Verifiable Autonomy Architecture

Written proposals are limited to 2 pages of technical content and up to 3 pages of appendix material that includes labor rates and hours, a current CV, and a summary of related projects. Selection of approximately 18 - 20 proposals will be based upon participant experience, proposed approach, and time available.

Research Objectives

1. **Examine correctness of service implementations and tie to assume/guarantee framework**
2. **Analysis of systems consisting of mixed continuous and discrete dynamics (hybrid systems) by using reachability, falsification, or other verification approaches**
3. **Construct a probabilistic model of subsystems and perform analysis using probabilistic model checking to determine robustness of components**
4. **Analyze system framework for security vulnerabilities**

Project Description

Introduction

We propose to explore falsification techniques for the analysis of hybrid systems. Using our previous work and developed tools, we propose to address both safety and security analysis of software controlled hybrid dynamical systems. We expect the research to yield techniques which can be used to analyze relevant subsystems of UxAS and other generic cyber-physical systems.

Specifically, we are interested in improving the existing automatic falsification methods and investigating their applicability in finding security vulnerabilities of controllers under attack. We model the system under test/attack as a sampled data control system (SDCS), where the controller program periodically samples and actuates a black model of the plant (a hybrid dynamical system). Finally, we want to benchmark such grey-box falsification techniques on UxAS sub-systems. To accomplish these objectives, we propose the below directions.

- *Automatic falsification*: Apply grey-box falsification techniques to UxAS subsystems.
- *Plant Models*: Investigate standardized models for hybrid dynamical systems which are conducive to falsification analysis. The models will be constructed using the available black box plant simulators or data.
- *Security Analysis*: Transform the problem of searching for attack signals, (which can compromise the safe operation of the system) into a falsification problem.

Automatic falsification has been explored in our previous works [1, 2, 3]. Construction of piecewise affine (PWA) plant models for reachability analysis has been explored in [4] with preliminary results. Security analysis for linear systems has been explored in [5, 6].

Background And Challenges

Reachability analysis of hybrid systems is a undecidable for all but the simplest kind [7]. Existing analysis can be partitioned into verification [8, 9, 10, 11, 12] and falsification techniques [13, 14, 15]. The verification procedures use over-approximations to verify a given property whereas current falsification techniques are comparable to testing methodologies and search for concrete violations of the given property.

We are interested in analyzing hybrid systems which result due to the pairing of software controllers with continuous dynamical systems. These are commonly modeled as sampled data control systems.

Sampled Data Control System (SDCS) consists of two components, as illustrated in Figure 1. (a) A discrete time plant model P , and (b) a controller implementation C described by a program whose semantics are formally defined. Finally, the closed-loop parallel composition assumes that the continuous plant has been discretized with the controller's sampling period

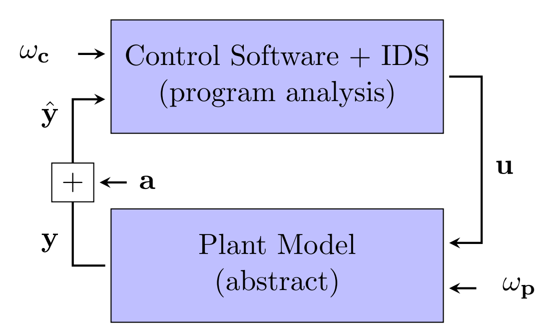

Figure 1: Closed loop symbolic execution.

Δ_t. The SDCS model allows for modeling of measurement noise at the controller and plant disturbances using exogenous input ω_c and ω_p. Additionally, the generic attack model is described as an additive input $\mathbf{a}$ to the plant's output $\mathbf{y}$, at the sensor.

Existing analysis for software controlled plants separately tests the software controller and the plant. To test an SDCS, existing tools require its translation to hybrid automata representations (which can be prohibitive to construct), their performance suffers. Moreover, existing security analyses do not address such systems. A scalable and combined analysis is desirable as it avoids false positives. To achieve this, we propose building up on our earlier work of symbolic-numeric falsification [3]. The extension will be investigated by incorporating different models for the plant. In the past, PWA models have been proposed for modeling hybrid dynamical systems (surveyed in [16]), and their verification studied in [17, 18, 19, 20]. As the individual models are linear, they are amenable to formal analysis. Moreover, recent work on the formal analysis of neural networks has been explored using SMT solvers in [21, 22, 23, 24]. Due to recent advances in non-linear SMT solvers, we would like to explore such models in the present framework of falsification. Such symbolic models can be generated automatically or semi-automatically and can be composed with control code and model checked using mature model checkers [25].

Proposed Research

In our prior research, we have explored the problem of falsification in hybrid systems from the perspective of white/grey/black box testing using a combination of off-the-shelf optimization engines [1], multiple shooting and counter-example guided abstraction refinement (CEGAR) procedure [2]. This formed the basis for combined symbolic analysis of programs and black box analysis of hybrid systems for falsification analysis of sampled data control systems in [3]. Using these techniques, we propose to address the safety and security analysis for control system implementations specific to UxAS.

Safety Analysis of Sampled Data Control Systems We want to investigate the specific challenges that a complex software architecture like UxAS presents to the symbolic-numeric falsification analysis. We also want to explore relational PWA models of plants, specifically built for the purpose of reachability analysis. Relational abstractions [26] and our previous research [27]. Treating the system as a black box, we split the problem into (a) modeling the behavior of the system using a piecewise affine discrete time model and (b) encoding the search for falsification as a bounded model checking problem. Such a model is specialized for the given property. SMT solvers and optimization techniques can be used to model check the resulting system. Furthermore, we would like to explore models based on machine learning in the same vein using non-linear SMT solvers [28].

Security Analysis of Sampled Data Control Systems

We propose to extend the falsification framework to find attack signals. We focus on the most general attack model, where the sensor can be compromised. The model also includes an intrusion detection system, which further constraints on the attack signal, thereby focusing the search for non-trivial attacks. Using the falsification framework developed for searching exogenous disturbances, we propose to find attack signals.

References Cited

[1] A. Zutshi, S. Sankaranarayanan, J. V. Deshmukh, and J. Kapinski, “A trajectory splicing approach to concretizing counterexamples for hybrid systems,” in *IEEE Conf. on Decision and Control (CDC)*. IEEE Press, 2013.

[2] ——, “Multiple shooting, cegar-based falsification for hybrid systems,” in *Proceedings of the 14th International Conference on Embedded Software*. ACM, 2014, p. 5.

[3] A. Zutshi, S. Sankaranarayanan, J. V. Deshmukh, and X. Jin, “Symbolic-numeric reachability analysis of closed-loop control software,” in *Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control*. ACM, 2016, pp. 135–144.

[4] A. Zutshi, “Reachability analysis of cyber-physical systems using symbolic-numeric techniques,” Ph.D. dissertation, 2016.

[5] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. J. Pappas, “Robustness of attack-resilient state estimators,” in *ICCPS’14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)*. IEEE Computer Society, 2014, pp. 163–174.

[6] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, “Attack-resilient state estimation in the presence of noise,” in *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*. IEEE, 2015, pp. 5827–5832.

[7] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya, “What’s decidable about hybrid automata?” in *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*. ACM, 1995, pp. 373–382.

[8] A. Tiwari, “Hybridsal relational abstracter,” in *International Conference on Computer Aided Verification*. Springer, 2012, pp. 725–731.

[9] X. Chen, E. Ábrahám, and S. Sankaranarayanan, “Taylor model flowpipe construction for non-linear hybrid systems,” in *Real-Time Systems Symposium (RTSS)*. IEEE, 2012, pp. 183–192.

[10] G. Frehse, C. L. Guernic, A. Donzé, S. Cotton, R. Ray, O. Lebeltel, R. Ripado, A. Girard, T. Dang, and O. Maler, “Spaceex: Scalable verification of hybrid systems,” in *CAV*, ser. Lecture Notes in Computer Science, vol. 6806. Springer, 2011, pp. 379–395.

[11] M. Althoff and G. Frehse, “Combining zonotopes and support functions for efficient reachability analysis of linear systems,” in *Decision and Control (CDC), 2016 IEEE 55th Conference on*. IEEE, 2016, pp. 7439–7446.

[12] P. S. Duggirala, S. Mitra, M. Viswanathan, and M. Potok, “C2e2: a verification tool for stateflow models,” in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2015, pp. 68–82.

[13] Y. Annpureddy, C. Liu, G. Fainekos, and S. Sankaranarayanan, *S-taliro: A tool for temporal logic falsification for hybrid systems*. Springer, 2011.

[14] A. Donzé, "Breach, a toolbox for verification and parameter syntohesis of hybrid systems," in *Computer Aided Verification*. Springer, 2010, pp. 167–170.

[15] T. Dreossi, T. Dang, A. Donzé, J. Kapinski, X. Jin, and J. V. Deshmukh, "Efficient guiding strategies for testing of temporal properties of hybrid systems," in *NASA Formal Methods*. Springer, 2015, pp. 127–142.

[16] S. Paoletti, A. L. Juloski, G. Ferrari-Trecate, and R. Vidal, "Identification of hybrid systems a tutorial," *European journal of control*, vol. 13, no. 2-3, pp. 242–260, 2007.

[17] B. Yordanov, G. Batt, and C. Belta, "Model checking discrete-time piecewise affine systems: application to gene networks," in *Control Conference (ECC), 2007 European*. IEEE, 2007, pp. 2619–2626.

[18] B. Yordanov and C. Belta, "Formal analysis of discrete-time piecewise affine systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 12, pp. 2834–2840, 2010.

[19] X. D. Koutsoukos and P. J. Antsaklis, "Safety and reachability of piecewise linear hybrid dynamical systems based on discrete abstractions," *Discrete Event Dynamic Systems*, vol. 13, no. 3, pp. 203–243, 2003.

[20] G. Batt, C. Belta, and R. Weiss, "Model checking genetic regulatory networks with parameter uncertainty," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2007, pp. 61–75.

[21] L. Pulina and A. Tacchella, "Challenging smt solvers to verify neural networks," *AI Communications*, vol. 25, no. 2, pp. 117–135, 2012.

[22] ——, "Never: a tool for artificial neural networks verification," *Annals of Mathematics and Artificial Intelligence*, vol. 62, no. 3-4, pp. 403–425, 2011.

[23] ——, "Checking safety of neural networks with smt solvers: a comparative evaluation," in *Congress of the Italian Association for Artificial Intelligence*. Springer, 2011, pp. 127–138.

[24] G. Katz, C. Barrett, D. Dill, K. Julian, and M. Kochenderfer, "Reluplex: An efficient smt solver for verifying deep neural networks," *arXiv preprint arXiv:1702.01135*, 2017.

[25] D. Kroening and M. Tautschnig, "Cbmc–c bounded model checker," in *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, 2014, pp. 389–391.

[26] A. Tiwari, "Hybridsal relational abstracter," in *Computer Aided Verification*, ser. CAV'12. Springer-Verlag, 2012, pp. 725–731.

[27] A. Zutshi, S. Sankaranarayanan, and A. Tiwari, "Timed relational abstractions for sampled data control systems," in *Computer Aided Verification*. Springer, 2012, pp. 343–361.

[28] S. Gao, S. Kong, and E. M. Clarke, "dreal: An smt solver for nonlinear theories over the reals," in *International Conference on Automated Deduction*. Springer, 2013, pp. 208–214.

Principal Investigators

- Prof.Miroslav Pajic *(Citizenship Status:)*
- Dr.Aditya Zutshi *(Citizenship Status: Non-Immigration F-1 VISA, Indian citizen)*

CV

(updated: 10th March, 2017)

EDUCATION

University of Colorado, Boulder *May 2011 - July 2016*
Ph.D in Electrical and Electronics Engineering
Dissertation: Reachability Analysis of Cyber-Physical Systems using Symbolic-Numeric Techniques.
Adviser: Prof. Sriram Sankaranarayanan (Dept. of Computer Science)

University of Colorado, Boulder *Aug 2009 - May 2011*
M.S. in Electrical and Electronics Engineering
GPA: 3.80/4

Manipal University, Manipal, India *Aug 2003 - May 2007*
Bachelor of Engineering in Electronics & Communications
GPA: 8.43/10

PUBLICATIONS

Symbolic-Numeric reachability analysis of closed-loop control software. [Best Student Paper Award]
Aditya Zutshi, Sriram Sankaranarayanan, Jyotirmoy V. Deshmukh and Xiaoqing Jin
In Proceedings of the 19th International Conference on Hybrid Systems: Computation and Control (HSCC) (pp. 135-144). ACM, 2016.

Multiple shooting, CEGAR-based falsification for hybrid systems. [Best Paper Award]
Aditya Zutshi, Sriram Sankaranarayanan, Jyotirmoy V. Deshmukh, and James Kapinski.
In Proceedings of the 14th International Conference on Embedded Software (EMSOFT), p. 5. ACM, 2014.

A trajectory splicing approach to concretizing counterexamples for hybrid systems.
Aditya Zutshi, Sriram Sankaranarayanan, Jyotirmoy V. Deshmukh, and James Kapinski.
In 52nd IEEE Conference on Decision and Control (CDC), pp. 3918-3925. IEEE, 2013.

Timed relational abstractions for sampled data control systems.
Aditya Zutshi, Sriram Sankaranarayanan, and Ashish Tiwari
In Computer Aided Verification (CAV) (pp. 343-361). Springer Berlin Heidelberg

AWARDS & HONORS

Selected for French-American Doctoral Exchange (FADEx 2016: Cyber-physical Systems)
Best Paper Awards (EMSOFT 2014, HSCC 2016)
Manipal Inst. of Tech Scholarship (2003-04, 2004-05)

PROJECTS

Current

- **PWA-Modeling for Falsification:** We are working on improving the search for unsafe behaviors in black box dynamical systems by using symbolic methods. Using regression on numerical simulations, we build Piece-Wise Affine models. SMT solvers and linear programming is used to model check the PWA models. The generated counterexamples guide the falsification of safety properties.

Completed

- **S3CAM-X:** A tool to find unsafe behaviors in closed loop control software. We augmented S3CAM with symbolic software analysis to automatically generate test cases and find unsafe behaviors in grey-box closed loop control software (white-box control software + black-box hybrid dynamical systems). The usefulness of the approach was demonstrated by finding 'bugs' in several benchmarks.

- **S3CAM:** A tool to find violations of safety properties in black box descriptions of continuous hybrid dynamical systems. We proposed trajectory splicing to automatically search for error trajectories using only numerical simulations. A combination of multiple shooting and Counter-Example Guided Abstraction Refinement (CEGAR) was used.

- **Falsification using Trajectory Optimization:** We developed automatic falsification techniques based on multiple shooting and trajectory optimization. The aim was to find violations of safety properties in hybrid automata. The prototype used off-the-shelf optimization engines.

- **Timed Relational Abstractions:** We devised timed relational abstractions for sampled-data control systems: a combination of continuous hybrid dynamical systems and discrete controllers. We used interval arithmetic to compute verified (bounded matrix exponential) solutions to linear differential equations in conjunction with SMT solvers to model check their properties.

The implementations of the above projects can be found at: `https://github.com/zutshi`

TALKS

Reachability Analysis of Cyber-Physical Systems, French-American Doctoral Exchange Seminar (FADEx), July 2016

Symbolic-Numeric Reachability Analysis of Closed-Loop Control Software, April 2016.

- Robert Bosch GmbH, Renningen, Stuttgart, Germany
- Centre d'intgration (CEA), Palaiseau, France
- HSCC 2016, Vienna, Austria

Beyond single shooting: Iterative approaches to falsification, ACC 2015, Chicago, USA, July 2015.

Multiple Shooting, CEGAR-based Falsification for Hybrid Systems, EMSOFT 2014, New Delhi, India, Oct. 2014.

Falsification of safety properties for Hybrid Systems using trajectory splicing, Charles University, Prague, Czech Republic, Dec. 2013.

A Trajectory Splicing Approach to Concretizing Counterexamples for Hybrid Systems, CDC 2013, Florence, Italy, Dec. 2013.

Timed Relational Abstractions For Sampled Data Control Systems, MVD 2012, The University of Kansas, Lawrence, Kansas, USA, Sept. 2012

RESEARCH EXPIRIENCE

Duke University ***(Postdoctoral Researcher)*** Feburary 2017 - Present
Adviser: Prof.Miroslav Pajic *Durham, NC*
Security of cyber physical systems.

Toyota Technical Center ***(Internship)*** August 2014 - December 2014
Mentors: Dr.Jyotirmoy Deshmukh and Dr.James Kapinski *Gardena, CA*
Work published in HSCC 2016.

Toyota Technical Center ***(Internship)*** January 2013 - April 2013
Mentors: Dr.Jyotirmoy Deshmukh and Dr.James Kapinski *Gardena, CA*
Work published in CDC 2013 and EMSOFT 2014.

INRIA ***(Internship)*** July 2012 - August 2012
Mentor: Dr.Bertrand Jeannet *Grenoble, Rhone-Alpes, France*
Worked on abstract acceleration of loops describing discrete dynamical systems.
Used linear algebra techniques to soundly summarize loops.

SRI International ***(Internship)*** May 2011 - August 2011
Mentor: Dr.Ashish Tiwari *Menlo Park, CA*
Work published in CAV 2012.

PROFESSIONAL DEVELOPER EXPERIENCE

Toshiba August 2007 - July 2009
Associate Software Engineer *Bangalore, Karnataka, India*

· *Toshiba Media Framework* (based on OpenMax IL): Worked on implementation and test suite design. Developed GTK+ based GUI to demo the framework usage.
· *Full Segment ISDB-T(Integrated Services Digital Broadcasting - Terrestrial)*: Worked on design and implementation of OpenMAX IL components.

Roles Undertaken: designing, prototyping, implementing, testing, debugging and documenting.

Budget Justification [[Max91,500]]

Labor rate(s) and hours for proposed participants.

A. Senior Personnel

A1. Includes PI at 10% CY.

Aditya Zutshi XX hrs @ $XX
Miroslav Pajic XX hrs @ $XX

E. Travel

1) NC - OH $\$400 * 4 = \$1600$
2) S5 Conference $\$400$

Hotels/Car/etc

hotel: 150/day, apts: 1k/mo
car: 600/mo, may-aug: 2631