Verifiable real-time coordination for safe cooperative driving

CENIIT Project Final Report

Mikael Asplund <mikael.asplund@liu.se>

May 7, 2021

Introduction

Connected and autonomous vehicles (CAV) have the potential to radically transform the transportation sector to become more sustainable and more efficient. These cyber-physical systems have been studied and developed for decades, but in recent years we have seen a much more rapid development with real-world deployments and testbeds. However, there are a number of very hard problems that have yet to be solved relating to fault tolerance and security.

The overreaching ambition of this project has been to advance the knowledge on how to develop reliable and secure collaborative algorithms for safety-critical cyber-physical systems. By combining formal verification principles and methods for distributed algorithms with novel coordination protocols, we have contributed to the development of better, more secure and safer software. We have developed new coordination protocols, new formalisms for modelling and specifying their correctness, and significantly advanced the state of the art with regards to cybersecurity in the domain.

Summary of the most important scientific results

The project resulted in 9 journal publications and 17 peer-reviewed conference contributions in top-tier venues such as ACM TCPS, IEEE VNC, and Elsevier Computer Communications. We proceed to describe five important scientific results from the project.

Vehicular communication We have studied attack models and security mechanisms in vehicular communication. In particular, using platooning as a case study, we were able to characterise how different attack types affect system safety [13]. Later, we proposed the Vouch and Vouch+ protocols [10,4] that mitigate such attacks by means of location verification mechanisms. Recently we have leveraged formal verification techniques to analyse and formally prove security properties (and identify weaknesses) of communication protocols that are currently in pre-standardisation phase[1].

Formal model of coordination Fault-tolerant coordination of autonomous and semi-autonomous vehicles is an extremely challenging problem. In this project we have developed new formalisms for modelling and verifying such algorithms. For example, a recent paper in the ACM Transactions on Cyber-Physical Systems [5] provides a theoretical model for

[1] https://arxiv.org/abs/2105.02664

membership views of mobile entities, and shows bounds on the ability to verify such views. We have also used probabilistic model checking to verify liveness properties in for a group communication protocol [14], constraint solving to automatically verify correctness of intersection collision avoidance [11], and security verification of platoon configurations [21].

Group membership Another key result from the project are algorithms and protocols for intelligent coordination of mobile entities (e.g., vehicles). We have designed analysed a novel synchronous leader-based protocol called SLMP [14] that solves the problem of reliable group formation and communication despite an unreliable communication channel. We also propose security mitigation techniques to allow platoons to keep operating despite missing/false location information [9], and investigated dissemination mechanisms for manycast in mobile networks [23]. In another related work we developed a game-theoretic approach for resource sharing [18].

Attestation and assurance Starting from a thesis project by Mohammad Khodari which won the best thesis award by Computer Association in East Sweden, leading to publications in CPSS 2019 [6] and the ACM Transactions on Cyber-Physical Systems [1], we investigated methods for decentralised ECU attestation. This work led to further ongoing studies on decentralised state management for software update mechanisms, intrusion detection systems for trusted enclaves (on Intel SGX), as well as security assurance analysis of the RISC-V Keystone TEE.

Distributed ledgers Distributed ledger technologies have been proposed as a key enabler for large-scale coordination mechanisms. Therefore we have performed number of studies relating to blockchains and distributed ledgers. Some examples include (i) an investigation on the scalability of permissioned blockchains for the IKEA supply chain [2], (ii) decentralized identity management for maritime applications (Master thesis together with Sjöfartsverket), and (iii) performance measurements comparing blockchains with distributed databases [7]. Moreover, in an ongoing project we are studying DAG-based blockchain protocols such as Tangle as a basis for more versatile and verifiable version management.

Degrees and promotions

The project has contributed to the promotion of Mikael Asplund to Universitetslektor in 2016 and Docent in March 2018.

Summary of the master theses

The PI has supervised/examined 43 thesis projects during the CENIIT project, three were awarded best thesis award, and seven led to peer-reviewed publications. Here, we list five of the most relevant ones.

- Thelvar Guo, Daniel Herzegh, Availability of Smart Contracts that Rely on External Data. Master thesis, 2020, URI: urn:nbn:se:liu:diva-169358
- Oskar Lind, Master thesis, Defending against denial of service attacks in ETSI ITS-G5 networks, Master thesis, examiner, 2020, URI: urn:nbn:se:liu:diva-166369
- Gunnar Grimsdal and Patrik Lundgren, Examining the Impact of Microarchitectural Attacks on Microkernels: a study of Meltdown and Spectre, Master thesis, examiner, 2019, URI: urn:nbn:se:liu:diva-159999

- Theodor Flemming, Decentralized Identity Management for a Maritime Digital Infrastructure: With focus on usability and data integrity, Master thesis, examiner, 2019, URI: urn:nbn:se:liu:diva-155115
- Erik Andersson, Ariyan Abdulla, Heuristiska algoritmer för schemaläggning i realtidssystem med hänsyn till data beroenden„ Bachelor thesis, 2018, URI: urn:nbn:se:liu:diva-144794

Funded persons

The following persons have been funded during the project Mikael Asplund (PI) and Felipe Boeira (PhD student).

Industrial connections

Scania has been one of the main partners during this project. The collaboration started with the platoon development unit with Henrik Pettersson and Magnus Adolfson. Later, the focus has moved to connectivity and security with Pär Degerman, Ulrik Janusson, and Jörgen Wallebring. The collaboration has been in the form of a joint project on security of autonomous vehicles, meetings and workshops and a master thesis project. Ericsson has also participated in the project on security for autonomous vehicles and several master/bachelor theses has been supervised with them. Sectra has been a partner both with several research project applications, master theses, and one joint publication. Collaboration with Östgötatrafiken, VTI, and RISE has been going on in two projects relating to public transport. Other collaborations during the project has been through a number of student theses, with organizations such as Saab, Sjöfartsverket, FOI and Combitech.

Collaboration with other CENIIT projects

The PI has collaborated with Elina Rönnberg through joint supervision of a student thesis at Arcticus, and with Andrei Gurtov on a joint supervision of two Master's thesis projects, and two joint publications.

New research group

An (informal) research group on cyberphysical security is being built up by the PI. Two other research project have been started with Asplund as PI, and three as co-PI. He is currently supervising three PhD students (one as main supervisor), and a number of Master students. Several research assistants have been employed during the project and a postdoc is being recruited.

Publication list

The following peer-reviewed papers were published during the project.

[1] A. Rawat, M. Khodari, M. Asplund, and A. Gurtov, Decentralized Firmware Attestation for In-Vehicle Networks, ACM Transactionson Cyber-Physical Systems, 2020

[2] T. Sund, C. Lööf, S. Nadjm-Tehrani, and M. Asplund, Blockchain-based Event Processing in Supply Chains - A Case Study at IKEA, Robotics and Computer-Integrated Manufacturing, 2020.

[3] G. Grimsdal, P. Lundgren, C. Vestlund, F. Boeira, and M. Asplund, Can Microkernels Mitigate Microarchitectural Attacks?, in Secure IT Systems (A. Askarov, R. R. Hansen, and W. Rafnsson, eds.), Springer International Publishing, 2019. doi:10.1007/978-3-030-35055-0_15.

[4] F. Boeira, M. Asplund, and M. Barcellos, Decentralized Proof of Location in Vehicular Ad Hoc Networks, Computer Communications, 2019. doi: 10.1016/j.comcom.2019.07.024

[5] M. Asplund, Combining Detection and Verification for Secure Vehicular Cooperation Groups, ACM Transactions on Cyber-Physical Systems, 2020.

[6] M. Khodari, A. Rawat, A. Gurtov, and M. Asplund, Decentralized Firmware Attestation for In-Vehicle Networks, in 5th ACM Cyber-Physical System Security Workshop (CPSS), ACM, 2019. doi:10.1145/3327961.3329529.

[7] S. Bergman, M. Asplund, and S. Nadjm-Tehrani, Permissioned Blockchains and Distributed Databases: A Performance Study, Concurrency and Computation, Practice and Experience, 2019. doi:10.1002/cpe.5227

[8] F. Strömbäck, L. Mannila, M. Asplund, and M. Kamkar, A Student's View of Concurrency - A Study of Common Mistakes in Introductory Courses on Concurrency, in Proceedings of the 2019 ACM Conference on International Computing Education Research (ICER), ACM, 2019. doi:10.1145/3291279.3339415.

[9] F. Boeira, M.Asplund, M.P. Barcellos, Mitigating Position Falsification Attacks in Vehicular Platooning, Short paper in the proceedings of the 2018 IEEE Vehicular Networking Conference (VNC)

[10] F. Boeira, M. Asplund, M.P. Barcellos, Vouch: A Secure Proof-of-Location Scheme for VANETs, The 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 2018

[11] M. Asplund, Automatically Proving Correctness of Vehicle Coordination, ICT Express, 2018. doi: 10.1016/j.icte.2018.01.013

[12] M. Asplund, J. Lövhall, and S. Nadjm-Tehrani, In-store payments using Bitcoin, in Blockchains and Smart Contracts workshop (BSC), IEEE, 2018.

[13] Felipe Boeira, Marinho P. Barcellos, Edison Pignaton de Freitas, Alexey Vinel, and Mikael Asplund Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning, in proceedings of IEEE Vehicular Networking Conference (VNC), 2017. doi: 10.1109/VNC.2017.8275641

[14] M.Asplund, J. Lövhall, E.Villani, Specification, Implementation and Verification of Dynamic Group Membership for Vehicle Coordination, in proceedings of the 22nd IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2017), doi: 10.1109/PRDC.2017.57

[15] F. Boeira, M. P. Barcellos, E. Pignaton de Freitas, M. Asplund and A. Vinel, On the Impact of Sybil Attacks in Cooperative Driving Scenarios, in proceedings of IFIP Networking 2017 Conference and Workshops

[16] C.-Y. Lin, S. Nadjm-Tehrani, and M. Asplund, Timing-based Anomaly Detection in SCADA networks, in Proceesings of 12th International Conference on Critical Information Infrastructures Security (CRITIS), Springer, 2017.

[17] M. Asplund and S. Nadjm-Tehrani, Attitudes and perceptions of IoT security in critical societal services, IEEE Access journal, 2016. doi:10.1109/ACCESS.2016.2560919

[18] E. J. Vergara, S. Nadjm-Tehrani, and M. Asplund, Fairness and Incentive Considerations in Energy Apportionment Policies in ACM Transactions on Modeling and Performance Evaluation of Computing Systems, volume 2 issue 1, 2016, doi: 10.1145/2970816

[19] T. Hultman, A.Boudjadara, M.Asplund, Connectivity-optimal Shortest Paths Using Crowdsourced Data, *3rd International Workshop on Crowd Assisted Sensing, Pervasive Systems and Communications (CASPer)*, IEEE, 2016.

[20] R. Udd, M. Asplund, S. Nadjm-Tehrani, M. Kazemtabrizi, and M. Ekstedt, Exploiting Bro for Intrusion Detection in a SCADA System, in *Proceedings of the 2nd ACM Cyber-Physical System Security Workshop (CPSS)*, ACM, 2016.

[21] M. Asplund, Model-based Membership Verification in Vehicular Platoons, in *Dependable Systems and Networks Workshop (DSN-W), on Safety and Security of Intelligent Vehicles (SSIV 2015)*, IEEE. 2015.

[22] E.J. Vergara, S. Nadjm-Tehrani and M. Asplund, Sharing the Cost of Lunch: Energy Apportionment Policies, in *Q2SWinet'15: 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 2015

[23] M. Asplund and S. Nadjm-Tehrani, Rapid selection and dissemination of urgent messages over delay-tolerant networks (DTNs), chapter in *Advances in delay-tolerant networks (DTNs) Architecture and Enhanced Performance*, J. Rodrigues editor. Woodhead Publishing Series in Electronic and Optical Materials, Elsevier 2014. doi:10.1533/9780857098467.2.187.

[24] M. Asplund, Poster: Securing Vehicular Platoon Membership, in *Proceedings of IEEE Vehicular Networking Conference (VNC)*, IEEE, 2014. doi:10.1109/VNC.2014.7013324.

[25] B. Viel and M. Asplund, Why is indoor localization still so hard?, in *The 6th International Workshop on Information Quality and Quality of Service for Pervasive Computing, PERCOM Workshop*, March 2014. doi:10.1109/PerComW.2014.6815247

[26] A. P. Biazino, M. Asplund, E. J. Vergara, and S. Nadjm-Tehrani. Cooperative Proxies: Optimally Trading Energy and Quality of Service in Mobile Devices. *Computer Networks, Elsevier*, 2014. doi: 10.1016/j.comnet.2014.10.013