INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato práce vznikla za podpory projektu TeamIt, jenž je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky prostřednictvím grantu ESF CZ.1.07/2.3.00/09.0067.

Budování konkurenceschopných výzkumných týmů pro IT

Charakteristika výzkumných skupin

Brožura

31. 8 .2012

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ VUT V BRNĚ
Božetěchova 2, 612 66 Brno
tel.: +420 541 141 144, +420 541 212 219, fax: +420 541 141 170, 270
http://www.fit.vutbr.cz, http://teamit.fit.vutbr.cz

Obsah

Accelerated Network Technologies Research Group

Accelerated Network Technologies (ANT@FIT) research group was formed in September 2009 by group of researches ad PhD students at Faculty of Information Technology , Brno University of Technology. The research group deals with acceleration of time critical operations, which are used in devices for network infrastructure or devices for network monitoring and security. Network traffic processing speed is crucial in most of the network devices, because any packet drop can lead to lower quality of network services, affect precise monitoring or disallow intrusion detection and prevention. Nowadays solutions are either expensive or provide only limited performance. Therefore research group focuses on novel algorithms and architectures, which allow construction of devices and applications with higher throughput at lower price. We use standard processors, MultiCORES and FPGA technology and concentrate on time critical operations like packet header analysis and extraction, classification of packets, longest prefix match, pattern matching and flow CACHE management. Any improvement of these operations has direct impact to parameters and price of network devices and systems. Effective utilization of parallel processing can significantly increase processing speed, lower space complexity can improve parameters (more filtration rules or patterns) and reduction of hardware resources can decrease device or system price.

The research group also deals with design of devices and systems for network infrastructure, security and monitoring. In this area, we cooperate mainly with CESNET and Liberouter project and focus on system for high speed networks based on computer and acceleration cards, but we also design small size embedded systems with low power consumption and price.

The team is managed by Jan Kořenek, who is a researcher at Brno University of Technology since 2003, leader of hardware design group at Liberouter project since 2004 and is one of the founder of successful spin-off company INVEA-TECH. The team members has substantial experience in the network field, which was obtained by working on a number of European projects (including 6NET IST-2001-32603, SCAMPI IST-2001-32404, GEANT2 No. 511082) and on a number of locally funded projects (CESNET MSM6383917201 and VUT MSM002163528). In these projects, FPGA technology was used for an acceleration of IPv6 protocol routing, network traffic monitoring, NetFlow statistic measurement and fast regular expression matching in packet payload. Network devices and probes are hardware accelerated using FPGA technology, therefore the probes can provide precise and detailed information about the network no matter of 1Gbps and 10Gbps speed.

Research

Packet classification -is a task which is used in many network devices such a firewall, IDS or IPS systems. The classification matches packets with set of rules, which are usually defined by values, ranges or prefixes of packet header fields. Generally, the classification is a mathematical problem of multidimensional range search. Due to the rule set size and complexity of rules, it is very difficult to match all rules in very short time, which is needed by nowadays multi-gigabit networks. Therefore we focus on novel algorithms and architectures with reduced time and space complexity..

Pattern matching - is a time critical operation mainly used in IDS and IPS systems for detection of malicious network traffic by set of patterns, which are often described by strings or regular expressions. Pattern matching checks presence of patterns in packet payload or TCP streams. As every byte in packet payload has to be inspected, high computational power is required even for currently used gigabit networks. Moreover, set of patterns is converted to appropriate data structure, which can not easily fit to on-chip memory. Therefore we focus on design of novel algorithms and architectures with reduced space complexity and multi-gigabit throughput.

Longest Prefix Match -refers to an algorithm used by many network devices to select the most specific table entry (prefix) which matches for given IP address. The LPM operation is typically being performed by routers, but it's utilized in several classification methods as well and can be used by firewalls and other devices. The coming IPv6 protocol and growth of internet (and router tables) create new challenges which we address by our research. The goal is to explore and compare current LPM algorithms and design novel ones focused on high speed operation and low memory usage.

Flow Context Management – Keeping a context for every flow is an essential task of most network devices such as firewall, IDS and monitoring probes. Due to an excessive amount of flows context management is a challenge. We tackle research problems such as how to efficiently index and filter flow data as well as how to distribute them among computational resources.

Packet Header Analysis - s task which needs to be performed by all network devices in order to gather specific information from network packets like IP addresses, Ports, start of L7 layer etc. We are putting focus on developing and optimizing ASIC/FPGA IP core for network packet processing intended for multi-gigabit networks.

NetCOPE platform – NetCOPE was designed in scope of Liberouter project. It is a platform dedicated for acceleration of network applications using FPGA technology. Such an accelerated network application is usually composed of two parts:

1. *Acceleration core* – which is placed inside FPGA chip and implements time critical parts of application such as header field extraction, classification process, patter matching etc.;
2. *Software part of application* – usually provides management and control function. NetCOPE covers both – hardware and software part of the platform and precisely defines the general interface between them.

Current Research Projects

- TeamIT - Building Competitive Research Teams in IT, MŠMT, CZ.1.07/2.3.00/09.0067, 2009-2012, running
- Security-Oriented Research in Information Technology, CEZ MŠMT, MSM0021630528, 2007-2013, running
- Optical National Research Network and its New Applications, CESNET, MSM6383917201, 2004-2010, running (Participation on Liberouter project)

Packet Header Analysis

Packet protocol header analysis and extraction of header fields needs to be performed in all network devices. As network speed is increasing rapidly, high speed packet header processing is required. In most of the network devices is protocol analysis performed using multi-core network processor which provide sufficient throughput for this task. However there are applications where network processor needs to be extended with custom-made chip in order to reach required throughput or satisfy specific IO requirements. Fur such systems it could be beneficial to implement whole system on the single chip (SOC) in order to reduce cost per unit. For such system it is required to have IP core for fast protocol header analysis.

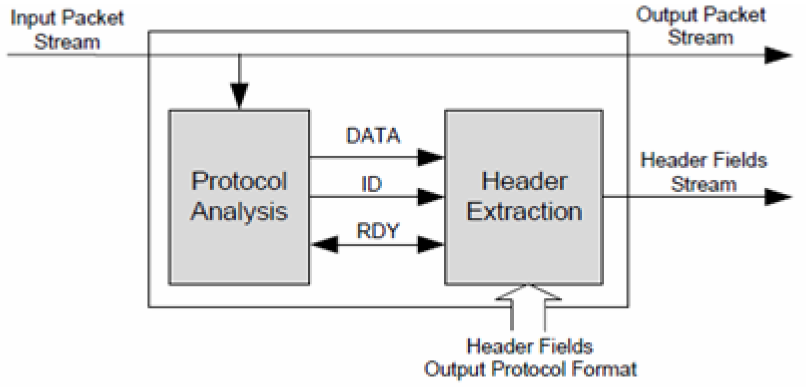


Figure 1.1: Architecture of Packet Header Analysis and Extraction Engine

We have proposed architecture of such IP which divide packet processing problem into two tasks: protocol analysis and header extraction. We have developed simple algorithm which automatically generate protocol analysis FSM based on network protocols described in our XML protocol description language. The protocol analysis engine is able to analyze up to 128 bits of packet data within 8 ns which is sufficient throughput for 10 Gbps networks. Configurable extraction engine is able to extract selected header fields and send them in fixed-length user specific packet format for additional processing (flow monitoring, classification).

Even through this concept has great throughput with a relatively small amount of consumed hardware resources there is a large space for optimizations and improving this architecture. Current work is putting focus on

1. Use of NetPDL language for specifying network protocols
2. Protocol analysis engine optimizations for time and area using techniques from high level synthesis
3. Extraction engine optimization for specified output frame format
4. Comparison of current architecture with approaches based on FPGA processors

Selected publications:

- **Kobierský Petr, Kořenek Jan, Polčák Libor**: Packet Header Analysis and Field Extraction for Multigigabit Networks, In: Proceedings of the 2009 IEEE Symphosium on Design and Diagnostics of Electronic Circuits and Systems, Liberec, CZ, IEEE CS, 2009, p. 96-101, ISBN 978-1-4244-3339-1
- **Dedek Tomáš, Marek Tomáš, Martínek Tomáš**: High Level Abstraction Language as an Alternative to Embeded Processors for Internet Packet Processing in FPGA, In: 2007 International Conference on Field Programmable Logic and Applications, Amsterdam, US, IEEE CS, 2007, s. 648-651, ISBN 1424410606

Pattern Matching

Pattern matching is a time critical operation for IDS and IPS systems such as Snort or Bro. Every byte of packet payload or data stream must be processed. We have focused mainly on regular expression matching, because regular expressions are more powerful than strings and their usage in IDS/IPS systems is steadily increasing. Regular matching algorithms can be divided into two groups according to the type of automaton used for implementation of regular expressions. First group is based on deterministic finite automata (DFA) and second is based on nondeterministic finite automata (NFA). First group is designed for usage in devices based on processors or ASICs and uses external memory for storage of transition table. Research in this group is mainly focused on lowering the memory consumption of transition table. Second group is designed for usage in reconfigurable hardware (FPGA) and exploits its inherent parallelism. Research in this group is mainly focused on reduction of

FPGA resources consumption.

Our research group introduced the NFA-split architecture and Perfect Hashing DFA and its variants. We have also studied formal reductions of NFA to further reduce utilization of FPGA resources. The NFA-split architecture combines both NFA and DFA to reduce FPGA resources utilization. The Perfect Hashing DFA uses perfect hashing to compact the transition table. The variants of this architecture further reduce the size of utilized memory.

Selected publications:

- **Kořenek Jan, Košař Vlastimil**: Efficient Mapping of Nondeterministic Automata to FPGA for Fast Regular Expression Matching, In: Proceedings of the 13th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems DDECS 2010, Vienna, AT, IEEE CS, 2010, p. 6, ISBN 978-1-4244-6610-8
- **Kaštil Jan, Kořenek Jan, Lengál Ondřej**: Methodology for Fast Pattern Matching by Deterministic Finite Automaton with Perfect Hashing, In: 12th EUROMICRO Conference on Digital System Design DSD 2009, Patras, GR, IEEE CS, 2009, p. 823-289, ISBN 978-0-7695-3782-5

Packet Classification

Packet classification is one of the basic steps in providing network security, enabling traffic policing, QoS provisioning, reliable transfers in VPN networks performed in network devices like firewalls or routers. Given a set of rules the goal is to find a best-matching rule to the header fields of incoming packets. Since classification involves many header fields, finding an algorithmic solution providing a wire-speed performance and acceptable memory requirements has achieved a great deal of interest in research community.

One of the promising techniques to cope with this problem is decomposition where classification is performed in several steps. The first is Longest Prefix Match done independently for every involved header field. The second is a mapping of the LPM results to the existing rule number. Using a perfect hashing approach for such a mapping it is possible to ensure fixed number of memory accesses and thus achieve constant time complexity which is essential for network security devices.

Perfect Hashing Crossproduct Algorithm for classification:

- provides wire-speed throughput independent of ruleset complexity
- significantly reduces memory resources using a hashing
- allows easy implementation in hardware
- is fully competitive to the other high-performance classification
- techniques

Selected publications:

- **Puš Viktor, Kořenek Jan**: Fast and scalable packet classification using perfect hash functions, In: Proceeding of the ACM/SIGDA international symposium on Field programmable gate arrays, New York, US, ACM, 2009, p. 229-236, ISBN 978-1-60558-410-2
- **Kořenek Jan, Puš Viktor**: Memory Optimization for Packet Classification Algorithms, In: Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, New York, US, ACM, 2009, s. 165-166, ISBN 978-1-60558-630-4

Flow Context Management

Keeping a state - context - per each flow is an essential task of most network devices such as stateful firewall, IDS, monitoring probes, QoS appliances and routers. Basic operation includes a lookup and update of a corresponding flow state per each incoming packet. Meanwhile, flows that are no longer active must be identified and expired. A flow is defined as a set of packets baring the same property, in most cases a 5-tuple of source and destination IP addresses, source and destination transport ports and protocol. Due to an excessive amount of such flows, context management is a challenge that has not been sufficiently addressed.

We focus on (a) various indexing algorithms to lookup and store a flow state, (b) filtering and sampling packet algorithms to reduce the load on a system and (c) various management techniques to identify inactive flow states as well as to identify flow states that are most relevant and is worth to keep them in memory at any cost.

Our basic indexing algorithm builds upon a direct addressing of a flow state where the address is a hash computed upon the 5-tuple of a flow. Naturally such scheme induce a huge amount of collisions, i.e., situations when two distinct flows share the same hash value. We evaluate such scheme analyticaly as well as using simulation on real traffic traces to estimate collision rate for various sizes of memory. Following the results we can design indexing scheme that reduces the amount of collisions but is still simple enough to fit FPGA implementation, for example Naive Hash Table (see Figure), Cuckoo Hashing and their modifications.

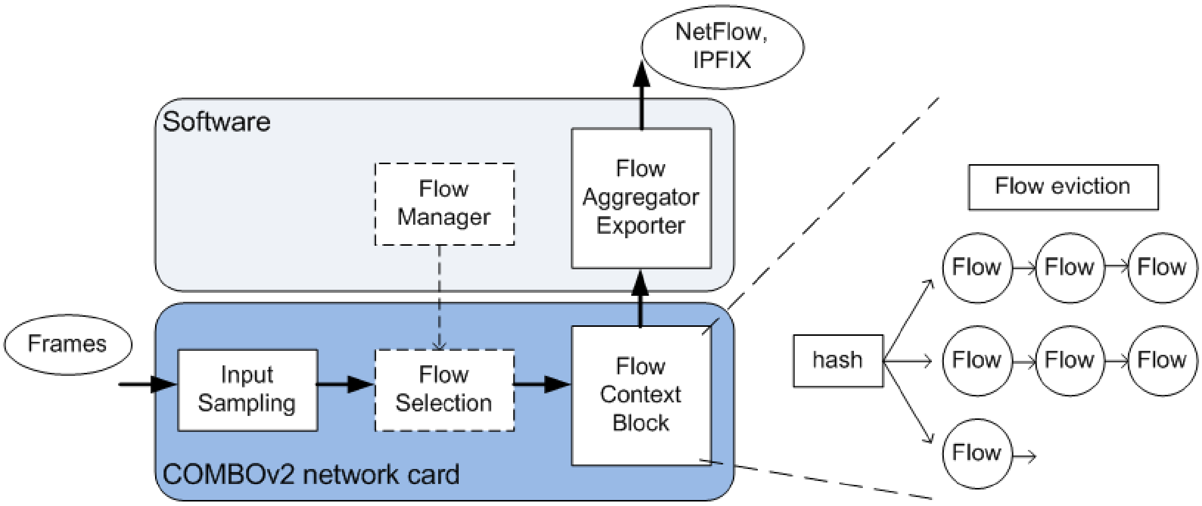


Figure 1.1: Scheme of Flow measurement system

Further, we experiment with filtering and sampling mechanisms and their impact on occupation of flow table as well as quality of data being measured. It is expected that different sampling methods suits different target application running above collected flow data. E.g., a firewall cannot loose a packet whereas a monitoring probe may drop packet and consequently correct the result of measurement based upon the sampling rate selected. Moreover certain application may focus only on a given type of flows (such as elephant flows) or subset of flows (such as flows belonging to a subnet or user).

To match a wire-speed performance when keeping flow states memory management plays an important role. The goal is to keep heavy-hitter flows in a fast memory while keeping small and slow ones in a large and slow memory. Such partitioning is possible due to well-known fact that only few flows accounts for majority of traffic volume. The hard part is to identify these heavy-hitters as standard algorithms (e.g., LRU - Least Recently Used) do not suit network data well. If a memory gets full eviction policy decides which flow states to expire. Its implementation must be easy and its application swift get rid of flows that are no longer alive or relevant. In this context we design and experiment with novel eviction policies, for example S3-LRU.

Selected publications:

- **Canini Marco, Li Wei, Žádník Martin, Moore Andrew W.**: Experience with High-Speed Automated Application-Identification for Network-Management, In: Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems, Princeton, US, ACM, 2009, p. 209-218, ISBN 978-1-60558-630-4
- **Žádník Martin et al**: Tracking Elephant Flows in Internet Backbone Traffic with an FPGA-based Cache, In: 19th International Conference on Field Programmable Logic and Applications, Prague, CZ, IEEE, 2009, p. 640-644, ISBN 978-1-4244-3892-1

- **Žádník Martin, Kořenek Jan, Lengál Ondřej, Kobierský Petr**: Network Probe for Flexible Flow Monitoring, In: Proc. of 2008 IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop, Bratislava, SK, IEEE CS, 2008, p. 213-218, ISBN 978-1-4244-2276-0

Networked and Embedded Systems Research Group

Networked and embedded systems (NES@FIT) research group was established in 2009 by a team of researches and PhD students sharing the strong interest in networking, networked and embedded systems and network design. The research group focuses on topics related to network security and employs methods that include formal specification and verification techniques, modeling and simulation, and monitoring and real-time analysis. Current research topics are:

- Formal methods for network configuration analysis
- Network Simulation and Modeling (NeSim)
- Network security, communication monitoring and analysis

The competences of the team members are sufficient to carry out the basic and advanced research tasks in the area of network security research. In particular, members of the research group have ability to:

- understand practical aspects of networking and definition of research objectives on the practical level. It helps us to state the ideas clearly and to keep the research in the direction of the given objectives,
- research and apply various formal methods in the context of networking and network security. Formal methods are used in a new domain not being studied previously.
- experience with simulation techniques for network traffic analysis and modeling, and the knowledge of traffic simulation and performance evaluation methods.
- experience with the program construction for preparing and conducting experiments. Also team members are familiar with writing and customizing various networking tools.

Team members have theoretical and industrial experiences in the following areas:

- practical aspects of network administration, network design and configuration,
- theory of networking concepts and security issues in networks,
- multicast traffic delivery, theory of routing protocols and algorithms,
- wireless and ad-hoc networking, and
- formal specification, modeling and verification methods.

The research group is led by Petr Matoušek, who has held an assistant professor position at Brno University of Technology since 2005 and has experiences from his previous research position in LIAFA, network administrator position in CERN, Switzerland, and technical training in Digital Engineering, Ireland. The team members have participated in several research projects aiming mainly at researching network security.

Formal methods for network configuration analysis

Network design is a complex task. Network specialists are expected to fulfill customers' requirements, while considering the limits of underlined technologies. The goal is to provide reliable network services as requested. Once the design is finished, the deployment phase is launched. It consists of installation and physical interconnection of the devices, setting up their configurations, and finally, network troubleshooting, in order to assure network functionality. Identification of potential problems as early as possible in the design phases is a serious argument for extra techniques and methodologies that verify and validate the results of the design process.

The goals of this research project consist of i) creation of a unifying model suitable for description of relevant aspects of real computer networks, including routing information, ACLs (access control lists), NAT (network address translation), dynamic routing policy and ii) delivering methods for automated verification of dependable properties (e.g., availability, security, survivability). The unique added value of the project is to specifically merge the research on formal methods with the research on network security to devise a new method for network security verification.

The recent work has focused on studying models and analysis techniques based on simulation and network monitoring. These models, nevertheless, do not take into consideration routing and packet filtering despite the fact that these aspects may significantly influence the traffic coverage observed in the network. The intensive research needs to be done in order to find new models that would include dynamic view on the network.

Similarly to hardware and software analysis based on simulation, the network simulation methods are useful mainly to observe properties given by normal behavior of the system. Simulation techniques are inefficient in catching "what if" cases that occur rarely in the system. However, the real world systems inevitably exhibit also the unusual behavior. The use of formal methods is better suited for checking these situations to uncover hidden problems.

Selected publications:

- Švéda, M., Ryšavý, O., De, S., G., Matoušek, P., Ráb, J.: Static Analysis of Routing and Firewall Policy Configurations, e-Business and Telecommunications, Heidelberg, DE, Springer Science+Business Media, 2012, p. 39-53, ISBN 978-3-642-25205-1
- Švéda, M., Ryšavý, O., De, S., G., Matoušek, P., Ráb, J.: Reachability Analysis in Dynamically Routed Networks, In: Proceedings of the IEEE ECBS 2011, Piscataway, NJ, US, IEEE CS, 2011, p. 197-205, ISBN 978-0-7695-4379-6
- Švéda, M., Ryšavý, O., Matoušek, P., Ráb, J.: An Approach for Automated Network-Wide Security Analysis, In: Proceedings of the Ninth International Conference on

Networks ICN 2010, Les Menuires, FR, IEEE CS, 2010, p. 294-299, ISBN 978-0-7695-3979-9

- Matoušek, P., Ráb, J., Ryšavý, O., Švéda, M.: A Formal Model for Network-wide Security Analysis, In: Proceeding of the 15 IEEE International Symposium and Workshop on the Engineering of Computer-based Systems, Belfast, GB, University of Ulster, 2008, p. 171-181, ISBN 0-7695-3141-5

Network simulation and modeling

Configurations of active devices define network communication. From this point of view, network behavior can be predicted and analyzed using configuration files. This project exploits discrete simulation of a network for automated analysis of security properties. Network topology is formally built using nodes (e.g., routers) and links. Nodes include network interfaces with IP addresses, filtering rules (express using ACLs), and routing processes. Using automated simulation with changing configuration (links going up and down), dynamic behavior of the network is observed and analyzed. The goal is to find out weak points of the network design and configuration.

Responsibilities of L2 layer include data delivery to/from adjacent network devices (either on point-to-point links or on shared segments), segmentation of set of hosts into VLANs and prevention against loops. Responsibilities of L3 layer is mainly routing, load-balancing and asymmetrical packet exchange, ACLs filtering, policing and shaping of traffic. Often we would like to test functionality of technologies implementing previously mentioned responsibilities in a safe environment. Simulation and modeling offer this opportunity.

Motivation behind this research is to deliver architecture and tools capable of the following:

1. Direct communication with network devices enabling to pull/push running configuration and dynamic state from/into routers and switches.
2. Creation of a network model based on information acquired through direct communication or based on a topology description.
3. Simulation of L2 switching and L3 routing using developed models.
4. Formal verification and analysis of multicast communication models with optional recommendations how to “repair” a running configuration with respect to results.

We have decided to extend OMNeT++ discrete event simulator, in particular, one of its framework called INET, which includes LAN/WAN network models. Our contribution consists of new and improved models for:

- unicast and multicast routing – IPv6 support and implementing logic of routing protocols RIP, RIPng, OSPFv3, PIM-DM, IS-IS;
- QoS – differentiated services support with DiffServ code marking and QoS enforcing with help of different queuing algorithms (e.g. FIFO, LLQ, WFQ, CBWFQ) and dropping algorithms (e.g. RED, WRED);

- L2 loop-preventing and high availability mechanisms – family of spanning tree protocols (e.g. STP, RSTP and MSTP), first simulation models for TRILL and protocols guaranteeing first hop redundancy (e.g. HSRP, VRRP, GLBP);
- alternative and experimental routing proposals like LISP and RINA.

We are also focused on ways of automated computer network topology discovery with help of protocols SNMP, CDP and LLDP. And our last field of interest is automated creation of topology simulation models through translation of vendor-specific configurations (using specific grammars) into independent network description format.

Selected publications:

- Veselý, V., Matoušek, P., Švéda, M.: Multicast Simulation and Modeling in OMNeT++, In: Proceedings of the IEEE 5th International ICST Conference on Simulation Tools and Techniques, Desenzano del Garda, IT, ICST, 2012, p. 298-301, ISBN 978-1-936968-47-3
- Veselý, V., Švéda, M.: L2 protocols in OMNeT++, IP Networking 1 -- Theory and Practice, Žilina, SK, EDIS ŽU, 2012, s. 37-40, ISBN 978-80-554-0494-3
- Matoušek, P., Ryšavý, O., De, S., G., Danko, M.: Combination of Simulation and Formal Methods to Analyse Network Survivability, In: Proceedings of the IEEE 3rd International ICST Conference on Simulation Tools and Techniques, Malaga, ES, ICST, 2010, p. 6, ISBN 978-963-9799-87-5
- Švéda, M., Ryšavý, O., Matoušek, P., Ráb, J., Čejka, R.: SECURITY ANALYSIS OF TCP/IP NETWORKS -- An Approach to Automatic Analysis of Network Security Properties, In: Proceedings of the International Conference on Data Communication Networking ICETE-DCNET 2010, Athens, GR, INSTICC, 2010, p. 5-11, ISBN 978-989-8425-25-6

Network security, communication monitoring and analysis

Network monitoring is an essential task of network management. Information obtained by monitoring devices gives a real picture of the network in production including transmitted data volumes, top hosts, a list of frequently used applications etc. Deep analysis of data collected by monitoring can reveal network attacks or detect misuse of network services. In addition, Data Retention Act requires each ISP to track user’s activities. Protocol IPv6 puts new challenges for network administrators in the context of user identification. Unlike IPv4, an IPv6 address no longer uniquely identifies a user or PC. IPv6 address can be randomly generated and keeps changing in time. PCs with IPv6 stack can also communicate via predefined tunnels over IPv4 infrastructure. That tunneled traffic mostly bypasses network security implemented via firewalls. In this paper, we identify major monitoring and security issues of IPv6 connectivity and propose a solution based on SNMP and Netflow data that helps to uniquely identify users. The solution requires an extended set of monitoring data to be collected from network devices.

Traditional monitoring approaches are usually not applicable to IPv6 traffic because of temporary addresses, different types of encapsulation of IPv6 over IPv4, non-unique mapping between data link addresses and IP addresses, tunneling, etc. Another challenge of IPv6 monitoring is tunneling IPv6 over IPv4. Tunnels encapsulate application data into tunneling protocols that have different IP headers and ports so the packets can bypass firewall rules. A real transition to the native IPv6 may last for months or years, so monitoring of tunneled traffic is actually required in order to detect stations that can be potentially sources of uncontrolled user traffic.

We developed an integrated system for IPv4 and IPv6 data communication monitoring. Today, ISPs identify their hosts based on the host's IPv4 addresses. Usually the ISP has a central Network Management System (NMS) that collects network statistics including a list of users with registered IPv4 and MAC addresses. MAC address is used in DHCP configuration to assign a correspond- ing IPv4 address. Registered MAC addresses together with system logs of DHCPv4 server and data from Radius server are sufficient enough to uniquely identify the user based on the IPv4 address. User monitoring of IPv6 traffic is more complicated. The IPv6 address is no longer a unique identifier as it was with IPv4 address. That is mainly because of temporary address as described above. There are two ways how IPv6 addresses can be assigned. Practical experience at BUT shows that stateful configuration using DHCPv6 does not work properly so only stateless configuration can be deployed.

Stateful IPv6 configuration uses DHCPv6 to provide IPv6 addresses and other configuration parameters. Unfortunately, there are several DHCPv6 limitations causing that it cannot be used for stateful addressing. The main reason is, that default gateway cannot be obtain via DHCPv6 so stateless configuration has to be deployed as well. This means that Windows systems use temporary address for communication instead of the address obtained through DHCPv6, because temporary addresses have higher priority. In addition, DHCPv6 client is not supported in Windows XP, which is still widely used. DHCPv6 also does not identify hosts with MAC ad- dress as DHCPv4, but with DHCP Unique Identifier (DUID). This cannot be easily used as user identifier.

Stateless IPv6 configuration is using RA (Router Advertisement) messages. The first part of the IPv6 address—network prefix—is assigned using RA messages together with default gateway and others options. The second part of the IPv6 address—interface ID—is generated using EUI-64 or privacy extensions. Because EUI generated with privacy extensions has higher priority than EUI-64, EUI also cannot be used as a unique identifier.

Similar issue needs to be addressed in Lawful Interception systems. These are designed to capture selected data from local communication as requested by security agencies. There are several standards for LI available that define requirements on intercepted data and architecture of LI system as a whole. Advent of IPv6 protocol unveils several shortcomings of current LI specifications. One of the major concerns is user identification for IPv6 no longer use traditional IPv4 address assignment methods. Current identification methods employing

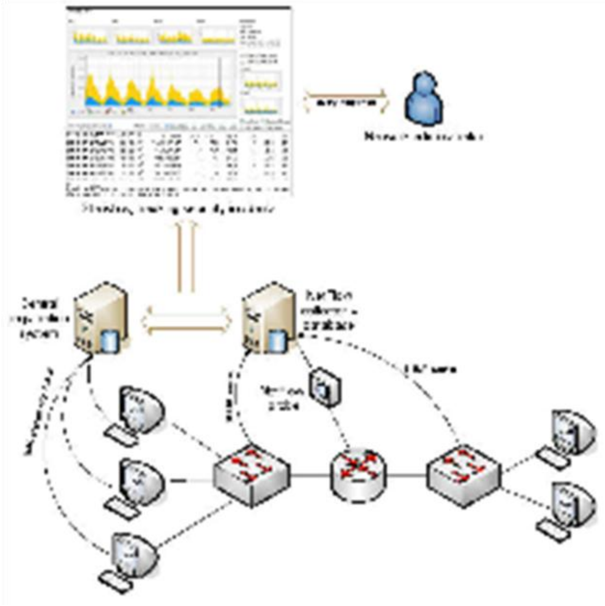


Figure: Integrated monitoring system for IPv4 and IPv6

RADIUS and DHCP are not sufficient for IPv6. Additionally, other forms of communication than one-to-one would become pervasive in IPv6 networks. Multicast allows establishment of groups of network nodes identified by special IPv6 addresses. SOHO networks often share one global IPv4 address and thus separation of a specific SOHO network user is technically impossible. In contrast, due to large number of available IPv6 addresses, any two computers do not share same IPv6 address. In cooperation with LEA recognition of specific users using distinct IPv6 addresses could be established; thus, privacy of users connected to SOHO networks could be increased.

Selected publications:

- Grégr, M., Matoušek, P., Podermański, T., Švéda, M.: Practical IPv6 Monitoring - Challenges and Techniques, In: Proceedings of the 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011), Dublin, IE, IEEE CS, 2011, p. 660-663, ISBN 978-1-4244-9220-6
- Polčák, L., Grégr, M., Kajan, M., Matoušek, P., Veselý, V.: Designing Lawful Interception in IPv6 Networks, In: Security and Protection of Information, Brno, CZ, UNOB, 2011, p. 114-126, ISBN 978-80-7231-777-6
- Elich, M., Grégr, M., Čeleda, P.: Monitoring of Tunneled IPv6 Traffic Using Packet Decapsulation and IPFIX, In: Traffic Monitoring and Analysis, Vienna, AT, Springer, 2011, p. 64-71, ISBN 978-3-642-20304-6

Graph@FIT Research Group

Besides teaching, the Graph@FIT group involved in the project is mainly focused on image/video analysis algorithms, signal processing algorithms, applications exploiting embedded systems, and advanced user interfaces. Graph@FIT has long-term activities that include research in the field of hardware accelerated functionality for embedded systems, specifically in the form of embedded video/signal processing modules.

Project activities of Graph@FIT include several EU funded projects in the field of signal and video processing (such as AMI or AMIDA projects) FP7-ARTEMIS projects (such as RECOMP, R3-COP, SMECY, or eSONIA), security oriented projects (such as CareTaker), and several locally funded projects (such as the Czech ministry of education funded projects Safety, Security, and Reliability, or Centre of basic research in computer graphics, or recently project D-NOTAM targeted on advanced user interfaces for Aeronautics funded by the Technology Agency of the Czech Republic).

Graph@FIT is a research group within the department of computer graphics and multimedia and it closely cooperates with the other groups within the department. The Department of Computer Graphics and Multimedia is responsible for teaching courses in the MSc specialization called Computer Graphics and Multimedia that covers computer graphics and multimedia, speech processing, human-machine interfaces, image and sound processing and compression, application interfaces for computer graphics and multimedia, and basics of applied computer graphics disciplines, such as computer-aided design, geographic information systems, etc. The Department of Computer Graphics and Multimedia is also responsible for teaching Signals and Systems, Computer Graphics Basics and Human-Machine Interface Design courses in Information Technology Bc programme.

Research activities of the department are mainly focused on general computer graphics algorithms, rendering, processing and recognition of speech signals, animation in three-dimensional space, modern methods of interaction in three-dimensional space, image processing, and applications. The main research topics from the above activities are:

- Computer graphics algorithms accelerated using DSP and FPGA,
- perceptually-based robust feature extraction for speech and speaker recognition
- very low bit rate coding
- realistic rendering of complex scenes and volume rendering,
- automatic determination of speech units
- large scale speech database collection
- animation of articulated structures, kinematics and dynamics,
- medical data processing and visualization and human body modeling reconstruction from VH data sets,
- parallel rendering implementation of signal processing and graphics algorithms.

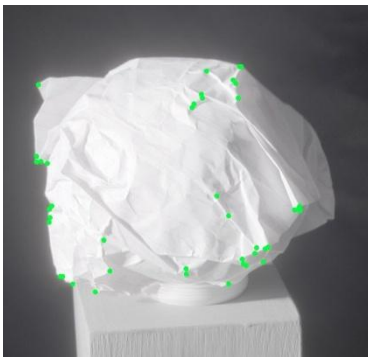
The majority of courses consist of lectures supplemented with projects and laboratory lessons. The knowledge that students gain during the lectures is further developed in the laboratory lessons by the practical experience and then practiced in the individually assigned projects and/or team projects. Most of the laboratory lesson assignments and projects are platform-independent.

The Department of Computer Graphics and Multimedia also organizes workshops of students' projects focusing on computer vision, sound and image processing, computer graphics and human-computer interfaces. The goal of the workshop is to present the results of both student and team projects, to meet and discuss the issue and making contacts for cooperation.

The team is led by Adam Herout (doc. Ing. Ph.D.). Adam Herout was born in 1978 in Bruntal, Czech Republic. He received electrical, electronics, and computer engineering education at the Faculty of Electrical Engineering, BUT Brno (Ing. 2001). He continued the studies and received Ph.D. degree from BUT Brno with the Ph.D. thesis titled Hardware acceleration of computer graphics (2004). He worked for a SME company Camea s.r.o. for six years in research and development of computer vision systems. He leads the Graph@FIT research group at the Faculty of Information Technology, Brno University of Technology. The research group and the Department of Computer Graphics and Multimedia was founded by Pavel Zemčík, who is still an anctive senior member of the team and he takes care of research project. Pavel Zemčík (Doc. Dr. Ing.) is an associate professor and the Vice-Dean at FIT BUT. His research interests include hardware-accelerated image and video processing, GPU-powered computing, machine learning and human-computer interaction. He has been involved in many European projects, including the above-mentioned projects AMIDA, CARETAKER, and TA2, as well as many national projects.

Recent Research Work Topics

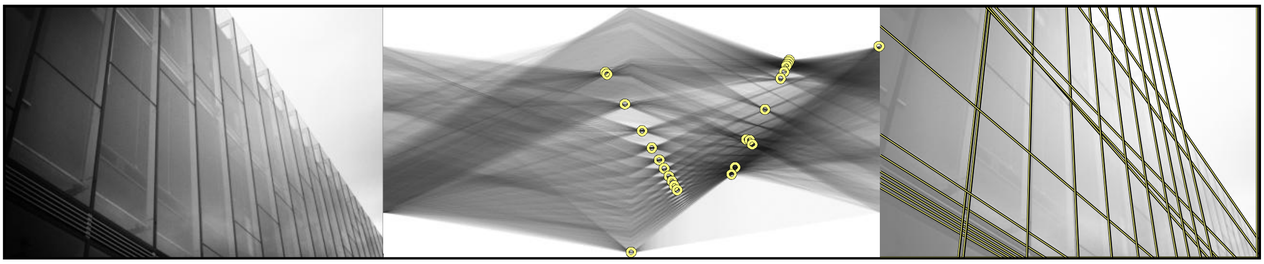
Feature Point (FP) detection is a fundamental part of many computer vision applications. The most important attribute of detected features is the repeatability - a measure how FP detection is independent of imaging conditions.



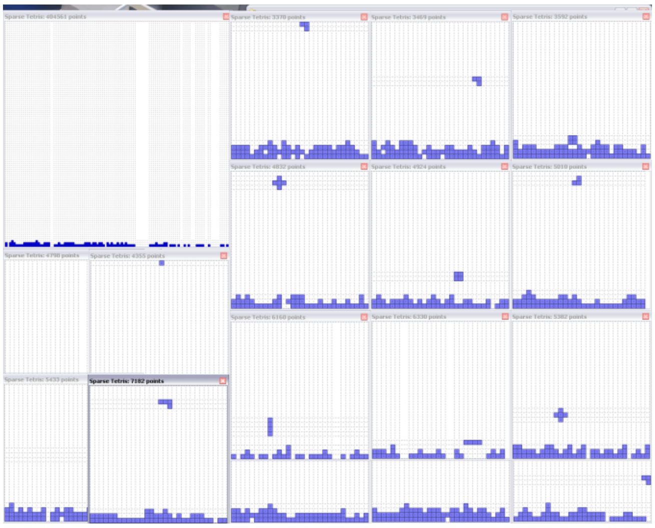
However, varying lighting conditions can affect FP detection significantly. High Dynamic Range (HDR) imaging techniques provide mechanisms to capture all the dynamic range of lighting within a scene, thus improving the repeatability of features significantly.

The Hough transform is a technique important for the computer vision. It is a commonly used algorithm for the detection of lines and curves in raster images. Recently, the Hough transform is also used for the detection of arbitrary objects in place of scanning window classifiers.

The line detection is a basic step in many tasks of computer vision such as detection of checkerboard-like patterns for the camera calibration or for the augmented reality.

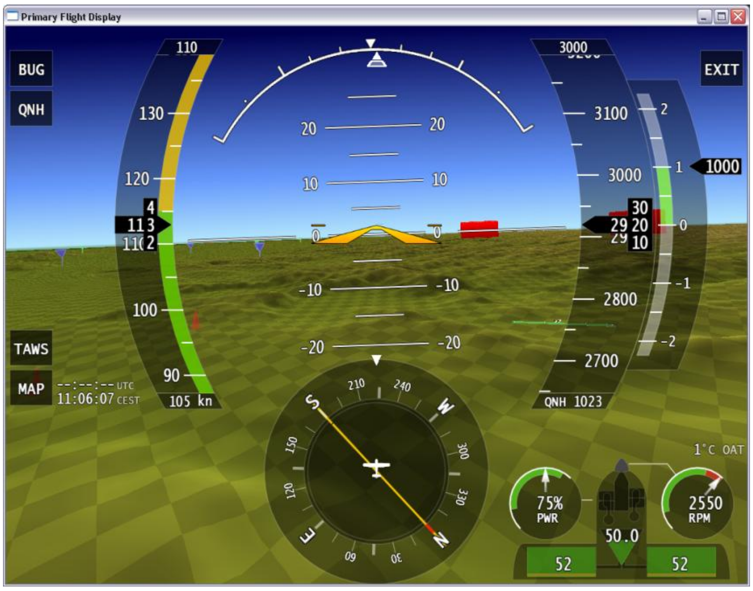


UberBlockMatrix is lighting-fast sparse block matrix implementation. Currently, we are using it for solving nonlinear incremental optimization problem in SLAM, where it performs better than other state-of-the-art libraries, with at least 70% margin. To test it, we needed some good test cases. Apart from University of Florida Sparse Matrix Collection and some hard-coded test cases, there was really no good data.

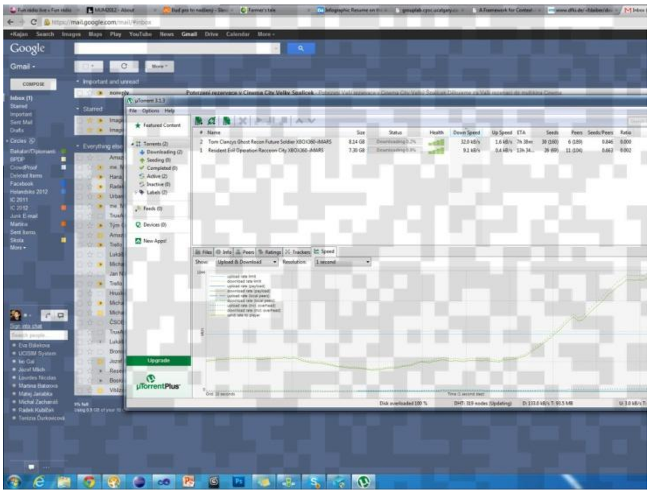

Sparse Tetris: 404561 points
Sparse Tetris: 3370 points
Sparse Tetris: 3469 points
Sparse Tetris: 3592 points
Sparse Tetris: 4832 points
Sparse Tetris: 4924 points
Sparse Tetris: 5010 points
Sparse Tetris: 4798 points
Sparse Tetris: 4355 points
Sparse Tetris: 6160 points
Sparse Tetris: 6330 points
Sparse Tetris: 5382 points
Sparse Tetris: 5433 points
Sparse Tetris: 7182 points

The nature of the problem suggests the use of cellular automata to generate pseudorandom patterns that would be used as blocks of a matrix, which would be in turn fed to our implementation as a test case. However, cellular automata often tend to produce oscillations or stabilize, not producing enough original "random" data. So after a little thinking about blocks we decided to use off-the-shelf implementation of tetris AI, and let it generate the test data for us. Since the AI is deterministic, it is easy to replicate test cases, on the other hand, the sequences are ultimately given by game field dimensions and the sequence of tiles that fall down, which can be easily parameterized by random number generator seed.

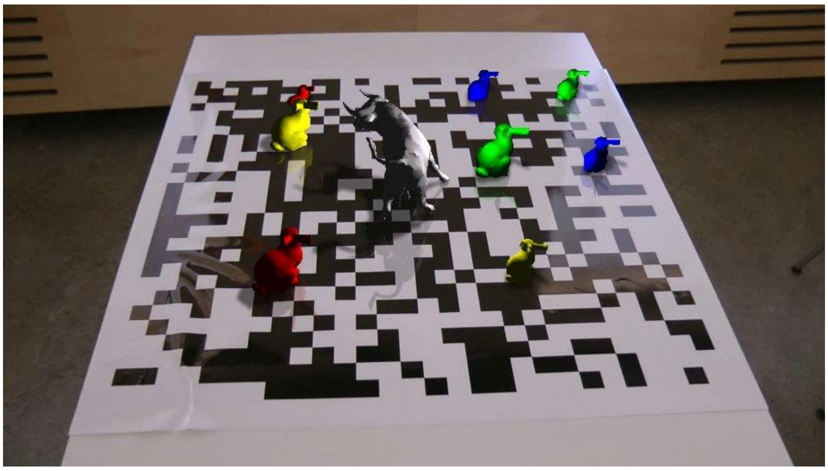
Primary Flight Display utilizes NVIDIA Tegra 2 embedded graphics processing unit. While not as powerful as the desktop-based GPUs, Tegra still has some considerable computing power. The architecture is, however, slightly different and behaves differently. In order to make smooth terrain visualization possible, some new memory allocation schemes were designed, improving memory transfers between the ARM4i CPU and the Tegra GPU.



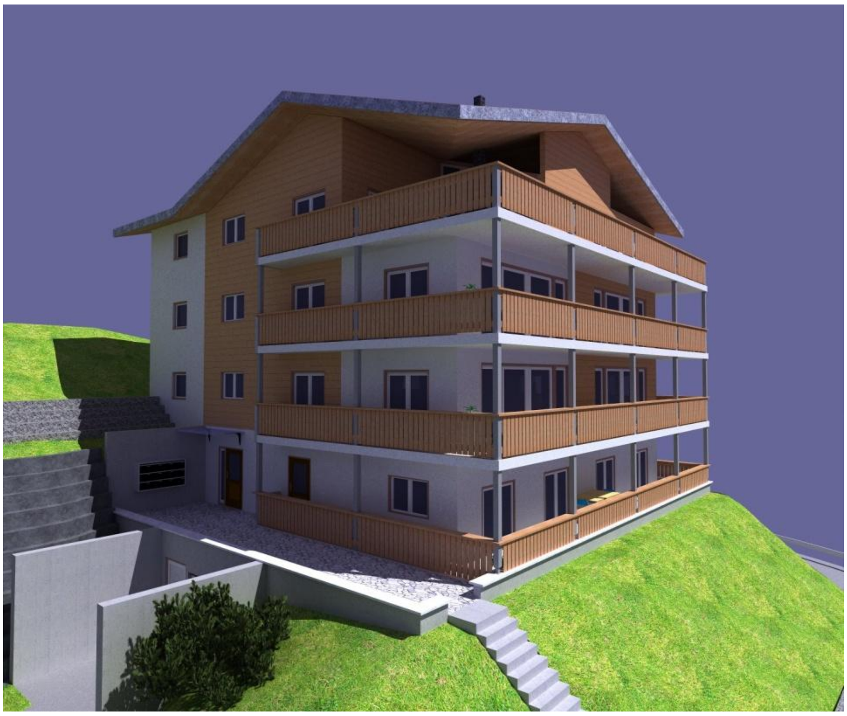
Although user tasks often span multiple heterogeneous devices, currently there is a lack of support for users to easily and intuitively migrate their tasks. To address this problem, we are developing a framework for reliable and unobtrusive **task migration** across devices based on uniform marker fields. It will allow for capturing the user's work state that is needed for a task and resuming it on a different device.



Fiduciary markers are used in different augmented reality systems to reliably establish the camera position within the scene. In some applications, a wider area needs to be covered by markers, but a large marker cannot be used because only a fraction of the area is to be viewed by the camera. To

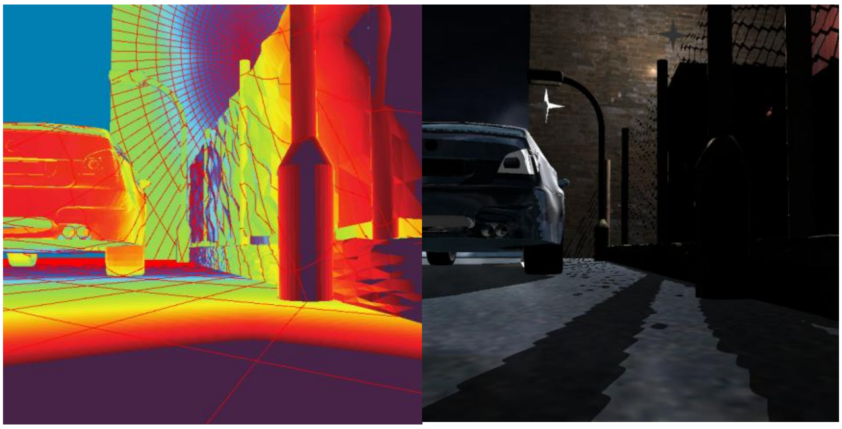


address this problem we are developing the concept of a **Marker Field**; a large-scale planar (or non-planar) marker composed of mutually overlapping partial markers. This allows for high freedom of camera movement while still being able to localize the camera in relation to the marker field.



Lexolights is a software for real-time high quality visualizations using realistic lighting specialized for CAD prototyping. High fidelity lighting is achieved using number of technologies. Modern OpenGL shader architecture provides per-pixel lighting, advanced shadow volumes algorithms provides fast and robust solution for arbitrary complex and sized models. Multipass processing is used allowing theoretically any number of light sources. Finally, raytracing and radiosity option is available using POV-Ray renderer.

The analysis of the aliasing error in the shadow mapping algorithm helps us to increase a density of sampling in a certain part of the shadow map. Our method extends the **Dual-Paraboloid mapping algorithm** that renders shadows cast from omnidirectional light source and it leads the high quality shadows in the 3D scene.



Selected Research Projects

- Robust & Safe Mobile Co-operative Autonomous Systems (R3-COP), Artemis JU, 2010-2013
- Smart Multicore Embedded SYstems (SMECY), Artemis JU, 2010-2013
- TA2 - Together Anywhere, Together Anytime (TA2), EU-7FP-ICT, 2010-2012
- Reduced Certification Costs Using Trusted Multi-core Platforms (RECMOP), Artemis JU, 2010-2013

Selected Recent Publications

- Herout, A., Hradiš, M., Zemčík, P.: EnMS: Early non-Maxima Suppression, In: Pattern Analysis and Applications, Vol. 2012, No. 2, DE, p. 121-132, ISSN 1433-7541
- Szentandrási, I., Herout, A., Dubská, M.: Fast Detection and Recognition of QR codes in High-Resolution Images, In: Proceedings of 28th Spring conference on Computer Graphics, Bratislava, SK, UNIBA, 2012, p. 8
- Hradiš, M., Kolář, M., Král, J., Láník, A., Zemčík, P., Smrž, P.: Annotating images with suggestions - user study of a tagging system, In: ACIVS 2012 Proceedings, Brno, CZ, Springer, 2012, p. 1-12
- Navrátil, J., Zemčík, P., Juránek, R., Pečiva, J.: A Skewed Paraboloid Cut for Better Shadow Rendering, In: Proceedings of Computer Graphics International 2012, Berlin, DE, Springer, 2012, p. 4, ISBN 978-1-85899-283-9
- Antikainen, J., Havel, J., Jošth, R., Herout, A., Zemčík, P., Hauta-Kasari, M.: Non-Negative Tensor Factorization Accelerated Using GPGPU, In: IEEE Transactions on Parallel and Distributed Systems (TPDS), Vol. 2011, No. 1111, US, p. 7, ISSN 1045-9219
  Dubská, M., Herout, A., Havel, J.: PClines - Line Detection Using Parallel Coordinates, In: Proceedings of CVPR 2011, Colorado Springs, US, IEEE CS, 2011, p. 1489-1494, ISBN 978-1-4577-0393-5
- Herout, A., Jošth, R., Juránek, R., Havel, J., Hradiš, M., Zemčík, P.: Real-time object detection on CUDA, In: Journal of Real-Time Image Processing , Vol. 2011, No. 3, DE, p. 159-170, ISSN 1861-8200
- Seeman, M., Zemčík, P., Juránek, R., Herout, A.: Fast bilateral filter for HDR imaging, In: Journal of Visual Communication and Image Representation, Vol. 2012, No. 1, 2011, Amsterdam, NL, p. 6, ISSN 1047-3203
- Vanek, J., Beneš, B., Herout, A., Šťava, O.: Large-Scale Physics-Based Terrain Editing Using Adaptive Tiles on the GPU, In: IEEE Computer Graphics and Applications, Vol. 2011, No. 1, US, p. 10, ISSN 0272-1716
- Zemčík, P., Přibyl, B., Herout, A., Seeman, M.: Accelerated Image Resampling for Geometry Correction, In: Journal of Real-Time Image Processing , Vol. 6, No. 3, 2011, DE, p. 9, Hanák, I., Herout, A., Zemčík, P.: Acceleration of the Detail Driven Method

for Hologram Generation, In: Optical Engineering, Vol. 49, No. 8, 2010, US, p. 9, ISSN 0091-3286

- Havel, J., Herout, A.: Yet Faster Ray-Triangle Intersection (Using SSE4), In: IEEE Transactions on Visualization and Computer Graphics, Vol. 2010, No. 3, US, p. 434-438, ISSN 1077-2626
- Herout, A., Zemčík, P., Hradiš, M., Juránek, R., Havel, J., Jošth, R., Žádník, M.: Low-Level Image Features for Real-Time Object Detection, Pattern Recognition, Recent Advances, Vienna, AT, IN-TECH, 2010, p. 111-136, ISBN 978-953-7619-90-9
- Zemčík, P., Hradiš, M., Herout, A.: Exploiting neighbors for faster scanning window detection in images, In: ACIVS 2010, Sydney, AU, Springer, 2010, p. 12, ISBN 978-3-642-17690-6
- Hanák, I., Zemčík, P., Žádník, M., Herout, A.: Hologram synthesis accelerated in field programmable gate array by partial quadratic interpolation, In: Optical Engineering, Vol. 8, No. 48, 2009, US, p. 1-7, ISSN 0091-3286

Research group STRaDe

Main contact person(s)

- Martin Drahanský, phone: +420 54114 1276, e-mail: drahan@fit.vutbr.cz
- Filip Orság, phone: +420 54114 1195, e-mail: orsag@fit.vutbr.cz

Research topics of the research group (research interests)

- biometric security systems
- security
- robotics
- intelligent systems
- wireless networks
- embedded applications
- military applications

Brief characteristics of the research group

Research group STRaDe (Security Technology Research and Development) is part of the Department of Intelligent Systems at the Faculty of Information Technology at the Brno University of Technology. The main goal of STRaDe is research and development of security technologies and that is both - hardware and software. The security technologies include vast amount of applications and devices. One large scope, at which we aim, is biometry. Nowadays, we cover practically all of available up-to-date technologies and metrics, e.g. fingerprint scanning and recognition, liveness detection, face detection, veins detection etc.

Sensor systems and their applications (e.g. in robotics, which is itself part of the group interests) are second important part of our research. In the relation to the robotics and biometry we aim at research of complex intelligent systems. Another scope of our research is digital video processing and hardware implementation of the video processing algorithms. Such implementations are parts of computer vision systems and applications including military systems.

The research group consists of 2 senior researchers and 8 junior researchers. We have got 2 PhD graduates over the past 5 years.

Key research equipment

Among the key equipment belong various fingerprint readers (sensors) using various technologies and many other biometrical devices e.g. for iris recognition, 3D face, hand geometry, veins, or handwriting. There are many other devices in our laboratory covering all research topics we aim at such as:

- thermo camera
- non- mydriatic fundus camera
- Osciloscop Tektronix DPO7254
- Various development kits made by Texas Instruments, Microchip and ST Microelectronics
- Signal Analyzer Rohde & Schwarz FSQ8
- SDKs for the software and hardware development

Unique know-how of the research group

- International patent no. WO/2010/009683: "A method of biometric identification of persons according to the hand and device for biometric identification of persons according to the hand."
- International patent no. WO/2007/036370: "Method and Apparatus for Detecting Biometric Features"
- Utility model no. 19364: "Liveness Detection on Fingers by Causation of Optical Changes"
- Industrial model: „Design of Mini-Sumo Robot"
- Specimen: "Sensor Data Acquisition Unit for UAV (SEDAQ)"
- Prototype: "ISTA – image stabilization"
- Software: "Algorithmic and mathematical principles of automatic number plate recognition systems"
- Legislation for the Czech National Security Authority: "Fingerprint Quality Testing"

Main collaborating industrial partners/application partners

- Digitus s.r.o., Čechova 656, CZ - 750 02 Přerov, CZ
- Fraunhofer-Gesellschaft, Hansastraße 27c, Munich, DE
- Microchip Technology Inc. 2355 West Chandler Blvd., Chandler, Arizona, USA
- RUTRONIK Elektronische Bauelemente CZ s.r.o. Slavičkova 1a, 63800 Brno, CZ

- STMicroelectronics, CH 1228 Plan-Les-Ouates, GENEVA, CH
- EVPÚ Defence s.r.o., Uherské Hradiště, Mařatice, Sadová 1385, CZ
- OPROX, a.s., Vnitřní 10, 602 00, Brno, CZ
- E-COM s.r.o., Čelakovského 689, 684 01 Slavkov u Brna, CZ
- Texas Instruments CZ, s.r.o., Praha 4, Nusle, Hvězdova 1716/2b, CZ

Main collaborating academic partners in the Czech Republic and abroad

- Gjøvik University College, Gjøvik. Norway
- Hannam University, Daejeon Korea
- Czech technical universities