Implications of Traffic Signal Security on Potential Deliberate Traffic Disruptions

Kenneth A. Perrine
(CORRESPONDING AUTHOR)
Research Associate
Network Modeling Center, Center for Transportation Research, Cockrell School of Engineering
University of Texas at Austin
1616 Guadalupe St.
Austin, TX 78701
Phone: 512-232-3123, Fax: 512-232-3070
E-Mail: kperrine@utexas.edu

Michael W. Levin
Graduate Research Assistant
Department of Civil, Architectural and Environmental Engineering
The University of Texas at Austin
301 E. Dean Keeton St. Stop C1761
Austin, TX 78712-1172
Phone: 512-471-3548, FAX: 512-475-8744
E-Mail: michaellevin@mail.utexas.edu

Melissa Duell
Research Associate
School of Civil and Environmental Engineering
University of New South Wales
Sydney, NSW, 2052, Australia
E-Mail: melissaduell@gmail.com

Stephen D. Boyles
Assistant Professor
Department of Civil, Architectural and Environmental Engineering
The University of Texas at Austin
301 E. Dean Keeton St. Stop C1761
Austin, TX 78712-1172
Phone: 512-471-3548, FAX: 512-475-8744
E-Mail: sboyles@mail.utexas.edu

Word count: Text: 5993; Figures: 6 x 250 = 1500; Total: 7493

Submission date: 30 July 2015

ABSTRACT

Traffic control systems, including signal controllers, sensors, and centralized coordination software, all have the capacity to be vulnerable to malicious attacks. Although several studies on outages and attacks have been conducted in the literature, the effects of attacks on signals have not been specifically studied. There is a need for risk assessments to be conducted within traffic operations agencies. A key factor in assessing risk is in gaining an idea of the hypothetical impact of an outage. In this study, a dynamic traffic assignment network is used to model a central business district, where traffic signal-controlled intersections are selectively disabled (effectively replaced with four-way stops). In one scenario, total delay is multiplied fivefold when a quarter of signals are randomly chosen and disabled. In scenarios where the attacker prioritizes the selection of signals according to intersection traffic volume, significantly fewer signals are needed to exert the same impact. To complement work conducted by agencies in drafting cybersecurity policies, recommendations are made for a suite of practical analysis tools that traffic operations and computer networking engineers can use to quickly check for the worst vulnerabilities.

INTRODUCTION

As traffic signal control technologies are improved and field equipment is updated, overall infrastructure connectivity increases. States and municipalities continue to install and maintain regional wired and wireless networks to enhance traffic management. One consequence of enhanced connectivity is increased risk of malicious attacks. Known breaches in industrial control systems has risen as these systems have become more technologically developed (***1***).

Traffic systems, including signal controllers, sensors, centralized coordination software, variable message signs, and networking devices all have the capacity to be vulnerable to attacks because of misconfigurations, lack of security features, and system failures. Attacks on signal operation (***2***), sensors (***3***), and variable message signs (***4***) have already happened, and many other potential vulnerabilities such as signal controller system access due to default passwords (***5***), susceptibilities to denial of service attacks (***6***), computer virus infestations (***1***), etc. exist.

Study of traffic systems vulnerability falls within a broader field of network vulnerability that includes other infrastructure areas as power distribution, water supply, etc. Traffic systems are unique in that performance largely depends upon individual people that directly affect the system operation (***7***). Each analyzed type of disruption and mode of transport further carries its own unique challenges and implications (***8***). One of the most important analyses is in the route choice behavior of travelers in the face of disruptions (***9***). Previous literature on network vulnerability has focused on link- or road-specific impacts. Because traffic signals have been assumed to be secure, the effects of a malicious attack on signals have not yet been studied.

Because the notion of ultimate, total security comes at a conceptually prohibitive cost (***1***), the response within a traffic management organization in addressing known and unknown vulnerabilities is often limited. In facilitating better cybersecurity, the organization must assess the risks of threats, prioritize known vulnerabilities, and choose how much to invest given limited resources (***6***). A useful practice in assessing risk is to estimate the severity of consequences that result from probable attacks.

The contributions of this paper are as follows: first, we review demonstrated and potential cybersecurity vulnerabilities that affect or could affect traffic signal controllers. Next, we present a methodology for estimating the impact of traffic signal controller outages within a city, under the assumption that travelers continue to attempt to carry out daily activities while disruptions are underway. We test this methodology on the downtown Austin city network on several likely hypothetical scenarios. Finally, in light of the significant results motivating improved security, we propose future development of reporting tools for rating signal security and predicting the likelihood of a successful attack.

Potential Vulnerabilities

A variety of potential vulnerabilities in traffic signal control equipment exist, each exploitable through malicious intents and hacking techniques. For example, one of the most common and low-level vulnerabilities is the presence of default usernames and passwords on standards-abiding traffic signal controllers. A possible hacking technique is to gain physical access to the regional wired, optical, or radio frequency (RF) computer network, methodically log into a series of controllers, and clear out each controller's firmware. This renders every hacked controller inoperable until each can be physically restored by trained field technicians. Even though the conflict monitors at each affected intersection would put the signal into flashing red operation (and possibly yellow depending on conflict monitor configuration) and maintain minimally safe traffic operations, the widespread impacts of this flashing operation may be severe, as shown in this paper.

A similarly possible attack could involve keeping traffic controllers operational, but forcing a green movement for an infinite amount of time (***2***). In this case, traffic safety is worse because of the possibility of drivers disregarding red indications after waiting for a long time, and dangerously entering conflicting traffic. In this scenario, after a certain amount of response time, city officials may choose to deploy police traffic directors and physically revert to flashing red operation to address the infinite red/green light problem.

When considering these examples, many traffic operations personnel are confident about the physical barriers imposed by traffic signal control cabinets thwarting such threats. Apart from this physical defense, few other barriers stand in the way of hackers. Importantly, manufacturers of signal control equipment often justify the presence of vulnerabilities by stating that customers and standards desire such vulnerabilities because of ease of use or other reasons (***10***). Such manufactures may openly leave the responsibility of implementing cybersecurity to the end user (***11***). Even so, many jurisdictions historically do not dedicate attention to building up additional defenses (***12***).

Although there is some awareness of threat possibilities, the seriousness and relevance of the threats are often underestimated by untrained personnel (***13***). As a result, organizations often set up security schemes to address a set of bare minimum requirements, potentially leaving open many other security holes (***14***). As Hu (***6***) argues, “ignorance is a self-reinforcing problem since organizations are reluctant to act on security concerns unless a real problem has been proven.” Likewise, proper attention and funding for improved cybersecurity may not be present until a major “security catastrophe” happens (***14***).

Another source of vulnerability lies within the processes of businesses that create traffic control products (***11***). It has been observed that rushed project schedules are a severe reality for companies that must expedite new products to market in order to gain a competitive advantage. This is often paired with a “fix-it later mentality” when concerning cybersecurity, where “later” may in fact mean “never”.

In the examples given above, physical access to the regional computer network can be gained by breaking into a traffic signal control cabinet, splicing into an active network from within a manhole or up on a power pole, or using RF transmitters on vulnerable wireless networks (***10***). Signal controllers may have already experienced an attack by insiders with privileged access as in the 2007 Los Angeles incident (***15***). Two disgruntled city employees disabled signals at four busy intersections for several days. However, attention should also be given to threats originating outside of an organization, as most attacks on industrial control systems within the new millennium have historically come from outsiders (***1***).

The question of how much damage one attacker can inflict may be affected by how much knowledge the attacker has on the inner workings of a system. Although it is possible for security practices to involve the protection of sensitive information, experience from industrial control fields has shown that the effectiveness of “security through obscurity” is diminishing (***1***). Many avenues have emerged online for exploitable information to be shared. The proprietary network control protocol for a popular traffic signal controller has been successfully reverse-engineered (***16***). Vulnerabilities in variable message signs have been shared online and exploited (***4***). RF communications to wireless detectors have been compromised and documented in an online blog (***3***). Other wireless exploits have allowed for success in tampering with traffic signal operations (***2***).

When assessing security vulnerabilities and determining potential fixes, the overall system can be divided among three levels (***14***). First, *network security* includes physical barriers to hardware and software barriers such as firewalls or virtual private network (VPN) devices. Second, *operating system (OS) security* pertains to system-level access to individual controllers or central computers, including user authentication. Third, *application-level* security pertains to security features that are specific to a software solution, such as a central software application that uses domain-specific communication protocols to control and monitor traffic controller software in the field. Traditional traffic operations practices and solutions have tended to focus on a minimal degree of security at the network level, with less flexible availability of operating system security options, and even fewer security features at the application level.

Another facet of security does not involve malicious attacks, but instead relates to operator and equipment failure (***4***). Intuitively, the effects of operator error or equipment failure are minimized when adequate security features and practices are in place. An example of inadequate application-level guarding against system failure was observed in the 2009 Montgomery County, Maryland incident, where coordination among 750 signals was lost for over a day, severely impacting the commutes of thousands (***17***).

Risk Assessment

Several cybersecurity guides indicate that risk assessment is a primary goal that should be accomplished before other steps are executed, such as drafting incident response plans (***18***,***19***). A simple model of risk is (***19***):

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

In some literature, "impact" may also be described as "consequence". Often impact can be based upon an estimate of financial loss, but it can also include other things such as health effects or environmental consequences (***1***). Estimating likelihood of a successful attack is said to be far more difficult as this can be a function of perceived threat, known vulnerabilities, and target attractiveness. Little historic data is available for assisting in making reasonable estimates on these factors. Furthermore, "most organizations are highly reluctant to report security incidents as they are viewed as potential embarrassments." (***1***) Despite complications, risk assessments help in answering questions on how much risk is acceptable in a given traffic operations system. In the cybersecurity guides, this also informs how response plans are made and prioritized. For significant work to be done, estimates need not necessarily be precise, but should be reasonable.

Despite efforts in risk estimation, prioritization of response plans, etc. there is a fundamental tension between usability and security (***6***). In considering one extreme limit, "we can't afford the infinite cost of perfect security." (***1***). On the other hand, some degree of planning should happen as reinforced by the saying, "if you fail to plan, then plan to fail" (***19***). There should be a balance between the impacts of active security practices and the level of security that is perceived as needed (***14***). Security that limits legitimate access gets more attention than "security that keeps the bad guys out", since the latter can go undetected for long periods of time.

The analysis of risk is challenged by lack of good statistics on computer security crimes (***6***), and at least as limited in the transportation field. When trying to acquire managerial and political buy-in for cybersecurity, it becomes necessary to quantify estimates of hypothetical losses. In our work, the traffic models on which these estimates are made may not represent all phenomena that occur in reality. Rather, balance must be found between simplicity and accurate portrayal of the real traffic system (***6***).

In attempts to assess the risk of vulnerabilities that, say, force affected intersections into flashing red operation, much insight can be gained by creating a set of hypothetical scenarios that characterize the effects of possible attacks, as seen in this research. The measured severity of problems in each scenario can then inform the best types of mitigations. For example, scenario results can highlight the positive and negative aspects of broadly safeguarding selected traffic corridors or urban regions versus finely limiting possible damage to individual intersections. In the end, a security policy that is drafted with the help of the risk assessment defines what "cybersecurity" really means within a given system (***20***).

To the best of the authors' knowledge, no immediate examples exist in the literature that attempt to quantify the effects of signal controller failures caused by attacks for the purpose of risk assessment. However, related work had been accomplished in hypothesizing the possible outcomes of unauthorized ramp meter tampering (***21***). In simulation, scenarios are devised at the expense of many simulated travelers that recreate for one vehicle a "VIP lane" (a path of travel on an expressway that is clear of congested traffic) and also a scheme that assists a getaway vehicle in fleeing from a crime scene.

DEMONSTRATION

To motivate greater attention to signal controller security, we quantify the potential impacts of hacking signals on a dynamic traffic assignment (DTA) model of the downtown Austin city network. We first develop a model of stop sign-controlled intersections for the cell transmission model (CTM) developed by (***22***,***23***) based on a DTA model of reservation-based intersection control (***24***). We use this model to demonstrate the effects of attacks on traffic signals, turning them into stop signs. A DTA model is well-suited to the analysis in this paper, because it can simulate network-wide impacts of intersection failures with computational efficiency (***25***).

Stop Sign Model

Our DTA traffic signal model cycles through its phases, assigning saturation flows at each time step proportional to the green time from active phases. This results in capturing both average intersection flow as well as average delays due to traffic signals. The design goals for the stop sign model are similar. We develop a model that attempts to predict both the average intersection capacity as well as the minimum delays due to stopping at the intersection.

Stop signs in the field can be well modeled by adapting the reservation-based intersection control developed for autonomous vehicles by Dresner and Stone (***26***). Reservations are essentially an evolution of stop signs that use digital communications and intersection agents to remove the requirement that all vehicles stop before entering the intersection and to reduce safety margins necessary for human drivers. Reservations have previously been modeled in DTA through the conflict region model of Levin & Boyles (***24***), which was shown to be compatible with the general intersection model requirements of Tampère et al. (***27***). For the purposes of this paper, we adapt the conflict region model for stop signs by adding safety margins and stopping delay. This creates two types of additional constraints on intersection flow: 1) reduced capacity across the intersection reflecting that all vehicles start moving from a complete stop; and 2) minimum delay in the last cell of the link due to the vehicle coming to a stop before entering the intersection. We use a single conflict region for the entire intersection to model how conflicting turning movements restrict intersection access. We define a *turning movement* to be a pair of links $(i,j) \in \Gamma^{-1} \times \Gamma$, where Γ^{-1} is the set of incoming links and Γ is the set of outgoing links for the intersection.

Turning Movement Capacity

Previous work on macroscopic models of stop signs (***28***,***29***,***30***) used intersection travel time required for each turning movement to estimate capacity for each turning movement. We estimate these times by geometrically estimating the distance traveled for each turning movement, and using the driver acceleration models of Wang et al. (***31***) to determine travel time. Wang et al. developed regression models of driver acceleration in the form

$$a = \alpha + \beta v \tag{1}$$

where a is acceleration, v is speed, and α and β are constants. For vehicles going straight, $\alpha = 1.883\text{m/s}$ and $\beta = -0.021\text{m/s}$. For vehicles making turning maneuvers, $\alpha = 1.646\text{m/s}$ and $\beta = -0.017\text{m/s}$.

For estimating distance, we distinguish between three types of turning movements: straight, right turns, and left turns. We assume that U-turns are not used in this model because in our DTA model, vehicle route choice is completely determined before vehicles depart and shortest paths are acyclic. Therefore, we do not code U-turns, which simplifies the analysis. Since the study network has 464 intersections, we use an automatic procedure based on the change in direction a vehicle makes along its turning movement. Let θ_i be the direction of link i. Then the change in direction for turning movement (i,j) is $\Delta\theta_{ij} = \theta_j - \theta_i$. Without loss of generality, let $\Delta\theta_{ij} \in [0,2\pi]$. If $\Delta\theta_{ij} \leq \frac{\pi}{4}$ or $\Delta\theta_{ij} \geq \frac{7\pi}{4}$, then (i,j) is labeled as a straight. If $\frac{\pi}{4} < \Delta\theta_{ij} < \pi$, (i,j) is labeled a left turn, and if $\pi < \Delta\theta_{ij} < \frac{7\pi}{4}$, (i,j) is labeled a right turn. Link directions are primarily determined from node coordinates, which implicitly assumes that links are straight. Since right angle turns are most common, we assume that left and right turns are right angles instead of using the estimation of link direction to determine the angle.

Vehicles going straight must cross some l_{ij} lanes, resulting in a distance of ℓl_{ij}, where ℓ is the lane width. For right turns, we assume that vehicles turn from the right-most lane of i into the right-most lane of j, traversing a quarter of the circumference of a circle with radius ℓ, resulting in distance $\frac{\pi}{2}\ell$. Vehicles making a left turn traverse a quarter of the perimeter of an ellipse with axes depending on the number of lanes crossed. Let $\hat{l}_i$ and $\hat{l}_j$ be the numbers of lanes crossed, then the axes are $\hat{d}_i = \left(\hat{l}_i + \frac{1}{2}\right)\ell$ and $\hat{d}_j \left(\hat{l}_j + \frac{1}{2}\right)\ell$. We approximate the distance as $\frac{\pi}{4}\left(3(\hat{d}_i + \hat{d}_j - \sqrt{\left(3\hat{d}_i + \hat{d}_j\right)\left(\hat{d}_i + 3\hat{d}_j\right)}\right)$ (Ramanujan's approximation). Without more specific data, we assume lane widths of 12 feet, which is a typical width for arterial roads (***32***).

Integrating equation (1), and using the appropriate distance d_{ij}, we approximate the solution to the equation

$$d_{ij} = \frac{\alpha\left(e^{-\beta t_{ij}} - 1\right)}{\beta^2} - \frac{\alpha t_{ij}}{\beta} \tag{2}$$

to find the travel time t_{ij} for turning movement (i, j). The maximum number of vehicles that can travel make the turning movement (i, j) in unit time, assuming no conflicting traffic, is then the inverse of t_{ij}, the time required per vehicle.

Minimum Delay

Since all vehicles must stop at the intersection, we impose a minimum delay in the last cell of the link of $\Delta t + \frac{v_\mathrm{f}}{a_\mathrm{d}}$, where Δt is the CTM timestep, v_f is the free flow speed of the link and a_d is the braking deceleration, which we assumed to be 15 feet per second for all vehicles. This produces an additional time step spent in the last cell leading to a stop sign, and possibly more for links with a high free flow speed.

Dynamic Traffic Assignment Model

To study the possible effects of targeted attacks on a traffic signal system, we applied the DTA model described in the previous sections to the downtown Austin city network. The downtown Austin network has 546 intersections, of which 464 have traffic signals, with the remaining 92 intersections being freeway merges or diverges, shown in Figure 1. The network has 1,247 links and 62,836 trips distributed over 64 zones and nine 15-minute departure time intervals. The traffic signal timings are based upon actual configurations in the field.

Using the method of successive averages, we found dynamic user equilibrium (DUE) for the base case network. In short, DUE involves the assignment of vehicles to travel routes such that all utilized routes between each origin/destination are equal, and no faster route exists. Due to the fact that hacking signals results in temporary and unexpected intersection control behavior, we assume that drivers are not aware of which signals are operating normally when they make their route choice decisions (and therefore there is no impact on their route choice). For the experiment presented in this section, we replaced some of the traffic signal controls with stop signs to simulate flashing red signals and simulated vehicle movement along the routes used for the DUE with normal signals.

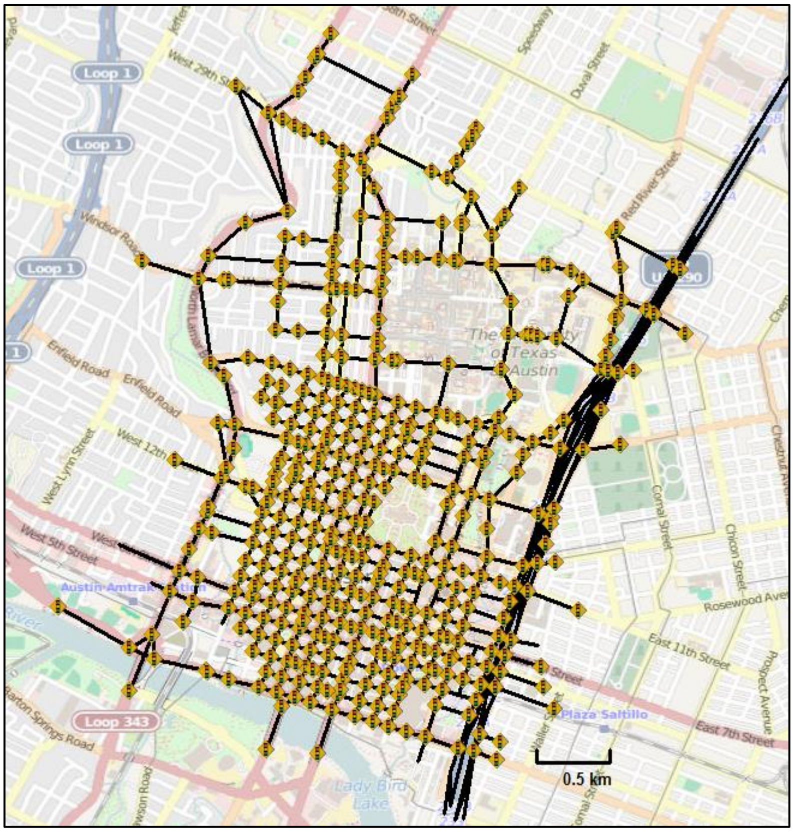

FIGURE 1 Signals in the downtown Austin network

This section presents the results for two methods of attacks on the signal system and two methods of intervention. We examine the impact of disabling varying numbers of traffic signals from a network-wide perspective using the metric of total system travel time (the sum of travel times for all vehicles modeled) and on individual vehicles. Additionally, we spatially analyze the impact on the average added delay for each travel zone.

Effects of Disabling Signals

As expected, the impact of disabling parts of the traffic signal system was significant, especially depending on the number of signals that were disabled. However, identifying which signals to target and in which order presented an additional question. In this experiment, we identified two methods for prioritizing the order in which signals were disabled. Both methods seek to impact the greatest amount of vehicles.

In the first method, the signals with the greatest amount of vehicle flow were targeted first. In the DTA model, the intersections with the greatest flow were identified based on the vehicle paths. Figure 2(a) presents the results for this method, where the horizontal axis indicates the number of signals that have been targeted, i.e., replaced with stop signs, and the vertical axis presents the total system travel time. In the base case, the total travel time of all vehicles was less than 20,000 hours, while in the worst case the network experienced gridlock, where there was no vehicle movement and the total travel time was 120,000 hours. Based on the United States Department of Transportation recommendation of around $13 per hour in traffic (***33***), the worst-case scenario could have a cost up to $1.5 million, or approximately $25 per vehicle.

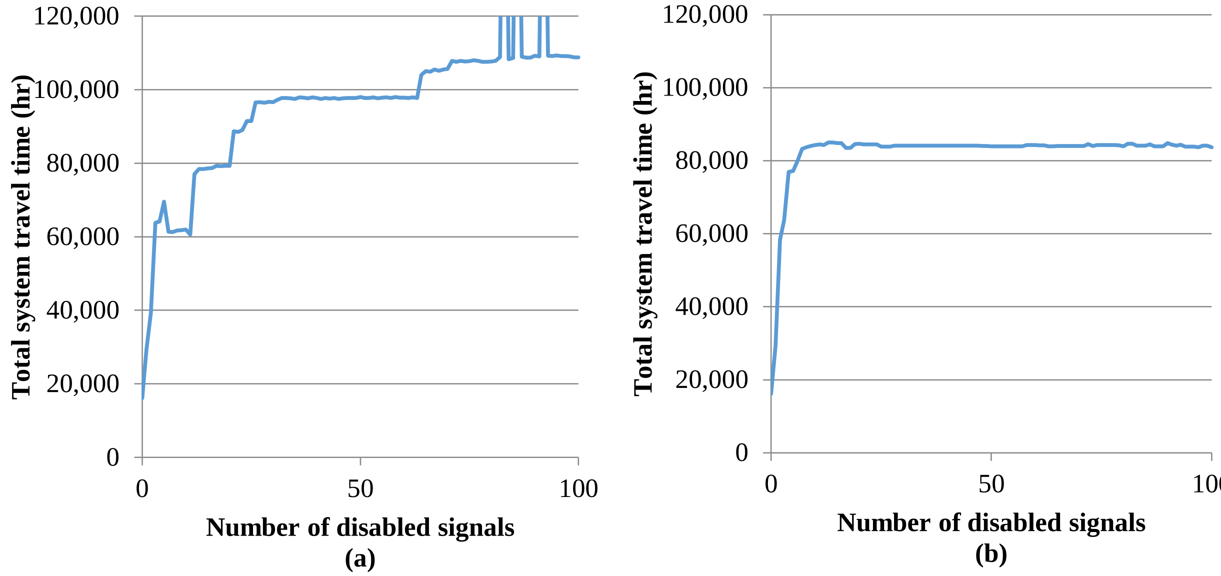

FIGURE 2 TSTT results for (a) the max-vehicle-flow targeting method, and (b) the max-affected-vehicles method

The second method for prioritizing which traffic signals to disable was based on maximizing the number of vehicles affected. This method used a greedy heuristic in which we first identified a subset of unaffected vehicles, disabled a signal at the intersection that had the greatest use from that subset of vehicles, removed those vehicles from the subset, and iterated. Figure 2(b) presents the results for the maximum number of affected vehicles method, where again the horizontal axis shows the number of disabled signals and the vertical axis shows the total system travel time in hours. While the max-affected-vehicles method resulted in a faster increase in total travel time with a fewer number of disabled signals, it would be the more difficult of the two methods for an attacker to implement.

Next, we further demonstrate the potential magnitude of the problem by examining the worst-case scenario. Figure 3 presents a spatial analysis of the average added delay (in minutes) for each origin zone. The average delay is colored in blue and scaled by size according to the legend in Figure 3. In addition, Figure 3 shows the total vehicle demand for each origin as a dot density plot centered on each zone. Each dot represents 100 vehicles, and thus, the zones with the greater number of clustered dots have a greater amount of demand and therefore a greater number of vehicles that would be affected by the added delay.

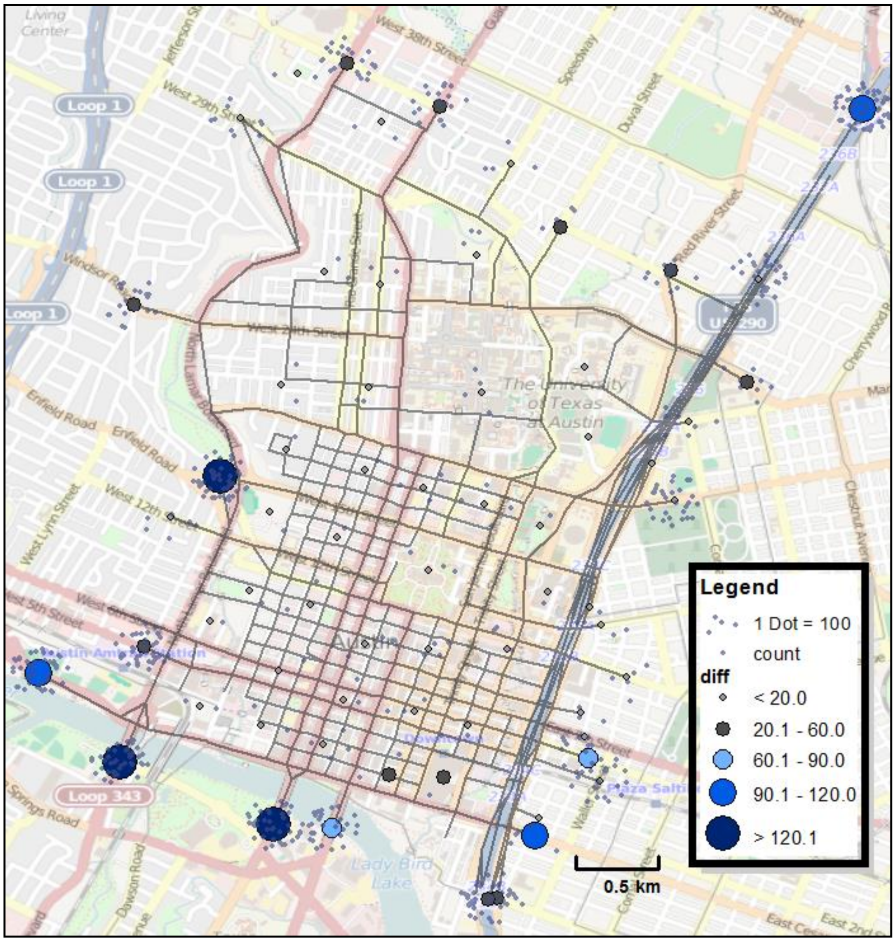

FIGURE 3 Average added delay in minutes for each origin zone

Figure 3 shows that each origin zone is not equally impacted. The origin zones in the center of the city have little to no added delay, in addition to also having less vehicle demand. The majority of the additional delay is experienced by the vehicles with an origin to the south of downtown Austin or on the west side at Enfield Road.

Figure 4 shows the same results except for each destination zone. Again, the circles represent the average added delay in minutes for each vehicle in that zone. The small red dots represent the vehicle demand centered on the destination zone, where each dot represents 100 vehicles. Unlike Figure 3, the added delay in the worst case scenario is more evenly distributed between all the destination zones and the location of the vehicle demand. While the zones in the center of the city appear to have a smaller average delay, they also have more vehicles, implying that they experience a greater proportion of the total delay.

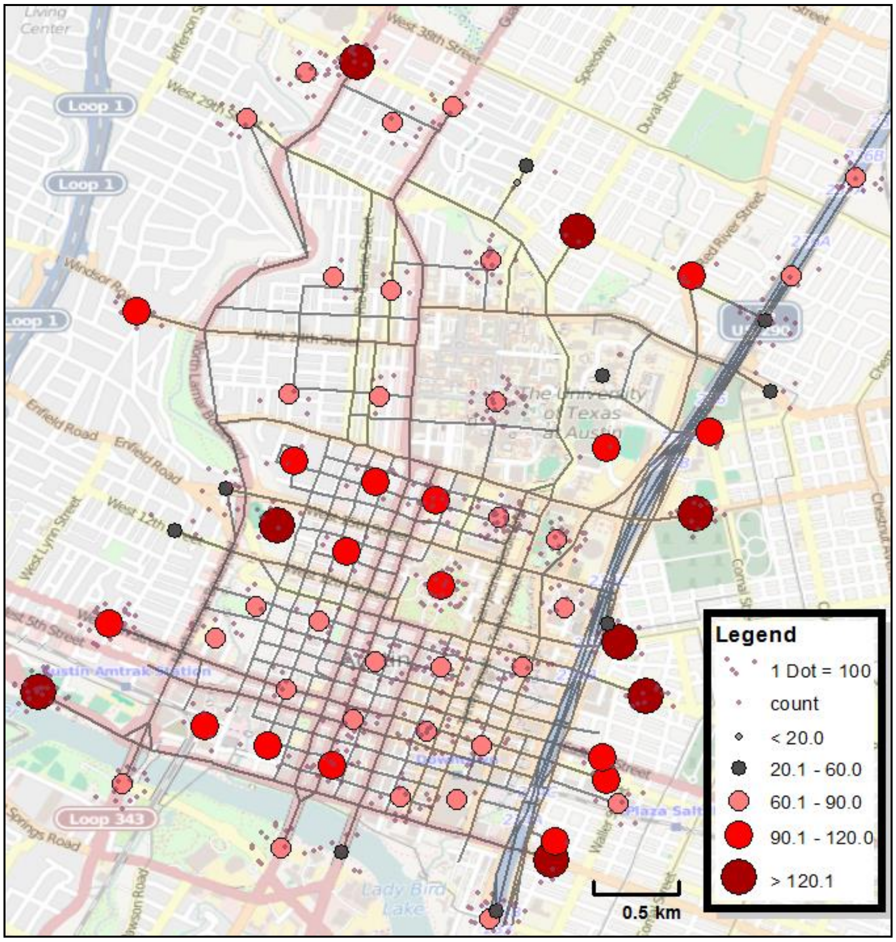

FIGURE 4 Average added delay in minutes for each destination zone

Finally, Figure 5 shows how the added delay in the worst case scenario as compared to the base case scenario (which totaled approximately 100,000 hours) is distributed among the individual vehicles. The horizontal axis shows the grouping of the minutes of added delay while the vertical axis shows the number of vehicles whose added delay was in that group. As indicated in Figures 4 and 5, vehicles were not equally impacted by the failure of the traffic signal system. In fact, over 5,000 vehicles experienced a small decrease in delay, while a majority of vehicles experienced an additional delay of between 0–50 minutes. However, an unfortunate subset of vehicles experienced an increased delay of several hours.

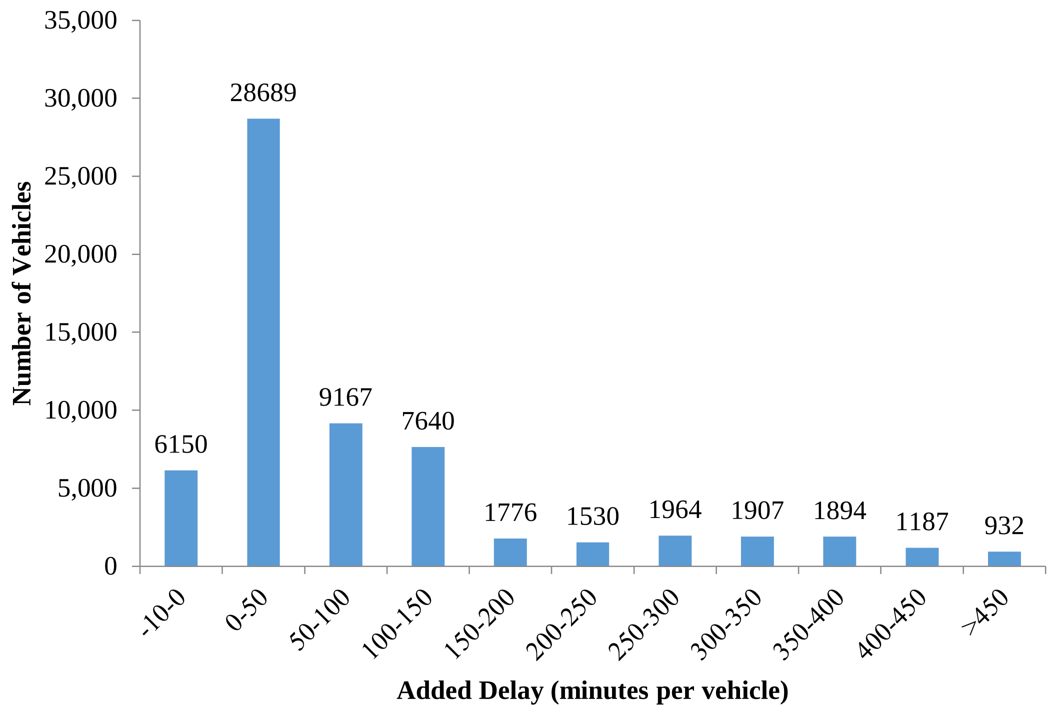

FIGURE 5 Frequency distribution of the worst case added delay in minutes for all vehicles

Effects of Limited Intervention

The previous section demonstrates the impacts in the worst case, where a significant number of traffic signals are disabled during the time of peak morning demand. However, this work also explores the scenario where some traffic signals are protected, called intervention strategies. The intervention strategy is to protect a number of signals, meaning that they cannot be disabled. Figure 6 shows the results for the intervention strategies.

In the first intervention scenario, shown in Figure 6(a), some subset of traffic signals is protected, shown on the horizontal axis, and the attacker does not know which traffic signals these are. If the attacker tries to disable a protected traffic signal, nothing happens. In the results shown in Figure 6, it is assumed that 30 traffic signals are attacked in descending order of intersection maximum traffic flow. As shown in Figure 6(a), if the attacker does not have information on the protected signals, the impacts of the attack can be partially mitigated, although there is still a significant amount of added delay. However, Figure 6(b) shows the intervention scenario in which the attacker has information on the protected signals, and therefore will try to disable only signals that are not protected. In Figure 6(b), the intervention strategy is not able to have much impact on the added delay in the network.

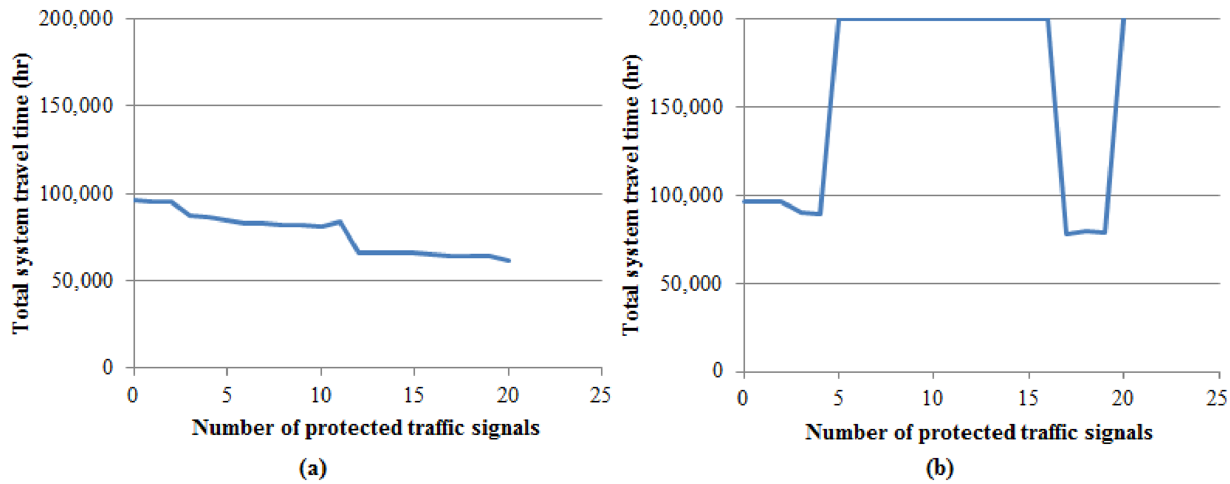

FIGURE 6 The impact of (a) intervention where attacker has no information and (b) intervention where attacker has information.

CONCLUSIONS

The overall trends depicted in methodology show increased system-wide delay as the number of disabled signals increases. In the random targeting scenario, delay is multiplied by 5 times when a quarter of signals are disabled. If attacks are prioritized according to busy intersections, significantly fewer signals are necessary to create a comparable impact. Importantly, the analysis on the effects of improving cybersecurity for a handful of intersections shows significant reduction in delay at the time of an attack but only in the case of the attacker not knowing which signals are protected. In general, improved cybersecurity leads to a reduction in damage. It follows that vulnerabilities must first be identified before security improvements can be most effectively applied.

Research projects in the field today address many of these security concerns, but they generally focus upon the documentation of policies, best practices, and the improvement of overall security awareness. One research needs statement focuses upon assessing the qualifications of agency employees for adequately addressing traffic-related security (***34***). More broadly, general computer security incident response and prevention guides have been drafted (***18***,***35***), including one that specializes in the transportation field (***19***). While these offer significant value to the domain of cybersecurity, policies and best practices are often expressed in voluminous, generalized ways that are not immediately accessible or useful to resource-limited traffic operations personnel or regional network engineers. For future research, we propose the creation of automated analysis tools that offer fast and useful risk assessments of existing systems and clearly documented solutions for the worst vulnerabilities.

One major function of security analysis is to bring about assurances that security practices already put into effect are working as intended (***20***). Automated analysis tools can provide a certain degree of assurance, as well as detection of unexpected security problems. Although automated tools cannot analyze all types of security, the primary motivation here is to alleviate the worst vulnerabilities, which may include 80% to 90% of vulnerabilities that currently exist.

Emphasis is placed upon the analysis of existing systems and assurances of intended operation. Indeed, with historic manufacture of proprietary traffic control software, the application level of security cannot be readily addressed or influenced without active intervention of the manufacturer and corresponding response time. Rather, more opportunities for improving today's existing systems lie in the areas of the network level and operating system level (***14***). For example, network level encryption can be facilitated by installing VPN hardware, and OS security can be improved by enabling better user authentication and access logging features.

To reduce costs associated with improving security of intersection controllers, more extensive game-theoretic analyses could determine the minimum number of security interventions necessary to ensure a given level of service after an attack. As mentioned previously, this will depend on the attacker's knowledge of the interventions.

We also propose for future work the creation of a ranking system that allows sets of automated analysis results to be compared with those of other jurisdictions or representative benchmarks. One example of a similar ranking system for a broader technological domain is the Common Vulnerability Scoring System (CVSS) (***36***). Likewise, detailed analysis results can be supplemented by practical documents that describe remedies, in the same spirit of brief notes provided by private industry and government (***37***,***5***,***38***). Some documents support the idea that it is generally easier for end users to "procure security features" than it is to "implement security" from scratch, where the former leverages proven solutions (***14***).

Concern has been expressed about the idea that discovered vulnerabilities and documented practices for remedies can be used by attackers for malicious purposes. Unless care is taken to protect information, there may be possible exposure of information having to do with previously unknown problems (***39***). In response to these concerns, it is observed that a significant amount of information is already publicly available. Further research should address these concerns in efforts to curtail the possible misuse of information. Nevertheless, fixing these flaws in signal controllers and other traffic control systems is a more permanent solution than relying on confidentiality of vulnerabilities.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support of the Data-Supported Transportation Operations & Planning Center.

REFERENCES

1. Byres, E., and J. Lowe. The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems. *Proceedings of the VDE Kongress*, Vol. 116, 2004.

2. Ghena, B., W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman. Green Lights Forever: Analyzing the Security of Traffic Infrastructure. In *Proceedings of the 8th USENIX Workshop on Offensive Technologies*, 2014.

3. Infosec Institute. *Hacking Traffic Light Systems*, (2014, September). http://resources.infosecinstitute.com/hacking-traffic-light-systems/. Accessed June 2015.

4. Sawin, D. *Control Systems Security Program: Transportation*, (2010, October). http://www.volpe.dot.gov/sites/volpe.dot.gov/files/docs/CSSPT_Conference_Presentation.pdf. Accessed June 2015.

5. Econolite. *Added Security for your Traffic Signal Network To Protect Your Traffic Control Devices*, (2014, September). http://www.econolite.com/files/7614/1141/6419/AN2152-

Added-Security-For-Your-Traffic-Signal-Network.pdf. Accessed June 2015.

6. Hoo, K. J. S. *How Much is Enough? A Risk Management Approach to Computer Security*. Stanford, California: Stanford University, 2000.

7. Wang, Z. et al. Recent Advances in Modeling the Vulnerability of Transportation Networks. *Journal of Infrastructure Systems*, Vol. 21, No. 2, June 2015.

8. Faturechi, R., and E. Miller-Hooks. Measuring the Performance of Transportation Infrastructure System in Disasters: A Comprehensive Review. *Journal of Infrastructure Systems*, Vol. 21, No. 1, March 2014.

9. Sullivan, J. L., L. Aultman-Hall, and D. C. Novak. A Review of Current Practice in Network Disruption Analysis and an Assessment of the Ability to Account for Isolating Links in Transportation Networks. *Transportation Letters*, Vol. 1, No. 4, pp. 271-280, October 2009.

10. Cerrudo, C. *Hacking US (and UK, Australia, France, etc.) Traffic Control Systems*, (2014, April). http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html. Accessed June 2015.

11. Bayless, S. H., S. Murphy, and A. Shaw. *Connected Vehicle Assessment: Cybersecurity and Dependable Transportation*. http://www.itsa.org/knowledgecenter/technology-assessment/cyber-security-and-dependable-transportation. Accessed June 2015.

12. Institute of Transportation Engineers. *Survey Results: Traffic Signal Systems Requirements Survey*, (2003, August). http://library.ite.org/pub/e267a385-2354-d714-517d-dc4cd091d64d. Accessed June 2015.

13. Fletcher, D. *NCHRP 20-59 (48): Effective Practices for the Protection of Transportation Infrastructure from Cyber Incidents*, (2014, January). http://trbcybersecurity.erau.edu/files/NCHRPProject.ppt. Accessed June 2015.

14. Lampson, B. W. Computer Security in the Real World. *Computer*, Vol. 37, No. 6, 2004, pp. 37-46.

15. Bernstein, S., and A. Blackstein. Key Signals Targeted, Officials Say. *Los Angeles Times*, January 9, 2007.

16. Goodspeed, T. Reversing the Econolite ASC/3 Traffic Light Controller. In *ToorCon Seattle*, 2008.

17. Halsey, A. Traffic Signals Disrupted, Creating Chaos in Montgomery. *The Washington Post*, November 5, 2009.

18. United States Department of Homeland Security. *NIPP 2013: Partnering for Critical Infrastructure Security and Resiliance*. 2013.

19. Frazier Sr, E. R., Y. Nakanishi, and M. A. Lorimer. *Surface Transportation Security, Volume 14: Security 101: A Physical Security Primer for Transportation Agencies*. Project 20-59 (28) NCHRP Report, 2009.

20. Bishop, M. What is Computer Security? *IEEE Security & Privacy*, Vol. 1, No. 1, 2003, pp. 67-69.

21. Reilly, J., S. Martin, M. Payer, and A. M. Bayen. On Cybersecurity of Freeway Control Systems: Analysis of Coordinated Ramp Metering Attacks. In *Transportation Research Boar 94th Annual Meeting*, No. 15-5248, 2015.

22. Daganzo, C. F. The Cell Transmission Model: A Dynamic Representation of Highway Traffi Consistent with the Hydrodynamic Theory. *Transportation Research Part B: Methodological* Vol. 28, No. 4, pp. 269-287, August 1994.

23. Daganzo, C. F. The Cell Transmission Model, Part II: Network Traffic. *Transportation Research Part B: Methodological*, Vol. 29, No. 2, pp. 79-93, April 1995.

24. Levin, M. W., and S. D. Boyles. Intersection Auctions and Reservation-Based Control in Dynamic Traffic Assignment. In *Transportation Research Board 94th Annual Meeting*, No. 15-2149, 2015.

25. Chiu, Y.-C. et al. Dynamic Traffic Assignment: A Primer. In *Transportation Research E-Circular (E-C153)*, 2011.

26. Dresner, K., and P. Stone. Multiagent Traffic Management: A Reservation-Based Intersectior Control Mechanism. In *Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 2*, 2004, pp. 530-537.

27. Tampère, C. M. J., R. Corthout, D. Cattrysse, and L. H. Immers. A Generic Class of First Order Node Models for Dynamic Macroscopic Simulation of Traffic Flows. *Transportation Research Part B: Methodological*, Vol. 45, No. 1, pp. 289-309, 2011.

28. Wu, N. Determination of Capacity at All-way Stop-controlled Intersections. *Transportation Research Record: Journal of the Transportation Research Board*, Vol. 1710, pp. 205-214, 2000.

29. Li, H., Z. Tian, and W. Deng. Capacity of Multilane All-Way Stop-Controlled Intersections Based on the Conflict Technique. *Transportation Research Record: Journal of the Transportation Research Board*, Vol. 2257, pp. 111-120, 2011.

30. Wu, N. Total Capacities at All-way Stop-controlled Intersections: Validation and Comparisor of Highway Capacity Manual Procedure and Addition-conflict-flow Technique. *Transportation Research Record: Journal of the Transportation Research Board*, Vol. 1802, pp. 54-61, 2002.

31. Wang, J., K. Dixon, H. Li, and J. Ogle. Normal Acceleration Behavior of Passenger Vehicles Starting from Rest at All-way Stop-controlled Intersections. *Transportation Research Record*

Journal of the Transportation Research Board, Vol. 1883, pp. 158-166, 2004.

32. Stein, W. J., and T. R. Neuman. *Mitigation Strategies for Design Exceptions*. FHWA-SA-07-011. 2007.

33. Transportation, U.S. Department of. *The Value of Travel Time Savings: Departmental Guidance for Conducting Economic Evaluations, Rev. 2 (2014 Update)*, (2014, July). http://www.transportation.gov/sites/dot.dev/files/docs/vot_guidance_092811c.pdf. Accessed July 2015.

34. Transportation Research Board. *Research Needs Statements: Data Management Competencies for Transportation Agencies*, (2014, February). http://rns.trb.org/dproject.asp?n=35479. Accessed July 2015.

35. Cichonski, P., T. Millar, T. Grance, and K. Scarfone. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61 Rev. 2. National Institute of Standards and Technology, 2012.

36. U.S. Department of Homeland Security. A Closer Look at CVSS Scoring. *ICS-CERT Monitor*, p. 2, October 2012.

37. Moxa. *Moxa Connection: Cybersecurity for Centralized Advanced Traffic Management Systems*, (2014, January). http://www.moxa.com/newsletter/connection/2014/01/feat_01.htm. Accessed June 2015.

38. USDOT/FHWA Office of Operations. *Cyber Security Advisory*, (2014, August). http://trbcybersecurity.erau.edu/files/CSAdvisory-20148-Final.pdf. Accessed June 2015.

39. Landwehr, C. E. Formal Models for Computer Security. *ACM Computing Surveys (CSUR)*, Vol. 13, No. 3, 1981, pp. 247-278.

1