BÀI #12 - BẢO MẬT CHUYỂN TIẾP

TS. HOÀNG SỸ TƯƠNG

- Các cuộc tấn công và phòng thủ trên mặt phẳng dữ liệu

ĐIỀU GÌ XẢY RA ĐỐI VỚI VẤN ĐỀ BẢO MẬT CHUYỂN TIẾP TRÊN MẶT PHẲNG DỮ LIỆU?

BẢO MẬT MẶT PHẲNG DỮ LIỆU

- Tiêm mã độc và sửa đổi các gói là các vấn đề về tính toàn vẹn của gói/dữ liệu, có thể được giải quyết bằng các kỹ thuật mã hóa
  - Mặc dù không được giải quyết hiệu quả... trong giây lát
- Chuyển tiếp sai chặng tiếp theo là một vấn đề về tuân thủ giao thức nhưng có thể được kiểm tra và báo cáo tương tự như tính toàn vẹn của gói/dữ liệu
- Việc rớt gói là một vấn đề về tuân thủ và tính khả dụng

TÍNH KHẢ DỤNG CỦA MẶT PHẲNG DỮ LIỆU

- Chỉ riêng các nguyên hàm mật mã không thể giải quyết các vấn đề về tính khả dụng ở mặt phẳng dữ liệu
  - Không thể cung cấp bất kỳ hình thức đảm bảo nào về việc phân phối dữ liệu qua các bộ định tuyến hoạt động sai
  - Nói chung, một mình tiền cryto không thể giải quyết vấn đề DoS
  - Tính khả dụng của mặt phẳng dữ liệu một phần là do hành vi tuân thủ của các nút định tuyến và một phần là do lỗi và lỗi không xác định

CÁC BIỆN PHÁP PHÂN PHỐI E2E

- Giả sử phân phối gói được đo từ đầu đến cuối bằng cách sử dụng chữ ký hoặc MAC
  - Mọi thông báo đều có chi phí xác thực gói, nhưng xác thực thông báo đã được mong muốn vì nhiều lý do khác
  - Rớt gói dẫn đến truyền lại end-to-end
  - Độ trễ cao nếu ACK cũng bị loại bỏ/sửa đổi
  - Sửa đổi gói buộc các bộ định tuyến mang các thông điệp không có thật đến tận nút đích

HẠN CHẾ

- Giả sử phân phối gói được đo từ đầu đến cuối bằng cách sử dụng chữ ký hoặc MAC
  - Mọi thông báo đều có chi phí xác thực gói, nhưng xác thực thông báo được mong muốn vì nhiều lý do khác
  - Rớt gói dẫn đến truyền lại end-to-end
  - Với độ trễ cao nếu ACK cũng bị loại bỏ/sửa đổi
  - Sửa đổi gói buộc các bộ định tuyến mang các thông điệp không có thật đến tận nút đích

CÁC BIỆN PHÁP PHÂN PHỐI TRÊN MỖI NÚT

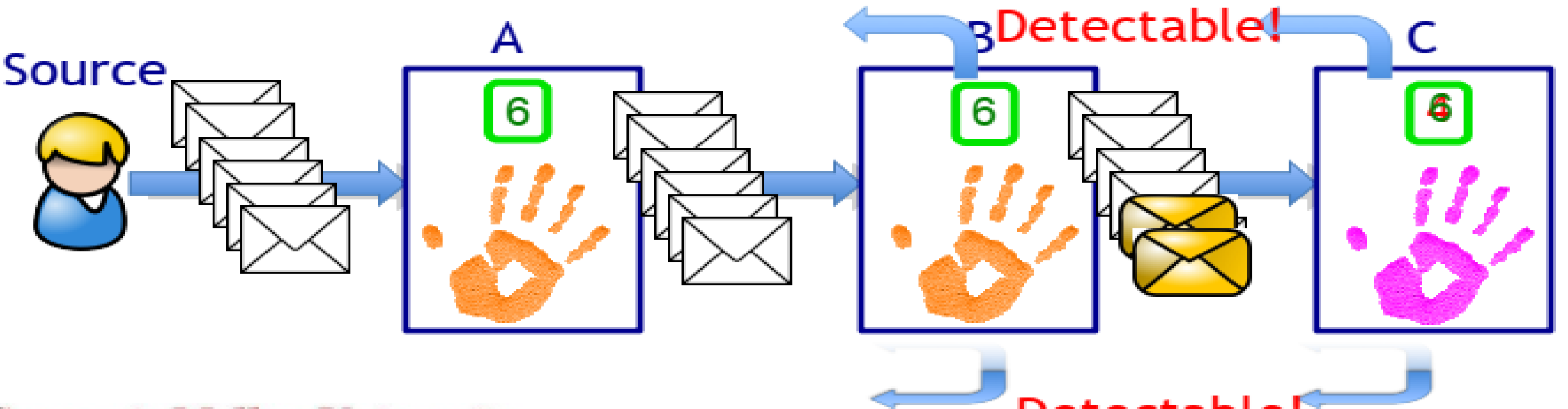
- Giả sử phân phối gói được đo trên mỗi nút
  - Xác minh mức độ chi tiết tốt hơn có thể yêu cầu nhiều chi phí hơn (ví dụ: MAC trên mỗi nút)
  - Các yêu cầu truyền lại nhanh hơn đưa ra bởi các bộ định tuyến trung gian, nhưng các bộ định tuyến độc hại cũng có thể yêu cầu truyền lại
  - Bộ định tuyến buộc phải tính toán và báo cáo nhiều hơn
  - Hàng xóm có thể được yêu cầu "nghe lỏm" hành vi

MAC NGẮN HẠN

- Thay vì phản ứng với hiệu suất kém, giám sát hiệu quả cao có thể cho phép giám sát liên tục với chi phí tối thiểu
- Một vài hiểu biết sâu sắc về thiết kế chính cho phép đạt được hiệu quả đáng kể bằng cách thực hiện những đánh đổi với khả năng phát hiện

BỘ ĐẾM SHORTMAC

- Xác thực gói bản địa hóa lỗi
  - Fault nội địa hóa theo dõi *số lượng gói tin, nội dung*
  - Xác thực W/pkt, đếm nội dung
  - Cách tiếp cận chỉ dùng bộ đếm mang lại trạng thái nhỏ và chi phí truyền thông thấp

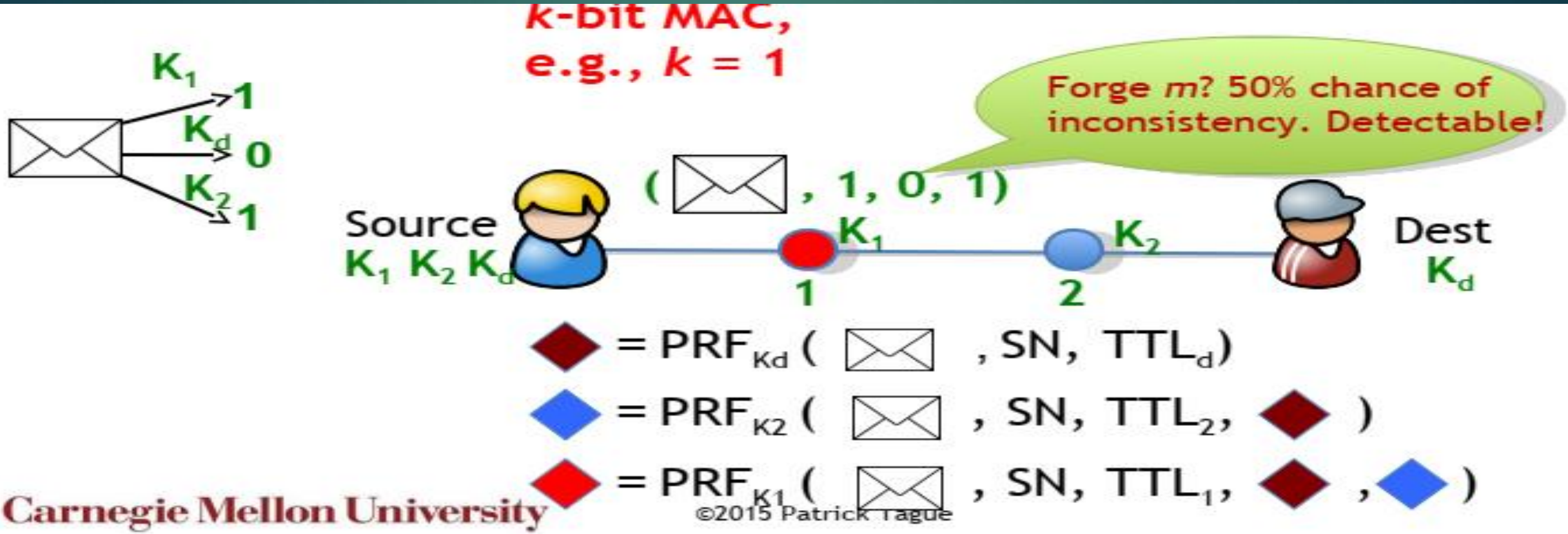


HẠN CHẾ TẤN CÔNG

- Hạn chế tấn công thay vì phát hiện
  - Phát hiện mọi hành vi sai trái? Tốn kém! Dễ bị lỗi!
  - Hấp thụ tấn công có tác động thấp: ngưỡng chịu đựng
  - Bẫy kẻ tấn công vào tình thế tiến thoái lưỡng nan
  - Kích hoạt các thuật toán xác suất với các giới hạn có thể chứng minh được

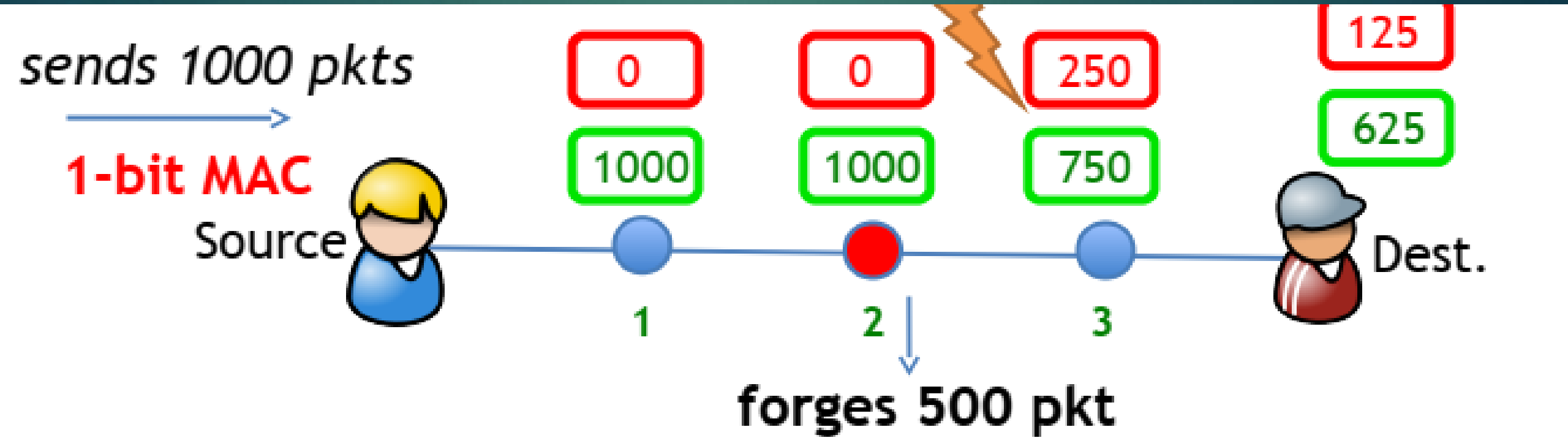
MAC NGẮN HẠN

- Đánh dấu gói ShortMAC
  - Hạn chế thay vì phát hiện các gói tin giả mạo
  - Nguồn đánh dấu mỗi gói bằng k bit (w/ keyed PRF)



PHÁT HIỆN SỬ DỤNG BỘ ĐẾM

- Bậc cao
  - Mỗi nút duy trì hai bộ đếm
  - Báo cáo bảo mật
  - Phát hiện dựa trên ngưỡng đối với các lỗi tự nhiên

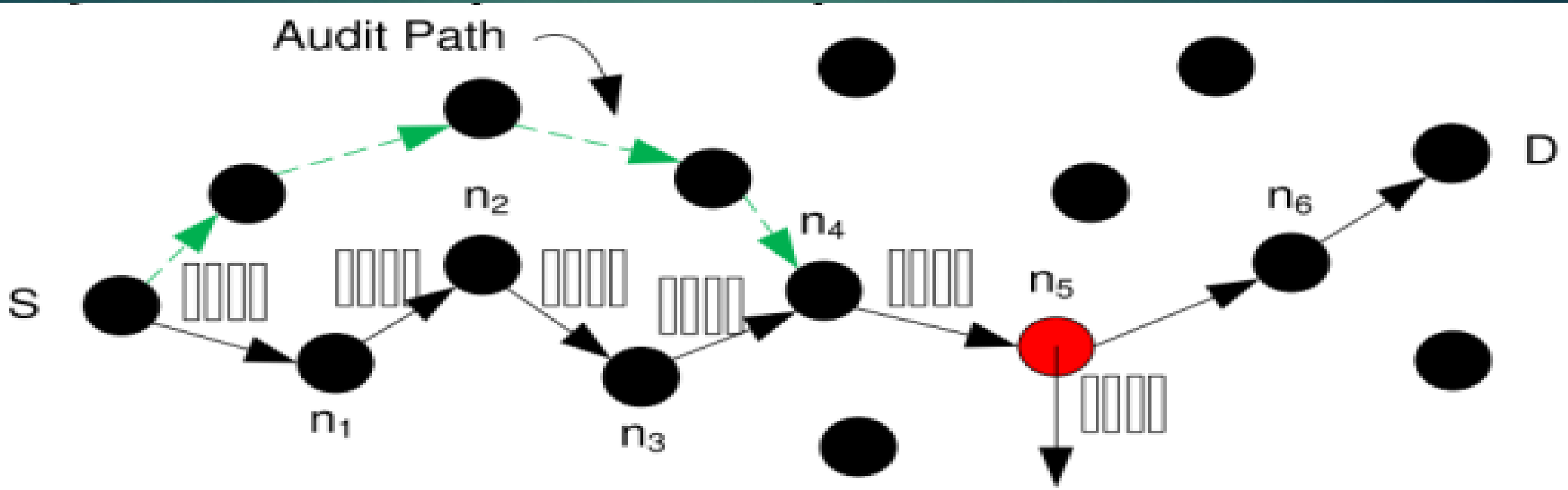


HẠN CHẾ

- ShortMAC được thiết kế cho Internet và có một số giả định ngầm hạn chế việc sử dụng nó trong các miền không dây
  - Phát hiện dựa trên giá trị ngưỡng cao hơn nhiều so với ngưỡng mất gói tự nhiên - trong mạng không dây, mức mất gói tự nhiên có thể cao
  - Nguồn phải chia sẻ khóa đối xứng theo cặp với mọi nút dọc theo đường dẫn

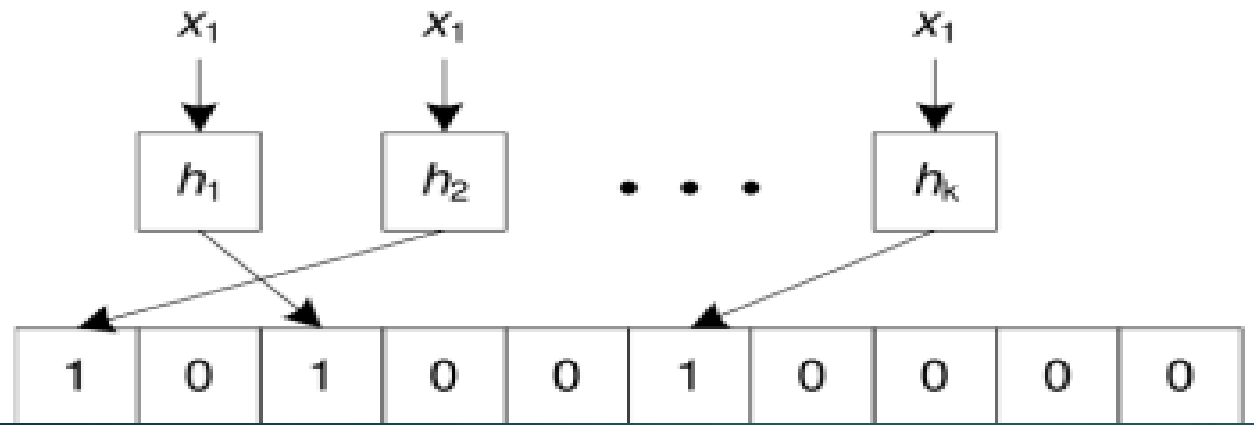
KIỂM TOÁN NGẪU NHIÊN TRONG MANET

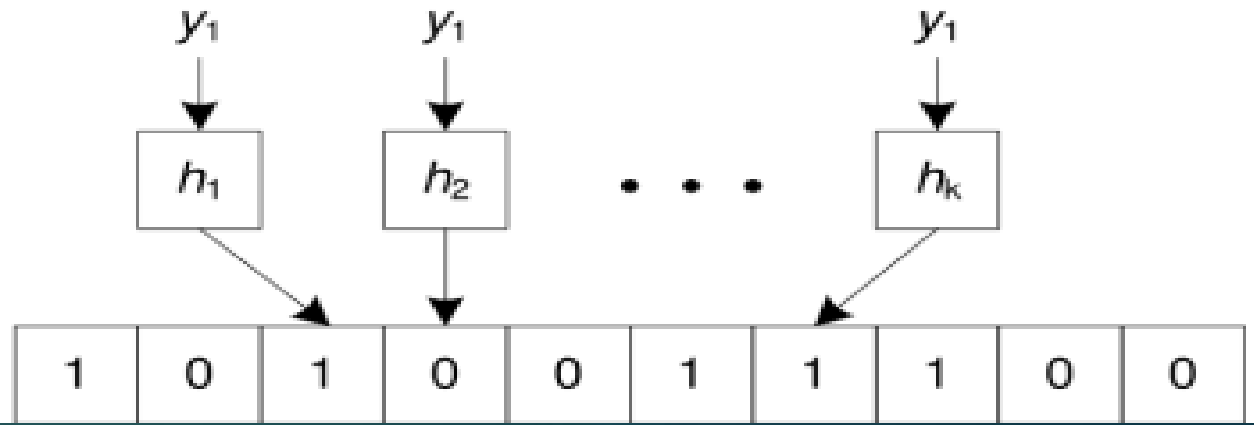
- Thay vì liên tục theo dõi hành vi chuyển tiếp của mọi nút, chỉ thực hiện kiểm tra đường dẫn khi hiệu suất đầu cuối xuống cấp
- Để kiểm tra một đường dẫn, nguồn xây dựng một đường dẫn kiểm tra rời rạc tới một nút trên đường dẫn và sử dụng đường dẫn này để thực hiện yêu cầu/phản hồi kiểm tra



KIỂM TOÁN HIỆU QUẢ

- Theo yêu cầu, một nút tạo bằng chứng về những gói mà nó đã xem
  - Báo cáo danh sách tất cả các gói tin không hiệu quả cần phải nén
  - Bộ lọc Bloom thực hiện nén danh sách gói bị mất dữ liệu:
    - *Một vectơ 2n-bit có thể lập chỉ mục bởi hàm băm n-bit*
    - *Mỗi trong số k hàm băm ánh xạ một gói thành một bit*
    - *k "0": không nhận được gói tin tương ứng*
    - *k "1": gói tương ứng có thể đã được nhận*





KIỂM TOÁN NGẪU NHIÊN

- REAct = Khả năng tính toán hiệu quả tài nguyên
  - Kiểm tra được kích hoạt bởi sự suy giảm hiệu suất
  - Nguồn S kiểm tra một nút N trên đường dẫn
  - Nếu bộ lọc Bloom được trả về từ N đủ gần với bộ lọc của S, thì kiểm tra một nút xuôi dòng
  - Khác, kiểm tra một nút ngược dòng của N
  - Cuối cùng, tìm kiếm sẽ hội tụ đến liên kết bị mất
  - Nguồn có thể thay đổi tuyến đường xung quanh liên kết bị mất để xác định nút nào đang hoạt động sai

HẠN CHẾ

- REAct giả định rằng kẻ tấn công có chiến lược tấn công tĩnh
  - Việc loại bỏ các gói khi không được kiểm tra sẽ hoạt động, nhưng nó sẽ cho phép phát hiện theo những cách khác
- REAct giả định rằng nhiều kẻ tấn công không thông đồng với nhau
  - Những kẻ tấn công thông đồng có thể trao đổi nhiệm vụ khi bị kiểm tra, do đó bỏ qua quá trình tìm kiếm

BUỔI 12.1:

THUYẾT TRÌNH SOW;

QUYỀN RIÊNG TƯ & ẨN DANH CỦA MẠNG

BUỔI 13:

NIỀM TIN VÀ UY TÍN