Transportation Research Part B 91 (2016) 366–382

Contents lists available at ScienceDirect

Transportation Research Part B

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

Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cyber-security

Jack Reilly[a,*], Sébastien Martin[b], Mathias Payer[c], Alexandre M. Bayen[d]

[a] University of California, Berkeley, 652 Sutardja Dai, Berkeley, CA 94720, United States
[b] Massachusetts Institute of Technology, United States
[c] Purdue University, 305 N University Street, West Lafayette, IN 47907, United States
[d] University of California, Berkeley, 642 Sutardja Dai, Berkeley, CA 94720, United States

ARTICLE INFO

Article history:
Received 27 September 2014
Revised 30 May 2016
Accepted 31 May 2016
Available online 13 June 2016

Keywords:
Traffic optimization
Ramp metering
Cybersecurity
Multi-objective optimization

ABSTRACT

This article presents a study on freeway networks instrumented with coordinated ramp metering and the ability of such control systems to produce arbitrarily complex congestion patterns within the dynamical limits of the traffic system. The developed method is used to evaluate the potential for an adversary with access to control infrastructure to enact high-level attacks on the underlying freeway system. The attacks are executed using a predictive, coordinated ramp metering controller based on finite-horizon optimal control and multi-objective optimization techniques. The efficacy of the control schemes in carrying out the prescribed attacks is determined via simulations of traffic network models based on the cell transmission model with onramps modeled as queue buffers. Freeway attacks with high-level objectives are presented on two illustrative examples: congestion-on-demand, which aims to create precise, user-specified pockets of congestion, and catch-me-if-you-can, which attempts to aid a fleeing vehicle from pursuant vehicles.

1. Introduction

Public traffic infrastructure is arriving in the cyber age with increasing connectivity between the different segments of roadways. For example, freeways are commonly instrumented with loop detectors that allow for real-time monitoring of roadway speeds Jia et al. (2001). Estimates of road traffic conditions are then fed directly into onramp traffic light metering or variable speed limit algorithms which regulate traffic flow to improve congestion Chen et al. (2014); Papageorgiou et al. (1991). Finally, these metering algorithms can be coordinated and controlled by a remote command and monitoring center, leading to a regional network of interconnected sensors and controllers Kotsialos et al. (2001); Papamichail et al. (2010); Pisarski and Canudas-de Wit (2013); Reilly et al. (2014); Timotheou et al. (2015). Increased efforts to build systems which understand and utilize the interconnectivity are evidenced by *integrated-corridor-management* (ICM) projects such as *Connected Corridors* Miller and Skabardonis (2010) and mobile applications which use GPS probe data to improve navigation Work et al. (2010).

[*] Corresponding author.
E-mail addresses: jackdreilly@berkeley.edu (J. Reilly), semartin@mit.edu (S. Martin), mpayer@purdue.edu (M. Payer), bayen@berkeley.edu (A.M. Bayen).

http://dx.doi.org/10.1016/j.trb.2016.05.017
0191-2615/© 2016 Elsevier Ltd. All rights reserved.

Integration of control infrastructure is exemplified by freeway networks instrumented with coordinated, predictive ramp metering control. Coordinated ramp-metering strategies have been investigated extensively Ben-Akiva et al. (2003); Cassidy and Rudjanakanoknad (2005); Haddad et al. (2013); Hegyi et al. (2002); Zhang and Levinson (2004) as a control scheme for improving and regulating freeway traffic conditions. Traffic management districts have investigated and piloted such schemes Ahn et al. (2007); Arthur MacCarley et al. (2002) due to their ability to anticipate congestion formation and distribute onramp queues across a corridor. In comparison, many ramp metering strategies used in practice Papageorgiou et al. (1991); Smaragdis et al. (2004) are more *reactive* and *decentralized* in nature, but require less communication infrastructure. Notably, the AMOC freeway traffic control tool developed in Carlson et al. (2010); Kotsialos et al. (2002, 2001) has been shown to reduce congestion 20–30% in realistic simulation environments.

Controllability analysis allows one to evaluate the effectiveness of integrated schemes such as coordinated metering. Given that onramp metering lights only exist at sparsely-distributed locations along a freeway stretch, one cannot expect metering lights alone to *exactly* achieve any desired objective. Rather, traffic dynamics will dictate congestion patterns at uncontrollable locations. The goal then is to select metering rates which produce congestion patterns *as close as possible* to the prescribed congestion. The deviation between the desired and resulting traffic states serve as an indication of the controllability of the system under study.

There exists a number of applications which make use of the above approach. As an example, one can use congestion pattern replication for traffic model calibration Jacquet et al. (2005). If one has accurately measured the congestion states at a given instance, then one could search for the optimal set of model parameters which would reproduce the observed congestion.

A consequence of increased controllability is the increased vulnerability and impact of a control system compromise. A compromise at any level of the traffic control infrastructure can lead to both direct access of an attacker to alter traffic lights and changeable message signs, and indirect access via spoofing of sensor readings, which may *trick* the control algorithms to respond to false conditions.

While much research has been conducted on the security of inter-connected vehicles Ward et al. (2013); Yan et al. (2013), the security of transportation management infrastructure Canepa and Claudel (2013); Ghena et al. (2014) has received less attention. A number of recent compromises underscore the importance of investigating infrastructure security. A man-in-the-middle attack on GPS coordinate transmissions from mobile navigation applications showed it is possible to trick navigation services into inferring non-existent jams Jeske (2013), while a similar attack used a fleet of mobile phone emulators to mimic the presence of many virtual vehicles on a roadway Tufnell (2014). A popular vehicle-detection sensor was revealed to use a type of wireless protocol vulnerable to data injection attacks, and a demonstration showed that the access point could be tricked into receiving arbitrary readings Zetter (2014). Even insider attacks on command centers have precedent as two Los Angeles traffic engineers in 2009 were found guilty of intentionally creating massive delays by adjusting signal times at key intersections Grad (2009).

Given the existence of such vulnerabilities and the scale at which they can be exploited, understanding the nature and costs of such attacks becomes paramount to public safety. In this work, we use freeway controllability to analyze the set of adversarial objectives an attacker could achieve with coordinated metering control.

To do so, we first construct a taxonomy of different vulnerability locations in traffic control systems, defining three distinct layers: physical, close-proximity, and virtual. With each potential attack, we also associate values pertaining to difficulty, impact, and cost of resources expended by the attacker. We motivate our classifications by presenting two scenarios that combine a number of attacks to accomplish a high-level goal.

We then focus our analysis on an in-depth exploration of freeway attacks using coordinated, predictive, ramp metering. The control scheme employed by the attacker uses finite-horizon optimal control based on the adjoint method for finding optimal metering rates to create a desired disruption via complex congestion patterns. We additionally give an overview of multi-objective optimization and discuss how such an approach is useful for solving high-level attack objectives which contain many conflicting sub-goals, such as permitting a fleeing vehicle to escape pursuants on a particular freeway stretch without overly congesting freeway regions irrelevant to the pursuit. While we focus our discussion to ramp metering, the approach is general enough to consider other freeway control attacks, such as modifying variable-speed-limit signs Chen et al. (2014); Muralidharan and Horowitz (2012); Reilly and Bayen (2014) or route-guidance message signs Lo and Szeto (2002); Samaranayake et al. (2014); Ziliaskopoulos (2000).

While counter-measures to the proposed attack methods are outside the scope of this work, potentially relevant approaches have been proposed for physically related problems. In Canepa and Claudel (2013), the problem of detecting spoofed GPS probe measurements from vehicles is posed as a mixed-integer linear programming problem. Amin et al. (2013a); 2013b) presents methods for detecting stealthy attacks on water SCADA systems is presented. In both scenarios, leveraging knowledge of the physical system under attack is key to detection. Using a similar approach for freeway system security may be promising.

The contributions of this article are enumerated along with its outline. We present a classification of a broad set of attacks on traffic control systems with their relation to the underlying physical and cyber infrastructure (Section 2). To study the feasibility of such attacks, we develop an adjoint-based multi-objective optimal controller to achieve arbitrary congestion patterns within the dynamical system's limits (Section 3). The controller is demonstrated for two scenarios using a macroscopic flow simulator based on the model in Delle Monache et al. (2014) (Section 4); in the first scenario, an attacker wishes to congest precise locations at precise times; in the second, we consider the aforementioned problem of constructing