The Electricity Journal 30 (2017) 52–61

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

Available online 20 June 2017

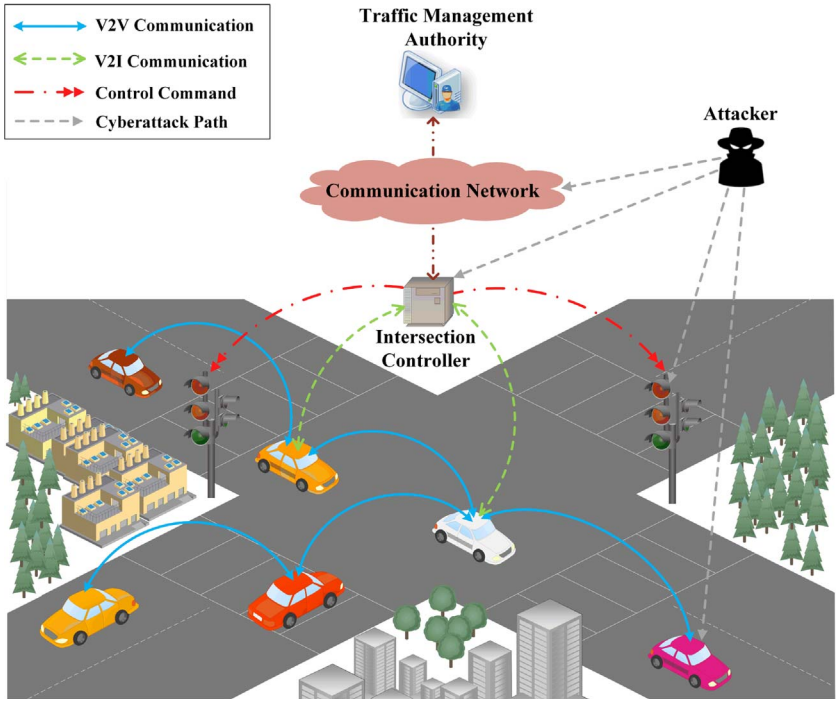

Fig. 1. Traffic management in smart cities.

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

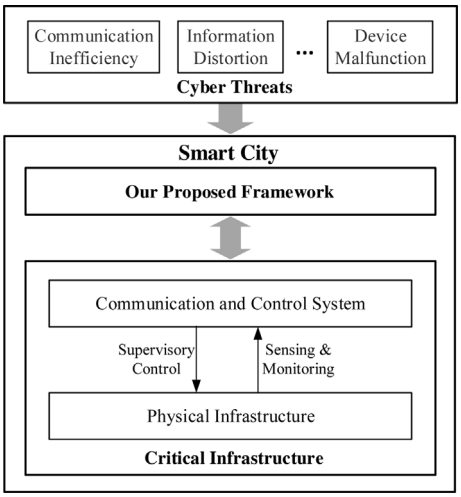

Fig. 2. Generalized framework for enhancing cybersecurity in a smart city.

substantially important infrastructure problem by developing cyber-physical modeling approaches in urban traffic management, the proposed study will reach out to a broader range of audiences for education and demonstration purposes. The proposed effort will engage high school, undergraduate, and graduate students, as well as auto commuters and traffic control aides, with a focus on underrepresented and minority groups. The educational plan is laid out based on the current educational activities and aims at fostering a generation of skilled engineers and researchers in this critical area of study.

2. Existing literature

In smart cities, the development of information and communication technologies (ICTs) enables drivers to interact with each other and cooperate with the traffic management authority by exchanging real-time traffic information, facilitating traffic management of urban transportation systems. The drivers report their trip information (e.g., destination and route preferences) voluntarily to the traffic management authority before embarking on their trips, while the traffic management authority uses the data to regulate traffic signals proactively at street intersections and provide drivers with additional routing suggestions (e.g., the fastest routes). Notably, traffic signals at street intersections play an important role in urban traffic management. In practice, traffic signals determine the waiting time at street intersections, and the potential congestion resulting from suboptimal traffic signal settings has a major impact on the drivers' travel time. There exist several studies on optimizing traffic signals at street intersections. However, most studies fail to take into account the interdependencies of driver route choices and the traffic management authority's signal settings. Instead, the signals are mainly conditioned on the premise that the driver routes are either pre-defined or remain unchanged during the travel between two destinations (Gartner et al., 1974; Lin and Wang, 2004; Ceylan and Bell, 2004; Yang and Yagar, 1995; Jovanović et al., 2017; Gartner et al., 1975; Le et al., 2015; Ma et al., 2014; Smith et al., 2015; Göttlich et al., 2015). In reality, drivers tend to use online information (e.g., websites, media) to gain better perceptions of traffic conditions and have an inclination to adjust their travel routes (Li et al., 2016a; Cheng et al., 2012; Varia et al., 2013; Jintamuttha et al., 2016; Du et al., 2013; Du et al., 2015) so as to avoid potentially congested areas and thereby actively participate in urban traffic management for achieving higher levels of travel efficiency and safety. Accordingly, a novel traffic management mechanism, which can work interactively with traffic signal settings and driver route choices, is required to meet challenges that drivers encounter daily in congested metropolitan areas.

Although the applications of advanced ICTs can help improve the operational flexibility and effectiveness in smart cities, it can also be the Achilles heel of urban traffic management (Wang et al., 2015; Elmaghraby and Losavio, 2014; Ijaz et al., 2016). In fact, urban transportation systems are continuously subject to a variety of potential cyber incidents due to increasing vulnerabilities in their communication and control infrastructures. Cyber incidents are the realization of cyber threats that actually or potentially jeopardize the data flows for traffic management. Cyber incidents usually result from deliberate attacks, inadvertent human errors, defective equipment or software, and natural disasters (Zhu et al., 2011; Cardenas et al., 2008; Jin et al., 2016). Noticeably, deliberate attacks may be launched by strangers (e.g., hackers, terrorists) and/or insiders (e.g., traffic control personnel) with various motivations (e.g., financial gain, political action, revenge, entertainment). With intimate knowledge and authorized access, insiders can easily circumvent security measures and perform insidious actions to cause considerable consequences, which is particularly difficult to prevent. In addition, cyber incidents can be realized by physical means (say, by locally sabotaging networking components) and/or logical means (say, by remotely manipulating data flows). Malware (e.g., worms, spyware, viruses) installed on either hardware devices or in software applications can also assist attackers in achieving the attack goal (e.g., affecting performance or availability of devices or services, sniffing out sensitive information) (Ramachandran and Sikdar, 2007).

The U.S. Department of Homeland Security released its critical infrastructure protection plan in 2013 to guide the national effort to enhance cybersecurity and cyber-resilience of many national critical infrastructures, including urban transportation systems (Department of Homeland Security, 2013). Recently, security analysts have displayed the vulnerabilities of urban transportation systems, especially in traffic signal control systems (Ghena et al., 2014; Laszka et al., 2016; Goodspeed, 2008; Cerrudo, 2014), which would lead to authentication violation, denial of service, and/or spoofing at both the network and device layers, with surprisingly inexpensive means. Ghena et al. analyzed the security of traffic infrastructure and discovered several vulnerabilities such as a lack of common security practices (e.g., the default username and password remains unchanged, the debug port remains open) and no encryption support in the wireless communication (Ghena et al., 2014). Goodspeed managed to compromise the database on an Econolite ASC/3 traffic controller to alter the configuration of light timing and policy (Goodspeed, 2008). In particular, Cerrudo built a reasonably-priced device to gain control of a number of traffic lights in the U.S. (Cerrudo, 2014).

These troubling issues strongly motivate our study to build a comprehensive approach to understanding the nature and mitigating cybersecurity vulnerabilities in urban transportation systems. Since there may exist various levels of malicious cyber means to exploit vulnerabilities in urban transportation systems, it is critical to evaluate by applying various metrics (e.g., number of congested roads, average travel time of drivers) the potential implications of such incidents on the traffic management performance and then deploy effective countermeasures to address the cybersecurity implications. Researchers have investigated various methodologies for evaluating the security and resilience of urban transportation systems, including finite-horizon optimal control to evaluate cyberattacks on monitoring and control components, game-theoretic approaches to analyze network performances and resilience of vehicular networks (Reilly et al., 2015; Alpcan and Buchegger, 2011), vulnerability analyses for transportation systems under the traffic signal tampering attacks (Li et al., 2016b), and road link closures due to natural disasters (Jenelius, 2010). However, we still do not have a comprehensive traffic management framework that can work interactively with traffic signal settings and driver route choices for protecting congested transportation systems from potential cyber incidents and introduce significant potentials for enhancing the traffic efficiency and safety in urban areas.

The centralized optimization methods for traffic management have previously scaled poorly with the size of the transportation system in metropolitan areas. In our work, a hierarchical traffic management system is proposed to suit large-scale and congested transportation systems with potential applications to managing other complex infrastructures in smart cities. As an integration of agents that are computer systems capable of achieving the assigned goals without human interventions (Chen, 2010; Bazzan and Klügl, 2014), a multi-agent system (MAS) is considered to be a reliable solution to realizing real-time intelligent management and control in complex systems (Dresner and Stone, 2005; Hernández et al., 2002; Kammoun et al., 2014; Karfopoulos and Hatziargyriou, 2013). In MAS, each agent communicates and collaborates with other agents for a global coherence and perceives and responds quickly to changes in local system conditions in order to achieve its design goals. Generally, MAS is robust, resilient, and flexible, with self-organization abilities (Liu et al., 2014; Wang et al., 2014). In particular, since each agent is capable of making decisions locally, MAS manages to reduce the dimensionality of the complex traffic management problem and achieve real-time performance with less computational burden (Weiss, 1999; Ksontini et al., 2015). Accordingly, we utilize MAS in our study to provide a means to develop a comprehensive management and control framework for large-scale dynamic transportation systems so that traffic management in large-scale urban transportation systems can be characterized as a highly distributed and evolving process through the cooperation and coordination of the

agents. Additionally, we deploy a host of reliable, robust, and high-performance agents within MAS in order to enhance the operational efficiency and cybersecurity of urban transportation systems. In our tool, the proposed configuration of MAS will solve the large-scale dynamic traffic management problem in an adaptive and cooperative fashion instead of the traditional time-consuming centralized numerical algorithms.

This study focuses on research, development, and prototype testing of a comprehensive framework for improving the efficiency and cybersecurity of urban traffic management. The proposed study considers the application of a wide range of state-of-the-art ICTs in urban transportation systems that can provide drivers and the traffic management authority with increased situational awareness and stronger decision-making capabilities. Given that an urban transportation system is a complex CPS and an important component of the smart city infrastructure that must operate reliably and trustworthily to ensure public safety, the proposed framework is concentrated on enhancing the operation management and the cybersecurity of this critical CPS. The project's synergy stems from a combination of theories, methods, and tools in four distinct areas of transportation engineering, networked control systems, operations research, and computer science.

3. Proposed steps for coordinated traffic management

Fig. 3 offers a schematic of the proposed study steps, implementation, and transition to practice. The four proposed steps are tightly coupled, leading to a successful development and prototype testing of a comprehensive framework for optimizing traffic management with reduced cybersecurity concerns in metropolitan areas. These STEPS are presented as follows.

3.1. Step 1: optimize urban traffic management by regulating signals in street intersections

Traffic signals in street intersections are viewed as decision points that can be adjusted in real time for improving the traffic management performance in urban transportation systems. Any traffic congestion at street intersections can directly lead to higher travel times and emissions. Indeed, congestion can be alleviated by optimizing the associated time for traffic signals that would regulate vehicle flows across the region in street intersections and result in improved local traffic throughputs and smoother regional traffic flows. Thus, intelligently regulating traffic signals in street intersections will catalyze the significant merits of the smart city implementation.

Traffic management in an urban transportation system will be modeled as a bi-level optimization problem that can be envisaged as a leader-follower strategic game involving two parties taking actions in sequence (Hausken and Zhuang, 2015; Su et al., 2007; Shen et al., 2014). Fig. 4 illustrates the hierarchy. In every iteration, each party optimizes its own objective considering the other's response; the traffic management authority (leader) coordinates traffic signal settings

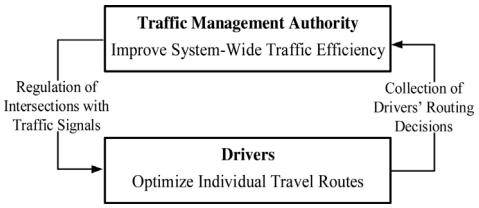

Fig. 4. Bi-level game-theoretic framework.

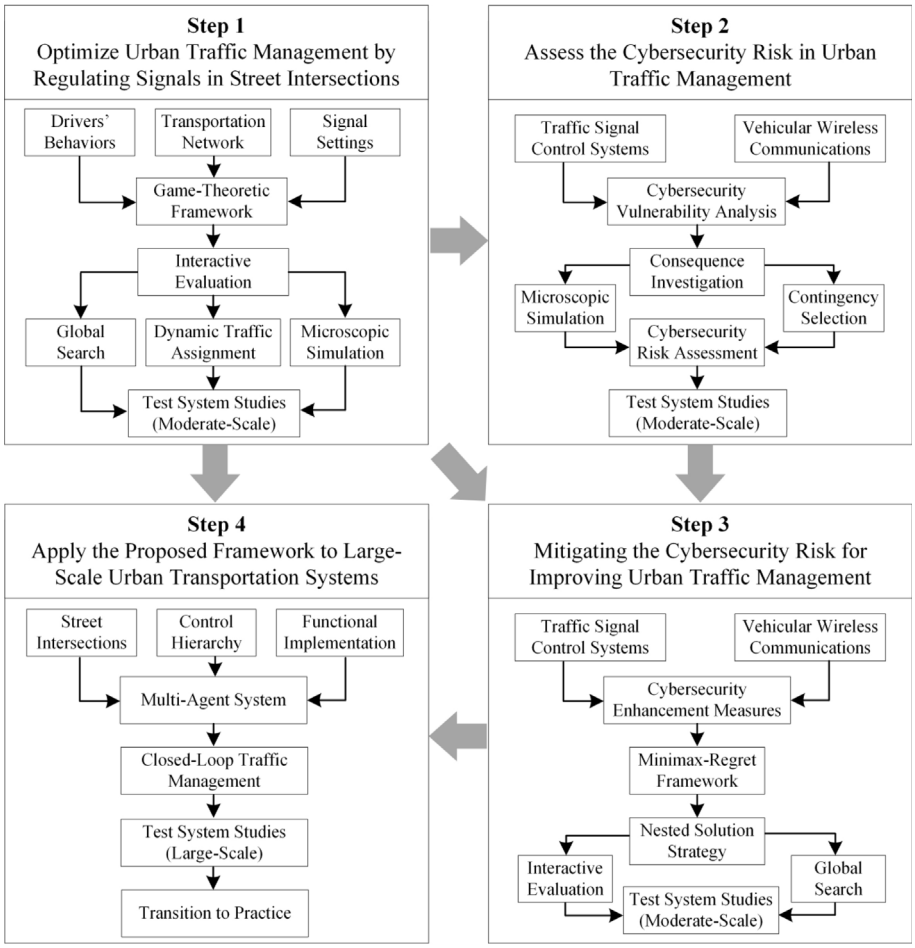

Fig. 3. Proposed steps of study and implementation.

among street intersection signals in order to reduce the potential traffic congestion, and accordingly drivers (follower) strategically determine their routing decisions for reducing their travel time. This step aims at developing an integrated framework for supporting the traffic management authority to improve the system-wide traffic efficiency by optimizing traffic signal settings at street intersections.

When the traffic management authority coordinates traffic signal settings, each intersection is seen as a player that tries to optimize its own signal settings to minimize the local traffic delay. In order to avoid the price of anarchy where the Nash equilibrium usually cannot guarantee the goodness of the system-wide performance, the traffic management authority recommends a strategy to each player according to a probability distribution over the set of strategy profile. Accordingly, the distribution leads to a correlated equilibrium (Aumann, 1974) if no player would want to deviate from the recommended strategy. Mathematically, the correlated equilibrium is defined as a probability distribution $p(s)$over the set of strategy profile $\mathbf{S}$ such that for each player i and every two different strategies s_i and $s_i^{'}$ in its strategy profile $\mathbf{S}_i$, the following inequality holds:

$$\sum_{s_{-i}} \{p(s_i, s_{-i})\cdot[u_i(s_i, s_{-i}) - u_i(s_i^{'}, s_{-i})]\} \geq 0, \forall\, i, \forall\, s_i, s_i^{'}, \in \mathrm{S}_i$$

where $u_i(s_i, s_{-i})$and $u_i(s_i^{'}, s_{-i})$ are play i's utility when it chooses strategy $s_i, s_i^{'} \in \mathrm{S}_i$ and the remaining players choose a strategy profile described by s_{-i}; $p(s_i, s_{-i})$ is the probability distribution corresponding to $u_i(s_i, s_{-i})$. Hence, the expected utility resulting from s_i of each player would not be increased by switching to a different strategy $s_i^{'}$, given that the strategy profile is drawn based on the probability distribution $p(s)$ over the set of strategy profile $\mathbf{S}$.

Considering the lower level optimization in Fig. 4, drivers would communicate with each other and with the traffic management authority in real time using vehicular wireless communication technologies (e.g., WiMAX (Pareit et al., 2012)). Accordingly, a mobile ad-hoc wireless network is formed to enable the unfettered sharing of accurate and timely information for improving the traffic efficiency and safety. The practical types of communication include vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) (Al-Sultan et al., 2014; Vegni and Little, 2011; Santa et al., 2008). V2V enables interactions and potential collaborations among drivers and provides suggestions on vehicle velocities for smoothing out the traffic flow and inter-vehicle distances for enhancing the road safety. V2I allows vehicles to interact with roadside communication units for the real-time traffic management. Accordingly, each intersection will be outfitted with a communication unit for interaction with approaching vehicles. This unit can also send control commands to adjustable traffic signals to deplete traffic queues at associated intersections. Accordingly, coordinated driving behaviors can be realized within a vehicle platoon (Li et al., 2015) so that they will obey a coordinated car-following mechanism (Gong et al., 2016) and go through street intersections smoothly and safely under the given traffic signal settings. After continuously communicating with each other and with the traffic management authority, drivers will get an optimal resolution for the lower level problem in Fig. 4.

The traffic flows in street intersections are strategically controlled by regulating the associated signals. Traffic signals within an intersection are coordinated by the upper level optimization in Fig. 4 using certain regulations for ensuring the smoothness of traffic flows across the intersection. Fig. 5 shows the representative four-phase traffic signals at an intersection. Three types of movements (i.e. going straight, turning right, turning left) are allowed in each phase. Conventionally, traffic signals are controlled by fixed-time logic (e.g. time of day, day of week) which is determined using the off-line historic traffic data. However, such a signal regulation mechanism can hardly handle fluctuating traffic flows, which can change substantially over time. We consider a traffic-responsive signal setting mechanism by utilizing real-time high-fidelity traffic data informed by the surrounding vehicles through V2I.

At each intersection, vehicles are recognized in the close proximity of the intersection (e.g. 50 m). Traffic signal settings such as the length

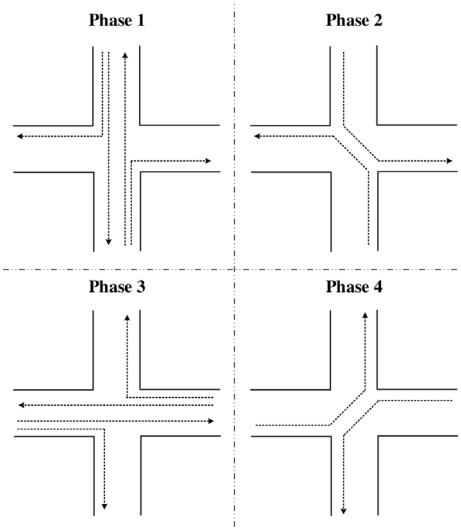

Fig. 5. Traffic signal phases.

of the next phase will be reset with the goal of maximizing the local traffic throughput. Several study challenges are introduced here such as queue length prediction. Multiple data resources, such as fixed-point data from loop detectors and trajectory data from V2I communications, will be integrated for this prediction, combined with the physical limits of vehicle dynamics.

There is at least one correlated equilibrium point for a finite game where a mixed-strategy Nash Equilibrium is an extreme point of the correlated equilibrium solution polyhedron (Aumann, 1974; Hart and Schmeidler, 1989; Nau et al., 2004). However, not every correlated equilibrium leads to a better system performance than a mixed-strategy Nash equilibrium. Existing study has proved that it is NP-hard to find an optimal correlated equilibrium in a congestion game (Papadimitriou and Roughgarden, 2008). Considering that this problem usually is analytically intractable (Zhu and Marcotte, 2000), we use time-discrete microscopic traffic simulators like *Simulation of Urban MObility* (SUMO) (Behrisch et al., 2011) which can track the dynamic traffic assignment in such conditions. In our simulation, vehicle movement can be simulated based on car-following and lane-changing theories, which renders the simulation results consistent with real-world scenarios. Furthermore, we obtain trajectories for each driver, which is important for extracting temporal and spatial dynamics of drivers' behavior. Considering the complex interactions among the traffic management authority and drivers, and among drivers, we develop an interactive evaluation platform to obtain the optimal or a satisfactory near-optimal solution with appropriate computational efforts. More specifically, the proposed platform integrates SUMO with Java (Java Software, 2017), and iteratively invokes Java and SUMO for implementing urban traffic control and management decisions and performing microscopic traffic simulation, respectively, as shown in Fig. 6.

3.2. Step 2: assess the cybersecurity risk in urban traffic management

As the first step towards understanding and mitigating cybersecurity vulnerabilities, we consider risk assessment (Cárdenas et al., 2011; Haimes, 2017; Bahr, 2014; Cherdantseva et al., 2016) as a foundation for perceiving the cybersecurity posture in an urban transportation

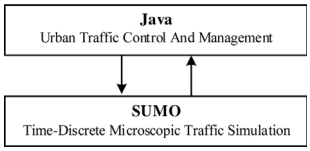

Fig. 6. Interactive evaluation platform.

system. In essence, risk assessment, which translates the cybersecurity posture into a quantifiable term, is a systematic and repeatable approach to the evaluation of potential consequences of cyber threats.

Urban transportation systems are facing a range of cyber threats. As a key component in traffic management, traffic signal control system often has multiple cybersecurity vulnerabilities that can be easily exploited in real life. The main components of a traffic signal control system include: controllers that control traffic signal states; sensors that detect traffic conditions; networking equipment that communicates with the traffic management authority, sensors, and other street intersections; and traffic light malfunction management units. We have conducted a comprehensive literature review of the possible cyber threats and summarized the high-level classifications in Table 1.

Here we offer a few samples of cyber threats originating from potential attackers. Since attackers can see the service set identifier (SSID) of the network that a traffic signal control system is connected to, they may just need to acquire a radio of the same model as the signal controller, which can be done through manufacturers (Ghena et al., 2014). After gaining access to the network, attackers attempt to gain access to the signal controller. Attackers could use FTP to write configuration changes to the controller's database to change the traffic light sequences. Typically, this uses default usernames and passwords that attackers can find directly from the manufacturer. In addition, attackers could perform a memory dump and reverse-engineer the memory information to write changes to the memory, resulting in light state changes or timing changes. If the protocol used to remotely control the signals is standard and unencrypted, attackers may engineer their own packets to send commands to the traffic signal controller. Accordingly, attackers gain access to a traffic signal control system, eavesdrop on traffic, and even manipulate the light states.

Physical consequences on the transportation system can be quantified by the degradation of traffic management performance. The severity of a cyber incident is generally expressed as

$$\mathcal{S} = \mathcal{P}_o - \mathcal{P}^*$$

where $\mathcal{P}_o$ represents the traffic management performance when there is no cyber incident in the transportation system; $\mathcal{P}^*$ is the worst possible traffic management performance in the case of the cyber incident. In particular, physical consequences of cyber incidents on the operational performance of the urban transportation network will be investigated in time-discrete microscopic traffic simulation. Mathematically, the identification of worst-case physical consequences is envisaged as a leader-follower game between attackers (leader) and drivers (follower). These two parties take actions in sequence in which attackers compromise the traffic signal control systems and modify traffic signal settings. Meanwhile, drivers change their routes to shorten their travel times based on the compromised traffic signals. Clearly, each party optimizes its own objective in response to the other party's response. Note that the attackers can dynamically adjust their attack strategies according to drivers' behaviors. In turn, drivers continuously seek fastest routes given the compromised traffic signals. It is also noteworthy that attacks tend to realize the system-wide traffic inefficiency in spite that drivers may cooperate to reduce their travel time.

It would not be possible to enumerate all possible forms of cyber incidents, let alone multiple incidents that may happen simultaneously. Thus, we select the most likely cyber incidents (defined as cyber contingencies) against the urban transportation system by performing a vulnerability analysis. Given a set of postulated cyber contingencies, we calculate the cybersecurity risk in the urban traffic management under a certain traffic condition as

$$\mathcal{R} = \sum_{i \in \mathbb{C}} \mathcal{L}_i \cdot \mathcal{S}_i$$

where $\mathcal{R}$ denotes the risk; $\mathbb{C}$ is the set of postulated cyber contingencies; $\mathcal{L}_i$ and $\mathcal{S}_i$ are the likelihood and severity of the i-th contingency, respectively. The likelihood of each cyber contingency and the severity of the resulting impact are two key elements of risk assessment. The former will be derived at the vulnerability analysis step by using the probabilistic approaches (e.g., Bayesian network), while the latter will be identified with the physical implications on the transportation system.

Table 1
Cybersecurity vulnerabilities in traffic signal control systems.

Classification	Vulnerability	Cyber Threat	Consequence
Compromise of the Controller	Authentication/ Authorization (Heimann and Chu, 2017)	Password cracking/social engineering	Used for coordinated attack of DoS, eavesdropping, spoofing, etc.
	Authentication/ Authorization (Heimann and Chu, 2017)	Access to debug port/memory dump	Used for coordinated attack of DoS, eavesdropping, spoofing, etc.
	Denial of Service (DoS) (Ghena et al., 2014; Zhang et al., 2014; N. E. M. Association, 2017)	Set all lights to red/restrict changing of light states	Traffic disruption, e.g., 4-way red
	DoS (Ghena et al., 2014; Zhang et al., 2014; N. E. M. Association, 2017; Park and Chen, 2015)	Set lights to invalid states	Traffic disruption, hardware error checking causes lights to go to default schedule
	Spoofing (Ghena et al., 2014; Cerrudo, 2014; N. E. M. Association, 2017)	Change state of intersection	Personal gain – change lights to favor attacker or to hinder emergency vehicles, terror attack
Compromise of Sensor Data	DoS (Cerrudo, 2014; Zhang et al., 2014; Park and Chen, 2015)	Flood access point with excess packets	Traffic disruption – system uses default schedule
	DoS (Cerrudo, 2014; Molisch et al., 2004; Dobersek, 1998)	Alter firmware/disable sensor/send no data	Traffic disruption
	Eavesdropping	Monitor communication over network (from sensors and/or controllers)	Coordinated attack/reverse engineering light state behavior
	Firmware Modification (Ghena et al., 2014; Molisch et al., 2004)	Upload firmware to access points and distribute to sensors	Invalidate data from sensors, disable sensors
	Spoofing (Ghena et al., 2014; Cerrudo, 2014; Dobersek, 1998)	Replay attack/reverse engineering/ saturate network with custom packets	Traffic disruption, e.g., ramps, street intersections
Physical Attack	Compromise Failsafe Equipment (Ghena et al., 2014; Heimann and Chu, 2017; Newton et al., 1997)	Tampering/removal/replacement of hardware failsafe	Terror attack, traffic disruption, possible accidents resulting in injuries, extensive monetary damage
	Compromise Light Controller Cabinet	Tampering/damage	Traffic disruption/personal gain
	Compromise Sensors/Access Points	Removal or damage of sensors	Traffic disruption (i.e., system uses default schedule)

Table 2
Countermeasures against cyber threats in traffic signal control systems.

Source	Vulnerability	Countermeasure
Controller	Authorization	Disable debug port (Zhang et al., 2014)
	Authentication	Change default username/password (Komanduri et al., 2011)
	Spoofing	Whitelist known authorized connections
	Eavesdropping/Authorization	Encrypt data on wireless communication channels (Ghena et al., 2014)
Sensor Data	Replay attack/Spoofing	Add timestamp to data sent to controller/encrypt traffic (Sensys Networks Inc., 2007)
	Firmware modifications	Whitelist known authorized connections
Physical Devices	Access to controller/MMU/Sensors	Make controller cabinet inaccessible/secure

3.3. Step 3: mitigate the cybersecurity risk in urban traffic management

Mitigating the cybersecurity risk in urban traffic management is critical for ensuring the traffic efficiency and safety. Although the cybersecurity risk in urban traffic management cannot be eradicated, it can be strategically marginalized by lowering the probability of occurrence of cyber contingencies and reducing their impacts on the operation of urban transportation systems.

In the face of a variety of cyber threats, we address cybersecurity concerns in urban transportation systems. Specifically, we consider the deployment of effective countermeasures against potential cyber incidents in both vehicular communications and traffic signal control systems. Our preliminary list of countermeasures for cyber threats in prevalent traffic signal control systems is given in Table 2. However, manufacturers would have to make certain changes to their current controllers to prevent any unauthorized access, such as disabling any debug port that attackers can use to gain access. The debug port allows attackers to perform memory dumps that can reveal passwords and other critical data regarding the system configuration (Zhang et al., 2014). Furthermore, passwords need to be changed from the factory default periodically (Komanduri et al., 2011).

In order to prevent malicious users from impersonating or altering the sensor communication network, encryption should be used to transmit the network data, which would prevent eavesdropping on sensor-to-controller and controller-to-controller communications. Sensors need to be designed so that firmware cannot be modified arbitrarily or without authorization. This requires the device manufacturers to allow known connections to make changes and take into account encryption and authorization techniques (Sensys Networks Inc., 2007). Communication between sensors and the controller should contain timestamps to prevent replay attacks of sensor data on the network.

Given a set of available countermeasures, a certain trade-off should be made to balance cybersecurity versus performance, cost, and usability. In order to evaluate the effectiveness of countermeasures comprehensively, we utilize a minimax regret criterion (Jiang et al., 2013; Chen et al., 2014). Here the risk without deploying any countermeasures is viewed as the regret for a combination of countermeasures under a certain traffic network condition. With this criterion in place, the traffic management authority will prioritize and implement a combination of countermeasures that are acceptable considering all possible traffic network conditions (which can be simply sampled as a set of representative scenarios). The corresponding countermeasures minimize the worst-case regret. Fig. 7 shows the general decision framework for realizing the minimax-regret approach.

In essence, the minimax-regret selection of countermeasures can be envisaged as a multi-player strategic game which involves three parties taking sequential actions: (1) the traffic management authority deploys countermeasures to secure the urban transportation system in order to reduce the potential consequences on traffic management due to cyber incidents; (2) cyber incidents deteriorate the traffic management performance by compromising the urban transportation system that lacks adequate cybersecurity measures; (3) drivers plan their individual

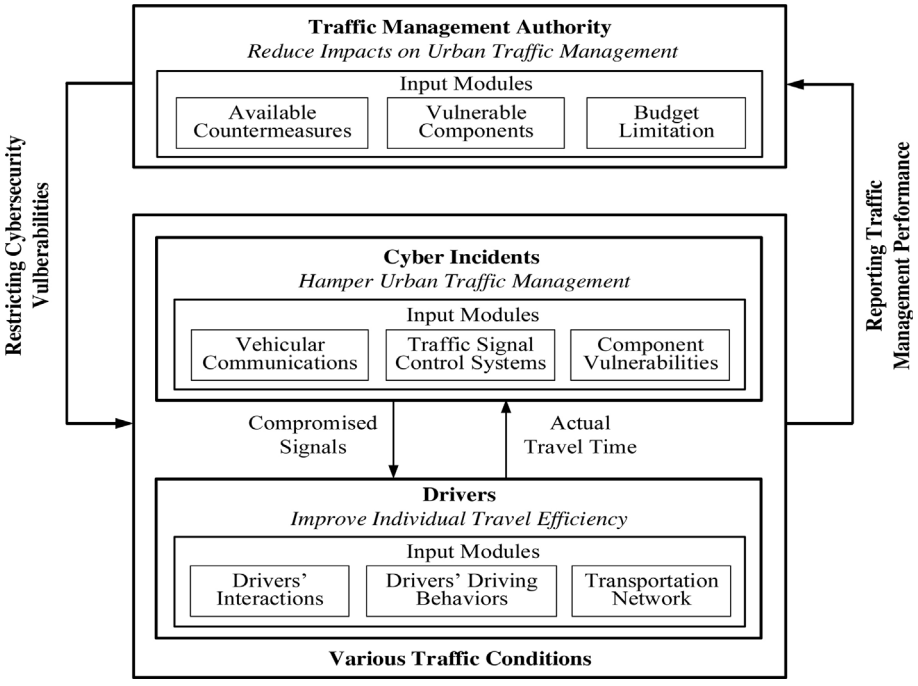

Fig. 7. Generalized framework for mitigating cybersecurity risks.

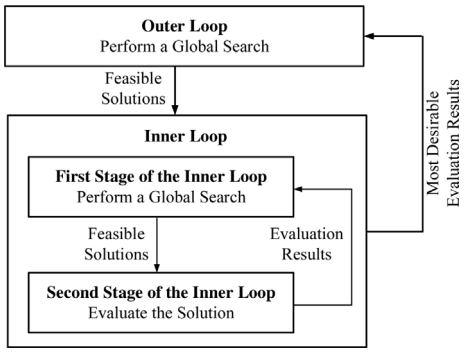

Fig. 8. Nested solution strategy.

routes to reduce their travel time according to their perceived information that is possibly compromised. Obviously, each group optimizes its own objective in consideration of the decisions from the preceding group (if any) as well as the responses from the subsequent group (if any).

In order to apply the minimax-regret framework to the complex three-level problem, we develop a nested solution strategy (as shown in Fig. 8) where the interactive evaluation platform implemented in Step 1 is applied in the inner loop. A global searcher (e.g., genetic algorithm (Davis, 1991), particle swarm optimization (Kennedy, 2011)) in the outer loop iteratively seeks a feasible set of countermeasures that are then passed to the inner loop for evaluating their effectiveness, while the effectiveness evaluation is accomplished iteratively by the proposed two stages of the inner loop. The effectiveness in terms of the worst-case traffic management performance after the deployment of the countermeasures selected in the outer loop is determined when the iteration terminates in the inner loop, while the search process in the outer loop continues until a satisfactory solution is obtained.

3.4. Step 4: apply the framework to large-scale urban transportation systems

The optimization of traffic management is computationally inefficient for large-scale urban transportation systems because this problem is intrinsically an NP-hard problem (Dresner and Stone, 2005; Hausken and Zhuang, 2015; Su et al., 2007). In these cases, MAS-based hierarchical control and management should be employed for improving the traffic efficiency and safety rather than the centralized scheme.

In order to fully utilize the advantages of MAS applications to large-scale urban transportation systems, we first define a series of control areas that are linked together by inter-area street intersections. Then, we apply a three-level MAS architecture consisting of the following types of agents: city controller (CC) at the highest level, area coordinator (AC) at the middle level, and intersection agent (IA) at the lowest level. Fig. 9 shows the pyramidal structure of the MAS. Each agent is responsible for controlling its domain and performing predefined communication and cooperation with other agents through real-time information exchange. A CC covers the entire transportation system in a metropolitan area. Each AC is responsible for a control area. Each IA configures and adjusts the traffic signal settings for directing the vehicles through the associated intersection. Each agent reacts to changes in the dynamic traffic condition and adapts itself to changing environments based on internal rules. In addition, IAs within the same control area are supervised by the associated AC, except that IAs at inter-area street intersections are directly supervised by the CC, while all the ACs are under the guidance of the CC. Through decomposition and coordination, this hierarchical control and management framework tend to achieve a tradeoff between local optima and global coherence when optimizing traffic signal settings.

Generally, the MAS operation is divided into two stages. At the first stage, MAS performs offline optimization on a slow timescale. The urban traffic management problem is decomposed into several independent local problems, each of moderate size. After the CC determines the signal settings at inter-area street intersections, each AC employs advanced modeling and simulation software to locally design optimal traffic signal settings for the area it manages, provided with the forecasted travel demands by the CC. Although each AC makes local decisions in a centralized setting, the computational burden of solving such local problems is remarkably alleviated. Accordingly, a high-quality near-optimal solution of the original problem is represented by the optimal solutions of local problems. By shifting the computation burden to ACs, this decentralized optimization mechanism strikes a balance between optimality and timeliness. At the second stage, MAS executes online adjustment and configuration on a fast timescale in order to flexibly adapt to changes in traffic conditions. Given the real-time traffic information at the regulated intersections, each IA quickly and automatically adjusts the traffic signal settings in a corrective manner as a response to traffic flow variations, which plays a vital role in guaranteeing the real-time performance of MAS in the presence of uncertainty. Moreover, each IA can have its own intra-level cooperative peers allocated and updated dynamically by the associated AC in order to achieve a tradeoff between global and local optimum. The detailed functions of each agent type in the proposed operational framework are discussed as follows.

At the end of each management period, MAS will objectively evaluate its performance in a look-back manner for handling the traffic condition uncertainties. The look-back evaluation provides a means for the MAS to learn from its historical operations so as to achieve the excellence in its decision making. Given the actual travel information collected across an urban transportation system, MAS re-optimizes and perfects the settings of intersection traffic signals in the previous management period. In addition to serve as a valuable baseline for measuring performance, the look-back evaluation will identify possible opportunities and provide timely feedback to spur continuous improvements in the MAS-enabled decision making process. In particular, in the look-back evaluation process, MAS exploits archived traffic data to gain insights into the causes of imperfectness of its operations. For instance,

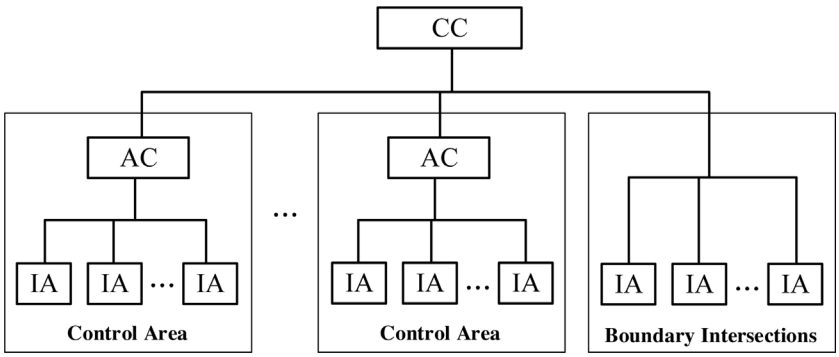

Fig. 9. Hierarchical structure of the multi-agent system.

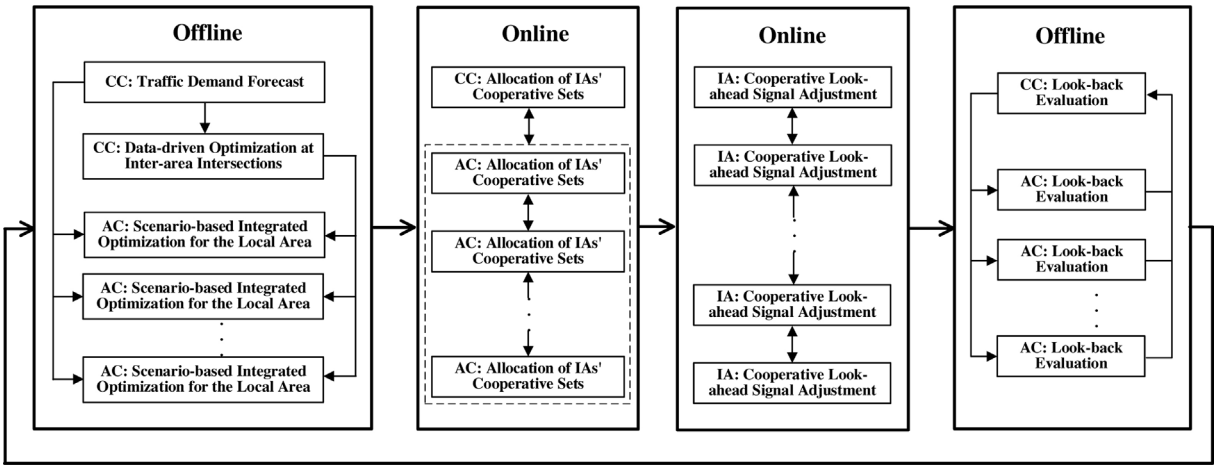

Fig. 10. Closed-loop traffic management based on the MAS.

MAS can attain a better knowledge of the spatio-temporal correlation among the traffic throughput of multiple street intersections, which guides the MAS to better understand the interrelationship between queue length and traffic signal settings at each intersection; MAS can even diagnose the bottlenecks for improving the traffic efficiency from the topological viewpoint and then provide suggestions on the transportation system expansion. The MAS-based traffic management process is complete using the look-back evaluation in a closed loop system presented in Fig. 10. Note that with multi-core processing capabilities, look-back evaluation can be performed in parallel to any real-time decision-making process.

We apply the Java Agent DEvelopment framework (JADE) environment (Bellifemine et al., 2000) to model the functionality of the MAS. The implementation of the MAS enhances the capability to operate autonomously and react proactively to the changing traffic flows. Meanwhile, individual agents are updated or replaced as the operational objective varies, which ensure the flexibility and extensibility of the proposed framework. The SUMO-based microscopic simulation for a large-scale urban transportation system will first be conducted, which will run in conjunction with the MAS simulated in JADE.

4. Final words

The outcome of the proposed study is to analyze the prevailing traffic congestion circumstances and develop a set of customized software applications for reducing both road congestion and cybersecurity concerns in the urban traffic management process, with the objective of ensuring the traffic efficiency and safety at the presence of cyber incidents. The proposed goal will be achieved via the prototype testing and the implementation of the proposed integrated framework for cyber-secure and efficient traffic management in metropolitan areas.

The proposed study will have profound impacts on urban mobility and sustainability by promoting the sound development and deployment of advanced techniques related to urban traffic management and critical infrastructure protection. The project results will directly impact the society by helping traffic engineers better design and implement applications in improving the traffic management performance. The proposed study will increase public awareness and facilitate the understanding of the complexity of cybersecurity issues and the required reaction plans among manufacturers, traffic management authorities, and auto commuters, and further exhibit the viability and importance of using emergent technologies in renewing traditional practices. The findings can significantly enhance the travel efficiency and the on-road safety, and further mitigate the cybersecurity risk in urban traffic management. Moreover, the study will enable a rapid and widespread deployment of new smart city applications in metropolitan areas.

References

Schrank, D., Eisele, B., Lomax, T., Bak, J., 2015. 2015 Urban Mobility Scorecard 39 Texas A & M Transportation Institue (August, p. 5).
Li, Z., Shahidehpour, M., Bahramirad, S., Khodaei, A., 2016a. Optimizing traffic signal settings in smart cities. IEEE Trans. Smart Grid early acce.
Chen, B., Cheng, H.H., 2010. A review of the applications of agent technology in traffic and transportation systems. IEEE Trans. Intell. Transp. Syst. 11 (2), 485–497.
Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., Halderman, J.A., 2014. Green lights forever: analyzing the security of traffic infrastructure. Proceedings of the 8th USENIX Conference on Offensive Technologies (p. 7).
Gartner, N., Little, J., Gabbay, H., 1974. Optimization of traffic signal settings in networks by mixed-integer linear programming. Transp. Sci. 9 (March).
Lin, W.-H., Wang, C., 2004. An enhanced mixed-integer LP formulation for traffic signal control. IEEE Trans. Intell. Transp. Syst. 5 (4), 238–245.
Ceylan, H., Bell, M.G.H., 2004. Traffic signal timing optimisation based on genetic algorithm approach, including drivers' routing. Transp. Res. Part B: Methodol. 38 (4), 329–342.
Yang, H., Yagar, S., 1995. Traffic assignment and signal control in saturated road networks. Transp. Res. Part A 29 (2), 125–139.
Jovanović, A., Nikolić, M., Teodorović, D., 2017. Area-wide urban traffic control: a bee colony optimization approach. Transp. Res. Part C Emerging Technol. 77, 329–350.
Gartner, N.H., Little, J.D.C., Gabbay, H., 1975. Optimization of traffic signal settings by mixed-integer linear programming: part I: the network coordination problem. Transp. Sci. 9 (4), 321–343.
Le, T., Kovács, P., Walton, N., Vu, H.L., Andrew, L.L.H., Hoogendoorn, S.S.P., 2015. Decentralized signal control for urban road networks. Transp. Res. Part C Emerging Technol. 58, 431–450.
Ma, X., Jin, J., Lei, W., 2014. Multi-criteria analysis of optimal signal plans using microscopic traffic models. Transp. Res. Part D Transp. Environ. 32, 1–14.
Smith, M.J., Liu, R., Mounce, R., 2015. Traffic control and route choice: capacity maximisation and stability. Transp. Res. Part B Methodol. 81, 863–885.
Göttlich, S., Herty, M., Ziegler, U., 2015. Modeling and optimizing traffic light settings in road networks. Comput. Oper. Res. 55, 36–51.
Cheng, H.Y., Gau, V., Huang, C.W., Hwang, J.N., 2012. Advanced formation and delivery of traffic information in intelligent transportation systems. Expert Syst. Appl. 39 (9), 8356–8368.
Varia, H.R., Gundaliya, P.J., Dhingra, S.L., 2013. Application of genetic algorithms for joint optimization of signal setting parameters and dynamic traffic assignment for the real network data. Res. Transp. Econ. 38 (1), 35–44.
Jintamuttha, K., Watanapa, B., Charoenkitkarn, N., 2016. Dynamic traffic light timing optimization model using bat algorithm. Control Science and Systems Engineering (ICCSSE),2nd International Conference On, 2016 181–185.
Du, L., Peeta, S., Kim, Y., 2013. Online stochastic routing incorporating real-time traffic information. Transp. Res. Rec. J. Transp. Res. Board 2334, 95–104.
Du, L., Chen, S., Han, L., 2015. Coordinated online in-vehicle navigation guidance based on routing game theory. Transp. Res. Rec. J. Transp. Res. Board 2497, 106–116.
Wang, P., Ali, A., Kelly, W., 2015. Data security and threat modeling for smart city infrastructure, in Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC). International Conference On, 2015 1–6.
Elmaghraby, A.S., Losavio, M.M., 2014. Cyber security challenges in Smart Cities: safety, security and privacy. J. Adv. Res. 5 (4), 491–497.
Ijaz, S., Shah, M.A., Khan, A., Ahmed, M., 2016. Smart cities: a survey on security concerns. Int. J. Adv. Comput. Sci. Appl. 7, 612–625.
Zhu, B., Joseph, A., Sastry, S., 2011. A taxonomy of cyber attacks on SCADA systems in Internet of things (iThings/CPSCom). 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing 380–388.
Cardenas, A.A., Amin, S., Sastry, S., 2008. Secure control: towards survivable cyber-physical systems in distributed computing systems workshops, 2008. ICDCS'08. 28th International Conference on 495–500.

Jin, D., Hannon, C., Li, Z., Cortes, P., Ramaraju, S., Burgess, P., Buch, N., Shahidehpour, M., 2016. Smart street lighting system: a platform for innovative smart city applications and a new frontier for cyber-security. Electr. J. 29 (10), 28–35.
Ramachandran, K., Sikdar, B., 2007. Modeling malware propagation in networks of smart cell phones with spatial dynamics in INFOCOM, 2007. 26th IEEE International Conference on Computer Communications. IEEE 2516–2520.
Department of Homeland Security, 2013. National infrastructure protection plan. [Online]. Available: www.dhs.gov/sites/default/files/publications/NIPP%25202013_Partnering%2520for%25%0A20Critical%2520Infrastructure%2520Security%2520and%2520Resilience_508_0.pdf.
Laszka, A., Potteiger, B., Vorobeychik, Y., Amin, S., Koutsoukos, X., 2016. Vulnerability of transportation networks to traffic-signal tampering. Proceedings of the 7th International Conference on Cyber-Physical Systems p. 16.
Goodspeed, T., 2008. Reversing the Econolite ASC/3 traffic light controller. ToorCon Seattle.
Cerrudo, C., 2014. Hacking US Traffic Control Systems. ([Online]. Available: https://defcon.org/images/defcon-22/dc-22-presentations/Cerrudo/DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf).
Reilly, J., Martin, S., Payer, M., 2015. On cybersecurity off reeway control systems: analysis of coordinated ramp metering attacks. Transportation Research Board 94th Annual Meeting.
Alpcan, T., Buchegger, S., 2011. Security games for vehicular networks. IEEE Trans. Mob. Comput. 10 (2), 280–290.
Li, Z., Jin, D., Hannon, C., Shahidehpour, M., Wang, J., 2016b. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. IET Cyber-Phys. Syst.: Theor. Appl. 1 (1), 60–69.
Jenelius, E., 2010. Large-scale Road Network Vulnerability Analysis. KTH.
Chen, B., 2010. A review of the applications of agent technology in traffic and transportation systems. IEEE Trans. Intell. Transp. Syst. 11 (2), 485–497.
Bazzan, A.L.C., Klügl, F., 2014. A review on agent-based technology for traffic and transportation. Knowl. Eng. Rev. 29 (3), 375–403.
Dresner, K., Stone, P., 2005. Multiagent traffic management An improved intersection control mechanism. Proceedings of the Fourth International Joint Conference on Autonomous Agents and Multiagent Systems 471–477.
Hernández, J., Ossowski, S., Garcıa-Serrano, A., Hernández, J., 2002. Multiagent architectures for intelligent traffic management systems. Transp. Res. Part C: Emerging Technol. 10 (5), 473–506 (6).
Kammoun, H.M., Kallel, I., Casillas, J., Abraham, A., Alimi, A.M., 2014. Adapt-Traf: an adaptive multiagent road traffic management system based on hybrid ant-hierarchical fuzzy model. Transp. Res. Part C Emerging Technol. 42, 147–167.
Karfopoulos, E.L., Hatziargyriou, N.D., 2013. A multi-agent system for controlled charging of a large population of electric vehicles. IEEE Trans. Power Syst. 28 (2), 1196–1204.
Liu, W., Liu, J., Peng, J., Zhu, Z., 2014. Cooperative multi-agent traffic signal control system using fast gradient-descent function approximation for V2I networks, in Communications (ICC) 2014. IEEE International Conference 2562–2567.
Wang, S., Djahel, S., McManis, J., 2014. A Multi-Agent based vehicles re-routing system for unexpected traffic congestion avoidance. Intelligent Transportation Systems (ITSC),IEEE 17th International Conference 2541–2548.
Weiss, G., 1999. Multiagent Systems: a Modern Approach to Distributed Artificial Intelligence. MIT press.
Ksontini, F., Mandiau, R., Guessoum, Z., Espié, S., 2015. Affordance-based agent model for road traffic simulation. Auton. Agents Multi Agent Syst. 29 (5), 821–849.
Hausken, K., Zhuang, J., 2015. Game theoretic analysis of congestion, safety and security. Traffic Transportation Theory. Springer.
Su, B.B., Chang, H., Chen, Y.-Z., He, D.R., 2007. A game theory model of urban public traffic networks. Phys. A Stat. Mech. Appl. 379 (1), 291–297.
Shen, Y., Yan, Z., Kantola, R., 2014. Analysis on the acceptance of global trust management for unwanted traffic control based on game theory. Comput. Secur. 47, 3–25.
Aumann, R.J., 1974. Subjectivity and correlation in randomized strategies. J. Math. Econ. 1 (1), 67–96.
Pareit, D., Lannoo, B., Moerman, I., Demeester, P., 2012. The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX. IEEE Commun. Surv. Tutorials 14 (4), 1183–1211.
Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H., 2014. A comprehensive survey on vehicular Ad Hoc network. J. Netw. Comput. Appl. 37 (1), 380–392.
Vegni, A.M., Little, T.D.C., 2011. Hybrid vehicular communications based on V2V-V2I protocol switching. Int. J. Veh. Inf. Commun. Syst. 2 (3–4), 213–231.
Santa, J., Gómez-Skarmeta, A.F., Sánchez-Artigas, M., 2008. Architecture and evaluation of a unified V2 V and V2I communication system based on cellular networks. Comput. Commun. 31 (12), 2850–2861.
Li, S.E., Zheng, Y., Li, K., Wang, J., 2015. An overview of vehicular platoon control under the four-component framework, in Intelligent Vehicles Symposium (IV). 2015 IEEE 286–291.
Gong, S., Shen, J., Du, L., 2016. Distributed computation based car-following control integrating optimal system performance for a platoon of autonomous vehicles. Transp. Res. Part B Methodol. 94, 314–334.
Hart, S., Schmeidler, D., 1989. Existence of correlated equilibria. Math. Oper. Res. 14 (1), 18–25.
Nau, R., Canovas, S.G., Hansen, P., 2004. On the geometry of Nash equilibria and correlated equilibria. Int. J. Game Theory 32 (4), 443–453.
Papadimitriou, C.H., Roughgarden, T., 2008. Computing correlated equilibria in multi-player games. J. ACM 55 (3), 14.
Zhu, D., Marcotte, P., 2000. On the existence of solutions to the dynamic user equilibrium problem. Transp. Sci. 34 (4), 402–414.
Behrisch, M., Bieker, L., Erdmann, J., Krajzewicz, D., 2011. Sumo-simulation of urban mobility-an overview, in SIMUL 2011. The Third International Conference on Advances in System Simulation 55–60.
Java Software, 2017. Oracle. [Online]. Available: https://www.oracle.com/java.
Cárdenas, A.A., Amin, S., Lin, Z.-S., Huang, Y.-L., Huang, C.-Y., Sastry, S., 2011. Attacks against process control systems risk assessment, detection, and response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security 355–366.
Haimes, Y.Y., 2017. Risk Modeling, Assessment, and Management. John Wiley & Sons, 2015.
Bahr, N.J., 2014. System Safety Engineering and Risk Assessment: a Practical Approach. CRC Press.
Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart, K., 2016. A review of cyber security risk assessment methods for SCADA systems. Comput. Secur. 56, 1–27.
Heimann, K.R., Chu, H.T., 2017. Traffic control system failure monitoring. Google Patents, 05-Jul-1994.
Zhang, Z., Lv, Z., Mo, J., Niu, S., 2014. Vulnerabilities analysis and solution of VxWorks. 2nd International Conference on Teaching and Computational Science.
N. E. M. Association, 2017. National Transportation Communications for ITS Protocol (NTCIP): Object Definitions for Actuated Traffic Signal Controller Units. National Electrical Manufacturers Association, 1997.
Park, B.B., Chen, Y., 2015. Quantifying the benefits of coordinated actuated traffic signal systems: a case study, KSCE J. Civil Eng. 19 (January (1)), 311–317.
Molisch, A.F., Balakrishnan, K., Chong, C.-C., Emami, S., Fort, A., Karedal, J., Kunisch, J., Schantz, H., Schuster, U., Siwiak, K., 2004. IEEE 802. 15. 4a channel model-final report. IEEE P802 15 (4), 662.
Dobersek, M.M., 1998. An Operational Comparison of Pre-time Semi-actuated and Fully Actuated Interconnected Traffic Control Signal Systems.
Newton, C., Mussa, R.N., Sadalla, E.K., Burns, E.K., Matthias, J., 1997. Evaluation of an alternative traffic light change anticipation system. Accid. Anal. Prev. 29 (2), 201–209.
Komanduri, S., Shay, R., Kelley, P.G., Mazurek, M.L., Bauer, L., Christin, N., Cranor, L.F., Egelman, S., 2011. Of passwords and people measuring the effect of password-composition policies. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2595–2604.
Sensys Networks Inc, 2007. Advantages of the Sensys wireless vehicle detection system.
Jiang, R., Wang, J., Zhang, M., Guan, Y., 2013. Two-stage minimax regret robust unit commitment. IEEE Trans. Power Syst. 28 (3), 2271–2282.
Chen, B., Wang, J., Wang, L., He, Y., Wang, Z., 2014. Robust optimization for transmission expansion planning: minimax cost vs. minimax regret. IEEE Trans. Power Syst. 29 (6), 3069–3077.
Davis, L., 1991. Handbook of Genetic Algorithms, vol. 115 Van Nostrand Reinhold, New York.
Kennedy, J., 2011. Particle Swarm Optimization, in Encyclopedia of Machine Learning. Springerpp. 760–766.
Bellifemine, F., Poggi, A., Rimassa, G., 2000. Developing multi-agent systems with JADE. Intelligent Agents VII Agent Theories Architectures and Languages. Springerpp. 89–103.

Zhiyi Li is pursuing a Ph.D. in the Electrical and Computer Engineering Department at the Illinois Institute of Technology, Chicago, where his research interests include cyber-physical power system and power system optimization. He received his B.S. degree from Xi'an Jiaotong University, Xi'an, China, in 2011 and M.S. degree from Zhejiang University, China, in 2014.

Mohammad Shahidehpour is Bodine Chair Professor and a Director of the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, and also a Research Professor at the King Abdulaziz University, Jeddah, Saudi Arabia. He is a Fellow of IEEE and AAAS and affiliated with the Renewable Energy Research Group at King Abdulaziz University. He received an Honorary Doctorate degree from the Polytechnic University of Bucharest, Bucharest, Romania. Dr. Shahidehpour is a member of the US National Academy of Engineering.