Methodology to Quantitatively Assess Impacts of 5G Telecommunications Cybersecurity Risk Scenarios on Dependent Connected Urban Transportation Systems

Paola Vargas[1] and Iris Tien, Ph.D., M.ASCE[2]

Abstract: The fifth generation (5G) technology standard for cellular networks is currently being developed and is in the early stages of rollout across the United States. This upgrade from 4G LTE (long-term evolution) will not only have implications for the telecommunications network itself, but also on the many critical infrastructure systems that will use and depend on 5G for operations and functionality. Cellular vehicle-to-everything (C-V2X) technology utilizes 5G and has the potential to improve the safety and efficiency of the transportation system by allowing vehicles to communicate with one another and automating certain driving features. However, it is important to consider the risks that 5G brings, including cybersecurity risks, and how attacks through the 5G network can disrupt a traffic network that includes C-V2X technology. This paper presents a method to characterize the effects of several risk scenarios. Compared to prior qualitative risk assessments, outcomes include quantitative indicators measuring system safety and performance for analysis. The approach enables a more detailed and rigorous assessment of interdependent systems risks between the telecommunications and transportation networks than previously possible, particularly in the transition to 5G. A range of potential risk scenarios are assessed. The results show that cyberattacks that alter the behavior of vehicles cause delays across the entire network, cascading across the system and affecting more than just the vehicles directly targeted. The simulations show different levels of traffic delays and numbers of collisions for each risk scenario, indicating that the effects of a cyberattack can differ widely depending on the specifics of the attack. The simulation is easily adaptable to the location, C-V2X features, and risk scenarios of interest. Results provide information to formulate and prioritize risk mitigation strategies as the technology is developed to minimize the impacts of these attacks and system disruptions. **DOI: 10.1061/AJRUA6.0001220.**

Author keywords: Risk assessment; Hazard analysis; Cybersecurity; Cyberattack; Connected and automated vehicles; Cellular vehicle-to-everything (C-V2X) communications; Smart transportation systems; Interdependent systems; Cascading effects.

Introduction

Fifth generation (5G) technology will bring improvements to the speed and reliability of the telecommunications network (CISA 2020). It also creates opportunities for improving capabilities in many other critical infrastructure sectors, including transportation systems (CISA 2020), and applications where real-time system monitoring, feedback, and control is desired. Cellular vehicle-to-everything communication (C-V2X) uses 5G to allow vehicles to communicate with other vehicles and roadside units (RSUs) that broadcast information about possible hazardous conditions on the road (GSMA 2019). Vehicles with V2X capabilities and some level of automation are then able to respond accordingly. This interdependence between the telecommunications and transportation systems means that attackers can take advantage of vulnerabilities within the 5G network to target smart vehicles and put passengers at risk. Previous studies have found interdependencies to be key in assessing infrastructure system vulnerabilities and risk (Guidotti and Gardoni 2018; Applegate and Tien 2019). The importance of considering such connections in assessments of system risk is increasing in criticality, particularly with the increasing dependencies of infrastructure systems on communications for operations. While 5G will increase the capabilities of connected transportation systems, it will also introduce new risks to the network. Within this environment, it is essential to understand how the new cybersecurity risks that come with 5G may have broader impacts on a traffic network with 5G-enabled vehicle automation. This study is the first of its kind to quantify the risks associated with 5G on connected dependent transportation networks. With 5G in the early stages of its rollout process and 5G-V2X technology at an even earlier stage of development, it is important to begin to anticipate the risks that will be faced and be able to quantitatively assess the risk landscape to identify critical risks and inform decisions to build safer systems for the future.

Background and Related Work

Most existing work assessing the cyber vulnerabilities of 5G is qualitative. Batalla et al. (2020) summarized security concerns and potential impacts largely based on theoretical assessment and expert opinion. The study characterized each scenario by probability of occurrence ("hard to imagine," "might happen," "certainly can happen") and the severity of consequences ("moderate,"

[1]Ph.D. Student, School of Civil and Environmental Engineering, Georgia Institute of Technology, North Ave. NW, Atlanta, GA 30332 (corresponding author). ORCID: https://orcid.org/0000-0001-7817-3735. Email: pvargasvargas3@gatech.edu

[2]Williams Family Associate Professor, School of Civil and Environmental Engineering, Georgia Institute of Technology, North Ave. NW, Atlanta, GA 30332. ORCID: https://orcid.org/0000-0002-1410-632X. Email: itien@ce.gatech.edu

Note. This manuscript was submitted on August 18, 2021; approved on November 29, 2021; published online on January 22, 2022. Discussion period open until June 22, 2022; separate discussions must be submitted for individual papers. This paper is part of the ***ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering***, © ASCE, ISSN 2376-7642.

"significant," "catastrophic"). It then combines these to classify each risk scenario into a "low," "medium," "high," or "critical" risk level. These categories provide a general assessment of the risk scenarios but give little detail characterizing the consequences and heavily depend on the qualitative evaluation done by the authors. It also does not include analysis of any specific impacts of 5G risks on interdependent networks.

Ahmad and Adnane (2016) investigated risk scenarios affecting connected and automated vehicles (CAVs), similarly assigning numbers based on qualitative categories for likelihood of occurrence and severity of the impacts. A risk score is then calculated for each risk scenario by multiplying the likelihood of occurrence and severity of impacts. This results in a numerical risk score but gives minimal detail about the type of impact caused by each risk scenario. While the method described is relevant to the evaluation of risk scenarios affecting CAVs, the study does not specifically target risk scenarios for 5G-enabled cellular V2X technology.

Farid et al. (2020) summarized the challenges that come with the integration of 5G technology into smart healthcare and transportation. Their work does not assess specific risk scenarios but rather provides an overview of the issues that must be addressed as these applications are developed. For smart transportation, these include privacy, the ethics of how to program a vehicle's response in the moments before an unavoidable collision, and who is responsible for collisions that occur between automated vehicles. For smart healthcare, these are focused more on the efficient and effective handling of patient data across multiple platforms.

Overall, there is a gap in the research of being able to quantitatively assess risks impacting the critical infrastructure networks interdependent with 5G. Those studies that do exist provide a general and largely qualitative examination of the risk landscape. The lack of real-world data and large number of unknowns at this early stage in the technology's development makes it challenging to do quantitative analysis. However, because of the safety implications of potential attacks on automated vehicles and connected transportation systems, it is essential to understand these risk scenarios and their impacts in as much detail as possible to properly prepare for these situations before they occur under real-world operational conditions. Simulations provide a way to understand the interdependent behavior of 5G and traffic networks in more detail without relying on observational data.

Use-case testing, the evaluation of a traffic network's performance in specific scenarios of interest, is an established method for testing the performance of CAVs (Yue et al. 2020). This can be done by collecting and analyzing real-world data and grouping like scenarios, an often time- and cost-ineffective approach. Microscopic traffic simulations provide a faster and less expensive way of simulating specific situations of interest (Yue et al. 2020). Yue et al. (2020) described a method for using a network level traffic simulation created using the Simulation of Urban Mobility (SUMO) software to extract a set of typical scenarios (e.g., U-turns, front and rear-end collisions), which can subsequently be used to evaluate the performance of a vehicle's connectivity or automation features using a set of indicators. This is valuable for evaluating the performance of CAVs in everyday driving conditions. However, the study does not consider scenarios caused by cyberattacks or malfunctions of the network that provides the vehicle connectivity and automation, or the impacts of these scenarios on network safety and performance.

Wang et al. (2019) simulated a network with C-V2X using 5G. However, the purpose of that paper is to simulate various implementations of connectivity and automation features to understand the reliability and efficiency of the telecommunications network through indicators including packet reception ratio, spectral efficiency, and data volumes. While this work helps to optimize the 5G-enabled C-V2X features, there is work to be done to understand the vulnerabilities of 5G in this smart vehicle application, particularly on the dependent transportation network and their consequences for drivers.

In this paper, we present a methodology to assess the interdependent relationship between a 5G network and vehicles with C-V2X features by simulating 5G risks scenarios in a traffic network containing CAVs to assess the impacts of potential risk scenarios on the safety and performance of the traffic network. The outcomes include multiple quantitative indicators related to system safety and performance for each scenario that are able to be used to compare impacts and make prioritization decisions across risk scenarios. The main advancement of the proposed methodology is that it provides more detailed information about various types of consequences (safety, efficiency) than previous work that qualitatively categorizes risk scenarios using expert opinion. The ability to provide quantitative indicators of risk scenario impacts minimizes the subjectivity of the classifications used in previous studies and allows for more objective comparison of the performance of the network under various targeted attack or system malfunction situations. The outcomes from simulations and analyses like these are especially important in an area as new as 5G-enabled C-V2X because they can help users, planners, and decision-makers to more rigorously and comprehensively understand cybersecurity risks. Being able to compare the outcomes based on the quantitative risk scenario indicators supports the development and prioritization of mitigation strategies to address vulnerabilities before systems are implemented to improve network performance and reduce the risks to drivers and system users.

Methodology

Simulation and Analysis Workflow

The analysis workflow takes relatively simple inputs defining the traffic network, vehicles, and communications parameters. Outputs of the simulation include vehicle-specific values, which are then converted into the quantitative indicators used to measure safety and performance of the network. The programs used for the simulations are the SUMO and MOSAIC programs developed by Eclipse. SUMO is a microscopic traffic simulator, which allows us to simulate the movement of many individual vehicles over a traffic network (Lopez et al. 2018). MOSAIC provides features to simulate cellular vehicle communication and vehicle automation features through applications (i.e., scripts that send/receive messages and specify a device's response to messages) used by the vehicles, RSUs, and the server in the SUMO simulation (Schrab and Protzmann 2021).

Inputs to the analysis include the map of the area of interest, comprising the network of roads over which the simulated vehicles will travel. This can either be a hypothetical network created within SUMO or a real-world network imported from OpenStreetMap (OpenStreetMap contributors 2015). For this study, the network used is a section of downtown Atlanta as shown in Figs. 1(a and b). Only publicly available data are needed to run this type of simulation. The number of vehicles and duration of the simulation is specified and can be adjusted to simulate typical traffic in the location of interest or based on time-of-day considerations. For this simulation, 650 vehicles are included over a simulation duration of 1,000 s. The vehicles travel along random routes through the network, defined using the SUMO program for random trips, which takes in the road network and generates a set of routes from random start points to random end points throughout the network. Trucks

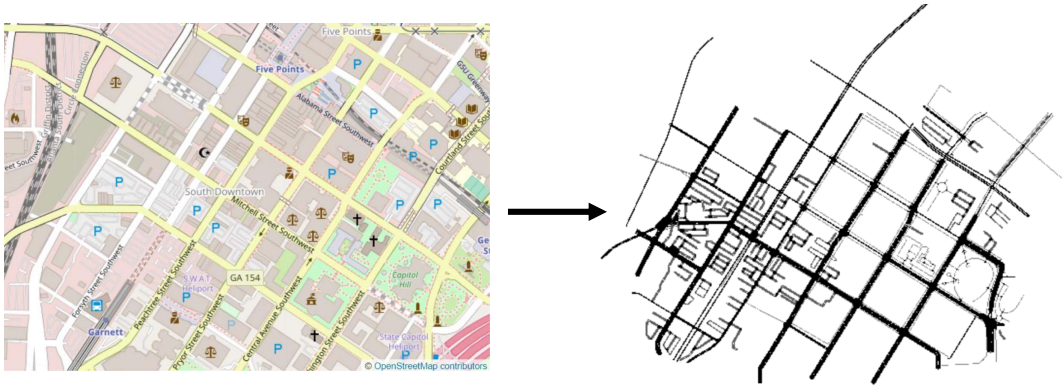

Fig. 1. (a) Section of downtown Atlanta used as an input to the SUMO simulation (base map © OpenStreetMap contributors); and (b) corresponding road network created and used for simulation and analysis.

and pedestrians can also be added into the simulation, although none were added here. The additional inputs needed to define the traffic scenario including vehicle automation and communication parameters are described in the following section.

To enable the 5G-based C-V2X communication, RSUs must be placed at specific locations throughout the network. No specific guidelines currently exist for RSU placement, and the coverage of a single unit depends on many factors including its installation height, sharp curves in the road, number of lanes, and the obstacles that surround the unit (Audi, Ericsoon, Qualcomm, Swarco, and Technische Universitat Kaiserlautern 2020). It is estimated that for highways, RSUs can be placed about 3 km apart (Audi, Ericsoon, Qualcomm, Swarco, and Technische Universitat Kaiserlautern 2020). In urban areas, RSUs can be placed uniformly throughout the network, or specifically in areas with high vehicle density. Typical distances between RSUs are 300–1,000 m, although in dense, urban areas, shorter distances may be necessary to account for interference from vehicles and buildings (5GAA 2019). Multiple more complex methods also exist to optimize RSU placement (Shi et al. 2020). In the methodology proposed in this paper, RSU devices are individually added at the desired latitude and longitude coordinates, so they can be placed at an existing RSU site or a planned RSU site. Without current standards for RSU distribution, for this simulation, RSUs were placed throughout the network at every intersection to provide full coverage for the urban area of study. Blocks are roughly 100 × 100 m. This RSU placement maximizes coverage along roads while minimizing overlap in the radii serviced by neighboring RSUs. Mavromatis et al. (2019) have found that street intersections are optimal locations for RSUs because they maximize line-of-sight coverage (important because buildings interfere with 5G signal). Additionally, RSUs can be installed on existing lamp posts and traffic lights, often found on or near street corners, to facilitate access for installation and maintenance (Mavromatis et al. 2019). The resulting RSU placement is both cost-efficient and feasible. However, the locations of the RSUs can easily be adjusted based on the network being studied and distributed as desired. The RSU communication ranges vary between 50 and 400 m as indicated in the risk scenario simulations. Fig. 2

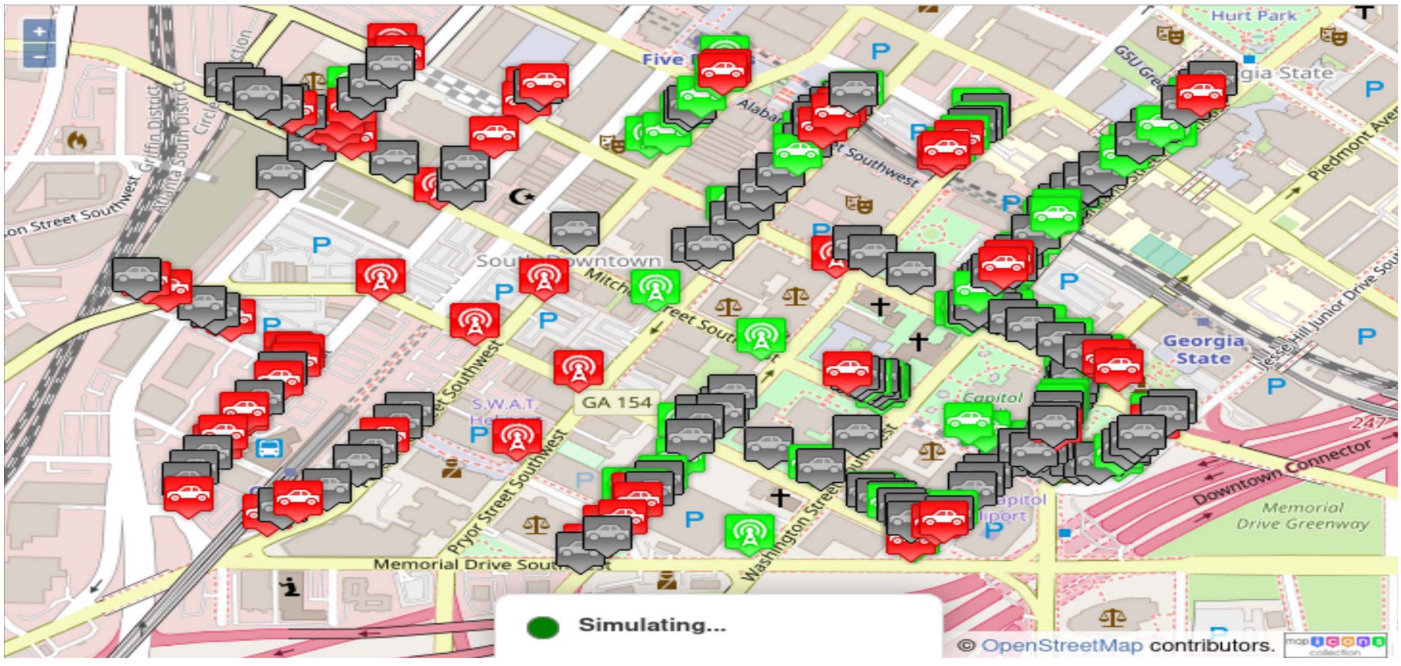

Fig. 2. Visualization of simulation with vehicles, RSUs, and message communications indicated. (Base map © OpenStreetMap contributors.)

ASCE-ASME J. Risk Uncertainty Eng. Syst., Part A: Civ. Eng., 2022, 8(2): 04022004

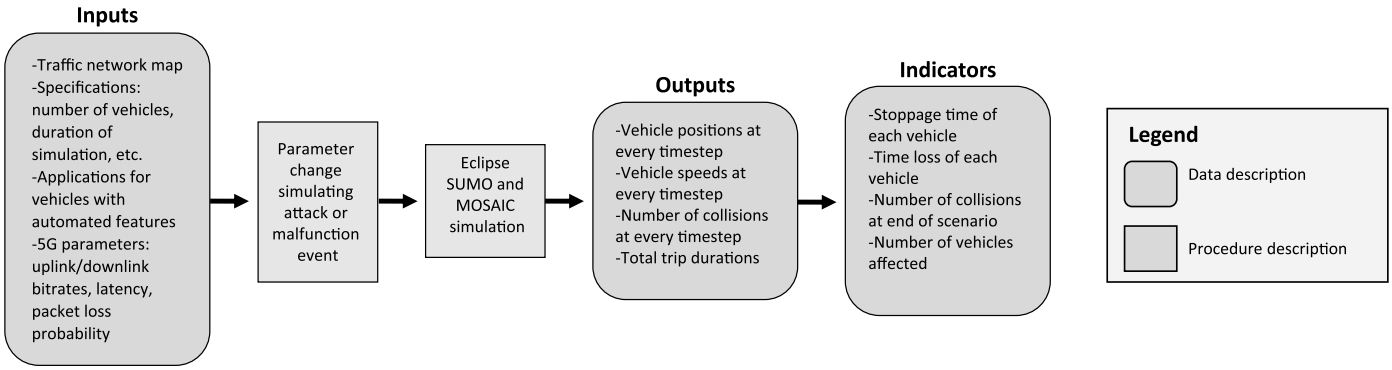

Fig. 3. Overall simulation and analysis workflow.

shows a visualization of the simulation, with individual vehicles indicated with the car icons and RSUs indicated with the antenna icons. The step size of the simulation is 1 s. RSUs and vehicles flash green when they are receiving a message and red when sending a message. Otherwise, the units appear gray.

Once the network and vehicles are defined, we are able to run simulations over a range of scenarios. The scenarios include any parameter changes that simulate an attack or malfunction event on the system. As individual vehicle outcomes are tracked, we obtain detailed outputs from each simulation and scenario. We then analyze the outcomes over the distribution of all vehicle outputs to obtain the quantitative indicators of the traffic network's performance. The overall simulation and analysis workflow is shown in Fig. 3. The rounded boxes in Fig. 3 describe the types of data input to and output from the traffic model, and the nonrounded boxes indicate main steps taken to generate the outputs.

5G Network

All C-V2X communications in this study are conducted over 5G. The following parameters were specified in the simulation for the 5G network. The maximum uplink and downlink bitrates were set to 1.5 gigabits per second (Gbps), the bitrates for mmWave (O'Donnell 2019). Messages were sent with a 3-ms latency (Ganesan et al. 2019). A packet loss probability of 0.08% was used to simulate a network reliability of 99.92%, a reliability found for 5G vehicle communication applications (Xiang et al. 2020).

Roadside Units

RSUs serve as relays between vehicles and between the server and vehicles. One characteristic of 5G is the use of many smaller RSUs to facilitate short-distance, high-speed communications between devices and, in this case, vehicles. RSUs also forward messages from the server out to any vehicles within their range. In several of the risk scenarios studied, RSUs forward information about hazardous conditions, whether correct or incorrect, to vehicles.

Server

The server acts as a traffic management center and has information about a wider network than do the individual RSUs. The server sends decentralized environmental notification messages (DENMs) to the appropriate RSU to forward to the vehicles within its broadcasting range. DENMs warn vehicles of hazards on the road, such as a collision ahead, an obstacle on the road, or otherwise hazardous environmental conditions in the area (e.g., fog, ice).

Vehicle Automation and System Communication Parameters

Within the network, the proportion of automated and nonautomated vehicles needs to be defined. While the vision for many is for fully automated transportation systems in the future, CAVs will enter the transportation system gradually as the technology becomes commercially available. A McKinsey study estimates that by 2030, about 50% of new vehicles sold will be "highly autonomous" and up to 15% of new vehicles sold will be fully autonomous (Kaas et al. 2016). The simulations in this study are composed of 50% nonautomated and 50% vehicles with the automated features subsequently described. This vehicle makeup represents a scenario relatively near-term in the future, with the proportion of nonautomated and automated vehicles easily adjusted to different future scenarios.

At the start of the simulation, each automated vehicle's distance sensor is activated, allowing it to detect the distance between itself and the vehicle ahead. This sensor has a range of 4 m (Jahromi 2019). At every time step (1 s), each vehicle broadcasts a cooperative awareness message (CAM) to all vehicles and RSUs within its broadcast range. The broadcast radius for CAVs can range from 360 to 700 m (Ganesan et al. 2019). In this simulation, each vehicle has a range of 400 m over which it can broadcast messages.

Each vehicle also has an automated emergency braking feature. Although the driver is still expected to be in full control of braking, this serves as an additional safety feature in case the driver does not react in time. This feature is based on functionality first described by Milanes et al. (2011). If the distance to the vehicle ahead has decreased by more than 7 m in the last time step (1 s) and the distance to the car ahead falls below 15 m, the vehicle will sharply reduce its speed.

When a vehicle detects a hazard using its activated environmental sensors in its vicinity, the vehicle determines whether this hazard is on its route. If it is on its route, the vehicle will reroute to the fastest alternative route. This is done by using a MOSAIC navigation module to find alternate routes to the vehicle's destination, assign each an expected travel time using a MOSAIC cost function, and then choose the alternate route with shortest expected travel time. Then, the vehicle will send a DENM to all vehicles and RSUs in its broadcasting radius alerting them of the hazard. Rerouting can only be done once by each vehicle due to the program's limitations. Unlimited rerouting would intractably increase computation time. If the vehicle receives a DENM warning of an environmental hazard in its vicinity, the vehicle will reduce its speed as a safety measure. DENMs can be sent by both vehicles and servers.

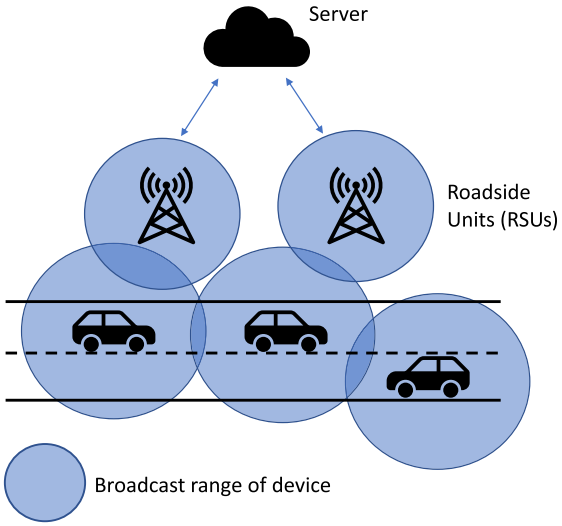

Fig. 4. C-V2X system diagram with vehicles, RSUs, and server.

In the overall C-V2X system, vehicles periodically broadcast 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 DENMs warning vehicles of hazardous conditions or traffic in their vicinity. A diagram illustrating the system is shown in Fig. 4. Table 1 provides a summary of the simulation settings and parameter values that are defined in the analysis, including overall simulation settings, 5G network parameters, and vehicle parameters.

In Table 1, the vehicle parameters are defined as follows: minGap is the minimum distance that a vehicle leaves between itself and the vehicle ahead when stopped, accel and decel are the typical acceleration and deceleration speeds of a vehicle, sigma denotes the driver imperfection value between 0 and 1 where 0 represents perfect driving, tau denotes the time headway (the time needed to reach the vehicle ahead while traveling at its current speed) that a vehicle attempts to maintain between itself and the vehicle ahead to be able to brake safely and leave the distance defined by minGap between itself and the vehicle ahead when stopped, speedFactor is a value greater than or equal to zero that represents the fraction of the speed limit that a vehicle will travel at under ideal conditions (e.g., if speedFactor = 1, the vehicle will travel at the speed limit under perfect conditions), communication range is the radius over which a vehicle can send messages to other vehicles and RSUs, and distance sensor range is the distance over which a vehicle can detect the distance between itself and the vehicles immediately ahead and behind.

The features included in this study simulate a low level of vehicle communication and automation. As this technology is developed and more automated vehicles are on the roads, additional features can be added to this model to simulate relevant scenarios more accurately. However, even with this low level of automation, the connection between 5G infrastructure and vehicles creates opportunities for attackers or telecommunications network malfunctions or disruptions to unexpectedly alter the behavior of the vehicles. Results in this study show the ranges of effects of these vulnerabilities across the transportation system.

Quantitative Performance Indicators

To assess the performance of the network, five main quantitative indicators are used. Time loss and stoppage time measure changes in network performance, the number of vehicles affected and the number of vehicles unable to enter the network measure overall impacts on the network, and the number of collisions measures safety over the network. All scenarios contain 650 vehicles. The time loss and stoppage time indicators are given for each vehicle in the analysis and for consistency in the comparison across vehicles, and these indicators are measured as a percentage of each vehicle's trip time. For example, 70% time loss means that the vehicle takes 70% more time to complete its trip than under ideal no traffic conditions; 80% stoppage time means that the vehicle spent 80% of its trip time stopped. The number of vehicles affected is counted as the cumulative number of vehicles in the scenario that are found to have a greater time loss or stoppage time than it would have had in a default scenario. The default scenario is one where no attacks or malfunctions occur. To show the impact of each risk scenario, results in the following sections for each risk scenario are

Table 1. Summary of simulation settings and parameter values

Parameter category	Parameter	Value	
General simulation settings			
	Time step (s)	1	
	Total simulation duration (s)	1,000	
	Total number of vehicles	650	
	RSU communication range (m)	50–400 (varies by simulation)	
5G network parameters			
	Uplink bitrate (Gbps)	1	
	Downlink bitrate (Gbps)	1	
	Latency (ms)	3	
	Packet loss probability (%)	0.08	
Vehicle parameters		Nonautomated	Automated
	minGap (m)	2.5	2.5
	Accel (m/s^2)	2.6	2.6
	Decel (m/s^2)	4.5	4.5
	Sigma	0.5	0.0
	Tau	1.0	1.0
	speedFactor	1.0	1.0
	Communication range (m)	400	400
	Distance sensor range (m)	4	4

Table 2. Summary of traffic network safety and performance indicators

Indicator	Description
Time loss	Time that is added to a vehicle's trip due to traveling at a slower than ideal speed. It is the time that the vehicle would need to complete the trip if it traveled at the speed limit for the entire trip subtracted from the time that the vehicle needed to complete its trip in the scenario. This is an indicator of traffic congestion along the vehicle's route.
Stoppage time	Time that a vehicle spends at unplanned stops during its trip. It is measured as the amount of time that a vehicle spends traveling at <0.1 m/s, also referred to as "waiting time" in programs such as SUMO. This is an indicator of more severe traffic congestion than indicated by time loss.
Number of vehicles affected	Used to estimate how widespread the impacts of each risk scenario are. A vehicle is counted as "affected" if it has a greater time loss or stoppage time than it did in the default scenario. If it has both an increased time loss and stoppage time, it is counted only once.
Number of vehicles unable to enter the network	The number of vehicles that were unable to even begin their trip because their trip's starting point was occupied by other vehicles during the entire simulation time. This signifies significant traffic congestion.
Number of collisions	The cumulative number of collisions that occurred in the scenario. This indicates severe safety consequences over the network.

shown in comparison with the outcomes in comparison with the default scenario. If a vehicle is found to have an increased time loss and stoppage time, it is counted as an affected vehicle only once. The number of vehicles unable to enter the network counts the cumulative number of vehicles that are unable to start their trips over the full scenario run time due to congestion throughout the network. The number of collisions is counted cumulatively over the full network and full scenario run time. Table 2 summarizes the safety and performance indicators defined and used in this study.

Additionally, for some of the risk scenarios, traffic congestion in the road network was so high that some of the 650 vehicles could not begin their trips. We counted the number of vehicles that did not enter the network as a quantitative performance indicator for each scenario as well.

Risk Scenarios

The risk scenarios analyzed in this study are summarized in Table 3 and are described in further detail in the results section for each specific scenario. Table 3 presents the types of attacks analyzed and how vehicles are affected within each attack scenario. For a given risk, we ran variations of each scenario to investigate the effect of parameters such as number of vehicles affected, number of RSUs affected, RSU radius, and RSU chosen on the results. In some cases, risk scenarios are combined to investigate compounding effects of multiple risks. Additional variations of the scenarios analyzed, as well as additional risk scenarios of interest, can be run using the proposed methodology. Although not a comprehensive list of all potential attacks on a smart transportation system, these scenarios represent a variety of ways in which the behavior of a vehicle can be manipulated and C-V2X features can be exploited via 5G to disrupt a transportation system. The risk scenarios analyzed represent a range of currently identified potential vulnerabilities of the interdependent 5G and traffic networks, affecting the behavior of vehicles in different ways, resulting in a comprehensive view of the impacts of 5G risks on connected transportation systems.

Table 3. Summary of risk scenarios analyzed

Type of attack	Vehicles affected
Jamming attack	Individual random vehicle
Fake environmental hazard warning	Vehicles within range of RSU
Forced sudden braking	Vehicles within range of RSU
Disabling of automated emergency braking feature	Vehicles within range of RSU
Disabling of automated emergency braking + forced sudden braking	Vehicles within range of RSU
Disabling of brakes	Vehicles within range of RSU
Disabling of brakes + forced sudden braking	Vehicles within range of RSU

Results

Jamming Scenario Targeting Individual Vehicles

This simulates a scenario in which an attacker seeks to inhibit a selected vehicle's ability to communicate with other vehicles. It was simulated by changing the driver imperfection value and removing vehicles' automation features. Drivers of vehicles with V2X capabilities and automated driving features have higher likelihoods of becoming distracted while driving due to overreliance on the vehicle's automation (Aria et al. 2016). The driver imperfection value, typically denoted as the sigma value, ranges from 0 to 1, with 0 representing perfect driving. In addition to disabling the vehicle automation features, the driver imperfection value was increased from 0.5 to 0.9. Fig. 5 shows the total distributions of time loss and stoppage time for all vehicles under this scenario. To investigate the differences in impact between single versus multiple vehicles being affected by a jamming attack, three risk scenarios were run, with one, two, and five vehicles being jammed. Fig. 5 shows these results compared with those from the default no attack or malfunction scenario. To quantify the differences in the distributions across the scenarios, Table 4 provides the statistics and corresponding quantitative indicators, including time loss, stoppage time, vehicles affected, and collisions, for the scenario outcomes.

To assess the impacts of each risk scenario over the full system, full distributions of values for time loss and stoppage time for each scenario are given. Included are results for not only how the vehicles targeted were affected, but also how their change in behavior affects the surrounding vehicles across the system, including cascading effects across vehicles not directly targeted. By doing this, system-level performance and impacts are investigated. From Fig. 5, the overall shapes of the distributions do not differ significantly. However, the center of the stoppage time distribution shifts slightly toward higher values as the scenario severity increases. This result is provided in Table 4, with the slight increase in mean stoppage time. To further examine severity in impacts of scenarios, extreme values of the distributions are also quantified. Greater than 80 and 95% time loss and stoppage time are chosen as the extreme impact thresholds. In the default scenario, there are no vehicles

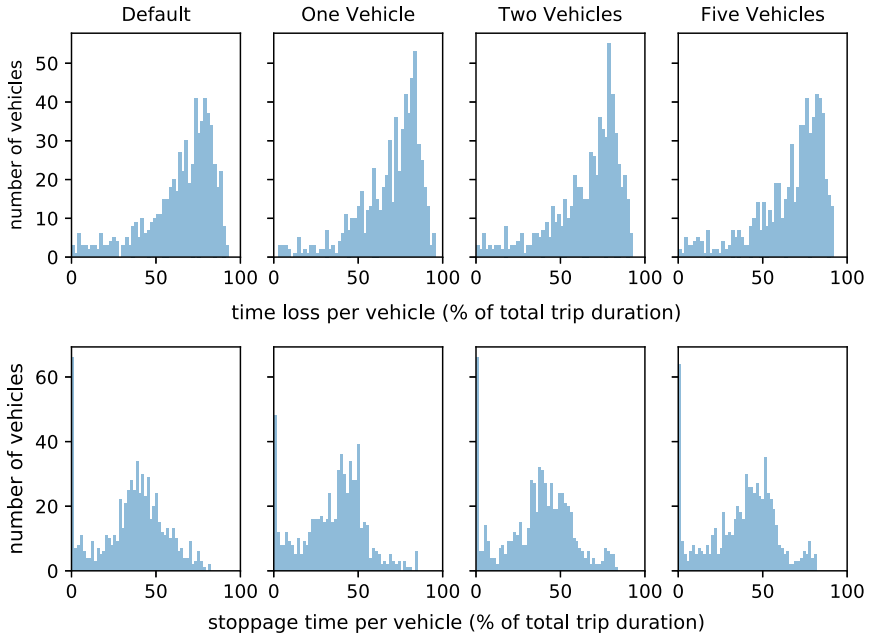

Fig. 5. Distributions of time losses and stoppage times for vehicles in jamming scenario with variations in number of vehicles affected.

Table 4. Indicator values for jamming scenario with variations in number of vehicles affected

Indicator	Default	One vehicle jammed	Two vehicles jammed	Five vehicles jammed
Mean time loss	74.9%	70.1%	71.4%	73.0%
Mean stoppage time	38.5%	38.4%	38.9%	41.6%
% vehicles affected	—	50%	49%	52%
Vehicles >80% time loss	35.4%	26.6%	23.7%	29.7%
Vehicles >80% stoppage time	1.2%	0.3%	0.3%	0.9%
Vehicles >95% time loss	0	0	0	0
Vehicles >95% stoppage time	0	0	0	0
% vehicles unable to enter network	0	0	0	0
# collisions	0	0	0	0

above 95% time loss or stoppage time. Few vehicles are stopped over 80% of their total trip time and a moderate amount have a time loss above 80% of their total trip time. The mean time loss is high because of the large number of vehicles in the network. However, nearly half of the vehicles spend no time stopped due to congestion.

Looking at the risk scenario results, the impacts of affecting a single vehicle are noticeable, particularly with half of the vehicles in the network being affected through some increase in stoppage time or time loss compared with the default scenario. However, changes to single vehicles (see the difference in results of the One Vehicle Jammed case and the Two Vehicles Jammed case in Table 4) are small and results show that the consequences depend more on the specific vehicle(s) targeted than the number of vehicles affected. This is because the vehicle routes vary widely and system-level outcomes are greatly impacted by the characteristics (e.g., trip route) of the specific vehicle(s) targeted. Jamming one vehicle may have a larger effect than jamming a different vehicle, simply because of what path it travels through the network. If a targeted vehicle travels along more congested roads, jamming it will likely affect more surrounding vehicles than a vehicle traveling through the roads with less traffic. Rather than attacks directly affecting an individual vehicle's behavior, scenarios impacting vehicles through the RSUs affect a larger number of vehicles, showing more consistent trends and larger effects, and are investigated next.

Fake Environmental Hazard Warning Sent to Vehicles Passing through Range of Affected Roadside Unit

In this scenario, the server sends a fake DENM and the affected RSU alerts vehicles that there is ice on the road at the RSU's location. Vehicles receiving this fake message respond by slowing down. To investigate the impact of varying RSU radii on the results, Fig. 6 shows the distributions of time loss and stoppage time for all vehicles under three risk scenarios, where the RSU has a radius of 50, 200, and 400 m. Table 5 provides the quantitative indicator values for the three RSU radius variations.

From Fig. 6 and Table 5, each increase in RSU radius has a large impact on the network indicators. There is a particularly large difference in the shapes of the distributions between the affected RSU having a radius of 50 versus 200 m cases. Blocks in the network are about 100-m wide and an RSU is placed at every corner. This means that when the radius is 200 or 400 m, the ranges of the RSUs will overlap, causing the vehicles in these overlapping regions to reduce their speed more drastically. In particular, the mean stoppage time is increased from 38.5% to 36.0% in the default and 50-m RSU cases, to 92.9% and 96.7% for the 200 and 400-m RSU cases, respectively. Similarly, mean time loss increases from 74.9% and 75.4% to 97.7% and 98.6%. From Fig. 6, the time loss and stoppage time distributions exhibit significant distribution mass at the extreme right-side values in the 200 and 400-m RSU cases. This change in vehicle distribution outcomes is reflected in the extreme values in Table 5, where, for example, the percentage of vehicles with greater than 80% stoppage time increases from 1.2%–2.8% to 75.0%–83.1% of vehicles for the default, 50, 200, and 400-m cases; and the percentage of vehicles with greater than 80% time loss increases 35.4%–35.9% to 74.9%–83.3%, respectively. Similar increases are found for the percentage of vehicles experiencing greater than 95% time loss and stoppage time. Finally, an increase in the number of vehicles not able to enter the network is also observed. In the 400-m RSU case, 30.8% of vehicles did not

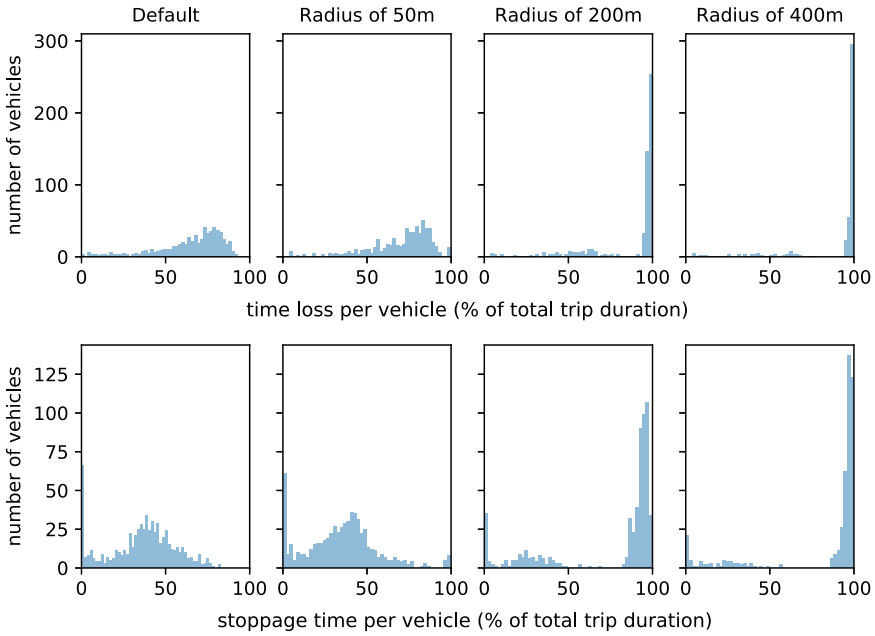

Fig. 6. Distributions of time losses and stoppage times for fake DENM scenario with variations in RSU radius.

Table 5. Indicator values for fake DENM scenario with variations in RSU radius

Indicator	Default	50-m RSU radius	200-m RSU radius	400-m RSU radius
Mean time loss	74.9%	75.4%	97.7%	98.6%
Mean stoppage time	38.5%	36.0%	92.9%	96.7%
% vehicles affected	—	50%	73%	61%
Vehicles >80% time loss	35.4%	35.9%	74.9%	83.3%
Vehicles >80% stoppage time	1.2%	2.8%	75.0%	83.1%
Vehicles >95% time loss	0	2.0%	72.4%	82.4%
Vehicles >95% stoppage time	0	2.0%	34.5%	64.2%
% vehicles unable to enter network	0	1.4%	11.2%	30.8%
# collisions	0	0	0	0

even have the opportunity to enter the network to start their trips due to the network being so congested from this disruption scenario.

To further investigate the potential impacts of a fake DENM scenario, the effect of the number of RSUs affected was also examined. Results are shown in Fig. 7 and Table 6 for one, two, and three RSUs being affected.

From Table 6, the One RSU scenario affects the network by increasing the number of vehicles that experience large amounts (>80%) of stoppage time. In addition, nine vehicles are unable to enter the network. Affecting the subsequent RSUs has a smaller additional impact on the network. The Two RSU scenario has a larger number of vehicles that never enter the network because the point from which they begin their trip is blocked with traffic.

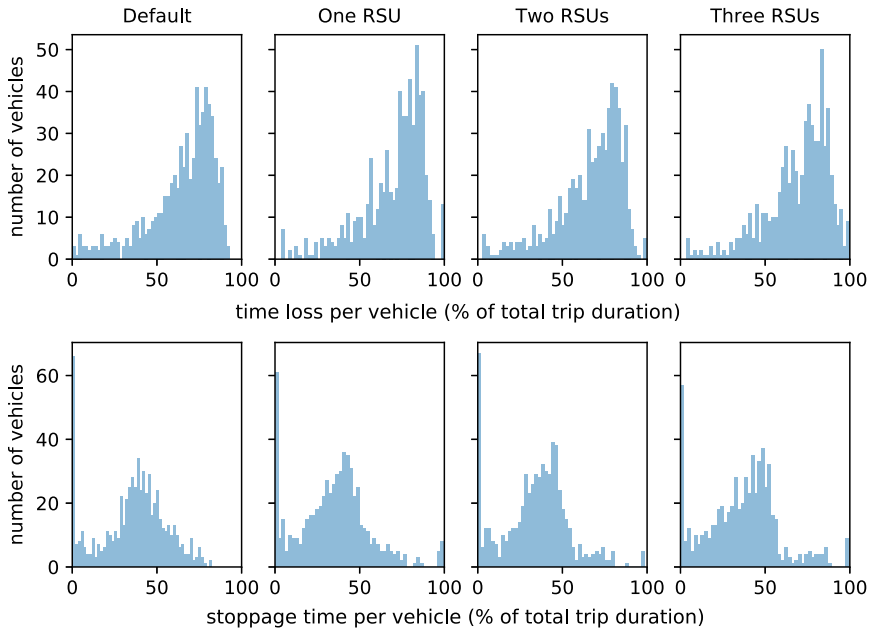

Fig. 7. Distributions of time losses and stoppage times for fake DENM scenario with variations in number of RSUs affected.

Table 6. Indicator values for fake DENM scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	75.4%	71.2%	73.9%
Mean stoppage time	38.5%	36.0%	36.3%	38.8%
% vehicles affected	—	50%	42%	54%
Vehicles >80% time loss	35.4%	35.9%	26.7%	33.9%
Vehicles >80% stoppage time	1.2%	2.8%	1.3%	4.1%
Vehicles >95% time loss	—	2.0%	0.8%	2.5%
Vehicles >95% stoppage time	0	2.0%	0.8%	1.4%
% vehicles unable to enter network	0	1.4%	2.8%	1.8%
# collisions	0	0	0	0

Table 7. Indicator values for fake DENM scenario with alternate combinations of affected RSUs

Indicator	Two RSUs	Two RSUs alternate	Three RSUs	Three RSUs alternate
Mean time loss	71.2%	71.9%	73.9%	72.0%
Mean stoppage time	36.3%	41.7%	38.8%	38.0%
% vehicles affected	42%	50%	54%	48%
Vehicles >80% time loss	26.%	29.3%	33.9%	27.7%
Vehicles >80% stoppage time	1.3%	4.5%	4.1%	10.9%
Vehicles >95% time loss	0.8%	3.0%	2.5%	10.3%
Vehicles >95% stoppage time	0.8%	2.7%	1.4%	9.2%
% vehicles unable to enter network	2.8%	1.8%	1.8%	0
# collisions	0	0	0	0

The effect, however, is small, and it is found that the impacts vary depending on which RSUs are chosen. For example, results for Two RSU and Three RSU alternate scenarios are shown in Fig. 8 and Table 7.

From Table 7, the Two RSU alternate results are similar to those of the Three RSU variations, supporting the conclusion that additional affected RSUs have a smaller impact on the network than the first affected RSU. However, the Three RSU alternate variation shows how much the choice of RSU matters, with a greater proportion of vehicles experiencing the extreme impacts of >95% time loss and >95% stoppage time compared to the results from the other scenarios. This suggests that multiple trials should be run for these scenarios, whether that means randomly varying the trips through the network or running a variation with different choices of assets affected for the particular study area, location characteristics, or scenarios of interest.

Forced Sudden Braking Affecting Vehicles Passing within the Range of an Affected Roadside Unit

In this scenario, 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, one vehicle is forced to brake harshly every time it reaches an arbitrary medium velocity of 40 km/h (25 mi/h). The results for this scenario are summarized in Fig. 9 and Table 8 for one, two, and three affected RSUs.

The effect of a single RSU being affected by this attack is large, as seen from the increases in all of the indicators in Table 8. The mean stoppage time in the One RSU scenario increased to 94.6% from the default mean stoppage time of 38.5%. Similarly, the mean time loss increased to 98.4% of the trip time. The percentages of vehicles with high amounts of time loss and stoppage time (>80 and >95%) all had large increases, indicating that this scenario caused a significant disturbance in the flow of traffic across the network. In addition, 14.5% of vehicles were unable to even enter the network and begin their trips due to increased network congestion. This attack can affect a large proportion of the network (i.e., 70%–80% of vehicles) without 70%–80% of the vehicles passing through the range of the RSU because the behavior of vehicles is permanently altered. This means that they brake suddenly for the rest of their trip, causing vehicles near them to react by slowing down. The overall impacts from this risk scenario, including cascading effects across the system, are also reflected in the shapes of the distributions, which change significantly between the default and attack

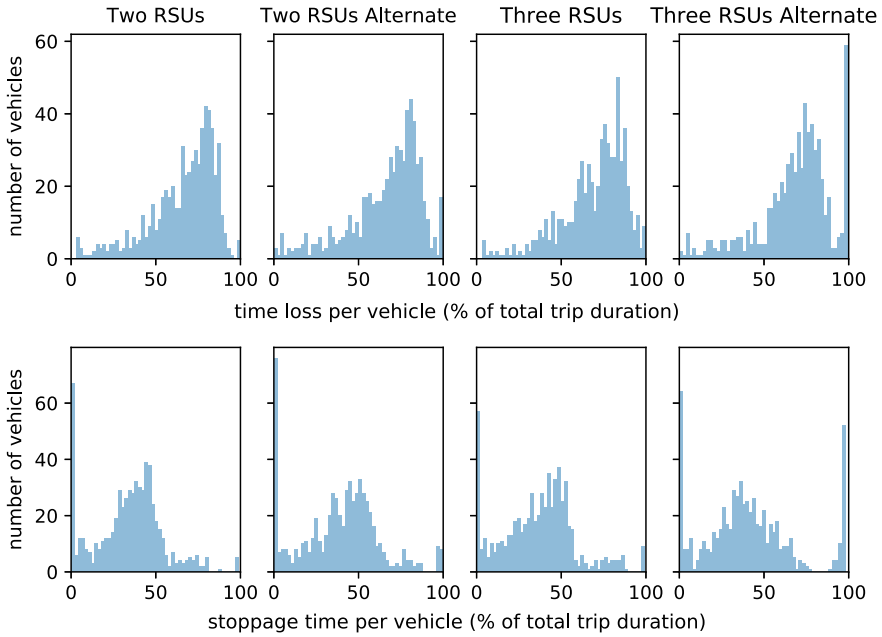

Fig. 8. Distributions of time losses and stoppage times for fake DENM scenario with alternate combinations of affected RSUs.

ASCE-ASME J. Risk Uncertainty Eng. Syst., Part A: Civ. Eng., 2022, 8(2): 04022004

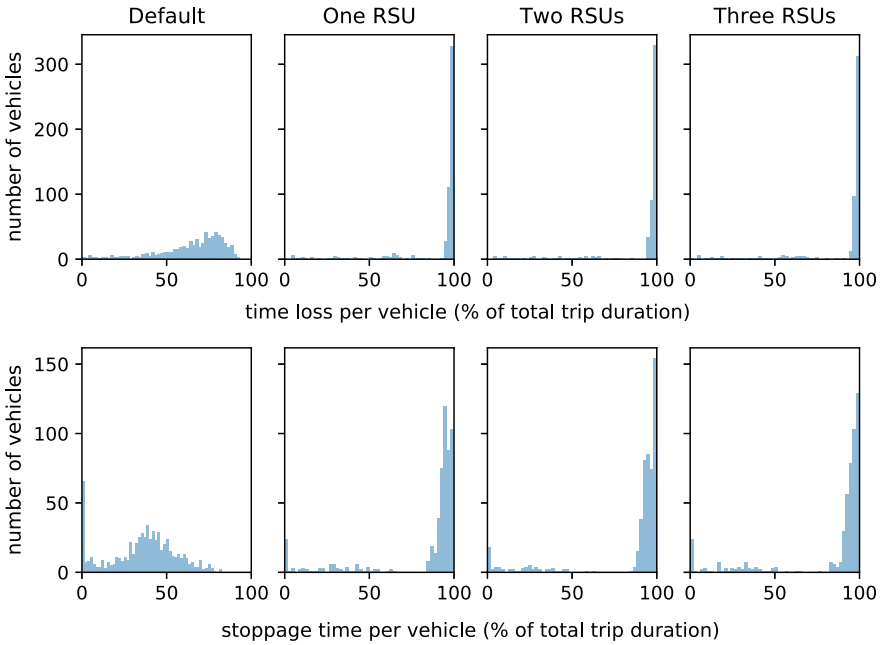

Fig. 9. Distributions of time losses and stoppage times for forced sudden braking scenario with variations in number of RSUs affected.

Table 8. Indicator values for forced sudden braking scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	98.4%	98.5%	98.5%
Mean stoppage time	38.5%	94.6%	95.1%	95.3%
% vehicles affected	—	78%	72%	74%
Vehicles >80% time loss	35.4%	84.7%	86.6%	85.5%
Vehicles >80% stoppage time	1.2%	83.8%	86.4%	85.1%
Vehicles >95% time loss	0	82.9%	85.5%	83.6%
Vehicles >95% stoppage time	0	46.4%	50.7%	53.1%
% vehicles unable to enter network	0	14.5%	19.5%	18.3%
# collisions	0	0	0	0

scenarios. This change is observed in Fig. 9, with large distribution mass shifted to the high time loss and high stoppage time values under the attack scenarios.

In this scenario, the effect of additional RSUs being affected leads to a small decrease in the performance of the network. Between the Two RSU scenario and the One RSU scenario, the mean time loss and stoppage times each increase by less than 1%. All other indicators increase by 2–5% each, suggesting that affecting an additional RSU increases traffic congestion, but to a much smaller degree than the first RSU. The number of vehicles affected decreases compared to the One RSU scenario, which may be attributed to the randomness of where the traffic congestion occurs. Increased stoppage times in one part of the network may decrease the traffic flow along other roads, decreasing the travel times for the vehicles traveling along those roads. Similar trends can be seen between the Two RSU and Three RSU scenarios, although in the Three RSU scenario, the largest increase is of 2.4% in vehicles with a stoppage time of >95%, and some of the indicator values decrease by about 1%. This reinforces the conclusion that RSUs affect the flow of traffic across a complex network differently and the choice of affected RSU matters. Future work includes investigating which characteristics (e.g., traffic within range, proximity to another RSU, proximity to an intersection or other road feature, etc.) cause an RSU to have a greater impact than another.

Disabling of Automated Emergency Braking Feature

In this scenario, when vehicles pass through an RSU's range, the emergency braking feature is disabled for the rest of the vehicle's trip. Note that the vehicle's brakes remain functional, and the driver is still able to brake manually. It is the automated vehicle feature that is disabled. Results of this scenario and variations where one, two, and three RSUs were affected are summarized in Fig. 10 and Table 9.

The indicator values in Table 9 show that no change occurs in the performance of the network due to the disabling of the emergency braking feature. The distributions in Fig. 10 are also unchanged across the default, One RSU, Two RSU, and Three RSU scenarios, showing that the vehicles' trips were completely unaffected by the disabling of this automation feature. It is likely that the vehicles did not need to use the emergency braking feature in this scenario. The following scenario combines this scenario with the forced sudden braking scenario to investigate the potential impacts of a compounded risks scenario.

Disabling of Automated Emergency Braking Feature and Forced Sudden Braking of Vehicles Passing through Range of Affected Roadside Unit

This scenario is a combination of two of the previous ones. Here, vehicles passing through the range of an affected RSU both brake suddenly throughout the remainder of their trip when they reach 40 km/h, and their emergency braking feature is disabled. It investigates the possible consequences of combined risks, with compounded effects across the network. Results of variations where one, two, and three RSUs are affected are shown in Fig. 11 and Table 10. A comparison of the indicator values from this combined risk scenario with the results from the individual *forced sudden braking* scenario from the previous section is provided in Table 11 in terms of percentage change for each indicator.

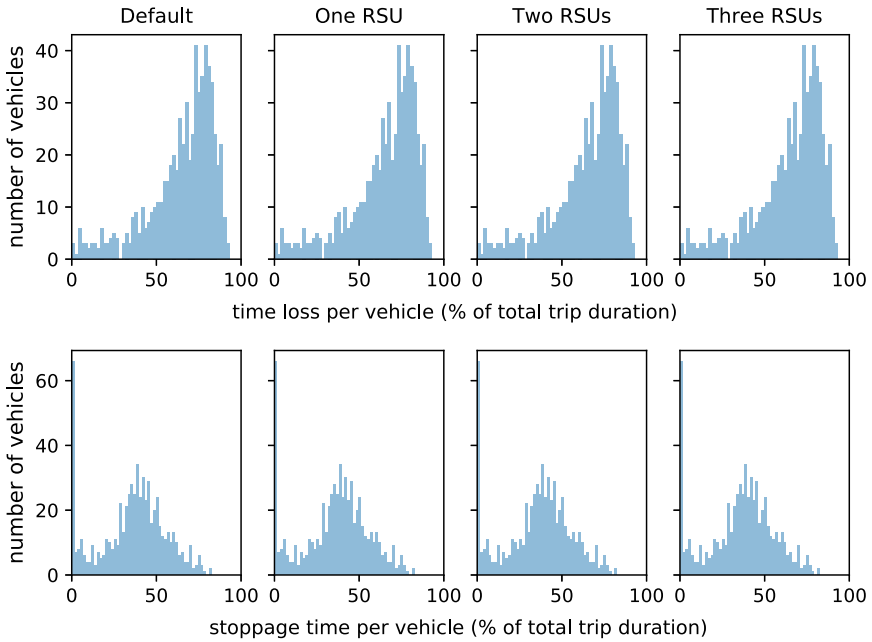

Fig. 10. Distributions of time losses and stoppage times for the disabling of emergency braking feature scenario with variations in number of RSUs affected.

Table 9. Indicator values for the disabling of emergency braking feature scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	74.9%	74.9%	74.9%
Mean stoppage time	38.5%	38.5%	38.5%	38.5%
% vehicles affected	—	0	0	0
Vehicles >80% time loss	35.4%	35.4%	35.4%	35.4%
Vehicles >80% stoppage time	1.2%	1.2%	1.2%	1.2%
Vehicles >95% time loss	0	0	0	0
Vehicles >95% stoppage time	0	0	0	0
% vehicles unable to enter network	0	0	0	0
# collisions	0	0	0	0

From Table 10, the performance of the network decreases slightly in each of the three variations of this combined risk scenario compared to the corresponding forced sudden braking scenario described in Table 8. For clarity, the differences in values between the individual *sudden braking* scenario and the combined *sudden braking + disabling of emergency braking* scenario are provided in Table 11. All except two of the indicators increase, indicating that the flow of traffic is disrupted even more with the disabling of the emergency braking feature in vehicles passing through the affected RSU. The magnitude of the increases varies, with the largest occurring for the number of vehicles with stoppage times >95% of trip duration. As the number of vehicles with stoppage times >80% did not increase to the same degree, this increase is due to many of the vehicles with already high (between 80% and 95%) stoppage times being affected disproportionately. This can be attributed to the fact that the same RSUs both caused sudden braking and disabled the emergency braking feature, affecting the same set of vehicles. This set of directly affected vehicles are likely to be the ones with highest stoppage times. The largest increases for each indicator can be seen in the One RSU scenario, while the increases are significantly smaller in the Two RSU and Three RSU scenarios. Similar to the other scenarios, the first RSU has the largest impact on the network while additional affected RSUs have a smaller effect. The shapes of the distributions in Fig. 11 are similar to those in Fig. 9, with a further shift toward the right. Although the disabling of emergency brakes alone had no effect on the network, it did exacerbate the negative impacts on the traffic network when combined with the sudden braking scenario.

Disabling of Brakes

All of the scenarios analyzed thus far, while in several cases causing significant network performance delays, no safety impacts in terms of increased collisions were observed. This scenario investigates a more severe safety concern in which when a vehicle passes through the range of an affected RSU, the brakes on the vehicle are disabled for the remainder of the vehicle's trip. Results of this scenario with one, two, and three affected RSUs are summarized in Fig. 12 and Table 12.

The permanent disabling of brakes, as expected, causes a large disturbance in the network, as shown by the distributions in Fig. 12 and the indicator values in Table 12. Even with one RSU affected, 178 collisions occurred, and 290 vehicles were not able to begin their trips through the network at all, suggesting heavy traffic congestion caused by the many collisions. Mean time loss and mean stoppage time are also very high (between 95% and 97%) for all three variations of the scenario. The indicators are similar for the three variations, with some increasing and some decreasing as the number of affected RSUs changes. In all cases, this scenario shows severe safety and efficiency consequences. Results show that affecting even just one RSU in this way leads to large systemwide impacts. Of particular concern is the safety impact, indicated by the large number of collisions in the network within the 1,000-s analysis time frame. It is critical to consider such risk scenarios as 5G is deployed and vehicles become increasingly connected and dependent on the 5G telecommunications network for operations.

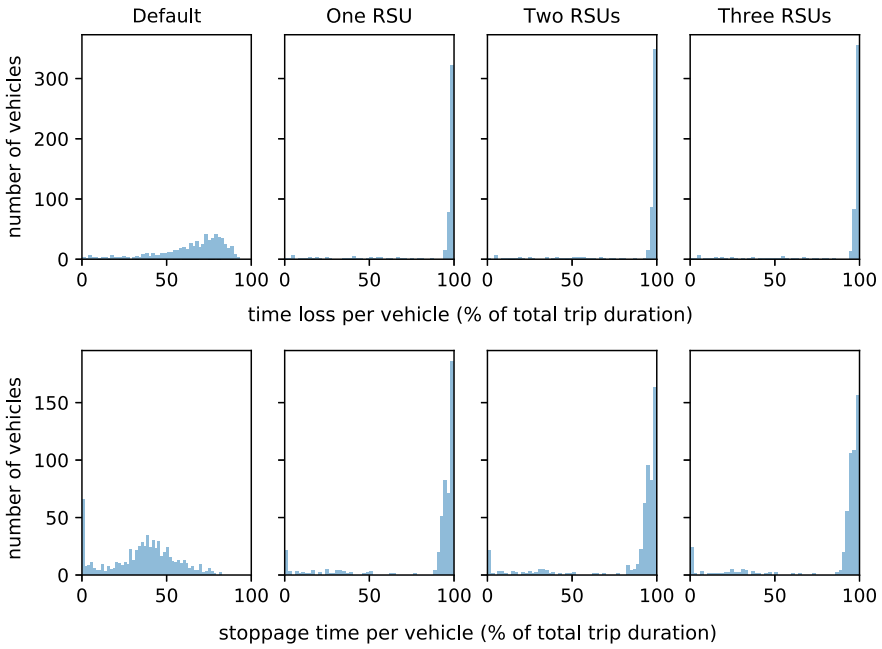

Fig. 11. Distributions of time losses and stoppage times for the disabling of emergency braking feature and forced sudden braking combined scenario with variations in number of RSUs affected.

Table 10. Indicator values for the disabling of emergency braking feature and forced sudden braking combined scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	98.8%	98.7%	98.7%
Mean stoppage time	38.5%	96.3%	95.7%	96.0%
% vehicles affected	—	65%	71%	70%
Vehicles >80% time loss	35.4%	86.3%	87.3%	87.3%
Vehicles >80% stoppage time	1.2%	85.9%	86.7%	86.9%
Vehicles >95% time loss	0	85.7%	86.5%	86.3%
Vehicles >95% stoppage time	0	65.6%	59.3%	65.3%
% vehicles unable to enter network	0	25.8%	20.2%	20.2%
# collisions	0	0	0	0

Table 11. Difference in indicator values between combined *disabling of emergency braking feature and forced sudden braking* scenario and individual *forced sudden braking*scenario (percentage change between Tables 10 and 8)

Indicator	One RSU	Two RSUs	Three RSUs
Mean time loss	+0.4%	+0.2%	+0.2%
Mean stoppage time	+1.7%	+0.6%	+0.7%
% vehicles affected	+13%	−1%	−4%
Vehicles >80% time loss	+1.6%	+0.7%	+1.8%
Vehicles >80% stoppage time	+2.1%	+0.3%	+1.8%
Vehicles >95% time loss	+2.8%	+1%	+2.7%
Vehicles >95% stoppage time	+19.2%	+8.6%	+12.2%
% vehicles unable to enter network	+11.3%	+0.7%	+1.9%
# collisions	0	0	0

Disabling of Brakes and Forced Sudden Braking of Vehicles Passing through Range of Affected Roadside Unit

Finally, this scenario represents the most extreme case in which vehicles' behavior is severely altered, causing very dangerous driving conditions. The attacker gains control over the vehicles' brakes, causing the vehicles to brake suddenly for the remainder of the trip, while also disabling the vehicles' brakes from manual operation. Results from variations of this scenario with one, two, and three affected RSUs are given in Fig. 13 and Table 13.

This scenario shows how combining multiple risk scenarios exacerbates the negative impacts of these attacks on the safety and performance of the network. While the individual *forced sudden braking* scenario caused mean time loss and stoppage times as presented in Table 8 that were similar to, and actually on average about 2% greater than, the corresponding values in this scenario presented in Table 13, it did not cause any collisions. Similarly, the mean time loss and stoppage times of each variation of the individual *disabling of brakes* scenario presented in Table 12 were similar to the corresponding values in this scenario. These indicators alone would suggest that the traffic network performance was close to, and in some cases more efficient than, the outcomes under this combined risk scenario compared to the individual risk scenarios. However, it is important to look across the indicators. From a safety point of view, the outcomes of the combined risk scenario were, in fact, catastrophic. The combination of disabling of brakes with forced sudden braking created more dangerous situations across the network where braking was necessary to avoid a collision; however, brakes were disabled, resulting in a significant increase in the number of collisions. All three variations of the previous scenario where brakes were disabled only had nearly 200 collisions. The number of collisions in the three variations here is about double that amount. More than half of the vehicles in the system were involved in collisions.

To better understand the cascading effects of such a severe event, we can look at the distributions in Fig. 13, where the results show a set of vehicles with time losses and stoppage times near 100%, as well as a set of vehicles with times losses and stoppage times near 0%, with few vehicles in between. This, along with the decreases in mean time loss and mean stoppage time described at the beginning of this section, suggest that this combined scenario caused a large number of collisions, which lead to

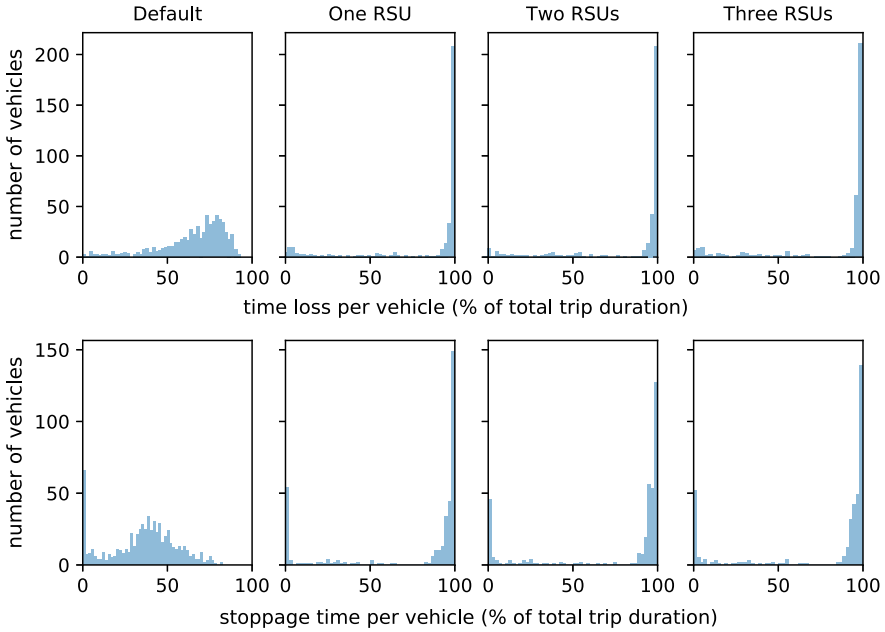

Fig. 12. Distributions of time losses and stoppage times for the disabling of brakes scenario with variations in number of RSUs affected.

Table 12. Indicator values for the disabling of brakes scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	98.9%	98.3%	98.4%
Mean stoppage time	38.5%	96.8%	95.5%	95.9%
% vehicles affected	—	44%	43%	48%
Vehicles >80% time loss	35.4%	74.7%	75.6%	74.7%
Vehicles >80% stoppage time	1.2%	74.7%	73.6%	74.2%
Vehicles >95% time loss	0	68.9%	70.5%	69.3%
Vehicles >95% stoppage time	0	56.7%	55.6%	57.2%
% vehicles unable to enter network	0	44.6%	46.3%	40.3%
# collisions	0	178	149	189

traffic congestion that slowed down vehicles behind the collision, while also reducing the flow of traffic along roads ahead of where the collisions occurred. This would allow vehicles traveling along those road segments to maintain low time loss and stoppage times. All three variations have similar values for all of the indicators and there is not a consistent increase in these as the number of affected RSUs increases. This suggests that for a network of this size, attacking additional RSUs has lesser effects on worsening the safety and performance of the network. However, the combined attack of disabling of brakes and forced sudden braking on any RSU, particularly if it occurs in an urban area, would lead to consequences across the system that are severe and potentially catastrophic.

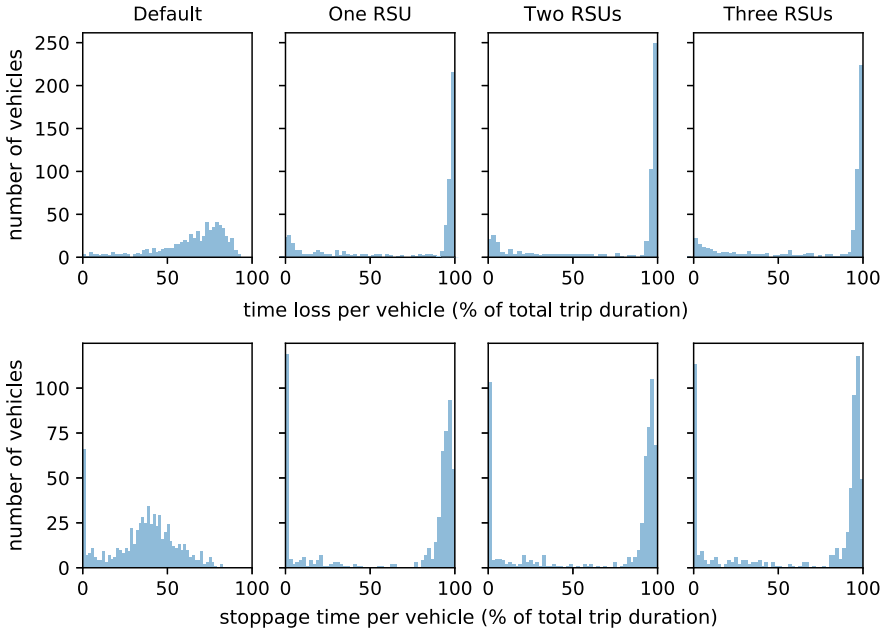

Fig. 13. Distributions of time losses and stoppage times for the disabling of brakes and forced sudden braking scenario with variations in number of RSUs affected.

Table 13. Indicator values for the disabling of brakes and forced sudden braking scenario with variations in number of RSUs affected

Indicator	Default	One RSU	Two RSUs	Three RSUs
Mean time loss	74.9%	96.9%	97.2%	96.8%
Mean stoppage time	38.5%	92.7%	93.5%	93.1%
% vehicles affected	—	59%	62%	62%
Vehicles >80% time loss	35.4%	66.8%	69.3%	65.8%
Vehicles >80% stoppage time	1.2%	66.1%	67.1%	64.2%
Vehicles >95% time loss	0	59.2%	64.5%	59.3%
Vehicles >95% stoppage time	0	34.3%	37.9%	37.7%
% vehicles unable to enter network	0	16.6%	16.3%	11.8%
# collisions	0	398	382	415

Comparison of Risk Scenarios

Looking across the analysis outcomes, the potential consequences for the risk scenarios vary widely. Some attacks cause significant delays (e.g., forced sudden braking), while others cause a large number of collisions (e.g., disabling of brakes), and others have no effect (e.g., disabling of automated emergency braking). Combining multiple risk scenarios amplifies the potential negative impacts. While the disabling of the emergency braking help feature did not have an effect on its own, it led to worse outcomes across nearly all of the indicators when combined with the sudden braking scenario. The combined risk scenario outcomes were also worse than those from the sudden braking scenario alone. These results show the importance of analyzing the impacts of potential risk scenarios individually, as well as in combination to capture potential compounded effects across the network.

Analyzing the results across the variations for each scenario, changing the range of the affected RSU has the largest effect on the results. Increasing the number of RSUs affected in some cases exacerbated the negative effects; however, the degree of impact depended on the particular RSU affected, as seen in the fake environmental hazard warning scenario. While this is difficult to generalize to all possible risk scenarios, using the analysis methodology presented here provides important information for gaining a better understanding of the cyber vulnerabilities at the intersection of the telecommunications and traffic networks. Comparing results across scenarios can facilitate prioritization of mitigation efforts and help to decide, for example, whether it is more pressing to prevent attackers from accessing multiple RSUs at once or to reduce the radius of RSUs.

In comparing results across indicators, while some indicators clearly show impacts that are more severe (e.g., collisions that affect system safety compared to time loss as a measure of system congestion and delays), others are not so straightforward (e.g., comparing the number of vehicles affected and mean time loss). Rather than combining the indicators into a single severity score, this paper provides quantitative assessments of the consequences of potential risk scenarios in finer detail than previously possible and a range of indicators that help users and stakeholders understand the types of impacts for which to prepare.

Conclusion

As 5G technologies develop, it is critical to be able to rigorously understand the risk landscape, particularly for critical infrastructure systems and functions that are and will be dependent on 5G for operations. This paper provides a methodology to provide quantitative assessments of the impacts of 5G risks on dependent connected transportation systems. The impacts of several likely cybersecurity risk scenarios are investigated. The results of the risk scenarios characterize the impacts of these risks on safety and efficiency in a traffic network. The indicators describing the vehicles with time loss and stoppage time above 80% and 95% of their trip times capture the vehicles severely impacted in the scenario. Collisions measure significant safety impacts. These indicators provide valuable information for system operators and managers to direct resources toward appropriate mitigation efforts to minimize the negative impacts of these potential risk scenarios.

The results show that even with a low level of automation and connectivity, the integration of 5G technology into a smart transportation system brings both safety concerns and the potential for significant disruptions and delays to the vehicles traveling through the network. Notably, these negative impacts are not limited to the vehicles being directly affected, nor to only automated vehicles. Unexpected trip delays and collisions occurred throughout the network, the result of cascading effects across the network that impact the entire system performance beyond just the vehicles directly targeted.

Quantifying the impacts of these risk scenarios through the defined indicators (time loss, stoppage time, number of collisions, and vehicles affected) provides a more specific and detailed characterization of the severity of the effects of a cyberattack or malfunction than has been previously studied. This allows for a better understanding of the impacts of risk scenarios, including distinguishing between those that cause safety concerns compared to inconvenient traffic delays, and characterizing the levels of impacts that might be expected from an attack. Looking at effects across the network enable us to understand the systemwide impacts of a given event.

The current approach is most useful for comparing the impacts of the risk scenarios with one another and to better understand how increasing certain parameters (e.g., RSU radius, number of vehicles affected, etc.) exacerbates these negative effects. The model can be easily modified to simulate a network in a different location or for systems with a specific set of connectivity and automation features. This flexibility makes it widely applicable for identifying and analyzing future risk scenarios that are of particular concern before they occur and before the technology is even implemented. Such an understanding will facilitate the development of mitigation strategies to better prepare these critical systems for these scenarios before they occur in a real-world setting.

Future Work

Because 5G and C-V2X technology is still in development, the risk scenarios simulated were based off of risks identified by researchers and attacks seen in similar contexts. However, as specific risks are identified throughout the rollout process, they can also be modeled using the proposed methodology. Once C-V2X communications become more widely implemented and there are more data available from surveys, sensors, and so on, the model can be compared to real-world instances of these risk scenarios and further refined. Multiple trials for each scenario can also be run with different sets of random trips, different affected RSUs, and different levels of traffic to gain a more in-depth understanding of a scenario. Once a particular risk scenario of interest has been identified, a more extensive analysis like this can provide important information such as why some RSUs have greater negative impacts than others when affected. This can help identify system components that may be bigger targets for cyberattacks so that any necessary extra security measures can be put in place. Finally, future work in this area involves adapting the simulation to reflect the continuing advances in

5G and C-V2X technology. As automated driving features are developed, they can be integrated into the simulation. As the 5G infrastructure needed for C-V2X is deployed, this model can be used to include those assets and functionality to simulate expanding scenarios of interest.

Data Availability Statement

All data, models, and code that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments

This material is based upon work funded by the US Department of Homeland Security under Cooperative Agreement No. 2015-ST-061-CIRC01-03.

References

5GAA. 2019. "C-ITS vehicle to infrastructure services: How C-V2X technology completely changes the cost equation for road operators." Accessed August 6, 2021. https://5gaa.org/wp-content/uploads/2019/01/5GAA-BMAC-White-Paper_final2.pdf.

Ahmad, F., and A. Adnane. 2016. "A novel context-based risk assessment approach in vehicular networks." *IEEE Network* 30 (3): 466–474. https://doi.org/10.1109/WAINA.2016.60.

Applegate, C. J., and I. Tien. 2019. "Framework for probabilistic vulnerability analysis of interdependent infrastructure systems." *J. Comput. Civ. Eng.* 33 (1): 04018058. https://doi.org/10.1061/(ASCE)CP.1943-5487.0000801.

Aria, E., J. Olstam, and C. Schwietering. 2016. "Investigation of automated vehicle effects on driver's behavior and traffic performance." *Transp. Res. Procedia* 15 (Jan): 761–770. https://doi.org/10.1016/j.trpro.2016.06.063.

Audi, Ericsoon, Qualcomm, Swarco, and Technische Universitat Kaiserlautern. 2020. "ConVex deliverable D4.1: Roadside ITS station specification." Accessed March 25, 2021. https://convex-project.de/onewebmedia/D4.1_Roadside-ITS-Station-Specification_rev1.pdf.

Batalla, J. M., E. Andrukiewicz, G. P. Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, and M. Imran. 2020. "Security risk assessment for 5G Networks: National perspective." *IEEE Wireless Commun.* 27 (4): 16–22. https://doi.org/10.1109/MWC.001.1900524.

CISA (Cybersecurity and Infrastructure Security Agency). 2020. "CISA 5G strategy: Ensuring the security and resilience of 5G infrastructure in our nation, department of homeland security." Accessed July 7, 2021. https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

Farid, A. M., et al. 2021. "Smart city drivers and challenges in urban-mobility, health-care, and interdependent infrastructure systems." *IEEE Potentials* 40 (1): 11–16. https://doi.org/10.1109/MPOT.2020.3011399.

Ganesan, K., P. B. Mallick, J. Lohr, D. Karampatsis, and A. Kunz. 2019. "5G V2X architecture and radio aspects." In *Proc., 2019 IEEE Conf. on Standards for Communications and Networking (CSCN)*, 1–6. New York: IEEE.

GSMA (Groupe Speciale Mobile Association). 2019. "Connecting vehicles today and in the 5G era with C-V2X." Accessed April 25, 2021. https://www.gsma.com/iot/wp-content/uploads/2019/08/Connecting-Vehicles-Today-and-in-the-5G-Era-with-C-V2X.pdf.

Guidotti, R., and P. Gardoni. 2018. "Modeling of interdependent critical infrastructure for regional risk and resilience analysis." In *Routledge handbook of sustainable and resilient infrastructure*, 507–528. London: Routledge.

Jahromi, B. 2019. "Ultrasonic sensors in self-driving cars." Accessed April 25, 2021. https://medium.com/@BabakShah/ultrasonic-sensors-in-self-driving-cars-d28b63be676f.

Kaas, H., et al. 2016. "Automotive revolution—Perspective towards 2030." https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/disruptive-trends-that-will-transform-the-auto-industry/de-DE.

Lopez, P. A., M. Behrisch, L. Bieker-Walz, J. Erdmann, Y. Flotterod, R. Hilbrich, L. Lucken, J. Rummel, P. Wagner, and E. Wiessner. 2018. "Microscopic Traffic Simulation using SUMO." In *Proc., 2018 21st Int. Conf. on Intelligent Transportation Systems (ITSC)*, 2575–2582. New York: IEEE.

Mavromatis, I., A. Tassi, R. J. Piechocki, and A. Nix. 2019. "Efficient millimeter-wave infrastructure placement for city-scale ITS." In *Proc., IEEE Conf. on Vehicular Technology (VTC)*. New York: IEEE.

Milanes, V., E. Onieva, J. Perez, J. Simo, C. Gonzalez, and T. de Pedro. 2011. "Making transport safer: V2V-based automated emergency braking system." *Transport* 26 (3): 290–302. https://doi.org/10.3846/16484142.2011.622359.

O'Donnell, B. 2019. "How fast will 5G really be?" Accessed November 19, 2019. https://www.forbes.com/sites/bobodonnell/2019/11/19/how-fast-will-5g-really-be.

OpenStreetMap contributors. 2015. "Planet dump." Accessed November 7, 2020. https://planet.openstreetmap.org.

Schrab, K., and R. Protzmann. 2021. "MOSAIC." Accessed March 25, 2021. https://github.com/eclipse/mosaic.

Shi, Y., L. Lv, H. Yu, L. Yu, and Z. Zhang. 2020. "A center-rule-based neighborhood search algorithm for roadside units deployment in emergency scenarios." *Mathematics* 8 (10): 1734. https://doi.org/10.3390/math8101734.

Wang, J., Y. Shao, Y. Ge, and R. Yu. 2019. "A survey of vehicle to everything (V2X) testing." *Sensors* 19 (2): 334. https://doi.org/10.3390/s.19020334.

Xiang, Y., T. Su, C. Brach, X. Liu, and M. Geimer. 2020. "Realtime estimation of IEEE 802.11p for mobile working machines communication respecting delay and packet loss." In *Proc., 2020 IEEE Intelligent Vehicles Symp. (IV)*, 1516–1521. New York: IEEE. https://doi.org/10.1109/IV47402.2020.9304651.

Yue, B., S. Shi, S. Wang, and L. Nan. 2020. "Low-cost urban test scenario generation using microscopic traffic simulation." *IEEE Access* 8 (Jun): 99. https://doi.org/10.1109/ACCESS.2020.3006073.