InSecTT Newsletter July 2021

CONTENT

Contents

Welcome!

This is the **July 2021 edition** of the InSecTT newsletter, highlighting news & achievements from InSecTT during Q2 2021.

Please distribute this newsletter to all interested parties in your organization. We appreciate your feedback, please send comments or requests to Insectt@v2c2.at.

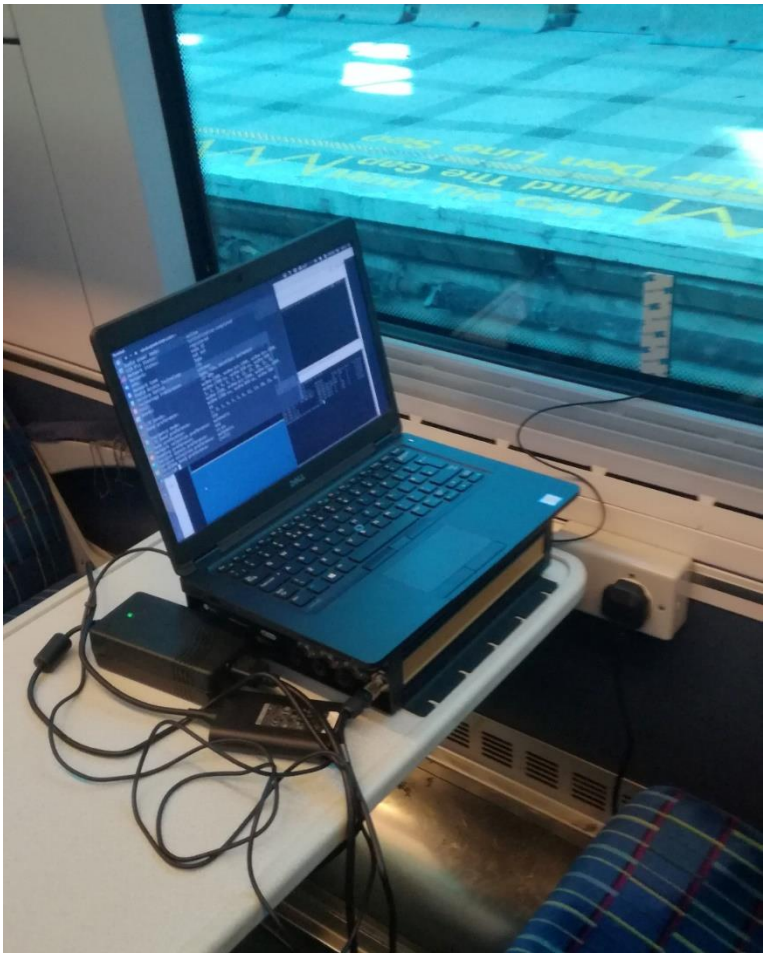
Enjoy the reading!

AI-supported link quality prediction

Jun 28, 2021

When travelling at high speeds, such as in a train, the quality of mobile connections changes constantly. However, onboard systems on trains need reliable, predictable connections, for diagnostic data about the train systems as well as for services such as passenger WiFi.

In InSecTT, researchers from Irish partner Munster Technological University (MTU) work on methods to estimate and predict connection quality. Real life mobile network data collected on journeys in Ireland are used as a basis to develop Artificial Intelligence solutions provide insight into the current and near-future quality that can be expected.

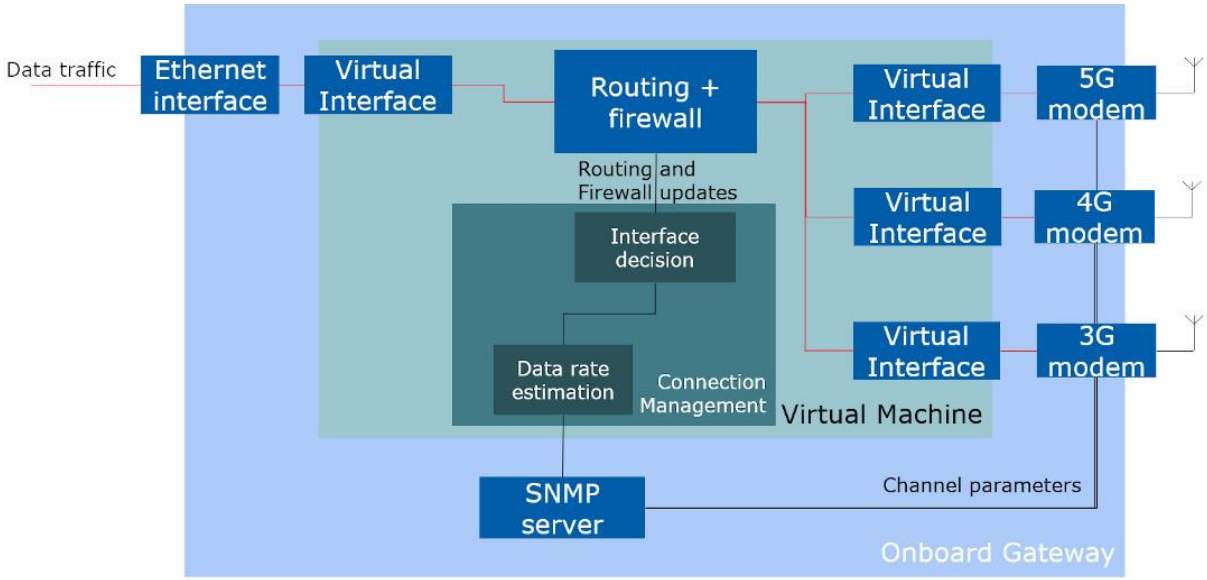


AI-enhanced onboard communication gateways

Jun 23, 2021

Onboard equipment on intelligent transportation systems such as smart trains or trams requires reliable uplinks to cloud services for traffic management, remote diagnostics and other services. Onboard communication gateways can feature multiple options, such as 4G and 5G links, potentially from different operators.

As part of the InSecTT project, research at Munster Technological University aims to create AI-enhanced solutions that make the best use of all connections that are available. Link quality is monitored in real time, and the data traffic coming from the onboard systems is assigned to the available connections to achieve efficient, reliable cloud uplinks.



MTU is a partner in InSecTT

Jun 21, 2021

Munster Technological University (MTU), Ireland's newest Technological University, established in January 2021, is one of four Irish partners in InSecTT. Researchers in MTU's Nimbus Centre work on methods and algorithms to manage vehicle to infrastructure (V2I) communication in a Smart City use case.

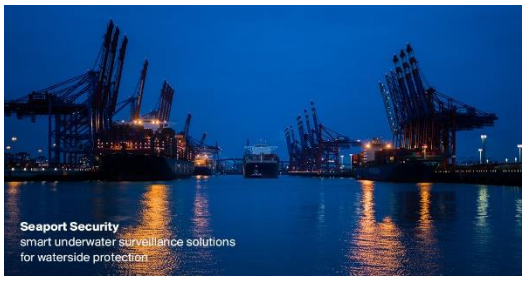
Artificial Intelligence methods are used to estimate and predict link quality and to dynamically manage and choose the most suitable connections in real time among a variety of interfaces, such as 5G and other technologies. The methods will be implemented and validated on rail-certified hardware provided by fellow Irish project partner Klas Telecom.

Security at Seaport: delivering effective and robust underwater surveillance solutions for waterside protection

Jun 16, 2020

Protection against surface and underwater threats has become a critical element to increase the efficiency and security of seaport operations.

Within the InSecTT Project, CINI-UNICAL is working in collaboration with Leonardo Spa on the development of an **AI-based interoperable underwater surveillance system** able to distribute accurate and reliable information in real-time in order to provide a timely and effective response to the potential threats.



Team ZED (InSecTT members) from TU Delft won the 4TU impact challenge

Jun 15, 2021

Team ZED (consisting of InSecTT members) from TU Delft won the 4TU impact challenge and will be one of the people to represent the Netherlands during the world forum in Dubai

Out of 8 teams from all technical universities of the Netherlands, on November 19th 2020, Team ZED won the finals of the 4TU impact Challenge. ZED (Zero Energy Development) won the competition with their IoT solution provider that creates wireless and battery free devices that harvest its energy from the ambient.

For the second time in a row, the four technical universities in the Netherlands organized the 4TU impact challenge. On this platform, students present their pioneering innovations for world problems. The winners of this competitions will go on a trade mission to the World Expo in Dubai 2021, together with representatives from ministry of foreign affairs and various other enterprises.

At this very moment there are over 35 million batteries in use, this number will only multiply in the next 5 years. This means that many batteries will end up in the garbage. By replacing many of these batteries with zero energy harvesting IoT systems, ZED contributes to sustainability and working conditions.

The InSecTT consortium meeting has started!

Jun 14, 2021

The InSecTT consortium meeting and its third general assembly is taking place right now in online form. Really nice to see people on the screen but we are looking forward to meeting everybody in person hopefully in autumn.

During the consortium meeting a General Assembly a Technical Board and a Strategic Board meeting will take place.

Research results, publications, reports on ongoing work, future planning, recent achievements and highlights are presented between today, June 14th and Thursday June 17th. And we are looking forward to having fruitful discussions and topic-specific sessions and workshops from all project areas.

UNIMORE HiPeRT Lab. involving in InSecTT

Jun 12, 2021

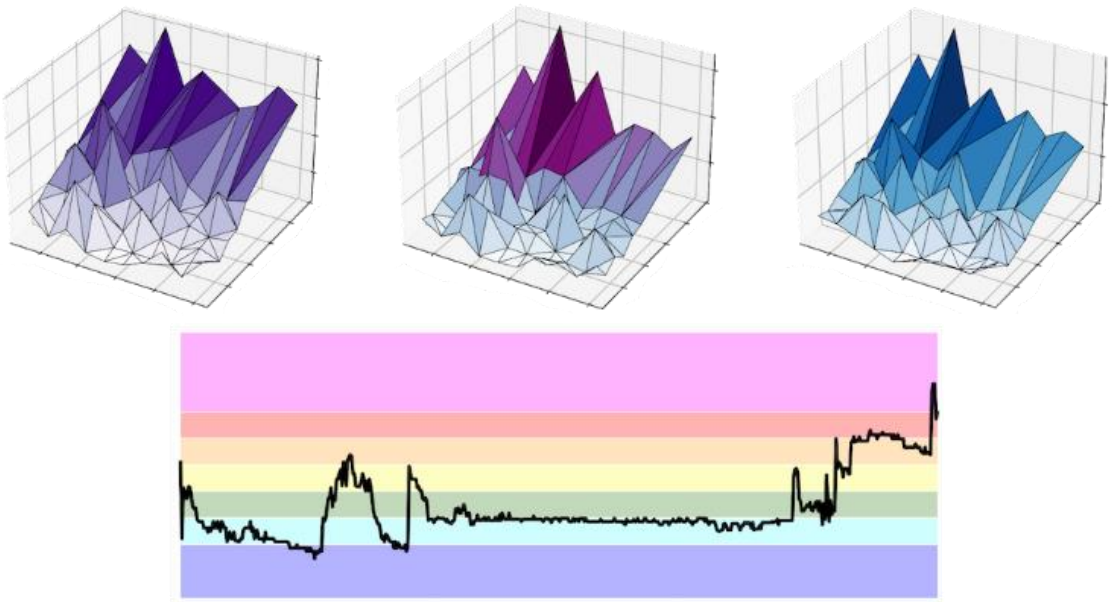
UNIMORE HiPeRT Lab.(the High-Performance Real-Time Laboratory at the University of Modena) is involved in InSecTT, providing optimized low-power embedded AI for intelligent safety and security of public transport in urban environment. It is contributing to the deployment of the AI solution, which is designing by UNIMORE AImagelab for the detection of dangerous/anomalous events related to bus public safety (e.g. brawls, aggressions, fires), with emphasis on the real-time performance of the system. The system is going to be installed and tested on SETA buses (SETA S.p.A is the operator of the local public transport service in the provincial areas of Modena, Reggio Emilia, and Piacenza).

Link: https://hipert.unimore.it/

AI-aided air quality monitoring in InSecTT scenarios

Jun 11,2021

In the last times, the air quality monitoring raised interest in everyday scenarios, with the need to guarantee healthy conditions in heterogeneous environments (even due to COVID-19 pandemic). To this end, distributed and efficient monitoring and prediction mechanisms may be required in both mobility and stationary situations, even considering the involvement of AI-based algorithms for identifying relevant Air Quality Indexes (AQIs). The InSecTT project will aim to involve these intelligent solutions in different environments to provide improved safety and health conditions to people travelling every day.



InSecTT presented at ISAECT 2021

Jun 10, 2021

The massive deployment of Internet of Things (IoT) architectures and applications has accelerated the need to allow data flows among heterogeneous networks. To this end, multi-interface gateways play a crucial role in many IoT applications and will impact future possibilities. Check out our work on “A Modular Multi-interface Gateway for Heterogeneous IoT Networking” to appear in the proceedings of the International Symposium on Advanced Electrical and Communication Technologies (ISAECT 2020).

Find out more on https://www.insectt.eu/ and https://iotlab.unipr.it/

On-the-fly vein biometric recognition

Jun 9, 2021

The UNIROMA3 unit of CINI, partner of the EU-funded #InSecTT Project, is developing an innovative device performing on-the-fly finger-vein-based biometric recognition, allowing a user being recognized while passing a hand over a sensor without requiring any contact, thus improving user convenience during both enrolment and recognition with respect to traditional recognition approaches.

Performing recognition exploiting vein patterns, that is, subcutaneous structures hard to capture without the consent of their owners, allows to inherently guarantee liveness detection, therefore representing an approach notably robust against presentation attacks, and thus suited to implement high-security access control systems for critical areas. The developed solution will rely on low-cost sensors and implement on-board processing.

"Mobile and Wearable Biometrics" on Elsevier Pattern Recognition Letters

Jun 8, 2021

How can Artificial Intelligence of Things help to improve productivity and safety during the Call for Papers for the Special Issue "Mobile and Wearable Biometrics" on Elsevier Pattern Recognition Letters (ISSN 0167-8655, IF 3.255).
The special issue seeks for recent and innovative developments in pattern recognition fields with applications to the design of biometric recognition systems for mobile and wearable contexts.
Topics of interest include the design of hardware architectures or software packages, as well as the proposal of artificial intelligence (AI) approaches requiring limited computational resources to be deployed in edge solutions, among others.
We would like to cordially invite you to contribute an article to the Special Issue.
For more information on the issue please contact the leading Guest Editor, Emanuele Maiorana (CINI unit at UNIROMA3 participating in the #InSecTT project), or please access the Special Issue website at: https://www.journals.elsevier.com/pattern-recognition-letters/call-for-papers/mobile-and-wearable-biometrics-vsimwb

ISSN: 0167-8655

Journal Metrics

- CiteScore: **6.7**
- Impact Factor: **3.255**
- 5-Year Impact Factor: **3.077**
- Source Normalized Impact per Paper (SNIP): **1.739**
- SCImago Journal Rank (SJR): **0.669**

Mobile and Wearable Biometrics (VSI:MWB)

The present special issue therefore seeks for recent and innovative developments in pattern recognition fields with applications to the design of biometric recognition systems for mobile and wearable devices. Topics of interest include, for example, the analysis and processing of the discriminative information (biosignals, images) which can be captured through mobile and wearable devices, the design of hardware architectures or software packages which could be effectively implemented in such environments, the proposal of machine learning approaches requiring limited computational resources, among others.

Guest Editors

Ph.D. Emanuele Maiorana, Roma Tre University, Italy

Ph.D. Ruggero Donida Labati, University of Milan, Italy

Prof. Shiqi Yu, Southern University of Science and Technology, China

InSecTT present at CVPR21

Jun 7, 2021

Class Activation Map (CAM) Methods are among the most used EXAI techniques. In order to progress research on the filed it is important to establish common metrics and benchmarks that allow to compare CAM methods. Check out our work on “Revisiting The Evaluation of Class Activation Mapping for Explainability: A Novel Metric and Experimental Analysis”. We will be present presenting our novel metrics at the Workshop on Responsible computer Vision @ CVPR2021.

Check the paper at https://arxiv.org/pdf/2104.10252.

Find out more on https://www.insectt.eu and https://aimagelab.ing.unimore.it/

InSecTT present at IJCNN'2021

May 28, 2021

InSecTT will be present to the International Joint Conference on Neural Networks (IJCNN'21) with two publications related to the transferability property of adversarial examples. (arxiv 2104.12679 and 2004.04919). Among its core objectives, InSecTT aims at improving the security of embedded A.I. models against threats focused on striking their integrity.

Find out more on https://www.insectt.eu/ and https://www.ijcnn.org/

Protect the integrity of embedded neural networks

May 27, 2021

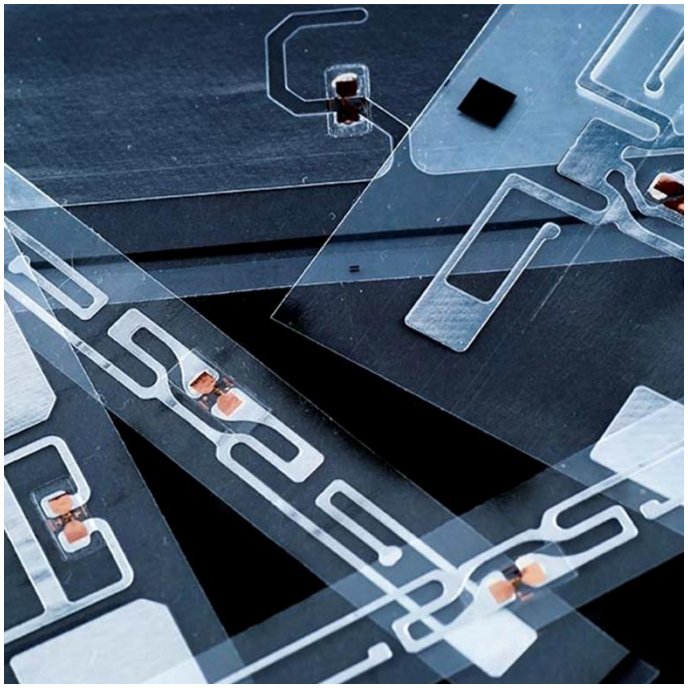
deployment of Artificial Intelligence. Everybody knows adversarial examples that fool a model by slightly altering an input inference. However, what happens with an adversary having a physical access to a device? InSecTT will use cutting-edge equipment (EM pulse, laser beam…) to deal with the impact of physical fault injection against embedded neural networks to propose innovative protections.

Research contributing to Standardization

May 26, 2021

Inventory and supply chain management based on RFID technology has become even more important with the rising number of online shopping.

In the project InSecTT, CISC ensures that tags and readers are on the right quality and performance level by developing new testing solutions conform to international standards.



Security of embedded neural network models

May 25, 2021

The large-scale deployment of Machine Learning models and specifically deep neural network model is an essential evolution for Artificial Intelligence. A major brake to this deployment concerns the security of these models. The traditional Machine Learning pipeline can be

threatened at every stage, from training to inference, with attacks focus on data or the model itself. The integrity, confidentiality and availability of a ML-based system are compromised with attacks such as adversarial examples, poisoning attacks, membership inference, model extraction, sponge examples… These attacks are deeply studied in the scientific community but, for an embedded system, the attack surface is wider since it must encompass physical threats that are related to the hardware features of the embedded platforms, such as side-channel or fault injection analysis.

With InSecTT, we aim at considering an overall attack surface with both algorithmic and physical threats. Our goal: propose innovative protections and help ML and IoT providers to evaluate and improve the robustness of their systems.

WLC: Wireless Charging Technologies

May 21, 2021

In the frame of the InSecTT Project, CISC Semiconductor is working on a new NFC-Based Wireless Charging Development Platform to Enable High-Performance Charging for Billions of Small IoT Devices.

RFID in Automotive

May 20, 2021

Do you know the requirements for RFID tags for Automotive applications?

Watch this video to discover insights about designing the best suitable RFID tags for load carriers and road tolling: https://youtu.be/OkYWeqPpryg

NFC interoperability testing

May 19, 2021

The number of NFC-enabled smartphones and tablets has grown within the last years and with this, the use of these devices as portable payment terminals. As contribution to the #InSecTT project, CISC brings NFC interoperability testing of mobile phones as qualified equipment to the next level: see for yourself on https://youtu.be/A_aSJ4J-QiM

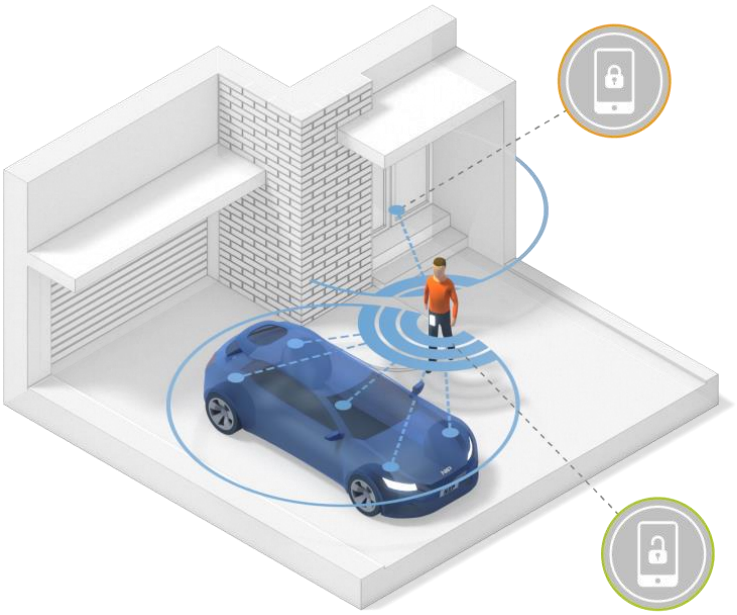
Security Testing of a multi-radio vehicle access system

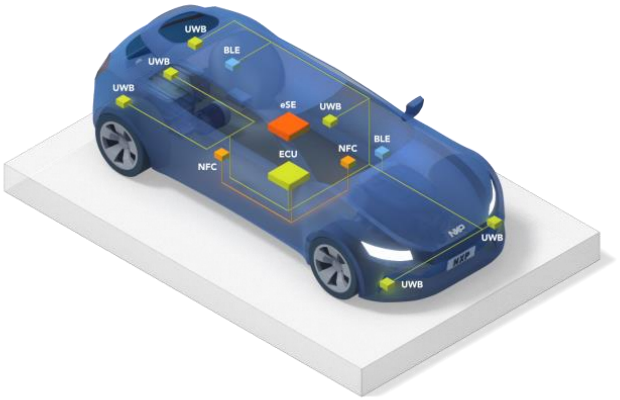
May 12, 2021

Car access is currently moving from vehicle OEM proprietary LF-RF-based access systems to more open car access solutions allowing, besides classical key fobs, also smart devices such

as phones to be used as car keys. To support such “Phone-as-a-key” solutions, future vehicle access systems will employ a new range of radio technologies: BLE for data communication and wake-up; UWB for secure ranging and localization; NFC for backup (e.g., battery of phone is off, but phone can still be used to unlock the card) as well as to enable “no-UI devices” such as smartcards.

While this mix of technology allows for new applications (e.g. phone as a key), it potentially also introduces new threats to car access systems. This scenario will aim for testing a “vehicle access system” against a range of possible attacks. Find out more about that on https://www.insectt.eu/

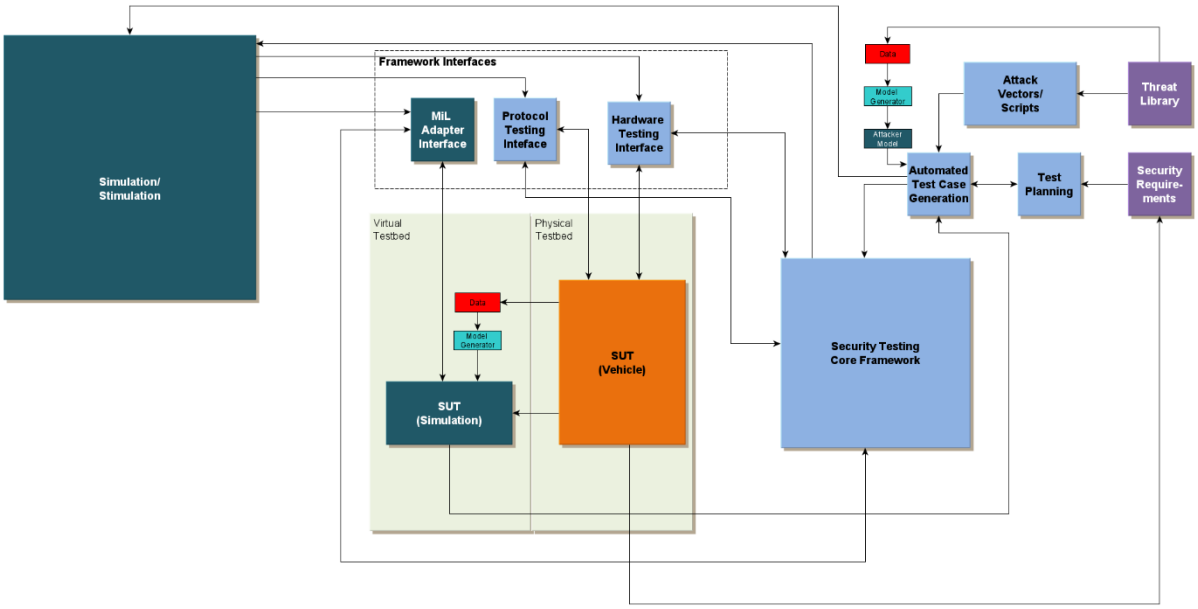




A Wireless Security Testbed for Smart CPSs

May 11, 2021

Cyber-physical systems (CPSs), ranging from small embedded devices to complex systems like vehicles, are more and more equipped with means for wireless connections. This opens up a broad surface potential attacks, even without physical access to the device. It is our goal to built-in security at any stage of product development, giving the opportunity to introduce security very early, when it is still easy to holistically integrate in an efficient way. However, it is crucial to also verify and validate this security at any stage in order to discover any flaws and fix them in the system design and development. In InSecTT, we therefore develop a testbed for discovering security-relevant flaws in CPSs (focusing on automotive systems) through the whole development life cycle. To achieve this, we are combining automated test case generation, sourced by a comprehensive threat database, with cutting edge simulation technologies, even allowing for the system itself either being physical or just a model (full or partly). This allows for testing system security and counteracting faults that cause potential breaches at the very stage they occur. To create such a testbed, we are researching methods for deriving attacks and generate test cases, simulate a system-under-test and/or its surroundings (including application, networks, environments like traffic and infrastructure, etc.), interfacing with the real or simulated system and a framework to orchestrate it all.

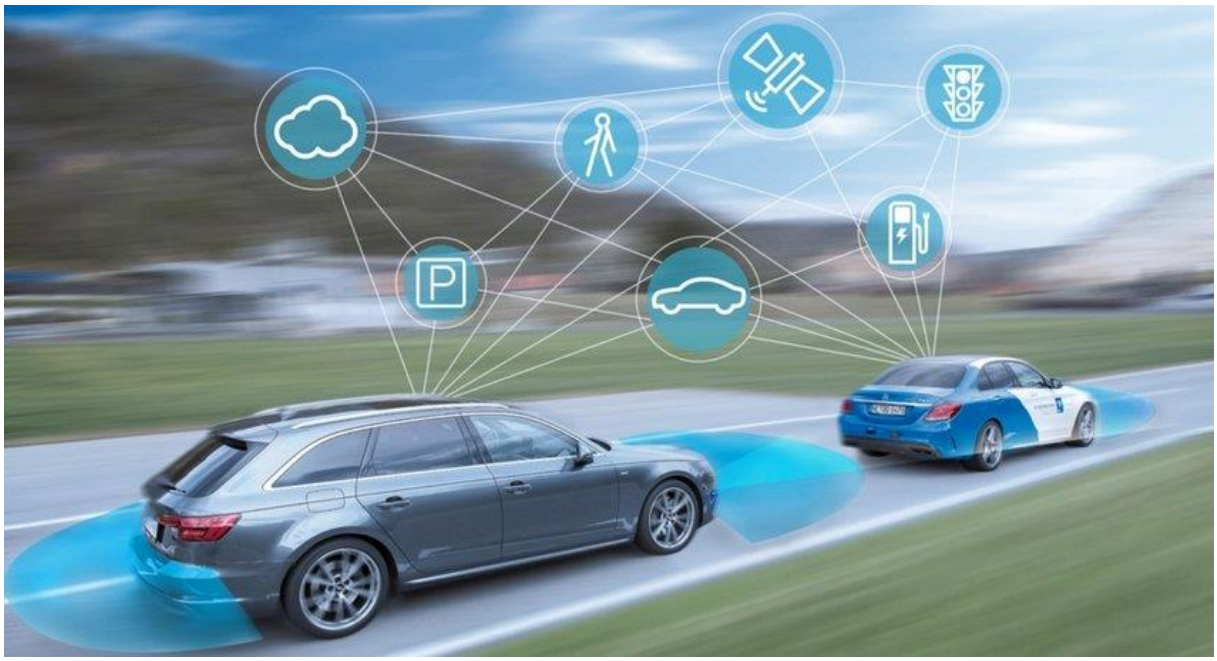


Cybersecurity Testing of V2x ITS-G5

May 10, 2021

Vehicle-to-vehicle communication (V2V), as well as communication to infrastructure (V2I), or cloud services etc. is commonly described as V2X. As this communication (and application layers) include also safety-relevant information, an attacker could cause serious harm using V2x as entry point.

The European research project InSecTT was started to work towards Intelligent, Secure and Trustable Things. This includes new ways and means to verify cybersecurity in systems like connected cars. Partners across Europe collaborate on a Wireless Security Testing Environment for smart IOT.



Automotive Cybersecurity

May 7, 2021

Vehicles typically provide means to connect mobile consumer devices like smart phones, tablets or headphones with functions of the vehicle (e.g., car stereo, hands-free speakers etc.). Such gateways are usually located in the head unit (also called infotainment unit) of the car. As these control units also have access to vehicular networks, they might potentially be used as an entry point for attacks, e.g. by a compromised smartphone. Potential Attack vectors are the Bluetooth and Wireless Interfaces of the unit. Testing is done by sending malicious messages to the unit in order to identify and exploit known vulnerabilities in protocol stacks. Once the infotainment is compromised, it may be used as a threshold for further movement on vehicle internal buses.

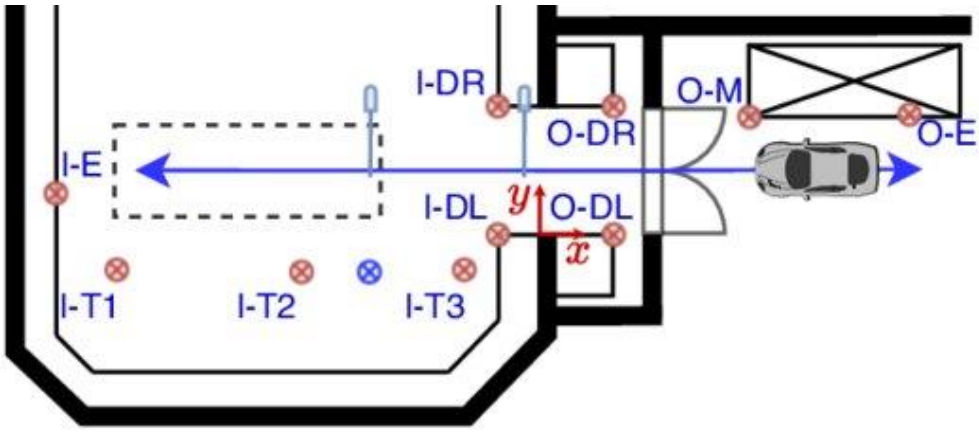
The European research project InSecTT was started to work towards Intelligent, Secure and Trustable Things. This includes new ways and means to verify cybersecurity in systems like connected cars. Partners across Europe collaborate on a Wireless Security Testing Environment for smart IOT.

InSecTT

RSSI-Based Machine Learning with Pre- and Post-Processing for Cell-Localization in IWSNs

May 5, 2021

Industrial wireless sensor networks are becoming crucial for modern manufacturing. If the sensors in those networks are mobile, the position information, besides the sensor data itself, can be of high relevance. E.g. this position information can increase the trustability of a wireless sensor measurement by assuring that the sensor is not physically removed, off track, or otherwise compromised. In certain applications, localization information at cell-level, whether the sensor is inside or outside a room or cell, is sufficient. For this, localization using Received Signal Strength Indicator (RSSI) measurements is very popular since RSSI values are available in almost all existing technologies and no direct interaction with the mobile sensor node and its communication in the network is needed. For this scenario, we propose methods to improve the robustness and accuracy of common machine learning classifiers, by using features based on short-term moments and a second classification stage using Hidden Markov Models. With the data from an extensive measurement campaign, we show the applicability of our method and achieve a cell-level localization accuracy of 93.5\%.

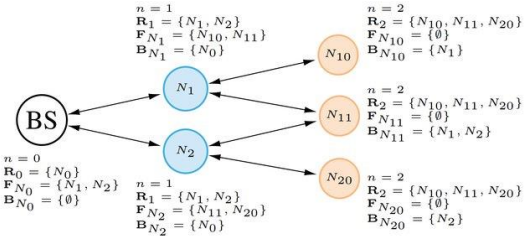


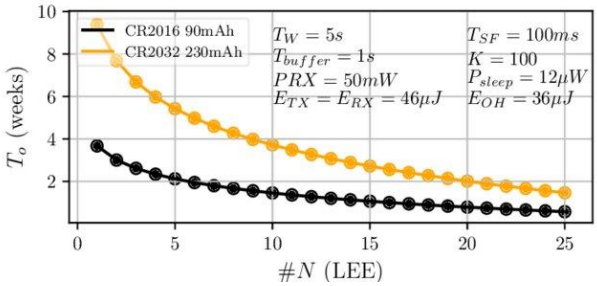
Quality of Service Based Minimal Latency Routing for Wireless Networks

May 19, 2021

Minimized and nearly deterministic end-to-end latency facilitates real-time data acquisition and actuator control. In addition, defined latency is an integral part of quality oriented service in order to get closer to the reliability of wired networks and at the same time take advantage of wireless networking. This paper introduces a QoS routing protocol capable of balancing power consumption between wireless sensor and actuator nodes while minimizing end-to-end

latency. We introduce a TDMA scheme in the routed wireless network to enable defined latency and in addition it improves the energy efficiency by avoiding collisions which eliminates time and energy consuming retries. Our novel routing method allows latency and round-trip times to be calculated in advance. We implemented a demonstrator and show experimental results of a wireless sensor network with our proposed routing scheme.





Cybersecurity in Industrial Manufacturing

Apr 16, 2021

Arçelik Global is one of the partners in the InSecTT Project from manufacturing domain. Arçelik Global provides an use case which aims to develop secure and reliable communication solutions for production Shopfloor.

The manufacturing and industrial robotics systems getting more connected everyday to increase the productivity. The use case will address the use of AI-enhanced secure and reliable communication technologies to enhance the security, safety, reliability in the manufacturing and production plants. The use of AI-integrated communication technologies will improve the reliability and security, for the two major goals, avoiding interrupts and mass damages due to the cyber attacks and providing a trusted system with high quality production.