IET Cyber-Physical Systems: Theory & Applications

Research Article

Assessing and mitigating cybersecurity risks of traffic light systems in smart cities

ISSN 2398-3396
Received on 20th October 2016
Revised on 2nd November 2016
Accepted on 4th November 2016
doi: 10.1049/iet-cps.2016.0017
www.ietdl.org

Zhiyi Li[1], *Dong Jin*[2], *Christopher Hannon*[2], *Mohammad Shahidehpour*[1] ✉, *Jianhui Wang*[3]

[1]*Robert W. Galvin Centre for Electricity Innovation, Illinois Institute of Technology, Chicago, IL 60616, USA*
[2]*Department of Computer Science, Illinois Institute of Technology, Chicago, IL 60616, USA*
[3]*Centre for Energy, Environmental, and Economic Systems Analysis, Argonne National Laboratory, Argonne, IL 60439, USA*
✉ *E-mail: ms@iit.edu*

Abstract: Intelligent traffic lights are critical cyber-physical systems that help smart cities to cut road congestion and vehicle emissions. However, they also open a new frontier of cybersecurity. Security researchers have demonstrated ways to compromise the traffic lights to cause potential traffic disruption and public safety degradation. This study aims to raise the public awareness of the cybersecurity issues in traffic light systems. The authors present a bi-level game-theoretic framework for assessing cybersecurity risks of traffic light systems, as the first step towards understanding and mitigating the security vulnerabilities. Additionally, they propose a minimax-regret-based methodology to guide the deployment of defensive measures in traffic light systems against cyberattacks.

1 Introduction

Intelligent transportation systems (ITS), an essential component of the ongoing evolution of smart cities, aim at perfecting decision making in traffic planning and traffic management. Cars, traffic lights, drivers, sensors, roadside units and other public infrastructures form a complex networked system of systems. This evolution will significantly improve citizens' quality of life by introducing many innovative ITS-based applications, such as optimal traffic signal control, safe intersection crossing, and emergency warning notifications, with the goals of enhancing travel efficiency, public safety, emergency response, and even disaster recovery. As the building blocks of an ITS, smart traffic lights are playing an increasingly significant role in traffic management. Networked traffic light systems today can coordinate to optimise the 'green time' for making smooth network-wide traffic flows and reducing exhaust emission pollution.

While the adoption of information and communication technologies on the traditionally standalone-hardware-device-based traffic light systems boosts control efficiency, they also open a new venue for potential cyberattacks. Security researchers have shown various vulnerabilities in traffic light systems [1–3], which would lead to authentication violation, denial of service, and/or spoofing at both network and device layers, with surprisingly inexpensive means. For example, Cerrudo built a $100 commodity device to gain the control of a number of traffic lights in the USA [1]. Maliciously controlling traffic lights to meet personal interests or hamper public safety would no longer occur just in movies but also potentially in real life. Cybersecurity is considered as one of the most important factors for the success of ITS applications, however, little is known about protecting this new cyber-physical system against intentional attacks or inadvertent errors. In particular, there are few studies on the cyber vulnerabilities and solutions of traffic light systems, as well as on the evaluation of the implications for the management of traffic networks if they are compromised.

Cybersecurity risks of traffic light systems imply the potential degradation of traffic management performance due to cyberattack-induced system malfunctions or failures. Conducting risk analysis not only provides an effective means to evaluate the implications of security vulnerabilities in those systems but also facilitates the selection and implementation of defensive measures against potential cyberattacks. Risk analysis paves the way for the traffic management authority to meet the challenges of ever-evolving cyber threats. In this paper, we conduct a comprehensive survey on known and potential cyber vulnerabilities of traffic light systems, assess the risks using a bi-level game-theoretic framework, and propose the corresponding countermeasures. The main contributions of this paper are listed as follows:

(i) We identify the importance of traffic signals in traffic management and develop traffic assignment methods that incorporate the effects of traffic signals under various network conditions.
(ii) We study the cybersecurity vulnerabilities of traffic light systems nowadays, as well as the corresponding defensive measures against the existing and potential cyberattacks.
(iii) We provide a general bi-level optimisation-based framework for assessing the cybersecurity risks of traffic light systems in terms of the physical implications on traffic networks.
(iv) We develop a minimax-regret-based approach to prioritising defensive measures for mitigating cybersecurity risks in traffic light systems; the approach ensures desired traffic management performance under various network conditions.

The remaining of this paper is organised as follows. Section 2 illustrates the role of traffic signals in traffic management. Section 3 analyses the vulnerabilities of traffic light systems. Section 4 presents a general framework for assessing cybersecurity risks of traffic light systems. Section 5 presents a detailed example to illustrate the physical implications of modified traffic signals due to cyberattacks. Section 6 provides a comprehensive approach to mitigating cybersecurity risks of traffic light systems based on the minimax-regret criterion. Section 7 overviews the related work, and Section 8 concludes this work.

2 Understanding the role of traffic signals

2.1 Traffic management in smart cities

In smart cities, strategic intersection control is realised by regulating the associated traffic signals. Traffic signals at an intersection are coordinated by a traffic light system under certain regulations and rules. Common traffic signal settings include cycle offset, phase

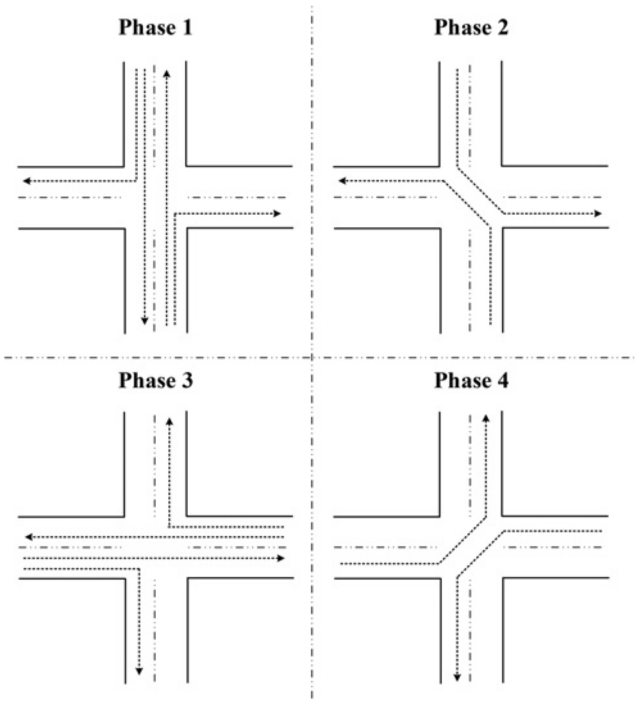

Fig. 1 *Traffic signals at a signalised intersection*

sequence, and phase length. Traffic signals can be represented by repeated cycles, and each cycle consists of several sequential phases. Noteworthy, a longer phase length in the direction with the heavier traffic flow helps to improve local traffic throughput at the intersection, whereas a proper cycle offset and a phase sequence are important for reducing the average waiting time at the intersection. Fig. 1 shows the intersection control by the representative four-phase traffic signals. At this intersection, two roads cross over one another and each road possesses two lanes in the opposite directions. Three types of movement are considered (i.e. going straight, turning right and turning left), and only the movement in the regulated directions (denoted as directed lines) is allowed in each phase.

Traffic signal settings actually impact drivers' route choices. Directly, traffic signals determine the waiting time at intersections, and indirectly, the cruise time on the roads is affected by the potential congestion resulting from suboptimal traffic signal settings. Meanwhile, drivers are capable of communicating with each other and with the traffic management authority in real time by means of vehicular wireless communication technologies.

Real-time information sharing between drivers and the traffic management authority facilitates the management of traffic networks. Drivers can gain a good understanding of the current traffic conditions and also become aware of potential congestion and hazards, whereas a traffic management authority is able to proactively and intelligently manage transportation systems to reduce traffic congestion.

2.2 Traffic assignment considering the effects of traffic signals

In smart cities, drivers can voluntarily report their trip information (e.g. destination and route preferences) either before departure or en-route. After anticipating the future traffic conditions based on the aggregated trip requests, a traffic management authority could provide drivers with routing suggestions (e.g. fastest routes) by performing a traffic assignment that manages to fulfil all the individual drivers' travel requirements with the guaranteed performance of network-wide traffic management. Additionally, traffic assignment can be performed to estimate the pattern of vehicle movements on the roads of the traffic network and obtain aggregated measurements for performance evaluation of traffic management.

Table 1 Notations

Notations	Definition
i, j	nodes in the network
$\boldsymbol{N}_i$	neighbouring nodes of i
$T_{\text{reach}}(i)$	total time consumed to reach i
$T_{\text{cruise}}(i, j)$	cruise time from i to j
$T_{\text{wait}}(i)$	waiting time at i

We develop three distinct methods for traffic assignment with the consideration of traffic signals' effects under different network conditions.

2.2.1 Static traffic assignment: In a network with light traffic (i.e. without concerns of road congestion), each driver can be assigned with any feasible route that has minimal implications on other drivers' route choices. In this condition, we can perform static traffic assignment by separately determining each driver's optimal route using a fastest-route algorithm. This algorithm inherits the advantages of the Dijkstra's algorithm [4] and takes into account the effects of waiting time due to traffic signals at signalised intersections. The details are described as follows and the notations are defined in Table 1.

Step 1: Assign the initial values for every node in the traffic network: for the starting node s, $T_{\text{reach}}(s) = 0$ and for the remaining nodes $T_{\text{reach}}(i) = 0$, $i \neq s$ and set

$$\boldsymbol{T} \leftarrow \{\text{all the nodes}\}, \quad \boldsymbol{S} \leftarrow \emptyset$$

Step 2: If the destination node d is not in $\boldsymbol{T}$, go to step 5. Otherwise, go to step 3.

Step 3: Choose i^* in $\boldsymbol{T}$ with the smallest value of $T_{\text{reach}}(i)$. If $T_{\text{reach}}(i^*) = \infty$, then go to step 5 (i.e. no feasible solution). Otherwise redefine $\boldsymbol{T} \leftarrow \boldsymbol{T} \backslash \{i^*\}$, $\boldsymbol{S} \leftarrow \boldsymbol{S} \cup \{i^*\}$

Step 4: For each node $j \in \boldsymbol{N}_{i^*} \cap \boldsymbol{T}$, if the current traffic light in the direction from i^* to j is 'red', set

$$T_{\text{reach}}(j) \leftarrow \min\{T_{\text{reach}}(j), T_{\text{reach}}(i^*) + T_{\text{cruise}}(i^*, j) + T_{\text{wait}}(i^*)\}$$

Otherwise, set

$$T_{\text{reach}}(j) \leftarrow \min\{T_{\text{reach}}(j), T_{\text{reach}}(i^*) + T_{\text{cruise}}(i^*, j)\}$$

where $T_{\text{cruise}}(i, j)$ is dependent on the cruise speed on road i–j.

Then go back to step 2.

Step 5: Stop and return $T_{\text{reach}}(d)$ as the solution.

2.2.2 Quasi-static traffic assignment: In a potentially congested network with moderate traffic, drivers' unregulated routing decisions may lead to unexpected road congestion, potentially causing adverse effects on other drivers' travel time. To capture the uncertainties of network congestions, traffic assignment can be done in a 'quasi-static' manner, that is, drivers' travel demands are assigned incrementally, fraction by fraction. Accordingly, the network-wide traffic pattern will change with time due to the 'existing' drivers on the road. Note that drivers' cruise time is inevitably affected by the existing traffic. Fig. 2 shows the general relationship between the cruise time and the traffic volume on a road. Clearly, the cruise time is almost stabilised when the existing traffic volume does not result in a congestion on the road, but the time increases significantly when

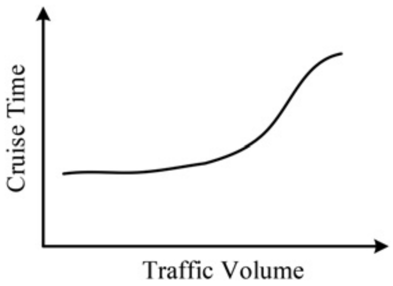

Fig. 2 *Cruise time on the road*

the road is congested. Our approach extends the ant colony optimisation algorithm [5] with time constraints and a new heuristic to avoid local optima, which is described as follows:

Step 1: Set the initial amount of pheromone on each road and the number of ants.
Step 2: Construct solutions for each ant. Each ant starts from the node s and probabilistically moves to the next node which is also added to its tabu list, until it has completed a solution, i.e. either it reaches the destination node d or the next node does not exist. Specifically, the ant at node i will move to node j with the probability of

$$p_{ij} = \frac{\left(\tau_{ij}\right)^{\alpha}\left(\eta_j + \gamma \cdot \lambda_{ij}\right)^{-\beta}}{\sum_{k\in N_i}\left(\tau_{ik}\right)^{\alpha}\left(\eta_k + \gamma \cdot \lambda_{ik}\right)^{-\beta}}, \quad \forall k \in \boldsymbol{N}_i$$

where τ_{ij} is the current amount of pheromone on road i–j; η_j is the Manhattan distance from j to d, which is defined as the distance measured along the grid axes at right angles, namely, $\eta_j = \left|j_x - d_x\right| + \left|j_y - d_y\right|$; λ_{ij} is the expected time spent on road i–j, which is calculated as $\lambda_{ij} = T_{\text{wait}}(i) + T_{\text{cruise}}\left(i, j\right)$; α, β and γ are user-specified parameters to balance the influence of τ_{ij}, η_j, and λ_{ij}.

Step 3: Update pheromones along all the routes taken by the ants travelling from s to d. First, the pheromone evaporation is considered for all roads in the network, which is implemented by $\tau_{ij} \leftarrow \left(1 - \rho_{ij}\right) \cdot \tau_{ij}$, where the different evaporation rates are employed for better computational performance

$$\rho_{ij} = \begin{cases} \rho_{\max} & \text{if } \tau_{ij} \geq \tau_{\text{avg}} \\ \rho_{\min} & \text{if } \tau_{ij} < \tau_{\text{avg}} \end{cases}$$

Then add the pheromone to the roads that the ants have traversed according to $\tau_{ij} \leftarrow \tau_{ij} + \sum_{m=1}^{M} \Delta\tau_{ij}^{m}$, where $\Delta\tau_{ij}^{m}$ is the amount of pheromone that ant m deposits on the road ij, and is defined as

$$\Delta\tau_{ij}^{m} = \begin{cases} \dfrac{\sigma}{T_{\text{reach}}(d)} & \text{if ant } m \text{ travels on road } ij \\ 0 & \text{otherwise} \end{cases}$$

and σ is a user-specified coefficient.

Step 4: Perform the elitist ant strategy. Save the ant with the local best solution, i.e. the minimum value of $T_{\text{reach}}(d)$, and find the ant g with the global optimal solution in the save list. Then enhance the pheromone along the routes ant g traversed $\tau_{ij} \leftarrow \tau_{ij} + \varsigma \cdot \Delta\tau_{ij}^{g}$, where ς is a user-specified coefficient.
Step 5: Go to step 2 if not exceed the iteration threshold, otherwise stop the algorithm and return the global optimal value of $T_{\text{reach}}(d)$ as the final solution.

2.2.3 Dynamic traffic assignment: In an actually congested network with heavy traffic, drivers' fastest routes are interdependent, which complicates traffic assignment and causes unexpected dynamics in the traffic network. With the proper assignment, drivers can finally arrive at the dynamic user equilibrium conforming to Wardrop's first principle. At the equilibrium, no driver can reduce the travel time by unilaterally changing the route within any time interval. Microscopic traffic simulation can help the traffic assignment in such dynamic conditions. In the simulation, vehicle movement can be simulated based on car-following and lane-changing theories, which renders the simulation results being consistent with real-world scenarios. Furthermore, trajectories can be obtained for each driver, which is important for extracting the temporal and spatial dynamics of drivers' behaviours.

The detailed procedure for performing the dynamic traffic assignment is illustrated below [6]:

Step 1: Determine the expected cruise time on each road for drivers departing from their origins at different time steps.
Step 2: Determine a pre-specified number of most fast routes as the candidate routes for each driver considering time-dependent cruise time on each road, which is approximated by the average speed on this road at this driver's departure (updated by the results of microscopic traffic simulation).
Step 3: Determine the probability of each route in the candidate set for the driver to choose. Each driver randomly takes the route according to the probabilities.
Step 4: Run the microscopic traffic simulation using the chosen routes and obtain the actual travel time.
Step 5: If the pre-defined termination criterion is met, terminate the algorithm; otherwise, continue the next iteration by restarting from step 2.

3 Analysing vulnerabilities of traffic light systems

3.1 Components in traffic light systems

The main components of the traffic light system at a signalised intersection are depicted in Fig. 3, including (i) controllers that control traffic light states, (ii) sensors that detect traffic conditions, (iii) networking equipment to communicate to the control centre, to the sensors, and to other intersections, (iv) and malfunction management units (MMUs) that verify safe light states.

The controllers are responsible for setting light states at the intersection. The controllers can operate in multiple modes: (i) pre-timed, i.e. light states change with predetermined intervals; (ii) semi-actuated, i.e. one direction to be always on until sensor data informs the controller to change; and (iii) fully actuated, i.e. receiving data from sensors that determine the optimal timings of the state changes [2]. The controller is typically locked in a metal cabinet near the intersection. In more modern traffic light systems, controllers located at nearby intersections are able to coordinate and result in up to 40% more efficient traffic through corridors [7]. The sensors detect cars commonly through induction loops; however, they can also use video detection, ultrasonic, microwave and radar detection methods. Induction loops are the most reliable but expensive to repair, and video detection can be affected by weather [8]. Traditionally, sensors were connected to the controller through a direct line. This is the most cost efficient and has the smallest barrier to entry compared with wireless communication. Access points can process, store and relay data through TCP/IP networks and can serve as many devices as necessary. The sensors that Cerrudo investigated in his work used IEEE 802.15.4 PHY protocol, commonly used by ZIGBEE devices [1]. The communication methods that the controllers use to communicate with nearby intersections and traffic control centres vary between 900 MHz, 5.8 GHz, and 4.9 GHz. These radios use various protocols, each containing potential security vulnerabilities. The MMU is responsible for detecting conflicting light states so that a dangerous state can be avoided. An example of a bad state that

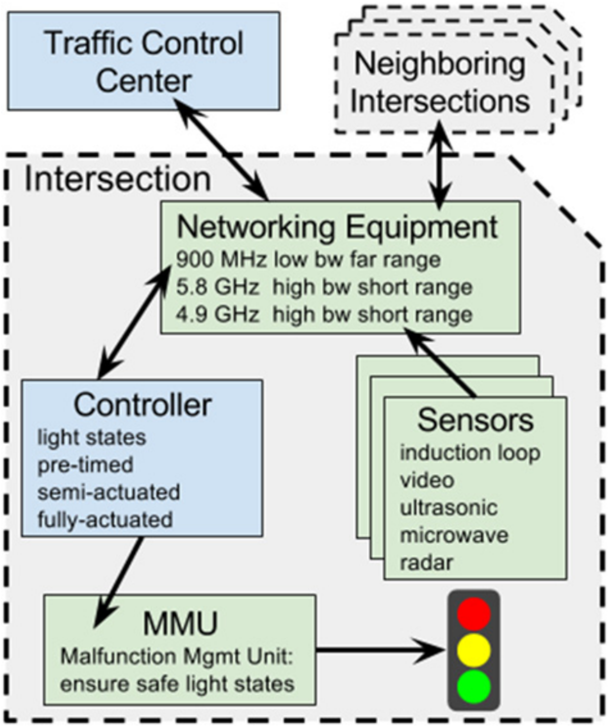

Fig. 3 *Main components in a traffic light system*

would be detected is when at a four-way intersection, there is a four-way green signal [9]. The MMU would detect this before it happens and set the lights to a default state or revert the controller to the pre-timed mode allowing traffic to continue but in a suboptimal condition [10].

3.2 Vulnerabilities of traffic light systems

We conducted a comprehensive literature review and summarised the high-level classification of the possible malicious activities in Table 2. Attacks on a traffic system are divided into three categories: controller attacks, sensor data attacks, and physical attacks.

(i) Controller attacks represent attacks that target the light controller. Authentication and authorisation classify attacks that attempt to gain privileged access to the controllers. On a successful intrusion, the attacker can initiate various denial of service (DoS) attacks on the traffic light system, causing the intersection to enter an undesired and potentially dangerous state. This can be done through spoofing light commands on the light's controller.

(ii) Sensor data attacks are attacks on the sensor data being communicated to the controller. A malicious party can send bogus packets to the access point. In the Sensys Networks sensors, if an attacker eavesdrops on sensor communications with traffic conditions S_1, they can resend the same signals at a later time when traffic conditions are S_2 ($S_2 \neq S_1$) [15]. This would create a replay attack, allowing the controller to operate with misinformed sensor information. If condition S_1 is high traffic North–South and S_2 is high traffic East–West, during a replay attack, the controller would change from seeing road condition S_2 to condition $S_1 + S_2$. This would reduce the efficiency of the intersection and can be used for personal gain. Additionally, some sensors used in traffic infrastructure are susceptible to firmware modification. This would require the attacker to reverse engineer the firmware protocol and exploit authentication issues in the network to upload modified firmware to the sensors [1].

(iii) Physical attacks directly compromise the hardware. Since traffic light systems are designed with resiliency to handle physical system failures, this resilience may also help to reduce the impact of any cyberattacks. However, coordinated attacks performed through a combination of cyber (typically little additional cost to launch at multiple points) and physical mechanisms present a significant threat to the vulnerable physical systems. For instance, the MMU that ensures no dangerous light states being configured (e.g. too short yellow, four-way green etc.) is done through hardware. If this hardware is damaged or removed, a coordinated cyberattack would cause dangerous light states leading to potential massive damage as well as traffic disruption.

3.3 Sample cyberattack scenarios

Traffic light systems in practice have multiple vulnerabilities that can be exploited. Since the attackers can see the service set identifier (SSID) of the network, they may just need to acquire the radio of the same model as the controllers, which can be done through social engineering the manufacturer to sell one [2]. After gaining access to the network, the attacker would attempt to gain access to the controller. The attacker could use file transfer protocol (FTP) to write configuration changes to the controller's database to change the light states. Typically, this uses default usernames and passwords that the attacker can find published directly from the manufacturer. In addition, an attacker 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. It is also possible to perform replay attacks when control commands are sent from the control centre to the traffic lights. If the protocol used to remotely control the lights is standard and unencrypted, the attacker can engineer their own packets to send commands to the light controller. Using these techniques, an attacker can gain access to a light controller network, eavesdrop on traffic, and even control the light states.

4 Assessing cybersecurity risks of traffic light systems

4.1 Cybersecurity risk assessment

Since there exist various malicious cyber means to exploit vulnerabilities of traffic light systems to take control of traffic signals, it is critical to evaluate the potential implications and deploy effective countermeasures to address the cybersecurity concerns. Risk assessment is becoming a foundation for perceiving the security posture in cyber-physical systems. Consciousness of the cybersecurity posture in traffic light systems allows the traffic management authority to determine and prioritise measures to guard against various cyber threats, thereby mitigating the potential implications on the management of traffic networks.

Basically, risk assessment, which manages to translate the present cybersecurity posture in quantifiable terms, is a systematic approach to evaluate the potential physical impacts on traffic networks that attackers can inflict by exploiting the cyber vulnerabilities of traffic light systems. In fact, traffic light systems may confront a range of cyber threats. It would not be possible to enumerate all the possible forms of cyberattacks, let alone multiple attacks which may happen simultaneously. Thus, the most likely cyberattacks (defined as cyber contingencies) against the traffic light systems should be selected first by performing a vulnerability analysis. Given a set of postulated cyber contingencies, we can assess the cybersecurity risk of a traffic light system under a certain traffic network condition by quantifying the following equation

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

where $\mathcal{R}$ denotes the risk; $\mathbb{C}$ is the set of postulated cyber contingencies; and $\mathcal{L}_i$ and $\mathcal{S}_i$ are the likelihood and severity of the ith contingency, respectively.

Table 2 Traffic light system security vulnerability

Classification	Attack techniques	Consequences/use cases
Cyberattack – light controller compromised		
authentication/authorisation [11]	password cracking/social engineering	used for coordinated attack of DoS, eavesdropping, spoofing etc.
authentication/authorisation [11]	access to debug port/memory dump	used for coordinated attack of DoS, eavesdropping, spoofing etc.
denial of service [2, 9, 12]	set all lights to red/restrict changing of light states	traffic disruption, e.g. four-way red
denial of service [2, 9, 12, 13]	set lights to invalid states	traffic disruption, hardware error checking causes lights to go to default schedule
spoofing [1, 2, 12]	change state of intersection	personal gain – change lights to favour attacker or to hinder emergency vehicles, terror attack
Cyberattack – sensor data compromised		
denial of service [1, 9, 13]	flood access point with excess packets	traffic disruption – system uses default schedule
denial of service [1, 14, 15]	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 behaviour
firmware modification [1, 2, 15]	upload firmware to access points and distribute to sensors	invalidate data from sensors, disable sensors
spoofing [1, 2, 14]	replay attack/reverse engineering/saturate network with custom packets	traffic disruption, e.g. ramps, intersections
Physical attack		
compromise failsafe equipment [2, 9, 10]	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 – system uses default schedule

The likelihood of each cyber contingency and the severity of the resulting impact are two key elements of risk assessment. The former is derived at the vulnerability analysis step by using the probabilistic approaches (e.g. Bayesian network), while the latter is identified with the physical implications in traffic networks (denoted as cyber-physical consequences), which is detailed in the following subsection.

4.2 Bi-level framework for evaluating cyber-physical consequences

For each selected contingency under a traffic network condition, the cyber-physical consequences can be quantified as the degradation of traffic management performance, which can be generally expressed as

$$\mathcal{S}_i = \mathcal{P}_o - \mathcal{P}_i^*, \quad \forall i \in \mathbb{C}$$

where $\mathcal{P}_o$ represents the traffic management performance without any cyberattack in the traffic light systems; and $\mathcal{P}_i^*$ is the worst possible traffic management performance under the cyber contingency. Traffic management performance can be evaluated by various metrics (e.g. the number of congested roads, the average travel time of drivers).

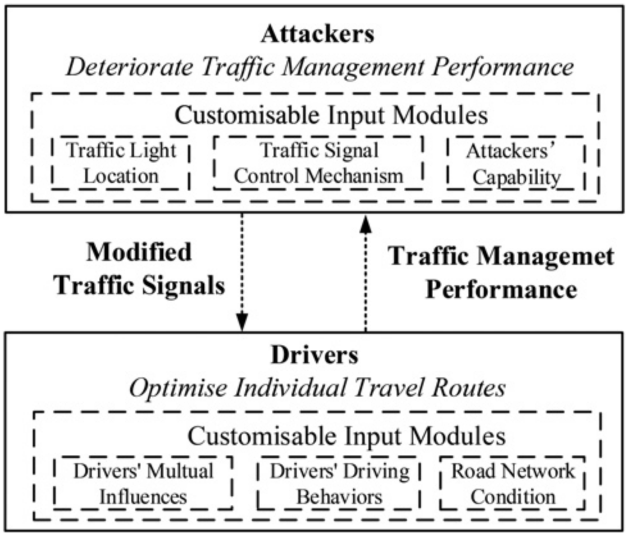
Attackers
Deteriorate Traffic Management Performance
Customisable Input Modules
Traffic Light Location
Traffic Signal Control Mechanism
Attackers' Capability
Modified Traffic Signals
Traffic Managemet Performance
Drivers
Optimise Individual Travel Routes
Customisable Input Modules
Drivers' Multual Influences
Drivers' Driving Behaviors
Road Network Condition

Fig. 4 *Bi-level framework for evaluating cyber-physical consequences in traffic networks*

As an important step towards cybersecurity risk assessment, we develop a general bi-level framework for evaluating the worst-case cyber-physical consequences under various contingencies. As shown in Fig. 4, this framework allows the customisable formulation of both upper-level and lower-level problems, and the flexibility enables us to plug in various input modules with different level of details.

Mathematically, the identification of worst-case cyber-physical consequences can be envisaged as a leader–follower game between attackers (leader) and drivers (follower). These two parties take actions in sequence. Attackers make decisions on compromising the traffic light systems and modifying their settings to change the traffic signals in order to degrade traffic management performance, whereas drivers take and change their routes to shorten their individual travel time based on the compromised traffic signals. Clearly, each party optimises its own objective in consideration of one another's response. Note that the attackers can dynamically adjust their attack strategies according to drivers' behavioural changes. In turn, individual drivers continuously find their own fastest routes given the compromised traffic signals. It is also noteworthy that attacks tend to realise the network-wide travel inefficiency in spite of the fact that drivers make route choices non-cooperatively for their individual optima.

4.3 Interactive solution framework

Reasonably, all the lower-level problems representing the individual drivers' route-choice behaviours can be integrated as a single traffic assignment problem managed by the traffic management authority, as discussed in Section 2.2. However, the resulting bi-level optimisation problem is intrinsically difficult to solve (usually analytical intractable) mainly due to the tight couplings between the two levels, especially when the dynamic traffic assignment is considered.

We propose an interactive solution framework (as shown in Fig. 5) to obtain the optimal or a satisfactory near-optimal solution with appropriate computational efforts. More specifically, this framework iteratively employs a global searcher (e.g. genetic algorithm, particle swarm optimisation) to find a feasible solution

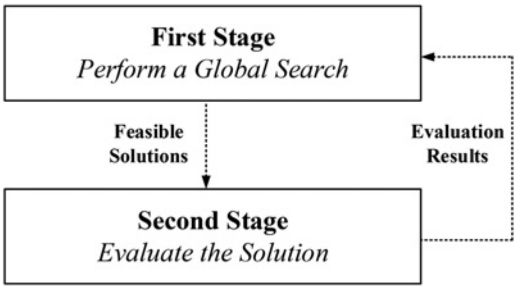

Fig. 5 *Interactive solution framework*

(i.e. an attack plan), and then evaluate the quality of solution in terms of the level of traffic network performance degradation by performing the specified traffic assignment methods. Time-discrete microscopic traffic simulation can also play a role in modelling the traffic network dynamics. Additionally, traffic-adaptive signals are increasingly realised in smart cities, which efficiently overcome the disadvantages of pre-time signals by making prompt responses to any changes in the detected traffic situation. These traffic light systems can be then modelled as agents, while the Java agent development framework (JADE) environment is advantageous in modelling multi-agent systems. With the integration of all the features provided by these methods and/or tools, the cyber-physical consequences can be then quantified in an efficient and reliable fashion.

5 Illustrating cyber-physical consequences in traffic networks

5.1 Model formulation

To illustrate the potential consequences on traffic networks resulting from compromised traffic signals, let us explore a sample scenario by ‘replaying’ a movie scene in *The Italian Job* – a successful robbery escape through intelligently planned routes with the help of compromised traffic lights. In this scenario, an attacker as a part of the robbery team remotely changes the traffic signals in a coordinated manner. After manipulating the traffic signals, the attacker facilitates the escape of the robbers while thwart the policemen to apprehend them.

We create a mesh road network with no possibility of congestion, whose parameters are listed in Table 3. Without loss of generality, each traffic light has two different states indicating traffic flow regulations in two different directions, which are repeated periodically in the regulated intersection and initially exclusive with any neighbouring intersection. The robbers begin to run away at the bottom-left of the network and the policemen start at the bottom-right point, while both parties view the top-right point as their destination. If the policemen can arrive at the destination earlier than the robbers, they will catch the robbers. Otherwise, the robbers succeed in escaping from the policemen. The start time of the policemen is 5 min later than that of the robbers, considering that the NYC’s average 911 end-to-end response time is approximately 5 min in 2014 [16]. To stress the role of traffic light systems, both parties are assumed to obey the regulation of traffic signals at each intersection.

We model this problem in the bi-level optimisation formulation (see Fig. 6), where the upper level determines the traffic signal manipulating strategy that simply changes the original state to the opposite, and the lower level is comprised of the two adversaries’ decisions on their own fastest routes from two different origins to the same destination. The attack’s objective is to maximise the time gap between their partners and the policemen on reaching the destination. Given the compromised traffic signals, the robbers manage to take an optimal route with the minimum possible waiting time at the intersections, while the policemen have to spend much longer waiting time on their routes.

Table 3 Parameters of the road network

network size	8 mile × 8 mile
block length	1 mile
vehicle speed	72 mile/h
traffic light location	at each intersection
traffic light changing frequency	1/min

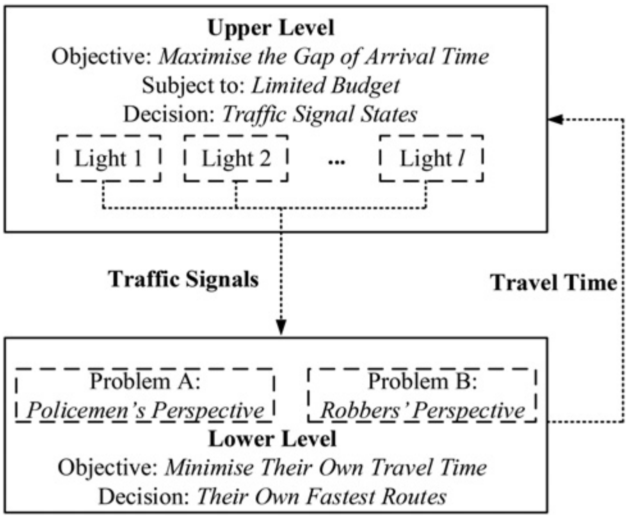
Upper Level
Objective: Maximise the Gap of Arrival Time
Subject to: Limited Budget
Decision: Traffic Signal States
Light 1
Light 2
...
Light l
Traffic Signals
Travel Time
Problem A:
Policemen's Perspective
Problem B:
Robbers' Perspective
Lower Level
Objective: Minimise Their Own Travel Time
Decision: Their Own Fastest Routes

Fig. 6 *Specific bi-level optimisation framework for the Italian job scenario*

5.2 Solution methodology

We solve this bi-level problem by using the genetic algorithm [17], which is capable of offering high-quality near-optimal solutions with affordable computational cost. Accordingly, the original problem is decoupled into two single-level problems to be solved in sequence. Furthermore, the inherent parallel structure enables the parallel execution of the genetic algorithm to accelerate the solution speed. The main solution process is described as follows:

Step 1: Initialisation. We randomly generate the initial population, where each individual represents a candidate solution that is encoded as a real-valued string of length n. Each gene represents an indexed traffic light in the road network and n is determined by

$$n = \lfloor N/c \rfloor$$

where N is the budget and c is the cost to compromise a traffic light.

Step 2: Fitness evaluation. Individual’s fitness is the value of the objective function of the upper-level problem, which is computed after solving all the lower-level problems by the modified Dijkstra’s algorithm.

Step 3: Evolution. The population is updated by replacing all individuals at the current generation, with new potential solutions based on each individual’s fitness. We implement this step using the following genetic operators:

Selection: Individuals of the current generation are randomly chosen as the parents of the next generation using a roulette wheel mechanism until the number of parents is equal to the size of the population.

Mating and *crossover:* Parents are selected and arranged in couples to produce two solutions of the next generation. For simplicity, we implement a single-point crossover by randomly selecting a location in the parent strings and swapping the right-side substrings.

Mutation: Individuals are randomly self-mutated to avoid the premature convergence and maintain the population diversity.

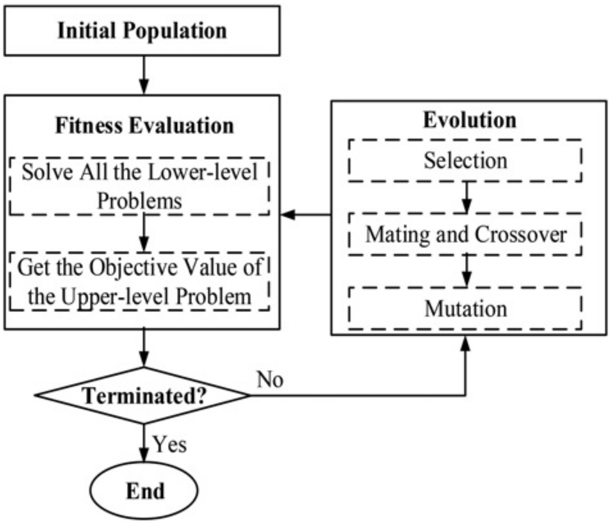

Fig. 7 *Solution method based on the genetic algorithm*

Step 4: Termination check. If the iteration counter does not exceed the threshold, we go to step 2, otherwise we stop the algorithm and return the global best value as the final solution.

The whole process for solving the bi-level problem is shown in Fig. 7.

5.3 Experimental results

The average time for obtaining high-quality solutions using the genetic algorithm is less than 1 min when the size of the population is set to 20 and the generation limit is set to 50. Fig. 8 shows the fastest routes for both parties before and after the attacker manipulating traffic signals at five intersections on the synthetic road network, where the locations of the compromised traffic lights are marked in purple dots. Fig. 8 also shows the fastest routes for the policemen and the robbers (as marked in red and blue, respectively) as well as the arrival time at the destination after the robbers begin to escape. With the help of the compromised traffic light systems, the robbers manage to escape from the chasing policemen. Furthermore, the relationship between the time gap and the number of compromised traffic light systems is shown in Fig. 9. The negative sign means that the robbers arrived later than the

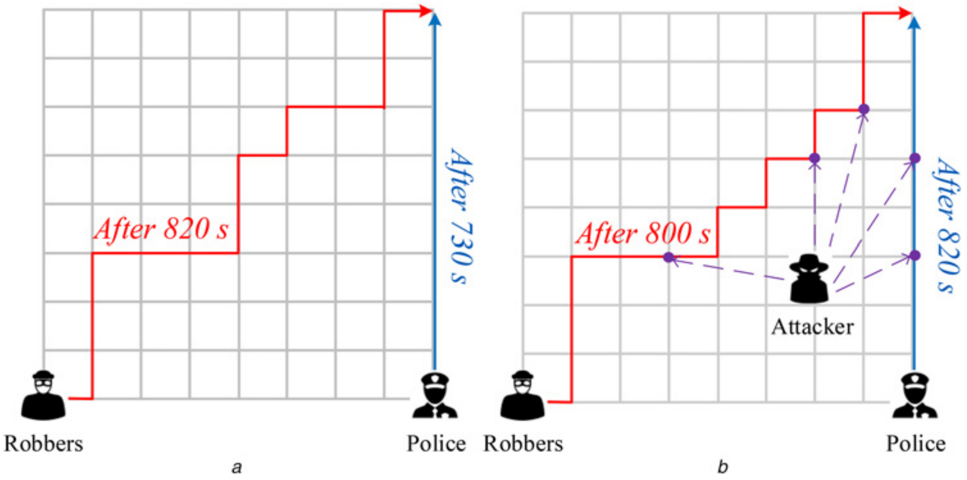

Fig. 8 *Fastest routes before and after compromising traffic lights*

a Original traffic network
b Compromised traffic network

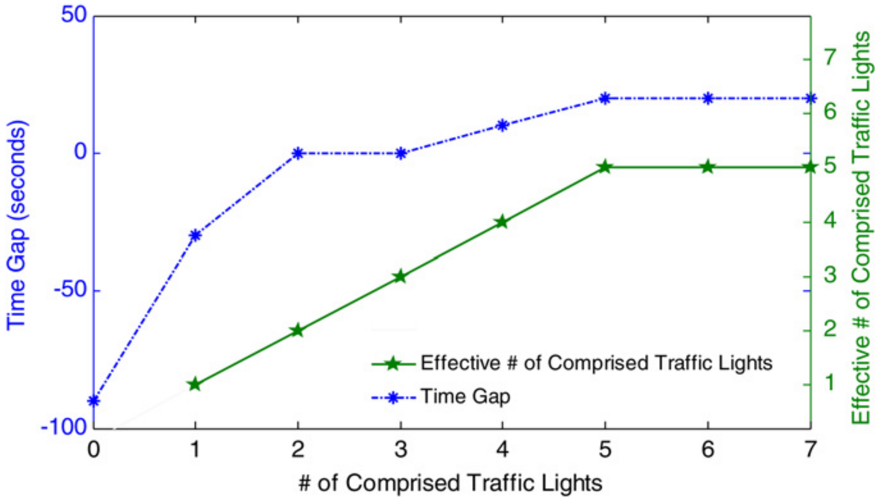

Fig. 9 *Time gap against the number of compromised traffic lights*

Table 4 Countermeasures against cyberattacks in traffic light systems

Vulnerability	Countermeasure
Controller	
authorisation	disable debug port [11]
authentication	change default username/password [18]
spoofing	whitelist known authorised connections
eavesdropping/ authorisation	encrypt data on wireless communication channels [2]
Sensor data	
replay attack/spoofing	add timestamp to data sent to controller/ encrypt traffic [15]
firmware modifications	whitelist known authorised connections
Physical devices	
access to controller/MMU/ sensors	make controller cabinet inaccessible/secure

policemen. Initially, the time gap increases with more compromised traffic lights. However, the increase of time gap halts after a certain threshold, which indicates that compromising additional traffic lights generates no further gain for the escapees.

6 Mitigating cybersecurity risks

6.1 Prevention and countermeasures

To ensure safety and order in traffic infrastructure, security concerns must be addressed when designing traffic systems. We summarise the existing countermeasures against cyberattacks in traffic light systems in Table 4. Manufacturers are required to make certain changes to their current controllers to prevent unauthorised access. The most critical precaution is disabling any debug port that attackers can use to gain access. The debug port allows for attackers to perform memory dumps that can reveal passwords and other critical data regarding the system configuration [11]. Furthermore, passwords need to be changed from the factory default. They should be applied with good practice and changed periodically [18]. To prevent malicious users from impersonating or altering sensor communication on the network, encryption should be used to transmit all data on the network. This would prevent eavesdropping on the sensor to controller communication as well as controller to controller communication. Sensors need to be designed so that firmware cannot be modified arbitrarily or without authorisation. This requires the manufacturers to enable the devices to only allow known connections to make changes, also taking into account encryption and authorisation techniques [15]. Communication between the sensors and the controller should contain timestamps to prevent replay attacks of sensor data on the network.

6.2 Minimax-regret framework for mitigating cybersecurity risks

Given a set of countermeasures, we have to make certain trade-offs to balance cybersecurity versus performance, cost, and usability. To quantify the effectiveness of countermeasures, we utilise a popular subjective decision rule, namely, the minimax-regret criterion. Here the regret for a combination of countermeasures under a certain traffic network condition is defined as the risk under this condition with no countermeasures being deployed. With this criterion, the traffic management authority is capable of prioritising and implementing the combination of countermeasures that are acceptable under all possible traffic network conditions (which can be simply sampled as a set of representative scenarios). The corresponding countermeasures manage to minimise the worst-case regret. Fig. 10 shows the general decision framework for realising the minimax-regret approach.

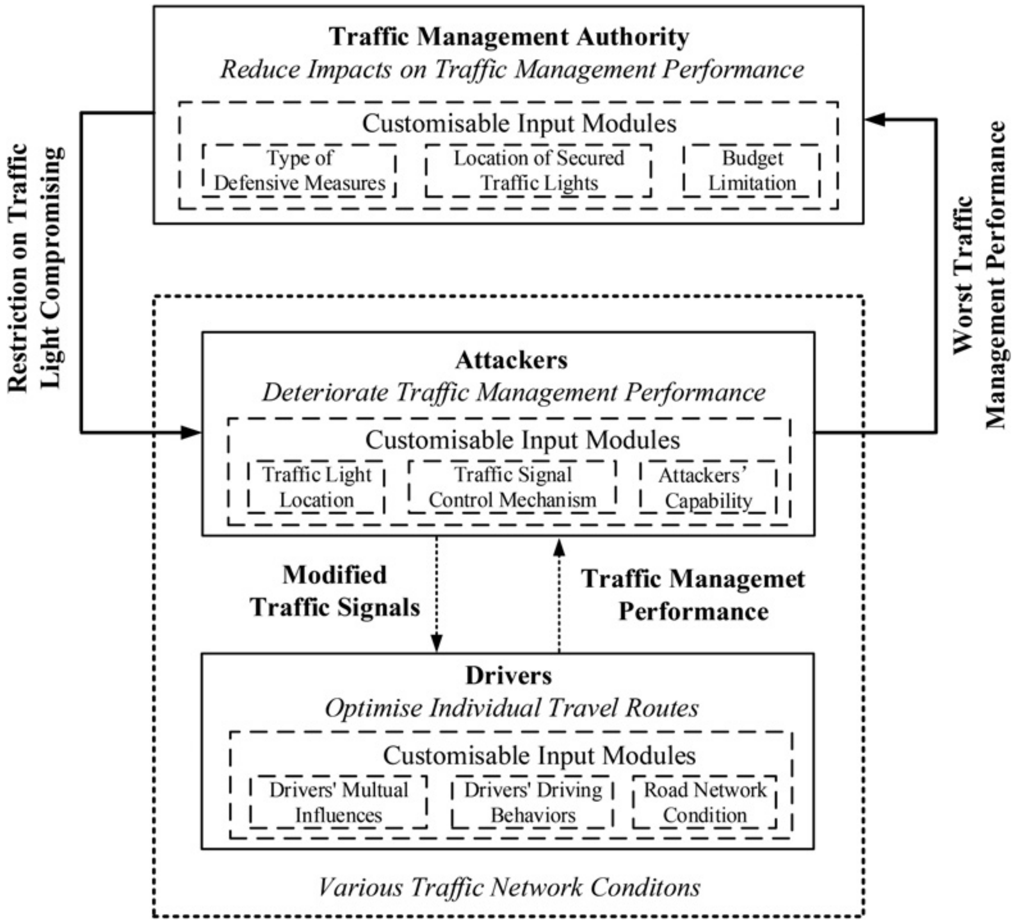
Traffic Management Authority
Reduce Impacts on Traffic Management Performance
Customisable Input Modules
Type of Defensive Measures
Location of Secured Traffic Lights
Budget Limitation
Restriction on Traffic Light Compromising
Worst Traffic Management Performance
Attackers
Deteriorate Traffic Management Performance
Customisable Input Modules
Traffic Light Location
Traffic Signal Control Mechanism
Attackers' Capability
Modified Traffic Signals
Traffic Managemet Performance
Drivers
Optimise Individual Travel Routes
Customisable Input Modules
Drivers' Multual Influences
Drivers' Driving Behaviors
Road Network Condition
Various Traffic Network Conditons

Fig. 10 *Generalised framework for mitigating cybersecurity risks*

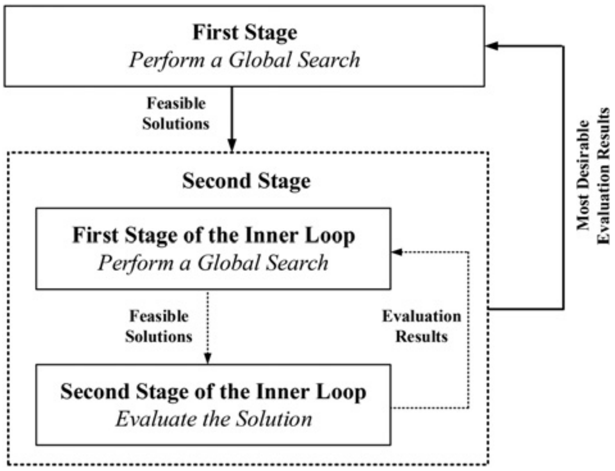

Fig. 11 *Layered solution framework*

In essence, the minimax-regret selection of countermeasures can be envisaged as a multi-player strategic game which involves three parties taking actions in sequence: (i) the traffic management authority deploys countermeasures to secure the traffic light systems in order to reduce the potential cyber-physical consequences on traffic management; (ii) attackers compromise the traffic light systems lacking adequate security measures in order to deteriorate traffic management performance; and (iii) drivers hope to improve traffic management performance by finding their individual fastest routes. Obviously, each group optimises 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).

6.3 Layered solution framework

To solve the complex three-level problem fitting the minimax-regret framework, we develop a layered solution framework (as shown in Fig. 11) where all the solution methods are discussed in Section 4.3 can be viewed as the inner loop. A global searcher at the first stage iteratively seeks a feasible set of countermeasures that are then passed to the second stage for evaluating their effectiveness, while effectiveness evaluation is accomplished iteratively in the inner loop. Only when the iteration terminates in the inner loop, the effectiveness in terms of worst-case traffic management performance can be finally determined and the search process at the first stage continues until a satisfactory solution is obtained.

7 Related work

U.S. Department of Homeland Security released the critical infrastructure protection plan in 2013 to guide the national effort to enhance cybersecurity and cyber-resilience of many national critical infrastructures including transportation systems [19]. Recently, security researchers have demonstrated various cyber vulnerabilities in the deployed traffic light control systems, which strongly motivate our work on building the optimisation-based framework to understand those vulnerabilities of traffic light systems. Ghena *et al.* [2] analysed the security of traffic infrastructure and discovered several vulnerabilities such as lack of common security practice (e.g. the default username and password remains unchanged, the debug port remains open) and no encryption support in the wireless communication. Cerrudo [1] reverse engineered the wireless communication protocol, and built a $100 commodity device to spoof the wireless sensors to tamper the traffic light timing signals. Goodspeed [20] managed to compromise the database on an Econolite ASC/3 traffic controller to alter the configuration of light timing and policy. The researchers have also investigated various evaluation methodologies for transportation system security and resilience, including finite-horizon optimal control to evaluate attacks on monitoring and control components, game theory based approaches to analyse network performance [21] and resilience of vehicular networks [22], and vulnerability analysis frameworks for transportation networks under the traffic signal tampering attacks [23] and road link closures due to natural disasters [24].

8 Conclusion

Cybersecurity is playing an increasingly important role in the evolution of smart cities. Evidently, security vulnerabilities of traffic light systems render the traffic management subject to a variety of cyber threats, either intentionally or inadvertently. Therefore, it is critical to assess and mitigate cybersecurity risks of traffic light systems in order to guarantee the benefits brought by ITS (e.g. enhanced road safety, improved traffic efficiency). This paper presents generic risk-based frameworks for evaluating the implications of compromised traffic signals as well as guiding the deployment of defensive measures in the traffic light systems. This paper aims to lay the foundation of future research on mitigating vulnerabilities of traffic light systems and raise the public awareness of cybersecurity issues of ITS applications in smart cities.

9 Acknowledgments

This work was partly sponsored by the Air Force Office of Scientific Research (AFOSR) under grant FA9550-15-1-0190. J. Wang's work was supported by the US Department of Energy (DOE)'s Office of Electricity Delivery and Energy Reliability. 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 AFOSR and DOE.

10 References

1 Cerrudo, C.: 'Hacking US traffic control systems', available at: https://www.defcon.org/images/defcon-22

2 Ghena, B., Beyer, W., Hillaker, A., *et al.*: 'Green lights forever: analyzing the security of traffic infrastructure'. Proc. Eighth USENIX Conf. Offensive Technologies, 2014

3 Laszka, A., Potteiger, B., Vorobeychik, Y., *et al.*: 'Vulnerability of transportation networks to traffic-signal tampering'. Seventh ACM/IEEE Int. Conf. Cyber-Physical Systems (ICCPS), April 2016

4 Dijkstra, E.W.: 'A note on two problems in connexion with graphs', *Numer. Math.*, 1959, **1**, (1), pp. 269–271

5 Dorigo, M., Birattari, M., Stutzle, T.: 'Ant colony optimization', *IEEE Comput. Intell. Mag.*, 2006, **1**, (4), pp. 28–39

6 Li, Z., Shahidehpour, M., Khodaei, A., *et al.*: 'Optimizing signal settings of traffic lights in smart cities', *IEEE Trans. Smart Grid*, doi: 10.1109/TSG.2016.2526032

7 Park, B., Chen, Y.: 'Quantifying the benefits of coordinated actuated traffic signal systems: a case study'. Technical Report VTRC 11-CR2, Virginia Research Transportation Council, Charlottesville, VA, July, 2010

8 American Public Transportation Association (APTA) Published Standards, http://www.apta.com/resources/standards/Pages/default.aspx

9 Minnesota Department of Transportation: 'Traffic signals 101 – controller operations', available at: http://www.dot.state.mn.us/trafficeng/p-ubl/signals101/2014/06_Controller_Ops.pdf

10 Heimann, K., Chu, H: 'Traffic control system failure monitoring'. U.S. Patent 5327123 A, 5 July 1994

11 Dept. of Homeland Security, Advisory (ICSA-10-214-01), *Wind River VxWorks Vulnerabilities*, ICS-CERT, 2 August 2010

12 National Transportation Communications for ITS Protocol. 1202. NTCIP object definitions for ASC, 2007

13 Dobersek, M.: 'An operational comparison of pre-time, semi-actuated, and fully actuated interconnected traffic control signal systems', 1998. available at: http://epublications.marquette.edu/dissertations/AAI9912724

14 IEEE 802.15.4 PHY Standard for information technology, telecommunications and information exchange between systems, October 2003

15 Sensys Networks Inc.: 'Advantages of the Sensys™ wireless vehicle detection system', 2007, available at: http://www.sensysnetwork-s.com/white-papers/

16 NYC Analytics: '911 performance reporting: 911 end to end detail', available at: http://www.nyc.gov/html/911reporting

17 Davis, L.: ‘Handbook of genetic algorithms’ (Van Nostrand Reinhold, New York, 1991), vol. 115

18 Komanduri, S.: ‘Of passwords and people: measuring the effect of password-composition policies’. Proc. SIGCHI Conf. Human Factors in Computing Systems, 2011

19 Department of Homeland Security: ‘National infrastructure protection plan’, available at: www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

20 Goodspeed, T.: ‘Reversing the Econolite ASC/3 traffic light controller’. ToorCon Seattle, 2008

21 Reilly, J., Martin, S., Payer, M., *et al.*: ‘On cybersecurity off reeway control systems: analysis of coordinated ramp metering attacks’, Transportation Research Board 94th Annual Meeting, 11-Jan 2015

22 Alpcan, T., Buchegger, S.: ‘Security games for vehicular networks’, *IEEE Trans. Mob. Comput.*, 2011, **10**, (2), pp. 280–290

23 Laszka, A., Potteiger, B., Vorobeychik, Y., *et al.*: ‘Vulnerability of transportation networks to traffic-signal tampering’. 2016 ACM/IEEE Seventh Int. Conf. Cyber-Physical Systems (ICCPS), 2016, pp. 1–10

24 Jenelius, E.: ‘Large-scale road network vulnerability analysis’. PhD thesis, KTH, 2010