Saint-Petersburg State University of Aerospace Instrumentation

Department of Information Systems and Security

Dean of the faculty: Dr. Prof. E. Krouk

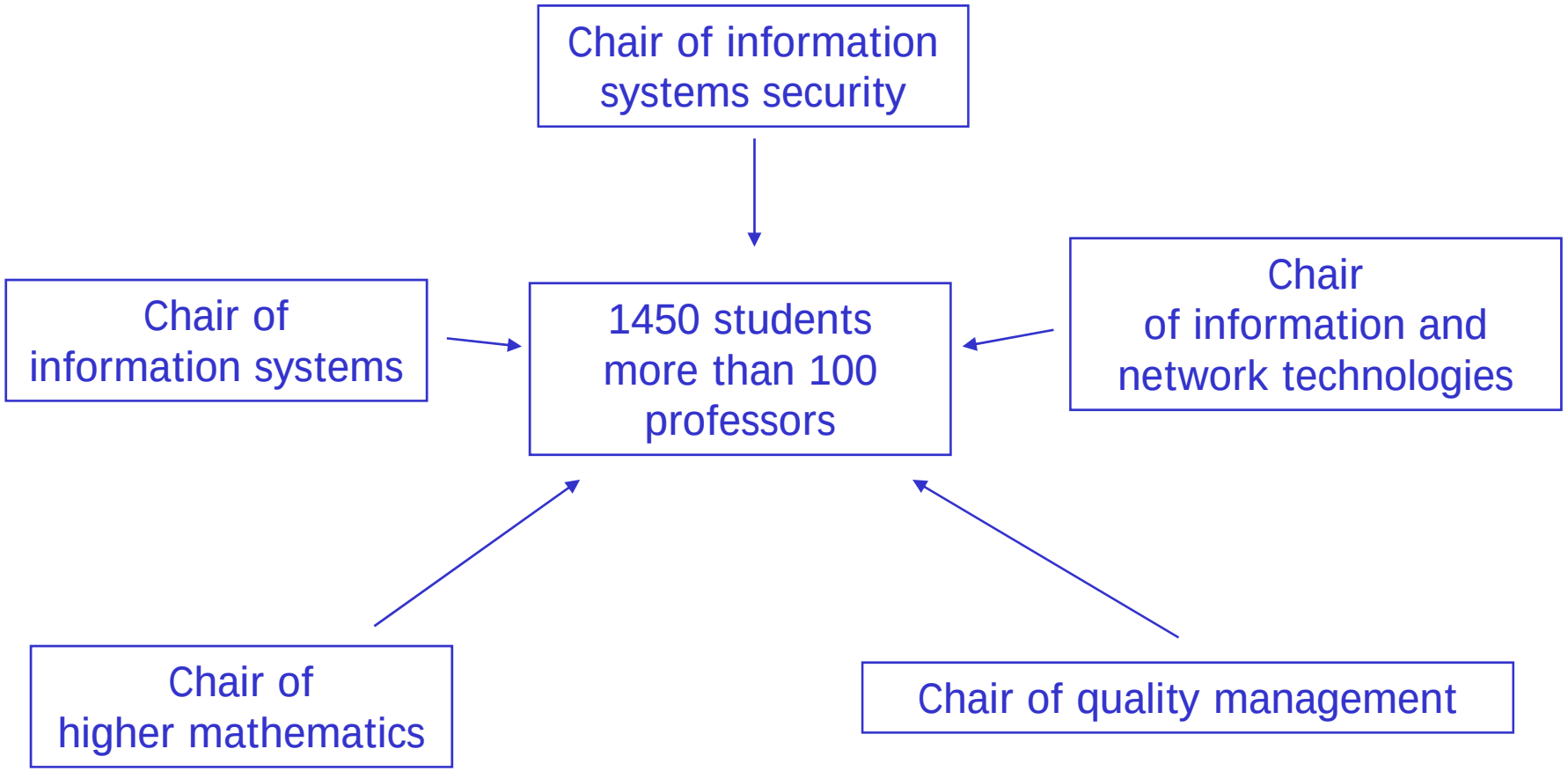
Presenter: Ann Ukhanova

Main branches in Russia

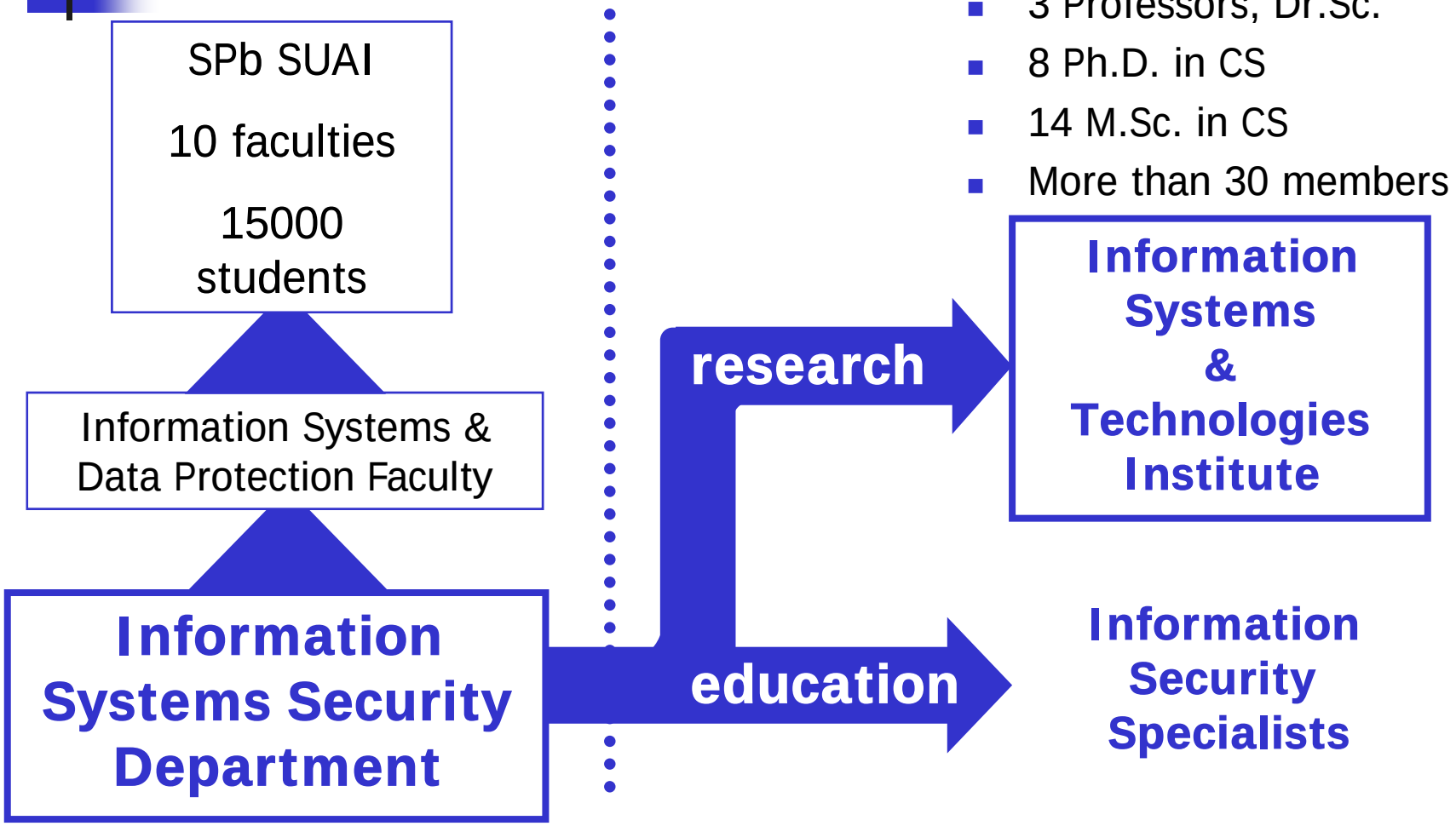
Saint-Petersburg State University of Aerospace Instrumentation: Today

- Ten faculties
  - Faculty of aerospace instruments and systems
  - Faculty of radio engineering, electronics and communication
  - Faculty of control systems
  - Faculty of computer systems and programming
  - **Faculty of information systems and data protection**
  - Faculty of management and social technologies
  - Faculty of military education
  - Faculty of economics
  - Faculty of law
  - Faculty of evening classes and distance education
  - Faculty of additional professional training
- 42 chairs, 13 institutes and centers, Over fifty directions of training
- 15 000 students from Commonwealth of Independent States, China, India, Sri Lanka, Tunisia, Morocco, Malaysia, Thailand, South America
- 600 tutors, 500 with scientific degree
- North-West Center of New Information technologies
- UNESCO Chair of Engineering Distance Education

Information Systems & Data Protection Faculty



Information Systems Security (ISS) Department



- 3 Professors, Dr.Sc.
- 8 Ph.D. in CS
- 14 M.Sc. in CS
- More than 30 members

ISS Dept International Academic Activities

- France
  - INRIA
  - Bordeaux Technical U.
  - Cachan-Besanson Research Centre
- Germany
  - Ulm U.
  - Stuttgart U.
  - Karlsruhe U.
- Bulgaria
  - Mathematical Institute
- Finland
  - FRUCT
  - Turku U.
  - TUCS
- Sweden
  - Lund U.
- The Netherlands
  - Technical U. of Eindhoven
- China
  - Beijing Aerospace U.
- US
  - Riverside U.
  - Indiana State U.
  - Maryland U.
- Italy
  - Catania U.

ISS Dept International Industrial Activities

- US
  - Intel
  - Seagate
  - Cadence
- France
  - Renault
- Finland
  - Nokia
- South Korea
  - Samsung
  - Keri Institute
  - Daewoo
- Germany
  - Nokia-Siemens Networks
- China
  - Institute 21

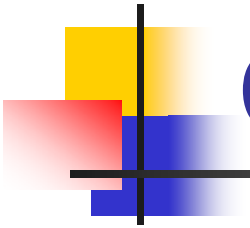
ISS Dept Overview

Research Groups

- Code applications
- Data communication
- Network security
- Video transmission
- Systems engineering

Research Directions

- Linear code decoding
- Multimedia compression
- Wireless video transmission
- Access control methods
- Network security
- Steganography
- Systems verification



Outline

- Telecommunications
- Video coding & transmission
- Software performance engineering
- Network Security
- Mobile services

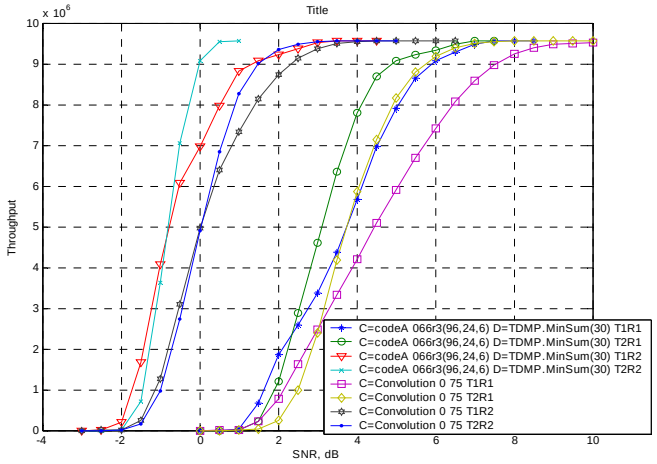
Telecommunications

Telecom Core competencies

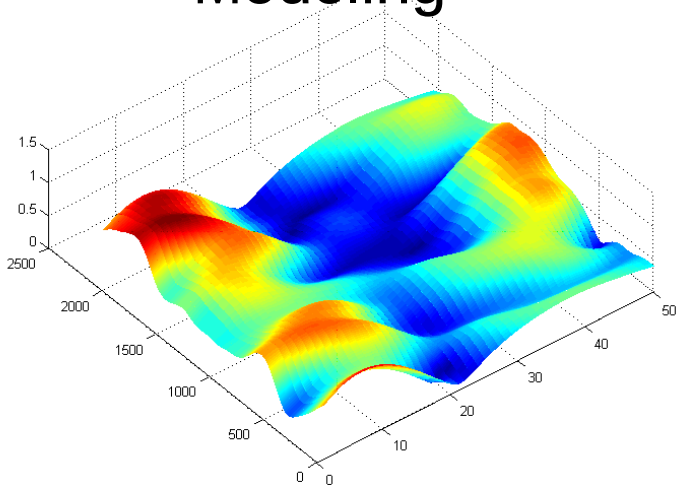
- Core competencies = solutions for
  - wired transmission at 10Gbps
    - IEEE 802.3an
  - wireless transmission
    - IEEE 802.11a/g/n (WiFi)
    - IEEE 802.15
    - IEEE 802.16e (WiMax)
    - 3GPP LTE
- Simulation tools for PHY layer of wired and wireless communication systems
- Hardware implementation
  - DSP+FPGA prototyping

Telecom Core competencies

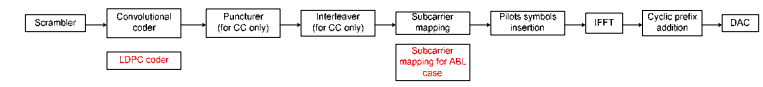
Research

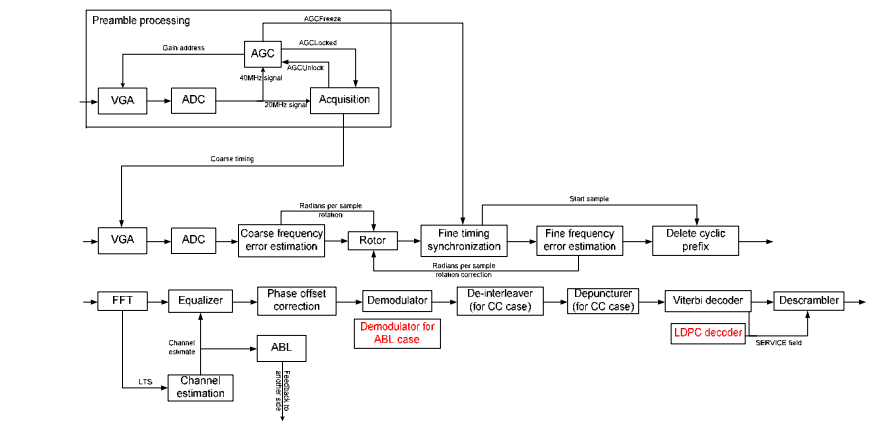


Modeling

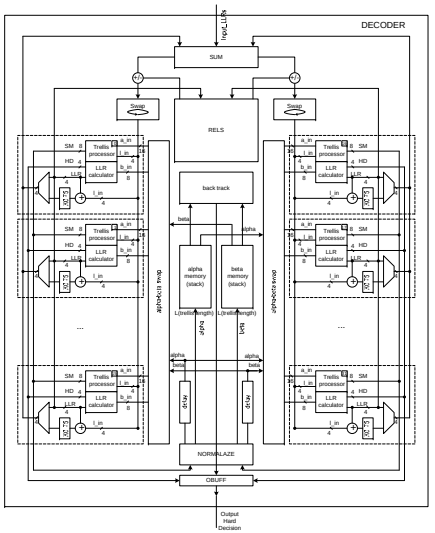


Standardization





Hardware design



Telecom algorithms research

- Error-correction codes applications
  - LDPC, Turbo-codes, Reed-Solomon, concatenated Trellis-RS
- MIMO systems research
- PHY layers algorithms design, completed communication systems modeling (time/frequency synchronization, channel estimation, equalization and etc)
- DSP algorithms design

Implementations & Prototyping skills

- Hardware design
  - RTL design (Verilog) of FEC decoders (Convolutional, Turbo, LDPC)
  - FPGA prototyping
- Software design
  - Software tools for PHY/MAC layer simulations
  - Optimization for DSP Processors

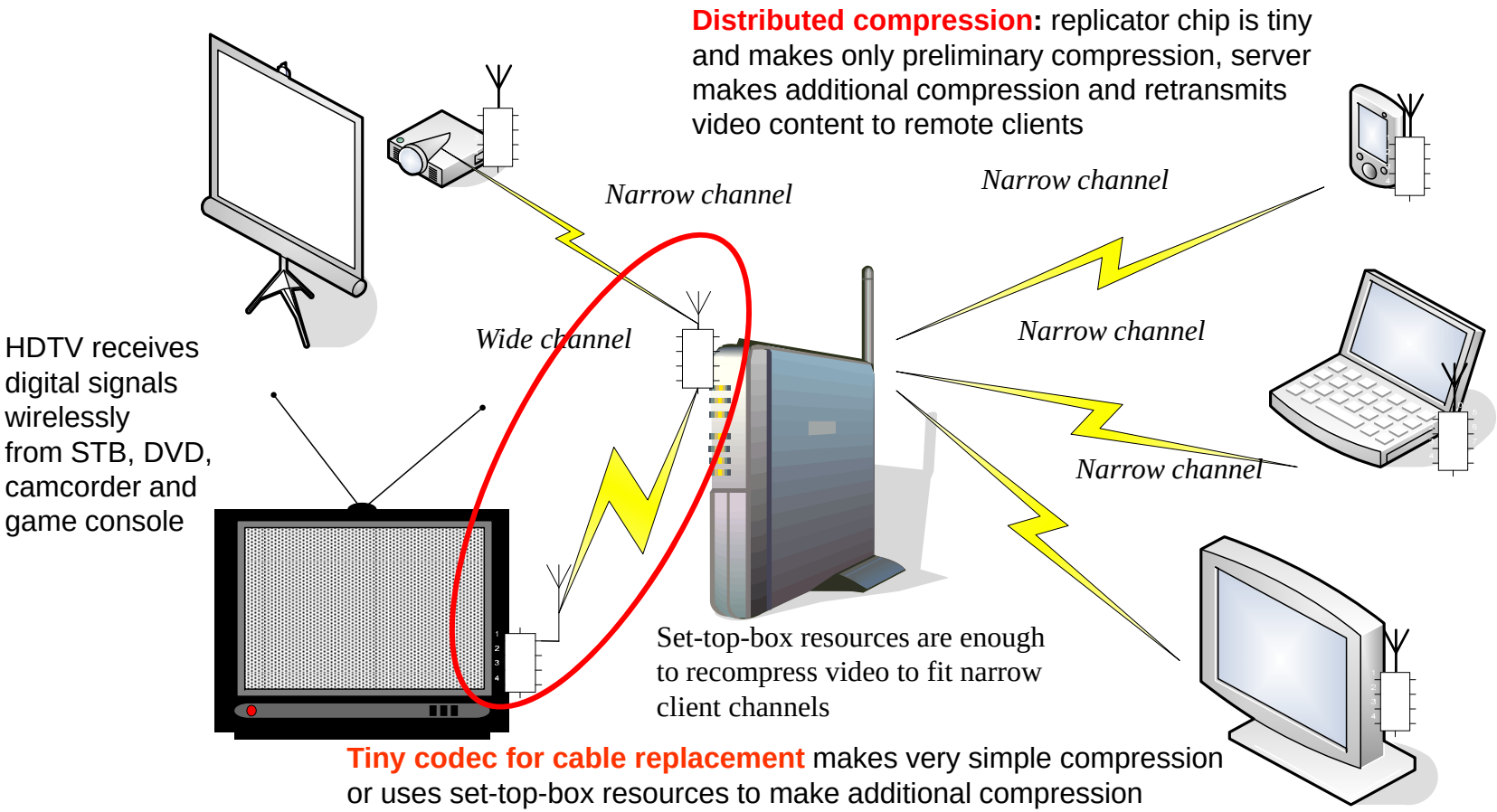
Video Coding & Transmission

Video coding & processing

- Video over Wireless transmission
  - Solutions for Cable Replacement Program
    - HDTV1080i transmission over wireless channel
      - UWB, 802.11n, 802.3.15c
    - Joint (compression & transmission) simulation models
    - Adaptation & rate control for time-varying channels
- Video coding for specific applications
  - Lossy: JPEG2000, H.264/AVC, JPEG I/P etc.
  - Lossless: JPEG-LS, CALIC etc.
- Identification
  - Image recognition (text/video/borders/icons detection)
  - Model Identification
- Hardware implementation
  - FPGA prototyping

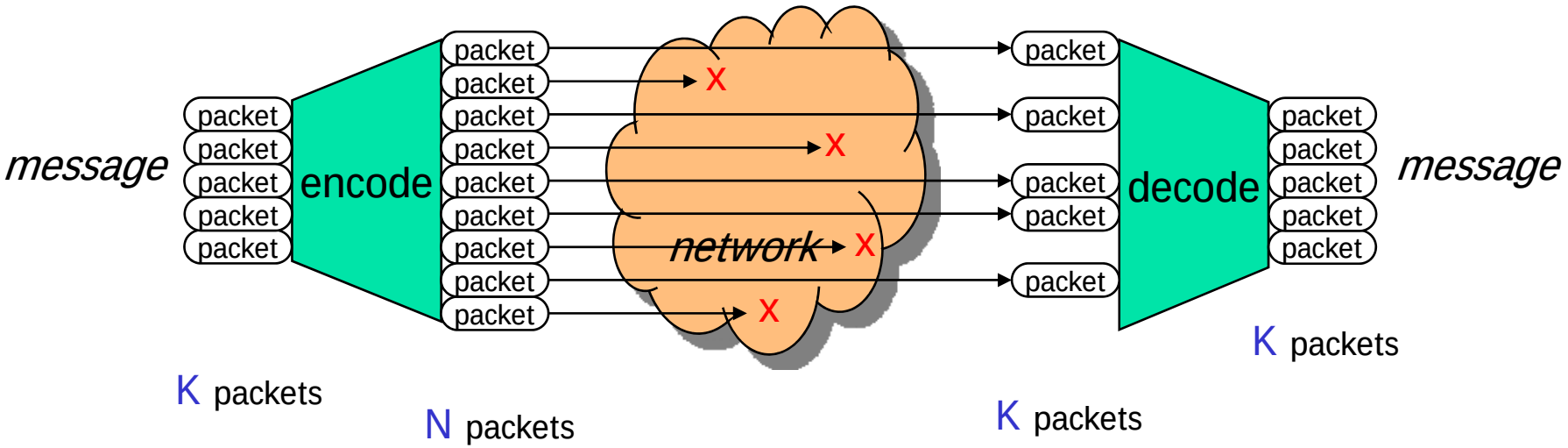
Video over WPAN: Cable Replacement

- Video compression for wireless replication
  - Tiny codec for cable replacement: 1-5m, p2p
  - Scalable & distributed compression: 3-20m, p2mp, range-based QoS



Coding above PHY

- Redundancy decrease message delay



T(without coding) > T(with coding) !!!

- Latency critical applications:
  - Real-time video transmission, voice over IP, conferencing etc.

RnD Directions & Technologies

Transmission Research

- ”Black box” estimation
- Transport Coding
- RnD: .11,.16, UWB, 15.3

Lossy Compression Research

- Colorspace transforms
- H.264/AVC, MPEG X
- JPEG 2000
- Rate/Delay Control

Lossless Compression Research

- JPEG-LS
- CALIC
- Arithmetic Coding
- Low complexity entropy coding

Papers & Conferences 2008

ASMTA 2008

Springer

Lecture Notes in Computer Science

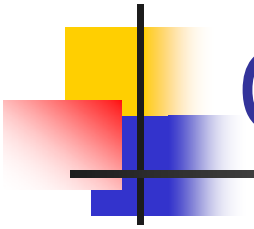
15th International Conference on
ANALYTICAL and STOCHASTIC MODELLING TECHNIQUES and APPLICATIONS
Nicosia, Cyprus 4-6 June 2008
http://www.comp.glam.ac.uk/ASMTA2008/
Co-Sponsored by IEEE UKRI Computer
The conference is organized in conjunction with the
22nd European Conference on Modelling & Simulation
http://www.scs-europe.net/conf/ecms2008/

ECMS

IEEE

COST 290

Software performance engineering



Core Competencies

- Development and analysis of distributed protocols (ad-hoc, sensor, p2p, smart spaces)
- Performance analysis of distributed software
  - Prediction of performance on early stages of design
  - Finding bottle-necks in existing software
- Endurance and stress testing
- Dependability analysis of distributed software
  - Verification
  - Estimation of reliability and availability

Implementation: simulation tool

- Lab is developing the tool, which
  - Takes UML model of software as input
  - Translates it into the simulation model and execute this model
  - Calculates the following measures
    - Performance = number of request successfully processed by the system per time unit
    - Availability = probability to loose request on the entrance of the system
    - Reliability = probability to loose request inside the system

Network Security

Information Security in Wireless Networks

- Confidentiality
- Key Management and Access Control
- Secret Sharing
- Digital Signature
- Authentication
- Secure routing and intrusion detection
- Secure (hidden) calculations
- Speeding up the ECC systems
- Secure aggregation in Sensor Networks
- Watermarking for video and audio content
- Standardization Activity

Main topics

Key Management and Access Control

- **Multi-level Access Control Encryption Scheme**
  - Users belong to Security Classes (SC)
  - Information is encrypted by its owner
  - Only users from higher SC and owner can decrypt information of users from lower classes
  - New property: anonymity of users
- **Light-weight Key Management for Large Sensor Networks**
  - Small number of keys per node, computationally light-weight algorithm
  - New property: high resilience to nodes capture (as before as after deployment) and possibility of adding mobile nodes

Confidentiality

- **Code-based Public Key Encryption Scheme**
  - Generalization of McEliece cryptosystem
  - Shortening public/private keys
  - New property: Faster than RSA cryptosystem

Main topics

Digital Signature

- Multiple-time Signature Scheme
  - Signature which can be used only limited amount of times
  - Low complexity of signing and verification procedures
  - New property: Multi-time signature based on CFF based on Griesemer codes
- Distributed RSA Signature
  - Application: certificate authority in infrastructure less networks
  - New property: Faster algorithm for distributed RSA signature

Authentication

- Authentication by localization
  - Signal structure for node authentication
  - New property: Node authentication by localization in the wireless network

Main topics

- Acceleration of arithmetic on elliptic curves
  - New multiplication algorithm for ECC in field of characteristic 3
  - New property: modification of Kobliz algorithm for characteristic 3
- Secure aggregation in Sensor Networks
  - For reducing of network power some nodes (aggregators)
    - gather information from other nodes
    - send aggregated information to the base station
- Watermarking for video and audio content
  - New property: Usage of error correcting codes with unequal error correcting capability for DWM.

Standardization Activity

- Area
  - IEEE 802.11i defines general security features for 802.11 family of the standards
  - But some members of the family require enhancements of .11i
  - 802.11s Mesh Networks
  - 802.11w Security for Management frames
- Results
  - Proposals to appropriate TG

Mobile Services

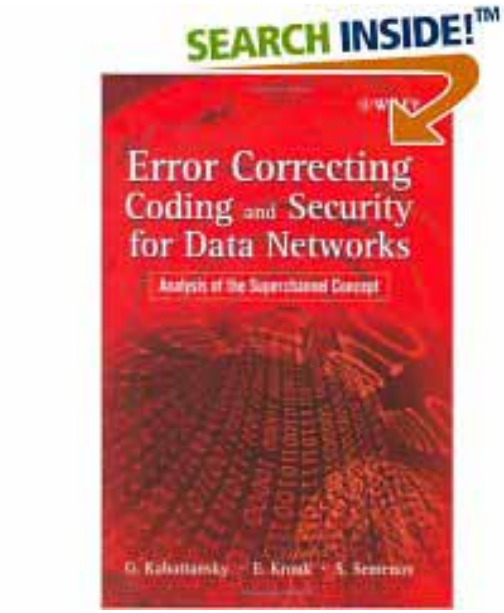
SUAI-NOKIA Joint Laboratory

- Mission: creation of mobile application and services and promoting mobile web services
- Focus areas
  - Mobile software development
  - Widgets development
  - Using mobile devices for Smart Space
- Focus technologies
  - WidSets
  - Web RunTime widgets

Main Results

Research Groups	Patents	IEEE Publications
Data Communications	12	8
Linear Code Decoding	11	11
Multimedia Compression	2	4
Network Security	7	5

Latest publications



- Grigorii Kabatiansky, Evgenii Krouk, Sergei Semenov **Error Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept**
- Joint coding on all network layers

Thank you!

http://www.k36.org
http://www.k36.org/wlsec/
http://www.k36.org/21may/
http://www.k36.org/ais/

http://www.guap.ru
http://www.suai.ru