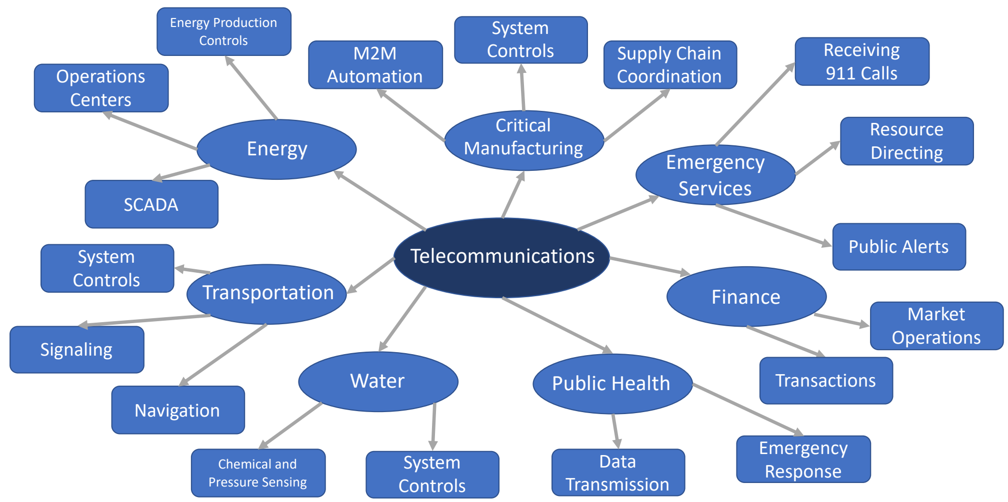
Assessing Risks of 5G: Comparisons Across End-to-End Elements and Interdependent System Risks

Iris Tien, Ph.D.
Williams Family Associate Professor
School of Civil and Environmental Engineering
Georgia Institute of Technology

Critical Infrastructure Resilience Institute (CIRI) Webinar
April 29, 2021

Motivation

- Telecommunications increasingly connected to critical infrastructures
- Identify risks across end-to-end elements of telecommunications system, particularly in transition to 5G for cellular network
- Comprehensively analyze these risks
  - Create framework to quantify impacts of risks
  - Ability to compare different risk elements
  - Evaluate impacts of telecommunications risks on connected critical infrastructure functions
  - Understand risks on interdependent infrastructure systems



- Understand full risk profile to protect critical infrastructure functions relying on 5G for increasing asset automation, monitoring, and control

Advancement on best practices / current state of the art

Current practice		Advancement
Entities currently evaluate telecommunications risk by individual element, e.g., implement security protocols or develop trusted suppliers	→	Comprehensively assess risk across multiple disparate elements, including physical and service-based elements, within a single framework
Qualitative assessments of risk	→	Quantitative assessment of risk, including quantitative measures of risk impacts where available, also facilitates comparisons across risk factors
Focus solely on telecommunications system and risks	→	Characterize impacts of telecommunications risk on connected critical infrastructure functions

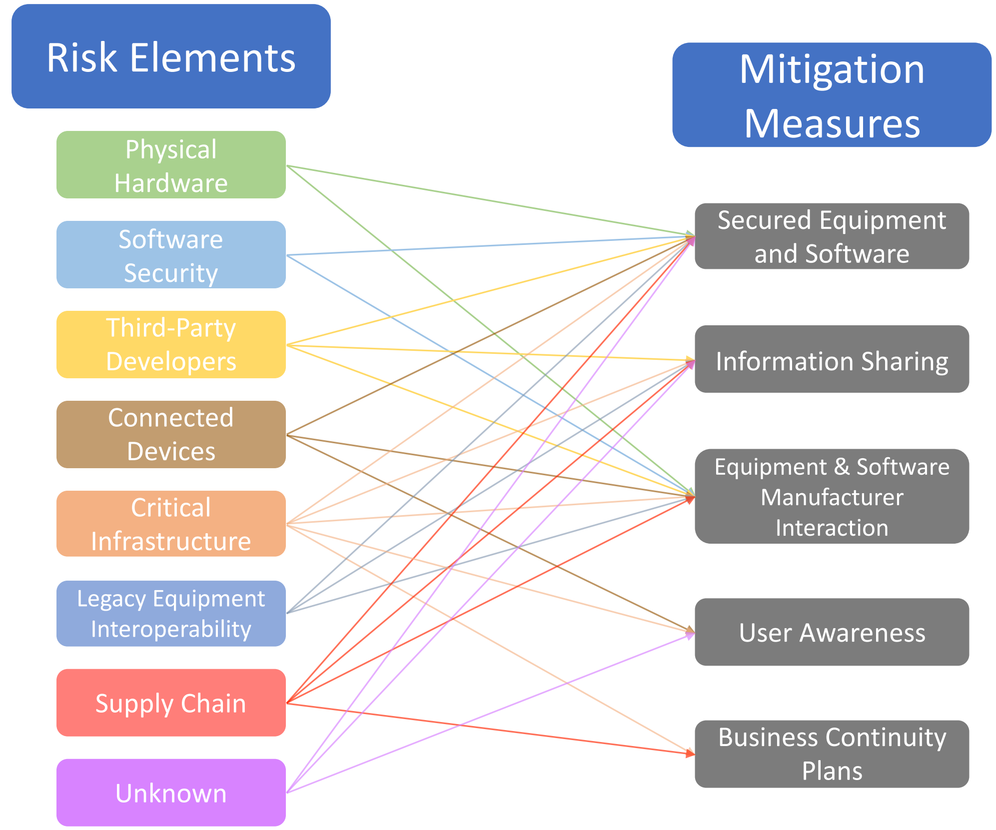
Outline

- Build risk profile of 5G
- Quantify impacts of risks
  - Risks affecting public directly and indirectly
- Compare across multiple risk elements

- Conduct interdependent system case study
  - 5G and connected transportation system
- Define and vary analysis parameters
- Compare quantitative impacts across risk scenarios

Build risk profile of 5G

- Integrate information from across stakeholder interviews to build risk profile of 5G
- Identify risk elements and form recommendations for corresponding risk mitigation measures
- Within each risk category, characterize specific potential risk scenarios and identify consequences



Quantify impacts of risks

- The following aspects of each risk scenario are considered:
  - Expected number of people affected
  - Probability of occurrence
  - Severity of impacts
  - Time required to restore full service (recovery time), includes time needed to detect a problem (e.g., cyberattack)
- Quantitative estimates used where available, qualitative scores used where necessary

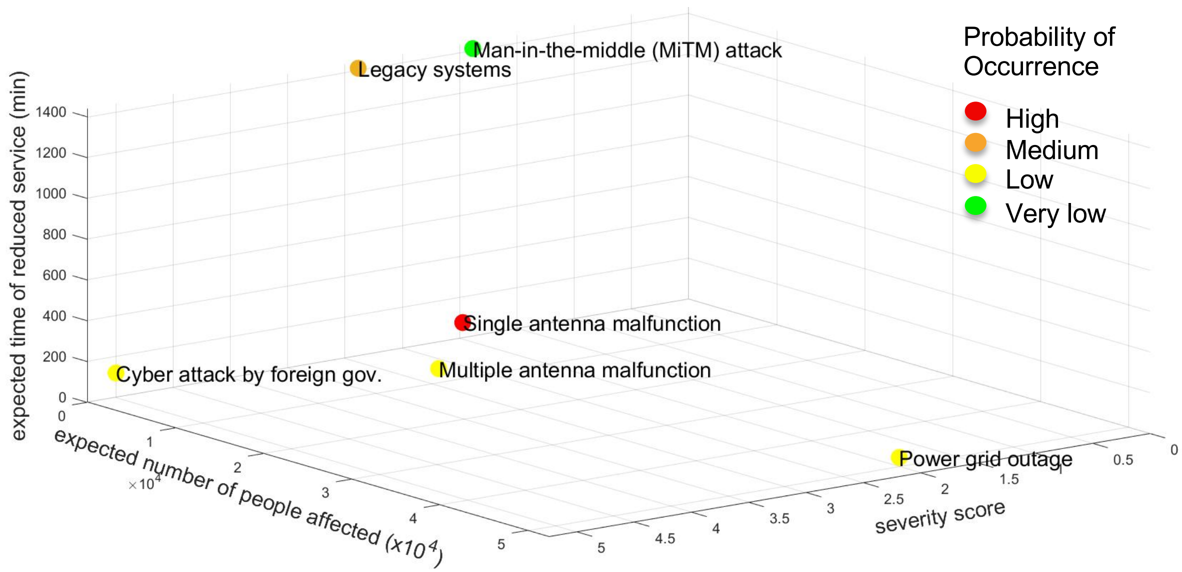
Severity Score	Description
Severe 5	Life threatening, indefinite loss of service, threat to national security
High - 4	Private information theft
Moderate - 3	Temporary loss of service (extended), limited ability to expand network
Low - 2	Temporary loss of service (short)
Very Low - 1	Service lag

Characterize risk elements

- Distinguish between risk elements that affect the public directly vs. indirectly
- Some risks affect the public directly
  - e.g., telecommunications attack/malfunction scenarios
- Some risks affect the public indirectly
  - e.g., dependence of parts from overseas suppliers, effects of these risks impact the public more indirectly
- For these latter risks: as quantitative measure of risk impacts and consequences
  - Measure: *expected number of people affected* → *expected economic impact*

Comparison of risks

- Risks affecting the public directly

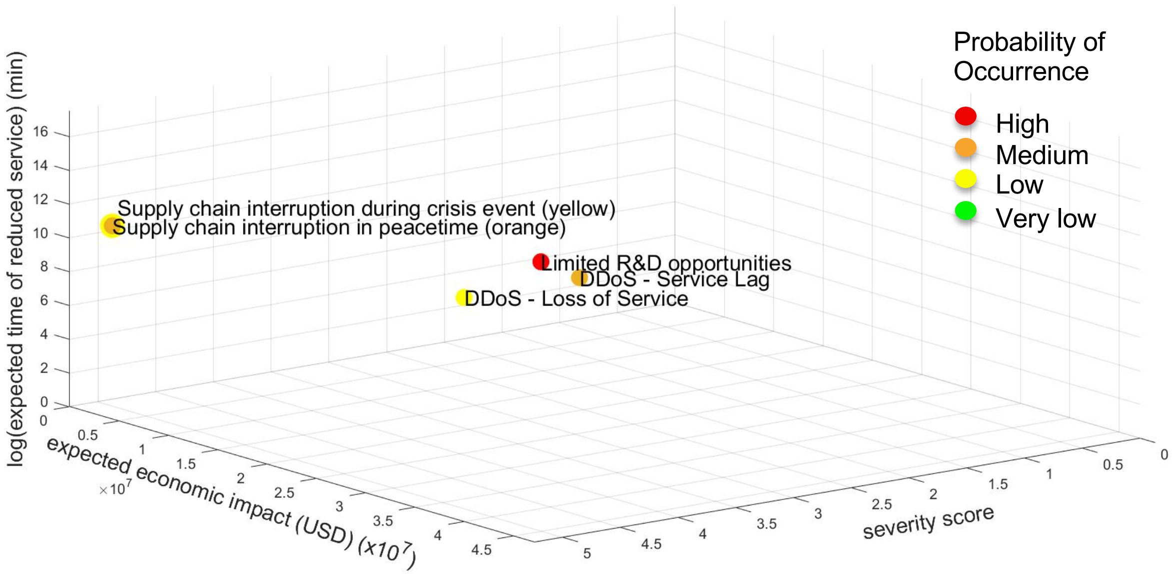


- Approach shows various aspects of each risk separately rather in one combined score, giving a more comprehensive image of the risk landscape
- Allows for a better understanding of which risks are of concern and why
- Ex: Malfunction of single antenna has highest probability of occurrence, relatively long recovery times, and moderate severity of impacts. Range of a single antenna is fairly small, and relatively small number of customers will be affected. It may be determined that speeding up repair process would be most effective mitigation effort for this risk scenario.

Shown: expected number of people affected, severity of impacts, and expected time of reduced service (recovery time) along axes; probability of occurrence denoted by color

Comparison of risks

- Risks affecting the public indirectly



- Approach again shows various aspects of each risk separately so they can be compared across varying risk quantification measures
- Allows for a better understanding of which risks are of concern and why, and comparison across risk elements
- With many risk elements of consideration, ongoing work to continue to characterize and plot out varying risk elements

Shown: expected economic impact, severity of impacts, and expected time of reduced service (recovery time) along axes; probability of occurrence denoted by color

Interdependent system case study

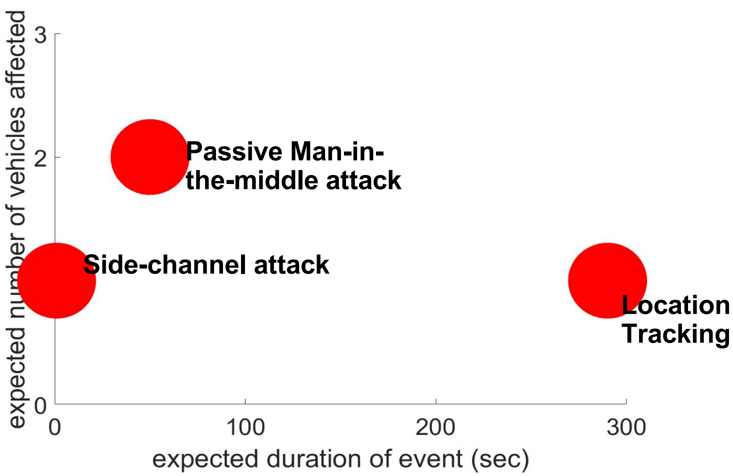
- Connected Devices risks → Interdependent system case study
  - Transportation system / Connected and Automated Vehicles
- Many high-stakes applications of 5G technology, essential to evaluate the consequences of a failure of the telecommunications system on interdependent systems
- Consider impacts of 5G risks on the transportation system (including connected and automated vehicles (CAVs) and smart transportation infrastructure)
- Consider privacy risks and safety/performance risks

Aspect	Privacy Risks	Safety/Performance Risks
Probability of occurrence	"Low", "Medium", or "High"	"Low", "Medium", or "High"
Expected duration of the event	typical duration of a similar attack	typical duration of a similar attack
Expected number of vehicles affected	typical number of vehicles affected in similar attack	*number of vehicles whose travel time increased or were involved in collisions
Severity of the consequences	best match by category	*increase in time loss and time spent stopped due to traffic, number of collisions

* From simulations developed and conducted as part of this project

Privacy risks

Name	Description
Side-channel	“Leaked” information (ex. energy consumption or hardware temperature) is used to infer private information about a vehicle
Passive Man-in-the-middle	Messages sent by a vehicle are intercepted but not altered in any way
Location tracking	Attacker gains access to the location of a target vehicle



Severity Score	Description

- Variations of eavesdropping attacks
- Similar probabilities of occurrence and severities
- Relatively short duration, typically targeted attacks expected to affect only one or two vehicles each

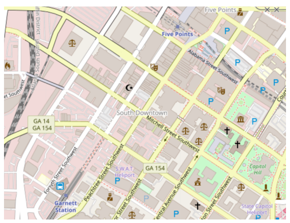
Probability of occurrence: Low Med High

Safety/performance risks

- To quantify impacts of 5G risks on safety/network performance
- Simulate various telecommunications system failure scenarios and analyze the interdependent impacts on the transportation system
- Outputs to quantify severity of impacts to enable comparison across multiple risk scenarios
  - *Time Loss* – time added to a vehicle's trip from driving below the ideal speed limit
  - *Stop Time* – time spent completely stopped on the road throughout the trip
  - *Number of collisions*
  - *Number of vehicles affected* – increase in time loss, stop time, or collision
- Compare quantitative risk scenario impacts with outcomes from default (no failure/attack) scenario

Workflow for simulations and analysis

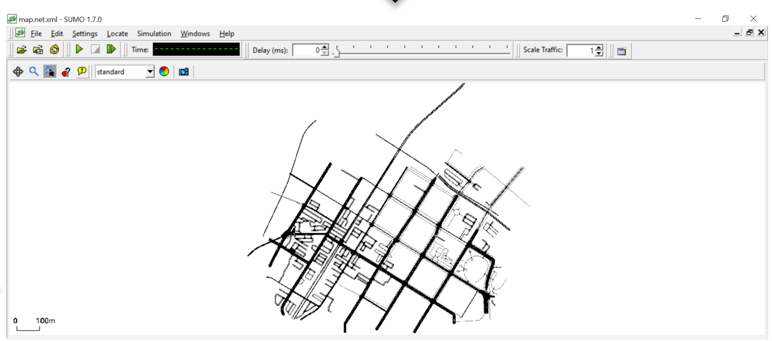
- Simulations conducted using Eclipse's SUMO and MOSAIC programs integrating 5G and transportation network parameters



Parameter change simulating attack or malfunction event

Parameters defining the characteristics and routes of the vehicles in the scenario

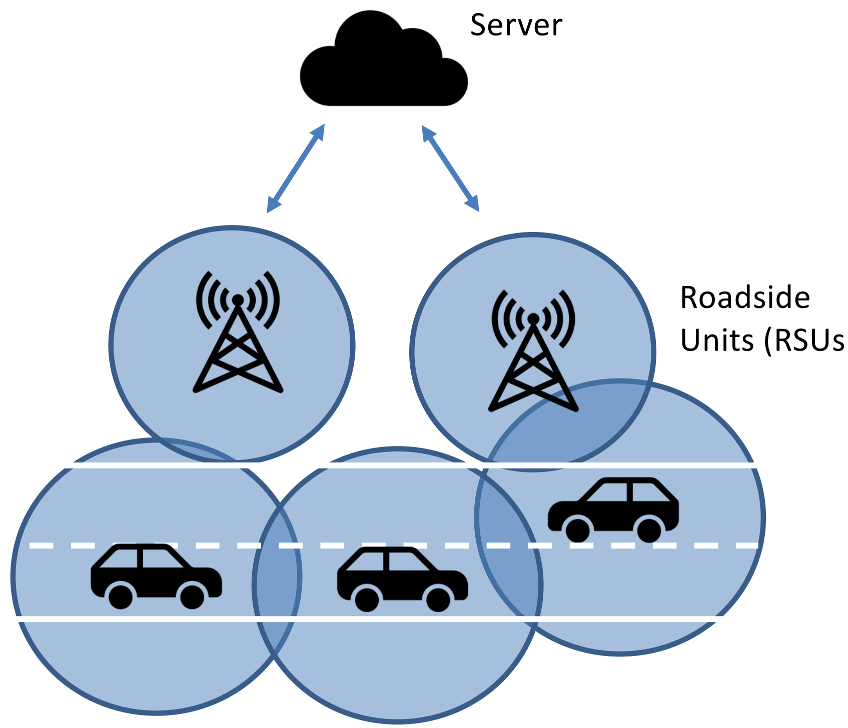
Simulated vehicle-to-vehicle and vehicle-to-infrastructure 5G communication



Output indicating:
- Vehicle positions
- Vehicle speeds
- Collisions
- Traffic congestion

Simulation parameters

- Duration of simulation: 1000 sec
- Step size: 1 sec
- 50% automated & 50% non-automated vehicles
- Vehicles periodically broadcast messages (CAMs) containing information about themselves and sensor data about their surroundings to other vehicles and RSUs within range. The other vehicles can react appropriately to this information.
- RSUs forward the gathered information to the server, which has a larger overview of the network. The server then sends messages (e.g., DENM warnings) to vehicles of hazardous conditions or traffic in their vicinity.



Types of messages

CAM (Cooperative Awareness Message)

- Contains information about a vehicle's location, speed, acceleration, direction, type (car, truck, emergency vehicle, etc.), and size
- Messages sent to all vehicles (only vehicles with V2X capability) and RSUs within the sender's broadcast range

DENM (Decentralized Environmental Notification Message)

- Contains information about hazardous road conditions (fog, ice, rain, obstacle on road, …) or unusual traffic conditions
- Transmits the type of hazard and its location to vehicles that are in within a radius of the hazard
- Driver can then be notified, or the vehicle can respond automatically by rerouting, slowing down, changing lanes, etc.

5G network parameters

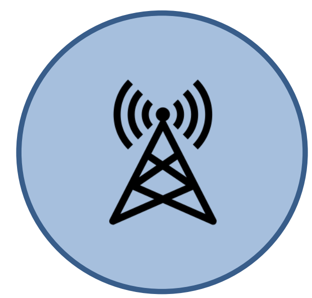
- Max uplink and downlink bitrates: 1.5 Gigabits per second (Gbps), the bitrates for mmWave
- 3ms latency, 99.999% reliability
- Packet loss probability: 0.08% for vehicle communication applications
- RSU placement
  - No specific guidelines exist; coverage of a single unit depends on many factors, including installation height, sharp curves in the road, number of lanes, obstacles that surround the unit
  - In urban areas, RSUs can be placed uniformly throughout the network, or specifically in areas with high vehicle density
  - For this study, RSUs evenly distributed throughout the network at every intersection to cover the whole network
  - Blocks are roughly 100m x 100m

Vehicle automation

- 5G-enabled vehicle automation
- At start of simulation
  - Activates vehicle distance sensor to detect distance with vehicle ahead
  - Range of distance sensor: 4m
- At every timestep
  - Broadcast CAM to all vehicles/RSUs within a 400m radius
    - Broadcast radius can range from 360m to 700m
  - Emergency braking
    - If the distance to the vehicle ahead has decreased by more than 7m in the last time step (1 sec) & the distance to car ahead falls below 15 m, activate emergency braking

Roadside Units (RSUs)

- RSUs forward messages from the server out to any vehicles within their range
- In several of the following scenarios, RSUs forward information about hazardous conditions



Server

- Server acts as a traffic management center and has information about a wider network than do the RSUs
- Processes information received from RSUs and sends decentralized environmental notification messages (DENMs) to relevant RSU so it can warn vehicles in the vicinity
- Because latency is increased when a message travels from a vehicle, through an RSU, to the server and back, efforts have been made to do some of the prioritization of risks at the RSUs

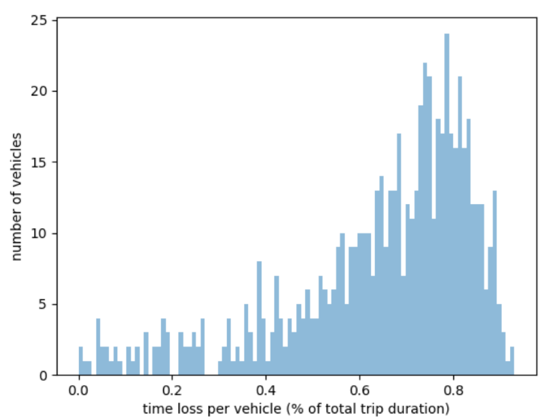
Simulation visualization

Sending V2X Message

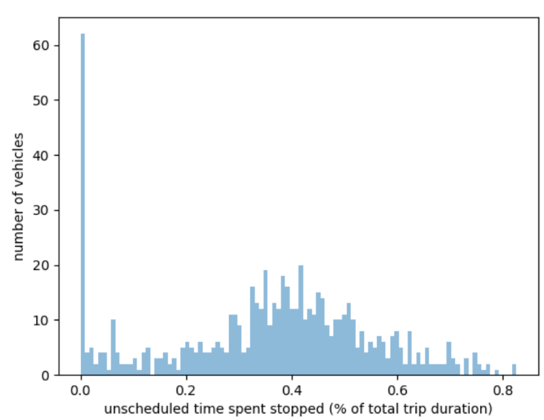
Receiving V2X Message

Default scenario

- No risk event scenario
- 650 vehicles in the network over the duration of this simulation scenario
- Distributions of outcomes over all vehicles
  - Time loss and stop time as a % of total trip time



Time loss (TL)



Stop time (ST)

Indicator	Value
Mean stoptime	38.2%
Mean timeloss	70.3%
% Veh affected	-
Veh > 80% ST	0.3%
Veh > 80% TL	22.5%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn’t enter network	0

Risk scenarios

1) Jamming of message from vehicle
   – Affects vehicle
   – Vary # vehicles affected
2) Fake DEN message
   – Affects RSU
   – Vary RSU radius
   – Vary # RSUs affected
3) Forced sudden braking of vehicle
   – Affected through RSU
   – Vary # RSUs affected

1) Jamming of message from vehicle

- Simulated by changing driver imperfection value and removing vehicles' automation features
- Drivers of vehicles with V2X capabilities and automated driving features have higher likelihoods of being inattentive and becoming distracted (and making a mistake if automation fails) while driving due to overreliance on the vehicle's automation
- Driver imperfection value sigma ranges from 0 to 1, with 0 representing perfect driving; driver imperfection value increased from 0.5 to 0.9

1) Jamming risk scenario outcomes

Default | One vehicle jammed | Two vehicles jammed | Five vehicles jammed

Stop Time

Time Loss

- Results affecting single vehicle (vs. default) noticeable, though changes by individual vehicle small
- Depends on which vehicle(s) jammed based on its path through the network
- Other measures show little change
- Scenarios impacting RSUs (next analyses) impact multiple vehicles, show larger effects

Default

Indicator	Value
Mean stoptime	38.2%
Mean timeloss	70.3%
% Veh affected	-
Veh > 80% ST	0.3%
Veh > 80% TL	22.5%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

One vehicle jammed

Indicator	
Mean stoptime	38.4%
Mean timeloss	70.1%
% Veh affected	50%
Veh > 80% ST	0.3%
Veh > 80% TL	26.6%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

Two vehicles jammed

Indicator	Value
Mean stoptime	38.9%
Mean timeloss	71.4%
% Veh affected	49%
Veh > 80% ST	0.3%
Veh > 80% TL	23.7%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

Five vehicles jammed

Indicator	Value
Mean stoptime	41.6%
Mean timeloss	73.0%
% Veh affected	52%
Veh > 80% ST	0.9%
Veh > 80% TL	29.7%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

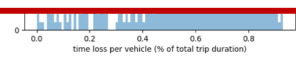
2) Fake DEN message

- Expand risk scenario from single vehicle impacts to impacting RSUs impacting multiple vehicles
- Server sends a fake DEN (Decentralized Environmental Notification) message
- Affected RSUs alert vehicles that there is ice on the road at the RSU's location
- Vehicles receiving this fake message respond by slowing down

2) Fake DENM risk scenario outcomes (vary RSU radius)

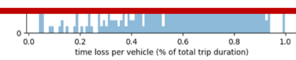
- Large radius affects many vehicles, shape (and values) of distributions completely changes
- Vehicles that didn't enter network: edges of network so congested, vehicle did not even have opportunity to enter network to start trip

Default



Indicator	Value
Mean stoptime	38.2%
Mean timeloss	70.3%
% Veh affected	-
Veh > 80% ST	0.3%
Veh > 80% TL	22.5%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

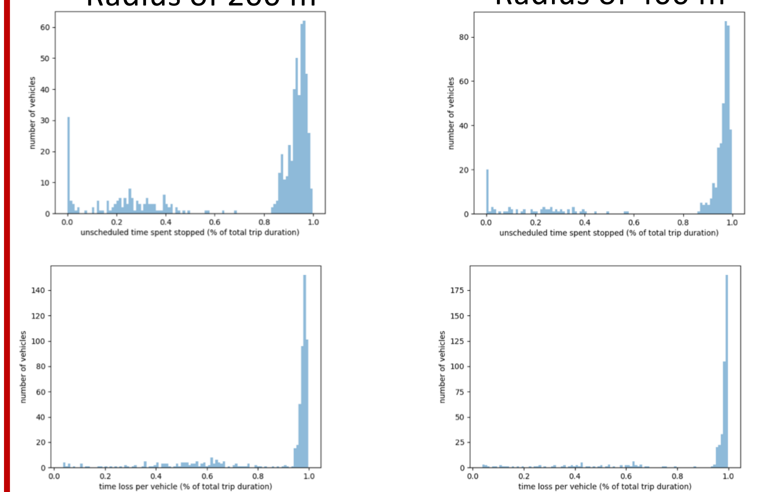
Radius of 50 m



Indicator	Value
Mean stoptime	36.0%
Mean timeloss	75.4%
% Veh affected	50%
Veh > 80% ST	2.8%
Veh > 80% TL	35.9%
Veh > 95% ST	2.0%
Veh > 95% TL	2.0%
Veh didn't enter network	1.4%

Radius of 200 m

Radius of 400 m



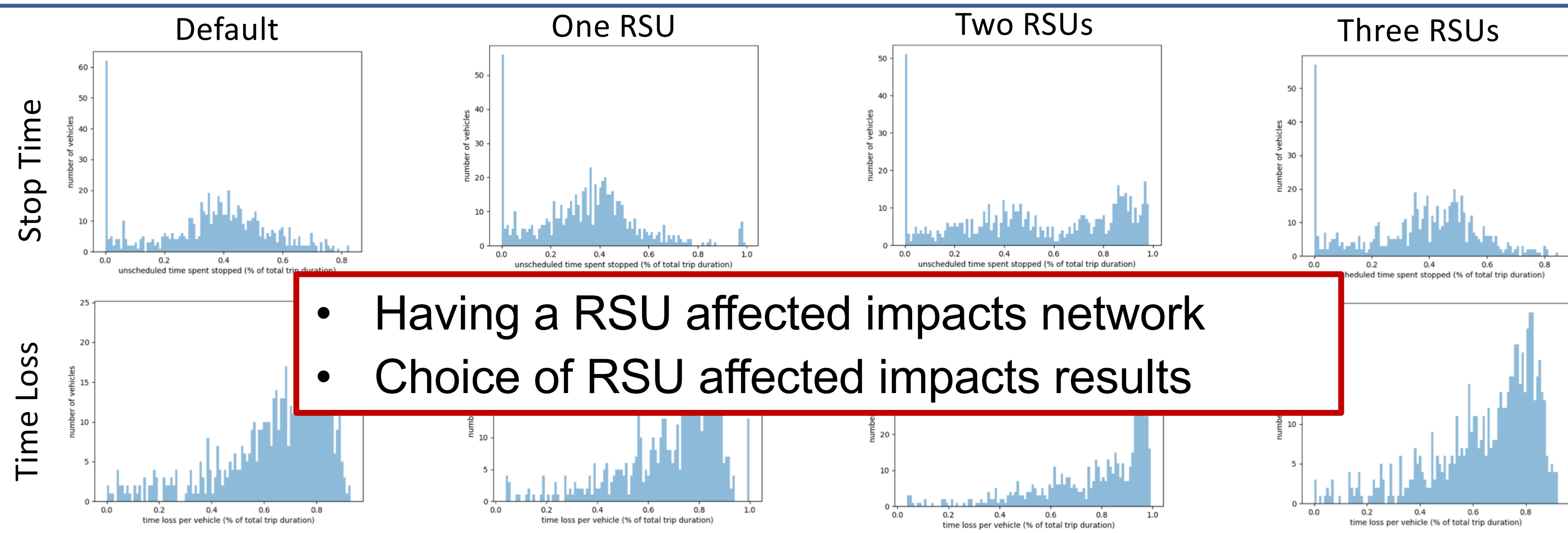
Radius of 200 m:

Indicator	Value
Mean stoptime	92.9%
Mean timeloss	97.7%
% Veh affected	73%
Veh > 80% ST	75.0%
Veh > 80% TL	74.9%
Veh > 95% ST	34.5%
Veh > 95% TL	72.4%
Veh didn't enter network	11.2%

Radius of 400 m:

Indicator	Value
Mean stoptime	96.7%
Mean timeloss	98.6%
% Veh affected	61%
Veh > 80% ST	83.1%
Veh > 80% TL	83.3%
Veh > 95% ST	64.2%
Veh > 95% TL	82.4%
Veh didn't enter network	30.8%

2) Fake DENM risk scenario outcomes (vary # RSUs affected)



- Having a RSU affected impacts network
- Choice of RSU affected impacts results

Default

Indicator	Value
Mean stoptime	38.2%
Mean timeloss	70.3%
% Veh affected	-
Veh > 80% ST	0.3%
Veh > 80% TL	22.5%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

One RSU

Indicator	Value
Mean stoptime	36.0%
Mean timeloss	75.4%
% Veh affected	50%
Veh > 80% ST	2.8%
Veh > 80% TL	35.9%
Veh > 95% ST	2.0%
Veh > 95% TL	2.0%
Veh didn't enter network	1.4%

Two RSUs

Indicator	Value
Mean stoptime	36.3%
Mean timeloss	71.2%
% Veh affected	42%
Veh > 80% ST	1.3%
Veh > 80% TL	26.7%
Veh > 95% ST	0.8%
Veh > 95% TL	0.8%
Veh didn't enter network	2.8%

Three RSUs

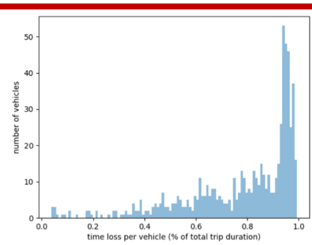
Indicator	Value
Mean stoptime	38.8%
Mean timeloss	73.9%
% Veh affected	54%
Veh > 80% ST	4.1%
Veh > 80% TL	33.9%
Veh > 95% ST	1.4%
Veh > 95% TL	2.5%
Veh didn't enter network	1.8%

2) Fake DENM risk scenario *alternate* outcomes (vary # RSUs affected)

- Difference between two and three RSUs affected is small, additional affected RSUs have smaller impact on the network than the first affected RSU
- Choice of RSU affected matters

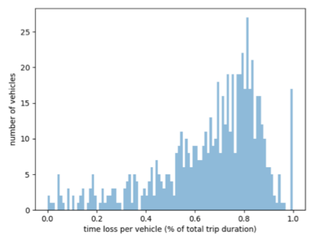
Time Loss

Two RSU



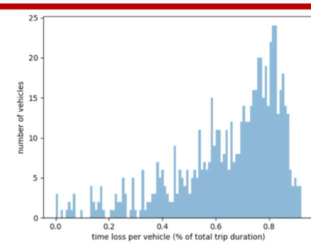
Indicator	Value
Mean stoptime	36.3%
Mean timeloss	71.2%
% Veh affected	42%
Veh > 80% ST	1.3%
Veh > 80% TL	26.7%
Veh > 95% ST	0.8%
Veh > 95% TL	0.8%
Veh didn't enter network	2.8%

Two RSU *Alternate*



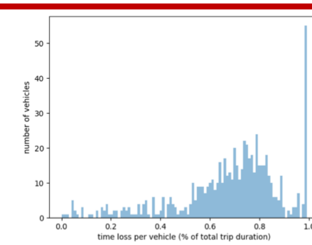
Indicator	Value
Mean stoptime	41.7%
Mean timeloss	71.9%
% Veh affected	50%
Veh > 80% ST	4.5%
Veh > 80% TL	29.3%
Veh > 95% ST	2.7%
Veh > 95% TL	3.0%
Veh didn't enter network	1.8%

Three RSU



Indicator	Value
Mean stoptime	38.8%
Mean timeloss	73.9%
% Veh affected	54%
Veh > 80% ST	4.1%
Veh > 80% TL	33.9%
Veh > 95% ST	1.4%
Veh > 95% TL	2.5%
Veh didn't enter network	1.8%

Three RSU *Alternate*



Indicator	Value
Mean stoptime	38.0%
Mean timeloss	72.0%
% Veh affected	48%
Veh > 80% ST	10.9%
Veh > 80% TL	27.7%
Veh > 95% ST	9.2%
Veh > 95% TL	10.3%
Veh didn't enter network	0

3) Forced sudden braking of vehicle

- Affected through RSU
- When a vehicle passes through the range of an affected RSU, it is altered so that it brakes harshly and unexpectedly throughout the rest of its trip
- To simulate a high-risk case of this scenario, a vehicle is forced to brake harshly every time it reaches a medium velocity of 25mph
- Scenario of an attacker wanting to cause a dangerous situation on the road

3) Forced sudden braking risk scenario outcomes

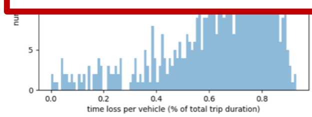
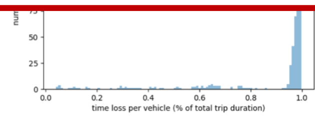
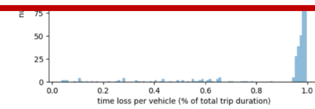
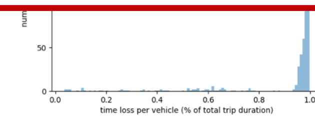
Default | One RSU | Two RSUs | Three RSUs

Stop Time




- Impact of a single RSU being affected is large
- Significant increases across all measures of risk scenario impacts
- Privacy risks are fairly contained
- Risks affecting RSUs have greater impacts than individual vehicle attacks
- Impact depends on specific vehicle or RSU and severity of scenario

Time Loss

Default

Indicator	Value
Mean stoptime	38.2%
Mean timeloss	70.3%
% Veh affected	-
Veh > 80% ST	0.3%
Veh > 80% TL	22.5%
Veh > 95% ST	0
Veh > 95% TL	0
Veh didn't enter network	0

One RSU

Indicator	Value
Mean stoptime	94.6%
Mean timeloss	98.4%
% Veh affected	78%
Veh > 80% ST	83.8%
Veh > 80% TL	84.7%
Veh > 95% ST	46.4%
Veh > 95% TL	82.9%
Veh didn't enter network	14.5%

Two RSUs

Indicator	Value
Mean stoptime	95.1%
Mean timeloss	98.5%
% Veh affected	72%
Veh > 80% ST	86.4%
Veh > 80% TL	86.6%
Veh > 95% ST	50.7%
Veh > 95% TL	85.5%
Veh didn't enter network	19.5%

Three RSUs

Indicator	Value
Mean stoptime	95.3%
Mean timeloss	98.5%
% Veh affected	74%
Veh > 80% ST	85.1%
Veh > 80% TL	85.5%
Veh > 95% ST	53.1%
Veh > 95% TL	83.6%
Veh didn't enter network	18.3%

Conclusions

- Assessing risks of 5G
- Provide a way to compare across risk elements and risk scenarios
  - Compare elements by measures of risk impacts, quantitative where possible (expected number of people affected/expected economic impact, probability of occurrence, severity of impacts, time required to restore full service)
  - Include risks across interdependent systems and functions (e.g., connected transportation system)
  - Quantify impacts of varying risk scenarios by scenario type and severity
- Ongoing work
  - Continue finding reliable, quantitative estimates of risk impact measures
  - Simulate additional risk scenarios and variations

Acknowledgements:

- Joseph Cathey
- Paola Vargas

Department of Homeland Security Award #2015-ST-061-CIRC01

Contact: **itien@ce.gatech.edu**