On Modeling and Understand Vehicle Evacuation Attacks in VANETs

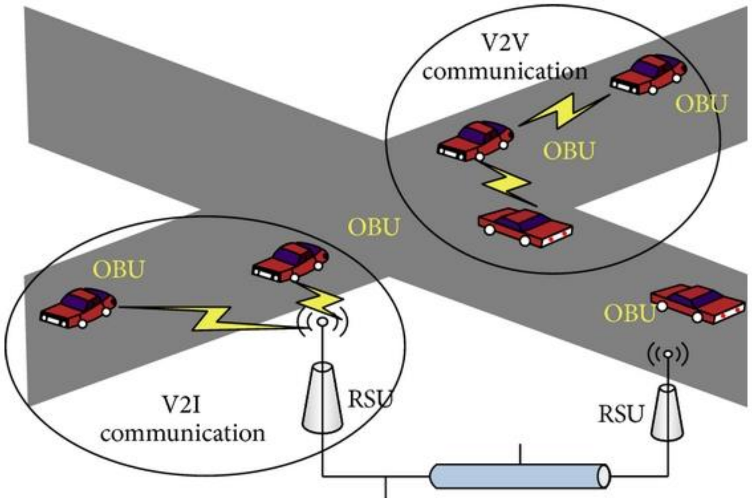
MINGKUI WEI, SAM HOUSTON STATE UNIVERSITY

ZHUO LU, UNIVERSITY OF SOUTH FLORIDA

WENYE WANG, NORTH CAROLINA STATE UNIVERSITY

VANET Security

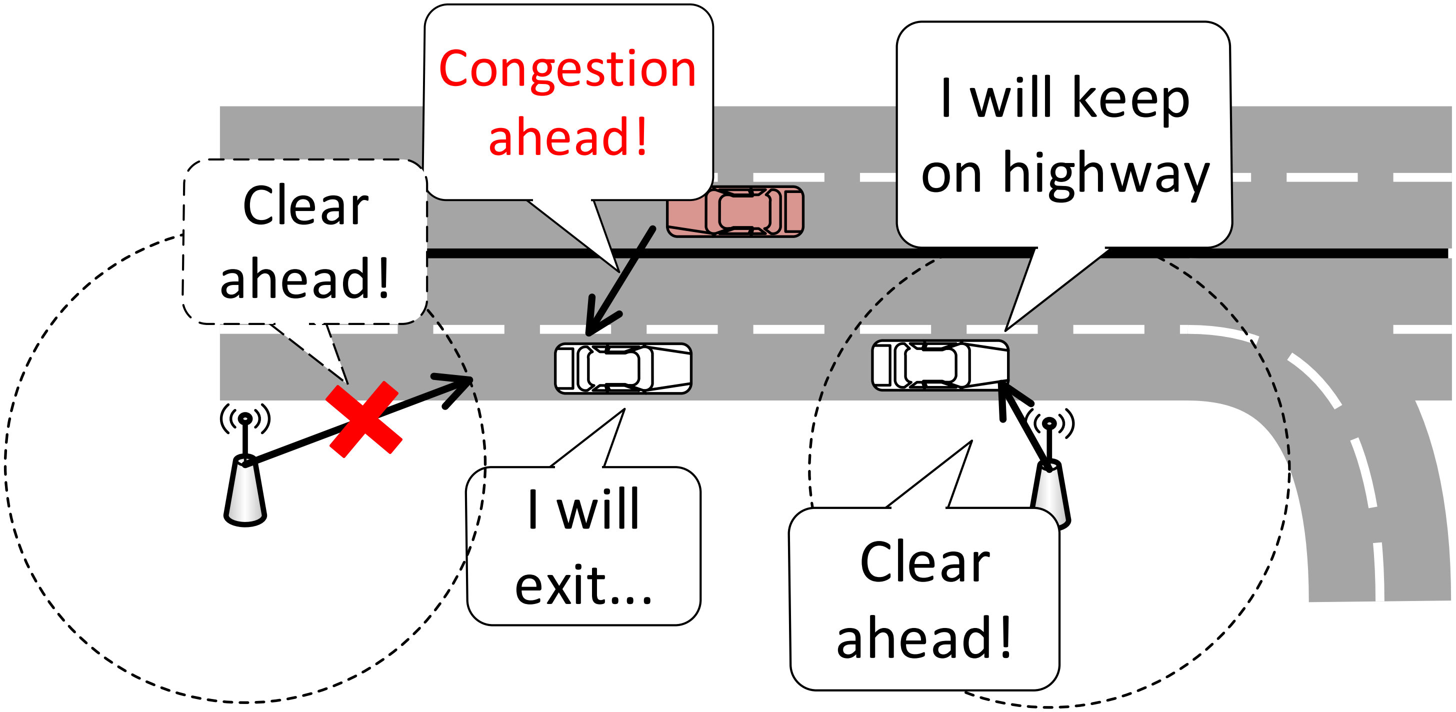
- Vehicular Ad-hoc Network
  - V2V and V2I network.
  - Authentication in partially connected, distributed and highly dynamic network.



- Existing works:
  - Secure authentication infrastructure [Li'07, Nowey'06].
  - Protocols to preserve user privacy [Zhang'11, Pan'13].

- What's Missing:
  - Rely on communications, which are not reliable in VANET.
  - Not effective with extreme long delay.

Motivation



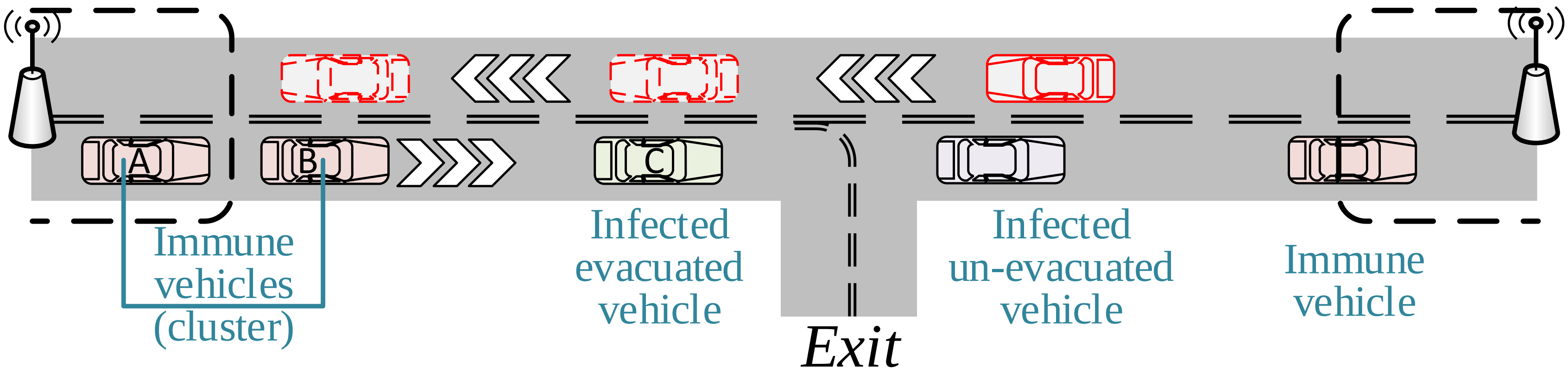
- Physical character matters!
- Inherited from delayed information exchange, and is unavoidable.
- Understanding and minimizing the impact are imperative.

Research Question

- Research Questions
  - How message delay escalates the consequence of cyber-attacks in the physical domain?

- Objectives
  - *Model* the vehicle evacuation attack.
  - *Identify* the correlation between delay and security.

Vehicle Evacuation Attack: the Model



- When the malicious and benign vehicles are in contact:
  - Immune: vehicles that are still connected to RSU.
  - Infected: vehicles that are not connected to RSU.
  - Evacuated: infected vehicles that has an Exit in front.
- Objective:
  - Number of infected/evacuated vehicles.
  - Correlation between such number and message delay.

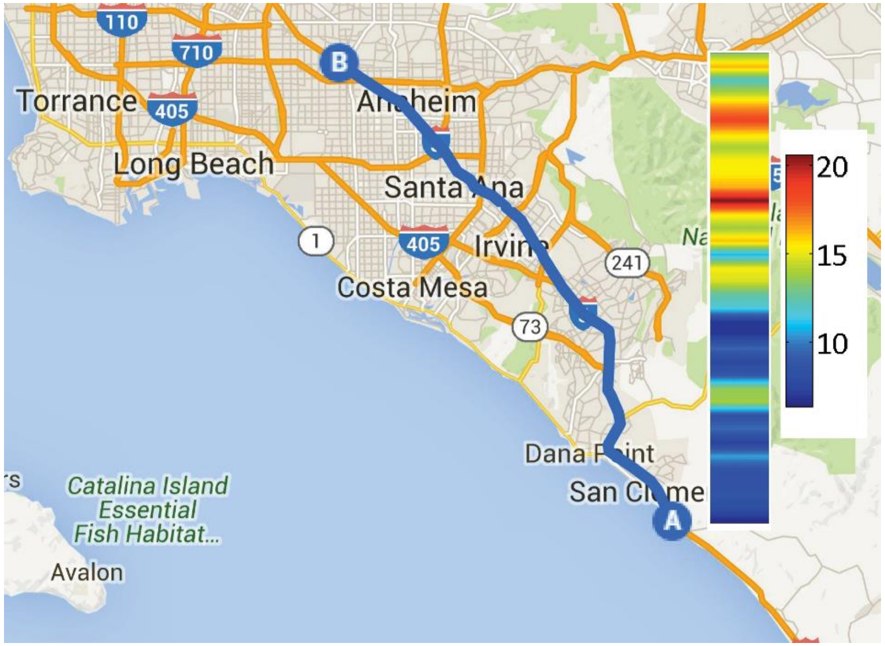
Challenges and Approaches

- Challenges
  - Model the Vehicle Evacuation Attack.
    - Connectivity of vehicles.
    - Practical distribution of vehicles on the highway.

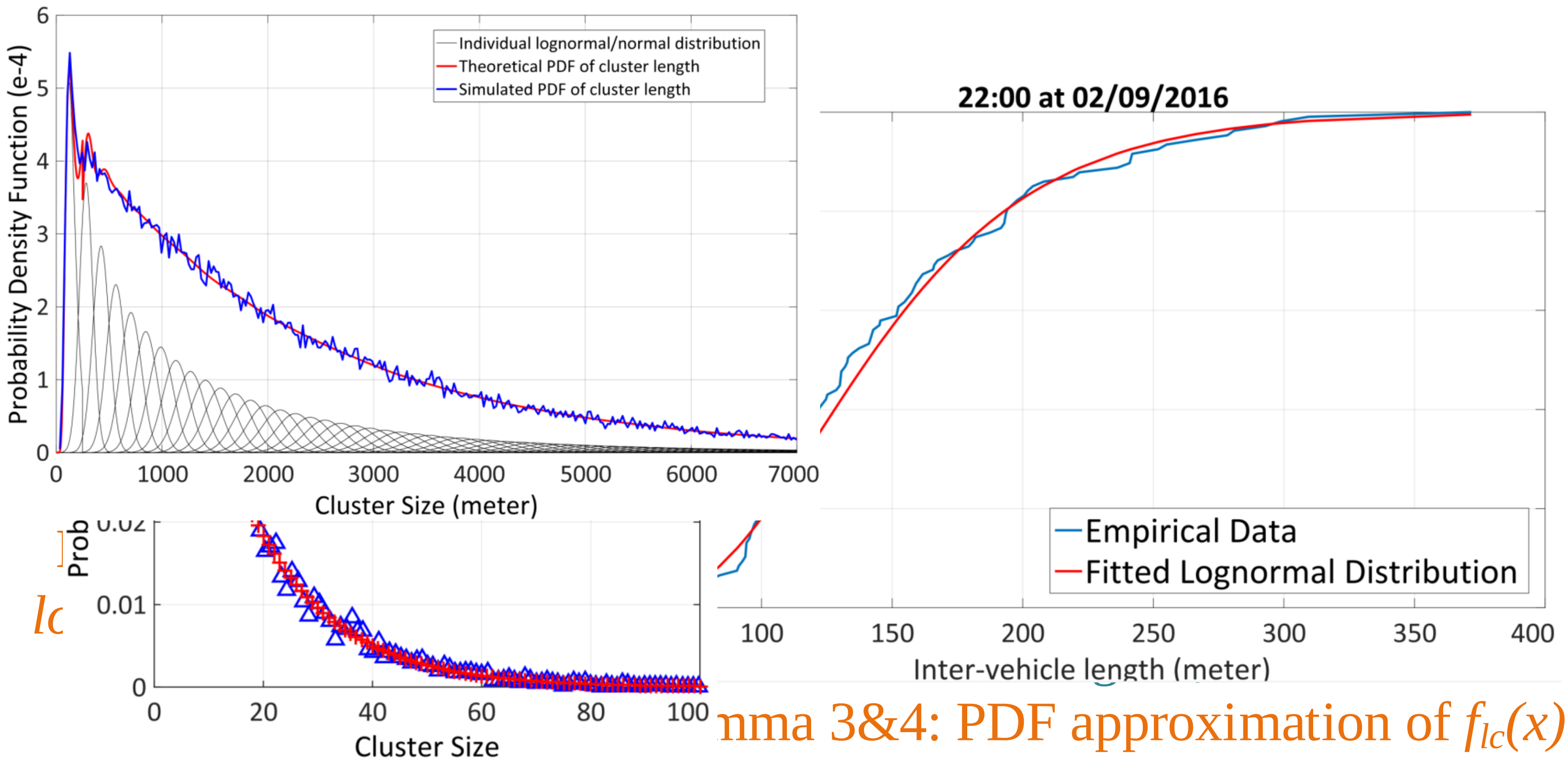
- Approaches
  - Obtain a real-world transportation dataset.
  - Derive statistical properties of vehicles and clusters.
  - Mathematically model and evaluate the attack.

PeMS: the Dataset

- Caltrans Performance Measurement System (PeMS).
  - Managed and released by the Department of Transportation.
  - Chose the section Interstate 5 Northbound (I5-N), CA.
  - 44.4 miles long.
  - 333 sensors.



Vehicles' Statistical Properties



...mma 3&4: PDF approximation of $f_{lc}(x)$

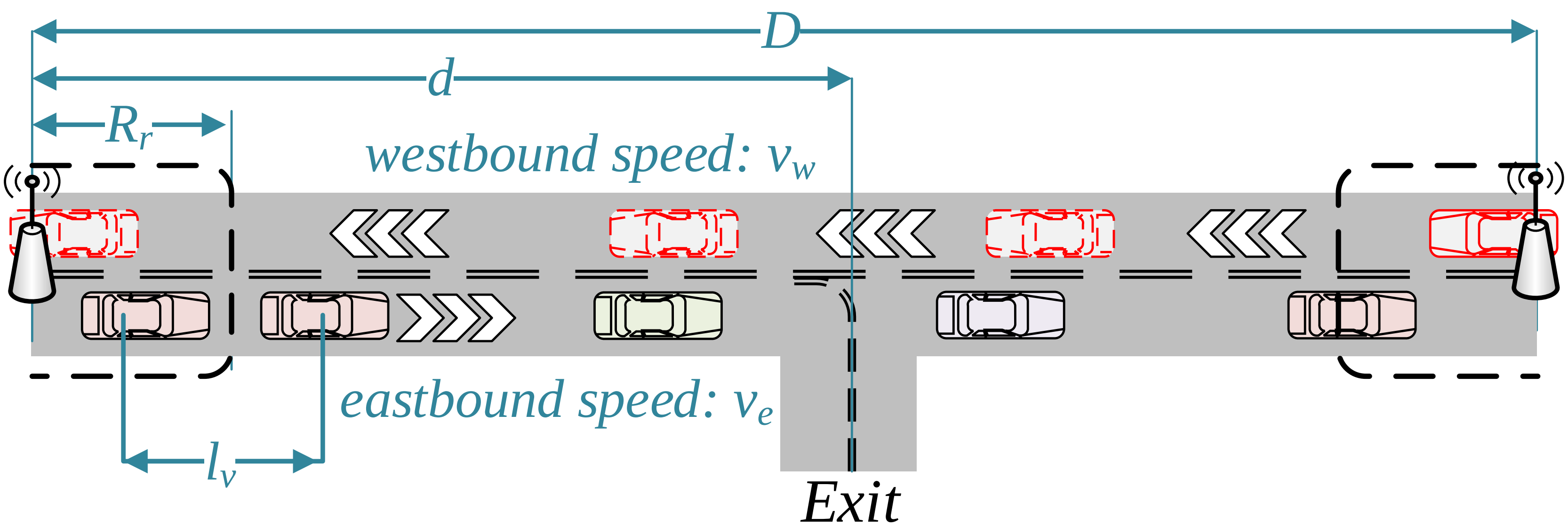
- Lemma 1 & 2: dataset analysis.
- Lemma 3 & 4: Innovative proposal based on classic theory and simulation observation.

Theorem: Evacuated Vehicles

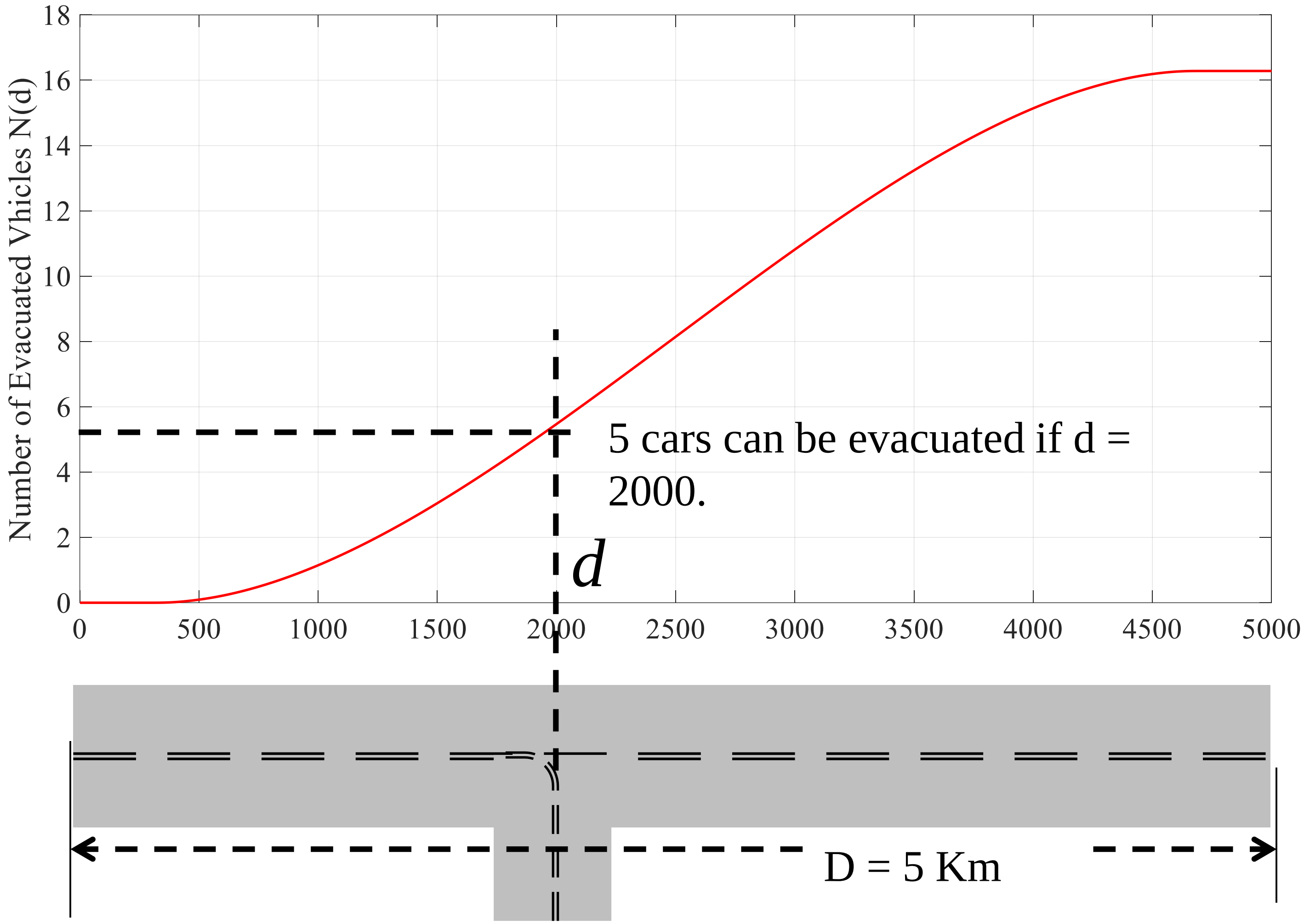
The number of evacuated vehicles is given by:

$$N(d) = \frac{(1+v)}{E[l_v]} \int_0^d \left(\int_0^{x-R_r} f_{l_c}(y)dy \cdot \int_0^{D-R_r-x} f_{l_c}(y)dy \right) dx,$$

where $v = v_e / v_w$.



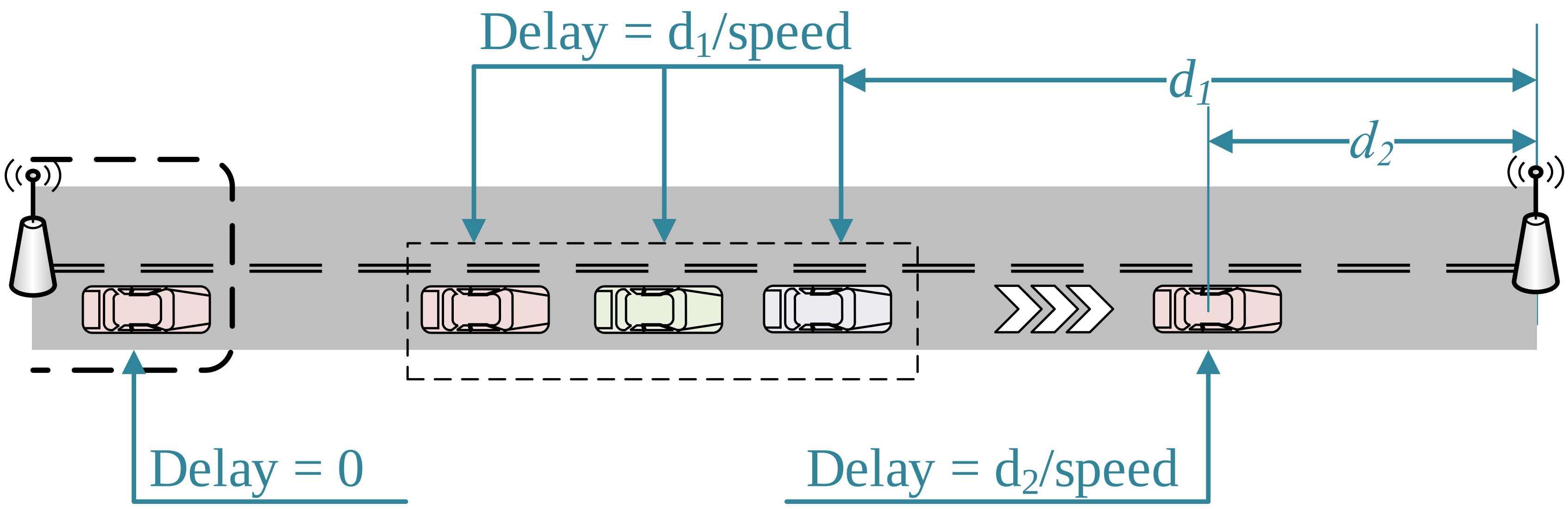
N(d) Increase According to d



Theorem: Average Message Delay

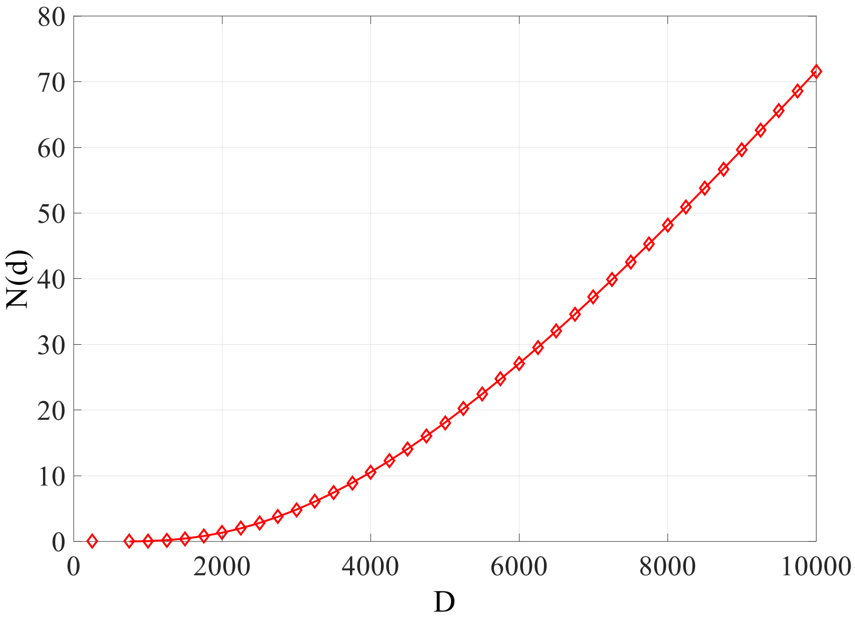
The average message delay is given by:

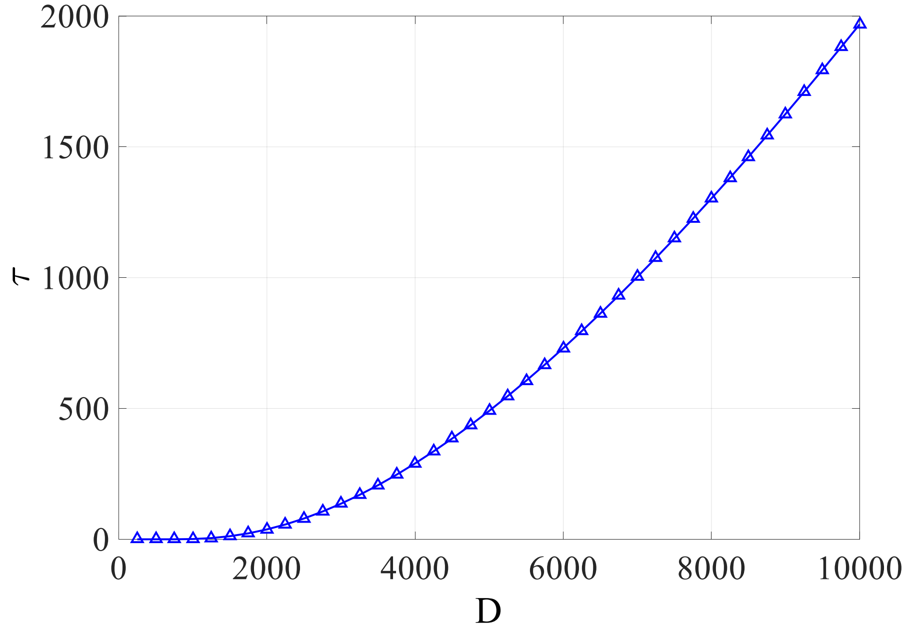
$$\tau = \int_0^{D-2R_r} f_{l_c}(x) \frac{(D-2R_r-x)^2(D-2R_r-2x)}{2vD^2} dx.$$



Comparison between τ and $N(d)$

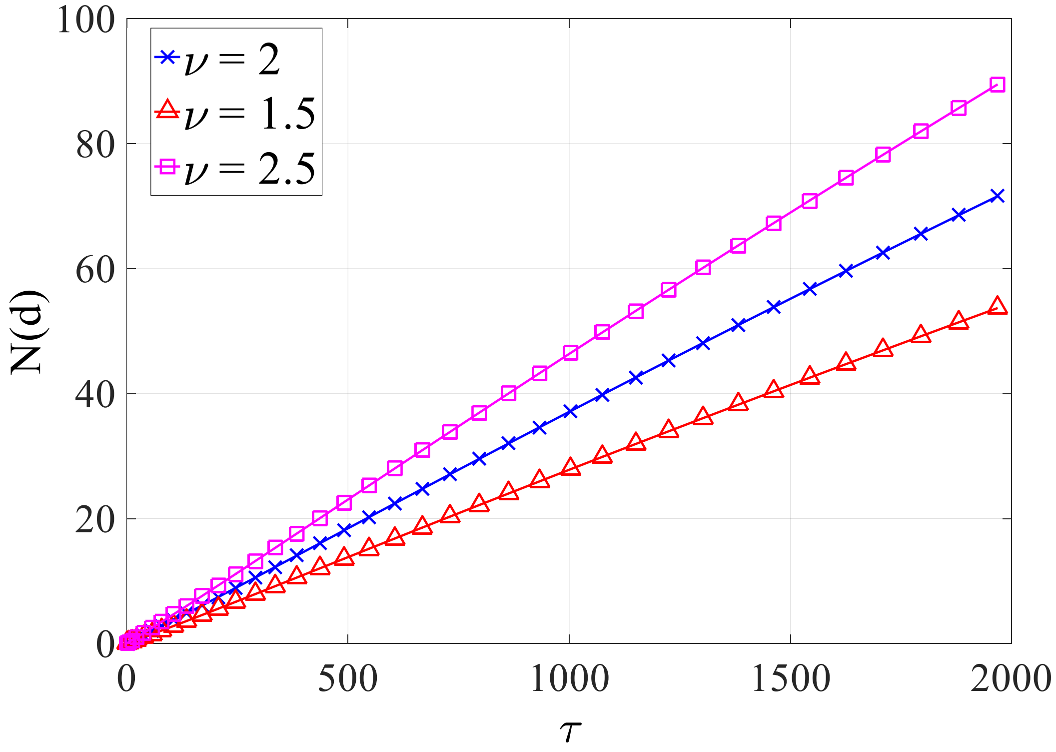
- Question: correlation between delay and security?





- Left figure: $N(D)$ as D changing.
- Right figure: τ as D changing.
- Observation: same trend, different scale.

Correlation between τ and $N(d)$



- Plot of $\tau - N(D)$: *linear relationship*.
- Reducing delay and enhancing security can be implemented at the same time.

Conclusion

1. It is critical to study the cyber-system (VANET) in the context of the cyber-physical system (Intelligent Transportation System).
2. Message delay is linearly related to the significance of vehicle evacuation attack.
3. Identified statistical characters of vehicles on the highway system.

Thank you!

Thank you

Please address any of your questions to Mingkui Wei (mwei@shsu.edu).