Impact Evaluation of Falsified Data Attacks on Connected Vehicle Based Traffic Signal Control Systems

Shihong Ed Huang
University of Michigan, Ann Arbor
edhuang@umich.edu

Yiheng Feng
Purdue University, West Lafayette
feng333@purdue.edu

Wai Wong
University of Michigan, Ann Arbor
waiwong1012@connect.hku.hk

Qi Alfred Chen
University of California, Irvine
alfchen@uci.edu

Z. Morley Mao
University of Michigan, Ann Arbor
zmao@umich.edu

Henry X. Liu
University of Michigan, Ann Arbor
henryliu@umich.edu

***Abstract*—Connected vehicle (CV) technologies enable data exchange between vehicles and transportation infrastructure. In a CV environment, traffic signal control systems receive CV trajectory data through vehicle-to-infrastructure (V2I) communications to make control decisions. Comparing with existing data collection methods (e.g., from loop-detectors), the CV trajectory data provide much richer information, and therefore have great potentials to improve the system performance by reducing total vehicle delay at signalized intersections. However, this connectivity might also bring cyber security concerns.**

In this paper, we aim to investigate the security problem of CV-based traffic signal control (CV-TSC) systems. Specifically, we focus on evaluating the impact of falsified data attacks on the system performance. A black-box attack scenario, in which the control logic of a CV-TSC system is unavailable to attackers, is considered. A two-step attack model is constructed. In the first step, the attacker tries to learn the control logic using a surrogate model. Based on the surrogate model, in the second step, the attacker launches falsified data attacks to influence the control systems to make sub-optimal control decisions. In the case study, we apply the attack model to an existing CV-TSC system (i.e., I-SIG) and find intersection delay can be significantly increased. Finally, we discuss some promising defense directions.

I. Introduction

Advanced communication technologies such as Dedicated Short Range Communication (DSRC) and cellular LTE/5G enable vehicles and transportation infrastructure to communicate with each other in real-time. Vehicles that have communication capabilities are referred as connected vehicles (CVs). The communication mechanism greatly enhances information exchange between CVs and transportation infrastructure and therefore has great potential to improve various mobility applications, including traffic signal control (TSC), a critical component in urban traffic operation. Different from conventional traffic control systems that depends on infrastructure-based sensor data, a CV-based traffic control system (CV-TSC) utilizes CV trajectory data as input to make control decisions. A typical CV-TSC system is illustrated in Figure 1. Each CV is equipped with an On-Board Unit (OBU), which broadcasts Basic Safety Messages (BSMs). A BSM records a CV's information including its location, speed, heading, and acceleration. Consecutive BSMs represent the vehicle trajectory. On the infrastructure side, an intersection is equipped with a Roadside Unit (RSU), a signal controller, and traffic signals. The RSU receives BSMs (i.e., CV trajectories), which are used to optimize traffic signal timing plans. The signal controller executes the optimal signal timing plans and controls traffic signals to display corresponding colors. The signal controller is usually connected to a transportation management center (TMC), which sends commands remotely to the signal controller (e.g., time-of-day signal timing plans). Meanwhile, the RSU continuously broadcasts Signal Phase and Timing (SPaT) messages, which record current signal status (i.e., green/yellow/red) and remaining time. Based on continuously received BSMs, the CV-TSC system responds to real-time traffic demands by updating the signal timing plans dynamically. Over the past decade, various CV-TSC models have been proposed and significant mobility

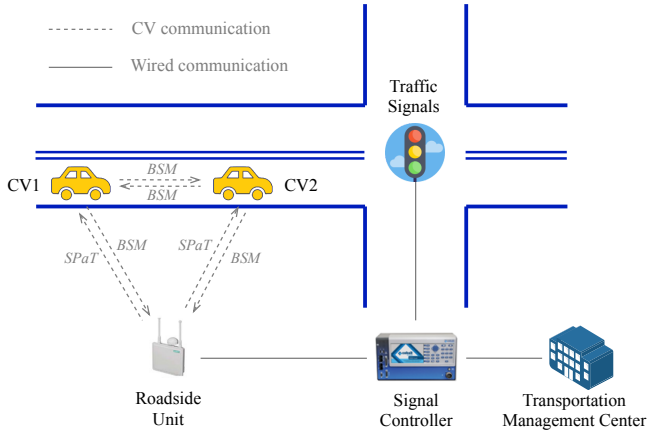

Fig. 1. Illustration of a connected vehicle based traffic signal control system

Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021
25 February 2021, Virtual
ISBN 1-891562-68-1
https://dx.doi.org/10.14722/autosec.2021.23005
www.ndss-symposium.org

improvements are observed [10]. Because of this benefit, it is envisioned that CV-TSC systems may gradually replace the conventional TSC systems in the future [23].

Despite great improvements in system performance, the new trait, connectivity between vehicles and infrastructure, might open a new door to cyber attacks. The benefit of CV-TSC systems can be achieved only if the systems are secure in cyberspace. Therefore, cyber security is a crucial component when developing CV-TSC systems. However, most of the existing CV-TSC models are designed without considering cyber security issues and thus may be vulnerable to cyber attacks. Before developing defense strategies, it is important to identify potential cyber threats and investigate the impact of cyber attacks. Existing studies on this topic usually consider a "white-box" attack scenario, which assumes that attackers have full access to the traffic control system and/or control logic so that they can manipulate the traffic signal phasing and timing freely [4], [7]–[9], [15], [19], [24]. For example, Perrine et al. [19] assumes that the traffic signals can be selectively disabled to flashing-red status (equivalent to a four-way stop-sign intersection) without explaining how the attack is conducted. Chen et al. [4] assumes that the source code of the signal control model is known to the attacker so a comprehensive analysis can be performed. "Manipulating signal phasing and timing freely" is a very strong and unrealistic assumption. For most of the commercial traffic control systems, various levels of protection from hardware (e.g., Malfunction Monitoring Unit) to software (e.g., controller firmware) are designed to prevent such manipulations, no mentioning access to the source code. Thus, it is necessary to build an attack model and evaluate the impact of cyber attacks under real-world scenarios where the controller hardware and control logic are inaccessible.

In this paper, we aim to evaluate the impact of falsified data attacks on CV-TSC systems by considering a "black-box" attack scenario, in which the attackers do not know the details of the signal control system and do not have physical access to the system (e.g., signal cabinet). Attackers first need to learn the signal control logic using a surrogate model that includes critical traffic features. With the learned model, the optimal signal timing plan generated from the control system can be predicted by the attackers using received CV trajectories. Then the attackers alter the critical traffic features and subsequently the signal timing plan by injecting falsified CV data into the system. The impact of attacks is measured by comparing the total vehicle delay before and after attack. In the case study, we apply the proposed attack model on I-SIG, an existing CV-TSC system. Results show that falsified data attacks can create excessive delay at the intersection and degrade the performance of the CV-TSC system. We also briefly discuss two defense strategies as future research directions.

The remainder of this paper is organized as follows. Background knowledge on traffic signal control is introduced in Section II. Section III presents the attack model, including how attackers may learn the signal control logic and how attackers may generate falsified data to launch attacks. Section IV presents a comprehensive case study, which realistically evaluates the impact of falsified data attacks on I-SIG. In Section V, we discuss two defense strategies. Related studies regarding cyber attacks on CV-TSC systems are introduced in Section VI. Finally, conclusions are drawn in Section VII.

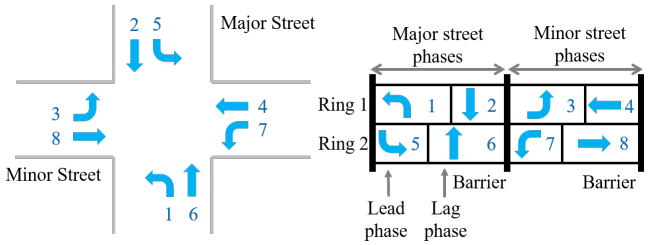

Fig. 2. Ring-barrier structure

II. Background

A. Traffic Signal Control

This study assumes that the CV-TSC system uses a ring-barrier phasing. The ring-barrier structure [13] illustrated in Figure 2 is the standard traffic signal phasing setting in North America. Starting from the major street and moving clockwise, the through phases are labeled as phases 2, 4, 6, and 8. Starting from the left-turn phase that is next to phase 6 and moving clockwise, the left-turn phases are labeled as phases 1, 3, 5, and 7. Ring 1 includes phases 1 to 4 and ring 2 includes phases 5 to 8. A barrier separates major street phases (phases 1, 2, 5, and 6) from minor street phases (phases 3, 4, 7, and 8). The phases that operate first within a barrier in each ring are called lead phase (e.g., phases 1 and 5) and the other phase (e.g., phases 2 and 6) is called lag phase. Therefore a barrier includes two lead phases and two lag phases. A signal optimization algorithm changes phase sequence and allocates green time of each phase to minimize/maximize predefined performance indexes, based on collected traffic data (e.g., CV trajectories).

B. I-SIG

In this study, I-SIG system from the Multi-Modal Intelligent Traffic Signal System (MMITSS) project is selected as the targeted CV-TSC system [23] for case study. Both simulation and field experiments have demonstrated the effectiveness of I-SIG in terms of delay reduction and mobility improvement [6]. The reason for choosing I-SIG is that it is one of the most cited work related to CV-TSC and the proposed framework has been adopted by many other studies. The control logic of I-SIG system is briefly introduced. At the beginning of each barrier, I-SIG takes a snapshot of the trajectories received from all the CVs within the RSU's communication range. Each trajectory is converted to an ETA (estimated time of arrival), which is calculated as the CV's distance to stop bar divided by its speed. Based on the ETAs of each signal phase, an arrival table is constructed. Then I-SIG solves an dynamic programming (DP) based optimization problem with the objective to minimize total vehicle delay or total queue length. Each barrier is considered as one stage in the DP formulation. Ideally, I-SIG should plan as many stages as needed so that all the vehicles can be properly served. For real-world implementations, however, I-SIG plans only two stages (i.e., one signal cycle) because of computational limitations in the edge computing device and real-time performance requirement. I-SIG then executes the timing plan of the first stage (the four phases in the current barrier) and arranges the phase sequence of the second stage (the four phases in the

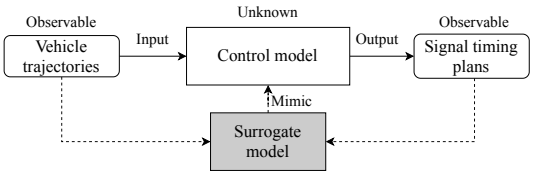

Fig. 3. The process of learning control logic

next barrier). When a new barrier starts, I-SIG repeats this optimization process. For more details, please refer to [6].

III. Attack Model

The proposed attack model includes two steps. In the first step, the attacker tries to learn the control logic using a surrogate model. Based on the surrogate model, in the second step, the attacker launches falsified data attacks to influence the control system to make sub-optimal decisions.

A. Learning Control Logic

In a real-world implementation, a CV-TSC system utilizes vehicle trajectories (i.e., BSMs) as the input and generates optimal signal timing plans. Both vehicle trajectories and signal timing plans are observable to the attacker in the forms of BSMs and SPaT messages respectively, because all messages are transmitted in a broadcast mode. The actual signal control logic, however, is unknown to the attacker. In order to launch effective attacks, the attacker needs to learn the control logic first using a surrogate model. The surrogate model takes the same trajectories as the input and outputs predicted signal timing plans. Historical BSM and SPaT data can be used to train the surrogate model. The attacker uses the surrogate model as the replacement of the real control logic when launching attacks. The whole learning process is illustrated in Figure 3.

1) Surrogate Model: A signal timing plan includes two parts, green time of each phase and phase sequence. The prediction of green time can be considered as a regression problem because green time is continuous. In contrast, the prediction of phase sequence is a classification problem since there is a finite number of possibilities for phase sequences. In this study, decision tree regression/classification [2] is adopted to be the surrogate model. Decision tree models are chosen because they are easy to implement and their output always falls within the feasible ranges, i.e., minimum and maximum green time. Most importantly, decision tree models possess inherent "if-then-else" structures and can effectively map nonlinear relationships, making signal control algorithms particularly easy to fit into programmatic structures. The input features to the surrogate model are critical traffic features extracted from observed CV trajectories.

2) Critical Traffic Features: Different CV-TSC systems use different objectives and performance indexes to optimize the signal timing plan. Since the objectives are typically functions of one or more traffic features, the signal timing plan should be closely related to these associated traffic features. For example, a signal controller may allocate green time based on the queue length of each phase, or a signal controller may terminate a green phase when there is a large headway. A list of common traffic features applied in existing studies include queue length (QL), number of approaching vehicles (NAV), headway (HW), estimated time of arrival (ETA), vehicle delay (VD), and flow rate (FR). These traffic features will be used in the case study in Section IV.

For a particular CV-TSC system, usually not all traffic features are utilized to optimize the signal timing. We define the traffic features that determine the signal timing plan as critical features. When falsified data alter the values of these critical features, signal control decisions are changed accordingly. As a result, the attacker needs to identify the critical features that have a significant impact on the signal timing plan before launching attacks. Identifying critical features from the list of features is a feature selection problem. In this study, a sequential forward selection algorithm (SFS) is applied [1]. Starting from an empty feature set, SFS greedily searches for the best features that can improve the prediction performance. John et al. [12] suggests using SFS for identifying useful features and shows that SFS can improve the performance of decision tree models. The output of SFS is a set of critical features. Note that in Section III-A1, only critical features are used as the input features of the decision tree models.

B. Falsified Data Generation

In the previous section, the attacker has obtained the surrogate model $\boldsymbol{f}(\cdot)$ by training the decision tree models. Then the attacker launches attacks by broadcasting falsified trajectories using the compromised communication device (i.e., OBU). Based on received real CV trajectories, the attacker can compute critical traffic features $\boldsymbol{X_o}$ (e.g., queue length) identified in the previous step, and use the trained surrogate model to predict the signal timing plan, i.e., $\boldsymbol{f}(\boldsymbol{X_o})$. $\boldsymbol{f}(\boldsymbol{X_o})$ is referred to as the pseudo-optimal timing plan because it is not the exact timing plan generated from the actual control system, but a plan predicted by the trained surrogate model. By injecting falsified trajectories, the attacker tries to alter the values of the critical features from $\boldsymbol{X_o}$ to $\boldsymbol{X_a}$. Similarly, the attacker can predict the signal timing plan with the altered critical feature, i.e., $\boldsymbol{f}(\boldsymbol{X_a})$. The dissimilarity between the pseudo-optimal timing plan and the timing plan under attack are computed using the L2 norm. The attacker's objective is to maximize the dissimilarity by generating falsified trajectories that can alter the values of the critical features, as shown in the following problem (**P1**):

$$\max_{\boldsymbol{X_a}} \quad \|\boldsymbol{f}(\boldsymbol{X_o}) - \boldsymbol{f}(\boldsymbol{X_a})\|_2 \tag{1}$$

$$\text{s.t.} \quad \boldsymbol{X_a} \in \Omega_{\boldsymbol{X_a}|\boldsymbol{X_o}} \tag{2}$$

In **P1**, the feasible region $\Omega_{\boldsymbol{X_a}|\boldsymbol{X_o}}$ is dependent on $\boldsymbol{X_o}$. For example, after injecting a falsified stopped vehicle (a falsified vehicle has a legitimate trajectory in the form of BSMs but is not physically on road), the new queue length cannot be smaller than the originally observed queue length.

When broadcast by the attacker's OBU, the falsified trajectory is mixed with regular CV trajectories. The RSU collects all the trajectories and uses them as input data for traffic signal optimization. Thus, the generated signal timing plans are influenced by the falsified trajectory, and thus are no longer optimal. As a result, vehicles may spend extra time passing the intersection and hence the total travel time is increased.

This attack model aligns with a recent study on black-box attacks against unknown machine learning models [18]. By using a surrogate model, the attacker crafts adversarial images to fool a target model so that the target model would output erroneous predictions.

IV. Attack Evaluation

In this section, a case study is presented to evaluate the impact of the proposed attack model on the I-SIG system.

A. Simulation Setup

A simulation environment is built using Matlab. A typical 4-leg intersection with eight phases is modeled. Each approach has one left-turn lane and one through lane. Right-turn lanes are not explicitly modeled since their phase allocations are usually the same as adjacent through lanes. The car-following model from the NGSIM project is used to model vehicle motions [25]. The minimum green time and the maximum green time are set to be 5 seconds and 30 seconds for each phase, respectively. The transition time between phases (i.e., yellow and red clearance time) is 4 seconds. The traffic demand for each movement is 400 veh/h. The communication range is set to be 300 meters. The free flow speed is 15.65 m/s. The resolution of the simulation is 10 Hz, which is consistent with the frequency of CV communication [21]. Attacks are launched every time I-SIG optimizes the signal timing plan.

B. Applying the Proposed Attack Model

1) Learning Control Logic: Because I-SIG executes optimized signal timing for one barrier each time, the surrogate model only needs to predict the green time of the four phases in the current barrier. The surrogate model consists of two decision tree regression models. The output of the first decision tree model (labeled as Tree 1) is the barrier length (i.e., lead phase plus lag phase). The second decision tree model (labeled as Tree 2) outputs the green time of the lead phase. Then the green time of the lag phase can be calculated by subtracting that of the corresponding lead phase from the barrier.

A 30-hour simulation is run to generate a data set needed for both training and validation. Totally, 2206 optimizations are conducted. 80% of the data are randomly chosen for training, while the remaining 20% are used for validation. Mean absolute error (MAE), mean absolute percentage error (MAPE), and root mean square error (RMSE) are utilized to quantify errors for a given set of traffic features. The errors are defined as the differences between predicted phase (barrier) duration and the phase (barrier) duration generated by original I-SIG. The SFS is applied to the list of common features and the results are shown in Table I. In the first round, only one feature is used for fitting the decision tree models. The model with NAV has the least error for both trees. Therefore, NAV is added to the critical feature set. In the second round, two features are used for fitting the decision tree models, with one feature fixed to be NAV. The model with NAV and ETA has the least error. Thus, ETA is chosen as the second feature and added to the critical feature set. This process is repeated to find the third feature. However, the models with three features are all worse than the best model in the second round. Thus, NAV and ETA are identified as critical features. We note that the two identified critical features are consistent with the findings from a previous vulnerability analysis on I-SIG [4].

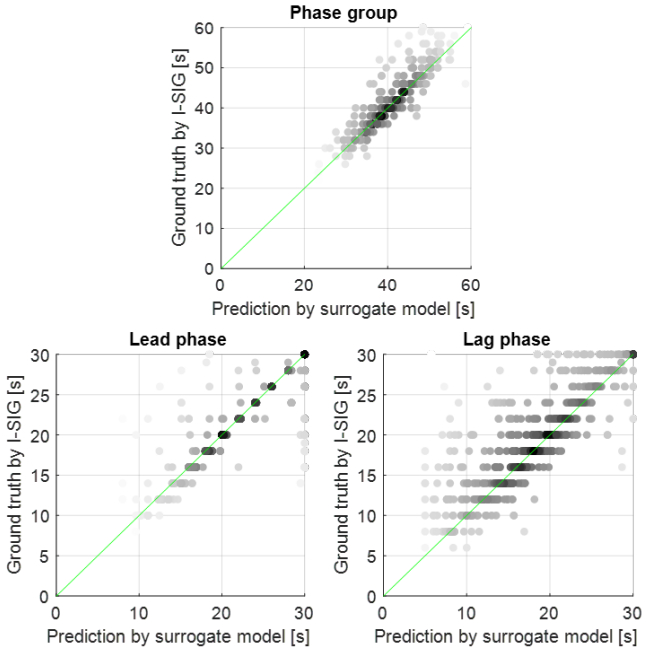

Fig. 4. Comparison between I-SIG and the trained surrogate model

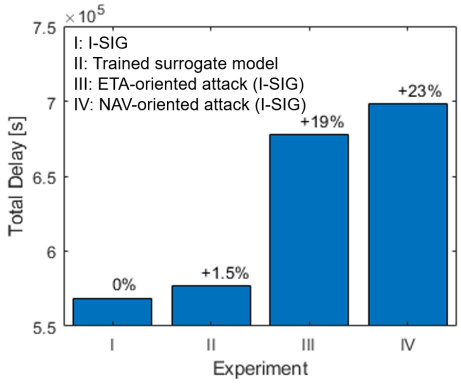

Fig. 5. Total delay for each experiment

Figure 4 shows the effectiveness of the trained surrogate model, in which the prediction by the trained surrogate model and the ground truth generated by I-SIG are compared. The color depth represents the density of the data. The majority of the data lie on or near the 45-degree line, indicating that the surrogate model has a good prediction accuracy. The MAE for lead phase and barrier duration prediction are only 0.52s and 1.33s respectively (Table I). The prediction of the lag phase has a relatively greater error because it is estimated indirectly from the barrier and the lead phase.

2) Evaluating the Impact of Attacks: Four simulation experiments are conducted to assess the impact of the proposed attack model. Each experiment lasts for 5 hours, with the exact same traffic demand and vehicle arrival patterns. The total delay for each experiment is shown in Figure 5.

In Experiment I, the original I-SIG system operates normally without attacks. This experiment serves as the bench-

TABLE I. APPLYING SFS FOR IDENTIFYING CRITICAL TRAFFIC FEATURES

	Tree 1 (Barrier)				Tree 2 (Lead Phase)			
	Feature set	MAE[s]	MAPE	RMSE[s]	Feature set	MAE[s]	MAPE	RMSE[s]
Round 1	QL	3.6771	9.32%	4.6842	QL	2.6690	14.34%	3.6185
	NAV	1.3967	3.46%	2.3786	NAV	1.1888	6.82%	2.2235
	HW	6.0618	15.53%	7.5209	HW	3.3484	17.76%	4.4968
	ETA	5.4608	14.04%	6.7911	ETA	3.8290	19.84%	4.6471
	VD	6.4353	16.45%	8.0939	VD	4.8858	25.85%	6.0647
	FR	4.6341	11.76%	5.7694	FR	3.4285	17.85%	4.2815
Round 2	NAV+QL	1.6386	4.06%	3.0106	NAV+QL	1.2375	7.01%	2.6973
	NAV+HW	1.5842	3.89%	2.8640	NAV+HW	1.1151	6.29%	2.3574
	NAV+ETA	1.3287	3.26%	2.3469	NAV+ETA	0.5205	2.95%	1.5097
	NAV+VD	1.6177	3.97%	2.9335	NAV+VD	1.3257	7.64%	2.8670
	NAV+FR	1.5162	3.74%	2.5721	NAV+FR	1.1948	6.86%	2.2860
Round 3	NAV+ETA+QL	1.3959	3.46%	2.5778	NAV+ETA+QL	0.5513	3.10%	1.7964
	NAV+ETA+HW	1.4065	3.48%	2.5982	NAV+ETA+HW	0.5398	3.07%	1.7040
	NAV+ETA+VD	1.3977	3.44%	2.5750	NAV+ETA+VD	0.5404	3.02%	1.7978
	NAV+ETA+FR	1.4059	3.49%	2.4968	NAV+ETA+FR	0.5398	3.04%	1.6367

mark for all the other experiments. In Experiment II, the trained surrogate model is used to generate signal timing plans and control the traffic signals. However, no falsified CV data are injected to the system. As evidenced by a small increase of 1.5%, the total delay is very close to the benchmark. This indicates that the trained surrogate model could effectively mimic the actual signal control logic. In Experiment III, the attacker is assumed to attack I-SIG based on the feature ETA. To achieve this, the attacker alters ETA by manipulating the location and speed data in the falsified BSMs. It is worth noting that only one falsified trajectory is injected into the system per attack. The total delay increases by 19%. In Experiment IV, the attacker is assumed to attack I-SIG based on the feature NAV. The attacker alters NAV by injecting multiple falsified trajectories to different phases per attack. The total delay increases by 23%. Results indicate that the ETA attack (only one falsified trajectory) is more effective than the NAV attack (multiple falsified trajectories) because it can trigger a vulnerability called "last vehicle advantage" in the I-SIG's logic. When under ETA attack, the I-SIG algorithm extends the green time to the maximum value to serve the fake vehicle. However, the NAV attack only adds fake vehicles into the arrival table, which only marginally increase the green time allocation. More details about the ETA attack can be found in our previous study [4]. These experiment results show that the proposed "black-box" attack model is effective in increasing intersection delay, even with a limited budget. In the original study, the maximum delay decrease brought by I-SIG is 16.33% [6]. It means that our proposed attack model can completely reverse the benefit brought by the CV technology.

V. DEFENSE STRATEGY

Although the focus of this study is on the impact evaluation of falsified data attacks, defense strategies are briefly discussed. Because the attacker needs to learn the control logic before attack, one natural defense strategy is to interfere with the learning process. For example, we may add noise to the optimized signal timing plans. This may increase the difficulty in learning the surrogate model. However, when the environment is benign (i.e., no attacks), adding noise makes the system operate under sub-optimal conditions. Thus, a trade-off needs to be made between security and efficiency.

Another defense strategy is to proactively identify falsified trajectories before they are utilized by the control system. The falsified trajectories are generated to alter the values of the critical features, which does not represent true traffic conditions. For example, in our case study, to alter ETA to a large value, the attacker needs to generate a falsified trajectory which shows that the falsified vehicle approaches the intersection with a low speed. Such falsified trajectories are behaviorally different from normal trajectories. By applying methods from the area of misbehavior detection, we may be able to identify abnormal (falsified) trajectories. We will investigate this defense strategy in our future research.

VI. RELATED WORK

Based on the general structure of a CV-TSC system in Figure 1, three attack surfaces can be identified at a connected intersection: the transportation infrastructure (RSU, signal controller, and traffic signals), the TMC, and the CVs. Usually, the transportation infrastructure is deployed in an agency's local network with firewall protection. It is difficult to access the infrastructure devices remotely from the public domain. In order to initiate an attack, attackers have to open up the signal control cabinet and establish a wired connection to the devices. Once attackers gain access to the system, they can directly manipulate the signal timing. Alternatively, attackers may trespass into the TMC and send control commands to the signal controller directly. These attacks are referred to as direct attacks, which have been investigated by previous studies [5], [9], [15], [19], [20]. These studies mainly focus on conventional traffic control systems, for instances, fixed-timing signal control [15] and ramp metering control [20].

The other type of attack towards the traffic control system is indirect attacks, in which attackers try to influence signal control decisions by injecting falsified data. Indirect attacks can be launched from the vehicle side. By exploiting software vulnerabilities, it is practically feasible that attackers hack into the communication devices in their own CVs and broadcast falsified messages. This is similar to compromising other Electronic Control Units as demonstrated in the literature [3], [14]. Alternatively, attackers may hack into their vehicles' internal networks. This can be achieved in many ways. For example, attackers may hack into the infotainment system of the vehicle [16]. Once attackers are in the vehicle's internal network, they would be able to take control of a wide range

of vehicle functions [14], including sending malicious BSMs that contain falsified data elements. Because attackers have arbitrary access to their own vehicles, indirect attacks are much more achievable. Recent studies have shown that falsified input data can indeed influence system control decisions and significantly downgrade the system performance. For example, influencing routing decisions in social navigation systems by generating virtual traffic jams (e.g., Google map, Waze) [11], [22], or increasing total travel delay by affecting signal control decisions [4], [7], [8], [17], [24].

VII. Conclusion

In this paper, we aim to investigate the security problem of CV-TSC systems. Compared to the literature, this study considers a more realistic attack scenario in which the control logic of CV-TSC systems is unavailable to the attacker. We assume that the attacker may learn the signal control logic using a surrogate model and identify critical traffic features. With the learned model, the signal timing plan generated by the control system can be predicted by the attacker. Falsified BSMs then can be constructed to alter the values of the critical traffic features. Consequently, the signal control decisions are influenced. The attacker is assumed to find the "best" value of the critical features by maximizing the dissimilarity between the pseudo-optimal timing plan and the resultant signal timing plan under attack. A comprehensive case study is conducted with I-SIG as the selected CV-TSC system. We find that the surrogate model can effectively mimic the actual control logic of I-SIG, which is sensitive to two critical traffic features: ETA (estimated time of arrival) and NAV (number of approaching vehicles). Two types of attacks are launched based on these two features. Simulation experiments show that the total delay increases by 19% and 23% respectively under these two attacks. This indicates that even though the control logic is unknown, an attacker is still able to cause severe damage to the CV-TSC system. To protect the system, two defense strategies are briefly discussed. Based on the findings of this paper, future work will focus on the proactive defense strategy to safeguard CV-TSC systems from falsified data attacks. The goal of the defense strategy is to detect anomaly in BSMs and filter out falsified trajectories before applying them in the CV-based applications.

Acknowledgment

This research is supported in part by NSF through Grant SaTC #1930041, CNS #1850533, CNS #1929771, USDOT UTC Grant 69A3552047138 and Mcity at the University of Michigan for financial support. The views presented in this paper are those of the authors alone.

References

[1] S.-T. Bow, *Pattern recognition and image preprocessing*. Marcel Dekker New York, 2002.

[2] L. Breiman, *Classification and regression trees*. Routledge, 2017.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, vol. 4. San Francisco, 2011.

[4] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, "Exposing congestion attack on emerging connected vehicle based traffic signal control," in *Network and Distributed Systems Security (NDSS) Symposium*, 2018.

[5] J. M. Ernst and A. J. Michaels, "Framework for evaluating the severity of cybervulnerability of a traffic cabinet," *Transportation Research Record*, vol. 2619, no. 1, pp. 55–63, 2017.

[6] Y. Feng, K. L. Head, S. Khoshmagham, and M. Zamanipour, "A real-time adaptive signal control in a connected vehicle environment," *Transportation Research Part C: Emerging Technologies*, vol. 55, pp. 460–473, 2015.

[7] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyberattacks with falsified data," *Transportation research record*, vol. 2672, no. 1, pp. 1–11, 2018.

[8] A. Ghafouri, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Vulnerability of fixed-time control of signalized intersections to cyber-tampering," in *2016 Resilience Week (RWS)*. IEEE, 2016, pp. 130–135.

[9] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*, 2014.

[10] Q. Guo, L. Li, and X. J. Ban, "Urban traffic signal control with connected and automated vehicles: A survey," *Transportation research part C: emerging technologies*, vol. 101, pp. 313–334, 2019.

[11] T. Jeske, "Floating car data from smartphones: What google and waze know about you and how hackers can control traffic," *Proc. of the BlackHat Europe*, pp. 1–12, 2013.

[12] G. H. John, R. Kohavi, and K. Pfleger, "Irrelevant features and the subset selection problem," in *Machine Learning Proceedings 1994*. Elsevier, 1994, pp. 121–129.

[13] P. Koonce and L. Rodegerdts, "Traffic signal timing manual," United States Federal Highway Administration, Tech. Rep., 2008.

[14] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[15] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos, "Vulnerability of transportation networks to traffic-signal tampering," in *2016 ACM/IEEE 7th International conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2016, pp. 1–10.

[16] S. Mazloom, M. Rezaeirad, A. Hunter, and D. McCoy, "A security analysis of an in-vehicle infotainment and app platform," in *10th {USENIX} Workshop on Offensive Technologies ({WOOT} 16)*, 2016.

[17] P. Oza, M. Foruhandeh, R. Gerdes, and T. Chantem, "Secure traffic lights: Replay attack detection for model-based smart traffic controllers," in *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security*, 2020, pp. 5–10.

[18] N. Papernot, P. McDaniel, I. Goodfellow, S. Jha, Z. B. Celik, and A. Swami, "Practical black-box attacks against machine learning," in *Proceedings of the 2017 ACM on Asia conference on computer and communications security*, 2017, pp. 506–519.

[19] K. A. Perrine, M. W. Levin, C. N. Yahia, M. Duell, and S. D. Boyles, "Implications of traffic signal cybersecurity on potential deliberate traffic disruptions," *Transportation research part A: policy and practice*, vol. 120, pp. 58–70, 2019.

[20] J. Reilly, S. Martin, M. Payer, and A. M. Bayen, "Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security," *Transportation Research Part B: Methodological*, vol. 91, pp. 366–382, 2016.

[21] D. SAE, "J2735 dedicated short range communications (dsrc) message set dictionary," *Society of Automotive Engineers, DSRC Committee*, 2009.

[22] M. B. Sinai, N. Partush, S. Yadid, and E. Yahav, "Exploiting social navigation," *arXiv preprint arXiv:1410.0151*, 2014.

[23] USDOT, "Multi-modal intelligent traffic safety system," https://www.its.dot.gov/research_archives/dma/bundle/mmitss_plan.htm, 2019, online; Accessed: 2019-05-21.

[24] C.-C. Yen, D. Ghosal, M. Zhang, C.-N. Chuah, and H. Chen, "Falsified data attack on backpressure-based traffic signal control algorithms," in *2018 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2018, pp. 1–8.

[25] H. Yeo, A. Skabardonis, J. Halkias, J. Colyar, and V. Alexiadis, "Oversaturated freeway flow algorithm for use in next generation simulation," *Transportation Research Record*, vol. 2088, no. 1, pp. 68–79, 2008.