01 Jan 2023

Securing The Transportation Of Tomorrow: Enabling Self-Healing Intelligent Transportation

Elanor Jackson

Sahra Sedigh Sarvestani
Missouri University of Science and Technology, sedighs@mst.edu

Recommended Citation

E. Jackson and S. S. Sarvestani, "Securing The Transportation Of Tomorrow: Enabling Self-Healing Intelligent Transportation," *Proceedings - International Computer Software and Applications Conference*, pp. 946 - 949, Institute of Electrical and Electronics Engineers, Jan 2023.
The definitive version is available at https://doi.org/10.1109/COMPSAC57700.2023.00126

2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) | 979-8-3503-2697-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/COMPSAC57700.2023.00126

Securing the Transportation of Tomorrow: Enabling Self-Healing Intelligent Transportation

Elanor Jackson and Sahra Sedigh Sarvestani
Department of Electrical and Computer Engineering
Missouri University of Science and Technology
Rolla, MO, USA
{efj5n8, sedighs}@mst.edu

***Abstract*—The safety of autonomous vehicles relies on dependable and secure infrastructure for intelligent transportation. The doctoral research described in this paper aims to enable self-healing and survivability of the intelligent transportation systems required for autonomous vehicles (AV-ITS). The proposed approach is comprised of four major elements: qualitative and quantitative modeling of the AV-ITS, stochastic analysis to capture and quantify interdependencies, mitigation of disruptions, and validation of efficacy of the self-healing process. This paper describes the overall methodology and presents preliminary results, including an agent-based model for detection of and recovery from disruptions to the AV-ITS.**

***Index Terms*—autonomous vehicles, intelligent transportation system, self-healing, modeling, cyber attack, survivability**

I. Introduction

Autonomous vehicles (AVs) are emerging as a means of increasing the efficiency, sustainability, and safety of ground transportation. They carry the potential to reduce emissions and traffic congestion, decrease the likelihood of accidents, and make transportation more accessible to disabled individuals. Achieving this vision requires large-scale and complex infrastructure that includes sensors, road-side units, real-time communication capacity, data centers, and cloud computing. The intelligent infrastructure required to support the deployment of AVs is denoted as AV-ITS.

The computing and communication that imbues the AV-ITS with intelligence creates vulnerabilities absent from less advanced transportation. Cyber components can fail as a result of design flaws or undetected error, and the integral role played by the cyber infrastructure makes it a high-value target for potential bad actors. Ever present is deterioration and exposure, which can lead to accidental failures in physical components. The dynamic, episodically-connected nature of AVs presents a unique challenge to resilience.

This paper describes doctoral research that aims to enable self-healing AV-ITS by detecting disruptions, predicting failure sequences, and deploying recovery mechanisms to maintain system integrity. While the focus of this research is on fortifying systems against cyber attacks, it also applies to disruptions that result from accidental failure. The proposed research entails the investigation of vulnerabilities, which informs the prioritization of disruptions based on their probable consequences. The results will be validated through high-fidelity simulation. To date, the research has led to the creation of a purpose-built, open source simulation environment that enables fault injection testing for survivability evaluation. The insights gained from this research will help fortify the AV-ITS against future disruptions, through criticality analysis, with the goal of increasing survivability.

II. Research Challenges and Related Work

In an intelligent transportation system (ITS), advanced computing and communication technologies are used for decision support, anomaly detection, and mitigation of failure. The American National Standards Institute (ANSI) and National Institute of Standards and Technology (NIST) have published standards for ITSs, traffic and travel information, controller area networks (CAN), and cyber security frameworks, e.g., ANSI ASTM E2213-03(2018) specification provides standards for dedicated short range communication (DSRC), medium access control, and physical layer specifications for telecommunication and information exchange between roadside and vehicle systems [1]. The NIST cybersecurity framework is being adopted for ITS applications [2], [3].

The CARMA Program [4], spearheaded by the U.S. Department of Transportation (USDOT), investigates and develops new technology with cooperative driving automation (CDA), which requires greater connectivity between regular vehicles and AVs and increases the reliance on ITS infrastructure. In coordination with USDOT, Tampa, Wyoming, and New York City have participated in the Connected Vehicle Pilot Program - a feasibility study for emerging ITS technology [5]. The pilots, which concluded in Dec. 2021, collectively focused on increasing compliance with traffic laws, pedestrian safety, and monitoring of long-haul trucking over major highways. The program has yielded a treasure trove of data.

This paper builds on review of available literature on the dependability and security of AVs [6]. Notable studies include [7]–[9], which investigate the cyber threats associated with the ITS. Particularly relevant is [9], which discusses possible solutions, but acknowledges that there is not a ’one size fits all’ mitigation or fortification strategy for cyber attacks. Another example is [10], which uses game theory to identify

The authors gratefully acknowledge funding from NSF DUE-1742523, DEd GAANN awards P200A180095 and P200A210121, and the Intelligent Systems Center at the Missouri University of Science and Technology.

979-8-3503-2697-0/23/$31.00 ©2023 IEEE
DOI 10.1109/COMPSAC57700.2023.00126

distinguishing features of new threats. A self-healing ITS could adjust mitigation and fortification strategies based on the specific disruption, possibly allowing for creative solutions to disruption events.

Survivability, defined as a measure of the critical functionality retained by a system under failure or attack, is a key measure for AV-ITS; as the system is required to function despite anomalies. Recent studies on this topic were found to be scarce; the most notable study [11] is from 2004.

Ref. [12] proposes a method to optimize self-adaptation in automotive systems by reconfiguration that compares alternatives with respect to how well they maintain safety-related objectives. A simulation-based approach to achieving self-healing in interdependent power networks is investigated in [13]. Chaos theory is used in [14] to evaluate self-adaptive and self-healing systems.

The doctoral research described in this paper aims to bridge these gaps by illuminating the operation and failure of ITS components, identifying interdependencies among them, and quantifying the effect of failure or attack on critical functions. The insights gained will inform mechanisms that enable self-healing that aims to maximize the survivability of the AV-ITS.

III. Methodology

Figure 1 depicts the operation of the AV-ITS as a cycle that begins with monitoring for disruption. Detection is followed by classification, which informs failure prediction and mitigation, with the goal of deploying resources that interrupt and/or limit the impact of the disruption. The system then enters a recovery stage.

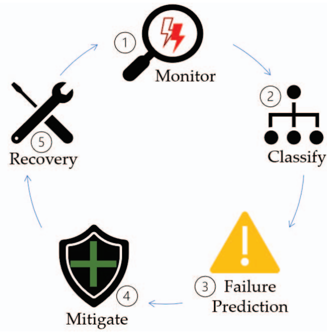

Fig. 1. Operation of an intelligent, self-healing AV-ITS.

The ultimate goal of the proposed research is to increase the resilience of AV-ITS against failure and attack, by guiding each stage of the cycle and equipping the AV-ITS with up-to-date information about potential disruptions, mitigation strategies, failure paths, and recovery strategies. Four research tasks will be carried out to this end.

Task 1: Qualitative Modeling The proposed research began with the study of models, methods, and tools available for analysis of AV-ITSs. The fundamental challenge we identified is the abundance of interdependencies among and between cyber and physical components. Understanding the interdependencies can illuminate possible disruption vectors and areas of vulnerability. To this end, we plan to create a generic and extendable depiction of the AV-ITS and detail the functionality of each component and any interactions with other components, vulnerabilities, and associated standards.

Task 2: Stochastic Quantitative Modeling In this stage, we plan to quantify interdependencies [15]–[18], predict resulting failure paths, and evaluate survivability for the system. We plan to use Petri nets and Markov reward models to capture the relationships and uncertainties involved and to employ neural networks to predict failure propagation. We will build on a significant body of similar analyses for other intelligent critical infrastructure, most prominently smart grids [19].

Task 3: Mitigation of Disruptions The mitigation strategy will be informed by the results of the first two research tasks. The understanding gained will be used to identify, isolate, and mitigate the effects of specific vulnerabilities. We will create a recommendation system to determine which mitigation strategies should be deployed based on the disruption, system resources, and predicted failure sequence(s). We will investigate correlations among failures and apply heuristics to optimally fortify the system. The classification of disruption and mitigation strategies, respectively, will be evaluated in terms of response time, dimensionality, and accuracy.

Task 4: Self-Healing Model To demonstrate the effectiveness of the proposed self-healing AV-ITS, we will create a model that abstracts relevant AV-ITS components and accurately reflects interactions with the disruption detection, classification, and recommendation system. Response time is vital for the AV-ITS application; these systems would need to operate in near real-time and without burdening the AV-ITS elements or altering their operation outside of the scope of disruption prevention and mitigation. To evaluate the impact of the self-healing AV-ITS, we can compare the operation of a basic AV-ITS with an augmented version that includes monitoring, classification, and mitigation. Metrics will include availability and survivability.

A. Validation

A high-fidelity simulation environment has been created for validation of the proposed approach. Simulation environments allow for safe, cost-effective, and repeatable testing and promote collaboration between researchers through a shareable platform. A plenitude of literature examines reliability and availability of individual components and protocols of the ITS through Veins (Vehicle in-Network Simulation) [20]. An exhaustive list of publications is available at [21]. While simulation platforms such as Veins, CARMA and Car Learning to Act (CARLA) exist, we found that current simulation environments do not have fault injection testing natively built into the platform. Fig. 2 depicts the environment we have created to remedy this problem. We enable fault injection for survivability analysis by integrating three open-source simulation tools: CARLA, Autoware Autonomous Driving Stack, and Robot Operating System Penetration Testing Tool (ROSPenTo). An in-depth review of AV simulators and our purpose-built simulation environment can be found in [22].

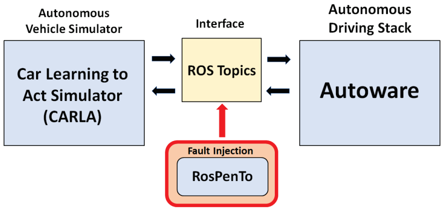

Fig. 2. Functional block diagram of the simulation environment.

IV. Results to Date

As of the date of submission, Task 1 and part of Task 4 have been completed. Specifically, we have created a) a generic and extensible abstraction of the AV-ITS, along with documentation of standards, component-level interactions, and vulnerabilities; and b) an agent-based model of the AV-ITS that abstracts the core-functionality of each component.

Agent-based modeling was chosen because it allows each component in the AV-ITS to be modeled as an independent agent within a larger system, facilitating focus on specific aspects of the AV-ITS. The agent-based model, which serves as the basis for evaluating the self-healing AV-ITS, is described in the remainder of this section.

A. Agents

The proposed model includes three agent populations, representing the vehicle, the pedestrian, and intelligent infrastructure that is represented by a roadside unit (RSU), respectively. Each agent population hosts a dynamic number of agents, each of which are independent and autonomous and possess decision-making capability [23]. The agents interact with one another over distinct communication paths, specifically, vehicle-to-pedestrian (V2P) and pedestrian-to-vehicle (P2V); vehicle-to-vehicle (V2V); and infrastructure-to vehicle (I2V) or vice-versa (V2I). These agent interactions can be seen in Fig. 3.

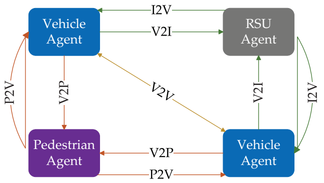

Fig. 3. Communications in the proposed AV-ITS model.

B. Agent State Chart

Each agent is based on the same state chart (depicted in Fig. 4), which includes the Vulnerable, Disrupted, AttemptingDefense, PartialRecovery, and Defunct states. The state chart reflects the high-level stages of a disruption: normal operation, impacted but unaware, aware of disruption and attempting defense, and recovering or non-operational. Each state is described below.

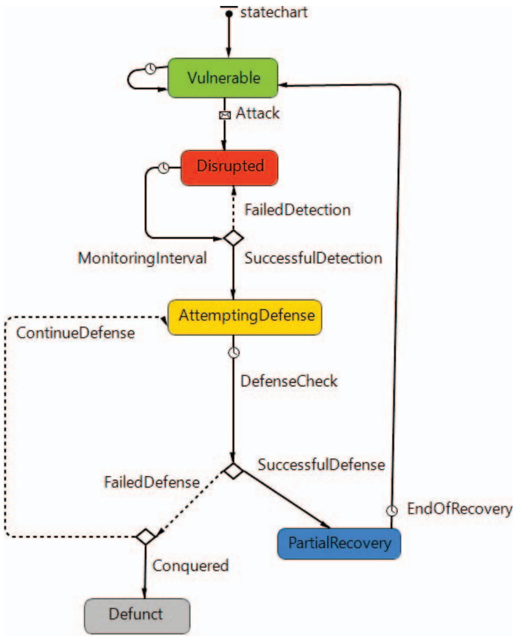

Fig. 4. State chart for each agent.

- **Vulnerable:** Each agent begins in a *fully operational* state, where it is vulnerable to disruption. Disruptions are passed from one agent to the next when they communicate. At this stage of the research, we assume that an arbitrarily selected agent is the initial origin of a disruption. Each agent has a probability of *InfectionProbability* of receiving a message that will cause it to transition to the Disrupted state.
- **Disrupted:** When an agent has fallen victim to a disruption that it has not yet detected. This is similar to the latent period of a virus. In this state, the agent can spread the disruption to other agents by communicating with them. In the Disrupted state, an agent scans for anomalies every *MonitoringInterval* time units. The interval should be chosen such that it does not cause undue burden on the agent's operation. Detection of the disruption, which occurs with a probability of *ProbabilitySuccessfulDetection* in each interval, triggers a transition to the AttemptingDefense state.
- **AttemptingDefense:** The agent is aware of and has successfully detected an active disruption and is attempting to defend against the disruption by employing mitigation strategies. The CheckDefense interval dictates how often the agent will scan for disruption eradication, which happens with a a probability of *ProbabilitySuccessfulDefense*. Upon successful defense the agent will transition to the PartialRecovery state. If the defense is not successful, there is a probability of *DefunctProb* that the agent will become non-operational, and transition to the Defunct state.
- **PartialRecovery:** Reflects an agent that is undergoing

necessary repairs due to a disruption. Recovery of all functionality returns the agent to the (fully functional, but) Vulnerable state. At this stage of the research, the duration to full recovery is assumed to be uniformly distributed between *RecoveryMin* and *RecoveryMax*.

- **Defunct:** When an agent being damaged beyond repair and has been permanently removed from the AV-ITS. This is a terminal state.

C. Scalability and Refinement

The model also allows for continuous improvement. For example, states can be added to reflect the communication or actions of agents at a more granular level. A disrupted agent can send an alert to warn surrounding vehicles of an active disruption, allowing them to heighten their defenses and decrease their *MonitoringInterval* in an effort to mitigate any potential disruptions. Furthermore, agents can be added to represent other components of the AV-ITS.

V. Conclusion and Specific Contributions

Our proposed research will significantly extend the existing body of work by creating a mathematical framework that enables a self-healing AV-ITS to increase the survivability of critical infrastructure. The findings can be applied to other disciplines that utilize autonomous technologies, such as advanced manufacturing, while enabling better understanding of other large-scale and complex infrastructures, such as smart grids and intelligent water distribution networks.

Large-scale use of AVs is inevitable. The proposed research can contribute to the safety and security of systems that employ this emerging technology. Understanding interdependencies is key to predicting and mitigating the effects of disruption, which in turn enables resilience. Justifiable reliance on AVs carries the promise of greater sustainability and safety for ground transportation and can be of immeasurable value to communities large and small.

References

[1] American National Standards Institute, "ASTM E2213-03(2018): Standard Specification For Telecommunications And Information Exchange Between Roadside and Vehicle Systems - 5-GHz Band Dedicated Short-Range Communications (DSRC), Medium Access Control (MAC), And Physical Layer (PHY) Specifications," 2018, accessed: 04-16-2023. [Online]. Available: https://www.astm.org/e2213-03r18.html

[2] U.S. Department of Transportation Intelligent Transportation Systems Joint Program Office ITS Cybersecurity Research Program, "General cybersecurity references and guides," 2023, accessed: 04-15-2023. [Online]. Available: https://www.its.dot.gov/research_areas/cybersecurity/guides.htm

[3] National Institute of Standards and Technology, "Cybersecurity framework," 2023, accessed: 04-15-2023. [Online]. Available: https://www.nist.gov/cyberframework

[4] U.S. Department of Transportation Federal Highway Administration, "CARMA program overview," 2023, accessed: 04-14-2023. [Online]. Available: https://highways.dot.gov/research/operations/CARMA

[5] ——, "Intelligent transportation systems connected vehicle pilots," 2023, accessed: 02-01-2023. [Online]. Available: https://www.its.dot.gov/pilots/index.htm

[6] J. L. King, E. Jackson, C. Brinker, and S. Sedigh Sarvestani, "Wheel tracks, rutting a new Oregon trail: A survey of autonomous vehicle cybersecurity and survivability analysis research," ser. Advances in Computers. Elsevier, 2023, vol. 130.

[7] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Trans on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[8] B. Zeddini, M. Maachaoui, and Y. Inedjaren, "Security threats in intelligent transportation systems and their risk levels," *Risks*, vol. 10, no. 5, 2022.

[9] J. Harvey and S. Kumar, "A survey of intelligent transportation systems security: Challenges and solutions," in *Proc IEEE Intl Conf on Big Data Security on Cloud (BigDataSecurity)*, 2020, pp. 263–268.

[10] H. Sedjelmaci, M. Hadji, and N. Ansari, "Cyber security game for intelligent transportation systems," *IEEE Network*, vol. 33, no. 4, pp. 216–222, 2019.

[11] J. Waite, M. Benke, N. Nguyen, M. Phillips, S. Melton, P. Oman, A. Abdel-Rahim, and B. Johnson, "A combined approach to ITS vulnerability and survivability analyses," in *Proc IEEE Conf on Intelligent Transportation Systems*, 2004, pp. 262–267.

[12] B. Klöpper, S. Honiden, J. Meyer, and M. Tichy, "Planning with utility and state trajectory constraints in self-healing automotive systems," in *Proc IEEE Intl Conf on Self-Adaptive and Self-Organizing Systems*, 2010, pp. 74–83.

[13] E. Pournaras, M. Ballandies, D. Acharya, M. Thapa, and B.-E. Brandt, "Prototyping self-managed interdependent networks - self-healing synergies against cascading failures," in *Proc IEEE/ACM 13th Intl Symp on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, 2018, pp. 119–129.

[14] M. A. Naqvi, S. Malik, M. Astekin, and L. Moonen, "On evaluating self-adaptive and self-healing systems using chaos engineering," in *Proc IEEE Intl Conf on Autonomic Computing and Self-Organizing Systems (ACSOS)*, 2022, pp. 1–10.

[15] E. Casalicchio and E. Galli, "Metrics for quantifying interdependencies," in *Critical Infrastructure Protection II*, M. Papa and S. Shenoi, Eds. Springer US, 2008, pp. 215–227.

[16] S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001.

[17] Y. Wang, J.-Z. Yu, and H. Baroud, "Quantifying the interdependency strength across critical infrastructure systems using a dynamic network flow redistribution model," in *Proc 30th European Safety and Reliability Conf and 15th Probabilistic Safety Assessment and Management Conf*, Nov 2020.

[18] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety*, vol. 121, pp. 43–60, 2014.

[19] K. Marashi, S. Sedigh Sarvestani, and A. R. Hurson, "Quantification and analysis of interdependency in cyber-physical systems," in *Proc 3rd Intl Workshop on Reliability and Security Aspects for Critical Infrastructure (ReSA4CI '16)*, Toulouse, France, Jun. 2016.

[20] C. Sommer, R. German, and F. Dressler, "Bidirectionally Coupled Network and Road Traffic Simulation for Improved IVC Analysis," *IEEE Trans on Mobile Computing (TMC)*, vol. 10, no. 1, pp. 3–15, January 2011.

[21] "Veins publications webpage," 2022, accessed: 04-16-2023. [Online]. Available: https://veins.car2x.org/publications/

[22] E. Jackson, C. Brinker, J. King, A. Muecke, S. Sedigh Sarvestani, and A. R. Hurson, "A simulation environment for fault injection studies of autonomous vehicles," *IEEE Intelligent Transportation Systems Magazine*, 2023, under review.

[23] C. M. Macal, "Tutorial on agent-based modeling and simulation: Abm design for the zombie apocalypse," in *Proc Winter Simulation Conference*, 2018.