Connected cars can lie, posing a new threat to smart cities

June 7 2018, by Qi Alfred Chen And Z. Morley Mao

What algorithm turned these lights red? Credit: monticello/Shutterstock.com

The day when cars can talk to each other – and to traffic lights, stop signs, guardrails and even pavement markings – is rapidly approaching. Driven by the promise of reducing traffic congestion and avoiding

crashes, these systems are already rolling out on roads around the U.S.

For instance, the Intelligent Traffic Signal System, developed with support from the U.S. Department of Transportation, has been tested on public roads in Arizona and California and is being installed more widely in New York City and Tampa, Florida. It allows vehicles to share their real-time location and speed with traffic lights, which can be used to effectively optimize the traffic timing in coordination with the real-time traffic demand to dramatically reduce vehicle waiting time in an intersection.

Our work, from the RobustNet Research Group and the Michigan Traffic Laboratory at the University of Michigan, focuses on making sure these next-generation transportation systems are secure and protected from attacks. So far we've found they are in fact relatively easy to trick. Just one car that's transmitting fake data can cause enormous traffic jams, and several attack cars could work together to shut down whole areas. What's particularly concerning is that our research has found the weakness is not in the underlying communication technology, but in the algorithms actually used to manage the traffic flow.

Misleading an algorithm

In general, algorithms are meant to take in a variety of inputs – such as how many cars are in various locations around an intersection – and calculate an output that meets a particular goal – such as minimizing their collective delay at traffic lights. Like most algorithms, the traffic control algorithm in Intelligent Traffic Signal System – nicknamed "I-SIG" – assumes the inputs it's getting are honest. That's not a safe assumption.

The hardware and software in modern cars can be modified, either

physically through the car's diagnostic ports or over wireless connections , to instruct a car to transmit false information. Someone who wanted to compromise the I-SIG system could hack her own car using such methods, drive to a target intersection and park nearby.

Once parked near the intersection, we've found that the attacker could take advantage of two weaknesses in the algorithm controlling the light to extend the time a particular lane of traffic gets a green light – and, similarly, the time other lanes get red lights.

The first vulnerability we found, which we call "last vehicle advantage," is a way of extending the length of a green-light signal. The algorithm keeps an eye on approaching cars, estimates how long the line of cars is and determines how long it thinks it will take for all the vehicles in a line of traffic to get through the intersection. This logic helps the system serve as many vehicles as possible in each round of light changes, but it can be abused. An attacker can instruct her car to falsely report joining the line of cars very late. The algorithm will then hold the attacked light green long enough for this nonexistent car to pass, leading to a green light – and correspondingly, red lights for other lanes – that is much longer than needed for the actual cars on the road.

We called the second weakness we found the "curse of the transition period," or the "ghost vehicle attack." The I-SIG algorithm is built to accommodate the fact that not all vehicles can communicate yet. It uses the driving patterns and information of newer, connected cars to infer the real-time location and speed of older, noncommunicating vehicles. Therefore, if a connected car reports that it is stopped a long distance back from an intersection, the algorithm will assume there is a long line of older vehicles queuing ahead of it. Then the system would allocate a long green light for that lane because of the long queue it thinks is there, but really isn't.

These attacks happen by making a device lie about its own position and speed. That's very different from known cyberattack methods, like injecting messages into unencrypted communications or having an unauthorized user logging in with a privileged account. Therefore, known protections against those attacks can do nothing about a lying device.

Results from a misinformed algorithm

Using either of these attacks, or both in concert with each other, can allow an attacker to give long periods of green lights to lanes with little or no traffic and longer red lights to the busiest lanes. That causes backups that grow and grow, ultimately building into massive traffic jams.

This sort of attack on traffic lights could be just for fun or for the attacker's own benefit. Imagine, for example, a person who wants to have a faster commute adjusting his own traffic-light timing, at the expense of other drivers' delays. Criminals, too, might seek to attack traffic lights to ease their getaways from crime scenes or pursuing police cars.

There are even political or financial dangers: A coordinated group could shut down several key intersections in a city and demand a ransom payment. It's much more disruptive, and easier to get away with, than other ways of blocking intersections, like parking a car across traffic.

Because this type of attack exploits the smart traffic control algorithm itself, fixing it requires joint efforts from both transportation and cybersecurity fields. This includes taking into account one of the broadest lessons of our work: The sensors underlying interactive systems – such as the vehicles in the I-SIG system – aren't inherently trustworthy. Before engaging in calculations, algorithms should attempt to validate

the data they're using. For example, a traffic-control system could use other sensors – like in-road sensors already in use across the nation – to double-check how many cars are really there.

This is just the beginning of our research into new types of security problems in the smart transportation systems of the future, which we hope will both discover weaknesses and identify ways to protect the roads and the drivers on them.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation