Chapter

Intersection Management, Cybersecurity, and Local Government: ITS Applications, Critical Issues, and Regulatory Schemes

Yunfei Hou, Kimberly Collins and Montgomery Van Wart

Abstract

This article focuses on the cybersecurity issues of intersection management—an element of transportation management systems—for local governments. Until relatively recently, concerns about and research needs for intersection cybersecurity have been largely ignored, and local governments have focused on other types of cyber threats, relying instead on private sector vendors to provide equipment that is safe against attacks. To address the gap in the literature, this article provides a short overview of the types of components used in intelligent transportation systems (ITS) and reviews the critical issues for local governments. Further, it discusses some current efforts to remediate the vulnerabilities in ITS and examines the current regulatory framework. This review of the issues is augmented by an analysis of local government perspectives using the Delphi method. The article concludes with some recommendations.

Keywords: transportation cybersecurity, transportation management systems, intelligent transportation systems, local government, intersection management

1. Introduction

As the transportation systems of the US grew and became more complicated to manage, intelligent management systems were used to more effectively and efficiently manage traffic. However, Intelligent transportation systems (ITS) technologies and applications have brought enormous opportunities and challenges. ITS deployment appears to have the most broad-based benefit in the area of improved mobility (ITS-JPO 2015–2019) [1], and in terms of opportunities and a sub-function of Smart Cities, intelligent systems are already providing advantages related to:

- Efficient timing/coordination of lights based on sensors, remote traffic monitoring and control,

- Traffic management based on road sensors, CCTV, satellites, cameras, metering, and electronic toll collections,

- Transit signal priority, and

- Traveler information systems (TIS).

Still, even while making the most of the technologies that already exist and integrating those advancements into vehicles and infrastructure where possible, the challenges of ITS technologies and their security implications are also enormous. A failure to identify significant vulnerabilities, and properly address them can leave a municipality at the mercy of a state actor or a misguided teen alike.

This article will present the challenges introduced by cyberspace and ITS. It will review cybersecurity incidents that have impacted local governments in the remaining of Section 1. It will provide an overview of ITS management and critical issues in Section 2 and 3 respectively. Then in Section 4 and 5, the results of a small but multi-perspective study of local government experiences and perceptions about local government cybersecurity issues and ITS are reported. The article ends with practical and research recommendations in Section 6, and Section 7 concludes this paper.

1.1 The challenges of cyberspace and ITS

Cyberspace is a unique environment that easily and readily allows governments, criminals, terrorists, and even mischievous juveniles to mask their identity while they wreak havoc or disable a system [2]. Right now, the average breach in America takes around 5 months to discover [3, 4]. Public agencies historically relied on "security through obscurity" to avoid attack or exploitation, knowing that a system may be vulnerable, but relying on the thought that a system's weaknesses were not common knowledge and persons with malicious intent were unlikely to find them [5]. This approach worked relatively well prior to the digital revolution, but from the late 1990s on, agencies have switched to extremely common commercial technologies such as Wi-Fi and Ethernet for field devices (traffic signals, sensors, dynamic messaging signs, etc.) that communicate with central monitoring systems. This resulted in a significant increase in the attack surface of ITS and thus a significant increase in the risk to ITS.

Cybersecurity threats present themselves in a variety of ways. They may be:

- External or internal attacks (bad actor(s) outside or inside the system)

- Software attacks (both immediate and ongoing or evasive by design)

- Physical manipulation (intentional and/or unintentional exploitation of hardware)

- Single acts or a combination of discrete steps threaded together [2]

The technologies that were once obsure and expensive are now readily available and low cost. As such, it has essentially eliminated any value from reliance on security through obscurity. The safe and efficient operation of a traffic management system relies largely on the application of advanced technologies [6]. And while new technologies have greatly enhanced how traffic signals work and efficiently operate, these technologies have also increased the exposure to numerous cybersecurity threats [7]. Of specific interest here are the cybersecurity threats posed by various types of connectivity, not only external, but also from "credible" sources [8, 9]. Although these threats can extend in severity all the way to the level of terrorism, some of those primary threats include:

- Denial of Service, such as jamming Wi-Fi signals or blocking access to authorized users [10, 11].
- Traffic congestion, such as wrongly rerouting/timing vehicles
- Individual/multiple traffic signal control, such as changing all lights green [12].
- Autonomous/connected vehicle manipulation, such as seizing command of a vehicle's braking system [13].
- Spear phishing, such as targeted online attempts to steal sensitive information, either directly from a credible actor/employee or from the system itself [14, 15].
- Privacy issues, such as bad actors tracking specific vehicles via different sensors in different positions [7].
- These issues are not just theoretical. There have been major incidents that have taken place in recent years throughout the United States. Local governments can be particularly vulnerable as they lack the resources both human and financial to prepare themselves against possible threats. The following section will present three short cases of cyber incidents in local governments.

1.2 Local government cybersecurity incidents

Local governments have been shown to be susceptible to cyberattacks. According to a 2016 report [16], 44% percent of local governments said they experience cyberattacks at least daily. It is believed that the actual rate of cyberattacks is much higher, since less than 60.1% of local governments actually catalog or count how often their systems are attacked. The magnitude of cybersecurity incidents ranges from mischievous attacks (e.g., road signs manipulation) to attacks that interrupt the daily activities of governments (e.g., infected servers that interrupt activities). The following provides a famous example of hacking into the city of Atlanta, followed by some examples of agencies affected by hacking incidents in of ITS in Southern California.

1.2.1 The City of Atlanta

Perhaps the most devastating known cyberattack in the United States against a government agency occurred against the city of Atlanta in March of 2018 [17, 18]. Atlanta was hit by a variation of ransomware called "SamSam" [19, 20]. The perpetrators of this attack are still at-large and unknown.

The city of Atlanta suffered major inconveniences as a result of the SamSam ransomware cyberattack. The security issues in the system had ironically been pointed out 2 months before the attack in January 2018 by the Atlanta City Auditor's Information Security Management System Pre-Certification Audit. The most crucial concerns noted in the audit report revolved around the disregard of establishing IT security control procedures [21]. The main issues listed included the lack of creating and maintaining Information Security Management System (ISMS) formal policies and procedures; lack of creating a comprehensive annual plan to aid in the meeting of security goals and compliance; and the lack of available staffing that "impact their ability to stay ahead of the security issues, such as migration of obsolete operating systems, patch management, and vulnerability management" ([21], p. 16). On March 22, 2018, the vulnerabilities were exploited by the SamSam ransomware, even though the city had been forewarned.

In June 2018, almost 3 months after the attack, it was reported that the city was still struggling to recover [22]. Over one-third of 424 software programs used by the city remain unusable or partly unusable. The ransomware attack took down crucial city systems that aid the city in managing police records, infrastructure maintenance requests, and revenue collection.

The ransom demanded by the SamSam hackers was a total of $51,000 in Bitcoin. Atlanta reportedly did not pay the ransom, but the initial cost of restoring the city's computer network amounted to $2.7 million dollars [23]. In a recent budgetary meeting, the interim CIO requested an increase of $9.5 million dollars to the $35 million already allocated to the IT department. The extra budget allocation would serve to continue the city's efforts of restoring the city's computer network [24]. Overall, the SamSam ransomware cyberattack had significant impacts on the City of Atlanta's computer network, showing local government agencies the importance in keeping their systems up-to-date.

1.2.2 California department of transportation

One documented prominent instance of hacking in the study area caused an episode of public concern. In December 2015, an unknown person hacked into a California Department of Transportation (Caltrans) digital road sign in the City of Corona along the 15 freeway, a major arterial highway. The signal was hacked to display a political message endorsing the then-presidential candidate for office, current U.S. President Donald Trump. The sign displayed the message "The Inland Empire Supports Donald Trump, Merry Xmas". The hacker was able to gain physical access to the road signal, hack the system, and obtain the security passcode to change the road sign message.

In a local news segment regarding the event, an official for the Riverside County Transportation Commission, explained that this hacking incident, although seemingly benign, is very much a public nuisance because it interferes with relaying drivers with vital information about transportation construction projects and delays that could be occurring [25]. Furthermore, the hacking of public signs by vandals is both a distraction to drivers and unsettling to public confidence. While a seeming minor nuisance, this type of act can create dangerous or even life-threatening situations. For example, signs can be used to redirect traffic to hazardous areas. They can also be used as part of complex coordinated attack, where creating traffic jams will slow or block responding vehicles.

1.2.3 Orange County transportation authority

In another incident in the study region, the Orange County Transportation Authority (OCTA) had a bout with ransomware in February 2016. The attack, carried out by unknown hackers, affected around 88 of OCTA's 400 servers. The ransomware affected approximately 20 internal applications that controlled payroll, email, etc. Fortunately, transportation systems were not affected [26].

The hackers demanded $8500 dollars, but OCTA chose to ignore the ransom demand and had internal staff and contractors bring the system back to normal. It took approximately two and a half days to restore the system servers. The total cost of the ransomware attack was around $660,000—approximately $330,000 went to internal labor costs and contractors, and $218,000 was paid to Microsoft and another contractor to eliminate any remaining malicious code, and to help them devise a plan to prevent another attack [27].

2. Overview of ITS applications at signalized intersections

In this section, an overview of ITS components and applications at signalized intersections is discussed. This overview will provide the needed foundation for understanding the major components of ITS to better appreciate the cybersecurity issues discuss in a later section.

2.1 Components in traffic signal systems

The modern traffic intersection consists of various sensors, controllers, malfunction management units, and communication devices. **Figure 1** illustrates some common devices found at intersections.

Sensors employing ultrasonic, microwave, and radar technology, as well as induction loops and video cameras are all used to detect traffic conditions at intersections. The induction loop is the most popular sensor for vehicle detection. These devices are buried under the pavement and detect vehicles by measuring a change in electric current due to the metal body of a vehicle. Video cameras are also frequently used at intersections, and rely on computer vision software to detect and classify vehicles. It is worth noting that video traffic detectors are usually stationary. Additionally, cameras are installed to provide live and steerable video feed to traffic management centers. Microwave, radar, and ultrasonic sensors are less common, but can be used for special applications. Aside from detecting fine-grained vehicle presence, Bluetooth/Wi-Fi traffic detectors are sometime installed at intersections to track vehicle travel time and speed. These sensors detect and time-stamp a Bluetooth/Wi-Fi MAC address from smartphones and in-vehicle hands-free audio, then use the time-stamps of subsequent detections of that address to determine vehicle travel time across known distances between sensors.

Controllers are responsible for setting light timing patterns at intersections. Sensors are directly connected to the controller, allowing it to adaptively adjust signal timings based on traffic conditions. Traffic signal controllers can operate in several modes: 1) pre-timed, e.g., signal states change with predetermined intervals; 2) actuated, e.g., one or more directions are green, based on sensor input; 3) coordinated, e.g., controllers of nearby intersections can be interconnected to share timing information and react to sensor input. Traffic signal controllers are typically locked in a metal cabinet by the side of the traffic signal's pole.

Networking equipment for traffic signals may include both hard-wired and wireless systems. In urban areas, traffic controllers are usually hard-wired through optical or cable networks. Traffic controllers may communicate with each other and with

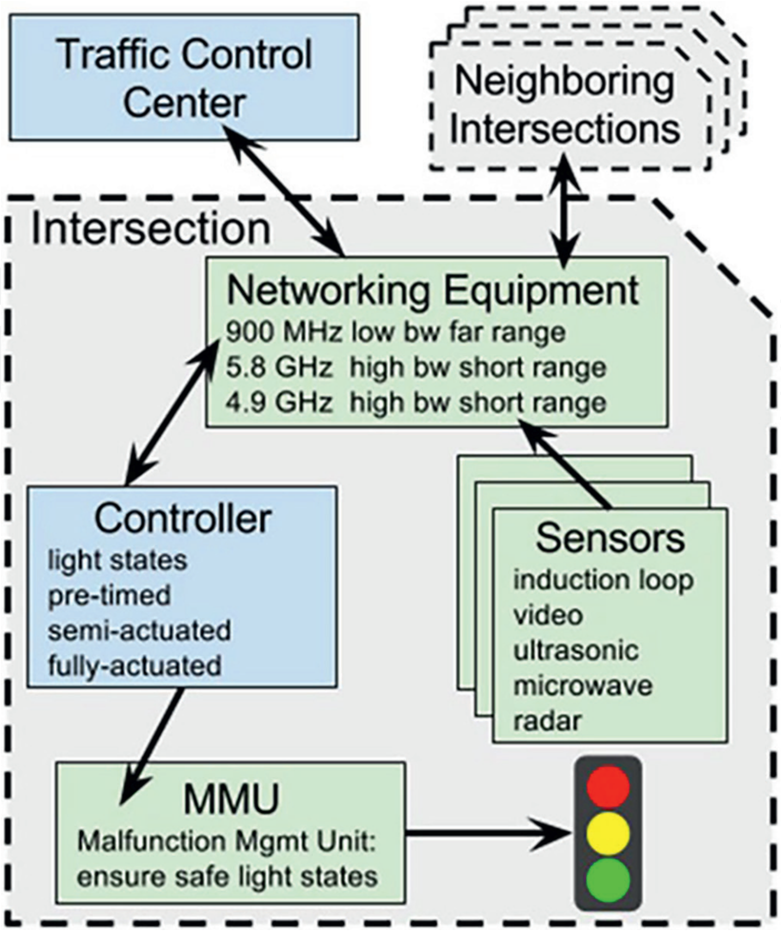

Figure 1.
Main components of a traffic signal system [28].

traffic management centers. When intersections are geographically distant, wireless systems are frequently used. According to FCC regulations, these wireless systems operate on the ISM band at 900 MHz or 5.8 GHz, or in the 4.9 GHz band allocated for public safety. Communication between sensors has traditionally been connected to the traffic controller through a direct line. If wireless sensors are used, an intersection may be equipped with access points and repeaters to process, store, and relay data. Wireless systems for traffic signal controllers and sensors usually run on proprietary protocols derived from IEEE 802.11 or IEEE 802.15 standards.

Malfunction Management Units (MMU), also known as conflict monitor units (CMU), are hardware-level fail-safe mechanisms. The MMU monitors the outputs of the controller, and if a fault is detected (e.g., green signaling in all directions, or too short of a red light duration), the MMU overrides the controller and forces it to switch the intersection to a known-safe configuration (e.g., red lights flashing for all directions). While MMU prevents displaying a potentially hazardous combination of signals, its safe configurations are pre-defined and thus suboptimal. If the MMU detects a fault state, it requires manual intervention to reset.

Traffic Control Center, also known as traffic management center (TMC) or traffic operations center, is the facility that monitor and control transportation-related information, and coordinate responses to traffic incidents. Traditional traffic control center uses closed-loop network equipment (such as video camera and vehicle counters) to monitor traffic condition and coordinate construction activity, roadway advisories, incident management etc. As traffic control centers are moving toward providing intermodal, interregional and interagency traffic management services, their increasing complexity leads to increases in vulnerability of cyber-attacks.

2.2 Technologies for signalized intersections

While the traffic management infrastructure was traditionally built on closed, proprietary systems, the industry is currently on a journey to switch to more connected, responsive and secured networking. Virtually all aspects of a transportation management system are susceptible to cyber threats [2]. Nevertheless, the change to a connected system must happen due to increasing traffic demands, maintenance costs, and the complexity of legacy systems. On the other hand, consumers are demanding new transportation solutions that can provide safer, more efficient, and sustainable travel options. To this end, a wide range of transportation technologies have been proposed. What follows is a brief review some of the most important general applications.

ATMS/Central System: Advanced traffic management systems (ATMS) consist of transportation management centers, field infrastructure, and mobile units communicating in real time to monitor and manage transportation systems. Real-time traffic data from cameras, speed sensors, etc. are sent into a central system where it is integrated and processed (e.g., for incident detection), and may result in actions taken at traffic infrastructures (e.g., change of signal timing, roadside messages). ATMS are the commend centers for reducing congestion, enhancing safety, and providing faster emergency response times. The main functions of an ATMS are: signal performance measurement, system assessment (collecting data), strategy determination, strategy execution, and strategy evaluation.

Dynamic Message Signs: Dynamic Message Signs, also known as Variable Message Signs, are the large, electronic signs which overhang or appear along roadways. The signs are typically used to display information about traffic conditions, travel times, construction, and road incidents.

Adaptive and Coordinated Signal Control: Adaptive signal control refers to technologies that capture current traffic demand data using sensors such as induction loops, and adjust traffic signal timing to optimize traffic flow accordingly. Coordinated traffic signal systems attempt to further improve efficiency by creating a green wave along multiple intersections (e.g., a long string of green lights) (e.g., progression) for drivers. The objective of adaptive and coordinated signal control is to provide effective signal timing settings within a range of operating conditions. It works by collecting current demand information from sensors (e.g., advance detection), evaluating performance using system specific algorithms at a central controller, and then implementing modifications based on the outcome of that evaluation via a communication network.

Transit Signal Priority and Emergency Vehicle Priority: Transit signal priority (TSP) is a set of operational improvements that modifies signal timing to favor transit vehicles (e.g., busses). TSP reduces dwell time for transit vehicles by holding green lights longer or shortening red lights. TSP systems require four components: a detection system aboard the transit vehicle; a priority request generator which can be aboard the vehicle or at a centralized management location; a strategy for prioritizing requests; and an overall TSP management system. Emergency Vehicle Priority (EVP, also known as signal preemption) is a similar application designed for special events such as a responding fire engine or police car. EVP and TSP applications can be built on a similar infrastructure, with the major difference being that signal preemption interrupts the normal signal operation rather than adjusting current signal timing.

Eco-Signal: The basic premise of the Eco-Signal concept is that if a driver has accurate information about the upcoming signal status, the vehicle speed can be adjusted accordingly to avoid stops and vehicle operation associated with increased fuel consumption (e.g., hard acceleration maneuvers). Eco-Signal application requires Signal Phase & Timing (SPaT) information from traffic controllers, which is a standard function of connected vehicle-ready traffic controllers (SAE J2735 standards). Several companies are working on commercializing such applications. They solicit traffic signal timing information from local agencies and offer a share of their revenue.

V2V/V2I Communication: V2V and V2I communication are the enabling technologies of Intelligent Transportation Systems. Vehicle to vehicle (V2V) communication is the ability to wirelessly exchange information such as speed and position between vehicles. This allows vehicles to broadcast and receive directional messages creating a net of "awareness" of other vehicles in proximity. Vehicle to infrastructure (V2I) communication is the ability to wirelessly exchange information with a structure such as a traffic signal. This can be used to gather information on traffic and road conditions. There are two mainstream technologies used in V2V/V2I communication: 1) cellular networks, such as 5G and 4G LTE, and 2) Dedicated Short Range Communication (DSRC). Cellular networks relies on cellular infrastructure along the road, while DSRC only connects vehicles in their vicinities and works in an ad-hoc manner.

Bluetooth/Wi-Fi Traffic Probe: As mentioned in Section 2.1, a basic Wi-Fi/Bluetooth sensor system for traffic monitoring consists of a Wi-Fi/Bluetooth probe device that scans for other Wi-Fi/Bluetooth-enabled devices in its radio proximity (usually within 90 feet), and then stores the data for future analysis and use. These applications may include measurements of traffic presence, density, and flow, as well as longitudinal and comparative traffic analysis.

Third Party Traffic Data: The rise of smartphone and in-vehicle apps allow large-scale vehicle probe data to be collected in real-time. Third party traffic data collected by companies such as Waze and INRIX can be used to improve traffic management.

Public agencies traditionally use third party data in an aggregated fashion such as origin-destination analysis, operation monitoring, and performance measurement. In recent years, there is a growing interest to integrate third party traffic information into Advanced Traffic Management Systems (ATMS) for real-time signal timing adjustments.

3. Critical issues related to the cybersecurity of intersection management

As the components and technologies of intersection management have evolved to address the needs of a growing municipalities and transportation systems, new problems have been created. By having various elements of ITS connected via wireless and wired networks, threats of a cybersecurity nature are now a higher risk. This section will discuss the critical cybersecurity issues related to intersection management, and provides an overview of the current regulatory framework in California, USA.

Transportation systems include many modes: air, ships, and a variety of ground modes. In addition to roads, ground modes include trains, inland waterways, subways, bike ways, pedestrian travel, etc. Here we only focus on intersection management and upcoming Connected Automated Vehicles (CAV) issues. However, it should be noted that many reports focus on "critical" transportation systems. Such systems are generally thought to be air and train systems; while intersection management and TMS generally are considered significant, they are not as critical in terms of the immediate, catastrophic consequences of cyber vulnerabilities. However, the field of TMS has become aware of: (1) the issues of cybersecurity related to intersection management, (2) the fact that vulnerabilities are extensive, (3) the increasing importance of cyber issues because of CAV and public information/service expectations, (4) the perception that public sector traffic experts do not have consistently adequate training and staff to deal with cyber issues, and (5) the fact that industry vendors have not been reliable partners in cybersecurity.

3.1 The magnitude

From an historical perspective, the number of reported attacks and incidents is still very small and non-catastrophic, despite the series of Hollywood movie portrayals of hijacked intersection management systems to the contrary. However, in 2014, cybersecurity expert Cesar Cerrudo presented the results of extensive white-hat hacking of Sensys intersection management systems at the DefCon 22 conference. An extensive YouTube video of that presentation has been watched over 15,000 times. He not only showed how the system he hacked was vulnerable to manipulation, ransom, and potential denial-of-service, but also showed that even the simplest security measures had not been taken in the primary field test site (Washington, DC) [29], and that the vendor was misleading about the level of security provided, and initially unresponsive about cybersecurity issues as not "their" problem. Cerrudo also pointed out that most deficient sensor systems could not be retrofitted, and would need to be completely replaced when more rigorous cybersecurity standards were implemented. He estimated the then-current replacement cost of the legacy sensors at $100,000,000. Cerrudo's presentation was highly reported on and put the industry on notice. It is hoped that improvements will be made by vendors to provide better cyber safeguards (such as simple encryption), and greater transparency [30]. While improvements in the industry are likely, the private sector also must improve. One cybersecurity expert reported that of the 250 traffic control systems he was able to discover on the internet, 49 had open devices because the username and password were disabled [31].

These are not one-off anomalies. There are numerous challenges to intersection management. While the following list is not comprehensive, it will sketch out the magnitude of the problem.

- The various devices used in intersection management frequently have low levels of cybersecurity built into them, and some legacy devices are essentially devoid of security.

- The industry has been slow to respond and be proactive in providing security controls that anticipate the next phase of black-hat hacking.

- Cyber threats to TMS systems are not only introduced by way of individual devices, but also through the amalgamations of various devices and systems that provide nexus-point vulnerabilities.

- Federal guidance on cybersecurity has tended to be generic to date. Cybersecurity testing results of devices in the form of qualified traffic control equipment lists normally comes from state agencies. It is unclear how in-depth their testing is, especially related to program error detection that can lead to vulnerabilities. Qualified product lists, generally adopted by local governments from the state level, do not provide any information or guidance other than statements that they have been found to be acceptable on a variety of engineering factors, of which cybersecurity is only one.

- The public sector agencies who use intersection management the most are the smallest and most financially stretched. Municipalities have an enormous array of cyber threats and vulnerabilities, many of which they perceive as far more critical than traffic control systems.

- With a skills gap now estimated at 300,000 in the US [32, 33], smaller agencies (counties and municipalities) often cannot compete for top-notch cybersecurity experts because of an extremely tight market.

- Building cybersecurity awareness via training and quality control programs among TMS personnel is an aspect of the larger local government problem.

3.2 Assessing the risk: foreseeable attack scenarios

We conducted a literature review on cybersecurity vulnerabilities of traffic signal systems in recent years, and a high-level of summary is presented in **Table 1**. We then considered various types of attacks that could exploit those vulnerabilities and the consequences that could result. What follows is a description of several foreseeable attack scenarios and the damage that could be done.

a. Controller attacks represent attacks that target at the light controller. An attacker may attempt to gain privileged access to the controllers. On a successful intrusion, lights could be changed to be green along the route the attacker is driving. An attacker may also initiate various denial of service (DoS) attacks on the traffic light system, causing the intersection to enter an undesired and potentially dangerous state. Alternatively, an attacker could trigger the MMU to take over, which will cause the lights to enter a safe but suboptimal state (e.g., flashing

Classification	Attack techniques	Consequences/use cases
Cyberattack on traffic controller [34, 35]	password cracking, social engineering to acquire device	control traffic signal, send commands to the controller
Cyberattack by sniffing [29, 30]	sniffing sensor identification information, commands, etc.	send falsifying commands and data, manipulation of devices
Cyberattack on traffic sensor [35, 36]	wireless sensors spoofing	destabilize the traffic network
Physical attack on traffic controller [35]	Sabotaging physical networking components	affect performance, availability of devices or services
Cyberattack on traffic controller [37]	denial-of-service attack	take down the network to which the traffic signal is connected
Cyberattack on traffic sensor [38]	data spoofing, masquerade as connected vehicles to send data	influence the signal control algorithms by sending invalid data

Table 1.
Cybersecurity vulnerabilities in traffic signal systems.

all-red). Since MMU can only be reset with physical access to the controller while an attack can be triggered remotely, an adversary can disable traffic signals faster than technicians can be sent to repair them.

b. Sensor data attacks are assaults on the sensor data being communicated to the controller. A malicious party can send bogus packets to the access point, thus leading the traffic controller to operate with misinformed traffic information. For example, in a spoofing attack, an attacker can trick the loop detector by pretending to be multiple vehicles going through a road segment. Additionally, sensors used in traffic signal systems may be susceptible to firmware modification; an attacker can modify the firmware with corrupted data which will cause the sensor to no longer function (also known as "bricking" a device).

c. Physical attacks that directly tamper with the hardware such as vandalism and graffiti are common problems with public infrastructure, and traffic signal systems are designed with resiliency to handle such physical system issues. However, coordinated attacks performed through a combination of cyber and physical attacks present a significant threat to the systems. For instance, if the MMU (a hardware fail-safe device) is damaged or removed, a coordinated cyberattack can trigger dangerous light timing patterns, leading to potential massive damage and/or traffic disruption.

3.3 Efforts to address the issues

While the challenges are numerous, there have been two ongoing efforts to address the TMS cybersecurity weaknesses are worthy of mention. A state-funded initiative in Florida at the National Center for Transit Research is called Enhancing Cybersecurity in Public Transportation [14]. That initiative is to: identify and mitigate transit cybersecurity liabilities, and facilitate ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers. A second ongoing effort is being spearheaded by the Southwest Research Institute, funded by the National Cooperative Highway Research Program for approximately $750,000 [39] and due to be completed 8/15/2019. The description of the project is to develop guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (including traffic signal systems, intelligent transportation systems, vehicle-to-infrastructure systems (V2I), and closed-circuit television systems) and, secondarily, on informing the agency's response to an attack. The guidance will address the vulnerability of field devices (e.g., traffic signal controllers and cabinets, dynamic message signs, V2I roadside units, weigh-in-motion systems, road-weather information systems, remote processing and sensing units, and other IP-addressable devices), field communications networks, and field-to-center communications. It will not address vulnerabilities within a traffic management center, within center-to-center communications, or due to insider risk (accidental or intentional).

It is anticipated that the guidance will take the form of a web-based deliverable that uses a guided risk-based decision tree (similar to a capability maturity model) to identify the most relevant content for a user. The users will range from small, local agencies with limited risks and limited capabilities to those with substantial traffic management systems and more resources available to protect them. If a viable approach and host for the implementation and maintenance (including updating content and addressing emerging technologies) of this type of product is not found, a traditional NCHRP document will be produced. NCHRP has begun discussions with the National Operations Center of Excellence as a possible host, but they should not be contacted by proposers regarding this effort (NCHRP 03–127). The most extensive and up-to-date listing of resources for TMS is the first draft of a Cybersecurity Literature Review and Efforts Report by Ramon and Zajac [40].

3.4 The current regulatory framework for intersection management

The dependence on and seamless integration of technology into everyday activities and operations has exposed the critical need to address cybersecurity [2]. The strategy at the national level has focused its regulatory schemes to aid cybersecurity by providing rules or guidance about security practices to be used by public agencies (based on IS0 27,001), and by providing legal standards or guidance about equipment to either/both vendors in terms of product standards, and public agencies in terms of qualified product lists (based on ISO 27002). This and more are captured in the National Institute of Standards and Technology, *"Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)"* for the federal system (2018) [41].

To improve resilience to cyber-incidents and reduce cyber threats, at the federal level, rules have focused to date on consistent use of traffic control devices via the Manual on Uniform Traffic Control Devices (MUTCD) which is a part of 23 Code of Federal Regulations, Part 655, Subpart F [42]. While MUTCD rules are national in scope, they do not regulate cybersecurity standards at this point. Unlike some other highly critical areas of transportation such as the Cyber Air Act of 2016 in which cybersecurity standards were implemented via such agencies and government corporations as the National Institute of Standards and Technology and the Radio Technical Commission for Aeronautics, *cybersecurity of intersection management is not federally regulated.*

However, the federal government has provided general guidance about cybersecurity such as the Framework for Improving Critical Infrastructure Cybersecurity (2017), as have private organizations [43]. The federal guidance includes the Roadmap to Secure Control Systems in the Transportation Sector (2012), National Security Strategy for Transportation Security (2015), and the Federal Highway Administration Cybersecurity Program Handbook (2017).

Aligning with the DOT, DHS, and TSA, the American Public Transportation Association (APTA) has broadly identified four priorities for transportation agencies to consider, and at a minimum to address, regarding an agency's information and communication technology (ICT) infrastructure [2]. The federal government is likely to issue some initial rules and guidance on connected and autonomous vehicles cybersecurity in the near future which will have an impact on TMS in the US and elsewhere.

States tend to have the best resources to provide qualified, preferred traffic control systems lists. In California (the location of the empirical in-depth study), that is the Caltrans Transportation Electrical Equipment Specification (TEES) report, last re-issued in 2009 [44], but with supplements (called Errata) in 2010, 2014, and 2018. California's TEES guidance is used by many other states in the country, as well as local governments in California. Other than the brief mention of a password file (CA TEES, p. 46, 9.2.7.6.2), there had been no robust cybersecurity guidance in the 2014 revision (aka errata update). However, the recent errata report has included substantially enhanced cybersecurity specifications for equipment. The new standard promotes embedded cybersecurity systems and phase out customize-after-purchase approaches. Use of the TEES list by local government agencies is not mandated, but is frequently voluntarily adopted. The state is taking an aggressive stand on cybersecurity in general at an enterprise level with a Security Operations Center in the CA Department of Technology's Office of Information Security. While this resource will likely bolster prevention of hacking of state agencies for private information and help prevent ransomware and denial-of-service attacks, it seems unlikely to have much effect in the near future on state or local intersection management issues. It should be noted that while most qualified equipment lists do not have an official regulatory status because they are dynamic, in practice they function like regulatory protocols at the time a contract is let.

Although city and county CIOs listed cybersecurity as their primary focus in 2017 [45], local governments do not seem to understand the scope of their problems, let alone have much in place beyond generic cybersecurity protocols, and few are equipped to stave off threats [4, 46]. Twenty-five years ago in the southwest US, a teenage computer whiz hacked into software that controlled city traffic signals. Since then, not much has changed [47]. Recent cyber-attacks (e.g., two LA traffic engineers were found guilty of intentionally creating massive delays by adjusting signal times [48], and reports (Cesar Cerrudo demonstrated how he accessed traffic-light systems in dozens of cities, and University of Michigan students conducted experiments that manipulated over 1000 lights in one city alone) have heightened cybersecurity concerns dramatically, making them the top priority according to some public officials perception surveys [47]. Striking shortages of IT and cybersecurity personnel have been widely reported [33]. Internal practices and policies with existing personnel create tremendous gaps in local government's cyber responses [4]. Further, local governments are cash-strapped and aren't easily convinced, for example, that they must manually update every signal controller to thwart vulnerabilities at intersections [10].

4. Study of local government cybersecurity preparedness and concerns

As a result of our review of the various issues described in previous sections, we chose to conduct a study of one local government region as a test case to see if what we were discovering was as prevalent as it seemed. We conducted a Delphi-expert type of study to investigate the status of local government cybersecurity preparedness and concerns. We collected 18 questionnaires from directors of public agency transportation systems, as well as conducted six Zoom interviews spanning 14 city/county transportation agencies in Riverside and San Bernardino Counties. We also interviewed two consulting companies in the area. A typical intersection management team in the study region consists of 2 to 4 traffic engineers and technicians who manage day-to-day operations for about 100 to 400 traffic signals. Regarding the traffic controller hardware, over 90% of surveyed intersections were found to be using McCain systems. The majority of them use McCain 170 series controllers. For new deployment and upgrade projects, McCain 170 models are usually replaced by the McCain 2070 series which supports McCain and third party application software (e.g., applications mentioned in Section 2.2), and meets ATC 5.2b standards.

5. Study findings

In this study we identified 3 significant findings, they were: 1) connected devices are named the top threats, 2) cities lack cybersecurity support, and 3) cities need to plan for future technology.

Connected devices are named the top threats. Among the 1157 traffic signals surveyed in this study (refer to **Figure 2**), 67.6% of them are connected (i.e., with signal coordination, remote traffic management capabilities), and about 10% support connected vehicle applications (which comes with newer models of traffic controllers such as the McCain 2070 series).

As transportation agencies build advanced and connected traffic signal infrastructure, they are becoming more aware of the potential threats to their systems. The majority of transportation professionals in this study agree that transportation cybersecurity is a priority for their organizations. In addition, 83% of transportation professionals said that connected devices and cloud infrastructure are among the most challenging risks to defend against attacks.

To meet demands for information access, traffic management teams recognize that data must be made available in real time. Controlling access to data, and making sure it's available to those who need it, is a key concern for system managers. They also recognize that this problem will continue to grow, as most agencies plan to replace closed, proprietary systems with connected and advanced systems. Although there is no incidence of transportation related cybersecurity breaches found in this survey, cybersecurity problems are a constant concern for local governments.

Lack of cybersecurity support. Experienced security personnel can help transportation professionals navigate through security challenges, but cybersecurity is lacking. All the transportation agencies participated in this survey rely on their agency's IT department for security tasks, and many agencies work with contractors to manage their network. Most of the transportation professionals in this survey said they are not aware if their agencies follow standardized information security practices or participate in a security standards body. Two out of the 11 cities have formal written security strategies. Transportation professionals recognize the impact of the dearth of expertise: 67% said they believe a lack of trained personnel is a major obstacle to adopting advanced security processes and technology.

As cybersecurity operations capabilities become more sophisticated and specific, transportation authorities need to be able to recruit, compensate, and retain the type of high-caliber talent necessary to protect critical infrastructure.

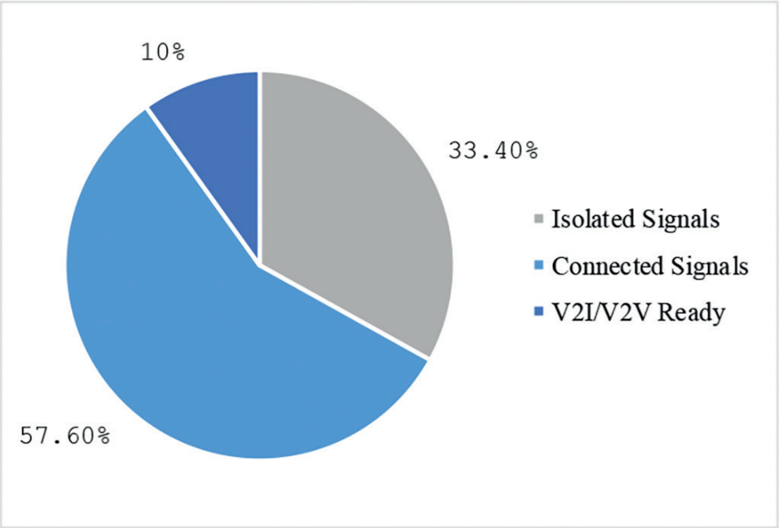

Figure 2.
Types of intersection controllers.

Need to plan for future technology. The fact that transportation, like other critical infrastructure, requires new technologies to meet the ever-increasing demand may drive decisions about developing ITS applications. An overview of technologies surveyed in this study can be found in Section 2.2. Over half the cities have plans for Intelligent Transportation Systems or Traffic Signal Management. However, nearly 80% of the agencies said that they are underfunded for their transportation needs (**Figure 3**). At the city level, ATMS/Central system, Advance Detection, and Wireless

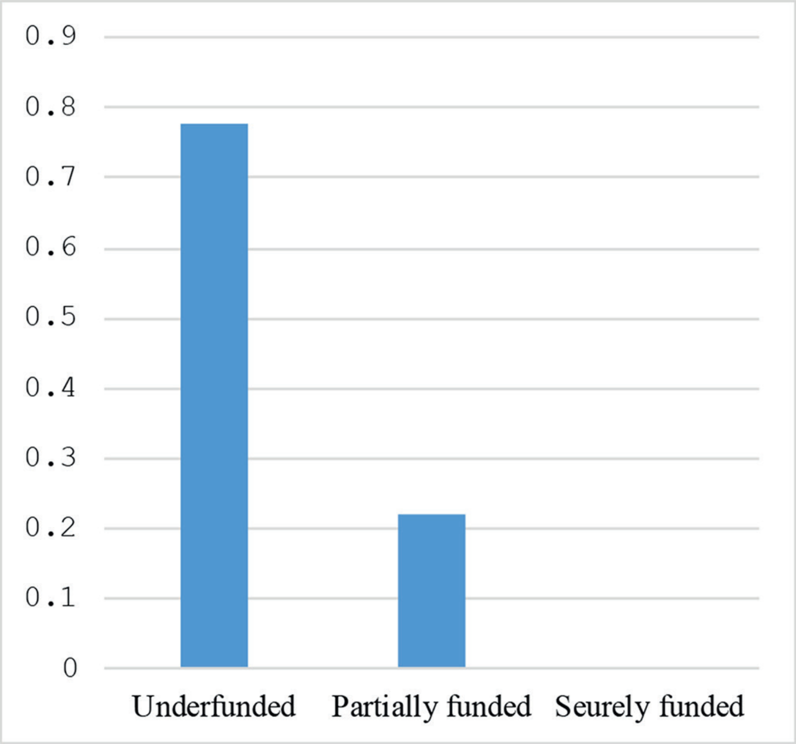

Figure 3.
Cities' funding status on transportation technology.

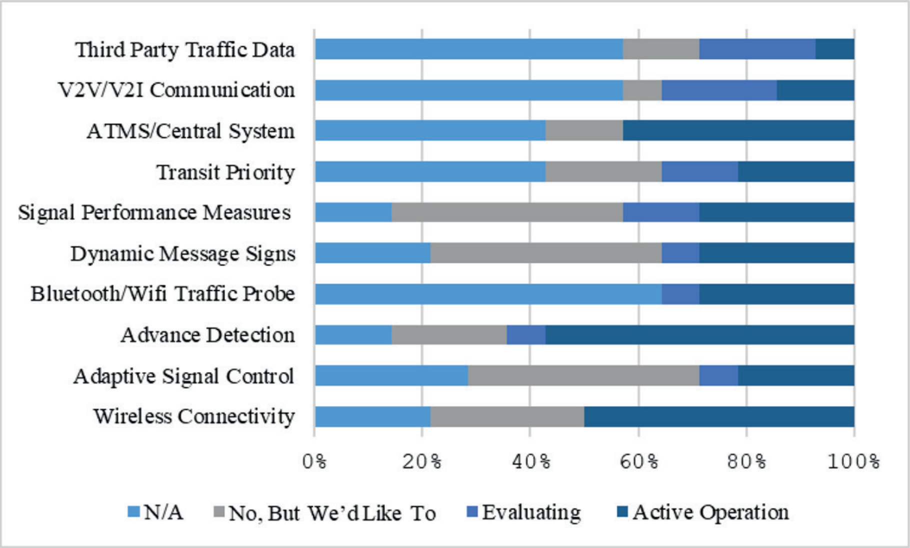

Figure 4.
Cities' plan for ITS applications.

Connectivity are listed as the top applications in active operation. As for future deployment, Signal Performance Measures, Dynamic Message Signs, and Adaptive Signal Control were noted as the technologies that cities would like to implement (refer to **Figure 4**). In order to move the implementation of these technologies forward, a number of actions need to be taken.

6. Recommendations

While we have shown there to be numerous issues as it relates to cybersecurity and ITS, we provide several recommendations, each of which can go a long way toward improving the current state municipalities find themselves in.

- Cybersecurity audits and assessments

  Perhaps the most important and the most immediate recommendation that can readily be implemented is to run comprehensive security audits and assessments. No organization wants or enjoys being audited. However, without conducting a structured, methodical audit, it will be difficult, if not impossible, to know just how serious the vulnerabilities are that a municipality is under. Audits may not need to be often. Just a baseline assessment and stock taking of what and where the issues are can go a long way toward making the ITS safer.

  In the case of California and the hacking of the digital road signs, even a basic audit would have revealed the physical security and password issue that could easily been remedied. In the case of Atlanta, while they had an audit, they did not act on the findings of the audit. The reason for this, at least in part was due to funding.

  This recommendation also supports each of the three findings from our study. Conducting an audit would help municipalities identify all of the connected devices and their associated risk which would be essentail for making a case for supporting cybersecurity. The findings from an audit would be the basis for planning for what future technologies to implement.

- Funding

  Throwing money at a problem usually will not solve it. However, not having enough money will almost certainly cause problems. If the TMS is understaffed and underfunded, then it is only a matter of time before more and likely graver events such as the one in Atlanta will take place. Likewise, continuing to operate on outdated equipment that lacks security and proper support presents significant risk. The bottom line is by not providing at least adequate funding for TMS is welcoming a catastrophe in the near future.

- Increase awareness

  Knowing there is a problem is a major part of the battle. Many municipalities have many other pressing issues that require immediate attention. Limited resources and time make it unlikely that these local governments will discover on their own just how serious the problem can be. An informational website with videos, research, and presentations materials should be made available. Local governments should have short presentations made to help them become aware and provide guidance on the steps to take to remediate current vulnerabilities and what to look for when implementing new systems in the future.

- Conferences with ITS security focus

  As this paper has shown, there are so many aspects to cybersecurity and ITS that needs attention, that a conference would be a logical event address those issues. It could be a location that national experts can develop greater awareness of the vulnerabilities and threats local governments face, review ways to assess the risks they are under and give access to vendor demonstrations that can reduce exposure to threats. Provide mini-conference on transportation cybersecurity in the local regions to showcase local resources and to highlight local issues.

- More research is needed

  The limitations of this study were its small scope and the focus on mid to small size jurisdictions. Additional review of large local governments would be highly useful. Also, the study region was dominated by a single provider; other areas with other providers may have different issues. Additional research opportunities exist to look at the coordination of technology risk assessments related to ITS; at an applied level, additional efforts to disseminate the information of risk assessments seems overdue.

7. Conclusion

Cybersecurity issues are an ever-expanding part of the digital age, and intersection management is no exception. Hackers have shown themselves increasingly adept at infiltrating various systems, and intersection and sign management systems are likely to become prime targets if plans, devices, and protocols are not more highly protected. Currently, the prospects of having to retrofit some recently-acquired ITS systems are already looming because of complacent cyber concerns and insufficient design robustness.

From our regional study, we found evidence that indeed, many local governments are not prepared for cyber-attacks or have limited resources to prepare a comprehensive cybersecurity system. All too often, serious problems that exist go unnoticed, or ignored until it is too late. Let us hope that we do not wait for a catastrophic attack to occur before we do something about it.

Author details

Yunfei Hou[1]*, Kimberly Collins[2] and Montgomery Van Wart[2]

1 School of Computer Science and Engineering, California State University, San Bernardino, USA

2 Department of Public Administration, California State University, San Bernardino, USA

*Address all correspondence to: hou@csusb.edu

References

[1] Intelligent Transportation Systems Joint Program Office. ITS-JPO 2015-2019 ITS Strategic Plan, ITS Research Fact Sheets-Benefits of Intelligent Transportation Systems. ITS-JPO. Available from: www.its.gov/communications/its_factsheets.htm

[2] American Public Transportation Program. APTA SS-ECS-RP-001-14, Cybersecurity Considerations for Public Transit. 2014. Available from: www.apta.com/.../2014%20Q2%20Public%20Comment/RP_cyber_security_considera

[3] Ensey C. California Sets Cybersecurity Example for States to Follow. The Hill; 2016. Available from: www.Thehill.com'blogs/.../289099-california-sets-cybersecurity-example-for-states-to-follo...

[4] Prall D. The Weakest Link in Your Cybersecurity Chain. American City and County; 2017. Available from: https://www.americancityandcounty.com/2017/05/30/the-weakest-link-in-your-cybersecurity-chain/

[5] Fok E, Murphy R, Phomsavath K, Walker J. Taming cyber risks. Public Roads, Federal Highway Administration, FHWA-HRT-15-006. 2015;**79**(2). Available from: www.fhwa.dot.gove/publications/publicroads/15sepoct/01.cfm

[6] Nellore K, Hancke G. A Survey on urban traffic management system using wireless sensor networks. MDPI, Sensors. 2016;**16**(2):2016. Available from: www.mdpi.com/1424-8220/16/2/157

[7] Chandran D, Zhang Y, Cheng L-C. A survey on cybersecurity of traffic signal systems. In: The 30th Annual Conference of International Chinese Transportation Professionals Association; May 19-21, 2017; Houston, TX, USA. 2017. Available from: www.uh.edu/technology/people/directory/_cv/zhang-yunpeng.pdf

[8] Gheyas I, Abdallah A. Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. Big Data Analytics. 2016;**30**:2016

[9] Hill J. FBI: More Cyber Attacks Now Originate from Legitimate Credentials. Via Satellite; 2017. Available from: www.satellitetoday.com/telecom/2017/11/08/fbi-cyber

[10] Pagliery J. Traffic Lights are Dangerously Easy to Hack. CNN Tech, The Cybercrime Economy; 2014. Available from: www.money.cnn.com/2014/21/technology/secuurity/traffic-lights-hack/

[11] Rouse M. Denial-of-Service Attack. SearchSecurity.com; 2016. Available from: www.searchsecurity.techtarget.com/contributor/Margaret-Rouse/2016

[12] Schlack B. Cybersecurity issues in signal systems. In: Washtenaw County Road Commission Annual Meeting Presentation. 2015. Available from: www.itscalifornia.org/contents/AnnualMeetings/2015/Presentations/TS7-2-WCRC-ATMSCyberSecurity.pdf

[13] Rockwell M. Traffic Cybersecurity Gets a Red Light. FCW, The Business of Federal Technology; 2014. Available from: www.fcw.com/articles/2014/08/28/traffic-lights-cyber-risks.aspx

[14] Barbeau S, Ligatti J. Enhancing Cybersecurity in Public Transportation. National Center for Transit Research, Ongoing; 2017. Available from: www.nctr.usf.edu/research/projectscopes

[15] Giandomenico N. What is spear-phishing? Defining and differentiating spear-phishing from phishing. Digital Guardian. 2016;**27**:2016. Available from: www.digitalguardian.dom/blog/wht-is-spear-phishing-defining

[16] UMBC, University of Maryland, Baltimore County. Cybersecurity 2016 Survey. 2016. Available from: https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf

[17] Blinder A, Perlroth N. A Cyberattack Hobbles Atlanta, and Security Experts Shudder. The New York Times; 2018. Available from: https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html

[18] Kearney L. With Paper and Phones, Atlanta Struggles to Recover from Cyber Attack. Reuters; 2018. Available from: https://www.reuters.com/article/us-usa-cyber-atlanta/with-paper-and-phones-atlanta-struggles-to-recover-from-cyber-attack-idUSKBN1H70R0

[19] Boyd C. Sam Sam Ransomware: What You Need to Know. Malwarebytes Labs; 2018. Available from: https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/

[20] Hay Lily N. The Ransomware That Hobbled Atlanta Will Strike Again. Wired; 2018. p. 2018. Available from: https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/

[21] City Auditor's Office City of Atlanta. Compliance Audit: ISO/IEC 27001 ISMS Precertification Audit. 2018. Available from: http://www.atlaudit.org/uploads/3/9/5/8/39584481/2017_iso-iec_27001_isms_precertification_audit_-_january_2018.pdf

[22] Hatmaker T. The Damage from Atlanta's huge Cyberattack is Even Worse than the City First Thought. TechCruch; 2018. Available from: https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/

[23] Deere S. Atlanta's network almost recovered from cyber attack, cost still unknown. The Atlanta Journal-Constitution. 2018. Available from: https://www.ajc.com/news/local/atlanta-network-almost-recovered-from-cyber-attack-cost-still-unkown/k6srGim85Q8dKwUFPbcDhN/?icmp=np_inform_variation-test

[24] Freed B. Atlanta Ransomware Attack was Worse than Originally Thought. StateScoop. 2018. Available from: https://statescoop.com/atlanta-ransomware-attack-was-worse-than-originally-thought

[25] McMillian R. Corona Caltrans Sign Displays 'Vote Donald Trump' Message. ABC 7; 2015. p. 2015. Available from: http://abc7.com/news/corona-caltrans-sign-hacked-with-pro-trump-message/1137513/

[26] Graham J. Cyberattack Cost OCTA $660,000 to Fix, Held Servers for Ransom. Orange County Register. 2016. Available from: https://www.ocregister.com/2016/08/05/cyberattack-cost-octa-660000-to-fix-held-servers-for-ransom/

[27] Jessica K. OCTA Takes Steps to Avoid Repeat of Cyber Attack. Orange County Register; 2017. Available from: https://www.ocregister.com/2017/01/24/octa-takes-steps-to-avoid-repeat-of-cyber-attack/

[28] Li Z, Jin D, Hannon C, Shahidehpour M, Wang J. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. IET Cyber-Physical Systems: Theory & Applications. 2016;**1**(1):60-69

[29] Cerrudo C. Hacking Washington DC Traffic Control Systems. IOActive Blog; 2014. Available from: www.ioactive.com/2014/07/hacking-washington-dc-traffic-control.html

[30] Cerrudo C. An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. IOActive White Paper; 2015. Available from: www.ioactive.com/pdfs/IOActive-HackingCitiesPaper_CesarCerrudopdf

[31] Wolski C. Lost Control of Traffic Control Systems. 360 Degree Cyber Security; 2018. Available from: www.360cybersec.com/category/cyber360-blog/

[32] Hughes C. 3 Tips to Reduce Cybersecurity Gaps. CSO, Cybersecurity Insights; 2017. Available from: www.csoonline.com/Databreach

[33] Moskites T. The Most Critical Gap in Cybersecurity Today: Talent. CSO; 2016. Available from: www.csoonline.com/Technology

[34] Ghena B, Beyer W, Hillaker A, Pevarnek J, Halderman JA. Green lights forever: Analyzing the security of traffic infrastructure. WOOT. 2014;**14**:7-7

[35] Li Z, Shahidehpour M. Deployment of cybersecurity for managing traffic efficiency and safety in smart cities. The Electricity Journal. 2017;**30**(4):52-61

[36] Ghafouri A, Abbas W, Vorobeychik Y, Koutsoukos X. Vulnerability of fixed-time control of signalized intersections to cyber-tampering. In: Resilience Week (RWS). IEEE; 2016. pp. 130-135

[37] Ivanova Y. Modelling the impact of cyber attacks on the traffic control centre of an urban automobile transport system by means of enhanced cybersecurity. In: MATEC Web of Conferences. Vol. 133. EDP Sciences; 2017. p. 07001

[38] Chen QA, Yin Y, Feng Y, Mao ZM, Liu HX. Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. Network and Distributed Systems Security (NDSS) Symposium; San Diego, CA, USA. 2017

[39] Zajac D. Principal Investigator on NCHRP 03-127. Cybersecurity of Traffic Management Systems, Project Effective Date; 2017. Available from: www.systemoperations.transportation.org/wp-content/upload/

[40] Ramon M, Zajac D. Cybersecurity Literature Review and Efforts Report, NCHRP Project 03-127. San Antonio, TX: Cybersecurity of Traffic Management Systems, Southwest Research Institute; 2018. Available from: www.onlinepubs.trb.org/…/NCHR03-127_Cybersecurity_Literature_Review.pdf

[41] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. 2018. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[42] US Department of Transportation. Federal Highway Administration, Manual on Uniform Traffic Control Devices, 2009 MUTCD with Revisions 1 and 2. 2012. Available from: www.mutcd.fhwa.dot.gov/kno_2009r1r2.htm

[43] Baldrige Cybersecurity Excellence Builder. Key Questions for Improving Your Organization's Cybersecurity Performance. 2016. Available from: www.nist.gov/…/baldrige-cybersecurity-initiative

[44] California Department of Transportation. TEES Report. 2010. Available from: www.dotca.gov/trafficcops/tech/tees

[45] Shueh J. Cybersecurity Reigns as Top Priority for City and County CIOs in 2017. Statescoop; 2017. Available from: www.Statescoop.com/cybersecurity-reigns-as-top-priority-for-city-and

[46] Palmer D. Ransomware: An Executive Guide to One of the Biggest Menaces on the Web. ZDNet; 2017. Available from: https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/

[47] Bigelow P. Traffic lights could be next big cyber attack threat [w/ videos]. Autoblog. 2014;**26**. Available from: www.autoblog.com/2014/11/26/traffic-lights-could-be-next

[48] Reilly J, Martin S, Payer M, Bayen A. On cybersecurity of freeway control systems: Analysis of coordinated ramp metering attacks. In: Transportation Research Board 94th Annual Meeting; Washington, DC. 2015. Available from: www.trid.trb.org/view.aspx?id=1339121