

ФАКУЛТЕТ ТЕХНИЧКИХ НАУКА

ИЗВЕШТАЈ О ОЦЕНИ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ

-обавезна садржина- свака рубрика мора бити попуњена

(сви подаци уписују се у одговарајућу рубрику, а назив и место рубрике не могу се мењати или изоставити)

I ПОДАЦИ О КОМИСИЈИ
DATA ABOUT THE JURY
<p>1. Датум и орган који је именовao комисију The date and the council that has nominated the jury</p> <p>26.09.2019, Декан Факултета на основу одлуке Наставно-научног већа Факултета техничких наука Универзитета у Новом Саду</p> <p>2. Састав комисије са знаком имена и презимена сваког члана, звања, назива уже научне области за коју је изабран у звање, датума избора у звање и назив факултета, установе у којој је члан комисије запослен: Members of the jury:</p> <ol style="list-style-type: none"> 1. Др Јелена Иветић, доцент, Теоријска и примењена математика, 01.04.2014, Факултет техничких наука, Универзитет у Новом Саду 2. Др Љубо Недовић, доцент, Теоријска и примењена математика, 01.01.2018, Факултет техничких наука, Универзитет у Новом Саду 3. Др Силвиа Гилезан, редовни професор, Теоријска и примењена математика, 24.02.2005, Факултет техничких наука, Универзитет у Новом Саду 4. Др Hugo Filipe Mendes Torres Vieira, principal researcher, Теоријско рачунарство, 01.10.2019, С4, Universidade de Beira Interior, Covilhã, Португалија 5. Др Јованка Пантовић, редовни професор, Теоријска и примењена математика, 24.06.2010, Факултет техничких наука, Универзитет у Новом Саду
II ПОДАЦИ О КАНДИДАТУ
DATA ABOUT THE CANDIDATE
<p>1. Име, име једног родитеља, презиме: Name, parent name, surname: Иван, Сениша, Прокић</p> <p>2. Датум рођења, општина, држава: Birth date, place and country: 07.09.1990, Шабац, Србија</p> <p>3. Назив факултета, назив студијског програма дипломских академских студија – мастер и стечени стручни назив Master studies: Природно-математички факултет, Математика, мастер математичар</p> <p>4. Година уписа на докторске студије и назив студијског програма докторских студија Doctoral studies, year of enrollment and study programme: 2014, Математика у техници</p> <p>5. Назив факултета, назив магистарске тезе, научна област и датум одбране: --</p> <p>6. Научна област из које је стечено академско звање магистра наука: ---</p>

III НАСЛОВ ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Развој и анализа формалних модела за коришћење и дељење ресурса у дистрибуираним софтверским системима

III PHD THESIS TITLE:

Formal modeling and analysis of resource usage and sharing in distributed software systems

IV ПРЕГЛЕД ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Навести кратак садржај са знаком броја страна, поглавља, слика, шема, графикона и сл.

Докторска дисертација је написана на енглеском језику, на 156 страна и подељена је у 4 поглавља са следећим садржајем:

Резиме на српском

Резиме на енглеском језику

1. Увод
2. Формални рачун за поверљиво преношење имена
 - 2.1. Синтакса
 - 2.2. Акциона семантика
 - 2.2.1. Особине система са означеним преласцима
 - 2.3. Редукциона семантика
 - 2.4. Бихевиорална еквиваленција
 - 2.4.1. Релација строге еквиваленције
 - 2.4.2. Карактеризација особине непрослеђивања
 - 2.5. Примери
 - 2.5.1. Аутентификација
 - 2.5.2. Моделовање група и скривених имена
 - 2.5.3. Групе отвореног типа
 - 2.6. Кодирање прослеђивања
 - 2.6.1. Кодирање
 - 2.6.2. Операциона кореспонденција
 - 2.7. Закључне напомене
3. Формални рачун за плутајуће ауторизације
 - 3.1. Неформални приказ модела
 - 3.2. Синтакса
 - 3.3. Акциона семантика
 - 3.4. Редукциона семантика
 - 3.4.1. Резултати хармоничности
 - 3.4.2. Процеси са грешком
 - 3.5. Бихевиорална семантика
 - 3.6. Типска анализа
 - 3.6.1. Увод у типове
 - 3.6.2. Увод у типове кроз примере
 - 3.6.3. Типски систем
 - 3.6.4. Одсуство грешке код типизираних процеса
 - 3.6.5. Илустрација типских правила кроз примере
 - 3.6.6. Алгоритам за проверу типа процеса
 - 3.7. Пример
 - 3.8. Примене
4. Закључак
 - 4.1. Кратак преглед доприноса
 - 4.2. Стање у области
 - 4.3. Правци даљих истраживања

Литература

Дисертација садржи 116 литературних јединица. Кључна документација дата на почетку тезе садржи изводе и основне податке о докторској дисертацији на српском и енглеском језику. Након кључне документације дат је резиме на српском језику.

IV PhD THESIS OVERVIEW:

The doctoral dissertation is written in English, on 156 pages, organised into 4 chapters, with the following content:

Abstract in Serbian

Abstract in English

1. Introduction
2. A calculus for confidential name passing
 - 2.1. Syntax
 - 2.2. Action semantics
 - 2.2.1. Properties of the labeled transition system
 - 2.3. Reduction semantics
 - 2.4. Behavioral equivalence
 - 2.4.1. Strong barbed equivalence
 - 2.4.2. A characterization of the non-forwarding pi processes
 - 2.5. Examples
 - 2.5.1. Authentication
 - 2.5.2. Modeling groups and name hiding
 - 2.5.3. Open-ended groups
 - 2.6. Encoding forwarding
 - 2.6.1. The encoding
 - 2.6.2. Operational correspondence
 - 2.7. Remarks
3. A calculus of floating authorizations
 - 3.1. Preview of the model
 - 3.2. Syntax
 - 3.3. Action semantics
 - 3.4. Reduction semantics
 - 3.4.1. Harmony results
 - 3.4.2. Error processes
 - 3.5. Behavioral semantics
 - 3.6. Type analysis
 - 3.6.1. Background on types
 - 3.6.2. Introducing types by examples
 - 3.6.3. Typing discipline
 - 3.6.4. Type safety
 - 3.6.5. Illustrating typing rules by examples
 - 3.6.6. Type-checking
 - 3.7. Extended example
 - 3.8. Towards applications
4. Conclusion
 - 4.1. Summary of contributions
 - 4.2. Related work
 - 4.3. Future work

Bibliography

Bibliography consists of 116 references. Key documentation given at the beginning of the thesis contains copies of the basic data on doctoral dissertation in Serbian and English language. After the key documentation, an extended abstract in Serbian language is given.

V ВРЕДНОВАЊЕ ПОЈЕДИНИХ ДЕЛОВА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ:

Наслов докторске дисертације прецизно одражава предмет истраживања и добијене резултате.

Глава 1 представља увод у саму дисертацију који укључује неформалну дискусију о главним појмовима и концептима који ће се проучавати, као и кратак преглед структуре дисертације. У овом делу, кандидат даје неопходну мотивацију и истиче значај теме истраживања.

Глава 2 уводи нови формални модел за мобилне процесе са ограниченом могућношћу преноса поверљивих информација. Дати формални модел је процесни рачун, назван „Пи рачун за поверљивост” (Цпи), који представља један фрагмент Пи рачуна. Основна разлика у односу на Пи рачун лежи у особини да се у посматраном фрагменту примљена имена канала не могу даље прослеђивати. Осим увођења синтаксе и семантике, као и анализе понашања система, додатно је испитивана могућност кодирања Пи-рачуна у Цпи-рачун.

Глава 3 уводи нови формални рачун за изучавање контроле приступа ресурсима у дистрибуираним мобилним системима. Овај рачун представља проширење једног познатог рачуна за моделовање ауторизација, где се проширење односи на увођење дељених ресурса. Под ауторизацијом, у овом моделу, сматрамо право које процес поседује за коришћење одређених канала. У односу на познати модел синтакса је остала неизмењена, али семантички је промењено значење домена ауторизације, што је омогућило да се уведе контрола дељења ауторизација и принцип њиховог бројања.

Глава 4 резимира научне доприносе кандидата који су представљени у овом раду, али и додатно коментарише остале научне резултате који припадају ужој научној области кандидата и који су прихваћени за штампу, али нису детаљно обрађени у оквиру саме дисертације. Поред тога, ова глава садржи детаљну анализу праваца истраживања који су уско повезани са темом дисертације, укључујући директно цитирање релевантне литературе.

На основу свега наведеног, Комисија позитивно оцењује све делове докторске дисертације.

V EVALUATION OF PARTS OF PhD THESIS:

The title of doctoral dissertation accurately describes the research subject and obtained results.

Chapter 1 is an introduction to the dissertation itself, beginning with an informal discussion of the main notions and concepts to be studied, as well as with a brief overview of the structure of the dissertation. In this chapter, the candidate provides the necessary motivation and highlights the importance of the research topic.

Chapter 2 introduces a novel formal model for mobile processes with limited ability to disseminate confidential information. The formal model is a process calculus, called Confidential Pi-calculus (Cpi), which represents a fragment of the Pi-calculus. The main difference with respect to the Pi-calculus lies in the fact that a received channel name cannot be forwarded later on. In addition to introducing the syntax and the semantics, as well as analyzing the behavior of processes, the possibility of encoding the Pi-calculus into the Cpi-calculus is explored.

Chapter 3 introduces a novel formal calculus for studying access control of resources in distributed mobile systems. This model is a refinement of one well known authorization modeling calculus, where the refinement refers to the introduction of floating shared resources. By authorization, in this model, we mean the right that the process possesses to use certain channels. Compared with the previous model, the syntax remained unchanged, but the meaning of the domain of authorization is semantically altered, which enabled the introduction of authorization sharing control and the principle of accounting.

Chapter 4 summarizes the scientific contributions of the candidate presented in the thesis, and further comments on other scientific results that belong to the candidate's narrow scientific field, which have been accepted for publication, but are not presented in the dissertation itself. In addition, this chapter provides a detailed analysis of the research directions that are closely related to the topic of the dissertation, including the direct citation of relevant literature.

Based on all of the above, the Jury gives positive evaluation to all parts of the PhD thesis.

VI СПИСАК НАУЧНИХ И СТРУЧНИХ РАДОВА КОЈИ СУ ОБЈАВЉЕНИ ИЛИ ПРИХВАЋЕНИ ЗА ОБЈАВЉИВАЊЕ НА ОСНОВУ РЕЗУЛТАТА ИСТРАЖИВАЊА У ОКВИРУ РАДА НА ДОКТОРСКОЈ ДИСЕРТАЦИЈИ

LIST OF PUBLICATIONS THAT ARE RESULTS OF THE PHD THESIS

Таксативно навести називе радова, где и када су објављени. Прво навести најмање један рад објављен или прихваћен за објављивање у часопису са ISI листе односно са листе министарства надлежног за науку када су у питању друштвено-хуманистичке науке или радове који могу заменити овај услов до 01.јануара 2012. године. У случају радова прихваћених за објављивање, таксативно навести називе радова, где и када ће бити објављени и приложити потврду о томе.

1. I. Prokić, J. Pantović, and H. T. Vieira. A calculus for modeling floating authorizations. Journal of Logical and Algebraic Methods in Programming, 107:136 - 174, 2019. (M21)
2. J. Pantović, I. Prokić, and H. T. Vieira. A calculus for modeling floating authorizations. In C. Baier and L. Caires, editors, Formal Techniques for Distributed Objects, Components, and Systems - 38th IFIP WG 6.1 International Conference, FORTE 2018, Madrid, Spain, June 18-21, 2018, Proceedings, volume 10854 of Lecture Notes in Computer Science, pages 101-120. Springer, 2018. (M33)
3. I. Prokić. The Spi-calculus: a model for confidential name passing. In M. Bartoletti, L. Henrio, A. Mavridou, and A. Scalas, editors, Proceedings 12th Interaction and Concurrency Experience, ICE 2019, Copenhagen, Denmark, 20-21 June 2019, volume 304 of Electronic Proceedings in Theoretical Computer Science, pages 115-136. Open Publishing Association, 2019. (M33)

VII ЗАКЉУЧЦИ ОДНОСНО РЕЗУЛТАТИ ИСТРАЖИВАЊА

Главе 2 и 3 дисертације садрже оригиналне научне доприносе кандидата.

Најзначајнији доприноси из Главе 2 су следећи:

- Уведен је нови формални рачун за моделовање дистрибуираних мобилних процеса са контролисаном комуникацијом поверљивих информација;
- Формулисана је особина непрослеђивања поверљивих информација и показано је да је Цпи процеси задовољавају;
- Показано је да је Цпи рачун погодан за анализу неких раније проучаваних значајних особина процесних рачуна, као што је на пример креирање затворених домена за канале;
- Испитана је експресивност Цпи рачуна у односу на неке карактеристичне примере: проверу аутентичности имена канала, репрезентацију креирања затворених домена за канале, репрезентацију затворених и отворених група;
- Испитана је експресивност Цпи рачуна у односу на Пи рачун користећи неке познате и у литератури прихваћене критеријуме, који се заснивају на кодирању једног рачуна у други.

Најзначајнији доприноси из Главе 3 су следећи:

- Уведен је нови формални рачун за моделовање дистрибуираних мобилних процеса у којима је дељење ауторизација за приступ ресурсима контролисано и засновано на њиховом бројању;
- Испитано је понашање новог формалног система и истакнуте су неке особине од кључног значаја, доказивањем идентитета који их описују;
- Формулисан је појам грешке до које може доћи у систему са дељеним ауторизацијама и уведен је типски систем који елиминише процесе који могу довести до неауторизованог приступа ресурсима;
- Уведен је алгоритам за проверу типа процеса, који је захтевао додатну модификацију претходно уведеног типског система. Доказано је да су наведена два система међусобно еквивалентна;
- Приказано је коришћење уведеног формалног модела на апликативном примеру из домена коришћења лиценцираног приступа ресурсима;
- Приказана је једна могућа имплементација модела, у виду екстензије програмског језика Go.

На основу наведеног, Комисија закључује да резултати тезе представљају значајан допринос у развоју основа мобилних рачуна и теоријског рачунарства.

VII CONCLUSIONS AND RESULTS OF THE RESEARCH

The most significant contributions of Chapter 2 are the following:

- A novel formal calculus for modeling distributed mobile processes with controlled communication

of confidential information is introduced;

- The non-forwarding property of confidential information is formulated and it is proven that Cpi processes satisfy it;
- The Cpi-calculus is shown to be suitable for the analysis of some significant features of process calculi, such as creation of closed domains for channels;
- The expressiveness of the Cpi-calculus was examined with respect to some characteristic examples: authentication of channel names, representation of creation of closed domains for channels, representation of closed and open-ended groups;
- The expressiveness of the Cpi-calculus with respect to the pi-calculus was studied, using some well-known criteria, which are based on the encoding of one model into the other.

The most significant contributions of Chapter 3 are the following:

- A new formal calculus for modeling distributed mobile processes is introduced, in which authorization sharing for access to resources is controlled and based on their counting;
- Behavior of the new formal model has been examined and some of the key features are highlighted, proving behavioural identities that describe them;
- The concept of an error that can occur in a system with shared authorizations is formulated and a type system that eliminates processes that can lead to unauthorized access to resources is introduced;
- The type system is refined so as to move towards a type checking algorithm, addressing the issue of performance. These two systems are shown to be equivalent;
- An example, inspired by the notion of “Bring your own licence” from the licence setting, is given, showing one possible application of the introduced model;
- One possible implementation of the model is presented, in the form of an extension of the Go programming language.

The Jury considers previously listed research results as a significant contribution to development of foundations of mobile computing and theoretical computer science.

VIII ОЦЕНА НАЧИНА ПРИКАЗА И ТУМАЧЕЊА РЕЗУЛТАТА ИСТРАЖИВАЊА

Експлицитно навести позитивну или негативну оцену начина приказа и тумачења резултата истраживања.

Дисертација је написана прегледно и систематично. Оригинални резултати су јасно и прецизно формулисани, особине су детаљно доказане и дате су одговарајуће илустрације на примерима из примене у рачунарству.

Текст ове дисертације је од стране Библиотеке Факултета техничких наука у Новом Саду службено проверен на подударност, користећи софтвер за детекцију плагијаризма iThenticate. Резултати те провере су разматрани од стране свих чланова комисије. Комисија сматра да је степен подударности очекиван и занемарив.

VIII EVALUATION OF THE PRESENTATION AND INTERPRETATION OF THE RESEARCH RESULTS

The dissertation is well organized and clearly written. Original results are clearly and precisely formulated, all the properties are proved in detail, and adequate illustrations from applications in software practices are presented.

The Library of Faculty of Technical Sciences in Novi Sad has officialy checked the diseration for plagiraism violation using iThenticate plagiraism detection service. The results are studied by all members of the Jury. The Jury considers that the degree of matchings is expected and negligible.

IX КОНАЧНА ОЦЕНА ДОКТОРСКЕ ДИСЕРТАЦИЈЕ: FINAL EVALUATION OF THE DOCTORAL DISSERTATION

Експлицитно навести да ли дисертација јесте или није написана у складу са наведеним образложењем, као и да ли она садржи или не садржи све битне елементе. Дати јасне, прецизне и концизне одговоре на 3. и 4. питање:

1. Да ли је дисертација написана у складу са образложењем наведеним у пријави теме?

Докторска дисертација је у потпуности написана у складу са образложењем у пријави теме.

Is the dissertation written entirely in accordance with the reasoning given in the application?

The dissertation is written in full accordance with the explanations given in the research proposal.

2. Да ли дисертација садржи све битне елементе?

Докторска дисертација садржи све битне елементе. Предмет, циљеви и задаци истраживања су прецизно дефинисани. Добијени резултати истраживања, дискусија и закључна разматрања су детаљно описани. Анализирано је стање у области, а списак коришћене литературе указује на темељно проучавање и познавање области истраживања.

Does the dissertation contain all the relevant elements?

The dissertation contains all the relevant elements. The subject, objectives and tasks of the research are precisely defined. The research results, discussion and concluding remarks are described in detail. The state of the art is analysed, and a list of references indicates a fundamental knowledge of the field of research.

3. По чему је дисертација оригиналан допринос науци?

Дисертација представља и анализира оригиналне моделе. Резултати представљени у дисертацији публиковани су у једном раду у врхунском међународном часопису и презентовани на две релевантне међународне конференције.

In what way the dissertation provides original scientific contribution?

The thesis presents and analyzes original models. The results shown in the thesis are published in one international scientific journal and presented in two international scientific conferences.

4. Недостаци дисертације и њихов утицај на резултат истраживања

Комисија закључује да докторска дисертација нема недостатака.

The dissertation shortcomings and their impact on research results

The Jury concludes that the doctoral dissertation has no shortcomings.

X ПРЕДЛОГ:

Комисија позитивно оцењује докторску дисертацију мастер математичара Ивана Прокића, под насловом „Развој и анализа формалних модела за коришћење и дељење ресурса у дистрибуираним софтверским системима”, и предлаже да се докторска дисертација прихвати, а кандидату одобри одбрана.

EVALUATION RECOMMENDATION:

The Jury positively evaluates the doctoral dissertation of master mathematician Ivan Prokić, entitled “Formal modeling and analysis of resource usage and sharing in distributed software systems” and recommends to accept the dissertation and approve its defence.

Др Јелена Иветић, доцент
Факултет техничких наука
Универзитет у Новом Саду
председник комисије

Др Љубо Недовић, доцент
Факултет техничких наука
Универзитет у Новом Саду
члан комисије

Др Силвиа Гилезан, редовни професор
Факултет техничких наука
Универзитет у Новом Саду
члан комисије

Dr Hugo Filipe Mendes Torres Vieira, principal researcher
C4, Universidade da Beira Interior, Covilhã
члан комисије, ментор

Др Јованка Пантовић, редовни професор
Факултет техничких наука
Универзитет у Новом Саду
члан комисије, ментор