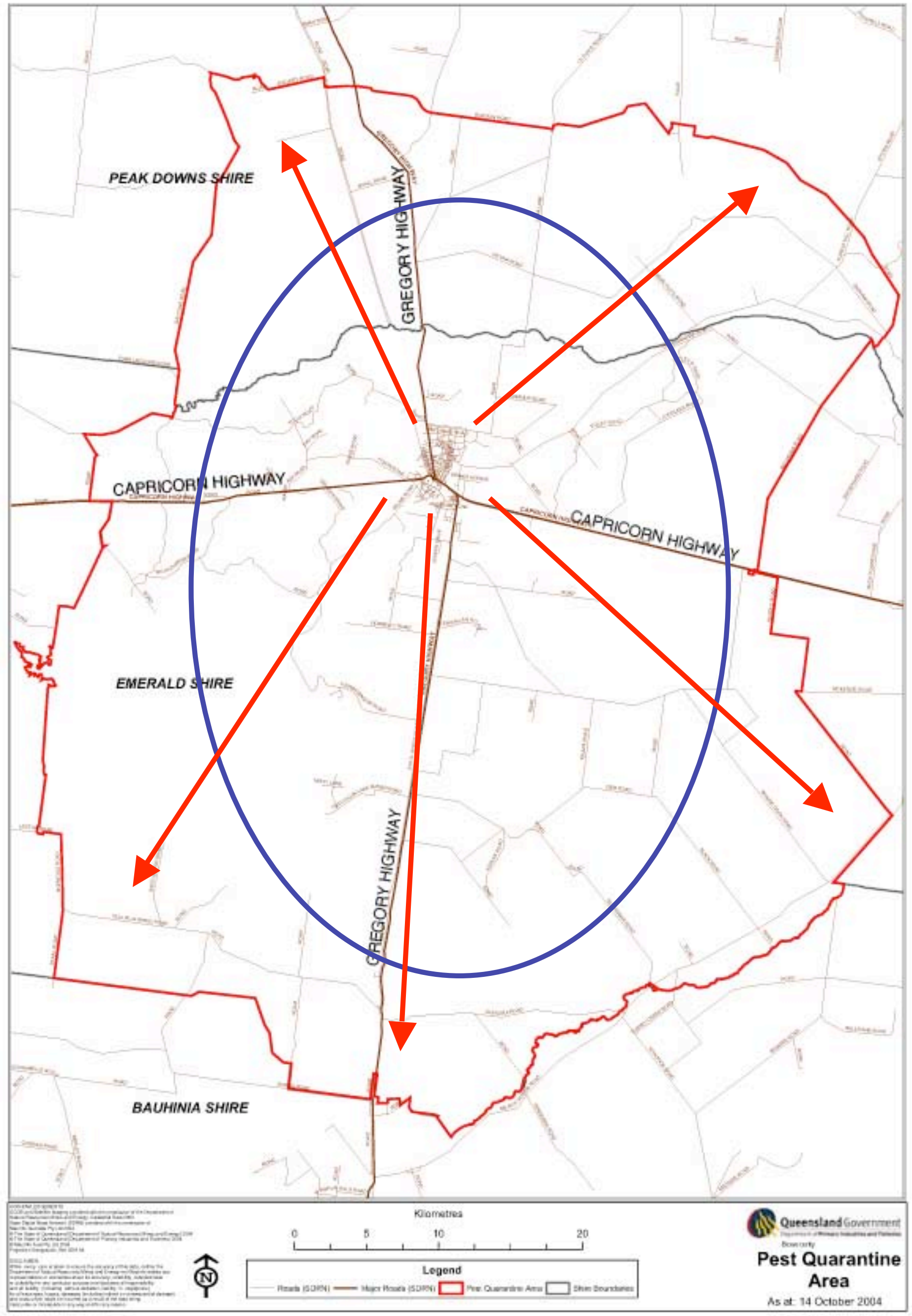
Computer Ecology: Responding to Mobile Worms with Location-Based Quarantine Boundaries

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

Pest Quarantine Area Map in Australia



Mobile Worm, 'Cabir'

- A Cabir outbreak at the packed ad hoc network, Helsinki Olympic Stadium (300 nodes in 50m–by–50m)
- Characteristics:
  - Multi–radio support → <u>direct local interactio n</u> (e.g., Bluetooth) → Alternative propagatio n path of worms/virus
  - Mobility (V): traffic pattern related
  - Limited connectivity (Cr): geographical prox imity (within 10m≈30feet)

Wired Intrusion Detection

- Conventional scheme [4, 5]
  - Prevention, Treatment and Containment
  - Containment technique is characterized by
    - Reaction time (How fast?)
    - Detection method (anomaly / signature-based)
    - Strategy (address blacklisting / content filtering)
    - Deployment scenario (placing containment syst ems)

Wireless Intrusion Detection

- Simple example[3] (in wireless network)
  - Resource constrained: mobile nodes instea d of routers, gateways or firewalls
  - Cooperation needed (mobile devices or ho neypot devices) → delay
  - Human analysis needed due to a high false alarm probability → delay
  - We don't have any practical ad hoc networ k example nor IDS

$$\Delta T = T_A - T_O$$

- There exists a time delay between outbreak to alarm. The reasons are:
  - Distributed processing delays
  - Communication processing delays
  - Human analysis
- Effects of ΔT
  - During this time, malware can spread further → imperfect containment

Assumptions

- Patient 0: the analyst can accurately loc ate the patient 0
- T_o: time of outbreak
- Location server (infrastructure): service provider can locate each mobile node.

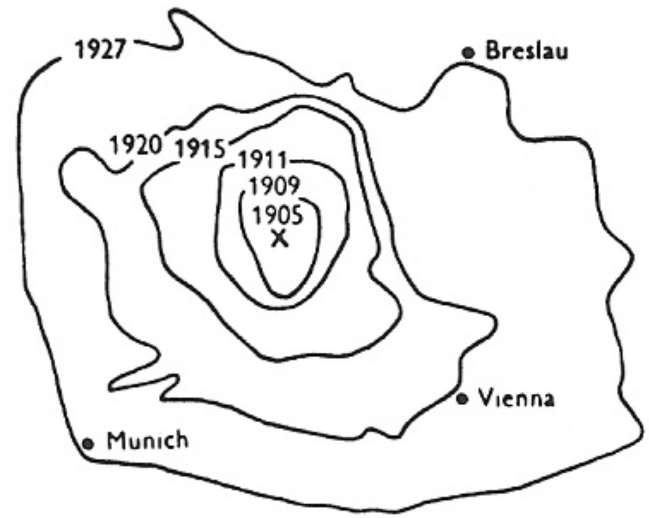
- How about inaccurate T_o and patient 0?
→ more robust algorithm needed!!

Wireless Intrusion response architecture

- Possible responses given Open Mobile Alliance Client Provisioning Architecture
  - sends a warning
  - turns off the compromised nodes
  - disables local interaction
  - installs patches
  - installs port or content-based filters
- Intrusion response planning problem
  - Def: identifying an optimal set of infected nodes
  - Requires a quarantine boundary

A Macroscopic Models of Worm Propagation from Ecology

- Spread of muskrats in Europe (1905)
- Dispersal was modeled by diffusion model (Skellam,1951)
- Hostile barrier might be needed to halt the spread of muskrats



- Estimating quarantine boundary in mobile worm is an analogous problem
- Toxic pollutants in under groundwater
  - Advection term (explaining the mean flow) is added to diffusion-reaction equation

Cont. (PDE)

- Diffusion-reaction equation

$$\frac{\partial S}{\partial t} = \frac{D}{r}\frac{\partial}{\partial r}\left(r\frac{\partial S}{\partial r}\right) + \alpha S \qquad (1)$$

$$S = (m/4\pi Dt)\exp(\alpha t - r^2/4Dt) \qquad (2)$$

$$R = 2\sqrt{\pi\alpha D}t \qquad (3)$$

- Advection equation only

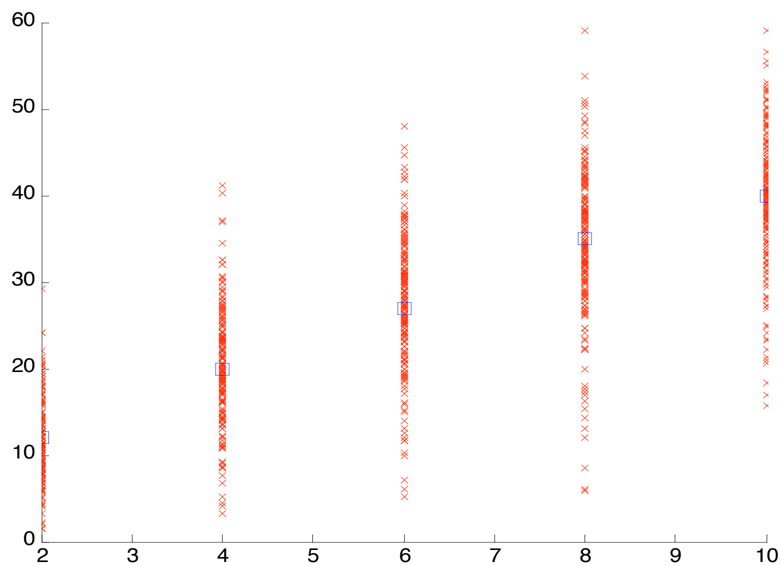
$$\frac{\partial S}{\partial t} = -\frac{\partial}{\partial x}(uS) - \frac{\partial}{\partial y}(vS) + \alpha S \qquad (4)$$

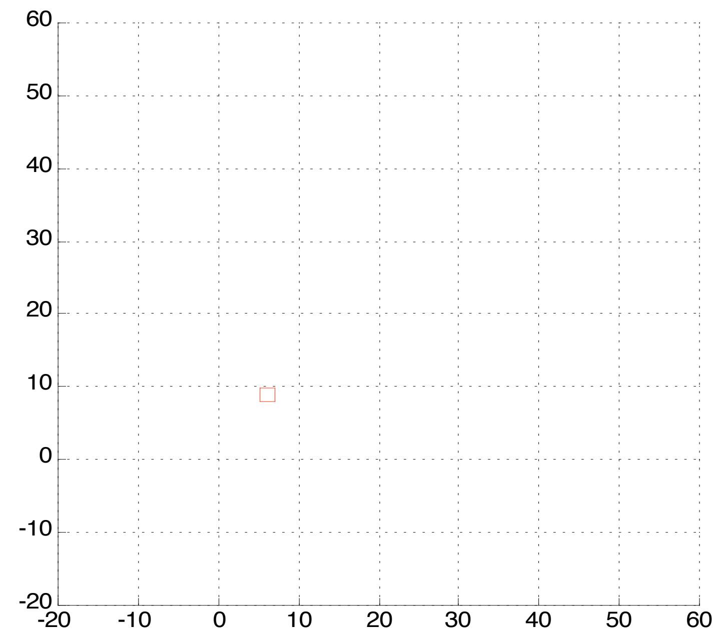
Quarantine boundary estimation

- Propagation speed (v'):
  - Isotropic circle ($R = v' * \Delta T$)
  - Rectangle ($L = v' * \Delta T$)
- Question) How to estimate ' v' '?
- Answer)
  - Pedestrian scenarios: empirically simulation -based approach
  - Vehicular scenarios: simple analytic eq.

Preliminary example: Estimating Diffusion in Random Walk Model

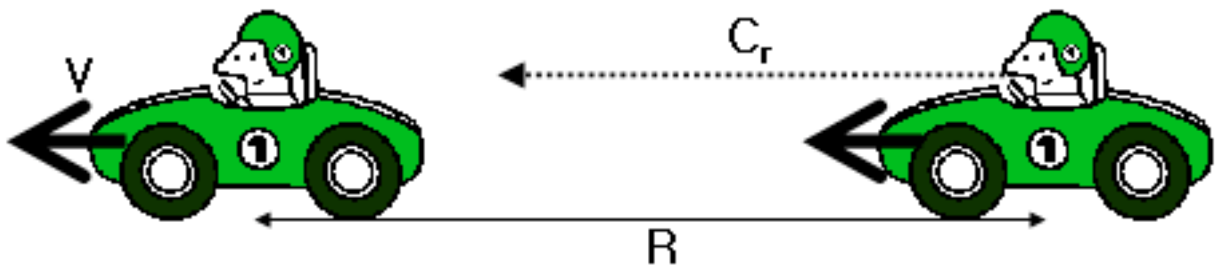
- Boundary estimation (r) and response



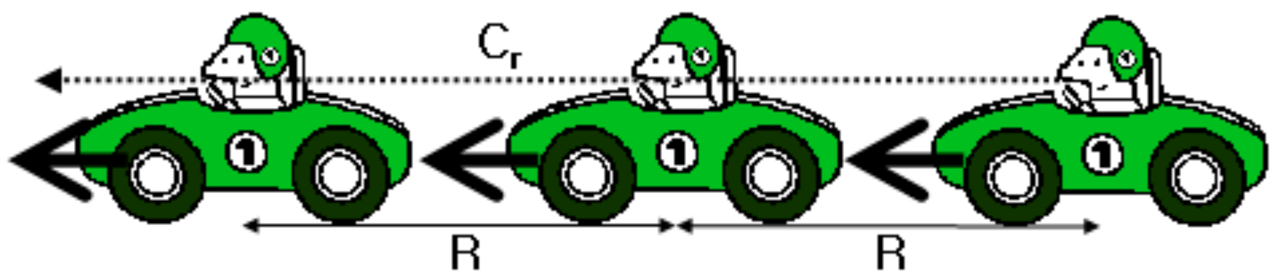


- What if the infected nodes move with the mea n flow (=advection)?

Algorithm: Propagation speed est imation



(a) Full speed

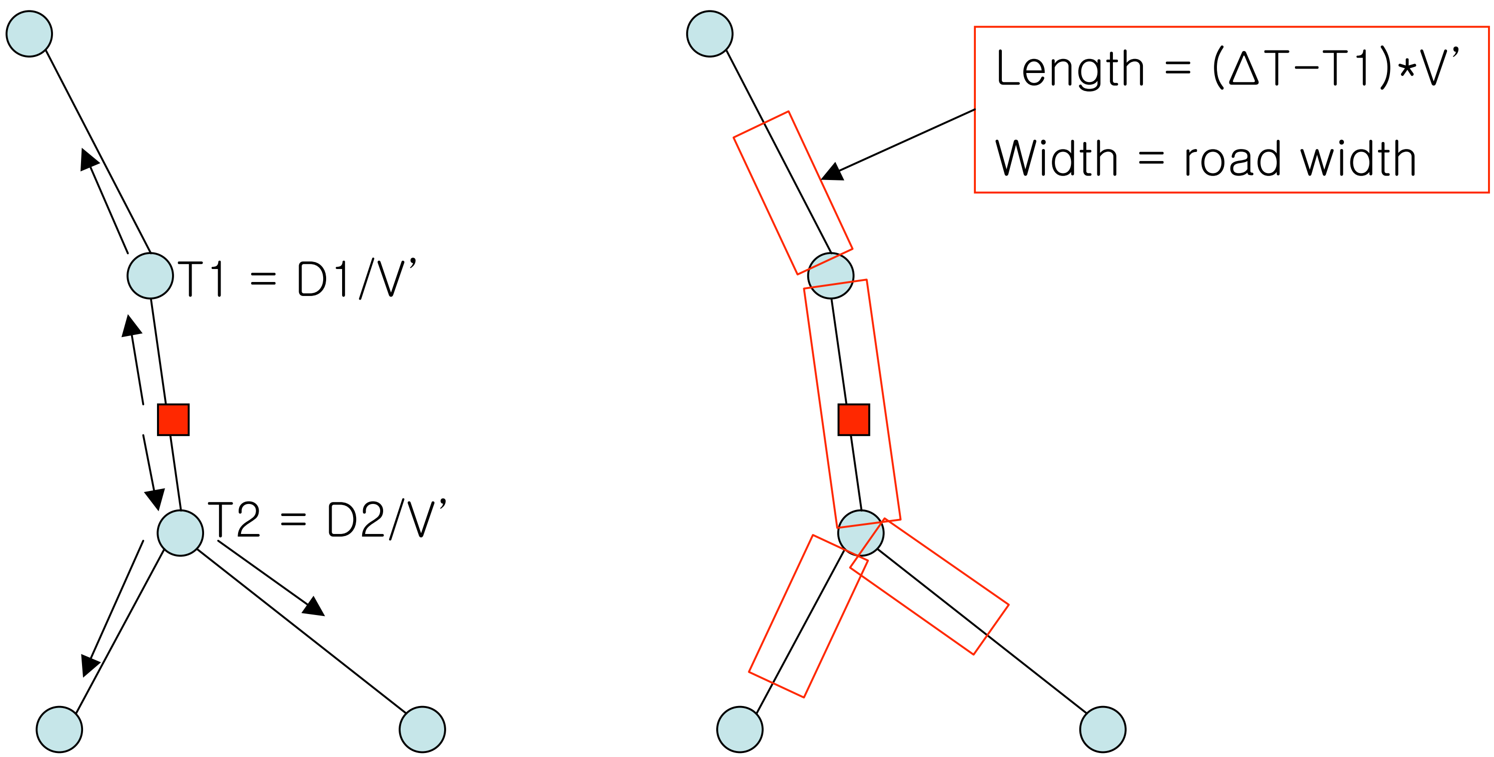


(b) Traffic jam

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

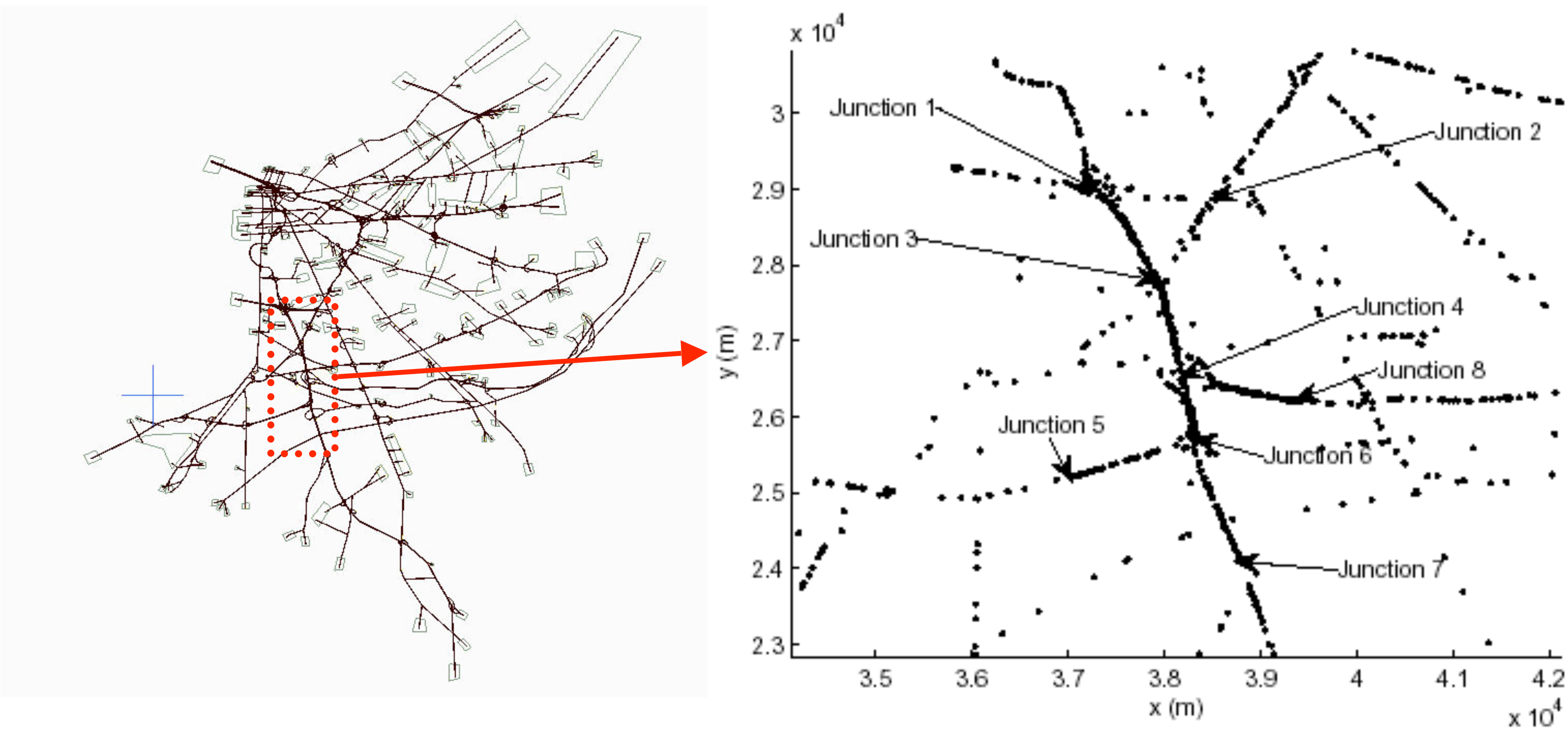
Algorithm: Spatial Boundary

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



VANET (1st step: map extraction)

- Southern New Jersey Highway Network



VANET (2nd step: Road classification)

- Inter-State highway (e.g., NJ-Turnpike)
  - It has fewer entries and exits
  - Advection only
- State highway (e.g., Route 18, Route 1, 287)
  - It has many entries and exits on local roads while It has mean flows
  - Advection-diffusion
- Local roads network
  - It can be modeled by 2D-random walk, thus diffusion only

VANET (3rd step: polygon merge)

- Build an advection model
  - Using traversal of the road network graph and a propagation speed estimation
- Rectangular quarantine boundary
  - width: the number of lanes on each road
  - length: the frontal wave of propagation
- Merge rectangles into polygon
  - Implementation by ‘Polybool’ function in MATLAB
- Check nodes within polygon
  - By using ‘Point in Polygon’ algorithm

Evaluation

- Measures
  - Detection probability (Pd)
  - False alarm probability (Pf)
  - Jaccard similarity

$$J = \frac{2\left(|X \bigcap Y|\right)}{|X| + |Y|} = \frac{2P_d(1 - P_f)}{1 + P_d - P_f}$$

- Target scenarios
  - A vehicular ad hoc network (VANET)
  - Ex. Southern New Jersey Highway Networks

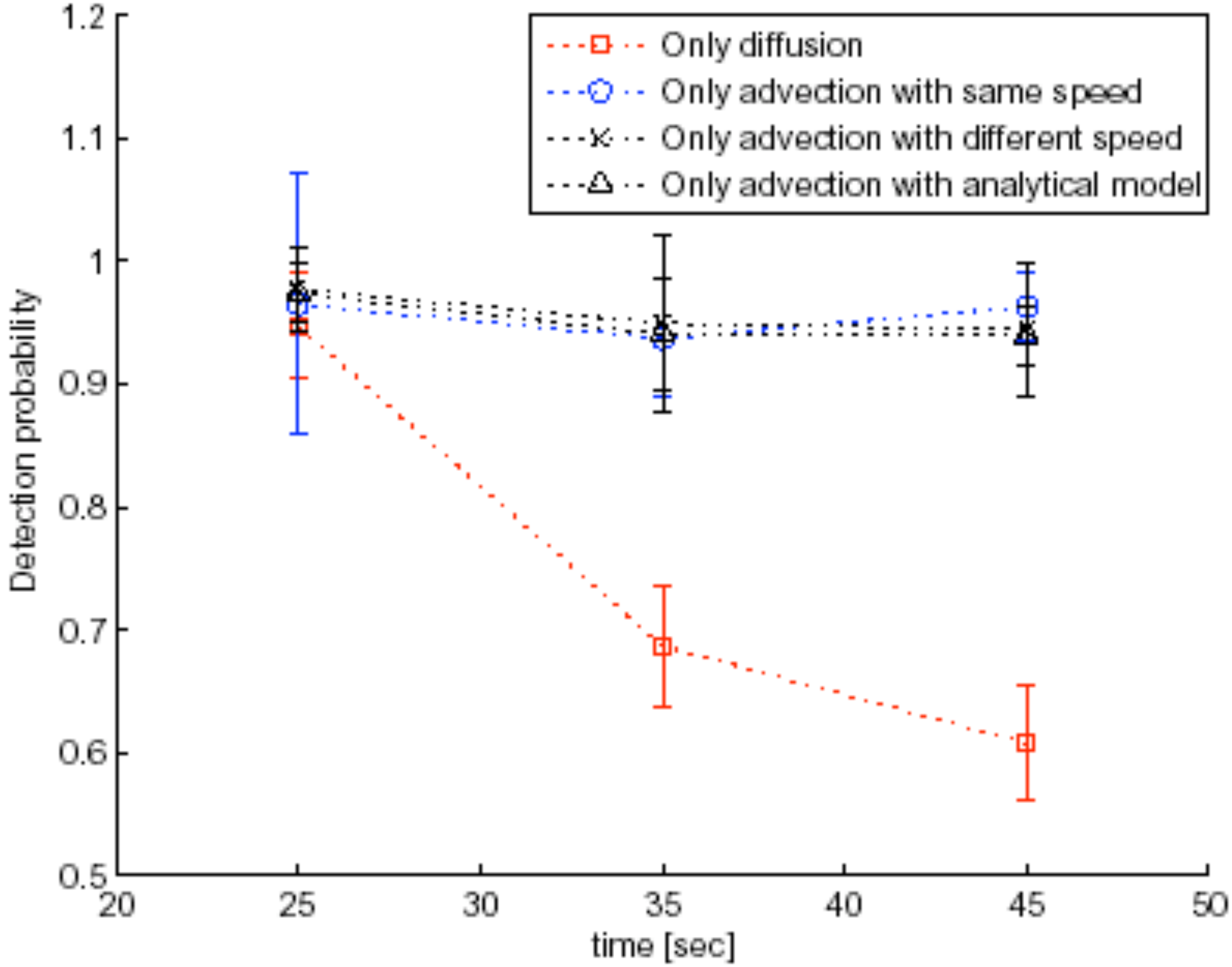
Cont.

- Simulation model
  - SIR model (infection probability=1)
  - Randomly chosen initially infected nodes on the link between J3 and J4
  - Time delay (25 sec ~ 45 sec)
  - Communication range (50m, 100m and 200m)
  - Vehicular scenario
    - PARAMICS → Calibrated from real traffic data
    - Southern New Jersey Highway network
    - x, y position was recorded at every 0.5 sec

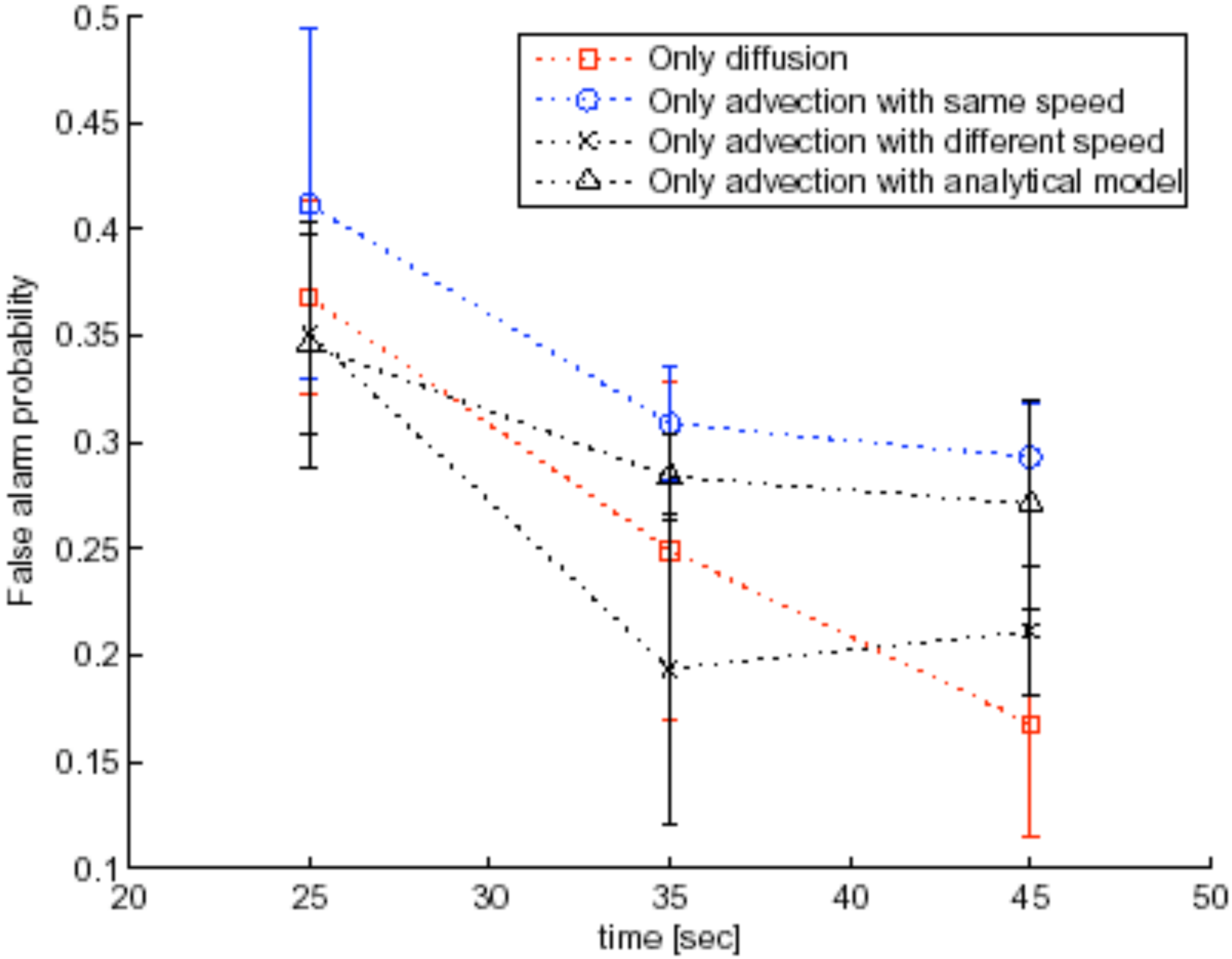
Results (VANET)

- Baselines to compare
  - Diffusion-reaction model (A)
  - Advection model
    - With having same propagation speed on all roa ds (B.1)
    - With having different estimated propagation spe eds on all roads from empirical method (B.2)
    - With having different estimated propagation spe eds on all roads from analytical model (B.3)

Cont. (Detection Prob.)



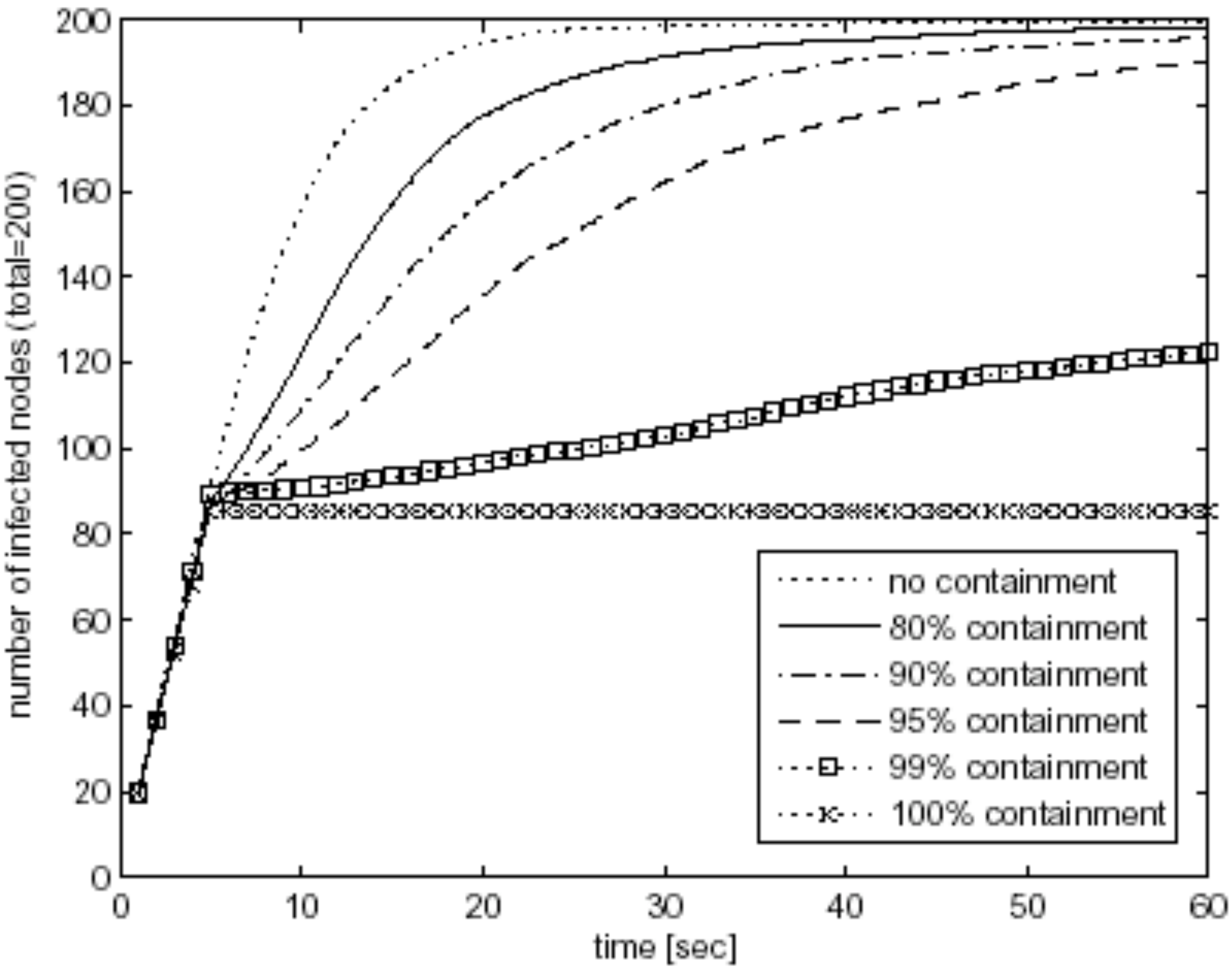
Cont. (False-alarm Prob.)



Discussion

- Imperfect containment:
  - But 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
- For the optimum Jaccard similarity:
  - We choose a smaller radius than R
- Repeated application of intrusion respo nse

Imperfect containment



Discussion (Ecology and Worms)

- Allee effect
  - Def) reduced per capita reproduction when animals are scarce
  - Useful for describing the dynamic change of the infection rate
- Two competing species (Predator-Prey model) propagation
  - Useful for competition or cooperation of m alicious codes

Other Related Work

- 1. Khayam and Radha (MSU)
  - Infection rate of active worms over time in VANET
- 2. Wu and Fujimoto (Gatech)
  - Information propagation speed in VANET
- 3. Zhang and Lee (Gatech)
  - Intrusion detection for wireless ad hoc network
- 4. Moore and colleagues (CAIDA)
  - The existing containment methods for Internet
- 5. Vern Paxson (ICIR)
  - Modeling malware via PDE from epidemiology

Conclusion

- We proposed an architecture for a servi ce provider
  - In hybrid ad hoc network (with wide-area in frastructure network)
  - Location-based quarantine boundary estim ation techniques (diffusion & advection)
  - The results on application of algorithms to r eal road networks

Further works and comments

- Analytic approach for estimating v’ in pedestri an scenarios and α in VANET
- State wide area simulation (NJ-Turnpike)
- Design of robust algorithm to inaccurate patie nt 0 and time of outbreak.
- Estimation of the propagation speed from intr usion reports
- Maintaining partial outages of the wide-area wireless network after intrusion response