ARTICLE IN PRESS

The Electricity Journal xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

The Electricity Journal

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

Special Issue: Contemporary Strategies for Microgrid Operation & Control

Deployment of cybersecurity for managing traffic efficiency and safety in smart cities[☆]

Zhiyi Li[a], Mohammad Shahidehpour[a,b,*]

[a] Illinois Institute of Technology, Chicago, USA
[b] King Abdulaziz University, Saudi Arabia

ARTICLE INFO

Keywords:
Smart cities
Smart grid
Cybersecurity
Traffic management
Energy efficiency

ABSTRACT

Boosting the concept of smart cities for implementing an intelligent management of traffic congestion while reducing cybersecurity concerns will not only be more efficient for reducing traffic congestion but also more resilient to cyber incidents. In this paper we proposed a framework that can act as a generalized firewall and work interactively with several critical infrastructures in a smart city to protect the respective operations from a variety of cyber threats. The objective is to develop several steps for a comprehensive traffic management framework in smart cities that facilitates the cooperation among drivers and between drivers and the traffic management authority. The transformative nature of the proposed study supports its applications to a variety of networked critical infrastructures, including electricity, gas, water, rails, and telecommunications, as they intend to respond effectively to a wide range of weather- or human-related disruptions. The contributions of this paper include: Improving the traffic management performance in urban transportation systems, assessing and mitigating the cybersecurity risk in urban traffic management, and facilitating efficient and cyber-secure traffic management in metropolitan areas; Developing and testing an interactive simulation platform for evaluating the traffic management performance under various traffic conditions; Validating and demonstrating the applications in a practical urban transportation system; Disseminating the proposed study results to a wide range of concerned audiences via user-group meetings, detailed education forums, and a close collaboration with the local traffic management authority.

1. Introduction

The traffic management framework will protect urban transportation systems in congested zones from possible cyber incidents while creating the potential for significant enhancements to traffic efficiency and safety in metropolitan areas. With widespread utilization of cutting-edge technologies in information, communication, computing, and control, metropolitan areas are dramatically increasing their interest in migrating to smart cities approaches. As a critical infrastructure, the transportation system serving a metropolitan area plays a vital role in addressing urban sustainability and mobility concerns. Metropolitan areas commonly confront severe traffic congestion. which increases air pollution, fuel usage, and travel time. For example, certain parts of Chicago are among the most congested areas in the U.S. In 2014, Chicago drivers cumulatively suffered over 302 million hours of travel delays with a total congestion cost estimated at $7,222,000,000 (Schrank et al., 2015). It is therefore of practical importance to proactively manage increasingly high and complex traffic congestion in accordance with the merits of smart cities approaches.

As the use of vehicular wireless communications becomes more widespread in metropolitan regions, drivers will be capable of communicating with each other and with the traffic management authority in real time for managing emergencies and congestion. Such real-time information sharing enables both drivers and the traffic management authority to gain increased situational awareness on the dynamics of traffic conditions (Li et al., 2016a). Accordingly, drivers can gain a good understanding of present traffic conditions and become aware of potential hazards, whereas the traffic management authority is able to use the pertinent data to intelligently manage traffic in congested hotspots within the transportation system. Considering that congested street intersections often signify bottlenecks for improving traffic efficiency (Chen and Cheng, 2010), the traffic management authority

[☆] Smart cities approaches enable the implementation of intelligent management of traffic congestion that also reduce cybersecurity concerns. The framework proposed here can act as a generalized firewall and also work interactively with several critical smart city infrastructure elements to protect those operations from cyber which also threats, with implications for other realms including electricity, gas, water, rail transportation and telecommunications.

[*] Corresponding author at: Galvin Center for Electricity Innovation Illinois Institute of Technology, 10 West 35th Street, Chicago, IL 60616, United States.
E-mail address: ms@iit.edu (M. Shahidehpour).

http://dx.doi.org/10.1016/j.tej.2017.04.003

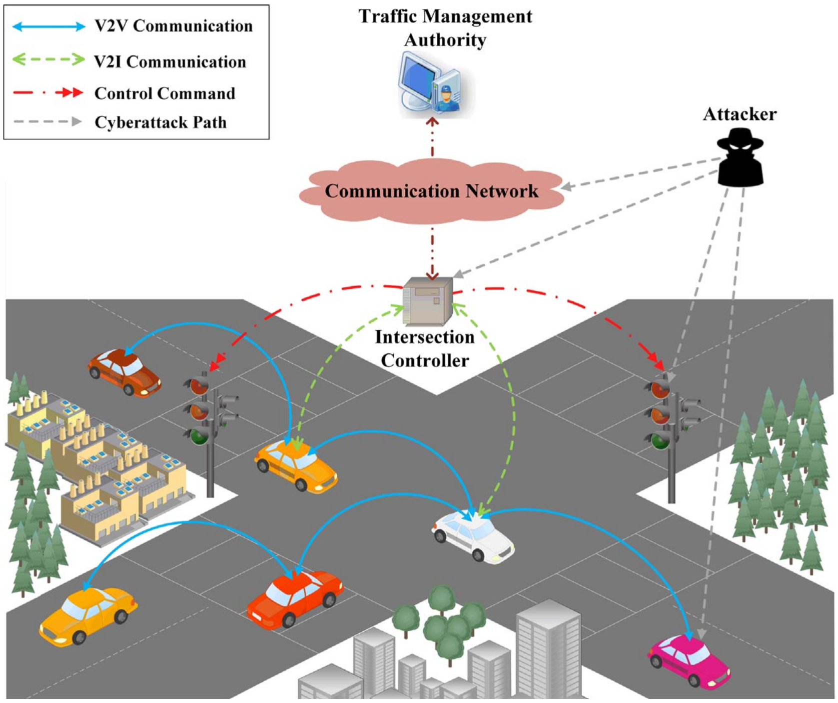

Fig. 1. Traffic management in smart cities.

commonly puts more emphasis on regulating traffic signals at these street intersections in order to reduce local congestion and improve overall traffic management performance in the designated areas.

Urban transportation systems typically are cyber-physical systems where cybersecurity is considered as one of the most important factors in meeting the needs of reliable and resilient operations under various conditions. A clear understanding of the cybersecurity posture in an urban transportation system allows the traffic management authority to determine and prioritize measures to guard against various cyber threats, thereby mitigating their potential implications. A pilot security awareness project demonstrated the possibility of seizing control of more than 100 traffic signals in a metropolitan area from a single point of access (Ghena et al., 2014), which means maliciously controlling traffic signals to meet personal interests or hamper public safety is no longer a fiction but a reality that can endanger human life. Fig. 1 illustrates potential communication paths and cyberattacks on traffic management in smart cities. Accordingly, urban transportation systems should be adequately protected against a variety of cyber threats, either intentional malicious attacks or inadvertent human errors. To date, however, little focus is given to cybersecurity vulnerabilities and the corresponding countermeasures in urban transportation systems.

Considering the growing cybersecurity concerns, and in response to ongoing critical needs in reducing traffic congestion in urban areas, this article focuses on developing a comprehensive framework and supporting theories for a cyber-secure and efficient traffic management system in metropolitan areas. It is anticipated that the promising role of the proposed framework in improving traffic efficiency and safety in metropolitan areas and its inherent cybersecurity design is the catalyst for boosting the development of metropolitan areas towards smart cities.

The contributions of this study include: (1) Taking into account interactions among regional drivers and between the drivers and the traffic management authority for optimizing traffic management in urban transportation systems; (2) Formulating and offering solutions for generalized game-theoretic models that will improve traffic management performance with and without cyber incident implications; (3) Facilitating the application of cyber-secure and efficient traffic management in large-scale urban transportation systems; (4) Developing an efficient, reliable, and user-friendly simulation tool that will be publicly available for evaluating traffic management performance by using open-source software packages, and (5) Validating and demonstrating the developed traffic management tool in a specific section of Chicago in collaboration with the local traffic management authority and making the results available to other traffic management authorities. An interdisciplinary team of experts (representing electrical engineering, transportation engineering, and computer science) has been assembled to facilitate the exchange of ideas among participating disciplines, tackle the traffic management challenges from diverse viewpoints, and further guarantee the successful completion of the project via simulation and prototyping of the software tool.

As illustrated in Fig. 2, our proposed framework can act as a generalized firewall that works interactively with several critical infrastructure elements in a smart city and protects the respective operations from a variety of cyber threats. This holds significant potential for radically transforming current practices in urban traffic management systems, and protecting critical infrastructures from cyber threats. In addition to the proposed novelty in intelligently solving a

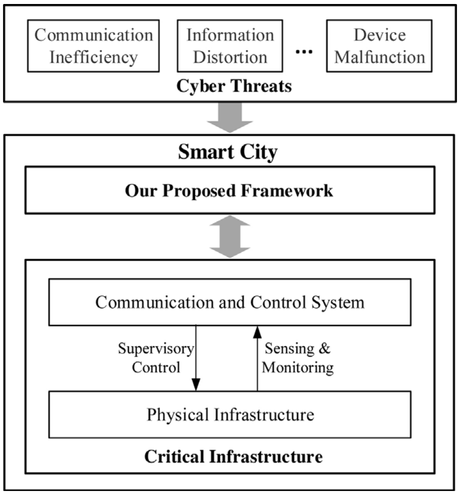

Fig. 2. Generalized framework for enhancing cybersecurity in a smart city.