KuVS Newsletter

2022-12

Back to Contents

Contents

KuVS Newsletter

Editor Message

Dear KuVS members,

we welcome you to the 16th (and Christmas) edition of the KuVS newsletter.

This newsletter is providing you with all information that you need to know about the KuVS community from the last half a year. This edition features reports, calls for papers and participations, as well as dissertations completed within the KuVS community.

At the end of the newsletter, you again find some riddles from Rolf Windenberg based on his mathematically oriented reform of English orthography.

More information and recent editions of our newsletter are available on https://www.kuvs.de/newsletter/.

We hope you enjoy reading this edition of the KuVS newsletter. We as editors wish you merry Christmas and a happy new year.

The newsletter editors,

Oliver Hohlfeld
Universität Kassel
Mathias Fischer
Universität Hamburg
Corinna Schmitt
Universität der Bundeswehr München
Andreas Blenk
Siemens

KuVS Newsletter

Announcements

Movement of persons

- **Prof. Dr. Oliver Hohlfeld** (full-professor at Brandenburg University of Technology) accepted the offer for a full professorship (W3) on distributed systems at the University of Kassel.

Announcements

New seminar, Connect-Them-All

'Connect them all' is a collective initiative to make some contribution in the field of IoT. It is a great platform for tech enthusiasts to explore new topics and interact with the community. There will be talks by experts every month where they will discuss their latest research and take questions during the discussion session post-presentation. Stay tuned to know more about the upcoming events.

Video Archive:

https://www.youtube.com/playlist?list=PLK_Ujz7qXyqPFsaU13jGbtrJyOllHPJT_

For more info - www.connect-them-all.net

Organizers:

- Prof. Dr. Anna Förster — Comnets, University of Bremen - https://www.uni-bremen.de/comnets/people/personal-profiles/prof-dr-anna-foerster
- Dr. Marco Zennaro — Science, Technology and Innovation Unit, The Abdus Salam International Centre for Theoretical Physics - http://users.ictp.it/~mzennaro/
- Prof. Dr. Pietro Manzoni — Department of Computer Engineering, Universitat Politècnica de València - https://pmanzoni.github.io/
- Dr. Fredrik Ahlgren — Faculty of Technology, Linnæus University - https://lnu.se/en/staff/fredrik.ahlgren/

KuVS Newsletter

Awards

KuVS Awards 2021

- Best Bachelor thesis:
  - Tobias Kröll, TU Darmstadt (Advisor: Matthias Hollick)
- Best Master thesis:
  - Alexander Brundiers, Uni Osnabrück (advisor: Nils Aschenbruck)
  - Marvin Härdtlein, TU Darmstadt (advisor: Ralf Steinmetz)
- Best PhD thesis:
  - Manisha Luthra, TU Darmstadt (advisor: Ralf Steinmetz, Boris Koldehofe)
  - Amaury Van Bemten, TU München (advisor: Wolfgang Kellerer)

Congratulations to all winners of the KuVS award 2021!

2022 DEKRA Security Award The IMMUNE[1] consortium and as part of that also KuVS member Mathias Fischer received the *DEKRA Security Award 2022*[2]. The project was joint work with Airbus Defense and Space, Fraunhofer AISEC and Fraunhofer SIT, IABG, IFAK, Siemens, and University Hamburg. The consortium developed novel security monitoring and response mechanisms based on SDN and TSN to protect future industrial facilities against cyber attacks.

IEEE LCN Lifetime Achievement Award During the 47th IEEE LCN banquet on Tuesday evening, Prof. Dr. Burkhard Stiller received the ”LCN Lifetime Achievement Award”. Dr. Tim Strayer, an LCN Steering Committee Member from Raytheon BBN Technologies, U.S.A., handed over this award to Burkhard as well as to Dr. Matthias Frank, University of Bonn, Germany, since the two had worked with and for LCN about half of their personal lives!

Burkhard did participate as a paper author in 1993 for the first time in IEEE LCN, did later work on different Organization Committee positions, run two General Chair tasks of LCNs in 2004 and 2005, was before once a TPC Co-chair in 2002 and once a TPC Chair in 2003, and is part of the LCN Steering Committee (formally called Standing Committee) since 2006. In 2009 Burkhard hosted as the Local Chair LCN in Zürich, Switzerland. Eventually, in November 2022 Burkhard was elected Steering Committee Chair of LCN, the longest running IEEE conference series in the research and development area of networking, sponsored by the IEEE Computer Society, especially the Technical Committee on Computer Communications, for which Burkhard served as a chairman between 2008 and 2013.

[1] https://immune-projekt.de/

[2] https://www.dekra.de/de/dekra-award/

KuVS Newsletter

4 Awards for Allan M. de Souza (Universität Bern) The PhD thesis of Allan M. de Souza, advised by Prof. Torsten Braun (Universität Bern) received the 1st place award for best Ph.D. thesis at Latin American Computing Conference, the 2nd place award at the Brazilian Computer Society Conference 2022, the 1st place award for best Ph.D. thesis at Brazilian Symposium of Computer Networks and Distributed Systems - SBRC 2022, and the 2nd place award for the best Ph.D. thesis in Computer Science defended in Brazil in 2021.

KuVS Newsletter

VDE Bayern Award

Wenn im Netz die Stricke reißen

Wie kann der Datenverkehr im Internet auch in Zukunft möglichst störungsfrei fließen? Diese Frage hat der Informatiker Stefan Geißler in seiner Doktorarbeit untersucht. Dafür hat er jetzt den VDE Bayern Award 2022 erhalten.

"Damit der Datenverkehr im Internet trotz ständig steigender Anforderungen weiterhin reibungslos fließen kann, muss man die Flexibilität im Netz erhöhen, um so schneller und einfacher auf neue Anforderungen reagieren zu können. Das lässt sich zwar auch mit moderner Hardware erreichen – was allerdings aufwendig und teuer ist. Einfacher geht es, wenn man dafür Software einsetzt."

So beschreibt Dr. Stefan Geißler den wesentlichen Inhalt seiner Doktorarbeit, die er im Frühjahr 2022 beendet hat. Jetzt wurde er dafür ausgezeichnet: Geißler ist einer der Gewinner des diesjährigen VDE Bayern Awards in der Kategorie „Wissenschaft“. Mit dem Preis zeichnet der VDE Bayern herausragende technische und wissenschaftliche Leistungen sowie Schulen mit herausragenden MINT-Initiativen und innovative Firmengründungen aus.

Geißler hat an der Julius-Maximilians-Universität Würzburg (JMU) Informatik studiert und mit dem Master abgeschlossen. Für seine Promotion hat er am Lehrstuhl für Informatik III (Kommunikationsnetze) bei Professor Tobias Hoßfeld geforscht. Seit dem 1. April 2022 arbeitet er dort als Postdoc.

Mechanismen zur Bewertung der Leistungsfähigkeit

"Bislang fehlen Methoden, um die Leistungsfähigkeit der Netze zu messen, zu modellieren und vorherzusagen", sagt Stefan Geißler. In seiner Dissertation hat er deshalb technische und analytische Mechanismen entwickelt, mit denen sich die Leistungsfähigkeit softwarebasierter Netzfunktionen und komplexer Dienste bewerten lassen.

Bei der Bewertung muss es allerdings nicht bleiben. Wenn beispielsweise die Kapazität einer Hardware-Komponente nicht mehr ausreicht, die aktuelle Datenmenge zu bewältigen, so kann mit Softwarelösungen dynamisch auf diese Situation reagiert werden.

Überlastkontrolle ist das dazugehörige Stichwort: „Wenn alle Stricke reißen, muss man mit Hilfe der Software die Last intelligent verteilen und beispielsweise Teilmengen, die in dem Moment nicht so wichtig sind, blockieren“, erklärt der Informatiker. Das von ihm dafür entwickelte Verfahren bereitet Geißler momentan gemeinsam mit seinem Projektpartner Emnify zur Patentanmeldung vor.

Energieeffizienz rückt in den Fokus

Für seine Arbeiten hat Geißler bereits drei Best Paper Awards und weitere Auszeichnungen erhalten. Auch als Postdoc bleibt er dem Thema treu – ergänzt um einen weiteren Bereich. „Wenn es um den Netzausbau geht, rückt zunehmend das Thema ‚Nachhaltigkeit‘ in den Fokus“, sagt er. Da geht es dann beispielsweise um die Frage, wie lange eine Software einsatzfähig ist, wie oft sie durch neue Programme ersetzt werden muss. Aber auch ganz konkret um die Energieeffizienz, mit denen die jeweiligen Komponenten ausgestattet sind.

Klar, dass auch das Internet möglichst nachhaltig arbeiten soll. Oberstes Prinzip für den Informatiker ist jedoch immer: Die Qualität darf darunter nicht leiden. Dazu will er mit seiner Forschung beitragen.

Über den VDE Bayern

Der VDE Bayern zählt rund 5.000 persönliche Mitglieder und über 200 Mitgliedsunternehmen. Mit jährlich rund 200 Veranstaltungen bietet er in Bayern eine wichtige Informationsplattform zum interdisziplinären Wissensaustausch und -transfer für Hochschulen, Industrie, Handwerk, Behörden, Verbände und die Politik.

Kontakt

Dr. Stefan Geißler, Lehrstuhl für Informatik III (Kommunikationsnetze), T: +49 931 31-83134, stefan.geissler@informatik.uni-wuerzburg.de

KuVS Newsletter

Ehrendoktorwürde für Prof. Ralf Steinmetz

Prof. Ralf Steinmetz: „Unsere Kommunikationssysteme sind auf Gefahren wie Naturkatastrophen, Angriffe oder Stromausfälle nicht gut vorbereitet“

Prof. Dr.-Ing. Ralf Steinmetz hat im Rahmen der Feierlichkeiten zu 50 Jahre Informatik an der RWTH Aachen neben der Informatikerin Prof. Dr. Christel Baier die Ehrendoktorwürde verliehen bekommen. Im Interview erzählt der Professor der TU Darmstadt, wie seine Forschung dazu beiträgt, unsere Kommunikationssysteme auf künftige Herausforderungen vorzubereiten.

Herr Prof. Steinmetz, schon seit langem warnen Sie vor den Gefahren eines Ausfalls der Kommunikationssysteme. Mit Ihrer Forschung – für die Sie nun mit der Ehrendoktorwürde der RWTH Aachen ausgezeichnet wurden – treiben Sie technische Methoden voran, um unsere Gesellschaft für einen solchen Ausfall zu wappnen. Was hat es damit auf sich?

Prof. Ralf Steinmetz: Den Ehrendoktortitel habe ich für meine wissenschaftliche Leistung im Bereich leistungsfähiger, skalierbarer und adaptiver Kommunikationssysteme und Multimedia-Technologien verliehen bekommen. Zusammen mit der Informatik-Professorin Klara Nahrstedt habe ich einige der essentiellen Ideen für den DFG-Sonderforschungsbereich „MAKI – Multi-Mechanismen-Adaption für das künftige Internet“ initial auf den Punkt gebracht. Klara Nahrstedt hat uns überzeugt, dass diese Idee der extremen Adaptivität langfristig und praxisnah ist.

Was steckt dahinter?

Prof. Steinmetz: Wir dachten, es wäre sinnvoll, Bestehendes zu nehmen und anzupassen, anstatt ein neues Internet zu erfinden. Aktuell sind unsere Kommunikationssysteme auf Gefahren wie Naturkatastrophen, Angriffe oder Stromausfälle nicht gut vorbereitet. Nun könnte man alle Komponenten und Systeme mehrfach parallel laufen lassen wie in der Raumfahrttechnik. Unser Ansatz ist es aber, die Systeme hochadaptiv zu entwickeln und je nach Situation die unterschiedlichen Möglichkeiten zu nutzen, die wir bereits haben. Diese Idee der Adaptivität, also dem automatischen Umschalten zwischen verschiedenen Mechanismen, finden wir schon heute, wenn wir beispielsweise das Smartphone mit uns herumtragen. Es schaltet automatisch zwischen mobiler 5G- oder LTE-Datenübertragung und WiFi hin und her.

Das Smartphone bevorzugt dabei WiFi, weil man davon ausgeht, dass dies für den Nutzer am kostengünstigsten ist. Anders sieht es aus, wenn man etwa an autonom fahrende Autos denkt. Hier ist Zuverlässigkeit der Kommunikationstechnik das wichtigste Kriterium. Bei Schwärmen von kleinen Satelliten geht es um Effizienz, beim Filmschauen um eine möglichst hohe Datenrate. Wie kommt hier Ihre Idee der Adaptivität zum Einsatz?

Prof. Steinmetz: Genau, die Randbedingungen liegen in unterschiedlichster Form vor. Unter diesen Kriterien versuchen wir dann, das Beste daraus zu machen und nehmen unterschiedlichste Systeme, unterschiedlichste Möglichkeiten, um Daten zu übertragen. Das System entscheidet am Ende automatisch über die Idealform. Wenn ich mich heutzutage zum Beispiel mit einem Freund verabreden möchte, muss ich entscheiden: Nutze ich WhatsApp, Signal, die E-Mail, das Telefon? Es wäre viel einfacher, wenn ich meine Nachricht in der von mir gewünschten Form losschicke und das System sich dann selbst den besten Weg aussucht, wie die Daten oder Informationen weitergereicht werden. Das adaptiert sich einfach, das wäre viel nutzerfreundlicher.

Und wie gut funktioniert das schon?

Prof. Steinmetz: Das funktioniert teilweise sehr gut. Wie im Fall der Smartphones, die zwischen 5G- oder LTE-Datenübertragung und WiFi wechseln, ist eine Umschaltung auf der physikalischen untersten Ebene im Schichtmodell des Internets schon in Produkten integriert – auch ohne unser Zutun. Das Gleiche kann ich jedoch auch auf der Anwendungsebene oder für jede Art von Datenübertragung anpassbar machen. Mit dem Sonderforschungsbereich MAKI haben wir gezeigt, dass dies an vielen Stellen möglich ist. In der Praxis muss sich die Idee der Adaptivität allerdings noch bewähren und durchsetzen. Leider ist das schwierig, weil es die Geschäftsmodelle einzelner Firmen untergraben würde. Unternehmen und Organisationen, die hinter Messaging-Diensten wie WhatsApp stecken, haben beispielsweise wenig Interesse an einer adaptiven Lösung, welche Kommunikation über alle Messenger hinweg ermöglichen würde. Die Firmen binden die Nutzer aus ökonomischen Gründen an die eigene Plattform.

Was schwebt Ihnen demgegenüber vor? Wie wünschen Sie sich das Internet?

Prof. Steinmetz: Ich wünsche mir, dass die Leute Adaptivität als eine große Chance verstehen, gerade in Bezug auf Resilienz. Der Mensch soll auf einfache Art Technik nutzen können, und die Technik soll sich verlässlich in Krisensituationen verhalten. Wir sehen das mit dem Gas heute, wir sehen das mit dem Strom: Wir brauchen bei kritischen Ressourcen eine gewisse Autarkie, und Kommunikationsnetze sind fraglos essenziell. Ohne sie sähe unsere Welt ganz anders aus. Sie müssen auch dann funktionieren, wenn das Netz ausfällt. In einem solchen Fall könnte ich eine Zeit lang mobile Daten nutzen, mir ein eigenes Netz mit anderen bauen oder über Satelliten gehen. Also gilt es, alle Varianten in irgendeiner Form nutzen zu können. Da muss ich dann irgendwann entscheiden: Welche Daten sind wichtig, was ist unwichtig, was ist kritisch?

Also Kommunikation über alle Anwendungen, Technologien und Geräte hinweg.

Prof. Steinmetz: Ja, warum nicht? Angenommen, die Webcam des Laptops fällt aus. Warum kann ich stattdessen nicht einfach das Smartphone oder meine Spiegelreflexkamera nutzen? Bis ich die mit dem Laptop verbunden habe, dauert es ewig. Aber eigentlich könnte es so einfach sein. Es ist alles da, die Geräte müssten nur miteinander reden können. Innerhalb eines Ökosystems, zum Beispiel von der Firma Apple, funktioniert einiges gut. Aber warum kann ich nicht einen Sensor eines Apple-Gerätes ganz einfach mit einem Android-Smartphone verbinden?

Für welche Firmen wäre es interessant, auf euch zuzugehen und die Forschung in die Praxis umzusetzen?

Prof. Steinmetz: Absolventen von uns sind bereits bei Google gelandet, bei Apple, Spotify, Deutscher Telekom, Netflix, Intel oder Siemens, bei allen möglichen Systemherstellern. Dort gibt es ein Interesse an diesen Kenntnissen und Technologien. Bei kleineren Firmen ist es etwas schwieriger. Die haben ja nicht den Durchgriff auf ganze Systeme, die sie mit ihren Kunden ausprobieren könnten.

Wie lang ist der Weg, der noch vor uns liegt?

Prof. Steinmetz: Man kann sich noch viele Jahre damit beschäftigen, wesentliche Erkenntnisse in die Praxis in einer gut anwendbaren Form umzusetzen. Und durch diese bescheuerte Weltlage, die wir heute haben, wird es viel schwieriger. Es gibt immer mehr Abgrenzungen. Es ist nicht mehr wie vor vielleicht fünf oder zehn Jahren, als alles offen war und man sagen konnte, das wird schon funktionieren. Resilienz ist ein Thema, das uns erst noch richtig auf die Füße fällt in den nächsten Jahren. Wir müssen viel dafür tun und es wird teuer und unangenehm werden. Verlässlichkeit kostet, und man sieht den Nutzen nicht sofort. Das wird ein steiniger Weg.

Vielen Dank für das Interview!

Das Interview führte Christine Wachter, verantwortlich für die Wissenschaftskommunikation am Fachgebiet Multimedia Kommunikation der TU Darmstadt.

Zur Person: Prof. Ralf Steinmetz

Prof. Dr.-Ing. Ralf Steinmetz leitet an der TU Darmstadt das Fachgebiet Multimedia Kommunikation an der Schnittstelle von Elektrotechnik und Informatik. Er ist 1956 in Santiago de Chile geboren. Internationale Anerkennung erlangte er durch wegweisende wissenschaftliche Arbeiten zur Synchronisation multimedialer Datenströme, durch Beiträge zur Peer-to-Peer-Technologie, auf welchen heutige Streaming-Dienste und Mediatheken basieren, sowie durch die Idee einer systemweiten Adaptivität durch Übergänge von Kommunikationsmechanismen. Hierzu hat er weltweit den Begriff der „Transition“ für verteilte und kommunizierende Systeme geprägt.

KuVS Newsletter

Finished PhD Theses

Ahmad Rabay

Heinrich Heine University Düsseldorf (advisor Kalman Graffi)

Title: P2P Fog Computing: Enhancing Fog-based IoT Scenarios with Distributed Hash Tables

Abstract: Internet of Things (IoT) is here to stay, and has changed the technological landscape where existing legacy technologies started to struggle meeting with the emerging needs of IoT. A vital example is Cloud computing, which for decades, has served the internet backbone with a centralized computing and storage model. With the massive growth of IoT, the centralized computing model of the cloud encountered growing challenges, such as network bandwidth constraints, which is the main focus of this research. Fog computing is a new computing architecture which overcomes the limitations of the centralized cloud with a layer of connected, geographically distributed, heterogeneous fog nodes located at the proximity of the end users. Those fog nodes act like mini clouds which have the computing and storage capabilities to handle part of the edge traffic, reducing the bandwidth load of the cloud. However fog nodes are resource constrained in terms of storage capabilities and computational power. Therefore, any resource intensive requests which cannot be single handed by the fog nodes, the cloud needs to be contacted. The challenges arise in this endeavor are discussed in this research. We propose a new model called peer-to-peer fog (P2P Fog) which combines the capabilities of fog computing with peer-to-peer (P2P) network mechanism in order to support the cloud node meeting the increasing demands of IoT devices. Even though each fog node has a limited computational capabilities, our proposed P2P Fog model combines the computational capabilities of the fog nodes creating a larger pool of resources. Which provides an approach to increase the amount of requests handled by the fog nodes, in order to reduce the requests that will be sent through to the cloud. As a pre-study, we conduct an exploratory research on implementing cloud computing in business enterprise systems. Since the emergence of cloud computing it has been utilized almost everywhere. However, one area which faces many uncertainties to implement the cloud is ERP systems. This research investigates the main challenges that are restraining the market of implementing ERP systems using cloud computing from the market perspective and introduces solution to these challenges. The goal of this research is to helps the market and researchers get a better view about ERP in the cloud, as well addresses some of the issues and limitations of the cloud computing model. As mentioned earlier, cloud computing has been utilized, at various extends, almost everywhere, including emerging technologies such as IoT. Our novel P2P Fog computing model aims to overcome the limitations faced by cloud computing and fog computing when dealing with the huge data volume resulted from the emergence of IoT. The P2P Fog model enhances the fog computing model by introducing P2P mechanism between the fog nodes at the fog layer to empower the fog nodes capabilities. This allows the sole fog nodes to collaborate with the other fog nodes at the fog layer using P2P overlays to aggregate their computational capabilities and create a larger pool of resources to meet the IoT devices needs at the proximity of the end user. Hence minimize the requests to the

cloud and further reduce the bandwidth consumption of the cloud. The P2P distributed hash table (DHT) based overlays considered for this research are: Chord, Pastry and CAN. With a simulator environment configured to imitate an IoT setup, the different P2P Fog configurations are implemented, evaluated and compared in terms of their bandwidth consumption in order to figure out under which overlay the P2P Fog model performs better. The simulation outputs, which are done using a P2P simulation software called ”PeerfactSim.KOM”, show that Pastry overlay produces better outcomes in terms of reducing the bandwidth consumption compared to cloud computing, conventional fog computing, Chord

Ahmad Reza Cheraghi

Heinrich Heine University Düsseldorf (advisor Kalman Graffi)

Title: Nature-Inspired Algorithms for Mobile, Communicating, and Sensing Robot Swarms

Abstract:

Imagine a world full of robots created to do mundane or dangerous tasks, for example cleaning, carrying heavy objects, protecting us, or searching for survivors in dangerous places. These are examples for the future. But, the complexity of developing these robots should not be underestimated. The hardware and software need to be designed, developed, and tested. Each robot needs to have artificial intelligence. Additionally, the collaboration and communication among robots must work seamlessly. In this dissertation, we deal with robot swarm, based on three problem statements including 11 research questions. Robot swarms are groups of robots that accomplish tasks that are either impossible to solve by one robot or time-consuming. It is an emerging scientific field. We design, develop, and evaluate a simulator and seven nature-inspired algorithms for robot swarms. Before doing so, however, we conducted research on robot swarms and summarized 217 publications. The result is an overview of robot swarms’ past, present, and future. In addition, a comprehensive review of the current state-of-the-art network simulators has been prepared. This survey compares 25 simulation tools for peer-to-peer, opportunistic, and mobile ad-hoc networks. We built a new simulator for robot swarms called Swarm-Sim based on the gained insights. Swarm-Sim is easy to understand as it is written in Python. It has an API that is easy to learn, allowing the implementation of a scenario and solutions for various robot swarm tasks. It has an advanced GUI, which displays the animation of the simulation either in 2D or 3D, and allows for changes to the environment ad-hoc. Therefore, Swarm-Sim is a simple to learn and easy to apply simulator to develop and evaluate robot swarm algorithms. This dissertation’s central and essential contribution is the nature-inspired robot swarm algorithms. We implemented and evaluated seven algorithms on the Swarm-Sim and categorized them into three application areas. The first application task is the swarm coating. With swarm coating, the robot swarm is to enclose an arbitrarily shaped object from all sides. We have developed two algorithms for this purpose. Swarm communication is the second application area. We deal with how robots can communicate with each other within the swarm. Both indirect and the direct communication is considered. Last but not least, we deal with swarm movement. We present two algorithms for coordinated movement within the swarm and how to motivate the robot swarm to move in different directions. As a result, this dissertation provides three modules with ten contribution, presented with summaries from ten papers. The summaries contain two surveys about robot swarms and network simulators, one article about the Swarm-Sim simulator, and seven nature-inspired algorithms for robot swarms. We hope that with this dissertation we have made an important contribution to the scientific community and to the further development of robot swarms.

Ralf Kundel

TU Darmstadt (advisor Ralf Steinmetz)

Title: Accelerating Network Functions using Reconfigurable Hardware. Design and Validation of High Throughput and Low Latency Network Functions at the Access Edge

Abstract:

Providing Internet access to billions of people worldwide is one of the main technical challenges in the current decade. The Internet access edge connects each residential and mobile subscriber to this network and ensures a certain Quality of Service (QoS).

However, the implementation of access edge functionality challenges Internet service providers: First, a good QoS must be provided to the subscribers, for example, high throughput and low latency. Second, the quick rollout of new technologies and functionality demands flexible configuration and programming possibilities of the network components; for example, the support of novel, use-case-specific network protocols. The functionality scope of an Internet access edge requires the use of programming concepts, such as Network Functions Virtualization (NFV).

The drawback of NFV-based network functions is a significantly lowered resource efficiency due to the execution as software, commonly resulting in a lowered QoS compared to rigid hardware solutions. The usage of programmable hardware accelerators, named NFV offloading, helps to improve the QoS and flexibility of network function implementations.

In this thesis, we design network functions on programmable hardware to improve the QoS and flexibility. First, we introduce the host bypassing concept for improved integration of hardware accelerators in computer systems, for example, in 5G radio access networks. This novel concept bypasses the system's main memory and enables direct connectivity between the accelerator and network interface card. Our evaluations show an improved throughput and significantly lowered latency jitter for the presented approach.

Second, we analyze different programmable hardware technologies for hardwareaccelerated Internet subscriber handling, including three P4-programmable platforms and FPGAs. Our results demonstrate that all approaches have excellent performance and are suitable for Internet access creation. We present a fully-fledged User Plane Function (UPF) designed upon these concepts and test it in an end-to-end 5G standalone network as part of this contribution.

Third, we analyze and demonstrate the usability of Active Queue Management (AQM) algorithms on programmable hardware as an expansion to the access edge. We show the feasibility

of the CoDel AQM algorithm and discuss the challenges and constraints to be considered when limited hardware is used. The results show significant improvements in the QoS when the AQM algorithm is deployed on hardware.

Last, we focus on network function benchmarking, which is crucial for understanding the behavior of implementations and their optimization, e.g., Internet access creation. For this, we introduce the load generation and measurement framework P4STA, benefiting from flexible software-based load generation and hardwareassisted measuring. Utilizing programmable network switches, we achieve a nanosecond time accuracy while generating test loads up to the available Ethernet link speed.

Yannic Schröder

TU Braunschweig (advisor Lars Wolf)

Title: InPhase – Localization in the Internet of Things

Abstract:

The InPhase system provides ranging and localization capabilities to Internet of Things devices. InPhase uses the Phase Measurement Unit in existing IEEE 802.15.4 radio trans- ceivers to measure the phase response of the radio channel. Hence, it only requires a software component to enable ranging and localization on many devices. This allows retrofitting these capabilities to existing hardware platforms at no additional cost via a firmware update.

The system requires two sensor nodes to measure the phase response of the radio channel cooperatively. We demonstrate it using the 2.4 GHz band and sample the phase response across 200 different frequencies. From this data, we derive the distance between the two devices via our Complex-valued Distance Estimation Algorithm. This algorithm can compute the distance from the measured phase response robustly. It is evaluated and compared to two other state-of-the-art algorithms regarding the accuracy, precision, and susceptibility to noise and errors in the phase data.

We investigate the physical properties of the measurement: the influence of multipath propagation and different types of antennas. We demonstrate the influence of multipath propagation in a controlled environment and propose a mitigation algorithm to reduce the harmful influence of multipath propagation on phase-based ranging. We demonstrate the advantage of this algorithm in a realistic scenario with strong multipath propagation. We found that different antenna types introduce varying distance errors to the measure- ment. We compared the ranging performance of four different antenna types in an anechoic chamber. Some antennas exhibit an exceptionally high measurement error depending on their orientation, while others work reasonably well across different rotation angles. Further, we extend the Active Reflector Principle to allow concurrent ranging with multiple reflectors. This can speed up the measurement when one device needs to measure distances to multiple other devices, e.g., for localization. However, the theoretical speed-up cannot be achieved in practice due to transmission errors induced by other systems and technologies competing for wireless channel access.

Finally, we present ways to derive location information from phase response data. We employ a particle filter and extend it to use additional information from the distance estimation algorithm. The InPhase localization system is tested in a competition against 14 competitors and scores a Mean Absolute Error of 0.95 m in a 3D live tracking scenario of a moving person.

Muriel Figueredo Franco

Universität Zürich (advisor Burkhard Stiller)

Title: CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment

Abstract:

The increasing number of cyberattacks and their potential disruptive impacts cause significant concerns for companies, governments, and society. A successful cyberattack can, for example, cause financial losses due to business disruption, affect the privacy of people due to data leakages, and make critical resources completely inaccessible for interested stakeholders. This puts cybersecurity at the center of a digital society and as one of the anchors to all technologies and industries that support a connected and automated society. Therefore, it is essential to look at cybersecurity not only as a technical problem, but also from the economic, societal, and legal perspectives.

Today, companies still neglect planning and investments in cybersecurity due to different factors. First, they face budget constraints and do not see cybersecurity investments as a priority. Secondly, the high amount of information and planning complexities makes implementing a cybersecurity strategy cumbersome for companies that do not have in-house expertise. Finally, companies, especially Small and Medium-sized Enterprises (SME), do not see themselves as the target of a potential cyberattack. This utterly wrong view makes SMEs one of the main targets of cyberattacks worldwide, since the likelihood of successful cyberattacks is higher than companies with a well-defined cybersecurity strategy. Therefore, there is still a need for approaches that support companies, especially SMEs, during the cybersecurity planning and investment phases. These phases include supporting the understanding and definition of cybersecurity requirements, the definition of the budget and investment path to achieve a proper level of cybersecurity, and the selection of protections with a positive return on investment, while also satisfying specific business demands.

This PhD thesis addresses these gaps in cybersecurity planning and investments by proposing the CyberTEA approach. This approach is composed of a five-phase methodology, a framework, and a set of solutions for cybersecurity planning and investment, considering the technical requirements of cybersecurity and its economic dimensions, such as the potential economic impacts of cyberattacks and the cost-benefit of protections available on the market to protect against specific threats. The methodology describes the key phases to consider during the cybersecurity planning and investment, while the framework maps and implements the components needed to be considered to support the tasks required in each phase. A set of new

solutions are also designed and implemented to (i) simplify the risk assessment of companies, (ii) analyze and classify cyberattacks, (iii) calculate the optimal investment in cybersecurity, and (iv) recommend protections based on businesses profile. Furthermore, supplementary solutions for cybersecurity planning are placed to contribute to additional aspects and challenges faced by the cybersecurity market, such as information sharing, cyber insurance, and marketplaces for protection.

Quantitative and qualitative evaluations were conducted to analyze different aspects that give evidence of the feasibility, accuracy, and performance of the proposed solutions. These experiments were adapted for each solution according to its dimensions and features under evaluation. The results highlight (a) the potential of simplified risk assessment in companies using selected attributes, (b) the feasibility and benefits of visualizations to understand and investigate cyberattacks traffic, (c) the capacity of ML-based techniques to classify cyberattacks and predicts risks correctly, (d) the role of conversational agents as an ally for cybersecurity awareness and risk management, (e) the benefits of solutions that integrate cybersecurity metrics during the decision process, and (f) the feasibility of protection recommender systems. Finally, an end-to-end case study is conducted to show the application of the proposed methodology in a company, supported by the information obtained with each one of the solutions implemented as part of this PhD thesis. All of these evaluations and contributions show evidence of scientific advances in cybersecurity planning while highlighting and paving the path for stakeholders (e.g., decision-makers, developers, researchers, and companies) to implement more cost-effective solutions and strategies related to cybersecurity. This also contributes to understanding the relationship and dimensions of economic and technical aspects of cybersecurity, thus, providing directions for further advances in the field and its multidisciplinary facets.

KuVS Newsletter

Nemanja Ignjatov

Universität Wien (advisor Peter Reichl)

Title: Trustworthy Context-Aware Access Control in IoT Environments Based on the Fog Computing Paradigm

Abstract: The strongly increasing connectivity and interest in today's Information Technology (IT) infrastructure resulted in a huge amount of interconnected networks building the Internet of Things (IoT). In parallel, a rapidly changing landscape of innovative services for end-users could be observed. Cloud Computing (CC) provides computing and storage resources for the vast majority of IoT services. Still, further IoT development strives for building low-latency, reliable, highly distributed systems, for which CC fails to satisfy the requirements. Computing capabilities distribution paradigms, among others Edge Computing (EC) and Fog Computing (FC), aim to deploy computing and storage resources at the IoT net- works' edge. Through that, a distance gap between Things and CC Data Centers is bridged, enabling the innovative IoT services development.

Future IoT developments need to be accompanied by appropriate system architecture and security concepts to allow safe usage, overall security, and improved usability in the complex IoT ecosystem. Well-researched, traditional network security mechanisms like public-key encryption or X.509 certificates often cannot be applied in IoT systems, primarily due to the Things' computational constraints. Additionally, heterogeneity, scale, and geographical distribution of IoT networks impose challenges for the security management which traditional protocols and frameworks fail to satisfy through centralized CC architectures. Finally, security management often involves human effort for security policy configuration, which appears to be cumbersome and error-prone for non-tech-savvy users. For those reasons, improving IoT security requires rethinking of the traditional security mechanisms in multiple directions: (i) offloading and distributing security management through paradigms like EC or FC, (ii) reducing computational requirements for security procedures and protocols like encryption or TLS, and (iii) automating security policy management in IoT through data analysis in IoT environments, adapting to its current state and minimizing users' effort required for the security management.

This dissertation contributes a novel FC-based solution comprising protocols, data models, and guidelines for distributing security services at the IoT network's edge. First, trust management in the Cloud - Fog - Thing continuum is introduced, enabling scalable and reliable trust management both in local and global IoT environments. Additionally, computation requirements concerning minimization and trust management application on Things have been thoroughly examined, allowing the solution's utilization in End-to-End (E2E) security scenarios. Second, an Access Control (AC) distribution model has been developed, allowing AC operations availability in ”offline” use-cases, that is, without connection to the Cloud, relying just on FC resources. Furthermore, security policy management has been automated by adapting access policy based on the IoT environment's context information. In order to develop context-aware access policies, the following contributions have been made: (1) a generic data model for integration of context information in access policies, (2) protocols for exchanging context information, and

(3) guidelines for integrating context information in AC services. The designed and realized approaches have been evaluated for their performance, operability, and applicability based on a real-world Smart Home Management system - COSYLab. Lastly, the analysis of the evaluation results leads to the conclusion that proves the applicability of the implemented solution in FC-based IoT systems, ensuring beneficial capabilities for hosting distributed IoT services, such as (i) offloading computational requirements from resource-constrained Things and remote Cloud Servers and (ii) reducing overall latency of the provided IoT services.

KuVS Newsletter

Raphael Labaca Castro

Universität der Bundeswehr München (advisor Gabi Dreo Rodosek)

Title: Machine Learning under Malware Attack

Abstract: Machine Learning (ML) has become key in supporting decision-making processes across a wide array of applications, ranging from autonomous vehicles and stream- ing recommendations to network traffic analysis. Because of the massive amounts of information available, researchers and practitioners have largely focused on improving the performance of ML models. These efforts led to novel applications that can now overcome human performance nearly in every domain.

Despite being highly accurate, these algorithms have been shown to be prone to returning incorrect predictions. This means that the trustworthiness of a model may be compromised in terms of both training and testing time. In other words, committed adversaries may be able to manipulate input data (e.g., images and network traffic) to resemble objects from another class, performing what is known as evasion attacks. They may also use another strategy called poisoning, which includes injecting undesirable data into the training set. Both approaches aim to mislead the model to predict the wrong label for a given object.

While adversarial attacks may target how a model is induced to predict a certain class for an object (e.g., classifying a red traffic light as green), this is normally sufficient with a wrongly predicted label or the opposite class for binary classification, which is generally the case in the context of malware (e.g., classifying malicious software as harmless).

In the event of manipulating objects for evasion attacks, these are known as adversarial examples and pose multiple security risks. On many occasions, as in malware classification, such behavior needs to be further examined to assess the degree to which predictions can be trusted.

Therefore, studying adversarial attacks can help identify systemic weaknesses in ML classifiers. These attacks reveal weak spots in the model that allow carefully manipulated objects to be incorrectly classified, hence compromising the quality of predictions. In fact, by investigating multiple strategies to generate successful adversarial examples, models can be evaluated from multiple perspectives and potentially hardened against adversarial examples. However, it is worth noting that while attacks generally materialize in the feature domain and are convertible to the problem space, where they exist in the real world, this is not always the case in the context of malware, especially in Portable Executable (PE) files. In this context, generating real adversarial malware examples often requires modifications that preserve binary integrity at the byte level. Thus, creating effective attacks using PEs is not a trivial task.

In this study, we present a framework that contains a suite of input-specific attacks using PE malware targeting ML-based classifiers, in which the adversaries have limited knowledge about target classifiers. We then explore multiple approaches in which the adversary leverages hard labels from the model and does not have any prior knowledge of the architecture or access to the training data. To deeply understand the model's behavior, we additionally study full-knowledge attacks based on gradient information.

First, we introduce universal adversarial attacks in the problem space for PEs. The underlying goal here is to show whether the generation of adversarial examples can be automated and generalized without relying exclusively on input-specific attacks to generate effective adversarial examples.

We also propose a defense strategy that leverages knowledge from the aforementioned universal attacks to increase the cost of generating adversarial examples and, therefore, improve the target model against carefully crafted objects produced by adaptive adversaries. We envision a holistic approach that facilitates the identification of systemic vulnerabilities and enhances the classifier's resilience at a reasonable cost.

Next, we perform a statistical analysis of malware features by evaluating the impact of real-world attacks in the feature domain, which provides clarity for model predictions under unexpected input.

Finally, we release our Framework for Adversarial Malware Evaluation and make the source code available to encourage participation and further research into this fascinating topic and promote the evaluation and building of more resilient malware classifiers.

Michael Steinke

Universität der Bundeswehr München (advisor Wolfgang Hommel)

Title: Framework-Konzepte für Managementplattformen in föderierten softwarebasierten Netzen

Abstract:

Heutige IT-Infrastrukturen unterscheiden sich stark von denen vor 20 Jahren. Hatte man in herkömmlichen Netzen zuvor noch einen sehr starken Fokus auf den Einsatz von IT-Ressourcen und Netzkomponenten als starre Verschmelzung aus Hardware und Funktion, so werden sie inzwischen in vielerlei Hinsicht als dynamisch, modular und vielschichtig verstanden: Paradigmen wie Netz- und Systemvirtualisierung sowie Network Functions Virtualization (NFV) erlauben einerseits eine feingranulare logische Kapselung verfügbarer IT-Ressourcen in ver- schachtelten virtuellen Netzen. Software-Defined Networking (SDN) beschreibt andererseits ein Managementparadigma für eine programmierbare sowie zentralisierte Verwaltung dieser Ressourcen. In dieser Arbeit werden derartige Netze als softwarebasierte Netze (SN) bezeichnet. Föderierte softwarebasierte Netze (FSN) beschreiben SNs, in denen IT-Ressourcen mehrerer Partner zusammengeschlossen, genutzt und auch gemeinsam koordiniert gemanagt wer- den. Das technische Werkzeug zur Unterstützung des Netzmanagements ist eine Managementplattform. Sie implementiert das Managementkonzept, die sogenannte Managementarchitektur.

FSNs können jedoch stark variierend ausgeprägt sein, beispielsweise in ihrem Zweck, der Zusammensetzung der IT-Ressourcen oder der Organisation des Managements. Eine einheitliche Managementarchitektur und eine diese umsetzende Managementplattform für FSNs kann es daher nicht geben, sondern vielmehr müssen darin fixe sowie an den jeweiligen Anwendungs- fall anzupassende Bausteine berücksichtigt werden. Entsprechend erfüllen auch bestehende Managementplattformen nicht alle Anforderungen für einen geeigneten Einsatz in beliebigen FSNs und weisen höchstens in Teilmodellen eine gewisse Nutzbarkeit auf.

Das Ziel dieser Dissertation ist die Unterstützung der Spezifizierung und Implementierung von geeigneten Bausteinen von Managementarchitekturen in FSNs durch die Entwicklung und Bereitstellung entsprechender Framework-Konzepte. Ein besonderer Fokus dieser Arbeit liegt dabei in der geeigneten Realisierbarkeit dieser Architekturbausteine in einer Managementplattform, sowie der Definition von Schnittstellen der Bausteine untereinander im Sinne der Bereitstellung eines zusammenhängenden Gesamtkonzepts. Im Rahmen einer systematischen Vorgehensweise werden in dieser Dissertation dazu einerseits grundlegende Charakteristika des Betriebs von FSNs sowie andererseits von Föderationen in SNs neu erarbeitet. Auf dieser Basis werden begründet drei repräsentative Szenarien und 80 Anforderungen an Managementplattformen in FSNs abgeleitet und beschrieben. Den Kernbeitrag der Arbeit stellen die beschriebenen Framework-Konzepte dar. Sie können allein für sich stehend genutzt werden, um bestehende Managementplattformen in einzelnen Teilbereichen für das Management von FSNs zu komplementieren. Sie können jedoch auch als zusammenhängendes Gesamtkonzept genutzt werden, um anwendungsfallspezifisch geeignete Managementplattformen von Grund auf neu zu entwickeln. Die Frameworks wurden zu großen Teilen implementiert und ihre Eignung zur Beschreibung

einer Managementarchitektur für FSNs im Kontext eines beispielhaften Szenarios angewendet. In einer zusätzlichen Evaluierung werden schließlich die Erfüllung von Performanzkriterien an die Frameworkimplementierung der Kernprozesse des Netzmanagements untersucht.

KuVS Newsletter

Project News

Mit maschinellem Lernen zu mehr Zufriedenheit im Internet

Wie lassen sich Datenströme im Internet besser verteilen, so dass möglichst viele Nutzer zufrieden sind? Diese Frage untersucht der Würzburger Informatiker Michael Seufert mit einer neuen Emmy-Noether-Nachwuchsgruppe.

Michael Seufert hat Informatik, Mathematik, Wirtschaftsmathematik und Erziehungswissenschaften studiert. Von seinem ursprünglichen Plan, Lehrer zu werden, ist er im Laufe des Studiums abgekommen. (Bild: Gunnar Bartsch / Universität Würzburg)

Rund 4,9 Milliarden Menschen weltweit waren nach Angaben der International Telecommunication Union, einer Organisation der Vereinten Nationen, im Jahr 2021 im Internet unterwegs. Damit ist die Anzahl der "Onliner" innerhalb von zehn Jahren um rund 2,73 Milliarden gestiegen. In Deutschland haben mehr als 66 Millionen Menschen im vergangenen Jahr das Internet genutzt. Durchschnittlich haben sie dort 149 Minuten am Tag verbracht – bei Jugendlichen waren es sogar 241 Minuten.

Während auf der einen Seite durch den Netzausbau die Download-Geschwindigkeit steigt, wachsen auf der anderen Seite die Anforderungen von Nutzerinnen und Nutzern und den Anwendungen mindestens genauso schnell. Dadurch kommt es trotz Ausbau der Infrastruktur zu Verzögerungen, Engstellen oder gar Überlast – und wird es auch zukünftig kommen.

Für Abhilfe sorgen könnte ein Netzmanagement, das die beschränkten Ressourcen in den Netzen besser zuteilt. Wie dieses mit Hilfe künstlicher Intelligenz seine Aufgaben erfüllen könnte, erforscht der Informatiker Dr. Michael Seufert. Die Deutsche Forschungsgemeinschaft (DFG) hat ihm dafür jetzt eine Forschungsgruppe im Rahmen ihres Emmy-Noether-Programms genehmigt.

Ein nutzerzentriertes Netzmanagement

Ausgestattet mit rund zwei Millionen Euro kann Seufert in den kommenden sechs Jahren sein Ziel verfolgen, ein nutzerzentriertes Netzmanagement zu entwickeln, das dazu beiträgt, dass auch bei Engpässen im Netz möglichst viele Nutzerinnen und Nutzer zufrieden mit der angebotenen Leistung sind. Wobei "Netz" in diesem Fall ein weitgefasster Begriff ist. Dazu gehören WLAN genauso wie Mobilfunk-, DSL-, Kabel- oder Glasfasernetz.

"Zunehmende Datenmengen und steigende Anforderungen der Nutzerinnen und Nutzer bleiben eine Herausforderung für Betreiber von Kommunikationsnetzen", beschreibt Seufert den Hintergrund seines Forschungsprojekts. Ein Ausbau der Infrastruktur könnte dagegen helfen, ist allerdings teuer und langwierig. Zudem sei auch damit nicht garantiert, dass für alle User und alle Anwendungen wie beispielsweise Videokonferenzen, Musikstreaming, Online-Gaming oder Cloud-Anwendungen, die gewünschte Qualität zur Verfügung steht. Quality of Experience, oder kurz QoE, lautet der Fachbegriff dieser subjektiven Dienstgüte.

QoE-Fairness ist ein weiterer Begriff, der in Seuferts Forschungsprojekt eine zentrale Rolle einnimmt. Dahinter steckt, vereinfacht gesagt, der Gedanke, dass bei Engpässen im Netz der Verkehr so geregelt wird, dass eine möglichst große Zahl von Nutzerinnen und Nutzer trotzdem mit der angebotenen Leistung möglichst zufrieden ist. Erreicht werden soll dies über das Netzmanagement. Dieses kann bei Engpässen Netzressourcen, wie etwa die Bandbreite, so zuteilen, dass QoE und QoE-Fairness maximal mögliche Werte erreichen.

Maximale Zufriedenheit für möglichst viele

Was Seufert konkret vorhat, ist, mit Hilfe des maschinellen Lernens (ML), Modelle zu entwickeln, die die hohe Komplexität der Wechselwirkungen zwischen Nutzer, Anwendungen und Netzen besser abbilden als bisherige Modelle. "Um die Quality of Experience für beliebige Internetanwendungen ermitteln zu können, muss man das Wechselspiel zwischen QoE und Nutzerverhalten messen und modellieren", sagt der Informatiker.

Zusätzlich plant er, die Methoden des maschinellen Lernens für den Einsatz auf verschlüsseltem Netzverkehr anzupassen. Verschlüsselung hat zwar den Vorteil, dass die Privatsphäre der Endnutzer gewahrt bleibt. Netzbetreibern bringt sie allerdings den Nachteil, dass diese nicht mehr so leicht erkennen können, welche Anforderungen Applikationen an das Netz stellen und wie zufrieden Endnutzer sind. "Durch angepasste ML-Modelle kann man zukünftig wieder genauere Abschätzungen über Applikationsanforderungen und Nutzerzufriedenheit vornehmen, die Privatsphäre der Endnutzer bleibt aber geschützt", sagt Michael Seufert.

Flexibel auf steigende Anforderungen reagieren

Hat man Probleme im Netz erkannt oder sind Beeinträchtigungen für die Endnutzer absehbar, muss die Netzkonfiguration – und damit die Behandlung der Datenströme im Netz – verbessert werden. Seufert will dafür maschinelles Lernen in Form eines verstärkenden Lernens einsetzen – in der Fachsprache Reinforcement Learning (RL) genannt. Netze sollen dabei lernen, wie sie sich automatisiert und flexibel selbst auf die jeweiligen Anforderungen anpassen können. Hier will die Forschungsgruppe die Grundlagen dafür erarbeiten, dass die eingesetzten RL-

Modelle für verschiedene Netzarten und unterschiedliche Netzbedingungen eine jeweils optimale Netzkonfiguration lernen können.

Ziel sei es letztendlich, Netze flexibel so auf die jeweiligen Anforderungen zuzuschneiden, dass QoE und QoE-Fairness der Nutzer bei unveränderten Ressourcen steigen. Dies komplementiere den Ausbau der Netzinfrastruktur und ermögliche es Netzbetreibern, die steigenden Anforderungen in den Kommunikationsnetzen zu bewältigen.

Michael Seuferts Lebenslauf

Dr. Michael Seufert hat an der Julius-Maximilians-Universität Würzburg Informatik, Mathematik, Wirtschaftsmathematik und Erziehungswissenschaften studiert. 2011 erlangte er das Diplom in Informatik und das erste Staatsexamen für das Lehramt an Gymnasien in Mathematik und Informatik, 2018 den Bachelor of Science in Wirtschaftsmathematik.

Stationen seiner Karriere waren das FTW Forschungszentrum Telekommunikation Wien (2012-2013) und das Digital Insight Lab am Center for Digital Safety and Security des AIT Austrian Institute of Technology GmbH in Wien (2018-2019).

Von 2013 bis 2017 arbeitete Seufert als wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Kommunikationsnetze (Prof. Dr.-Ing. Phuoc Tran-Gia) der Universität Würzburg. Mit einer Arbeit über die subjektiv empfundene Dienstgüte von adaptivem Videostreaming und Netzmanagement zur Verbesserung der QoE für diese Internetanwendung wurde er 2017 promoviert.

Seit 2019 ist er Akademischer Rat auf Zeit und Postdoc am Lehrstuhl für Kommunikationsnetze (Prof. Dr. Tobias Hoßfeld) der Universität Würzburg, seit Oktober 2022 leitet er dort seine DFG Emmy-Noether-Nachwuchsforschungsgruppe “ML-basiertes Monitoring und Management von QoE für nutzerzentrierte Kommunikationsnetze (UserNet)”.

Emmy-Noether-Nachwuchsgruppen

Das Emmy Noether-Programm der DFG soll herausragend qualifizierten Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftlern die Möglichkeit eröffnen, sich durch die eigenverantwortliche Leitung einer Nachwuchsgruppe über einen Zeitraum von sechs Jahren für eine Hochschulprofessur zu qualifizieren.

Kontakt

Dr. Michael Seufert, Lehrstuhl für Informatik III (Kommunikationsnetze), T: +49 931 31-88475, michael.seufert@uni-wuerzburg.de

AI Service Centre Berlin Brandenburg tryAI@HPI

In November 2022, The German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung) awarded four service centers for artificial intelligence. One of them is the AI Service Centre Berlin Brandenburg (KI-Servicezentrum Berlin Brandenburg), hosted at the Hasso Plattner Institute in Potsdam.

As artificial intelligence is a very broad field, we will focus on its currently most popular form: machine learning (ML). Our centre's main goal is to provide help in taking the second step in using machine learning (ML): A lot of potential users of ML have take some first steps, for example, by experimenting with ML techniques on a small scale, following popular tutorials. On the other hand, there is a lot of material available for an experiment user population, catering to experts in the field. But there is not much help available for an intermediate expertise level, for users who are interested in taking a second step but are not yet experts.

To address the needs of such users, this service centre will provide opportunities to try out AI in various forms, with proper support and consulting. We intend to support users in the whole lifecycle of their ML applications: from identifying possible goals, curating data, using and fine-tuning pre-trained models, selecting proper training algorithms, to choosing and configuring a proper infrastructure, deciding between on-premise or cloud-based setups.

We will support these consulting activities by research along two dimensions: methods and operations. In methods-oriented research, we plan to look into some of the topics mentioned above like pre-trained models, and in addition topics like training at the edge or energy-efficient ML. In operations-oriented research, we look at resource-management approaches for an infrastructure that has to deal with ML load as well as conventional load, in various forms. E.g., how to share resources between interactive, explorative training load with typical batch processing.

Both research and consulting is supported by an dedicated infrastructure. We will deliberately configure it in a very heterogeneous manner, including various accelerators, CPU, or memory architectures, to provide an experimental environment both for users of our center as well as a research environment and testbed for, e.g., resource management approaches.

This project started in November 2022. At the time of this writing, the tentative schedule is to have a first instance of this new infrastructure available in the middle of 2023. We look forward to interacting with a wide range of users, not only from the Berlin-Brandenburg region.

DFG SPP 2378 "Resilient Worlds"

13 projects are funded within the DFG priority program Resilient Worlds (more information https://www.resilient-worlds.org):

1. Automated Resilience Verification and Resilience by Design
   - Lehrstuhl für Theoretische Informationstechnik, TU Munich
     Holger Boche (PI)
   - Lehrstuhl für Informationstheorie und Maschinelles Lernen, TU Dresden
     Rafael Schaefer (PI)
2. NIC-Level Co-Processors for Resilient Coded Networking and Computation
   - TU Munich
     Carle, Georg and Herkersdorf, Andreas
3. ResCTC: Resilience through Cross-Technology Communication
   - Telecommunication Networks (TKN), TU Berlin
     Falko Dressler (PI), Anatolij Zubow (PI)
   - FU Berlin
     Gerhard Wunder (PI)
4. One Code to Rule Them All: A Coding-Based Solution for Resilient Future Communication Networks
   - Deutsche Telekom Chair of Communication Networks, TU Dresden
     Frank H. P. Fitzek (PI), Juan Alberto Cabrera Guerrero (PostDoc)
5. Collective Resilient Unattended Smart Things (CRUST)
   - Sustainable Communication Networks (ComNets), University of Bremen
     Anna Förster (PI)
   - Secure Mobile Networking Lab (SEEMOO), TU Darmstadt
     Matthias Hollick (PI)
6. Resilient Power-Constrained Embedded Communication Terminals (ResPECT)
   - Telecommunications Lab, Saarland University
     Thorsten Herfet (PI), Kai Vogelgesang (PhD Student), Marlene Böhmer (PhD Student)

- Chair of Computer Science 4 (Distributed Systems and Operating Systems), FAU Erlangen
  Wolfgang Schröder-Preikschat (PI), Luis Gerhorst (PhD Student), Peter Wägemann (PostDoc)

7. ReNO: Resilient Integration of Machine Learning for Enhanced Network Operation

   - University of Kassel
     Oliver Hohlfeld (PI)
   - Technical University of Berlin
     Stefan Schmid (PI)

8. Resilience meets secure networked control

   - Chair for IT Security and Cryptography, University of Wuppertal
     Tibor Jager (PI)
   - Chair of Control and Cyberphysical Systems, TU Dortmund
     Moritz Schulze Darup (PI)

9. Resilience by multi-connectivity network design in industrial IoT environments (REINDEER)

   - Institute for Communications Technology, TU Braunschweig
     Eduard A. Jorswieck (PI)
   - Institute of Operating Systems and Computer Networks, TU Braunschweig
     Lars C. Wolf (PI)

10. Resilient Safety-Critical Systems through Run-time Risk Assessment, Isolation, and Recovery (RESURREC)

    - Chair of Computer Engineering, University of Passau
      Stefan Katzenbeisser (PI)
    - Applied Cyber Security Darmstadt (ACSD), Darmstadt University of Applied Sciences
      Christoph Krauß (PI)

11. Multi-Agent Reinforcement Learning Framework towards Automotive Resiliency and Survivability of Mission-Critical Networks against Volatile Resource Flow

    - Decision Making, University of Tübingen
      Setareh Maghsudi (PI)

12. Resilient Communication with Programmable Hardware (ReCoPro)

- Kommunikationsnetze, University of Tübingen
  Michael Menth (PI), Steffen Lindner (PhD Student)

13. Coordination Funds

- Telekommunication Networks (TKN), TU Berlin
  Falko Dressler (PI)

BMWK project RESISTANT

Project in the BMWK Luftfahrtforschungsprogramm VI-2: Resilient Zero-Trust Avionics Platform supported by Digital Security Twins and Aircraft-SOCs (RESISTANT)

Consortium: Airbus Defense and Space GmbH, Fraunhofer SIT, Fraunhofer AISEC, IABG mbh, IFAK e.V., Siemens AG, Universität Hamburg (Prof. Dr. Mathias Fischer), Universität Stuttgart (Prof. Dr. Björn Annighöfer)

In RESISTANT, the zero-trust principle is to be transferred to the safety-critical avionics sector. This allows great flexibility in integrating software and hardware from the COTS domain, since non-trust is the basic assumption and the platform can deal with it. This is done by adding missing IT security and zero trust mechanisms to existing platforms and integrating them into a secure ”platform-of-platforms”. For safety-critical functions, the PAFA-ONE project's self-organizing platform will be enhanced, and for non-safety-critical functions and ground IT infrastructure, the DELIA project's hypervisor-based platform will be enhanced. These new platforms will additionally allow flexible positioning of critical services and provide monitoring functionality. This will allow increased fault and attack tolerance by reconfiguring network services and restoring the original redundancy as a result of a failure or attack. This requires a paradigm shift in the HW and SW design of such a computing platform, which will be investigated in the safety-critical and non-safety-critical domains. Aviation-grade zero-trust infrastructures and mechanisms need to be developed and validated, and also the relation to certification regulations in terms of cyber security needs to be shown. In addition, the platform will provide the necessary monitoring and intervention capabilities for the security twins and ASOC.

Based on the new zero-trust platform, an Aircraft Security Operation Center (ASOC) is being designed that will allow detailed monitoring of aircraft and entire aircraft fleets. To this end, the monitoring results are to be used to generate as well as to compare digital (security) twins for the detection of (unknown) errors and attacks, but also for risk assessment and the determination of suitable options for action. Since live, high-bandwidth communication with the aircraft will continue to be available only to a limited extent in the foreseeable future, the alerts about cyber attacks resulting from detailed platform monitoring must first be processed locally in the aircraft in order to be able to take countermeasures as locally as possible (example: exclude compromised components from the on-board network). Once the aircraft has access to the communications infrastructure (e.g., airport), collected alerts are sent to an ASOC and correlated and processed across the entire aircraft fleet using artificial intelligence (AI) and machine learning.

BMBF project FIIPS@HOHE

BMBF project in the programm IoT security in smart home, production and sensitive infrastructures: Ein Frühwarn-, Informations- und Intrusion Prevention-System für die Sicherheit privater Heimnetze FIIPS@Home)

Consortium: Universität Hamburg (Prof. Dr. Hannes Federrath, Prof. Dr. Mathias Fischer), Goethe-Universität Frankfurt am Main (Prof. Dr. Kai Rannenberg), Tenzir GmbH

Private networks have become a worthwhile target for hackers. In addition to security vulnerabilities in routers, the trend toward smart homes and the Internet of Things (IoT) is also responsible for this. Home networks offer multiple opportunities for infiltration through sometimes flawed and often poorly secured IoT devices, outdated PCs, and vulnerable services. More and more smart devices (e.g., TVs, vacuum-cleaning robots) collect data about the living conditions of residents and evaluate it ”to improve the service” or for advertising purposes. IoT devices are often not developed with security in mind, as they are intended to be inexpensive, resource-saving and uncomplicated (via plug-and-play) to integrate into the home network. Compromised IoT devices are the starting point for further attacks, e.g., by botnets. With the increasing importance of the home office in public authorities and companies, insecure devices in home networks are thus also becoming a serious threat to companies.

FIIPS@Home will develop a collaborative early warning, information and intrusion prevention system (FIIPS) and make it available to home users. For low-threshold entry, a free mobile application (FIIPS app) will be provided that gives an overview of the devices in the home network, performs simple vulnerability scans, and thus creates problem awareness for IT security risks in the home network. As a second expansion stage, an active sensor component (FIIPS stick) is being developed that can be easily installed on inexpensive USB compute sticks. This is to be constantly present in the home network, determine device fingerprints and continuously detect attacks on the home network. The third stage of expansion for the best possible protection is an active middlebox that can separate connections and seal off subnetworks.

KuVS Newsletter

Event Reports

KuVS - AI in Networking Summer School 2022

This year, KuVS organized a new edition of its well-recognized summer school series. Frank Kargl, Olaf Landsiedel and Amr Rizk jointly organized and prepared a highly interesting program on the topic of "AI and Machine Learning in Communication Networks". Generous support came from GI KuVS and the DFG Collaborative Research Centre 1053 MAKI.

The aim of this summer school was to introduce fresh PhD students to currently relevant topics in the intersection of programmable networks and AI/machine learning. Challenged by the high infection rates in the winter 2021/22, the organizers decided to divide the summer school into two parts, an online event in February and an in-person week in July 2022. The first part of the summer school was a Spring Mini-Course starting with an introduction to the state of the art in AI and machine learning and then including talks by renowned experts on topics like decision making in network management, network and distributed systems programming and boosting network applications using machine learning techniques.

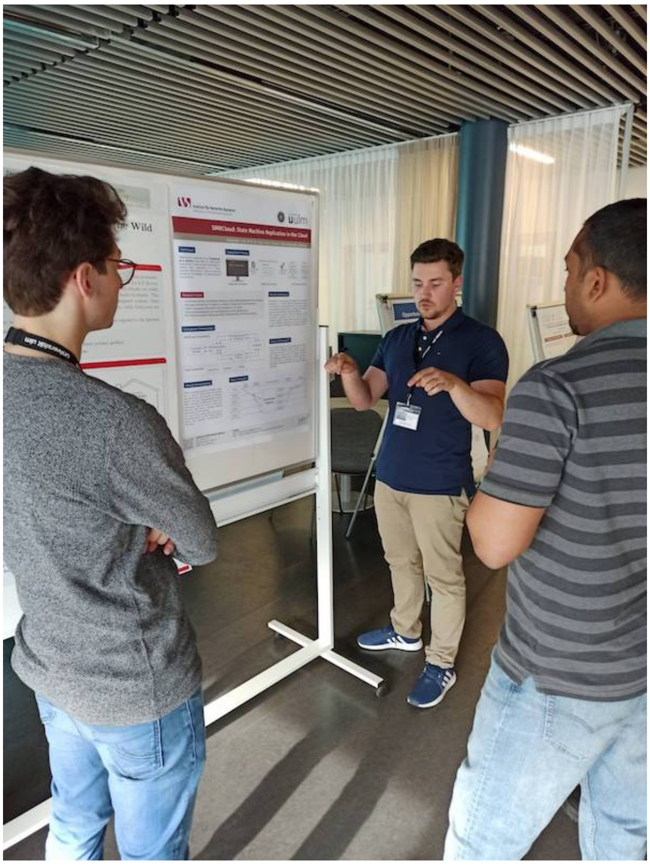
Specifically, the Mini-Course consisted of the following series of 90-minute lectures:

- Vasileios Belagiannis, Ulm University, Machine learning and deep learning basics
- Andreas Blenk, Technical University of Munich, Need for Speed: Applying Machine Learning to Network Management
- Carsten Binnig, Technical University of Darmstadt, Learned DBMS Components 2.0: From Workload-Driven to Zero-Shot Learning
- Aaron Ding, TU Delft, Bring Intelligence to the Edge: Lessons and Roadmap for Edge AI
- Fabien Geyer, Technical University of Munich, Performance Evaluations of Computer Networks with Graph Neural Networks
- Nic Lane, University of Cambridge, Federated Learning 101 and Research Opportunities using Flower
- Konrad Rieck, Technische Universität Braunschweig, Not that smart! Security Vulnerabilities in Machine Learning
- Stefan Schmid, Technical University of Berlin, Principles of self-* communication networks: data-driven optimization and verification
- Tanja Zseby, Vienna University of Technology, Machine Learning for Network Security

While the online event was mostly focused on presentations, the in-person event, which happened in July 2022 at Schloss Reisensburg near Ulm, was fully focusing on interactions and discussions. It included two Ph.D. poster sessions, a talk on paper reading/reviewing by Andreas Blenk followed by an extensive Shadow TPC hands-on sessions, research problem formulation and a tutorial on adversarial machine learning by Stephan Kleber. The summer school concluded with a hackathon on problems that were pitched by the PhD students themselves.

To complement this very demanding and exhausting schedule, we spent a half-day visit to nearby Legoland Deutschland where attendees could visit many famous European places and regions replicated in miniature-scale with Lego bricks or join many of the other attractions the park offers. As the temperatures on that day were well beyond 30 degrees, still everyone was happy to arrive back in the comparatively cool walls of the castle for a barbecue dinner.

Reykjavík Summer School on Secure and Reliable Distributed Systems



Vom 13. bis 23. Juni 2022 fand eine Summer School zum Thema sichere und zuverlässige Verteilte Systeme an der Universität Reykjavík in Island statt. Die Organisatoren Prof. Franz J. Hauck (Univ. Ulm) und Hans P. Reiser (Univ. Reykjavík) konnten ca. 20 Teilnehmer und Teilnehmerinnen aus fünf Ländern begrüßen. Die Summer School wurde vom DAAD unterstützt, so dass keine Teilnahmegebühren anfielen. Für Unterkunft und Verpflegung mussten die Teilnehmenden jedoch selbst aufkommen.

Zwölf internationale Dozierende lehrten eine bunte Mischung von Aspekten zum Themengebiet, z.B. verschiedene Aspekte zu State-Machine Replication und Blockchains, Sicherheit und Privacy, Testen und Benchmarking. Als interessantes Anwendungsfeld wurden beispielsweise künftige Energienetze thematisiert. Das Programm wurde abgerundet durch eine Postersession der Teilnehmenden, die im Rahmen eines gemeinsamen Abends stattfand. Gut aufgenommen wurden auch die Kurzvorträge der Dozierenden zu einem brandaktuellen Forschungsthema mit anschließender Diskussion. Eine gemeinsame Exkursion zu den isländischen Naturattraktionen ließ Raum für ganz andere Erfahrungen aber auch zu fachlichem und privatem Austausch unter Teilnehmenden und Dozierenden.

KuVS Calls and Announcements

In this section you find an overview on calls for papers and participation in the german-speaking area.

IEEE ICC™

IEEE ComSoc IEEE

IEEE International Conference on Communications

Roma Convention Center
May 28 - June 1, 2023

Sustainable Communications for Renaissance

Call for Papers

2nd Int. Workshop on Green and Sustainable Networking (GreenNet 2023)

Energy efficiency and **sustainability** have become of paramount importance in all human activities. Regarding ICT, it has been long recognized that its impact on helping reduce the carbon footprint of other activities can be significant; then, it would be odd if the same principle would not apply to ICT itself.

The goal of the **2nd Int. Workshop on Green and Sustainable Networking (GreenNet 2023)** is to address **emerging concepts and challenges** related to energy efficiency and sustainability for networked services, by pursuing sustainability in the context of ongoing developments such as 5G and beyond, 6G, usage of AI/ML or distributed ledger solutions and with different network access technologies.

To this aim, the Workshop will also address advanced traffic and power models, as well as management and control strategies, along with Application Programming Interfaces (APIs), to be used for the lifecycle management and optimization of Physical and Virtual Network Functions, the creation and dynamic reconfiguration of network slices, and the balance between sustainability in terms of energy efficiency and performance.

Furthermore, the goal is to not only consider an energy efficient and sustainable access network but complete network, monitoring, and management solutions from data generation to data processing and further usage.

The trade-off between availability, resiliency, programmability, and energy efficiency is a key challenge. Monitoring methods and metrics for power consumption, energy efficiency, as well as sustainability are important, as well as benchmarking of solutions based on well-defined KPIs.

TOPICS OF INTEREST

We seek original completed and unpublished work not currently under review. **Topics of interest include, but are not limited to:**

- Traffic modeling and prediction for performance and power representation
- Management and control mechanisms for the dynamic optimization of the trade-off between power, energy efficiency, sustainability and performance, availability, resilience
- Benchmarking of solutions w.r.t. energy efficiency and sustainability based on KPIs
- Sensor and industrial automation networks
- Evolutionary strategies for the achievement of 6G energy-efficiency KPIs and Quality of Information improvement
- AI/ML techniques for power and performance management in virtualized environments
- AI/ML for slicing energy efficiency, fog/cloud MEC virtualization, self-x technologies, adaptation, automation, and zero-touch
- Architectural solutions toward network sustainability
- Energy-efficiency and sustainability in all parts of networked services
- Multi-technology solutions
- Coping with the end of Moore’s law
- Role of standardization including network energy efficiency and sustainability metrics

PAPER SUBMISSION

All papers for Workshops should be submitted via EDAS.
Full instructions on how to submit papers are provided on the IEEE ICC 2023 website:
https://icc2023.ieee-icc.org/

Important Dates

Paper Submission Deadline
20 January 2023

Acceptance Notification
06 March 2023

Camera Ready
15 March 2023

Registration for Accepted Papers
15 March 2023

Workshop Date
28 May or 01 June 2023

Organizing Committee

Roberto Bruschi
(University of Genoa, CNIT, Italy)
Franco Davoli
(University of Genoa, CNIT, Italy)
Hesham ElBakoury,
(Futurewei Technologies, Santa Clara, USA)
Timothy O'Farrell
(University of Sheffield, UK)
Tobias Hoßfeld
(University of Würzburg, Germany)
Frank Loh
(University of Würzburg, Germany)

Workshop Website

https://sites.google.com/view/greennet2023/home

WueWoWAS'23 in Würzburg

WueWoWAS'23 is a three-day workshop on next-generation communication networks. The goal of the workshop is to provide attendees with an opportunity to foster both their understanding of the current state of the art and to learn from experienced researchers in the field.

The KuVS Fachgespräch - Würzburg Workshop on Modeling, Analysis and Simulation of Next-Generation Communication Networks (WueWoWAS'22) focuses on preliminary and ongoing research (or previously published hot topic papers) on next-generation communication networks. General topics include but are not limited to

- Next-generation network architectures and services: 5G, 6G, IoT, Industrial networks
- Concepts for future networks: softwarization, edge computing, AI and ML, automation.
- Evaluation of performance, reliability and resilience: measurements, modeling, simulation, analysis on QoS, QoE, energy efficiency, etc.

The workshop will take place in-person in Würzburg, Germany from 28.06.2023 until 30.06.2023. Last years workshop program can be found on the workshop website: https://lsinfo3.github.io/WueWoWas2022/

Calls for Papers and Presentations

- **2nd Workshop on Secure and Reliable Communication and Navigation in the Aerospace (SRCNAS)**
  in conjunction with the 24th IEEE WoWMoM Boston, Massachusetts, USA
  June 12-15, 2023 (half or one-day workshop)
  Paper Submission: January 31, 2023
  Acceptance Notification: March 31, 2023
  Camera Ready Submission: April 15, 2023
  https://www.unibw.de/code/events/srcnas-workshop/

- **20th Conference on Detection of Intrusions and Malware & Vulnerability Assessment**[3],
  July 12-14, 2022 Hamburg, Germany
  Paper submission (Cycle 2): February 1st, 2023
  Notification (Cycle 2): April 5th, 2023
  Camera-ready deadline: April 19th, 2023

[3] https://dimva2023.de

Fun

How 2 Shor10 English Texts

Riddles Based on a "Mathematically Oriented Reform" of English Orthography

Rolf Windenberg (alias: Nigel Fred Brown)

The Rules:

1. Usage of mathematical symbols and of numbers
2. Capital letters are pronounced as in the alphabet

Examples:

(Trafalgar)^2 [meaning: Trafalgar Square]
$\sqrt{66}$ [meaning: Route 66]
Y R U so Z 2dA ? [meaning: why are you so sad today ?]

The Riddles *(Solutions, see on next page)***:**

- *Beginners:* **U Z th@ U R so tired**
- *Playing with Capital Letters:* **gRdN**
- *Advanced Persons:*
  he had 4got(10) 2 repEt the nU –on @ home
- *Experts:*
  he's afr8 of no 1 + ∀way6 tremely cool, 2
- *Geniuses:*
  U sL melons; could I get a <1/4ree persons?

Fig. 1: Illustration to assist the reader in solving the fourth riddle (source: [1])

[1] Windenberg, R., Hasselfang, R.W.: How 2 Shor10 English Texts. Shaker Media Verlag, Düren, ISBN 978-3-95631-590-9, 2017

Solutions of the riddles (by Rolf Windenberg):

- you said that you are so tired [because: *U*-*Z*-th-*@*-*U*-*R*-so-tired]
- garden [because: g-*R*-d-*N*]
- he had forgotten to repeat the lesson at home [because: he-had-*four*-got-*ten*-*two*-rep-*E*-t-the-*less*-on-*@*-home]
- he's afraid of no one and always extremely cool, too [because: he's- afr-*eight*-of-no-*one*-*and*-*all*-way-*six*-tremely-cool,-*two*]
- you sell melons; could I get a smaller one for three persons ? [because: *U*-s-*L*-melons; could-I-get-a-*smaller*-*one*-*fourth*-ree-persons ?]

KuVS Newsletter

Next Newsletter - Deadline May 15th

Next newsletter : 06/2023

Deadline for submissions and contributions : 15th May 2023

We ask you for submissions in English. Topics can be from the following time frame: December 2022 - May 2023

- Fachgruppe KuVS
  - Geschäftsberichte der GI – KuVS – Fachgruppe
  - ...
- News from the working groups
  - Dissertations
  - Awards
  - News form persons
  - Open positions
  - ...
- New projects (DFG, BMBF, KMU, etc.)
  - Initiatives
  - Larger projects
  - ...
- Calls and news from events, conferences, etc.
  - Reports (Conferences, workshops, Fachgespräche, Dagstuhl, doctoral summer/winter schools, ...)
  - Call for papers and participation (conferences (supported by or hosted in Germany/Austria/Switzerland), Fachgespräche, Summer Schools, ...)
  - ...
- Announcements and important dates

The preferred submission format is text, e.g., using markdown language. Call for papers can also be submitted as PDFs.

Submissions should be done by sending emails to the editors:

mailto:oliver.hohlfeld@b-tu.de mailto:mathias.fischer@uni-hamburg.de

mailto:corinna.schmitt@unibw.de mailto:andreas.blenk@tum.de