BÀI #11 - BẢO MẬT ĐỊNH TUYẾN VÀ CHUYỂN TIẾP

TS. HOÀNG SỸ TƯƠNG

BÀI #11 - BẢO MẬT ĐỊNH TUYẾN VÀ CHUYỂN TIẾP

- Khái niệm cơ bản về định tuyến trong mạng ad hoc
- Điều khiển mặt phảng tấn công và phòng thủ
- Các cuộc tấn công và phòng thủ trên mặt phẳng dữ liệu

HÃY BẮT ĐẦU VỚI MỘT SỐ KHÁI NIỆM CƠ BẢN VỀ ĐỊNH TUYẾN MANET

GIAO THỨC ĐỊNH TUYẾN PHỔ BIẾN

Định tuyến trạng thái liên kết (LS)

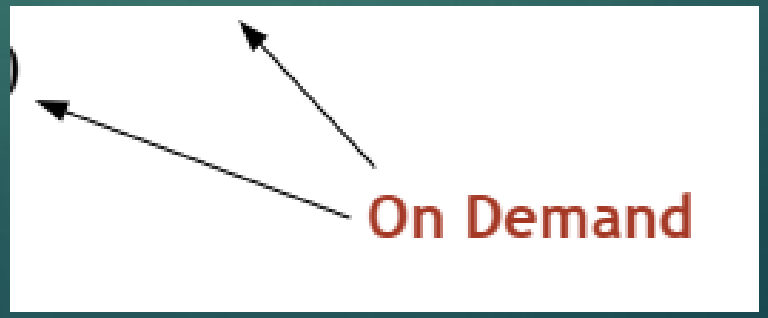
- Định tuyến trạng thái liên kết được tối ưu hóa (OLSR)

Định tuyến vectơ khoảng cách (DV)

- Vectơ khoảng cách theo trình tự đích (DSDV)

- Vectơ khoảng cách theo yêu cầu ad hoc (AODV)

- Định tuyến nguồn động (DSR)



ĐỊNH TUYẾN THEO YÊU CẦU

- Định tuyến theo yêu cầu có một số ưu điểm và nhược điểm trong MANETs
  - Hiệu quả:

    (+) Thông tin định tuyến không được thu thập và cập nhật liên tục, chỉ thực hiện khi cần thiết

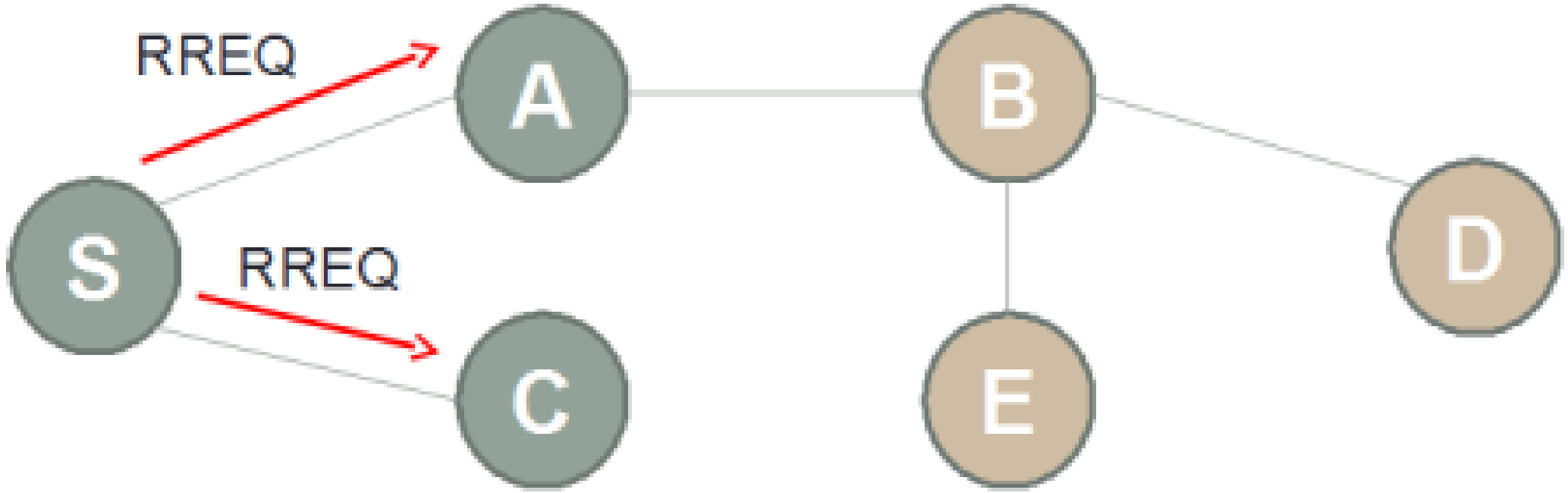
    (-) Chi phí thu thập thông tin một lần có thể cao hơn
  - An toàn:

    (+) Các nút nguồn nhận thức được toàn bộ đường dẫn, không giống như các thuật toán phân tán chỉ tập trung vào chặng tiếp theo

    (-) Thông tin dài hạn thường không có sẵn
  - Nhìn chung ưu điểm nhiều hơn nhược điểm nên định tuyến theo yêu cầu (đặc biệt là định tuyến nguồn) được ưa chuộng

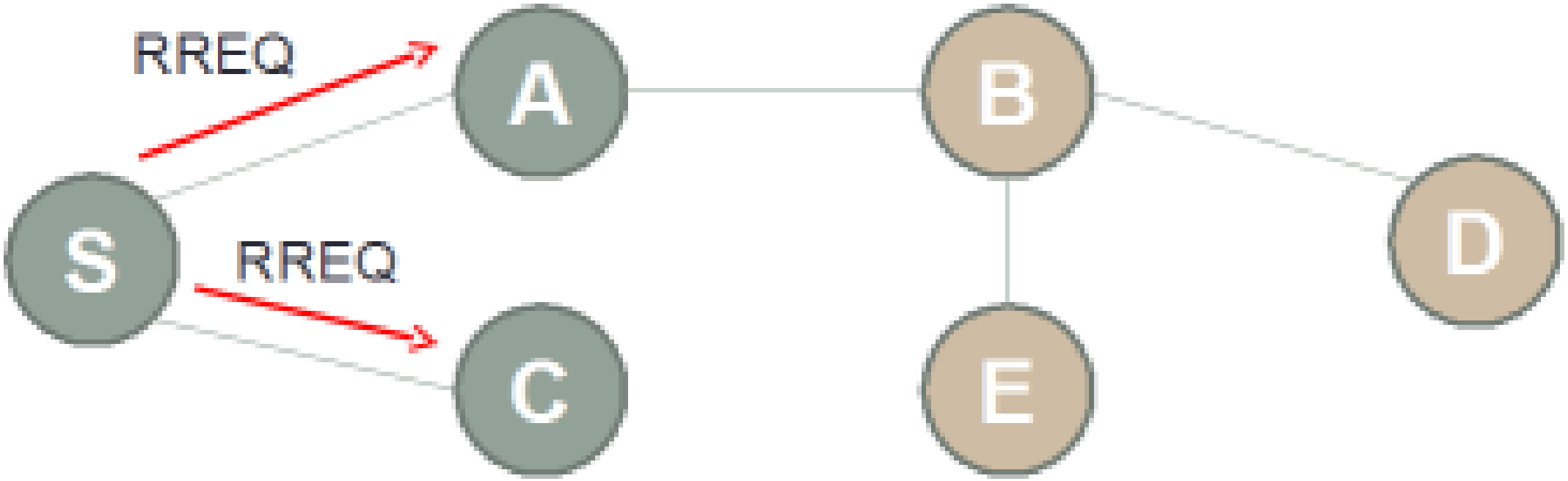
KHÁM PHÁ TUYẾN ĐƯỜNG

- Nguồn S và các nút lân cận sử dụng trao đổi thông báo điều khiển để khám phá tuyến đường từ S đến đích D



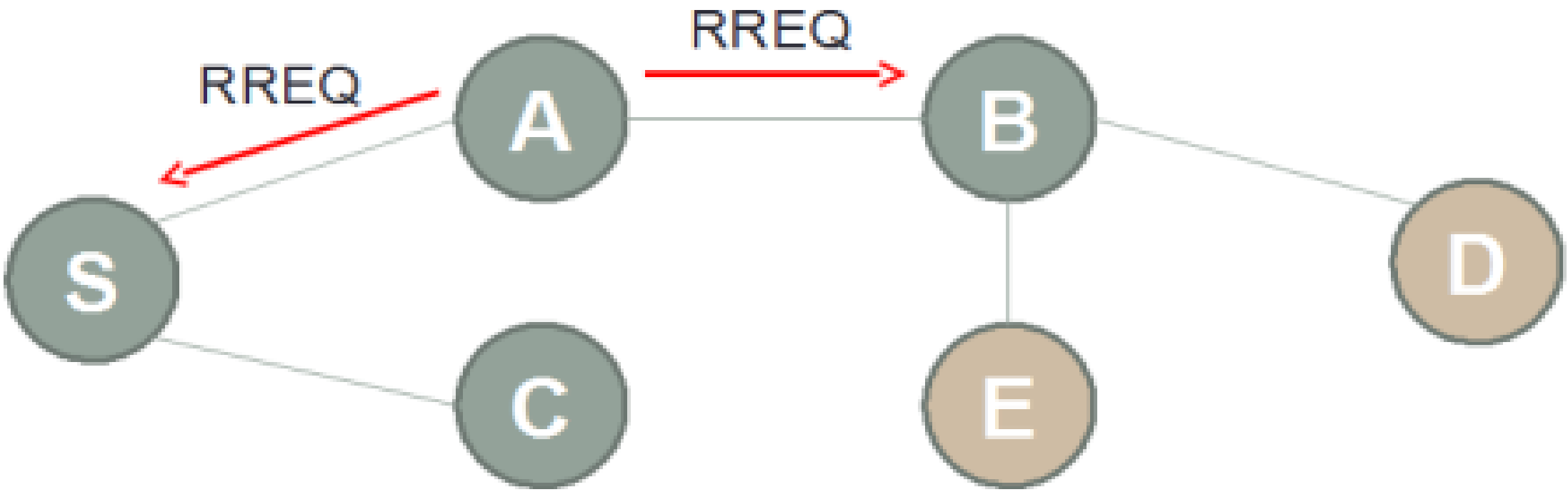
KHÁM PHÁ TUYẾN ĐƯỜNG

- tấn công Flooding yêu cầu tuyến đường:
  - Nguồn S quảng bá gói yêu cầu định tuyến (RREQ) tới hàng xóm



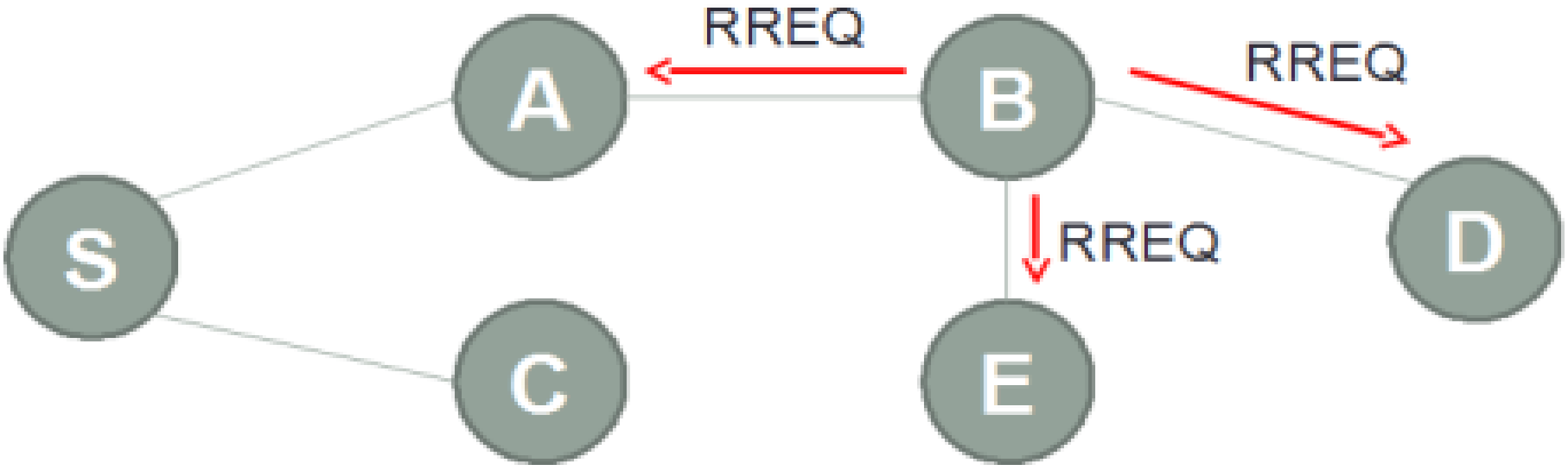
KHÁM PHÁ TUYẾN ĐƯỜNG

- Chuyển tiếp RREQ:
  - Nếu hàng xóm không có mối quan hệ trước với đích, nó sẽ quảng bá thêm RREQ



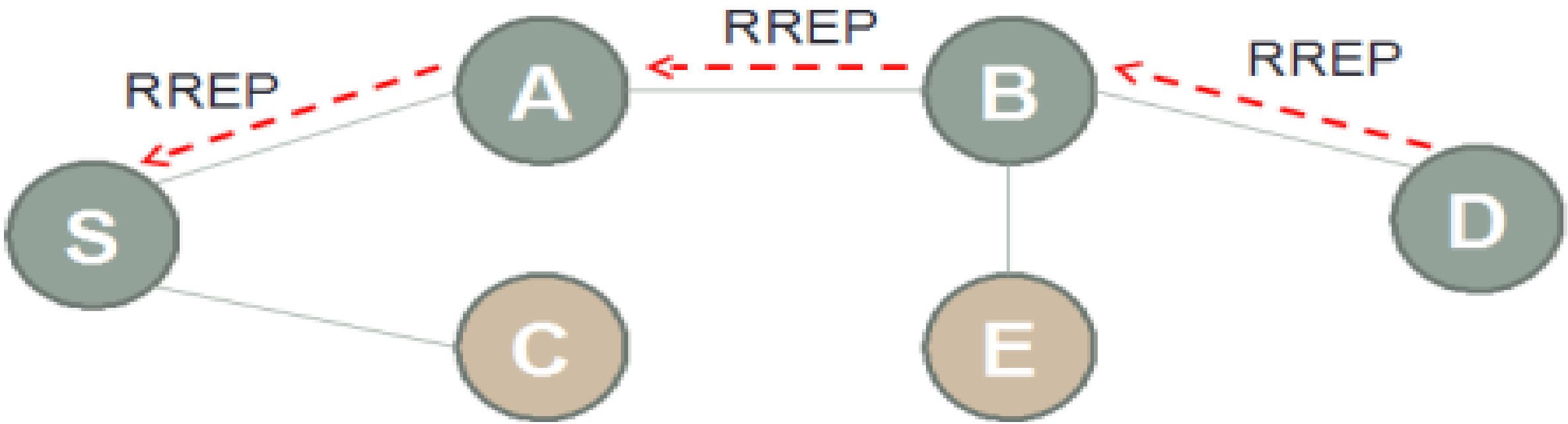
KHÁM PHÁ TUYẾN ĐƯỜNG

- flooding các gói điều khiển để khám phá các tuyến đường
  - Khi gói RREQ đến đích hoặc một nút biết đích, nút sẽ gửi một gói RREP đến nguồn thông qua đường dẫn được định tuyến



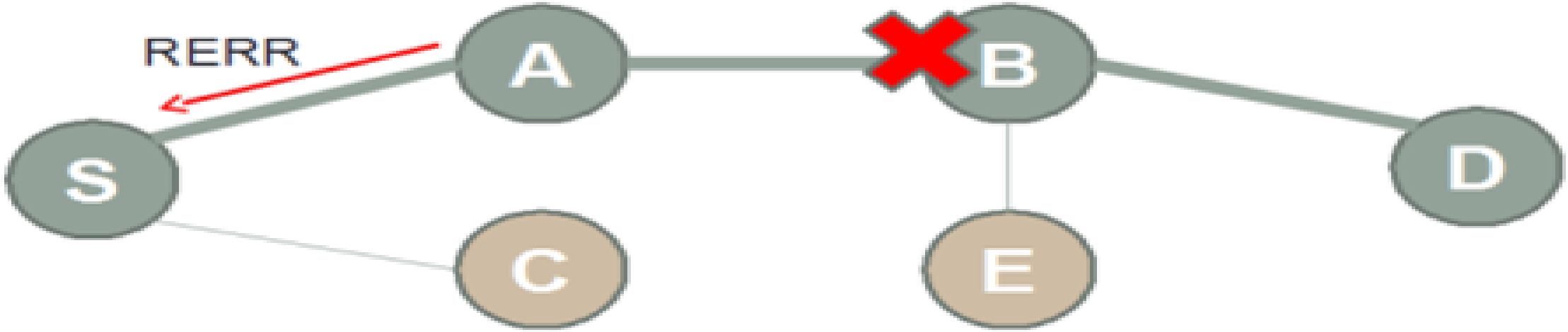
KHÁM PHÁ TUYẾN ĐƯỜNG

- Khi nhận được RREQ, D (hoặc một nút khác biết D) sẽ phát một bản tin Trả lời định tuyến (RREP) trở lại S dọc theo đường đã tìm thấy



BẢO TRÌ TUYẾN ĐƯỜNG

- Nếu một nút không thể tiếp cận chặng tiếp theo
  - Gửi gói điều khiển lỗi định tuyến (RERR) để thông báo cho các láng giềng ngược dòng
  - Thay thế bộ đệm định tuyến (DSR) hoặc khám phá lại



AODV SO VỚI DSR

AODV	DSR
Bảng định tuyến • một tuyến đường cho mỗi điểm đến	Bộ đệm định tuyến • nhiều tuyến đường cho mỗi điểm đến
Luôn chọn những con đường mới hơn • Số thứ tự	Không có cơ chế rõ ràng để hết hạn các tuyến đường cũ
Flood khám phá thường xuyên hơn để đảm bảo độ tươi	Định tuyến nguồn • Các nút trung gian học các tuyến trong 1 chu kỳ khám phá

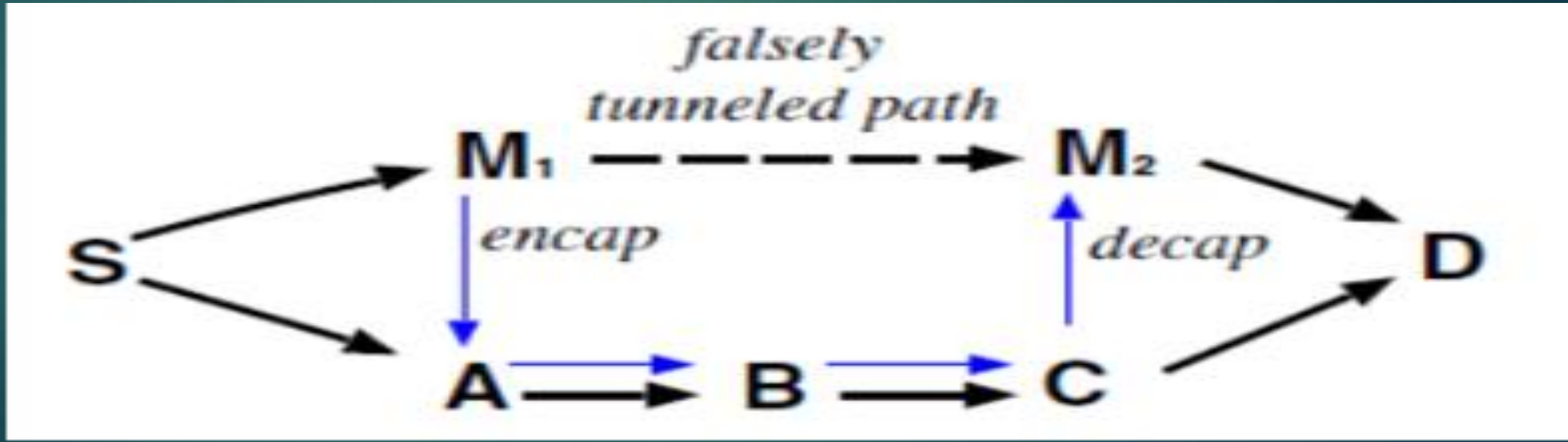
LÀM THẾ NÀO KẺ TẤN CÔNG CÓ THỂ CAN THIỆP HOẶC THAO TÚNG ĐỊNH TUYẾN MANET?

TẤN CÔNG SỬA ĐỔI

- Sửa đổi phần tiếp theo AODV
  - AODV sử dụng seq# làm dấu thời gian (thứ tự cao hoặc mới)
  - Kẻ tấn công có thể tăng seq# để làm cho đường dẫn của nó hấp dẫn
- Sửa đổi số bước nhảy DSR
  - DSR sử dụng #hops để đạt hiệu quả (#hops thấp)
  - Kẻ tấn công có thể hạ thấp/tăng #hops để thu hút/đẩy lùi

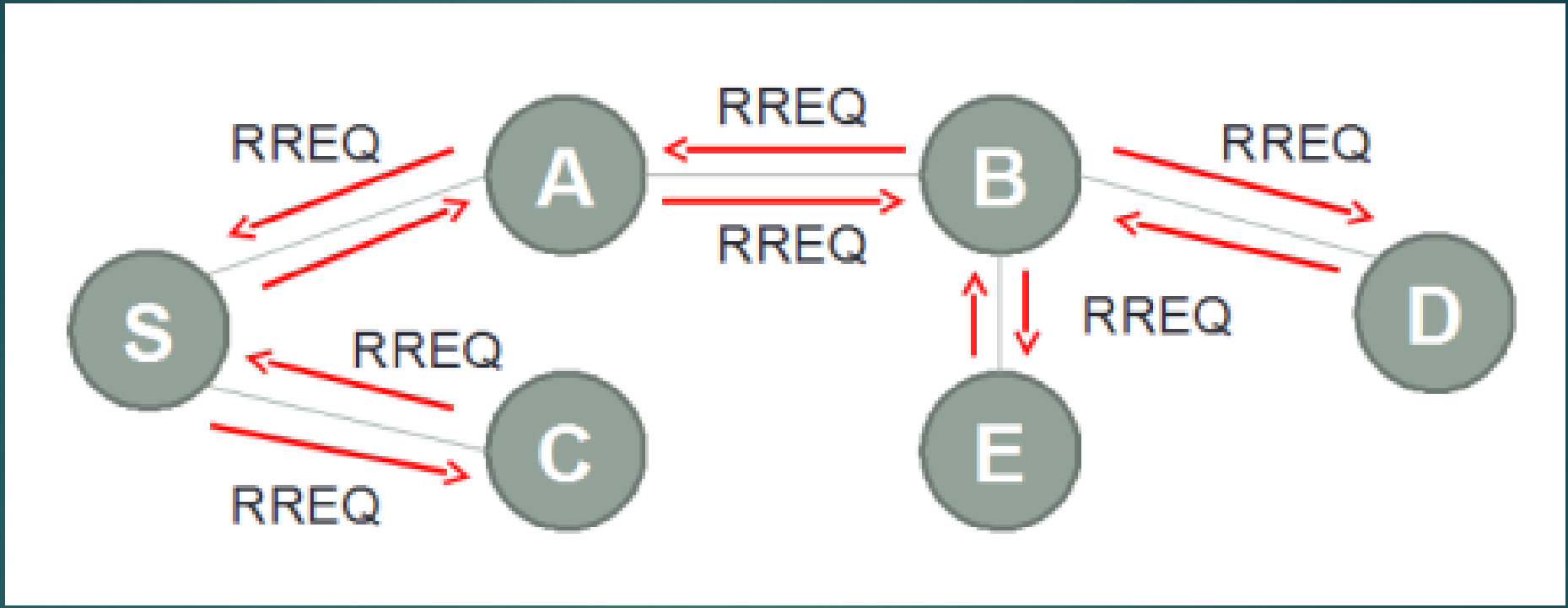
TẤN CÔNG SỬA ĐỔI

- Sửa đổi tuyến đường DSR
  - Tuyến đường không tồn tại (DoS)
  - Vòng lặp (cạn kiệt tài nguyên, DoS)
  - Không kiểm soát để ngăn chặn các vòng lặp sau khi khám phá tuyến đường (thêm một cuộc tấn công vào mặt phẳng dữ liệu, chúng ta sẽ đến sau)
- Đường hầm



Flooding RREQ

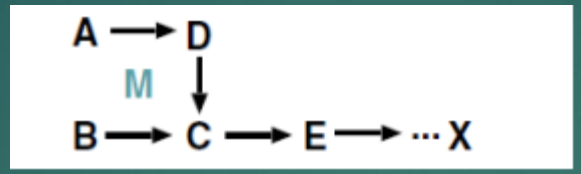
- Làm ngập mạng với các RREQ đến một địa chỉ đích không thể truy cập được



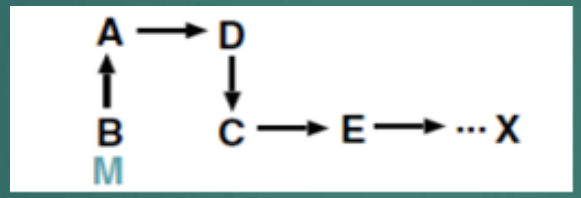
Ví dụ: S liên tục gửi gói RREQ đến đích X

Giả mạo AODV/DSR

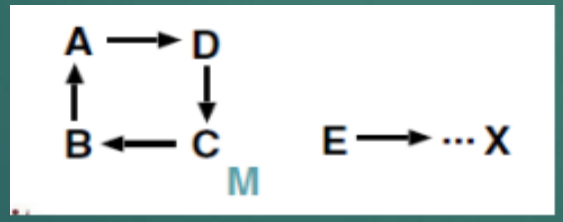
- Kẻ tấn công lắng nghe RREQ/RREP từ hàng xóm



- Gửi RREP "hấp dẫn" với ID giả mạo

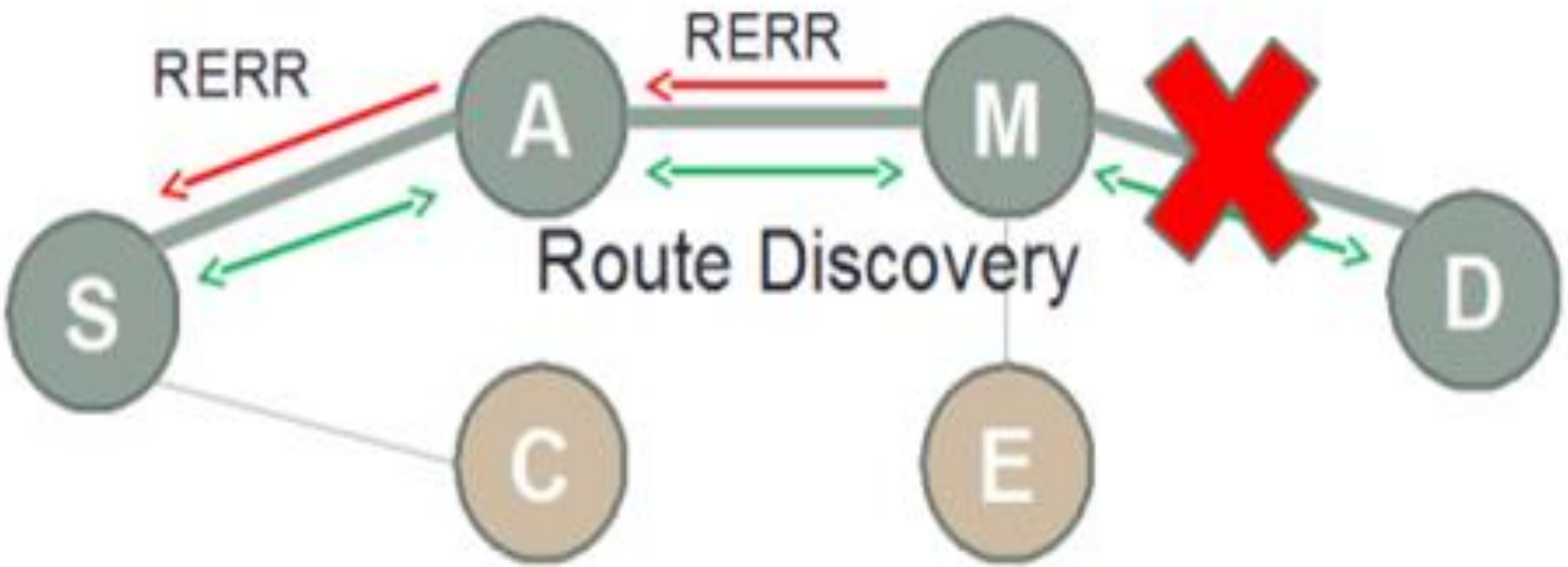


• Giả mạo nhiều ID hơn với kết quả thú vị



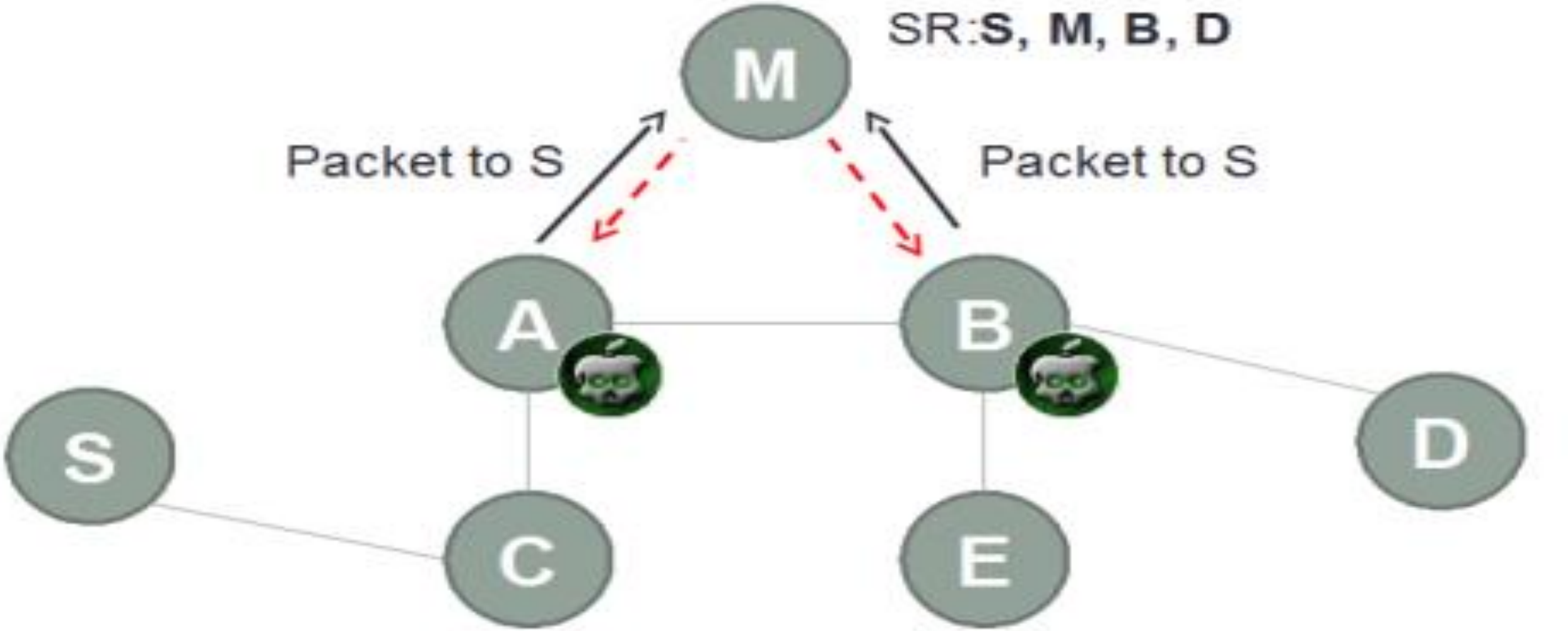
TẤN CÔNG GIẢ MẠO - FABRICATION ATTACKS

- DoS chống lại AODV/DSR bằng cách giả mạo các lỗi xảy ra trên các tuyến đường



TẤN CÔNG GIẢ MẠO - FABRICATION ATTACKS

- Đầu độc DSR route cache



AN NINH MẶT PHẲNG ĐIỀU KHIỂN - CONTROL-PLANE SECURITY

- Làm thế nào để đảm bảo rằng một đường dẫn được thiết lập có thể hiệu quả (ví dụ: ngắn) và/hoặc đáng tin cậy?
- Làm cách nào để ngăn chặn kẻ tấn công thao túng quá trình khám phá/xây dựng đường dẫn?
- Những phương pháp đo nào có thể được sử dụng để định lượng giá trị của một đường dẫn?
  - *Chiều dài? Độ trễ? Lòng tin?*

BẢO MẬT ĐỊNH TUYẾN DV

- Định tuyến vectơ khoảng cách (DV) là một trong những cách tiếp cận cổ điển đối với định tuyến mạng
- SEAD: Định tuyến DV Ad hoc hiệu quả an toàn
  - Dựa trên giao thức DSDV sử dụng số thứ tự để chống lặp định tuyến và không đồng bộ quá trình cập nhật
  - Sử dụng chuỗi băm để xác thực cập nhật định tuyến
  - Dựa vào các cơ chế hiện có để phân phối hàm băm (hash)

BẢO MẬT ĐỊNH TUYẾN LS

- Định tuyến trạng thái liên kết (LS) là cách tiếp cận cổ điển khác đối với định tuyến mạng
- SLSP: Giao thức trạng thái liên kết an toàn
  - Các cặp địa chỉ MAC/địa chỉ IP được ràng buộc bằng chữ ký số
  - Cho phép phát hiện tái sử dụng và thay đổi địa chỉ
  - Cập nhật trạng thái liên kết chỉ được ký và quảng bá trong một vùng giới hạn, với số bước nhảy được xác thực bằng chuỗi băm.

- SRP xác thực trao đổi single hop trong yêu cầu DSR và trả lời tin nhắn
  - Vì bảo vệ là hop-by-hop, SRP qua DSR dễ bị thay đổi đường dẫn (hoặc tham số khác)

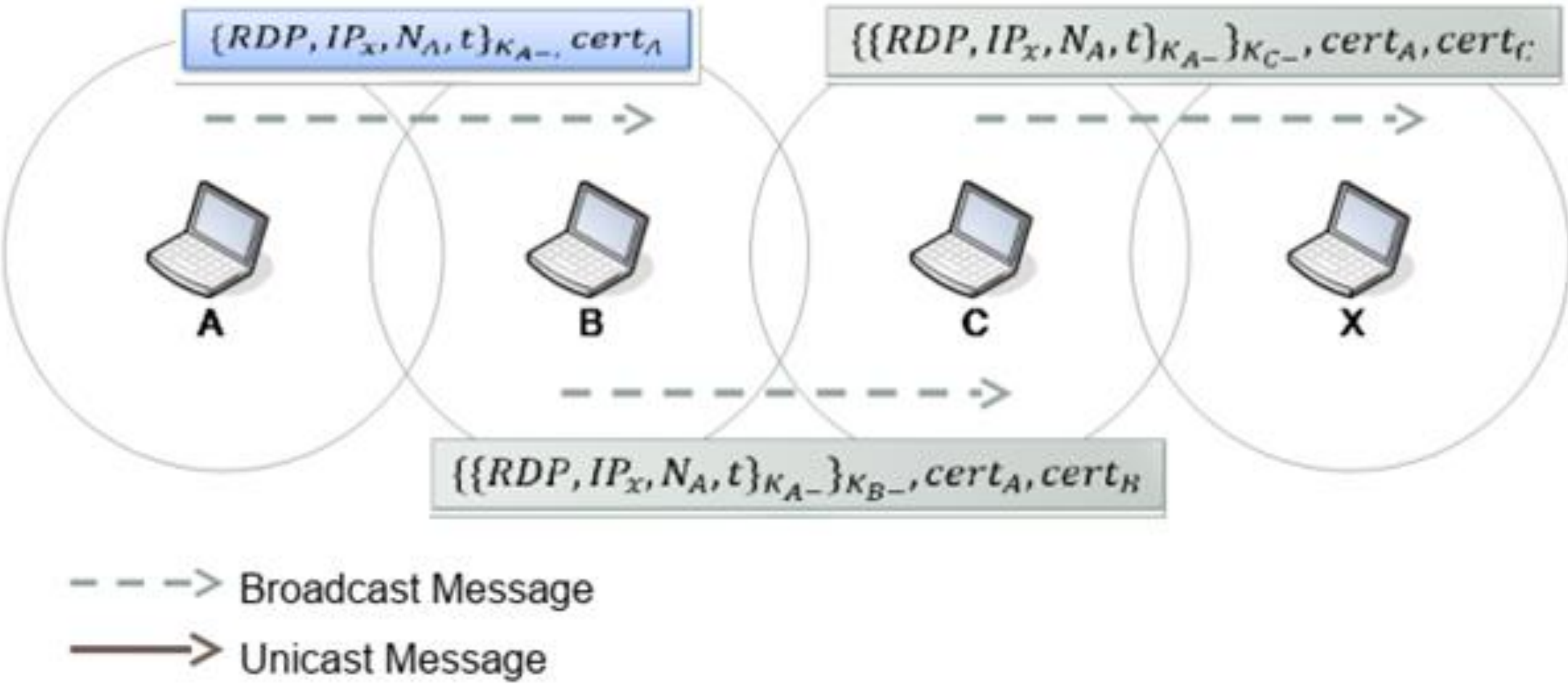
SAODV

- AODV an toàn đưa chữ ký vào giao thức định tuyến AODV để xác thực các trường thông báo khác nhau
  - *Các thông báo RREQ và RREP được ký và số bước nhảy được xác thực bằng chuỗi băm*

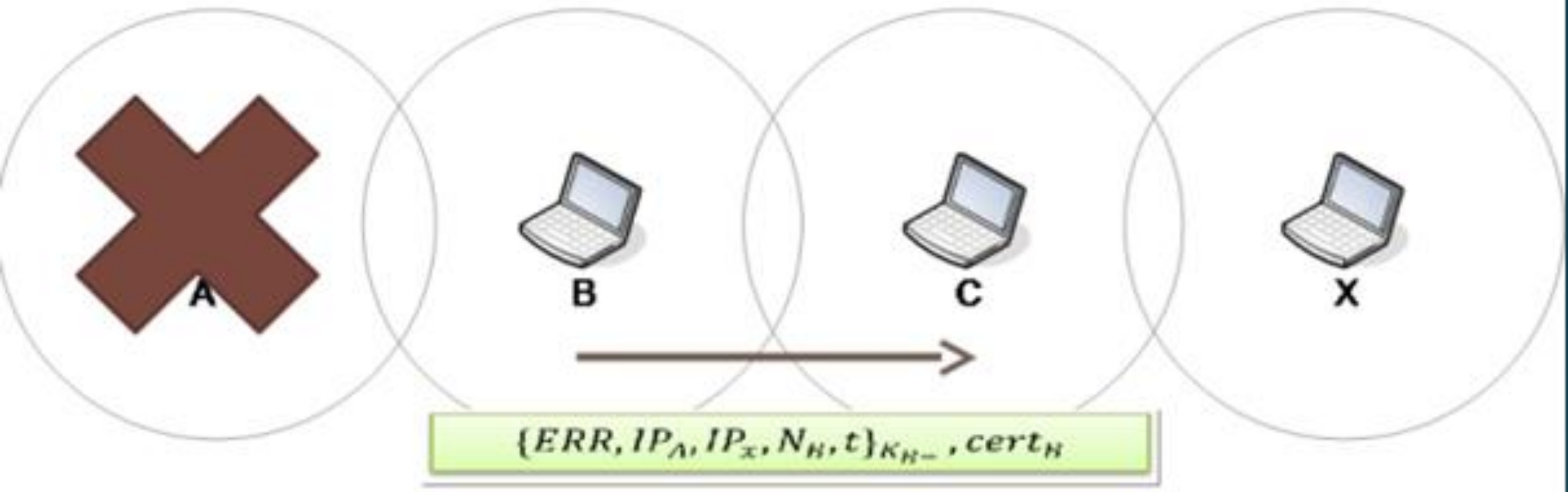
ARAN

- ARAN: Định tuyến được xác thực cho Mạng Ad hoc (dựa trên AODV)
  - Sử dụng chứng chỉ mật mã và khóa bất đối xứng để đạt được xác thực, tính toàn vẹn của thông báo và tính không từ chối
  - Cần quy trình chứng nhận sơ bộ trước quy trình khởi tạo tuyến đường
  - Thông điệp định tuyến được xác thực tại mỗi bước nhảy từ nguồn đến đích và ngược lại

XÁC THỰC. KHÁM PHÁ TUYẾN ĐƯỜNG



XÁC THỰC THIẾT LẬP TUYẾN ĐƯỜNG

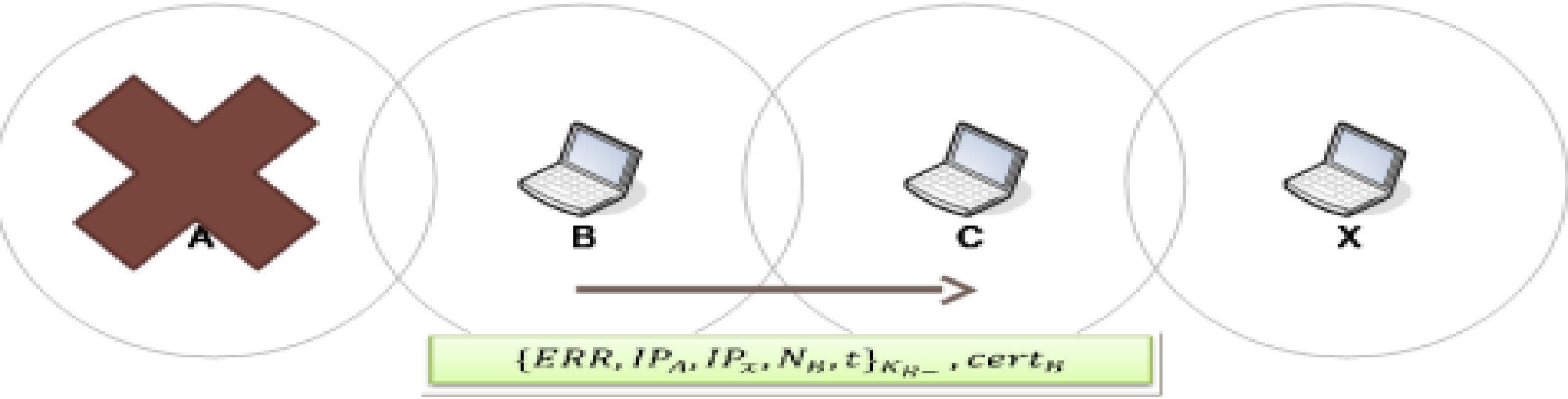


Broadcast Message

Unicast Message

XÁC THỰC DUY TRÌ TUYẾN ĐƯỜNG

- Send ERR message to deactivate route



Broadcast Message

Unicast Message

BẢO MẬT ARAN

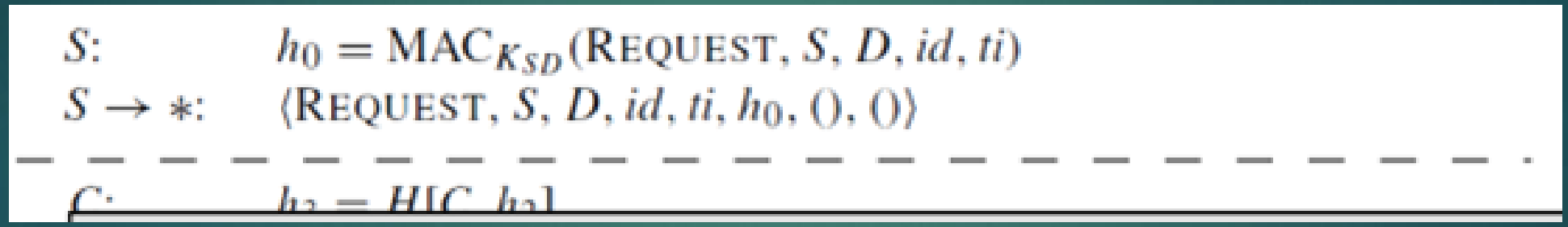
- Tấn công sửa đổi
  - Ngăn chuyển hướng sử dụng seq# hoặc #hops
  - Ngăn chặn DoS với các tuyến nguồn đã sửa đổi
  - Ngăn chặn các cuộc tấn công đường hầm
- Tấn công mạo danh
  - Ngăn chặn hình thành vòng lặp bằng cách giả mạo
- Tấn công giả mạo
  - Ngăn chặn giả mạo lỗi tuyến đường

HẠN CHẾ CỦA ARAN

- ARAN dựa vào PKI
  - Yêu cầu bên thứ ba / cơ sở hạ tầng đáng tin cậy
  - Yêu cầu một trong hai:
    - Chi phí liên lạc đáng kể để tương tác với TTP để cập nhật/thu hồi trong thời gian ngắn
    - Cập nhật chứng chỉ, danh sách thu hồi, v.v. bị trễ.

ARIADNE

- Ariadne là một giao thức định tuyến theo yêu cầu an toàn được xây dựng trên DSR và Tesla
  - DSR: Định tuyến nguồn động, Tesla: Thời gian hiệu quả Xác thực chịu tổn thất luồng (xác thực phát sóng)
  - Yêu cầu tuyến đường và trả lời thông báo được xác thực



Ariadne dễ bị chuyển tiếp độc hại bởi những kẻ tấn công trên đường dẫn định tuyến đã chọn - yêu cầu một cơ chế bổ sung để phản hồi tình trạng mất/chất lượng đường dẫn

BÀI 12:

BẢO MẬT CHUYỂN TIẾP;

QUYỀN RIÊNG TƯ & ẨN DANH MẠNG