IARIA

Panel #2

ATHENS
March 2024

InfoSys 2024 & InfoWare 2024

Theme:

Challenges on Systems Performance, Resilience, and Robustness

CONTRIBUTORS

Athens
March 2024

Moderator

Emeritus Prof. Dr. **Fritz Laux**, Reutlingen University, Germany,
fritz.laux@fh-reutlingen.de

Challenges for Software development

Panelists

- Prof. Dr. **Eugen Borcoci**, National University of Science and Technology POLITEHNICA Bucuresti (UNSTPB), Romania, Eugen.Borcoci@elcom.pub.ro

  Challenges for high speed telecommunications

- Dr. **Faouzi Adjed**, IRT SystemX, France, faouzi.adjed@irt-systemx.fr

  Challenges in Machine Learning

- Assoc. Prof. Dr. **Atreyee Sinha**, Edgewood College, USA
  ASinha@edgewood.edu

  Challenges for Large Language Models

- Prof. Dr. **Oliver Michler**, Technical University Dresden, Faculty of Transportation, Germany,
  oliver.michler@tu-dresden.de

  Challenges for the security of communication networks

IARIA

Chair Position

ATHENS
March 2024

- Software insufficiencies are more likely than Hardware weakness and failures.
- Overly complex software is prone to errors and makes systems slow.
- Software is often not well tested and is far from being “fool proof”.

⇘The best prerequisites for Performance and Robustness are lean and well tested software.

IARIA

Panelist Position

Athens
March 2024

Eugen
Borcoci
UNSTPB

- **Challenges on Systems Performance and Robustness**

- **Performance and Robustness**
  - **System requirements:** *functional* (correctness) and *non-functional* (performance, robustness, scalability, reliability, ..). Some requirement can belong to functional or non-functional category, depending on system objective (e.g. security in mission critical systems – is functional)
  - **Performance, robustness-** Sets of characteristics/requirements - very diverse, multi-dimensional, depending on system nature, objectives, scale, environment, implementation technologies, etc.
  - **Performance:** the measure of how well a system executes its intended tasks within specific constraints, such as speed, responsiveness, throughput, scalability, and resource utilization
    - Evaluation process: define metrics, collect data, analyze data, review the strategy. ...
    - Examples: metrics for a communication network at PHY layer: bandwidth, throughput, latency, jitter, error rate; traffic capabilities at network level, user perceived (Quality of Experience -QoE)

IARIA

Panelist Position

Athens
March 2024

- **Challenges on Systems Performance and Robustness**
- **Performance and Robustness** (cont'd)
- **Robustness :** the system can remain functional under adverse conditions
  - Robustness principles: observability, recoverability, responsiveness, and task conformance
  - IT&C case: robustness can be related to many areas, e.g. software/programming, security, communication networks, services, AI/ML technologies, etc.
- Robustness examples
  - ability of a computer system to cope with errors during execution and cope with erroneous input
  - a communication network capacity to maintain functionality, against of adverse conditions: security attacks, nodes/links-down, traffic overload, PHY layer problems (especially in wireless and space communication), etc.

- **Performance and robustness are not independent**; also, they are related/overlapping to other characteristics like stability, scalability (horizontal, vertical), reliability, etc.

IARIA

Panelist Position

Athens
March 2024

- **Challenges on Systems Performance and Robustness**
- **6G Performance Requirements and Challenges- examples**

- ***Extreme data rates:*** up to 1 Tbps (indoor and outdoor)
- *Challenges*: to achieve 1 Gbps user data rate guaranteed at 95% of user locations
- ***Enhanced spectral efficiency (SE) and coverage***
  - the max SE up to 60 bps/Hz), based on MIMO and different modulations The user-experienced SE is expected to be ~3 bps/Hz
  - uniform SE and the same for the entire coverage area
- *Challenges:* new techniques needed at the PHY layer (supporting broadband connectivity & high mobility)
- ***Very wide bandwidth:***
  - in the (mmWave) range, bandwidth up to 10 GHz and also THz bands
  - visible light (VLC), can support bandwidths up to 100 GHz
- ***Enhanced energy efficiency****:* at user level and also at network level
  - *Challenges*: achieve Tbps order per second per Joule; to develop energy efficient communication strategies
- ***Ultra-low latency and jitter:*** < 0.1 ms for bandwidth >10 GHz; jitter ~ 1 μs
- ***High connection density*** *:* 10^7 devices/km^2
- ***Extremely high reliability:***
  - *Challenges*: to meet mission and safety-critical applications requirements

- **General challenges** – to support IoT; high precision manufacturing; holographic, VLC and 3D communications; to include AI in all network segments (access, transport, core).

Panelist Position

Athens
March 2024

- **Machine Learning model performances and robustness**

The mathematical interpretation of a robust model is primarily defined by its stability function. However, in Machine Learning (ML) models, the assessment of robustness is more explicitly emphasized in the context of classification as opposed to tasks such as data segmentation or data generation.

Model performance is a measurement that assesses the results between a model's predictions and the ground truth within a test dataset. Nevertheless, depending on the specific objectives of the model, this measurement might overlook crucial information

- **Model performances evaluation**
  Several measures are used for evaluating ML Model performances and its interpretation.
  - A use of single evaluation approach of ML models may be insufficient to accurately reflect its real performances
  - For the same model objective, two measures could be interpreted differently.
  - Wrong use of metrics in case of bounded measurement in case of regression for examples.

- **Adversarial examples**
  - The adversarial examples can be defined as examples with slight perturbation that cause the model to alter its decision.

- **Adversarial attacks learning**
  - The adversarial learning involves incorporating adversarial examples into the learning process.

- **Robustness evaluation**
  - Formal evaluation : formally demonstrates the local stability of the model
  - Empirical evaluation: Evaluates empirically the lack of robustness

Faouzi
Adjed
IRT
SystemX

Panelist Position

Athens
March 2024

- Robustness and Scalability of Large Language Models (LLMs)

Atreyee Sinha
Edgewood College, Madison, WI, USA

asinha@edgewood.edu

ROBUSTNESS is a critical aspect of deploying Large Language Models (LLMs) in real-world applications.

- LLMs have low generalization performance when applied to out-of-distribution (OOD) test data
- LLMs are vulnerable to various types of adversarial attack.
- LLMs trained on biased datasets may perpetuate and amplify biases in their outputs, leading to unfair or discriminatory outcomes.
- Addressing biases and promoting fairness in LLM-generated content is crucial for ethical deployment and societal impact.

Panelist Position

Athens
March 2024

Robustness and Scalability of Large Language Models (LLMs)

SCALABILITY is a fundamental challenge in developing and deploying Large Language Models (LLMs) at scale.

- As language models expand in size and intricacy, it is crucial to prioritize transparency and interpretability, especially when deploying these models in sensitive areas such as healthcare or finance.
- Scaling LLMs to larger sizes while managing computational costs poses challenges in resource allocation and optimization.

Atreyee Sinha
Edgewood College,
Madison, WI,
USA

asinha@edgewood.edu

Panelist Position

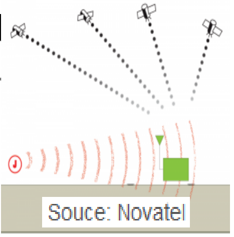
Athens
March 2024

- Increasing Performance in IT yes, but always under the Umbrella of Security, Availability and Sesilience ⇒ Theory

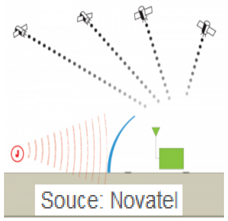
- **Subproblem: Jamming and Spoofing ⇒ IT explanations by way of example GNSS/GPS**
  - **Jamming:** emits a signal that overlays the original signal so that the GNSS receiver can no longer decode the real satellite signal + be intentional (in bad faith) or unintentional
  - **Spoofing:** is the purposeful transmission of false GNSS signals, for example to conceal the user's true position + be intent (in bad faith as criminal / or in good faith as emulation fea complex IT devices in relation to RF and on + is more diffic detect than jamming
    - **Solutions to protect against Jamming and Spoofing:**
      - **both:** Minimization of interference power ⇒ directional or beamforming antenna
      - **Spoofing (1):** Spatial resolution of the interferer ⇒ Bearing method with antennas
      - Spoofing (2): Signal statistics ⇒ Reception level statistics as difference between satellite as transmitter (20000km/space) and near-earth transmitter (x km/surface)

Oliver Michler

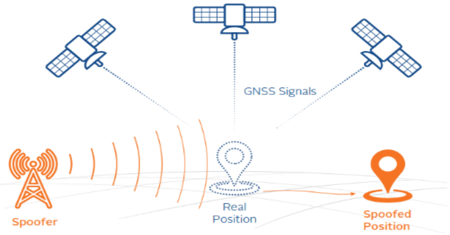
TUD, Institute



Souce: Novatel



Souce: Novatel



Souce: Novatel

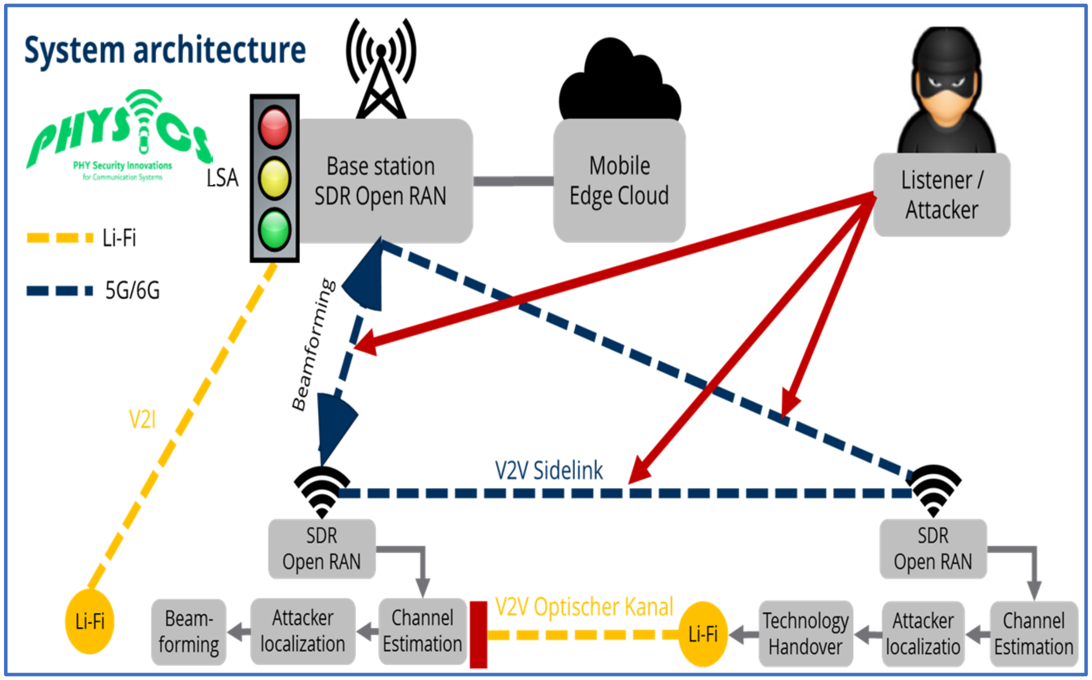
Panelist Position

Athens
March 2024

- Increasing Performance in IT yes, but always under the Umbrella of Security, Availability and Resilience ⇒ Practice
  - **Own Research Project “PHYSICS”** ⇒ aim of novel and integrated detection, mitigation and compensation strategies for attacks on communication networks (V2X), so that the requirements of security, resilience and privacy of communication infrastructures are met

Oliver Michler
TUD, Institute of Traffic Telematics

Source: photoschmidt/ Shutterstock.com)



- ✓ **Physical Layer / Channel properties**
- ✓ **Network / Protocol**
- ✓ **Mathematics / Statistics**
- ✓ **Informatics / Artificial Intelligence**
- ✓ **Legal experts / Politics**

Source: www.weka-akader