Transportation Research Part B 139 (2020) 473–495

Contents lists available at ScienceDirect

Transportation Research Part B

journal homepage: www.elsevier.com/locate/trb

Security analysis for fixed-time traffic control systems☆

Anthony Lopez[a,*], Wenlong Jin[b], Mohammad Abdullah Al Faruque[a]

[a] Embedded and Cyber-Physical Systems Lab, 5440 Engineering Hall, University of California, Irvine, CA 92697, USA
[b] Institute of Transportation Studies, 4038 Anteater Instruction and Research Bldg, University of California, Irvine, CA 92697-3600, USA

ARTICLE INFO

Article history:
Received 2 February 2019
Revised 25 June 2020
Accepted 8 July 2020
Available online 4 August 2020

Keywords:
Security
Link queue model
Double ring road network
Stability
Traffic flow
Fixed-time traffic control
Intelligent transportation systems

ABSTRACT

Wireless communication is being used as an enabling technology with traditional fixed traffic control systems in this transitional era toward Intelligent Transportation Systems (ITS). Unfortunately, major security concerns have arisen with respect to ever-increasing complexity and interconnectivity, and a noticeable lack of attention for security in these systems. Addressing concerns is a colossal challenge as it requires thorough development and formal analysis of a system model with respect to security. To tackle this challenge, we present a novel formal attack modeling and impact analysis methodology based on the Link Queue Model (LQM) of traffic flow inside a double ring road network, which is equivalent to a grid network with homogeneous links. We develop attack models as functions of tampered traffic control settings (e.g., green time ratios, cycle length, retaining ratios) with outputs equivalent to mobility impacts on the traffic network (e.g., time until system reaches state convergence, asymptotic average network flow). Further, for a given attack model, we define and identify vulnerable states: states that are critical to protect because they lead to negative impacts under the given attack model. Using our methodology we found that for certain vulnerable states, after only a few cycles of tampered control settings an attacker could cause a real impact of 1.5x speed-up in gridlock state convergence or 37%-99% drop in the asymptotic average flow rate. These results imply potentially drastic financial costs for cities and all involved drivers if similar attacks were performed on a real traffic control system.

1. Introduction

1.1. Motivation

Transportation systems play a major role for goods, services, and people. To ensure that transportation systems are fulfilling their role to the fullest, an extensive amount of work has been put into traffic management schemes to reduce or prevent congestion (Papageorgiou et al., 2003; U. S. D. Transportation, 2018). Congestion arises when the demand for a certain part of the transportation infrastructure is greater than the services/supply it may provide. Preventing or reducing traffic congestion may reduce environmental and health issues, improve safety, and help save money and time for people

☆ This material is based upon work supported by the National Science Foundation Graduate Research Fellowship Program under grant no. (DGE-1839285) for Anthony Lopez. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

* Corresponding author.
E-mail addresses: anthl10@uci.edu (A. Lopez), wjin@uci.edu (W. Jin), alfaruqu@uci.edu (M.A. Al Faruque).

https://doi.org/10.1016/j.trb.2020.07.002
0191-2615/

and services. In fact, according to a 2010 White Paper by the European Commission (Gemeinschaften, 2001), the "external costs of road traffic congestion alone amount to 0.5% of Community GDP [Europe]" and will continue to increase if nothing is done to mitigate its impacts (Papageorgiou et al., 2003).

Traffic control is immensely improving with the rise of wireless technology for sensoring, data transfer, and remote control (Webster, 1958; Sorensen et al., 2008).

According to the U.S. Department of Transportation Federal Highway Administration, "on average, adaptive signal control technologies improve travel time by more than 10%. In areas with particularly outdated signal timing, improvements can be 50% or more" (U. S. D. Transportation: Federal Highway Administration, 2011). Furthermore, the U.S. Department of Transportation has established a long-term Intelligent Transportation Systems (ITS) program to encourage the widespread use of ITS across the nation (U. S. D. Transportation, 2018). ITS are combinations of subsystems that work with one another to improve transportation performance. Each subsystem is made up of loops between sensors of physical phenomena (e.g., number of vehicles, vehicle speeds, vehicle presence), controllers and traffic agencies. To fully grasp a comprehensive understanding of the performance of ITS, each of its subsystems require individual modeling and analysis.

To aid existing and traditional traffic control systems and to prepare for upcoming implementations of ITS, wireless communication is being used as an enabling technology (Dobersek, 1998). Wireless communication enables the remote control over the signal timings of one or several intersections, and the transfer of information between sensors, controllers, and traffic management agency servers. Although there has been a shift toward implementing ITS, fixed-timing plans are still the most common throughout the world due to legacy and regulatory issues. In 2008, 90% of traffic control systems throughout the U.S. were fixed-timing control systems (Koonce et al., 2008). With the introduction of wireless communication to these and more advanced systems, security concerns are on the rise (Cerrudo and Spaniel, 2015; Hasbini et al., 2016; Kelarestaghi et al., 2018; Agadakos et al., 2017; Hossain et al., 2015).

In recent years, it has been found that modern traffic control wireless networks are vulnerable to sensor tampering and cyber attacks due to a lack of attention in their security (no attack detection/prevention, weak or no encryption/authentication) during the manufacturing and installation processes (Cerrudo, 2015; Ghena et al., 2014). Besides experimental studies, there are real attacks such as the train control network hack by a Polish teen in 2008 causing four trams to derail (Leyden, 2008) and the insider attacks on the traffic control network at a major Los Angeles intersection (Weber, 2009).

Although at first glance these security weaknesses are fixable and may appear to not represent all traffic control systems, it is generally agreed upon that some present and future vulnerabilities cannot be prevented because these systems require long life times, have complicated software-upgrading methods, and are becoming more interconnected with other devices and the Internet each day (Laszka et al., 2016; Zhang et al., 2011). In fact, in 2014, a whopping 15,000+ existing wireless devices (sensors and controller) deployed across 45 U.S. states and 10 countries were found to be potentially vulnerable to exploits that could lead to remote modifications of traffic timing control. Despite such a serious finding, the sensor's vendor ignored the report at the time. Such a negative reaction clearly demonstrates the high chance of existence of exploitable vulnerabilities in similar and/or other devices in traffic control systems (Cerrudo, 2013).

The objectives of attackers may vary, but in general they involve some form of congestion since they are prevented from forcing the system into an unsafe state to directly cause accidents (due to hardware fail-safes against remote modifications or easy detection of physical tampering). An attacker may be a person with a personal vendetta who wants to slow down the travel time of their enemy/enemies, or perhaps one or more members of a company/organization that desire to reduce traffic for their benefits and/or increase it against competitors. They may even be a recreational hacker interested in causing trouble for fun or a malicious one determined to cause havoc for major cities.

Existing works on ITS security include case studies on traffic control wireless networks (Ghena et al., 2014; Cerrudo, 2015), connected and autonomous cars (Evtimov et al., 2017; Thing and Wu, 2016; Chen et al., 2018; Checkoway et al., 2011; Hubaux et al., 2004; Wan et al., 2016), ride sharing applications (Yuan et al., 2016) and sensors in freeway traffic control systems (Reilly et al., 2016; 1755). Works (Ghena et al., 2014; Cerrudo, 2015) have demonstrated that networked traffic systems are vulnerable to a variety of cyber attacks. Other works (Ghafouri et al., 2016; Laszka et al., 2016; Reilly et al., 1755; Chen et al., 2018; Shoukry et al., 2018) attempt to quantify cyber-physical impacts of traffic control cyber-attacks and also attempt to solve for optimal attacks. Shoukry et al. (2018) also tries to design a traffic network that is resilient to Sybil (fake car) attacks. These works demonstrate that attacks on traffic control systems should not be underestimated and that it is critical to research how to formalize these attacks and their impacts. Tools should be developed to effectively aid traffic designers and engineers in the secure design and maintenance of these systems.

1.2. Motivational example

In Fig. 1 we illustrate a motivational example where a fixed-timing traffic controller is hacked and the malicious entity modifies the signal control settings (we elaborate how this is possible in Section 3). The network model is composed of two intersecting one-way roads, where cars on one road can only cross the intersection when it is their respective signal phase (two signal phases). The modifications include a reduction of green time for the first phase and an increase for the second phase. This attack causes congestion, a reduction in average speed and traffic flow (like that in the right side of Fig. 1), and eventually gridlock, where the average traffic flow is equal to zero. If a traffic management agency detects the changes

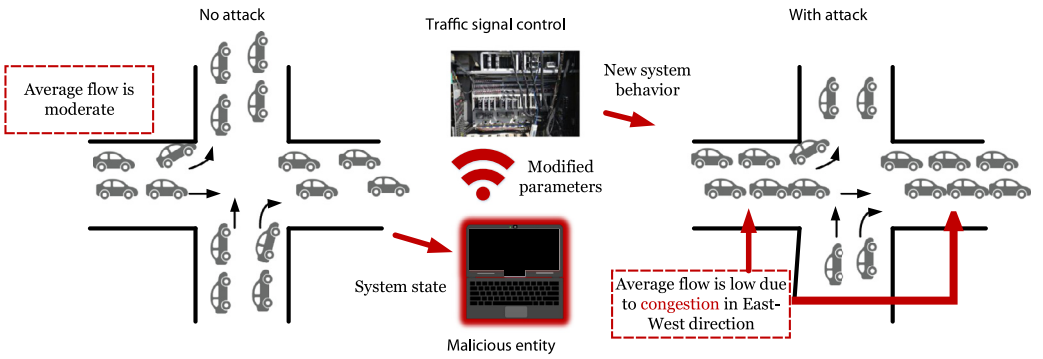


Fig. 1. Motivational example of the potential effects (congestion in one or both directions) due to malicious modifications on traffic signal control settings of ITS.

after several cycles and reverts the system settings to how they originally were, the long-term impact of the attack may still remain if the attacker carefully chose the modifications and attack timing.

1.3. Research challenges and contributions

To model similar attacks to the one in the motivational example, related works (Chen et al., 2018; Ghafouri et al., 2016; Laszka et al., 2016) have implemented existing traffic network and behavior models such as the Cell Transmission Model (CTM) (Daganzo, 1995) and the single queue model-based network model (Varaiya, 2013). Still, most of these models contain limited analytical properties, miss certain behaviors, and are challenging to use for larger grid networks (e.g., Manhattan grid networks). To address these challenges, we make use of the system model proposed in Gan et al. (2017). This system model includes the Link Queue Model (LQM) (Jin, 2012; Ubiergo and Jin, 2016) and Double Ring Road Network. The system model may be used to perform analysis of traffic network state properties (e.g., periodicity, stability) and to efficiently compute performance metrics (e.g., timing, flow) for different configurations of traffic networks, control parameters and attack models.

Regarding the differences between this work and aforementioned related transportation system security works: (1) they typically use different metrics (e.g., average waiting time, average queue lengths, or average speed) than we do, (2) they use different traffic network models and dynamics, (3) our system model is uniquely suitable for studying stability properties of states of general networks, and (4) our attack models have a low overhead cost associated with simulations due to our modeling choices (Jin, 2012).

In our attack modeling methodology, we focus on two control system objectives and one performance metric that an attacker may target: (1) response time, (2) equilibrium system states (NFD), (3) system state stability. One category of attacks isolates the response time as a target and either reduces or increases it according to the stability of the state and its average network flow. Another attack category targets and exploits the state stability itself by modifying the signal settings in a certain manner. Once the signal settings are changed, the system may potentially exit its current state and enter undesirable states. Of primary interest for us is how an attacker may direct the system from a state with high average asymptotic network flow to a state with a lower flow or gridlock behavior (asymptotic zero average network flow).

Our methodology does have its shortcomings, including that our traffic model is macroscopic rather than microscopic, that it assumes periodicity for certain states, that it is not able to observe all the possible state-related situations, and that it is not currently able to approximate phenomena such as lane changing. However, despite these shortcomings, our work faces and overcomes several research challenges: (1) determining how, which, and to what extent the controller settings may be attacked, (2) identifying potentially vulnerable system states using periodicity and stability properties from our traffic network models and dynamics, (3) creating attack models that are meaningful (e.g., challenging to detect and/or detrimental to the average network flow) from both the exploitable control settings and potentially vulnerable states, and (4) simulating and experimenting our attack models and demonstrating their usefulness. While the comparison between our work and other commercial car-following simulation tools, such as SUMO (Behrisch et al., 2011), might be helpful, these tools and corresponding car-following models suffer from their own weaknesses (e.g., randomness, complexity) and lack of analytical properties. Thus, this paper instead aims to serve as a foundation for more rigorous security analysis methodologies for transportation systems and may be compared and integrated with such commercial simulation tools in other works.

The contributions and order of contents of the methodology presented in this paper are outlined as follows:

1. defining the Double Ring Road and Link Queue Model, and how Density Evolution Orbits, Poincare Maps, and Network Fundamental Diagrams may be derived from them (Section 2),
2. providing an overview of attack vectors for fixed-time traffic control systems with wireless communication capability (Section 3),

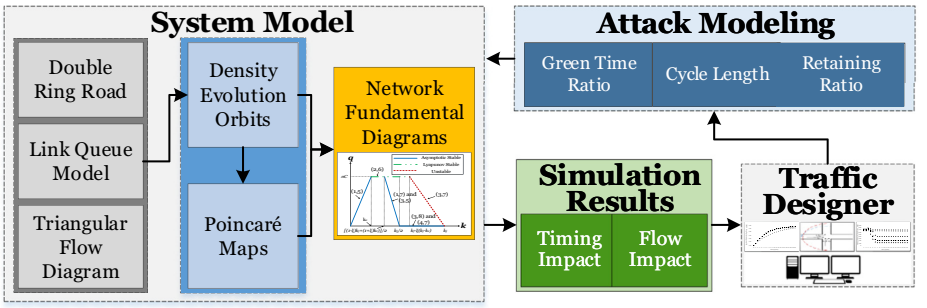


Fig. 2. Our proposed security analysis methodology and its role in the traffic management chain.

3. using analytical insights to identify vulnerable states (reducing the state space) and to develop attack models as functions of the traffic network state and control settings (Section 4).
4. simulating our attack models and evaluating their impacts in terms of metrics that are unique and "directly related to the decision-making and objectives of traffic control" (U. S. D. Transportation, 2018) (Section 5).

As shown in Fig. 2, we envision that this methodology will be useful in the future as part of the traffic management chain to develop (design-time) and maintain (run-time) a provably secure ITS. Where a system is *provably secure* if it is *secure by design/construction* (Foundation, 2018): given an attacker model where the attacker has access to the system and a specified amount of computational resources, the basic security requirements may still be met (Koblitz, 2007; Goldwasser and Micali, 1984; Rogaway, 2009). In design-time, the methodology may be built upon to choose optimal static control settings for a given traffic network under performance and security expectations. For real-time, efficient strategies may be implemented in response to detection of unexpected attacks to return the system to a state with a more favorable behavior.

2. System model

One may use the Link Queue Model (LQM) to formulate traffic flows in various network levels. In this paper, we discuss how it may be used in the context of a single ring road network, a double ring road network, and Manhattan-like grid networks.

2.0.1. Background and related work

There are several differences between the LQM and models from other works. LQM is able to capture a relationship between the turning ratios, the signal settings, and the initial densities in the form of an NFD derived from stationary/fixed states. Only few other works have considered the turning ratios and signal settings and few works studied multivaluedness (multiple possible flows for a given average density), but even then, these works lack definitions in what potential stationary states are and they lack studies on state stability properties. Works that did recognize the existence of potential stationary states and stability properties lacked in efficiency.

A similar model to the LQM is the Link Transmission Model (LTM) but there are several differences between them. First, the LQM is based on the linkâs average density, rather than just the number of vehicles over each link. Second, the LQM assumes that the network has an average density that remains constant. And third, the link/road density in the LQM is directly related to supply and demand ordinary differential equations. On the other hand, the LTM uses delayed differential equations as functions of in- and out-fluxes. These delayed differential equations make the LTM infinite-dimensional and not as mathematically tractable as traditional link-based models. Lastly, unlike most other models, the LQM with the Double Ring Road Network Model or grid network can incorporate both signal settings and route choice behaviors and we can observe different NFDs for different combinations of them (whereas NFDs derived from other models only depend on one of or none of these). In addition, before the LQM and analytical work in Gan et al. (2017), it was still unclear as to how many stationary states there are in a signalized Double Ring Road Network and what their stability properties are with respect to the signal settings, turning ratios, and initial densities.

Besides the LTM, another related model is the Cell Transmission Model (CTM), which estimates the traffic at each cell in a link rather than the entire link. However, the Cell Transmission Model (CTM) with signalized Double Ring Road used an infinite-dimensional dynamical system due to the kinematic wave model and therefore it is very challenging to solve traffic statics and dynamics. In previous work (Jin, 2012), all these models were qualitatively compared and the comparisons indicate that the LQM is the most efficient in terms of both time and memory. This is because the number of state variables needed to be computed is the number of link densities for LQM; whereas LTM requires two computations and the tracking of older flux values per time step and the CTM requires tracking values per each cell in the link.

The LQM introduced in Jin (2012) can be a useful tool for solving freeway and arterial traffic control and observation problems. This is shown by some of its applications published in major research journals such as: Point Queue Mod-

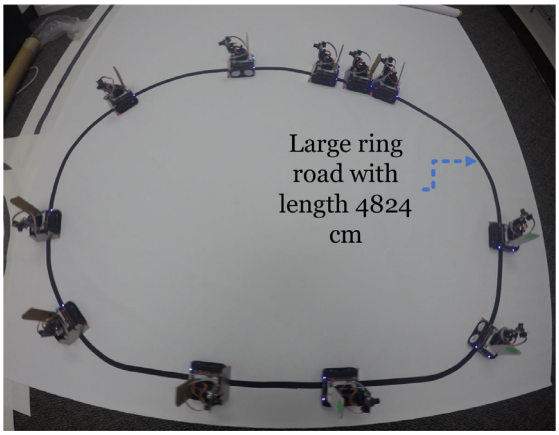


Fig. 3. Test-bed for single road model.

Table 1
Testing results of single road model testbed.

Ring road size (cm)	Number of cars	Average speed (cm/s)	Shockwave speed (cm/s)
2376	≥ 5	14.5	11
2376	< 5	≥ 20	none
4389	≥ 7	15.5	11.5
4389	$< 7 \geq$	20	none
4824	≥ 12	21	12
4824	< 12	28	none

els (Jin, 2015), variable speed limit control of a lane-drop bottleneck (Jin and Jin, 2015; 2014), signalized grid network analysis and control (Gan et al., 2017), and urban traffic estimation for real-world settings (Gu et al., 2017).

2.1. Single ring road and lab test-bed

In a Japanese research experiment where different numbers of drivers drove vehicles within a single ring road, it was observed that there were specific numbers of vehicles that would lead to a change in network behavior within the context of average network flow. These numbers of vehicles are generally denoted as critical densities. For example, as the number of vehicles increased past a critical density, a traffic jam would occur after some time despite no presence of a bottleneck (Sugiyama et al., 2008). Within the context of a single ring road model, the LQM also reflects similar behaviors as the Japanese experiment (Julia Carrillo, 2015). In order to emulate more realistic traffic behaviors like those in the Japanese experiment, we have implemented a lab test-bed of robotic vehicles following each other on a single ring road (Fig. 3). They use the Optimal Velocity Model (OVM) car-following algorithm based on information from their sensors (cameras) and parameters (e.g., permissible distances). Some testing results of the model presented in Table 1 matched the behaviors observed in (Sugiyama et al., 2008). As the LQM also models this type of behavior, the robotic vehicle experiment was a step above simulation to importantly show how it could model realistic scenarios.

Unfortunately, the LQM and single road model is not able to capture more interesting behaviors of a traffic network with turning movements. Thus, in this work we use a more expanded version of the LQM along with a double ring road network model to cope with such turning movements. As the lab test-bed has been created, we plan to build upon it to emulate this developed model along with the rest of our attack models in our future work.

2.2. Summary of traffic control settings and system model variables

To help the readers follow the paper, readers may refer to this section for definitions of used traffic control settings and system variables.

- T refers to the traffic signal cycle time (seconds).
- $\pi_i T \in (0, 1), i \in \{1, 2\}$ refers to the effective green time (seconds) where π_i refers to the effective green time ratio for phase i.
- $t_L = T - \sum \pi_i T$ refers to the total lost time t_L (seconds) within the cycle (seconds), which is the sum of yellow and red times, and the time that was not effectively used by vehicles to cross the intersection.
- $\xi_i \in (0, 1), i \in \{1, 2\}$ refers to the retaining ratio of vehicles in ring i.
- L refers to the length of the ring road (miles).

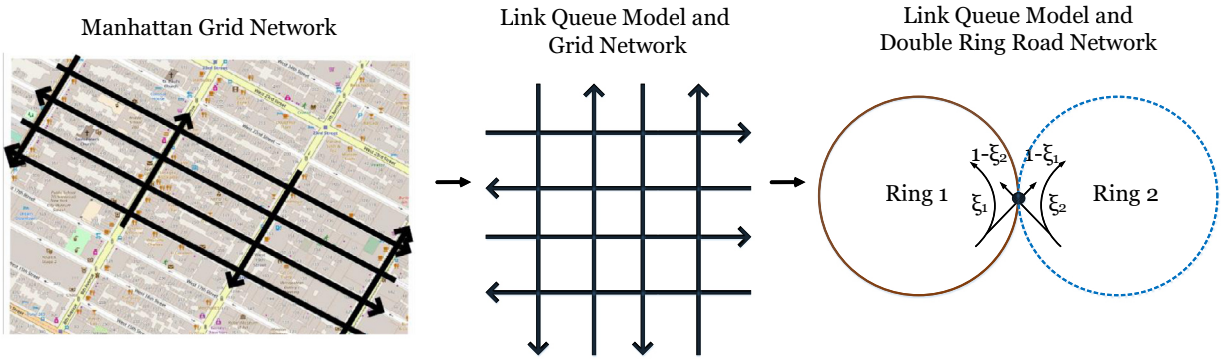


Fig. 4. Flow of abstracting an actual grid network (like in Manhattan) to double ring road network and link queue model.

- k_j is equal to 150 vehicles per mile and refers to traffic jam density.
- k refers to the average density in the network (vehicles per mile), $k \in [0, k_j]$.
- k_i^* refers to a fixed system state where the density of ring i will be the same value after a full cycle, $k_i \in [0, k_j]$.
- k_c refers to the critical density and is approximately $\frac{k_j}{5}$ (vehicles per mile).
- q_0 refers to the overall average traffic flow (vehicles per hour).
- R_{p,k_1} refers to the interval that k_1 satisfies for a given DEO region R_p
- $R_{p,k}$ refers to the interval that k satisfies for a given DEO region R_p
- R_p refers to the tuple of the intervals, $(R_{p,k_1}, R_{p,k})$.
- R refers to the set of all R_p, such that $p \in [1, 8]$ as shown in Fig. 6 (9 and 10 are ignored).
- A DEO is a sequence of visited (k_1, k) regions over a single cycle. DEOs of states are represented as $(p_1, p_2) | p_1 \in [1, 4] \, and \, p_2 \in [5, 8]$.

2.3. Double ring road network

The *Double Ring Road Network* model of a *homogeneous symmetric one-way road intersection* is made up of two ring roads that are connected with each other. Larger symmetric one-way road grid networks may also be abstracted with this model (see Fig. 4). Furthermore, asymmetric and complex networks may also be decomposed into multiple symmetric one-way road grid networks. Additionally, each 2x2 one-way road network is actually similar to a single two-way intersection and an entire traffic network may be converted accordingly. Therefore, this network model and the LQM is applicable for all Urban Traffic Control systems (UTC) (Gan et al., 2017).

Each ring road has length L in miles (mi) and Ring 1 corresponds to South-North roads while Ring 2 corresponds to East-West roads. The connection point of the ring roads helps model turning cars at intersections. This model is based on the concept that the network will reach a periodic state after a long time, which means that the network's outflow is equal to the network's inflow.

In this model, there are two signal phases corresponding to each ring road's turn. Therefore, both the roads and signal phases are identified by $i \in [1, 2]$. In each signal phase, there is an effective green time $\pi_i T$ in seconds, where π_i is the effective green time ratio and T is the total cycle time. The signal regulation is handled by the indicator functions $\delta_1(t)$ and $\delta_2(t)$ in Eqs. (1) and (2). In the first phase, cars from the first ring are moving across the intersection and the cars from the second must wait. The opposite is true for the second phase. In addition to the effective green times, there are also lost times, t_L, per each phase such that $2t_L = T - (\pi_1 + \pi_2)T$. Therefore, it is not required that $\pi_1 + \pi_2 = 1$. The lost time includes the start-up lost time (caused by vehicles' reactions and limited accelerations when signals turn green) and the clearance lost time (caused by wasted yellow and red times).

$$\delta_1(t; T, t_L, \pi_1) = \begin{cases} 1 & \text{for } t \in [nT, nT + \pi_1 T], \\ & n \in \mathbb{N}_0 \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

$$\delta_2(t; T, t_L, \pi_1) = \begin{cases} 1 & \text{for } t \in [nT + t_L + \pi_1 T, \\ & (n+1)T - t_L], \, n \in \mathbb{N}_0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Each ring also has a retaining ratio $\xi_i(t)$ and turning ratio $1 - \xi_i(t)$ to specify how many cars remain on the same ring road or turn, respectively. For analytical purposes we fix these retaining ratios and therefore we use ξ_i as the notation from now on. $k_i(t)$ is the average density in vehicles per mile (vpm) in ring i over a cycle, and k (vpm) is the total average density in the network. When either or both rings have density equal to the traffic jam density, i.e., $k_i(t) = k_j$, then *gridlock* occurs.

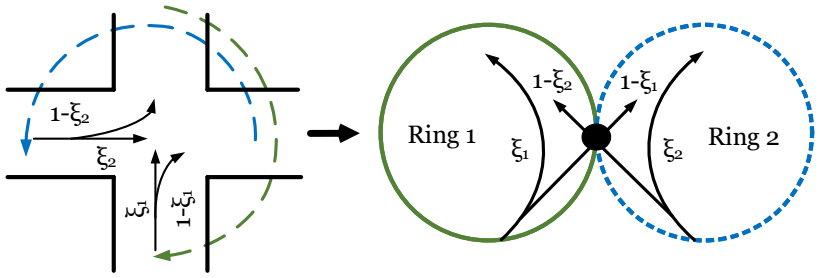


Fig. 5. A signalized one-way intersection and corresponding abstracted double ring road network model. ξ_i is the retaining ratio that corresponds to either the N-S or E-W roads in the network model.

Note that, we only consider $k_i(t)$ as a variable over time since k is constant. Furthermore, if we know $k_1(t)$ and k, we may easily derive $k_2(t)$. See Fig. 5 for a closer visualization of how an intersection is abstracted by the Double Ring Road Network.

2.4. Link queue model

2.4.1. Behavior modeling and formulation

We denote S_i in vehicles per hour (vph) for the amount of supply traffic flow for the downstream link and we denote D_i (vph) as the amount of demand traffic flow from the upstream link. Both S_i and D_i are constrained by a critical density k_c and are directly related to the traffic influx $f_i(t)$ (vph) and outflux $g_i(t)$ (vph) of the ring roads. The outfluxes are restricted by the demands of the upstream links and the supplies of the downstream links. The definitions for S_i and D_i (Eqs. (3) and (4)) are derived from the empirical triangular traffic flow diagram in Eq. (6) from Gan et al. (2017) and are functions of the densities in each ring.

$$D_i(t) = Q(\min\{k_i(t), k_c\}) = \begin{Bmatrix} v_f k_i, & k_i(t) \in [0, k_c] \\ C, & k_i(t) \in [k_c, k_j] \end{Bmatrix} \tag{3}$$

$$S_i(t) = Q(\max\{k_i(t), k_c\}) = \begin{Bmatrix} C, & k_i(t) \in [0, k_c] \\ \frac{C(k_j - k_i)}{k_j - k_c}, & k_i(t) \in [k_c, k_j] \end{Bmatrix} \tag{4}$$

where $C = v_f k_c$ is the maximum average flow known as the capacity, v_f is the free flow speed at 60 mph, $k_i(t)$ is the average density in ring i over a cycle, and k is the total average density in the network.

From S and D we can derive functions for the in-fluxes $f_i(t)$ and out-fluxes $g_i(t)$:

$$g_1(t) = \delta_1(t)\min\{D_1(t), \frac{S_1(t)}{\xi_1(t)}, \frac{S_2(t)}{1-\xi_1(t)}\} \tag{5a}$$

$$g_2(t) = \delta_2(t)\min\{D_2(t), \frac{S_2(t)}{\xi_2(t)}, \frac{S_1(t)}{1-\xi_2(t)}\} \tag{5b}$$

$$f_1(t) = g_1(t)\xi_1(t) + g_2(t)(1-\xi_2(t)) \tag{5c}$$

$$f_2(t) = g_1(t)(1-\xi_1(t)) + g_2(t)\xi_2(t) \tag{5d}$$

From these equations, we can derive a nonlinear ordinary differential equation $\frac{dk_1(t)}{dt}$ (see Eq. (6)) to compute the evolution of the ring densities over time with respect to the signal settings. Further, from $g_1(t)$ and $g_2(t)$, we may calculate an important metric in traffic engineering: the asymptotic average network flow $q(t)$ (see Eq. (7)). $q(t)$ is bounded by $C = v_f k_c = 900vph$ where the traffic is moving at free flow v_f. Note that it is generally computational heavy to evaluate the integrals of g_1 and g_2.

$$\frac{dk_1(t)}{dt} = \frac{1}{L}(f_1(t) - g_1(t)) = -\frac{(1-\xi_1)}{L}g_1(t) + \frac{(1-\xi_2)}{L}g_2(t) \tag{6}$$

$$q(t) = \frac{\int_{s=t-T}^{t} g_1(s)ds + \int_{s=t-T}^{t} g_2(s)ds}{2T} \tag{7}$$

2.5. System states, density evolution orbits, and poincare maps

Using the Double Ring Road Network model and LQM, a system state may be represented by a tuple $(k_1(t), k)$, where $k_1(t)$ is the current density of the first ring road and k the overall average density (from which we can easily derive $k_2(t)$).

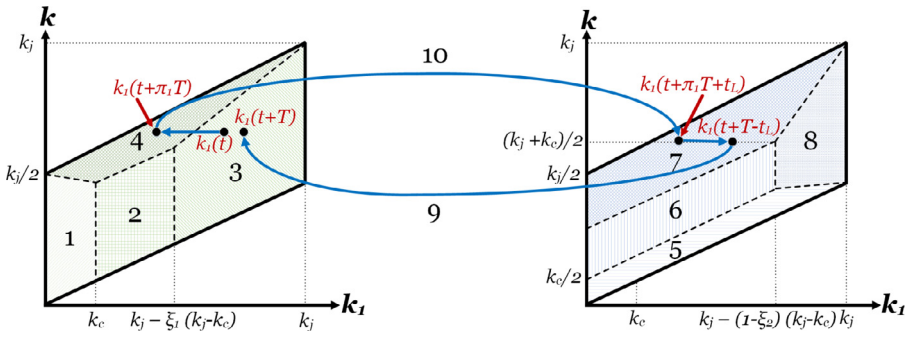


Fig. 6. Example of density evolution orbit of (k_1, k) over one cycle.

A more macroscopic state representation can be made with a Density Evolution Orbit (DEO). A DEO is a sequence (k_1, k) regions visited in a single cycle. It can be attained via analytical insights from the ring road densities and signal settings or derived from simulations. In our previous work (Gan et al., 2017), we identified 10 unique (k_1, k) regions with unique traffic behaviors, $\frac{dk_1(t)}{dt}$. Regions 1–4 correspond to behaviors in phase 1 ($\delta_1 = 1$) and regions 5–8 correspond to behaviors in phase 2 ($\delta_2 = 1$). Regions 9 and 10 correspond to the times between each phase when no vehicles are moving.

The DEO regions specify just how filled the two rings are and, therefore, the entire network. It is important to know how much density is allocated to each ring at the start because it may correspond to an average asymptotic network flow (if it is a fixed state). The basic idea is that the more symmetric the two ring densities are, the higher the average network flow, while the more asymmetric is it, the lower the average network flow. We therefore may use these regions as a guideline to identify which states are vulnerable and what signal settings must be modified to successfully cause an attack. To identify these regions, for each phase we analyzed the influence of changes in D and S with respect to different relationships between k_1, k_2, k, k_c and k_j on the behavior function: $\frac{dk_1(t)}{dt}$. For instance, relationships such as $k_1 > k_c$ and $D_1 = C < \frac{S_1}{\xi_1}$ means that there is a separation between Region 1 and Region 2 at $k_1 = k_c$ because when $k_1 < k_c$, the behavior function will change.

We focus on initial states that only visit one region in each phase, and therefore denote their DEOs as (p_1, p_2) where $p_1 \in [1, 4]$ and $p_2 \in [5, 8]$. In Fig. 6, we provide an example of a DEO over regions in the (k_1, k) space. We provide bounds and behaviors per each region in Table 4. From now on, we denote the set of all region boundaries as R and an individual region as $p \in [1, 10]$ with boundaries for k_1 and k in $R_p \in R$.

From the initial states, signal settings, and DEOs, we may compute Poincare Maps to analyze traffic network state properties. A Poincare Map (Teschl, 2012) is a function P that maps an initial ring density value $k_1(t)$ to a ring density value on the nth cycle $k_1(t + nT)$ and is made up of smaller Poincare Maps for each phase transition. In cases where there is high periodicity such that $k_1(t) = k_1(t + nT)$ for $n \in \mathbb{N}$ we refer to $k_1(t)$ as a fixed state k_1^* with respect to the system signal settings. Potential fixed states where only one region of the (k_1, k) space is visited during each phase were identified in our previous work. We focus on these fixed states (k_1^*, k) and we also refer to each fixed state by its DEO.

When the network is in *gridlock*, it means that one or both of the rings is full (k_j). If the network is gridlocked, it is only possible for (4,7) or (3,8) to be the current DEO and they are both fixed for any $\xi \in (0, 1)$. The possible DEOs that have fixed states when the **network is not gridlocked are**:

- (1,5), (1,7), (2,6), (3,5), and (3,7) for $0.5 < \xi < 1$;
- (1,5), (2,6), and (4,8) for $0 < \xi < 0.5$;
- (1,5), (2,6), (4,7), and (3,8) for $\xi = 0.5$

With fixed states, the computation of the asymptotic average network flow $q(t)$ can be approximated and redefined with $q(k)$ as $t \to \infty$ instead (see Eq. (8)). This is important as we can then map each pair of $k_1^* = k_1(nT)$, $n \in \mathbb{N}_0$ and k to an average asymptotic traffic flow q. In turn, this mapping allows us to analytically derive an approximate closed-form formula for a Macroscopic/Network Fundamental Diagram (MFD/NFD), which is useful in practice.

$$q(k; k_1^*) = 2\frac{\int_{s=t-T}^{t} g_1(s)ds}{2T} \approx \frac{g_1(k_1^*) + g_1(k_1(nT + \pi T))}{2} \tag{8}$$

We have derived several signal over different signal settings for different fixed states (examples are provided in Fig. 7. The characteristics in our NFDs were consistent with those from previous literature but new ones existed too. Particularly, there were multiple possible flows (i.e., multivaluedness) for some density values and branches with different stability properties. This means that for the same average density, there are two possible values for the average network flow and potential to change signal settings to sway a system from an unfavorable state with low average network flow to a state with higher average network flow. Note, however, that the opposite is of interest for an attacker. Branches represent many possible fixed states, where each fixed state has a stability property.

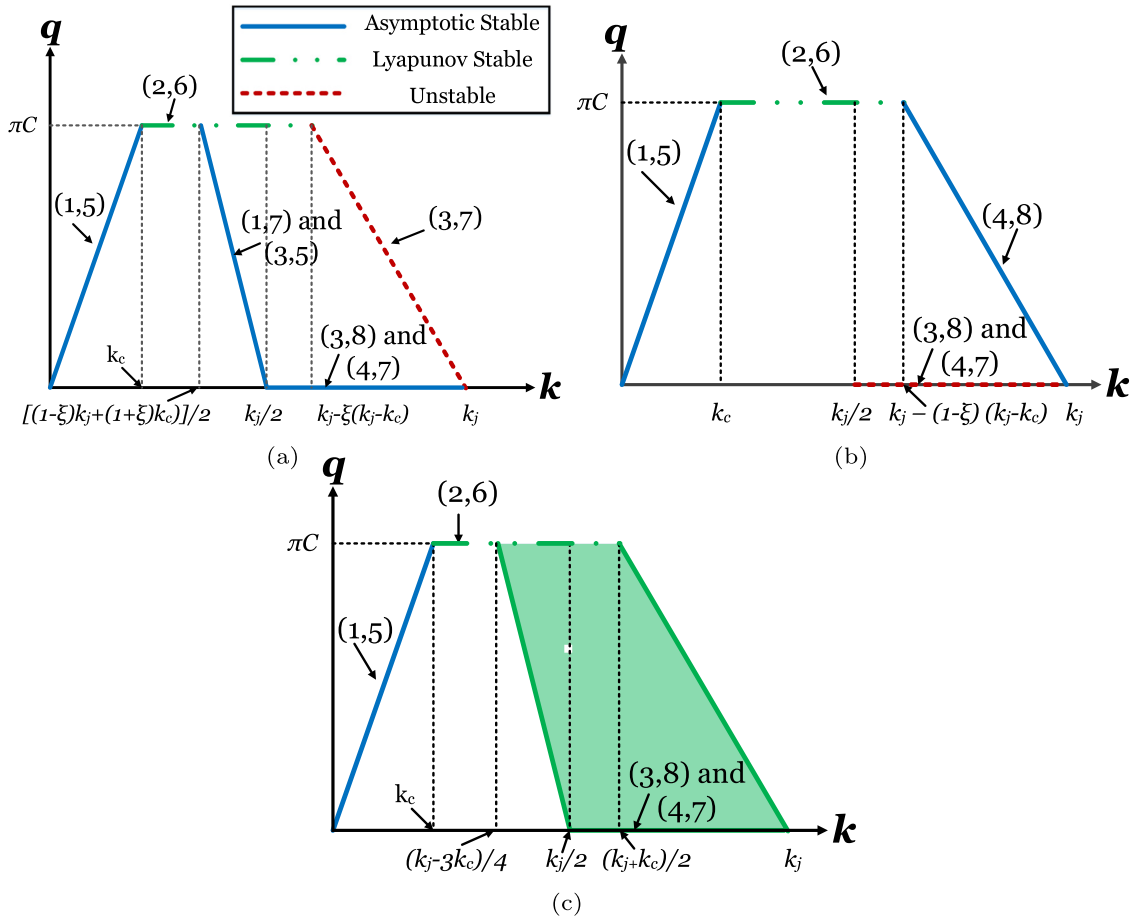


Fig. 7. Poincare Map-based approximate NFDs when $\pi_1 = \pi_2 = \pi$ for various retaining ratios, $\xi = \xi_1 = \xi_2$. In Figure a, $0.5 < \xi < 1$, in Figure b, $0 < \xi < 0.5$, and in Figure c, $\xi = 0.5$.

Combining our network model and Poincare Maps, we are able to analyze the stability properties of fixed states. It is important to be able to analyze the stability properties of states to understand which ones are undesirable/desirable and critical for proper traffic control. Unstable fixed states are the most vulnerable ones such that even a small perturbation (e.g., from random noise or changes to signal settings) will completely change the system behavior. Lyapunov stable fixed states can handle perturbations up to a certain limit while asymptotic stable fixed states are able to handle any perturbations as long as the signal settings remain the same. Having these properties in mind, we identify potentially vulnerable states and evaluate the impacts of attacks on control settings with respect to these states.

3. Attack surface

In traffic control networks such as those in Michigan (Ghena et al., 2014), Seattle, New York, and Washington DC (Cerrudo, 2013), wireless technologies are assisting fixed-time traffic control systems by connecting traffic controllers with loop detectors, nearby controllers, traffic management agencies, and vehicles. However, as mentioned, these wireless networks are prone to having or eventually having security vulnerabilities. There are three primary approaches of access (two via exploiting wireless network vulnerabilities) that an attacker can take to modify the signal timing plan. In this section, we discuss attack vectors for how this could be done for each approach of access.

3.1. Physical/direct access

An attacker could open up the traffic controller box (cabinet) to tamper with the equipment and modify any control setting (even remove the fail-safe equipment and cause an all-green light configuration). Obviously, this kind of attack would catch a lot of attention (e.g., video camera detection, suspicious activity reports) and is therefore not particularly a viable method for attackers.

3.2. Indirect access

Vehicle detectors and On-Board Units (OBUs) were found to be vulnerable to hacking and could be used for spoofing attacks (Chen et al., 2018). Thus, the spoofing attack (e.g., deceiving the controller about existence of cars) would indirectly cause a modification to the signal timing plan at an intersection. Such an attack would have merit for adaptive timing control systems because of the instant impact. For fixed-timing control systems, the attack would have an effect on the decision-making of the traffic management agency and may lead to an update of a less-than-optimal signal timing plan. However, the difference between the attack start time and the response time will reduce the effectiveness of such an attack on fixed-time control systems.

3.3. Remote access

In this section, we will go into detail how an attacker may directly modify the timing plan via wireless communication. In order to perform a remote access attack to the traffic controller, an attacker must first obtain access into the wireless network of the traffic control system. Cerrudo (2014) and Ghena et al. (2014) observed through their experiments that there is a tendency for poor or nonexistent security in traffic controller wireless networks. This is because of either the carelessness or insufficient knowledge of controller installers and manufacturers. Although vendors of these vulnerable controllers were kept private in these works, Cerrudo (2014) studied controllers that were distributed in USA and 10 other countries while Ghena et al. (2014) studied controllers from a different vendor deployed in Michigan.

Let us take the controllers that Ghena et al. (2014) studied as an example on how an attacker may gain access. First, an attacker would need a radio wireless card matching the same frequency as that of the controller (in this case, 5.8 GHz or 900 MHz). Then, they would need to implement the same network protocol, which they can discover via social engineering attack or a reverse engineering attack (slightly more complicated if frequency hopping is implemented, but still feasible), and gain access to the private network by exploiting the security vulnerabilities (e.g., weak encryption keys, passwords). A traffic controller network for a specific intersection could then be accessed more than half a mile away. They could also attempt to use a drone to perform a mobile attack. Either way, the connectivity range is attractive for attackers who wish to remain undetected throughout the lifetime of the attack (Ghafouri et al., 2016).

3.3.1. Modifying traffic signal settings

Having access into the private controller network implies access to all other controllers on the same network. However, even if an attacker had access to a traffic control system, *due to hardware-based solutions (malfunction management units) they cannot force unsafe signal combinations (e.g., green-green or red-red)* (Ghena et al., 2014; Urbanik et al., 2015). Nevertheless, the attackers would still be able to modify the scheduling of traffic signals or force a blinking red phase (but the latter is easily detectable).

Continuing with the previous example, modifying the traffic signal settings could be done via two methods after gaining network access: (1) sending memory modification commands to the debug port in the controller's VxWorks OS or (2) using remote control commands provided in the National Transportation Communications for ITS Protocol (NCTIP) 1202. The VxWorks debug port issue may have been patched, but (as far as we know) the remote control attack vector remains. Remote control commands include malicious logic statements, activating any button on the controller, or modifying light timings (shorten or lengthen phase times). Since all the controllers are connected in a one-hop manner to their neighbors, an attacker may perform a small or large scale attack depending on their resources and objectives.

3.3.2. Attaining system state knowledge

With or without access to the wireless network, the attacker may easily attain knowledge about the current state of the system, which includes the current timing plan configuration and the physical state of the intersection (i.e., densities and DEO). If they had no access to the network, the attacker can easily use their own sensors (e.g., phone, camera) or observations because the traffic intersection is in a public space. While if they did have access, they can use the measurements from existing loop detectors and/or cameras. We may also assume that, with the introduction of more technology (i.e., image processing, smarter sensors) it will be even easier to accurately estimate the current system state.

3.3.3. Attack timing

Despite the different possible roles, we assume that the attacker does not desire to be easily detected. This means that their attacks may be subtle yet may have profound long-term effects on the system behavior. Fixed timing signal plans are regularly updated (even hourly) to address traffic demands or for reasons such as major traffic changes, time of day, and inspections. If the attacker can modify the signal timings around the same time that the timing plan is regularly updated or quickly reverse their modifications after a short time, the changes will not be trivially detectable. Even if detected, it may be too late (response time varies considerably (Urbanik et al., 2015)), as the impact from an attack may already have forced the system en route to a targeted state, despite reversed settings by the agency.

After gaining some level of access the attacker can perform an attack on the integrity (i.e., the signal timing) and consequently the availability (i.e., traffic flow, control response time) of the traffic control system. For a graphic overview on the steps an attacker would take discussed in this section, please refer to Fig. 8. Note that it is general enough to consider

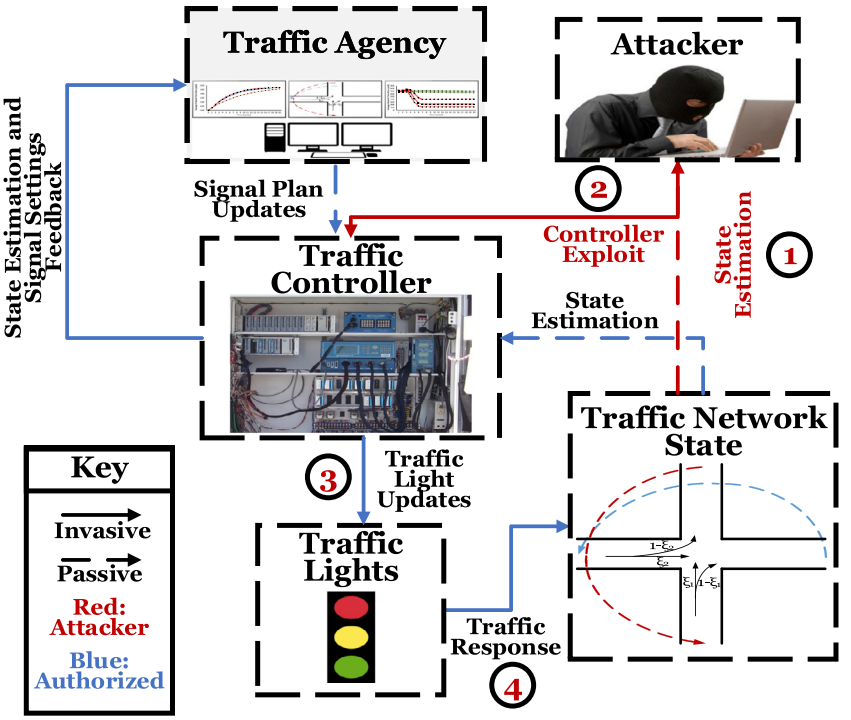


Fig. 8. Attack strategy and attack vector. **Step 1**) The attacker estimates the system state (may also be done after Step 2), **Step 2**) The attacker performs an exploit to gain controller access (most likely remotely), **Step 3**) The attacker now has authorized access to update the traffic signal cycle at will (under realistic constraints), **Step 4**) The updates will cause one or more detrimental impacts on the average and asymptotic traffic behavior.

the different potential controller exploits discussed in this section. To assess the impacts of such attacks, we define attack models, identify potentially vulnerable states, and evaluate attack impacts.

4. Attack modeling & impact analysis

An attack model consists of the system model (LQM simplified as first DEOs and then Poincare Maps for analytical purposes) and attacks on various system control parameters through vulnerability exploits in the aforementioned attack surface. In a sense, an attack model is similar to a closed-loop control system model but where the attacks are anti-controls. In this section, by using the Density Evolution Orbits and Network Fundamental Diagrams in Section 2.5, we determine potential initial and final (targeted) state tuples derive average network flow attack impacts from the Poincare Map-based NFDs that are most desirable for an attacker. Then, along with the behavior differential equations in Section 2.4 and limitations of the attacker in Section 3, we come up with attacks on the controller settings to achieve these impacts.

The general attack model is defined as: $AM(M, x_0, \Delta) =$

$$\begin{cases} \text{Convergence Time Impact: } t_{conv,\Delta},\ (t_{conv,\Delta} - t_{conv}), & \text{for } DEO_\Delta = DEO_0 \text{ and } \pi_{1,\Delta} = \pi_{2,\Delta} \\ \text{Asymptotic Average Flow Impact: } q_\Delta,\ (q_\Delta - q_0) & \text{for } DEO_\Delta \neq DEO_0 \text{ and } \pi_{1,\Delta} \neq \pi_{2,\Delta} \end{cases}$$

First, we define the inputs to AM. The system model M is a vector of the following: NW, $k_i(t)$, k, π_i, $\delta_i(t)$, $\xi_i(t)$, $D_i(t)$, $S_i(t)$, $f_i(t)$, $g_i(t) | i \in \{1, 2\}$) where the network variable NW is a tuple with the number of intersections with link length L and the initial cycle length T (see Section 2 for definitions of the other variables). The initial system state x_0 can be defined in terms of the original traffic control settings and initial traffic densities of each road before the start of the attack. The traffic control settings at time t_0 include π_1, π_2, and T. Traffic densities are $k_1(t_0)$, $k_2(t_0)$, and k.

We consider an intelligent attacker whose objective is to force the system into a targeted density evolution behavior via modifying control parameters. The variable Δ is a tuple of the modifications and their timings that the attacker plans to perform: the new cycle length, T_Δ; the new effective green time ratios $\pi_{1,\Delta}$ and $\pi_{2,\Delta}$; the starting time of the attack t_{start}, the duration of the attack t_Δ and ending time of the attack $t_{start} + t_\Delta$ (when the modifications return to normal), and the ending time of the simulation/measurements t_{finish} s.t. $t_{finish} \geq t_{start} + t_\Delta$; the starting state of attack x_0 with DEO_0 and time t_0, and ending state of attack x_Δ with DEO_Δ at time t_{finish}.

In this paper, we assume that only one type of signal setting (green time ratios, cycle length) will have nonzero modifications during an attack. Modifying the allocations of green time or modifying the cycle length itself will directly affect

the effective green time ratios. We only study modifications on these settings because, despite having the ability to modify multiple other parameters, an attacker would be extremely interested in a low number and amount of modifications to destabilize the system. Furthermore, we do not consider modifications to the retaining ratios (which could be changed through route guidance application exploits) in this paper. Although we do not consider combinations of parameter modifications in these attacks, the attack strategies discussed in this work are simple yet may cause serious impacts on the traffic network. However, we argue that an attacker would be most interested in the simplest changes to create a sufficient amount of havoc. Additionally, this work is a foundational basis to other works that tackle research problems such as: deriving the most effective attack or analyzing and understanding the effects of modifying several different parameters at the same time.

There are two types of attack behavior categories for *AM* that we will study in this section. The first category - Non-State-Changing - speeds up or slows down the system's convergence to a fixed state behavior (especially the gridlock state). The second category - State-Changing - causes one or several state change(s) and reduces the asymptotic average flow. For Non-State-Changing attacks, the new time at which the system will converge to its expected stationary behavior is denoted as $t_{conv,\,\Delta}$ and the original convergence time is t_{conv}. Thus, the impact is $t_{conv,\,\Delta}$ - t_{conv}, where t_{conv} depends on the designer-based range of permissible performance metrics (e.g., densities, asymptotic average flow-rate). For both attack categories, in particular State-Changing attacks, another impact is difference in average flow rates, $q_\Delta - q_0$, which can be predicted from the initial and final DEOs (if known) for states, x_0 and x_Δ.

4.1. Non-state-changing attacks

Non-state-changing attacks will not theoretically change the DEOs of fixed states if the attacker chooses to modify the cycle length or the green time ratios such that $\pi_{1,\Delta} = \pi_{2,\Delta} = \pi_\Delta$. Instead these modifications will cause the expected asymptotic or stationary behavior of the state to be reached at a different time $t_{conv,\,\Delta}$ instead of the original expected time t_{conv}. We assume that original settings are $\pi_1 = \pi_2 = \pi \neq \pi_\Delta$. In the following sections, we consider attacks to speed up the convergence of asymptotic stable gridlock states. Recall from Fig. 7 that asymptotic stable gridlock states are states with DEO of either (3, 8) or (4, 7). Thus, a designer and an attacker would be strongly interested in identifying when the system is in a state with one of these DEOs.

4.1.1. Gridlock speed-up attack when $DEO_0 = DEO_\Delta = (3, 8)$

Given $\pi = \pi_1 = \pi_2$, $\xi > 0.5$, $k_1(0)$, k and $DEO_0 = DEO_\Delta = (3,\ 8)$, an attack with π_Δ such that $\pi_\Delta = \pi_{1,\Delta} = \pi_{2,\Delta} > \pi$ will create a new convergence time $t_{\Delta,\,conv}$ such that $t_{\Delta,\,conv} < t_{conv}$. For a DEO of (3, 8), we know that eventually k_1 will reach k_j given the signal settings from our previous work. The Poincare Map equation corresponding to this DEO is $k_1(nT) = k_j(1 - e^{(\gamma_2-\gamma_3)\pi nT}) + k_1(t)e^{(\gamma_2-\gamma_3)\pi nT}$ where $\gamma_2 = ((1-\xi_1)k_c)/L\xi_1(k_j - k_c)$ and $\gamma_3 = v_f k_c/L(k_j - k_C)$. Since the exponent includes the green time ratio and since $\lambda > 0$, then it is easy to see that with values of π_Δ such that $\pi_\Delta > \pi$, the rate of density growth will increase and therefore lead to $k_{1,\Delta}(t_{start} + t_\Delta) > k_1(t_{start} + t_\Delta)$ where $k_{1,\Delta}$ is the ring road density when there is an attack while k_1 is the normal expected density without attack. Because of this, even if the growth rate returns to normal after attack completion, the system will still more quickly converge to the limit, i.e., $t_{conv,\,\Delta} < t_{conv}$. Using the same logic, similar impacts will occur when the attacker modifies the cycle length such that $T_\Delta > T$.

In Fig. 9, we visually demonstrate the convergence time impacts of this attack model for different π_Δ where $t_{Start} = 1T$ and $t_\Delta = 10T$. Poincare Map settings include: $L = 0.25,\ \pi = 0.3,\ \xi = 0.75,\ k_1(0) = 120,$ and $k = 75$. When $T = 90$ s, the maximum impact logically occurs for $\pi_\Delta = 0.5$ and is $t_{conv} - t_{conv,\Delta} = 20T - 13T = 7T$. Hence, there is a gridlock convergence speed up of $20T/13T = 1.53$. This means that the agency has 7T less time to detect and respond with setting changes to guide the system to a favorable state instead.

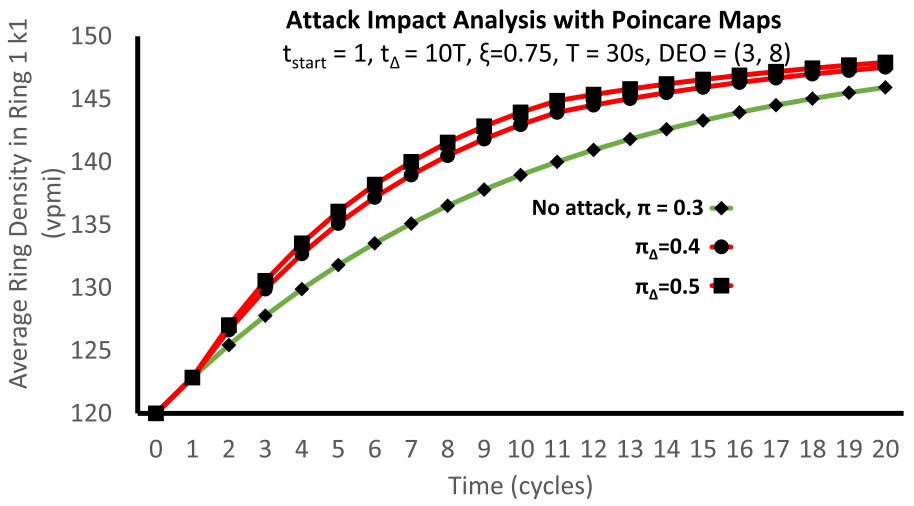
Although it appears that the system reaches the steady state value around nearly the same time, the biggest concern should be that even just a few cycles of reduced convergence time may be highly costly for drivers and the traffic agency. This is because the later the reaction of the traffic control system authorities, the more pronounced the effects of the attack and the more difficult it is to reverse the attack. In addition to looking at just the asymptotic limit, it is important to note the trajectory of traffic behavior from start to finish and how there are pronounced effects before the asymptotic limit is reached. Furthermore, these figures describe an example where the attack was for a finite duration (10 cycles) and not from start to finish. If the attack was performed the entire time, it would be clear that the convergence would be even more rapid.

4.1.2. Gridlock speed-up attack when $DEO_0 = DEO_\Delta = (4, 7)$

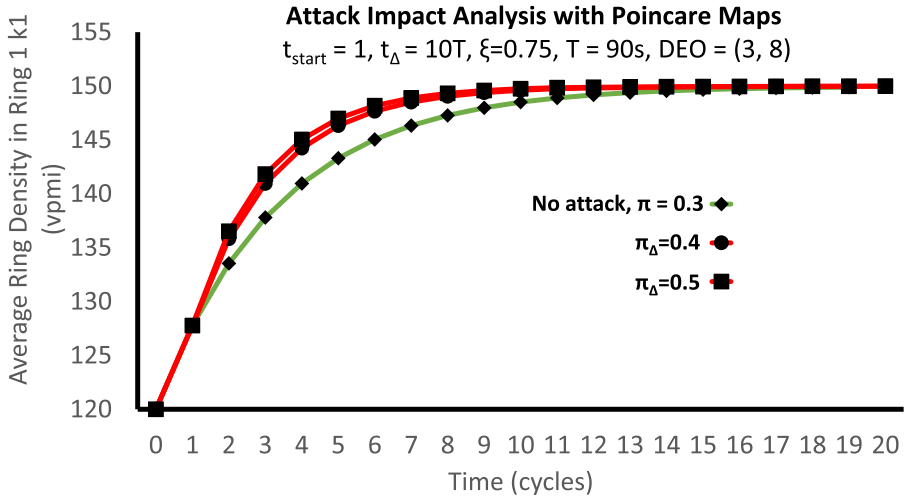
For $DEO_0 = DEO_\Delta = (4,\ 7)$ when $\xi > 0.5$, we know that eventually k_2 will reach k_j and therefore k_1 will eventually reach $2k - k_j$. Similar to the previous case, the Poincare Map equation for an initial state with this DEO can be used to compute how much more quickly the system reaches gridlock, $t_{conv,\,\Delta} \leq t_{conv}$, when $\pi_\Delta > \pi$ or $T_\Delta > T$.

4.2. State-changing attacks

For state-changing attacks, the modified green time ratios will satisfy $\pi_{1,\Delta} \neq \pi_{2,\Delta}$. When $\pi_{1,\Delta}$ and $\pi_{2,\Delta}$ are unequal, it is difficult to predict the density growth and intermediary states may be non-fixed states. Therefore, we cannot only rely on the analytical or numerical solutions and must simulate our model to prove and define an attack impact on the



(a) $T = 30s$ and attack timing settings are $t_{start} = 1T$ and $t_{\Delta} = 10T$.



(b) $T = 90s$ and attack timing settings are $t_{start} = 1T$ and $t_{\Delta} = 10T$.

Fig. 9. Graphs of Poincare Maps for k_1 with $\pi = 0.3$, $\xi = 0.75$ and initial states with DEO = (3, 8) where $\pi_{1,\Delta} = \pi_{2,\Delta} \in \{0.4, 0.5\}$.

asymptotic average network flow. However, we can still reduce the complexity of attack impact estimation for state-changing attacks. This may be achieved by identifying states with DEO_0 that are vulnerable to attacks with target DEO_{Δ} through an "estimation" of the direction of the growth of (k_1, k) from the sum of the exponential coefficients in the Poincare Map equations. Let λ in Eq. (9) be the sum of these exponential coefficients. If λ is zero, then the system is in a possibly fixed state. If λ is nonzero, the density evolution is nonzero and k_1 is either constantly increasing or decreasing.

$$\lambda(k_1, k) = A_{p_2} k_1 + B_{p_2} + A_{p_1} k_1 + B_{p_1} \tag{9}$$

where $p_1 \in [1, 4]$ & $p_2 \in [5, 8]$ and A and B are exponential coefficients corresponding to the region-based definitions of the differential equation $\frac{dk_1}{dt}$ (which has been derived and defined in previous work)

Given the attack model, we may identify if an initial state is vulnerable if the direction of density evolution leans toward the regions of the targeted DEO, DEO_{Δ}. Therefore, given an initial state x_0 with a DEO_0, we study the direction of growth under malicious modifications with an updated version of λ denoted as λ_{Δ} in Eq. (10). Note that we only consider an attack on one of the parameters (either both green time ratios or the cycle length).

$$\lambda(k_1, k)_{\Delta} = (A_{p_2} k_1 + B_{p_2}) \pi_{2,\Delta} T_{\Delta} + (A_{p_1} k_1 + B_{p_1}) \pi_{1,\Delta} T_{\Delta} \tag{10}$$

where $p_1 \in [1, 4]$ & $p_2 \in [5, 8]$

Given DEO_0 and $\pi_{1,\Delta}$ and $\pi_{2,\Delta}$, all region boundaries R, Poincare Maps, and NFDs for $\xi = 0.5$ and $\pi_1 = \pi_2 = \pi$ (see Fig. 7), we may use λ_{Δ} to discover potentially vulnerable states with DEOs of interest to an attacker. As an example, we

found two types of initial DEOs of interest for an attacker. These DEOs are (2, 6) and (4, 8). These initial DEOs correspond to "possible stationary" states according to the Poincare-Map based NFDs. States with DEO of (2, 6) have k_1 and k values that satisfy R_3 and R_8 when $\xi = 0.5$ but not when $\xi \neq 0.5$. Similarly, initial states with $DEO_0 = (4, 8)$ share common ranges of k_1 and k values with regions R_3, R_8, R_4 and R_7. Hence, for demonstration purposes we describe how to assess which states are vulnerable to State-Changing attacks when: (1) $DEO_0 = (2, 6)$ and $DEO_\Delta = (3, 8)$, and (2) $DEO_0 = (4, 8)$ and $DEO_\Delta \in \{(4, 7), (3, 8)\}$. For all potentially vulnerable initial states, we may analytically estimate and infer some insights from the attack impact $q_\Delta - q_0$ from the initial (DEO_0) and targeted (DEO_Δ) DEOs, as $q(k)_{DEO_0} - q(k)_{DEO_\Delta}$ using the NFDs. However, since the attack impact is also a function of k_1, we require simulation to compute the actual k_1 at the end of the attack at time $t_{start} + t_\Delta$.

4.2.1. Scenario when $\text{DEO}_0 = (2, 6)$ *and* $DEO_\Delta = (3, 8)$

Given $x_0 = (k_1(0), k)$ with DEO_0 of (2, 6) and $\xi_1 = \xi_2 = \xi = 0.5$. From the definitions of the region boundaries, it is clear that k_1 must increase for a change in DEO from (2, 6) to (3, 8) as long as k satisfies the boundaries of k for all regions R_2, R_3, R_6, R_8. For this scenario to be successful, $\lambda_\Delta > 0$ for the DEO of $x(t)$ must be satisfied so that (k_1, k) will increase and move toward a state with DEO of (3, 8) according to the region boundary definitions in our analytical studies. In the initial state with $DEO_0 = (2, 6)$, it is notable that $\lambda = 0$ since it is considered a stationary Lyapunov stable state. Thus, if $\pi_{1,\Delta} < \pi_{2,\Delta}$ then λ_Δ will be greater than zero.

4.2.2. Scenario when $\text{DEO}_0 = (4, 8)$ *and* $DEO_\Delta \in \{(4, 7), (3, 8)\}$

When the initial DEO is (4, 8) and $k_1 = k$ for stability and k satisfies the boundaries of (4, 7) or (3, 8), an attack may be successful as long as $\pi_{1,\Delta} > \pi_{2,\Delta}$ and $\xi \leq 0.5$ for $DEO_\Delta = (4, 7)$ or $\pi_{1,\Delta} < \pi_{2,\Delta}$ for $DEO_\Delta = (3, 8)$. This idea can also be extracted from similar logic to that in the previous section.

5. Experimental results

We will confirm the validity of each attack model by simulation with different levels of complexity.[1] First, we will use LQM and the Double Ring Road Network model. Then, going up a level of complexity, we will compare the impacts of the same attacks on a symmetric one-way grid network model of multiple intersections[1]. For our experiments, we let $T = 30$ s and $T = 90$ s for various runs, $L = 0.25$ and $t_{finish} = 20T$. We also choose an update time step of 0.05 s. Table 3 contains information on the range and number of initial states tested for each attack model. $DEO_0 \in [(3, 8), (4, 7)]$ correspond to Non-State-Changing attacks and $DEO_0 \in [(2, 6), (4, 8)]$ correspond to State-Changing attacks.

5.1. LQM with double ring road network

5.1.1. Non-state-changing attacks on asymptotic gridlock states

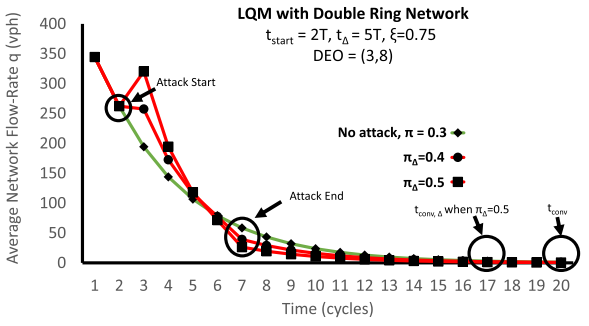
To validate our analytical observations in Section 4.1, we simulated the attacks with the LQM and Double Ring Road Network. Below are figures describing the impacts of different modified green time ratios on the asymptotic stable gridlock states under the constraint that $\pi_{1,\Delta} = \pi_{2,\Delta}$ and the DEO does not change. We consider two cases where modifications included $\pi_\Delta = \pi_{1,\Delta} = \pi_{2,\Delta} \in \{0.4, 0.5\}$: (1) $t_{start} = 2T$ and $t_{start} + t_\Delta = 7T$ (Fig. 10a and b), (2) $t_{start} = 1T$ and $t_{start} + t_\Delta = 11T$ (Fig. 10c and d).

As can be seen in Fig. 10a and b, for an attack with $t_{start} = 2T$ and $t_\Delta = 5T$ with $\pi_\Delta = 0.5$, the approximate average impact is $t_{conv,\Delta} - t_{conv} = 20T - 17T = -3T$ (1.17 convergence speedup) for both DEOs. In Fig. 10c and d, we have $t_{start} = 1T$ and $t_\Delta = 10T$. When $\pi_\Delta = 0.5$, the impact is $-6T$ (1.4 convergence speedup) for initial states with DEO = (4, 7) and $-7T$ (1.5 convergence speedup) for initial states with DEO = (3, 8). The sudden yet temporary rise in flow for attacks on initial states with DEO = (3, 8) is possibly due to order of phases (ring 1 first) and the increase in green time. As this is just a motivational case study, more severe impacts may occur from longer-lasting or earlier-starting attacks. Additionally, combinations of different attack categories may add up to more detrimental impacts.

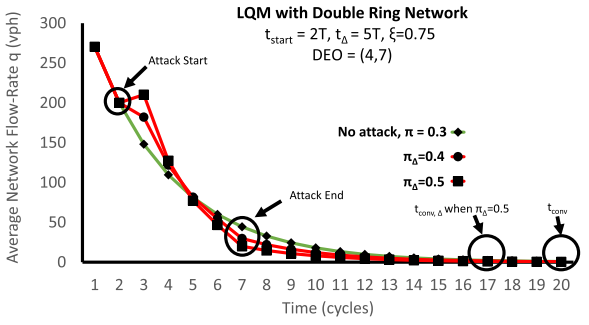
Having an effective green time ratio of 0.3 may be deemed as unrealistic in practice since this would mean for a cycle length $T = 90$ s, the lost time tlost would be 18 s and each effective green time would be 27 s. Although this satisfies the minimum green time and maximum green time constraints for a traffic signal cycle of 90 s, this would be quite unrealistic in practice since a lot of time would be wasted for just waiting. Therefore, we consider a closer-to-realistic case of 13.5 s for each lost time where the effective green time ratios would then be 0.35 for both phases and 9 s for each lost time for effective green time ratios of 0.4. Thus, when the attacker gains access, when the system is in an asymptotic gridlock state with DEO = (3, 8) or (4, 7), they have the option of increasing the cycle length or decreasing the lost time to accelerate the convergence to gridlock (since the effective green time ratios are increased as a result). However, they are still constrained by the minimum lost time, which is about 3 s per phase. Thus, the most the attacker can force the effective green time ratios for $T = 90$ s would be about 0.48 where 43 s would be the green time for each phase.

In Fig. 11, we have the simulation results for this situation for $\xi = 0.75$, π=0.35, $\pi_\Delta = 0.48$, $t_{start} = 1T$ and $t_\Delta = 10T$, thus showing that the attack is very capable of reducing the control response time for the system engineers. We can see

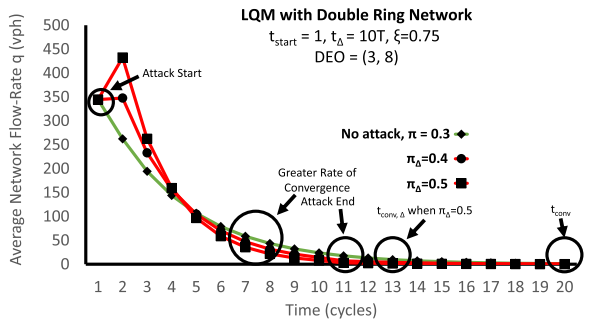
[1] All simulation code for this section is provided in https://github.com/AICPS/LQM_traffic_sec_official.



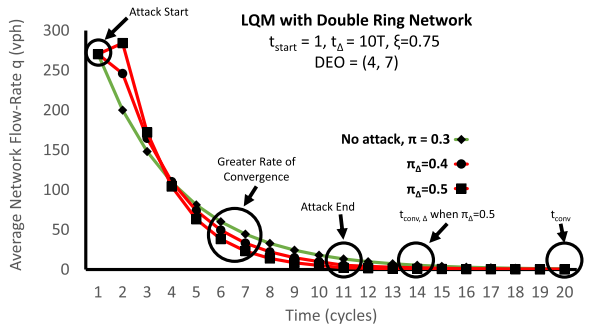
(a) $DEO_\Delta = (3, 8)$, $T = 30s$, $t_{start} = 2T$, and $t_\Delta = 5T$.



(b) $DEO_\Delta = (4, 7)$, $T = 30s$, $t_{start} = 2T$, and $t_\Delta = 5T$.



(c) $DEO_\Delta = (3, 8)$, $T = 90s$, $t_{start} = 1T$, and $t_\Delta = 10T$.



(d) $DEO_\Delta = (4, 7)$, $T = 90s$, $t_{start} = 1T$, and $t_\Delta = 10T$.

Fig. 10. Non-state-changing attack simulations for LQM and double ring road network with $t_{finish} = 20T$, $\pi = 0.3$, $\xi = 0.75$, $\pi_\Delta = \pi_{1,\Delta} = \pi_{2,\Delta} \in \{0.4, 0.5\}$.

that the line corresponding to no attack hits very close to gridlock (less than 0.5 average flow-rate) at around $16T$ and the attack line hits very close to gridlock at $11T$ in the figure. This means the convergence speed-up is $16T/11T$, which is approximately 1.5x. We also found that if we set the initial effective green time ratios to 0.4, the initial convergence time is around $15T$ and the behavior is quite close to when they are initially 0.35.

Although demonstrated and studied in previous work, we also provide some results when the retaining ratios are chosen randomly from a range of values under the studied non-state changing attack model. For the non-state-changing attack

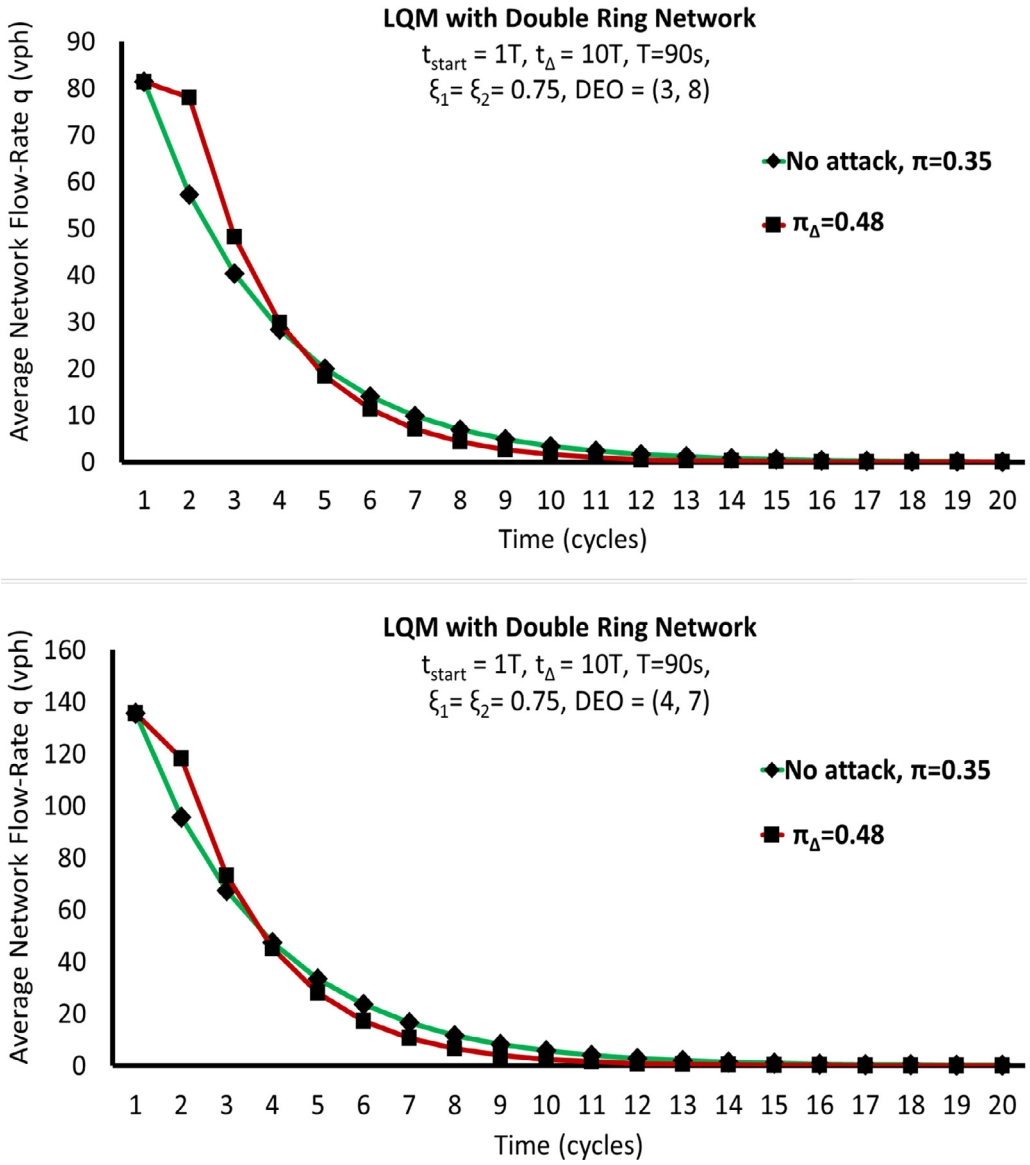


Fig. 11. Non-state-changing attack model simulations with higher and more realistic initial effective green time ratio π=0.35 and modified effective green time ratio π_Δ=0.48. These effective green time ratios are more realistic because the lost times are more reasonable per cycle. Acceleration of convergence time and reduction of control response time is apparent here just as it is in previous simulations. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

model, we had assumed a retaining ratio of 0.75 in our simulations. In the following results, we assume a random retaining ratio chosen from the range of [0.51–0.99] for both rings (common in practice and in reality as well Roess et al., 2019). In Figs. 12 and 13, we may observe the effects of having asymmetric and random retaining ratios for each ring ($\xi_1 = 0.901$, $\xi_2 = 0.813$ and $\xi_1 = 0.571$, $\xi_2 = 0.945$) on the system and attack modeling behaviors. We can see that the overall behaviors are similar to the results in the previous graphs despite the random and unequal retaining ratios. Note, there are some clear unique behaviors for the simulations regarding $\xi_1 = 0.571$ and $\xi_2 = 0.945$ for $DEO_\Delta = (3, 8)$ because the difference between ξ_1 and ξ_2 is large and the larger retaining ratio is for the less congested ring (ring 2). Thus it will take a longer time to converge to the asymptotic limit. Results for other identified vulnerable states provide similar insights and confirm that as long as the retaining ratios are within the specified range of [0.51–0.99], the attack model is applicable.

5.1.2. State-changing attacks on initial stationary states

In Fig. 14a, the initial states have a DEO of (2, 6) and the initial settings are $\pi = \pi_1 = \pi_2 = 0.5$, $T = 90$ s. The attack parameters include $(\pi_{1,\Delta}, \pi_{2,\Delta}) \in \{(0.4, 0.6), (0.35, 0.65), (0.3, 0.7)\}$ where $t_{start} = 2T$, $t_\Delta = 5T$, and $t_{start+\Delta} = 7T$. In Fig. 14b, the initial states have a DEO of (4, 8) with same initial signal settings and simulation settings as above.

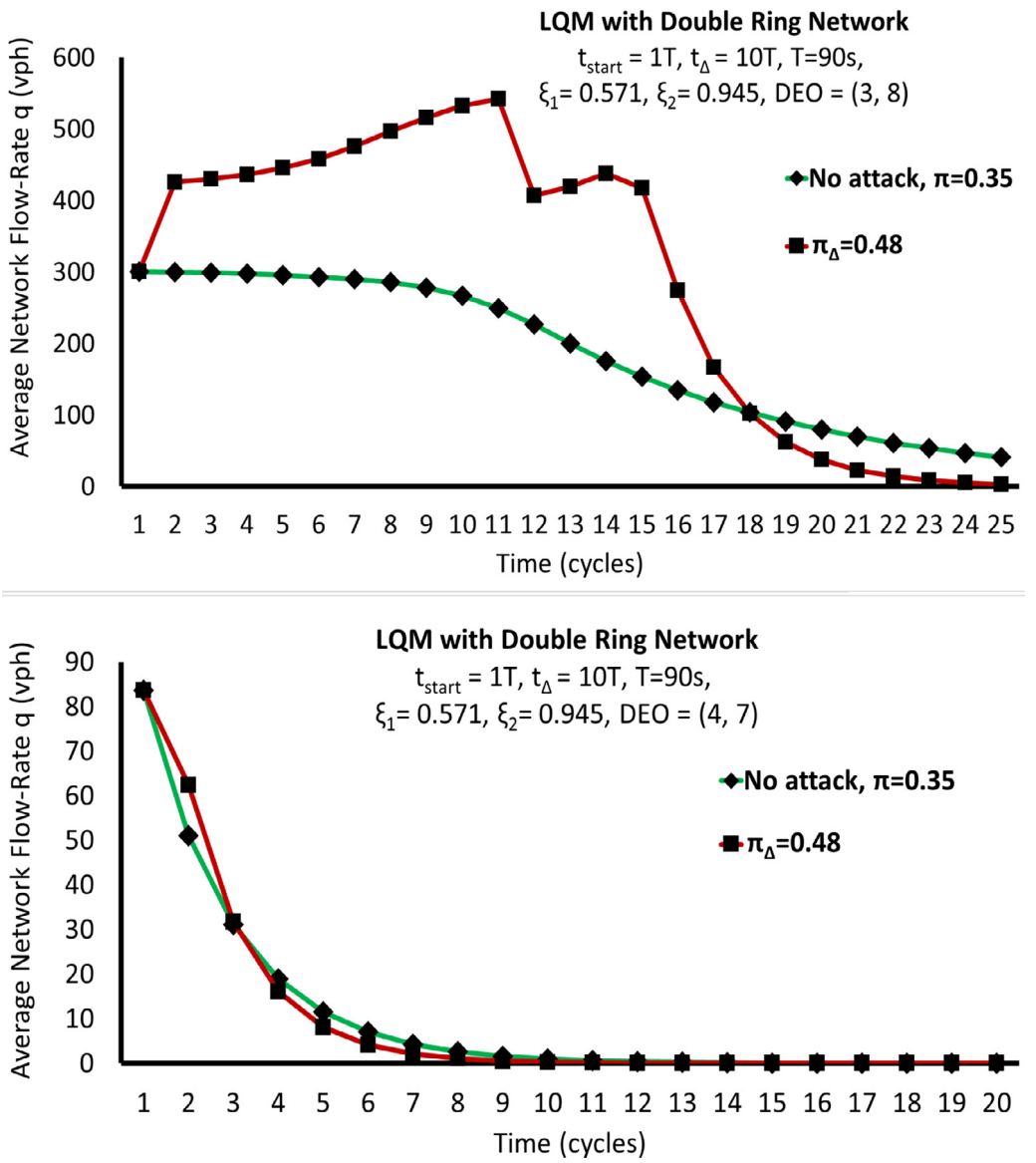


Fig. 12. Non-state-changing attack model simulations with randomly selected and asymmetric retaining ratios, $\xi_1 = 0.571$ and $\xi_2 = 0.945$. For a targeted $DEO_\Delta = (3, 8)$, the initial state is $(k_1, k) = (144, 84)$ and for a targeted $DEO_\Delta = (4, 7)$, the initial state is $(k_1, k) = (15, 76)$.

Notice that the overall impacts are greater on initial states with DEOs of (4, 8) rather than attacks on those with (2, 6). This is because of the order of phases and that $\pi_{1,\Delta} < \pi_{2,\Delta}$. If $\pi_{1,\Delta} > \pi_{2,\Delta}$ instead, the effectiveness of increasing the duration and modifications would be reversed. To give a better idea on the impacts of these state-changing attacks, we provide Table 2. The rows correspond to the different combinations of initial states, DEOs, and attack timing settings while the columns refer to different modifications. From just a few cycles of modified green time ratios, an attack can vary from 37% to a 99% drop in average flow.

5.2. LQM with grid network

We have evaluated the same attacks in Section 2.3 using LQM and a grid network (like that in Fig. 4) where each ring number corresponds to each direction (E-W and N-S) at each intersection and cars leaving the network are added back to their respective entrances to maintain the overall density (more details are in Jin, 2003; Gan et al., 2017).

We opted to not provide the grid network simulation results for the 4×4 grid network (with 32 links) since we found that the results from the Double Ring Road Network and the grid network simulations on average are similar to each other

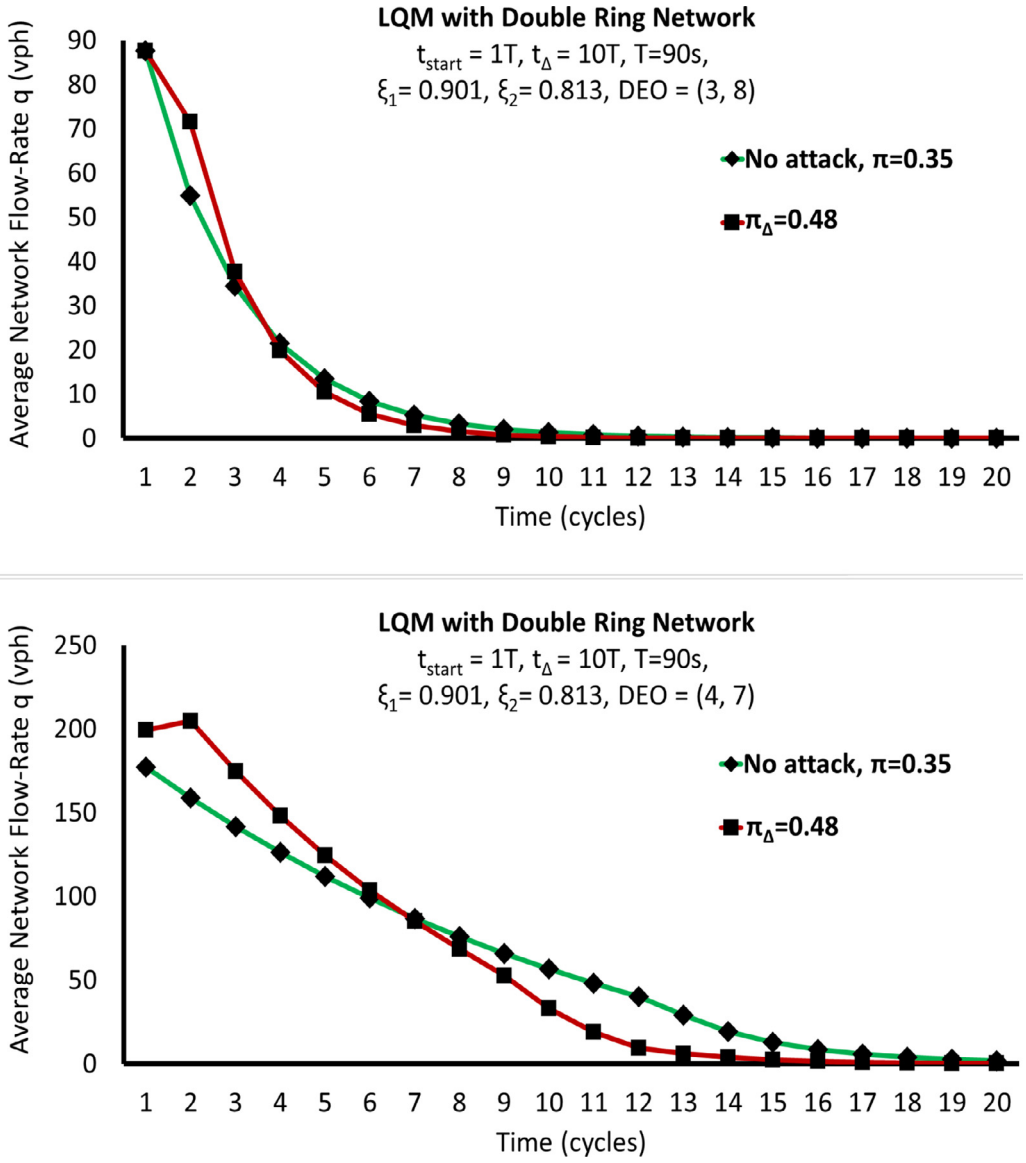
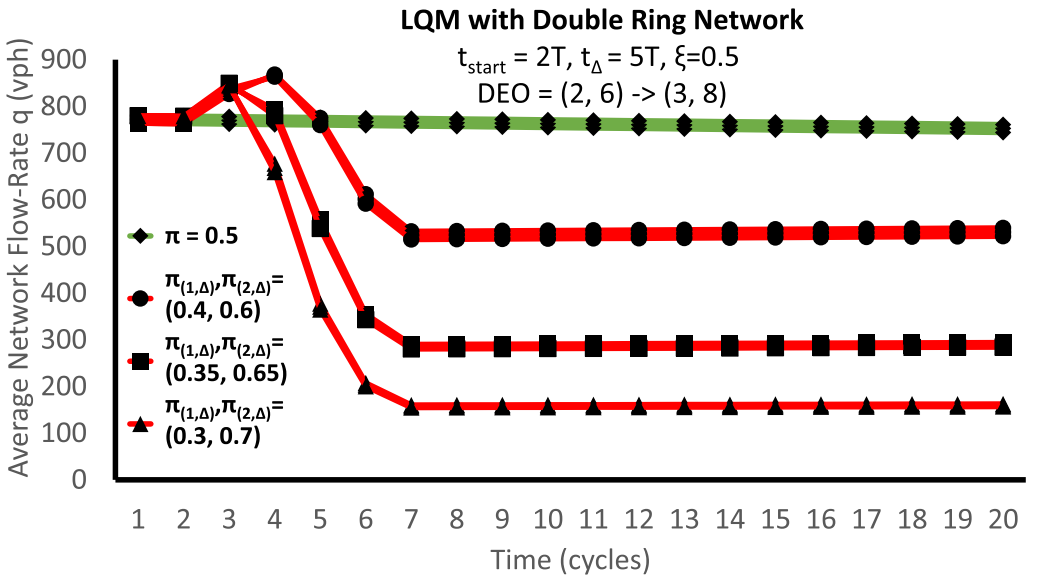


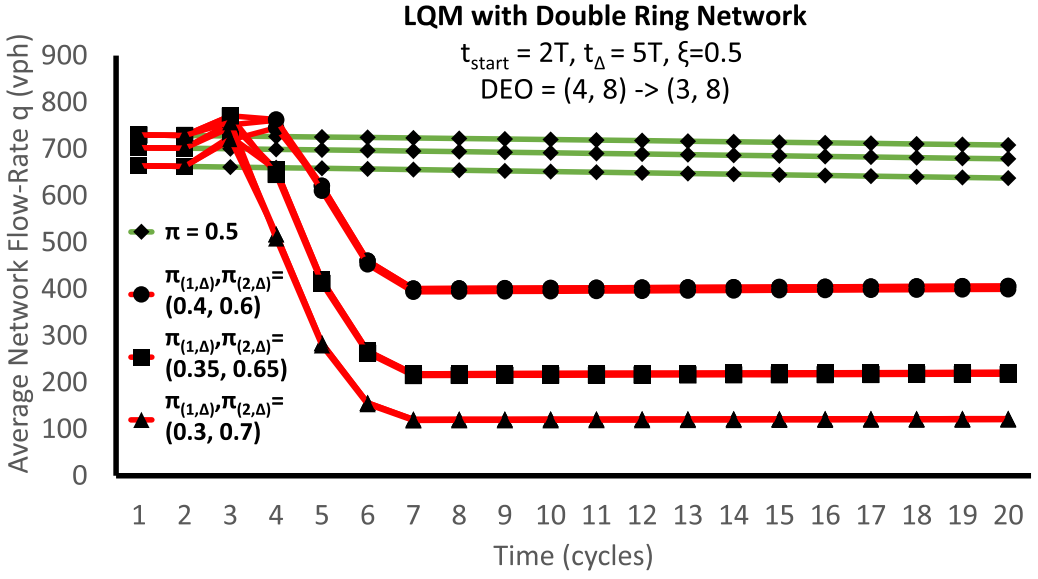
Fig. 13. Non-state-changing attack model simulations with randomly selected and asymmetric retaining ratios ξ_1= 0.901 and ξ_2= 0.813. For a targeted $DEO_\Delta = (3, 8)$, the initial state is $(k_1, k) = (144, 84)$ and for a targeted $DEO_\Delta = (4, 7)$, the initial state is $(k_1, k) = (15, 76)$.

Table 2
Average impact metric $q_\Delta - q_0$ (in vph) and average drop in flow (in percentage) for the considered State-Changing Attack models ($\xi = 0.5$, $\pi = 0.5$, $DEO_\Delta = (3, 8)$).

	Attack Modifications		
Initial State and Timing Parameters	$\pi_{(1,\Delta)}, \pi_{(2,\Delta)}$= 0.4, 0.6	$\pi_{(1,\Delta)}, \pi_{(2,\Delta)}$= 0.35, 0.65	$\pi_{(1,\Delta)}, \pi_{(2,\Delta)}$= 0.3, 0.7
DEO_o = (2, 6) t_{start}, t_Δ = 2T, 5T	-334.45 42%	-543.34 68%	-655.31 83%
DEO_o = (2, 6) t_{start}, t_Δ = 1T, 11T	-691.15 37%	-767.35 66%	-786.59 81%
DEO_o = (4, 8) t_{start}, t_Δ = 2T, 5T	-256.29 45%	-399.25 70%	-475.87 83%
DEO_o = (4, 8) t_{start}, t_Δ = 1T, 11T	-500.41 86%	-552.56 97%	-565.73 99%



(a) Attacks on three initial states with DEO = (2, 6).



(b) Attacks on three initial states with DEO = (4, 8).

Fig. 14. Simulations with LQM and double ring road network of state-changing attacks. Attack timing settings are $t_{start} = 2T$ and $t_\Delta = 5T$.

with above 95% accuracy. The similarity was computed via the L1 norm and by using the grid network simulation results as the nominal values.

We have further simulated the LQM with a larger 6x6 grid network with 72 links and provide simulation results in Fig. 15 for an initial density $(k_1, k) = (144, 84)$ (same initial state as results in Figs. 12 and 13). The top graph refers to simulations when the link retaining ratios are randomly selected (e.g., $\xi_i \in [0.51, 0.99]$) at the beginning but remain the same throughout the simulation, and the bottom graph refers to simulations when they are equal to 0.75 (e.g., ξ=0.75) using $\pi = 0.35$ and $\pi_\Delta = 0.48$). For this case study, it is clear that from the top graph, the average grid network flow is slightly less than the average Double Ring Road Network flow. From the bottom graph, we can see that the overall grid network average flow is higher (almost double) for random retaining ratios with respect to the Double Ring Road simulation data. It is clear that the randomness of retaining ratios will have a significant effect on the understanding of traffic behaviors. Importantly, however, is that no matter the retaining ratio settings, the expected asymptotic behavior of the grid network simulations match that of the Double Ring Road Network, as we had hoped in our analysis of possibly fixed asymptotic gridlock states.

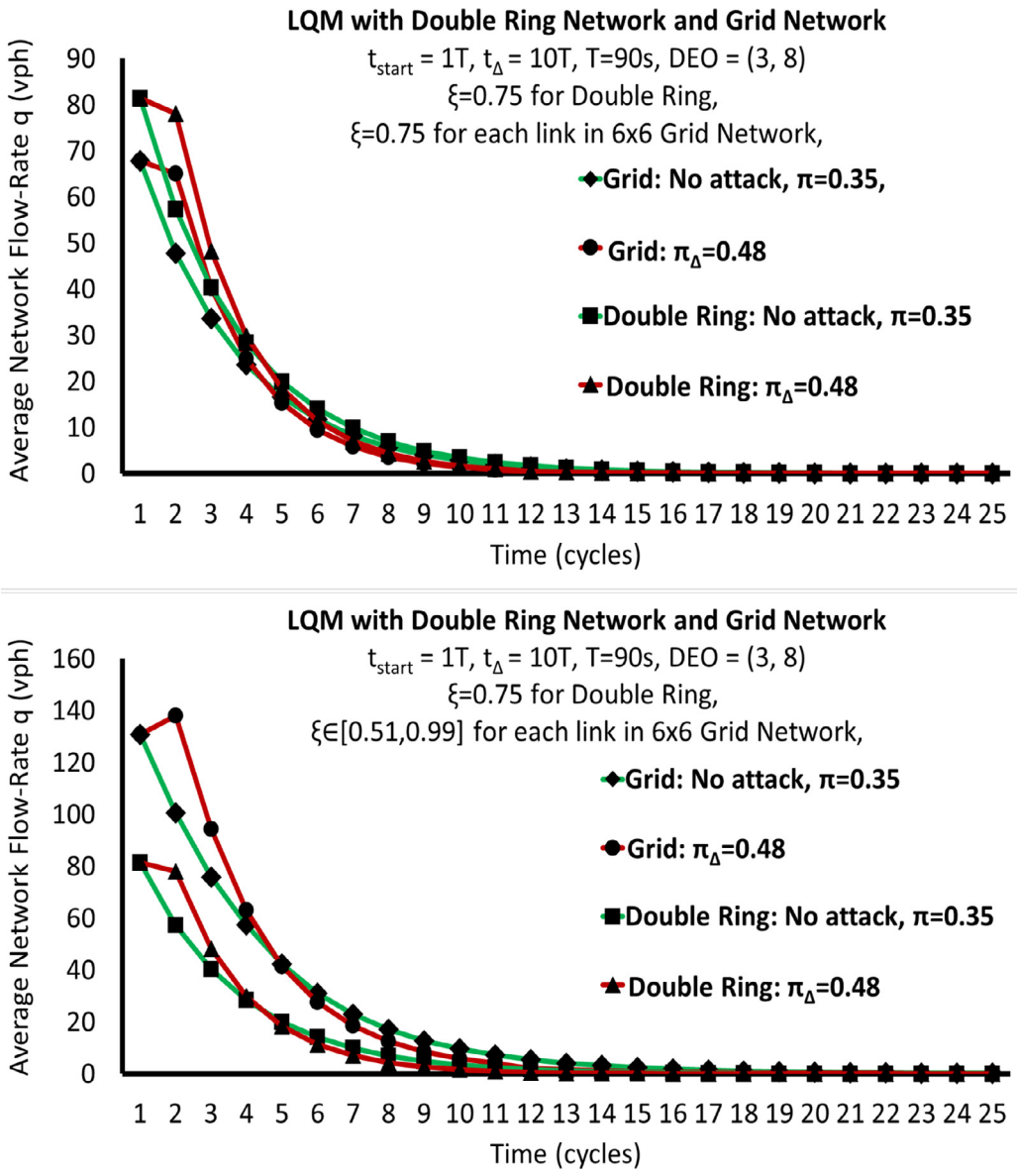


Fig. 15. Non-state-changing attack simulation result comparisons between double ring road network and 6x6 grid network. Top: grid network with all link retaining ratios $\xi = 0.75$. Bottom: grid network with randomized link retaining ratios $\xi \in [0.51, 0.99]$.

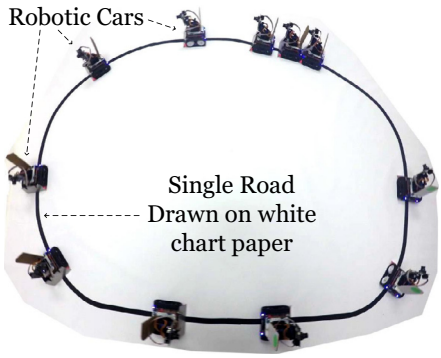


Fig. 16. Another setup of the test-bed for single road model with length 4824 cm and 11 robotic vehicles (larger version of test-bed shown in Fig. 3).

Table 3
Experimental setup: number of different initial states according to range of density values (k_1, k) values per each type of pair of DEO and turning ratio combination studied in our attack models (both Non-State Changing and State-Changing).

DEO of Initial State (π=0.5 & T=90s)	Number of Tested Initial States and Range of (k1, k) Values
DEO_o = (2, 6) ξ=0.5	100 (72, 75) – (90, 84)
DEO_o = (4, 8) ξ=0.5	310 (91, 85) – (150, 150)
DEO_o = (3, 8) ξ=0.75	1520 (2, 76) – (148, 149)
DEO_o = (4, 7) ξ=0.75	1471 (118, 76) – (150, 149)

Table 4
Boundary conditions for region $R_p = R_{p,k_1}, R_{p,k}$ where $R_p \in R$ that make up a density evolution orbit (DEO).

Region (p)	Signal phase indicators ($\delta_1(t)$, $\delta_2(t)$)	Conditions (R_{p,k_1}, $R_{p,k}$)	$\frac{dk_1}{dt}$
1	(1,0)	$0 < k_1 < k_c,\ \frac{k_1}{2} \le k \le \frac{k_j}{2} - \frac{((1-\xi)k_j-(2-\xi_1)k_c)k_1}{2k_c}$	$\frac{-(1-\xi_1)}{L} D_1$
2	(1,0)	$k_c \le k_1 < k_j - \xi_1(k_j - k_c),\ \frac{k_1}{2} \le k \le \frac{\xi_1 k_j + (1-\xi_1)k_c + k_1}{2}$	$\frac{-(1-\xi_1)}{L} C$
3	(1,0)	$k_j - \xi_1(k_j - k_c) \le k_1 \le k_j,\ \frac{k_1}{2} \le k \le \frac{2\xi_1 - 1}{2\xi_1} k_j + \frac{k_1}{2\xi_1}$	$\frac{-(1-\xi_1)}{L} \frac{S_1}{\xi_1}$
4	(1,0)	$0 < k_1 < k_j,\ max\{\frac{k_j}{2} - \frac{[(1-\xi_1)k_j-(2-\xi_1)k_c]k_1}{2k_c}, \frac{\xi_1 k_j + (1-\xi_1)k_c + k_1}{2}, \frac{2\xi_1-1}{2\xi_1} k_j + \frac{k_1}{2\xi_1}\} < k \le \frac{k_j + k_1}{2}$	$\frac{-(1-\xi_1)}{L} \frac{S_1}{1-\xi_1}$
5	(0,1)	$0 \le k_1 \le k_j,\ \frac{k_1}{2} \le k \le \min\{\frac{k_1 + k_c}{2}, \frac{k_1}{2} + \frac{k_c(k_j - k_1)}{2(1-\xi_2)(k_j - k_c)}\}$	$\frac{(1-\xi_2)}{L} D_2$
6	(0,1)	$0 \le k_1 \le k_j - (1-\xi_2)(k_j - k_c),\ \frac{k_1 + k_c}{2} < k \le \frac{k_j + k_1 - \xi_2(k_j - k_c)}{2}$	$\frac{(1-\xi_2)}{L} C$
7	(0,1)	$0 \le k_1 \le k_j,\ max\{\frac{k_j + k_1 - \xi_2(k_j - k_c)}{2}, \frac{(1-2\xi_2)k_j + k_1}{2(1-\xi_2)}\} < k \le \frac{k_1 + k_j}{2}$	$\frac{(1-\xi_2)}{L} \frac{S_2}{\xi_2}$
8	(0,1)	$k_j - (1-\xi_2)(k_j - k_c) < k_1 \le k_j,\ \frac{k_1}{2} + \frac{k_c(k_j - k_1)}{2(1-\xi_2)(k_j - k_c)} < k < \frac{(1-2\xi_2)k_j + k_1}{2(1-\xi_2)}$	$\frac{(1-\xi_2)}{L} \frac{S_2}{1-\xi_2}$
9	(0,0)	and transition from $(\delta_1(t), \delta_2(t)) = (1, 0)$	0
10	(0,0)	and transition from $(\delta_1(t), \delta_2(t)) = (0, 1)$,	0

Lastly, the attack impact on the convergence time is similar despite the different network models and retaining ratios. With respect to the Double Ring Road Network when $\xi = 0.75$, the attack impact is $t_{conv} - t_{conv,\Delta} = 16T - 12T = 4T$ and $16T/12T = 1.3x$ convergence speedup. With respect to the grid network when $\xi = 0.75$ for each link, the attack impact is $t_{conv} - t_{conv,\Delta} = 15T - 12T = 3T$ and $15T/12T = 1.25x$ speed up, which is quite close to 1.3x! And finally, when $\xi \in [0.51, 0.99]$ for each link in the grid network, the attack impact is $t_{conv} - t_{conv,\Delta} = 22T - 18T = 4T$ and $22T/18T = 1.2x$ speedup! Thus, although the exact times of the convergence is different for the grid network with random retaining ratios per each link, the actual impact on the convergence is similar (10% average distance between each other and same overall behaviors) for all three cases, showing the value of our attack models and their analysis.

It is true, however, that the dependencies and connections are definitely not negligible and some subtle behaviors in a grid network with microscopic modeling behaviors and/or other more dynamic road networks may be missed. The Double Ring Road Network Model abstracts the grid network well since both models follow the same inflow and outflow definitions for the intersections of roads and because we assume that the grid network is a closed network with periodic boundary conditions. A noticeable difference is that we cannot observe certain unstable traffic behavior patterns in the grid network simulations. This means that Poincare Maps are not always usable to clearly define the unstable state traffic behaviors in experiments or practice. Nevertheless, in experiments or in practice, we may use our defined DEOs to identify if a state is potentially in an unstable state or not, providing the possibility to detect or analyze the impact of a potential attack.

In our previous work (Gan et al., 2017; Gan, 2014), we have shown that the results of simulating LQM with the double ring road and those with the grid network are still quite similar for when we assume symmetric retaining ratios, signal settings and initial densities. Yet when these are randomized throughout the grid network, we have only found some slight differences in the analytical results (e.g., with lower average densities, the grid network will converge to gridlock with random retaining ratios). Compared to other system and attack models, our models offer unique insights with respect to overall average network behaviors. It is built from simpler differential equations and even from Poincare Maps, which are extremely challenging to derive in traffic modeling theory. Through them, we have discovered new traffic network behaviors and insights within the context of a methodology for attack modeling and analysis on connected fixed time traffic control systems. Through this work, more rigorous ITS security models, analysis and design methods, and simulation tools may be developed to ensure the security and safety of promising ITS use cases.

6. Conclusion

In this paper, we developed a methodology to model attacks on connected fixed-timing traffic control systems and evaluate their impacts on traffic networks such as grid networks in Manhattan. The methodology is built upon the Link Queue Model (LQM) which is an abstracted form of the Cell Transmission Model (CTM). However, it remains as accurate and more efficient to simulate than the CTM. For certain settings, Poincare Maps can be analytically and numerically derived to quickly estimate the performance of the system given the initial state and settings. Otherwise, we use the LQM and Double Ring Road Network to simulate either non state-changing or state-changing attacks on intersections or grid networks and evaluate their impacts. A simple attack that modified the green time ratios from (0.5, 0.5) to (0.35, 0.65) for 5 cycles could potentially cause an average drop in flow rate of 66%. Under certain settings, the attack could even cause a 99% drop in average flow (gridlock)!

Lastly, the proposed attack modeling and impact analysis methodology can easily be built upon with more complex attacks (e.g., combinations of small changes, turning ratio modifications) and metrics (e.g., deviation from optimal state). In turn, these attacks may be used as part of a security analysis tool to come up with a robust and resilient traffic control system design. In such a traffic control system, attack detection and mitigation may be possible through additional computing devices and sensors integrated with control logic that can predict or identify a potential attack at any given moment.

CRediT authorship contribution statement

Anthony Lopez: Conceptualization, Methodology, Software, Data curation, Writing - original draft, Visualization, Investigation, Validation, Writing - review & editing. **Wenlong Jin:** Supervision, Writing - review & editing. **Mohammad Abdullah Al Faruque:** Supervision, Writing - review & editing.

Acknowledgments

The second author would like to thank the PSR and UCCONNECT University Transportation Centers for their financial support.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.trb.2020.07.002

References

Agadakos, I., Chen, C.-Y., Campanelli, M., et al., 2017. Jumping the air gap: modeling cyber-physical attack paths in the internet-of-things. In: Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and Privacy. ACM, New York, NY, USA, pp. 37–48.
Behrisch, M., Bieker, L., Erdmann, J., Krajzewicz, D., 2011. Sumo–simulation of urban mobility: an overview. In: Proceedings of SIMUL 2011, The Third International Conference on Advances in System Simulation. ThinkMind.
Cerrudo, C., 2013. Hacking US (and UK, Australia, France, etc.) traffic control systems. https://ioactive.com/hacking-us-anduk-australia-france-etc/.
Cerrudo, C., 2014. Hacking US traffic control systems. In: Proc. DEFCON, pp. 1–5.
Cerrudo, C., 2015. An emerging US (and world) threat: cities wide open to cyber attacks. Secur. Smart Cities.
Cerrudo, C., Spaniel, D., 2015. Keeping smart cities smart: preempting emerging cyber attacks in US cities. Inst. Crit. Infrastruct. Technol.
Checkoway, S., McCoy, D., Kantor, B., et al., 2011. Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium.
Chen, Q.A., Yin, Y., Feng, Y., et al., 2018. Exposing congestion attack on emerging connected vehicle based traffic signal control. Network and Distributed Systems Security (NDSS) Symposium 2018.
Daganzo, C.F., 1995. The cell transmission model, part II: network traffic. Transp. Res. Part B 29 (2), 79–93.
Dobersek, M. M., 1998. An operational comparison of pre-time, semi-actuated, and fully actuated interconnected traffic control signal systems.
Evtimov, I., Eykholt, K., Fernandes, E., et al., 2017. Robust physical-world attacks on machine learning models. arXiv:1707.08945 CoRR.
Foundation, N. S., 2018. Computer and network systems (CNS): core programs program solicitation NSF 18–569. https://www.nsf.gov/pubs/2018/nsf18569/nsf18569.htm.
Gan, Q., 2014. Macroscopic modeling and analysis of urban vehicular traffic. UC Irvine Ph.D. thesis.
Gan, Q.-J., Jin, W.-L., Gayah, V.V., 2017. Analysis of traffic statics and dynamics in signalized networks: a poincaré map approach. Transp. Sci. 51 (3), 1009–1029.
Gemeinschaften, K.E., 2001. White Paper-European Transport Policy for 2010: Time to Decide. Office for Official Publications of the European Communities.
Ghafouri, A., Abbas, W., Vorobeychik, Y., Koutsoukos, X., 2016. Vulnerability of fixed-time control of signalized intersections to cyber-tampering. In: Resilience Week (RWS), 2016. IEEE, pp. 130–135.
Ghena, B., Beyer, W., Hillaker, A., et al., 2014. Green lights forever: analyzing the security of traffic infrastructure. WOOT 14, 7.
Goldwasser, S., Micali, S., 1984. Probabilistic encryption. J. Comput. Syst. Sci. 28 (2), 270–299.
Gu, Y., Qian, Z., Zhang, G., 2017. Traffic state estimation for urban road networks using a link queue model. Transp. Res. Rec. 2623 (1), 29–39.
Hasbini, M.A., Cerrudo, C., Jordan, D., et al., 2016. The smart city department cyber security role and implications. Secur. Smart Cities.
Hossain, M.M., Fotouhi, M., Hasan, R., 2015. Towards an analysis of security issues, challenges, and open problems in the internet of things. In: Services (SERVICES), 2015 IEEE World Congress on. IEEE, pp. 21–28.
Hubaux, J.P., Capkun, S., Luo, J., 2004. The security and privacy of smart vehicles. IEEE Secur. Privacy 2 (3), 49–55.
Jin, H.-Y., Jin, W.-L., 2015. Control of a lane-drop bottleneck through variable speed limits. Transp. Res. Part C 58, 568–584.
Jin, W., 2003. Kinematic wave models of network vehicular traffic. arXiv:0309060.
Jin, W.-L., 2012. A link queue model of network traffic flow. arXiv:1209.2361.
Jin, W.-L., 2015. Point queue models: a unified approach. Transp. Res. Part B 77, 1–16.
Jin, W.-L., Jin, H., 2014. Analysis and design of a variable speed limit control system at a freeway lane-drop bottleneck: a switched systems approach. In: 53rd IEEE Conference on Decision and Control. IEEE, pp. 1753–1758.

Julia Carrillo, M., 2015. Robotic cars test platform for connected and automated vehicles Master's thesis. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2016-03-28.
Kelarestaghi, K. B., Heaslip, K., Gerdes, R., 2018. Vehicle security: Risk assessment in transportation. arXiv:1804.07381.
Koblitz, N., 2007. The uneasy relationship between mathematics and cryptography. Not. AMS 54 (8), 972–979.
Koonce, P., Rodegerdts, L., Lee, K., et al., 2008. Traffic signal timing manual. US department of transportation, federal highway administration, 1200 New Jersey avenue, se Washington, DC 20590, publication number fhwa-hop-08-024, June 2008.
Laszka, A., Potteiger, B., Vorobeychik, Y., et al., 2016. Vulnerability of transportation networks to traffic-signal tampering. In: Proceedings of the 7th International Conference on Cyber-Physical Systems. IEEE Press, p. 16.
Leyden, J., 2008. Polish teen derails tram after hacking train network: turns city network into hornby set.
Papageorgiou, M., Diakaki, C., Dinopoulou, V., et al., 2003. Review of road traffic control strategies. Proc. IEEE 91 (12), 2043–2067.
Reilly, J., Martin, S., Payer, M., Bayen, A.M., 2016. Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security. Transp. Res. Part B 91, 366–382.
Reilly, J., Martin, S., Payer, M., et al., 1755. On cybersecurity of freeway control systems: analysis of coordinated ramp metering attacks 2. Transportation Research Board 94th Annual Meeting.
Roess, R.P., Prassas, E.S., McShane, W.R., 2019. Traffic Engineering, fifth ed. Pearson/Prentice Hall.
Rogaway, P., 2009. Practice-oriented provable security and the social construction of cryptography. Unpublished essay.
Shoukry, Y., Mishra, S., Luo, Z., Diggavi, S., 2018. Sybil attack resilient traffic networks: a physics-based trust propagation approach. In: Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems. IEEE Press, pp. 43–54.
Sorensen, P., Wachs, M., Min, E.Y., et al., 2008. Moving Los Angeles: Short-Term Policy Options for Improving Transportation. Rand Corporation.
Sugiyama, Y., Fukui, M., Kikuchi, M., et al., 2008. Traffic jams without bottlenecks-experimental evidence for the physical mechanism of the formation of a jam. New J. Phys. 10 (3), 033001.
Teschl, G., 2012. Ordinary Differential Equations and Dynamical Systems, 140. American Mathematical Society Providence.
Thing, V.L.L., Wu, J., 2016. Autonomous vehicle security: a taxonomy of attacks and defences. In: 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 164–170.
U. S. D. of Transportation, 2018. About ITS Standards: ITS Standards and the U.S. DOT ITS Research Initiatives. Technical Report. https://www.standards.its.dot.gov/LearnAboutStandards/ResearchInitiatives.
U. S. D. Transportation: Federal Highway Administration, 2011. Adaptive Signal Control Technologies. Technical Report. https://www.fhwa.dot.gov/innovation/everydaycounts/edc-1/pdf/ascbrochure.pdf.
Ubiergo, G.A., Jin, W.-L., 2016. Mobility and environment improvement of signalized networks through vehicle-to-infrastructure (V2I) communications. Transp. Res. Part C 68, 70–82.
Urbanik, T., Tanaka, A., Lozner, B., et al., 2015. Signal Timing Manual. Transportation Research Board.
Varaiya, P., 2013. Max pressure control of a network of signalized intersections. Transp. Res. Part C 36, 177–195.
Wan, J., Lopez, A.B., Faruque, M.A.A., 2016. Exploiting wireless channel randomness to generate keys for automotive cyber-physical system security. In: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), pp. 1–10.
Weber, S., 2009. City sees red after engineers hack traffic signals: Engineers hacked traffic system as part of a labor protest.
Webster, F.V., 1958. Traffic signal settings. Technical Report.
Yuan, C., Thai, J., Bayen, A.M., 2016. Zubers against zlyfts apocalypse: an analysis framework for dos attacks on mobility-as-a-service systems. In: Proceedings of the 7th International Conference on Cyber-Physical Systems. IEEE Press, Piscataway, NJ, USA. 24:1–24:10. http://dl.acm.org/citation.cfm?id=2984464.2984488.
Zhang, J., Wang, F.-Y., Wang, K., et al., 2011. Data-driven intelligent transportation systems: a survey. IEEE Trans. Intell. Transp. Syst. 12 (4), 1624–1639.