Towards formalization of wireless vehicular networking

Ramneet Kaur, Jungyeol Kim, Oleg Sokolsky, Saswati Sarkar, Radoslav Ivanov, Insup Lee

PRECISE LAB

School of Engineering and Applied Science

University of Pennsylvania

04/17/2020

Outline

- Motivation
- Problem statement
- Related work
- Contributions
- Background
  - Clustered epidemiological differential equations (CEDE) in vehicular networks
  - Hybrid systems
- Formalization of the CEDE representable V2X transportation system
  - CEDE representation of the V2X transportation system
  - Hybrid System for the CEDE representable V2X transportation system
  - Analysis of the V2X transportation system modeled as the hybrid system
- Case study
  - Example of a V2X equipped transportation system
  - CEDE for the considered system
  - Transportation system for the considered system
  - Analysis of the desired properties as reachability problems in the hybrid system
  - Experiments for reachability in Flow*
    - For safety and congestion properties
    - For analysis of V2X network policies
- Future work

Motivation

- Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) technologies, together V2X, enable vehicles to wirelessly exchange important safety and congestion information
- This exchange is expected to help save lives, prevent injuries and ease traffic congestion

Motivation

- Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) technologies, together V2X, enable vehicles to wirelessly exchange important safety and congestion information
- This exchange is expected to help save lives, prevent injuries and ease traffic congestion
- The realization of this promise however critically depends on the deployment of judicious wireless and vehicular control strategies
- To that end, one needs mechanisms to model, evaluate and control V2X

Motivation

- Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) technologies, together V2X, enable vehicles to wirelessly exchange important safety and congestion information
- This exchange is expected to help save lives, prevent injuries and ease traffic congestion
- The realization of this promise however critically depends on the deployment of judicious wireless and vehicular control strategies
- To that end, one needs mechanisms to model, evaluate and control V2X, which is what we seek to obtain by proposing deployment of formal methods in the field of V2X

Problem Statement

- Modeling a V2X equipped transportation system as a hybrid system that allows
  - Formal verification of the desired properties, such as safety, congestion, etc., of the V2X equipped transportation system

Problem Statement

- Modeling a V2X equipped transportation system as a hybrid system that allows
  - Formal verification of the desired properties, such as safety, congestion, etc., of the V2X equipped transportation system
  - Analysis of the V2X network policies followed in the transportation system

Related work

- A recent work [1] proposed modeling of V2V equipped transportation system as Clustered Epidemiological Differential Equations (CEDE)
    - As the number of vehicles increase, under some regularity condition, the distribution of vehicles in a stochastic model for V2V converge to the solutions of the deterministic CEDE
- The paper
    - Does not considers modeling of the transportation system to capture abrupt changes in the system
    - Does not formalizes safety and congestion objectives of the transportation system, let alone verify those

[1] J. Kim, S. Sarkar, S. S. Venkatesh, M. S. Ryerson, and D. Starobinski, "An epidemiological diffusion framework for vehicular messaging in general transportation networks," Transportation Research Part B: Methodological, vol. 131, pp. 160–190, 2020.

Contributions

- This work complements the research in [1] by
  1. Extending the modeling approach of [1] to capture abrupt changes caused by traffic and communication flow in the system by modeling a CEDE representable V2X transportation system as a hybrid system

Contributions

- This work complements the research in [1] by
  1. Extending the modeling approach of [1] to capture abrupt changes caused by traffic and communication flow in the system by modeling a CEDE representable V2X transportation system as a hybrid system
  2. Proposing verification of desired properties for the V2X transportation system by verifying these properties on its proposed hybrid system via reachability

[3] X. Chen, E. Abraham, and S. Sankaranarayanan, “Flow*: An analyzer for non-linear hybrid systems,” in International Conference on Computer Aided Verification. Springer, 2013, pp. 258–263

Contributions

- This work complements the research in [1], [2] by
  1. Extending the modeling approach of [1] to capture abrupt changes caused by traffic and communication flow in the system by modeling a CEDE representable V2X transportation system as a hybrid system
  2. Proposing verification of desired properties for the V2X transportation system by verifying these properties on its proposed hybrid system via reachability
  3. Verifying the safety and congestion properties of an example of a CEDE representable V2X transportation system in Flow* [2]

[3] X. Chen, E. Abraham, and S. Sankaranarayanan, "Flow*: An analyzer for non-linear hybrid systems," in International Conference on Computer Aided Verification. Springer, 2013, pp. 258–263

Contributions

- This work complements the research in [1], [2] by
  1. Extending the modeling approach of [1] to capture abrupt changes caused by traffic and communication flow in the system by modeling a CEDE representable V2X transportation system as a hybrid system
  2. Proposing verification of desired properties for the V2X transportation system by verifying these properties on its proposed hybrid system via reachability
  3. Verifying the safety and congestion properties of an example of a CEDE representable V2X transportation system in Flow* [2]
  4. Performing safety analysis of the V2X network policy followed in the example with the help of verification experiments performed in Flow*

[3] X. Chen, E. Abraham, and S. Sankaranarayanan, “Flow*: An analyzer for non-linear hybrid systems,” in International Conference on Computer Aided Verification. Springer, 2013, pp. 258–263

Background

1. Clustered epidemiological differential equations (CEDE) in vehicular networks [1]

- Road divided into J clusters
  - Vehicles move from cluster i to cluster j with mobility rate λ_{ij}

- Each vehicle on the road equipped with V2V technology

- One message propogated by V2V technology on the entire road
  - Message is propogated from cluster i to cluster j with communication rate β_{ij}

- Informed Vehicles (I) – Fraction of vehicles on the road that has received the message

$$\dot{I}_j(t) = -\sum_{k\neq j}^{J} \lambda^I_{jk} \cdot I_j + \sum_{k=1}^{J} \beta_{kj} \cdot I_k \cdot S_j + \sum_{k\neq j}^{J} \lambda^I_{kj} \cdot I_k \quad (j = 1, 2, \ldots, J)$$

- Non-informed vehicles (S) – Fraction of vehicles that has still not received the message

$$\dot{S}_j(t) = -\sum_{k\neq j}^{J} \lambda^S_{jk} \cdot S_j - \sum_{k=1}^{J} \beta_{kj} \cdot I_k \cdot S_j + \sum_{k\neq j}^{J} \lambda^S_{kj} \cdot S_k \quad (j = 1, 2, \ldots, J)$$

Background (Cont..)

2. Hybrid System

- Combination of discrete and continuous behavior

- Consists of
  - A set of modes with continuously evolving (or flowing) variables and
  - A set of discrete instantaneous transitions (representing jumps) between modes

Background (Cont..)

2. Hybrid System

- Combination of discrete and continuous behavior

- Consists of
  - A set of modes with continuously evolving (or flowing) variables and
  - A set of discrete instantaneous transitions (representing jumps) between modes

- Safety verification for hybrid systems is often viewed as a reachability problem
  - Given a hybrid system S, a set of initial states, I and a set of “safe” states for S, one can check if all executions of S starting from I stays within the set of safe states of S

CEDE representation of the V2X transportation system

- We extend the CEDE representation of the V2V to the V2X transporation system by
  - Introducing an additional term, η_i, representing the communication rate between non-informed vehicles in cluster i and a roadside infrastructure
  - η_i represents the V2I communication in the V2X technology

$$\dot{I}_j(t) = -\sum_{k\neq j}^{J} \lambda_{jk}^{I} \cdot I_j + \sum_{k=1}^{J} \beta_{kj} \cdot I_k \cdot S_j + \sum_{k\neq j}^{J} \lambda_{kj}^{I} \cdot I_k + \eta_j S_j \quad (j = 1, 2, \ldots, J)$$

$$\dot{S}_j(t) = -\sum_{k\neq j}^{J} \lambda_{jk}^{S} \cdot S_j - \sum_{k=1}^{J} \beta_{kj} \cdot I_k \cdot S_j + \sum_{k\neq j}^{J} \lambda_{kj}^{S} \cdot S_k - \eta_j S_j \quad (j = 1, 2, \ldots, J)$$

Hybrid System for the CEDE representable V2X transportation system

- A transportation system is comprised of
  1. A road infrastructure defined as CEDE for the V2X system
  2. A set of boolean variables
     - Representing the presence or absence of the modeled environmental conditions
  3. A set of events that modify mobility and communication parameters. An event consists of
     - A guard, which in its simplest form is a change in the value of an environment variable or, in general, maybe a predicate over the values of environment variables
     - An action, which is an assignment of constant values to parameters
  4. A timed automata that describes the evolution of the environment variables over time
  5. An initial valuation for the environment variables

Hybrid System for the CEDE representable V2X transportation system (Cont..)

- The model of the transportation system defined in the previous slide gives rise to a hybrid system with
  - Modes
    - There is one mode for each valuation of the environment variables
    - Is an instantiation of the CEDE with parameter values defined by the action of an event resulting in that mode
  - Transitions
    - Caused by evolution of environment variables
    - Is a change to the parameter values defined by guard of an event causing the transition

Analysis of the V2X system modeled as a hybrid system

1. Identify desired properties of the system in terms of traffic densities and values of the environment variables
   - For e.g., vehicle density over a certain threshold can be deemed dangerous in a particular cluster with the environmental condition of snowfall in that cluster

2. Formalize undesirable properties (negation of desired properties) as state predicates and

3. Apply hybrid system reachability analysis to see if an undesirable property is reachable in the chosen scenario for the evolution of environmental conditions

Case study

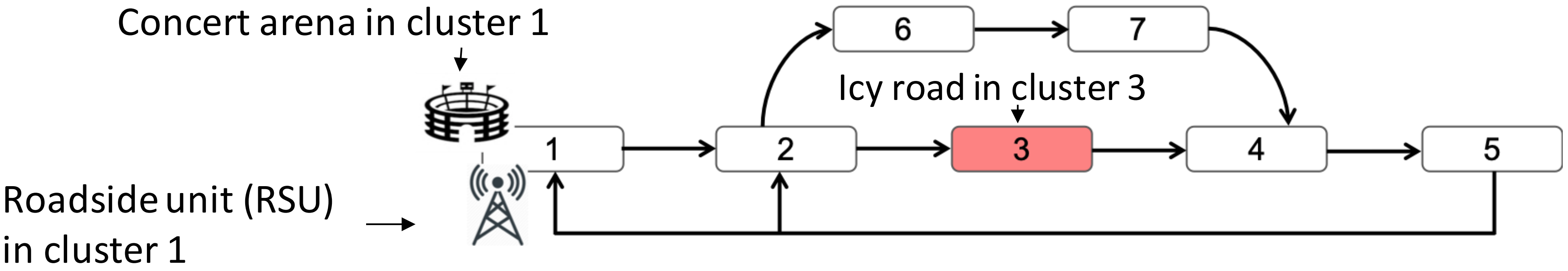
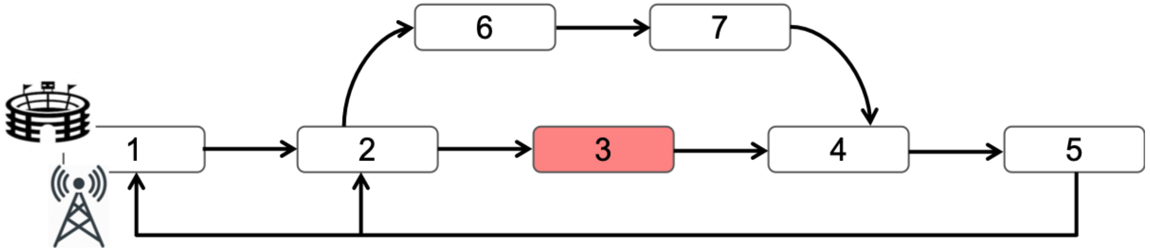


Fig- An example of a V2X equipped transportation system with 7 clusters

- Consider travelers commuting from cluster 2 to cluster 4
  - Under normal circumstances, travelers prefer the shorter path through cluster 3, to the longer one through clusters 6 and 7
- Suppose road in cluster 3 becomes icy
  - As soon as the RSU receives this message, it starts propagating it to the vehicles in cluster 1
- Sometime before the concert starts until sometime after the concert starts, the traffic density from cluster 5 to cluster 1 would increase
  - Similarly, after the concert ends, traffic density from cluster 1 to cluster 2 would also increase

CEDE for informed vehicles in the considered system



$$\dot{I}_1(t) = -\lambda^I_{12} I_1 + \beta I_1 S_1 + \lambda^I_{51} I_5 + \eta_1 S_1$$

$$\dot{I}_2(t) = -\left(\lambda^I_{23} + \lambda^I_{26}\right) I_2 + \beta I_2 S_2 + \lambda^I_{12} I_1 + \lambda^I_{52} I_5 + \eta_2 S_2$$

$$\dot{I}_3(t) = -\lambda^I_{34} I_3 + \beta I_3 S_3 + \lambda^I_{23} I_2 + \eta_3 S_3$$

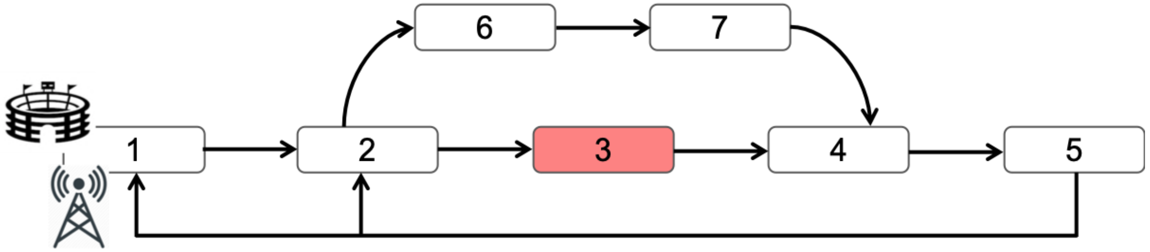
$$\dot{I}_4(t) = -\lambda^I_{45} I_4 + \beta I_4 S_4 + \lambda^I_{34} I_3 + \lambda^I_{74} I_7 + \eta_4 S_4$$

$$\dot{I}_5(t) = -(\lambda^I_{51} + \lambda^I_{52}) I_5 + \beta I_5 S_5 + \lambda^I_{45} I_5 + \eta_5 S_5$$

$$\dot{I}_6(t) = -\lambda^I_{67} I_6 + \beta I_6 S_6 + \lambda^I_{26} I_2 + \eta_6 S_6$$

$$\dot{I}_7(t) = -\lambda^I_{74} I_7 + \beta I_7 S_7 + \lambda^I_{67} I_6 + \eta_7 S_7$$

CEDE for non-informed vehicles in the considered system



$$\dot{S}_1(t) = -\lambda^S_{12} S_1 - \beta I_1 S_1 + \lambda^S_{51} S_5 - \eta_1 S_1$$

$$\dot{S}_2(t) = -\left(\lambda^S_{23} + \lambda^S_{26}\right) S_2 - \beta I_2 S_2 + \lambda^S_{12} S_1 + \lambda^S_{52} S_5 - \eta_2 S_2$$

$$\dot{S}_3(t) = -\lambda^S_{34} S_3 - \beta I_3 S_3 + \lambda^S_{23} S_2 - \eta_3 S_3$$

$$\dot{S}_4(t) = -\lambda^S_{45} S_4 - \beta I_4 S_4 + \lambda^S_{34} S_3 + \lambda^S_{74} S_7 - \eta_4 S_4$$

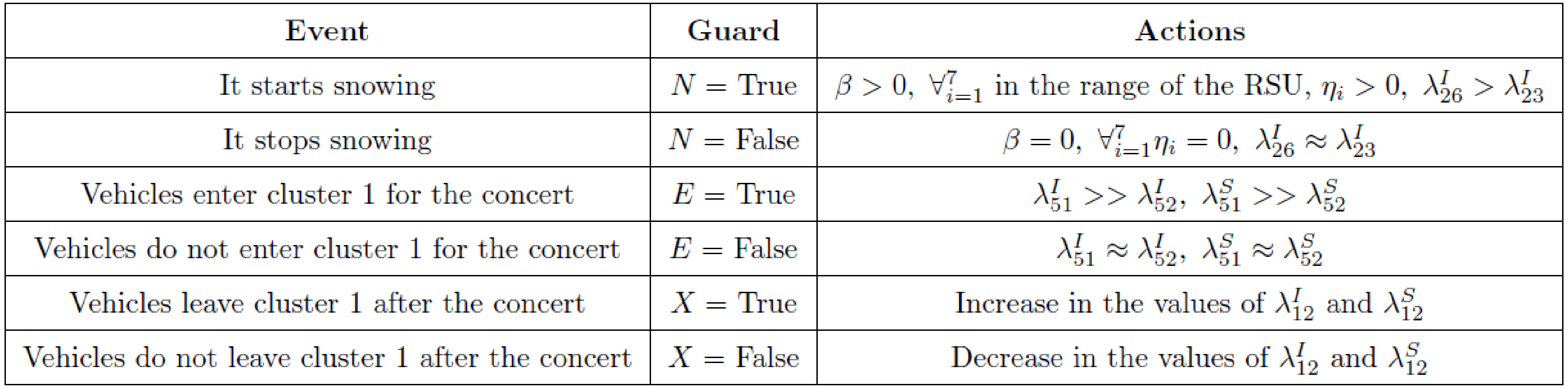
$$\dot{S}_5(t) = -(\lambda^S_{51} + \lambda^S_{52}) S_5 - \beta I_5 S_5 + \lambda^S_{45} S_4 - \eta_5 S_5$$

$$\dot{S}_6(t) = -\lambda^S_{67} S_6 - \beta I_6 S_6 + \lambda^S_{26} S_2 - \eta_6 S_6$$

$$\dot{S}_7(t) = -\lambda^S_{74} S_7 - \beta I_7 S_7 + \lambda^S_{67} S_6 - \eta_7 S_7$$

Transportation system for the considered system

- Road infrastructure
  - CEDE equations for the informed and non-informed vehicles
- Boolean variables - {N, E, X}
  - N, E, and X represent snow, entry of vehicles in cluster 1 for concert and exit of vehicles from cluster 1 after the concert finishes
- Events



Event	Guard	Actions
It starts snowing	$N =$ True	$\beta > 0,\ \forall_{i=1}^{7}$ in the range of the RSU, $\eta_i > 0,\ \lambda_{26}^{I} > \lambda_{23}^{I}$
It stops snowing	$N =$ False	$\beta = 0,\ \forall_{i=1}^{7} \eta_i = 0,\ \lambda_{26}^{I} \approx \lambda_{23}^{I}$
Vehicles enter cluster 1 for the concert	$E =$ True	$\lambda_{51}^{I} >> \lambda_{52}^{I},\ \lambda_{51}^{S} >> \lambda_{52}^{S}$
Vehicles do not enter cluster 1 for the concert	$E =$ False	$\lambda_{51}^{I} \approx \lambda_{52}^{I},\ \lambda_{51}^{S} \approx \lambda_{52}^{S}$
Vehicles leave cluster 1 after the concert	$X =$ True	Increase in the values of λ_{12}^{I} and λ_{12}^{S}
Vehicles do not leave cluster 1 after the concert	$X =$ False	Decrease in the values of λ_{12}^{I} and λ_{12}^{S}

Table representing events with the corresponding guard and actions

Hybrid system for the considered system (Cont..)

- Timed Automata
  - Vehicles enter cluster 1 for the concert in the time inverval [a, b]
  - The concert goes on during the time interval [b, c]
  - Audience leaves cluster 1 in the time interval [c, d]
  - We do not impose any timing constraints on the timed automaton for the event of N (or ¬N)

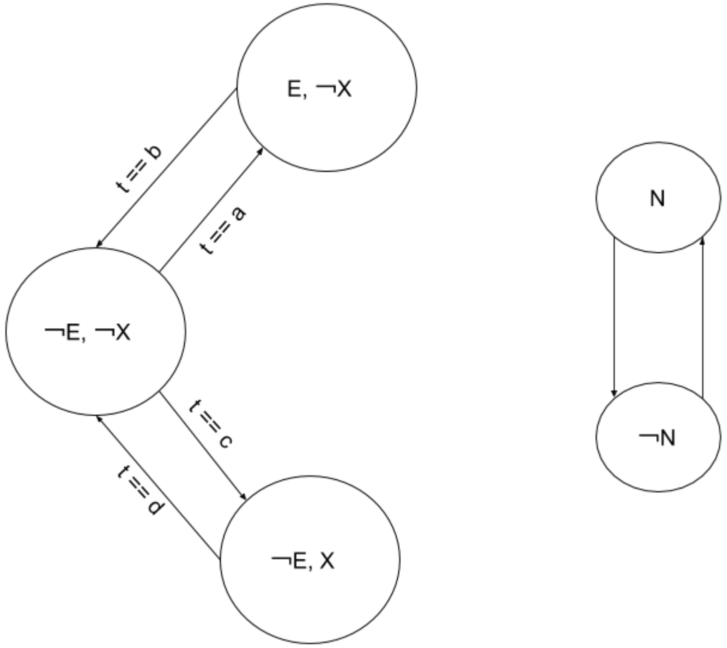


Fig- Timed automata for evolution of the environment variables, {N, E, X} over time

- Initial valuation of the environment variables
  - {N=false, E=false, X=false}

Hybrid system for the considered system (Cont..)

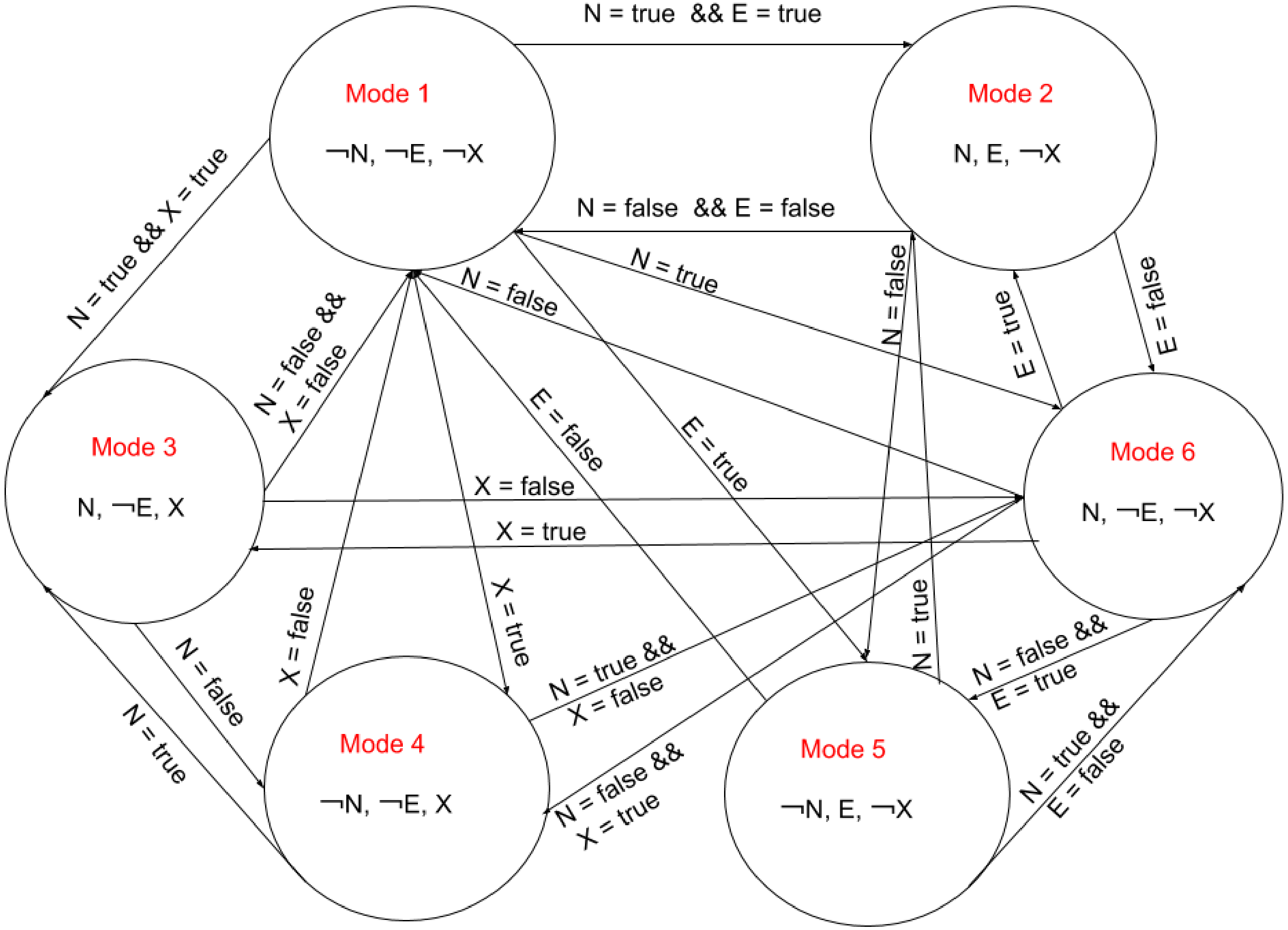
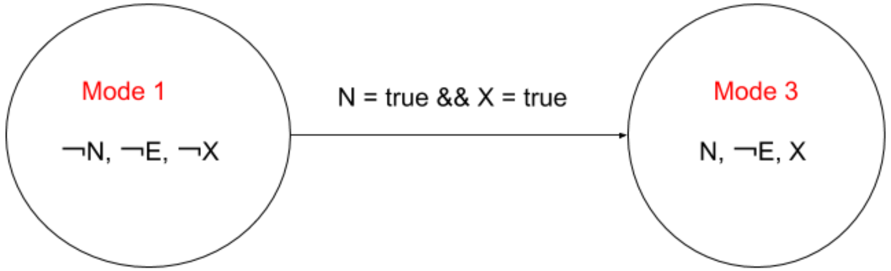


Fig- Hybrid system for the considered transportation system

Experiments for desired properties in Flow*

- Verification of the desired properties for a subset of the hybrid system



- Mode 1 represents the scenario of no snow in cluster 3 with the ongoing concert in cluster 1
- Mode 3 represents the scenario of ongoing snowfall in cluster 3 and the audience is leaving cluster 1 after the concert
- We want to verify that

  1. Safety property- $I_3 + S_3 < 0.2$
  2. Low-congestion property- $I_6 + S_6 < 0.3$

  holds true in Mode 3

Experiments for desired properties in Flow* (Cont..)

- Initial mode in simulation is Mode 1
  - Cluster 1 was initialized with a range of 30 to 35% of total vehicles
  - Remaining vehicles were uniformly distributed among all other clusters
- The system starts in Mode 1 for 10s and transitions to Mode 3 for next 10s
- The value of $\beta = 0$ and $\forall_{i=1}^{7},\ \eta_i = 0$ in Mode 1 as it is not snowing
- The value of $\beta = 3$ and $\eta_1 = 1, \forall_{i=2}^{7}, \eta_i = 0$ in Mode 3
- The values of the mobility rates in Mode 1-

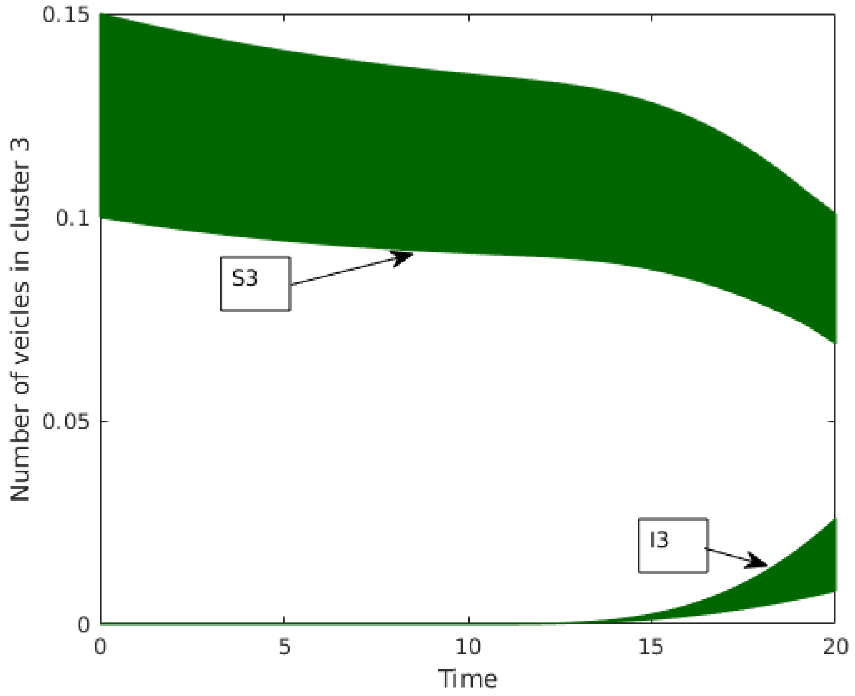
$$\lambda_{12}^{I(or\ S)} = \lambda_{67}^{I(or\ S)} = \lambda_{34}^{I(or\ S)} = \lambda_{74}^{I(or\ S)} = \lambda_{45}^{I(or\ S)} = 0.03$$

$$\lambda_{23}^{I(or\ S)} = \lambda_{26}^{I(or\ S)} = \lambda_{51}^{I(or\ S)} = \lambda_{52}^{I(or\ S)} = 0.015$$

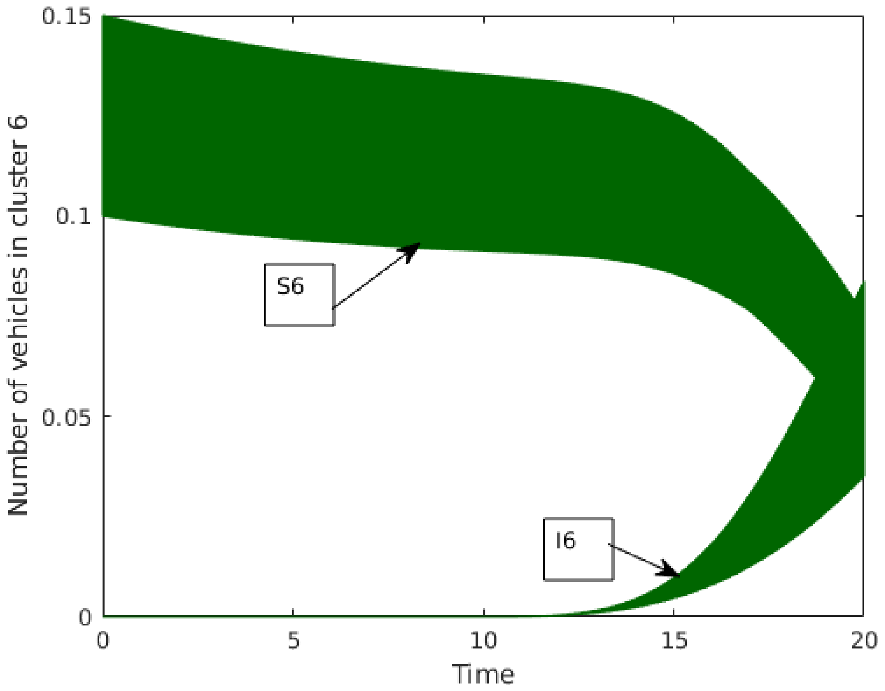
- The changes in the mobility rates in Mode 3-

$$\lambda_{26}^{I} = 0.024,\ \lambda_{23}^{I} = 0.006,\ \lambda_{12}^{I} = 0.04 \text{ and } \lambda_{12}^{S} = 0.04$$

Verification results of the desired properties



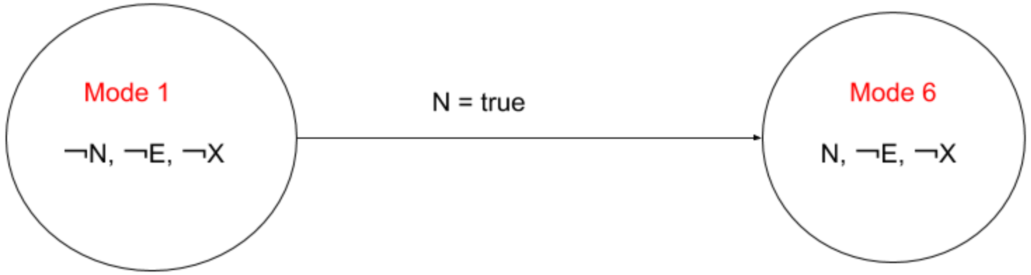
Verification of the safety property in Mode 3 in Flow*



Verification of the low-congestion property in Mode 3 in Flow*

Experiments for analysis of network policies in Flow*

- Analysis of the network policies
  - Deciding the values of the communication parameters to maintain system's safety
  - On a subset of the hybrid system



- Mode 1 represents the scenario of no snow in cluster 3 with the ongoing concert
- Mode 6 represents the scenario of snowfall in cluster 3 with the ongoing concert
- We want to analyze the values of β and η_1 for the V2X network such that it satisfies
  - Safety property- $I_3 + S_3 < 0.1$ in Mode 6

Experiments for analysis of network policies in Flow* (Cont..)

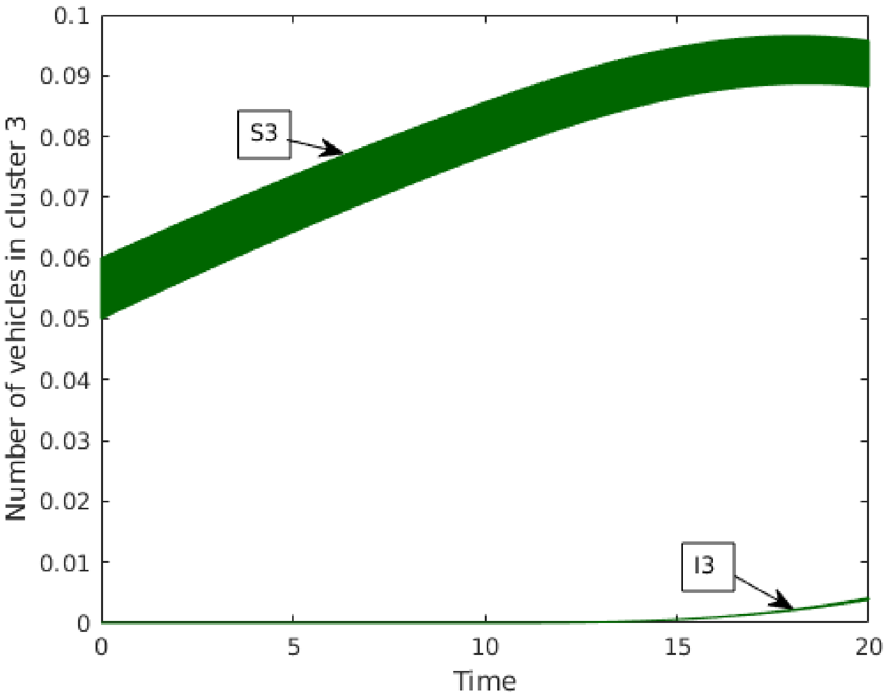
- Initial mode in simulation is Mode 1
  - Clusters 1 and 2 were initialized with a range of 30 to 40% of total vehicles
  - Clusters 3, 6 and 7 were initialized with a range of 5 to 6% of total vehicles
  - Cluster 4 was initialized with a range of 10 to 20% of total vehicles
  - Cluster 5 was initialized with a range of 15 to 25% of total vehicles
- The system starts in Mode 1 for 10s and transitions to Mode 6 for next 10s
- The value of $\beta = 0$ and $\forall_{i=1}^{7},\ \eta_i = 0$ in Mode 1 as it is not snowing
- The values of the mobility rates in Mode 1-

$$\lambda_{12}^{I(or\ S)} = \lambda_{67}^{I(or\ S)} = \lambda_{34}^{I(or\ S)} = \lambda_{74}^{I(or\ S)} = \lambda_{45}^{I(or\ S)} = 0.03$$
$$\lambda_{23}^{I(or\ S)} = \lambda_{26}^{I(or\ S)} = \lambda_{51}^{I(or\ S)} = \lambda_{52}^{I(or\ S)} = 0.015$$

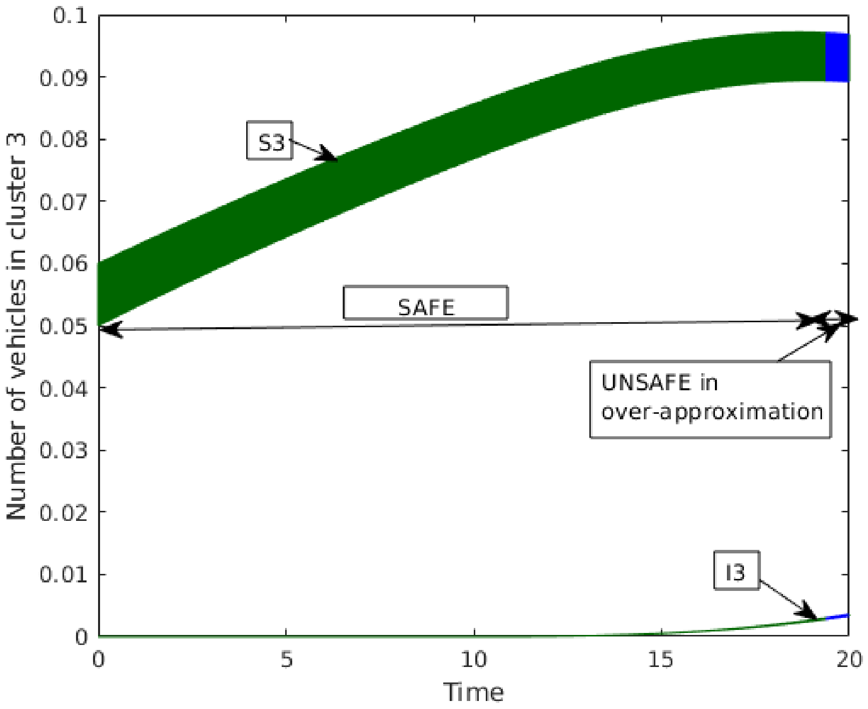
- The changes in the mobility rates in Mode 6-

$$\lambda_{26}^{I} = 0.024, \lambda_{23}^{I} = 0.006$$

Verification results for the analysis of communication parameters



Verified safety property by Flow* with values of $\beta = 0.8,\ \eta_1 = 0.8, \forall_{i=2}^{7},\ \eta_i = 0$ in Mode 6



Unsafe in over-approximation by Flow* with values of $\beta = 0.9,\ \eta_1 = 0.9, \forall_{i=2}^{7},\ \eta_i = 0$ in Mode 6

Future work

- While running the experiments for verification of hybrid systems, we ran into scalability issues of formal method tools that try to solve verification via reachability

- We plan to investigate and enhance these tools so that they can be used in the transportation community for safety verification

Thank You for your attention!
Q&A