Munich Internet Research Retreat 2016

https://www.cm.in.tum.de/mir3/2016

Vaibhav Bajpai
bajpaiv@in.tum.de

Aaron Yi Ding
ding@in.tum.de

Mirja Kühlewind
mirja.kuehlewind@tik.ee.ethz.ch

Georg Carle
carle@in.tum.de

Lars Eggert
lars@netapp.com

Wolfgang Kellerer
wolfgang.kellerer@tum.de

Jörg Ott
ott@in.tum.de

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.
The authors take full responsibility for this article's technical content. Comments can be posted through CCR Online.

ABSTRACT

This article summarizes the two-day Munich Internet Research Retreat (MIR) held in November 2016. The goal of the retreat was to provide a forum for both academic and industrial researchers to exchange ideas and get feedback on their current work. It was organized in a spirit that is similar to highly interactive "Dagstuhl" seminars, with a very limited number of full-length talks, while dedicating most of the time to poster sessions and group discussions. Presentations delivered during the seminar are made publicly available [25].

1. INTRODUCTION

The MIR originated from informal discussions of different research groups at TUM and a team at NetApp on diverse topics related to networking. The discussions brought together PhD students and post-docs to present their respective research (including both work in progress as well as polished results) and provided an informal setting for intense and rich exchange among participants involved. We realised that there was notable potential in reaching out further, which eventually led to the instantiation of the MIR.

The main mission of the MIR is to ensure mutual awareness of different teams working on current (complementary) topics in networking. We want to lay the foundations for establishing, broadening, and deepening cooperation among a variety of groups doing networking research. In order to foster easily sustainable relationships, our initial scope has been deliberately limited to the area around Munich (which may reach as far as 400 km in some cases). As a common denominator, we target like-minded teams within the region, where the common mindset stems from practical research in networked systems, paired with interest and efforts in the Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF) and the ACM SIGCOMM and SIGMOBILE communities.

The purpose of the MIR is threefold: 1) We seek to provide recurring opportunities for companies to get in touch with research groups that have expertise in fields relevant to the former. 2) We aim to support researchers in understanding current and emerging research and engineering problems from the commercial development and deployment perspectives. 3) We like to offer reality feedback to academic researchers and out-of-the-box ideas to those from industry. Overall, we hope to foster future bi- or multi-lateral collaboration between academics and industry.

The retreat is organized in a highly interactive fashion, combining posters (for providing variety) and group discussions intertwined with plenary talks that stimulate discussions. Organization directions are shaped by the feedback of the participants, keeping the format constantly evolving. We borrow some elements from the renowned Dagstuhl seminars: We limit the number of participants to $\sim$40 to maintain interactivity and allow all participants to meet one another. We hold the retreat in Raitenhaslach away from the daily activities to ensure focus and include an overnight stay and a social dinner to foster continued interaction and allow for digesting ideas. The seminar is by invitation only, and we put an emphasis on the industry, picking PhD students with matching topics, which helps with obtaining a compatible and energetic mix of people. Because we know that everybody's time is scarce, we organize each retreat in a way that it occupies just two days including arrival and departure. With a target of two workshops per year, presently scheduled for May and November, we shall be able to continuously engage with a growing regional community even if individuals cannot participate on every occasion.

Towards this mission, the 1st MIR retreat was organized on November 24–25, 2016 at the TU Munich (TUM) Science and Study Center in Raitenhaslach, Germany. Presentations on topics such as: Software Defined Networks (SDN), Network Function Virtualization (NFV), Information-Centric Networking (ICN), Internet of Things (IoT), Internet measurements and security-related research were solicited. The retreat consisted of ten invited presentations and several posters presenting early and upcoming research, with six breakout sessions to discuss topics of interests in an informal setting. Synopses of these sessions are described in this report in more detail.

2. INVITED PRESENTATIONS

The invited presentations were intended as a basis for triggering discussions and identifying areas for group work.

2.1 Edge Computing Considered Harmful

Current work on Mobile Edge Computing is motivated by ambitious goals for low latency and performance improvements in next-generation mobile networks. This talk challenges the mainstream notion of running application-specific VMs at the network edge and discusses the related security/privacy issues. We argue that low latency should be first-order general requirement and will point at corresponding network- and transport layer approaches. Finally, the talk will discuss opportunities for more flexible and secure approaches to edge computing.

2.2 Digital Sovereignty in the Post-Snowden Era

In this talk, Alexander von Gernler (genua GmbH) emphasizes the need for the availability of trustworthy hardware and operating systems for the common user. The postulation is that without these means, democracy will suffer in the long run, as people need not only to be unwatched and uncensored when pursuing their forming and expressing of political opinion, but they also need to feel unwatched and uncensored. If these prerequisites are not met, chilling effects will occur, and the users will adjust their behavior to whatever they think is socially appropriate. The talk finishes by enumerating some possible ways out of the situation, and appeals to the conscience of the computer scientists around, as they are needed to explain the problem to society, and ultimately solve it.

2.3 On software network management

In this talk, Artur Hecker (Huawei) argues that the paradigm change brought by software networks does not suit well planning approaches for network dimensioning and design, including but not limited to planning or pre-provisioning of management and control planes. As an example, OF SDN and ETSI NFV silently rely on pre-established, fixed control networks; opening these up for programmability currently bears risks [33] with respect to the integrity of the control plane easily leading to a self-lockout. Prior art targeted similar problems using OpenFlow enhancements [34]. In contrast, Artur proposes a new model and protocol, sort of a least common denominator for software networks. The only well-defined purpose of the latter would be to autonomously bootstrap, construct, adjust and maintain control plane including the elastic placement of control compute nodes [24] and control paths without presuming any particular network purpose.

2.4 FlexNets: It's all about Flexibility

New requirements for communication networks include the need for dynamic changes of the required networking resources. Providing the required flexibility to react to those changes and being cost efficient at the same time has recently emerged as a huge challenge in networking research. With SDN and NFV, three concepts have emerged in the networking research, which claim to provide more flexibility. However a deeper understanding of the flexibility vs. cost trade-off is missing so far in networking research. In this talk, Wolfgang Kellerer (TUM) proposes a definition for flexibility as a new measure for network design space analysis [22] and gives an illustrative example with SDN controller placement.

2.5 An Accidental Internet Architecture

The Internet, as seen from the point of view of the applications, services, and user agents it connects, is defined by the interfaces it provides. In this talk Brian Trammell (ETH Zürich), introduced PostSockets [38], a work-in-progress proposal to re-imagine the Internet from a new API down. PostSockets provides for secure, message-oriented, explicitly multipath, asynchronous communication. It separates long-term state (cryptographic identity and resumption parameters) from ephemeral per-path state (transport connection windows, session secrets), and is suitable both for reliable message stream transports (such as QUIC for HTTP/2) as well as for partially-reliable media applications. PostSockets is intended to allow applications to be developed separate from (possibly runtime-bound) transport protocol dynamics, in turn accelerating the deployment of recent innovations at Layer 4

2.6 Measuring IPv6 Performance

A large focus of IPv6 measurement studies in the past has been on measuring IPv6 adoption on the Internet. This involved measuring addressing, naming, routing and reachability aspects of IPv6. However, there has been very little to no study on measuring IPv6 performance. Vaibhav Bajpai (Jacobs University Bremen) shows that his dissertation work fills this gap. He uses 80 dual-stacked SamKnows [3] probes deployed at the edge of the network to measure IPv6 performance of operational dual-stacked content services on the Internet. He presents a comparison of how content delivery [4, 1] over IPv6 compares to that of IPv4. He shows how in the process, he also identified glitches in this content delivery [15] that once fixed can help improve user experience over IPv6. His also points out areas of improvements [5] in the standards work for the IPv6 operations community at the IETF. This study can be relevant for network operators that are either in the process of or are in early stages of IPv6 deployment.

2.7 Classification of IPv4-IPv6 Siblings

With the growing deployment of IPv6, the question arises whether and to what extent this new protocol is co-deployed with IPv4 on existing hardware or whether new hardware or proxy solutions are deployed. Understanding the resulting cross-dependencies between IPv4 and IPv6 hosts will add a significant level of insight into Internet structure and resilience research. In this talk, Minoo Rouhi (TUM) presented an active measurement technique to determine whether an IPv4-IPv6 address pair resides on the same physical host. The measurement technique is based on measuring clock skew through TCP timestamps, and introduces new capabilities to classify nonlinear clock skews. In their studies, they achieve 97.7% accuracy on a ground truth data set of 458 hosts and have proved this technique's value by applying it to 371K sibling candidates, of which they classify 80K as siblings. A

technical report on this work has been published [32]. Further, the classified siblings as well as additional data and all code from this work have been released [32] for public use.

2.8 SWIFT: Predictive Fast Reroute upon Remote BGP Disruptions

Fast rerouting upon network failure is a key requirement when it comes to meet stringent service-level agreements. While current frameworks enable sub-second convergence upon local failures, they do not protect against the much frequent remote failures. In contrast to local failures, learning about a remote failure is fundamentally slower as it involves receiving potentially hundred of thousands of BGP messages. Also, pre-populating backup forwarding rules is impossible as any subset of the prefixes can be impacted.

In this presentation, Laurent Vanbever (ETH Zurich) presented SWIFT, a general fast re-route framework supporting both local and remote failures. SWIFT is based on two novel techniques. First, SWIFT copes with slow notification by predicting the overall extent of a remote failure out of few control-plane (BGP) messages. Second, SWIFT introduces a new data-plane encoding scheme which enables it to quickly and flexibly update the impacted forwarding entries.

SWIFT have been implemented by the ETH Network Systems Group (NSG) and its performance benefits have been demonstrated by showing that SWIFT is able to predict the extent of a remote failure with high accuracy (93%) and SWIFT encoding scheme enables to fast-converge more than 95% of the impacted forwarding entries. Overall, SWIFT reduces the average convergence time from few minutes to few seconds.

2.9 Open Platforms for Cyber-physical systems

For many cyber-physical systems, there is a strong trend towards open systems which can be extended during operation by instantly adding functionalities on demand. In this talk, Christian Prehofer (Fortiss) discussed this trend in the context of networked systems in the automotive, medical and industrial automation areas and elaborated the research challenges of platform for such open, networked systems. A main problem is that such CPS applications shall be able to access and modify safety critical device internals. Further, results of the TAPPlications (Trusted Applications for open CPS) project were presented, which develops an end-to-end solution for development and deployment of trusted applications [28]. This includes trusted hardware and virtualization of networking and CPU, as well as dedicated execution environments and development support for trusted applications.

2.10 Collaborative intrusion handling using the Blackboard-Pattern

Defending computer networks from ongoing security incidents is a key requirement to ensure service continuity. Handling incidents is a complex process consisting of the three steps: 1) intrusion detection, 2) alert processing and 3) intrusion response. For useful and automated incident handling a comprehensive view on the process and tightly interleaved single steps are required. Existing solutions for incident handling merely focus on a single step leaving the other steps completely aside. Incompatible and encapsulated partial solutions are the consequence. In this talk Holger Kinkelin (TUM) proposed an approach [20] on incident handling based on a novel execution model that allows interleaving and collaborative interaction between the incident handling steps using the Blackboard Pattern. Their holistic information model lays the foundation for a conflict free collaboration. The incident handling steps are further segmented into exchangeable functional blocks distributed across the network. To show the applicability of their approach, typical use cases for incident handling systems were identified and tested based on their implementation.

3. PARALLEL GROUP WORK

The afternoon sessions were used to discuss selected topics in more depth in smaller groups. This section summarizes the discussions of each group.

3.1 SDN/NFV Measurements

With the introduction of SDN, Network Virtualization (NV), and NFV, the programmability and flexibility of our networks is promised to increase. With these new concepts, networking tasks will be pushed on commodity hardware where they are programmed as software. However, this introduces new uncertainties in the provided performance of these next generation networks as, in particular, commodity hardware and software are not designed for network processing. Accordingly, new sophisticated measurement procedures are needed to benchmark hardware and software components when faced with network packet processing. Besides, as virtualization introduces an abstraction layer, this might come with a performance overhead that needs to be considered and quantified. For this purpose, existing measurement tools, such as MoonGen [14], could be used to evaluate the performance for high data rate with accurate precision. Furthermore, tools designed for measuring non-virtualized and virtualized SDN networks (such as `perfbench`) could measure the overhead of virtualization components, such as network hypervisors. Measurements should be conducted on software platforms as well as real networking testbeds. Hence, testbeds need to be built that include commodity servers, e.g., making use of accelerated network cards via Data Plane Development Kit (DPDK), networking functions in software, e.g., functions running in docker containers, orchestration tools for virtual environments, e.g., HyperFlex [9] and OpenStack, as well as hardware that can generate realistic network traffic, e.g., Spirent Test Center. Generally, the performance evaluation of virtualized networks and SDN networks is an important task for the design of future communication networks.

3.2 SDN++: Applications Perspective

The breakout session entitled SDN++ dealt with SDN from the perspective of how to apply SDN, and how to introduce improvements to SDN (thereby creating SDN++), for better

meeting the identified requirements. Participants of the breakout session were Laurent Vanbever, Artur Hecker, Wolfgang Kellerer, Edwin Cordeiro and Georg Carle, the latter also being the presenter of the results. The method of the working group was first to identify relevant application areas of SDN, then assess to which extent known SDN approaches have shortcomings (i.e., identifying the 'SDN pain areas'), and subsequently identifying promising approaches for improving SDN. The application areas of SDN were (1) establishing means for programmability of the network, which can be used for improving certain network properties, (2) management of advanced cellular networks, in particular 5G networks, for different capabilities such as network slicing, and (3) providing means to add sophisticated control functionality to corporate networks, such as adding flexible access control. Identified weaknesses of existing SDN were the fact that existing SDN southbound interfaces, in particular OpenFlow, operate on a low level of abstraction, which makes programming of the network time-consuming and error prone. Identified areas of improvement and need for further work were specifying suitable high-level interfaces and abstractions. There further is the need to develop tools that are capable of automatically translate high-level specifications to low-level configuration. A complete tool chain is required. This includes measurement tools that are capable of monitoring changes. Network programmability is beneficial for measurement tools. It is expected that SDN management tools will facilitate to deal with the programmability of networks. Furthermore, verification tools will allow to detect and prevent attempts of wrongly programming the network. These tools will form a network operating system, with tools that operate on top of the operating system functions. Another need for improvement is the development of a clear transition path from today's networks to future SDN-based networks. This includes to identify which legacy functionalities from today's networks we assume being able to depend on in SDN deployments.

3.3 QUIC

QUIC [21] is a new UDP-based reliable transport protocol with built-in security. The protocol is optimized for HTTP/2 [8] that is currently being standardized by the IETF. QUIC was originally proposed by Google and has already seen large-scale deployment for Google services and in Google Chrome. Since September 2016 a new IETF working group reviews the design of QUIC in order to publish a QUIC protocol specification with IETF consensus. The break out session discussed how the IETF should approach on how the information encrypted in the QUIC packets might be made available to legitimate network management or firewall functions. The session also went into retrospect on historical protocol innovations (such as HIP [27] and SCTP [36]) that failed to get widely deployed to understand whether one needs to be Google (or a large CDN player) to be able to deploy a protocol on the Internet today. It was mentioned how good ideas and engineering also needs the right incentives to see deployment and how partial deployability with one large CDN player already brings benefits. QUIC is witnessing rapid adoption also because Google controls both endpoints (browser and servers). As such, two endpoints that can agree on an exchange that does not require middleware updates makes it easier to deploy an innovation in practice, but still only influential organizations have that leverage. Dave Thaler [37] lays out strategies to allow smooth transitions of future protocol innovations. Cost and benefit tradeoffs of simpler deployability and clean-state designs were discussed. The deployment incentives need to be aligned to allow early adopters to see the investment benefits. It was also mentioned how operator networks remain opaque to designers of network protocols and for the need for additional large-scale measurement initiatives that help bring visibility into how current network operate in practice would be useful for protocol innovation.

3.4 DDoS Defense beyond Centralization

The danger of Distributed Denial-of-Service Attack (DDoS) attacks makes web services buy services of a few large companies, such as Akamai or Cloudflare. Usually, this comes with a loss of control on the side of the web service over defensive measures, e.g., which connections are blocked. Furthermore, we believe that this centralization of the Internet is threatening the freedom of the Internet as users cannot bypass the use of services of certain companies anymore. They lose their authority to select the ones they want to use. In order to overcome this problem, we propose to make DDoS protection a service of ISPs to web services and in further steps between ISPs and IXPs. If a web service is in trouble it can alarm its ISP and can influence connections blocked by the ISP on its behalf. Details need further research.

3.5 Security

The security breakout session covered civil liberties and privacy. Firstly, the group set its focus and decided not to discuss the topics of trustworthy hardware or civil liberties, but instead to concentrate on SDN security and problems of cloudification. Key results: 1) Customer networks are converging: Customers want less own hardware, and want to be more independent and to lease remote services and equipment rather than owning it. 2) Virtualization (which happens when you cloudify applications) amplifies known problems in traditional fields like security, trust, verifiability or visibility. 3) A special challenge is the cloudification of services that already utilize virtualization in the traditional model, for example sandboxes that analyze malware. For a cloud case, one would end up with nested virtualization, which in turn comes with even new problems concerning performance and visibility of the virtualization to the malware being inspected. 4) Encryption of data still leads to the usability of cloud scenarios being reduced to mostly SaaS, because homomorphic encryption is still not there to solve these problems. 5) Special problems with end-to-end security, e.g., there is more end-to-end encryption happening, which is good. As a downside however, it makes life harder for people

inspecting traffic in the middle if termination of encrypted connections is done in the cloud, there will be an unencrypted last mile as new security issue arising from this scenario.

3.6 IoT and ICN

The breakout session on Internet of Things (IoT) and Information Centric Networking (ICN) covered the open problems and research directions for applying ICN technique to IoT. The identified problems include: 1) Limitation of existing protocols such as Constrained Application Protocol (CoAP) that handles poorly the frequent leaving/joining events in the network. 2) The stereotype of "IoT gateway design" has hindered novel design. 3) We still have not yet come up with a suitable Internet architecture that integrates IoT coherently.

The group discussed how to bring ICN schemes to IoT, and highlighted several open questions: 1) Where does the network end nowadays? This question couples with the ICN where nodes can contribute to the computation/content along the path. 2) What functions on gateway functions we can remove? 3) How to do naming "translation" without changing name/label? 4) Can we do packet processing while it is passing through queue? 5) How to avoid looping in the network functions? This is a key concern since we need to keep a boundary for resource usage in the network. 6) How to maintain the state on the constrained nodes?

Regarding potential research directions, the group deem the following items important: 1) Design of end-to-end naming scheme, to facilitate IoT application composition and bring down the overhead of porting applications for the cloud to "gateways". 2) Semantics for individual sensor and equivalence group. 3) Trade accuracy with replication. 4) A new computation abstract suitable for IoT. 5) Abstract of distributed registry for network function. 6) Rethink how we distribute computing and content.

4. POSTERS

Participants were encouraged to bring posters to present their recent research work.

4.1 Cost of Security in the SDN Control Plane

In OpenFlow enabled SDN, network control is carried out remotely via a control connection. In order to deploy OpenFlow in production networks, security of the control connection is crucial. For OpenFlow connections, TLS encryption is recommended by the specification. This work [13] analyzes the TLS support in the OpenFlow ecosystem. In particular, a performance measurement tool was implemented for encrypted OpenFlow connections, as there is non available. The first results show that security comes at an extra cost and hence further work is needed to design efficient mechanisms taking the security-delay trade-off into account.

4.2 The Baltikum Testbed

The poster showed a high-level overview to the recent activities [14, 16, 29, 30] in the Baltikum Testbed. The testbed which is focused on performance measurements of x86-based packet processing systems provides an automated, documented, and reproducible experiment workflow. The poster presented several activities, comprising the load generator MoonGen [14], automated benchmarks of routers and OpenFlow switches, and different performance studies, including an IPsec gateway with NIC-offloading.

4.3 Boost Virtual Network Resource Allocation

Rapidly and efficiently allocating virtual network resources, i.e., solving the online Virtual Network Embedding (VNE) problem is important in particular for future communication networks. This poster proposes a system [12] using an admission control to improve the performance for the online VNE problem. The admission control implements a Neural Network that classifies virtual network requests based on network representations, which are using graph and network resource features only. They demonstrate via simulations that the admission control, i.e., the Neural Network filters virtual network requests that are either infeasible or that need too long for being efficiently processed. Thus, this admission control reduces the overall system runtime, i.e., it improves the overall calculation efficiency for the online VNE problem. Generally, this work demonstrates the ability to learn from the history of VNE algorithms. It is possible to learn the behavior of algorithms and how to integrate this knowledge when solving future problem instances.

4.4 HyperFlex

The virtualization of SDN allows multiple tenants to share a physical SDN infrastructure, where each tenant can bring its own controller for a flexible control of its virtual SDN network (vSDN) [10]. In order to virtualize SDN networks, a network hypervisor is deployed between the physical infrastructure and the tenants' controllers. The poster presents, HyperFlex [9, 7], a flexible, reliable and dynamic SDN virtualization layer. HyperFlex achieves the flexibility of deploying hypervisor functions as software or alternatively using available processing capabilities of network nodes. It also provides resources isolation for the control plane of vSDNs. Additionally, HyperFlex supports the dynamic migration of network hypervisor instances on run time. These features [6, 11] are key steps towards vigorous slicing in 5G.

4.5 SafeCloud

The poster gives an overview of the cloud security activities of the SafeCloud project [31]. SafeCloud usage for the user requires privacy and in SafeCloud a variety of privacy-enhanced services are developed. This includes cryptographic databases and secure multiparty computation. Security and resilience mechanisms add diverse and censorship-resistant storage, multipath and route monitoring.

4.6 sKnock: Scalable Secure Port Knocking

Port-knocking is the concept of hiding remote services behind a firewall which allows access to the services' listening

ports only after the client has successfully authenticated to the firewall. This helps in preventing scanners from learning what services are currently available on a host and also serves as a defense against zero-day attacks. Existing port-knocking implementations are not scalable in service provider deployments due to their usage of shared secrets. The poster introduces an implementation [35] of port-knocking based on x509 certificates aimed towards being highly scalable.

4.7 SarDiNe

The BMBF project SarDiNe is motivated by the advent of the virtualization of complete enterprise networks. Software defined networks (SDN) tremendously ease the creation and management of virtual networks which leads to new challenges in security policy enforcement. Traditionally, networks were separated physically and security was mainly enforced by firewalls placed at gateway positions between the physical networks. With highly dynamic virtual networks it remains unclear where to place firewalls, especially if higher security measures like filtering on the application layer are needed.

The poster presents SarDiNe, which proposes to virtualize firewall functionality as well and dynamically place it on commodity hardware managed by cloud techniques and spread across the network. Then, the SDN is used to dynamically reroute traffic via these virtual network functions (VNF). This approach promises a scalable and cost-efficient security solution applicable to many different setups. As main use case is to elaborate a bring-your-own-device (BYOD) scenario and there is also interest in exploiting the SDN to provide parts of the filtering functionality in its fast switching hardware. The result is a hybrid VNF-SDN firewall which aims at a cost reduction in terms of computation resources needed for scaling and latency imposed by the rerouting.

4.8 Securebox

Securebox [17, 18] is an affordable and deployable platform for securing IoT networks. This proposal targets an alarming spot in the growing IoT industry where security is often overlooked due to device limitation, budget constraint, and development deadline [19]. In contrast to existing host-centric and hardware-coupled solutions, it empowers a cloud-assisted model dedicated to IoT networks. In specific, Securebox allows to 1) flexibly offload and onload security and management functions to cloud and edge components; 2) offer advanced security services to end users in an affordable manner; 3) ease the upgrade and deployment of new services to guard against abrupt security breakouts. Its collaborative and extensible architecture enforces rapid update cycles and can scale with the growing diversity of IoT devices.

4.9 StackMap

StackMap [39] leverages the best aspects of kernel-bypass networking into a new low-latency OS network service based on the full-featured TCP kernel implementation, by dedicating network interfaces to applications and offering an extended version of the netmap API for zero-copy, low-overhead data path alongside control path based on socket API. For small-message, transactional workloads, StackMap outperforms baseline Linux by 4 to 78% in latency and 42 to 133% in throughput. It also achieves comparable performance with Seastar, a highly-optimized user-level TCP/IP stack that runs on top of DPDK.

4.10 PATHspider

There is an increasing deployment of middleboxes in today's Internet. While middleboxes provide in-network functionality that is necessary to keep networks manageable and economically viable, any packet mangling – whether essential for the needed functionality or accidental as an unwanted side effect – makes it more and more difficult to deploy new protocols or extensions of existing protocols. For the evolution of the protocol stack, it is important to know which network impairments exist and potentially need to be worked around. While classical network measurement tools are often focused on absolute performance values, the poster presents a new measurement tool, called PATHspider [23] that performs A/B testing between two different protocols or different protocol extension to perform controlled experiments of protocol-dependent connectivity problems as well as differential treatment. PATHspider is a framework for performing and analyzing these measurements, while the actual A/B test can be easily customized. This poster describes the basic design approach and architecture of PATHspider and gives guidance how to use and customize it.

4.11 FlexNets

Communication networks have emerged to become the basic infrastructure for all areas of our society with application areas ranging from social media to industrial production and health care. New requirements include the need for dynamic changes of the required resources, for example, to react to social events or to shifts of demands. Existing networks and, in particular, the Internet cannot meet those requirements mainly due to their ossification and hence limitation in resource allocation, i.e., lack of flexibility to adapt the available resources to changes of demands on a small time-scale and in an efficient way. In recent years, several concepts have emerged in networking research to provide more flexibility in networks through virtualization and control plane programmability. In particular, the split between data plane and a centralized control plane as defined by Software Defined Networking (SDN) is regarded as the basic concept to allow flexibility in networks. However, a deeper understanding of what flexibility means remains open. In this project, flexibility focuses on the dynamic changes in time and size of a network that is characterized by its resources (link rate and node capacities) and connectivity (network graph). It is the objective of this research to analyse the fundamental design space for flexibility in SDN-based networks with respect to cost such as resource usage, traffic overhead and delay. The outcome will be a set of quantitative arguments pro and contra certain design choices. An analytical cost model to quantitatively assess the trade-off for flexibility vs. cost will be developed. To assess flexibility with respect

to general graph properties a graph model will be designed. The detailed analysis is based on three use cases: dynamic resource allocation, QoS control, and resilience. In the state of the art, selected aspects of flexibility have been explored for certain network scenarios, a fundamental and comprehensive analysis is missing.

4.12 AutoMon

Performance monitoring and trouble shooting of user impacting anomalies in enterprise networks require the correlation of multiple different data sources such as ticket systems, component health monitoring, and flow monitoring systems. To perform a root cause analysis for the incident, multiple teams must coordinate and correlate the data manually. Detection and resolution often occurs only after users have reported problems. In the BMBF project AutoMon [2], the performance monitoring and analysis will be automated. The poster presents the context, approaches and advantages of such a solution.

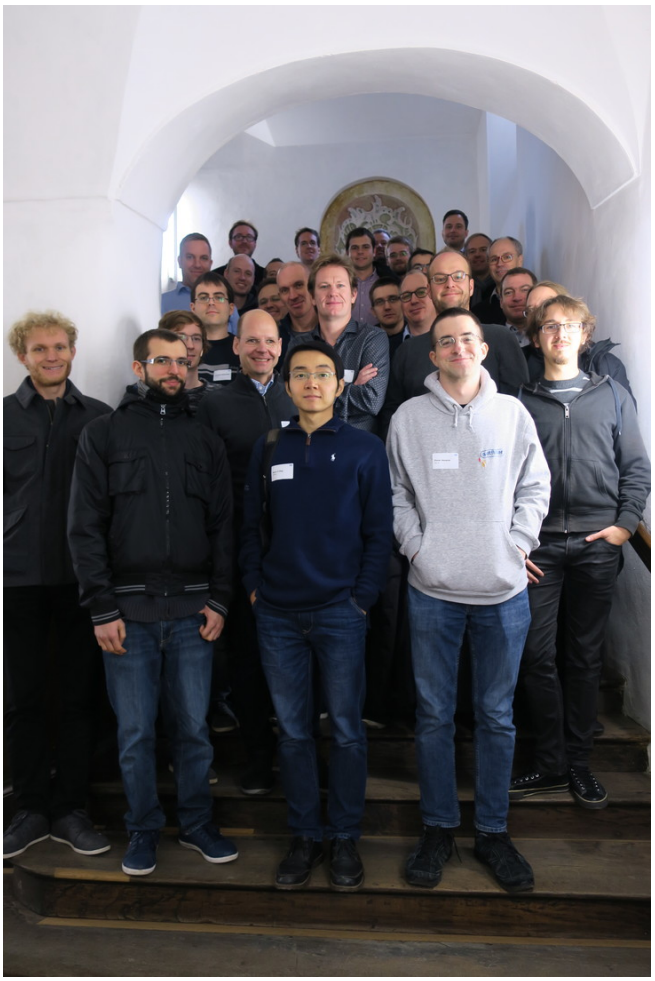
5. CONCLUSIONS AND NEXT STEPS

The 1st Munich Internet Research retreat concluded successfully on November 24–25, 2016. All the presentation material and contact information of presenters are available online [25]. A second iteration of the retreat is planned for May 23–24, 2017 with a webpage currently available online [26]. The readers are encouraged to contact the organizers to learn more about the the next retreat.

We also collected some feedback from the participants. Academic participants expressed that this retreat was a good chance to talk to fellow researchers, although the topics were quite diverse. While the 1st retreat was open in terms of topics (as will be the upcoming 2nd retreat), we are considering running workshops focused on topic areas as an option for the future. Industrial participants found the breakout sessions useful since it helped them to get an overview of current academic research. It was mentioned that such an interaction also helps bring some of the academic research back to the industry. Longer breakout sessions (by reducing the number of invited presentations) and dedicated sessions for doctoral candidates were advised. The idea of inviting more industry participants was also suggested.

Acknowledgements

This seminar was located at the TUM Science and Study Center in Raitenhaslach, Germany, supported by NetApp, Huawei, and TUM. The organizers would like to thank the participants (alphabetically ordered by first name) for their contributions—Aaron Yi Ding (TUM CM), Alberto Martínez Alba (TUM LKN), Alexander von Gernler (genua GmbH), Andreas Blenk (TUM LKN), Arsany Basta (TUM LKN), Artur Hecker (Huawei), Brian Trammell (ETH Zürich), Christian Prehofer (fortiss, TUM), Claas Lorenz (genua GmbH), Daniel Raumer (TUM NET), Dirk Kutscher (Huawei), Edwin Cordeiro (TUM NET), Florian Westphal (Red Hat), Georg Carle (TUM NET), Hagen Paul Pfeifer (Rohde & Schwarz), Heiko Niedermayer (TUM NET), Holger Kinkelin (TUM NET), Johannes Naab (TUM NET), Jörg Ott (TUM CM), Lars Eggert (NetApp), Laurent Vanbever (ETH Zürich), Marco Hoffmann (Nokia Bell Labs), Markus Klügel (TUM LKN), Matthias Wachs (TUM NET), Minoo Rouhi (TUM NET), Mirja Kühlewind (ETH Zurich), Nemanja Djeric (TUM LKN), Paul Emmerich (TUM NET), Pavel Laskov (Huawei), Peter Babarczi (TUM NET), Raphael Durner (TUM LKN), Rastin Pries (Nokia Bell Labs), Rolf Winter (University of Applied Sciences Augsburg), Sebastian Gallenmüller (TUM NET), Vaibhav Bajpai (Jacobs University Bremen), Wolfgang Kellerer (TUM LKN). Special thanks to Johannes Naab for reviewing the manuscript.



6. REFERENCES

[1] S. Ahsan, V. Bajpai, J. Ott, and J. Schönwälder. Measuring YouTube from Dual-Stacked Hosts. *Passive and Active Measurement Conference (PAM)*, 2015.

[2] AutoMon – Automated Performance Monitoring. http://automon-projekt.de/en.

[3] V. Bajpai and J. Schönwälder. A Survey on Internet Performance Measurement Platforms and Related Standardization Efforts. *IEEE Communications Surveys and Tutorials*:1313–1341, 2015.

[4] V. Bajpai and J. Schönwälder. IPv4 versus IPv6 - who connects faster? *IFIP Networking Conference*, 2015.

[5] V. Bajpai and J. Schönwälder. Measuring the Effects of Happy Eyeballs. *Applied Networking Research Workshop (ANRW)*, pp. 38–44, 2016.

[6] A. Basta, A. Blenk, H. B. Hassine, and W. Kellerer. Towards a dynamic SDN virtualization layer: Control path migration protocol. *Conference on Network and Service Management (CNSM)*, pp. 354–359, 2015.

[7] A. Basta, A. Blenk, Y. Lai, and W. Kellerer. HyperFlex: Demonstrating Control-Plane Isolation for Virtual Software-Defined Networks. *International Symposium on Integrated Network Management (IM)*, 2015.

[8] M. Belshe, R. Peon, and M. Thomson. Hypertext Transfer Protocol Version 2 (HTTP/2). RFC 7540 (Proposed Standard), Internet Engineering Task Force, May 2015. URL: http://www.ietf.org/rfc/rfc7540.txt.

[9] A. Blenk, A. Basta, and W. Kellerer. HyperFlex: An SDN Virtualization Architecture with Flexible Hypervisor Function Allocation. *IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 2015.

[10] A. Blenk, A. Basta, M. Reisslein, and W. Kellerer. Survey on Network Virtualization Hypervisors for Software Defined Networking. *IEEE Communications Surveys and Tutorials*:655–685, 2016.

[11] A. Blenk, A. Basta, J. Zerwas, M. Reisslein, and W. Kellerer. Control Plane Latency With SDN Network Hypervisors: The Cost of Virtualization. *IEEE Trans. Network and Service Management*:366–380, Sep. 2016.

[12] A. Blenk, P. Kalmbach, P. v. d. Smagt, and W. Kellerer. Boost Online Virtual Network Embedding: Using Neural Networks for Admission Control. *Conference on Network and Service Management (CNSM)*, pp. 10–18, 2016.

[13] R. Durner and W. Kellerer. The cost of Security in the SDN control Plane. *CoNEXT Student Workhop*, 2015.

[14] P. Emmerich, S. Gallenmüller, D. Raumer, F. Wohlfart, and G. Carle. MoonGen: A Scriptable High-Speed Packet Generator. *Proc. ACM IMC*, pp. 275–287, 2015.

[15] S. J. Eravuchira, V. Bajpai, J. Schönwälder, and S. Crawford. Measuring Web Similarity from Dual-stacked Hosts. *Conference on Network and Service Management (CNSM)*, 2016.

[16] S. Gallenmüller, P. Emmerich, F. Wohlfart, D. Raumer, and G. Carle. Comparison of Frameworks for High-Performance Packet IO. *Proc. ACM ANCS*, pp. 29–38, 2015.

[17] I. Hafeez, A. Y. Ding, L. Suomalainen, S. Hätönen, V. Niemi, and S. Tarkoma. Demo: Cloud-based Security as a Service for Smart IoT Environments. *Workshop on Wireless of the Students, by the Students, & for the Students (S3@MobiCom)*, 2015.

[18] I. Hafeez, A. Y. Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma. Securebox: Toward Safer and Smarter IoT Networks. *ACM Workshop on Cloud-Assisted Networking (CAN)*, 2016.

[19] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott. Security and Privacy in Device-to-Device (D2D) Communication: A Review. *IEEE Communications Surveys Tutorials*, 2017.

[20] N. Herold, H. Kinkelin, and G. Carle. Collaborative Incident Handling Based on the Blackboard-Pattern. *ACM Workshop on Information Sharing and Collaborative Security*, pp. 25–34, 2016.

[21] J. Iyengar and M. Thomson. QUIC: A UDP-Based Multiplexed and Secure Transport. Internet-Draft draft-ietf-quic-transport-01, Jan. 2017.

[22] W. Kellerer, A. Basta, and A. Blenk. Using a Flexibility Measure for Network Design Space Analysis of SDN and NFV. *Proc. IEEE Infocom*, pp. 423–428, 2016.

[23] I. R. Learmonth, B. Trammell, M. Kühlewind, and G. Fairhurst. PATHspider: A Tool for Active Measurement of Path Transparency. *Applied Networking Research Workshop (ANRW)*, pp. 62–64, 2016.

[24] Y. Liu, A. Hecker, R. Guerzoni, Z. Despotovic, and S. Beker. On optimal hierarchical SDN. *IEEE International Conference on Communications (ICC)*, 2015.

[25] Munich Internet Research Retreat 2016. Presentation Materials: https://www.cm.in.tum.de/en/mir/2016.

[26] Munich Internet Research Retreat 2017. https://www.cm.in.tum.de/en/mir/2017.

[27] P. Nikander, A. V. Gurtov, and T. R. Henderson. Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks. *IEEE Communications Surveys and Tutorials*:186–204, 2010.

[28] C. Prehofer, O. Horst, R. Dodi, A. Geven, G. Kornaros, E. Montanari, and M. Paolino. Towards Trusted Apps platforms for open CPS. *International Workshop on Emerging Ideas and Trends in Engineering of Cyber-Physical Systems (EITEC)*, pp. 23–28, Apr. 2016.

[29] D. Raumer, S. Gallenmüller, P. Emmerich, L. Mardian, and G. Carle. Efficient Serving of VPN Endpoints on COTS Server Hardware. *IEEE International Conference on Cloud Networking (Cloudnet)*, pp. 164–169, 2016.

[30] D. Raumer, S. Gallenmüller, F. Wohlfart, P. Emmerich, P. Werneck, and G. Carle. Revisiting Benchmarking Methodology for Interconnect Devices. *Applied Networking Research Workshop (ANRW)*, 2016.

[31] SafeCloud. http://www.safecloud-project.eu.

[32] Q. Scheitle, O. Gasser, M. Rouhi, and G. Carle. Large-Scale Classification of IPv4-IPv6 Siblings with Nonlinear Clock Skew. *CoRR*, 2016.

[33] L. Schiff, S. Schmid, and M. Canini. Ground Control to Major Faults: Towards a Fault Tolerant and Adaptive

SDN Control Network. *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops*, pp. 90–96, 2016.

[34] L. Schiff, S. Schmid, and P. Kuznetsov. In-Band Synchronization for Distributed SDN Control Planes. *Computer Communication Review*:37–43, 2016.

[35] D. Sel, S. H. Totakura, and G. Carle. sKnock: Port-Knocking for Masses. *IEEE Symposium on Reliable Distributed Systems Workshops (SRDSW)*, 2016.

[36] R. Stewart. Stream Control Transmission Protocol. RFC 4960, Internet Engineering Task Force, Sep. 2007. URL: http://www.ietf.org/rfc/rfc4960.txt.

[37] D. Thaler. Out With the Old and In With the New: Planning for Protocol Transitions. Internet-Draft draft-iab-protocol-transitions-05, Jan. 2017.

[38] B. Trammell, C. Perkins, T. Pauly, and M. Kühlewind. Post Sockets, An Abstract Programming Interface for the Transport Layer. Internet-Draft draft-trammell-post-sockets-00, Oct. 2016.

[39] K. Yasukata, M. Honda, D. Santry, and L. Eggert. StackMap: Low-Latency Networking with the OS Stack and Dedicated NICs. *USENIX Annual Technical Conference (USENIX ATC)*, pp. 43–56, 2016.