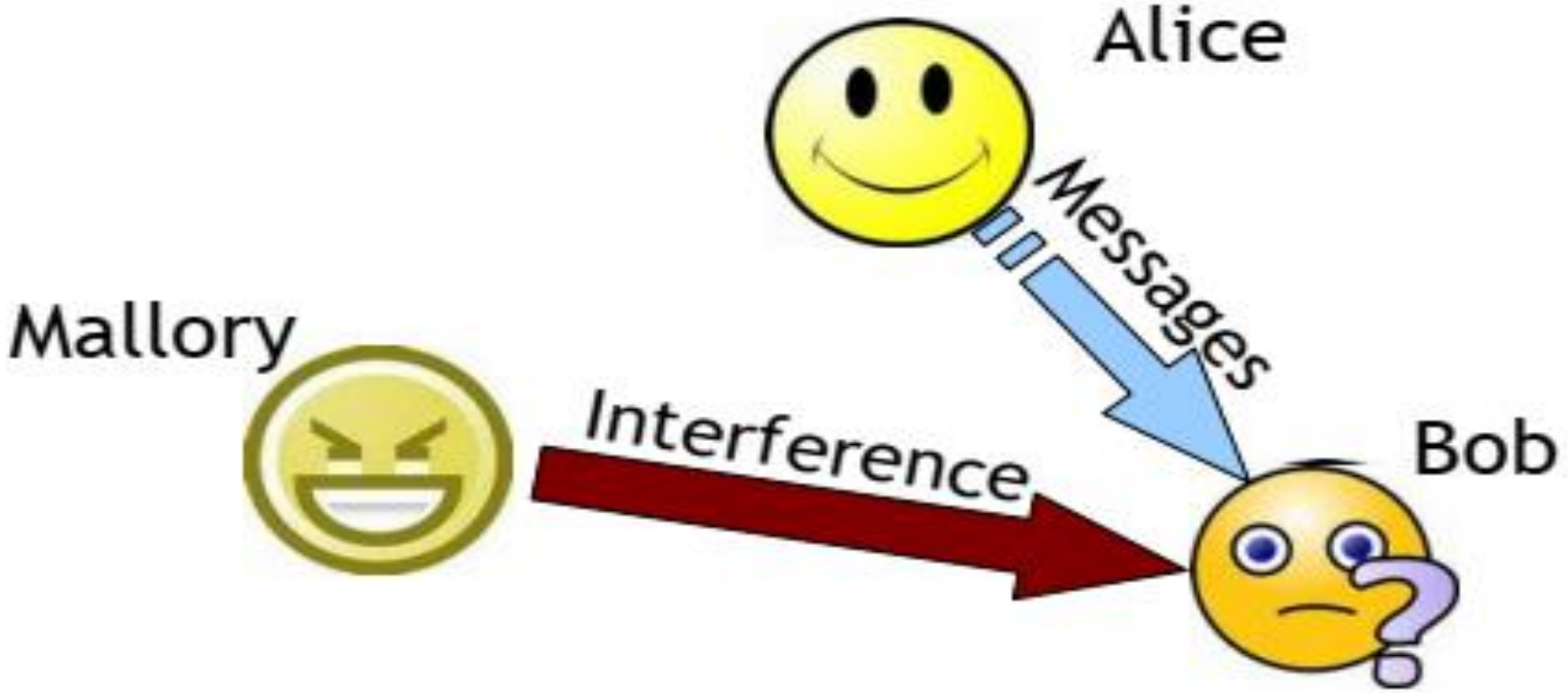
BÀI #5 – GÂY NHIỄU, "BẢO MẬT TẦNG VẬT LÝ"

- Tấn công gây nhiễu và phòng thủ
- Bảo mật sử dụng thuộc tính tầng vật lý
- Xác thực sử dụng thuộc tính tầng vật lý

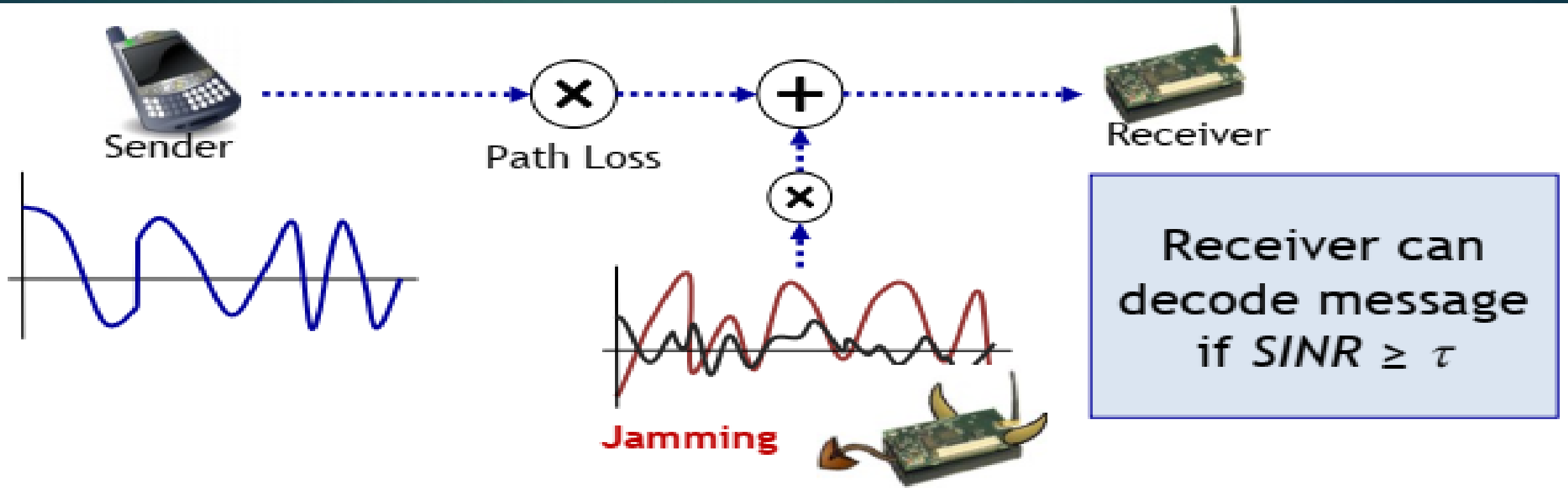
TẤN CÔNG GÂY NHIỄU (JAMMING)

TẤN CÔNG GÂY NHIỄU (JAMMING)

• Về mặt khái niệm, gây nhiễu là một cuộc tấn công từ chối dịch vụ tầng vật lý nhằm ngăn chặn giao tiếp không dây giữa các bên



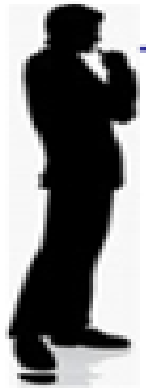
CÁC TẤN CÔNG JAMMING HOẠT ĐỘNG NHƯ THẾ NÀO?



Chèn SINR gây ra lỗi giải mã và mất gói

Nhưng, nó phức tạp hơn thế nhiều...

VẤN ĐỀ HÌNH HỌC - GEOMETRY MATTERS



Attacker can be MUCH quieter than speaker

- Ma trận SINR nắm bắt các tác động của hình học

SINR metric captures effects of geometry

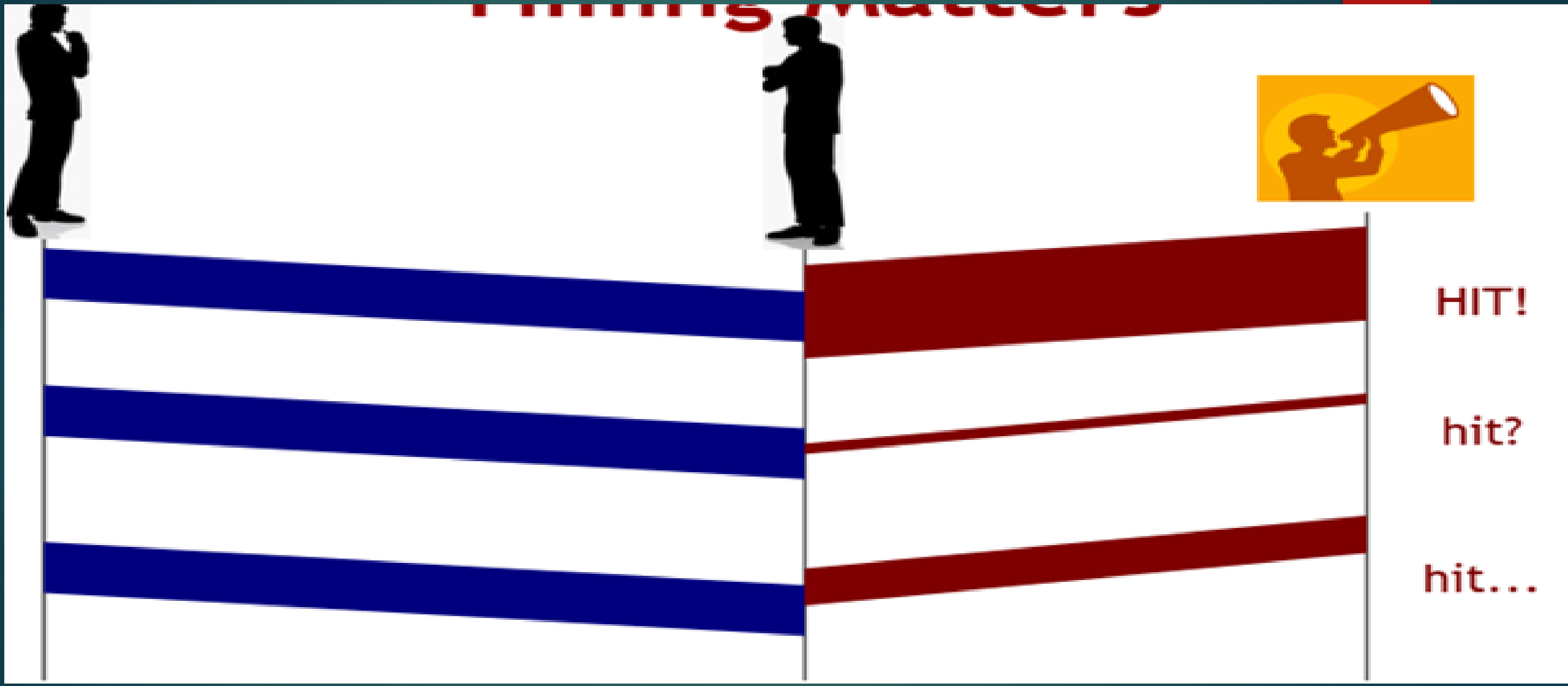
SINR = (Rx signal power) / (noise power + Rx jamming power)

Often modeled as $P_{tr} = k_t P_t d_{tr}^{-\alpha}$

Typically random variable N_0

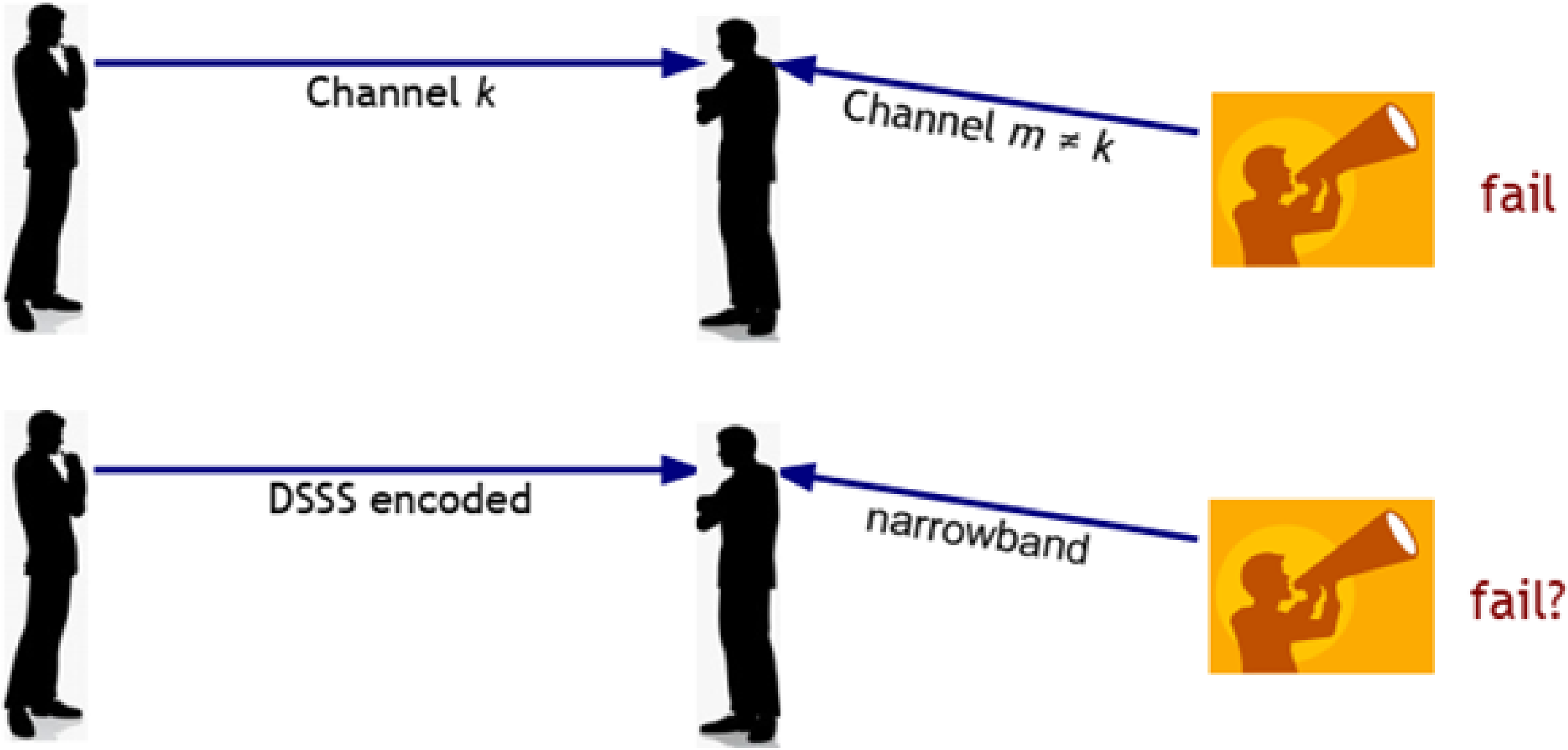
Often modeled as $P_{jr} = k_j P_j d_{jr}^{-\alpha}$

VẤN ĐỀ THỜI GIAN



- Có thể được lập mô hình dưới dạng một phép nhân (ngẫu nhiên) trong thuật ngữ “I” của ma trận SINR

VẤN ĐỀ TRỰC GIAO



GÂY NHIỄU TỔNG QUÁT - GENERALIZED JAMMING

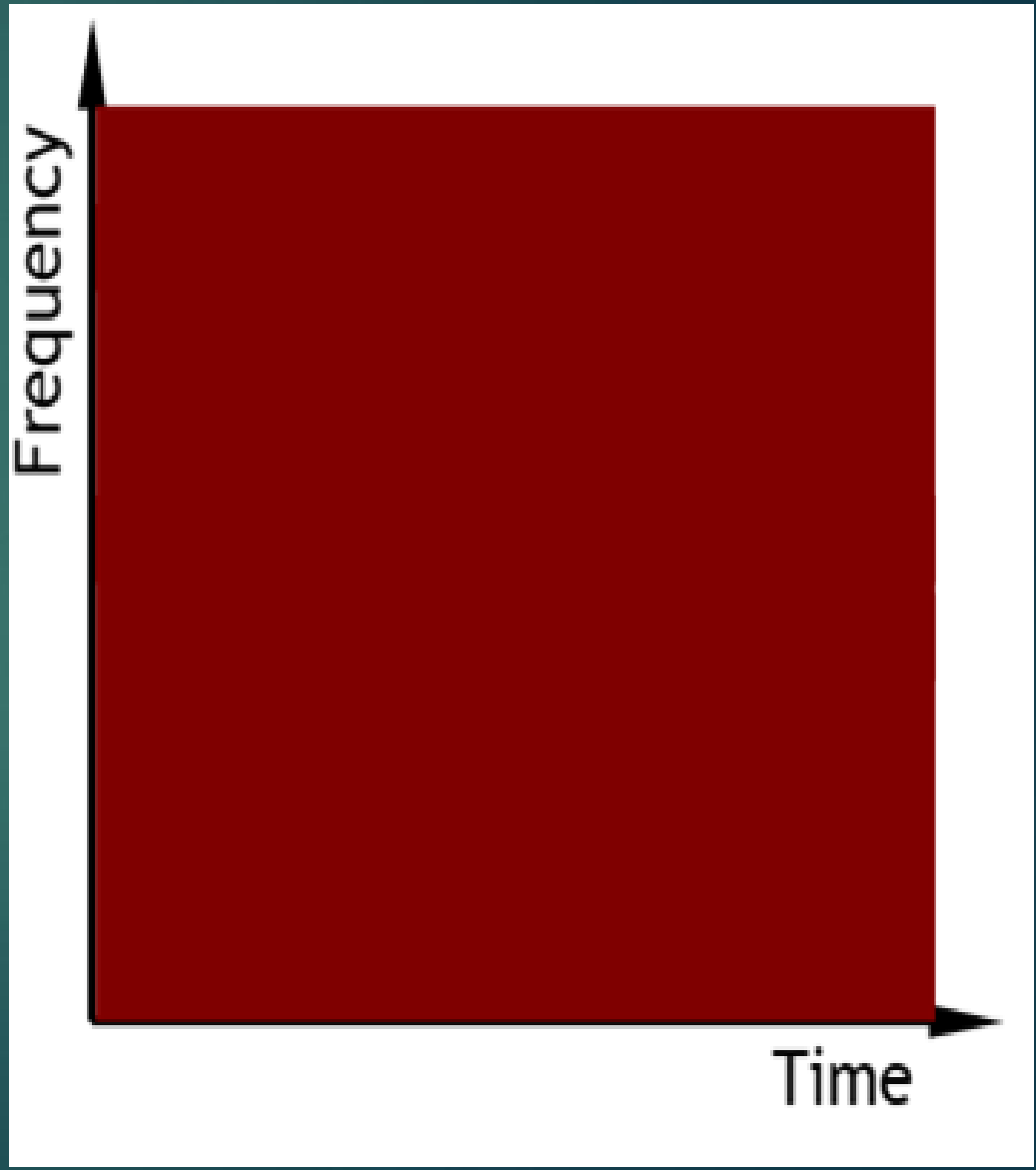
- Thiết bị gây nhiễu phân bổ năng lượng/tín hiệu cho các tài nguyên theo thời gian, tần số, v.v. khác nhau theo chiến lược tấn công S

  – Hiệu ứng E(S) của tấn công

  – Chi phí C(S) của cuộc tấn công

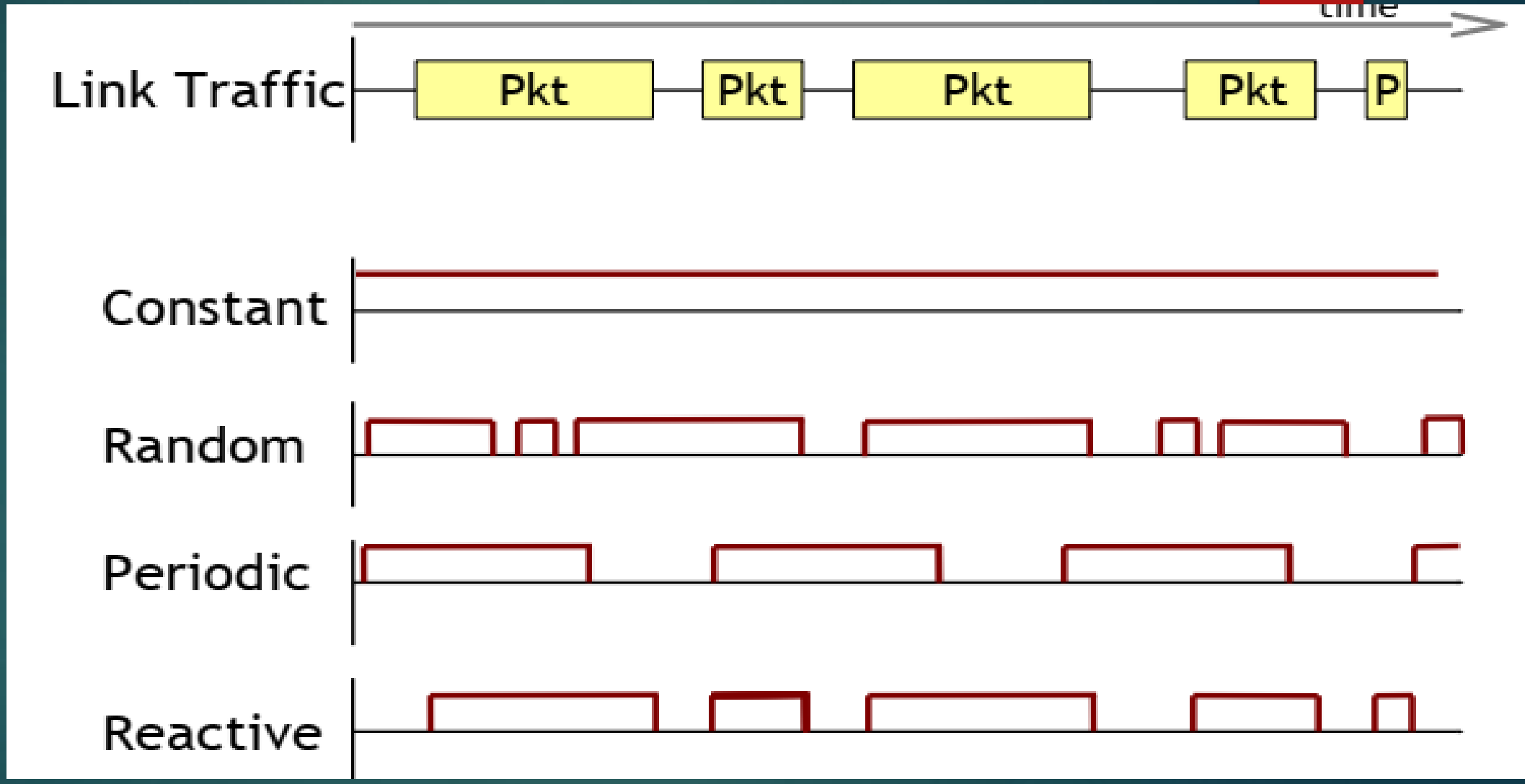
  – Rủi ro R(S) bị phát hiện/ trừng phạt

  – Với các số liệu khác, tối ưu hóa xuất hiện



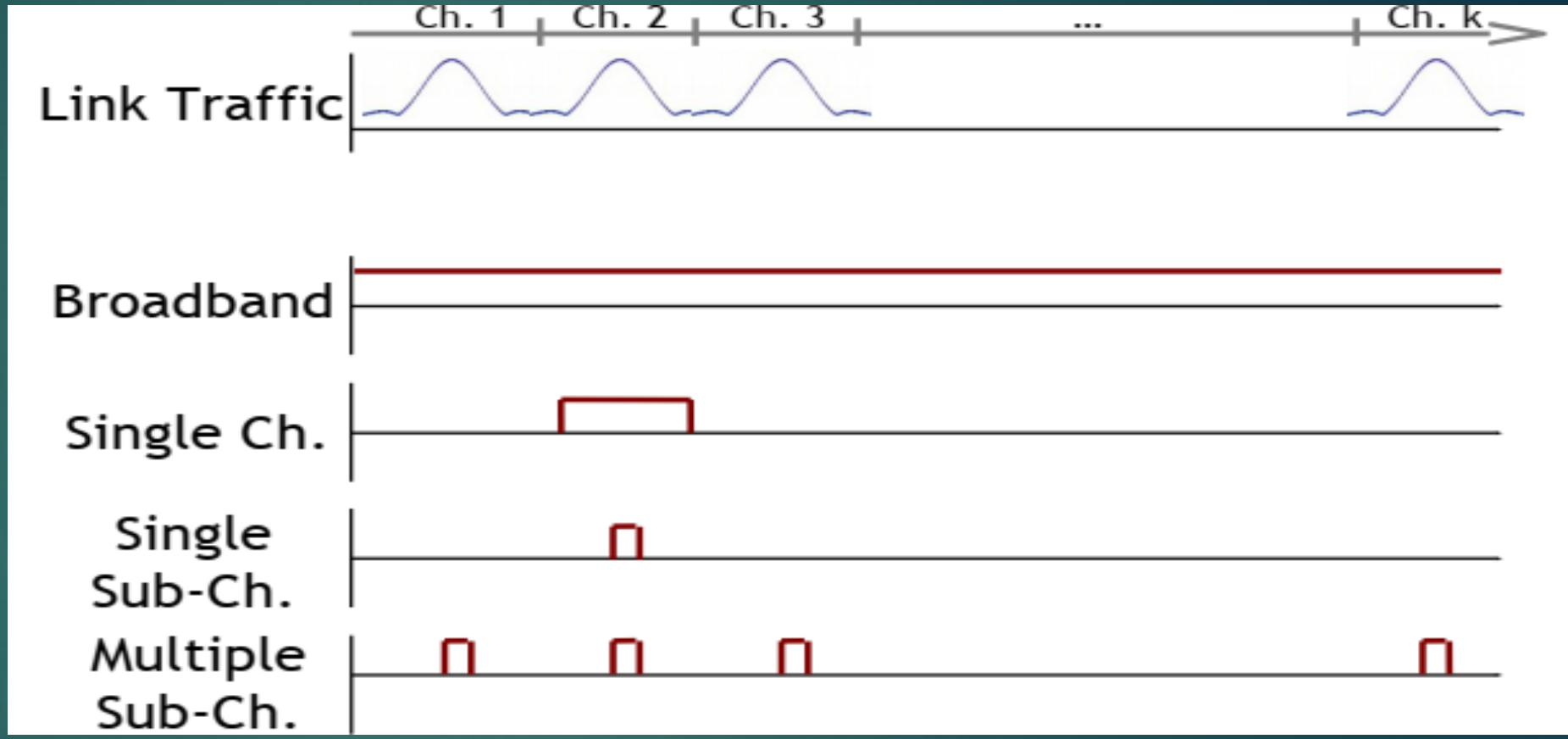
CHIẾN LƯỢC GÂY NHIỄU
Miền thời gian

- Liên kết lưu thông
- Không thay đổi
- Ngẫu nhiên
- định kỳ
- Hồi đáp nhanh



CHIẾN LƯỢC GÂY NHIỄU
Tần số khu vực

- Liên kết lưu lượng
- Băng thông rộng
- Single Ch.
- Single Sub-Ch.
- Multiple Sub-Ch.



LÀM THẾ NÀO CHÚNG TA CÓ THỂ BẢO VỆ CHỐNG GÂY NHIỄU?

PHÁT HIỆN VÀ PHÒNG THỦ CÁC TẤN CÔNG GÂY NHIỄU

- **Mục tiêu:** phát hiện và khoanh vùng các cuộc tấn công gây nhiễu, sau đó né tránh chúng hoặc phản ứng với chúng
- **Thách thức:** phân biệt giữa các hành vi đối nghịch và tự nhiên (kết nối kém, hết pin, tắc nghẽn, lỗi nút, v.v.)
  - *Một số mức độ lỗi phát hiện sẽ xảy ra*
  - *Thích hợp triển khai trong mạng cảm biến*
- **Cách tiếp cận:** phát hiện thô dựa trên quan sát gói tin

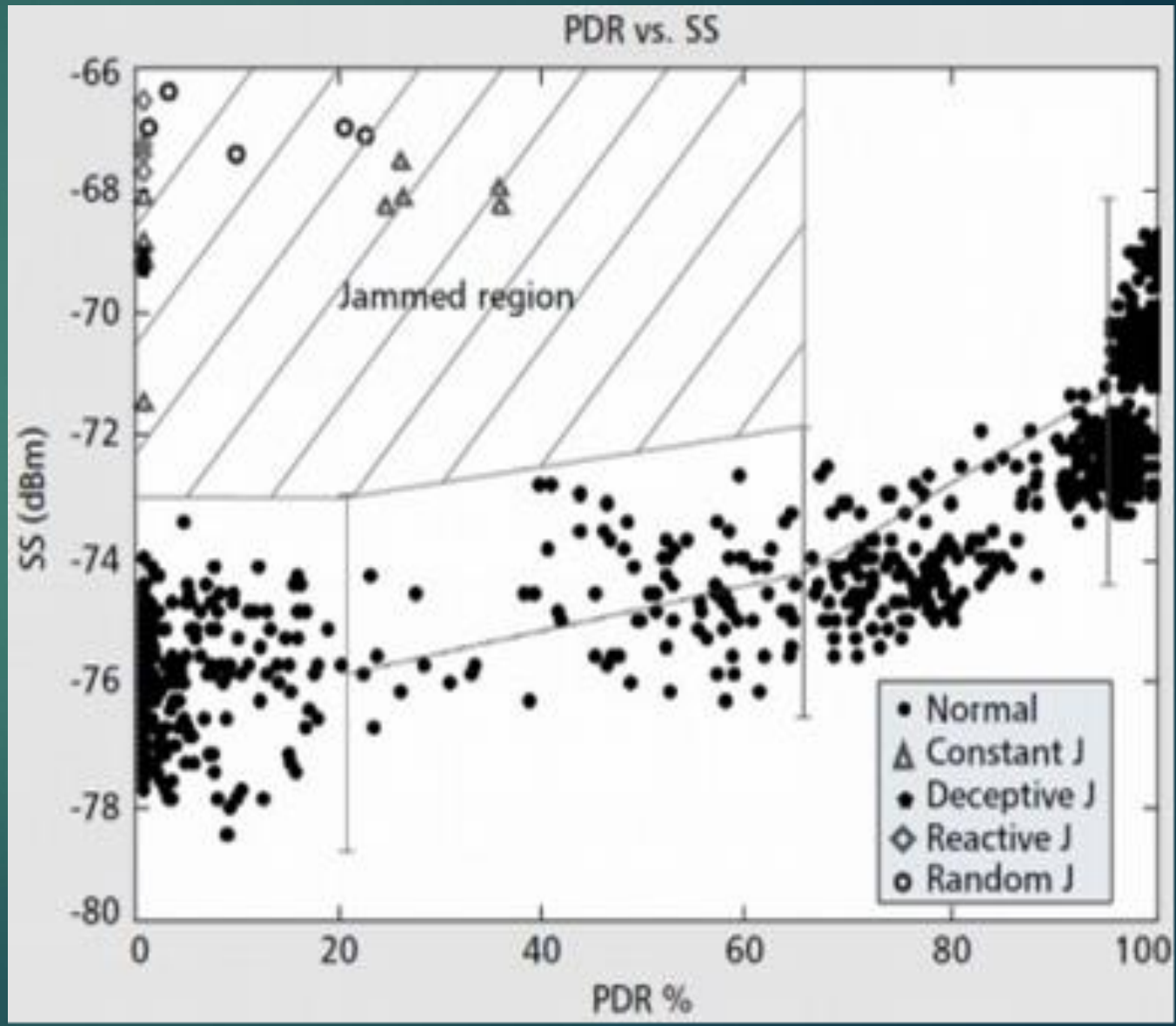
THỐNG KÊ PHÁT HIỆN TẤN CÔNG

- Cường độ tín hiệu nhận được (RSSI)
  - *Tín hiệu gây nhiễu sẽ ảnh hưởng đến phép đo RSSI*
  - *Rất khó phân biệt giữa nhiễu/tự nhiên*
- Thời gian cảm nhận sóng mang
  - *Giúp phát hiện gây nhiễu khi hoạt động sai của MAC*
  - *Không giúp ích cho các trường hợp ngẫu nhiên hoặc phản ứng*
- Tỷ lệ phân phối gói (PDR)
  - *Gây nhiễu làm giảm đáng kể PDR (xuống ~0)*
  - *Mạnh mẽ đối với tắc nghẽn, nhưng các tấn công khác (lỗi nút) cũng khiến PDR → 0*

PHÁT HIỆN TẤN CÔNG NÂNG CAO

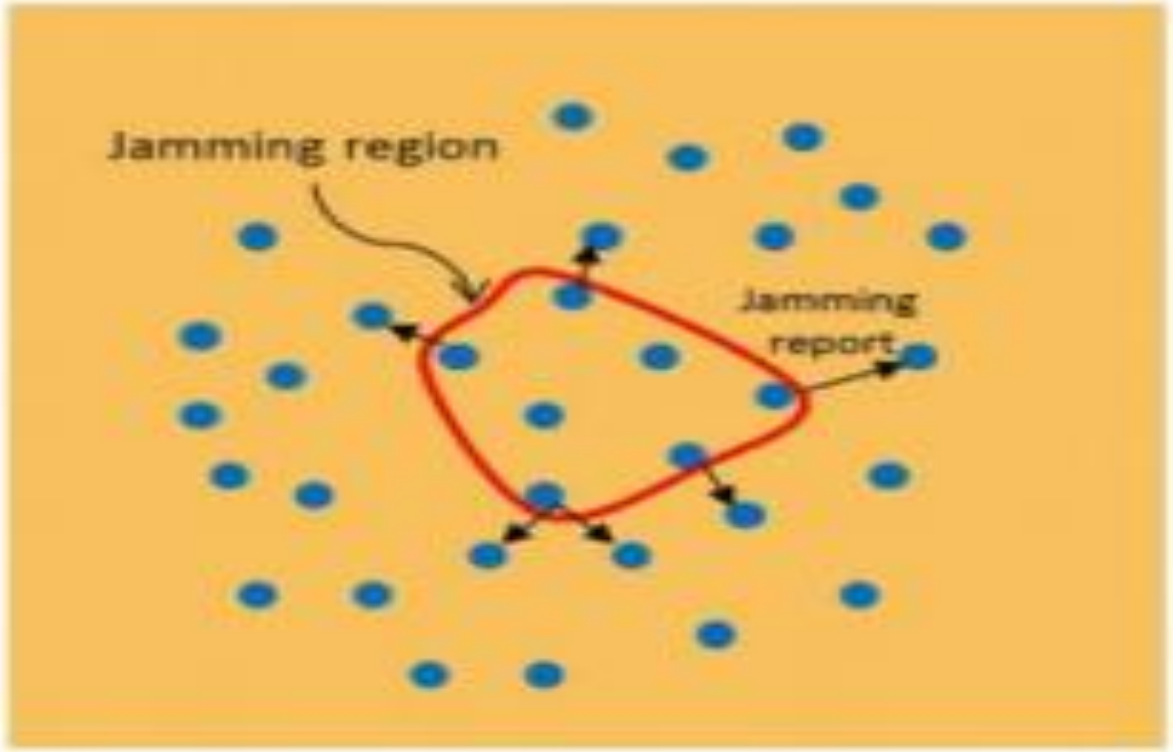
- Kết hợp nhiều số liệu thống kê trong phát hiện có thể giúp
  - PDR cao + RSSI cao → OK
  - PDR thấp + RSSI thấp → Kết nối kém
  - PDR thấp + RSSI cao → ? → Tấn công gây nhiễu?

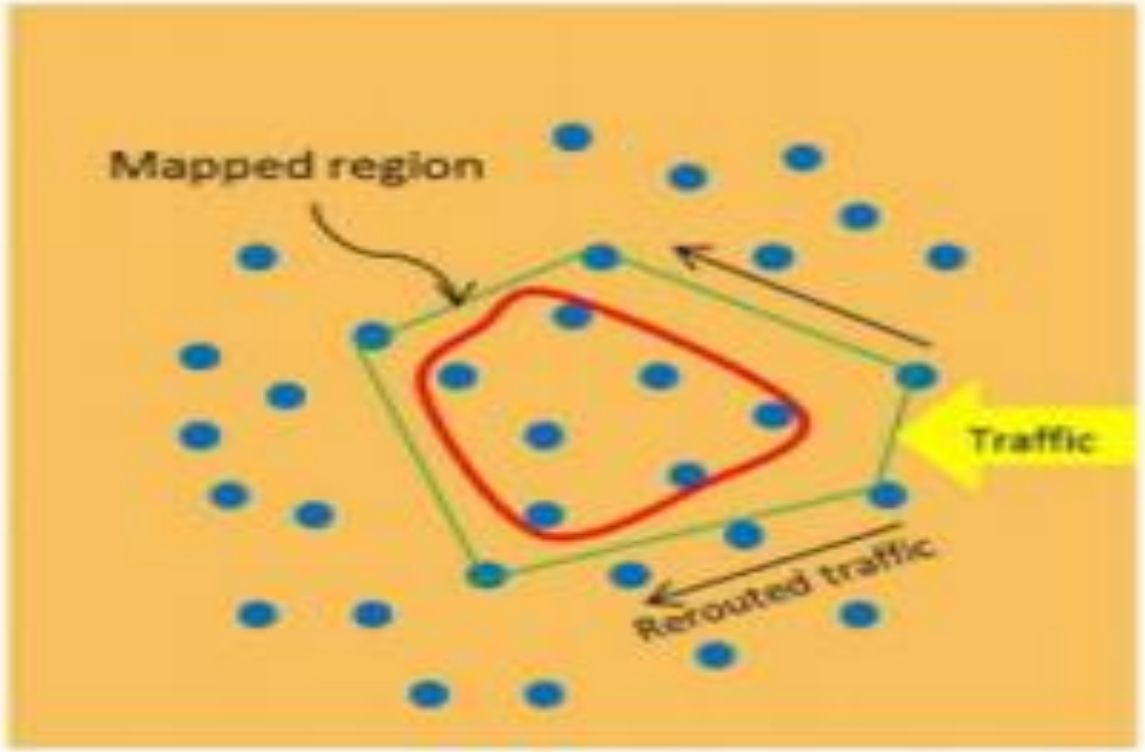
Hãy cẩn thận: điều này giả định RSSI có thể được đo chính xác



LẬP BẢN ĐỒ KHU VỰC BỊ KẸT

- Dựa trên các kỹ thuật phát hiện nâng cao, các nút có thể tìm ra khi chúng bị kẹt
- Tại ranh giới của khu vực bị kẹt, các nút có thể nhận được thông báo cho các nút không bị kẹt
- Các nút không bị kẹt có thể cộng tác để thực hiện phát hiện ranh giới bằng cách sử dụng thông tin vị trí





TRÁNH GÂY NHIỄU

- Các nút trong vùng bị nhiễu có thể tránh được cuộc tấn công, về mặt quang phổ hoặc không gian

  – Né tránh phổ → "Lướt kênh" để tìm phổ mở và nói chuyện với các nút không bị kẹt

  – Né tránh không gian → rút lui ra khỏi khu vực kẹt xe

    - *Cần bù cho khả năng phân vùng mạng của thiết bị gây nhiễu di động*

CÁC CHIẾN LƯỢC TẤN CÔNG VÀ PHÒNG THỦ ĐỘNG THÌ SAO?

PHÁT HIỆN VÀ GÂY NHIỄU TỐI ƯU

- **Thiết lập vấn đề:** mỗi mạng và thiết bị gây nhiễu có quyền kiểm soát xác suất truyền và gây nhiễu ngẫu nhiên

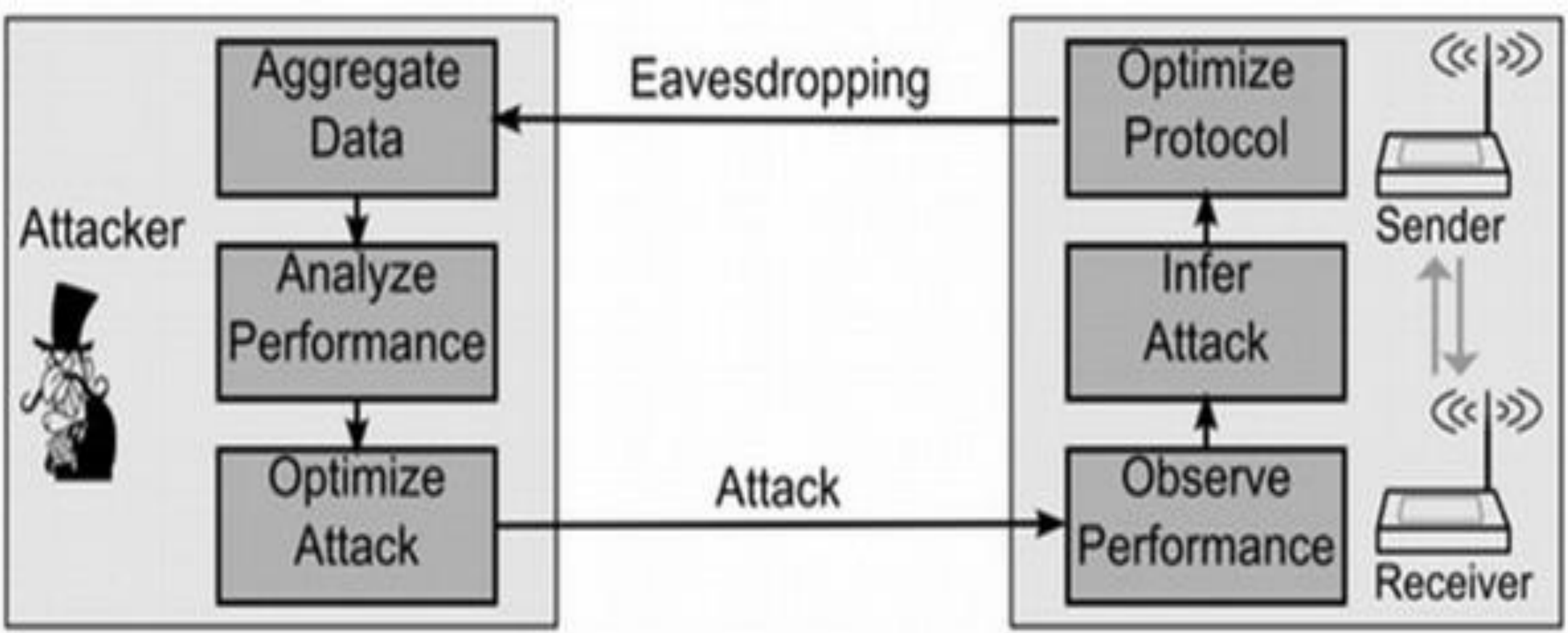
  – Tham số mạng y là xác suất mỗi nút sẽ truyền trong một khe thời gian

  – Tham số tấn công q là xác suất thiết bị gây nhiễu sẽ truyền trong một khe thời gian

- Đối thủ có thể tìm hiểu về các mục tiêu thông qua quan sát và tối ưu hóa cho min-max/max-min

TRÒ CHƠI GÂY NHIỄU

• Điều gì sẽ xảy ra nếu cả bên tấn công và bên phòng thủ đều tự do thích ứng với nhau?

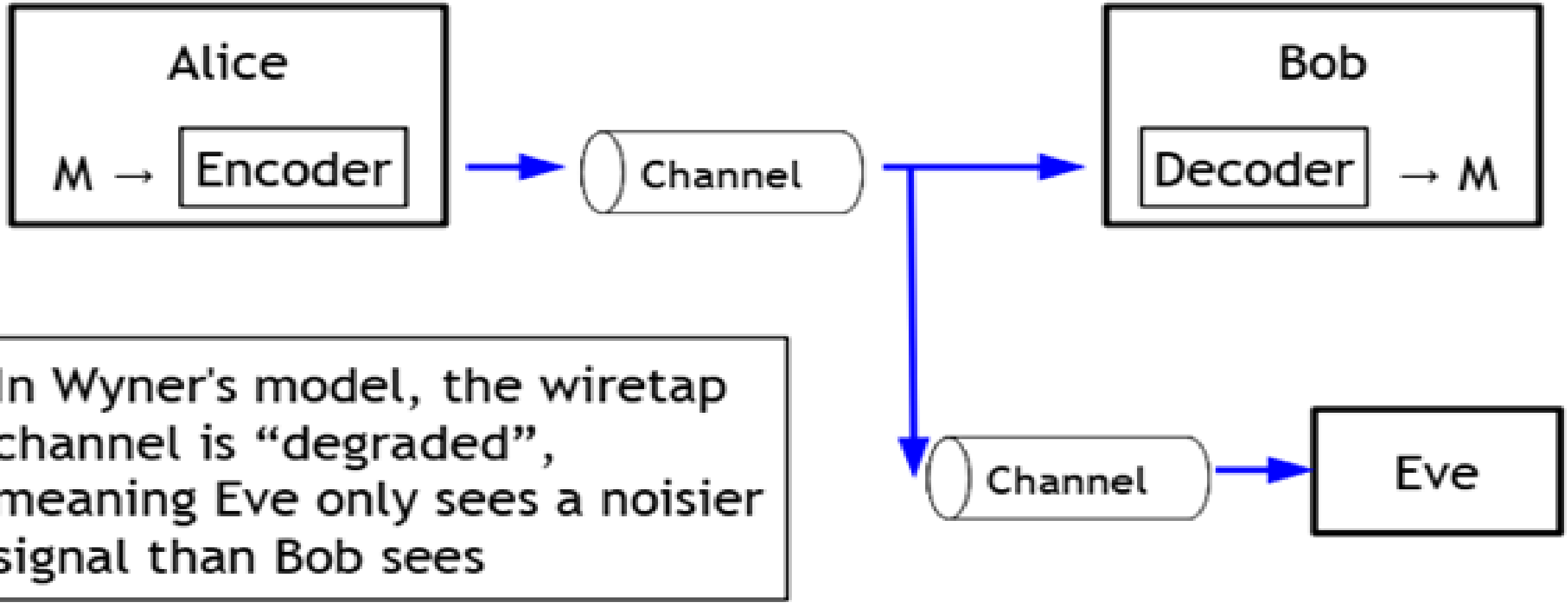


LÀM THẾ NÀO CÁC THUỘC TÍNH CỦA PHƯƠNG TIỆN KHÔNG DÂY CÓ THỂ GIÚP ĐẠT ĐƯỢC LIÊN LẠC AN TOÀN?

RÌNH MÒ BỮA TIỆC

“NGHE LÉN” - WIRETAPPING

• Năm 1975, A. D. Wyner định nghĩa kênh nghe lén để chính thức hóa hoạt động nghe trộm



CÔNG SUẤT BÍ MẬT - SECRECY CAPACITY

- Vì kênh Alice → Eve nhiễu hơn kênh Alice → Bob:

  – Eve không thể giải mã mọi thứ mà Bob có thể giải mã

  – Tức là tồn tại một cách mã hóa sao cho Alice có thể mã hóa các thông điệp mà Bob có thể giải mã nhưng Alice thì không

  – Có một Lý thuyết thông tin rất hay về khái niệm khả năng giữ bí mật, cụ thể là lượng thông tin bí mật mà Alice có thể gửi cho Bob mà Eve không thể giải mã được

  – Tôi sẽ để lại chi tiết cho bạn khám phá

KẺ NGHE TRỘM HẠ CẤP - DEGRADED EAVESDROPPER?

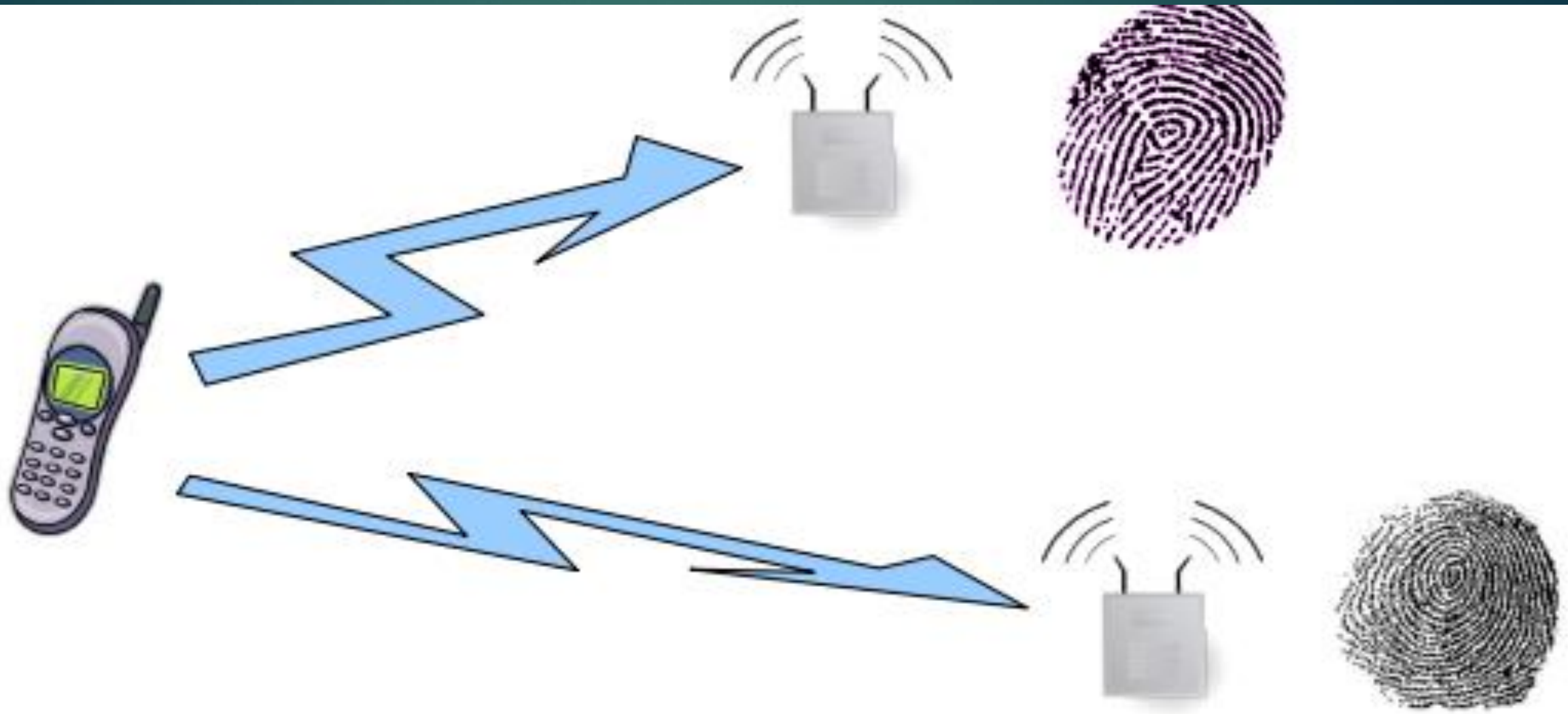
• Trong một tình huống thực tế, có hợp lý không khi cho rằng tín hiệu của kẻ nghe trộm bị suy giảm hơn tín hiệu của người nhận?

- *Chắc là không.*

• Chúng ta có thể làm gì khác để tạo ra quy mô có lợi cho kênh Alice-Bob?

SỰ ĐA DẠNG CỦA NGƯỜI NHẬN

Tín hiệu do máy phát phát ra trông "khác" với máy thu ở các vị trí khác nhau



ĐO LƯỜNG + PHẢN HỒI

- Thông tin trạng thái kênh (CSI):

  – CSI là thuật ngữ được sử dụng để mô tả các phép đo điều kiện của kênh

  – Nếu Alice biết CSI cho Bob và cho Eve, cô ấy có thể tìm thấy mã hóa thích hợp bằng cách sử dụng các phép đo

  – Nếu Alice và Bob tương tác lặp đi lặp lại, phép đo và phản hồi thực sự làm tăng khả năng bảo mật

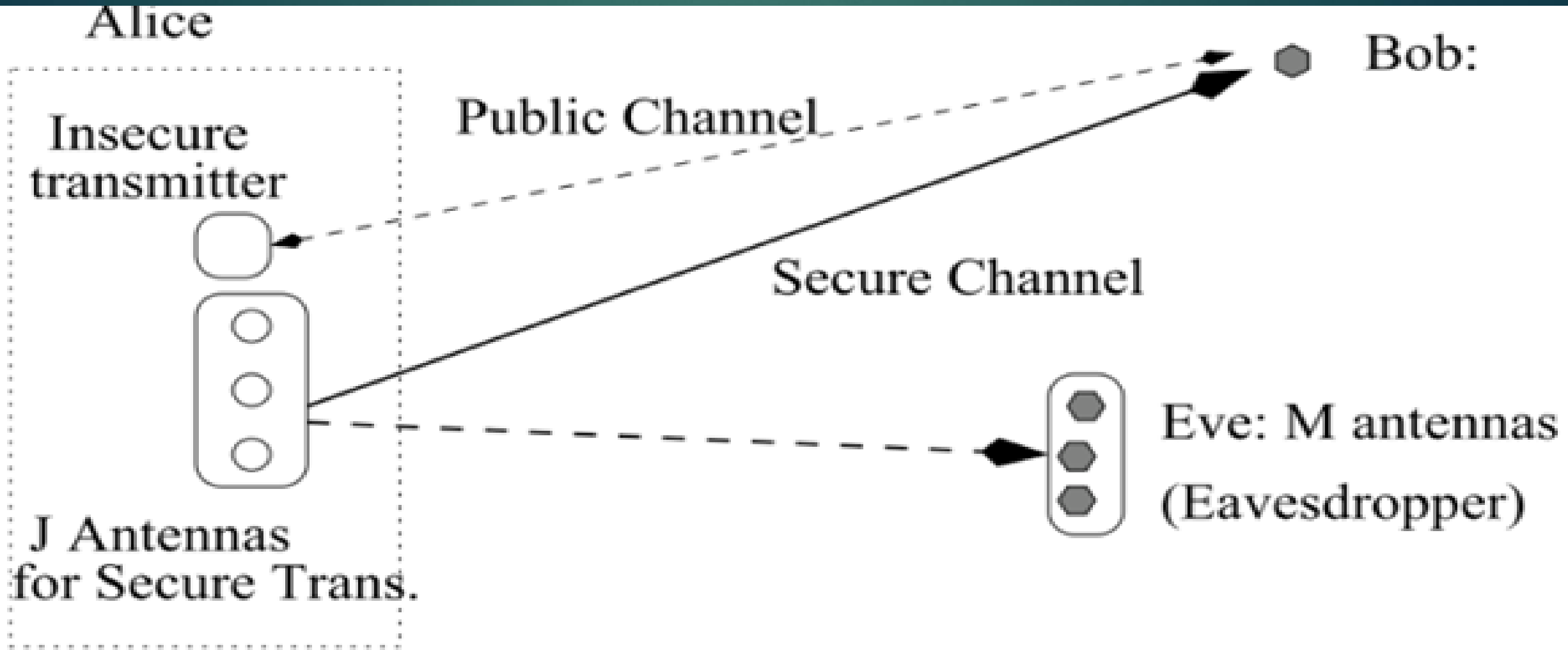
    • Điều này có thể cho phép dung lượng bảo mật *>0 ngay cả khi kênh của Eve ít nhiễu hơn kênh của Bob*

GÂY NHIỄU TỐT

- Nếu Alice có tính đa dạng ở dạng nhiều đài hoặc một số cộng tác viên:
  - Alice & bạn bè có thể sử dụng đòn tấn công gây nhiễu để ngăn Eve nghe lén
  - Miễn là chúng không làm kẹt Bob cùng một thời điểm
  - Ví dụ: nếu biết hình dạng triển khai, Alice có thể điều chỉnh công suất, cấu hình ăng-ten, v.v. để SINR của Bob cao nhưng SINR của Eve thấp

TRUYỀN MẢNG AN TOÀN

• Điều khiển ăng-ten có thể được sử dụng để truyền với xác suất bị chặn thấp



ỨNG DỤNG

- Xây dựng năng lực bảo mật:

  – Nếu hai thiết bị có thể giao tiếp với xác suất cao đảm bảo rằng những kẻ nghe trộm không thể nghe thấy chúng, bất cứ điều gì chúng nói đều là bí mật

  – Tin nhắn bí mật → các khóa!

  – Hiện nay có thể tạo khóa bí mật bằng cách sử dụng các thuộc tính vốn có của phương tiện không dây

ĐỌC THÊM

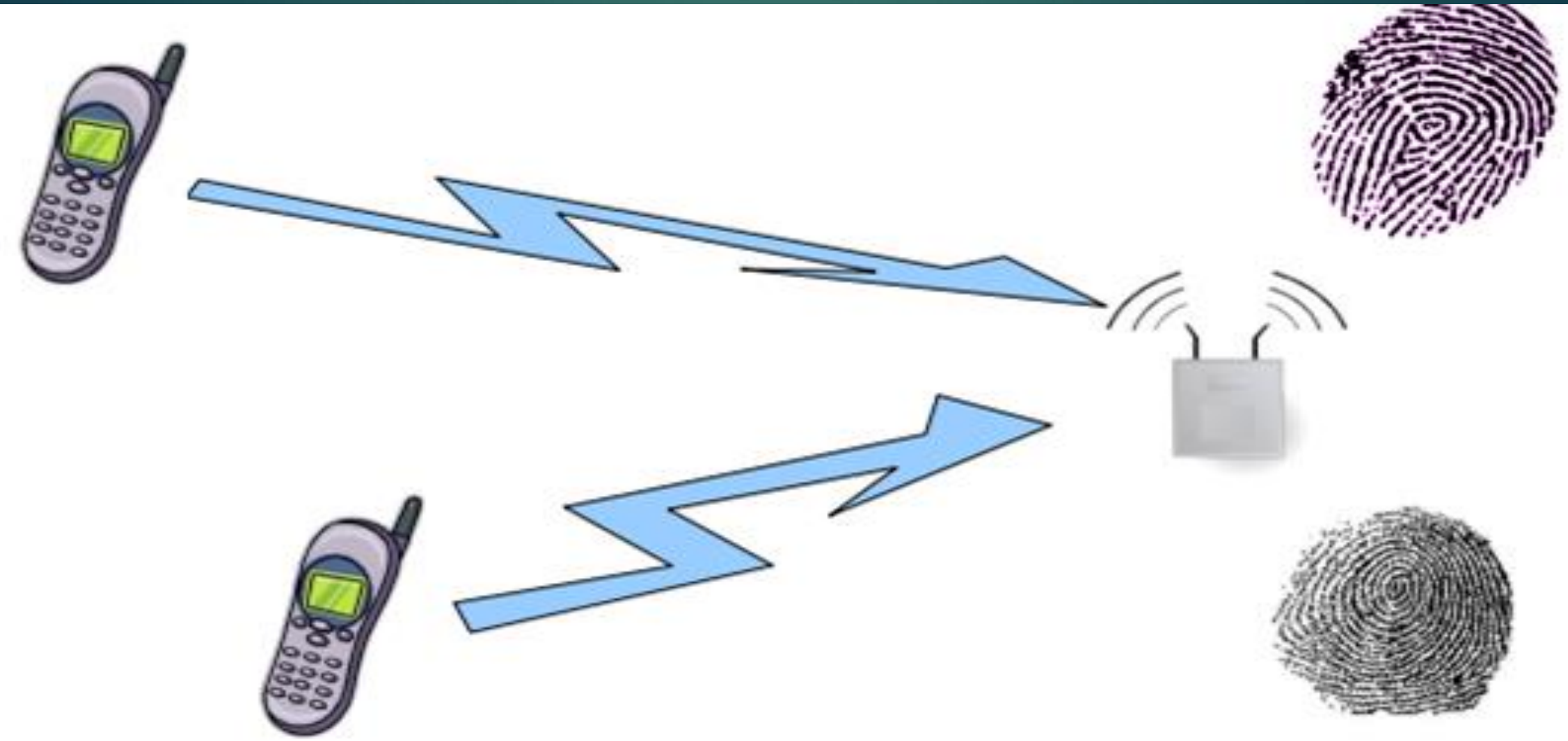
- Để có một bản tóm tắt thực sự tốt về khả năng bảo mật, hình thức hóa, tạo khóa bí mật và nhiều chi tiết tuyệt vời khác:
  - *"Bảo mật tầng vật lý - Physical layer security" của Bloch và Barros*
    - *Có sẵn dưới dạng sách điện tử thông qua thư viện CMU*

NHIỀU LỢI ÍCH HƠN CHO BUỔI TIỆC?

THUỘC TÍNH TẦNG VẬT LÝ CÓ THỂ GIÚP XÁC THỰC!

SỰ ĐA DẠNG CỦA NGƯỜI GỬI

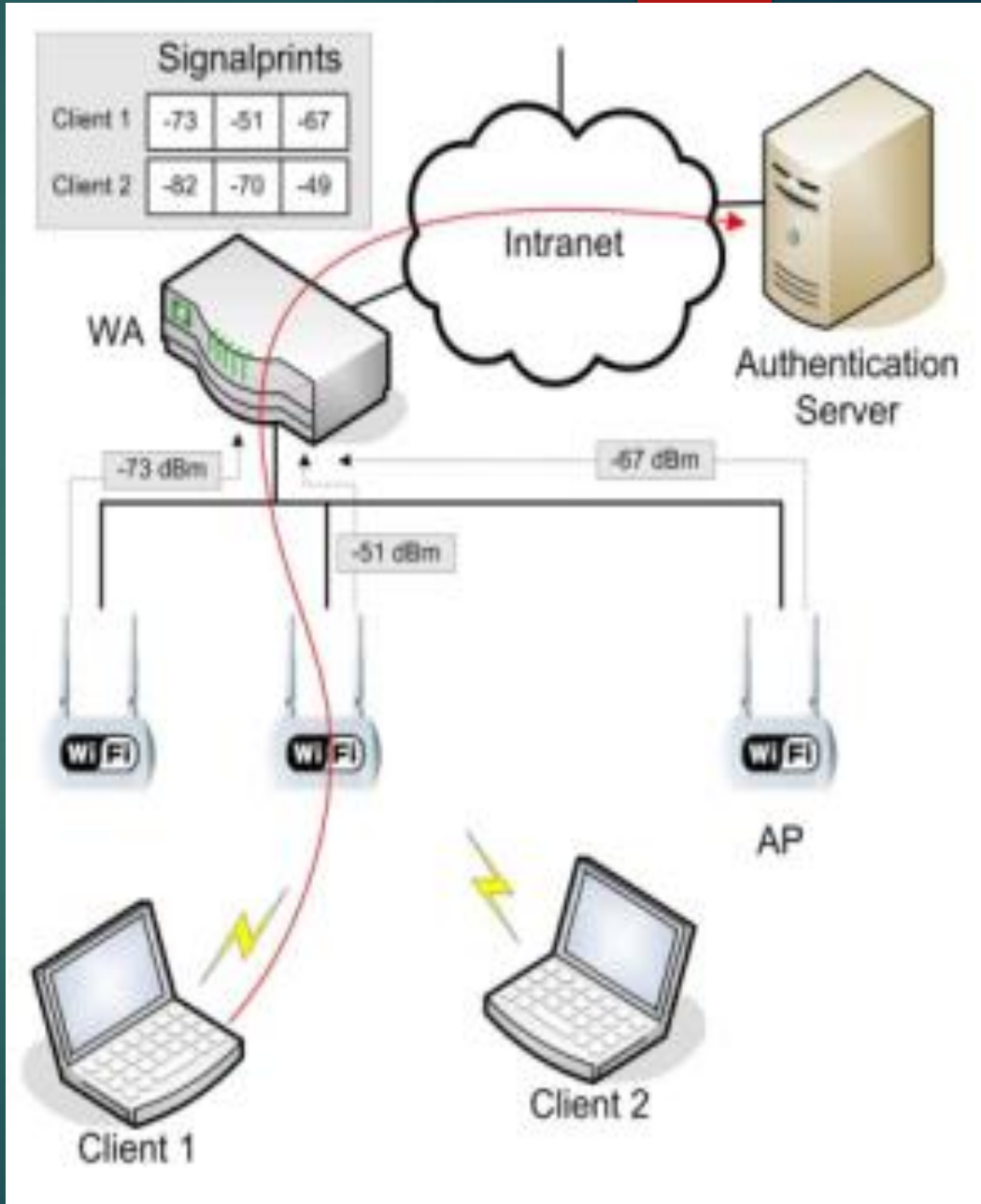
- Tín hiệu được thu bởi người nhận từ người gửi ở các vị trí riêng biệt trông "khác nhau"



- Trong một mạng WLAN có nhiều AP, mỗi AP sẽ thấy các đặc điểm khác nhau của các gói từ mỗi người gửi

  – Mỗi AP có thể đo các tính năng gói khác nhau, một số tính năng tương đối tĩnh trên các gói: ví dụ: cường độ tín hiệu nhận được

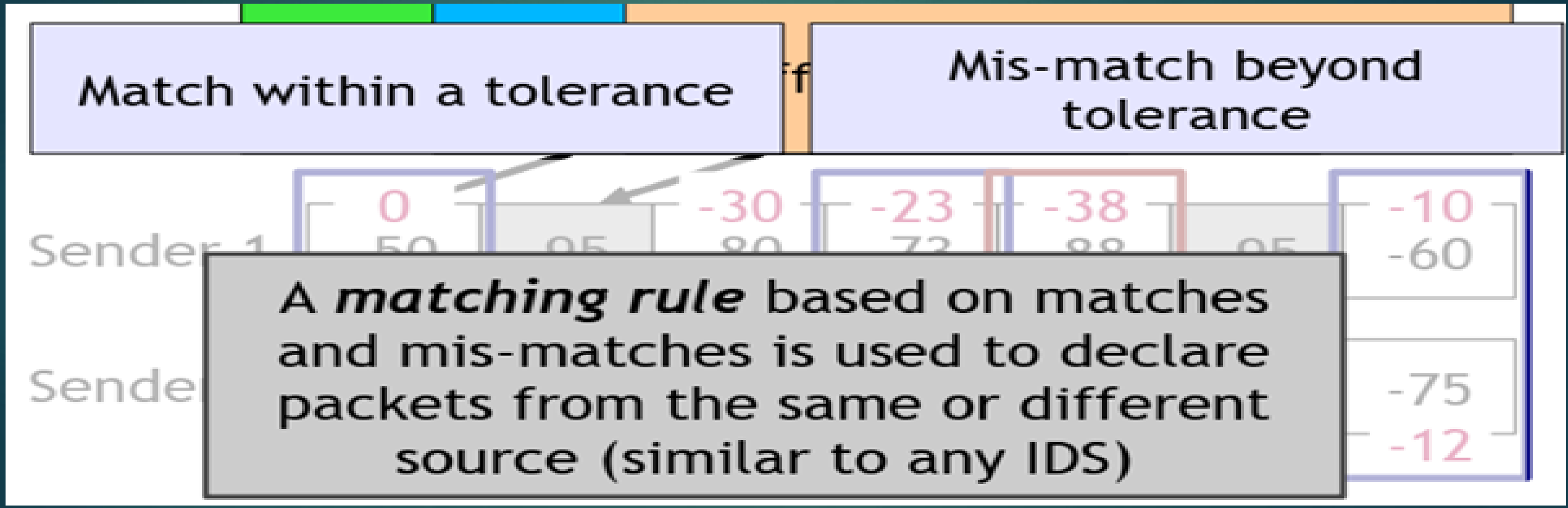
  – Máy chủ back-end có thể thu thập các phép đo và lưu giữ lịch sử các gói từ những người gửi khác nhau



XÁC MINH & ĐỐI SÁNH

• Yêu cầu thẩm định:

– Kiểm soát công suất truyền mạnh mẽ, dao động ngẫu nhiên và lỗi



Quy tắc so khớp dựa trên sự trùng khớp và không khớp được sử dụng để khai báo các gói từ cùng một nguồn hoặc khác nhau (tương tự như bất kỳ IDS nào)

THUỘC TÍNH IN TÍN HIỆU

- Khó giả mạo
  - *Nút giả mạo sẽ yêu cầu kiểm soát phương tiện*
  - *Kiểm soát công suất truyền tạo ra RSS thấp hơn ở mọi AP; phân tích khác biệt cho thấy kiểm soát quyền lực*
- Tương quan với vị trí thực tế
  - *Kẻ tấn công cần phải ở gần thiết bị mục tiêu*
- Các gói tuần tự có bản in tín hiệu tương tự
  - *Các giá trị RSSI có mối tương quan cao đối với người gửi và người nhận cố định*
    - Lưu ý: không tương quan cao với khoảng cách, nhưng tương quan rất cao với các lần truyền tiếp theo

HẠN CHẾ

- In Dấu tín hiệu với bất kỳ luật đối sánh phù hợp nào không thể phân biệt giữa các thiết bị ở gần nhau

  – *Các cuộc tấn công giả mạo có thể xảy ra nếu dễ dàng đạt được sự gần gũi về mặt vật lý*

- Không thể phát hiện các cuộc tấn công tốc độ thấp

  – *Nhưng, các cuộc tấn công tốc độ thấp có tác dụng hạn chế*

- Kẻ tấn công nhiều ăng-ten có thể gian lận

- Không thể in các thiết bị có tính di động cao

TÓM TẮT

Can thiệp và nghe trộm là hai lỗ hổng cơ bản nhất nhưng ít được hiểu nhất của mạng không dây. Vẫn còn rất nhiều việc phải làm.

BÀI 6:

MỐI ĐE DỌA LỚP LIÊN KẾT; BẢO MẬT WI-FI