VULNERABILITY OF TRAFFIC CONTROL SYSTEM UNDER CYBER-ATTACKS USING FALSIFIED DATA

Yiheng Feng (Corresponding Author)
Transportation Research Institute (UMTRI), University of Michigan
2901 Baxter Rd, Ann Arbor, MI, 48109
Email: yhfeng@umich.edu

Shihong Huang
Department of Civil and Environmental Engineering, University of Michigan
2350 Hayward Street, Ann Arbor, MI, 48109
Email: edhuang@umich.edu

Qi Alfred Chen
Department of Electrical Engineering and Computer Science, University of Michigan
2260 Hayward Street, Ann Arbor, MI 48109
Email: alfchen@umich.edu

Henry X. Liu
Department of Civil and Environmental Engineering, University of Michigan
Transportation Research Institute (UMTRI), University of Michigan
2350 Hayward Street, Ann Arbor, MI, 48109
Email: henryliu@umich.edu

Z. Morley Mao
Department of Electrical Engineering and Computer Science, University of Michigan
2260 Hayward Street, Ann Arbor, MI 48109
Email: zmao@umich.edu

Word Count: 5206 words of text +9 tables/figures x 250 = 7456 words
Submission Date: August 1st, 2017
Prepared for Presentation and Publication at the 97th Annual Meeting of the Transportation Research Board,
January 2018, Washington D.C.

ABSTRACT

Existing traffic control systems are mostly deployed in private wired networks. With the development of wireless technology, vehicles and infrastructure devices will be connected through wireless communications, which might open a new door for cyber attackers. It is still not clear what types of cyber-attacks can be performed through infrastructure-to-infrastructure (I2I) and vehicle-to-infrastructure (V2I) communications, whether such attacks can introduce critical failure to the system, and what impacts of cyber-attacks on traffic operations are. This paper investigates the vulnerability of traffic control system in a connected environment, where four typical elements including signal controllers, vehicle detectors, roadside units (RSUs), and onboard units (OBUs) are identified as the attack surfaces. The paper mainly focuses on attacking actuated and adaptive signal control systems by sending falsified data, which is considered as an indirect but realistic attack approach. The objective of an attacker is to maximize system delay with constraints such as budget and attack intensity. Empirical results show that different attack scenarios result in significant differences regarding delay and some ineffective attacks may even improve the system performance. Simulation results from a real world corridor show that critical intersections, which has a higher impact on congestion, can be identified by analyzing the attack locations. Identification of such intersections can be helpful in designing a more resilient transportation network.

Key Words: Cyber-security, Cyber Attack, Traffic Control System, Falsified Data, Actuated and Adaptive Control

MOTIVATION

Existing transportation infrastructure is usually isolated regarding connectivity since all vehicles are operated independently, and traffic control systems are mostly deployed in a private wired network. With the development of wireless technology, vehicles and infrastructure will be connected through wireless communications (e.g., Dedicated Short Range Communication (DSRC) or cellular network), which might open a new door for cyber attackers. Cyber-security of transportation systems has been a growing research area in the past few years, but most efforts are focused on inter-vehicle communications. As a critical part of the transportation infrastructure, existing traffic control systems have a profound impact on the safety and efficiency of urban traffic flow, but are very vulnerable to cyber-attacks due to the "systematic lack of security consciousness" (*1*). For example, an Argentinian security expert hacked into New York City's wireless vehicle detection system with a cheap wireless device. The vulnerabilities he found allowed anyone to take complete control of the devices and send fake data to the traffic control systems (*2*). Although traffic signals were not directly controlled, fake vehicle data could cause severe traffic congestion and increase crash risks. Another example involved hacking into a variable message sign in Austin, Texas, and displaying "Zombie Ahead" instead of correct traffic information (*3*). To systematically investigate the cybersecurity of transportation infrastructure, The National Cooperative Highway Research Program (NCHRP) started a new project to develop guidance for transportation agencies on mitigating the risks from cyber-attacks towards traffic management systems[1].

However, it is still not clear what types of cyber-attacks can be performed through infrastructure-to-infrastructure (I2I) and vehicle-to-infrastructure (V2I) communications, whether such attacks can create critical failure to traffic control system, and what are the impacts of cyber-attacks on traffic operations. A systematic study of the vulnerabilities of the existing traffic control system and corresponding remedies need to be established. The objective of this paper is to investigate potential attack surfaces, and the adversarial consequences of such attacks may bring to the traffic network.

First, four possible attack surfaces of the traffic control system in a connected environment is identified, including signal controllers, vehicle detectors, onboard units (OBUs), and roadside units (RSUs). We focus our analysis on attacking actuated and adaptive signal control systems by sending falsified data from either hacked vehicle detectors or compromised OBUs. The attack is modeled as an optimization problem with the objective to maximize system delay and constraints such as the number of compromised devices and attack intensity. Analysis of a hypothetical intersection shows that some attacks are very effective regarding increasing total delay, while others are not. Finally, a real-world corridor is used to evaluate the proposed attack methods.

The rest of this paper is organized as follows. Section 2 provides a brief review of related work. In section 3, four attack surfaces with different attack strategies are identified. Section 4 presents the traffic model to represent the vehicle dynamics and the attack model. Section 5 evaluates the effectiveness of different attack strategies at a hypothetical intersection and a real-world corridor. Section 6 gives the conclusions and outlines the directions of future work.

RELATED WORK

[1] http://apps.trb.org/cmsfeed/TRBNetProjectDisplay.asp?ProjectID=4179

In this section, a brief overview of cyber-security related transportation infrastructure studies is provided. Ghena et al. (*1*) analyzed the security of a currently deployed traffic signal control system and found the controller network could be infiltrated through its wireless infrastructure. Once on the network, the controller could be accessed by the operating system's debug port or through NTCIP commands. Although the safety of the signal operations was protected by the Malfunction Management Unit (MMU), the attackers could generate very inefficient signal timing plans which might cause traffic congestion and even denial of service. This study mainly demonstrated how to leverage existing design flaws to gain control of the signal system, but didn't provide detailed attack strategies and corresponding consequences.

Laszka et al. (*4*) and Ghafouri et al. (*5*) studied the vulnerability of fixed-time signal control to cyber-attacks. The attacks were formulated as mathematical programming problems with different objectives such as worst-case network accumulation, worst-case lane accumulation, and risk-averse target accumulation. Heuristic and decomposition algorithms were implemented to solve the problem at a network level. A precondition of tampering fixed time signal control is that the attacker can access and manipulate signal controller directly. This is not a very realistic assumption unless the attacker can access the traffic signal cabinet physically. On the other hand, it is much easier to falsify input data to influence the control decisions under actuated or adaptive control. Toward this end, Jeske (*6*) investigated Google and Waze navigation systems and demonstrated how attackers could take control of the navigation system and influence the traffic flow by sending false location information. Tufnell (*7*) have successfully hacked into Waze maps and generated fake GPS coordinates to create virtual traffic jams. However, neither of the two studies incorporated the fake data into traffic control systems and analyzed the consequences.

Other than tampering traffic signal operations, Reilly et al. (*8*) presented a study on attacking freeway ramp metering to generate arbitrarily complex congestion patterns. Finite-horizon optimal control and multi-objective optimization techniques were used to launch attacks on coordinated ramp metering controllers. Different attack scenarios were designed and conducted. Results showed arbitrary congestion-on-demand patterns could be created with enough controlled ramps.

Although how to detect and protect the system from cyber-attacks is beyond the scope of this paper, some approaches have been proposed to detect anomaly from traffic flow patterns. For example, Canepa and Claudel (*9*) tried to detect falsified probe-based vehicle data using LWR traffic flow model. The detection was posed as a mixed integer linear feasibility problem. Zhang et al. (*10*) quantified anomaly by proposing an anomaly index in both spatial and temporal perspectives, based on dictionary-based compression theory. The original intention was to identify non-recurrent traffic flow pattern caused by incidents, but this method could be potentially used to detect cyber-attacks and design defense strategies.

THREAT MODEL

Before presenting the attack model, the threat model of a "connected" intersection is introduced and shown in FIGURE 10. Here "connected" refers to that the intersection and vehicles are equipped with wireless communication devices (such as RSU and OBUs) and can communicate with each other. While exact deployments are different from location to location, we consider four typical elements in the traffic control system as possible attack surfaces:

- Traffic signal controller: used to generate signal timing plans based on different control strategies, including fixed-time, actuated and adaptive. If traffic signals are under actuated or adaptive control, the controller utilizes data from vehicle detectors and RSU to make control decisions.
- Vehicle detectors: used to detect vehicles and generate service calls to signal controller. If vehicle detectors are configured as system detector, it can also be used to provide volume and speed information.
- OBU in vehicles: used to generate vehicle-related information (e.g., Basic Safety Messages (BSMs)) and broadcast the information to other vehicles and infrastructure through Over The Air (OTA) messages.
- RSU at intersections: used to broadcast infrastructure related messages (e.g., Signal Phasing and Timing, MAP) and receive vehicle information. It provides input data (e.g., trajectory) to signal controller.

Based on the attack surfaces, two types of attacks are identified: direct attack and indirect attack. Direct attack refers to hacking into the signal controller and RSU and changing the signal timing plans directly. To launch direct attacks, an attacker needs physical access to the devices, which requires the attacker to open up the signal controller cabinet and connect to the signal controller or the RSU using an Ethernet cable. Indirect attack refers to tampering data from vehicle detectors and OBUs. Usually, only part of the input data can be falsified. Indirect attacks are more realistic to conduct. For example, spoofing into wireless vehicle detectors (*2*), or compromising OBUs in private vehicles. This paper focuses on indirect attacks under actuated and adaptive signal control. For actuated signal control, we assume signal controller utilizes vehicle detector data to perform actuation logic. Compromised vehicle detectors may generate fake vehicle calls or cancel real vehicle calls. For adaptive signal control, we assume signal controller generates optimal signal plans based on BSM data from connected vehicles (CVs). Compromised OBUs may insert virtual vehicles on the roadway that don't exist.

TRAFFIC AND ATTACK MODELS

To model the transportation network and quantify the consequences of cyberattacks, a traffic flow model is needed. The cell transmission model (CTM) (*11*, *12*) is applied for two reasons. The CTM is a macroscopic traffic model so that it can be used to simulate network traffic with thousands of vehicles and attack scenarios in an efficient way. Meanwhile, compared to other link-based flow and density models, CTM divides roadway into homogeneous segments, so that attacks can be launched at different locations (cells). In this section, we will first introduce how to model actuated and adaptive signal control with CTM. Then the attack model will be presented.

Cell Transmission Model

CTM is a first-order approximation to LWR partial differential equation. The model assumes a triangular fundamental diagram and discretizes space into homogeneous cells and time into intervals. The cell length is equal to one-time interval multiplied by free-flow speed defined in the fundamental diagram. CTM was originally developed to model highway traffic with a single entrance and exit (*11*). Later the model was extended to represent network traffic (*12*), which allows it to model traffic flows at signalized intersections. A typical intersection in CTM is shown in FIGURE 11.

There are six types of cells: ordinary cell, merging cell, diverging cell, intersection cell, source cell and sink cell. An ordinary cell has one preceding cell and one following cell and has limited jam density and capacity. A diverging cell has one preceding cell and multiple following cells while a merging cell has multiple preceding cells and one following cell. An intersection cell is similar to an ordinary cell except that the flow is controlled by signal timing. Source cells and sink cells are responsible for generating and exiting vehicles. Due to space limitation, for the detailed formulation of CTM, refer to (*11*, *12*).

The parameters of the CTM model in this paper is configured as follows. Free flow speed v is set to 54 km/h (15 m/s). Backward shockwave speed w is set to 18 km/h (5m/s). The maximum flow rate Q_m is set to 1800 veh/h and the corresponding critical density k_m is 33.33 veh/km and jam density k_j is 133.33 veh/km. Time step is set to 2 seconds, which is similar to the unit extension time in actuated control. As a result, the cell length is 30m.

Model actuated signal control with CTM

To model actuated signal control with CTM, we assume stop-bar detectors are installed in intersection cells. The density ratio of cell i at time t can be calculated as $d(i,t)=n(i,t)/N(i)$. Where, $n(i,t)$ is the number vehicles in cell i at time t, and $N(i)$ is the maximum number of vehicles in cell i. A critical density ratio d_c is defined for each intersection cell. The actuation logic is modeled based on d_c. If density ratio of intersection cell i at time t is less than the critical density ratio, then the current phase is terminated. Otherwise, extend green to next time step.

To determine the best d_c, we ran a series of simulation with different values of d_c. Vehicle delay in cell i at time t is defined as the difference between $n(i,t)$ and number of vehicles that can be discharged from the cell $y(i,t)$, because in CTM vehicles are either in free flow speed (discharged to the following cell) or in queuing state (remain in current cell).

$$D = \sum_{t \in T} \sum_{i \epsilon I} [n(i,t) - y(i,t)] \quad (1)$$

Both lower and higher critical density ratios result in higher vehicle delay. Lower critical density ratios correspond to longer unit extension times while higher critical density ratios correspond to shorter unit extension times. The lowest delay occurs when d_c=0.25, which is the critical density ratio (k_m/k_j=0.25) that separates free flow and congestion regime. For a vehicle actuation logic, it is appropriate to terminate green when the traffic state changes from congested to free flow. Therefore, d_c=0.25 is used in numerical experiments.

Model adaptive signal control with CTM

The adaptive control algorithm is adapted from (*13*, *14*). Signal optimization is formulated as a dynamic programming (DP) problem, in which each phase is considered as one stage in DP. A forward recursion is used to calculate performance measures and record optimal value function. The objective of the forward recursion is to choose an optimal signal plan with minimal total vehicle delay. A backward recursion is used to retrieve the optimal solution.

The major difference of the algorithm applied in this study from the original algorithm is the performance function calculation. In previous DP formulations, the performance measures were calculated from an arrival table, which included estimated time of arrival and requested phase of each vehicle. However, CTM is a macroscopic model in which individual vehicle information is not available. To accurately calculate vehicle delay, a snapshot of the current network condition is taken at the beginning of each signal optimization. A parallel CTM simulation is executed based on the snapshot as initial network condition to generate vehicle delays in each DP iteration.

The signal optimization algorithm plans as many stages (phases) as necessary until all vehicles in the snapshot pass the intersection cells. A rolling horizon scheme is adopted in which the optimization is performed at the beginning of each phase to include recent vehicle arrivals.

Attack Model

It is assumed that an attacker has limited resources. For example, the number of vehicle detectors can be tampered, or the number of OBUs can be compromised are limited. As a result, an attacker needs to choose a subset of locations or devices to maximize the profit, which is defined as maximization of network congestion. Formally, an attack A is defined as:

$$A = (S, \{n'(i,t) | \forall i \in S\})$$

Where S is the set of cells can potentially be under attack and $n'(i,t)$ is the number of vehicles in the cell under attack. Attacks are conducted through increasing or decreasing number of vehicles in a cell to mimic the change of stop-bar detector data and BSM distribution.

The attack model can be expressed as:

$$\max_{A} D(A) \tag{2}$$

s.t

$$|S| \leq B \tag{3}$$

$$n'(i,t) \leq \min\big(n(i,t) + \varepsilon, N(i)\big), \forall i \in S \tag{4}$$

$$n'(i,t) \geq \max(n(i,t) - \varepsilon, 0), \forall i \in S \tag{5}$$

The objective function means an attacker intends to maximize total vehicle delay. The first constraint indicates that the attacker is limited by budget B. The next two constraints represent the cautiousness of the attacker. The number of vehicles can be changed is limited by a threshold ε and road physical limits. If the data deviates a lot from the normal range, the attacker can be detected by the defense models more easily.

NUMERICAL EXAMPLES

In this section, numerical results based on a hypothetical intersection and insights on the effectiveness of the attacks are presented first. Then a real-world six-intersection corridor in Ann Arbor, MI is built to evaluate the attack models. All models are coded in Matlab.

A Hypothetical Intersection

The layout of a hypothetical intersection is shown in FIGURE 11. It is a typical four-leg intersection with all vehicle movements. There are four signal phases: eastbound and westbound left turn (phase 1), eastbound and westbound through (phase 2), northbound and southbound left turn (phase3), and northbound and southbound through (phase 4).

Right turn vehicles are not restricted by traffic signals. The minimum green time is set to 5 time steps (10s) and the maximum green time is set to 20 steps (40s) for each phase. The length of each approach is 10 cells (including the intersection cells), which is similar to the DSRC communication range. Traffic demand is set to 1000 veh/h eastbound/westbound and 800 veh/h northbound/southbound. Vehicle arrivals follow a Poisson distribution. Turning ratios of each approach are the same and set to 0.2/0/7/0.1 for left turn, through, and right turn respectively. Simulation runs for 1000 time steps with 100 steps as a warm-up period.

FIGURE 12 shows total delay and congestion pattern of eastbound approach under actuated and adaptive control without attacks. This serves as the baseline for our comparison. Different colors represent different congestion levels, with green to be no congestion and red to be the severest congestion.

Attack under Actuated Control

Under actuated control, it is assumed that stop-bar detector data can be manipulated by the attacker so that number of vehicles at intersection cells can be added (generate fake vehicle calls) or subtracted (cancel real vehicle calls). This results in two attack modes *M*=2. To cause maximum damage, the attacker changes the detector data as much as possible, but within the threshold ε=0.5. Then $n'(i,t)$ is equal to either $\min\big(n(i,t)+\varepsilon, N(i)\big)$ or $\max(n(i,t)-\varepsilon, 0)$. The budget B is set to 4 so that all phases can be attacked. To thoroughly analyze the effectiveness of all attack scenarios, we enumerate all the possibilities, which result in a total number of 80 different cases:

$$\sum_{p=1,2,3,4} C_P^p * M^p = 80$$

Where *p* is the signal phase index, and *P* is the total number of phases.

FIGURE 13 shows total vehicle delay and average total delay by the number of attacking phases. It can be seen from FIGURE 13 (a) that the effectiveness of different attacks varies a lot. FIGURE 13 (b) shows the trend that attacks cause more vehicle delay when the number of attacking phases increases.

FIGURE 14 shows the comparison between most effective and least effective attacks at the eastbound approach. The most effective attack occurs when phase 2, 3 and 4 are under attack with subtracting vehicles at intersection cells corresponding to phase 2 and adding vehicles at intersection cells corresponding to phases 3 and 4. The resultant total delay can be six times higher than the baseline scenario. The least effective attack occurs when attacking intersection cells related to phase 1 and 3, with subtracting vehicles on both phases. It is interesting to see that the resultant total delay (36441) is even smaller than the baseline scenario (38396), which indicates that the attack improves the system performance. The reason is that actuated control is not the optimal control strategy. In certain cases when a phase is green with lower demand while other phases are red with higher demand, it is more efficient to terminate the lower demand phase earlier to serve other phases. In this case, phase 1 and 3 are left turn phases with lower demand. Subtracting vehicles shortens both phases, which gives more time to higher demand phases 2 and 4.

Attack under Adaptive Control

Under adaptive control, the control algorithm utilizes data from CV (e.g., BSMs) to generate optimal signal plans, so that every cell within the communication range can be potential targets. It is assumed that an attacker is only interested in manipulating the number of vehicles in ingress cells because vehicles in egress cells don't affect the signal optimization. The attacker can add or subtract vehicles at different number of approaches with the maximum number of attacking approaches A=4. If the attacker decides to attack one approach, then all ingress cells on that approach are affected. The threshold ε is also set to 0.5. Totally 30 attack scenarios are generated.

FIGURE 15 shows total vehicle delay of all attack scenarios and average total delay by the number of attack approaches. FIGURE 15 (a) compares the total delay of adding vehicles or subtracting vehicles when attacking the same approach(s). In general, adding fake vehicles are more effective than removing real vehicles. Because under current demand level (medium), green time wasted under longer cycle lengths can cause more delay than increased lost time with shorter cycle lengths. FIGURE 15 (b) shows the similar pattern that the average total delay increases with the number of attack approaches.

Another finding is that attacks under adaptive control are far less effective than under actuated control with the same attack intensity ε. The most effective attack under adaptive control causes 41199 vehicle delay, which is only 33.66% more than the baseline scenario. However, the most effective attack under actuated control generates delay 6 times more than the baseline scenario. Under adaptive control, all ingress cells (including intersection cells) are affected, while under actuated control, only intersection cells are affected. However, results suggest that adaptive control is more robust than actuated control. Adaptive control tries to minimize total delay under the impact of attacks based on inputs from all ingress cells, while actuated control logic can only accommodate instantaneous arriving flow at intersection cells, but doesn't have an overall picture of current traffic condition.

Plymouth Rd Corridor

Six consecutive intersections along Plymouth Rd at Ann Arbor, Michigan are modeled in CTM to evaluate the attack model under actuated control. To calibrate the model, video data of the six intersections were collected on May 16th, 2017, from 4:00 pm to 5:00 pm. Traffic volume of each approach, turning ratio of each movement and signal timing of each intersection were extracted from the video and used as input to the CTM model.

The corridor contains two T-shape intersections and four standard intersections. The standard intersections have four phases as defined in the previous section, while the T intersections have only two phases. Therefore, there are 20 signal phases along the corridor. Each of them is identified as a potential attack location. The minimum and maximum green time for the through movement along Plymouth Rd is set to 10 and 30 time steps, while the rest of the phases have 5 and 15 time steps for minimum and maximum green time. Each attack scenario lasts 2100 time steps, which contains 300 time steps of warm-up (no attack) period and 1800 time steps for performance evaluation (under attack). It is assumed that the attacker has a budget limit so that a maximum of four phases can be attacked. This results in a total number of 87440 attack scenarios. Due to this large number, the attack scenarios are carried out by Flux, a Linux-based high-performance computing cluster at the University of Michigan. 20 CPU cores are used to run the attack scenarios in parallel and the total computation time is 14 hours.

When only one phase is under attack, Scenario 7, which attacks phase 2 (through phase on the main arterial) at Intersection 2 by subtracting vehicles, has the highest delay. A snapshot of the corridor at the final simulation time step is shown in FIGURE 16. The intersection on the left is numbered as one, and the intersection on the right is numbered as six. When under attack, the signal controller always terminates phase 2 upon the minimum green time, which causes oversaturation for westbound through traffic and vehicle queue starts to accumulate. The queue eventually propagates to intersection 3 and causes spillover. The spillover prevents westbound through traffic at intersection 3 from entering the downstream link during green. Those through traffic constantly call for green extensions, which generates more delay for the cross street traffic due to long waiting time. The same situation happens when the queue propagates to intersection 4 and intersection 5. Notice that there is a long queue in the northbound approach of intersection 5 because this approach has heavy left turn traffic. The spillover on the main arterial prevents vehicles turning left from the cross street. The result indicates that phase 2 at intersection 2 is the critical phase along the corridor.

FIGURE 17 shows vehicle delay under all attack scenarios with different number of attacking phases. It can be seen that the average total vehicle delay increases with the number of attacking phases, which is consistent with previous results. If all four phases are under attack, the most effective way is to subtract vehicles from phase 2 (through movement on Plymouth Rd) at intersection 2 and phase 3 (left-turn phase on cross street) at intersection 6, at the same time add vehicles to phase 3 at intersection 2 and phase 2 at intersection 6.

Although trying all attack scenarios guarantees the optimal solution, it is unrealistic for an attacker to enumerate all the possibilities and find out the best strategy in real time. Thus, a simple greedy attack policy is proposed to find an effective attack strategy. The attacker starts with attacking one phase and enumerates all the scenarios to find the critical phase which causes the largest delay. Given the previous attacking phase, the attacker adds another phase and again enumerates all possibilities to find the second critical phase. This process is repeated until the budget (maximum number of phases) limit is reached. Take Plymouth corridor as an example, the total number of scenarios need to be simulated by the greedy attack policy is 40+38+36+34=148, assuming the budget is 4 phases. This number is significantly smaller than the total number of scenarios by enumeration. The maximum delay generated by the greedy attack policy is shown in FIGURE 18, with the delay from optimal attack strategy by enumeration. When only one or two phases are under attack, the attack strategies found by the greedy attack policy are the same as the optimal attack strategy. When more phases are under attack, the greedy attack policy still can find an attack strategy that is very close to the optimal solution, with much less time.

CONCLUSION AND FURTHER RESEARCH

In this paper, we investigated the vulnerabilities of traffic control system under cyber-attacks. We focused on attacking actuated and adaptive signal control systems by sending falsified data to influence signal timing plan generation. The primary goal of an attacker was to maximize network-wide vehicle delay with constraints such as budget and attack intensity. Results from a hypothetical intersection showed that some attacks could be very effective and cause severe congestion, while others may even reduce the total delay. Results from a real-world corridor showed that critical intersections, which had a higher impact on congestion, can be identified by analyzing the attack locations. Identification of critical intersections would be helpful in designing a more resilient transportation network.

To launch such attacks, an attacker needs to collect necessary information about the signal control system, such as phase sequence, minimum green time and maximum green time, etc. However, this paper focuses mainly on the consequences of the traffic systems under cyberattacks. We will explore other steps in the end-to-end exploitation, e.g., reconnaissance, in the future work. Moreover, we will extend our current results towards two directions. First, besides maximizing total delay, attackers may have other objectives such as obtaining personal gain (e.g., minimizing personal delay) or creating safety risks (e.g., causing more vehicles in dilemma zone). With different objectives, the attack strategies can be different. Second, it is necessary to consider the cyber-security problem from a defender's point view. Defense models need to be developed to detect attacks and protect the transportation infrastructure.

ACKNOWLEDGEMENTS

The authors would like to thank Mcity at the University of Michigan for the financial support. The views presented in this paper are those of the authors alone.

REFERENCES

1. Ghena, B., W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman. Green Lights Forever: Analyzing the Security of Traffic Infrastructure. Presented at the The 8th USENIX Conference on Offensive Technologies, Berkeley, CA, USA, 2014.
2. Prigg, M. Has New York's Traffic Light System Been HACKED? *DailyMail.com*, May, 2014. URL: http://www.dailymail.co.uk/sciencetech/article-2617228/New-Yorks-traffic-lights-HACKED-technique-work-world.html. Accessed: 07/302017.
3. Miller, J. R. Hackers Crack Into Texas Road Sign, Warn of Zombies Ahead. *Fox News*, Jan, 2009. URL: http://www.foxnews.com/story/2009/01/29/hackers-crack-into-texas-road-sign-warn-zombies-ahead.html. Accessed: 07/30/2017.
4. Laszka, A., B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos. Vulnerability of Transportation Networks to Traffic-Signal Tampering. Presented at the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), 2016.
5. Ghafouri, A., W. Abbas, Y. Vorobeychik, and X. Koutsoukos. Vulnerability of Fixed-Time Control of Signalized Intersections to Cyber-Tampering. Presented at the 2016 Resilience Week (RWS), 2016.
6. Jeske, T. Floating Car Data from Smartphones: What Google and Waze Know about You and How Hackers Can Control Traffic. Presented at the BlackHat Europe, 2013.
7. Tufnell, N. Students Hack Waze, Send in Army of Traffic Bots. *wired.co.uk*, , 2014.
8. Reilly, J., 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, 2016, pp. 366–382. https://doi.org/10.1016/j.trb.2016.05.017.
9. Canepa, E. S., and C. G. Claudel. Spoofing Cyber Attack Detection in Probe-Based Traffic Monitoring Systems Using Mixed Integer Linear Programming. Presented at the 2013 International Conference on Computing, Networking and Communications (ICNC), 2013.

10. Zhang, Z., Q. He, H. Tong, J. Gou, and X. Li. Spatial-Temporal Traffic Flow Pattern Identification and Anomaly Detection with Dictionary-Based Compression Theory in a Large-Scale Urban Network. *Transportation Research Part C: Emerging Technologies*, Vol. 71, 2016, pp. 284–302. https://doi.org/10.1016/j.trc.2016.08.006.
11. Daganzo, C. F. The Cell Transmission Model: A Dynamic Representation of Highway Traffic Consistent with the Hydrodynamic Theory. *Transportation Research Part B: Methodological*, Vol. 28, No. 4, 1994, pp. 269–287. https://doi.org/10.1016/0191-2615(94)90002-7.
12. Daganzo, C. F. The Cell Transmission Model, Part II: Network Traffic. *Transportation Research Part B: Methodological*, Vol. 29, No. 2, 1995, pp. 79–93. https://doi.org/10.1016/0191-2615(94)00022-R.
13. Sen, S., and K. L. Head. Controlled Optimization of Phases at An Intersection. *Transportation Science*, Vol. 31, No. 1, 1997, pp. 5–17.
14. Feng, Y., 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, 2015, pp. 460–473. https://doi.org/10.1016/j.trc.2015.01.007.

List of Figures

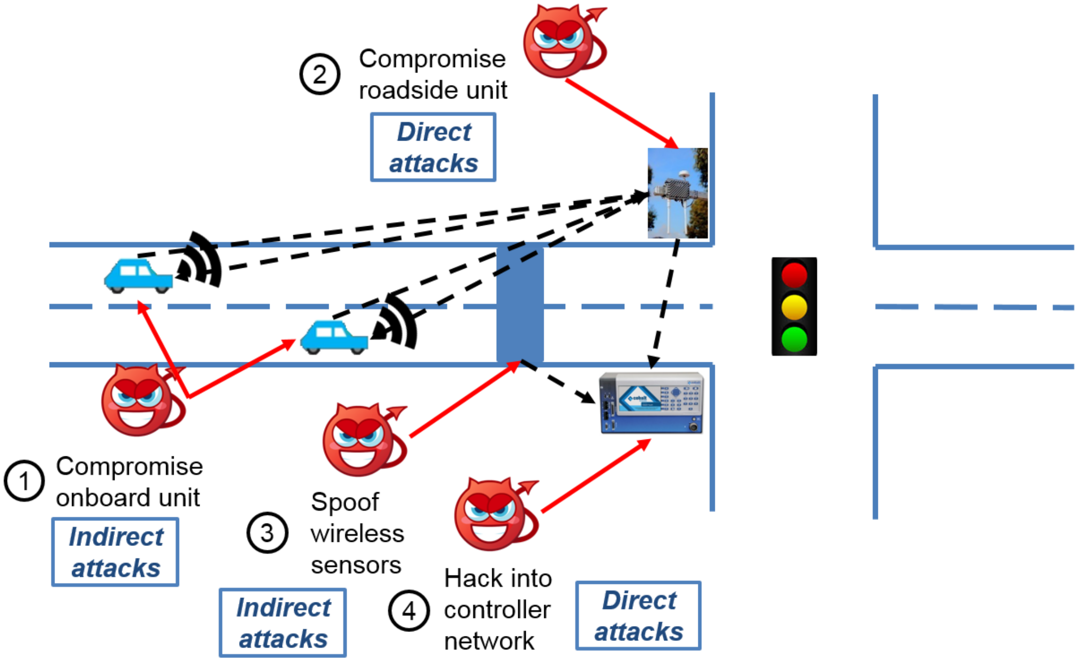


FIGURE 10 Intersection Threat Model.

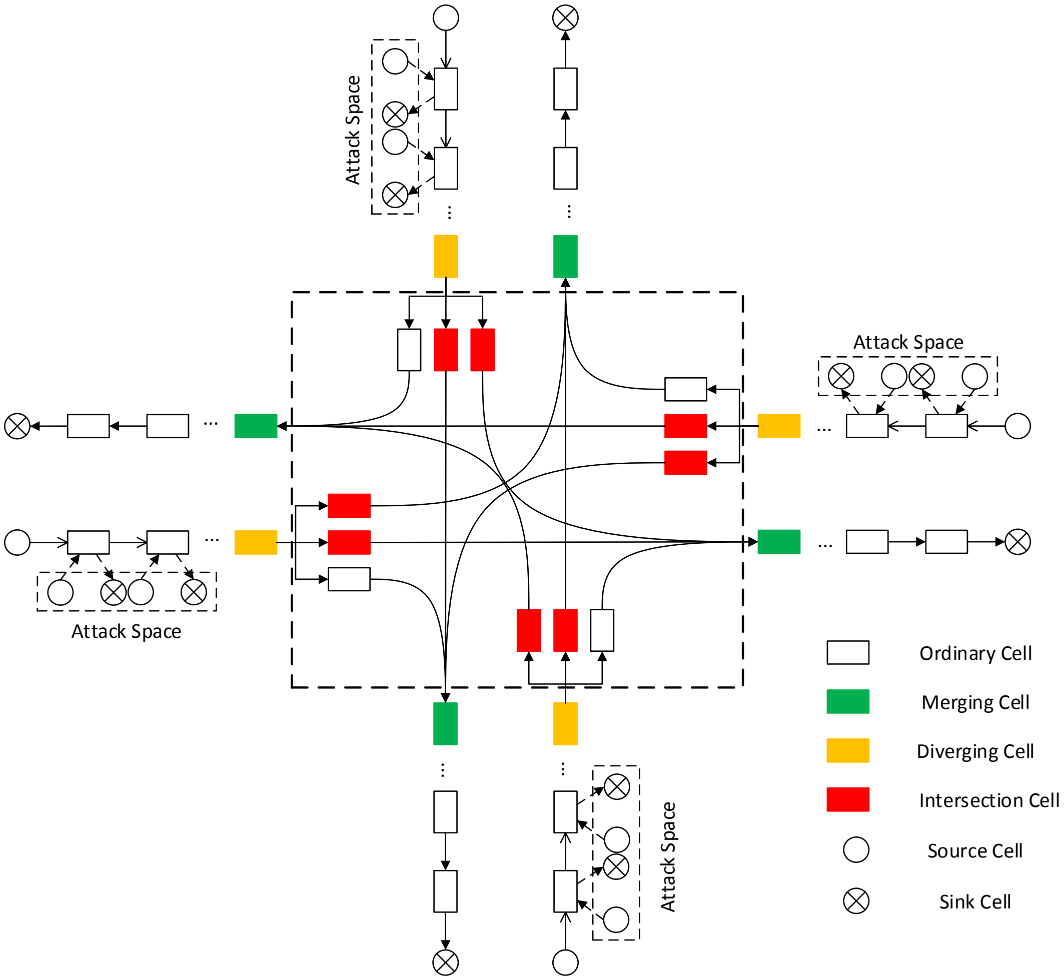
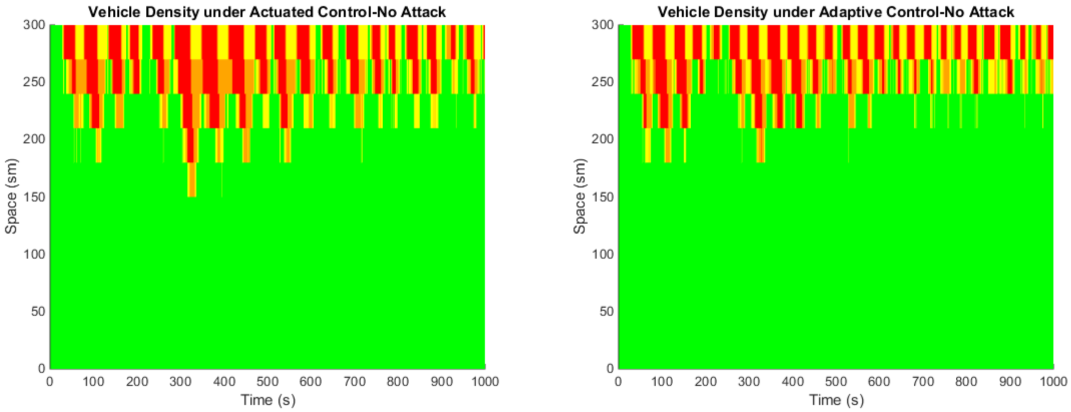


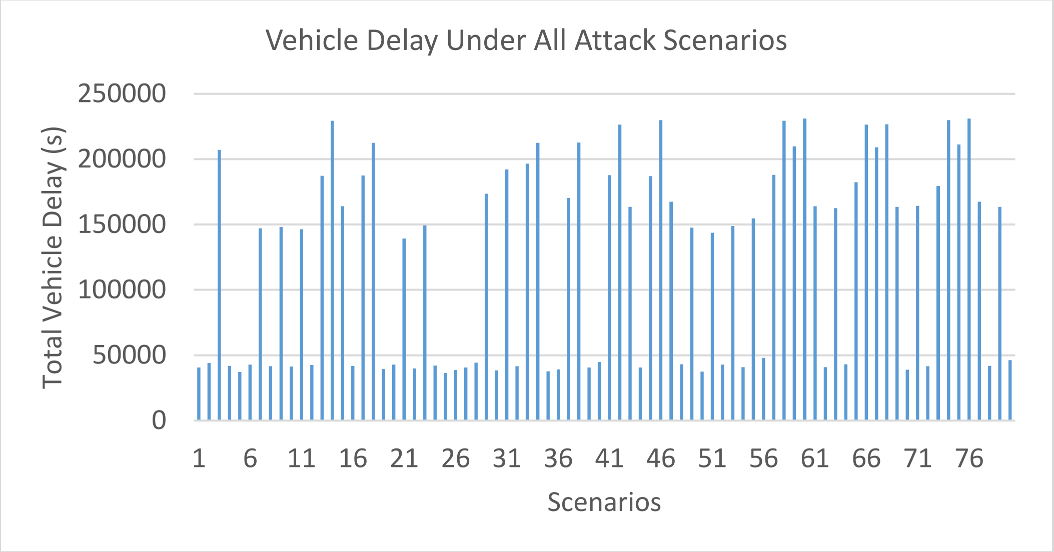
FIGURE 11 Intersection Representation of CTM with Attack Spaces.



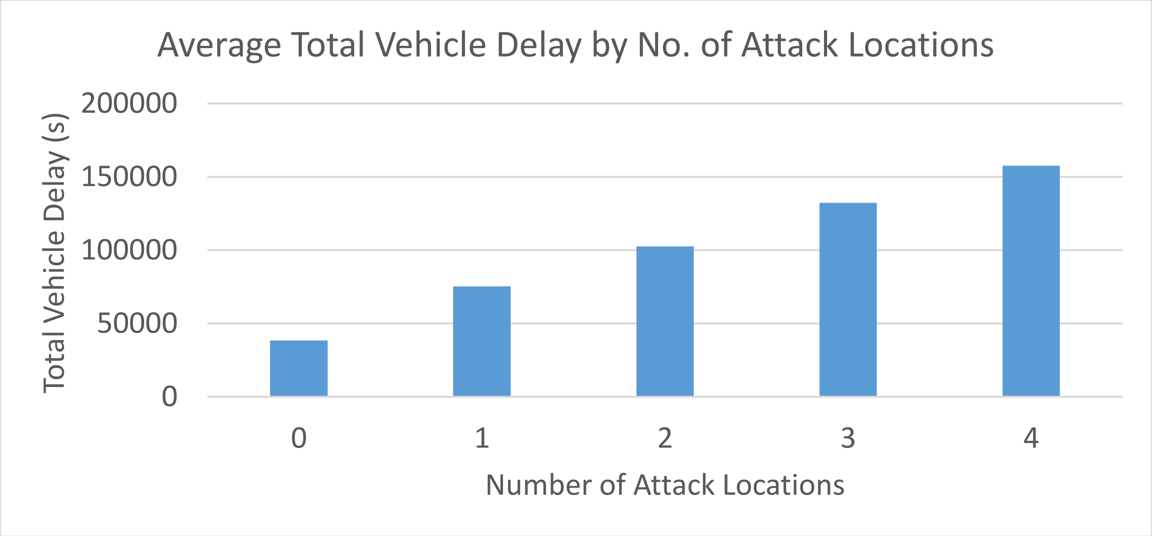
Total Delay: 38396
(a) Actuated control

Total Delay: 30823
(b) Adaptive control

FIGURE 12 Vehicle Delay Comparison without Attack.

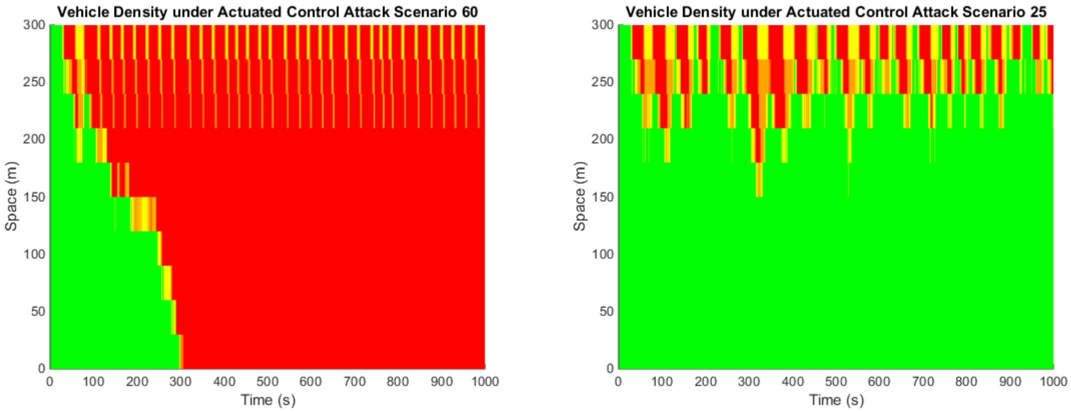


(a) Vehicle Delay Under All Attack Scenarios



(b) Average Total Vehicle Delay by Number of Attacking Phases

FIGURE 13 Vehicle Delay by Attack Scenarios and Number of Attacking Phases (Actuated Control).



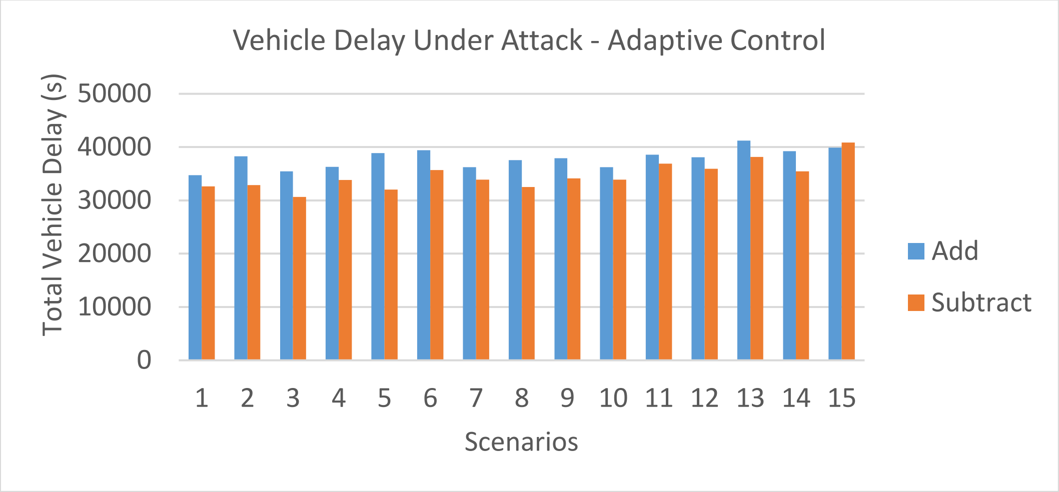
Total Delay: 231193

(a) Actuated control

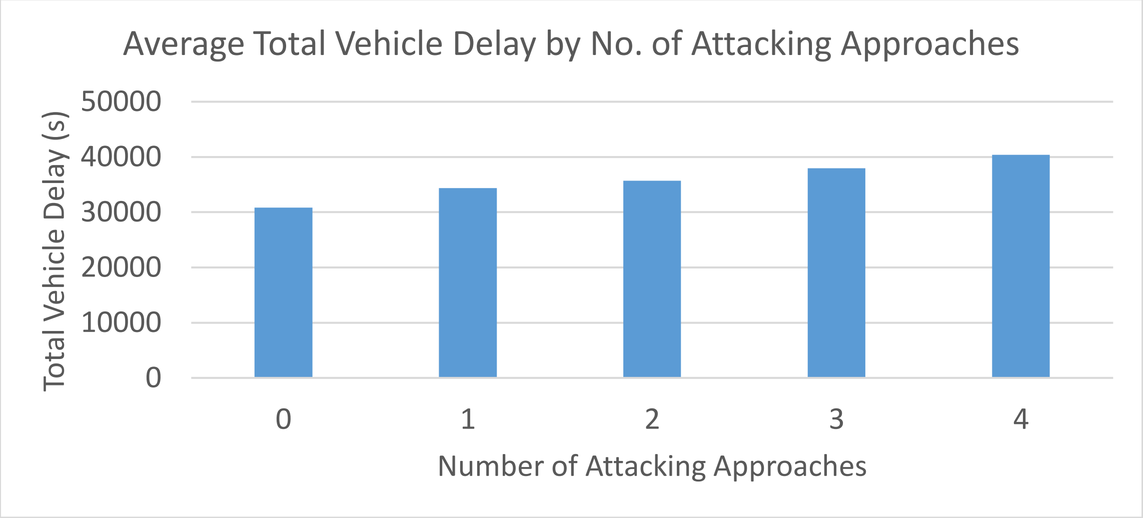
Total Delay: 36441

(b) Adaptive control

FIGURE 14 Comparison between the Most Effective Attack and the Least Effective Attack.



(a) Vehicle Delay under All Attack Scenarios



(b) Average Total Vehicle Delay by Number of Attacking Approaches

FIGURE 15 Vehicle Delay by Attack Scenarios and Number of Attacking Approaches (Adaptive Control).

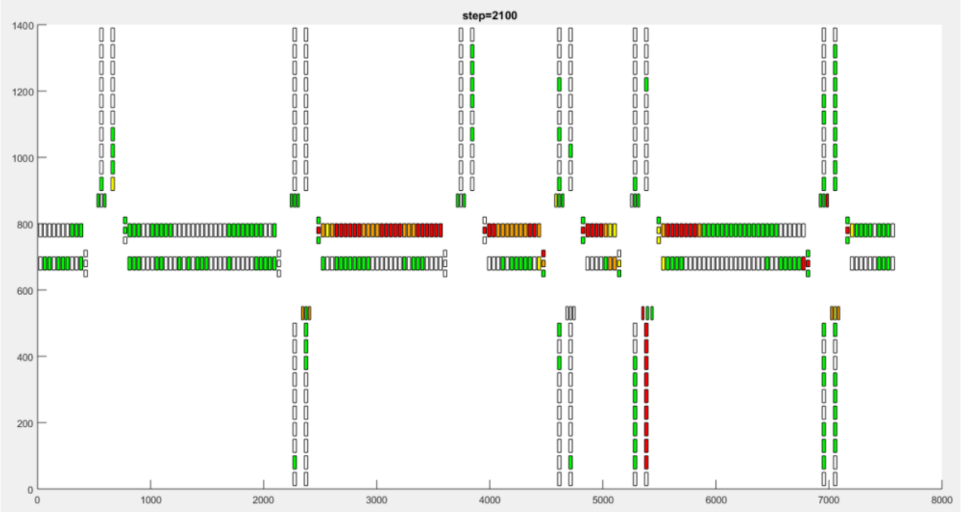


FIGURE 16 Snapshot of the Corridor at the Final Simulation Step.

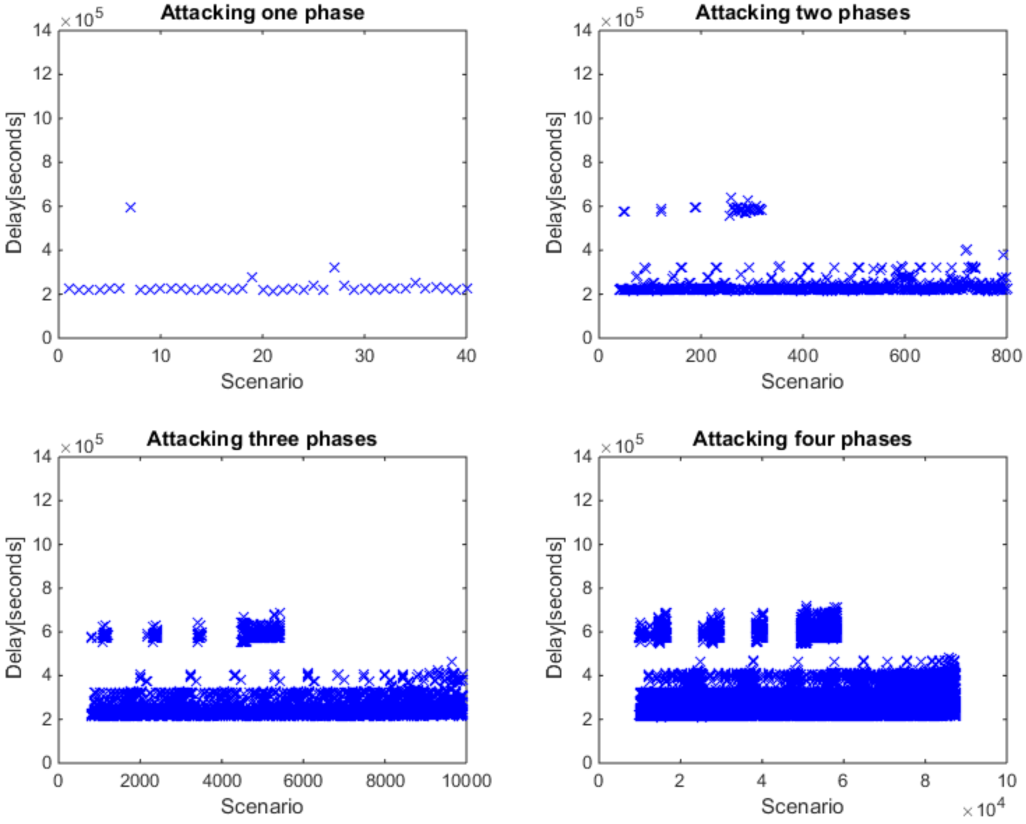


FIGURE 17 Vehicle Delay under All Attack Scenarios.

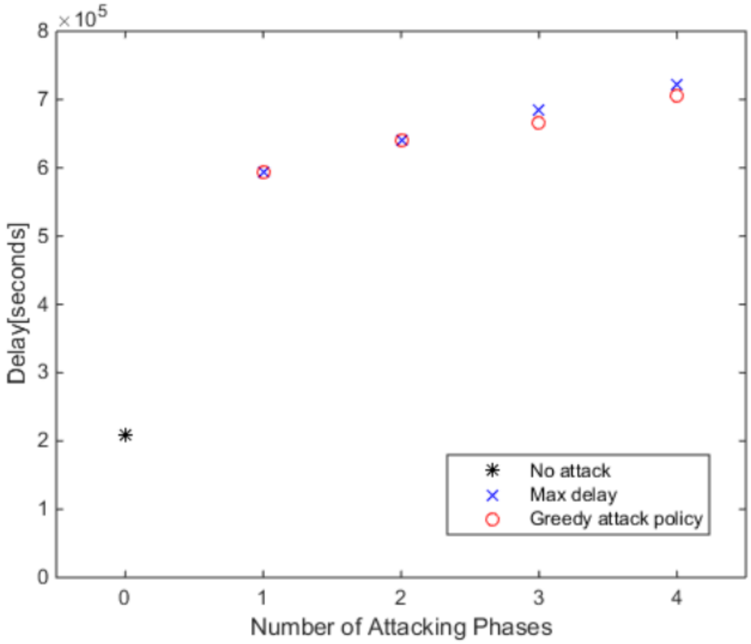


FIGURE 18 Comparison between Enumeration and Greedy Attack Policy.