BÀI #10 - CÁC MỐI ĐE DỌA Ở LỚP MẠNG; QUẢN LÝ ĐỊNH DANH

TS. HOÀNG SỸ TƯƠNG

BÀI 10

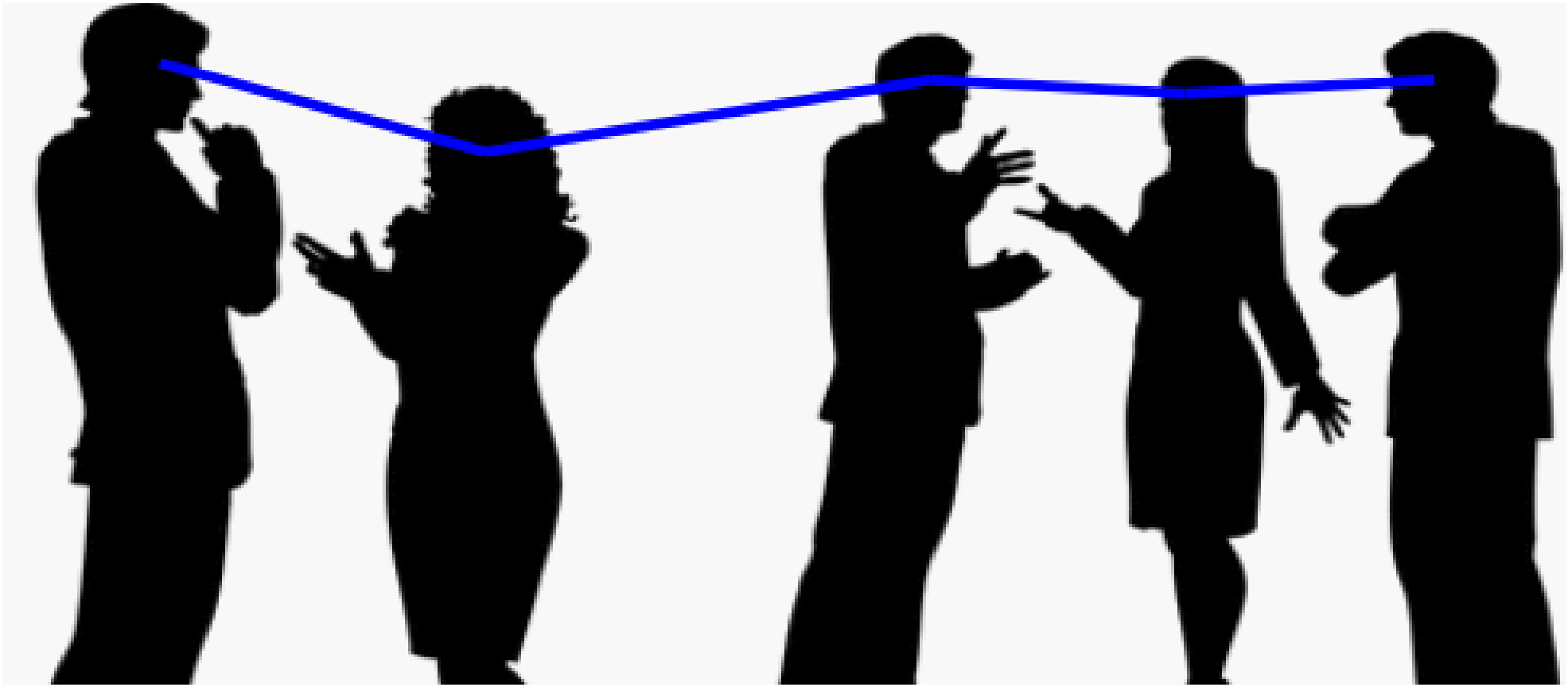
- Tóm tắt các mối đe dọa lớp mạng không dây
- Các mối đe dọa cụ thể liên quan đến định danh

MẠNG KHÔNG DÂY

Message Source

Relays / Routers

Sink / Destination



CHỨC NĂNG LỚP MẠNG

- Lớp mạng chịu trách nhiệm chính trong việc thiết lập các đường dẫn end to end và phân phối các gói tin qua chúng
- Bao gồm một số dịch vụ cơ bản:
  - ***Địa chỉ:*** *quản lý ID mạng*
  - ***Định tuyến:*** *tìm/thiết lập đường đi*
  - ***Chuyển tiếp:*** *chuyển gói tin*
  - *Tương tác với lớp Vận chuyển và lớp Liên kết/MAC*

ĐỊA CHỈ

- Trước khi có thể thực hiện định tuyến, các nút cần có ID hoặc địa chỉ
  - Các loại địa chỉ/ID từ địa phương đến toàn cầu, giống như trong hệ thống bưu chính (đường phố cho đến mã ZIP)
  - Trong các hệ thống quy mô rất lớn (ví dụ: Internet), các địa chỉ phải có một số loại cấu trúc
    - *Địa chỉ IP tuân theo một hệ thống phân cấp cụ thể và được sử dụng lại trong mỗi miền*
  - Trong một miền và trong các hệ thống quy mô nhỏ (ví dụ: MANET/WSN), các địa chỉ thường không có cấu trúc hoặc ngẫu nhiên
    - *Quản lý địa chỉ cần thiết trong một miền để ngăn trùng lặp và các tình huống lỗi khác*

GIẢI QUYẾT CÁC MỐI ĐE DỌA

- Có thể thay đổi địa chỉ tùy ý
  - Cho phép giả mạo địa chỉ
    - *Giả dạng (các) nút khác*
    - *Khả năng xảy ra một số lượng lớn các cuộc tấn công*
  - Thay đổi danh tính để tránh bị phát hiện/trừng phạt
- Kẻ tấn công có thể xâm nhập vào giao thức quản lý địa chỉ (ARP, DHCP) để gây ra sự cố
  - Gây trùng lặp địa chỉ
  - Buộc thay đổi địa chỉ thường xuyên
  - Thao tác trên các lược đồ chuyển tiếp

ĐỊNH TUYẾN

- Định tuyến = quản lý tuyến đường
  - *Định tuyến không liên quan đến việc gửi các gói thực tế từ nguồn đến (các) đích, chỉ thiết lập đường dẫn*
  - *Sống trong "mặt phẳng điều khiển"*
  - *Liên quan đến thiết lập/khám phá đường đi, bảo trì và phá bỏ*
- Những thách thức trong môi trường MANET/WSN
  - *Định tuyến sử dụng nhiều nút chuyển tiếp không đáng tin cậy*
  - *Hạn chế về nguồn lực và năng lực*
  - *Không có thẩm quyền trung tâm hoặc giám sát*
  - *Định tuyến an toàn thường dựa vào quản lý khóa hiện có*

MỐI ĐE DỌA ĐỊNH TUYẾN

- Cũng giống như các loại hành vi sai trái khác, bộ định tuyến có thể tham lam, không hợp tác hoặc độc hại
  - Các bộ định tuyến tham lam có thể từ chối các yêu cầu khám phá tuyến đường để tiết kiệm tài nguyên của chính chúng
  - Các bộ định tuyến không hợp tác có thể chọn chấp nhận có chọn lọc các yêu cầu định tuyến tới các nguồn/đích cụ thể
  - Các bộ định tuyến độc hại có thể thuyết phục các giao thức khám phá tuyến đường để các đường dẫn đi qua chúng, tránh chúng hoặc đi đường vòng không cần thiết

THU HÚT CÁC TUYẾN ĐƯỜNG

- Tấn công hố đen (Black hole):
  - Một bộ định tuyến độc hại phát tuyên bố sai về việc "gần" đích để thu hút tất cả lưu lượng truy cập và loại bỏ nó
- Tấn công lỗ xám (Gray hole):
  - Tương tự như tấn công lỗ đen, ngoại trừ nó chỉ loại bỏ một số gói tin một cách có chọn lọc
    - *Ví dụ: chuyển tiếp tất cả các gói điều khiển định tuyến nhưng loại bỏ tất cả dữ liệu*
- Tấn công worm hole:
  - Các bộ định tuyến thông đồng tạo ra một kênh ngoài băng tần đường dài có độ trễ thấp để thu hút các đường dẫn định tuyến và kiểm soát luồng dữ liệu

TÍNH TOÁN TUYẾN ĐƯỜNG

- Đường vòng:
  - *Một bộ định tuyến độc hại có thể sửa đổi/tiêm các gói điều khiển để buộc lựa chọn các tuyến phụ tối ưu*
- Đường vòng miễn phí:
  - *Các bộ định tuyến tham lam có thể tránh đi trên một tuyến đường đã chọn bằng cách quảng cáo độ trễ dài hoặc tạo "các nút ảo"*
- Có thể được coi là một hình thức tấn công Sybil, trong đó tất cả các "nhân cách" đều nằm trên đường định tuyến

TẤN CÔNG ĐỊNH TUYẾN SUBVERSION

- Danh sách đen có mục tiêu:
  - Trong bất kỳ giao thức định tuyến nào sử dụng danh sách đen, kẻ tấn công có thể buộc tội/vu khống/đổ lỗi cho người khác để buộc họ vào danh sách đen DoS
- Tấn công liên tục:
  - Kẻ tấn công có thể nhanh chóng phổ biến các yêu cầu giả mạo, khiến các yêu cầu hợp lệ sau đó bị loại bỏ

TẤN CÔNG CHUYỂN TIẾP

- Chuyển tiếp = quản lý dữ liệu điểm-điểm
  - Chuyển tiếp liên quan đến việc gửi các gói từ nguồn đến (các) đích trên các đường định tuyến đã cho
  - Sống trong "mặt phẳng dữ liệu"
  - Chuyển tiếp chính xác liên quan đến
    - *Gửi đúng gói tin*
    - *Duy trì trật tự gói tin*
    - *Tôn trọng tiêu đề và quy tắc*
    - *Chuyển tiếp kịp thời*
    - *Tôn trọng cơ chế kiểm soát tỷ giá*

CHUYỂN TIẾP MỐI ĐE DỌA

- Hành vi sai trái trong cơ chế chuyển tiếp (thường được gọi là chuyển tiếp Byzantine) bao gồm nhiều cách khác nhau để đi ngược lại các quy tắc chuyển tiếp
  - *Bỏ gói tin*
  - *Sửa đổi nội dung gói hoặc thông tin tiêu đề*
  - *Chèn các gói không có thật trên danh nghĩa của nguồn*
  - *Chuyển tiếp đến next hop sai*
  - *Không tôn trọng kiểm soát tốc độ (lũ lụt hoặc điều tiết)*

CÁC MỐI ĐE DỌA VỀ QUYỀN RIÊNG TƯ CỦA MẠNG

- Các giao thức định tuyến tiết lộ thông tin cho những kẻ nghe trộm tò mò/ác ý
  - Kẻ tấn công có thể lắng nghe các tương tác khám phá tuyến đường và tìm hiểu (1) vị trí của các nút nguồn và đích, (2) tương tác giữa các nút, (3) đường dẫn thường được sử dụng, (4) sự kiện mạng hoặc (5) dữ liệu
  - Đây là tất cả các vấn đề về quyền riêng tư của vị trí, quyền riêng tư của mạng và quyền riêng tư của dữ liệu do quá trình định tuyến
- Hãy xem xét chi tiết các mối đe dọa khác nhau này, bắt đầu bằng việc giải quyết

ĐỊNH ĐỊA CHỈ

- Trong mạng truyền thống, mỗi thiết bị (đài) có hai danh tính, dưới dạng địa chỉ
  - Địa chỉ MAC: địa chỉ phần cứng của radio cần thiết cho truyền thông lớp liên kết (ví dụ: 802.3, 802.11)
- Mã hóa cứng vào NIC
- Về lý thuyết, duy nhất và tĩnh
  - Địa chỉ IP: địa chỉ lớp mạng dùng để định tuyến và một số dịch vụ khác ở lớp cao hơn
- • Địa chỉ phần mềm ảo

ĐỊA CHỈ MAC

- Địa chỉ MAC trên Internet
  - Ethernet và WiFi sử dụng địa chỉ MAC để giao tiếp lớp liên kết
  - Độc lập với chức năng lớp cao hơn
  - Các khung lớp liên kết mang địa chỉ MAC nguồn và đích (mỗi khung 6B)
- Địa chỉ MAC trong các hệ thống khác
  - Không thường được sử dụng trong các mạng cảm biến do chi phí cao
  - Không cần thiết nếu địa chỉ khác có sẵn

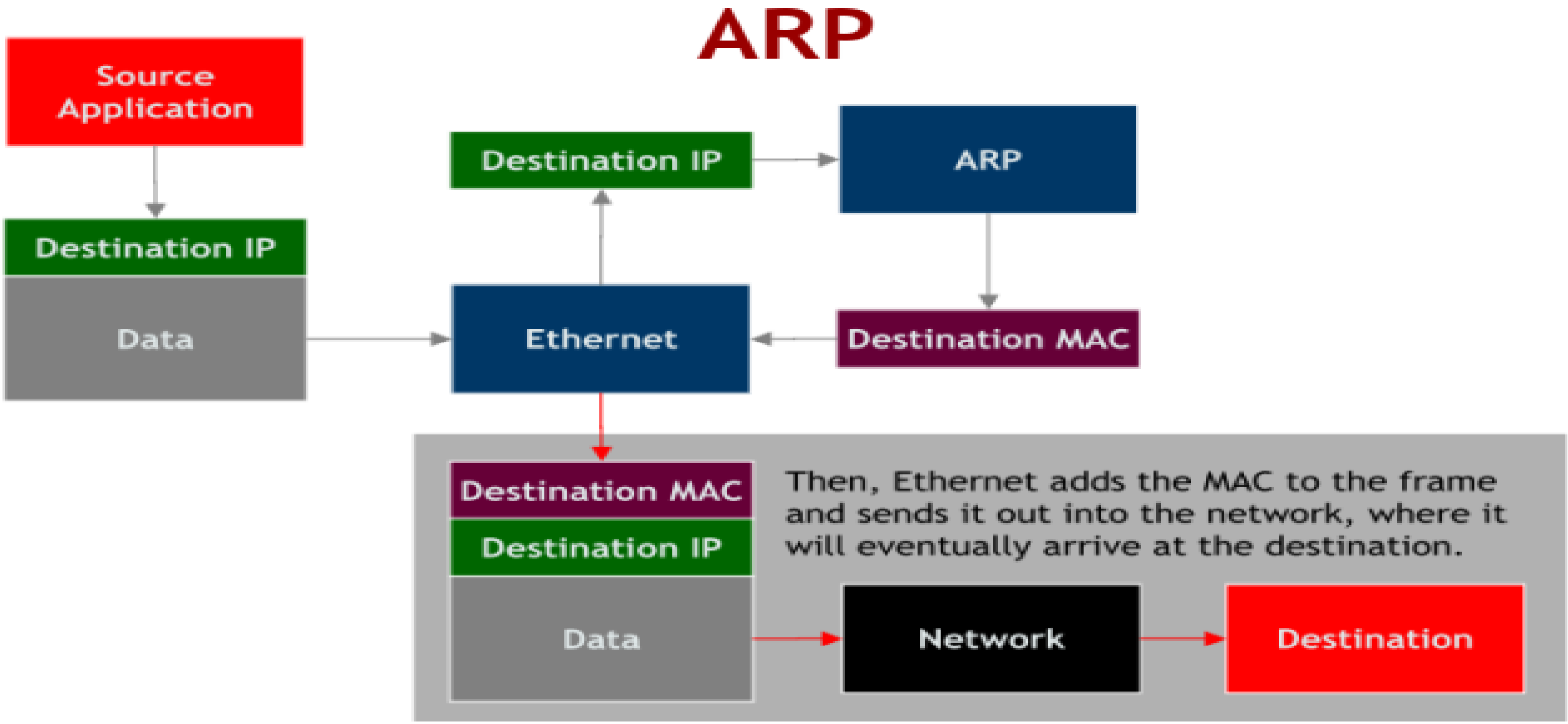
CÁC ĐỊA CHỈ IP

- Địa chỉ IP trên Internet
  - *Lớp mạng trở lên sử dụng địa chỉ IP cho một số mục đích nhận dạng*
  - *Không phụ thuộc vào bất cứ thứ gì bên dưới lớp mạng*
  - *Địa chỉ IP phải là duy nhất*
- Địa chỉ IP trong các hệ thống khác
  - *Để hỗ trợ các ứng dụng phổ biến, hầu hết các nhà thiết kế đều hướng đến việc hỗ trợ địa chỉ IP (ở một mức độ nào đó)*

PHÂN GIẢI ĐỊA CHỈ IP

- Trong hầu hết các miền Internet, địa chỉ IP được gán tập trung bằng DHCP và được liên kết với địa chỉ MAC bằng ARP
  - DHCP = Dynamic Host Configuration Protocol: host yêu cầu server cung cấp địa chỉ IP mà nó giữ cho đến khi hết hạn
  - ARP = Address Resolution Protocol: host hỏi các host khác địa chỉ MAC tương ứng với địa chỉ IP

ARP


ARP
Source Application
Destination IP
Data
Destination IP
ARP
Ethernet
Destination MAC
Destination MAC
Destination IP
Data
Then, Ethernet adds the MAC to the frame and sends it out into the network, where it will eventually arrive at the destination.
Network
Destination

HẠN CHẾ

- Địa chỉ MAC không còn bị ràng buộc bởi phần cứng
  - Hầu hết các hệ thống giống như Linux đều cho phép phần mềm thay đổi địa chỉ MAC được sử dụng, mặc dù địa chỉ MAC được mã hóa cứng
  - Nhiều thiết bị không có địa chỉ MAC (duy nhất)
- DHCP không thực tế đối với các hệ thống phân tán
  - Yêu cầu tập trung
  - Chi phí cao trong các hệ thống động
- ARP có chi phí cao trong các hệ thống phân tán
  - Yêu cầu tràn ngập yêu cầu

ĐỊA CHỈ PHÂN TÁN

- **Vấn đề:** Làm cách nào để xác định địa chỉ IP (hoặc danh tính phù hợp khác) trong một hệ thống phân tán sao cho:
  - *Địa chỉ nhỏ gọn (có thể) để liên lạc chi phí thấp trong các cảm biến hoặc thiết bị nhúng*
  - *Chi phí mạng (tương đối) thấp*
  - *Địa chỉ là (đủ) duy nhất*
  - *Hệ thống có thể tách và nối*
- Địa chỉ trùng lặp có thể được phát hiện và sửa chữa
- Không gian địa chỉ đủ lớn và động

MỘT VÀI CÁCH TIẾP CẬN

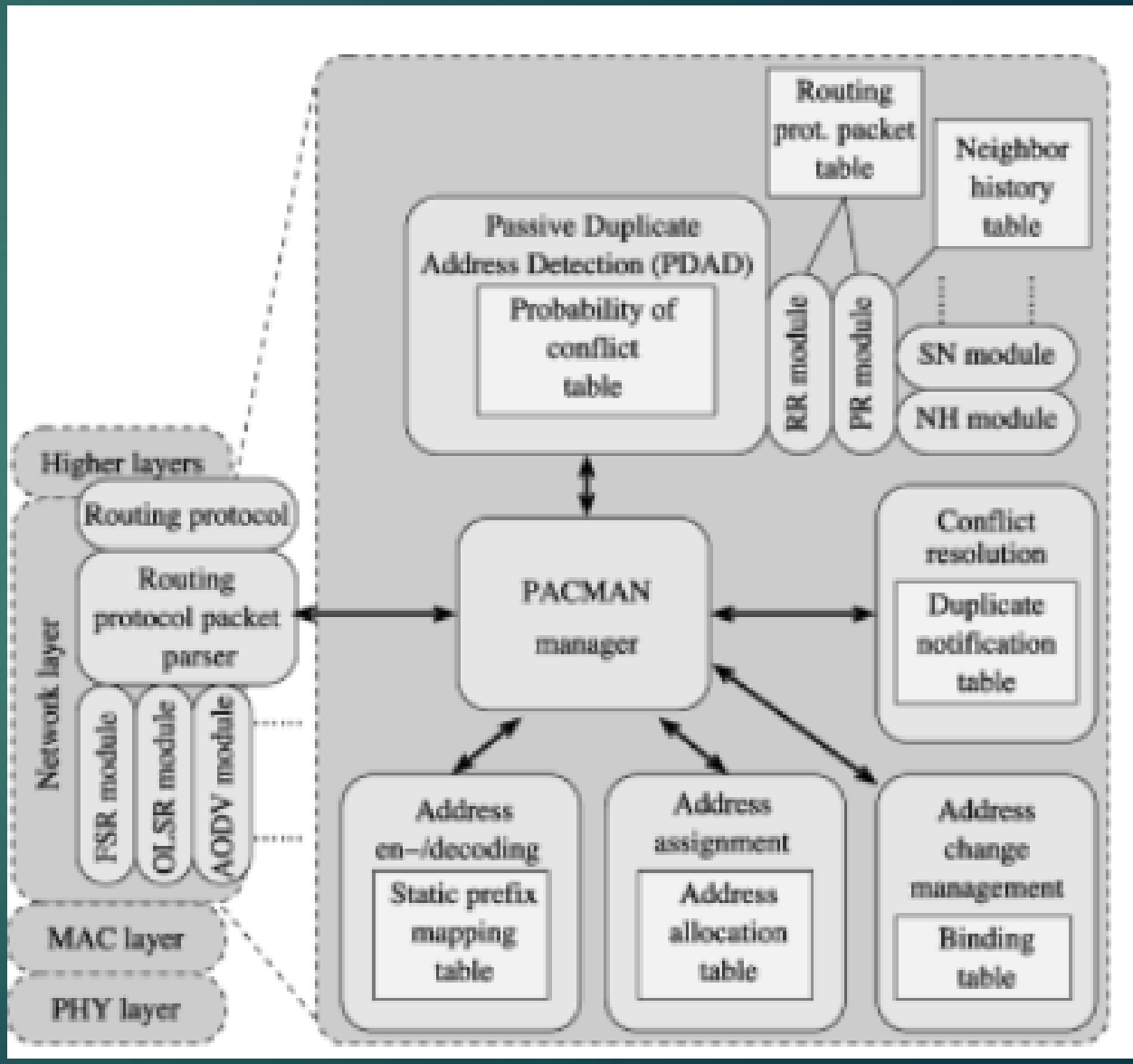
- Lựa chọn ngẫu nhiên với phát hiện địa chỉ trùng lặp (DAD)
  - *Gửi truy vấn đến địa chỉ đã chọn; nếu không có phản hồi, địa chỉ có thể không xung đột*
  - *Yêu cầu lan truyền một truy vấn qua toàn bộ mạng*
  - *Hợp nhất các mạng hiện có là khó khăn*
- MANETconf
  - *Cấu hình nút "khởi tạo" hoạt động giống như một máy chủ có thể gán địa chỉ cho "người yêu cầu" đến sau*
  - *Cấu hình thông báo các nút bị ngập và gán địa chỉ nếu không có nút nào phản hồi tiêu cực*
  - *Hợp nhất các mạng hiện có là khó khăn*

PACMAN

- PACMAN = Cấu hình Tự động Thụ động cho Mạng Ad hoc Di động
  - Kiến trúc cho cấu hình tự động địa chỉ MANET phân tán hiệu quả

PACMAN

- PACMAN = Cấu hình Tự động Thụ động cho Mạng Ad hoc Di động
  - Kiến trúc cho cấu hình tự động địa chỉ MANET phân tán hiệu quả

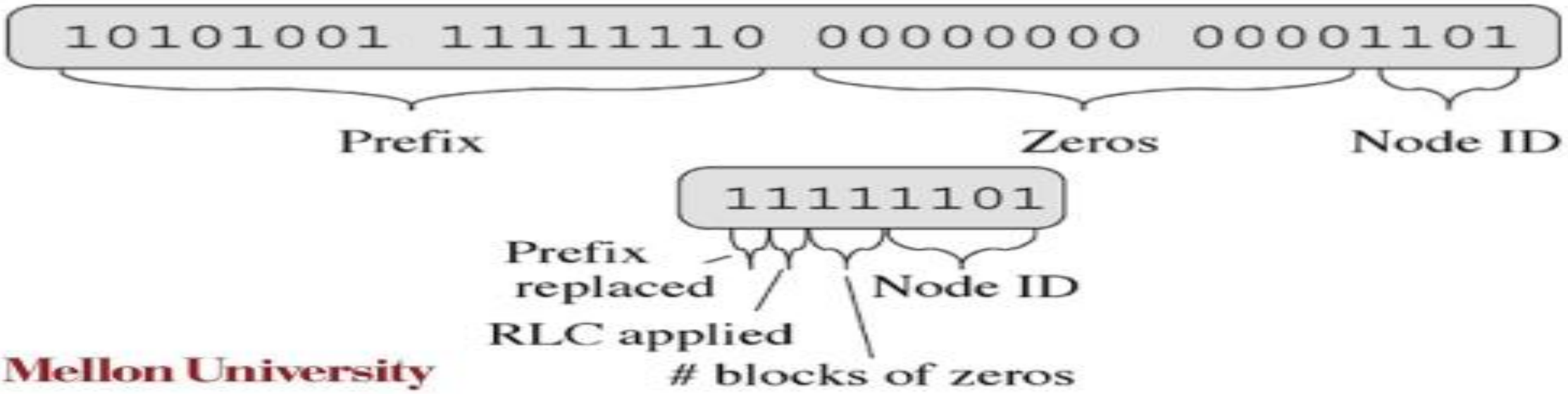


CHỈ ĐỊNH ĐỊA CHỈ

- Để tránh làm tràn mạng để kiểm tra tính duy nhất của địa chỉ, PACMAN chỉ định địa chỉ một cách thụ động và dựa vào mạng để phát hiện xung đột
  - Mỗi nút chọn địa chỉ của mình bằng thuật toán xác suất và danh sách các địa chỉ đã sử dụng

MÃ HÓA ĐỊA CHỈ

- Để giảm thiểu chi phí hoạt động, PACMAN mã hóa địa chỉ IP MANET
  - MANET sử dụng tiền tố IP cố định (2B cho IPv4, 8B cho IPv6)
  - ID nút chỉ cần $\log_2 N$ bit để hỗ trợ N nút
  - Pad có nhiều số 0 nhưng chỉ cần biết số #0s



DAD THỤ ĐỘNG

- PDAD dựa trên quan sát các sự kiện:
  - Không bao giờ xảy ra trường hợp địa chỉ duy nhất mà luôn xảy ra trường hợp trùng địa chỉ
    - *ví dụ: nhận phản hồi tuyến đường khi không có yêu cầu nào được gửi*
  - Thường không xảy ra trường hợp địa chỉ duy nhất nhưng đôi khi xảy ra trường hợp trùng địa chỉ
    - *ví dụ: trạng thái liên kết trong phản hồi tuyến đường thay đổi hoàn toàn*
- Khi phát hiện sự trùng lặp, ít nhất một nút có thể khởi tạo lại việc gán địa chỉ
  - Điều này cũng cho phép quản lý tương đối dễ dàng các sự kiện tách và hợp nhất mạng

VẤN ĐỀ BẢO MẬT

- PACMAN và nhiều cách tiếp cận tương tự không được thiết kế với các hành vi nguy hiểm
- Các mối đe dọa [Wang và cộng sự, 2005]:
  - **Giả mạo địa chỉ -** kẻ tấn công giả mạo địa chỉ IP của nạn nhân và chiếm đoạt lưu lượng mạng
  - **Xung đột địa chỉ -** kẻ tấn công đưa các thông báo (hoặc sự kiện) xung đột vào mục tiêu tấn công
  - **Hết địa chỉ -** kẻ tấn công yêu cầu nhiều địa chỉ để từ chối dịch vụ hoặc ngăn các nút tham gia
  - **Phản hồi phủ định -** trong trường hợp cần có sự chấp thuận để tham gia, kẻ tấn công có thể ngăn không cho các nút tham gia

TỰ ĐỘNG XÁC NHẬN MANET AN TOÀN

- Liên kết địa chỉ IP với khóa chung để xác thực quy trình cấu hình tự động
  - Nút A mới chọn một địa chỉ IP làm hàm băm của khóa công khai
  - A gửi một truy vấn tới mạng cho địa chỉ IP bằng cách sử dụng Thăm dò địa chỉ trùng lặp đã được xác nhận, tem thời gian
    - *Nếu nút nhận B có xung đột IP, nó sẽ kiểm tra chữ ký (tính xác thực, ngăn phát lại, v.v.) và trả lời có điều kiện bằng Thông báo xung đột địa chỉ được ký, đánh dấu thời gian*
    - Nếu A nhận được ACN từ B, nó sẽ kiểm tra chữ ký và bắt đầu lại theo điều kiện bằng một cặp khóa mới
    - Nếu không trả lời trong một khoảng thời gian cố định, A sẽ tham gia mạng bằng địa chỉ IP được tạo

LỢI ÍCH CỦA PHƯƠNG PHÁP TIẾP CẬN

- Buộc kẻ tấn công tìm khóa công khai để băm địa chỉ IP của nạn nhân trước khi khởi động cuộc tấn công
  - *Ngay cả với không gian địa chỉ tương đối nhỏ, chi phí tính toán/lưu trữ vẫn bị hạn chế*

Tự động cấu hình dựa trên sự tin cậy - Trust-Based Auto-Conf

- Hành vi sai trái trong mô hình “requester - initiator” (MANETconf)
  - Người khởi tạo có thể cố ý gán địa chỉ xung đột
  - Người yêu cầu có thể lặp đi lặp lại nhiều yêu cầu, gây cạn kiệt tài nguyên và/hoặc DoS
  - Các nút độc hại có thể tuyên bố sai rằng các địa chỉ ứng cử viên đã được sử dụng, gây ra quá nhiều yêu cầu, cạn kiệt tài nguyên và DoS
- Thay vì dựa vào các nút tùy ý, hãy theo dõi xem nút nào “tốt” và nút nào “xấu”

MÔ HÌNH TIN CẬY

- Đối với các nút A và B, sự tin tưởng của A vào B được đưa ra bởi $T_A(B)$
- Mỗi nút A có một giá trị ngưỡng tin cậy T_A^* sao cho nó sẽ chỉ tương tác với B nếu $T_A(B) > T_A^*$
- Giá trị niềm tin có thể được tính toán dựa trên các hành vi trong quá khứ

CHỌN MỘT INITIATOR ĐÁNG TIN CẬY

- Người yêu cầu mới N phát một Neighbor_Query với ngưỡng T_N^*
- Mỗi người nhận gửi cho N một câu trả lời InitREP với hàng xóm ID có giá trị tin cậy >= T_N^*
- N có thể chọn bộ khởi tạo của nó là hàng xóm xuất hiện trong nhiều bản tin InitREP nhất
- Một nút độc hại khó có thể được chọn trừ khi phần lớn các nút lân cận đều độc hại

KIỂM TRA ĐỊA CHỈ TRÙNG LẶP

- Nếu bộ khởi tạo A nhận được thông báo Add_Collision từ nút B để phản hồi Initiator_Request:
  - Nếu B đã từng nằm trong danh sách đen thì bỏ qua
  - Nếu $T_A(B) > T_A^*$ thì tin B và làm lại từ đầu
  - Nếu không, tuyên bố B là độc hại, thêm B vào danh sách đen và gửi thông báo Malicious_Suspect về B đến các nút khác
    - Các nút khác chỉ tin vào thông báo Malicious_Suspect của A nếu giá trị tin cậy của chúng trong A đủ cao

KIỂM TRA TRÙNG LẶP CỦA BÊN THỨ 3

- Nếu nút B phát hiện xung đột địa chỉ giữa hai nút khác, nó sẽ thông báo cho cả hai
- Nếu nút nhận A nhận được thông báo như vậy từ nút B:
  - Nếu B đã từng nằm trong danh sách đen thì bỏ qua
  - Nếu $T_A(B) >= T_A^*$ thì tin B và chọn địa chỉ mới
- - Còn không thì thêm B vào blacklist

TÍNH GIÁ TRỊ TIN CẬY

- A tính toán độ tin cậy của mình với B bằng cách:
  - Theo dõi và đo lường một số đặc điểm hiệu suất, bao gồm các hành vi trong quá khứ trong việc gán địa chỉ
  - Mỗi đặc trưng ánh xạ tới một giá trị trong [0,1]
  - Độ Tin cậy $T_A(B)$ là sự kết hợp có trọng số của các giá trị theo đặc điểm khác nhau
- Đối với các nút ở xa B, A phải dựa vào việc thiết lập đường dẫn tin cậy đến

TÓM TẮT

- Thảo luận về địa chỉ phân tán, các mối đe dọa và một vài cách tiếp cận để bảo mật cấu hình tự động
  - PACMAN: Tự động cấu hình thụ động cho MANET
    - [Weniger; JSAC 2005]
  - Tự động cấu hình địa chỉ an toàn cho MANET
    - [Wang, Reeves và Ning; MobiQuitous 2005]
  - Bảo mật cấu hình tự động trong MANET bằng sự tin cậy
    - [Hu và Mitchell; MSN 2005]

BÀI 11:

BẢO MẬT ĐỊNH TUYẾN VÀ CHUYỂN TIẾP