Exposing Falsified Data Attacks on CV-based Traffic Signal Control

Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z. Morley Mao, Henry X. Liu
University of Michigan
{*alfchen, yyucheng, yhfeng, zmao, henryliu*}@*umich.edu*

1 Introduction

With the recent development of connected vehicle (CV) technology across the world, vehicles and infrastructure will be connected through wireless communications. In the U.S., the Department of Transportation (DoT) has already proposed to mandate new vehicles to equip CV technology, and launched pilot programs to develop and test CV applications on real roads [1]. While having demonstrated the potential to greatly improve safety, mobility, and sustainability, such dramatically increased connectivity also opens a new door for cyber attacks. To ensure the security of vehicles and transportation infrastructure and, more seriously, the safety of drivers and pedestrians, it is highly important to understand the potential security challenges so that they can be proactively addressed before the actual deployment.

In this work, we perform the first security analysis of transportation infrastructure systems in a CV environment. As a first step, we target the DoT sponsored design and implementation of a CV application called Intelligent Traffic Signal System (I-SIG), which is responsible for one of the most basic transportation function, traffic signal control. Targeting a realistic threat, falsified data, we first analyze the attack surface of the I-SIG system and then perform security analysis with various attack goals. To understand the practical implications, the identified attacks are implemented and evaluated in realistic traffic settings. At last, we will propose a set of remediation strategies and secure design principles. In our preliminary results, we find an attack specific to the transition period of CV technology, in which I-SIG can be significantly affected, causing severe traffic jam.

2 Analysis Methodology

Threat model. This work assumes that the attackers are malicious vehicles sending messages with falsified data to the infrastructure-side CV applications. This is realistic since (1) vehicle owners can be malicious and deliberately control the CV equipment to send falsified data, and (2) even if the owner is legitimate, the CV equipment can be compromised, e.g., physically or wirelessly [2].

Attack goals. We target three attack goals: (1) *traffic congestion*: increase the total travel time of other vehicles, causing traffic congestion or even denial of service, (2) *personal gain*: decrease the travel time for the attacker's vehicle, at the cost of other vehicles' travel time, and (3) *safety attack*: increase the safety risk of other vehicles, e.g., by putting vehicle(s) into dilemma zone [3].

Analysis methodology. We first perform vulnerability analysis of the I-SIG system under the threat model by analyzing the potential impact of falsified messages. We then analyze whether these identified vulnerabilities can be practically exploited to achieve the three attack goals. For each attack goal, we exhaustively try all possible attack methods on the identified vulnerabilities and use synthetic traffic traces to quantify the attack results. For the highly effective attacks, we perform cause analysis and design targeted exploitation strategies. At last, the identified exploitation strategies are evaluated on a real-world map with synthetic and real-world traffic traces.

3 Initial Results

The I-SIG system has two operation modes depending on penetration rate (PR) of CV technology. When PR is high, it directly runs signal planning using an optimal algorithm. When PR is low, i.e., in the transition period of CV technology, the algorithm can be ineffective and EVLS (Estimation of unequipped Vehicle Location and Speed) is used to first infer the locations of unequipped vehicles and then run the planning algorithm.

The curse of the transition period. We find that EVLS can be significantly affected by falsified data. EVLS uses the data of the last stopped equipped vehicle to estimate the queue length. Thus, one single attack vehicle can report a falsified location data of the total lane length to cause EVLS to add a queue with tens of vehicles. We find that this attack can increase the total delay time by 20-50%, and sometimes even over 70%, causing severe traffic jam. Note that using I-SIG can decrease the total delay by up to 20%, but this attack can cause the traffic mobility becoming even worse than that without using I-SIG. This attack exploits the weakness in EVLS and thus only works for the transition period. This is a fundamental problem for the transition period: since low PR inevitably decreases the effectiveness of any CV-based planning algorithm, certain forms of inference are needed. However, if such inference is not robust, it can be manipulated to greatly affect the signal planning.

References

[1] "U.S. DoT Connected Vehicle Pilot Deployment Program," https://www.its.dot.gov/pilots/.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security*, 2011.

[3] Y. Zhang, C. Fu, and L. Hu, "Yellow Light Dilemma Zone Researches: A Review," in *Journal of traffic and transportation engineering*, 2014.