BÀI #8 - BẢO MẬT PHÁT SÓNG QUẢNG BÁ & QUẢN LÝ KHÓA

- XÁC THỰC PHÁT SÓNG QUẢNG BÁ
- QUẢN LÝ KHÓA NHÓM

TS. HOÀNG SỸ TƯƠNG

TRUYỀN THÔNG QUẢNG BÁ

- Mạng không dây có thể tận dụng thuộc tính **"lợi thế phát sóng quảng bá"** để gửi tin nhắn đến nhiều người nhận cùng một lúc
  - Trong “mô hình mạng ngôi sao” (như mạng WiFi), O(1) truyền đến tất cả N người nhận
  - Nói chung, O(N/d) truyền quảng bá tới N người nhận với mật độ d, sử dụng phương pháp chuyển tiếp

BẢO MẬT PHÁT SÓNG QUẢNG BÁ

Để tận dụng “lợi thế phát sóng quảng bá”

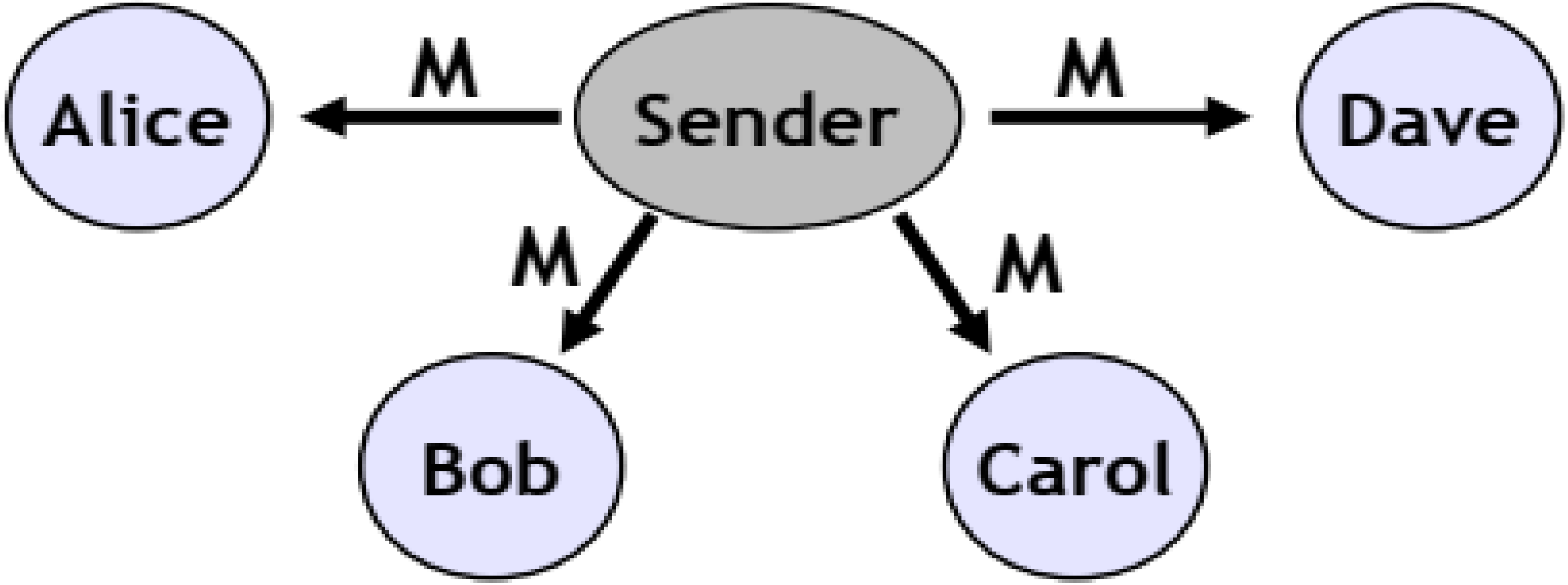
- Tất cả người nhận cần có khả năng xác thực người gửi/tin nhắn từ một lần truyền

- Tất cả người nhận cần có khả năng giải mã tin nhắn từ một lần truyền

- Ngoài ra, các cơ chế xác thực, giải mã và quản lý khóa cần hiệu quả

BẢO MẬT PHÁT SÓNG QUẢNG BÁ

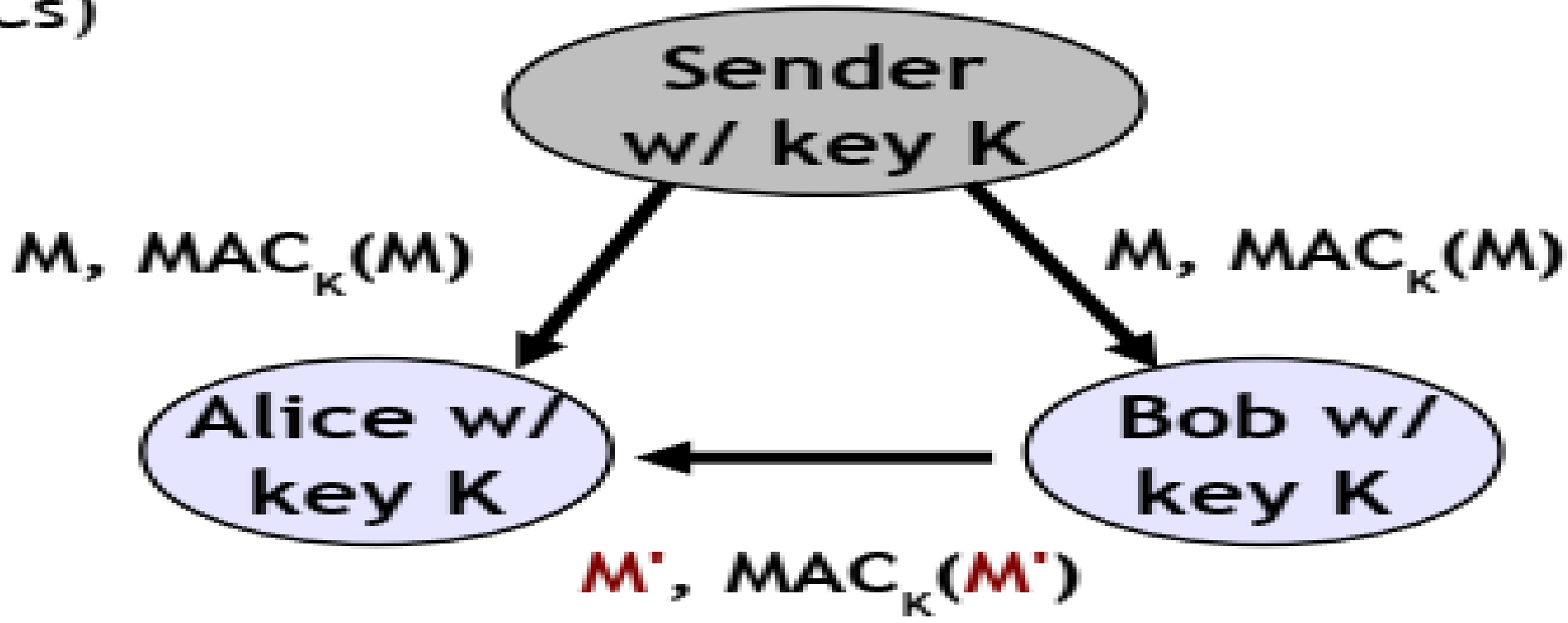
- Người gửi muốn phát một tin nhắn trong mạng không dây
- Để bảo vệ chống lại việc tiêm gói (Injection) và các mối đe dọa khác, cần xác minh nguồn gốc dữ liệu



CÁC CƠ CHẾ XÁC THỰC PHÁT SÓNG QUẢNG BÁ

- Mật mã khóa đối xứng và mã xác thực tin nhắn (MAC)
- Một số hình thức bất đối xứng là bắt buộc

1. Symmetric key crypto and message auth codes (MACs)



Some form of asymmetry is required

CÁC CƠ CHẾ XÁC THỰC PHÁT SÓNG QUẢNG BÁ

2. Chữ ký số (khóa công khai)

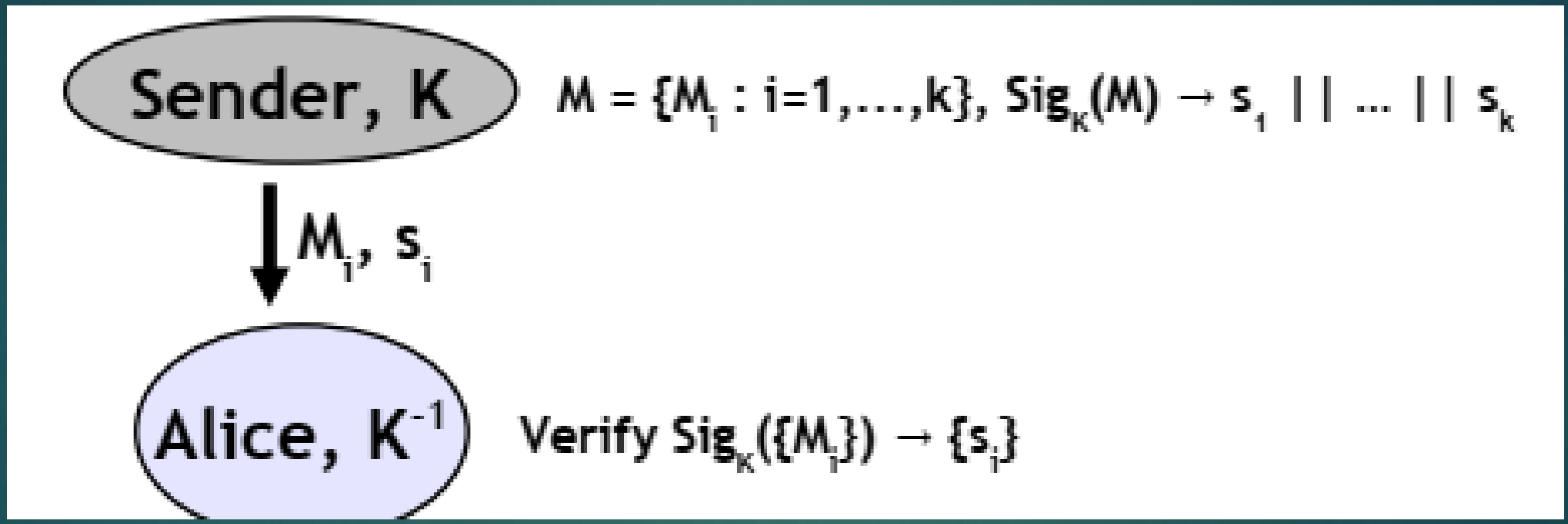
- Người gửi sử dụng khóa riêng để ký tin nhắn, tất cả người nhận xác minh bằng khóa chung tương ứng

- Ex: RSA 1024 bit signatures
  - High generation cost (~10 milliseconds)
  - High verification cost (~1 millisecond)
  - High communication cost (128 bytes/packet)
- Even more costly for low-end processors

CÁC CƠ CHẾ XÁC THỰC PHÁT SÓNG QUẢNG BÁ

3. Chữ ký khối gói

- Ký một tập hợp các gói, chữ ký phân vùng trên khối gói phân tán chi phí ký trên các khối dữ liệu lớn hơn



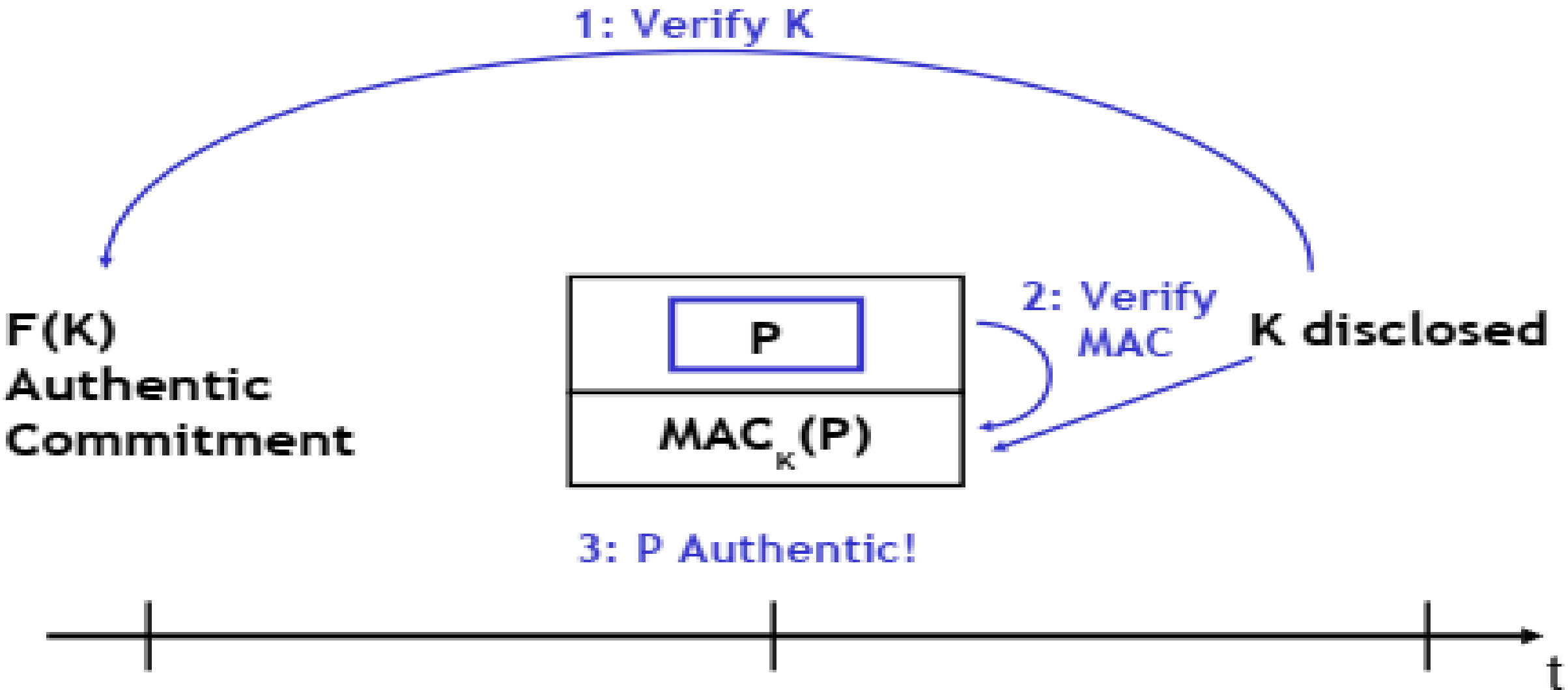
Hiệu quả hơn, nhưng mất 1 khối không xác minh dẫn đến không được xác minh

TESLA

- TESLA = Khả năng chịu mất luồng hiệu quả theo thời gian Xác thực
- Chỉ sử dụng mật mã đối xứng
- Bất đối xứng theo thời gian

  - Chỉ người gửi mới có thể tính toán MAC tại thời điểm t
  - Trì hoãn tiết lộ khóa để xác minh
  - Yêu cầu đồng bộ hóa thời gian lỏng lẻo

F: public one-way function

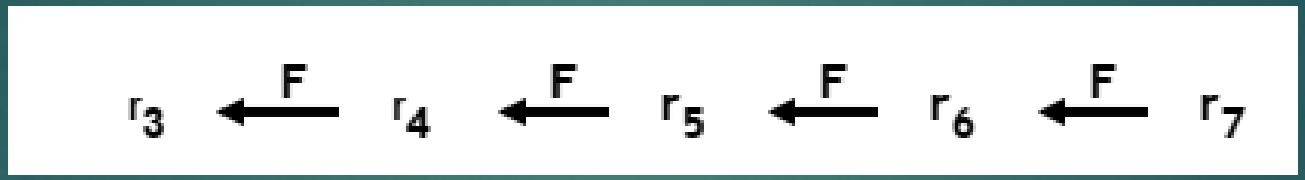


CHUỖI HÀM BĂM MỘT CHIỀU - ONE-WAY HASH CHAINS

- **Mật mã nguyên thủy linh hoạt**

  - Chọn r_N ngẫu nhiên và hàm một chiều công khai F

  - Với i=N-1,...,0 : $r_i = F(ri_{+1})$ thì công bố r_0



- **Thuộc tính**

  - Sử dụng đảo ngược thứ tự cấu tạo: r_1, r_2, r_N

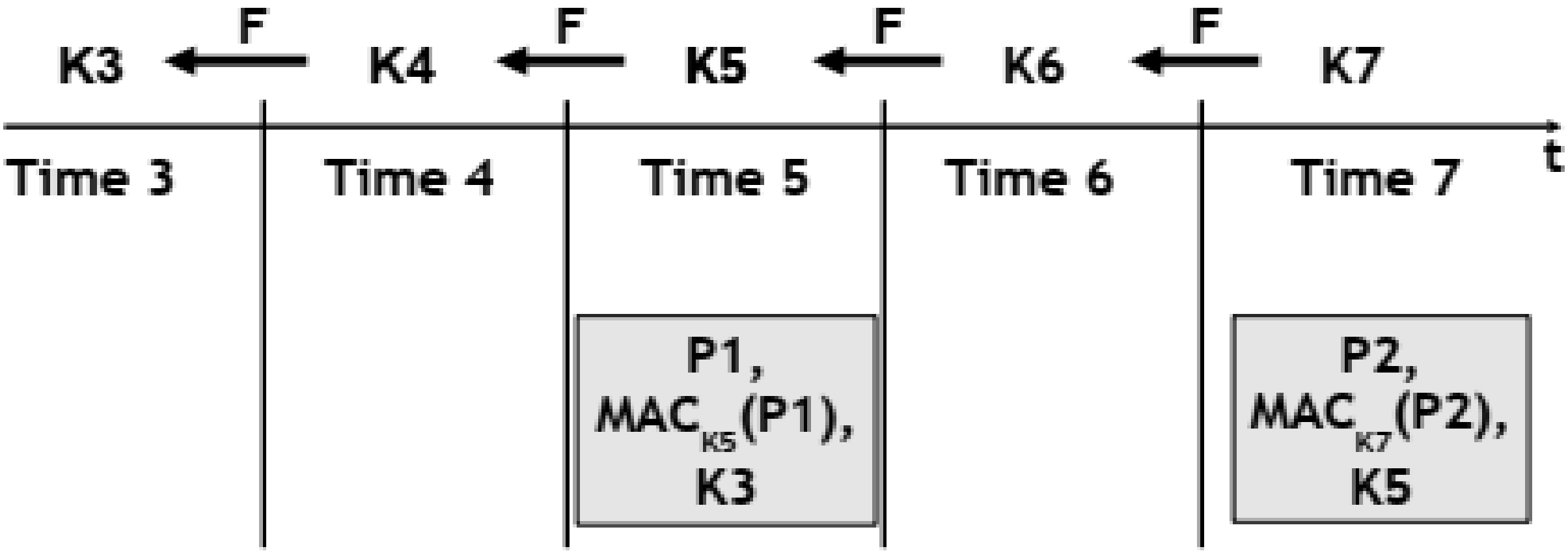
  - Không thể suy ra r_i từ r_j (j<i)

  - Xác thực hiệu quả r_i sử dụng r_j (j<i): $r_j = F^{i-j}(r_i)$

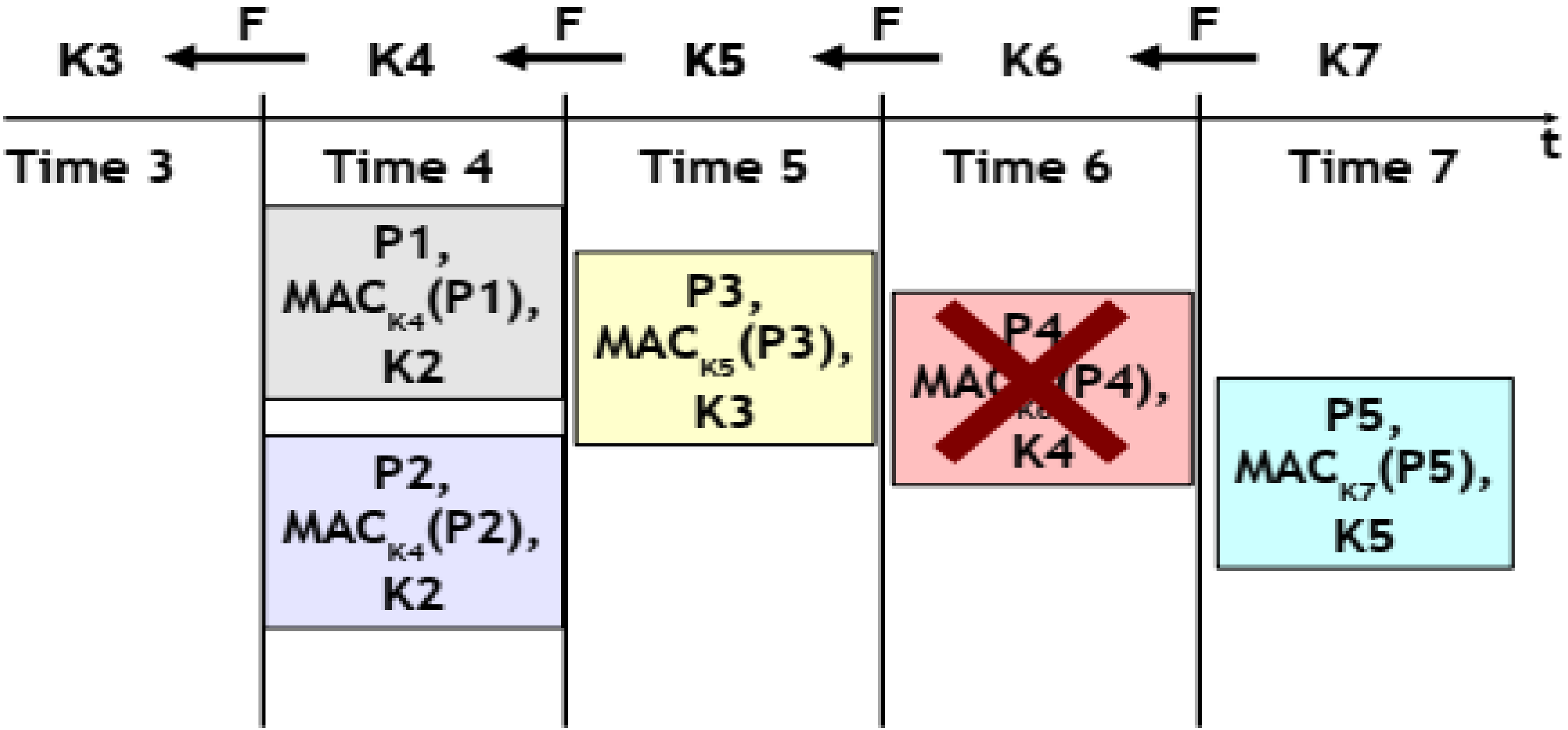
  - Độ bền với các giá trị còn thiếu

LỊCH TRÌNH TESLA

- Khóa bị hở khoảng 2 lần sau khi sử dụng
- Thiết lập máy thu: Authentic K3, lịch tiết lộ khóa



ĐỘ BỀN VỚI MẤT GÓI TIN - ROBUSTNESS TO PACKET LOSS



THUỘC TÍNH BẤT ĐỐI XỨNG

- Giá trị được tiết lộ của chuỗi khóa là khóa công khai, nó cho phép xác thực các thông báo tiếp theo (giả sử đồng bộ hóa thời gian)
- Người nhận chỉ có thể xác minh, không tự sinh khóa
- Với một thực thể đánh dấu thời gian đáng tin cậy, TESLA có thể cung cấp thuộc tính chữ ký số

TÓM TẮT TESLA

- Chi phí thấp
  - *– Giao tiếp (~ 20 byte)*
  - *– Tính toán (~ 1 tính toán MAC trên mỗi gói)*
- Khả năng chống mất gói hoàn hảo
- Không phụ thuộc vào số lượng người nhận
- Xác thực bị trì hoãn
- Các ứng dụng
  - *Truyền thông với độ tin cậy cao*
  - *Mạng cảm biến*
  - *Giao thức định tuyến an toàn*

CÁC NÚT RÀNG BUỘC CAO TRONG MẠNG CẢM BIẾN KHÔNG DÂY LÀ GÌ?

μTESLA CHO WSN

- Được đề xuất như một phần của kiến trúc SPINS
  - Giảm giao tiếp truyền thông so với TESLA, tiết lộ khóa trên mỗi chu kỳ thay vì trên mỗi gói
  - Bao gồm một số tối ưu hóa khác cho chi phí hoạt động tối thiểu, thực tế trong các thiết bị có tài nguyên hạn chế (severely-constrained devices)

SNEP CHO WSN

- SPINS cũng bao gồm Giao thức mã hóa mạng an toàn (SNEP) để cung cấp tính bảo mật, xác thực và làm mới dữ liệu.
  - SNEP giúp sinh khóa một cách hiệu quả
  - SNEP có cấu trúc gói bao gồm xác thực + mã hóa:
    - Dữ liệu được mã hóa bằng khóa chung + bộ đếm (để bảo mật ngữ nghĩa)
    - • MAC trên dữ liệu được mã hóa

$$A \rightarrow B: \quad \{D\}_{\langle K_{AB}, C_A \rangle}, \ \mathrm{MAC}\left(K'_{AB} C_A \,||\, \{D\}_{\langle K_{AB}, C_A \rangle}\right)$$

  - Tùy chọn nonce-exchange để tạo độ tươi cho khóa

TinySec

- Kiến trúc TinySec cung cấp một bộ bảo mật cho các mạng cảm biến không dây.
  - TinySec-Auth chỉ cung cấp xác thực
  - TinySec-AE cung cấp mã hóa xác thực

ĐỌC THÊM

- Xác thực quảng bá trong VANET
  - Studer và cộng sự, ESCAR 2008/JCN 2009.
  - -Raya và cộng sự, SASN 2005.
    - Các bài báo khác @ http://lca.epfl.ch/projects/ivc/
- ... trong WSN
    - Ren và cộng sự, WASA 2006.
- • Xác thực phát sóng quảng bá DoS-resilient
    - Gunter và cộng sự, NDSS 2004.
    - Karlof và cộng sự, NDSS 2004.

NGOÀI CÁC TÍNH NĂNG BẢO MẬT VÀ HIỆU SUẤT CỦA CÁC GIAO THỨC BẢO MẬT, VẤN ĐỀ QUẢN LÝ KHÓA THÌ SAO?

QUẢN LÝ KHÓA

- Làm cách nào để thêm một thành viên vào nhóm mà không cấp cho họ quyền truy cập vào các hoạt động trước đây của nhóm?
- Làm cách nào để xóa/thu hồi một thành viên khỏi nhóm mà không cấp cho họ quyền truy cập vào các hoạt động nhóm trong tương lai?
- Làm cách nào để cung cấp thông tin đăng nhập mới cho các thành viên nhóm?

QUẢN LÝ KHÓA CỦA NHÓM

- Việc thành lập, tham gia và rời nhóm có thể được kiểm soát hoàn toàn bằng cách phân phối và thu hồi khóa
  - Khóa mã hóa phiên (SEK) được cấp cho tất cả các thành viên trong nhóm (được sử dụng để phân phối/thu thập dữ liệu)
  - Các khóa mã hóa khóa (KEK) được cấp cho các thành viên trong nhóm được sử dụng để cập nhật SEK định kỳ
    - Thu hồi = không nhận được bản cập nhật SEK
    - •KEK_S cũng có thể cần được cập nhật
  - Việc cập nhật khóa phải rất hiệu quả để có thể thực hiện thường xuyên giúp giảm thiểu tác động của hành vi sai trái

THÁCH THỨC

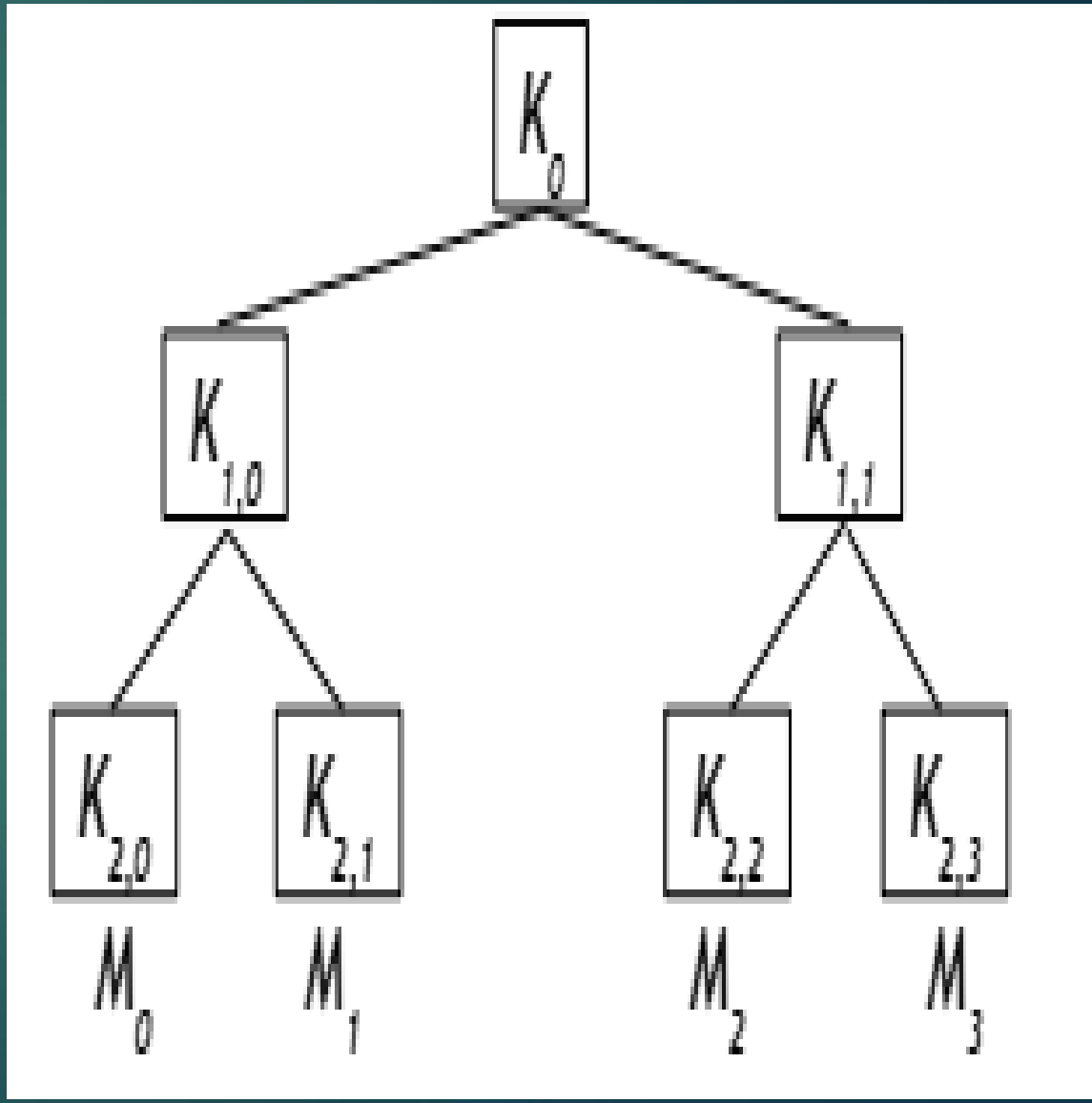
- Các mô hình tấn công đơn giản như nghe trộm, chèn/giả mạo thông điệp, giả mạo, v.v. có thể ảnh hưởng đến toàn bộ kiến trúc bảo mật
- Các giải pháp Unicast có thể không khả thi/không thực tế
- Mạng và dịch vụ là động và cần phải mở rộng quy mô
- Nhiều loại chi phí quản lý khác nhau
- Mối quan hệ tin tưởng ban đầu

QUY MÔ & TÍNH LINH ĐỘNG

- Tùy thuộc vào tình huống, quy mô nhóm có thể là 10, 100, 1000, 1000000, ...
- Tư cách thành viên nhóm và đăng ký dịch vụ có thể linh hoạt
  - *Có thể thay đổi theo thứ tự giây, phút, ngày, tháng,...*
  - *Tham gia và rời đi là ngẫu nhiên*
- Rất có thể, không có phương pháp "một kích thước phù hợp với tất cả"

PHÂN CẤP KHÓA LOGIC - LOGICAL KEY HIERARCHY

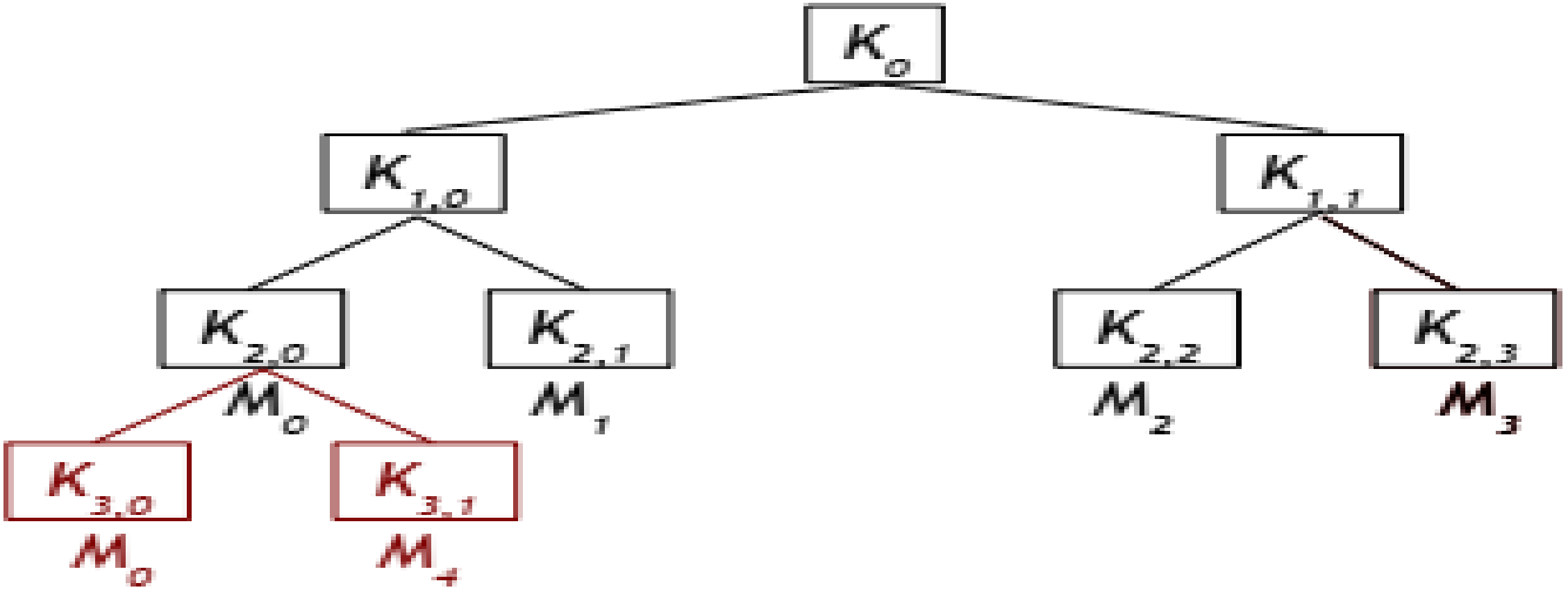
- LKH sắp xếp các thành viên trong nhóm trên cây m-ary
  - Lá cây tương ứng với thành viên có KEK riêng
  - Các nút cây bên trong đại diện cho các KEK của nhóm
  - Gốc cây đại diện cho SEK
  - Mỗi thành viên nhận được SEK và KEK dọc theo cây con trên tuyến



LHK BỔ SUNG

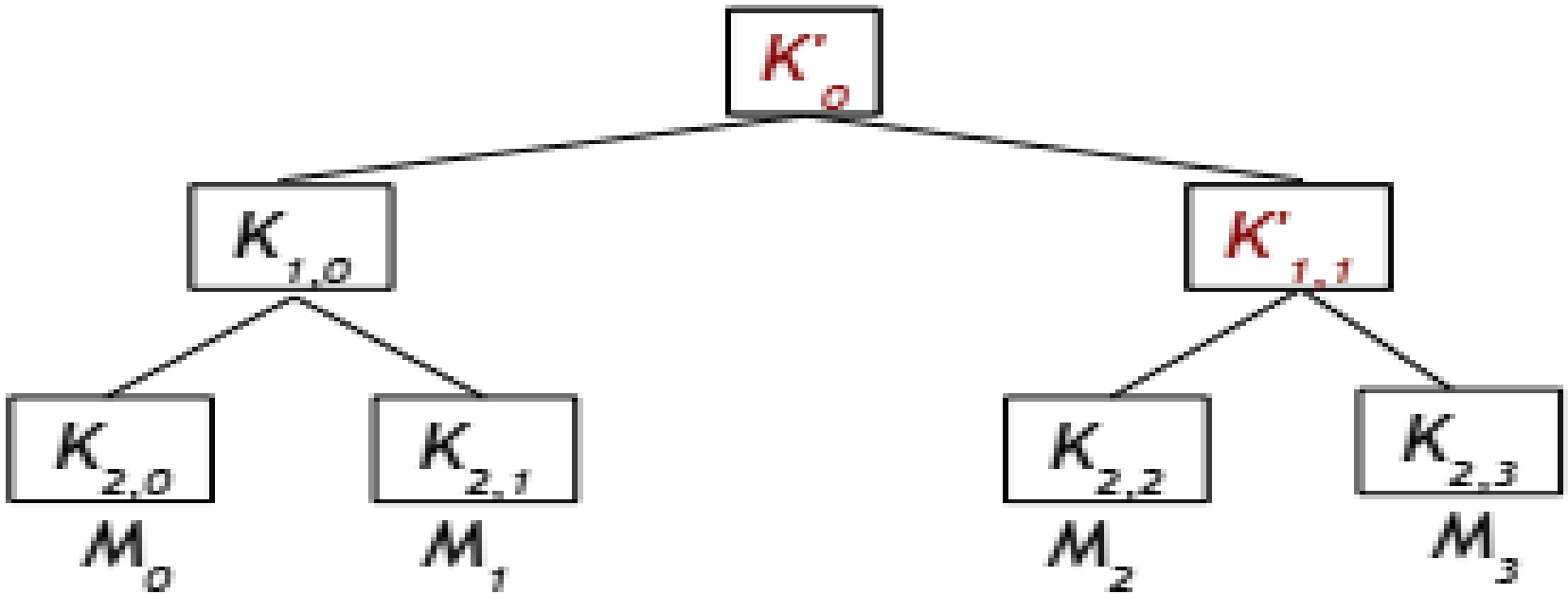
• Nếu M_4 muốn tham gia vào một nhóm và cây đã đầy

- Bắt đầu một cấp độ khác của cây



LOẠI BỎ LHK

- Nếu M muốn rời nhóm thì cập nhật SEK/KEKs
  - $\{K'_0, K'_{1,1}\}_{K_{2,2}}$
  - $\{K'_0\}_{K_{1,0}}$



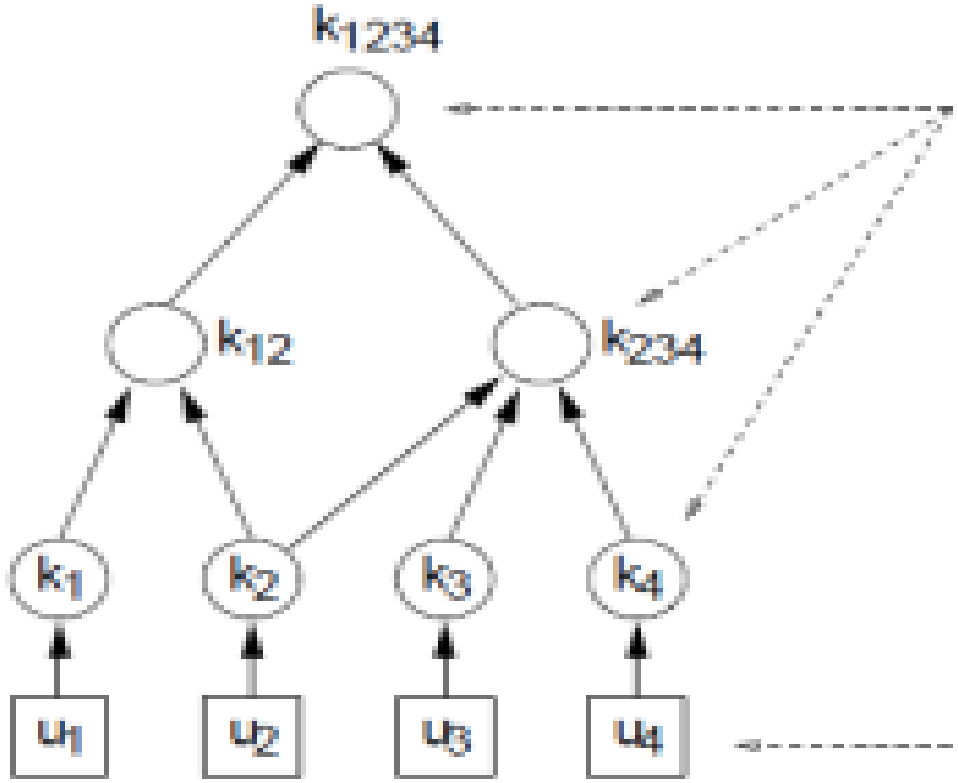
CHI PHÍ LKH - LKH OVERHEAD

- **Lưu trữ:**
  - Cơ quan nắm giữ tổng số O(N) khóa
  - Mỗi thành viên nắm giữ 1 SEK + O($\log_m$(N)) KEKs
- **Truyền thông:**
  - Yêu cầu phát sóng flood quảng bá cho mọi thông báo cập nhật, thông báo O($\log_m$ (N))/removal
    - *Lưu ý: mỗi tin nhắn có thể yêu cầu nhiều lần truyền...*
- **Tính toán:**
  - Hoạt động mã hóa/giải mã đối xứng

BIỂU ĐỒ KHÓA TỔNG QUÁT

Biểu đồ khóa khái quát hóa các cây chính để liên lạc nhóm an toàn

- Đồ thị tổng quát hóa LKH cho phép người dùng thuộc các nhóm tùy ý thay vì sử dụng cấu trúc cây



k-nodes

u-nodes

$$U = \{u_1, u_2, u_3, u_4\}$$
$$K = \{k_1, k_2, k_3, k_4, k_{12}, k_{234}, k_{1234}\}$$
$$R = \{\ (u_1, k_1),\ (u_1, k_{12}),\ (u_1, k_{1234}),$$
$$(u_2, k_2),\ (u_2, k_{12}),\ (u_2, k_{234}),\ (u_2, k_{1234}),$$
$$(u_3, k_3),\ (u_3, k_{234}),\ (u_3, k_{1234}),$$
$$(u_4, k_4),\ (u_4, k_{234}),\ (u_4, k_{1234})\ \}$$

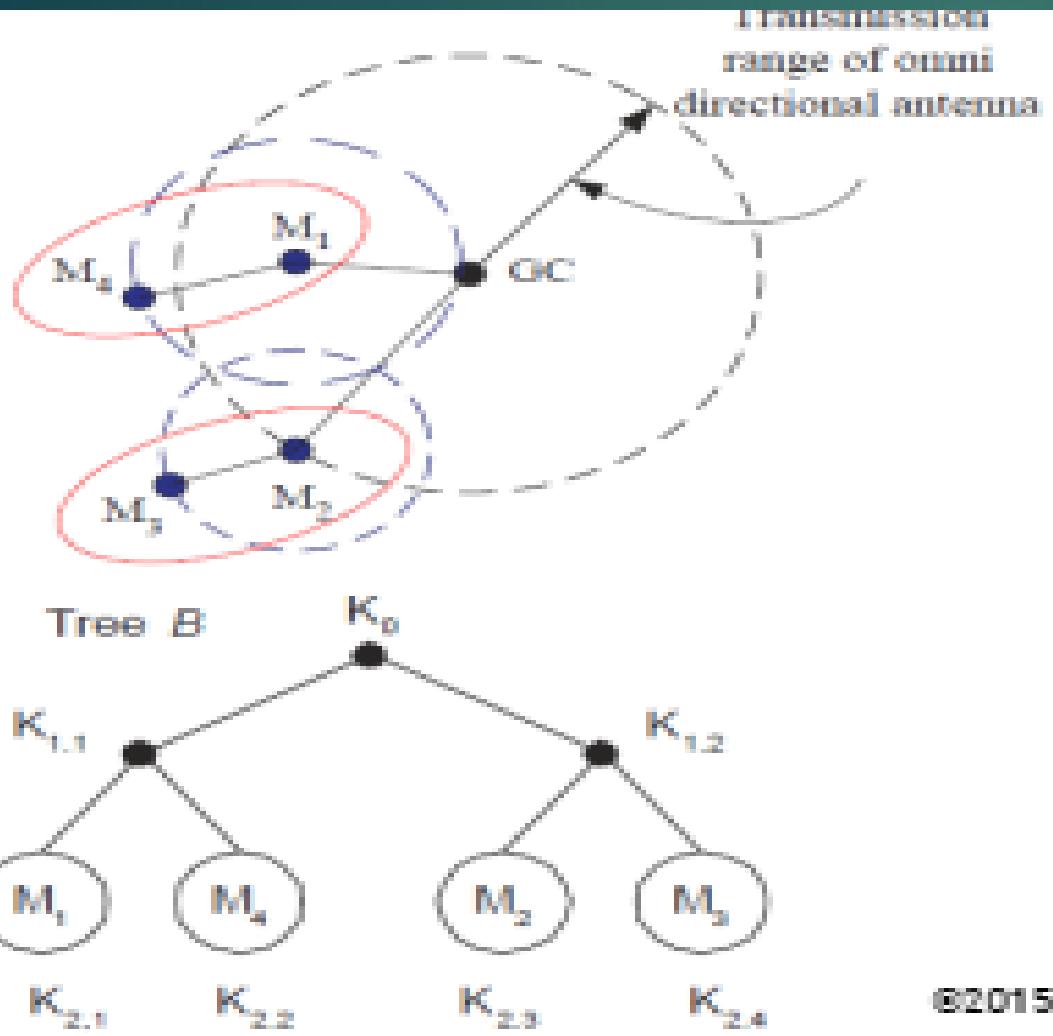
LÀM CÁCH NÀO ĐỂ CÁC QUY TRÌNH CẬP NHẬT NÀY CHUYỂN DỊCH SANG MIỀN KHÔNG DÂY?

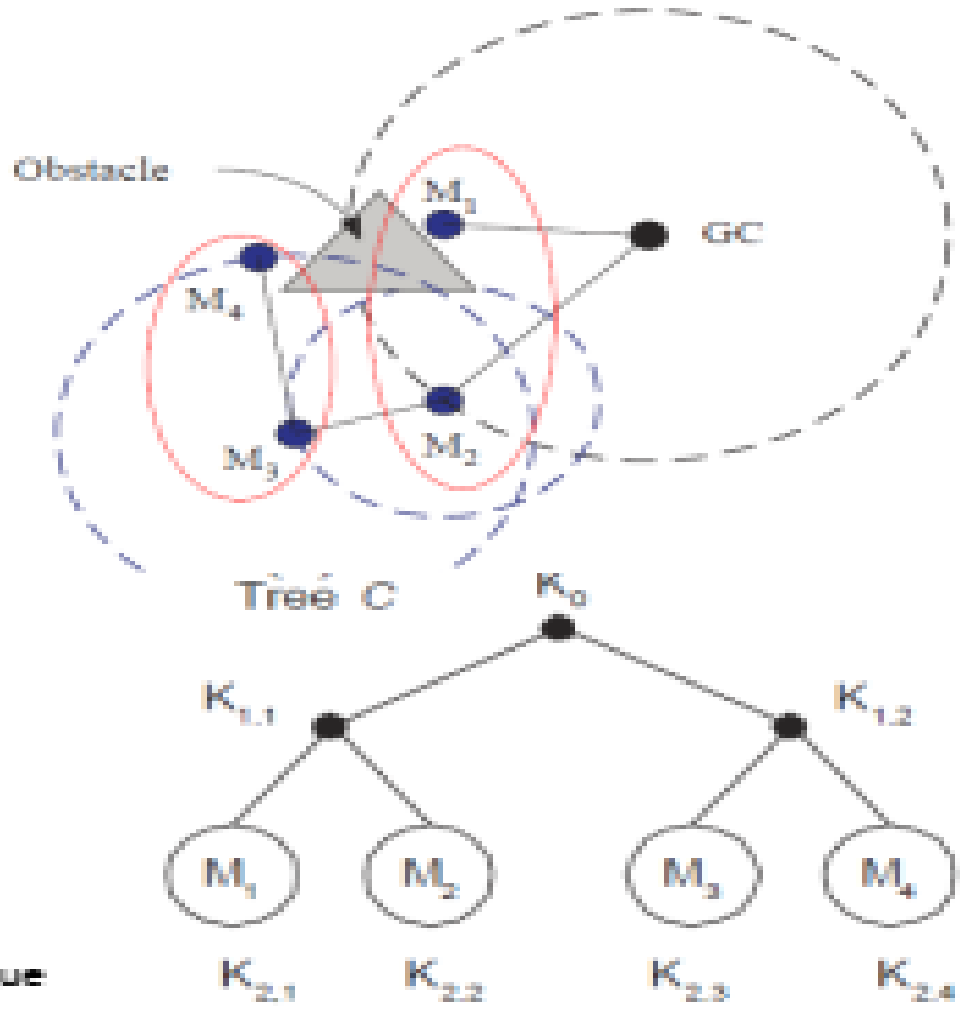
SỐ LIỆU

- Các kỹ thuật trước đây được mô tả tập trung vào một số thông báo cập nhật để quảng bá
  - Còn cấu trúc liên kết vật lý của mạng thì sao?
  - Chuyển tiếp tin nhắn qua nhiều liên kết không dây?
  - Tiêu hao năng lượng của các liên kết dài/mất kết nối?
  - Lợi thế phát sóng quảng bá?

CÂY KHÓA TIẾT KIỆM NĂNG LƯỢNG

• Các bản cập nhật quan trọng trong các mạng không dây lớn (WSN, MANET, v.v.) phải tiết kiệm năng lượng





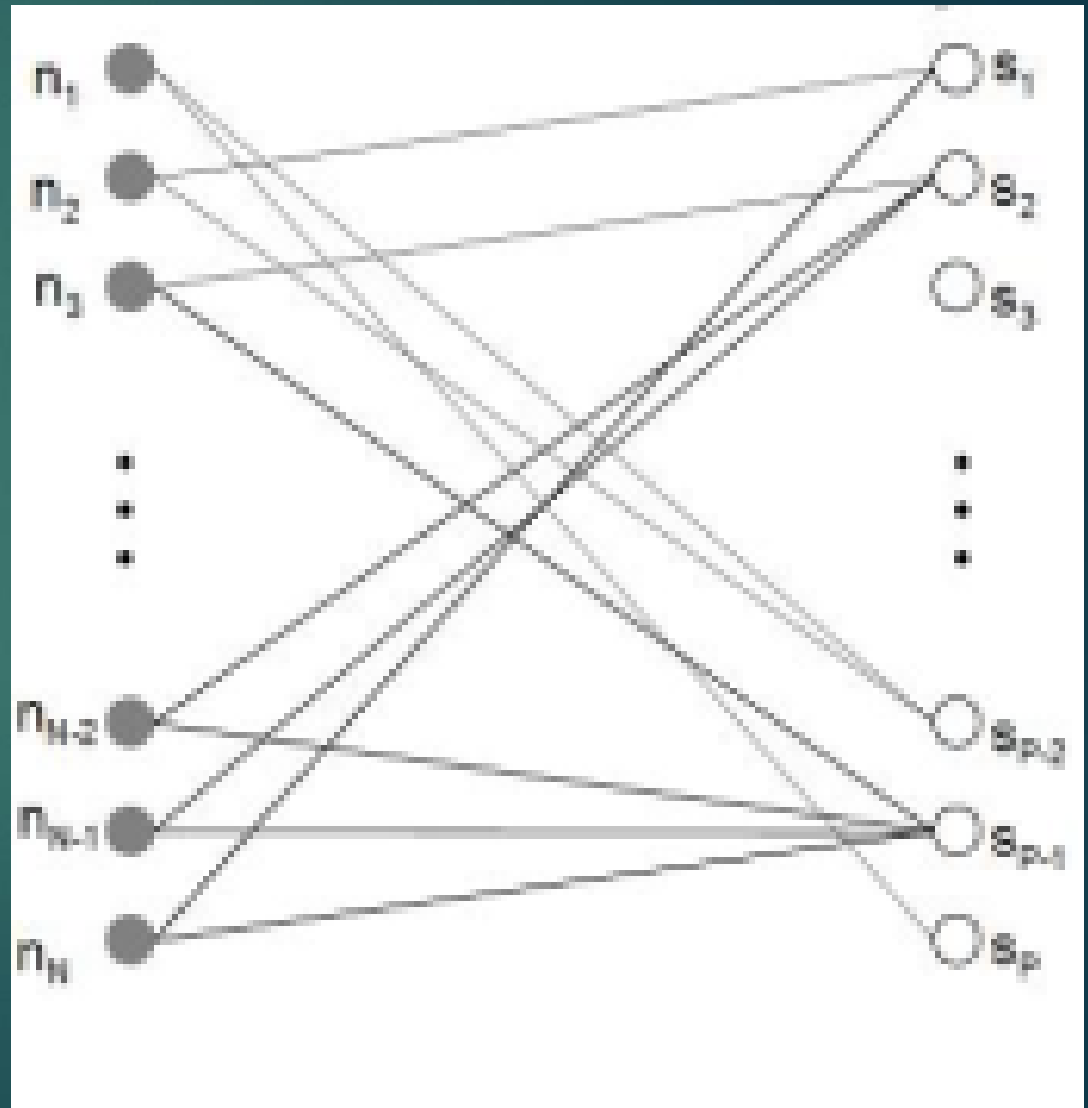
NHƯNG, TRONG TẤT CẢ CÁC CÁCH TIẾP CẬN NÀY, CÓ MỘT NHƯỢC ĐIỂM...

THỎA THUẬN KHÓA KHỞI TẠO

- Tất cả các phương pháp quản lý khóa này đều giả định rằng người dùng mới là người dùng hợp lệ có thể thiết lập KEK theo cặp với máy chủ
  - Khóa xác thực người dùng hợp lệ
    Valid user → authentication → keys
  - Vì vậy, thỏa thuận khóa khởi tạo yêu cầu các khóa có sẵn hoặc khởi tạo ngoại tuyến an toàn
  - Các giao thức như Diffie-Hellman và nhiều biến thể của chúng có thể hữu ích, miễn là chúng phù hợp với bối cảnh
  - Sự tương tác giữa con người – hệ thống mạng không dây (Human-in-the-loop) cho phép các cách tiếp cận khác nhau.

THỎA THUẬN KHÓA TRONG WSN

- Trong các hệ thống thách thức – challenged systems (WSN), thỏa thuận khóa thường rất tốn kém
- **Tùy chọn:** cơ quan chỉ định các khóa đối xứng - authority (KEK, v.v.) trước khi triển khai, các nút chia sẻ SEK/KEKs sau khi triển khai có thể khởi động các kết nối an toàn



BUỔI 9:

HÀNH VI SAI TRÁI (KHÔNG TUÂN THỦ QUY TẮC) CỦA MAC;