Falsified Data Attack on Backpressure-based Traffic Signal Control Algorithms

Conference Paper · December 2018

DOI: 10.1109/VNC.2018.8628334

5 authors, including:

Chia-Cheng Yen
University of California, Davis
12 PUBLICATIONS **40** CITATIONS
SEE PROFILE

Dipak Ghosal
University of California, Davis
192 PUBLICATIONS **9,383** CITATIONS
SEE PROFILE

Michael Zhang
Humber College
14 PUBLICATIONS **141** CITATIONS
SEE PROFILE

Falsified Data Attack on Backpressure-based Traffic Signal Control Algorithms

Chia-Cheng Yen[1], Dipak Ghosal[1], Michael Zhang[2], Chen-Nee Chuah[3] and Hao Chen[1]

[1]Department of Computer Science
[2]Department of Civil and Environmental Engineering
[3]Department of Electrical and Computer Engineering
University of California, Davis, CA, USA
Email: {ccyen, dghosal, hmzhang, chuah, chen}@ucdavis.edu

***Abstract*—In urban transportation, scheduling algorithms in traffic signal control (TSC) are important for achieving high throughput and low latency traffic flow, lowering accidents, and reducing emissions. As new scheduling algorithms are being developed particularly to leverage and accommodate connected and autonomous vehicles, there is increased potential for cyber-attacks on TSC that can undermine the benefits of new algorithms. Attackers can learn the behavior of scheduling algorithms and launch attacks to get scheduling priority and/or to create traffic panic and congestion. These attacks can compromise the system and significantly increase traffic delay and make TSC completely ineffective. In this paper, we compare the performance of different backpressure-based scheduling algorithms when they are under attack. We consider four different backpressure-based schemes, namely, delay-based, queue-based, sum-of-delay-based, and hybrid scheme that combines delay-based and queue-based schemes. We consider time spoofing attacks where individual vehicles arriving at an intersection can alter their arrival times. Through detailed simulation analysis we show that while the delay-based scheme has better fairness performance, it is more vulnerable to time spoofing attacks than the other schemes. We explore drawbacks of the delay-based scheme under different scenarios including non-homogeneous arrivals both for isolated intersection as well as multiple intersections. This study throws light on how to prevent time spoofing attacks on next generation TSC.**

***Index Terms*—Traffic signal control, Backpressure-based Scheduling, Time spoofing attacks, Delay distribution, Fairness, Simulation analysis**

I. Introduction

With the ever-increasing number of vehicles, the transportation system faces challenges such as traffic congestion, traffic accidents, and high energy consumption and the related emissions. In order to deal with these critical issues in the transportation systems, a significant body of research in the recent decades has investigated scheduling algorithms for traffic signal control (TSC) [1] [2]. According to data reported in [3], an urban road network equipped with advanced TSC system is capable of not only reducing average travel time of vehicles by 11.4% but also decrease traffic collisions by 6.7%, traffic delay by 24.9%, parking by 27%, while at the same time lower energy consumption. The data revealed the impacts of TSC on our future urban planning.

With connected and autonomous vehicles (CAV), the transportation system can be viewed as a cyber-physical system (CPS) [4] that is able to combine several multi-disciplinary technologies from computation, communication, and control to optimize the transportation system. In such a transportation-based CPS, CAV, and vehicular networks [5] are seamlessly integrated with roadside units and devices like cameras with the TSC. In the foreseeable future, pedestrians, bicyclists, vehicles, and traffic signals, can communicate using Vehicle to Vehicle (V2V), and Vehicle to Infrastructure (V2I) communication. New scheduling algorithms can be implemented in the transportation-based CPS to effectively improve the traffic throughput and delay characteristics. Towards this end, in this paper we consider backpressure-based scheduling algorithms in the TSC.

However, cyber-attacks are potential threats to new scheduling algorithms. In particular, an attack to the system can be launched by sending fake data on the trajectory or arrival time of a vehicle. We show that scheduling algorithms are quite vulnerable to falsified data because the TSC may not be able to efficiently avoid malicious information or easily filter out falsified data. Some researchers have already analyzed the impacts of such time spoofing attacks. In [6] and [7], they conducted the first security analysis on connected vehicle based transportation systems and provided possible attack strategies which could cause serious damage to a TSC. According to their study, they found that the total delay would increase 68% by only one attack. A number of different attacks that could significantly reduce the effectiveness of the TSC is summarized in [8], [9], and [10].

In this paper, we study the performance of scheduling schemes when they are under time spoofing attacks. We implement four different scheduling schemes based on the Backpressure algorithm in the TSC. These are delay-based scheme, queue-based scheme, hybrid scheme that combines delay-based and queue-based, and sum-of-delay-based scheme. The detailed discussion of the first three schemes can be found in [11] which compared the performance of these schemes under different traffic arrival rates. The study also explored the properties of delay-based scheme which can outperform queue-based scheme and provide a better fairness while facing

978-1-5386-9428-2/18/$31.00 ©2018 IEEE

the last vehicle problem. The idea of the last vehicle problem is borrowed from the last packet problem [12], which means that vehicles at a lane whose queue length is comparatively smaller than other lanes could not be served for a long period because the queue-based scheme offers a priority to the lane with larger queue length. We define an attack model in Section III to compromise these schemes. By analyzing the impact of the time spoofing attacks, we hope to discover ways to protect the TSC from cyber-attacks. The main contributions of this paper are summarized below:

- Through a detailed simulation analysis, we have analyzed the impact of time spoofing attacks on four different backpressure-based scheduling schemes. The analysis is based both on a single intersection as well as multiple-intersections under homogeneous and heterogeneous arrivals.
- We show that while delay-based backpressure scheme has good performance properties compared to queue-based scheme, it is more vulnerable to time spoofing attacks than queue-based scheme. A hybrid scheme that combines queue-based and delay-based schemes can be used to switch to queue-based scheduling when the attack is detected.
- We show that for a network of intersections, the knowledge of the heterogeneity in the arrivals can be exploited to magnify the impact of the time spoofing attack in the case of delay-based scheduling scheme.

The rest of this paper is organized as follows. In Section II, we introduce our TSC model for isolated intersection and multiple intersections. We also describe four different backpressure-based scheduling schemes. In Section III, we discuss the threat model. In Section IV, we discuss the results of the impact of the time spoofing attack in terms of the delay distribution and the fairness index for the four different scheduling schemes. Finally, we conclude and discuss future work in Section V.

II. Background

A. Backpressure

The backpressure routing algorithm was originally developed to optimize the throughput of a queuing network over a multi-hop radio network with random arrival rates [13]. In their work, they characterized a stability region that defines the region of arrival rate and service rates within which feasible policies exists such that the network is stable. They also found an optimal policy that achieves maximum throughput. The original work on backpressure control has been extended in the domain of wireless communication networks [12], [14], [15], and [16].

The concept of the backpressure was first applied to traffic signal control in [17]. They summarized some important definitions for network stability to aid in the modeling of the traffic network. In their algorithm, they considered the difference in the queue length between any two adjacent nodes in each time slot and then determined a feasible schedule by giving priority to the phase with the maximum difference. In this algorithm, at each intersection in each time slot, the decision regarding which phase of the traffic movement is scheduled is independently determined based on the queue length. The results show that the algorithm can achieve maximum network throughput and global optimality without any prior knowledge about arrival rates.

However, in practice, there exists a weakness for an algorithm that only takes queue length information into account. In [12] they addressed that the queue-based scheme suffers from larger delay when encountering the last packet problem in wireless networks. They proved that there is a linear relationship between queue lengths and delays in the fluid limit model. That is, for each link-flow-pair (s, k), $q_{s,k}(t) = \lambda_s w_{s,k}(t)$, they showed that the queue length grows when the delay becomes longer. This implies that the delay-based backpressure scheme is quite similar to the queue-based backpressure scheme. However, the delay-based scheme outperforms the queue-based scheme for the last packet problem.

Based on their work, we applied the delay-based backpressure traffic signal control scheme at an isolated intersection in [11] for solving the last vehicle problem. Besides, we further proposed a hybrid scheme that considers both queue and delay information and acquires the advantages of both the schemes. It can switch between the two methods using a tuning parameter. Depending on different traffic situations, the parameter determines whether the scheme behaves closer to the queue-based scheme or the delay-based scheme. We introduce other type of schemes in detail in Section II-C.

B. System Model

We assume an anonymous authentication scheme to deliver messages to the TSC system because we want to concentrate on misbehaviors for personal benefits in this paper. Our TSC system is a centralized scheduling system that receives messages from arriving vehicles and is equipped with four different scheduling schemes for optimizing decisions. Except for this central server, there are no other apparatuses for detecting the number and arrival times of vehicles. As shown in Fig. 1, vehicles will send a message to indicate their arrivals when they approach an intersection. Therefore, the system is fully aware of the number of vehicles by counting the number of messages and the arrival time of each individual vehicle in each lane. The system will consider the number of vehicles as the queue length and arrival time of the head vehicle as the Head-Of-Line (HOL). Our experiments analyze the impact of the time spoofing attack, which attackers (red vehicles) will send falsified arrival data to the system in order to disable the scheduling ability of the system. Other types of attacks such as DoS, Masquerade, GPS spoofing attack are not considered in this paper.

In our experiments, we model our TSC system at both an isolated intersection and multiple connected intersections by a queuing network with vertices and edges. Let $G = (V, E)$ be a directed graph where V indicates a set of vertices corresponding to different lanes and E denotes a set of edges

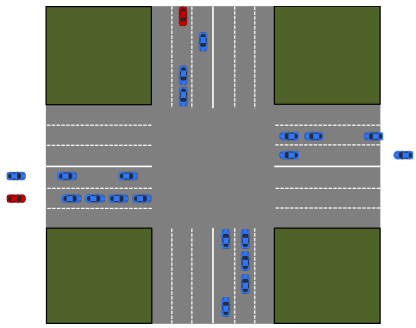


Fig. 1: The illustration of waiting vehicles and approaching vehicles at an isolated intersection.

corresponding to traffic movements between any connected lanes. Fig. 2 shows an example of 4 phases at an isolated intersection. In our simulations, we assume that each vehicle has a fixed routing path and this routing information is known beforehand.

Let $A_i(t)$ be the number of vehicles that arrives to the network in lane i at time slot t. It can be formulated as follows:

$$\lim_{t\to\infty}\frac{1}{t}\sum_{\tau=0}^{t-1}\mathbb{E}(A_i(\tau))=\lambda_i \tag{1}$$

where λ_i is an average arrival rate in lane i. Let $\vec{\lambda}=\{\lambda_1,\lambda_2,\ldots,\lambda_{|V|}\}$ be an arrival rate vector of the network. Let $Q_{i,j}(t)$ be the number of vehicles in lane i at the beginning of time slot t and will transfer to lane j. Here, we also use $Q_{i,j}$ to represent queue itself and $\vec{Q}(t)\triangleq[Q_{i,j}(t),(i,j)\in E]$ is the queue length vector at time slot t. Let $F_{i,j}(t)$ be the number of vehicles arriving in lane i for lane j until time slot $t\geq 0$, and $\hat{F}_{i,j}$ be the number of vehicles served at $Q_{i,j}$ until time slot $t\geq 0$. Based on the above, the queue length is given by:

$$Q_{i,j}(t)=F_{i,j}(t)-\hat{F}_{i,j} \tag{2}$$

Let $T_{i,j,k}(t)$ represent the sojourn time of k-th vehicle of $Q_{i,j}$ in the network at time slot t where this time is measured from the time when this vehicle arrives in the network. Let $W_{i,j}(t)$ be the sojourn time of the HOL vehicle of $Q_{i,j}$ in the network at time slot t. Therefore, $W_{i,j}(t)\triangleq T_{i,j,1}(t)$ and if $Q_{i,j}(t)=0$, it implies $W_{i,j}(t)=0$. Likewise, $\vec{W}(t)\triangleq[W_{i,j},(i,j)\in E]$ indicates the HOL sojourn time vector at time slot t.

$$U_{i,j}\triangleq t-W_{i,j}(t) \tag{3}$$

We define $U_{i,j}$ to be the time when the first vehicle (HOL) of $Q_{i,j}$ arrives in the network. A feasible schedule is a set of movements that can be scheduled concurrently. This is denoted as $\vec{p}\in\{0,1\}^{|E|}$. Let S_P be a set of all feasible schedules, e.g., vehicles are allowed passing from lane i to lane j at time slot t if $p_{i,j}(t)=1$. Otherwise, vehicles cannot move from lane i to lane j if $p_{i,j}(t)=0$. We use $\mu_{i,j}(\vec{p})$ to represent a transmission rate that vehicles move from lane i to lane j under a feasible schedule $\vec{p}$. We summarize all notations in Table I.

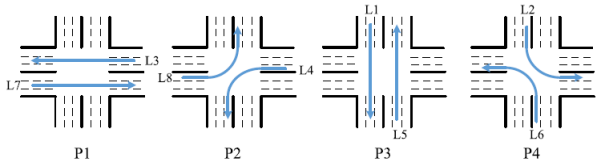


Fig. 2: The 4 phases for each intersection in our simulation.

TABLE I: Summary of Notations

Symbol	Description
$\mathcal{V}$	set of vertices (different lanes)
$\mathcal{E}$	set of edges (traffic movements between any two lanes)
$\vec{p}$	a schedule (movements that can be scheduled concurrently)
$\mathcal{S}_\mathcal{P}$	a set of feasible schedules
$\mu_{i,j}(\vec{p})$	transmission rate that vehicles move from lane i to lane j under a feasible schedule $\vec{p}$
$A_i(t)$	number of vehicles arriving to the network for lane i at time slot t
λ_i	average arrival rate for lane i
$Q_{i,j}(t)$	queue length of $Q_{i,j}$ at time slot t
$F_{i,j}$	number of vehicles arriving in lane i for lane j until time slot t
$\hat{F}_{i,j}$	number of vehicles served at $Q_{i,j}$ until time slot t
$T_{i,j,k}$	the sojourn time of the k-th vehicle of $Q_{i,j}$ in the network at time slot t
$W_{i,j}(t)$	sojourn time of the HOL vehicle of $Q_{i,j}$ in the network at time slot t
$U_{i,j}$	time when the HOL vehicle of $Q_{i,j}$ arriving in the network

C. Scheduling Schemes for Traffic Signal Control

In this section, we introduce four different scheduling schemes based on the Backpressure [12] and [11]. They are queue-based, delay-based, hybrid, and sum-of-delay-based scheduling schemes. Each of them determines an optimal phase at every time slot t by giving the priority to the lanes with the maximum pressure according to the factors they take into account, e.g., queue lengths, or delays. Therefore, they are able to schedule feasible movements to achieve maximum throughput. We describe the scheduling policies in the following subsections.

a) Queue-based Backpressure Scheduling Scheme: The formula of queue-based scheduling scheme that selects an optimal phase in each time slot t is given as follows:

$$\vec{p}^*(t)\in\underset{\vec{p}\in\mathcal{S}_\mathcal{P}}{\operatorname{argmax}}\sum_{P_{i,j}=1}\gamma_{i,j}\cdot Q_{i,j}(t)\cdot\mu_{i,j}(\vec{p}) \tag{4}$$

This formula calculates the sum of queue length multiplied by two weighted values $\gamma_{i,j}$ and $\mu_{i,j}(\vec{p})$. For vehicles from lane i to lane j, $(i,j)\in\mathcal{E}$, $\gamma_{i,j}$ is a positive constant that can put different emphases on movements. The other factor $\mu_{i,j}(\vec{p})$ denotes a traffic flow of vehicles that can be transferred through the connected edge when phase $\vec{p}$ is activated. Then, finally, this scheme will return a phase that maximizes the total pressure released.

b) Delay-based Backpressure Scheduling Scheme: The formula of delay-based scheduling scheme that selects an optimal phase in each time slot t is given as follows:

$$\vec{p}^*(t) \in \underset{\vec{p}\in\mathcal{S}_\mathcal{P}}{\operatorname{argmax}} \sum_{P_{i,j}=1} \gamma_{i,j} \cdot W_{i,j}(t) \cdot \mu_{i,j}(\vec{p}) \tag{5}$$

This formula calculates the sum of HOL vehicle sojourn time multiplied by two weighted values $\gamma_{i,j}$ and $\mu_{i,j}(\vec{p})$. As before, for vehicles from lane i to lane j, $(i,j) \in \mathcal{E}$, $\gamma_{i,j}$ is a positive constant that can put more emphasis on certain movements and $\mu_{i,j}(\vec{p})$ denotes a traffic flow of vehicles that can be transferred through the connected edge when phase $\vec{p}$ is activated. The scheme will return a phase that maximizes the total pressure released.

c) Hybrid Backpressure Scheduling Scheme: The formula of hybrid scheduling scheme that selects an optimal phase in each time slot t is given as follows:

$$\vec{p}^*(t) \in \underset{\vec{p}\in\mathcal{S}_\mathcal{P}}{\operatorname{argmax}} \sum_{P_{i,j}=1} \gamma_{i,j} \cdot [\eta_{i,j}^{(W)} W_{i,j}(t) + \eta_{i,j}^{(Q)} Q_{i,j}(t)] \cdot \mu_{i,j}(\vec{p}) \tag{6}$$

Based on both queue length and delay information, hybrid scheduling scheme can behave flexibly between queue-based and delay-based scheme by tuning two parameters, $\eta_{i,j}^{(W)}$, $\eta_{i,j}^{(Q)} \in [0,1]$. This design can be adjusted depending on the relative importance between queue length and delay. Therefore, the formula can calculate the sum of queue length and HOL vehicle sojourn time. It is able to determine to get closer to queue-based or delay-based scheme by using different $\eta_{i,j}^{(W)}$ and $\eta_{i,j}^{(Q)}$. Additionally, it also uses two weighted values $\gamma_{i,j}$ and $\mu_{i,j}(\vec{p})$. The definitions of these are the same as in the delay-based and queue-based schemes.

For a simple instance, we let $\eta_{i,j}^{(W)}$ be larger compared to $\eta_{i,j}^{(Q)}$ when a traffic arrival rate from lane i to lane j is low because we have to guarantee the fairness of the delay performance. Similarly, we let $\eta_{i,j}^{(Q)}$ be larger when a traffic arrival rate from lane i to lane j is high because the queue length need to be limited.

d) Sum-of-delay-based Backpressure Scheduling Scheme: Let $\overline{W}_{i,j}(t)$ be the sum of the sojourn time of all vehicles from lane i to lane j at time t where $T_{i,j,k}(t)$ is the sojourn time of the k-th vehicle of $Q_{i,j}$ at time t. Then, we have the sum-of-delay as follows:

$$\overline{W}_{i,j}(t) = \sum_{k=1}^{n} T_{i,j,k}(t) \tag{7}$$

Compared to the delay-based scheme, the sum-of-delay scheme considers not only HOL sojourn time but all sojourn times of vehicles from lane i to lane j, it determines an optimal phase in each time slot t by all vehicles.

$$\vec{p}^*(t) \in \underset{\vec{p}\in\mathcal{S}_\mathcal{P}}{\operatorname{argmax}} \sum_{P_{i,j}=1} \gamma_{i,j} \cdot \overline{W}_{i,j}(t) \cdot \mu_{i,j}(\vec{p}) \tag{8}$$

This formula calculates the sum of all sojourn times of vehicles multiplied by the same factors $\gamma_{i,j}$ and $\mu_{i,j}(\vec{p})$. As for the other schemes, it will return a phase that maximizes the total pressure released.

e) Scheduling Adaption for Multiple Intersection: The old metrics of queue length and delay are no longer suitable for requirements of multiple intersections. In order to capture traffic flows and guarantee the linear relation between queue lengths and delays at multiple intersections, according to [12] and [18], we need to redesign our schemes by applying new metrics introduced in [12] to further adapt to multiple intersections. Thus, instead of utilizing the old metrics, we apply the queue differential $\Delta Q_{u,i}$ and the delay differential $\Delta W_{u,i}$ where u denotes the u-th intersection and i, j represent different lanes. By applying these new metrics, scheduling scheme will schedule for the one with the maximum differential pressure as defined below:

$$\Delta Q_{u,i} \triangleq Q_{u,i}(t) - Q_{u+1,j}(t) \tag{9}$$

$$\Delta W_{u,i} \triangleq \hat{W}_{u,i}(t) - \hat{W}_{u+1,j}(t) \tag{10}$$

$$\hat{W}_{u,i} \triangleq W_{u,i}(t) - W_{u-1,j}(t) \tag{11}$$

III. Attack Model

In order to model a realistic attack scenarios, we hypothesize that there are multiple attackers arriving to an isolated intersection containing 8 lanes with different arrival rates and a multiple consecutive intersections with different arrival rates. The number of attackers is randomly distributed in 8 traffic lanes. Each driver could be a potential attacker who will attempt to compromise our system by spoofing its arrival time. They can either benefit from getting scheduled earlier than other vehicles that arrived before or paralyze the entire traffic to create chaos. In [6], they found that spoofing data is an effective strategy which causes serious delays for the TSC. Therefore, in this paper, we use the same definition of 'spoofing' as in [6], i.e., instead of masquerading as another vehicle by a fake ID, the attacker sends fake data such as arrival time. Based on this scenario, we define parameters for modeling a behavior of each attacker. Furthermore, we consider a complicated attacking strategy called a coordinated attack in which multiple attackers will work together to cripple the TSC.

A. Parameters

For evaluating the performance of each scheduling scheme when it is under attack, we set two adjustable parameters, attack ratio ρ and spoofing time σ where ρ indicates the rate that attackers could appear at the intersection and σ denotes the time (in second) that each attacker arrived at T_{actual} but he could spoof to our system by sending a spoofed time given by

$$T_{spoofed} = T_{actual} - \sigma \tag{12}$$

We let Φ be the total number of attackers such that

$$\Phi = \rho \sum_{\tau=0}^{t} A_i(\tau) \tag{13}$$

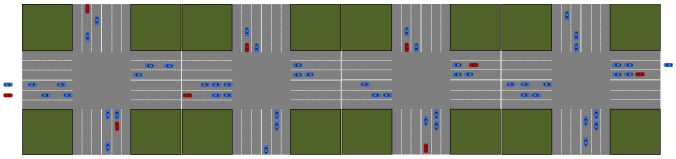


Fig. 3: The illustration of waiting vehicles and approaching vehicles at multiple intersections.

IV. Experimental Results

In this section, we discuss the results of the time spoofing attacks on the isolated and multiple intersections. All simulations for isolated intersection are based on above 4 phases mentioned in Fig 2. For simulations of multiple intersections, we only consider one row with four intersections containing simpler phases consisting of horizontal and vertical directions, e.g., Phase 1 and Phase 3 in Fig 2.

Based on [17] and our previous work [11], the traffic flow during time slot t is $R_m(1-e^{-\frac{Q(t)+I^a(t)}{R_m}})$ where $R_m = \mu_s T_s$ denotes the maximum value of the traffic flow, $Q(t)$ represents the queue length of this lane at the beginning of this time slot t, and $I^a(t)$ indicates the amount of the traffic flow reaching in this lane during time slot t. For our simulations, the parameter μ_s is 0.5 and T_s is 5s for every lane shown in Fig 2.

For evaluating the performance after attacks, we apply the Jain's fairness index [19] which is given by

$$f(\vec{d} = [d_1, d_2, \ldots, d_M]) = \frac{(\sum_{i=1}^{M} d_i)^2}{M \sum_{i=1}^{M} (d_i)^2} \tag{14}$$

where d_i indicates the delay of each vehicle i and M represents the total number of vehicles. The main idea of Jain index is to compare the total delay to individual delay. Hence, it divides the square of total delay by the sum of each square of individual delay. As the denominator becomes smaller, which means the delay of individual vehicle becomes lower as well, the f will increase. The system achieves a better fairness if Jain index is higher.

In the following paragraphs, we discuss the impact of the attacking strategies in several situations such as different traffic flows and multiple intersections. We organize figures for no attack first, followed by figures for when under attack, and then, figures for fairness. The entire simulation time is 10 hours and the time slot t is 5 second. By analyzing these patterns, we compare the impact of different strategies.

A. Random attack at an isolated intersection with homogeneous arrival rates

We first consider the isolated intersection. The arrival rates in 8 lanes at this intersection are homogeneous arrival rates using Poisson process. We set parameters $\vec{\lambda} = [1,1,1,1,1,1,1,1] * 0.125$ v/s/l (vehicles per second per lane) and attack ratio $\rho = 0.001$ (one attacker per thousand vehicles). Based on a long period simulation, there are thousands of vehicles approaching, $\rho = 0.001$ is sufficient to create traffic jams and compromise the system. For this case, we assume that each attacker is able to spoof its arrival time once in one lane at any time whenever it is approaching to this lane. Consequently, during the entire simulation, we consider a random attack pattern with the number of attackers in each lane can be defined by the equation (13) and the spoofed time is defined by equation (12) where σ is fixed to 500 seconds. The performance results of four scheduling schemes without attack and under attack are shown in Fig. 4.

Fig. 4a shows the delay performance of the four scheduling schemes. We observe that they perform almost the same and the delay-based scheme is slightly better than others because it can solve the last vehicle problem effectively. Fig. 4b shows the number of times each phase is selected by the four different scheduling algorithms as given in equations (4), (5), (6), and (8). The reason why the number of times each phase is scheduled by the queue-based scheme becomes unbalanced is because the queue length is based on the number of vehicles in the lane which is an integer. Hence, under the same arrival rate, the probability that queue lengths of different lanes are the same is high. When encountering this problem, we do not deal with balancing the four phases since optimizing the performance is not our first priority in this paper.

However, after being attacked, in Fig. 4e, we note that phases scheduled by the delay-based scheme vary much more than phases scheduled without attack. The number of times that the delay-based scheme schedules phase 2 is increased from 1794 to 1838 and phase 4 is increased from 1799 to 1822, which means attackers indeed compromised our system by spoofing their arrival times. When priority should be given for other phases, e.g., phases 1 and 3 is now taken away by the lane with attackers. By spoofing the system, attackers can acquire more scheduling times from victimized lanes. As a result, they can get scheduled quicker than other vehicles. We call this phenomenon **priority plundering**. The delay performance in Fig. 4d shows that the delay-based scheme is vulnerable to time spoofing attacks.

In addition, the priority plundering is also observed for the sum-of-delay-based and hybrid schemes. The variations are not as much as the delay-based scheme because they not only take the waiting time into account but also other factors. For example, the sum-of-delay-based scheme considers all waiting times of all vehicles and the hybrid scheme considers both the delay and the queue length. As a result, only a few attackers do not impact their performance. As a result, they can tolerate higher attack rate than the delay-based scheme.

Jain's fairness index shows the fairness without attack and under attack in Fig. 4c and 4f, respectively, where α represent the traffic load. For the delay-based scheme, after being attacked, we can observe that the fairness drops more than others. The fairness of sum-of-delay-based and hybrid schemes do drop slightly, but the influence is not as large as

for the delay-based scheme since the waiting time is just one of factors they consider. We note that the queue-based is not affected since it only takes the queue length into account and not the waiting time.

B. Coordinated attack at an isolated intersection with asymmetric arrival rates

Next, we study the case of asymmetric traffic arrival rates in 8 lanes at an isolated intersection. Specifically, we consider higher arrival rates in horizontal direction (lanes 3, 4, 7, 8) and lower arrival rates in vertical direction (lanes 1, 2, 5, 6). The parameters we use are $\vec{\lambda} = [0.2, 0.2, 1, 1, 0.2, 0.2, 1, 1] * 0.125$ v/s/l, the number of attackers is $\Phi = 5$, and spoofing time is 500 seconds.

In this scenario, instead of using random attack pattern, we investigate the impact of coordinated attack to our system. This means the attackers could possibly work as a team, trying to figure out weaknesses of the system. Under this assumption, they could attack together from the specific lanes. Hence, we first fix the number of attackers in lanes with lower arrival rates and limit attacks to only appear in these lanes. Then, we fix the number of attackers in lanes with higher arrival rates and limit attacks to only appear in the corresponding lanes. We compare the attacks from these two directions to see whether attackers can benefit from such attacking strategies.

Before discussing the results for the different attack strategies, we first look at Fig. 5a and 5d that show the performance of each scheduling scheme without attack. Compared to homogeneous arrivals, the delay-based scheme reveals it's advantage when confronting asymmetric arrivals. Because non-homogeneous arrivals will enhance the last vehicle problem from which the queue-based scheme suffers; hence, the delay-based scheme can outperform it very much. Mention to sum-of-delay-based and hybrid schemes, the former works similar to the delay-based because it considers all delays of all vehicles. The later utilizes the queue length as well as delay and we can decide to make it closer to the queue-based or the delay-based scheme by adjusting the parameter η. However, they both take multiple factors into account whenever making decision. As a result, asymmetric arrivals do not affect them very much.

Results for the case under attack are shown in Fig. 5c, 5e, and 5f. It is observed that attacks from lanes with lower arrival rates can lengthen the total delay of delay-based scheme. The number of times for phase 3 scheduled by the delay-based scheme increases from 1005 to 1152 and the number of times for phase 1 scheduled by the delay-based scheme reduces from 2602 to 2596 after being attacked in Fig. 5e compared to 5b. The lanes with higher arrival rates (lanes 3, 4, 7, 8) should have more scheduling times originally, but the priority is plundered by attackers in lanes with lower arrival rates. We observe that attackers can benefit from attacking in lanes with lower arrival rates. For phase 3 scheduled by the delay-based scheme (red bar in Fig. 5e), the increasing amount of times gained by spoofing in lower arrival lanes is 147 which is higher than 111 if they had spoofed from the higher arrival lanes. The sum-of-delay-based and hybrid schemes do not increase like the delay-based scheme. Hence even if they have coordinated attacks from the lower arrival lanes, it will not affect these schemes significantly.

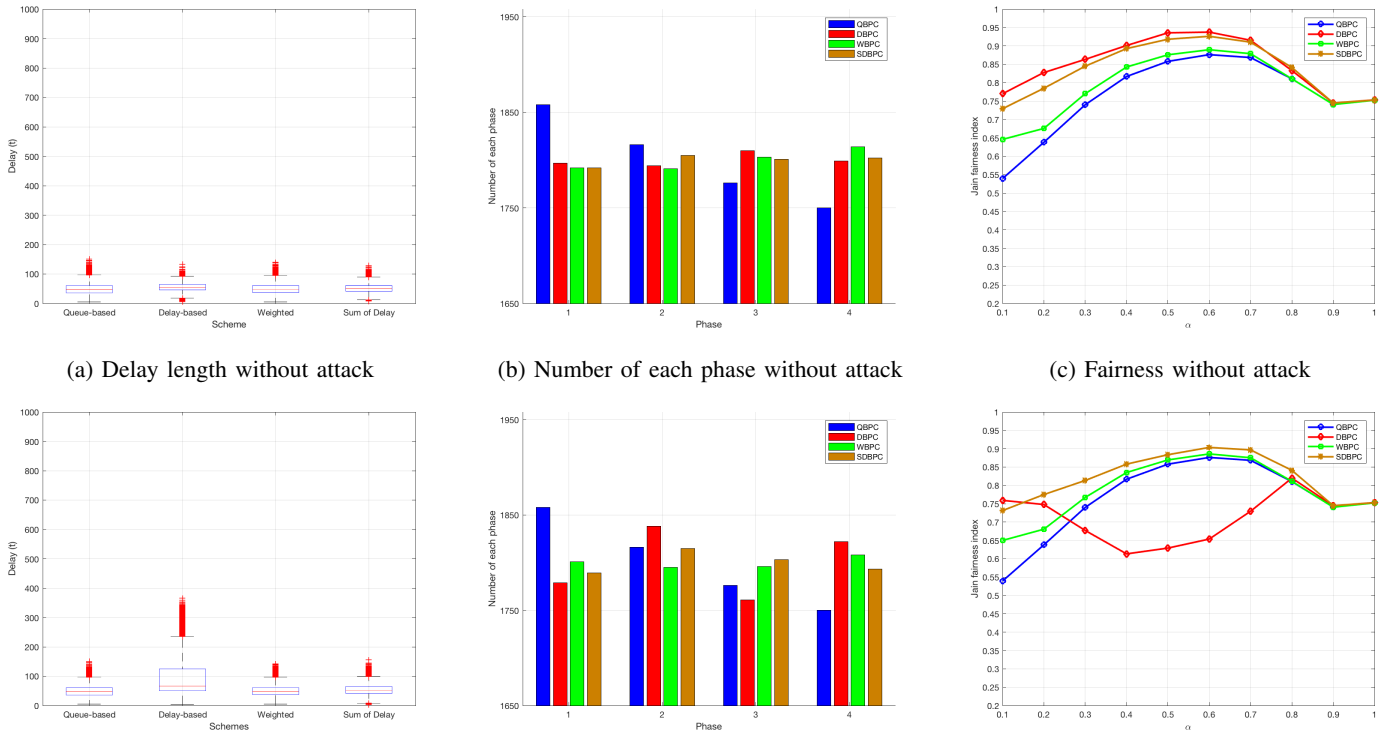
Furthermore, we compare the fairness of being attacked in lanes with higher arrival rates and lanes with lower arrival rates in Fig. 5c and 5f, respectively. The fairness of the sum-of-delay-based and hybrid schemes does not drop very much. But for the delay-based scheme, the results show that the fairness of being attacked in lanes with lower arrival rates (lanes 1 and 5) drops more than when the attack is launched from lanes with higher arrival rates (lanes 3 and 7). We also study the case of asymmetric traffic arrival rates in which the horizontal direction is low and vertical direction is high. Our results show that the same behavior that attackers can gain more scheduling times by spoofing in lanes with lower arrival rates than in lanes with higher arrival rates.

C. Coordinated attack at multiple intersections with homogeneous arrival rates

Using equations (9), (10), (11), we can redesign the four scheduling schemes for multiple intersections. As shown in Fig. 3, our simulation study is based on one row of four consecutive intersections. We focus on the traffic congestion at multiple intersections since vehicles are not just routing at a single one; hence, we construct our scenario that simplifies potential traffic directions within a single intersection rather than many complicated routes, eliminates the number of lanes from 8 to 4 (only lane 1, 3, 5, and 7 are activated).

We study the case of homogeneous traffic arrival rates in the 4 lanes at multiple intersections; each intersection has the same arrival rate $\vec{\lambda} = [1, 0, 1, 0, 1, 0, 1, 0] * 0.125$ v/s/l. We set attack ratio $\rho = 0.001$ and spoofing time is 500 seconds. Attackers are able to spoof even if they have already crossed the intersection and have entered the next one. This attack behavior will increase the total delay and cause a significant performance degradation. We observed (plots are not shown due to space limitations) that in the case of multiple intersections the total delay for the delay-based scheme increases compared to the isolated intersection (shown in Fig. 4d). Similarly, sum-of-delay-based and hybrid schemes are only slightly affected. Furthermore, the fairness of the delay-based scheme also drops rapidly compared to the case of the isolated intersection, especially when traffic load increases.

We also observed (not shown here due to space limitation) that attackers can compromise scheduling system by attacking from lanes with lower arrivals. Due to the lower arrivals (in lanes 3 and 7), **priority plundering** occurs at multiple intersections resulting in even worse performance. The number of times phase 1 is allocated for the delay-based scheme increased from 3121 to 3604. This corresponds to an increase of 15.4% compared to the isolated intersection case. The Jain's fairness index in Fig. 6 and 7 shows the attacks in vertical direction (lanes 1 and 5) and horizontal direction (lane 3 and 7), respectively. The fairness (attacking from lanes 3 and 7) for



(a) Delay length without attack (b) Number of each phase without attack (c) Fairness without attack

(d) Delay length under attack (e) Number of each phase after being attacked (f) Fairness after being attacked

Fig. 4: Performance comparison among four backpressure based scheduling schemes for homogeneous traffic flows at an isolated intersection.

the delay-based scheme is significantly lower than the fairness under attack from higher arrivals (lanes 1 and 5).

V. Conclusion and Future Work

We presented a study on the impact of time spoofing attacks on different backpressure-based scheduling algorithms in single and multiple intersections under both homogeneous and heterogeneous arrivals. We showed that the delay-based scheme is more vulnerable to time spoofing attacks compared to the sum-of-delay-based scheme. In addition, the hybrid scheme that combines delay-based and queue-based can withstand attacks if the weighting parameter can be properly adapted to force it to schedule phases to be more similar to the queue-based scheme when under attack. However, attacks other than the time spoofing attack studied in this paper can also be launched against TSC in general and the scheduling algorithm in particular. As a future work, we will perform a thorough vulnerability analysis of a network of TSCs and study the robustness of different scheduling algorithms and methods to mitigate the attacks.

References

[1] F. V. Webster, "Traffic signal setting," Road Res. Lab., HMSO, London, U.K., Tech. Paper 39, pp. 1–44, 1958.

[2] A. J. Miller, "Settings for fixed-cycle traffic signals," Oper. Res. Q., vol. 14, no. 4, pp. 373–386, 1963.

[3] D. Zhao, Y. Dai, and Z. Zhang, "Computational Intelligence in Urban Traffic Signal Control: A Survey," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) vol. 42, no. 4, pp. 485-494 July 2012.

[4] R. Baheti, and H. Gill, Cyber-physical systems. The impact of control technology, pp. 161-166, 2011.

[5] E. Uhlemann, "Introducing connected vehicles [connected vehicles]," IEEE Veh. Technol. Mag., vol. 10, no. 1, pp. 23–31, Mar. 2015.

[6] 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," Network and Distributed Systems Security (NDSS) Symposium, Feb. 2018.

[7] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, Z. M. Mao, "Vulnerability of Traffic Control System under Cyber-Attacks Using Falsified Data," 97th Annual Meeting of the Transportation Research Board, Jan. 2018.

[8] M. Raya, and J. Hubaux, "The security of vehicular ad hoc networks," in Proc. 3rd ACM Workshop Security of Ad Hoc Sensor Netw., Alexandria, VA, Nov. 2005, pp. 11–21.

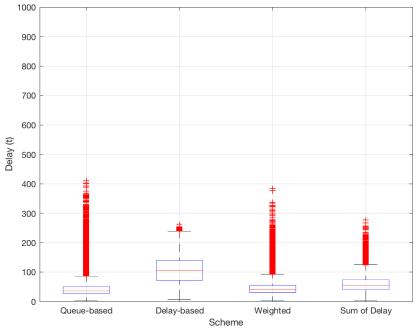
[9] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANET Security Challenges and Solutions: A Survey," Veh. Commun., vol. 7, pp. 7–20, 2017.

[10] F. Sakiz, and S. Sen, "A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV," Ad Hoc Netw., vol. 61, pp. 33–50, 2017.

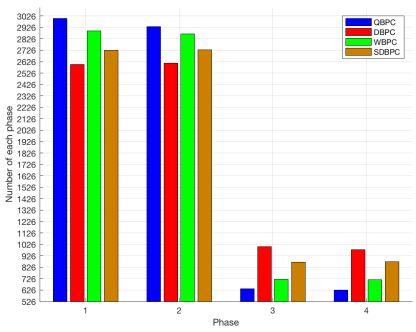
[11] J. Wu, D. Ghosal, M. Zhang, and C.-N. Chuah, "Delay-based Traffic Signal Control for Throughput Optimality and Fairness at an Isolated Intersection," IEEE Transactions on Vehicular Technology, vol. 67, no. 2, pp. 896–909, Feb. 2018.

[12] B. Ji, C. Joo, and N. B. Shroff, "Delay-based back-pressure scheduling in multihop wireless networks," IEEE/ACM Trans. Netw., vol. 21, no. 5, pp. 1539–1552, Oct. 2013.

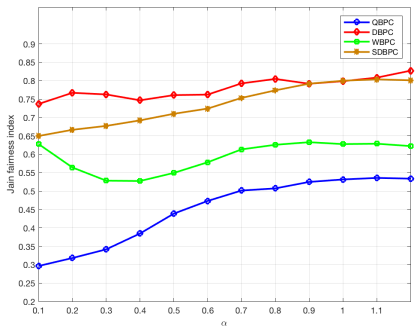
[13] L. Tassiulas, and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in



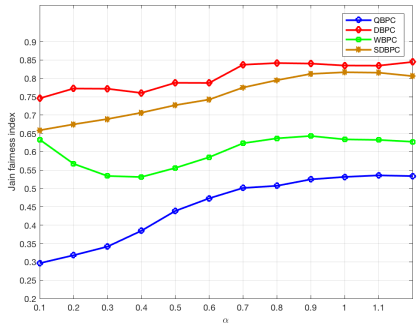
(a) Delay length no attack



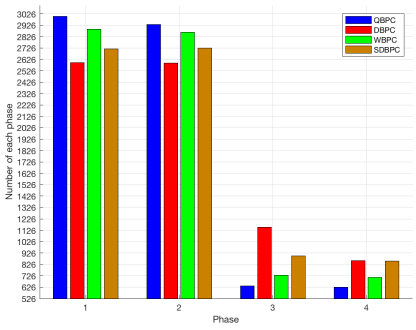
(b) Number of each phase no attack



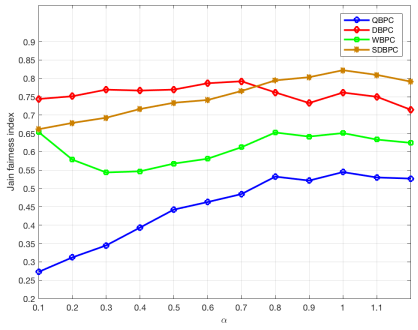
(c) Fairness after being attacked by lane 3 and 7



(d) Fairness without attack



(e) Number of each phase under attack



(f) Fairness after being attacked by lane 1 and 5

Fig. 5: Performance comparison among four backpressure based scheduling schemes for asymmetric traffic flows at an isolated intersection.

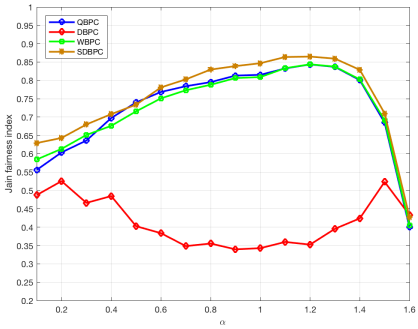


Fig. 6: Fairness comparison of the four scheduling schemes after being attacked by lanes 1 and 5 (higher arrivals).

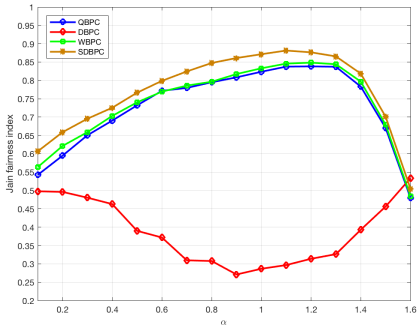


Fig. 7: Fairness comparison of the four scheduling schemes after being attacked by lanes 3 and 7 (lower arrivals).

multihop radio networks," IEEE Trans. Automat. Control, vol. 37, no. 12, pp. 1936–1948, Dec. 1992.

[14] M. J. Neely, E. Modiano, and C. E. Rohrs, "Dynamic power allocation and routing for time-varying wireless networks," IEEE J. Sel. Areas Commun., vol. 23, no. 1, pp. 89–103, Jan. 2005.

[15] M. J. Neely, and R. Urgaonkar, "Optimal backpressure routing for wireless networks with multi-receiver diversity," Ad Hoc Netw., vol. 7, no. 5, pp. 862–881, 2009.

[16] A. Sinha, and E. Modiano, "Optimal control for generalized network-flow problems," in Proc. IEEE Conf. Comput. Commun., 2017, pp. 1–9.

[17] T. Wongpiromsarn, T. Uthaicharoenpong, Y. Wang, E. Frazzoli, and D. Wang, "Distributed traffic signal control for maximum network throughput," in Proc. 15th Int. IEEE Conf. Intell. Transp. Syst., 2012, pp. 588–595.

[18] A. Sinha, G. Paschos, Chih-Ping Li, and E. Modiano, "Throughput-Optimal Multihop Broadcast on Directed Acyclic Wireless Networks," IEEE/ACM Transactions on Networking, vol. 25, no. 1, Feb. 2017.

[19] R. Jain, D.-M. Chiu, and W. R. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer system," Eastern Research Lab., Digital Equipment Corporation, Hudson, MA, USA, Rep. no. TR-301, vol. 38, 1984.