Responding to Mobile Worms with Location-Based Quarantine Boundaries

Baik Hoh (baikhoh@winlab)
Marco Gruteser (gruteser@winlab)

WINLAB
WIRELESS INFORMATION NETWORK LABORATORY

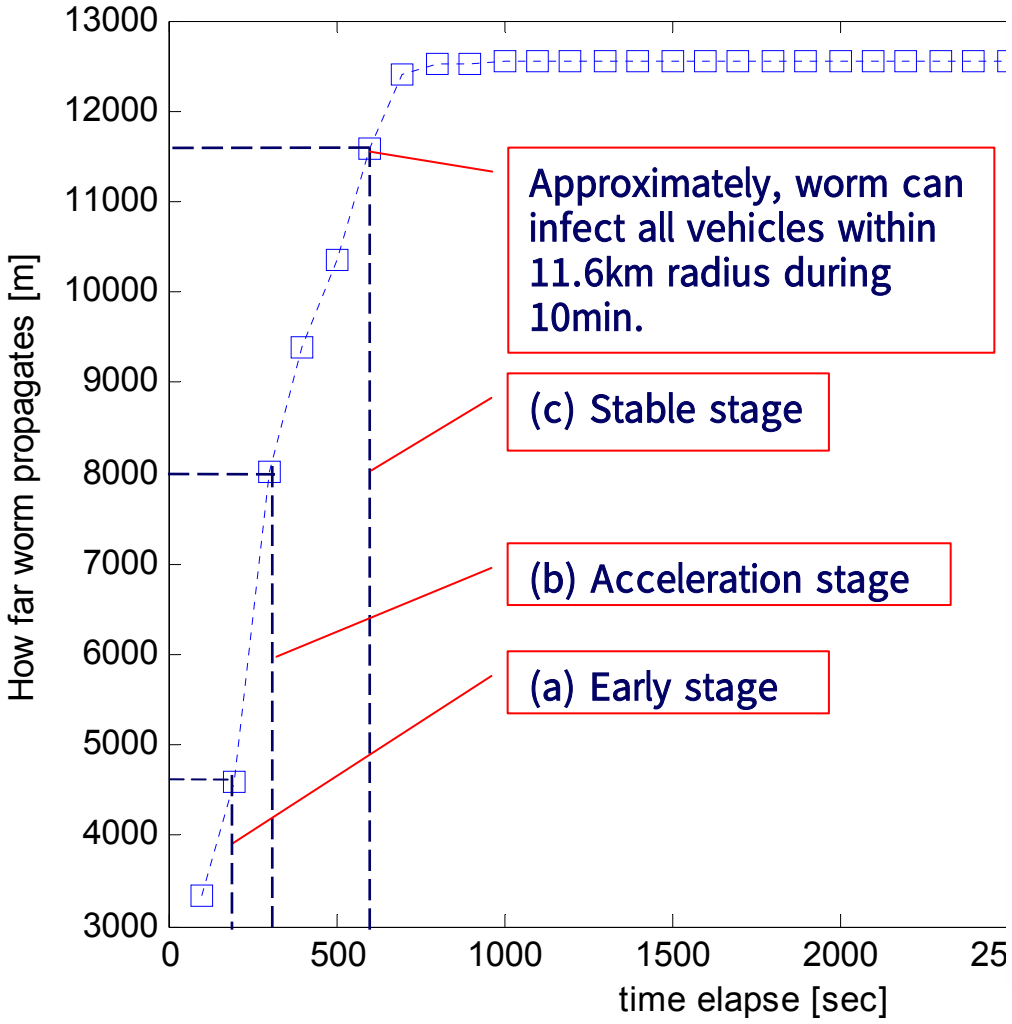
Threats of Mobile Worms

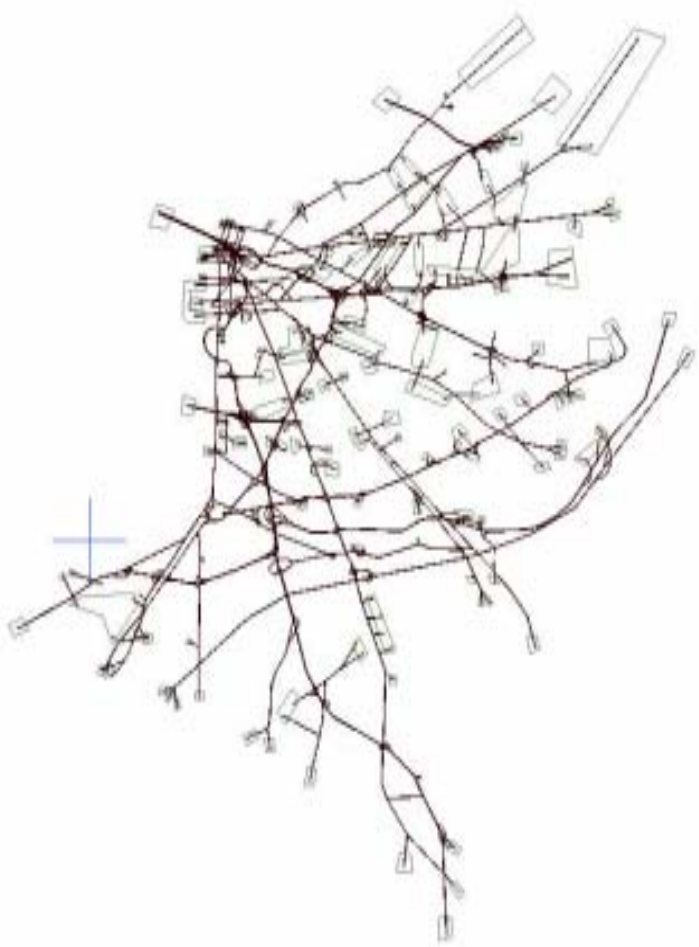
- Current Trends in Pervasive Devices
  - **Multi-radio support**: backhaul link (e.g., Cellular networks) and short-range communication (e.g., Bluetooth, DSRC)
  - Example: Cellular networks, Vehicular networks

- Mobile Worms / Malware over Peer-to-Peer interaction
  - Vulnerability: **Bluetooth buffer overflow** (e.g., BlueSmack Attack)
  - This allows malware to spread without user intervention

- Peer-to-peer replication over short-range wireless networks creates a challenge for intrusion detection and response
  - (High False Alarm) No conventional IDS deployed (Address blacklisting, Content filtering) over vehicular ad-hoc networks
    - No concentration point (e.g., gateways)
    - Resource limited nodes
  - (Distributed IDS) Delay needs special care on 'Intrusion Response'
  - No Partitioning of sub-network → Can we do virtually in ad-hoc?

A typical threat scenario (Vehicular Networks in New Jersey Southern Highway)





Do we have a short-term strategy for responding to unknown mobile worms spreading over NJ within 4 hours?

Am I building too high wall for imaginary monster?

-Do we have an example?

-Do we have any ad-hoc network in operation?

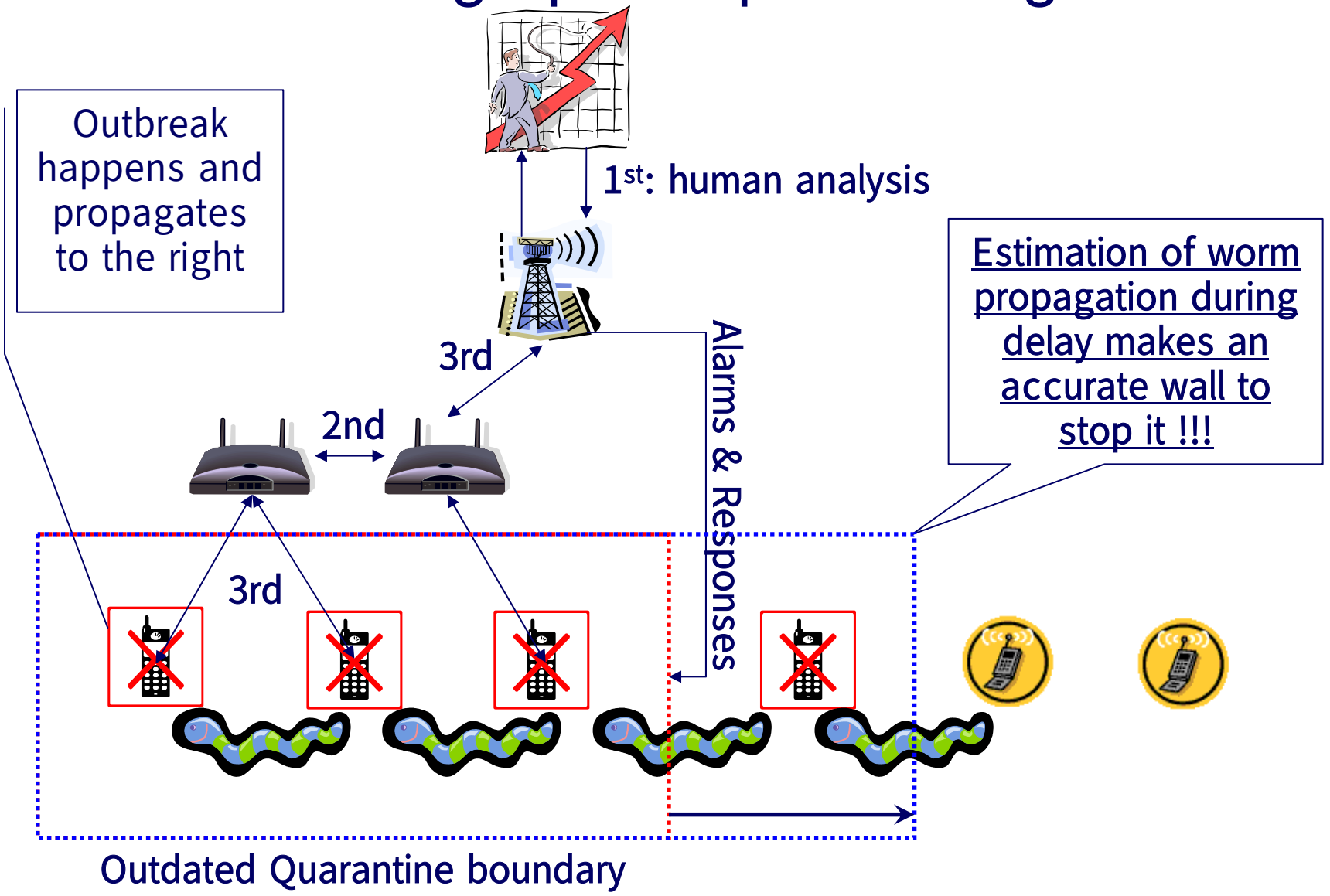
- Do we have a distributed IDS in real world?

- Is Intrusion Response more important than Intrusion Detection?

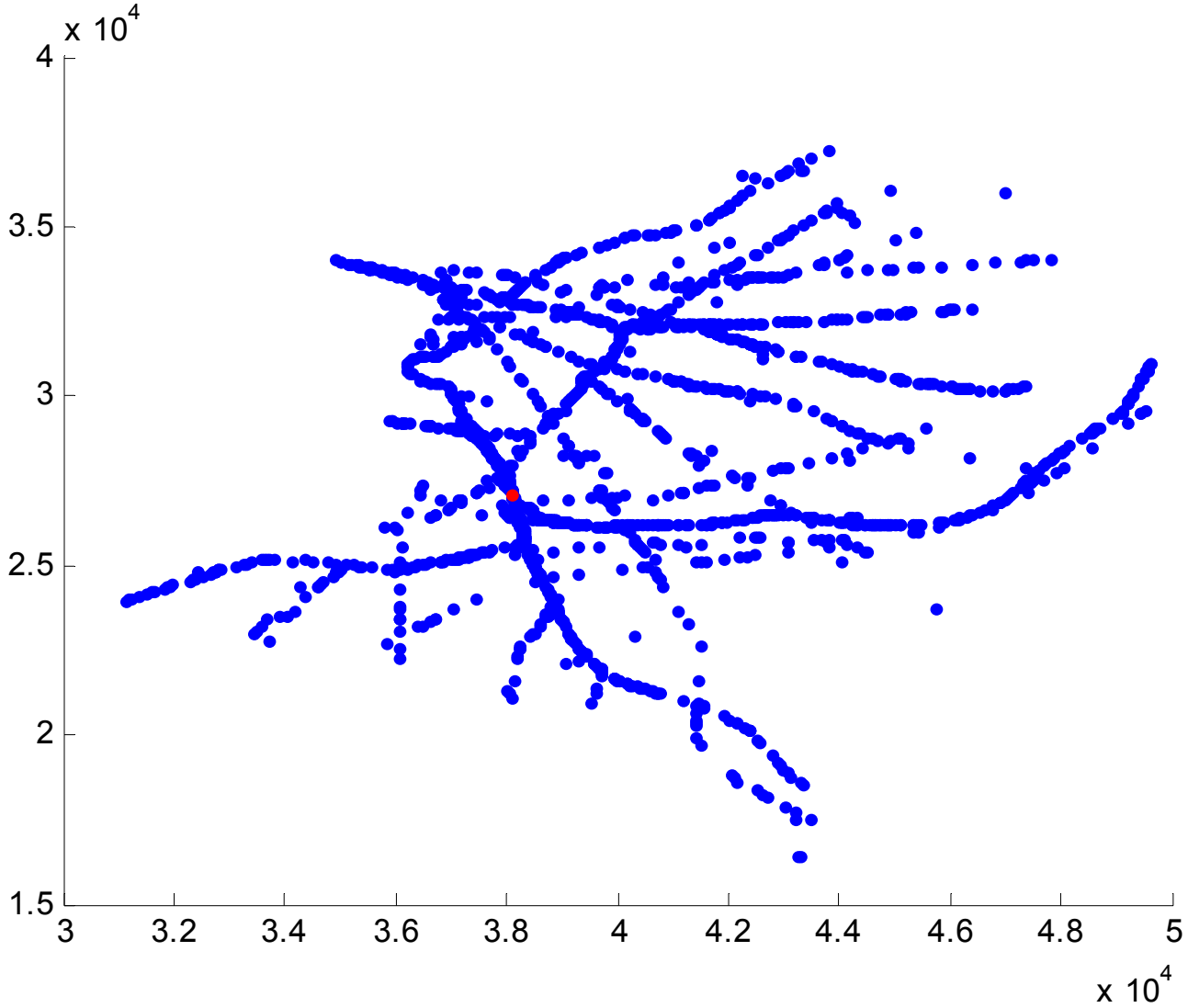
- Do we need Short-term strategy for developing a patch?

I'm Don Quixote? But, I'm fighting with realistic monster?

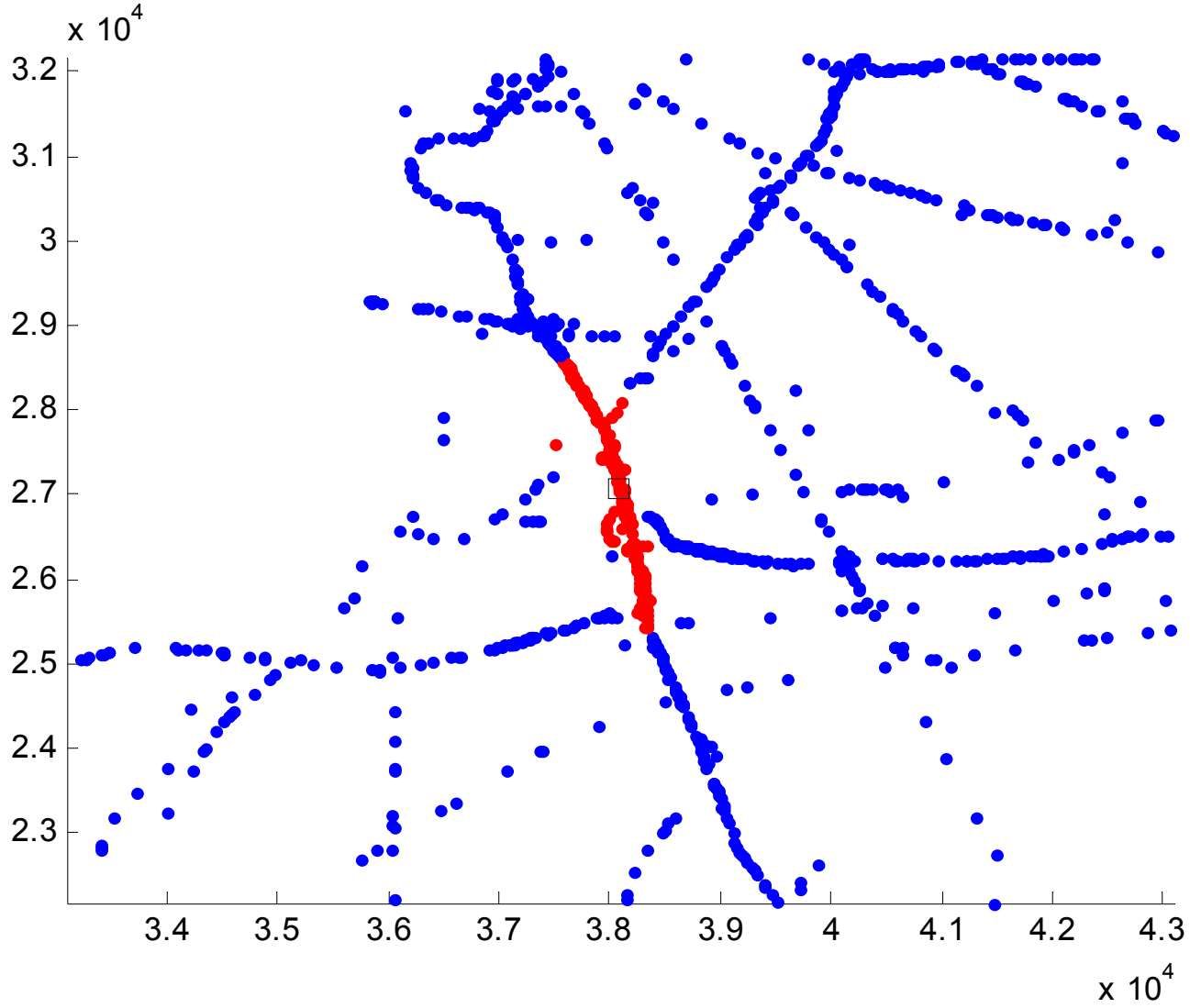
Infrastructure-aided Wireless Intrusion response architecture: Geographical partitioning



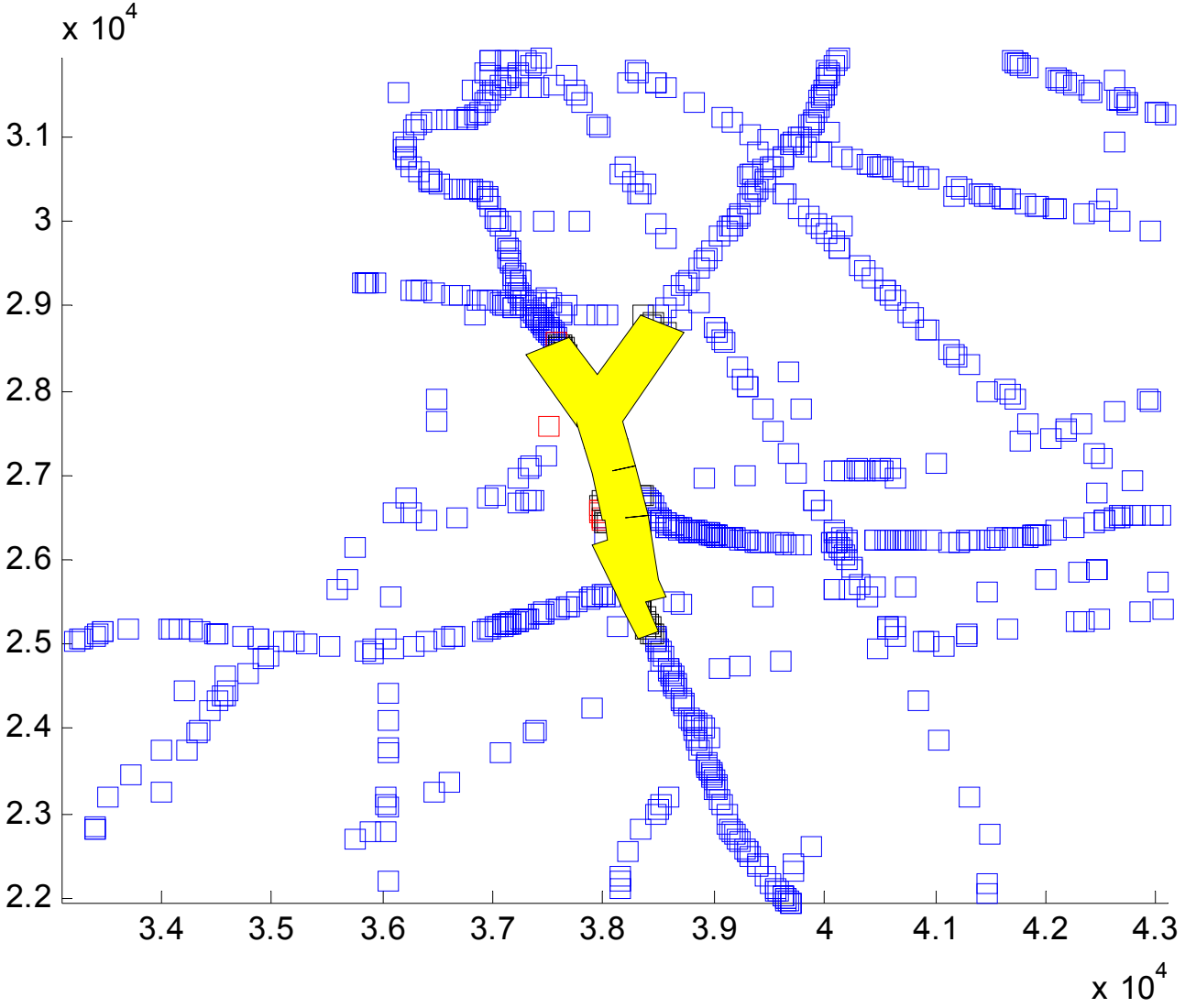
Graphical example: One Drop



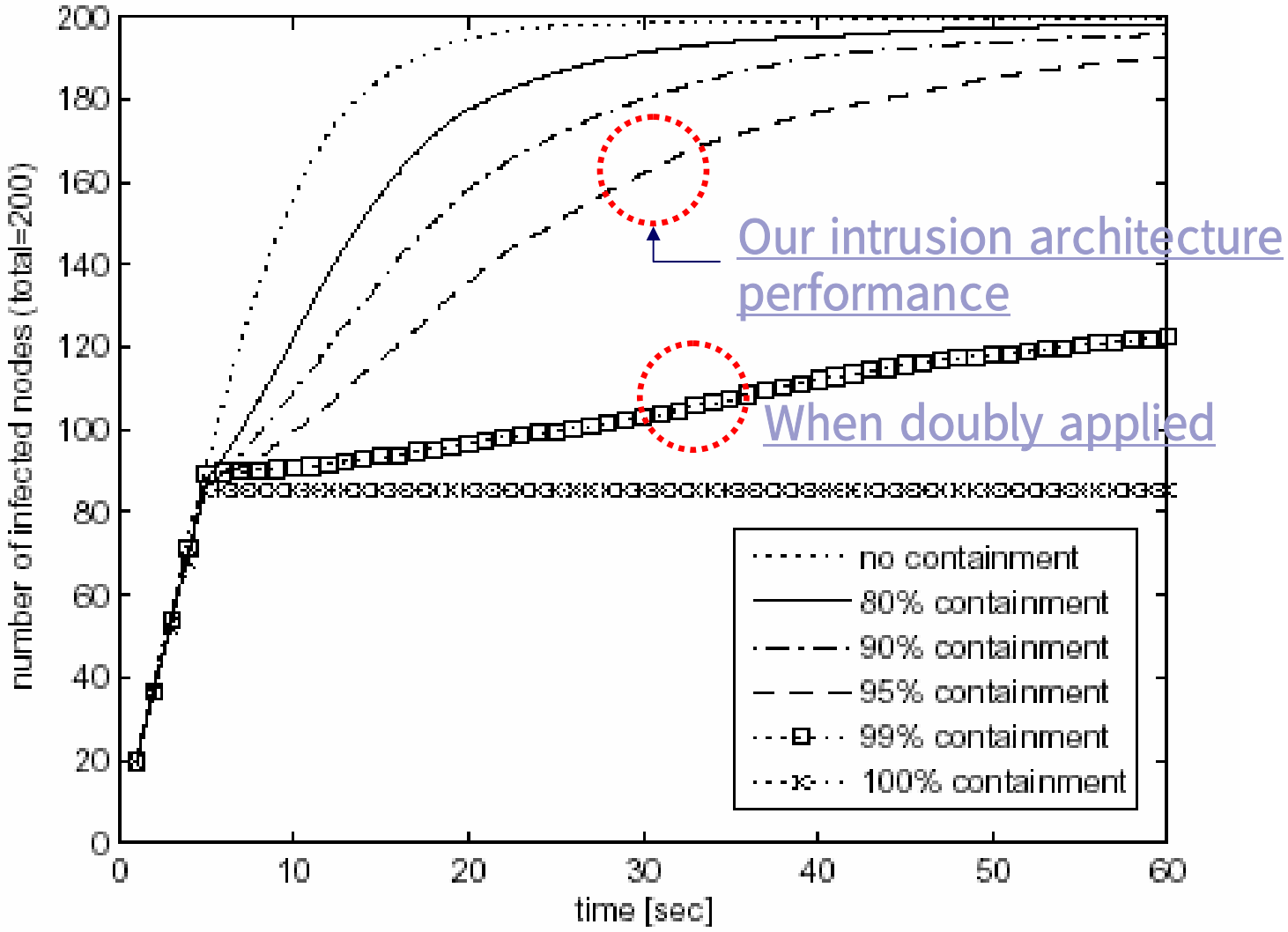
Graphical example: Spread



Graphical example: Quarantined



The effect of imperfect containment: **High detection** but **Low false positive**



Problem statement: $\Delta T = T_A - T_O$

- A time delay between outbreak to alarm.
  - Mobile worms can spread further → imperfect containment
  - We need an accurate boundary estimation
- We need an "Intrusion response planning strategy"
  - 1. Detect an accurate Patient 0
  - **2. Set an accurate quarantine boundary**
  - 3. Contain remotely under minimizing the impact of the worm (policy needed)

A Macroscopic Models of Worm Propagation from Ecology

- **Diffusion-Reaction model** from 'Spread of muskrats'
  - Propagation Speed, Circle
- **Advection-Diffusion model** from 'Toxic pollutants in underground water'
  - Propagation Speed, Rectangles
- Estimating quarantine boundary in mobile worm is an analogous problem

Model Parameter	Correspondence in automotive scenario
Diffusivity	Models minor roads and collector streets or pedestrian movements
Growth rate	Rate of new infections depends on density and distribution of susceptible nodes, communication range, and node velocity
Origin	Positions of initially infected nodes

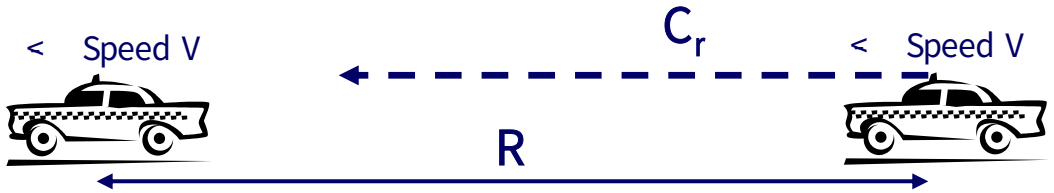
Assumptions

- IDS can accurately locate **Patient 0**
- **Location server (infrastructure)**: service provider can locate each mobile node.
- **Type of mobile worms:** unknown malware (or polymorphous)
- **Detection method:** a distributed anomaly detection
- 5% of All vehicles are **susceptible** (e.g., discoverable mode in Bluetooth)

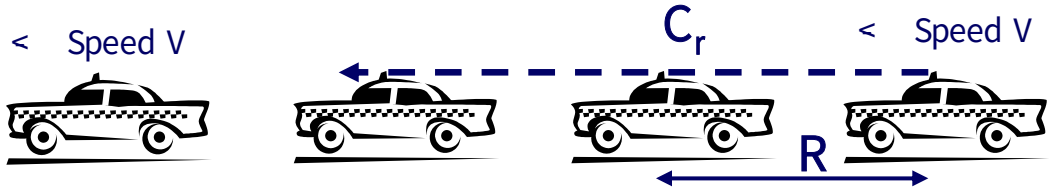
Quarantine boundary estimation

- Step1: Estimating the worm propagation velocity (v')
  - Pedestrian scenarios: empirically simulation-based approach
  - Vehicular scenarios: simple analytic model
- Step2: Estimating the spatial distribution
  - Isotropic circle ($R = v' * \Delta T$)
  - Rectangle ($L = v' * \Delta T$, W = road width)

Step1 (Vehicular scenario): Propagation speed estimation



(a) Full speed ($R>C_r$)

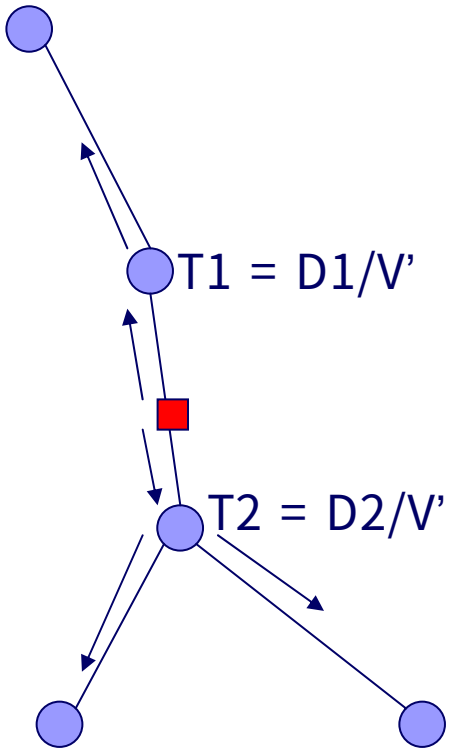


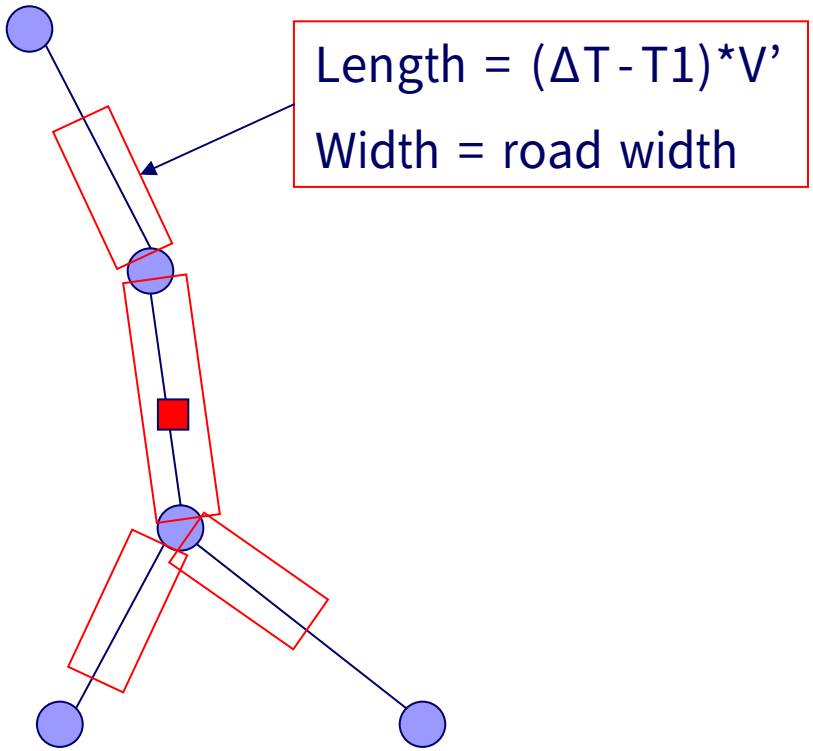
(b) Traffic jam ($R<C_r$)

$$V' = \begin{cases} V + nR\left\lfloor \frac{C_r}{R} \right\rfloor & \text{if } R \leq C_r \\ V & \text{else} \end{cases}$$

Step2 (Vehicular scenario): Spatial Boundary

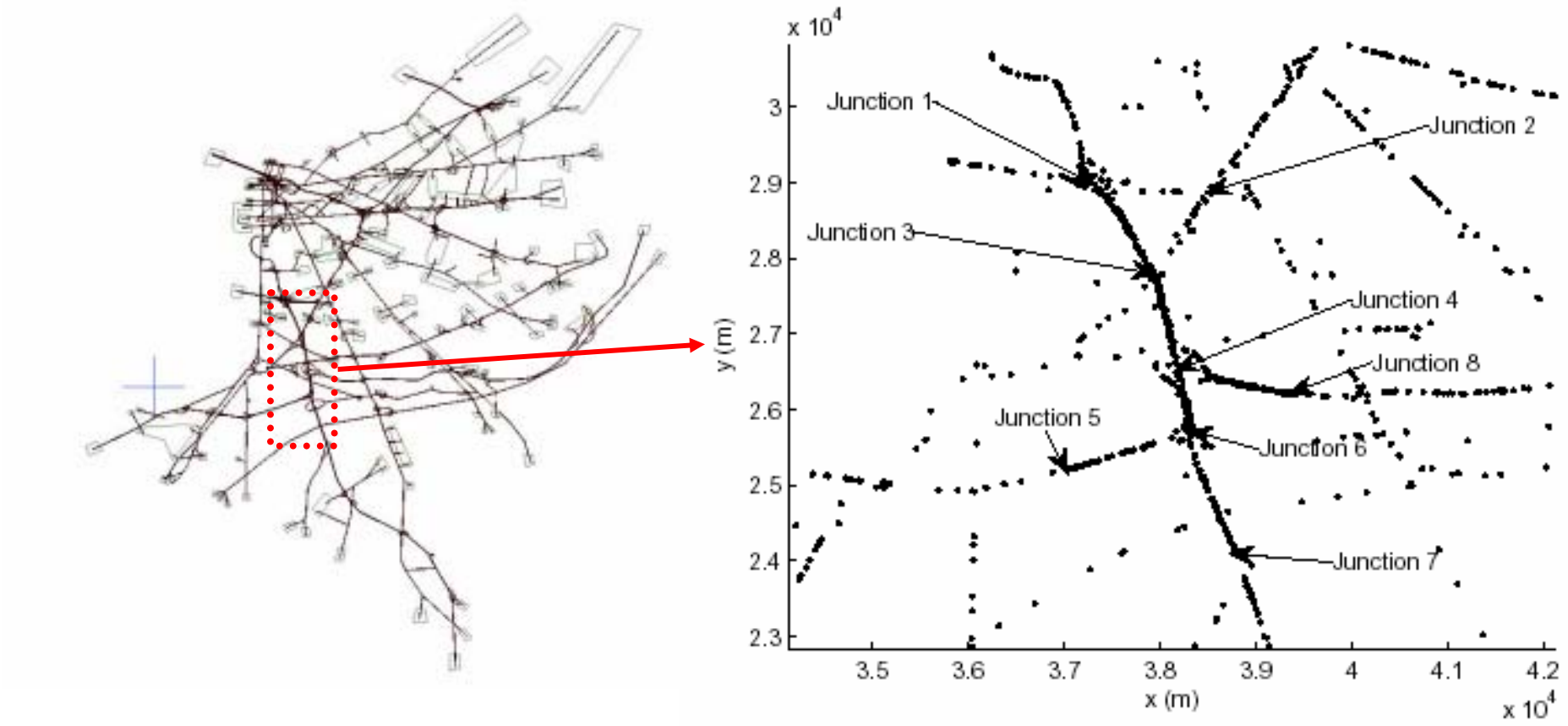
- V’ = α*n*Cr + V (α is a constant)
- A traversal of the road network graph





Simulation Results: VANET

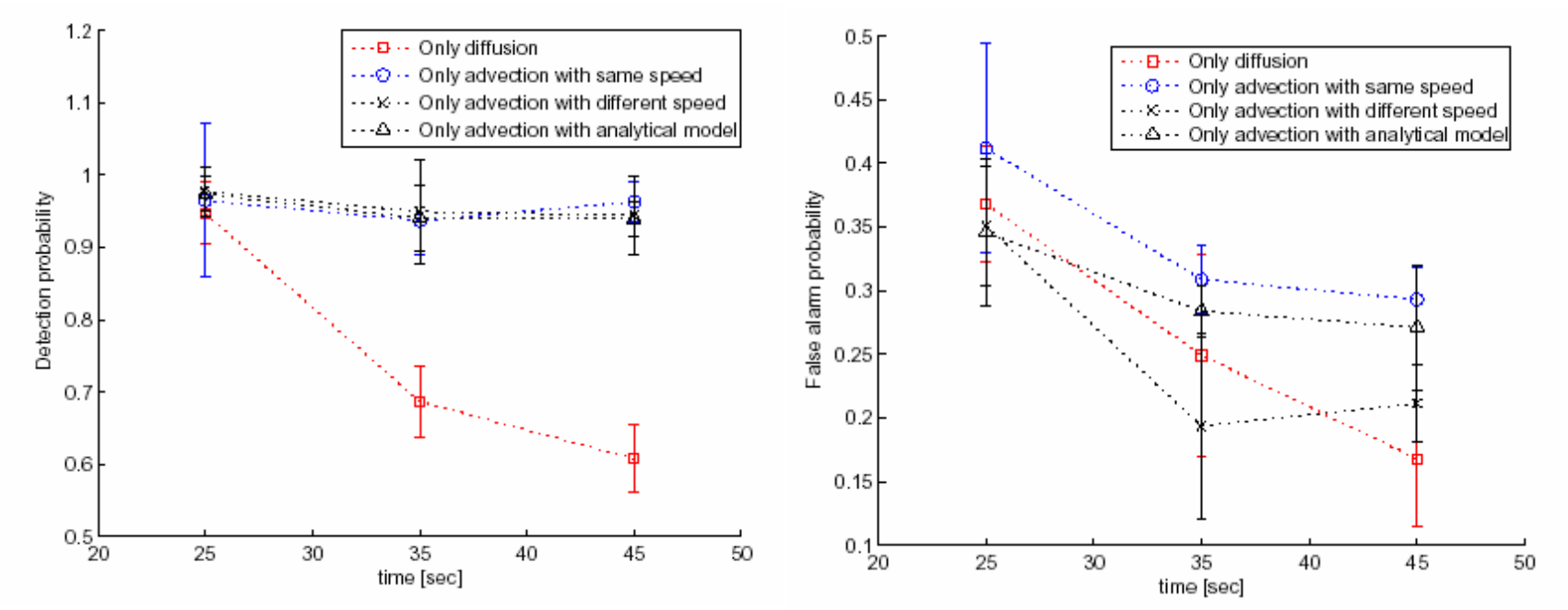
- Southern New Jersey Highway Network



Experiment setup

- Performance measures
  - Detection probability, False alarm probability
- Simulation parameters
  - SIR model (infection probability=1)
  - Randomly chosen initially infected nodes on the link between J3 and J4
  - Observation Time (25 sec ~ 45 sec)
  - Communication range (50m, **100m** and 200m)
  - Vehicular scenario: PARAMICS → Calibrated from real traffic data

Detection Probability & False Positive



Discussion

- 95% detection probability can slow the propagation of a worm
  - It yields additional analysis time for patch
  - It can act as a short-term defense
  - Repeated application of intrusion response
- Analytical model for V' works enough
  - It doesn't need a laboring job (no prior information) → only V and R from D.O.T.
  - 10% inferior to the best in Pf
- Patient 0 detection should be solved
  - Effect of inaccuracy on Pd & Pf
  - Method: Triangularization and Recursive Least Square

Conclusion & Further works

- We proposed an architecture for a service provider
  - Infrastructure-based approach
  - Location-based quarantine boundary estimation
- We verified algorithm to real road networks
- Patient 0 detection algorithm
- Design of robust algorithm to inaccurate patient 0 and time of outbreak.
- State wide area simulation (NJ Turnpike)
- Ecology – Security synergy: a stratified dispersal process