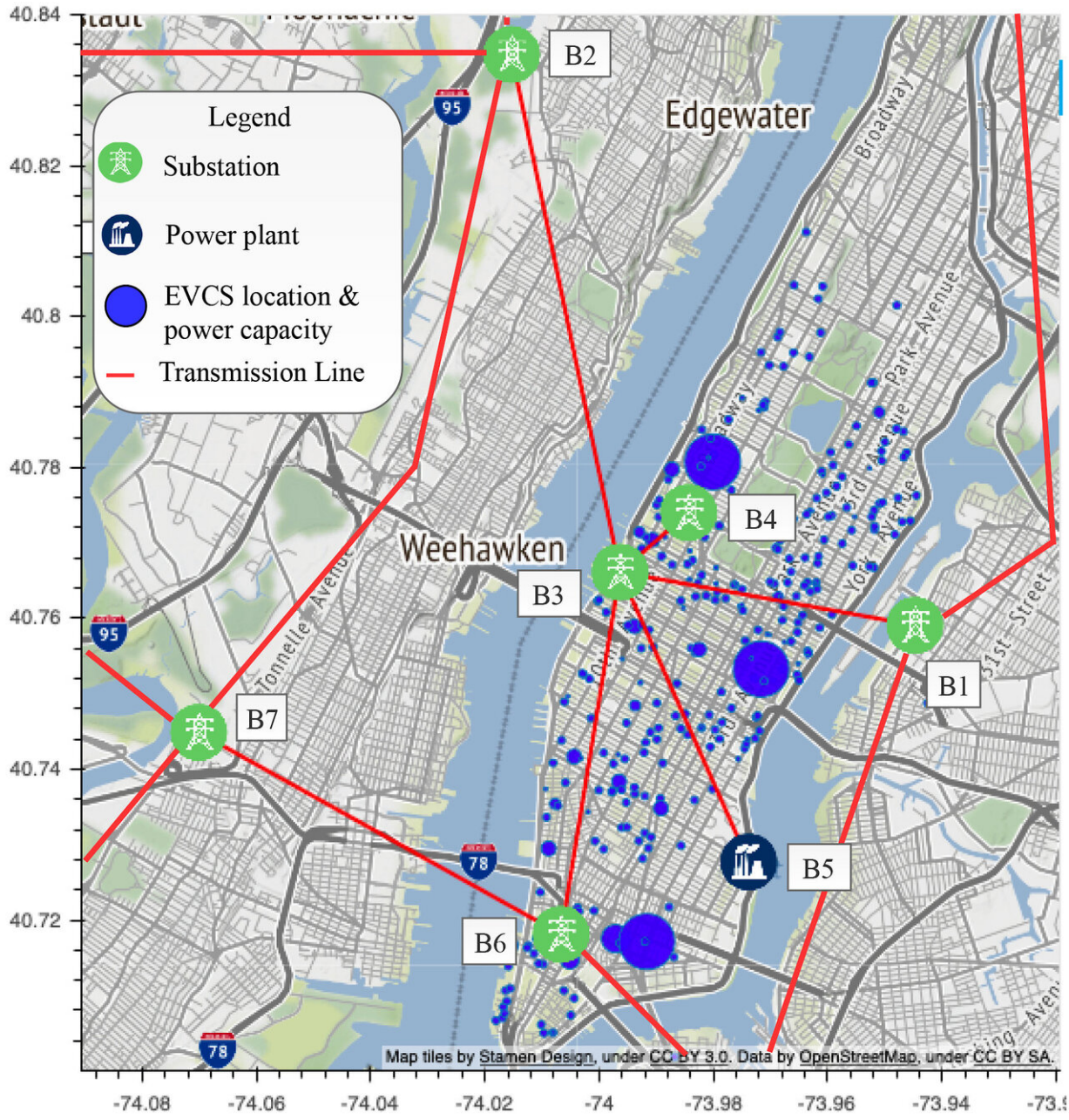
Electric car charging stations may be portals for power grid cyberattacks

August 15 2019



The map displays substations connected by transmissions lines along with electric vehicle charging stations. The size of the blue circles is proportional to the charging station demand. Such information can be used by hackers to disrupt either charging of electric vehicles or the power grid itself. Credit: NYU Tandon School of Engineering

Electric cars are an essential component of a lower-carbon future, but a new report from researchers at the New York University Tandon School of Engineering raises the specter that plug-in electric vehicles—and the charging stations that supply them—could be prime vectors for cyberattacks on urban power grids.

"In simulations using publicly available information about charging station usage in Manhattan and the structure of the island's power grid, our research team found that a fleet of just roughly 1,000 simultaneously charging electric vehicles would be adequate for mounting an attack whose effects could rival the blackout that affected the city's West Side last month," said Yury Dvorkin, assistant professor in NYU Tandon's Department of Electrical and Computer Engineering.

NYU Tandon doctoral candidate Samrat Acharya led the research in collaboration with Dvorkin and Professor Ramesh Karri, also from the Department of Electrical and Computer Engineering.

"This simulation is a wake-up call to the public and policymakers, and an encouragement to take steps to protect the data generated between electric cars and charging stations—most of which could be co-opted by a hacker with college-level skills," Dvorkin said.

Electric vehicle charging stations represent a link between plug-in electric vehicles and the power grid—a high-wattage access point that hackers can potentially exploit to manipulate the grid. Each vehicle that uses a public charging station generates data on its location and charging time, along with information on the average hourly power draw at each station. Information on power usage is critical for a malicious actor who wishes to manipulate demand at a particular charging station. This information is easily accessible, as it is transmitted wirelessly by third-party apps that cater to electric vehicle owners.

Information about the structure of the power grid is more fragmented and difficult to access; however, the research team demonstrated that a combination of public documents and resources available through industry standards-setting organizations and from utilities' public releases may be tapped to construct power grid topology and model the system components.

Together, these elements allow an attacker to use charging stations as portals to remotely manipulate electric vehicle charging and the power grid by causing instabilities that could range from barely noticeable to significantly disruptive.

Power grid attacks are not just the stuff of paranoid nightmares. In 2015, a sophisticated cyberattack crippled a power grid in Ukraine, and this year, a small-scale attack in the western United States became the first reported successful incursion on a domestic power grid. The NYU Tandon researchers emphasized that while the number of electric cars on the road today—about 1 million—is not concentrated in one place and is therefore insufficient to produce the impact reported in their simulations, the threat potential will unquestionably rise as the electric fleet grows. The Edison Electric Institute estimates about 9.6 million charging ports will support a remarkable 18.7 million plug-in electric vehicles by 2030—a disputed number, although all forecasters predict

remarkable increases. New York County—which includes Manhattan—has just over 2,500 electric vehicles registered.

At present, there is no consensus on a cybersecurity protocol to protect data generated by electric vehicle charging. The cybersecurity community has urged vehicle and power station component manufacturers, utility companies, third-party service providers (including app developers), and federal authorities to collaborate on a unified set of cybersecurity protocols and to issue guidelines to encourage electric vehicle owners to maintain strong passwords and change them regularly.

More information: Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? arxiv.org/pdf/1907.08283.pdf

Provided by NYU Tandon School of Engineering