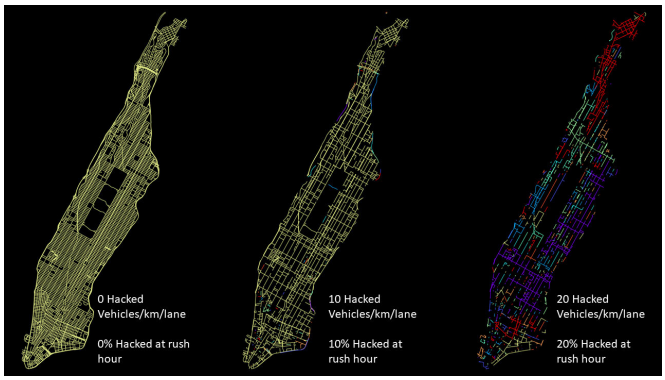
The first look at how hacked self-driving cars would affect New York City traffic

4 March 2019



Clusters of connected roads. Same color denotes roads that are part of the same cluster, i.e., all connected. When there are no hacked vehicles, all roads are connected (yellow). But as there are more hacked vehicles, more colors show up, and each cluster is inaccessible from the other. When somewhere between 10-20% of vehicles at rush hour hacked, the size of the largest cluster dramatically reduces. We call this threshold (~10-15 hacked vehicles/km/lane) the point of city fragmentation. Essentially half the city is inaccessible from the rest above this threshold. Credit: Skanda Vivek/ Georgia Tech

As automated cars become more commonplace, it is increasingly likely that internet-connected vehicles could be simultaneously disabled. Currently, regulators tend to focus on preventing individual incidents, like the pedestrian who was struck and killed by a self-driving Uber in Arizona last year. However, they fall short of addressing the effects of a large-scale hack in an urban setting.

This week at the 2019 American Physical Society March Meeting in Boston, Skanda Vivek will present his research on the cyber-physical risks of hacked internet-connected vehicles. He will also participate in a press conference describing the work. Information for logging on to watch and ask questions remotely is included at the end of this news release.

Vivek and his team found that even a small-scale hack, affecting only 10 percent of vehicles in Manhattan, could cause citywide gridlock and hinder emergency services. Based on these findings the team also developed a risk-mitigation strategy to prevent mass urban disruption from a few compromised vehicles.

Vivek, a postdoctoral researcher in the Peter Yunker lab at the Georgia Institute of Technology, used agent-based simulations to investigate how hacks could impact traffic flow in New York. He and his team, including Yunker, graduate student David Yanni and Jesse Silverberg, founder of Multiscale Systems Inc., ultimately discovered that by using percolation theory, a mathematical approach based on the statistical analysis of networks, they could quantify how these scenarios would play out in New York City in real time.

Moreover, their analysis helped the team develop a risk-mitigation strategy: using multiple networks for connected vehicles to decrease the number of cars that could be compromised in a single intrusion. "If no more than, say, 5 percent of connected vehicles were compartmentalized to the same network or utilized the same network protocols, the chance of citywide fragmentation would be low," Vivek said. "Therefore, a hacker with the intention of causing large-scale disruption faced with this compartmentalized multi-network architecture would be required to execute multiple simultaneous intrusions, which increases the difficulty of such an attack and makes it less likely to occur."

Stressing the urgency of this issue, Vivek commented that "compromised vehicles are unlike compromised data. Collisions caused by compromised vehicles present physical danger to the vehicle's occupants, and these disturbances would potentially have broad implications for overall traffic flow." Although there's been public scrutiny

on individual collisions, this work is needed because the "likely impacts of a large-scale hack on traffic flow have yet to be quantified," Vivek said.

Speaking to the inevitability of more autonomous systems on the road, "Connected cars are the future," Vivek said. "They hold tremendous potential for positive impact economically, environmentally, and, for former drivers no longer frustrated by congested commutes, psychologically. Our work is not in opposition to the future of connected cars. Rather, the novelty of our work lies in identifying and quantifying the underlying cyber-physical risks when multiple connected vehicles are compromised. By shining a light on these technologies at an early stage, we hope we can help prevent worst-case-scenarios."

More information: The 2019 APS March Meeting presentation "Cyber-physical risks of hacked Internet-connected vehicles," by Skanda Vivek, David B. Yanni, Peter Yunker and Jesse L Silverberg, will take place Monday, March 4, at 12:51 p.m. in room 108 of the Boston Convention and Exhibition Center. Abstract: meetings.aps.org/Meeting/MAR19/Session/B05.9

Provided by American Physical Society