BÀI #13 - QUYỀN RIÊNG TƯ & ẨN DANH CỦA MẠNG

TS. HOÀNG SỸ TƯƠNG

BÀI #13

- Rủi ro về tính riêng tư ở lớp mạng không dây
- Một số cách tiếp cận khác nhau trong các hệ thống/kịch bản khác nhau

CÁC VẤN ĐỀ VỀ QUYỀN RIÊNG TƯ CỦA MẠNG

- Tương tác lớp mạng trong mạng không dây thường để lộ thông tin về danh tính, ngữ cảnh, nội dung, mối quan hệ, v.v.
- Trong một số trường hợp, các biện pháp bảo vệ bằng mật mã có thể hữu ích, nhưng không phải lúc nào cũng đảm bảo tính an toàn cho mạng
- Trong một số trường hợp, bút danh là hữu ích, nhưng không phải lúc nào cũng đúng

ĐỐI SÁNH ID

- ID/địa chỉ mạng có thể hỗ trợ theo dõi, lập hồ sơ, tham chiếu, v.v.
  - *Ví dụ:* nhà cung cấp dịch vụ mạng thấy thiết bị A kết nối với mạng ở Pgh, sau đó đến mạng khác ở DC, rồi đến mạng khác ở SF dẫn đến nhà cung cấp dịch vụ có thể tạo hồ sơ của chủ sở hữu thiết bị
  - *Ví dụ:* kẻ nghe trộm nhìn thấy thiết bị A hiển thị và kết nối với mạng vào cùng một thời điểm mỗi ngày dẫn đến kẻ nghe trộm có thể lập hồ sơ tạm thời cho người dùng để biết khi nào họ sẽ vắng nhà

PHÂN TÍCH LƯU LƯỢNG TRUY CẬP

- Một bên tò mò hoặc mã độc có thể quan sát lưu lượng mạng và phân tích các mẫu lưu lượng để suy ra các mối quan hệ
  - ID ở dạng bản rõ có thể thực hiện việc này khá dễ dàng
  - Một cái gì đó như "bảo tồn dòng chảy" có thể cho phép tách dòng giao thông
  - Khả năng suy luận phụ thuộc vào một số yếu tố:
    - Khả năng hiển thị mạng - chế độ xem toàn cầu hay cục bộ?
    - Mật độ giao thông - phân bố giao thông dày đặc hay thưa thớt?
    - ……

PHÂN TÍCH THỜI GIAN

- Vì các hoạt động của mạng thường nhạy cảm với độ trễ, nên có mối tương quan giữa các sự kiện truyền tải.
  - *Ví dụ:* nút A truyền 10 gói, nút bên cạnh B truyền 10 gói có kích thước tương tự, có thể B đang chuyển tiếp lưu lượng của A
  - Tùy thuộc vào khả năng hiển thị và mật độ, rất ít thông tin khác là cần thiết (ví dụ: mã hóa lại gói hop-by-hop mạnh không ngăn cản phân tích thời gian)
  - ...

HIỂU VỀ RỦI RO

- Loại mạng nào? Dịch vụ?.....?
  - *WLAN, mạng xe di động, VANET, WSN, ...*
- Mục tiêu/mục đích của kẻ tấn công là gì?
  - *Theo dõi thời gian thực, khôi phục dấu vết quá khứ,...*
  - *Trộm cắp, an toàn cá nhân, tống tiền, tiếp thị xấu, giám sát,*
- Mức độ chi tiết nào là cần thiết để tấn công thành công?
  - *Quan hệ, vị trí cụ thể, khu vực cụ thể, ...*

THÁCH THỨC VỀ QUYỀN RIÊNG TƯ

- Hiểu các mục tiêu về quyền riêng tư
  - *Cái gì cần được bảo vệ?*
  - *Các quy tắc phải được thực thi là gì?*
- Hiểu mối đe dọa
  - *Mục tiêu, khả năng, phương pháp,... của kẻ tấn công là gì?*
  - *Tính thực tế của các giả định của kẻ tấn công?*
- Đo lường (Metrics)
  - *Làm thế nào để đo lường bảo vệ và thực thi quyền riêng tư?*
  - *Làm thế nào để đánh giá và kết hợp rủi ro?*

MỐI QUAN TÂM VỀ QUYỀN RIÊNG TƯ KHÁC NHAU

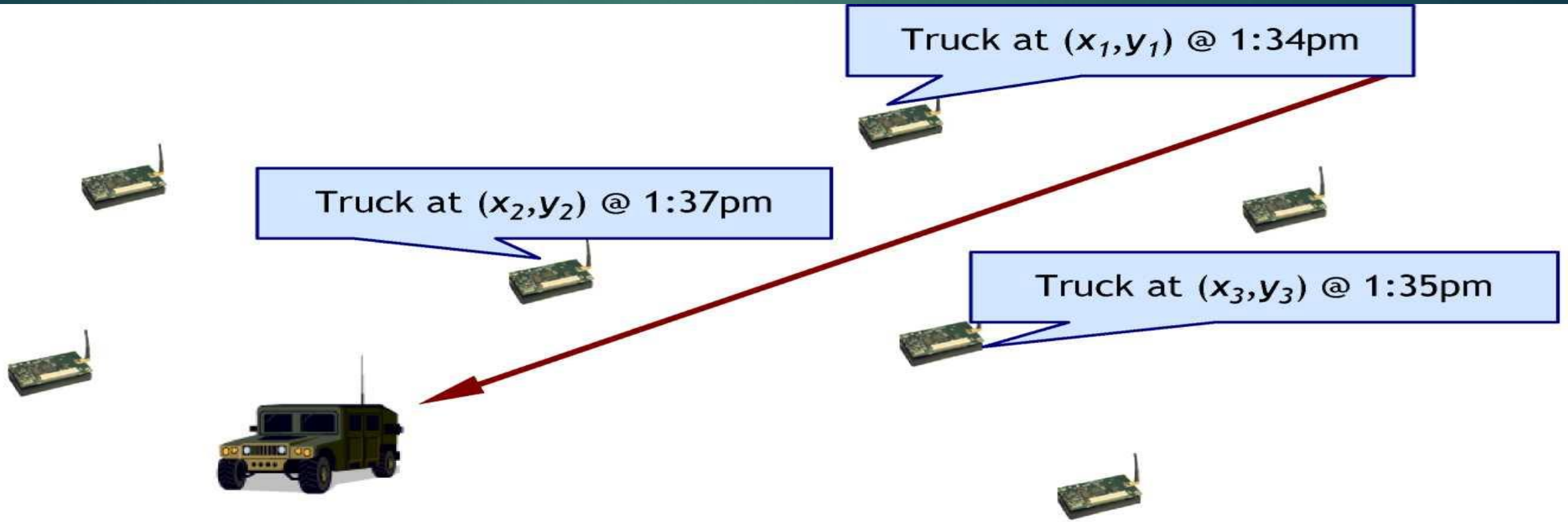
- Lập hồ sơ và theo dõi người dùng WiFi
  - *Điều này sẽ được đề cập ở phần tiếp theo*
- Suy luận sự kiện/đối tượng trong WSN
- Theo dõi người dùng/ô tô trái phép trong VANET

ẨN DANH LƯU LƯỢNG

- Trong các mạng nhiều bước nhảy (MANET/WSN), liên kết truyền dẫn có thể cho biết đường dẫn nào được sử dụng cho một phiên
  - Phân tích lưu lượng truy cập:
    - *Phân tích luồng gói tin thông qua mạng (với kiến thức toàn cầu) cho phép phân tách thành các luồng riêng lẻ*
  - Phân tích lưu lượng truy cập cục bộ:
    - *Nếu không có kiến thức tổng thể, thông tin về thời gian có thể làm lộ sự phân tách luồng trong một vùng lân cận*

QUYỀN RIÊNG TƯ CỦA VỊ TRÍ WSN

- Trong các mạng cảm biến, chúng ta thường không quan tâm đến việc bảo vệ các vị trí cảm biến, nhưng những gì chúng cảm nhận được có thể rất nhạy cảm



QUYỀN RIÊNG TƯ VỊ TRÍ NGUỒN

- Một trong những mục tiêu phổ biến trong WSN là che giấu vị trí của sự kiện được cảm nhận khỏi người quan sát
  - Tuy nhiên, lưu lượng truy cập được tạo sẽ ngay lập tức hiển thị bất kỳ sự kiện đơn lẻ nào
  - Thường được gọi là "Vấn đề thợ săn gấu trúc (Panda Hunter)"
    - *Cảm biến trong khu vực động vật hoang dã được sử dụng để theo dõi/nghiên cứu gấu trúc*
    - *Bất cứ khi nào một con gấu trúc đi ngang qua một cảm biến, nó sẽ tạo ra lưu lượng truy cập*
    - *Một thợ săn có thể theo dõi lưu lượng để tìm gấu trúc*

VẤN ĐỀ THỢ SĂN GẤU TRÚC (PANDA HUNTER)

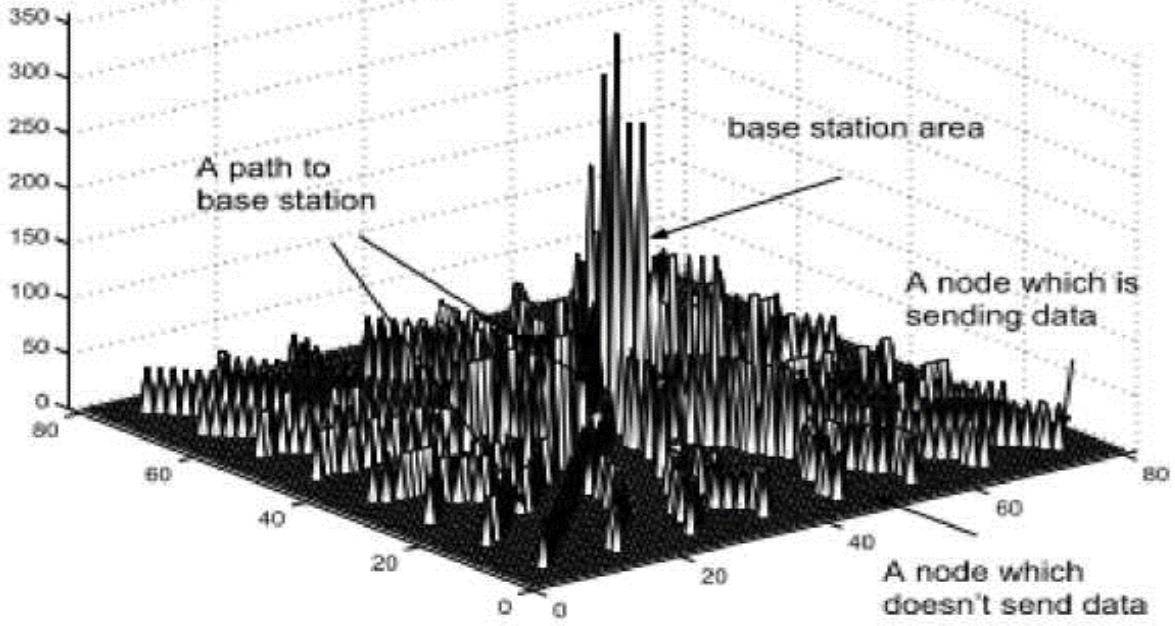
- Mục tiêu của WSN / phòng thủ:
  - Thu thập chính xác / nhanh chóng thông tin di chuyển của gấu trúc
  - Ẩn thông tin vị trí khỏi những kẻ săn gấu trúc có thể nghe lén lưu lượng WSN nhưng không giải mã được
- Mục tiêu của thợ săn gấu trúc:
  - Tìm hiểu vị trí của nguồn dữ liệu (gấu trúc) bằng cách phân tích thống kê lưu lượng truy cập

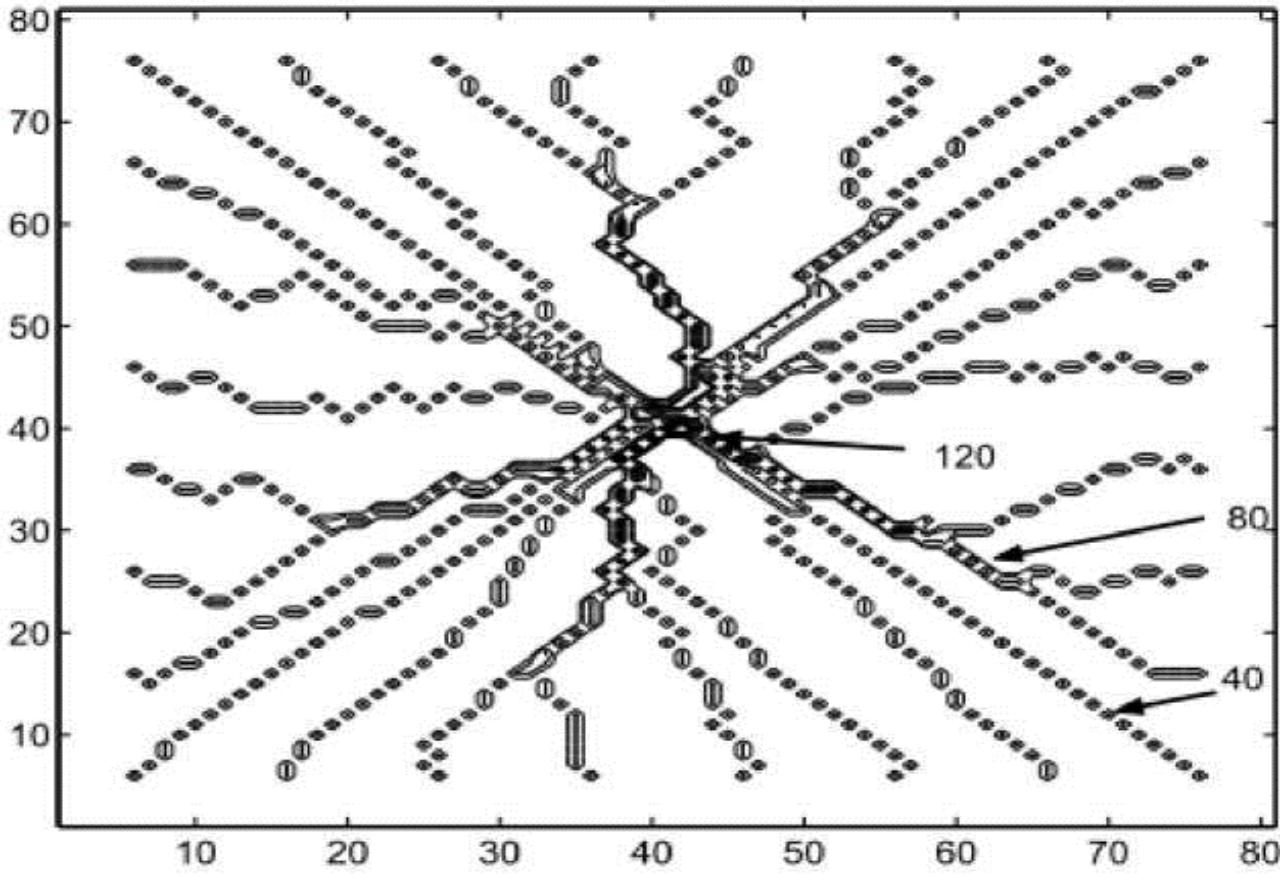
CHIẾN LƯỢC THỢ SĂN GẤU TRÚC

- Hai cách tiếp cận:
  - Chọn một vị trí trong mạng để theo dõi lưu lượng
    - *Đợi gấu trúc đi đâu đó tạo ra luồng lưu thông qua vị trí đã chọn, sau đó tìm gấu trúc*
    - *Có lẽ sẽ mất nhiều thời gian tùy thuộc vào khu vực, nhưng tốt hơn so với săn bắn ngây thơ*
  - Tìm trạm gốc và giám sát tất cả lưu lượng mạng
    - *Cần nhiều công việc hơn để tìm trạm cơ sở và nhiều lưu lượng truy cập hơn để phân tích tất cả cùng một lúc, nhưng bất kỳ lưu lượng truy cập nào liên quan đến gấu trúc đều có ở đây*

PHƯƠNG PHÁP CHỐNG PHÂN TÍCH

- Trong bối cảnh của Panda Hunter, có hai cách để giảm thiểu cuộc tấn công:
  - *Ngăn thợ săn tìm trạm cơ sở (nghĩa là quyền riêng tư của vị trí đích)*





LÀM NGẬP LỤT

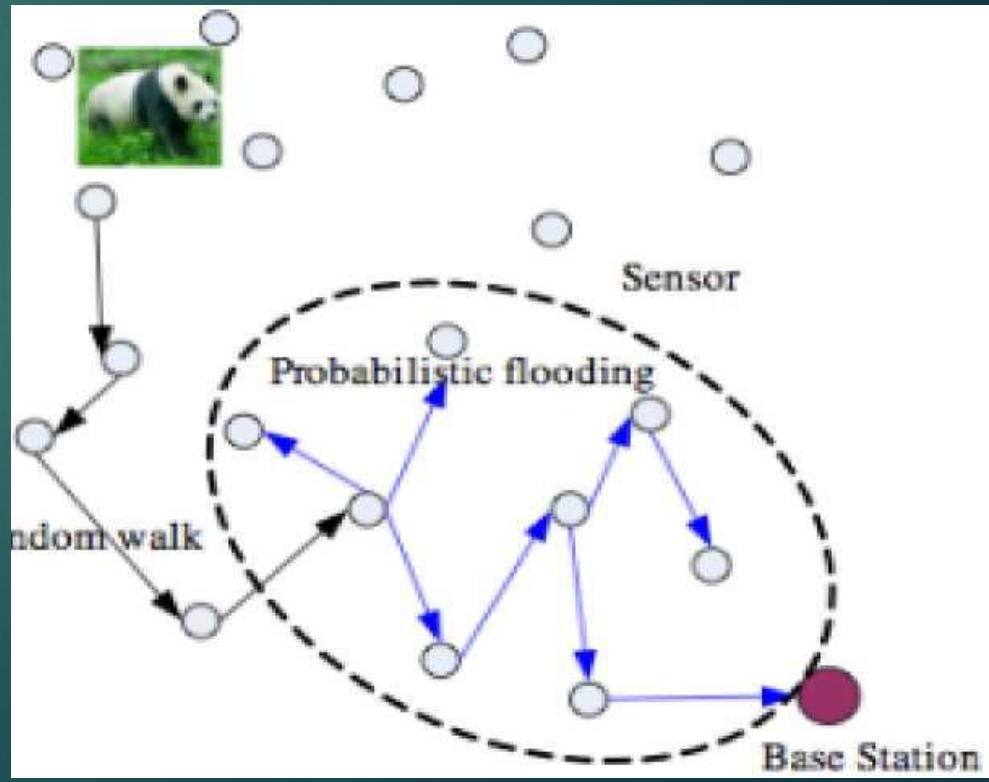
- Một cách tiếp cận phổ biến là ẩn dữ liệu sự kiện thực tế trong lưu lượng truy cập giả (“chaff”)
  - Làm ngập mạng với lưu lượng giả ngăn kẻ tấn công tìm ra đâu là thông tin thật
    - *Nếu có vẻ như gấu trúc ở khắp mọi nơi, thì nó ở đâu?*
  - Tất nhiên, ngập lụt lưu lượng mạng giả là rất nhiều công việc cho rất ít phần thưởng

XÁC SUẤT NGẬP LỤT

- Có thể thực hiện sự đánh đổi giữa chi phí ngập lụt và tính riêng tư của vị trí thu được bằng cách hướng dẫn mỗi nút chỉ chuyển tiếp lưu lượng giả với xác suất P
  - Ít lưu lượng truy cập giả làm giảm nhẹ quyền riêng tư
  - Lưu lượng truy cập giả ít hơn có nghĩa là chi phí thấp hơn
  - Các nút cần có khả năng phân biệt lưu lượng giả với lưu lượng thực hoặc cũng có thể giảm lưu lượng thực w.p. (1-p)

ĐỊNH TUYẾN NGẪU NHIÊN

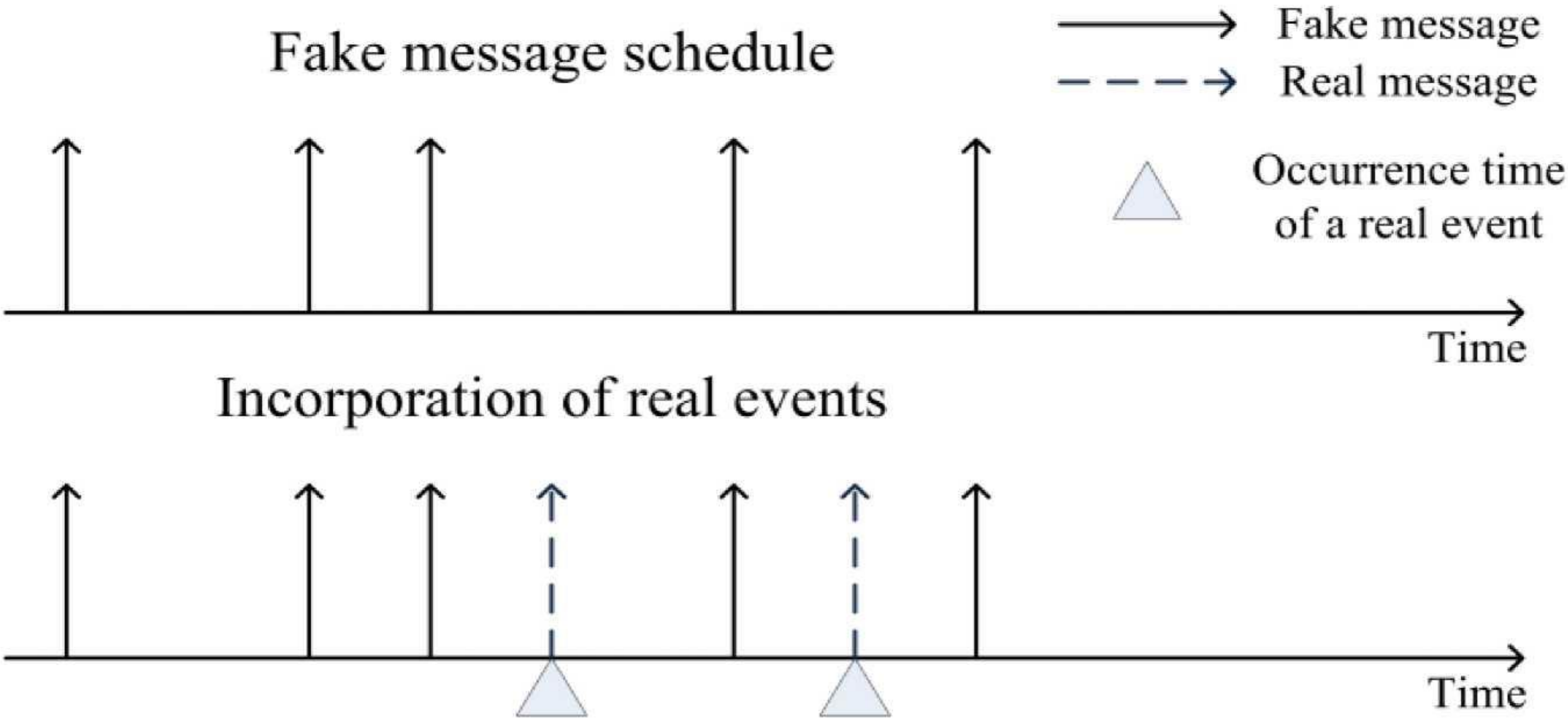
- Một kỹ thuật khác để giảm thiểu phân tích lưu lượng là định tuyến ngẫu nhiên
  - Bước nhảy tiếp theo rand({neigbors})
  - Luồng gói tin không xác định làm cho việc phân tích khó khăn hơn nhưng lại làm tăng độ trễ c
- Có thể kết hợp định tuyến ngẫu nhiên với prod ngập lụt R
  - Định tuyến ảo:



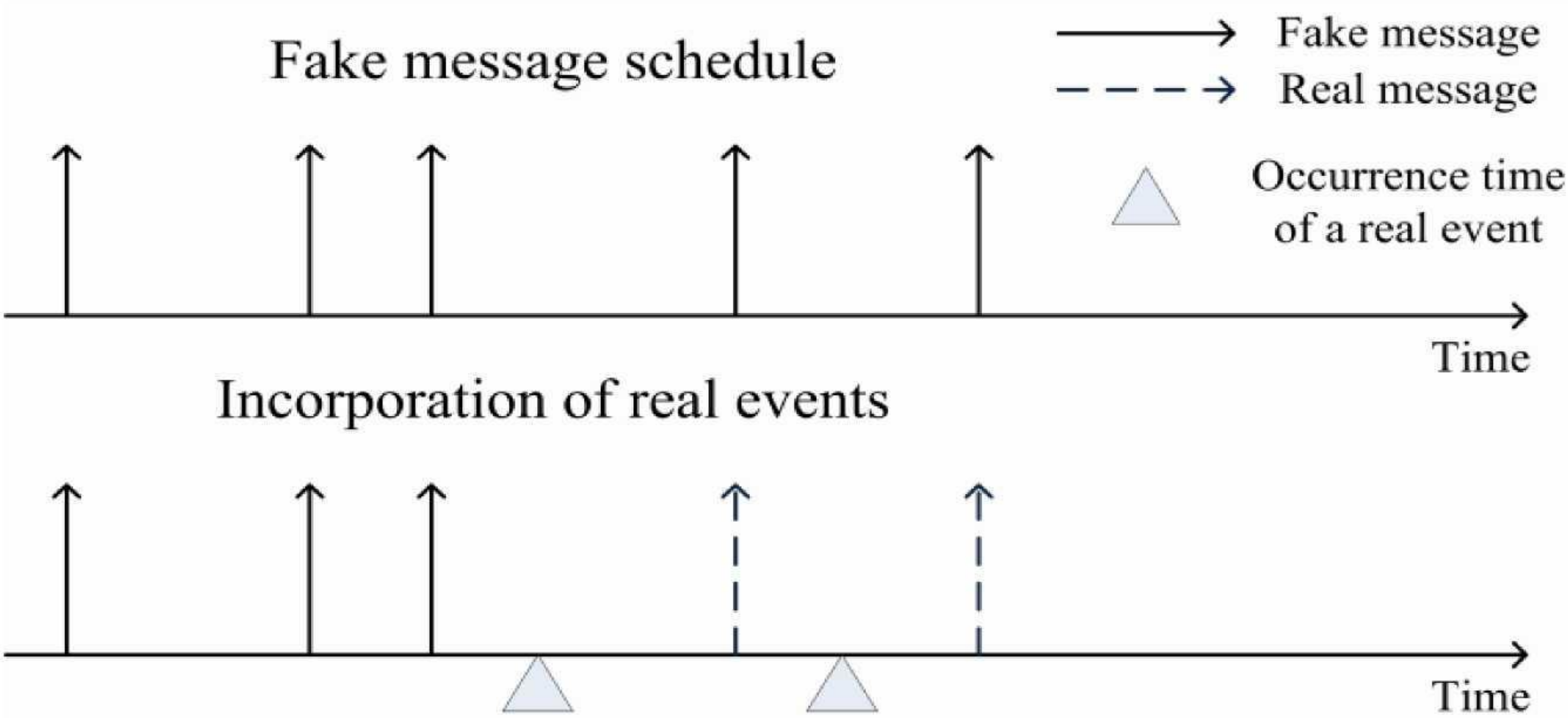
TƯƠNG QUAN TRUYỀN DẪN

- Để làm cho mọi việc trở nên khó khăn hơn, kẻ tấn công có thể phân tích thời gian tại một nút để tiếp tục phân tách các luồng tại một điểm
  - Trình tự truyền của hai nút lân cận có thể chỉ ra dữ liệu truyền lại trên cùng một đường dẫn
  - Hỏi: làm thế nào để các lần truyền lại không tương quan về mặt thống kê với các lần truyền ban đầu?
    - (ví dụ: [Alomair et al., Globecom 2010])

CÁCH TIẾP CẬN ĐƠN GIẢN

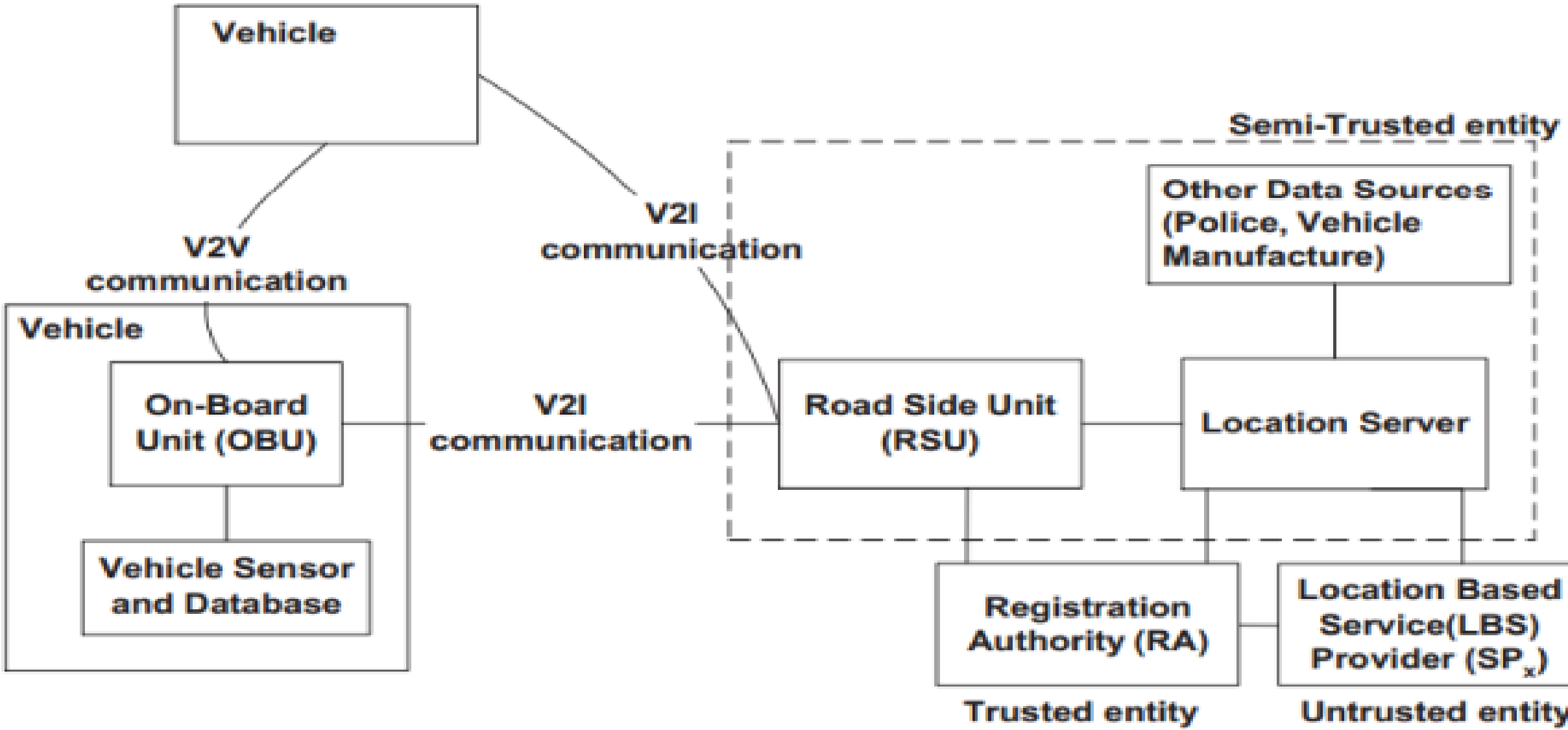


CÁCH TIẾP CẬN TỐT HƠN



CÒN VẤN ĐỀ VỀ QUYỀN RIÊNG TƯ VỊ TRÍ TRONG MẠNG DI ĐỘNG (VÍ DỤ: ANDNET) THÌ SAO?

LBS TRONG VANET



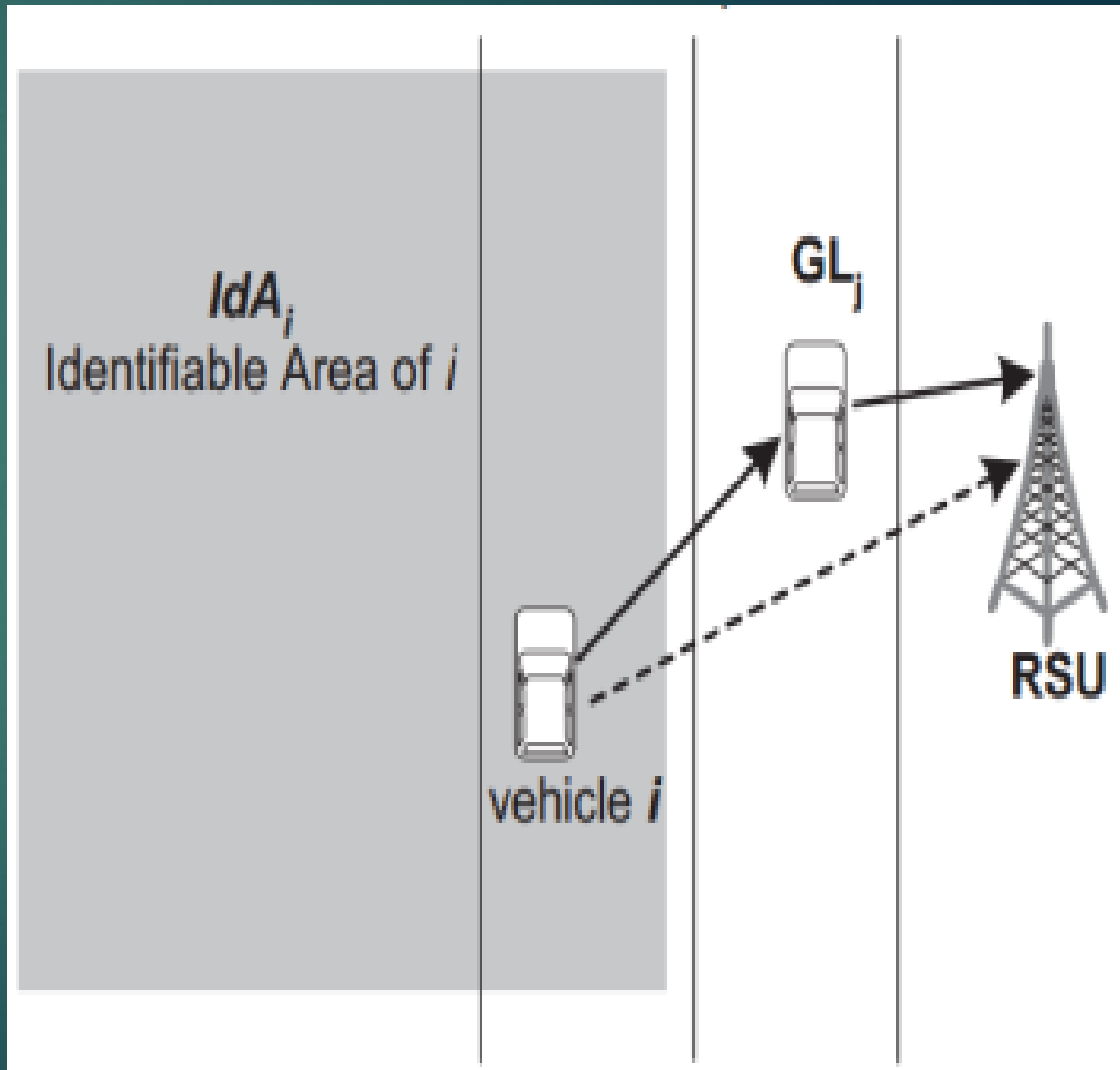
LÀM CÁCH NÀO ĐỂ NGĂN LBS KHÔNG ĐÁNG TIN CẬY THEO DÕI PHƯƠNG TIỆN?

AMOEBA

- Biệt danh + nhóm xác định vị trí riêng tư giữa các phương tiện trên đường cao tốc
  - Các nhóm tăng tính ẩn danh và giảm khả năng liên kết
  - Cập nhật bút danh và im lặng vào thời điểm thích hợp càng làm giảm khả năng liên kết
  - Điều khiển nguồn cho phép liên lạc nhóm mà không bị cơ sở hạ tầng nghe trộm

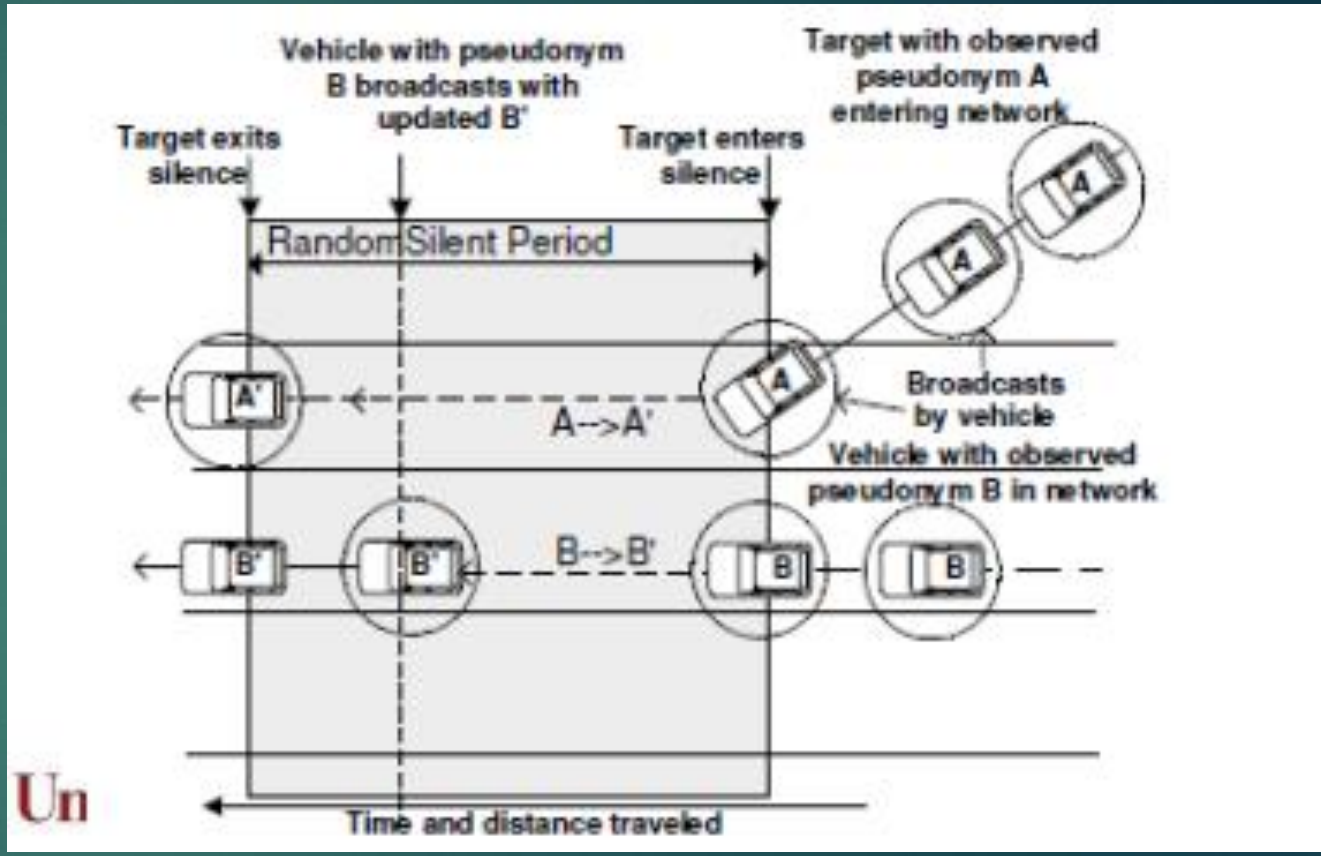
V2I - G2I

- Bảo vệ ẩn danh bằng cách nhóm lưu lượng truy cập mạng
  - Cho phép các phương tiện thành lập các nhóm đặc biệt
  - Trưởng nhóm trao đổi với RSU
  - Xoay vòng trưởng nhóm ngẫu nhiên

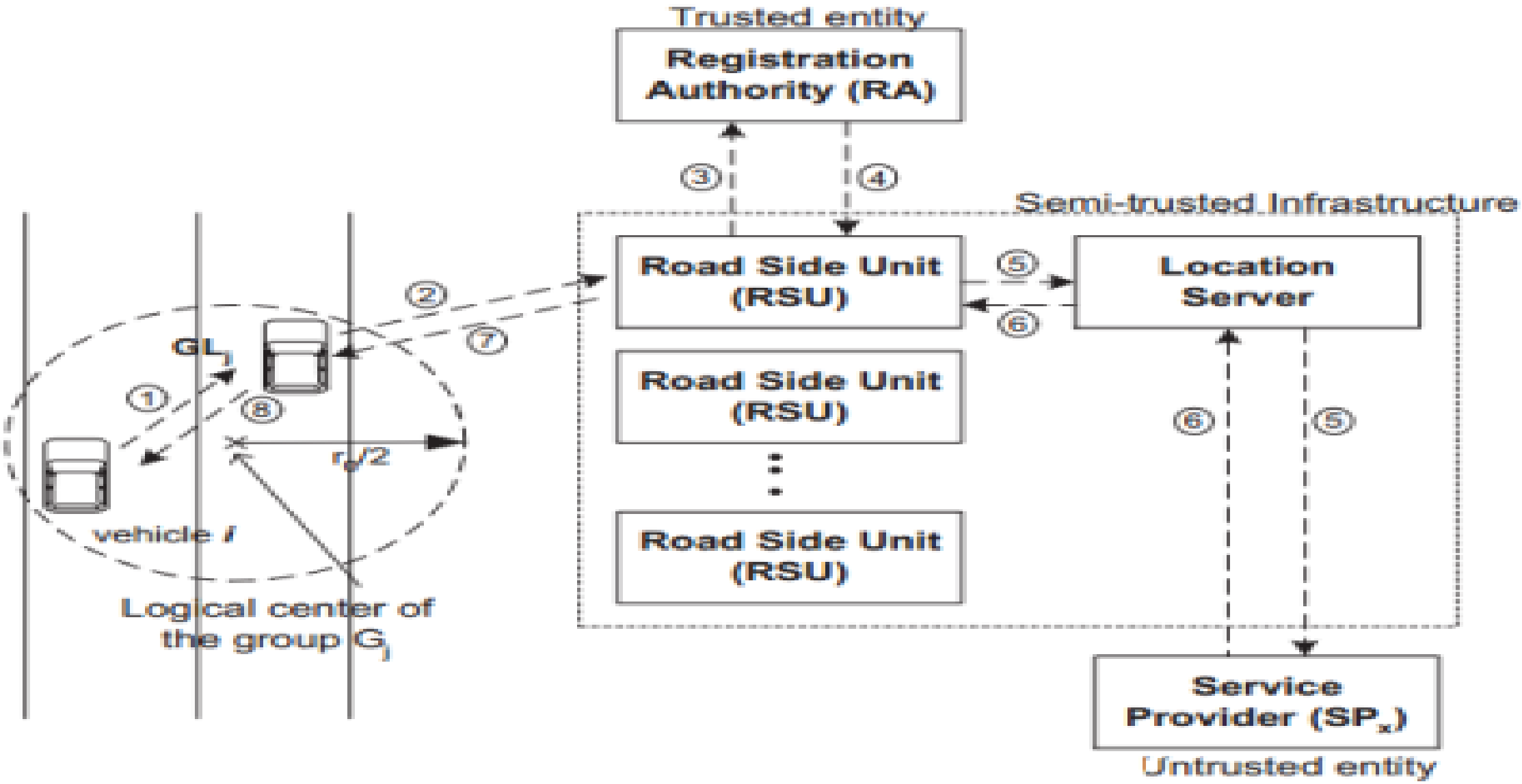


TẬN DỤNG SỰ IM LẶNG

- Ẩn danh cấu trúc đường bộ là không đủ
  - Khoảng thời gian im lặng ngẫu nhiên với cập nhật bút danh làm giảm khả năng liên kết nhưng gây ra các vấn đề về an toàn
  - Dựa vào các khoảng thời gian im lặng trong thời gian người lái xe tập trung cao độ, ví dụ: *khi chuyển làn hoặc nhập làn*



QUYỀN RIÊNG TƯ VÀ LBS



MỘT SỐ VẤN ĐỀ

- Trưởng nhóm đáng tin cậy?
  - Trưởng nhóm thỏa hiệp không có quyền riêng tư
  - Xoay giúp nhưng không giải quyết được
- Nhóm đáng tin cậy?
  - Các thành viên nhóm độc hại có thể tiết lộ thông tin cho LBS, giả mạo các yêu cầu LBS, v.v.
- •Thiếu kiểm soát đầu cuối trong V2I/LBS
  - Trả tiền dịch vụ?
  - Không kiểm soát phương tiện trong luồng dữ liệu
  - Các nhà lãnh đạo ác ý có thể can thiệp

TÓM TẮT

- Chúng ta đã thấy một số vấn đề về quyền riêng tư của vị trí duy nhất trong các hệ thống không dây rất khác nhau
  - Các vấn đề khác về quyền riêng tư của vị trí tồn tại trong các miền/bối cảnh khác, nhưng không có thời gian để đề cập đến tất cả
- Khi các hệ thống tiếp tục xuất hiện/phát triển, các vấn đề mới về quyền riêng tư sẽ phát sinh

BÀI 14:

ĐỘ TIN CẬY VÀ ĐỘ UY TÍN