Framework for Evaluating the Severity of Cybervulnerability of a Traffic Cabinet

Joseph M. Ernst and Alan J. Michaels

The increasing connectivity in transportation infrastructure is driving a need for additional security in transportation systems. For security decisions in a budget-constrained environment, the possible effect of a cyberattack must be numerically characterized. The size of an effect depends on the level of access and the vehicular demand on the intersections being controlled. This paper proposes a framework for better understanding of the levels of access and the effect that can be had in scenarios with varying demand. Simulations are performed on a simplistic corridor to provide numerical examples of the possible effects. The paper concludes that the possibility of some levels of cyberthreat may be acceptable in locations where traffic volumes would not be able to create an unmanageable queue. The more intimate levels of access can cause serious safety concerns by modifying the settings of the traffic controller in ways that encourage red-light running and accidents. The proposed framework can be used by transportation professionals and cybersecurity professionals to prioritize the actions to be taken to secure the infrastructure.

The concern about cybersecurity has become pervasive throughout every aspect of transportation engineering. This concern includes more traditional cybersecurity needs like protecting the computer network of a traffic management center (*1*) and the connected infrastructure like highway metering devices (*2*). Future-looking studies have simulated the effects of an attack on a connected vehicle network (*3*) or investigated the cybervulnerability of an autonomous vehicle (*4*). To make informed decisions about the necessary security measures in a cost-constrained environment, the consequence of a vulnerability must be understood in a measurable way.

As transportation devices become more connected, they become more vulnerable. One early example of this phenomenon was hackers changing dynamic message signs (*5*). Even though connected vehicles will bring new security challenges, vehicles on the road today are already connected enough for their safety-critical systems to be vulnerable, even if they are not autonomous (*6*).

While the effect of riding in a hacked vehicle is apparent, the cascading consequence of a hacked transportation infrastructure can be more difficult to characterize. Certainly the outcome depends on the hacker's level of access, but it also depends on how close the demand is to the capacity of the transportation system. One study showed some worst-case scenarios from an insider threat (*5*), and another showed the opposite extreme with a compromised vehicle detection sensor (*7*). Consideration of only one of these two extremes motivates very different investments in security.

This paper provides a framework to assist transportation professionals in evaluating the effect of a cybervulnerability with different levels of access while also accounting for the demand on the transportation system. Because the details of specific cyberthreats are found elsewhere, this paper focuses only on the effects of the various levels of access and not on how the access is achieved. Similarly, while other studies provide very sophisticated models of transportation networks, this paper focuses on an easily understood corridor and readily understood transportation metrics (i.e., travel time and percentage of red-light running). The paper is intended to be equally readable by both practitioners in transportation engineering and cybersecurity by focusing on critical points and avoiding extraneous details.

FRAMEWORK OF THREAT ASSESSMENT

The framework of threat assessment developed in this paper focuses on the four main levels of access depicted in Figure 1:

1. Vehicle detector,
2. Corridor synchronization,
3. Traditional Internet, and
4. Physical access.

Level 1 access is the ability to compromise a vehicle detector. Wireless systems are inherently more vulnerable than wired systems. Some wireless vehicle detectors have no security and can be accessed by a hacker from a distance of 1,500 ft (457.2 m)(*7*). Even if some security were implemented, small, low-power sensors are limited in the amount of security that can be implemented because of size, weight, and power constraints, as well as practical cost constraints. For this reason, these wireless attack surfaces are chosen as the first and least-intimate level of access that a hacker can achieve.

Another seemingly benign attack surface (Level 2) is the underlying synchronization of wireless links: by spoofing the observed timing signals that serve as the GPS position, navigation, and timing service, a vehicle may be controllably steered off course (*8*). If the traffic controllers in a synchronized corridor use GPS for time synchronization, a spoofed GPS signal may easily be used to drive well-designed light cycles out of synchronization, destroying network optimization. Modern traffic controllers are equipped with GPS interfaces; however, timing can also be achieved through network time servers or microwave communication links. When synchronization is implemented through wireless microwave signals, corrective actions to restore synchronization may also be disrupted.

Ted and Karyn Hume Center for National Security and Technology, Virginia Polytechnic Institute and State University, 1991 Kraft Drive, Blacksburg, VA 24060. Corresponding author: J. M. Ernst, jmernst@vt.edu.

Transportation Research Record: Journal of the Transportation Research Board, No. 2619, 2017, pp. 55–63.
http://dx.doi.org/10.3141/2619-06

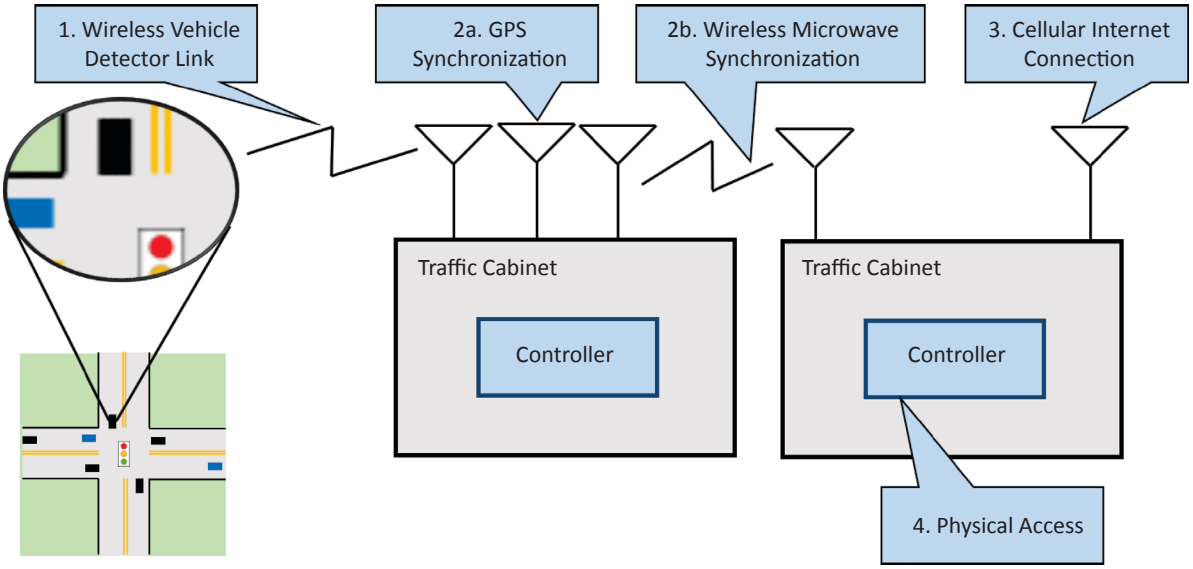

FIGURE 1 Four levels of access analyzed.

The third and fourth levels are more obvious. The third level is concerned with the increasing connectivity of the transportation infrastructure. Traffic cabinets are increasingly networked so that they are accessible from their associated traffic management center. This accessibility means that the security of the transportation infrastructure is limited by the security of the network. This paper investigates one of the possible safety concerns with a network attack: a change in the yellow-light interval. The fourth level is complete physical access to the traffic cabinet.

Other scenarios—including disrupting power to an intersection—though also of interest, are not considered here. In the example of disrupting power, drivers should treat the intersection as a four-way stop, but what real drivers might do is unclear. The response time of police and repair crews would also greatly affect the outcome. While human factors are important in all cyber–physical scenarios, this paper focuses on direct technological effects. A more precise model of detection and response to a cyberattack—as well as more detailed traffic simulations—could be used to investigate any of the described scenarios further.

SIMULATIONS

The simulations in this paper are meant to show clearly the effects that a hacker could have on a very simplistic corridor at each level of access. Realistic simulations can have a significant number of parameters and complexity that can make the effect of the hacker less clear. The simplistic simulations in this study used the Simulation of Urban Mobility (SUMO) software (http://sumo.dlr.de/wiki/Main_Page). The main corridor had six traffic lights that were either coordinated or actuated, depending on the vulnerability being shown (Figure 2). The side streets and the westbound traffic had low

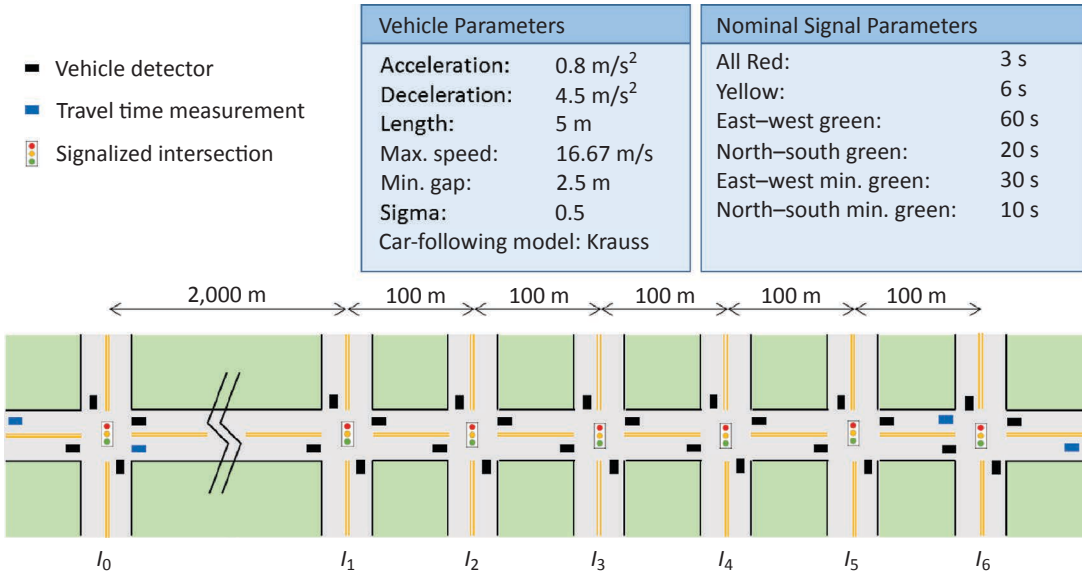

FIGURE 2 Simulated corridor used for all simulated scenarios.

volumes. The eastbound volume was varied to show the extent to which a hacker could affect the system with various levels of access and different vehicular demand.

Simulated Corridor

The simulations used to demonstrate cybereffects are based on a simplistic six-intersection corridor implemented in SUMO (Figure 2). East–west and north–south green times were used for the synchronized corridor, while east–west and north–south minimum green times were used for actuated scenarios. The effect of the cyberintrusion was measured by the change in travel time. The six intersections were spaced at 100 m (328 ft). This distance was chosen to be approximately a city block. While some cities have shorter city blocks [Portland, Oregon, 79 m (259 ft) and the New York borough of Manhattan, 80 m (262 ft)], others are longer [e.g., Sacramento, California, 120 m (394 ft)]. The exact spacing is not relevant to this study, but the spacing must be realistic to model the interactions between intersections. Similarly, nominal vehicle parameters and signal parameters were chosen not to be any specific real value but to be realistic values. SUMO uses these nominal values with a randomization parameter—sigma—to generate the vehicles for the simulation.

Each of the intersections can be run in a coordinated mode with a specified offset or in an actuated mode, which uses the inputs of the vehicle detectors and the minimum times specified. In this simplistic simulated corridor, none of the vehicles turn, and all roads are single lane, so no lane changes occur. While this feature is not realistic, it eliminates variables like origin–destination tables and lane-changing models. The simulated corridor was kept as simple as possible to highlight the effect of the cyberattack and to avoid confounding the results with other nuisance parameters. Because of the lack of lane changing and turning in these simplistic simulations, more complicated traffic patterns could likely accentuate the effects of each attack.

The simplest model for generating the start times of the vehicles at the edge of the network is Poisson arrivals. Because platooning is important for coordinated systems, a Poisson arrival would be too simplistic to model the intersection interactions correctly. To generate a more realistic platooning of the vehicles, an additional intersection was placed 2,000 m (6,562 ft) west of the first intersection in the corridor. This intersection used the random arrivals of the north–south traffic to divide the vehicles into platoons. The main metric of the effect of the cyberattack is the travel time of the eastbound vehicles. The travel time is measured from the blue travel time detector to the east of the platooning intersection (I_0) and at the exit of the eastbound system to the east of the last intersection in the corridor (I_6).

Simulation of Level 1 Access: Compromised-Vehicle Detector

In the simulation of Level 1 access, the intersections were uncoordinated and only switched to a north–south phase when both the minimum east–west green time had been met and a vehicle had triggered one of the north–south detectors. The wireless link to the southbound vehicle detector at Intersection I_5 was compromised so that the vehicle detector was effectively in recall (i.e., it was always detecting a vehicle). The scenario was varied by changing the demand on the eastbound movement because low-demand scenarios are likely to be less affected by detector malfunctions than higher-demand ones. A comparison of the original network and the compromised network appears in the results section.

While this scenario is similar to a situation with a failed detector, it is more serious. Most modern controllers can detect failed detectors and can both report this failure back to the traffic management center and modify the timing plan to minimize the effect of the failed detector. A compromised detector can simultaneously affect the intersection as if an demand on the phase is infinite and trigger the sensor in a way that will avoid the traffic controller's detection algorithms.

Simulation of Level 2 Access: Compromised Synchronization

In coordinated systems, synchronization of the clocks between the intersection controllers is mandatory. This synchronization is implemented in several ways. One way is that the controller is synchronized with an Internet time server. If the traffic cabinet is Internet connected, then there is no wireless synchronization to attack. Many traffic cabinets, however, are not Internet connected. In some corridors, one of the cabinets is connected to the Internet, but others are connected through microwave links along the corridor. The synchronization of the cabinets without a direct Internet connection is accomplished either over these microwave links or through GPS synchronization. Either one of these wireless links can be compromised (*9–11*).

The purpose of the Level 2 simulation is to show the extent to which a hacker can destabilize a coordinated network by simply adjusting the offset in one of the traffic controllers. This destabilization requires only the compromise of a wireless synchronization link and not a traditional cyberattack. The effect of the attack is measured by monitoring the eastbound travel time as the eastbound demand is varied.

Simulation of Level 3 Access: Compromised Network Connection

For Level 3 access, the hacker has access to the traffic controller through a traditional Internet link. Here, a wide range of attacks are available, including those described in the first two simulations. The hacker is not, however, able to turn conflicting phases green simultaneously because of the malfunction management unit (MMU), which sets the intersection in flash mode if the controller attempts such behavior. For this reason, this section focuses on another safety-critical setting: the yellow time.

Red-light running and the related dilemma zone is a significant area of research for transportation engineers because of the serious safety concerns (*12*). Included here are driver behavior studies to try to determine what drivers will do in various scenarios (*13*), weather-related studies for setting yellow times for rainy or wet conditions (*14*), and studies on how yellow-light timings affect red-light running (*15*). Other studies tried to use existing vehicle detectors (e.g., inductive loops) to detect red-light-running events (*16*).

While the SUMO system does not allow vehicles to collide, it allows them to run a red light if they do not have sufficient deceleration to stop before reaching the intersection. To show the danger of a hacker adjusting yellow times, this simulation adjusts the yellow time on the traffic lights. It then investigates the first vehicle to arrive at the intersection after the light changes yellow to determine

whether the vehicle stopped before the intersection, exited the intersection without running the red light, or ran the red light. These percentages of red-light running were calculated for a range of yellow times. While the other scenarios showed an increase in travel time, this scenario showed that a hacker can greatly increase the probability of red-light running, a significant safety concern.

Level 4 Access: Physical Access

This scenario is the most invasive, as the hacker has physical access to the traffic cabinet. In all previous scenarios, the conflict monitor or MMU does not allow conflicting phases of an intersection to turn green simultaneously. Because the MMU relies on a solder board for configuration, it cannot be remotely hacked. Once a hacker has physical access to the cabinet, the solder board in the MMU can be replaced to allow all lights to be simultaneously green. Requiring physical access makes having a widespread effect in a short time difficult; however, the physical access could still happen in advance, and the attack could be enabled later by a compromised network link.

No simulations were performed for Scenario 4, but it was included in the list of scenarios as part of the evaluation framework. Physical security is a very important part of intersection security because it protects this critical fail-safe device (MMU). The possibility of a Level 4 hack is particularly concerning because many cabinets are protected by a standard, readily available, physical key that they all share (*17*).

RESULTS

This section details the results of the simulations described in the previous section. The main metric used to show the effect of the cyberattack was increased travel time. Percentage of vehicles that run red lights was also considered, as well as qualitative descriptions of the effect in each scenario.

Level 1 Access: Compromised Vehicle Detector

The results of this scenario show the extent to which the travel time increased for each chosen value of demand for the eastbound movement. A steady flow of vehicles spaced by a 2-s headway produced 1,800 vehicles per hour (vph). This rate is considered a demand of 100% capacity without including any effect of the traffic signals. Because a traffic signal was used to perform platoons at the input of the system, the simulator was limited to less than 100%.

The actual capacity of the corridor is dependent on the northbound and southbound traffic. If no vehicles are detected on the northbound and southbound movements, then the actual capacity is equal to the maximum capacity. The minimum capacity corresponds to infinite demand on the northbound and southbound movements. This level of demand limited the eastbound–westbound green time to approximately 52% of the maximum capacity, 931 vph. This is the capacity of a single intersection, but the interactions between intersections causes the overall capacity to be lower, especially because the corridor was not coordinated in this scenario.

To get an idea of how the corridor was affected, this section first shows an example simulation at a demand of 1,000 vph at several time steps: 200, 500, 1,000, and 1,500 s (Figure 3). The uncompromised corridor is shown above the compromised corridor at each of the four time steps. The top corridor in each subfigure shows the simulation without a compromised vehicle detector; the bottom corridor in each pair shows the corridor with a compromised detector so that the north–south phase is in recall. These time instances show how the detector in recall can cause significant congestion. The first eastbound vehicles had just arrived at the intersection at 200 s (Figure 3*a*), so the corridors show no noticeable differences at this time. At 500 s (Figure 3*b*), some queuing occurred at intersections, but nothing that would indicate an issue. By 1,000 s (Figure 3*c*), the simulations had significantly diverged. The normal corridor was clearing the queues of the intersections, but the queues in the compromised corridor had begun to interact between intersections. By 1,500 s (Figure 3*d*), the queue of vehicles was growing uncontrol-

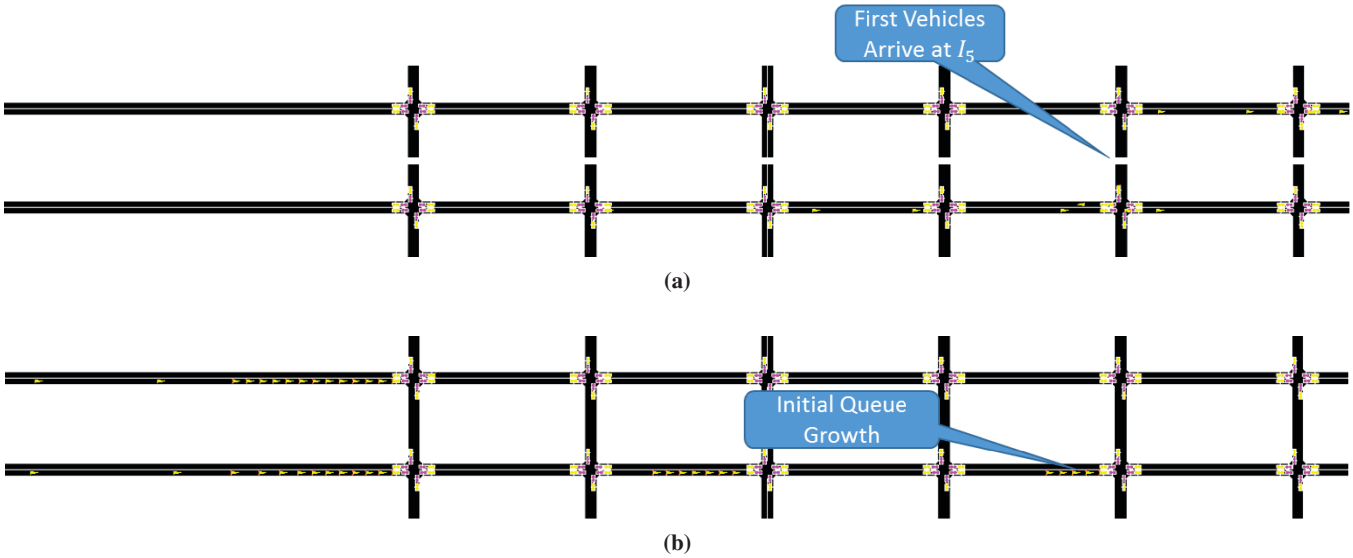

FIGURE 3 SUMO simulations at four time steps with westbound demand of 1,000 vph: (*a*) 200 s and (*b*) 500 s.
(continued)

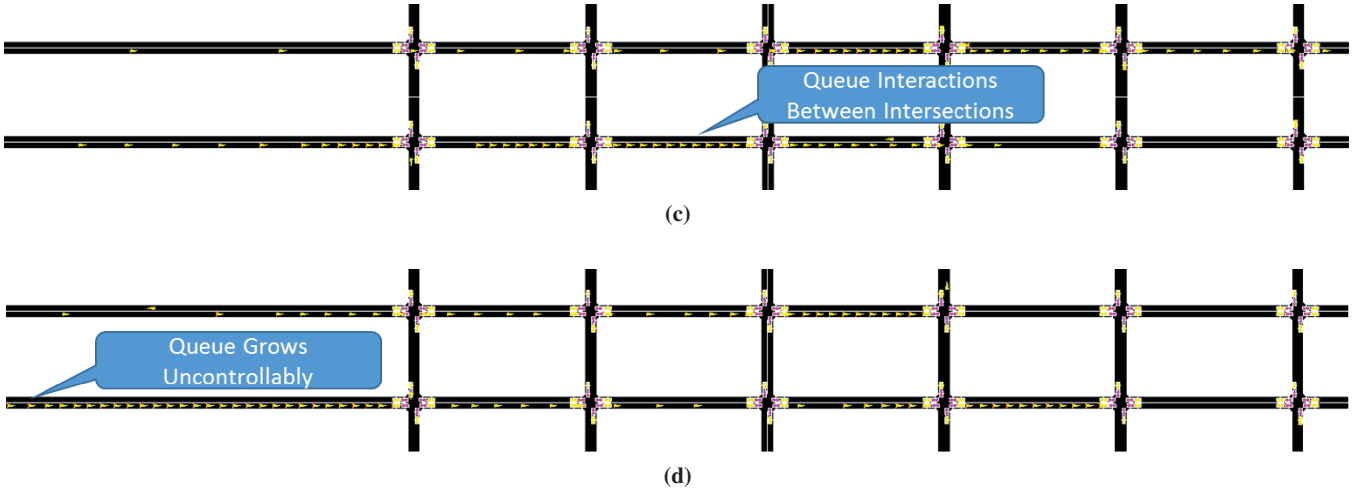

FIGURE 3 *(continued)* SUMO simulations at four time steps with westbound demand of 1,000 vph: (*c*) 1,000 s and (*d*) 1,500 s.

lably in the compromised corridor, but the queues continued to clear in the normal corridor.

For a more numerical analysis, 1-h simulations were run with the eastbound demand ranging from 10 to 1,800 vph, and the mean travel time was calculated. While the normal corridor's average travel time stayed roughly constant at about 200 s, the average travel time for the compromised corridor grew to over 1,000 s (Figure 4). Even for this very simple corridor with no turning or lane changes, a compromised vehicle detector can make a big difference if the vehicle demand is above the compromised corridor's capacity.

Scenario 2. Compromised Synchronization

The second scenario tested shows the effect of desynchronizing coordination of one of the intersections in the corridor. As in Scenario 1, the effected intersection was Intersection I_5. In Scenario 1, some time was required for the intersections to begin to interact. In Scenario 2, the intersection timings had no randomness, so vehicles started to queue immediately. To show this effect, each vehicle was plotted with its start time on the *x*-axis and its travel time on the *y*-axis (Figure 5) for Scenario 2 with an eastbound demand of

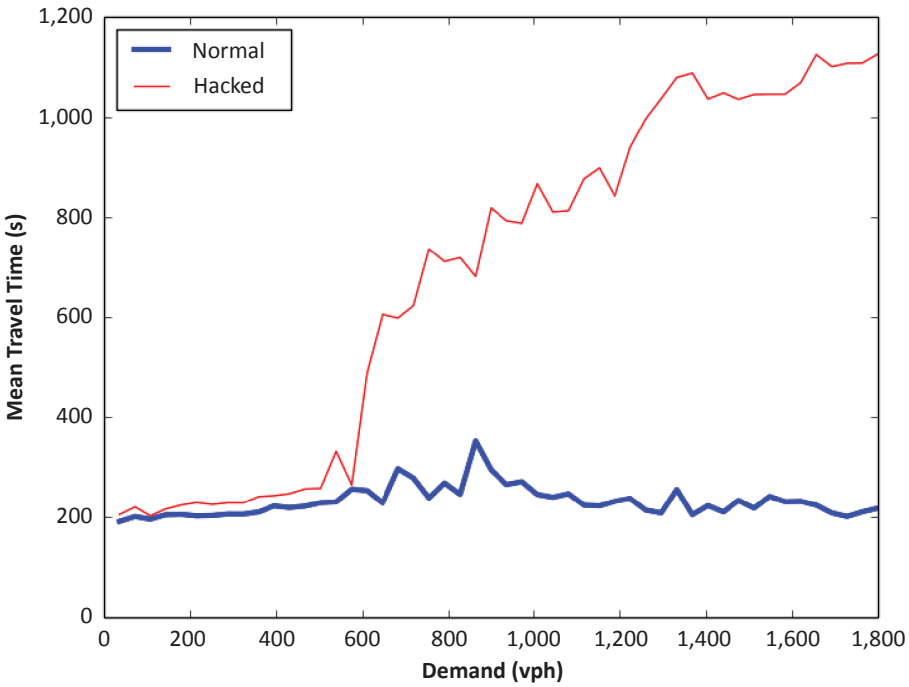

FIGURE 4 Average travel time for corridor with hacked sensor affected for eastbound demand above 600 vph.

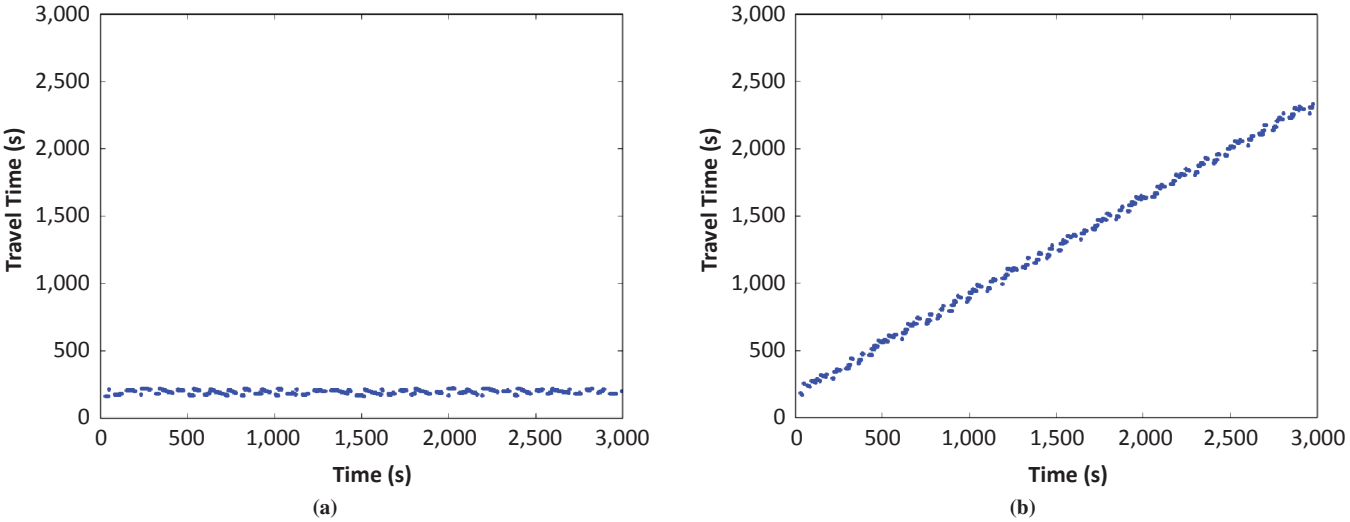

FIGURE 5 Travel times for normal coordinated corridor and coordinated corridor with bad timing offset for eastbound movement with eastbound demand of 1,000 vph: (*a*) normal coordinated corridor and (*b*) coordinated corridor with intersection timing offset.

1,000 vph. The normal corridor had a constant travel time, but the instantly growing queue generated by the intersection offset caused the travel time to grow linearly with time. The travel time for the normal coordinated corridor shows that the travel time was steady at about 200 s (Figure 5*a*). The travel time for Scenario 2 with the wrong offset applied to the fifth intersection shows that a queue started forming immediately, and after 3,000 s, the travel time had increased by over 2,000 s (Figure 5*b*).

A clearer understanding of the effect can be seen by consideration of a range of eastbound vehicle demand (Figure 6). The correctly coordinated corridor has no queuing effect (Figure 6*a*). By changing the offset of the fifth intersection, the travel times increased greatly, up to 3,000 s (Figure 6*b*). For eastbound demands of less than 400 vph, the corridor was unaffected, but as the demand increased, the queuing was significant. Although this type of synchronization is not used in the majority of synchronized corridors, this synchronization error represents a real threat for those that do.

Level 3 Access: Compromised Internet Connection

The evaluation of Level 3 access focuses on one of the yellow time settings because these are safety-critical settings, whereas the two attacks in the previous scenarios were able to affect only travel time. This scenario once again focuses on Intersection I_5. Most vehicles traveling through an intersection do not have the opportunity to run a red light, either because they pass through the intersection while the light is green or the light is already red upon arrival. For this

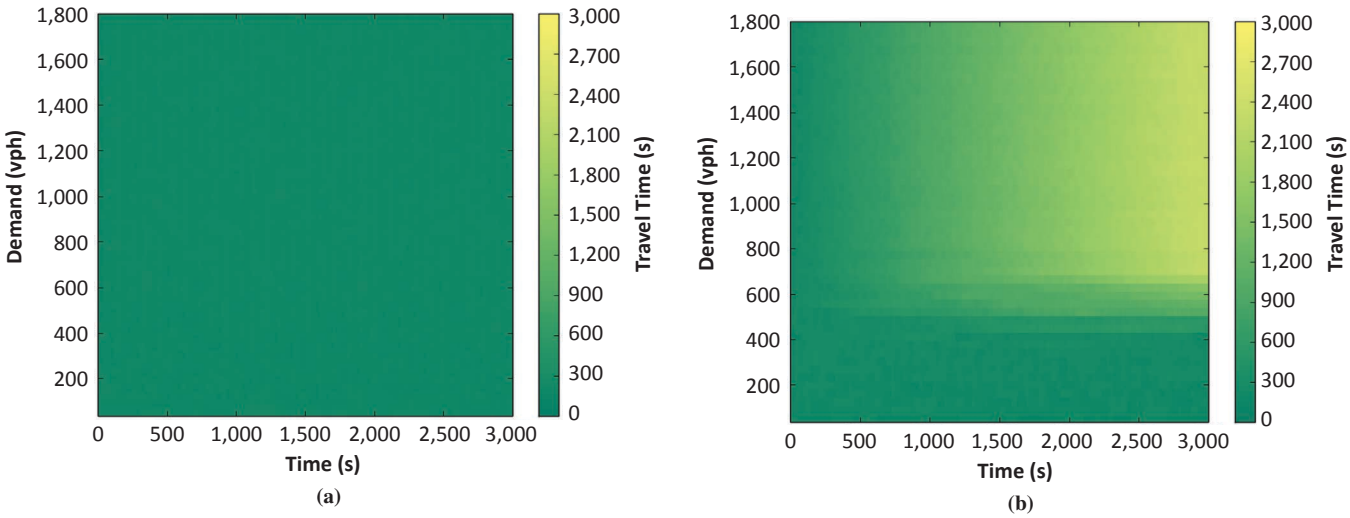

FIGURE 6 Difference between travel times with correctly coordinated corridor and one with single intersection with the incorrect offset caused by synchronization hack: (*a*) coordinated corridor and (*b*) coordinated corridor with single intersection offset error.

reason, only the first vehicle to exit the intersection after the light turns yellow is considered. This vehicle could fall into one of four situations:

1. It passes through the intersection before the light turns red.
2. It passes through the intersection while the light is red.
3. It stops at the intersection and then proceeds after the light turns green.
4. It arrives at the intersection after the light has already turned green.

Only Option 2 constitutes red-light running. Each cycle was evaluated to determine whether that first vehicle ran a red light. The results of this analysis show that red-light running was highly dependent on the yellow time (Figure 7). The figure shows that yellow time has a large effect on the percentage of cycles with a red-light running event. Because of the vehicle parameters chosen for the simulator, red-light running was almost eliminated with a yellow time of 2.5 s. Yellow times less than 1.5 s showed more than 50% of cycles with red-light running events. The specific yellow-time values are not as important as the trend because these values also greatly depend on the speed of the corridor, the deceleration of the vehicle, and the reaction time of the driver. While traffic controllers are designed with safeguards to prevent accidental setting of the green time below a safe value, these safe-value limits are also configurable and would be accessible to an adversary with this level of access. The important takeaway from this simulation is that a hacker could configure the yellow time such that most of the intersection cycles caused a driver to run a red light.

Scenario 4. Physical Access

No simulations were run for Scenario 4 because if hackers gain physical access to the traffic cabinet, then they can do anything. In movies, a hacker can cause conflicting phases of an intersection to turn green at the same time. In reality, this result is impossible without physical access because the definition of conflicting phases is implemented in a solder board (Figure 8). This board cannot be remotely hacked because the physical connections cause the intersection to convert to flashing red and yellow lights if conflicting green phases are activated. If a hacker gains physical access to a cabinet, then these protections can be compromised. In some newer traffic cabinets, the conflict monitor has been changed to be software configurable and uses a data key to store the phase-conflict data. This feature could pose an additional cybersecurity vulnerability.

Any physical access could be detected by the traffic management center because many cabinets log every event when the traffic cabinet door is opened. To replace the card in the conflict monitor, the attacker would have to reset the intersection, which would log even more suspicious events. While this scenario does not focus on the technological security challenges of a traffic cabinet, it does speak to the policy side of cyber–physical systems security. In the scenario with suspicious logged events, transportation engineers would be likely to investigate and confirm that the intersection is functioning properly. This scenario indicates that the intersection evaluation should also include attempts to activate conflicting phases to ensure that the conflict monitor has not been compromised.

While this section has focused on access to the conflict monitor, physical access to a traffic cabinet is likely to provide unlimited access to the intersection and entry into the network of traffic controllers. Another possible threat could be derived from access to camera feeds and real-time manipulation of the intersection phases. This section has focused only on one example of how physical access could be a problem.

CONCLUSIONS

This study provided a framework for cyberthreat assessment for evaluating the effect that a hacker can have on a transportation system with different levels of access: compromised vehicle detector,

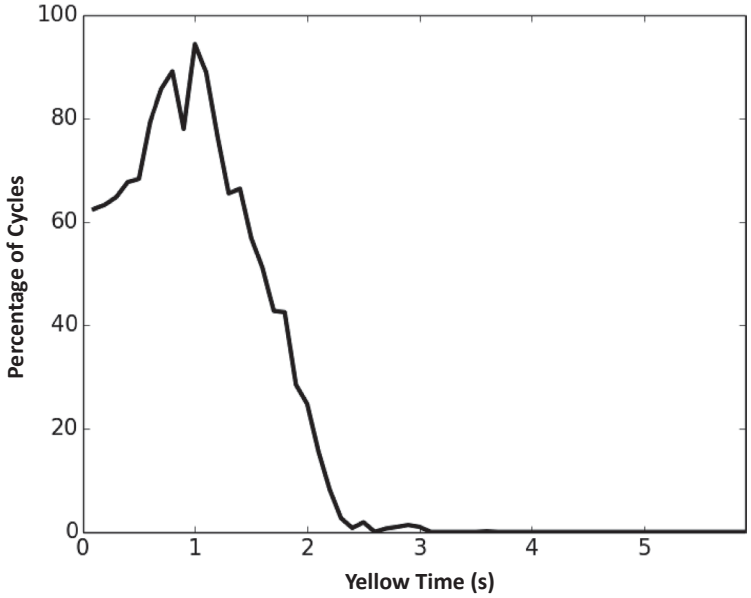

FIGURE 7 Effect of length of yellow time on red-light running.

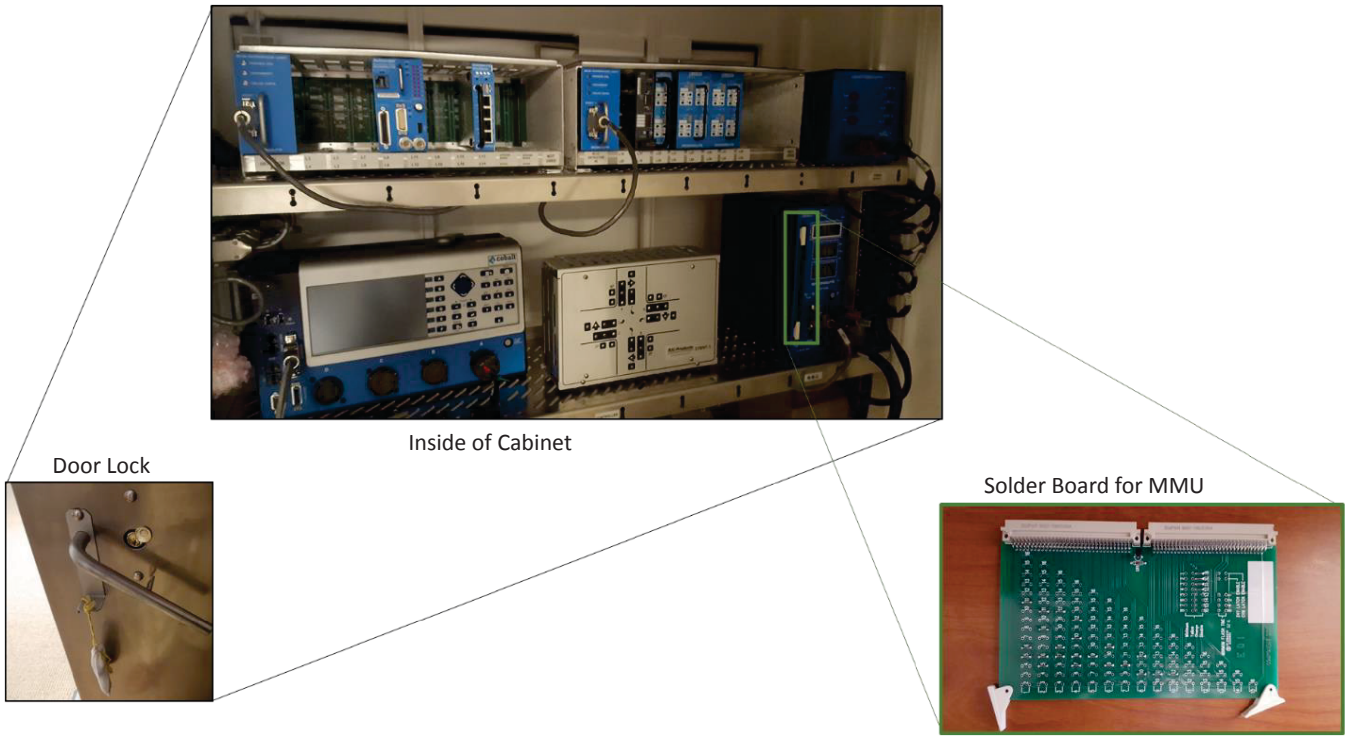

FIGURE 8 Traffic cabinet physical security: (*a*) inside of cabinet, (*b*) door lock, and (*c*) solder board for MMU.

compromised corridor synchronization, traditional Internet access, and physical access. The level of access in the first two scenarios was shown to increase travel time significantly, while the other two scenarios showed the possibility of safety concerns. This study used simplified traffic simulations and focused on the direct effects of the changes. Future work to incorporate human factors, policy, intrusion detection, and so on could help create a clearer picture of threat surfaces and recovery capabilities.

The simulations in the first scenario showed that, by a hacker causing a sensor to be in recall (for which it is always detecting a vehicle), the average travel time could be raised from 200 s to more than 1,000 s with an eastbound vehicle demand of 1,000 vph.

The second scenario showed the effect from compromised synchronization of one intersection in the corridor. By a hacker adjusting the offset of Intersection I_5, the travel time through the corridor was raised from approximately 200 s to more than 2,000 s. This change in travel time resulted from a large queue that started forming immediately in the simulation.

In Scenario 3, the simulation showed that—by lowering the yellow time—a hacker could cause a significantly higher rate of vehicles running red lights. While the increased travel times in the first and second scenarios are unfortunate, red-light running is a serious safety concern.

Scenario 4 did not have any associated simulations. It is difficult to simulate the worst possible case for the scenario, in which a hacker has physical access to the traffic cabinet. With this level of access, the hacker could replace the solder board in the MMU and make conflicting green phases run simultaneously. While red-light running is likely to increase the number of accidents, turning conflicting phases green is worse.

This evaluation framework has shown that the range of vulnerabilities for traffic signal controllers is large. In many cases, the vehicle volumes may be low enough that compromised sensors or timing offsets may be tolerable when compared with the expense of securing the systems. Because physical access allows a hacker the ability to do anything, including turning conflicting phases green simultaneously, physical security must be the priority for all intersections.

This framework for cyberevaluation is a step toward helping transportation engineers and cybersecurity professionals understand the types of threats that exist to the transportation infrastructure. This framework is intended to assist with the prioritization of the ever-growing need for cybersecurity in transportation infrastructure.

REFERENCES

1. Fok, E. Cyber Security Challenges: Protecting Your Transportation Management Center. *ITE Journal,* Vol. 85, No. 2, 2015, pp. 32–36.
2. Reilly, J., S. Martin, M. Payer, and A. M. Bayen. Creating Complex Congestion Patterns Via Multi-Objective Optimal Freeway Traffic Control with Application to Cyber-Security. *Transportation Research Part B: Methodological,* Vol. 91, 2016, pp. 366–382. https://doi.org/10.1016/j.trb.2016.05.017.
3. Hou, Y., Y. Zhao, A. Wagh, L. Zhang, C. Qiao, K. F. Hulme, C. Wu, A. W. Sadek, and X. Liu. Simulation-Based Testing and Evaluation Tools for Transportation Cyber–Physical Systems. *IEEE Transactions on Vehicular Technology,* Vol. 65, No. 3, 2016, pp. 1098–1108. https://doi.org/10.1109/TVT.2015.2407614.
4. Nowakowski, C., S. E. Shladover, C.-Y. Chan, and H.-S. Tan. Development of California Regulations to Govern Testing and Operation of Automated Driving Systems. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2489, 2015, pp. 137–144. https://dx.doi.org/10.3141/2489-16.
5. Ezell, B. C., R. M. Robinson, P. Foytik, C. Jordan, and D. Flanagan. Cyber Risk to Transportation, Industrial Control Systems, and Traffic

Signal Controllers. *Environment Systems & Decisions,* Vol. 33, No. 4, 2013, pp. 508–516. https://doi.org/10.1007/s10669-013-9481-2.
6. Miller, C., and C. Valasek. *Remote Exploitation of an Unaltered Passenger Vehicle.* Black Hat, 2015.
7. Perlroth, N. Traffic Hacking: Caution Light Is On. *New York Times,* June 10, 2015. http://bits.blogs.nytimes.com/2015/06/10/traffic-hacking-caution-light-is-on. Accessed Aug. 1, 2016.
8. Carroll, J. V. Vulnerability Assessment of the U.S. Transportation Infrastructure that Relies on the Global Positioning System. *Journal of Navigation,* Vol. 56, No. 2, 2003, pp. 185–193. https://doi.org/10.1017/S0373463303002273.
9. Motella, B., M. Pini, M. Fantino, P. Mulassano, M. Nicola, J. Fortuny-Guasch, M. Wildemeersch, and D. Symeonidis. Performance Assessment of Low-Cost GPS Receivers Under Civilian Spoofing Attacks. *Proceedings of the 5th ESA IEEE Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing.* NAVITEC, Noordwijk, Netherlands, 2010, pp. 1–8. https://doi.org/10.1109/NAVITEC.2010.5708018.
10. Shephard, D. P., J. A. Bhatti, T. E. Humphreys, and A. A. Fansler. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. *Proceedings of the ION GNSS Meeting,* Vol. 3, Nashville, Tenn., 2012.
11. Tippenhauer, N. O., C. Pöpper, K. B. Rasmussen, and S. Capkun. On the Requirements for Successful GPS Spoofing Attacks. *Proceedings of the 18th ACM Conference on Computer and Communications Security,* 2011, pp. 75–86. https://doi.org/10.1145/2046707.2046719.
12. Chang, G.-L., M. L. Franz, Y. Liu, Y. Lu, and R. Tao. Design and Evaluation of an Intelligent Dilemma-Zone Protection System for a High-Speed Rural Intersection. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2356, 2013, pp. 1–8. https://dx.doi.org/10.3141/2356-01.
13. Gates, T. J., H. McGee, Sr., K. Moriarty, and H.-U. Maria. Comprehensive Evaluation of Driver Behavior to Establish Parameters for Timing of Yellow Change and Red Clearance Intervals. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2298, 2013, pp. 9–21. https://dx.doi.org/10.3141/2298-02.
14. El-Shawarby, I., A.-S. G. Abdel-Salam, and H. Rakha. Evaluation of Driver Perception–Reaction Time Under Rainy or Wet Roadway Conditions at Onset of Yellow Indication. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2384, 2013, pp. 18–24. https://dx.doi.org/10.3141/2384-03.
15. Rakha, H. A., M. J. Baird, and I. El-Shawarby. Designing Traffic Signal Yellow and Change Intervals Considering Truck Impacts. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2438, 2014, pp. 33–44. https://dx.doi.org/10.3141/2438-04.
16. Lavrenz, S. M., C. M. Day, J. Grossman, R. Freije, and D. M. Bullock. Use of High-Resolution Signal Controller Data to Identify Red-Light Running. *Transportation Research Record: Journal of the Transportation Research Board,* No. 2558, 2016, pp. 41–53. https://dx.doi.org/10.3141/2558-05.
17. Tebow, L. Choose Who Has Control of the Traffic Signals. *IMSA Journal,* Jan. 2012, http://www.imsasafety.org/journal/ja12/15.pdf. Accessed Aug. 1, 2016.

The Standing Committee on Traffic Signal Systems peer-reviewed this paper.