Institute of Computer Science 4
Work Group Communication Systems
University of Bonn

Prof. Dr. Peter Martini

Since October 1996, Prof. Dr. Peter Martini has been holding the chair of Computer Science 4 at the Institute of Computer Science of the University of Bonn. He also heads the work group Communication Systems at this department with 16 scientific assistants, 3 technicians, a secretary and about 30 student research assistants (as of April 2009).

1. The Institute of Computer Science 4

At the University of Bonn, the Institute of Computer Science is structured in six departments. The department 4 (Communication and Distributed Systems) is home of both the work group "Communication Systems" headed by Prof. Dr. Peter Martini and the work group "Sensor Networks and Pervasive Computing" headed by Prof. Dr. Pedro José Marrón who changed to Bonn in 2007. Together, the closely co-operating groups cover a wide range of practical and application-oriented aspects of computer science.
Both groups primarily address real-world issues. Obviously, this requires strong partners both from the commercial world and from the area of transfer-oriented research institutes. Thus, it is quite natural that the Institute of Computer Science 4 enjoys very close co-operation with the Fraunhofer Institute "Intelligent Analysis and Information Systems" (IAIS) and the "Research Institute for Communication, Information Processing and Ergonomics" (in German: Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie, FKIE), both located next to Bonn. In fact, the Institute of Computer Science 4 is connected to these institutions by long-term co-operation contracts which form the basis of personal exchange and extensive co-operative activities in teaching as well as in research. Additionally, there has been close co-operation with the Fraunhofer Institute "Algorithms and Scientific Computing" (SCAI) for many years.
The Institute of Computer Science 4 also enjoys close co-operation with the Bonn-Aachen International Center for Information Technology (B-IT). B-IT offers highly selective International Master Programs in Applied IT as well as summer/winter schools for qualified students of computer science. The Institute of Computer Science 4 is engaged in these activities of B-IT with a wide range of labs, lectures, and project groups.

2. Research

The research of the work group Communication Systems is structured in four areas, each area being headed by a scientific assistant.

- Security and Efficiency in the Internet
- Tactical Multi Hop Networks
- Dynamic End-to-End Network Services
- Performance Engineering

Of course, in daily business, the real-world orientation results in a focus on co-operation possibilities and project chances. Research often is triggered by prototypes implemented by the group itself or by co-operation partners: In quite a few cases, the prototype turned out to be more a "proof of need for further research" than a "proof of concept".
In contrast to projects coming and going, the definition of the research areas stated above is meant to remain stable over years. It is meant to be a stabilizing structure, a framework for core competences of the work group which are obtained, enhanced and preserved beyond the

activities of individual people and beyond the requirements of specific projects. This stabilizing structure also makes sure that the students active with the work group find stable work areas and short direct paths to Bachelor, Master, Diploma and/or even Ph.D. theses.

2.1. Security and Efficiency in the Internet

This research area directed by Felix Leder includes activities aiming at a more secure and a more efficient operation of network components inside the Internet or of systems attached to the Internet. The basic principle of these activities is a systematic approach to the detection of threats and shortcomings and – where possible – to healing mechanisms.
Due to the real-world orientation, technical and mathematical/theoretical issues are accompanied by legal and economical aspects which can only be successfully addressed in close co-operation with government agencies or institutions.

2.1.1. Intrusion Detection and Honeypots

Today, IT systems are under attack all the time. Intrusion detection systems (IDS) are used to distinguish legitimate from malicious access. Usually, IDS identify attacks on the basis of stored patterns or abnormal network traffic. The reaction to attacks – alarm notification to administrators, automatic preventive mechanisms, migration of services, … - strongly depends on both the kind of attack and the application area where the components under attack are integrated.
For the collection of attack patterns and for a profound classification of the corresponding threat potential, “honeypots” turned out to be extraordinarily useful. Basically, honeypots are “victim systems” which keep track of attacks in a controlled way. Thus, they provide deep insight into the approach taken by the attacker and – in some cases - into the internal mechanisms of the malware captured.
The work group Communication Systems has more than 10 years of experience in this field. In close co-operation with the Federal Office for Information Security (BSI) these activities have been substantially intensified since 2007.
As a central component of comprehensive, real-world oriented research, the work group operates a system of different honeypots with sensors within the networks of different internet service providers. Valuable information is also collected via several sensors inside the university network as well as from the extensive integration into both the national and the international “honeypot community”. Some honeypot components developed by members of the work group have been deployed world-wide.
The work group is proud of Tillmann Werner who received the AFCEA student award 2008 for his diploma thesis on “automatic generation of complex intrusion detection signatures”. The thesis shows innovative ways how to automatically compute detection patterns from samples collected in honeypot systems. This allows for a rapid integration into intrusion detection systems and may improve the protection from attacks unknown so far. After finishing his diploma in computer science, Tillmann Werner joined the work group as a scientific assistant.

2.1.2. Malware Analysis

Our research on the “deep” analysis of malware is closely related to our activities in the area of honeypots. Instead of restricting ourselves to just observing the behavior of malware in something like a black box approach, reverse engineering allows us to extract the functionality of malware captured in honeypots. This approach also provides us with new ways of classifying polymorphic or metamorphic malware, i.e. malicious code preserving its functionality while mutating (sometimes rapidly) in order to hide from intrusion detection systems or virus scanners.

From our point of view, defense against the omnipresent botnets is the most important application area of the methods addressed here. Today, millions of zombie computers are part of these systems – distributing billions of spam messages and/or supporting the organized crime in various ways.
Recent spectacular stories of success include the analysis of “Storm” - a bot with tens of thousands of machines - and the analysis of “Conficker” - a bot with more than 10 million victim systems controlled by the “owners” of Conficker. Our activities reached extensive coverage by both technology-oriented media like “Heise” or “The Register” and the mass media, including TV and radio stations.
In a live demo at the Chaos Communication Congress 2008, Felix Leder and Tillmann Werner, both scientific assistants in the work group Communication Systems, showed how they were able to become part of the control structure of Storm. Due to its peer-to-peer approach, Storm had been considered undefeatable for quite a long time. Nevertheless, the deep analysis of the Storm malware allowed them to completely understand the functionality. In addition, they were able to design and implement software components able to eliminate Storm and to sanitize the tens of thousands systems infected by Storm at that point in time. The final step – starting this software and initiating an Internet-wide sanitization – was avoided for legal reasons only: From an objective point of view, doing so would have met the criteria of computer sabotage.

2.1.3. Consistent Routing across Domains

Routing across domains requires the exchange of reachability information across autonomous systems. Today, the Border Gateway Protocol (BGP) has become the de facto standard in productive systems operated by the Internet Service Providers. However, iBGP, the operational mode of distributing reachability information within a specific autonomous system, turned out to be susceptible to various anomalies and easy to manipulate in the way it is implemented today.
The effects can be observed in real life: In large autonomous systems, anomalies occasionally arise as nondeterministic or diverging subsystems. In some cases, incorrect configurations of individual systems resulted in nonreachability of You Tube or other “politically interesting” destinations from extensive parts of the Internet.
A complete re-design of a “robust Border Gateway Protocol” seems unfeasible due to the wide application of conventional BGP and due to the application across Internet Service Providers. Instead, the work group Communication Systems focuses on a step-by-step hardening of BGP which only relies on local architectures. This makes the techniques both future-proof and applicable in real systems on a long-term basis.
The basic idea of our approach to consistent routing across domains is a formal analysis of protocol functionality which provides a deep understanding of fundamental deficiencies of the protocol used today. As an example: The work group Communication Systems could show that oscillations are caused by information reduction techniques only. Studies performed in close co-operation with the German Telekom clarified that routing anomalies can completely be avoided by a suitable local architecture. However, excluding anomalies is only a first step in the direction of a robust, consistent and correct routing: The fast and reliable detection of manipulations is a goal equally important which has high relevance in real life. Based on the know-how obtained and as a continuation of related activities in this field, we are working on significant results and approaches for mastering theses challenges.

2.2. Tactical Multi Hop Networks

In this research area headed by Dr. Nils Aschenbruck, we work on the design and robust operation of wireless communication systems in tactical scenarios. Here a reasonable wired

communication infrastructure either has been destroyed or never has been deployed. This is a typical scenario for wireless multi hop networks: Both civil and military units require robust and fail-safe communication systems. For obvious reasons, the work group intensively co-operates with the armed forced oriented research institute FGAN-FKIE in this field.

2.2.1. Security

Both civil and military crises situations usually result in conflicting interests which come along with increased risks. Attacks against the multi hop routing such as “blackholes” and “wormholes”, jamming and others are effective and dangerous interventions into tactical multi hop networks. Thus, research on robust techniques for attack detection and reasonable countermeasures is one of the mayor activities by the work group Communication Systems. In tactical scenarios, the hierarchical communication structures usually are imposed anyway. This opens the door to the application of dedicated, specialized techniques. Strategies known from wired networks or from general multi hop scenarios are evaluated, adapted and optimized for the specific circumstances in these tactical networks.

2.2.2. Reality Oriented Scenario Modeling

Robustness of a communication system can only be guaranteed if all components have been thoroughly scrutinized with respect to performance issues. For scalability reasons and for the sake of reproducibility, this kind of studies often is done by simulations. Obviously, the results obtained strongly depend on the models used. However, for tactical scenarios there only is a very limited number of realistic models. Therefore, the work group addresses this field of realistic modeling for both civil and military scenarios. To ensure real life orientation, there is close co-operation with fire fighters, home land security, and armed forces. Raw data (movement and data traces) obtained from maneuvers provide a solid basis for realistic modeling.

The models custom-tailored to this specific field are used for performance studies with simulation and/or emulation. They allow for the sound design of algorithms, protocols and applications for tactical scenarios.

2.2.3. Application Development and Protocol Design

An additional field of interest is the design and development of applications and protocols for the units active in tactical scenarios. Both situational awareness and appropriate command/control require the collection of sensor data, the reliable transportation of the sensor data to the command station and sensor data fusion. Thus, distributed applications with a strong focus on sensor data fusion (in particular: tracking) have to be designed, implemented, and evaluated. Robust and optimized operation of this kind of applications requires parameterization and optimization of the protocols used. To ensure practicability, the applications and protocols designed are tested in maneuvers.

2.3. Dynamic End-To-End Network Services

In this research area headed by Dr. Matthias Frank, the work group Communication Systems has been active on the design, implementation and supervision of mechanisms for measuring and improving the end-to-end performance of communication systems for more than 15 years. Here, the focus is on the “look&feel” experienced by the end user. Internal network characteristics are subject to abstraction as far as possible.

2.3.1. Guaranteed Services

Today, the Internet is tailored around the idea of a “best effort service” which definitely is fine for the wide majority of applications. Of course, this statement only holds if significant

overload situations of specific network components can be avoided. Thus, the majority of problems are solved by "throwing bandwidth" at these problems.
For some applications, such as TV production with live transmission or specific kinds of grid computing, a significantly more reliable network service is required. This kind of service can only be reached by advance reservations and efficiency optimized scheduling of future data streams. Basically, the implementation of this kind of reservations can be achieved by techniques such as MPLS or GMPLS. However, there still is a wide gap been fundamental feasibility and flexible, practical applicability in this field. The work group Communication Systems has been active in the area of guaranteed services for many years with financial support by the German Research Foundation, the Federal Ministry of Education and Research and by the European Union.

2.3.2. Group Oriented Services

"Group oriented services" are becoming more and more important in areas where the best effort service is not sufficient but where hard service guarantees cannot or shall not be supported by the underlying networking technology. In these areas it seems attractive to look for mechanisms which are both co-operative and explorative: Explorative in the sense that the end systems estimate the available bandwidth by appropriate end-to-end mechanisms. Co-operative in the sense that the end systems co-ordinate their usage of the available network resources.
Of course, TCP is the "classic" approach of handling this challenge at the transport layer. However, the data streams of the corresponding applications often include several TCP streams. Thus, an application oriented co-ordination at a higher layer is required for reaching a co-operative and explorative behavior from an application point of view.
For many years, the work group Communication Systems has been active in research on various aspects of the area sketched here. In the recent past, basic research efforts on the integration of media servers played an important role. Currently, the area of command and control systems is in the centre of interest – with a focus on military environments.

2.3.3. Network Optimization

The analysis and improvement of the end-to-end of performance of network services is in the centre of interest of research activities where measurements are performed in real systems on an end-to-end basis. The major goal is to obtain important hints for the optimization of network parameters and for improvements to the protocol performance from simulations and emulations based on these measurements.
Measurements in public mobile communication systems of current and future generations have been performed extensively. With air time being (and remaining) a scarce resource and with the user experience massively influenced by the mobile device used, there still is a lot of room for improvement.
After several years of funding by the European Union, currently the activities are tailored to the requirements of bilateral co-operation with companies such as T-Mobile and T-Mobile International.

2.4. Performance Engineering

Today, we enjoy a wide range of both scientific results and available tools for the performance evaluation of complex systems. However, in the commercial world we note a wide gap between simply relying on the "educated instinct" of experienced staff on the one hand and the practical application of performance analysis tools on the other hand.
In the research area "performance engineering" headed by Patrick Peschlow, the work group Communication Systems tries to bridge (at least a part of) that gap for selected application

areas. An additional focal point is enhancing the efficiency of performance evaluation techniques.

2.4.1. Performance-Driven Modeling Methodologies

In close co-operation with companies such as Nokia or Capgemini, the work group Communication Systems was able to show that non-functional characteristics and requirements can seamlessly be integrated into the formal design process of commercial hardware and/or software. Using this approach, solid knowledge about performance issues becomes a part of the design process at a very early stage. This results in a profound understanding of the system performance to be expected.

When it comes to the development of complex systems, we find different modeling approaches with respect to the documentation of functional requirements and with respect to design decisions. However, in the commercial world the “Unified Modeling Language” (UML) has become an established way to go. This approach is additionally strengthened by the concepts of SysML and the UML-Marte-Profile.

The approach followed by the work group Communication Systems aims at extending this way of modeling by a seamless integration of performance annotations. To us, this seamless integration and maximum transparency seems to be necessary to make sure that the system developers are not slowed down in their daily work in an inappropriate way. The primary goal is acceptance and adoption of these new mechanisms and tools.

2.4.2. Performance Models

Annotating system models by performance aspects paves the way for the development of performance models which can be studied by mathematical analysis or by simulation. If done appropriately, these studies provide valuable hints with respect to the performance to be expected: Very general models support the design process in a very early stage by providing rough performance estimates. More specific models allow for more precise predictions based on additional details of the hardware and software modeled.

According to the approach followed by the work group Communication Systems, the transformation from a system model to a dedicated performance model is done in a completely automated way – transparent to the developer. Thus, there is no requirement for the developer to be familiar with details of the underlying theories. This approach avoids roadblocks for the users and allows for a wide application of performance engineering in the commercial world.

The analysis of complex distributed software environments is based on extended queuing networks which allow for the direct integration of trace files. Thus, developers are provided with dedicated support for incremental work where the design of new systems is based on experiences and performance data of previous versions.

In close co-operation with Nokia, the work group Communication Systems developed a performance model of embedded devices such as mobile phones, DVD players and vehicles equipped with ARM processors. These models allow developers to optimize and test hardware optimizations for specific scenarios without actually implementing these devices as prototypes.

2.4.3. Advanced Simulation Techniques

In recent decades, amazing progress has been achieved in simulation technology. Nevertheless, simulation of complex systems still quite often suffers considerably from the limits imposed by practical applicability in terms of simulation runtimes and/or memory requirements.

Several projects funded by the German Research Foundation DFG allowed the work group Communication Systems to do research on innovative techniques of dynamic distribution

(partitioning) of simulation runs to several CPUs or several computers. As primary application area we chose simulations of mobile ad hoc networks. Here, innovative combinations of state-of-the-art mechanisms and some new techniques turned out to provide excellent results. As an example: With commercial off-the-shelf multi-core computers, an almost optimum (i.e. linear) speedup has been reached for real-world oriented simulation scenarios. Future activities will focus on the extension of cloning techniques which allow for a dedicated analysis of alternative simulation runs without repeating common parts of the simulation over and over again. This approach results in both drastically reduced run times and drastically reduced memory requirements.
Cloning techniques also promise to be extremely relevant for the in-depth handling of simultaneous events and for simulations with deliberately imposed inaccuracies in event timing. In the areas addressed here, our group co-operates closely with researchers at the Florida International University.

3. Teaching

The full integration of research and teaching allows the work group Communication Systems to offer a wide range of courses – far more than required according to formal regulations derived from the funding of staff by the state of North Rhine-Westphalia. The basic idea of our teaching activities is to take interested students on a steep path to the current state-of-the-art in research and in the commercial world.
In the bachelor program "Computer Science" (courses in German) the work group Communication Systems annually offers the compulsory lecture "System-oriented Informatics". This lecture covers a wide range of topics such as key concepts of machine languages, essentials of compiler construction, and essentials of common operating systems. It also includes an introduction to fundamentals of Internet technology.
Based on the System-oriented Informatics, the work group also offers the annual compulsory lecture "System-oriented Programming" with extensive hands-on components with programming tasks. Here, the students learn about network programming and distributed programming from a write-your-own-programs perspective.
With the System-oriented Informatics in the second semester and the System-oriented Programming in the third semester of the bachelor curriculum, the students already are able to do complicated programming tasks in the area of networks and distributed systems just a little more than one year after they commenced their studies. Thus, they are able to do exciting tasks in the project groups offered by the work group Communication Systems. Typically, the portfolio of project groups includes "Malware Analysis", "Ad Hoc Networks", "Laser & Light" and "Tracking". Many students also become student research assistants taking active roles in our research projects.
The work group additionally offers a bachelor course "Communication in Distributed Systems" which is also held annually. In this course, the students achieve in-depth knowledge in selected areas of communication technology such as addressing, routing, flow control and congestion control.
In the internationally oriented master program "Computer Science" (courses in English), the work group is active annually in the first semester course "High Performance Networking". This lecture – organized in co-operation with the group headed by Prof. Marrón – both consolidates the basic knowledge usually achieved in bachelor programs and discusses selected hot topics in the area of networks and distributed systems. The course High Performance Networking provides the basis for the annual in-depth courses "Network Security" and "Mobile Communication". All of these courses organized by the work group Communication Systems include a substantial amount of practical exercises.
All master courses are also open both to the students still active in the diploma program "Computer Science" and to the students of "Media Informatics" at the B-IT. Some of the

courses are held several times during the same semester to allow for a seamless integration into the different curricula.
Finally, the work group Communication Systems offers courses in the framework of the “International Program of Excellence in Computer Science“ (IPEC) organized by B-IT as a special offer to intellectually gifted students who learn faster than others and want to shorten their time spent at the university by attending block courses during the free period.
In recent years, the quality of teaching could be improved substantially by financial resources which became available from tuition fees. In the computer science department, the newly established tuition fees enabled both a considerable modernization of the devices available in the laboratories and an extension of the course offerings. In particular, the extreme real-world orientation characteristic for all courses organized by the work group Communication Systems would be impossible without these additional resources.

Further information is available online at:
http://net.cs.uni-bonn.de