ITS-C 2018 – Security Summary

Thomas Rosenstatter, Chalmers University of Technology

Note that these summaries are interpretations of the talks and may differ from the presenter's view.

Keynotes

The keynotes were held by Jeff Schneider from Uber's Advanced Technologies Group, David Anderson from the U.S. Department of Energy and Arnaud de La Fortelle from MINES Paristech.
Jeff Schneider started his talk with an emphasis that the number of deadly accidents has increased in the U.S. in 2016 and 2017 since 2008. This increase is mainly caused by human drivers who are either not able to comprehend the current traffic situation anymore or are distracted by other thoughts. Schneider focussed his talk on the evolution of artificial intelligence in the automotive domain by first talking about the advantages and disadvantages of supervised learning and deep learning, also called imitation learning. Both approaches suffer from the problem to define safety cases, which is also the reason why AI is not applied in safety-critical systems yet.
David Andersson focussed on how the society and technology has changed and continues to change. He highlighted that 75 per cent of the population will live in urban mega-areas, that the population is still growing and ageing.
Arnaud de La Fortelle presented the challenges about globalisation and localisation of Cooperative ITS (C-ITS). The biggest challenge in mobility is the different needs and traffic structure of each city. "Paris is not San Francisco or Shanghai", they all need to develop/adopt their own local policies.

Real-Time Detection and Mitigation of DDoS Attacks in Intelligent Transportation Systems

Ammar Haydari and Yasin Yilmaz from the Department of Electrical Engineering, University of South Florida

The authors propose a method based on nonparametric statistical anomaly detection to timely detect and mitigate low-rate DDoS attacks in VANETs. This approach does not require a definition of protocols nor data types. The attack model of a low-rate DDoS is that the attacker has compromised several V2X capable nodes that slightly increase data traffic synchronously in order to interrupt regular network operations of Road-Side-Units (RSU).
The proposed detection model is based on Online Discrepancy Test (ODIT) for the reason that it is capable of quickly detecting even small anomalies in high-dimensional networks. The

authors additionally provide a method to identify the origin of the attack and consequently block the processing of traffic from these sources on the RSU.
The proposed method has been evaluated in a simulation environment comprising of OMNET++, SUMO and Veins.

Protecting Train Balise Telegram Data Integrity

*Huaqun Guo, Jonathan Zhi Wei Sim, Bharadwaj Veeravalli, Jiqiang Lu from A*STAR Singapore and National University of Singapore*

Balise is a passive transponder on the rails that provides location information to the Balise Transmission Module (BTM) on trains. The advantage of having balises deployed on the rail network is the precise localisation even in tunnels or other areas where GPS is not a reliable option. The telegrams exchanged through the balise and BTM are defined by the EUROSIG consortium and lack security. Thus, replay attacks, as well as the modification of the transmitted information, is possible.
The authors propose three security profiles that ensure authenticity and/or confidentiality. **Profile 1 - Data Integrity Checking with AES-CCM (Ciphertext)** proposes a new structure for the telegram containing additional parameters, such as baliseID, nonce and an authentication tag. The data of the balise is encrypted “offline” with an individual secret key per balise and further stored in the balise. **Profile 2 - Data Integrity Checking with AES-CCM (Plaintext)** provides data integrity and requires no changes in the balise. An internal database provides the BTM with a secret key, nonce and authentication tag. When the BTM receives the plaintext telegram it gets the before mentioned values and recomputes them with the received value. If both authentication tags match, the verification was successful. **Profile 3 - Data Integrity Checking with HMAC**, a HMAC is precomputed together with a secret key specific to the balise and stored in it. The verification is successful if the authentication tag from the balise and the computed tag using the secret key stored in an internal database match each other.

Comments: *It is interesting to see the challenges in other areas. However, the proposed profiles only prevent modifications of the telegrams, replay attacks are still possible due to the nature of balises (offline modules deployed on the rails). Additionally, this approach requires an internal database with all the secret keys, which also increases the time for verification due to delays when accessing the database.*

Enabling a Privacy-Preserving Synthesis of Representative Driving Cycles from Fleet Data using Data Aggregation

Arved Esser, Florian Kohnhäuser, Nadine Ostern, Kevin Engleson and Stephan Rinderknecht from TU Darmstadt

The authors present an aggregation technique of data from driving cycles in order to provide a representative synthesis of the data while still maintaining privacy. The proposed aggregation technique consists of three steps. (1) each type of information is linked to a certain loss in accuracy. (2) only distribution frequencies are gathered from raw time data. (3) combination of user profiles into a fleet profile.
The aggregation technique is not described in detail, as the authors focus on the assessment of the resulting aggregated data in terms of quality.

Special Session on Solving the autonomous vehicle safety assurance challenge

This session showed different views on safety assurance of autonomous vehicles.

Laura Farrade-Blanaar from RAND Corporation presented the report *Measuring Automated Vehicle Safety - Forging a Framework*[1]. Their framework consists of three frames: **(1) Settings**, where can safety be measured? In artificial settings, such as simulation and closed courses, and on public roads with and without a safety driver. **(2) Stages**, development, demonstration, and deployment. **(3) Measures**, when can safety be measured?

Prof. Huei Peng from the University of Michigan presented Mcity. Mcity is a test facility built for the purpose of testing connected and automated vehicles. In the course of this project, they developed around 27 so-called behaviour competence scenarios. In addition, Peng discussed the use of corner cases for safety assurance. In his opinion, one should not include all possible corner cases as safety case, as they are too rare and impossible to handle (he presented two examples).

Christoph Stiller, Karlsruhe Institute of Technology, presented their work on decision making and trajectory generation by analysing the impact of uncertain scenarios. For example, evaluating two options having the same trajectory for as long as possible and decide on one option when the trajectories depart from each other.

Michael Wagner, Edge Case Research, presented his thoughts on the importance of edge cases, i.e., the bicycle symbol indicating a bike lane is identified as a cyclist.

[1] https://www.rand.org/pubs/research_reports/RR2662.html