MODELING AND QUANTIFYING

CYBER ATTACKS ON SIGNALIZED TRAFFIC NETWORKS

Jacquan Pollard, Gurcan Comert, and David M. Nicol

ENGINEERING AT ILLINOIS

INFORMATIONTRUST INSTITUTE

ABSTRACT

Transportation networks are considered as one of the critical physical infrastructures for resilient cities (cyber-physical systems (CPSs)). In efforts to minimize adverse effects, Department of Homeland Security works with the National Highway Traffic Safety Administration of the US Department of Transportation. This project proposes to investigate anomaly detection at transportation networks particularly involving signalized traffic intersections. For different types of cyber attacks defined in the literature, risk areas, cost of different attacks, mitigation techniques, and detection of abnormal messages within driver, vehicle, and infrastructure context will be modeled via probabilistic graphical models (e.g., Belief Networks) and traffic simulations with various scenarios. Based on the selected metrics, risk probabilities are calculated for signal controllers. Impact of these probabilities on an example signalized traffic network are quantified in terms of average intersection queue lengths and delays (time spent in queue and server). In addition, effect of having redundant traffic sensing systems on intersection performance measures is also demonstrated.

PROBLEM STATEMENT

The primary goal for this paper is to develop models for signal control state based on possible attack surfaces from intelligent traffic signal components.

Particularly,

(1) Develop connected vehicle based signal system model with cyber-physical representation

(2) Apply a probabilistic expert system for modeling anomalies and attacks (malicious messages/benign failures) are produced

(3) Quantify risks with respect to number of different traffic states (from parameters: market penetration rate, traffic composition (vehicles to pedestrians), volume versus control reliability) and redundant surveillance systems (sensors)

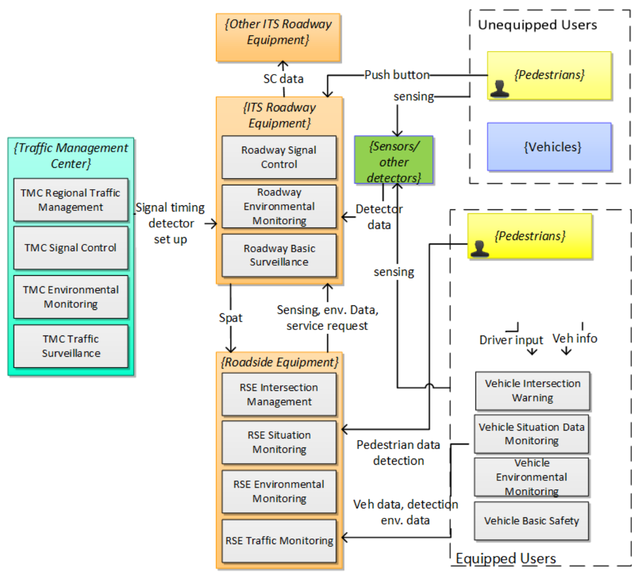


Fig 1. Intelligent Signal Infrastructure (CVRIA (2015))

METHODS

BELIEF NETWORKS

Belief (Bayesian) networks are graphical stochastic expert systems that depict conditional (in)dependences of probability distributions of interests such as complex joint distributions with high number of variables involving some conditional independences.

Probabilities in Eqn. (1) from BNs are propagated (posteriors) by the junction tree algorithm with $O(n^3)$ for marginal distributions. The algorithm actually yields the multiplication of conditional probabilities including the independences, thus, a simplified version.

The algorithm is on directed acyclic graphs first marries parent nodes, then triangulates and removes unnecessary links through generation of cliques and assignments, and message propagation (Barber (2012)).

Parent nodes such as p(WSA) require probability assumptions for uncertain evidence setting. Scales are shown in the Table 1 below.

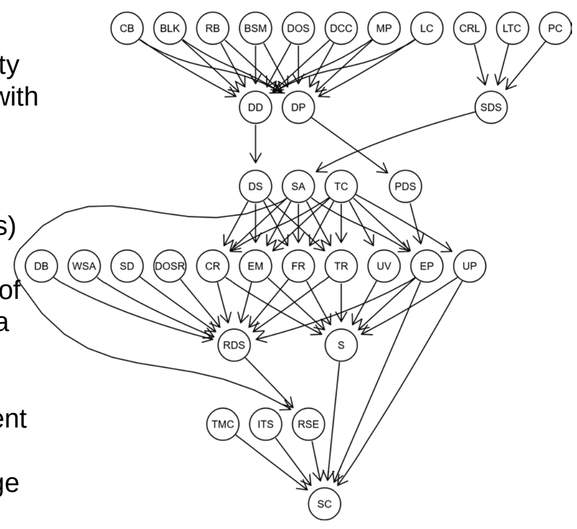


Fig 2. BN with additional surveillance (sensor)

Table 1. Attack surfaces and metrics (Petit and Shladover (2015))

Target	Attack Type	Feasibility	Metric	Detection	Metric
SA	LTC	low	(h,l,l)	med	(l,h,l)*(h,l,l)
	CRL	med	(l,h,l)	med	(l,h,l)*(l,h,l)
	PC	med	(l,h,l)	med	(l,h,l)*(l,h,l)
RSE	WSA	high	(l,l,h)	low	(h,l,l)*(l,l,h)
	DB	high	(l,l,h)	med	(l,h,l)*(l,l,h)
	SD	low	(h,l,l)	high	(l,l,h)*(h,l,l)
VEHs	CB	low	(h,l,l)	low	(h,l,l)*(l,h,l)
	BLK	med	(l,h,l)	low	(h,l,l)*(l,h,l)
	RB	low	(h,l,l)	low	(h,l,l)*(h,l,l)
	BSM	high	(l,l,h)	low	(h,l,l)*(l,l,h)
	DOS	high	(l,l,h)	low	(h,l,l)*(l,l,h)
	MP	high	(l,l,h)	med-high	(l,m,h)*(l,l,h)
	DCC	med	(l,h,l)	med	(h,l,l)*(l,h,l)
	LC	med	(l,h,l)	low	(h,l,l)*(h,l,l)
	DOSR	high	(l,l,h)	high	(l,l,h)*(l,l,h)

Table 2. Attack metrics and scales (NIST (2017))

Metric	Scale	Metric	Scale
low	25	none	1
medium	50	low	39
high	75	medium	69
		high	89
		critical	100

$$N = \{WSA, LTC, PC, DB, CRL, SD, DOSR, RB, DCC, LC, TC, UP, EP, CR, EM, FR, TR, UV, DD, PD, DS, PDS, RDS, SDS, RSE, S, ITS, TMC, SC\}$$

$$p(SC) = \sum_{N \setminus SC} \prod_{N \setminus SC} p(SC|pa(SC))$$

$$p(SC) = \sum_{\{S,RSE,\ldots,WSA\}} p(SC, S, \ldots, WSA) \quad (1)$$

$$p(SC) = p(SC|S, RSE, \ldots, WSA)p(S|UV, UP, EP, \ldots, TR) \ldots p(WSA)$$

SIMULATIONS

- Monte Carlo simulations (MCSs) are carried on BNs including series of intersections.
- BNs are simulated 10,000 times with 200 replications. CVs 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) car, emergency vehicles, freight, and transit respectively. Vehicle and pedestrian traffic are 95% and 5%.
- In order to address the sensitivity these probabilities are generated randomly from uniform distribution. Resulting expected utility for vulnerability are calculated out of 0-10 scale where up to 0.1 shows no risk/impact to 10 is highest vulnerability.
- Impact of derived risk probabilities on traffic are tested using a process simulator which can mimic horizontal queueing.

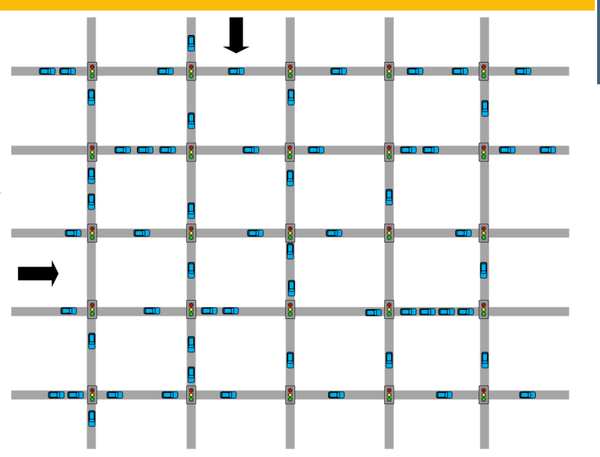


Fig 3. Network of Signalized Intersections

SIMULATIONS

- Set up: an isolated intersection was designed with 2 one-way approaches in order to find the saturation headway and volume.
- Pre-timed signal control with 45 seconds green and red phases was chosen to be able to compare with (Comert (2013)) performance measures.
- Very similar results are obtained with saturation headway 1.95 seconds/vehicle (spv) and volume between 900-1000 vehicle/hour (vph). Fig. 2. shows well known QL/Delay evolution with respect to volume. Rather nonlinear increase up to saturation and linear increase after saturation.

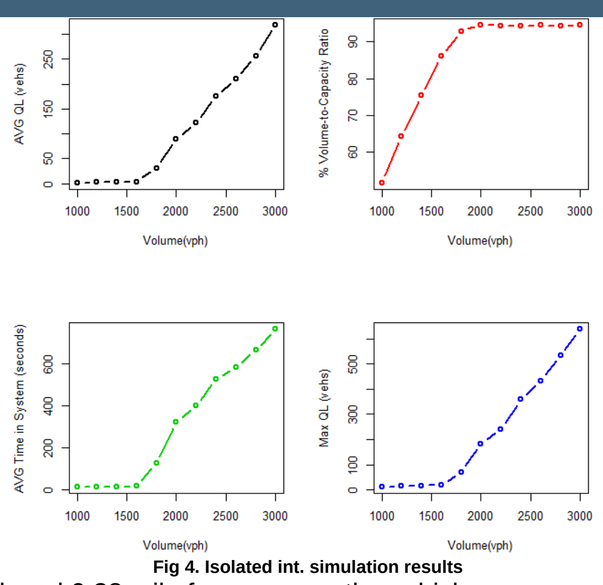


Fig 4. Isolated int. simulation results

- Signalized network includes 25 signals. Signal are placed 0.38 mile from one another which can accommodate 130 vehicle/approach and vehicles move exponentially with mean 46 seconds-30 mph average.
- Volumes levels 500,600,…,2000) vph/approach are used. Simulations are run for 1 hour with 100 replications.
- Impacts are reflected with {none, low, medium, high, critical} states {1.95,2.60,3.90,9.75,19.5} spv with average probabilities: with sensor {0.93,0.0685,0.00051,0.0005,0.00049} and without sensors {0.727,0.261,0.35,0.46,0.34}

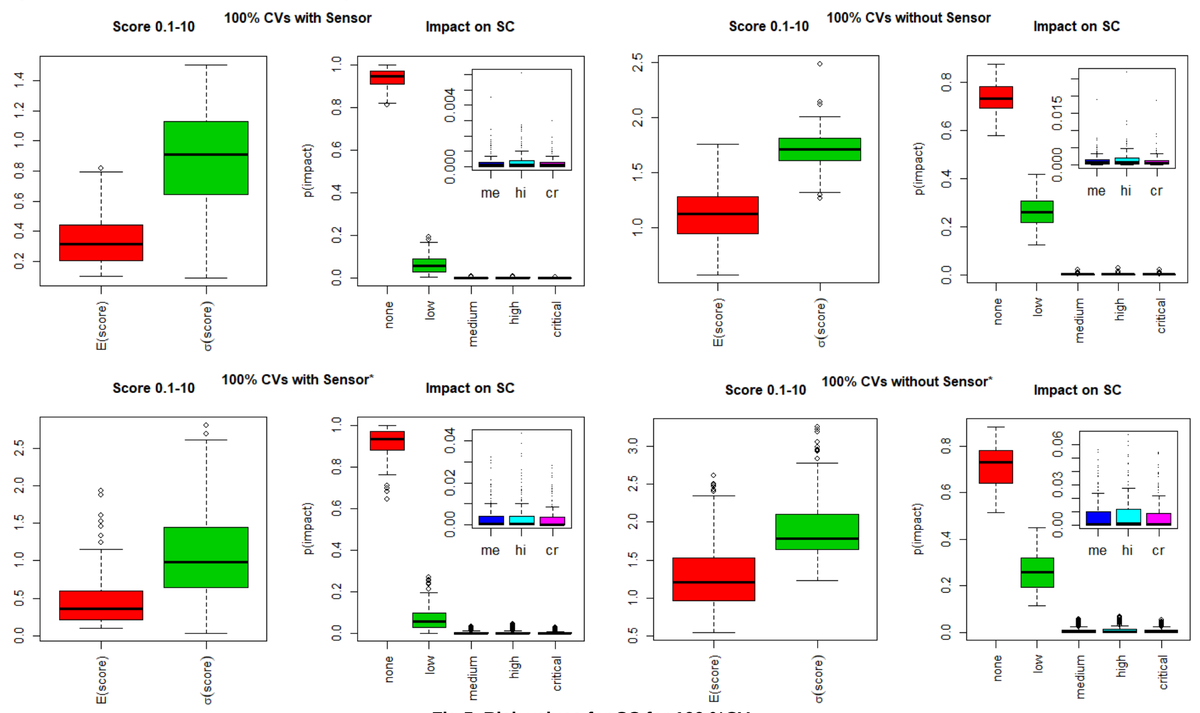


Fig 5. Risk values for SC for 100 %CV

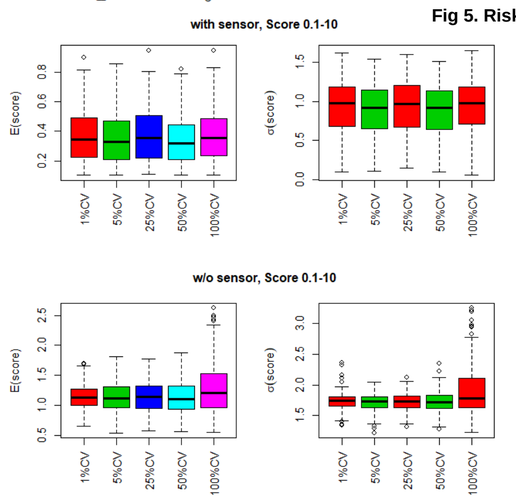
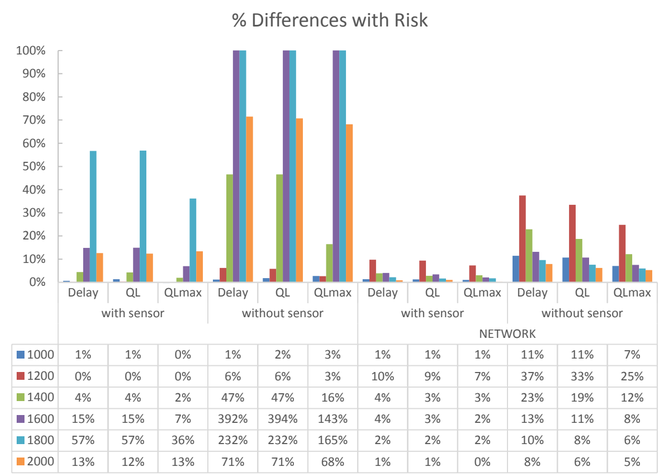


Fig 6. Risk values for SC at different %CV levels



	Delay	QL	QLmax	Delay	QL	QLmax	Delay	QL	QLmax	Delay	QL	QLmax
1000	1%	1%	0%	1%	2%	3%	1%	1%	1%	11%	11%	7%
1200	0%	0%	0%	6%	6%	3%	10%	9%	7%	37%	33%	25%
1400	4%	4%	2%	47%	47%	16%	4%	3%	3%	23%	19%	12%
1600	15%	15%	7%	392%	394%	143%	4%	3%	2%	13%	11%	8%
1800	57%	57%	36%	232%	232%	165%	2%	2%	2%	10%	8%	6%
2000	13%	12%	13%	71%	71%	68%	1%	1%	0%	8%	6%	5%

Fig 3. Intersection performance measure differences when risks are incorporated

CONCLUSIONS

- Analytical models for the attacks presented in Petit and Shladover (2015) are developed.
- Risk probabilities for any node on intelligent signal infrastructure can be calculated.
- Risks for signal controller are calculated w/o redundant traffic surveillance systems.
- Impacts of risk at signalized traffic networks are quantified as queue lengths and delays which can result as cost, fuel wastes, and emissions.
- At isolated signals w/o redundant systems can increase queues and delays by 15% and 125% respectively.
- At networks risk w/o redundant systems can increase queues and delays by 3% and 15% respectively. This can be due to low simulation run time.

FURTHER IMPROVEMENTS

- Microscopic traffic simulation including communications with more realistic vehicle movements.
- Expressing the systems as flow network for possible attack paths in order to optimize sensor deployment and minimize communication delays.

REFERENCES

1. Barber, D., 2012. Bayesian reasoning and machine learning. Cambridge University Press.
2. Comert, G., 2013. Simple analytical models for estimating the queue lengths from probe vehicles at traffic signals. Transportation Research Part B: Methodological 55, 59–74.
3. CVRIA, 2015. Physical diagram of intelligent signal system. http://local.iteris.com/cvria/html/applications, accessed: 2017-06-26.
4. NIST, 2017. Common vulnerability scoring system. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, accessed: 2017-06-30.
5. Petit, J., Shladover, S. E., 2015. Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems 16 (2), 546–556.

ACKNOWLEDGEMENTS

- This research is funded by Department of Homeland Security Summer Research Team Program for Minority Serving Institutions
- Critical Infrastructure Resilience Institute, ITI, University of Illinois, Urbana-Champaign

CSL: COORDINAT SCIENCE LA