Transportation Research Record

TRAJECTORY-BASED HIERARCHICAL DEFENSE MODEL TO DETECT CYBER-ATTACKS ON TRANSPORTATION INFRASTRUCTURE

--Manuscript Draft--

Full Title:	TRAJECTORY-BASED HIERARCHICAL DEFENSE MODEL TO DETECT CYBER-ATTACKS ON TRANSPORTATION INFRASTRUCTURE
Manuscript Number:	19-05008R1
Article Type:	Presentation Only
Order of Authors:	Wai Wong
	Shihong Huang
	Yiheng Feng
	Qi Alfred Chen
	Morley Mao
	Henry X Liu

TRAJECTORY-BASED HIERARCHICAL DEFENSE MODEL TO DETECT CYBER-ATTACKS ON TRANSPORTATION INFRASTRUCTURE

Extended Abstract
Paper No. 19-05008

Wai Wong
Department of Civil and Environmental Engineering, University of Michigan
2350 Hayward Street, Ann Arbor, MI, 48109
Email: waiwong@umich.edu

Shihong Huang
Department of Civil and Environmental Engineering, University of Michigan
2350 Hayward Street, Ann Arbor, MI, 48109
Email: edhuang@umich.edu

Yiheng Feng, Corresponding Author
Transportation Research Institute (UMTRI), University of Michigan
2901 Baxter Rd, Ann Arbor, MI, 48109
Email: yhfeng@umich.edu

Qi Alfred Chen
Department of Computer Science, University of California, Irvine
3062 Bren Hall, Irvine, CA, 92617
Email: alfchen@uci.edu

Z. Morley Mao
Department of Electrical Engineering and Computer Science, University of Michigan
2260 Hayward Street, Ann Arbor, MI, 48109
Email: zmao@umich.edu

Henry X. Liu
Department of Civil and Environmental Engineering, University of Michigan
Transportation Research Institute (UMTRI), University of Michigan
2350 Hayward Street, Ann Arbor, MI, 48109
Email: henryliu@umich.edu

Word count: 1688 words

ACKNOWLEDGEMENT
This research is funded by Mcity at University of Michigan. The views presented in this paper are those of the authors alone.

INTRODUCTION

The development of connected vehicles (CVs) provides a great opportunity for new vehicle-to-infrastructure applications, such as CV-based adaptive signal control algorithms *(1-9)*. Intelligent Traffic Signal System (I-SIG) *(9-11)*, as one of them, will be deployed in the USDOT CV deployment projects for real world implementation. However, such connectivity at transportation infrastructure also introduce potential vulnerabilities for cyber-attacks *(12)*. Feng et al. *(13)* showed that attacking CV-based adaptive signal control can cause 33.66% more delay. Chen et al. *(14)* performed a systematic analysis of vulnerability of I-SIG. They found that by adding only one falsified Basic Safety Message (BSM), the average delay was increased by 68% and the benefit of I-SIG could be completely reversed.

To overcome the cyber security issue and protect transportation infrastructures, some defense strategies have been proposed. In this study, indirect cyber-attacks, which refer to using falsified data to influence the decisions of infrastructure related applications are considered. An attack event is defined as a series of attacks (sending falsified BSMs) being launched over a period of time under the same CV identity. To make the data spoofing attack more realistic, it is assumed that with the protection of the Security Credential Management System *(15)*, the attacker is not able to send falsified data with multiple vehicle identities. Only one attack event can be launched at the same time. Typically, the objectives of attackers are unknown to defenders. Thus, as a defender, the objective is to design a generic defense framework that can identify each individual falsified trajectory data and remove it in real-time such that reliable CV data can be used for transportation infrastructure applications. This study, based on the knowledge of vehicle dynamics and trajectory cross-validation, proposes a generic, privacy-respecting and upgradable trajectory-based hierarchical defense (TBHD) framework to transportation cybersecurity. TBHD consists of three hierarchies. Level 1 is a pointwise checking that checks if data elements in the received BSMs fall within their feasible ranges. Level 2 is a multiple-point checking that checks if the consecutive BSMs of one CV obey the laws of physics. Level 3 is a multiple-trajectory checking that checks if two CVs' trajectories overlap with each other. Three sets of simulation studies were conducted to evaluate the performance of the defense framework at each level with different traffic demands and defense frequencies (DF). Results reveal that the proposed defense framework can detect most of the data spoofing attacks.

METHODOLOGY

The TBHD framework consists of three levels of defense. The three levels can be categorized as pointwise (Level 1), multiple-point (Level 2) and multiple-trajectory checking (Level 3).

Level 1 defense is designed based on the physical boundaries of vehicle dynamics, which checks if each element in the received BSMs of all the CVs falls within its feasible range. The location of a CV, (x, y), must fall within the road of interest (RoI) with a stretched boundary tolerance with a width of τ_{RoI}. The speed, v, must be between zero minus a small tolerance, τ_v and the free-flow speed, v_f, plus a small tolerance, τ_v. The acceleration, a, should fall into the range between minimum acceleration, a_{min}, minus a small tolerance, τ_a, and maximum acceleration, a_{max}, plus a small tolerance, τ_a. The heading of a CV, θ, must be in direction of its travelling approach, ϕ_i, $\forall i = 1, 2, 3\ and\ 4$, plus or minus a tolerance, τ_ϕ. The small tolerances, which are determined by users, account for the measurement errors of the GPS tracker, speedometer and accelerometer. A BSM violates any of these conditions will be categorized as an "attack"; otherwise a "non-attack".

Level 2 defense is developed based on equations of motion and the definitional equations of speed and acceleration, which checks if the consecutive BSMs of a CV obey the laws of physics.

Based on two consecutive snapshots (Δt = 0.1seconds), any consecutive BSMs of a CV do not follow these rules will be identified as an "attack"; otherwise a "non-attack". For instance, using the location information of a CV at time $t-1$ and t, the speed of that CV at time t can be estimated based on the definitional equations. The absolute difference between the estimated speed and the measured speed should be less than a threshold. The acceleration of a CV at time t can be checked in a similar manner. Assuming a constant acceleration in small time period Δt, the location, speed and acceleration information of a CV at time $t-1$ can be input into the equations of motion to predict the location of the CV at time t. The absolute difference between the predicted and measured location should be smaller than a threshold. Similarly, the predicted speed of a CV at time t can be checked in a similar manner. The values of the thresholds can be determined by users. They can be set to the values of 99% or 99.9% percentiles of the histograms constituted by the absolute differences of the predicted and measured quantities based on historical data or experiment.

Level 3 defense is formulated based on cross-validation of multiple CV trajectories, which checks if two CVs overlap with each other. A trajectory is classified into four bins: real-vehicle, unclassified, suspicious-fake-vehicle and identified-fake-vehicle. When a snapshot is taken, all the new CVs entering the communication range will first be placed in the unclassified bin. Each CV is checked if it overlaps with other CVs and re-distributed to the four bins according to a set of redistribution rules. A CV moved to the identified-fake-vehicle bin is identified as an "attack"; and a CV moved to the real-vehicle bin is identified as a "non-attack". In contrast, both the identities of CVs in the unclassified and suspicious-fake-vehicle bins are uncertain. To keep sufficient CV information while avoiding potential cyber-attacks, CV data from the unclassified and real-vehicle bins will be passed to applications, and CV data from both the suspicious-fake-vehicle and identified-fake-vehicle bins will be blocked.

FINDINGS

A random attack model that consists three levels of attacks, which are level 0.5 attack, level 1.5 attack and level 2.5 attack are introduced. Level 0.5 attack is the most generic random attack model that randomly generates BSMs based on a set of distributions. Level 1.5 attack randomly generates BSMs that can pass level 1 defense, while level 2.5 attack randomly generates BSMs that can pass levels 1 and 2 defense. Three sets of independent simulations (i.e., level 0.5 attack vs. level 1 defense, level 1.5 attack vs. level 2 defense, and level 2.5 attack vs. level 3 defense) are conducted to evaluate the performance of each of the three levels of defenses. Four different metrics, detection rate (DR), false alarm rate (FAR), false negative rate (FNR), and mean time to detection (MTTD), are adopted for the evaluation.

Simulation results for level 0.5 attack vs. level 1 defense with varying demand at fixed DF revealed that the DR, FAR and FNE were almost 100%, 0% and 0%, respectively, across different demands. The approximately constant MTTD of 0.45 sec at different traffic volume suggested that the MTTD should be independent of traffic demand. The almost 100% DR, 0% FAR and 0% FNR across different DF at a fixed demand demonstrated that the level 1 defense could accurately identify "attacks" for any defense frequency. The decreasing relationship between MTTD and DF suggested that the higher the DF the more responsive the level 1 defense would be.

Simulation results for level 1.5 attack vs. level 2 defense at fixed DF showed that the DR and FNR were extremely close to 100% and 0% for all the traffic demands, respectively. The FARs were about 0.4%. Nevertheless, such a small FAR is usually not damaging to a system. In return, the small sacrifice in efficiency could suppress the relatively damaging FNR to 0%. The MTTD, remaining at about 0.55 seconds for all traffic demand, was insensitive to the change of traffic

volume. The DR and FNR were almost 100% and 0%, respectively, for varying DF at fixed demand. The FARs were approximately 0.4% with different traffic volumes. The decreasing relationship between MTTD and DF suggested that the higher the DF the more responsive the level 2 defense would be.

Simulation results for level 2.5 attack vs. level 3 defense at fixed DF demonstrated that level 3 defense performed better at a higher traffic volume. The DR increased with volume from around 40% to 66%. The FNRs decreased from about 2.3% to 0.04% were minimal. The FARs decreased from about 4.4% to 1.9%. The MTTD also dropped steadily from about 12.5 seconds at 200 veh/hour/lane to 8.6 seconds at 500 veh/hour/lane. For the simulation series with varying DF at fixed demand, it was found that as the DF increased from 0.1Hz to 10Hz, the DR increased sharply from about 22% to 62%, and the FNR and MTTD dropped from around 2.3% to 0.4% and from about 15 seconds to 9 seconds, respectively. Though the FAR fluctuated slightly between 1% and 3%, it kept a general decreasing trend with DF. These suggested that the DF should always be set as high as possible to maximize the performance of level 3 defense.

CONCLUSIONS

This study proposes a generic defense framework for detecting and filtering trajectory data spoofing cyber-attacks of any objective and protecting the infrastructure related applications of any type to its greatest extent. The TBHD framework consists of three levels of defense. Level 1 defense is a pointwise checking that checks if data elements in the received BSMs fall within their feasible ranges. Level 2 defense is a multiple-point checking that checks if the consecutive BSMs of a CV obey the laws of physics. Level 3 defense is a multiple-trajectory checking that checks if two CVs overlap with each other. Comprehensive simulation studies revealed that the proposed TBHD framework is able to filter most of the data spoofing attacks.

This study assumed that an attacker has a limited budget and can initiate an attack event once at a time. However, it is possible that an attacker can afford a higher budget to launch multiple attack events simultaneously. Thus, one possible future research direction is to upgrade the TBHD framework to defense multiple falsified vehicle attacks.

REFERENCES

1. Goodall, N., B. Smith and B. Park. Traffic Signal Control with Connected Vehicles. *Transportation Research Record: Journal of the Transportation Research Board*, 2013, 2381: 65-72.
2. Priemer, C. and B. Friedrich. A Decentralized Adaptive Traffic Signal Control using V2I Communication Data. *Intelligent Transportation Systems*, 2009, ITSC'09. 12th International IEEE Conference on. IEEE, 2009: 1-6.
3. Lee, J., B. Park and I. Yun. Cumulative Travel-time Responsive Real-time Intersection Control Algorithm in The Connected Vehicle Environment. *Journal of Transportation Engineering*, 2013, 139(10): 1020-1029.
4. Guler, S.I., M. Menendez and L. Meier. Using Connected Vehicle Technology to Improve the Efficiency of Intersections. *Transportation Research Part C: Emerging Technologies*, 2014, 46: 121-131.

5. He, Q., K.L. Head and J. Ding. PAMSCOD: Platoon-based Arterial Multi-modal Signal Control with Online Data. *Transportation Research Part C: Emerging Technologies*, 2012, 20(1): 164-184.
6. He, Q., K.L. Head and J. Ding. Multi-modal Traffic Signal Control with Priority, Signal Actuation and Coordination. *Transportation Research Part C: Emerging Technologies*, 2014, 46: 65-82.
7. Pandit, K., D. Ghosal, H.M. Zhang and C.N. Chuah. Adaptive Traffic Signal Control with Vehicular Ad Hoc Networks. *IEEE Transactions on Vehicular Technology*, 2013, 62(4): 1459-1471.
8. Li, W. and X.J. Ban. Traffic Signal Timing Optimization in Connected Vehicles Environment. *Intelligent Vehicles Symposium (IV)*, IEEE, 2017: 1330-1335.
9. Feng, Y., K.L. Head, S. Khoshmagham and M. Zamanipour. A Real-time Adaptive Signal Control in A Connected Vehicle Environment. *Transportation Research Part C: Emerging Technologies*, 2015, 55: 460-473.
10. Feng, Y., M. Zamanipour, K.L. Head and S. Khoshmagham. Connected Vehicle–Based Adaptive Signal Control and Applications. *Transportation Research Record: Journal of the Transportation Research Board*, 2016, 2558: 11-19.
11. Sen, S. and K.L. Head. Controlled Optimization of Phases at An Intersection. *Transportation Science*, 1997, 31(1): 5-17.
12. Ghena, B., W. Beyer, A. Hillaker, J. Pevarnek and J.A. Halderman. Green Lights Forever: Analyzing the Security of Traffic Infrastructure. *WOOT 14*, 2014:7-7.
13. Feng, Y., S. Huang, Q.A. Chen, H.X. Liu and Z.M. Mao. Vulnerability of Traffic Control System under Cyberattacks with Falsified Data. *Transportation Research Record: Journal of the Transportation Research Board*, 2018, p.0361198118756885.
14. Chen, Q.A., Y. Yin, Y. Feng, Z.M. Mao and H.X. Liu. Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. *Network and Distributed Systems Security (NDSS) Symposium 2018*.
15. Whyte, W., A. Weimerskirch, V. Kumar and T. Hehn. A Security Credential Management System for V2V Communications, *2013 IEEE Vehicular Networking Conference*, 2013: 1-8.