BÀI 15. AN NINH TẦNG VẬN TẢI CỦA MẠNG KHÔNG DÂY

TS. HOÀNG SỸ TƯƠNG

BÀI 15. AN NINH TẦNG VẬN TẢI CỦA MẠNG KHÔNG DÂY

- ✓ CÁC SỰ CỐ AN NINH Ở TẦNG VẬN TẢI MẠNG KHÔNG DÂY
- ✓ TẤN CÔNG ĐỊNH HƯỚNG TẦNG VẬN TẢI
- ✓ OMNET++/INET

TẦNG VẬN TẢI

- Tầng vận tải chịu trách nhiệm quản lý phân phối nội dung end to end
  - Truyền thông định hướng kết nối
  - Độ tin cậy
  - Kiểm soát lưu lượng
  - Tránh ùn tắc
  - Ghép kênh
  - Giao hàng theo yêu cầu

VẬN CHUYỂN MULTIHOP KHÔNG DÂY

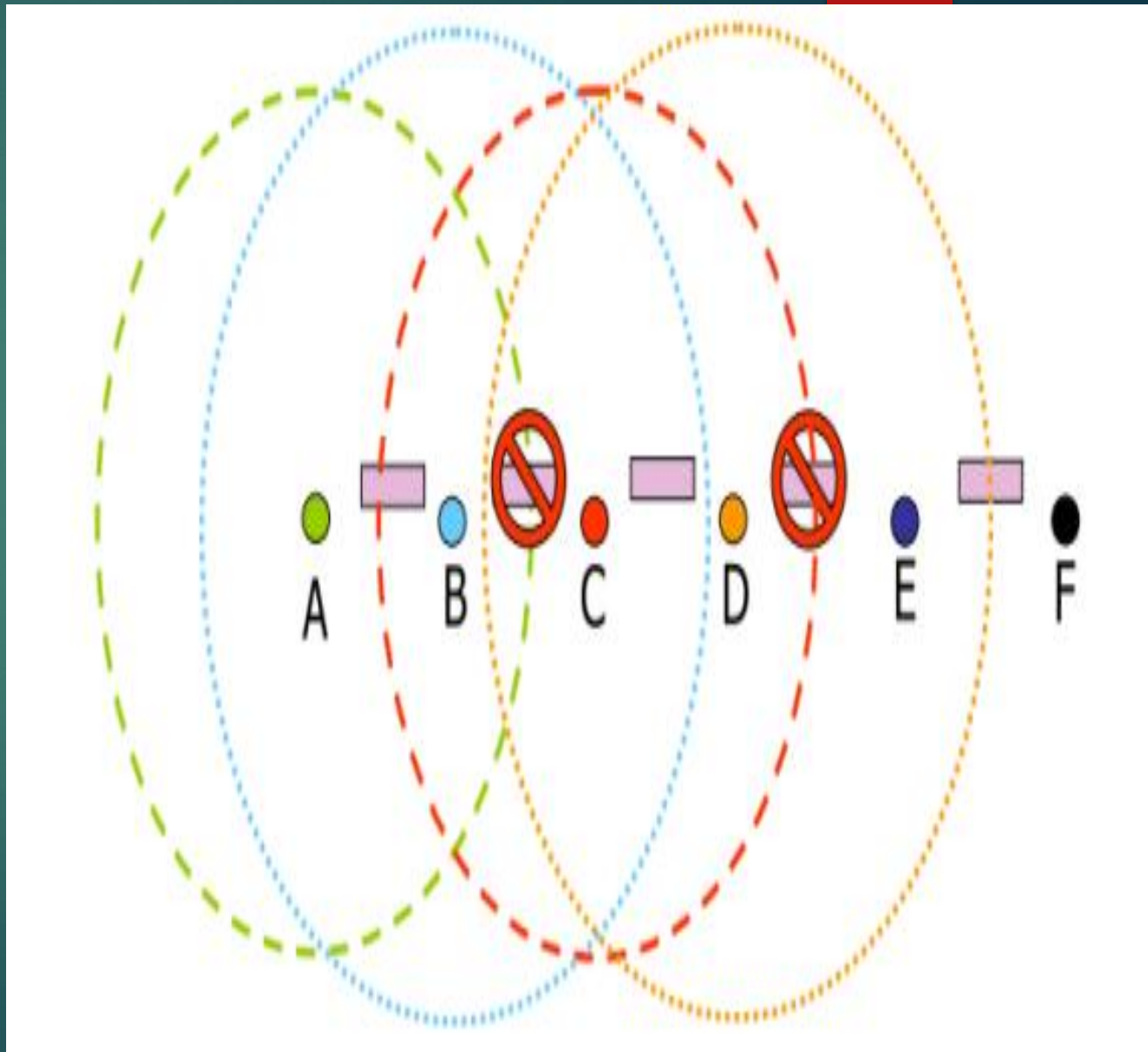
- Hiệu suất tầng vận tải bị ảnh hưởng bởi tất cả các giao thức bên dưới nó
  - Tầng vật lý
    - *Các cơ chế vận chuyển có thể hiểu sai lỗi: một trong những lý do lớn khiến TCP gặp khó khăn trong mạng không dây*
  - MAC
    - *Các luồng vận chuyển bị tranh chấp giữa các luồng và trong luồng*
  - Tầng mạng
    - *Các phiên vận chuyển tồn tại như là các đường dẫn định tuyến; duy trì đường dẫn – duy trì phiên*
    - *Tính di động: mất kết nối/mất đường dẫn gây ra các hành vi khác nhau trong các giao thức định tuyến khác nhau, tất cả đều ảnh hưởng đến quá trình vận chuyển*

TÁC ĐỘNG CỦA TẦNG VẬT LÝ → TẦNG VẬN CHUYỂN

- TCP diễn giải các lỗi và cố gắng giảm thiểu ảnh hưởng của chúng bằng cách sử dụng kiểm soát tắc nghẽn
  - Nhưng thường không phân biệt được mất các điểm nghẽn do lỗi đường truyền
  - Kiểm soát tắc nghẽn có thể được gọi khi không cần thiết
  - TCP + lỗi trong quá trình truyền = giảm thông lượng

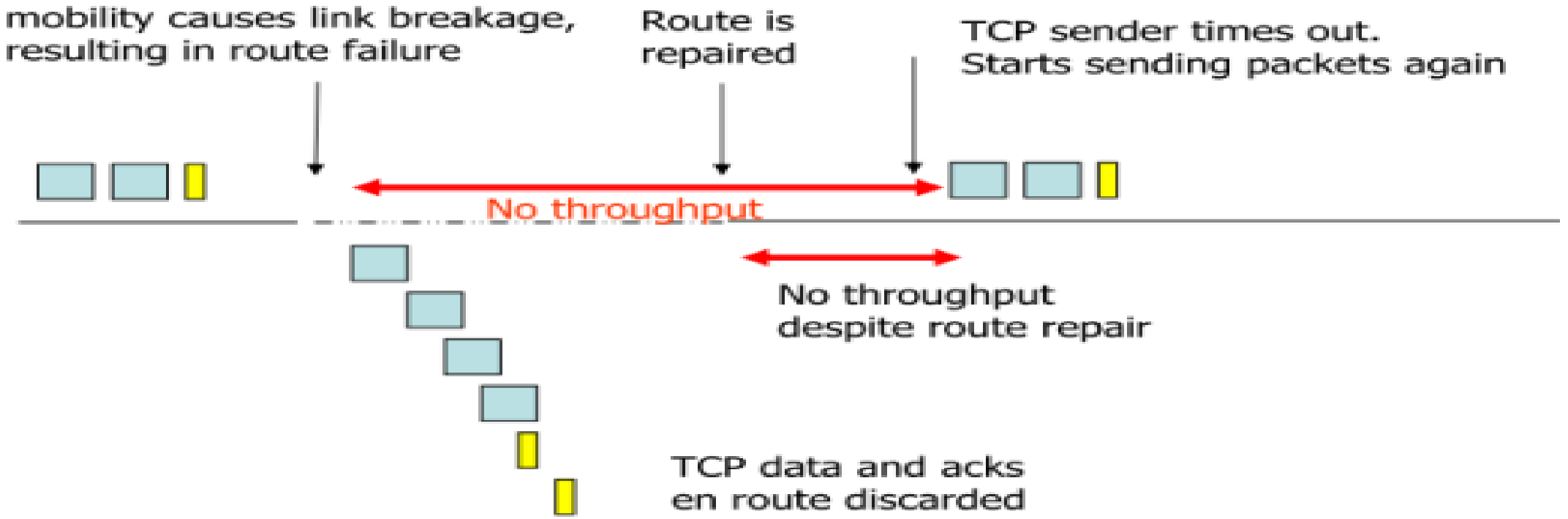
ẢNH HƯỞNG CỦA MAC → TẦNG VẬN TẢI

- Nhiều bước nhảy/đường dẫn hơn có nghĩa là mức sử dụng phương tiện nhiều hơn
  - Tăng tính cạnh tranh cho phương tiện, ngay cả giữa các nút trong cùng một đường dẫn định tuyến
  - Độ nhiễu cao hơn và thiết bị đầu cuối ẩn / tiếp xúc



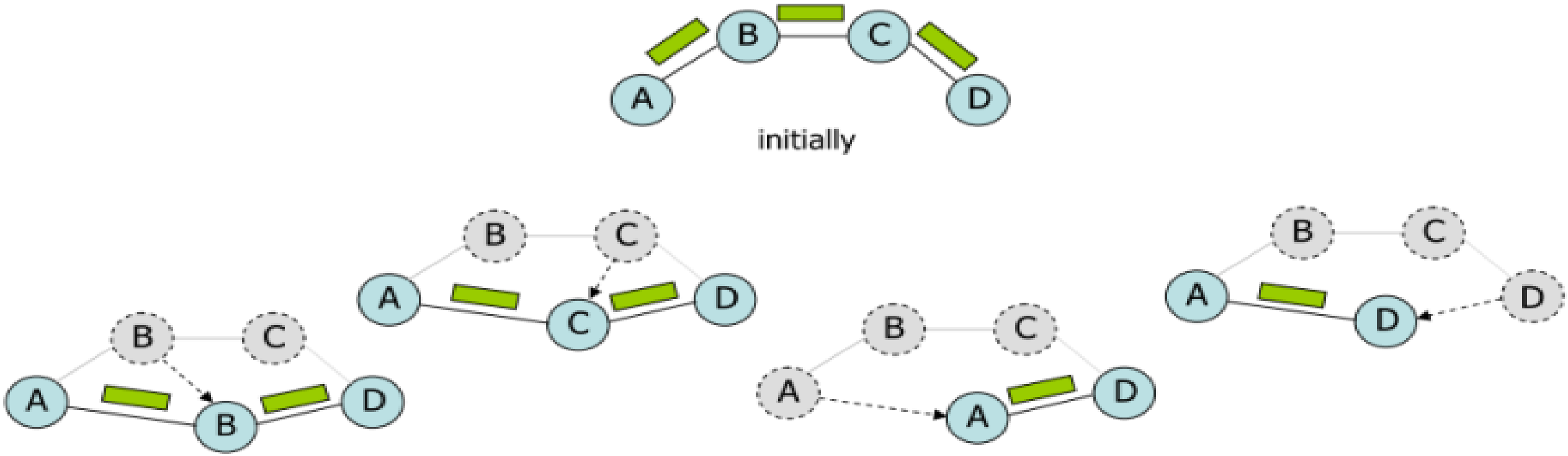
ẢNH HƯỞNG CỦA TÍNH DI ĐỘNG → TẦNG VẬN TẢI

- Tính di động của nút dẫn đến thay đổi tuyến đường
  - Tuyến có thể bị lỗi, mất dữ liệu trên tuyến cũ, tuyến mới được hình thành, hết thời gian TCP bắt đầu truyền dữ liệu trên tuyến mới



ẢNH HƯỞNG TÍNH DI ĐỘNG ⟶ TẦNG VẬN TẢI

- Tính di động của nút dẫn đến thay đổi tuyến đường
  - Tuyến đường có thể thất bại, tuyến đường ngắn hơn được hình thành

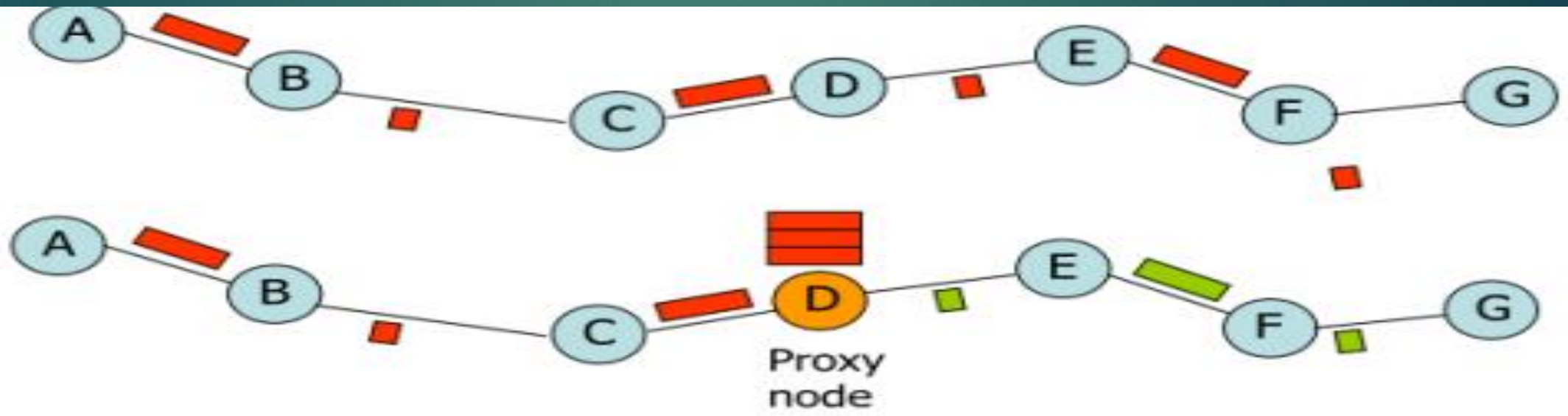


ẢNH HƯỞNG CỦA ĐỊNH TUYẾN → TẦNG VẬN TẢI

- Bộ nhớ đệm định tuyến can thiệp vào TCP (ví dụ: trong DSR)
  - Nhiều tuyến đường được lưu trữ để giảm chi phí khám phá
  - Ở Tầng mạng, quét nguồn để tìm tuyến trực tiếp
    - Các tuyến đường cũ hơn có thể đã bị hỏng do tính di động, v.v.
    - Hết thời gian chờ TCP, thiếu lưu lượng dữ liệu trong quá trình quét
  - Thay vì:
    - Vô hiệu hóa bộ nhớ đệm định tuyến
    - Thông báo lỗi liên kết (TCP-ELFN)
    - Thông báo tắc nghẽn hoặc thông báo không thể truy cập ICMP (ATCP)

CHIA TÁCH TCP

- Trong hỗn hợp có dây/không dây:
  - TCP chỉ chạy ở các điểm cuối và tại một proxy ở biên giới có dây/không dây
  - Proxy tăng tốc lưu lượng truy cập qua miền có dây
- Trong multihop không dây:
  - Proxy có thể được sử dụng để chia thành các đường dẫn ngắn



ƯU/NHƯỢC ĐIỂM CỦA CHIA TÁCH TCP

- **Ưu điểm:**
  - Cải thiện cơ hội TCP multi-hop bằng cách sử dụng các vòng lặp ngắn hơn và tiến hóa nhanh hơn
  - Truyền lại theo đường dẫn ngắn hơn, tiết kiệm năng lượng và giảm nhiễu
- **Nhược điểm:**
  - Phá vỡ E2E, do đó không còn tương thích với bảo mật đầu cuối như IPSec
  - Tăng bộ đệm tại các proxy, yêu cầu trí thông minh cao hơn tại các nút trung gian
  - Thay đổi/ngắt tuyến đường yêu cầu thay đổi proxy

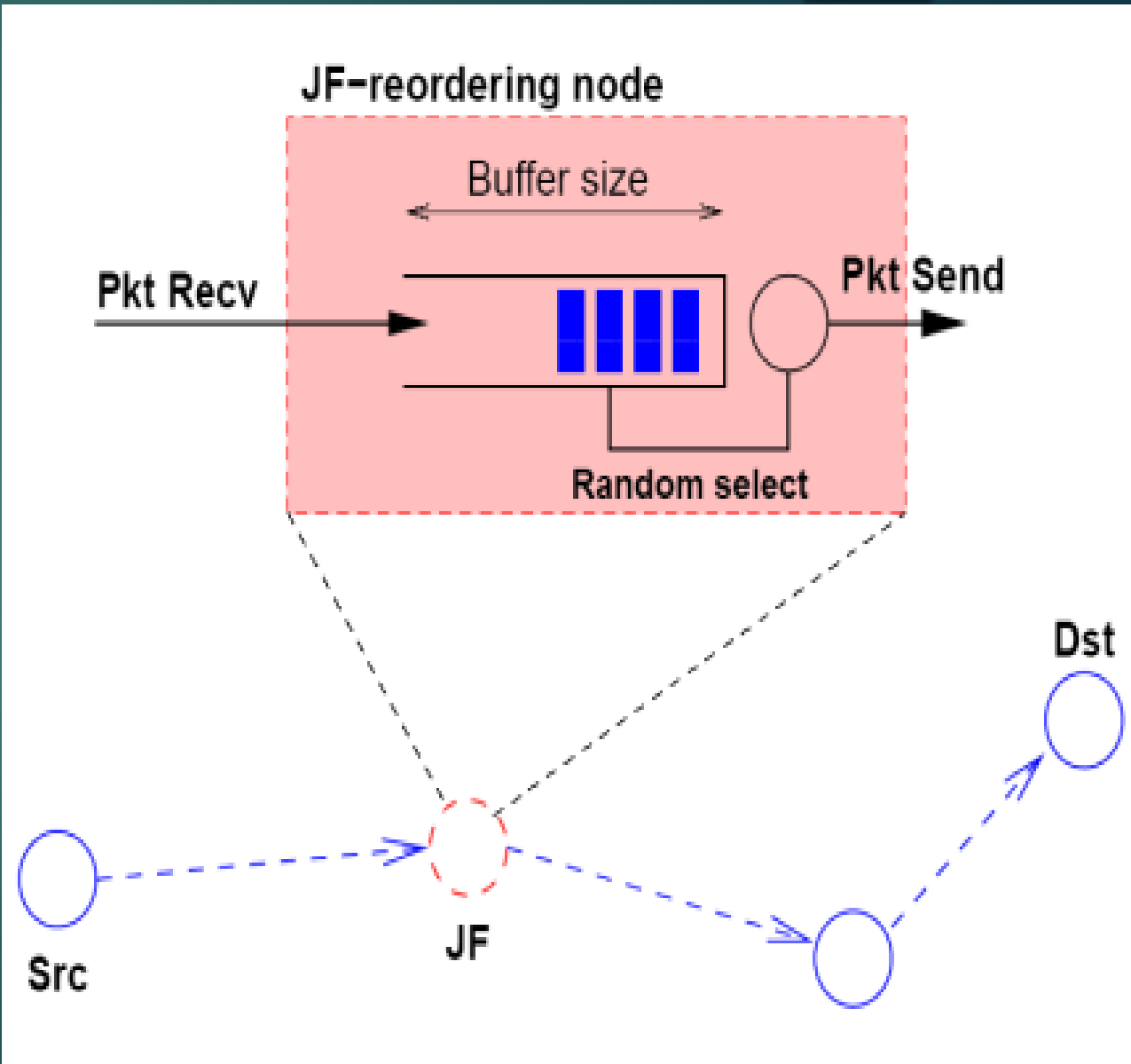
HÀNH VI SAI TRÁI

TẤN CÔNG JELLYFISH (JF)

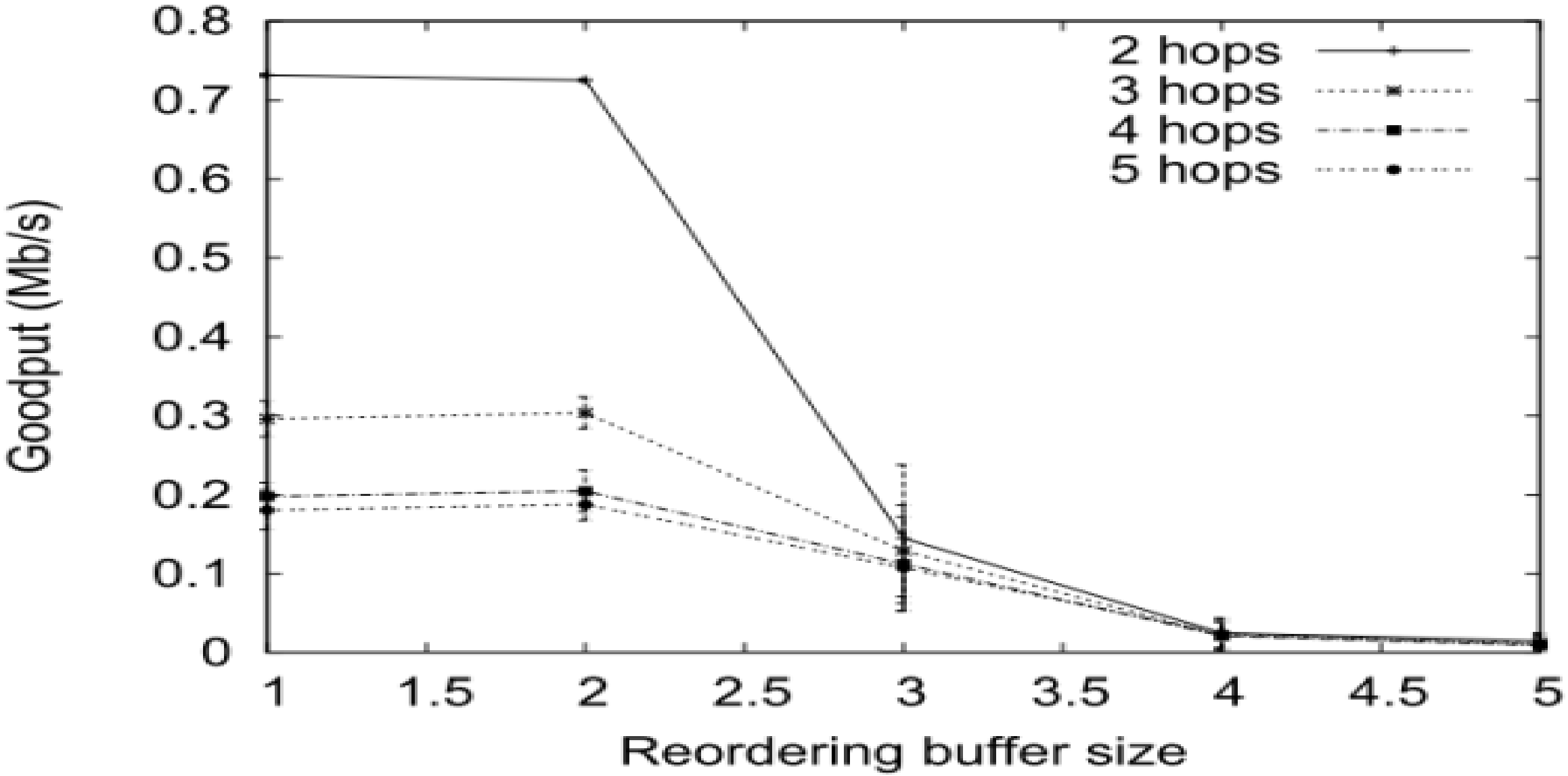
- JellyFish (JF) tấn công kiểm soát tắc nghẽn mục tiêu được sử dụng trong nhiều biến thể TCP và UDP
  - Các cuộc tấn công JF tuân thủ tất cả các yêu cầu giao thức kiểm soát và mặt phẳng dữ liệu ngoại trừ các hành động độc hại được nhắm mục tiêu bao gồm:
    - Sắp xếp lại các gói tin
    - Loại bỏ gói tin
    - Tăng phương sai trễ

JF ĐẶT LẠI THỨ TỰ GÓI TIN

- TCP sử dụng tích lũy ACK để đạt hiệu quả và dựa vào các ACK trùng lặp để phát hiện việc mất hoặc nhận không đúng thứ tự
  - *Tất cả các biến thể TCP đều cho rằng việc sắp xếp lại gói là một sự kiện tương đối hiếm và tồn tại trong thời gian ngắn*
- Tấn công đặt lại thứ tự JF
  - *Phân phối tất cả các gói nhưng sử dụng hàng đợi sắp xếp lại thay vì hàng đợi FIFO*

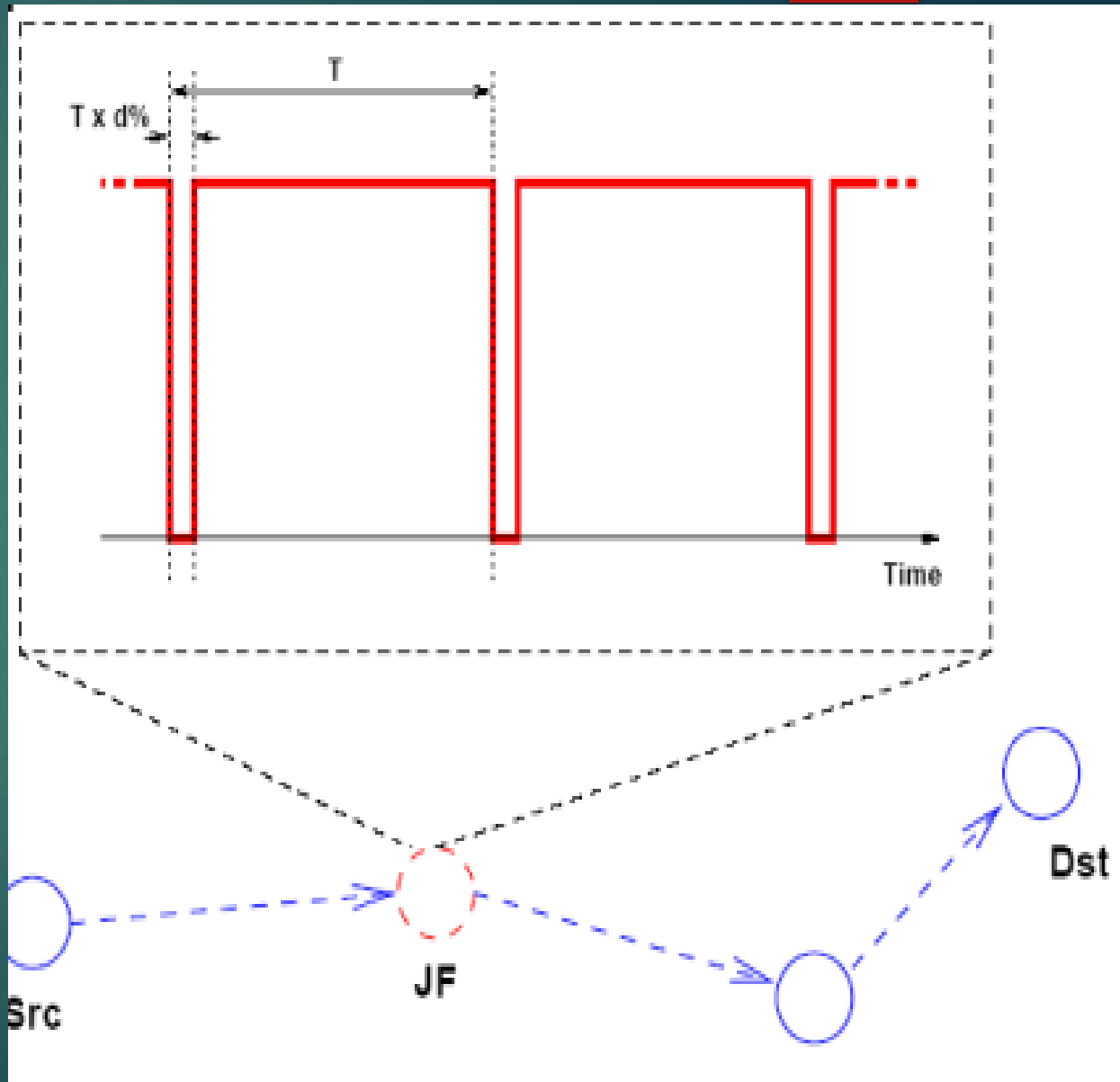


ẢNH HƯỞNG CỦA JF ĐẶT LẠI THỨ TỰ GÓI TIN

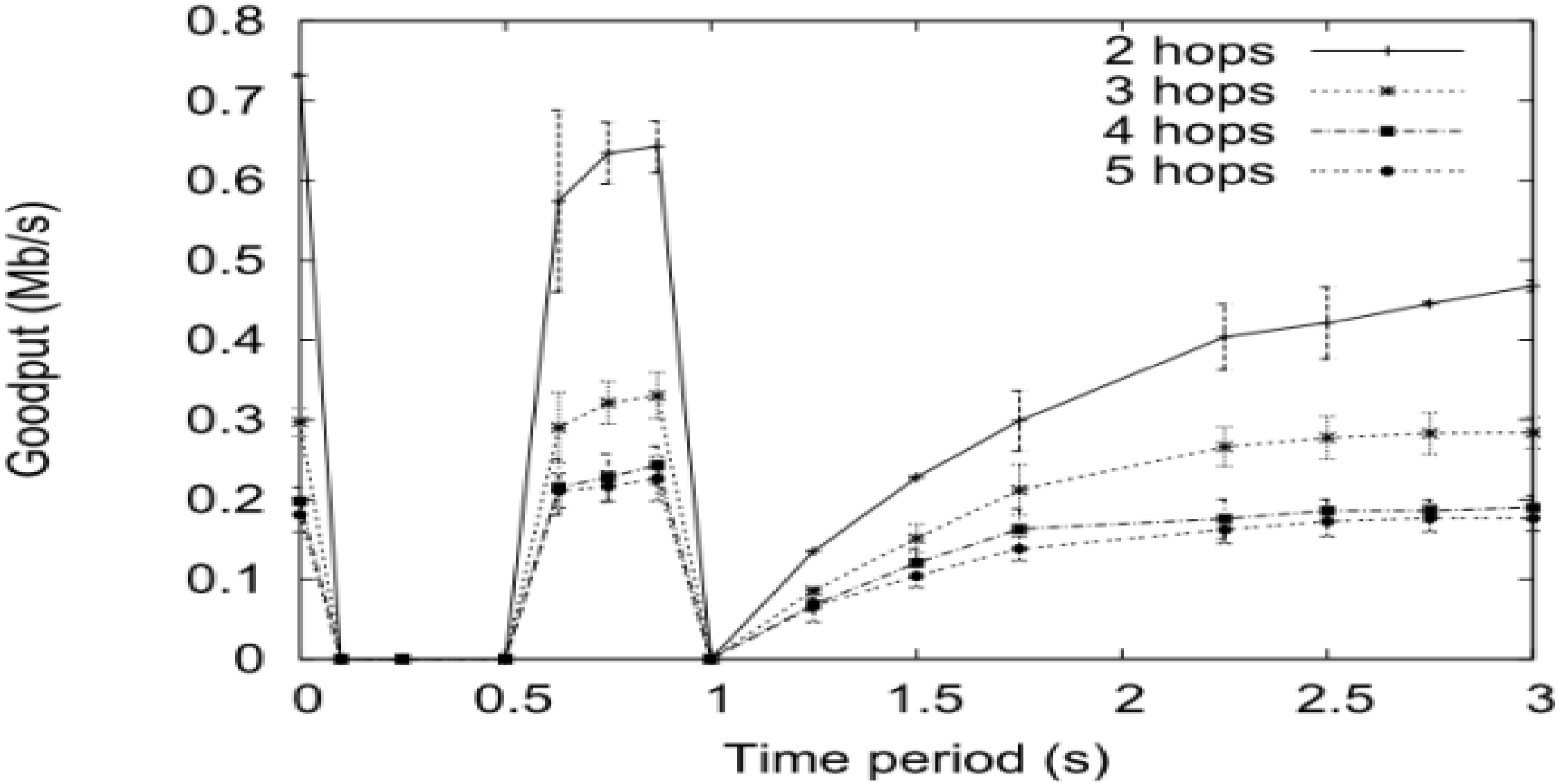


JF LOẠI BỎ ĐỊNH KỲ CÁC GÓI TIN

- Nếu mất gói xảy ra định kỳ gần thang thời gian truyền lại (~1 giây để giải quyết tắc nghẽn nghiêm trọng), thì thông lượng E2E gần như bằng không
- Cuộc tấn công loại bỏ gói đinh kỳ của JF
  - Loại bỏ gói trong thời gian rất ngắn với khoảng thời gian gần hết thời gian truyền lại

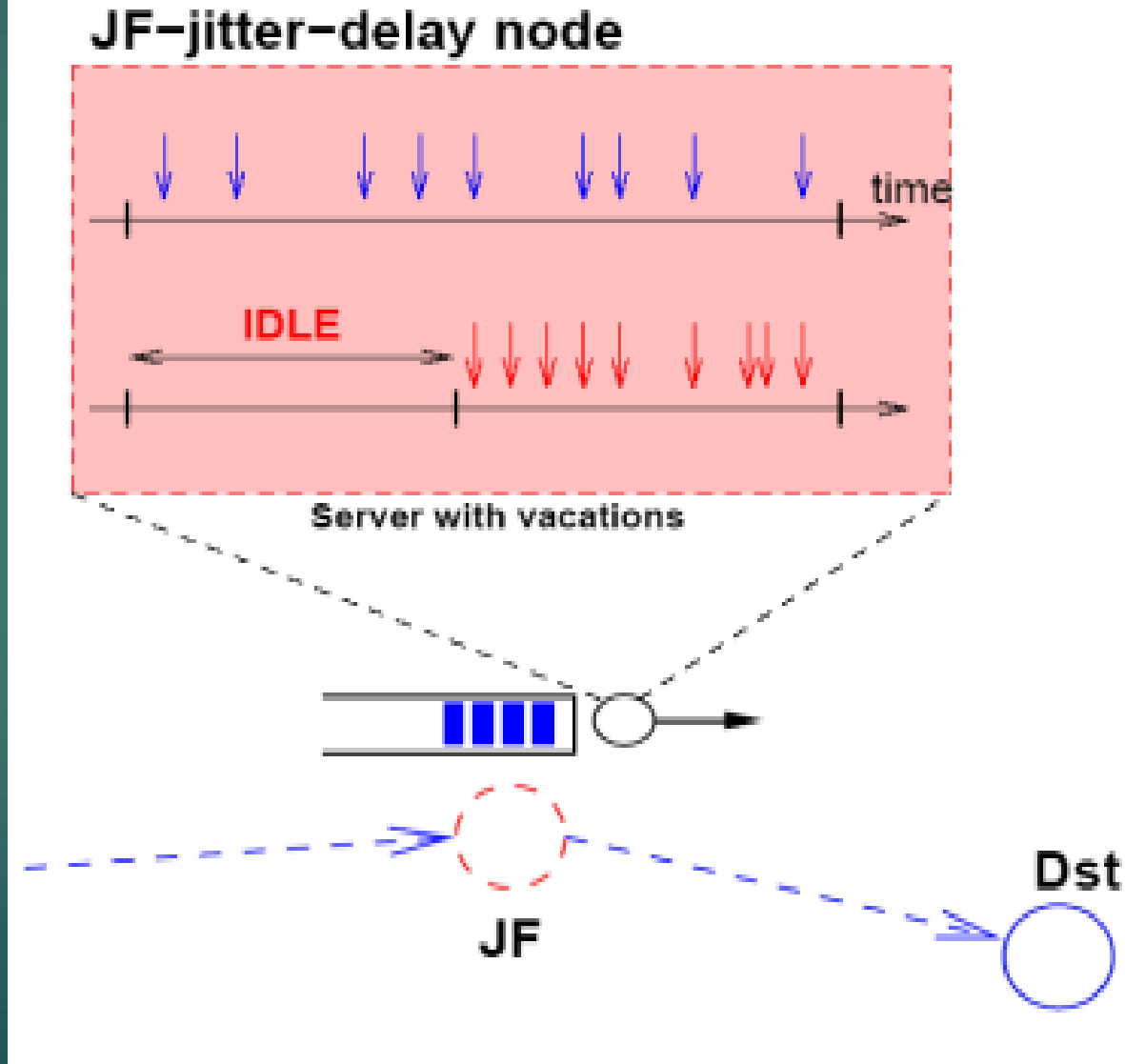


TÁC ĐNG CỦA JF PER. DROPPING

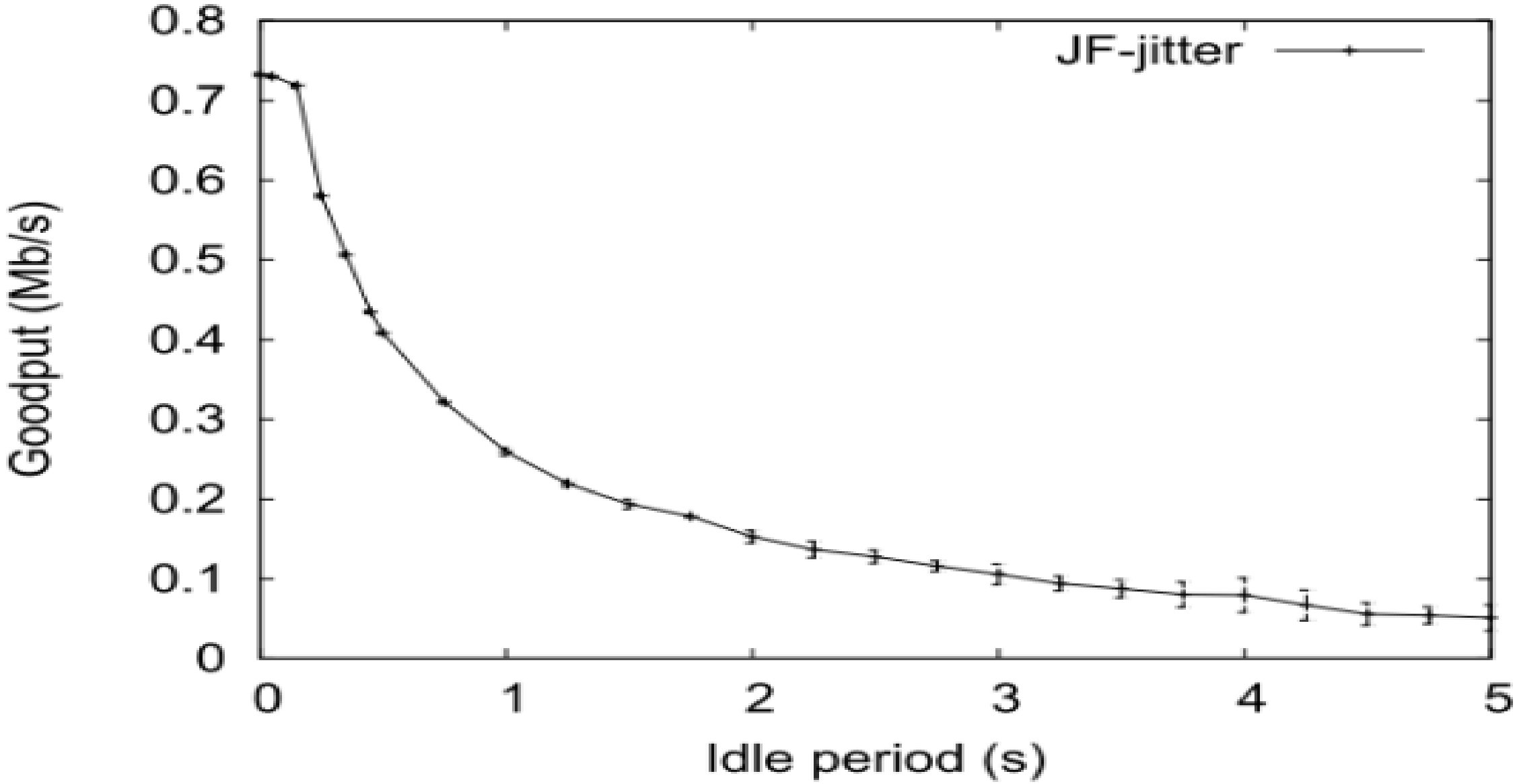


PHƯƠNG SAI TRỄ JF

- Thời gian khứ hồi thay đổi do tắc nghẽn và phương sai này được đo để ước tính các tham số giao thức quan trọng
- Tấn công phương sai trì hoãn JF
  - *Đưa vào độ trễ ngẫu nhiên khi chuyển tiếp từng gói, duy trì trật tự, nhưng tăng phương sai độ trễ*



TÁC ĐỘNG CỦA PHƯƠNG SAI TRỄ JF



PHÁT HIỆN CÁC CUỘC TẤN CÔNG JF

- Phát hiện dựa trên khả năng giám sát hành vi chuyển tiếp
  - *Sử dụng ACK thụ động hoặc "nghe lỏm" (ví dụ: Watchdog)*
  - *Rất nhiều phân tích và mô phỏng trong các bài báo*
- Khi bị phát hiện, nạn nhân có thể:
  - *Thay đổi đường dẫn định tuyến*
  - *Chuyển sang định tuyến đa đường*
  - *Tạo các tuyến dự phòng để sử dụng khi hiệu suất giảm*

CÒN CÁC GIAO THỨC TRUYỀN TẢI KHÁC NGOÀI TCP VÀ UDP THÌ SAO?

ĐỘ TIN CẬY TẦNG VẬN TẢI CỦA WSN

- Các nhà nghiên cứu đã đề xuất nhiều cơ chế vận chuyển thay thế cho WSN
  - *Cách tiếp cận dựa trên ACK, trên cơ sở end-to-end hoặc hop-by-hop*
- Kẻ tấn công tầng vận tải
  - Nghe trộm thông tin liên lạc trong mạng, giả mạo và đưa vào các thông báo điều khiển tầng vận tải
    - *1. Tấn công vào độ tin cậy*
    - *2. Tấn công tiêu hao năng lượng*

PHÂN TÍCH CÁC GIAO THỨC

- PSFQ - Bơm chậm, lấy nhanh
  - *Cơ chế hop-by-hop dựa trên NACK để khôi phục lỗi nhanh chóng bằng cách tìm nạp các phân đoạn từ hàng xóm*
- DTC - Bộ nhớ đệm TCP phân tán
  - *Độ tin cậy hop-by-hop dựa trên SACK (lên và xuống luồng) bằng cách sử dụng kết hợp ACK và NACK*
- Garuda
  - *Cách tiếp cận dựa trên NACK với phục hồi cục bộ bằng cách sử dụng các nút CORE có mục đích đặc biệt*
- RBC - Reliable Bursty Convergecast
  - *Sơ đồ ACK không có cửa sổ để khôi phục từng bước một với việc phân phối không theo thứ tự hiệu quả*

QUAN SÁT CHUNG

- Các lược đồ dựa trên ACK/NACK dễ bị kiểm soát tiêm gói
  - *ACK dễ bị tấn công độ tin cậy*
  - *NACK dễ bị tấn công làm cạn kiệt tài nguyên*
  - *SACK hoặc lai ACK/NACK kế thừa cả hai lỗ hổng*
- Ngăn chặn sự cạn kiệt tài nguyên trong các sơ đồ dựa trên NACK có thể cần xác thực mạnh hoặc hệ thống danh tiếng được thiết kế tốt
- Mọi giải pháp bảo vệ đều phải đánh đổi

TÓM TẮT

- Các loại hành vi sai trái ở tầng vận tải và khả năng phòng thủ
  - Các tấn công Jellyfish và hành vi không tuân thủ giao thức trong cài đặt TCP và UDP một cách tin cậy.

[Aad và cộng sự; MobiCom 2004]

  - Hành vi sai trái trong các giao thức vận tải thay thế cho mạng cảm biến không dây

[Buttyan và Csik; PerSens 2010]

BÀI 16:

AN NINH DỊCH VỤ XÁC ĐỊNH VỊ