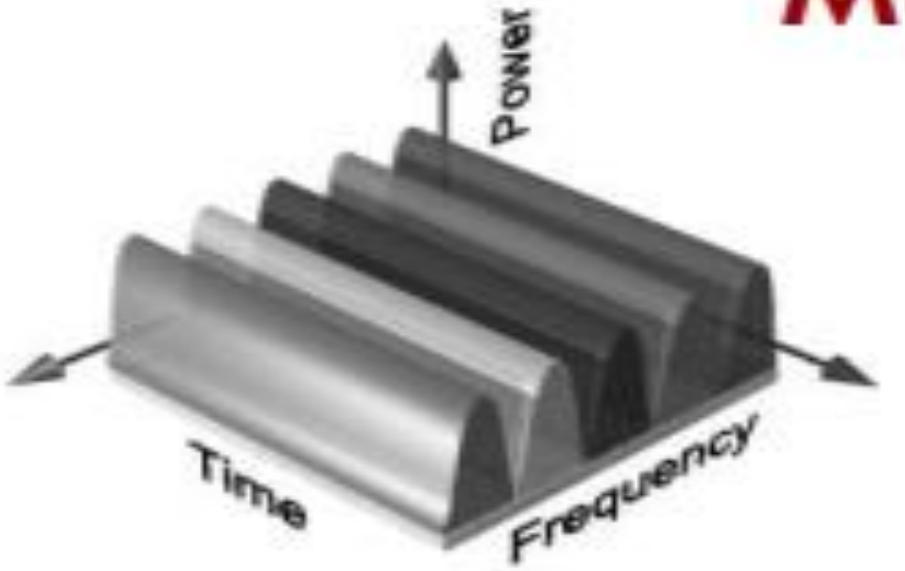
– Trải phổ nhảy tần (FHSS) được xây dựng trên FDM cho phép các thiết bị di chuyển giả ngẫu nhiên giữa các kênh tần số

• *Nếu một kênh đặc biệt tốt hoặc xấu, mọi người sẽ chia sẻ nó một cách ngẫu nhiên*

– Trải phổ chuỗi trực tiếp (DSSS) được xây dựng trên CDM cho phép các thiết bị di chuyển giả ngẫu nhiên giữa các không gian mã khác nhau

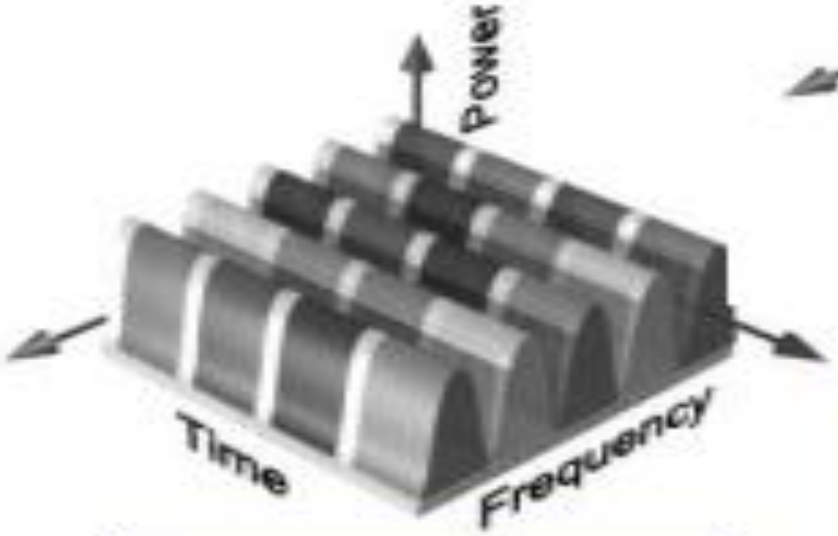
• *Không gian mã tương tự như dải tần số*

Multiplexing

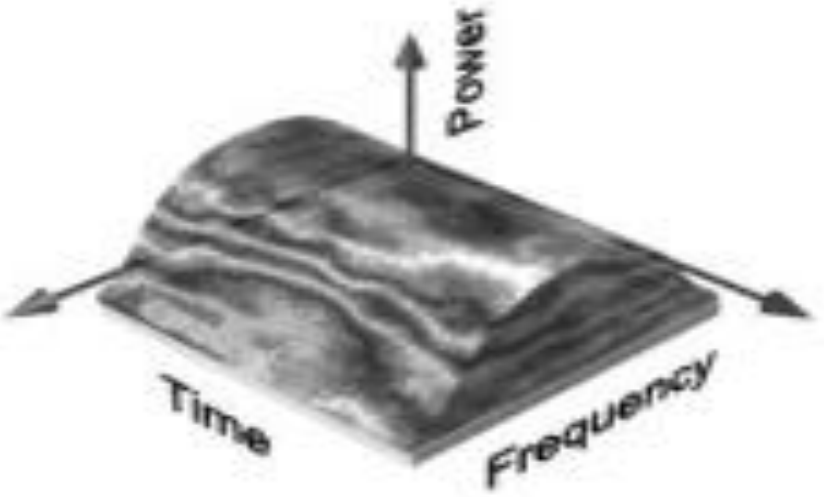


FDM - frequency division multiplexing

TDM - time division multiplexing (flip x-y)



TDM + FDM as in GSM

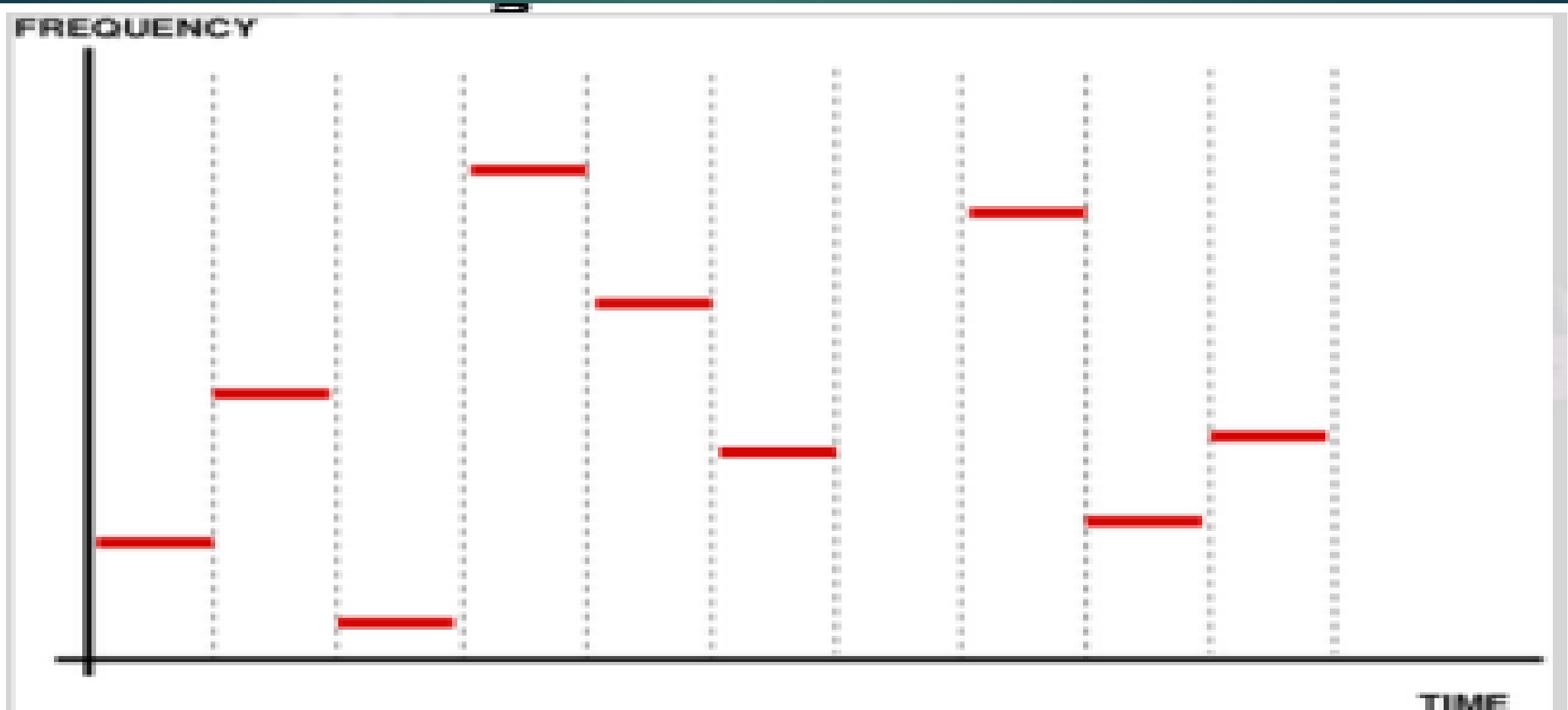


CDM - code division multiplexing

images from [Erik Lawson, SkyDSP.com]

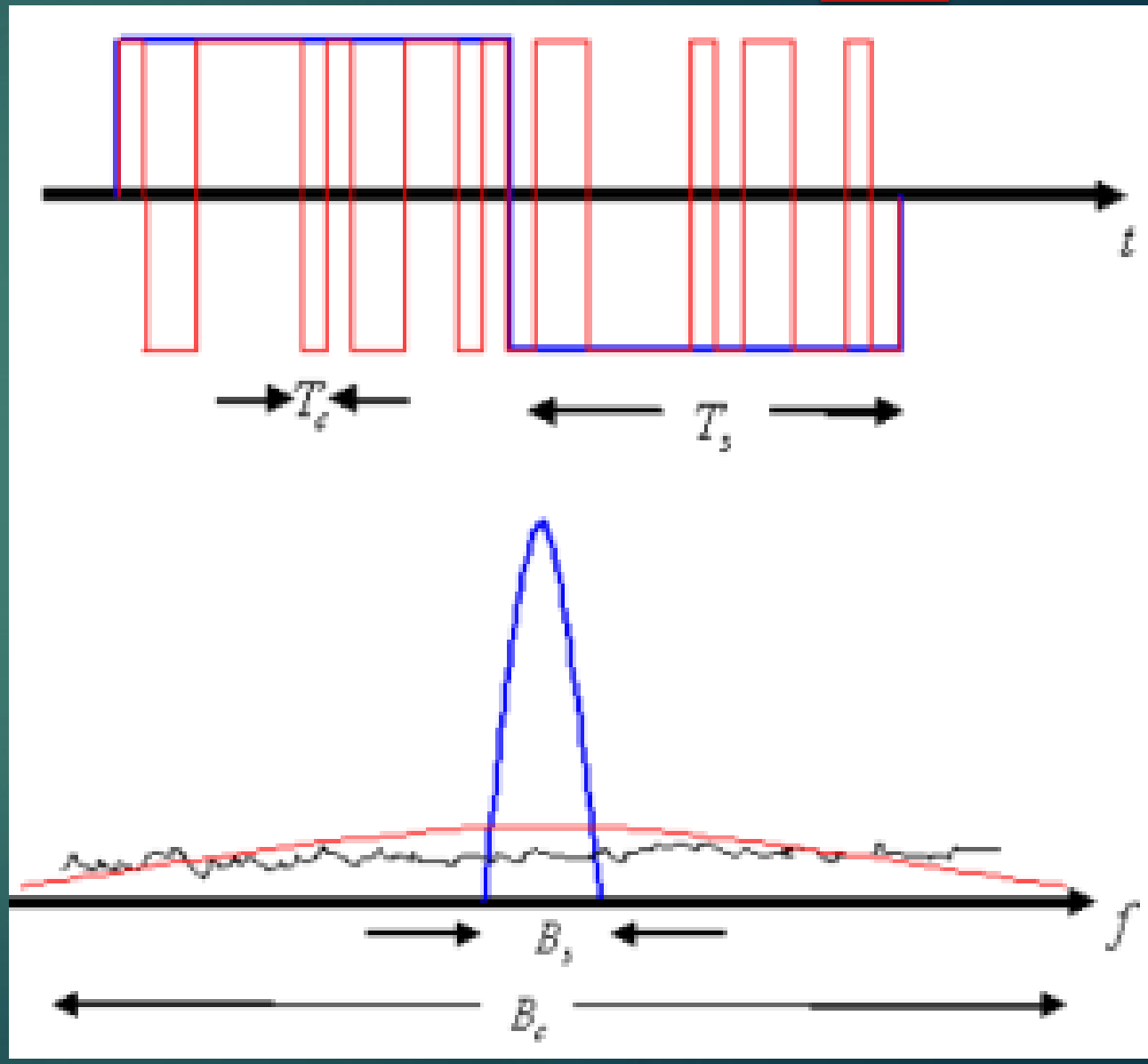
FHSS

- FHSS: Người gửi và người nhận đồng bộ hóa mẫu nhảy (hopping Pattern) qua băng thông rộng



MÃ HÓA DSSS - DSSS ENCODING

- Mã hóa DSSS ánh xạ các ký hiệu dài thành chuỗi các chip ngắn
- Thời lượng chip ngắn hơn có nghĩa là băng thông rộng hơn



LỢI ÍCH

- FHSS:
  - *Nhiễu băng hẹp chỉ có tác dụng trong một phần nhỏ thời gian*
  - *Máy nghe trộm một kênh không thể "theo dõi" tín hiệu và cần sử dụng băng thông rộng hơn nhiều để nghe được mọi thứ*
- DSSS:
  - *Nhiễu dải hẹp được "giải tán - despread" ở máy thu, giống như nhiễu dải rộng yên tĩnh hơn*
  - *Các tín hiệu khác (gần như) trực giao*
  - *Người nghe trộm phải biết/đoán mã để giải mã*

MÃ HÓA SS - CRYPTOGRAPHIC SS

- Dựa trên trải phổ cơ bản, chúng ta có thể thêm mã hóa ngẫu nhiên để làm cho lịch trình nhảy và trình tự mã trở nên bí mật

  – *Sử dụng khóa đối xứng làm đầu vào cho PRNG làm cho lịch trình nhảy hoặc trình tự mã trở nên bí mật*

- Trong cả hai trường hợp, điều này yêu cầu quản lý khóa đối xứng, có vấn đề của nó

CÁC VẤN ĐỀ VỚI TRẢI PHỔ

• Để chống lại sự tò mò/tham lam/ác ý một cách hiệu quả, các chuỗi nhảy (FHSS) và mã phát tán (DSSS) phải ở chế độ riêng tư

– *Trong nhiều giải pháp được triển khai, các mã này được cấp cho tất cả thành viên nhóm – nếu trở thành thành viên nhóm thì dễ dàng, không có rào cản*

– *Nếu thành viên nhóm được bảo vệ chặt chẽ, nó có thể bị mua chuộc hoặc đánh cắp không?*

• Nếu không lấy được mã thì có học được không?

– *Tái sử dụng mã cho phép phân tích và phục hồi thống kê*

CỨNG HÓA PHY

- Nếu vấn đề trải phổ không đủ thì còn phải làm gì thêm nữa?
  - – Đa dạng có thể bảo vệ chống lại nhiều mối đe dọa ở nhiều cấp độ
  - – Việc triển khai phải xem xét các mô hình mối đe dọa và thích ứng với các hành vi không mong muốn
    - *Ngăn chặn phân tích thống kê, thích nghi với việc học của kẻ tấn công*

BUỔI 5:

BẢO MẬT TẦNG VẬT LÝ