Kommunikation und Verteilte Systeme KuVS

KuVS Newsletter

Contents

KuVS Newsletter

KuVS Newsletter

Editor Message

Dear KuVS members,

we welcome you to the 13th edition of the KuVS newsletter, which is our third overall newsletter in pandemic mode. However, the country is now slowly opening up again. Therefore, also the hope increases that after all the virtual conferences in the last months, our class reunion NetSys (13-16 September in Lübeck) might take place in physical presence again.

Until then, 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.

Ihre Newsletter Editoren,
Oliver Hohlfeld
BTU Cottbus–Senftenberg
Mathias Fischer
Universität Hamburg

Corinna Schmitt
Universität der Bundeswehr München
Andreas Blenk
TU München/University of Vienna

KuVS Newsletter

Fachgruppe KuVS

Movement of persons

- **Prof. Dr.-Ing. Christoph Sommer** accepted an offer from TU Dresden as W3 full professor and chair of “Prozessmodellierung für vernetzte technische Systeme” (Networked Systems Modeling); more information is available on nsm.inf.tu-dresden.de.
- **Prof. Dr.-Ing. Amr Rizk** accepted an offer from Universität Duisburg-Essen as Professor of Computer Science (tenured) in the area of “Applied Informatics” leading the group of “Networks and Communication Systems” in April 2021; more information is available on FG NCS.

News from the Working Groups

3.1 Awards

"Æternum" was Awarded the Best Paper Award at IEEE International Conference on Blockchain and Cryptocurrency in 2021. The Communication Systems Group CSG, Department of Informatics IfI, University of Zürich UZH, Switezrland did show presence at ICBC 2021 with three accepted papers overall. Out those the full paper entitled "Æternum: a Decentralized Voting System with Unconditional Privacy" (to appear in https://ieeexplore.ieee.org/), researched and organized by Christian Killer with the team of Markus Knecht, Claude Müller, Bruno Rodrigues, Eder Scheid, Muriel Franco, Burkhard Stiller was awarded out of 226 papers submitted with the ICBC 2021 Best Paper Award.

This work is part of the larger project on "E-Voting: Blockchain-based Remote Electronic Voting", which started in 2018 to design, prototype, and evaluate the feasibility of deploying a Blockchain-based Remote Electronic Voting system, serving as a fully decentralized and secure platform for running eVoting.

KuVS Newsletter

3.2 Finished Habilitations

3.2.1 Dr. Corinna Schmitt

University of Zurich, WWF - Universität der Bundeswehr München

Title: Trust & Security in IoT: Monitoring with Constrained Devices

Abstract: Today nearly every device is connected directly or indirectly with the Internet leading to a network of networks building the so called ”Internet of Things” (IoT). The devices used show manifold diversity concerning resources, operating systems and communication standards. Usually they are configured to report measurements periodically and for a long period of time resulting in a big amount of data including sensitive information (e.g., GPS, IP addresses, names). These circumstances would not be a problem at all if the IoT would be a trustworthy environment. Looking at the news the reality is different; information becomes public due to hacking or misconfiguration of devices, standards and services used. Especially, the rise of third-party services, which might not be trustworthy but user friendly and the increased awareness of users concerning privacy make the situation even more complex. From the legal point of view, the rights of data owners are now increasingly protected and supported, either by appropriate consumer associations or by the EU General Data Protection Regulation (GDPR). However, users are still not enough informed about what happens with the data gathered as soon as they leave the controlled and owned environment, for example, when using an App of a third-party service provider to visualize their data. Questions concerning data owners are manifold such as ”Can I trust the third-party service provider that my data is only used for authorized processing based on signed contract?”, ”Is my data processed in a secure manner?”, and ”If data deletion is requested by me, can I be sure that it is really deleted and, thus, forgotten?”.

Therefore, this habilitation establishes a common understanding of the IoT, especially about challenges caused by constrained (= lightweighted) devices and concerns raised by users. Further, it presents an overview of communication standards used in the IoT show- ing that the IoT landscape is very complex and no clear layered architecture is identified yet. Thus, this habilitation specifies such an architecture for the IoT by defining clear layers and functional characteristics per layer. With this architecture and knowledge in place, a security analysis of the current situation is performed with special focus on how foreigners can get access to gathered data. Further, tools and techniques (e.g., attacker models, cryptography) are recommended to overcome the existing security problems in general but might not be applicable all the time (e.g., due to too less resources or other obligations of standards or algorithms use). The security issue becomes highly relevant when looking at constrained networks as part of todays IoT. Such constrained devices might become overwhelmed soon when performing complex security because they have limited computational capacity and memory in place. Thus, this habilitation focuses on lightweighted solutions securing communication between constrained devices. Further, due to the increasing mobility of users and the request to access the network and owned

data from everywhere in the world, outside services and interfaces need to be integrated in the environment. Such services should regulate the access to the network and its collected data leaving the complete control to the network and data owner in order to integrate a trustworthy service. Therefore, another focus of this habilitation is set on user authentication mechanisms in order to establish a trustworthy outside service fostering End-to-End (E2E) security beyond the classic boarders of a constrained network. This means only authorized persons can get access to the network and the network/data owner can grant, update and revoke privileges immediately. In turn this reduces the involvement of a third-party, i.e. administrator, to a minimum and ensures complete control to the network/data owner.

In order to prove that such assumptions and expectations can be fulfilled, a SmartHome/ SmartBuilding scenario is selected for the practical part of this habilitation. This scenario represents one of the famous application areas in the IoT and needs to address all afore- mentioned identified concerns and requests of the users. A constrained network represents the data source where periodically environmental data (e.g., temperature and humidity) is collected, transmitted in a secure manner to a gateway component which publishes the data gathered via a trustworthy service to authorized users. With this setup a trustworthy and flexible IoT framework to monitor environmental data with constrained devices is established, called SecureWSN (Secure Wireless Sensor Network). As SecureWSN is requested to be trustworthy it is assumed that trust is gained by a combination of privacy, security and transparency support realized in by different parts of SecureWSN's component. It is shown that for SecureWSN can address all identified user concerns including E2E security, privacy and trust support, mobile access, and complete data control by the network/data owner. Further, SecureWSN allows immediate request handling in order to react in time in emergency cases or to update granted privileges to avoid misuse of authorized access. In a first step an analysis of existing components (e.g., data format, security solution for device to device communication, and gateway functionalities) is performed, identifying the extensions and updates needed to address user's concerns and request (e.g., mobility support, heterogeneity support of devices, secure communication, and complete data control). In a second step design decisions are specified leading to requirements that need to be met by SecureWSN and a list of tasks that need to be modulated, implemented and integrated. Third, the tasks are addressed and realized having all constrains and assumptions in mind. Finally, each is evaluated to prove that SecureWSN faces all identified challenges and requests establishing a trustworthy and flexible IoT framework for constrained networks monitoring environmental data.

For more details about SecureWSN and publications around this topic check out the project's page.

3.3 Finished PhD Theses

3.3.1 Bruno Bastos Rodrigues

Faculty of Business, Economics and Informatics WWF of the University of Zurich UZH

Title: Blockchain Signaling System (BloSS)

Distributed Denial-of-Service (DDoS) attacks are one of the major causes of concerns for communication service providers. When an attack is highly sophisticated and no countermeasures are available directly, sharing hardware and defense capabilities become a compelling alternative. Future network and service management can base its operations on equally distributed systems to neutralize highly distributed DDoS attacks. A cooperative defense allows for the combination of detection and mitigation capabilities, the reduction of overhead at a single point, and the blockage of malicious traffic near its source.

Cooperative defense systems face many challenges, such as deployment complexity due to high coordination overhead, reliance on trusted and stable channels for communication and the need for effective incentives to bolster cooperation among all involved parties. These challenges impairing the widespread deployment of existing cooperative defense are: (a) high complexity of operation and coordination, (b) need for trusted and secure communications, (c) lack of incentives for service providers to cooperate, and (d) determination on how operations of these systems are affected by different legislation, regions, and countries.

Driven by challenges imposed in a cooperative network defense, Blockchain Signaling System (BloSS) is presented as an effective and alternative solution for security management, especially cooperative defenses, by exploiting Blockchains (BC) and Software-Defined Networks (SDN) for sharing attack information, an exchange of incentives, and tracking of reputation in a fully distributed and automated fashion. Therefore, BloSS was prototyped and evaluated through local and global experiments, without the burden to maintain, design, and develop special registries and gossip protocols.

Evaluation results based on the local and global prototyping of BloSS highlight its effectiveness in signaling information of large-scale DDoS attacks. The world-wide scale evaluation experimenting the interaction between Autonomous Systems (AS) victim of DDoS attack and ASes acting as mitigators, presented an average of 97 seconds to complete all eleven possible outcomes of the BloSS protocol. The reputation assessment, based on the transparency of actions carried out on BC using Beta reputation and individual thresholds of trust for each member, showed that the defined protocol is capable of punishing malicious providers and benefiting providers by acting honestly.

The definition of contracts in BloSS stipulates the cooperative logic based on BCs and allows for the increase of trust among cooperative operators due to their transparent exchange of selected information and respective incentives on a per request basis. Overall, the main achievement and advantages reached with the design, prototypical implementation, and evaluation of BloSS include (a) the use of an existing distributed infrastructure, the BC, to flare white- or blacklisted IP addresses and to distribute incentives related to the mitigation activities requested. Furthermore, it provides a proof-of-concept for (b) a cooperative, operational, and efficient decentralization of DDoS mitigation services, and (c) a compatibility of BloSS with existing networking infrastructures, such as Software-Defined Networking (SDN) and BC.

3.3.2 Gaetano Manzo

Universität Bern

Title: Design and Evaluation of Floating Content Services for Vehicular Applications

By offloading vehicular data transfers from the telecommunication infrastructure to direct vehicular-to-vehicular communication, oppor- tunistic communications reduce infrastructure investment, overload, and latency. However, performance studies of opportunistic communication models in vehicular networks mainly focus on content persis- tence without accounting for the system conditions that enable desired performance, such as the effectiveness with which the content object is replicated and made available. Thus, how to efficiently engineer a vehicular application characterized by an opportunistic communi- cation model remains an open and challenging issue, crucial for the provision of high quality-of-service for vehicular applications.

This thesis aims to provide the tools to efficiently engineer a vehicular application characterized by opportunistic network models. We lever- age on Floating Content (FC), an infrastructure-less opportunistic communication scheme that binds the local dissemination of infor- mation. The contributions of this thesis are summarized as follows. First, we design an enhanced method for configuring FC schemes in vehicular ad hoc networks. Our results suggest that it is always pos- sible to find a reasonable size of the communication area such that the content object persists for the whole target duration. Second, we propose approaches for fine-tuning FC parameters (e.g., replication and caching) to guarantee a minimum target performance level while minimizing resources used, such as bandwidth and storage. Numerical evaluations show that our deep learning architecture provides content replication and storage strategies much more efficient than analytical techniques. Third, we provide an efficient communication scheme for content retrieval in vehicular networks that adapts to a wide range of network topologies and settings. Our approach outperforms delay- tolerant models reducing the content storage by 30

Our approaches lay the foundation for the practical use of vehicular applications based on FC schemes in real scenarios.

KuVS Newsletter

3.3.3 Newton Wafula Masinde

HHU Düsseldorf / Honda Research Institute Europe

Title: Peer-to-Peer Mechanisms for Fully Decentralized, Secure and Scalable Online Social Networks

Social media usage in the twenty-first century has infiltrated many facets of everyday life. Depending on the users' needs, different social media platforms are available, such as social networks like Facebook and LinkedIn, blogs like Tumblr and WordPress, microblogs like Twitter, and media sharing networks like YouTube. Over the past decade, social networks have received much attention due to reliance on a centralized computing platform. We summarize the concerns into two categories, accumulated costs due to centralization and security and privacy concerns, which arise because of a single provider controlling and owning all the data uploaded. The need to offset the costs results in user data monetization, leading to privacy concerns. The prevailing proposal is to move to a decentralized computing model, which we anticipate will address the problems. The federated network is a break from the centralized model, with services provided by several independent providers. Federation also enables the network to become resilient to censorship and significantly reduces the costs incurred due to centralization but does not eliminate it. Therefore, even with the federated networks, monetization of user data can occur, but not to the same extent as the centralized OSNs.

Therefore, the alternative is to fully decentralize the computing platform and use the peer-to-peer (P2P) model to address both concerns. It transfers the infrastructural costs from providers to the users who, now, directly provide the infrastructure to keep the network running. It also ensures the users' data is private and stored on the users' devices. Besides this, it ensures that the network remains resilient to censorship. However, using P2P technology comes with the challenge of developing mechanisms that improve service delivery to match that offered by centralized online social networks (OSNs).

To motivate P2P technology for implementing DOSNs, we review social networks in general to discover the user requirements and system (functional and non-functional) requirements. We derive the technical aspects from these requirements into a four-fold architecture composed of the overlay, the core framework, social network elements, and the graphical user interface. The overlay offers support for address management, routing, and security. Storage, communication, searching mechanisms, access control mechanisms, and monitoring functionality are the core framework layers' components. The social networking elements form the application component, and the goal is a modular design for extensibility. Furthermore, we conduct an in-depth study on P2P component mechanisms that fulfill the technical requirements. We then study several proposed P2P OSNs to compare the implementations and what they achieve to satisfy the user, system, and technical requirements.

We build our research on LibreSocial, a P2P framework for OSNs, that has been in continuous development since 2008. First we give an in full description of it, as it's structure has not yet been presented in that depth. We view LibreSocial as an ideal candidate for a P2P OSN, as it allows easily to be extended to address the challenging demands that we face. Additionally, LibreSocial fulfills the defined technical aspects using a modular design to achieve a zero-trust network. We then conduct detailed benchmarking tests on LibreSocial. The tests aim to reveal the interaction between the social network elements with one another and the underlying services that the P2P components provide. We also seek to discover LibreSocial's ability to operate in the wild, how well it scales up and handles churn while remaining stable, and how the storage characteristics, particularly the number of replicas (replication factor), affect the performance of the application. We show that social network elements synergize well with one another, and the underlying services offered by the P2P components provide adequate support for the network. We also show that the network scales up to 2000 nodes without service degradation and handles churn well while remaining stable. Additionally, our results on the impact of the replication factor indicate a need to increase the number of replicas as the network scales up to maintain quality service.

As a way of improving service delivery, we propose three mechanisms. The first mechanism is metadata-based search techniques to solve retrieving of documents stored in a distributed data structure, such as a linked-list or set, using a multi-attribute query. We present two search techniques exhaustive and first-match, and four join algorithms Simple LocalJoin, Parallel LocalJoin, asynchronous NetworkJoin, and BloomJoin. We also consider three distributed data structures, binary tree, deep tree, and customized broad tree. We show that the appropriate combination of the search technique, join algorithm, and distributed data structure is necessary to achieve optimum local and network performance.

The second mechanism we propose is a social caching mechanism that takes advantage of social data to improve data availability. Using this mechanism, we aim to decrease the number of overlay requests by using the social interaction data to implement active dissemination for frequently accessed data and caching this in a social cache. We implement three strategies for selecting users whose data is to be cached, namely, random, trend, and social score selection strategies. We show that the social score strategy is the most advantageous. Using social score strategy, we implement a social cache mechanism and show that coupled with the regular cache, we can achieve 99% cache-based retrievals, but at some cost to the network due to the combination of active data dissemination and regular updates to the regular cache for freshness.

The last mechanism we propose is a capacity management protocol to address the social network's heterogeneous nature by differentiating strong nodes and weak nodes. In a social network, users connect with different devices having varying capacities (memory, bandwidth, and processing power). Further, the type of connection (LAN/WLAN or metered) is significant. Therefore low capacity devices or devices connecting via metered connections are considered weak nodes. To ensure a stable network, we aim at preventing the weak nodes from participating in routing storing of replication data. We show that, with the capacity management protocol, this is achievable. We also show that it is possible to have up to 75% of the network composed of weak nodes and maintain a stable network, although there will be some service delivery degradation.

In conclusion, in this work, we identify and elaborate on the main concerns raised with the current popular OSNs leading to proposals for considering decentralized solutions, specifically

P2P. We give the reasons for selecting the P2P platform and discuss the technical challenges of such a move. We then conduct a study to discover the necessary user and system requirements required to define the technical requirements for a P2P framework for OSNs. We present LibreSocial as a P2P-based OSN that fulfills the specified technical requirements, and provide a systematic and large-scale evaluation of LibreSocial. We then propose three mechanisms for improving service delivery, metadata-based search techniques for distributed data structures, a social caching mechanism for enhanced data availability and faster retrievals, and a capacity management protocol to support heterogeneous nodes. With these contributions, we address the open questions raised in this research.

3.3.4 Ermin Sakic

TU Munich / SIEMENS

Title: Analysis and Design of Distributed Control Plane Mechanisms in SDN-based Industrial Networks

This thesis analyzes the existing work, proposes, and evaluates novel designs surrounding the logically-centralized, physically-distributed Software Defined Networking (SDN) network control plane in industrial settings.

The motivation behind the presented work is two-fold. First, the recent rise in adoption of SDN in data-center and campus networks has sparked an interest in the corresponding technology transfer to the industrial domain. While the application of SDN for industrial use cases is well understood, necessary adaptation of SDN designs to fulfill the non-functional requirements and constraints of the industrial domain remains an open point. Second, recently proposed Ethernet extensions by the Institute of Electrical and Electronics Engineers (IEEE) 802.1 Time-Sensitive Networking (TSN) group improve the determinism of performance of distributed real-time applications, at the expense of an added network configuration complexity. Efficient management of the proposed TSN mechanisms can only be achieved by a centralized decision-making entity, equipped with admission control, scheduling, and planning logic. Future industrial networks will require an efficient interplay of data and control plane in order to enable strict End-To-End (E2E) latency, control plane response time, multi-tenancy and auto-configuration requirements imposed by the dynamic Industry 4.0 use cases. Combined with the prerequisite of robust operation, novel control plane designs are necessary in order to enable its guaranteed low response time while minimizing the associated deployment complexity.

Indeed, deployment of SDN in industrial scenarios requires catering for the issue of control plane dependability. The impact of distributed controller operation on resulting network performance is, however, under-investigated in existing literature. A provably robust logically-centralized industrial control plane design is necessary for its successful adoption in production settings.

We postulate the feasibility of using a highly-available and resilient SDN controller solution as an enabler of future softwarized industrial networks. To this end, we provide an analysis of the availability, reliability and response time properties of the existing consensus-based solutions. In order to achieve the low response times, we propose multiple enhancements to handling flexibly-consistent control state updates at scale. We furthermore define mechanisms for tolerating semantic faults in replicated controller state independent of the root cause (e.g., software / hardware bug, malicious takeover or diverged controller state). The proposed designs are validated analytically and empirically. To simplify the deployment of the resulting control plane, we propose a novel automated bootstrapping approach that omits any data plane dependencies, so to isolate the control and data plane responsibilities, providing for easier verification and analysis of the system's correctness.

Succinctly summarized, our thesis achieves four goals:

- Assessment and hardening of existing distributed SDN control plane designs: We provide the analytical guarantees for availability and response time metrics of state-of-the-art distributed SDN control plane proposals. Steady-state and transient analysis based on Stochastic Activity Networks (SANs) are used in dependability and performance evaluation. We furthermore assess corner cases impacting the correctness of existing control plane designs. In particular, scenarios of leader oscillation and unsuccessful election were reproduced with existing SDN controllers. To cater for and alleviate such issues, we propose for decoupling of the underlying failure detection procedure from controller state consensus.
- Design of a scalable fault-tolerant distributed control plane: We propose multiple designs for realizing a multi-controller SDN control plane that simultaneously enables a Fail-Stop-tolerant and scalable system operation. To this end, we introduce the notion of adaptive consistency, a state replication model that autonomously adapts to provide for a sufficient degree of consistency for the hosted SDN applications, under consideration of the constraints on the worst-case state divergence.
- Design of mechanisms for supporting reliable distributed control plane operation: To ensure correct handling of faults rooted in Byzantine events, we propose novel control mechanisms that guarantee a transparent system transition from faulty-to-stable state even if some controller replicas are computing unreliable outputs due to internal faults. The proposed control plane extensions optionally leverage programmable forwarding elements in order to minimize the footprint of controller instance replication.
- Automated bootstrapping of a highly-available and reliable distributed control plane: We propose two novel bootstrapping schemes to initialize a complex distributed system comprising arbitrary number of controller replicas. The in-band control plane is thus bootstrapped with availability guarantees - i.e., it is automatically protected against individual data plane and controller failures.

The majority of designs proposed in this thesis were evaluated under assumption of industrial network Key Performance Indicators (KPIs), i.e., they assume the respective typical topologies and parameter configurations. Nevertheless, the advantages of introduced designs apply to other domains, e.g., the data-center and campus SDNs.

3.3.5 Steffen Haas

Universität Hamburg

Title: Security Monitoring and Alert Correlation for Network Intrusion Detection

Attacks on IT systems can have network-wide impacts with tremendous consequences. For attack detection, the standard solution is to deploy an intrusion detection system (IDS). However, it reports too many alerts to be all analyzed by the security operations center (SOC), even with the help of alert correlation. This creates alert fatigue and the really sophisticated attacks, the advanced persistent threats (APTs), that trigger only a few inconspicuous alerts, go unnoticed. To mitigate the alert correlation problems, companies utilize security tools like security information and event management (SIEM) systems that correlate alerts and other security-relevant data. Although these systems provide extensive data analytics, they just summarize the overall security status of IT systems but fail to appropriately prioritize alerts and to make attacks in the alert data visible. A solution to achieve this is additionally impeded by the restricted visibility of the commonly deployed network intrusion detection systems (NIDSes), because not all attack aspects manifest in the network traffic. Furthermore, the NIDS location enables to capture the Internet traffic of the monitored network but not the traffic between hosts inside the network.

This dissertation presents mechanisms that enable a comprehensive detection and reconstruction of attacks. The novel contributions work towards a better overall detection accuracy at two different stages of the intrusion detection process. First, security monitoring is enhanced to produce high-quality monitoring data and to leverage it for an accurate reporting of alerts. Second, novel alert correlation mechanisms identify relations among the alerts and summarize the reconstructed attacks. In particular, a joint monitoring of hosts and the network correlates respective monitoring data in real-time. An extended visibility is established through the attribution of network flows to host processes. In addition, detectors leverage correlated network flows to robustly detect the characteristics of some distributed attacks despite restricted visibility in the monitoring data. The proposed alert correlation separates alerts belonging to high-volume attacks from the infrequent, i.e., spatially and temporally dispersed, alerts belonging to a stealthy APT. After aggregating and bringing together alerts of the same attack, they are correlated to reconstruct the attacks, highlighting the performed steps and how they interconnect. To scale with large networks, the proposed mechanisms integrate into a distributed monitoring and correlation platform that allows comprehensive intrusion detection when deployed to several locations inside the network. The deployment as a collaborative intrusion detection system (CIDS) is supported by another mechanism that efficiently exchanges summaries of alerts.

The developed approaches have been extensively evaluated individually and in combination with each other on the basis of real-world deployments, testbeds, and simulations. Furthermore, the contributions are discussed altogether along a detection pipeline. The overall system accurately detects attacks by correlating a variety of information. It achieved a real-time attribution for more than 96% of TCP connections in a real-world deployment. In realistic simulations, a peer-to-peer (P2P) botnet was detected robustly, as NetFlows covering the traffic from only 5% of the bots were sufficient. At the same time, the concise attack summary highlights attacks that threaten the network at large. Alert correlation experiments condensed real-world alerts into aggregations that correspond to 0.6% of the original amount of alerts. Using alert summaries reduced the exchange volume in a CIDS to about 1% of the full alert data.

3.4 Project News

3.4.1 Resilient Worlds

Resilient Worlds
Resilience in Connected Worlds – Mastering Failures, Overload, Attacks, and the Unexpected

In April 2021, the Senate of the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) established the Priority Programme "**Resilience in Connected Worlds – Mastering Failures, Over-load, Attacks, and the Unexpected (Resilient Worlds)**" (SPP 2378). The SPP is designed to run for six years in two phases.

The focus of the Resilient Worlds priority programme is, of course, on resilience. Citing from the SPP proposal, "[…] resilience is needed as the core property of the network infrastructure, from the Internet to the internet of things (IoT), from connected cars to complex cyber-physical systems (CPS) and resilience will be a primary research objective for the coming years. We expect that modern communication networks can deal with unknown and unforeseen events, both from within the network as well as from external sources. This requires a holistic view of the resilience problem, leading to appropriate and easy-to-handle solutions. Resilience evidently cuts through several thematic areas, such as information and network security, fault tolerance, software and hardware dependability, and network survivability […]"

The program committee consists of

- Falko Dressler, TU Berlin, School of Electrical Engineering and Computer Science, Telecommunication Networks
- Matthias Hollick, TU Darmstadt, Dept. of Computer Science, Secure Mobile Networking
- Milos Krstic, IHP, System Architectures Dept. and Uni Potsdam, Institute of Computer Science, Design- and Test Methodology
- Konrad Rieck, TU Braunschweig, Computer Science Dept., Institute of System Security
- Antonia Wachter-Zeh, TU München, Dept. of Electrical and Computer Engineering, Coding and Cryptography

We expect the call for proposals being published in June 2021. For more information, please see www.spp2378.de.

3.4.2 Adversarial Design Framework for Self-Driving Networks (ADVISE)

Principal Investigators: Dr.-Ing. Andreas Blenk, TU Munich, and Prof. Dr. Stefan Schmid, University of Vienna

Duration: 01.01.2021 - 31.12.2023

Link: https://www.ei.tum.de/lkn/research/dfg-advise/)

Funding agencies**:** DFG and FWF

Inspired by self-driving cars, the networking community is currently engaged in designing more automated and "self-driving" communication systems, aiming to overcome the cumbersome and error-prone manual approach to manage and operate networks. Ideally, such self-driving networks also allow to exploit the increasing flexibilities introduced by emerging new Internet technologies, such as software-defined and virtualized communication technologies. With these technologies, the networks allow to meet the stringent performance requirements of new networks (e.g., 5G and 6G) and workloads (e.g., low-latency tele-operation or high-bandwidth machine-to-machine type communication), by adapting to the context and demand.

The Internet, one of the largest and most complex artifacts built by mankind, has evolved organically over the last decades, and many design choices were taken based on experience and best practices. This project proposes a novel network framework to design and operate such networks, relying on the vision of such self-driving networks, and studying how to integrate Machine Learning and Artificial Intelligence concepts into existing networks. In order to overcome the potential concerns regarding the dependability of such Artificial Intelligence and Machine Learning approaches, we envision a hybrid solution which keeps the human in the loop. Hence, we first ask three fundamental questions in this project: how predictable are today's networks, i.e., user demands, workload traffic, and behavior of network functions? Can we make network design and algorithms data-driven and human interpretable? How to design a network framework that combines both, generative workload models and data-driven algorithms with guarantees?

The novelty of this project lies in the integration and application of Artificial Intelligence and Machine Learning on designing network algorithms. For the first time, Artificial Intelligence and Machine Learning should be integrated also in the testing and the developing phase of new networking solutions, and not only solely applied to solving problems. In terms of methodologies, we consider adversarial and game-theoretic approaches to test and optimize networks, to leverage the performance benefits from Machine Learning approaches while at the same time provide rigorous worst-case guarantees. Finally, a proof-of-concept implementation should demonstrate the new framework.

KuVS Newsletter

3.4.3 Dependability of Softwarized Networks

Principal Investigators: PD Dr.-Ing. habil. Carmen Mas Machuca, TU Munich, and Prof. Dr.-Ing. Wolfgang Kellerer, TU Munich

Duration: 01.05.2021 - 30.04.2024

Link: https://www.ei.tum.de/lkn/research/dfg-dependability-of-softwarized-networks/

Funding agency: DFG

Current networks require more flexibility and performance. Recent proposed solutions target network softwarisation (e.g., Software Defined Networking (SDN), Network Function Virtualisation (NFV)), which aim at reducing the complexity and specialization of hardware devices, by using commodity hardware combined with more complex software modules (e.g., SDN controller, network functions), which often run in a centralized position in the network. Not only the control plane, but also the data plane is being softwarized as proposed by the P4 concept. However, with the emergence of open source projects also for such critical network software, these software modules are developed by large and heterogeneous groups of programmers with different skills and expertise raising the risks of failure or interruptions when used by operators and providers. This project aims at proposing a framework to evaluate the dependability of software modules in softwarized networks and to advance solutions on how to improve their dependability. It is important to say that the project focuses on dependability studies based on the implementation and operation in networks, rather than pure software verification and validation techniques such as debugging or software quality control.

Dependability deals with the trustworthiness of a system by addressing the threats (including hardware and software faults, intended and casual faults), the attributes to assess the dependability (e.g., availability, testability) and means on how to enhance the dependability of the system. This project will study the dependability aspects of softwarized networks, focusing specially to the new and challenging software-related threats, and their impact on available attributes and means. For example, different SDN controllers are available, which differ not only on their capabilities and implementation, but also on the identified but yet unsolved bugs, the new release version process, the number and expertise of software developers, etc. In this project, we aim at proposing a methodology to compare different software modules and/or releases in terms of dependability and propose concepts on how the dependability could be improved (e.g., enhanced release process).

The objective of this project is to propose a dependability evaluation framework for softwarized networks. One challenge is to identify the new and more complex threats of softwarized networks, whose frequency and impact have been shown to be more harmful than well know threats. Another challenge is to propose new and more adequate metrics for a realistic dependability assessment. State of the art solutions are mainly focused on data plane dependability of traditional networks, by considering primarily particular and dedicated network components (e.g., switches, firewalls). However, these solutions are based on past well known threats. It has been shown that network softwarisation will cause new and challenging threats, which have to be modelled and included in the dependability assessment. For example, the clustering function of the controller, which enables load sharing among controllers as well as fault tolerance, has been identified as the cause of more than 20

In summary, the challenges we address are:

- Assess the quality and trustiness of a metric, which varies depending on the quality and trustiness of the input data, the type and accuracy of the used tool, etc.
- Identify the most important reliability- and security-related metric(s) mi that can be obtained from different models and define new ones that will improve the dependability evaluation.
- Find the most suitable dependability metric(s) depj definition as a function of the available metrics.
- Define a solid framework to perform a reliable and consistent evaluation of the dependability of software modules.

3.4.4 6G Zukunftslabor Bayern – 6G Future Lab Bavaria

Projektleitung: Prof. Dr.-Ing. Wolfgang Kellerer

Start: 01.05.2021

Dauer: 3 Jahre

***Fördergeber*:** Bayerisches Staatsministerium für Wirtschaft, und Energie

Figure 1: Copyright: TUM. Source: https://mediatum.ub.tum.de/652209?show_id=1601935

Während die Entwicklung und Realisierung der fünften Generation (5G) Mobilkommunikation in vollem Gange ist, beginnen in Forschung und Industrie bereits die konkreten strategischen Überlegungen für die folgende sechste Generation (6G) mit Zielhorizont im Jahr 2030. Die Wirtschaft und Wissenschaft im Freistaat Bayern sollen frühzeitig durch konkrete Grundlagenforschung in die Lage versetzt werden, 6G aktiv mitzugestalten und damit eine Vorreiterrolle einzunehmen. Erwartete wichtige Innovationssprünge werden in 6G hinsichtlich intelligenter und an die Umgebung anpassungsfähiger Kommunikation, Nachhaltigkeit, Verfügbarkeit und Sicherheit kritischer Infrastruktur erwartet.

An der Technischen Universität München ist am 1. Mai 2021 das 6G Pilotvorhaben „6G Zukunftslabor Bayern“ an den Start gegangen, das die wichtigsten Grundlagen für 6G erforscht und für weitere wissenschaftliche Untersuchungen, die wirtschaftliche Weiterentwicklung und Standardisierung aufbereitet. Die Ziele des 6G Pilotvorhabens sind, neuartige und grundlegende Mechanismen für 6G zu erforschen, ihre Realisierbarkeit in einer Proof-of-Concept Realisierung zu demonstrieren, sie hinsichtlich einer 6G Roadmap aufzubereiten und darin weiterreichende konkrete zukunftsweisende Forschungsfragen zu skizzieren.

Am „6G Zukunftslabor Bayern“ sind zwölf Professuren aus der Fakultät für Elektrotechnik und Informationstechnik und der Fakultät für Informatik beteiligt. Die PIs: Wolfgang Kellerer

(Projektleiter), Lehrstuhl für Kommunikationsnetze, Eckehard Steinbach, Lehrstuhl für Medientechnik, Holger Boche, Lehrstuhl für Theoretische Informationstechnik, Georg Carle, Network Architectures and Services, Klaus Diepold, Lehrstuhl für Datenverarbeitung, Reinhard Heckel, Machine Learning, Andreas Herkersdorf, Lehrstuhls für Integrierte Systeme, Gerhard Kramer, Lehrstuhl für Nachrichtentechnik, Carmen Mas Machuca, Lehrstuhl für Kommunikationsnetze, Jörg Ott, Chair of Connected Mobility, Georg Sigl, Lehrstuhl für Sicherheit in der Informationstechnik, Wolfgang Utschick, Methoden der Signalverarbeitung, Antonia Wachter-Zeh, Codierung für Kommunikation und Datenspeicherung.

Flankiert wird das „6G Zukunftslabor Bayern“ von weiteren Projekten der Bayerischen 6G Initiative. So das „Thinknet 6G“, eine Vernetzungsplattform, die alle relevanten nationalen und internationalen Stakeholder zum Thema 6G zusammenbringt. Die Zusammenarbeit erfolgt über Diskussionsforen und Workshops, die für alle offen stehen. Prof. Wolfgang Kellerer ist akademischer Sprecher und Peter Merz von der Firma Nokia der Sprecher aus der Industrie. Die dritte Säule der Bayerischen 6G Initiative bilden regelmäßige Ausschreibung für Verbundprojekte.

- http://www.6g-future-lab.de
- http://www.thinknet-6g.de

3.5 PhD Positions

The Distributes Systems Group at the Universität Kiel offers a PhD position on ”Networking and Edge AI” - see
https://www.ds.informatik.uni-kiel.de/en/news/open-phd-position-on-wireless-networking-

The Connected Mobility Group at the Technische Universität München offers a PhD position on ”Edge Resource Modeling and Management in 6G”
see https://www.in.tum.de/cm/jobs/

The Research Institute CODE announces several openings for PhD positions - see https://www.unibw.de/code/karriere:

- Moderne Identitätsmanagementsysteme im Rahmen von dtec.bw
- Bereich Quatenkommunikation im Rahmen von dtec.bw
- IT-Sicherheit - Cyber Range/Simulierte Netz Umgebung (akt. befristet auf 2 Jahre)
- Protokollbasierte IT-Sicherheitsanalyse im Bereich Taktischer Datenlinks (akt. befristet auf 3 Jahre)
- Programmanalyse und Systemsicherheit

The Austrian Institute of Technology offers different PhD positions - see https://jobs.ait.ac.at/Jobs

The Group for IT-Security for Software and Data at the Universität der Bundeswehr München offers a ”research position in the LIONS Project” by dtec.bw
see https://www.unibw.de/stellenausschreibungen/wissenschaftliche-mitarbeiterinnen-und-mi
fakultaet-informatik/inf-wm-e13-lions-dtec-bw.pdf

3.6 Faculty Positions

Several open positions are available also in 2021 at the Technischen Hochschule Ingolstadt - see https://www.thi.de/karriere/wen-wir-suchen

- Forschungsprofessur Big Data-Technologien
- Forschungsprofessur Business Development and Transformation Management
- Forschungsprofessur Intelligente autonome Flugführung
- Forschungsprofessur Intermodale Mobilität und Künstliche Intelligenz
- Forschungsprofessur KI-gestützte Luftfahrttechnik und Produktentwicklung

- Forschungsprofessur Technology Assessment and Cultural Management
- Professur Baubetrieb und Bauverfahrenstechnik
- Professur Elektronik und integrierte Schaltungstechnik
- Professur Medienpsychologie und Digital Marketing
- Professur Produktdesign
- Professur Software-Architekturen und Distributed Computing
- Professur Software-Entwicklung und Grundlagen der Informatik
- Professur Visual Computing und Multimedia

Event Reports

4.1 Bericht Capture-The-Flag - Cube Apocalypse (postponed from 2020)

Corinna Schmitt, FI CODE, Universität der Bundeswehr München

https://www.unibw.de/code/events/ctf_apocalypse/view

In the familiar Jeopardy format, our Capture the Flag event was held on April 23-24, 2001 completely digitally for the first time. To ensure that the teams can solve not only software challenges but also hardware challenges, as in previous years, we came up with something special: Each of the more than 30 registered teams received a care package with food, drinks, information, goodies and, of course, the hardware challenge.
To create as much live feeling as possible, a WebEx conference run parallel to the game interface during the entire event. This year, our Technical Director Prof. Wolfgang Hommel was in charge of the welcome and award ceremony.
For more details check out the event page.

Calls and Announcements

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

5.1 Overview on dates

Calls for Participation

- **Annual CODE Conference 2021** - Neubiberg, Germany, July 20.-22, 2021 (all-digital event): https://www.unibw.de/code/events/jahrestagungen
- **IFIP Networking 2021** - Espoo, Finland, June 21-24, 2021: https://networking.ifip.org/2021
- **International Workshop on Collaborative Cyber Security Education (CS-EDU)** - Vienna, Austria, August 17, 2021 (all-digital event): https://www.ares-conference.eu/workshops/cs-edu-2021/
- **1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain (SRCNAS)** - Vienna, Austria ,September 6, 2021 (all-digital event): https://concordia-h2020.eu/workshop-SRCNAS-2021/
- **6th IEEE European Symposium on Security and Privacy** - Vienna, Austria September 6-10, 2021 (all-digital event): https://www.ieee-security.org/TC/EuroSP2021/
- **17th International Conference on Wireless and Mobile Computing, Networking and Communications** (WiMob) - Bologna, Italy, October 11-13, 2021: http://www.wimob.org/wimob2021/
- **Conference on Networked Systems (NetSys 2021)** - Lübeck, Germany, September 13-16, 2021: https://netsys2021.org

5.2 Calls for Papers

5.2.1 CODE 2021 - Call for Ph.D. and Masters' Research Proposals

CODE 2021 (https://www.unibw.de/code-events/), July 20-22, Munich (this year remote event), features a scientific workshop on (early stage) Ph.D. as well as masters' theses research proposals in the area of IT security. Research proposals are short papers describing the current state of the student's research. Proposals from an early stage of the thesis are explicitly welcome and desired. The topic must be related to IT security research.

A proposal needs to include a clear description of the research problem and the chosen approach, argue why the problem is hard and the approach novel, and it has to outline the results achieved to date. Specific, low-level technical details are to be avoided. Papers should have no more than two (in exceptional cases three) authors: the student and one or two advisors. Each submission must be written in English and must comprise at least 4 and no more than 6 pages, including all references and figures/tables, in the LNCS paper format.

Authors will have the opportunity to attend the entire CODE conference, which is an invitation only event. The Ph.D. and masters' workshop will be fully virtual so that no travel costs incur. The registration is free of charge for the speakers of the workshop.

Submission Guidelines:

Authors are invited to submit their manuscripts via email to code@unibw.de. The manuscript must follow the Springer Lecture Notes in Computer Science (LNCS) guidelines (https://www.springer.com/gp/computer-science/lncs/conference-proceedings-guidelines). The submission should be original work by the authors, not be published or currently submitted for publication elsewhere.

Important Dates:

- Submission deadline: Jun 25, 2021
- Acceptance notification: Jul 09, 2021
- Camera ready deadline: Jul 16, 2021
- Day of workshop: Jul 22, 2021

5.2.2 WiMob 2021 - Call for Papers

The 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) is an international forum for the exchange of experience and knowledge among researchers and developers concerned with wireless and mobile technology. For seventeen years, the International WiMob conference has provided unique opportunities for researchers to interact, share new results, show live demonstrations, and discuss emerging directions in - Wireless Communication, - Wireless Networking, Mobility and Nomadicity, - Ubiquitous Computing, Services and Applications, - Green and sustainable communications and network computing and - Security on Wireless and mobile Networks.

WiMob 2021 will take place in Bologna, Italy, October 11-13 2021.

WiMob 2021 is soliciting high quality technical papers addressing research challenges in the areas of wireless communications, wireless networking, mobility, nomadicity, ubiquitous computing, services and applications. Papers should present original work validated via analysis, simulation or experimentation. Practical experiences and Testbed trials also are welcome.

WiMob 2021 will host FIVE parallel symposia, including but not limited to the following topics:

- Wireless Communications (WC)
- Wireless Networking, Mobility and Nomadicity (WNMN)
- Ubiquitous Computing, Services and Applications (UCSA)
- Green and Sustainable Communications and Network Computing (GSCN)
- Security on Wirelessand Mobile Networks (SWMN)

Important Dates

- Extended Deadline: June 21, 2021
- Notification of Acceptance: July 30, 2021
- Camera ready Date: September 15, 2021
- Conference: October 11-13, 2021

Instructions for Paper Submission

Authors are required to submit fully formatted, original papers (PDF), with graphs, images, and other special areas arranged as intended for the final publication. Papers should be written in English conforming to the IEEE standard conference format (two- column, 10 pt font, etc., including figures, tables, and references). The review submissions are limited to six pages, with two additional pages for final papers (additional charges may apply for additional pages). Conference content will be submitted for inclusion into IEEE Xplore as well as other Abstracting and Indexing (A&I) databases. Each accepted paper must be presented at the conference by one of the co-authors or a third party, otherwise it will not be indexed and archived through IEEE Xplore. Only timely submissions through EDAS at https://edas.info will be accepted. For more details, please visit the WiMob'2021 official website (http://wimob.org/wimob2021) and Facebook page for WiMob. Accepted papers will be published in the conference proceedings and presented for inclusion in IEEE Xplore Digital Library.

5.2.3 SRCNAS 2021 - 1st Workshop on Secure and Reliable Communication and Navigation in the Aerospace Domain

The digital revolution is here, transforming the way we live as it finds its way into a wide variety of domains including transportation, smart home, eHealth and knowledge transfer, but it also affects the way the airspace operates. New data-hungry applications, and increasing degrees of automation beg the question whether the available resources, like bandwidth, data formats, and radio standards are still adequate. This is particularly questionable in aviation, where data is produced, evaluated and distributed with ever decreasing latency, and these data is usually very sensitive, sometimes even safety-critical, but the underlying technical systems are often a half-century old. For these data, protection from unauthorized access, misuse, and manipulation is absolutely essential. Various statistics show that the communication backbone in aviation has proved a coveted target for cyber-attacks, particularly as the security infrastructure is largely outdated and data poorly secured, especially during exchange or update processes. Manifold investigations showed that also signaling used for navigation purposes became a target of attackers by tampering the signals (e.g., using radio interference or spoofing of navigation receivers), as it depends on satellite navigation, particularly GPS, as a low-cost, widely available source of reliable positioning. These examples call for a variety of solutions and technologies increasing safety & sustainability of the involved industry.

Therefore, this workshop deals with the topic of secure and trustworthy communication and navigation in aviation. Here, not only current vulnerabilities will be identified, but also concrete research results will be presented and discussed. While a few years ago, the airspace could only be accessed for commercial purposes by incumbent operators and the scope of communication was limited, it has already changed due to digitalization. It will change even more significantly with the arrival of new entrants in the air space, such as unmanned aerial vehicles. This means that in the near future a high number of aircraft will have to share common resources of space and data volume in unprecedented ways. Further convoluted by a lag in the development of international technical standards, as unmanned aerial vehicles will enter the system, these data will have to be analyzed or exchanged even faster between even more operators in order to sustain the safety and economic viability of aviation. We invite experts and researchers from various areas of aeronautics and telecommunications to discuss the topic and specify any challenges and frameworks for the future. Selected papers will be presented at the workshop and included in the EuroS&P 2021 proceedings.

For further details about the Workshop check on the respective webpage https://concordia-h2020.eu/workshop-SRCNAS-2021/.

Topics of interest among others in the investigates area are:

- Threat propagation in safety-critical networks
- Security risk assessment, mitigation, assurance and testing
- Model-based security engineering

- Security strategies and solutions (e.g., secure communication and navigation protocols, secure networking and hardware security)
- Application of artificial intelligence (e.g., neural networks, threat detection and prevention)
- Use-cases in commercial and private sector
- Link-Layer Security
- Quantum/Post-Quantum Security and applications in Aerospace

Important Dates

- Extended Deadline: June 6, 2021
- Notification of Acceptance: July 2, 2021
- Camera ready Date: July 16, 2021
- Workshop: September 6, 2021

Paper Submission Guidelines:

All submissions must be original work. Plagiarism (whether of others or self) will be grounds for rejection. The submitter must clearly document any overlap with previously published or simultaneously submitted papers from any of the authors. Failure to point out and explain overlap will be grounds for rejection. Simultaneous submission of the same paper to another venue with proceedings or a journal is not allowed and will be grounds for automatic rejection. Submitting multiple distinct papers is of course allowed. EuroS&P 2021 includes an author response period, which gives authors the chance to comment on reviews their papers received. Papers may not be withdrawn between the start of the author response period and acceptance notification. Contact the program committee chairs if there are questions about this policy.

Papers must be submitted in a form suitable for anonymous review: no author names or affiliations may appear on the title page, and papers should avoid revealing their identity in the text. When referring to your previous work, do so in the third person, as though it were written by someone else. Only blind the reference itself in the (unusual) case that a third-person reference is infeasible. Contact the program chairs if you have any questions. Papers that are not properly anonymized may be rejected without review.

Papers must not exceed 10 pages total (including the references and appendices). Papers must be typeset in LaTeX in A4 format (not ”US Letter”) using the IEEE conference proceeding template with the appropriate options from EuroS&P 2021. Failure to adhere to the page limit and formatting requirements can be grounds for rejection. Submissions must be in Portable Document Format (.pdf). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Your document should render correctly in Adobe Reader XI and when printed in black and white.

5.2.4 MaLeNe 2021 - 1st International Workshop on Machine Learning in Networking

MaLeNe 2021 aims at providing an international forum for researchers addressing emerging concepts and challenges related to machine learning in networking. The workshop will aim to address opportunities where machine learning can bring benefits to networking in different facets, such as network monitoring, management, and security. Together with flexible and programmable networks this paves the way towards a more proactive and autonomous network design and "self-driving" networks. The long-term vision is that configuration decisions can be made in real-time in an automated fashion before service and experience degradation occurs. The workshop will combine original paper presentations with a motivating keynote to thoroughly explore this challenging topic. For details see the conference page under https://netsys2021.org/workshops/malene/.

Authors are invited to submit papers that fall into or are related to the topic areas listed below:

- Methodology
  - Data sets for benchmarking, verification, proof of concept
  - Data augmentation
  - Performance evaluation methodology (best practices)
  - Good standards for data publishing
  - Data prediction and generation (e.g., GANs)
  - Dimensionality reduction (e.g., autoencoder)
- Machine Learning Algorithms
  - Classical methods like supervised, unsupervised, reinforcement learning
  - Deep methods vs non-deep methods
  - Graph neural networks
  - Advanced methods like adversarial, transfer
- Generalizability
  - Transfer of trained models (e.g., small to large networks, enterprise to data center)
  - Federated learning (combine models trained for different data sets)

  - Machine unlearning
  - Catastrophic forgetting

- Explainability
  - Visualization
  - Understanding decisions of ML-based systems (e.g., management, traffic engineering)
  - Game-theory-based approaches to approximate guarantees

- Networking for Machine Learning and AI
  - Network architectures
  - Network applications
  - Network use cases (data center, enterprise, etc.)
  - Network resource management (e.g., algorithms, schedulers)
  - In-network processing

- Applications in Networking
  - Network monitoring, especially from encrypted traffic (e.g., traffic classification, QoE)
  - Network configuration (e.g., suggest optimal configurations, “spell-check” text-based configuration data)
  - Network planning (e.g., reconfigurable data centers, job placement)
  - Network management (e.g., autonomous management, self-driving networks)
  - Network security (e.g., intrusion detection, covert channels, firewall)
  - Advanced networks (e.g., 5G to 6G, industry, slicing)

- Hot Topics from Machine Learning
  - Self-supervised learning
  - Intrinsic motivation, empowerment, curiosity
  - Language processing in networking
  - Meta-artificial intelligence (learning to learn)

Important Dates

- Submission deadline: June 13, 2021
- Notification of acceptance: July 8, 2021

- Final submission/Camera-ready version and registration: July 22, 2021
- Workshop date: September 13 or 14, 2021

Submission Details:

- All contributions should be submitted as PDF documents. Submissions may be up to 12 pages long (11pt font, one-column format) plus 4 pages for references. Template: https://netsys2021.org/participation/
- Accepted workshop papers are included in the adjunct proceedings of the NetSys Conference and are published by ECEASST as Open Access.
- Link to submission system: https://easychair.org/conferences/?conf=netsys2021 (select track: Workshop MaLeNe)

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]
√66 [meaning: Route 66]
Y R U so Z 2dA ? [meaning: why are you so sad today ?]

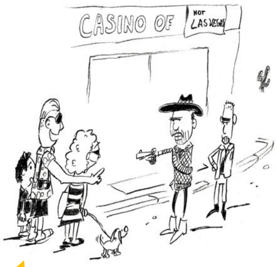

Fig. 1: Illustration to assist the reader in solving the fourth riddle (source: [1])

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

- *Beginners:* **∅ compares 2 U**
- *Playing with Capital Letters:*
  (he + nEds) hLp 2 RTQl8 simple sN10ces
- *Advanced Persons:*
  this gr8 bayern tEm 1 the (3 • in) 2020
- *Experts:*
  V R fascin8ed by ∀ the 1 Rmed b+its in reno
- *Geniuses:* **the Tcher was |ly| frustr8ed 2 C th@ ∀most ∀ pupils knU ∅**

[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):

- nothing compares to you [because: *nothing*-compares-*two*-*U*]
- he needs some help to articulate simple sentences [because: (he-n-*E*-ds-*sum*)-h-*L*-p-*two*-*R*-*T*-*Q*-l-*eight*-simple-s-*N*-*ten*-ces]
- this great Bayern team won the triple in 2020 [because: this-gr-*eight*-bayern-t-*E*-m-*one*-the-*(triple-in)*-2020]
- we are fascinated by all the one-armed bandits in Reno [because: *V*-*R*-fascin-*eight*-ed-by-*all*-the-*one*-*R*-med-b-*and*-its-in-reno]
- the teacher was absolutely frustrated to see that almost all pupils knew nothing [because: the-*T*-cher-was-*absolute*-ly-frustr-*eight*-ed-*two*-*C*-*th*-*@*-most-*all*-pupils-kn-*U*-*nothing*]

KuVS Newsletter

Next Newsletter

Next newsletter : 12/2021

Deadline for submissions and contributions : 15th November 2021

We ask you for submissions in English. Topics can be from the following time frame: May 2021 - November 2022.

- 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