TRR
JOURNAL OF THE TRANSPORTATION RESEARCH BOARD

*Article*

Transportation Research Record
1–14

DOI: 10.1177/0361198118784378
journals.sagepub.com/home/trr
SAGE

# Modeling Cyber Attacks at Intelligent Traffic Signals

**Gurcan Comert[1], Jacquan Pollard[1], David M. Nicol[2], Kartik Palani[3], and Babu Vignesh[3]**

**Abstract**

Transportation networks are considered one of the critical physical infrastructures for resilient cities (cyber-physical systems). In efforts to minimize adverse effects that come with the advancement of vehicular technologies, various governmental agencies, such as the U.S. Department of Homeland Security and the National Highway Traffic Safety Administration (NHTSA), work together. This paper develops belief-network-based attack modeling at signalized traffic networks under connected vehicle and intelligent signals frameworks. For different types of cyber attacks, defined in the literature, risk areas and impacts of attacks are evaluated. Vulnerability scores, technically based on the selected metrics, are calculated for signal controllers. In addition, the effect of having redundant traffic sensing systems on intersection performance measures is demonstrated in terms of average queue length differences.

Resilience of critical infrastructures is defined as their ability to withstand an upsetting event, deliver essential levels of service during it, and recover quickly after it. With the increase of connected systems, cyber attacks that can target critical infrastructure systems are becoming more troubling. Transportation networks are considered one of the critical physical infrastructures for resilient cities (cyber-physical systems [CPSs] [*1*]). According to recent reports (*2–4*), several benefits are foreseen from upcoming technologies such as connected and autonomous vehicles (CAVs), including up to 80% reduction in fatalities from multi-vehicle crashes and prevention of the majority of human-error-related incidents, which takes out about 94% of all incidents. These intelligent applications, however, come at a price; for example, in 2015 alone 1.5 million vehicles were recalled because of cybersecurity vulnerabilities. NHTSA's current research focuses on CAVs that are heavily involved in secure implementations which will enable the field and its technology experts to harness efficient, reliable, and secure system design (*3*). Some of these topics can be listed as anomaly-based intrusion detection systems, cybersecurity of firmware updates, cybersecurity on heavy vehicles, vehicle-to-vehicle (V2V) communication interfaces, and trusted vehicle-to-everything (V2X) communications (*5*). The main goals for any critical infrastructure are quick detection of attacks and rapid mitigation efforts (*6*). There are many attack types, of which some can be resolved via detection and some require redundant systems and sensors. In intelligent transportation systems (ITS), to increase security and resiliency in case of possible attacks or benign system errors during different events, research is likewise needed into detection using various sensors and data types. Research is also necessary to enhance confidence in sensor readings by checking consistency with other sensors and information sources as well as validating control system commands (*7*). This paper investigates attack modeling and impacts on intelligent signals. For different types of cyber attacks defined in the literature (e.g., [*8*]). risks are calculated via probabilistic graphical models (e.g., the Bayesian network [BN] [*9*]) and quantified by system simulations.

In the literature, related studies with analytical graphical models include factor graphs, BNs, and Markov random fields (*10*). Two detailed works on current attack types, survey studies on CPS security, list possible attacks and discuss their mitigation techniques (*11*, *12*). In these

[1]Department of Physics and Engineering, Benedict College, Columbia, SC
[2]Department of Electrical and Computer Engineering, University of Illinois, Urbana-Champaign, IL
[3]Coordinated Science Laboratory, University of Illinois, Urbana-Champaign, IL

**Corresponding Author:**
Address correspondence to Gurcan Comert: comertg@benedict.edu

studies, abstract cyber-physical models for smart cars are presented. Possible attacks are listed as criminal, privacy, tracking, profiling, political threats with different structures replay, command (message) injection, eavesdropping, and denial of service (DOS).

Existing research efforts on vehicular communications discuss possible attacks and their mitigation methods (*5*, *8*). A recent study on current signal cabinets presents the idea that the possible impact of attacks could be unmanageable queues (*13*). Overall, ITS applications require protocols that conflict with anonymity and privacy requirements. The research looks at quantifying such risks and at traffic control in the case of either lost or faulty communications. In sum, studies on the quick detection of such cases and possible redundant data resources for cost effective control are needed for improving the resiliency of transportation networks.

Moreover, model-based attacks, usually for power grids, are investigated by researchers (*14*). Intrusion models for different control systems and proper modeling for moving systems, as in vehicular or mobile ad hoc network (VANET/MANET) cases, are well-investigated in (*11*), in which reputation management in vehicular networks is recommended. Possible revoking or blacklisting of information contributors is also recognized in a similar survey study specifically on cooperative ITS (*8*). Driver privacy and safety critical applications are also starting to be investigated by the researchers (*15*).

The particular contributions of this paper can be listed as:

- Development of a connected vehicle-based signal system model with cyber-physical representation
- Application of a probabilistic expert system (BN) for modeling anomalies and attacks (malicious messages or benign failures)
- Presentation of the impact of redundancy systems (sensors) and a number of different traffic states (from parameters: market penetration rate, and vehicle–pedestrian traffic composition versus control reliability)

The rest of the paper is organized as follows. Section 2 introduces the problem and the approach. Section 3 explains the analytical modeling and BNs. Section 4 presents simulations from BNs. The section also describes analysis with and without sensors at an isolated traffic signal. Finally, section 5 summarizes findings and addresses possible future research directions.

## Methodology

The main objective of this paper is to develop analytical graphical models for quantification of possible attack impacts on intelligent traffic signal components through controller states. First, a BN is generated based on the physical model of an intelligent traffic signal given in Figure 1 which is adopted from (*16*). Second, different attack surfaces, scenarios, and possible impacts for risks are obtained from (*5*). Finally, the two previous steps are combined and standard vulnerability scores from (*17*) are calculated.

In Figure 1, possible intelligent signal components (i.e., physical devices) are depicted. The signal controller unit has a processor, memory, and connections (e.g., ethernet, wireless, or other ports). Although simplified, the figure is part of the field test architecture of connected adaptive signals (*18*). In an arterial setting, each intersection would have a communication device and a controller overseen by a single traffic management system. For communication among the devices, the security certificate authority (e.g., Security Credential Management System [SCMS]) is interfaced to the roadside equipment (RSE) and used to provide security certificates to trusted on-board equipment (OBE).

In the figure, various modes of passenger vehicles, emergency vehicles, freight, transit, motorcycles, and other motorized travelers are represented as vehicles. Pedestrians represent any other nonmotorized modes such as bicycles. These vehicles and pedestrians can also be equipped; that is, they could have an OBE or portable device which can communicate traffic control system (via RSE). In this study, the traffic control system consists of the signal controller, other surveillance technologies and environmental sensors, and an RSE. The RSE radio manages the 5.9 GHz Dedicated Short Range Communications (DSRC) between vehicles and the infrastructure. Specific channels are designated for vehicles to broadcast basic safety messages (BSM-channel 172) and RSE to broadcast the map message (MAP), the signal phase and timing messages (SPaTs), and signal status messages (SSM-channel 182).

In a broader view of the traffic network, signal controllers can be positioned as part of a traffic management system in which different control devices can be connected and coordinated for various transportation modes. These modes can be sensed by different detection technologies (fixed-inductive loops, video, infrared, radar, magnetic plates, pedestrian buttons or solely mobile-GPS, and cell phones, etc.). These detectors provide information to the signal control algorithms for presence to change or extend phases. These communications can be direct (pedestrian push button) or based on inference (video cameras–queues).

The functions of the signal controller can be listed as processing traffic sensor data, pedestrian protection, conflict monitoring, and giving indicative output data for roads, other signals, or users. It also monitors RSE operation and provides a device interface for field

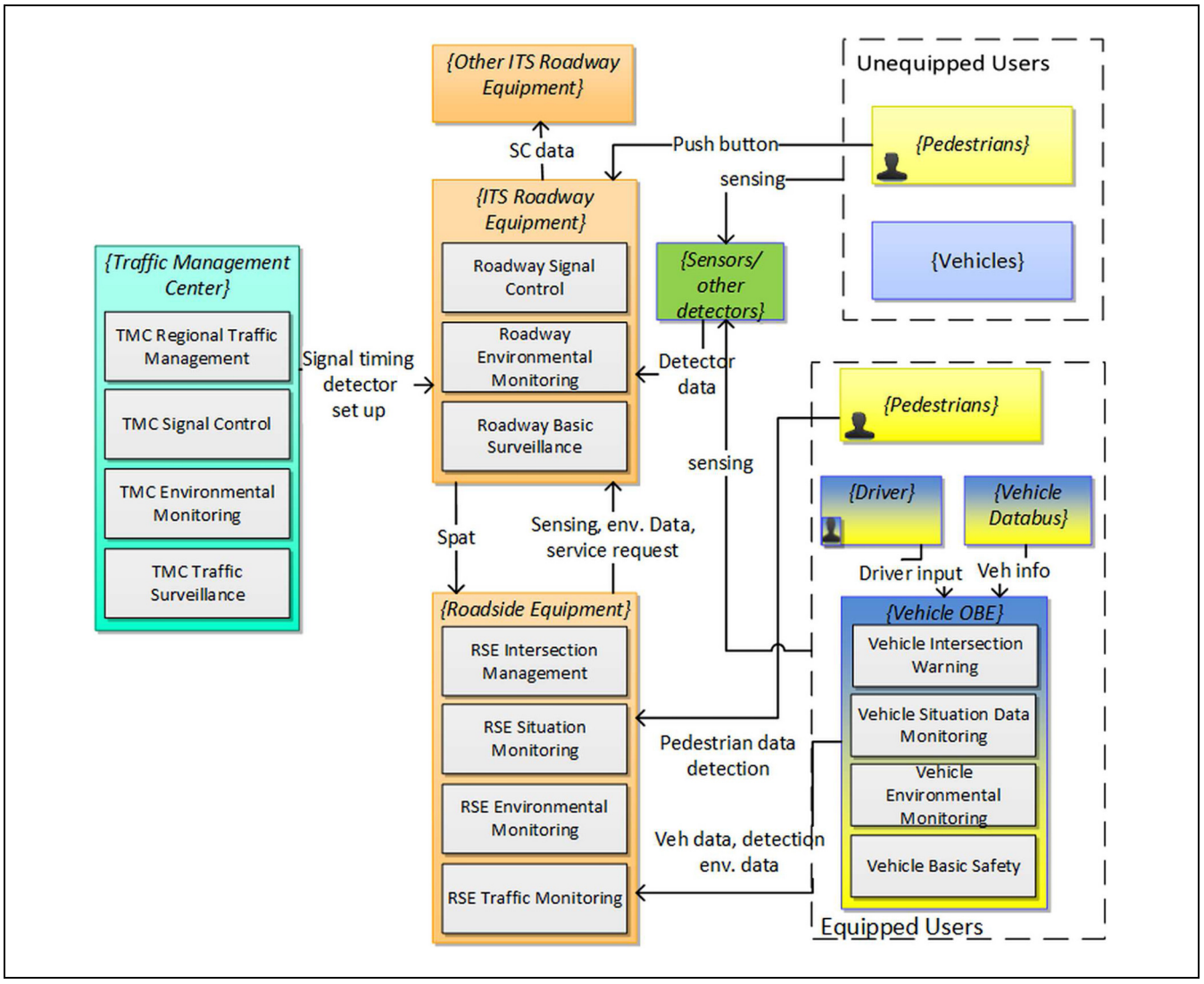



**Figure 1.** A possible intelligent signal adopted from (*16*).

management stations. The impacts on applications can be listed as data distribution for eco-signaling, eco-transit, emergency vehicle preemption, freight signal priority, pedestrian mobility, red light violation warning, and transit priority. In this study, for simplicity, the impacts of cyber attacks are quantified as changes in service times, specifically average queue lengths (*13*).

## Bayesian Networks

Bayesian (belief) networks are stochastic graphical expert systems that depict conditional (in)-dependences of probabilities of interest. Basically, they are expressions of complex joint distributions with a large number of variables involving levels of conditional independences. They can be used for finding probability distributions of a variable with multiple states which can be expressed as replications of such a variable with unobserved states (i.e., hidden Markov models); some variables can also be assumed as parameters connecting different realizations, therefore calculating the posterior probabilities of such parameters.

BNs in a cybersecurity context are utilized to model hypothesized communications and to generate risk and reliability in the presence of possible attacks (*9*, *19*, *20*). Example cases on safety can be found in (*21*, *22*). The literature involving simulation and analytical models also addresses different attack types. From a cybersecurity viewpoint, in general they include message injection, replay, data manipulation, eavesdropping, routing, DOS, and coordinated multiple attacks. However, in this study they are revised for a connected vehicle (CV) framework (*5*). The physical model Figure 1 introduced above is modified with the addition of multiple modes, detection

**Table 1.** Attack Surfaces for Equipped Vehicles and Pedestrians

| Target | Type | Feasibility | Metric | Detection | Metric |
|---|---|---|---|---|---|
| SA | LTC | low | $[h\ l\ l]$ | med | $[l\ h\ l]^T \times [h\ l\ l]$ |
| | CRL | med | $[l\ h\ l]$ | med | $[l\ h\ l]^T \times [l\ h\ l]$ |
| | PC | med | $[l\ h\ l]$ | med | $[l\ h\ l]^T \times [l\ h\ l]$ |
| RSE | WSA | high | $[l\ l\ h]$ | low | $[h\ l\ l]^T \times [l\ l\ h]$ |
| | DB | high | $[l\ l\ h]$ | med | $[l\ h\ l]^T \times [l\ l\ h]$ |
| | DOSR | high | $[l\ l\ h]$ | high | $[l\ l\ h]^T \times [l\ l\ h]$ |
| | SD | low | $[h\ l\ l]$ | high | $[l\ l\ h]^T \times [h\ l\ l]$ |
| VEHs | CB | low | $[h\ l\ l]$ | low | $[h\ l\ l]^T \times [l\ h\ l]$ |
| | BLK | med | $[l\ h\ l]$ | low | $[h\ l\ l]^T \times [l\ h\ l]$ |
| | RB | low | $[h\ l\ l]$ | low | $[h\ l\ l]^T \times [h\ l\ l]$ |
| | BSM | high | $[l\ l\ h]$ | low | $[h\ l\ l]^T \times [l\ l\ h]$ |
| | DOS | high | $[l\ l\ h]$ | low | $[h\ l\ l]^T \times [l\ l\ h]$ |
| | MP | high | $[l\ l\ h]$ | med-high | $[l\ m\ h]^T \times [l\ l\ h]$ |
| | DCC | med | $[l\ h\ l]$ | med | $[h\ l\ l]^T \times [l\ h\ l]$ |
| | LC | med | $[l\ h\ l]$ | low | $[h\ l\ l]^T \times [h\ l\ l]$ |

*Note*: vehs = vehicles; pedes = pedestrians.

interfaces, and a series of other signals in simulation. The critical issue, though, when data are obtained only from CVs, is that any error could result in significant costs. Therefore, the impacts of back up surveillance systems and attacks in a cyber-physical context are investigated.

In the study, multiple BNs are generated to see the impact of having redundant detection systems which can be treated as additional costs. BNs are utilized to calculate conditional probability distributions and expected vulnerabilities and their standard deviations via Monte Carlo simulations. Some predictions are also provided given assumed evidences for different scenarios. Thus, a mixture of various BN usages is incorporated into this paper. First, variables (nodes) and their discrete states are defined. Note that these are assumptions mostly compiled from (*5*, *17*). Second, nodes and respective edges are formed from Figure 1. These nodes are mainly variables that are affecting signal control states. Parental nodes (attack surfaces) along with their vulnerability scores are given in Table 1. Metrics from (*17*), (low, med, high) and (none, low, med, high, cri), represent likelihoods of attacks, states of a node after an attack, and detection probabilities. Standard values for such metrics are also described below. The last column of the table, for example, shows a conditional probability matrix of $p(\text{SDS}|\text{LTC})$ in multiplication of $[l\ h\ l]^T_{(1\times 3)}$ and $[h\ l\ l]_{(1\times 3)}$ matrices. It basically denotes the probability of detection given a fake long-term certificate (LTC) attack. The marginal distribution of LTC is also given as $[h\ l\ l]$ because feasibility is low.

The model's system constraints or assumed variables, and their descriptions and metrics (states) are given in Table 2. For an example description, a signal controller box is denoted by (SC). Traffic composition (TC) consists of equipped and unequipped roadway users that are denoted as pedestrians (EP), cars (CR), emergency vehicles (EM), freight trucks (FR), transit (TR), unequipped pedestrians (UP), and unequipped vehicles (UV). This is by no means an exhaustive list of possible attacks, and extensions can easily be incorporated into the developed networks. For instance, satellite systems or time source manipulations can be incorporated on multiple surfaces along with detailed feasibility and impact of such attacks. If available, more complex metrics or probability distributions can be included for feasibility of the attacks.

Figure 2 shows designed BNs under assumed dependencies among the nodes given in Table 2. Figure 2*a* is a BN with single signal controller including a sensor (additional detection) node. This is critical as the reliability of the SC could increase via additional ground truth checks as well as control via this sensor which could be quantified using simulation in subsection. However, this would involve additional cost. Similarly, detection nodes can be seen as a cost for monitoring and delay of communications. In the figure, SC is connected on pedestrian push buttons (it is assumed that there is no impact on the SC state), other ITS which can be other signals, TMC, S, and most importantly RSE. Transition of the risk at an SC to series of other SCs (i.e., ten controllers) is demonstrated by the BN in Figure 2*b*.

Now, suppose all the nodes in Table 2 $N = \{\text{SC,SA,...,DCC,LC}\}$. Given:

$$p(\text{SC}) = \sum_{N/\text{SC}} \prod_{N/\text{SC}} p(\text{SC}|\text{pa(SC)}) \tag{1}$$

where pa(SC) represents the parental variables of SC. Simply when nodes are incorporated, Equation 1 follows:

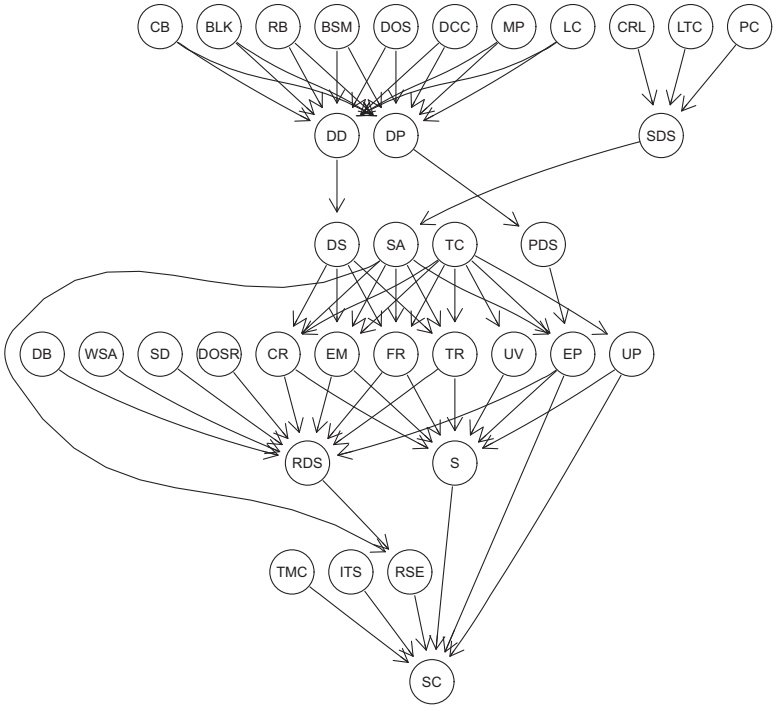
**Table 2.** Nodes on the Designed BNs with Assumed Metrics

| Node | Description | States |
|---|---|---|
| SC | signal controller | none, low, med, high, cri |
| SA | certificate (security) authority | low, med, high |
| RSE | roadside equipment | low, med, high |
| TC | traffic composition | UP, EP, UV, CR, EM, FR, TR |
| UP | unequipped pedestrians | none, low, med, high, cri |
| EP | equipped pedestrians | none, low, med, high, cri |
| UV | unequipped vehicles | none, low, med, high, cri |
| CR | regular equipped vehicles | none, low, med, high, cri |
| EM | emergency vehicles | none, low, med, high, cri |
| FR | freight trucks | none, low, med, high, cri |
| TR | transit vehicles | none, low, med, high, cri |
| ITS | other ITS devices | low, med, high |
| TMC | traffic management center | low, med, high |
| S | sensor | true, false |
| DD | detection by driver | low, med, high |
| DP | detection by pedestrian | low, med, high |
| DS | detection by system (vehs) | low, med, high |
| PDS | detection by system (pedes) | low, med, high |
| RDS | detection by system (RSE) | low, med, high |
| SDS | detection by system (SA) | low, med, high |
| LTC | fake long-term certificate | low, med, high |
| CRL | fake certificate revocation list | low, med, high |
| PC | pseudonym certificate | low, med, high |
| WSA | wrong safety warning and signal phasing | low, med, high |
| DB | database and map poisoning | low, med, high |
| DOSR | denial of service (RSE) | low, med, high |
| SD | device shutdown | low, med, high |
| CB | sending channel busy | low, med, high |
| BLK | block pseudonym change | low, med, high |
| RB | remote reboot | low, med, high |
| BSM | send/intrusion/fake basic safety message | low, med, high |
| DOS | denial of service (vehs, pedes) | low, med, high |
| MP | database and map poisoning (vehs) | low, med, high |
| DCC | distributed congestion control mechanisms | low, med, high |
| LC | location tracking | low, med, high |

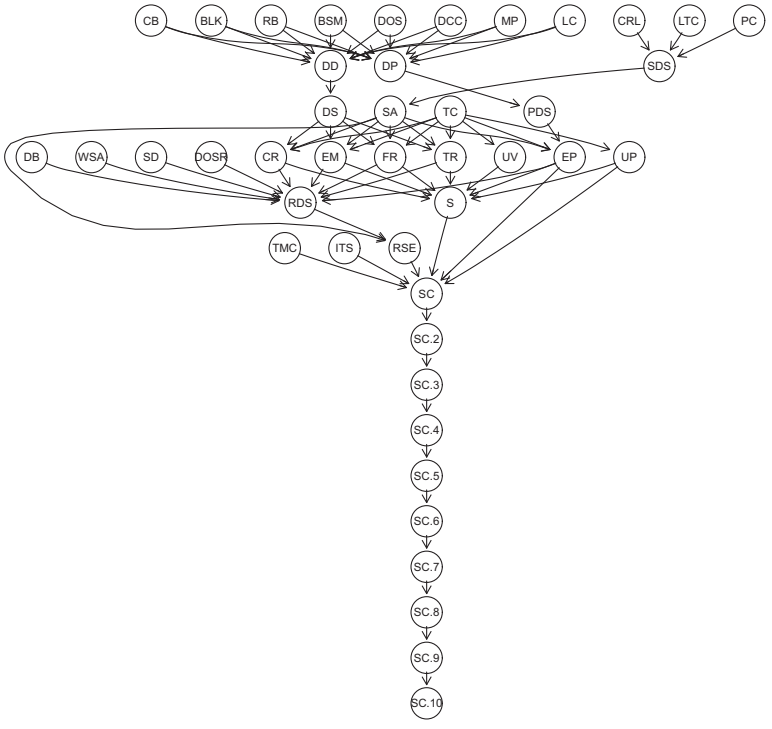
*Note*: vehs = vehicles; pedes = pedestrians.

$$\begin{aligned} p(\mathrm{SC}) &= \sum_{(S,\,\mathrm{RSE},\,\ldots,\,\mathrm{WSA})} p(\mathrm{SC},\mathrm{S},\mathrm{RSE},\ldots,\mathrm{WSA}) \\ &= p(\mathrm{SC}|\mathrm{S},\mathrm{RSE},\ldots,\mathrm{WSA})p(\mathrm{RSE}|\mathrm{RDS},\ldots) \\ &\quad p(\mathrm{S}|\mathrm{UV},\mathrm{UP},\mathrm{EP},\ldots,\mathrm{TR})\ldots p(\mathrm{WSA}) \end{aligned} \tag{2}$$

Probabilities in Equation (2) from BNs are propagated (posteriors) by the junction tree algorithm with $O(n^3)$ time complexity for marginal distributions. The algorithm actually yields the multiplication of conditional probabilities including the independences, a simplified version. The algorithm, on directed acyclic graphs, first marries parent nodes, then triangulates and removes unnecessary links through generation of cliques and assignments, and reports message propagation (*22*). Note that parent nodes $p$(WSA) require probability assumptions for uncertain evidence setting. Scales are adopted from (*5*) and assigned from (*17*). Specifically state vectors (levels) for RSE (low, med, high) and SC (none, low, med, high, cri) are assigned with maximum probabilities (0.25, 0.50, 0.75) and (0.01, 0.39, 0.69, 0.89, 1.0) respectively. Note that for RSE these probabilities represent low (affected by a serious attack, failure like), med (less affected), and high (working) states. For SC, the state probabilities are none (not affected), low (working state), med (still working, but service times would be affected), and high and cri, which are highly affected states in which traffic is disrupted with long delays (e.g., hazardous conditions for emergency vehicles). To address the sensitivity, these probabilities are generated randomly from a uniform distribution and the resulting posteriors are obtained as distributions for each state rather than a single value. Moreover, the resulting expected utilities for vulnerabilities are calculated on a scale of 0–10, on which up to 0.1 shows no risk or impact and 10 means cri vulnerability. BNs are coded and developed using gRain package in R (*23*). Examples of




(a) Bayesian network with single signal controller




(b) BN of progression of risk from a single SC

**Figure 2.** Designed BNs.

**Table 3.**

Propagated $p$(SC|RSE), $p$(SC|S), and $p$(RSE|RDS) with sensor.

| | | SC | | | | | | RSE | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | none | low | med | high | cri | | low | med | high |
| RSE | low | 0.923 | 0.076 | 0.00002 | 0.00003 | 0.00002 | RDS | 0.007 | 0.198 | 0.794 |
| | med | 0.923 | 0.076 | 0.0001 | 0.0001 | 0.00004 | | 0.890 | 0.057 | 0.053 |
| | high | 0.923 | 0.076 | 0.00005 | 0.0002 | 0.0001 | | 0.999 | 0.00003 | 0.00003 |
| S | true | 0.937 | 0.062 | 0.00006 | 0.00008 | 0.00005 | | | | |
| | false | 0.703 | 0.296 | 0.00031 | 0.00041 | 0.00024 | | | | |

Propagated $p$(SC.10|SC), $p$(SC.10|S), and $p$(SC.10|RSE) with sensor.

| | | SC.10 | | | | |
|---|---|---|---|---|---|---|
| | | none | low | med | high | cri |
| SC | none | 0.372 | 0.340 | 0.195 | 0.059 | 0.033 |
| | low | 0.279 | 0.328 | 0.254 | 0.088 | 0.049 |
| | med | 0.172 | 0.291 | 0.320 | 0.132 | 0.084 |
| | high | 0.142 | 0.268 | 0.330 | 0.153 | 0.106 |
| | cri | 0.116 | 0.251 | 0.341 | 0.169 | 0.122 |
| RSE | low | 0.366 | 0.339 | 0.199 | 0.062 | 0.034 |
| | med | 0.360 | 0.338 | 0.202 | 0.064 | 0.035 |
| | high | 0.358 | 0.337 | 0.203 | 0.065 | 0.036 |
| S | true | 0.366 | 0.339 | 0.199 | 0.062 | 0.034 |
| | false | 0.347 | 0.337 | 0.211 | 0.068 | 0.037 |

propagated conditional distributions are shown in Table 3. Given different states of RSE, probabilities for SC states are calculated. Notice that they are all high for the none state as states of other nodes are also affecting the SC. If S is false, though, $p$(SC = none) decreases. Similar probabilities can be calculated easily for other higher nodes. For instance, detection state transition to RSE can be calculated as $p$(RSE|RDS). Reasonably, from the table, if the detection state is low, RSE can be at high state, else RSE is at failing low state. Likewise, the propagation of risks to a series of other SCs (from Figure 2*b*) is also represented. For instance, at SC.10, probabilities of $p$(SC = low) and $p$(SC = med) are significantly higher. Note that impacts at attacked SC's RSE and S states do not play an important role. This can be seen from the equal probabilities across different states.

## Simulations

### *Types of Simulation*

Analyzing the cyber-physical model, impact on an SC is propagated through service times (see Figure 2*a*). Primary objectives are quantification and identification of possible problems. These would yield risk areas, impacts, and possible solutions for more resilient systems. Monte Carlo simulations (MCSs) are carried out on BNs, including a series of intersections as well as replications of complete BNs. MCSs generate probability distributions and expected utility as well as dispersion so that confidence intervals can be generated. A second approach generates a Bayesian framework for posterior probability of a critical node common among these signals, such as SA, considering it as a parameter.

This section presents numerical results for BNs with and without redundant surveillance systems. MCSs are run for 10,000 cycles which result in state probabilities, and in expected, and standard deviation of, vulnerabilities. Simulations are repeated 200 times to obtain distributions of these measures for CV market penetrations of $p$ = (0.01, 0.05, 0.10, 0.20, 0.50, 0.75, 0.90, 1.00), which is constituted by (CR = 0.80, EM = 0.03, FR = 0.07, TR = 0.10). Vehicle and pedestrian traffic are 95% and 5%, respectively. In Figure 3*a*, probabilities, expected value, and standard deviation of vulnerability of SC are presented. Boxplots are used to show the ranges within 200 replications, as metrics are assigned randomly from uniform distribution. Probabilities are used to calculate the moments. The probability of SC being at the no effect level is about 93% and about 6% at low impact. These values vary in the ranges 0.80–0.99 and 0–0.20, respectively, changing the central tendency and the dispersion of vulnerabilities. The expected value certainly falls mostly into the low impact ($> 0.1$) region. The median of standard deviations is about 0.9. Thus a simple confidence interval for mean level (0.37) with mean

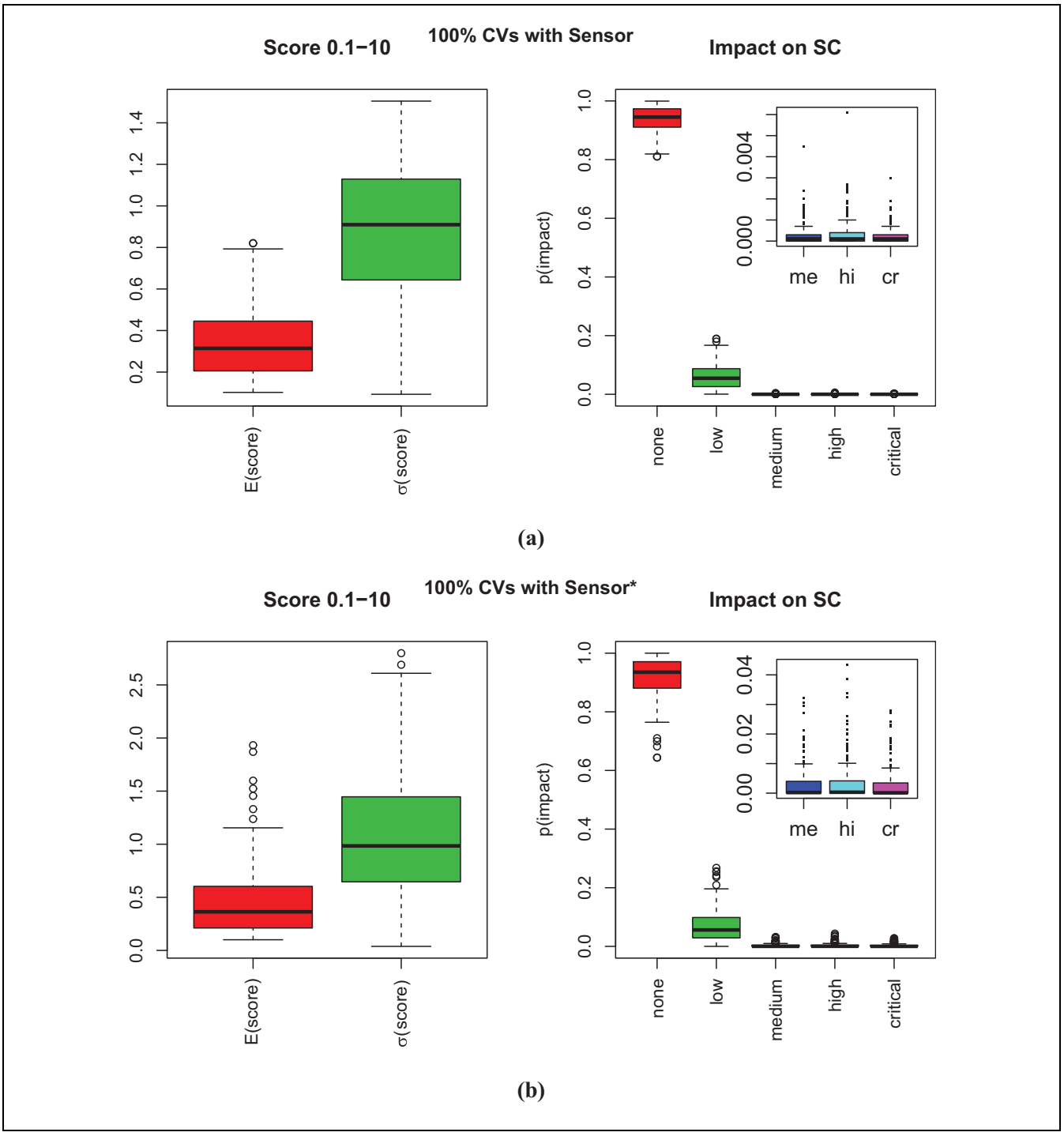



**Figure 3.** Simulated score values from BN with sensors.

standard deviation (0.93) $\mu \pm 2\sigma$ would be within (0, 2.23), which is still in the low impact scale.

Further simulations are carried out to check the effect of randomly generating all metric values. These values are only assigned for 200 replications but not for each node on BNs. Figure 3*b* shows somewhat higher expected values; however, much higher standard deviations with risk likelihoods vary more. Still, median values are very close; with the mean values (0.57, 1.32), the same confidence interval in this case would be (0, 3.20), very close to medium risk level. This could be due to not exploring enough of the metric ranges and resulting higher dispersions. Therefore, a completely random approach would give more robust results. Similar

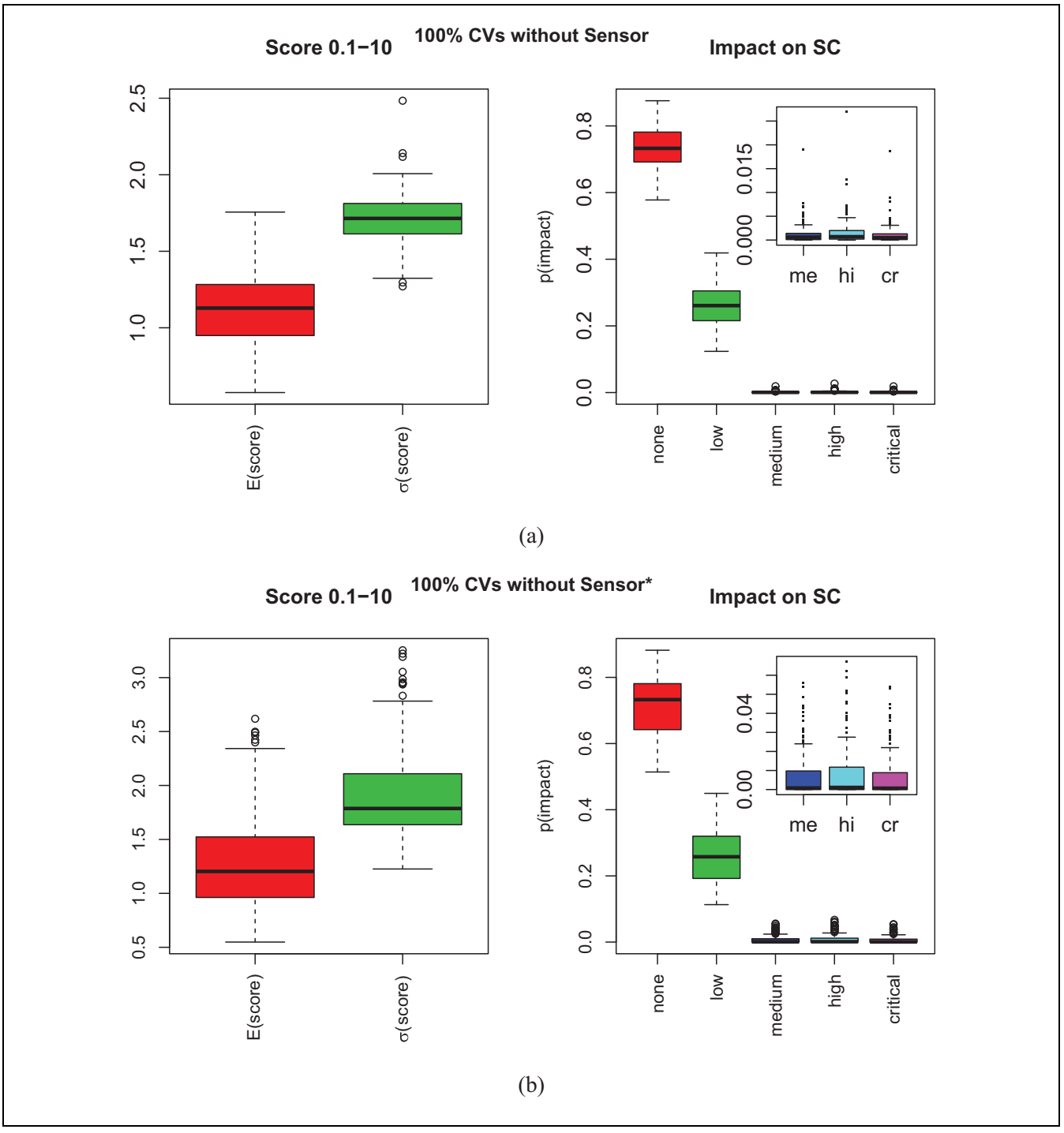



**Figure 4.** Simulated score values from BN without sensors.

results are demonstrated in Figure 4 for the without sensor case. They reveal much higher risk levels and variations. Risk likelihood is still mainly within low level; however, the low state is more probable than none. The confidence interval in this case would be (0,4.81), with mean and standard deviation values of 1.19 and 1.81, respectively. In this case vulnerability falls into the much more serious med level. As before, the less random version yields higher dispersion, with confidence interval (0, 5.03) with means 1.28 and 1.87. Furthermore, basic progression of the risk present on signal control to the next 10 signals is represented in Figure 2*b*. The vulnerability of SC and SC.10 signal controllers is presented in Figure 5. From the figure, it

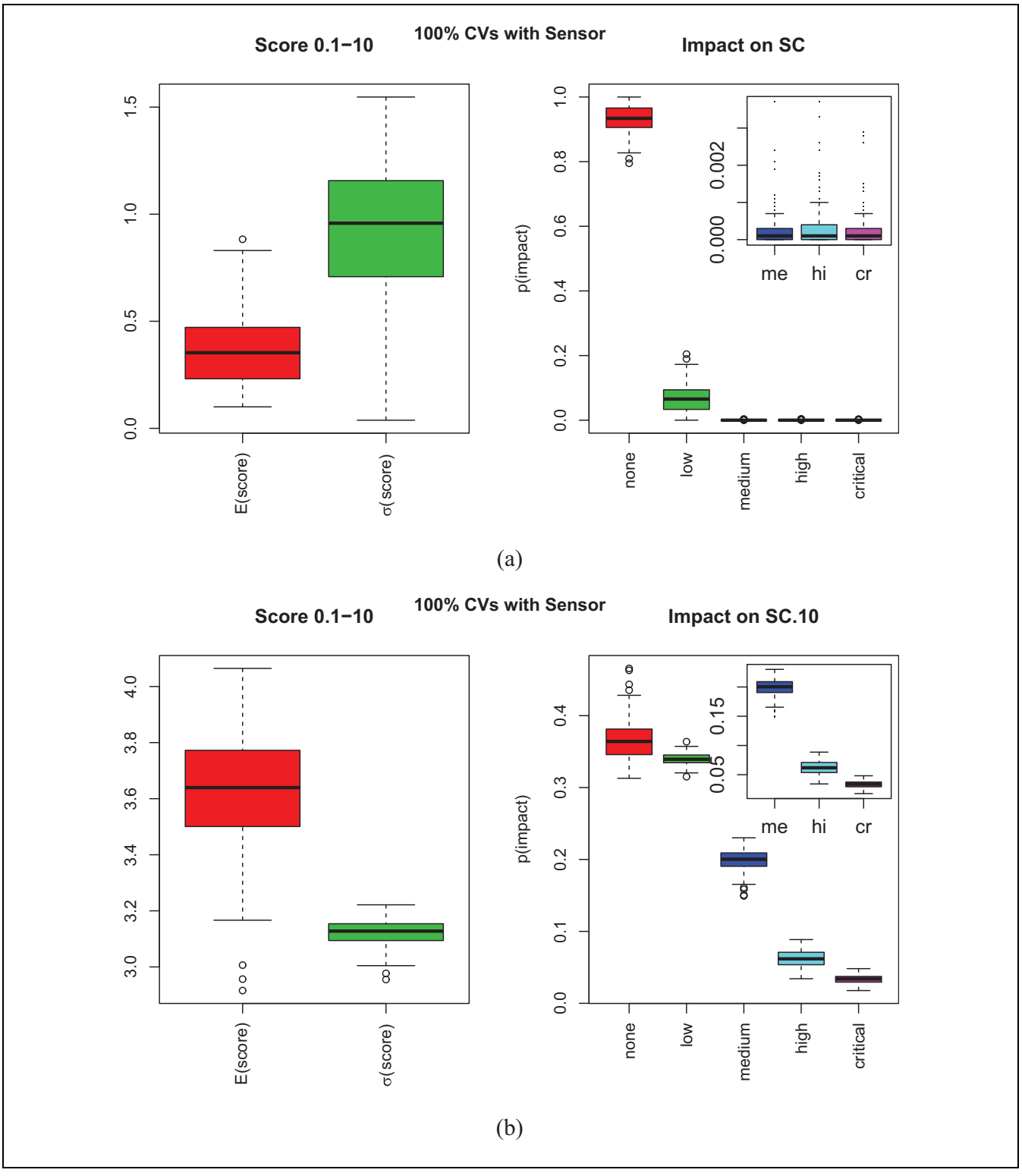



**Figure 5.** Simulated score values from BN with sensors.

is observed that the risk, on moving from SC to SC.10, increases in a serial scheme based on defined transition probabilities, which is intuitive. The average score standard deviation is about 3.1, with mean level 3.65. Thus, the vulnerability score is already very close to med level and confidence intervals would fall into all serious levels, med to high impact scales (0, 9.85). In this system, however, dependency is only through SC nodes, not

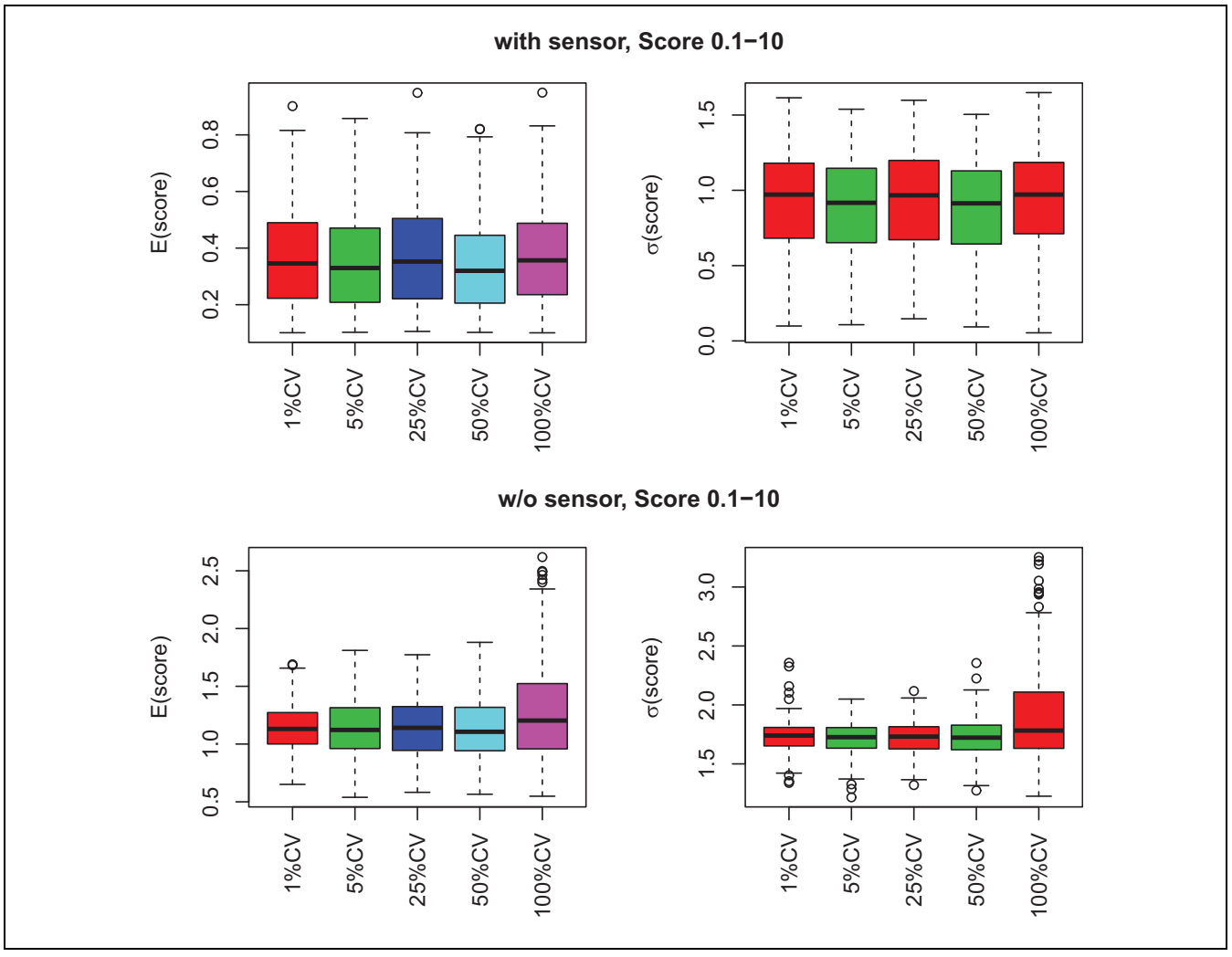


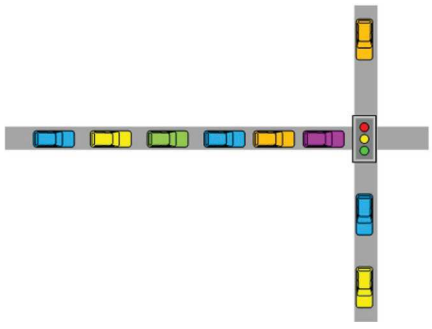

**Figure 6.** Risk values for SC at different %CV levels.

others. Thus, overall risk may change if other nodes are included.

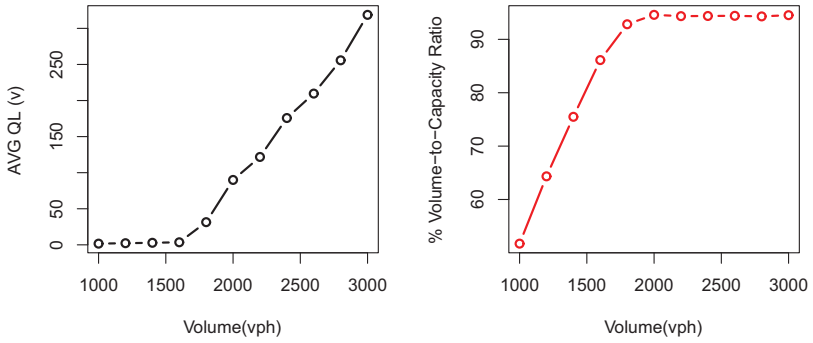
Figure 6 is given to demonstrate the impact of CV market penetration. This is incorporated as increasing likelihood of CVs in TC by multiplying unequipped modes with $(1-p)$ and weighing CVs with $p$. Thus, as $p$ increases, CV population will increase, resulting in more communications with RSE and SC. However, based on this method, CV percentage does not have a significant effect on SC vulnerability level. Certainly, it should be noted that a different incorporation (i.e., network design) might show otherwise.

## *Traffic Process Simulations*

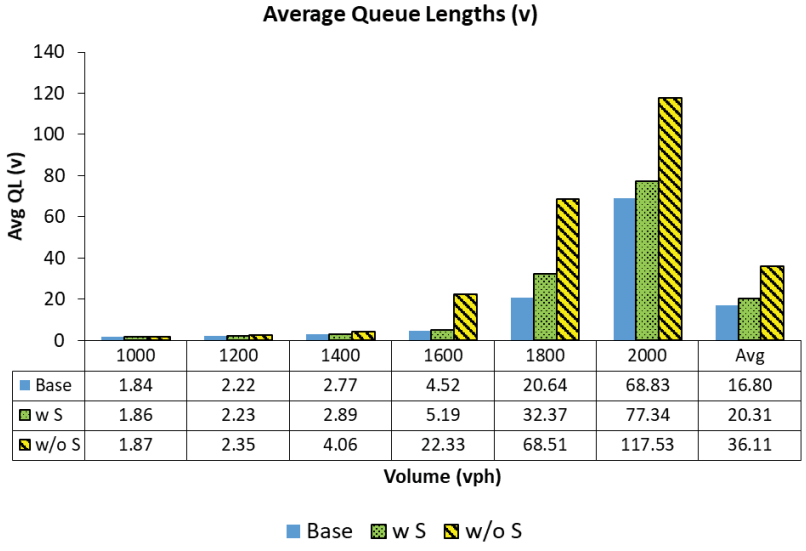
A possible quantification of the impact of state probabilities on an isolated signalized intersection is shown via traffic queue simulations using a ProModel Process Simulator. For simplicity, the signal control method is assumed to be fixed and communications are not included. Changes are incorporated only through service times. Average queue lengths are demonstrated for regular and affected scenarios with and without sensors. The intersection is designed with approaches that can accommodate a maximum of 130 average-length cars per approach (Figure 7*a*). For the simulation set up, first the saturation level is found. To compare with the results from microsimulations (*24*), an isolated intersection with two one-way approaches is designed with 45 s green for each approach and volumes = (500, 600, 700, …, 2000) vehicles per hour (vph) per approach. Similar results are observed with saturation at about 1000 vph per approach. Simulations are run for 1 h (40 cycles) and 100 replications. Figure 7*b* below shows volume versus average queue lengths as number of vehicles (v) and volume-to-capacity ratios (utilization). From the figure, the saturation point can be seen at close to 2000 vph with capacity of 23 vehicles per cycle and 1.95 seconds per



(a) A possible isolated intelligent signal




(b)




| | 1000 | 1200 | 1400 | 1600 | 1800 | 2000 | Avg |
|---|---|---|---|---|---|---|---|
| Base | 1.84 | 2.22 | 2.77 | 4.52 | 20.64 | 68.83 | 16.80 |
| w S | 1.86 | 2.23 | 2.89 | 5.19 | 32.37 | 77.34 | 20.31 |
| w/o S | 1.87 | 2.35 | 4.06 | 22.33 | 68.51 | 117.53 | 36.11 |

(c)

**Figure 7.** Process traffic simulation results.

vehicle (spv) discharge rate. Using the same volume rates, this time up to 2200 vph per intersection, possible interruptions are generated from the probability distribution BNs. Impacts are reflected on 1.95 spv, with (none, low, med, high, cri) = (1.95, 2.60, 3.90, 9.75, 19.5) spv and average probabilities, with sensors, of (0.930, 0.069, 0.0005, 0.0005, 0.0005) and, without sensors, of (0.730, 0.260, 0.003, 0.004, 0.003), respectively. Figure 7*c* demonstrates an overall summary of the impact of risk levels on queue lengths that are obtained from simulations which are medium level realistic between microscopic and point queue simulations. The figure provides the overall evolution of base performance measures for with sensor and without sensor scenarios. As would be expected, impact increases as volume gets higher. The impact on a single intersection is much higher, about 15% average queue length (QL) increase with a sensor. Without any sensor, changes are much higher with average 125% of average queue length across all volume levels.

## Conclusions

In this paper, models are developed based on BNs for possible attack risks on intelligent signals in a CV framework. From these models, risk probabilities and expected utilities (impacts) are deduced for SCs with and without redundant traffic surveillance systems. The impact of risks at an isolated signalized traffic intersection is quantified via simulations as average queue length differences, which can be interpreted as meaning higher cost, higher fuel consumption, and higher emissions. From simple simulations with and without redundant systems, the impact of risk is estimated as an increase of queues by

averages of 15% and 125%, respectively. Further improvements are possible via:

- Quantification of impacts of derived risks at signalized traffic networks via simulations as different performance measures
- Microscopic traffic simulation including communications with more realistic vehicle movements
- Expression of the systems as a flow network for possible attack paths to optimize sensor deployment and minimize communication delays
- Inclusion of alternative CV market penetration incorporation

A continuation study would aim to generate data using part real equipment and part simulations. Then, it would utilize this data to develop crucial detection models for critical components and generate mitigation efforts. It is essential to have optimum deployment as unnecessary control can result in communication delays, leading to problems for safety critical applications such as collision warning. As a systematic approach, similar methodology would be adopted for different ITS applications.

## Acknowledgments

This research is supported by the U.S. Department of Homeland Security Summer Research Team Program and was conducted at the Critical Infrastructure Resilience Institute, University of Illinois, Urbana-Champaign. It was managed by ORAU. The research is also partially supported by USDOT Regional University Transportation Center for Connected Multimodal Mobility and NSF Grant Nos. 1719501 and 1400991.

## Author Contributions

The authors confirm contribution to the paper as follows: study conception and design: GC; data collection: GC; analysis and interpretation of results: GC; draft manuscript preparation: GC. The author reviewed the results and approved the final version of the manuscript.

## References

1. Cárdenas, A. A., S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. *Proc., 6th ACM Symposium on Information, Computer and Communications Security*, ACM, 2011, pp. 355–366.
2. Kaiser, L. *Transportation Industrial Control System (ICS) Cybersecurity Standards Strategy 2013–2023*. Technical Report. National Highway Traffic Safety Administration, 2013.
3. National Highway Traffic Safety Administration. *Cybersecurity Best Practices for Modern Vehicles*. Technical Report No. DOT HS 812 333. National Highway Traffic Safety Administration, USDOT, 2016.
4. Beck, K. *Smart Security? Evaluating Security Resiliency in the U. S. Department of Transportation's Smart City Challenge*, 2017.
5. Petit, J., and S. E. Shladover. Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, No. 2, 2015, pp. 546–556.
6. Nicol, M. D. *Critical Infrastructure Resilience Institute*, 2016, talk, USCG.
7. Peisert, S., J. Margulies, D. M. Nicol, H. Khurana, and C. Sawall, Designed-In Security for Cyber-Physical Systems. *IEEE Security & Privacy*, Vol. 12, No. 5, 2014, pp. 9–12.
8. van der Heijden, R. W., S. Dietzel, T. Leinmüller, and F. Kargl. Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. *arXiv preprint arXiv:1610.06810*, 2016.
9. Al-Sultan, S., A. H. Al-Bayatti, and H. Zedan. Context-Aware Driver Behavior Detection System in Intelligent Transportation Systems. *IEEE Transactions on Vehicular Technology*, Vol. 62, No. 9, 2013, pp. 4264–4275.
10. Cao, P., E. Badger, Z. Kalbarczyk, R. Iyer, and A. Slagell. Preemptive Intrusion Detection: Theoretical Framework and Real-World Measurements. *Proc., 2015 Symposium and Bootcamp on the Science of Security*, ACM, 2015, p. 5.
11. Mitchell, R., and I.-R. Chen. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. *ACM Computing Surveys (CSUR)*, Vol. 46, No. 4, 2014, p. 55.
12. Humayed, A., J. Lin, F. Li, and B. Luo. Cyber-Physical Systems Security—A Survey. *arXiv preprint arXiv: 1701.04525, 2017*.
13. Ernst, J. M., and A. J. Michaels. Framework for Evaluating the Severity of Cybervulnerability of a Traffic Cabinet. *Transportation Research Record: Journal of the Transportation Research Board*, 2017. 2619: 55–63.
14. Sridhar, S., and M. Govindarasu. Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Transactions on Smart Grid*, Vol. 5, No. 2, 2014, pp. 580–591.
15. Sucasas, V., G. Mantas, F. B. Saghezchi, A. Radwan, and J. Rodriguez. An Autonomous Privacy-Preserving Authentication Scheme for Intelligent Transportation Systems. *Computers & Security*, Vol. 60, 2016, pp. 193–205.
16. CVRIA. *Physical Diagram of Intelligent Signal System*, 2015. http://local.iteris.com/cvria/html/applications. Accessed June 26, 2017.
17. NIST. *Common Vulnerability Scoring System*, 2017. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator. Accessed June 30, 2017.
18. Head, L., W. B. Zhang, G. Duncan, E. Raamot, and R. Jose. *MultiModal Intelligent Traffic Signal System Phase II: System Development, Deployment and Field Test-MMITSS*. Technical Report. Center for Transportation Studies, University of Virginia, 2016.
19. Huang, J., and D. M. Nicol. Evidence-Based Trust Reasoning. *Proc., 2014 Symposium and Bootcamp on the Science of Security*, ACM, 2014, p. 17.
20. Wan, J., D. Zhang, S. Zhao, L. Yang, and J. Lloret. Context-Aware Vehicular Cyber-Physical Systems with Cloud

Support: Architecture, Challenges, and Solutions. *IEEE Communications Magazine*, Vol. 52, No. 8, 2014, pp. 106–113.
21. MacKay, D. J. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003.
22. Barber, D. *Bayesian Reasoning and Machine Learning*. Cambridge University Press, 2012.
23. Højsgaard, S. Graphical Independence Networks with the gRain Package for R. *Journal of Statistical Software*, Vol. 46, No. 10, 2012, pp. 1–26.
24. Comert, G. Simple Analytical Models for Estimating the Queue Lengths from Probe Vehicles at Traffic Signals. *Transportation Research Part B: Methodological*, Vol. 55, 2013, pp. 59–74.

*The Standing Committee on Critical Transportation Infrastructure Protection (ABR10) peer-reviewed this paper (18-06284).*