BÀI #19 - BẢO MẬT & QUYỀN RIÊNG TƯ CỦA VANET

TS. HOÀNG SỸ TƯƠNG

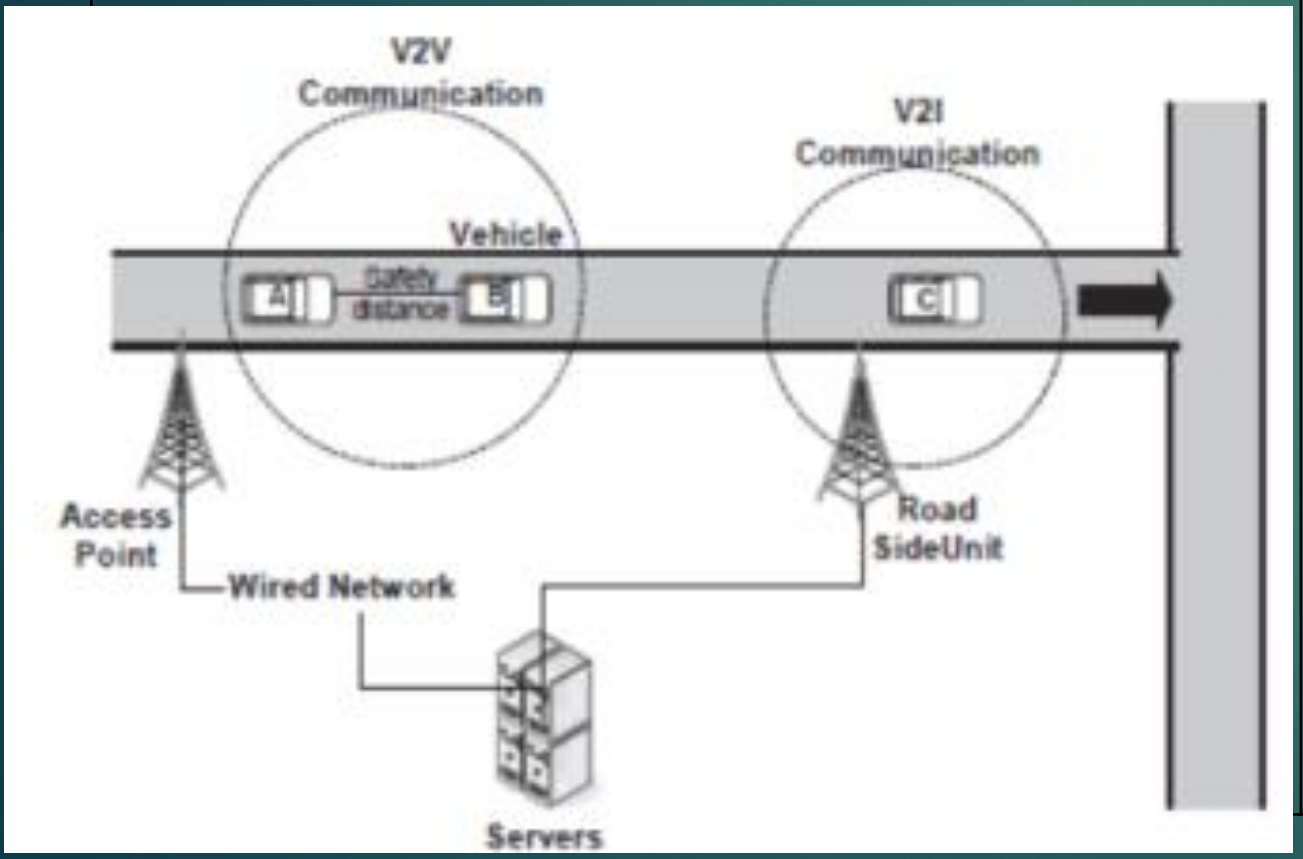
BÀI #19 - BẢO MẬT & QUYỀN RIÊNG TƯ CỦA VANET

- Đánh giá một số nội dung của Vanet
- Các cuộc tấn công không dây ảnh hưởng đến an toàn của các phương tiện như thế nào
- Đề cập ngắn gọn về những thách thức về quyền riêng tư của mạng giao tiếp trên ô tô

VANETs

VANET = Mạng ad hoc cho ô tô

- Ô tô có thể nói chuyện và với cơ sở hạ tầng ven đường



Ứng dụng cần quan tâm:

- Quản lý an toàn lái xe tự động
- Giám sát chất lượng / tình trạng đường thụ động
- Giải trí trong xe
- Dịch vụ dẫn đường
- Ghi nhận ngữ cảnh:

"Tuyến đường thay thế này sẽ nhanh hơn và nó sẽ đi qua Primanti Bros yêu thích của bạn."

CÁC THÀNH PHẦN VANET

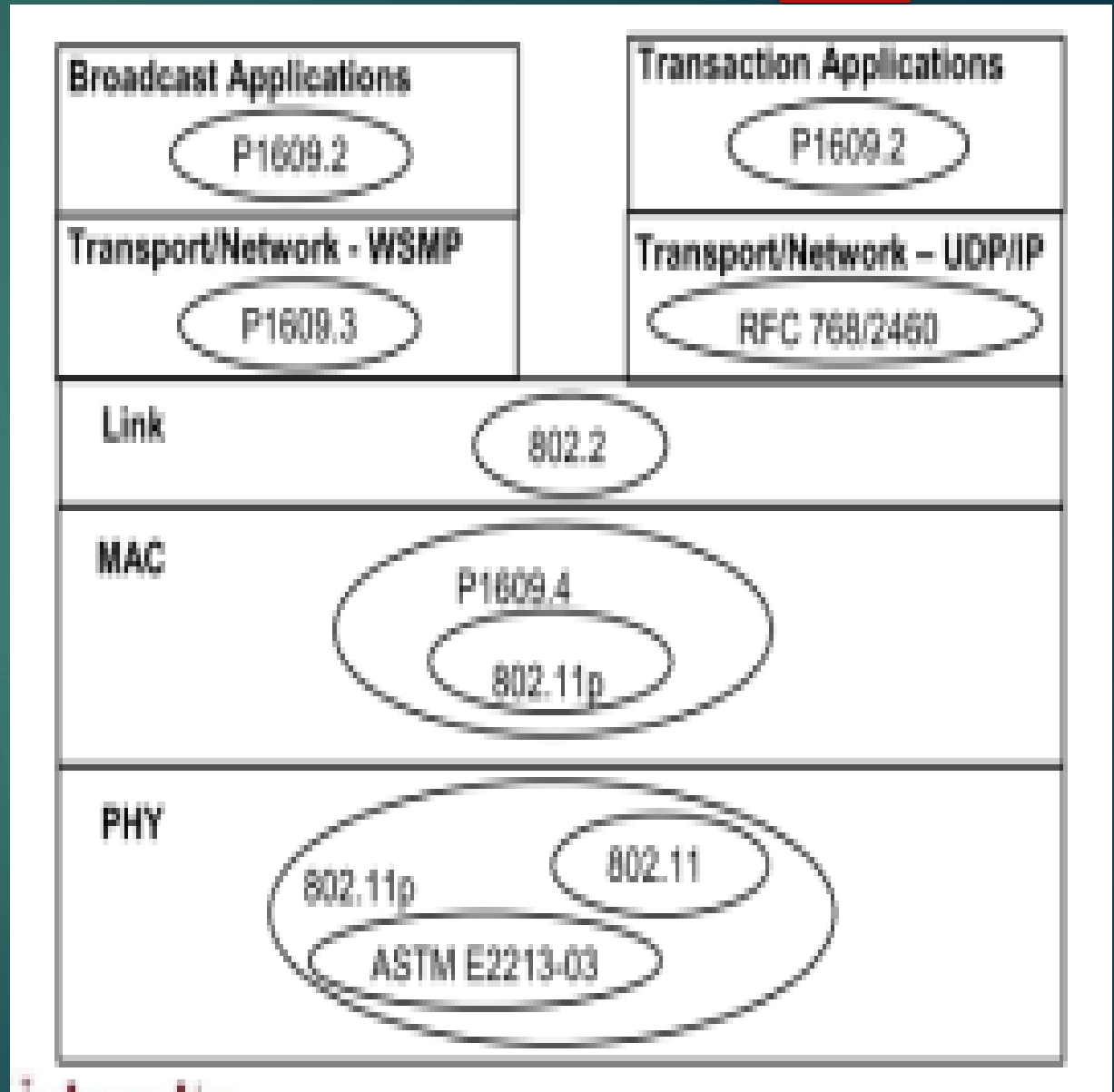
- Các thiết bị của người dùng tương tác với xe bằng WiFi Bluetooth, NFC, giao tiếp trực quan, v.v.
- Cảm biến trên bo mạch giao tiếp với bộ điều khiển bằng cách sử dụng giao tiếp năng lượng thấp

  Ví dụ: ZigBee cho TPMS
- Kết nối mạng di động (ví dụ: GSM, LTE)
- Hệ thống nhắn tin an toàn giữa các phương tiện

802.11p và DSRC

- 802.11p mở rộng tiêu chuẩn 802.11 để bao gồm các giao tiếp trên ô tô trên băng tần 5,9 GHz
  - Cho phép giao tiếp động mà không cần thiết lập BSS (nghĩa là không có SSID) để vận hành phi tập trung một cách nhanh chóng
  - Không liên kết, không xác thực, không kiểm soát truy cập...
  - Cũng bao gồm các cơ chế quản lý và đồng bộ hóa kênh
- Giao tiếp tầm ngắn chuyên dụng
  - Giao tiếp một và hai chiều dựa trên chuẩn 802.11p
  - Xây dựng trên tiêu chuẩn PHY cũ hơn ASTM E2213-03

- Truy cập không dây trong môi trường giao tiếp trên ô tô
  - Ngăn xếp không dây dành cho liên lạc giữa phương tiện với phương tiện và phương tiện với cơ sở hạ tầng
  - Dựa trên họ tiêu chuẩn IEEE P1609
  - Được xây dựng trên nền tảng 802.11p/DSRC



NHỮNG LOẠI HỆ THỐNG AN TOÀN XE NÀO ĐƯỢC XÂY DỰNG TRÊN NGĂN XẾP KHÔNG DÂY NÀY?

HỆ THỐNG AN TOÀN CHO XE Ô TÔ

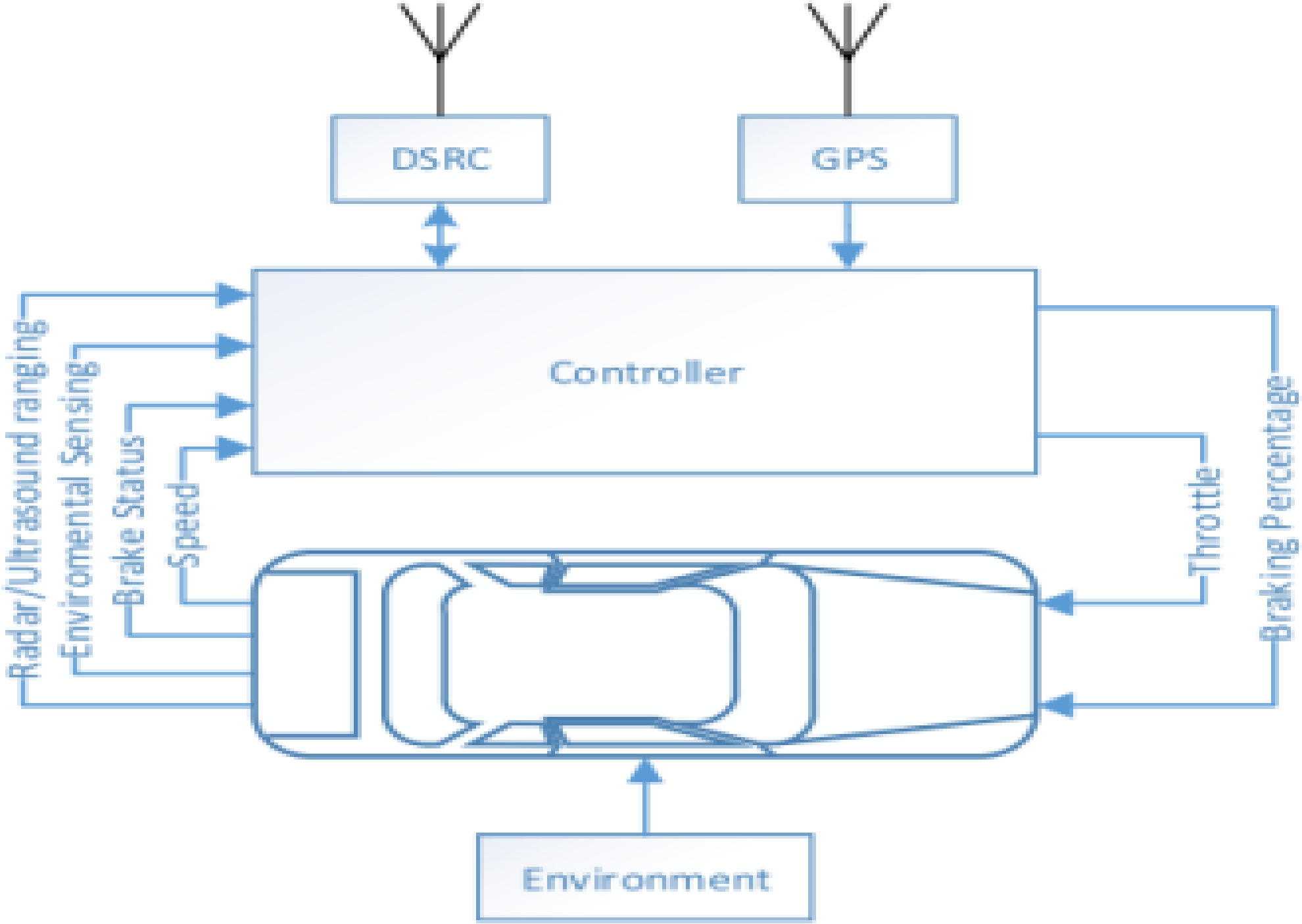
- Xe mới có nhiều hệ thống con không dây khác nhau
  - Cảnh báo trong quá trình lái xe, ví dụ: giám sát áp suất lốp

    Cảm biến van báo cáo cho bộ điều khiển TPMS - không dây vì chúng ở bên trong bánh xe...
  - Kiểm soát hành trình thích ứng

    Bộ điều khiển nhận tín hiệu từ nhiều nguồn khác nhau, bao gồm các phương tiện khác, RSU, đèn hiệu/màn hình, v.v.
  - Tránh va chạm, Tự phanh

    Cảnh báo đến từ các phương tiện khác, cảm biến, v.v.
  - Tự lái

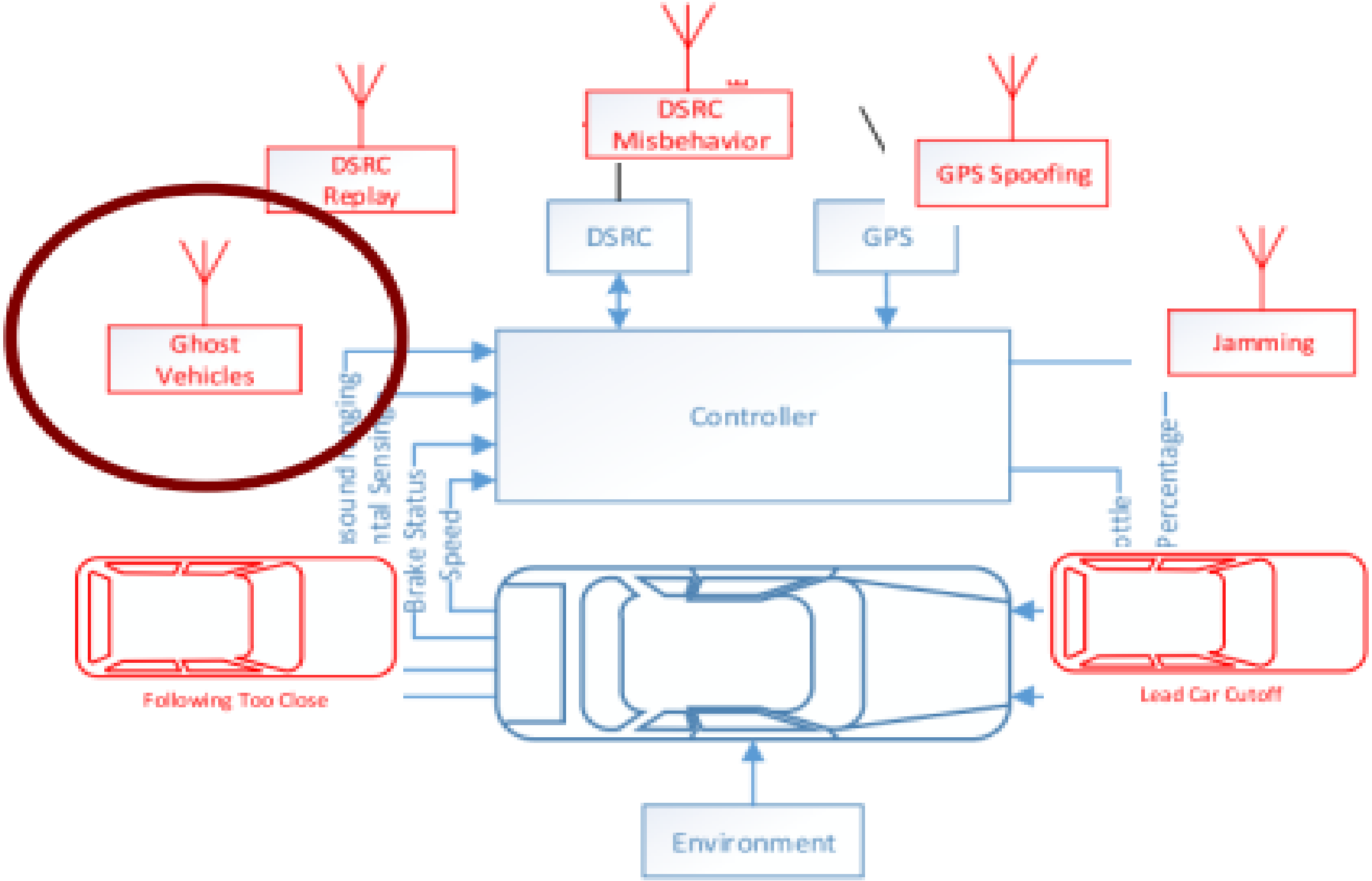
    Tất cả những điều trên và hơn thế nữa.


DSRC
GPS
Controller
Radar/Ultrasound ranging
Enviromental Sensing
Brake Status
Speed
Throttle
Braking Percentage
Environment

BỘ ĐIỀU KHIỂN NỐI MẠNG

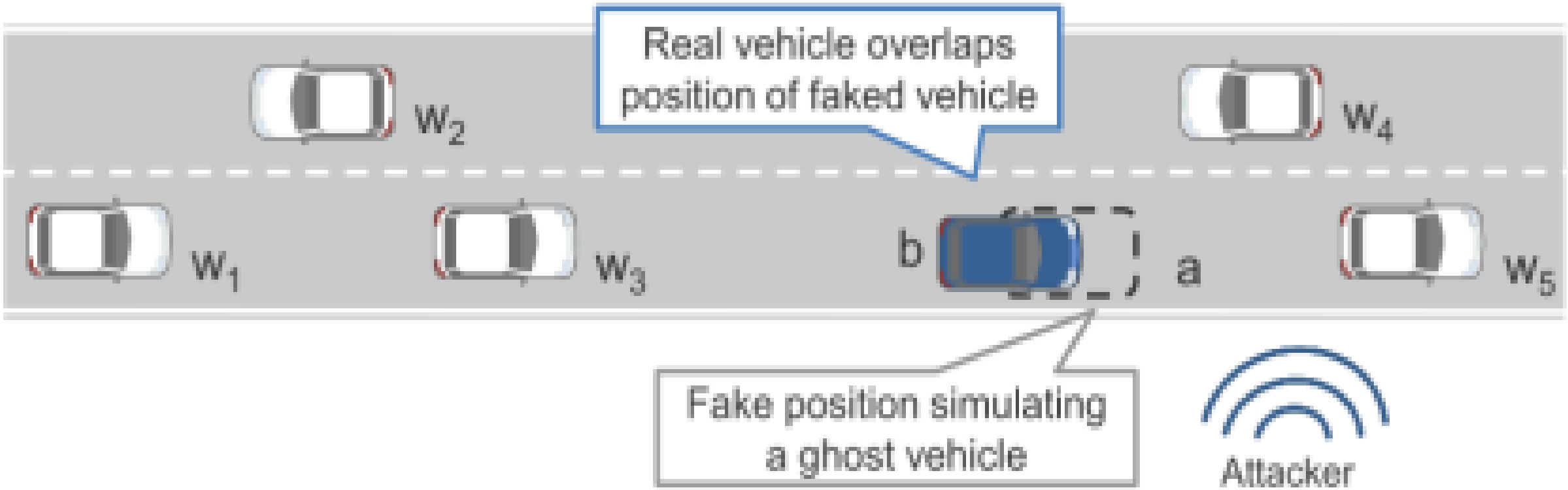
- Bất cứ khi nào bạn đặt mạng bên trong vòng điều khiển, mạng sẽ ảnh hưởng đến bộ điều khiển
  - Mất gói dẫn đến mất kiểm soát
  - Gói giả mạo làm cho việc ra quyết định kém hiệu quả
  - Lỗi GPS dẫn đến điều khiển sai thế giới quan
  - Độ trễ trên mạng/máy tính đãn đến làm chậm quá trình điều khiển và dẫn đến làm giảm độ chính xác
  - Tất cả những điều này đều tiềm ẩn những tác dụng phụ xấu đối với hệ thống an toàn của xe

NGOÀI CÁC VẤN ĐỀ LIÊN LẠC KHÔNG DÂY NÓI CHUNG, MỘT SỐ MỐI ĐE DỌA TIỀM ẨN LÀ GÌ?


DSRC Replay
DSRC Misbehavior
GPS Spoofing
Ghost Vehicles
DSRC
GPS
Jamming
Controller
Brake Status
Speed
Percentage
Following Too Close
Lead Car Cutoff
Environment

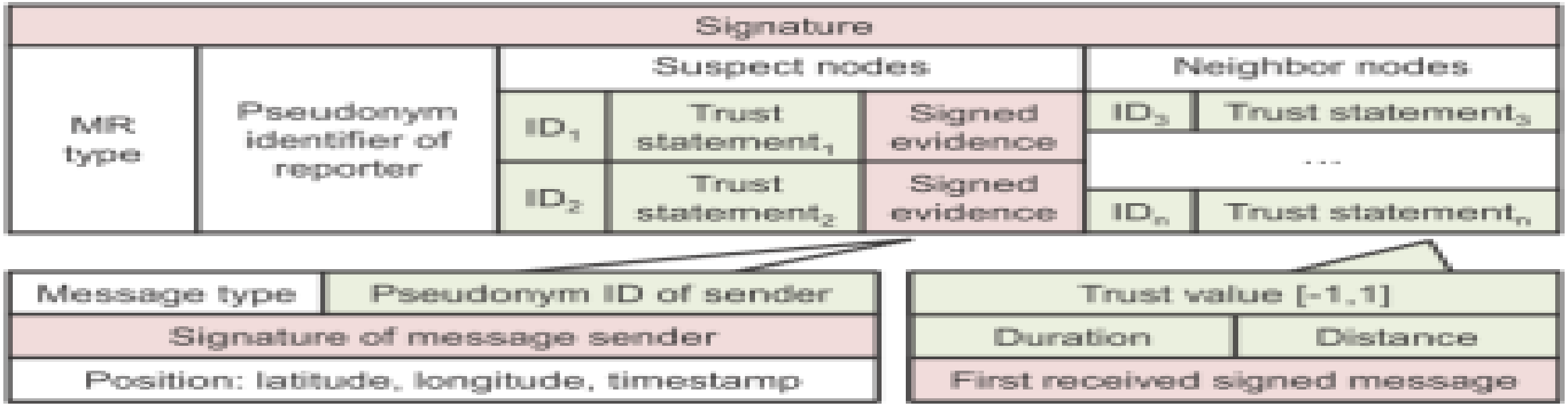
GHOST VEHICLES

- Xe ma là kết quả của các báo cáo sai lệch, thường do kẻ tấn công Sybil thực hiện
  - Người trong nội bộ có thể ký và bảo vệ các báo cáo một cách hợp lý, vì vậy việc phát hiện phải dựa vào các báo cáo vô hiệu hóa bằng cách nào đó
  - Hệ thống niềm tin và danh tiếng?



ĐÁNH GIÁ HÀNH VI SAI TRÁI

- Hệ thống phát hiện hành vi sai trái có thể phát hiện sự không nhất quán trong dữ liệu di động được báo cáo
  - Phát hiện cục bộ được giới hạn trong các khu vực có thể quan sát được (nghĩa là bị giới hạn bởi phạm vi liên lạc)
  - Cũng giới hạn thời gian hiệu lực ngắn của dữ liệu di động
  - Tùy thuộc vào sự thay đổi ID của kẻ tấn công, chiến thuật động



MỘT SỐ GIẢ ĐỊNH

- Xe có thể tùy ý chuyển đổi giữa các chứng chỉ giả
- Thông tin vị trí rất chính xác

  GPS, phương pháp định vị mang tính tương đối

  Cảm biến bổ sung: máy ảnh, radar

- Tính khả dụng của kết nối giữa các nút cục bộ và thực thể trung tâm không được đảm bảo

  Loại trừ những kẻ tấn công là mục tiêu lâu dài

  Độ trễ không phải là một mối quan tâm lớn

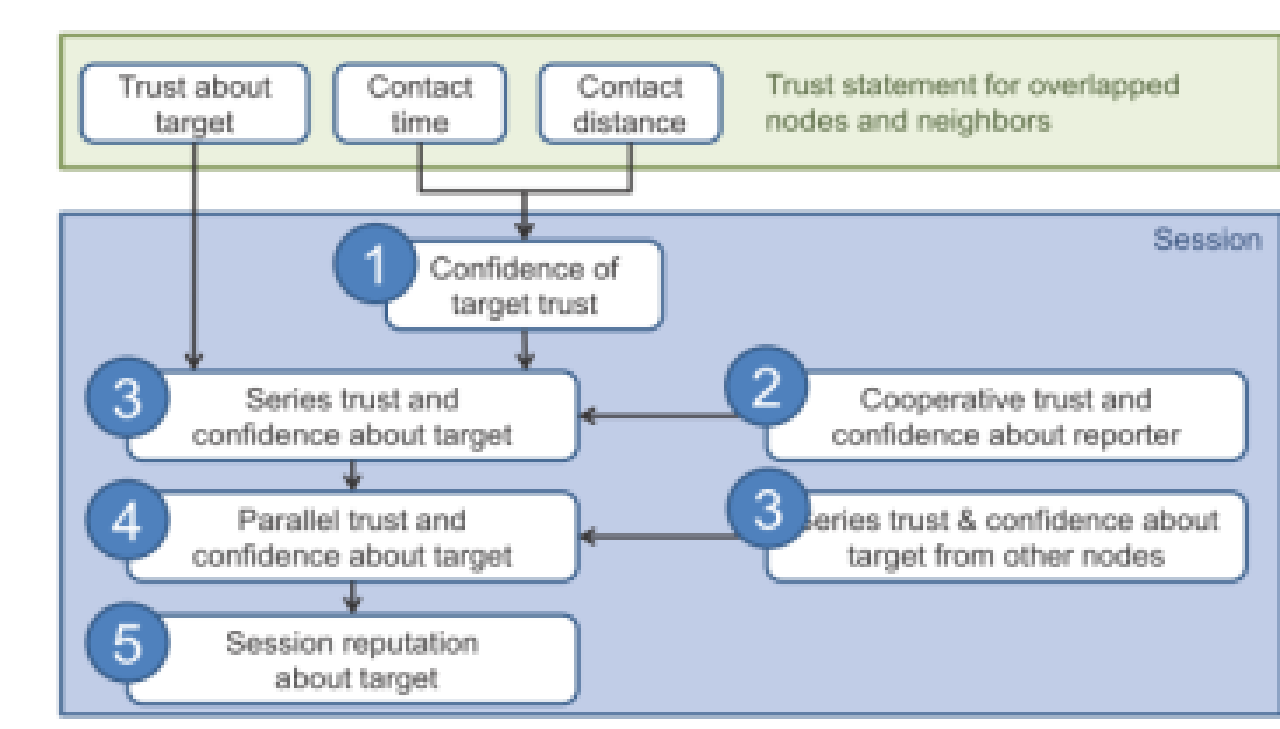
ĐÁNH GIÁ ĐỘ UY TÍN

- Danh tiếng được tính toán tập trung bởi Cơ quan đánh giá hành vi sai trái (MEA) bằng cách sử dụng các báo cáo về hành vi sai trái từ các nhân chứng và thông tin từ các nghi phạm

Tin cậy: *xu hướng được quan sát để hành xử như mong đợi, nhận giá trị trong [-1,1], mặc định là 0*

Bí mật: *mức độ chắc chắn trong giá trị tin cậy, thực chất là trọng số trong [0,1]*

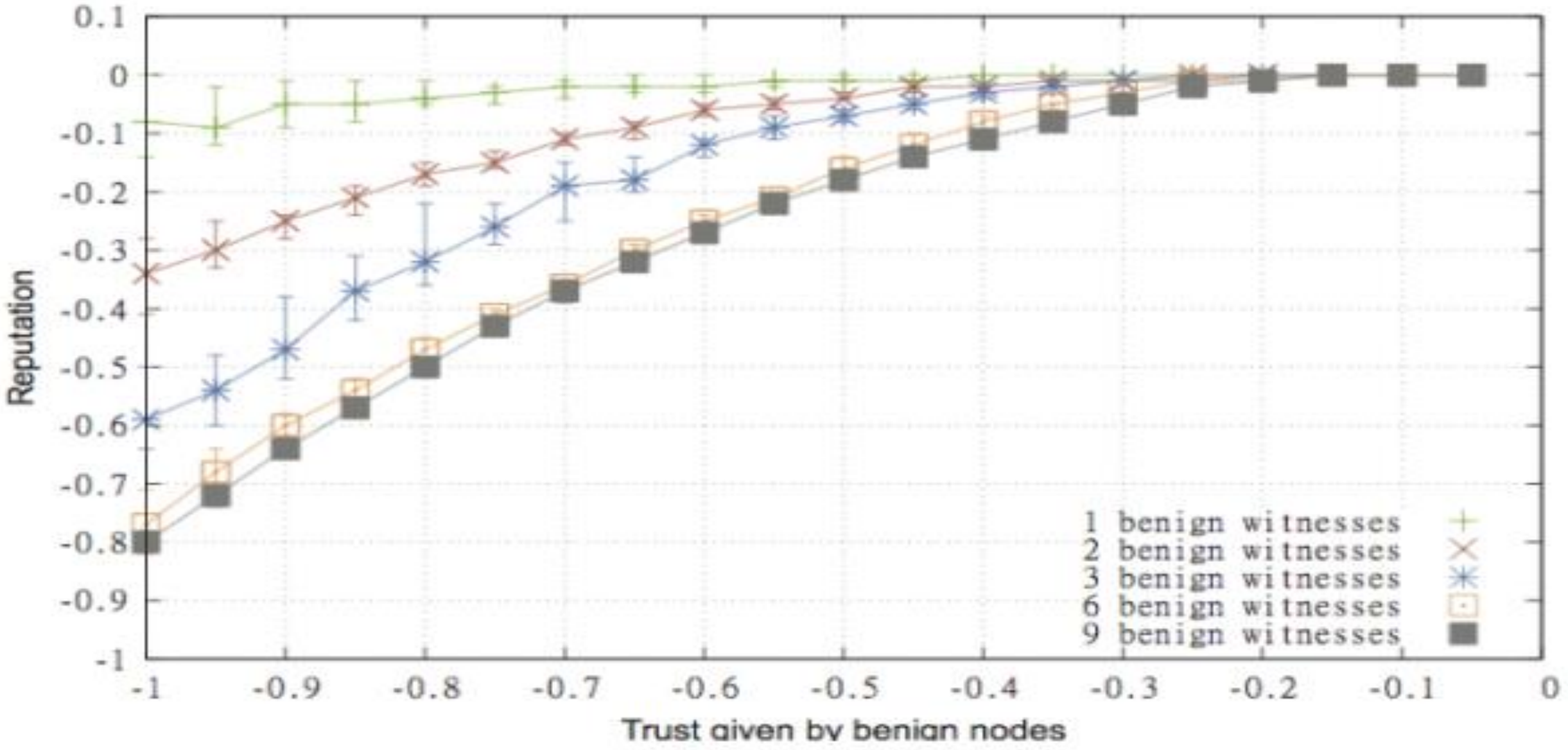
Uy tín: *thực chất là độ tin cậy x độ tin cậy, giá trị ở mức [-1,1]*



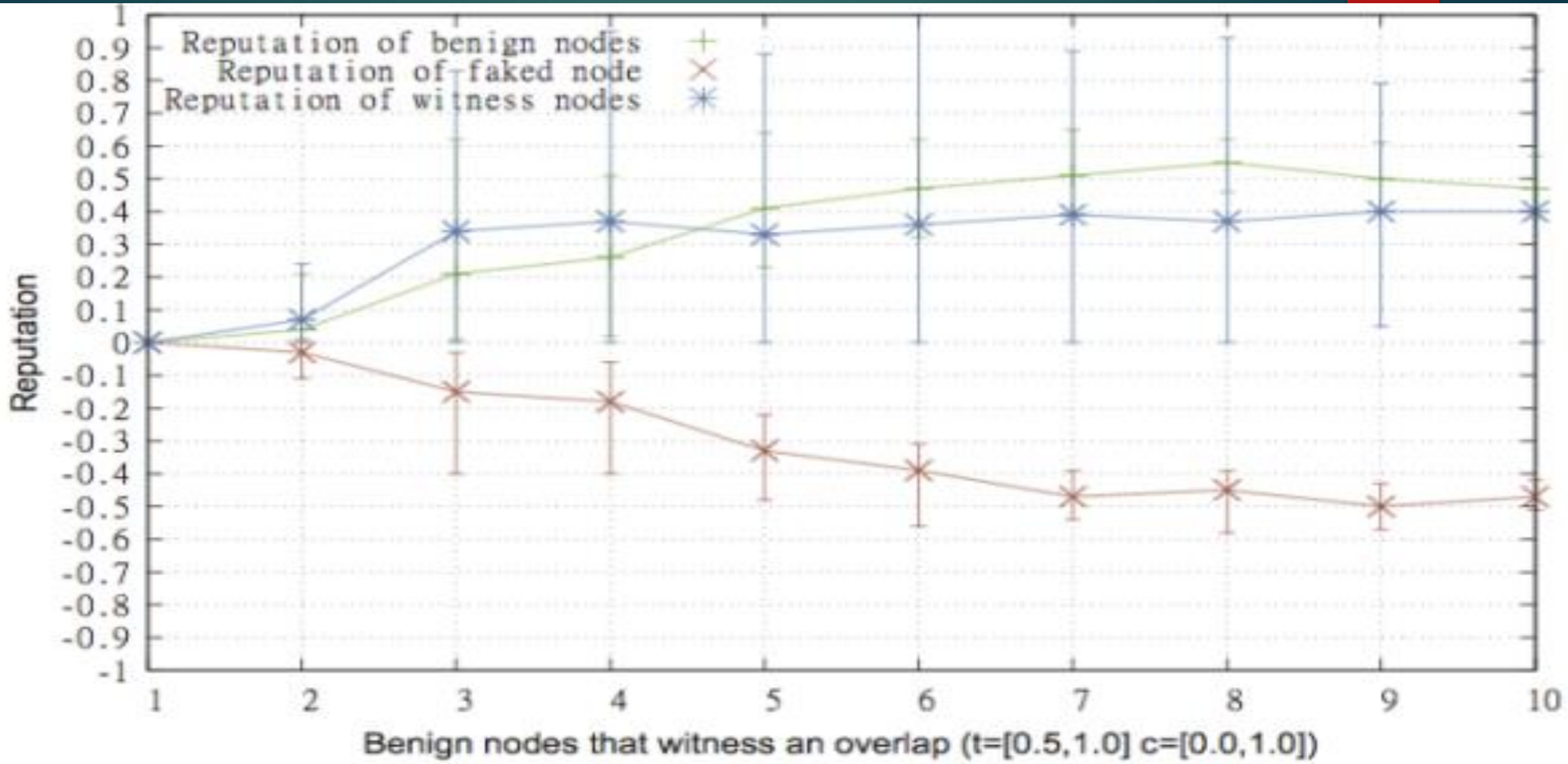
NHẬN DẠNG XE MA

- Xe có danh tiếng tiêu cực “vượt quá ngưỡng” có thể được xác định là ma
- Hỏi: Âm tính giả (tuyên bố xe thật khi là xe ma) nghiêm trọng như thế nào?
- Hỏi: Dương tính giả (tuyên bố là xe ma khi đó là xe thật) nghiêm trọng như thế nào?

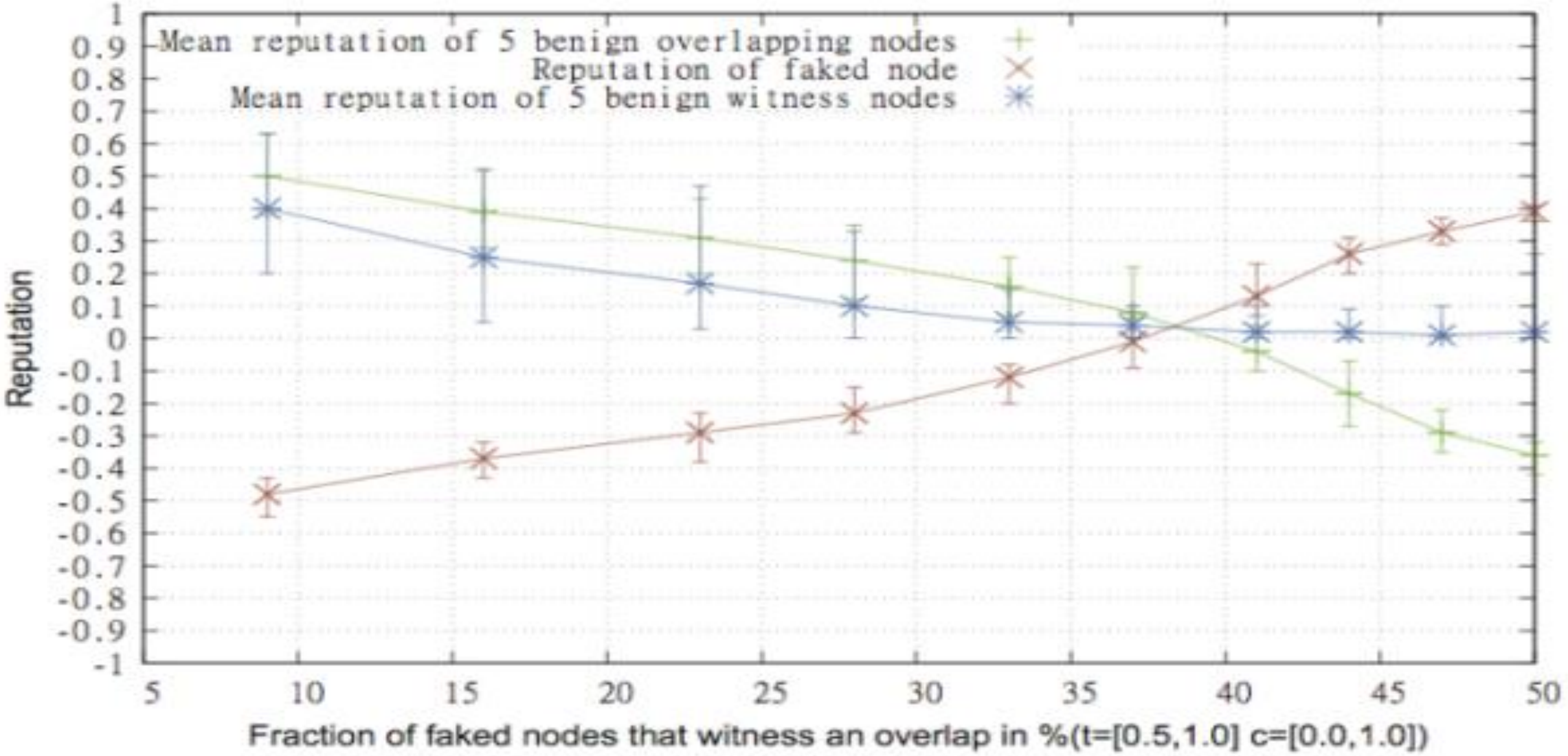
ĐÁNH GIÁ

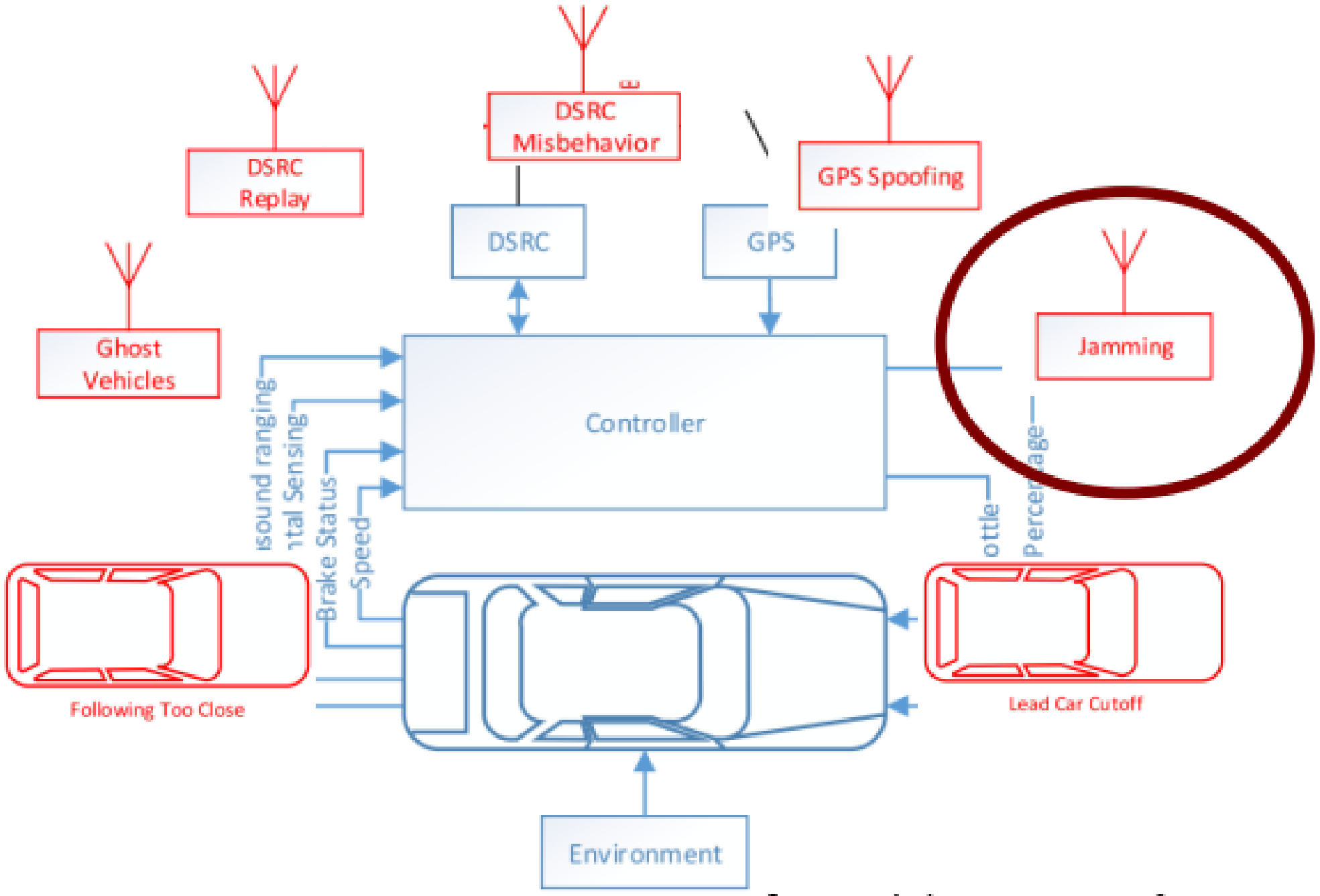

Reputation
Trust given by benign nodes
0.1
0
-0.1
-0.2
-0.3
-0.4
-0.5
-0.6
-0.7
-0.8
-0.9
-1
-1
-0.9
-0.8
-0.7
-0.6
-0.5
-0.4
-0.3
-0.2
-0.1
0
1 benign witnesses
2 benign witnesses
3 benign witnesses
6 benign witnesses
9 benign witnesses

ĐÁNH GIÁ


Reputation of benign nodes
Reputation of faked node
Reputation of witness nodes
Reputation
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
-0.1
-0.2
-0.3
-0.4
-0.5
-0.6
-0.7
-0.8
-0.9
-1
1
2
3
4
5
6
7
8
9
10
Benign nodes that witness an overlap (t=[0.5,1.0] c=[0.0,1.0])

ĐÁNH GIÁ


Mean reputation of 5 benign overlapping nodes
Reputation of faked node
Mean reputation of 5 benign witness nodes
Reputation
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
-0.1
-0.2
-0.3
-0.4
-0.5
-0.6
-0.7
-0.8
-0.9
-1
5
10
15
20
25
30
35
40
45
50
Fraction of faked nodes that witness an overlap in %(t=[0.5,1.0] c=[0.0,1.0])


DSRC Misbehavior
DSRC Replay
GPS Spoofing
DSRC
GPS
Ghost Vehicles
Jamming
Controller
isound ranging
rtal Sensing
Brake Status
Speed
ottle
Percentage
Following Too Close
Lead Car Cutoff
Environment

ĐÁNH GIÁ DSRC

- UIUC DSRC Simulator: mô hình hóa chính xác môi trường mạng xe cộ

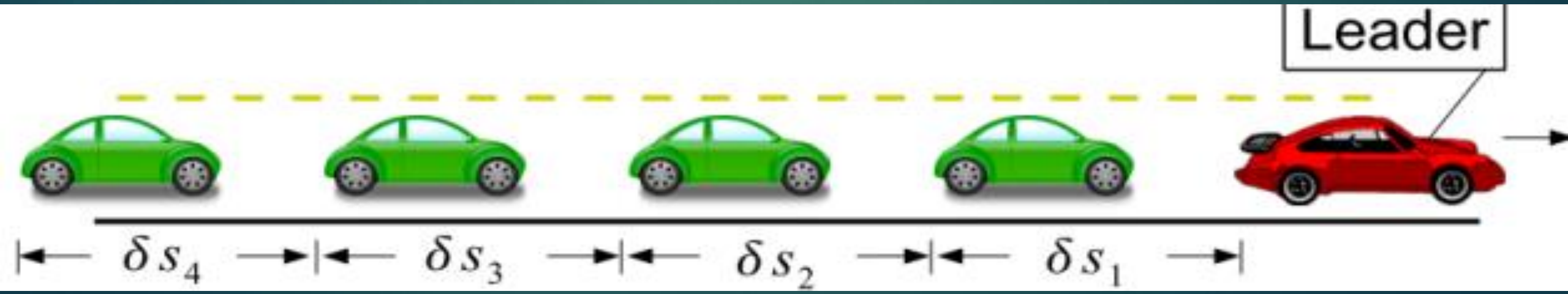
  5 phương tiện: 1 lãnh đạo, 4 tuân theo

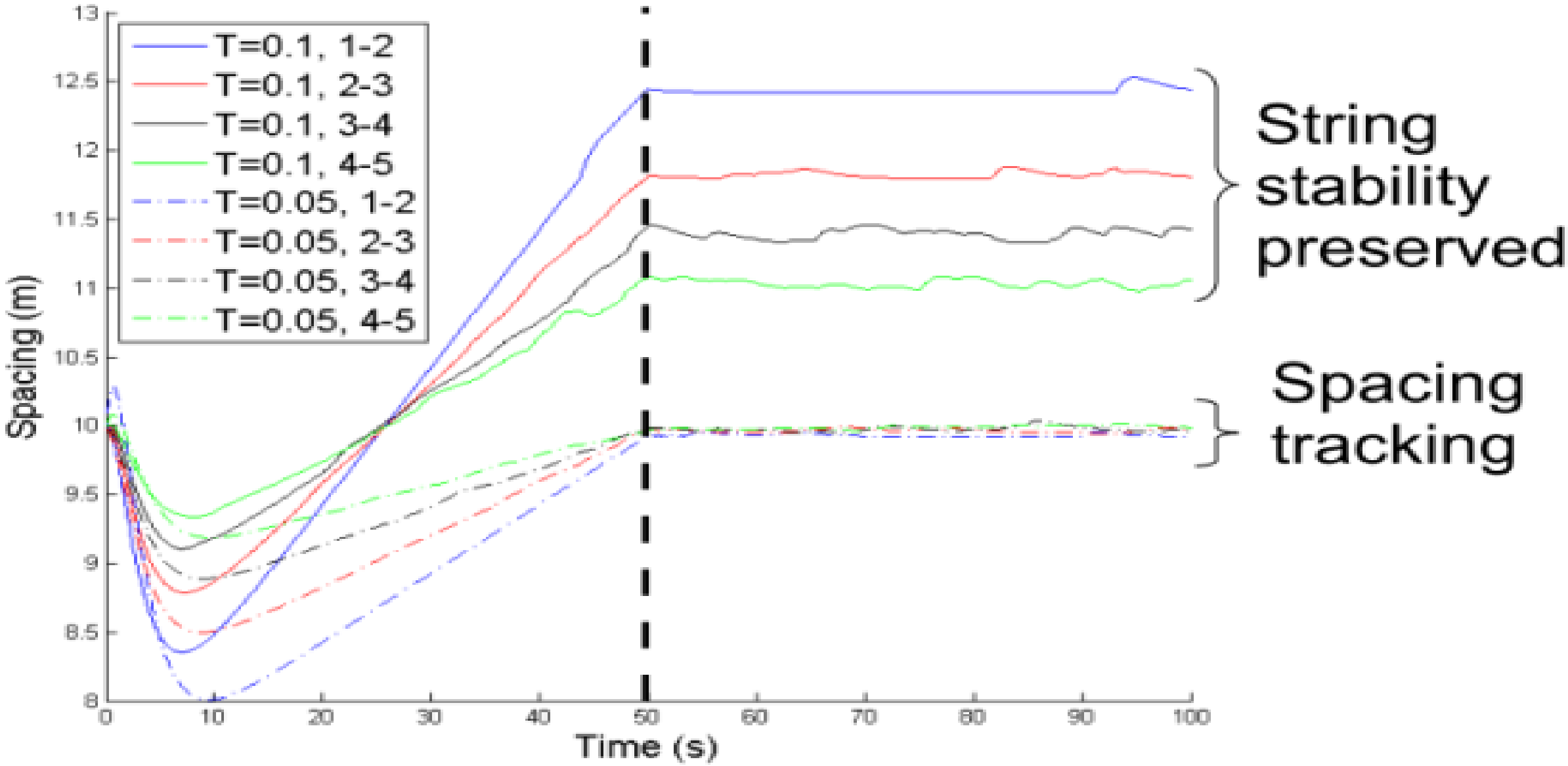
  Khoảng cách lý tưởng và ban đầu 10m

  Xe dẫn đầu tăng tốc với tốc độ 1 m/s2

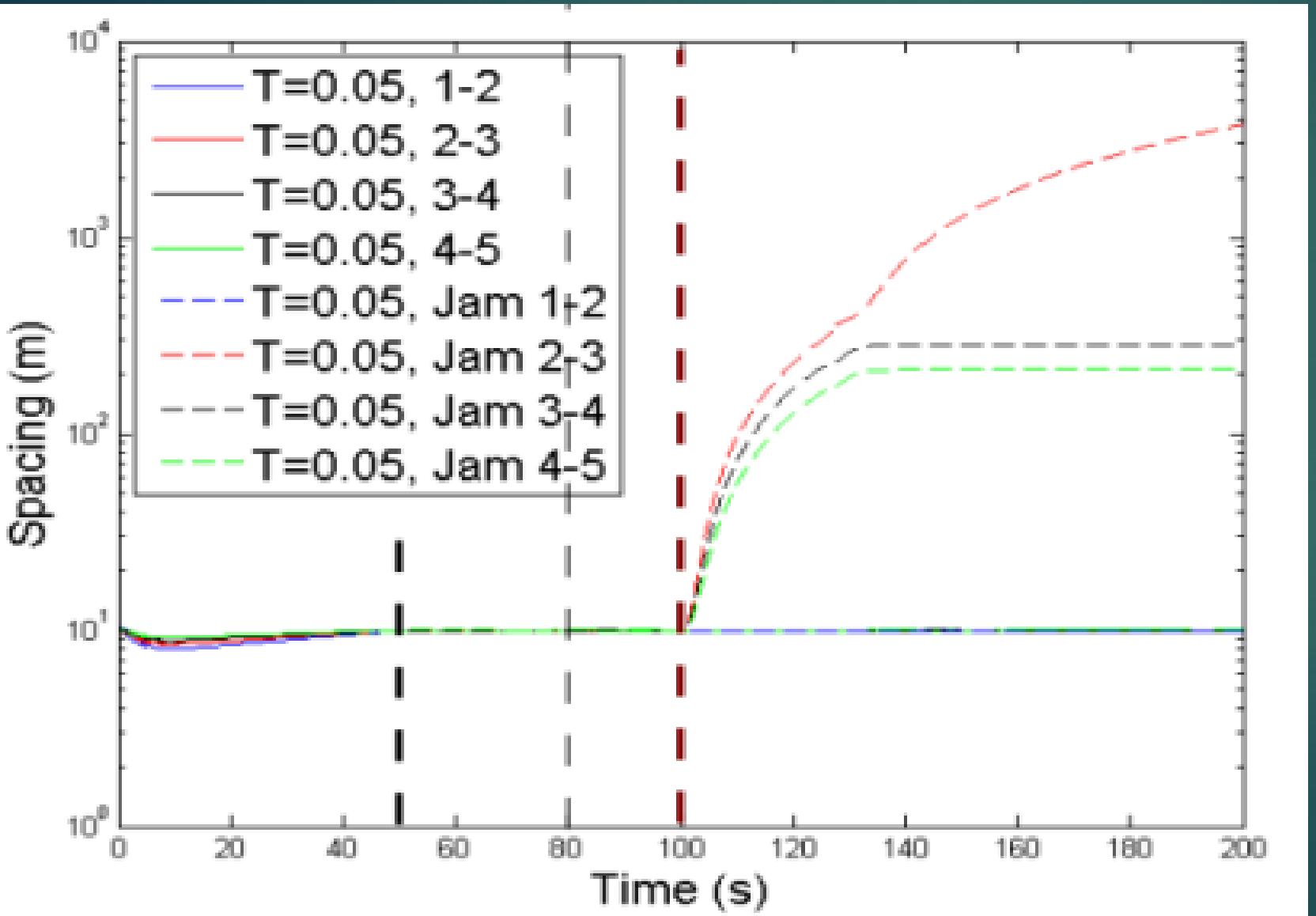
- So sánh điều khiển (không hỏng hóc) với tình huống gây nhiễu

  Kẻ tấn công biết trạng thái của phương tiện phía trước




T=0.1, 1-2
T=0.1, 2-3
T=0.1, 3-4
T=0.1, 4-5
T=0.05, 1-2
T=0.05, 2-3
T=0.05, 3-4
T=0.05, 4-5
Spacing (m)
Time (s)
String stability preserved
Spacing tracking

ẢNH HƯỞNG CỦA THIẾT BỊ GÂY NHIỄU



Vị trí DSRC phát sóng ở 20 Hz

Giới hạn tốc độ dẫn đầu: 50 m/s

Thiết bị gây nhiễu bật ở mức 100 giây

NHIỀU GÂY NHIỄU THÚ VỊ HƠN

- Chiến lược gây nhiễu mới: kẹt khi tăng tốc

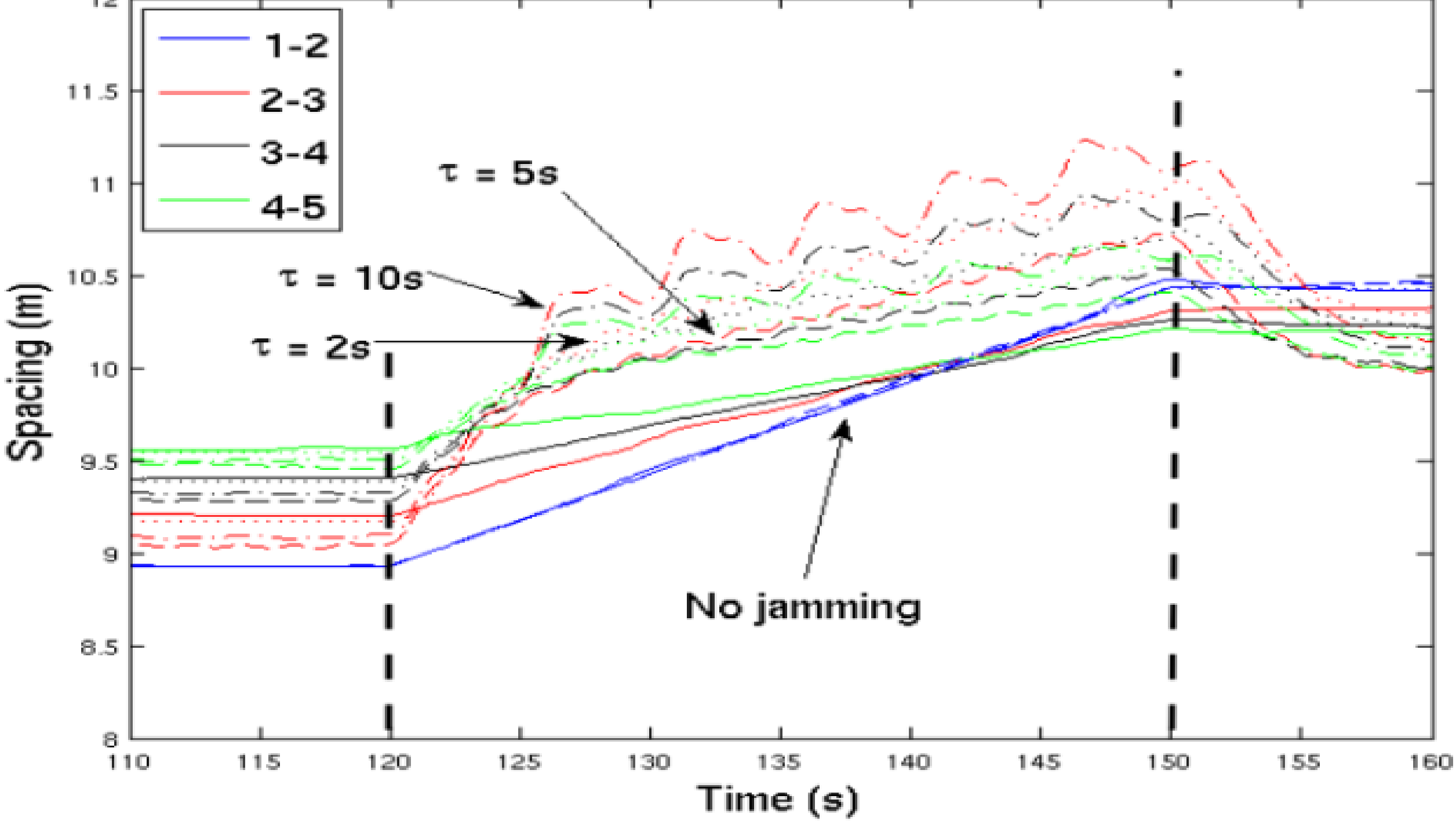
  Chu kỳ nhiệm vụ 50%, thời gian thay đổi trong {2, 5, 10} giây

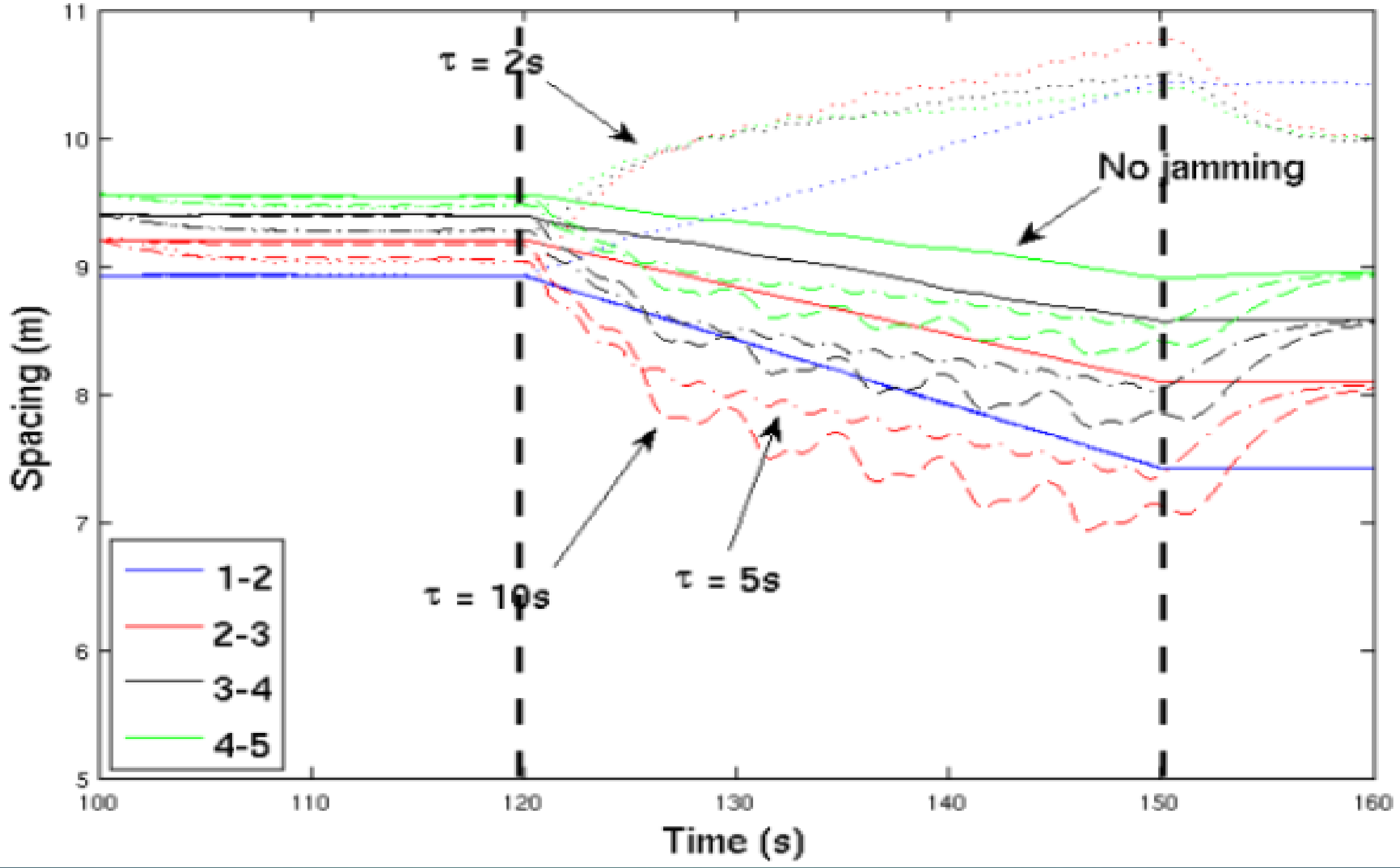
  Jammer bật ở 100 giây

- Hành vi của xe dẫn đầu cũng thú vị hơn:

  Bắt đầu với tốc độ 30m/s

  Tăng/giảm tốc 1m/s2 từ 120-150s


1-2
2-3
3-4
4-5
τ = 5s
τ = 10s
τ = 2s
No jamming
Spacing (m)
Time (s)
11.5
11
10.5
10
9.5
9
8.5
8
110
115
120
125
130
135
140
145
150
155
160


τ = 2s
No jamming
τ = 10s
τ = 5s
1-2
2-3
3-4
4-5
Spacing (m)
Time (s)
11
10
9
8
7
6
5
100
110
120
130
140
150
160

CÒN VẤN ĐỀ RIÊNG TƯ TRONG MẠNG KẾT NỐI Ô TÔ THÌ SAO?

TÍNH RIÊNG TƯ TRONG MẠNG KẾT NỐI Ô TÔ

- Mọi thứ chúng ta đã nói trước đây liên quan đến quyền riêng tư của mạng đều áp dụng cho phương tiện
- Tuy nhiên, xe có nhiều hệ thống phụ không dây được kết hợp thành một nền tảng duy nhất

  Một số nhận dạng không dây (DSRC, WiFi, LTE, TPMS, v.v.) và nhận dạng không dây đang được sử dụng (biển số xe, nhận dạng hình ảnh, v.v.)

  Nhiều ứng dụng/dịch vụ hoạt động đồng thời với các yêu cầu khác nhau

  Quản lý danh tính/bút danh có thể cần xem xét tất cả những điều này cùng nhau, cân nhắc nhiều sự đánh đổi

KẾT LUẬN

- Một số mối đe dọa/hành vi sai trái cơ bản nhất trong mạng không dây có tác động nghiêm trọng và đôi khi không thể đoán trước đối với phương tiện
- Vấn đề mở: làm thế nào để thiết kế bộ điều khiển phương tiện mạnh mẽ trước các mối đe dọa không dây? ... các giao thức không dây đảm bảo cho việc điều khiển phương tiện?

BÀI 20:

BẢO MẬT & QUYỀN RIÊNG TƯ CỦA IOT