

INFORMATICS

Problems of cryptographic primitives implementations in network protocols

supervisor: doc. RNDr. Jozef Jirásek, PhD.

study form: full time

Annotation: Nowadays, secure internet protocols are using several cryptographic primitives at the same time in different combinations and in different modes. Even though the individual primitives are subject to many security analyzes, their current use can lead to further unexpected vulnerabilities. The work will analyze the possibilities of parallel attacks on the primitives, used cryptographic functions and the methods of their use with the intention of proving the feasibility of specific safety objectives, or propose protection against identified vulnerabilities.

System resources protection of mobile devices against network attacks

supervisor: doc. RNDr. Jozef Jirásek, PhD.

study form: full time

Annotation: Work will address the current vulnerabilities of protecting system resources of mobile devices on Android platform and mechanisms used to exploit vulnerabilities to unauthorized access, or to modify sensitive system data with subsequent modification of stored data. The aim of the thesis is to propose a mechanism for timely capture of such attacks and to create additional tools to increase system security.

Plasticity and attention in spatial hearing

supervisor: doc. Ing. Norbert Kopčo, PhD.

study form: full time

Annotation: In everyday situations, humans are exposed to multiple concurrent stimuli in complex, continuously changing environments. To correctly extract relevant information, they adapt their processing to reflect the specifics of the current scene, and they learn from previous experience to improve the perceptual strategies used. The current project proposes to perform a series of behavioral experiments, brain imaging studies, and computational modeling to study how attention and mechanisms of implicit and explicit learning are used to cope with complex listening environments for speech processing, sound localization, and learning of new phonetic categories.

Cross-modal interactions and spatial auditory processing

supervisor: doc. Ing. Norbert Kopčo, PhD.

study form: full time

Annotation: Vision influences how we perceive space by hearing. Ventriloquism effect and after-effect are phenomena illustrating short-term plasticity in spatial hearing induced by visual signals. Visual attentional cuing also influences spatial auditory processing both in terms of sound localization and spatial benefit in speech perception. The current project will examine the effect of visual information on spatial auditory perception by performing behavioral experiments, neuroimaging studies, and computational modeling.

Brain-training games for spatial hearing

supervisor: doc. Ing. Norbert Kopčo, PhD.

study form: full time

Annotation: Solutions designed to enhance auditory processing when hearing thresholds are within normal limits are very limited and none are as recognized or as widely available as are hearing aids and cochlear implants. The project aims to contribute to the development of novel procedures to rehabilitate auditory processing deficits (APD) by developing a brain training game based on modern auditory neuroscience and the results of the EU Horizon 2020 ALT grant. The development of auditory brain training game will be in collaboration with University of California, Riverside Brain Game Center and Oregon Health State University. The main goal of the games is to develop and test rehabilitative techniques that restore auditory function for those who perform poorly on tests of APD by training various aspects of auditory processing.

Natural language processing

supervisor: doc. RNDr. Stanislav Krajči, PhD.

study form: full time

Annotation: It is necessary to understand the structure of a grammatical sentence to work satisfactory with a natural language. The syntactical analysis of a sentence is a problem where computer science methods can be applied effectively. Our database of almost all Slovak word forms would be very helpful in this process. The student's task will be to use this database for proposal and implementation of an algorithm for the delinearization of a Slovak sentence to its tree structure, the nodes of which contain its words and the edges their relationships based on equity of appropriate set of their grammatical categories.

Heterogeneous concept lattices

supervisor: doc. RNDr. Stanislav Krajči, PhD.

study form: full time/external

Annotation: Formal concept analysis is a data-mining method applied to a rectangular matrix of data in which each row corresponds to some object, each column corresponds to some possible attribute, and the matrix field value denotes a membership of the column attribute for row object. One of the goals of this method is to find so-called concepts, which are stable (in some sense) pairs of subsets of objects and attributes. The method can be considered a nice application of the algebraic notion of a Galois connection. It has been described in detail by Ganter and Wille, in particular for the so-called crisp case with binary matrix data. A natural question that arises is what happens if the matrix data are non-binary...

Community detection in social networks

supervisor: doc. RNDr. Gabriel Semanišin, PhD.

study form: full time

Annotation: Social networks provide new phenomenon in a communication and information exchange. They combine features of standard communication networks with effects know from some areas of biology and medicine. Social networks can be modelled by graph-theoretical concepts. These models allow studying conditions that determine the intensity of information spreading.

Real-time processing of cybersecurity data

supervisor: doc. RNDr. Gabriel Semanišin, PhD.

consultant: RNDr. JUDr. Pavol Sokol, PhD.

study form: full time

Annotation: A proper reaction on cybersecurity threats and attacks plays an important role for solution of security incidents. Time that is necessary for processing and analysis of cybersecurity data belongs among the most important parameter affecting proper reaction. That is why the present security systems require processing of big amount of data in real time. The goal of the thesis is to analyze available security solutions and compare them with respect to their effectivity and applicability in real life. The other goal is to design an environment enabling representation, integration and analysis of security data allowing elimination of cybersecurity threats in real time.

Graph theoretical and algorithmic aspects of communication networks

supervisor: doc. RNDr. Gabriel Semanišin, PhD.

study form: full time

Annotation: The development of Internet of Things requires solutions for various aspects of a communication in computer and sensor networks. These networks can be modelled by graph-theoretical concepts. Such models provide bases for a formulation and solution of algorithmic problems that are related to network creation, data transfer and securing. These topics are studied very extensively and relatively big number of recent papers with significant theoretical and practical impact was published recently.

Modeling and algorithms for construction of smooth curves

supervisor: doc. RNDr. Csaba Török, CSc.

study form: full time

Annotation: Recently we proposed a new approach to solving the tridiagonal systems on a uniform grid of nodes. One of the goals of the thesis is to investigate the effect of the given approach on the nonuniform grid and the inversion of tridiagonal matrices. Classic cubic splines of class C^2 are implicit. We succeeded to express them in an explicit form that enables a design of a linear model for approximation and estimate of spline coefficients. The second goal is to analyze the properties of LS estimate of coefficients and their comparison with B-splines. The third goal is finding of criterion of optimal stopping in on-line approximation according to prediction in an appropriate metric.