SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY
A INFORMATIKY

Ing. Igor Kazlov

Autoreferát dizertačnej práce

Analýza udalostných systémov s viacerými inštanciami

na získanie: vedecko-akademickej hodnosti
philosophiae doctor, PhD.

v doktorandskom študijnom programe: Aplikovaná informatika
v študijnom odbore: 9.2.9 aplikovaná informatika

Bratislava 2019

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Ing. Igor Kazlov

Autoreferát dizertačnej práce

Analýza udalostných systémov s viacerými inštanciami

na získanie: vedecko-akademickej hodnosti
philosophiae doctor, PhD.

v doktorandskom študijnom programe: Aplikovaná informatika
v študijnom odbore: 9.2.9 aplikovaná informatika

Bratislava 2019

Dizertačná práca bola vypracovaná: v externej forme doktorandského štúdia na Ústave informatiky a matematiky FEI STU v Bratislave.

Predkladateľ: Ing. Igor Kazlov
FEI STU Bratislava

Školiteľ: prof. RNDr. Gabriel Juhás, PhD.
FEI STU Bratislava

Oponenti: Ing. Ivana Budinská, PhD.
Ústav informatiky SAV
Dúbravská cesta 9
845 07 Bratislava

doc. Ing. Zoltán Balogh, PhD.
FPV UKF v Nitre
Trieda A. Hlinku 1
949 74 Nitra

Autoreferát bol rozoslaný dňa: .....

Obhajoba dizertačnej práce sa koná: 26. 8. 2019 o 13:00.

Na: Fakulte elektrotechniky a informatiky STU,
Ilkovičova 3, 812 19 Bratislava, v miestnosti C502.

prof. Dr. Ing. Miloš Oravec
dekan FEI STU

Obsah

1 Úvod **1**

2 Ciele dizertačnej práce **2**

3 Dosiahnuté výsledky dizertačnej práce **2**

3.1 Algoritmus detekcie uviaznutí 2

3.2 Strojová korekcia procesu 3

4 Literatúra **4**

5 Výber publikovaných prác dizertanta **6**

6 Citácie prác dizertanta **6**

7 Summary **8**

1 Úvod

Dňa 14. augusta 2003 sa viaceré vysoko zaľudnené oblasti severovýchodu a stredozápadu USA spolu s kanadskou provinciou Ontário nečakane ocitli bez elektrickej energie (blackout). Týmto masívnym výpadkom bolo zasiahnutých približne 15 miliónov ľudí, pričom s udalosťou súvisí najmenej 11 úmrtí a ďalšie tisíce ľudí uviazli v metre alebo vo výťahoch mrakodrapov. Ekonomická strata výpadku, ktorý vo väčšine dotknutých oblastí trval 2 až 3 dni, bola vyčíslená na 6,4 miliardy amerických dolárov. K tejto závažnej udalosti prispelo viacero faktorov a zlyhaní, pričom jedným z hlavných bola softvérová chyba v systéme energetického manažmenu (energy management system), kde dva procesy dokázali v tom istom čase zapísať svoje hodnoty do dátovej štruktúry zdieľanej pamäte, čo spôsobilo že nechcená nekonečná slučka zabránila spusteniu alarmu, ktorý mal upozorniť na ešte len vznikajúcu situáciu. [1]

Súčasný ľudský život je vo svojich mnohých aspektoch ovplyvnený technológiu a do vysokej miery sa prelína s počítačom riadenými dynamickými systémami, pričom tento trend má rastúcu tendenciu. Otázka bezpečnosti a najmä korektnosti systémov a ich procesov vo všeobecnosti predstavuje významný problém súčasnosti a ešte väčšiu výzvu do budúcnosti.

Jednou z prominentných oblastí, v ktorej je realizovaný výskum so zameraním sa na verifikáciu a korektnosť, sú takzvané diskrétne udalostné systémy a ich podtrieda, *work-flow procesy*. Známym príkladom work-flow procesov používaných v praxi sú *biznis procesy*. Work-flow procesy majú jednoznačne určený začiatočný a (zamýšľaný) konečný stav. Formálne modelované procesy je samozrejme možné analyzovať na mnohé vlastnosti, pričom v našej práci sme sa zamerali na korektnosť v zmysle absencie uviaznutí, takzvaného mŕtveho stavu (v angličtine deadlock) a schopnosť procesu vždy dosiahnuť svoj želaný finálny stav.

Špecifickú a zároveň veľmi významnú triedu work-flow procesov tvoria procesy s viacerými inštanciami, kde podľa jedného predpisu procesu súčasne beží viacero jeho inštancií (cases). Príkladom je oblasť poisťovníctva, keď súbežne existuje viacero poistných udalostí, ktoré všetky patria pod jeden všeobecný proces vybavovania poistnej udalosti. Jednotlivé inštancie procesu sú na sebe nezávislé a navzájom sa ovplyvňujú jedine pomocou zdieľaných zdrojov, konkrétne ich nedostatkom. Inštancia procesu si na svoj beh potrebuje dočasne prepožičať zdieľané zdroje, ale ak sú v určitom momente všetky zdroje alokované, inštancie musia počkať, kým sa opäť uvoľnia. Pretože počty zdieľaných zdrojov sú na začiatku dané, „priveľké“ množstvo súbežne bežiacich inštancií procesu môže spôsobiť, že nové inštancie

budú musieť počkať. Tiež predpokladáme, že zdroje počas behu inštancií nie sú zničené ani vytvorené, sú vždy len dočasne prepožičané. Existuje fenomén, kde aj keď je proces s jednou inštanciou korektný, počas súbežného behu viacerých inštancií môže dôjsť k takzvanému uviaznutiu, neželanému mŕtvemu stavu – deadlock.

2 Ciele dizertačnej práce

V prácach [2, 3, 4] pristupujú autori k otázke korektnosti work-flow sietí so zdieľanými zdrojmi štrukturálnym spôsobom analýzou takzvaných *syphons* a *traps*, dobre známych z analytického aparátu Petriho sietí [5]. V spomínaných prácach modelujú viaceré inštancie jednou sieťou, avšak jednotlivé inštancie v týchto sieťach nie sú úplne oddelené a ich vzájomným miešaním môže vzniknúť neočakávané správanie „navyše“, ktoré odporuje intuitívnemu chápaniu nezávislosti inštancií.

Problém s miešaním prípadov autori v [6] vyriešili pomocou takzvanej produkčnej siete. Ich sieť so zdieľanými zdrojmi – Resource-Constrained Workflow Nets (RCWF) transformujú na produkčnú sieť, kde sú jednotlivé inštancie oddelené. Nevýhoda analytického prístupu zvoleného v spomínanej práci je obmedzenie na jeden druh zdieľaných zdrojov.

Naša práca nadväzuje na [6] a má za cieľ rozšíriť analytický aparát pre RCWF siete nasledovným spôsobom:

1. vytvoriť všeobecný deterministický algoritmus na detekciu uviaznutí, kde
   (a) počet súbežných inštancií siete nie je ohraničený
   (b) počet druhov zdieľaných zdrojov nie je obmedzený
2. navrhnúť automatizovaný spôsob predchádzania uviaznutí pre nekorektné siete založený na modifikácii siete – korekcia siete.

3 Dosiahnuté výsledky dizertačnej práce

3.1 Algoritmus detekcie uviaznutí

V práci sme predstavili spôsob modelovania viacerých inštancií procesu pomocou Petriho sietí. Definovali sme *run-time* sieť, kde sa jednotlivé inštancie neovplyvňujú, s výnimkou zdieľania zdrojov, na ktoré musia čakať. V práci sme sa zaoberali procesmi, ktoré sú korektné pre jednu inštanciu, pričom takúto vlastnosť je triviálne otestovať, pretože stavový priestor jednej inštancie je vždy ohraničený.

Ďalej sme pomocou tejto run-time siete definovali dynamickú korektnosť – teda ak pre ľubovoľný počet inštancií nie je možné dosiahnuť stav mŕtvy stav, uviaznutie.

Neohraničený počet inštancií predstavoval problém, pretože stavový priestor run-time siete je takisto neohraničený a nebolo možné priamo otestovať vlastnosť korektnosti tak, ako ho určuje definícia. Na vyriešenie tohto problému sme definovali takzvaný *základný deadlock* a nebezpečné značkovanie.

Podstata nebezpečného značkovania, nebezpečného miesta a základného deadlocku je založená na vlastnosti, že každá inštancia, ktorá sa podieľa na vzniku základného dynamického uviaznutia, je nevyhnutne v stave, v ktorom má alokované zdroje a každý možný nesledujúci stav, alebo krok tejto inštancie bude tiež alokovať ďalšie zdroje. Odhalili sme, každá „uviaznutá“ inštancia v základnom deadlocku musí spĺňať túto požiadavku.

Pre všetky uviaznutia, vrátane tých, ktoré nespĺňajú vlastnosť základného deadlocku, platí, že tieto uviaznutia v sebe základný deadlock obsahujú vo forme akéhosi „podstavu“. Základný deadlock nám zároveň definuje „množinu minimálnych uviaznutí“, pre ktoré sme preukázali, že ich je vždy ohraničený počet. Keďže každý deadlock v sebe vždy musí obsahovať základný deadlok, potom stačilo nájsť množinu základných deadlockov. Formálne sme definovali algoritmus na detekciu dynamickej korektnosti a dokázali sme správnosť našich tvrdení.

3.2 Strojová korekcia procesu

V oblasti pružných výrobných systémov (flexible manufacturing systems) je problematika zdieľania zdrojov veľmi široko študovaná, pričom ich systém sa do značnej miery podobá workflow sieťam so zdieľanými zdrojmi. Napríklad v prácach [7, 8, 9, 10, 11] je do modelu pridaný plánovač (scheduler), ktorý má uviaznutiu zabrániť. V našej práci sme zvolili odlišný prístup, kde sa počas behu procesu nevykonáva žiadne riadenie, plánovanie či analýza. Korekcia, modifikácia procesu prebieha ešte pred jeho „spustením“, nasadením.

V práci sme riešili prípad, kedy je daný len model dynamicky nekorektného procesu a tento vstup prirodzene neobsahuje sémantiku, význam, či metadáta. Nie je zrejmé, ktoré časti procesu môžu byť pozmenené a ktoré musia byť v rámci korekcie zachované, teda nie je daný súbor obmedzení pre modifikáciu, korekciu siete. Keďže v procese môže súbežne prebiehať viacero inštancií, je teda možné hovoriť o jeho „paralelnom výkone“ alebo výkone čo do počtu inštancií. V práci sme problém chýbajúcich obmedzení modifikácie procesu obišli tým, že naša modi-

fikácia siete zníži paralelný výkon procesu pri stavoch, kde existuje priama hrozba dosiahnutia uviaznutia. Samotné uviaznute tak nie je dosiahnuteľné a modifikovaná sieť je korektná.

Prvý problém spomínaného prístupu predstavovala minimalizácia znižovania výkonu – zakázané správanie siete musí byť minimálne. Druhý problém spočíval v tom, že modifikácia siete, ak nie je realizovaná správne, môže vytvoriť nové nekorektné stavy, ktoré v pôvodnej RCWF sieti neexistovali. Tretí problém spočíval v tom, že vyjadrovacia sila Petriho sietí má určité obmedzenia a neumožňuje rozdeliť (obmedziť) správanie procesu ľubovoľným spôsobom.

V práci sme definovali takzvané *resource transactions*, pričom každá táto transakcia predstavuje množinu kauzálne súvisiacich spustení prechodov. Prvý prechod transakcie zdroje vždy alokuje („berie“) a ostatné prechody transakie tieto isté zdroje postupne vracajú. Dokončená transakcia má nulovú bilanciu zdrojov, teda všetky jej zdroje sú vrátené. V stavovom priestore procesu (v grafe dosiahnuteľnosti) sa transakcie opakujú, preto hovoríme o typoch transakcií. Jednotlivé stavy procesu sme skúmali z hľadiska počtov prechádzajúcich (typov) transakcií a na ich základe sme rozdelili stavový priestor procesu na dve množiny želaných a nežiadúcich stavov.

Správanie procesu rozdelené pomocou transakcií zachováva korektnosť a pomocou metód syntézy Petriho sietí (teória regionov [12]) je možné obmedziť najmenšiu množinu nežiadúceho správania. V práci sme ukázali výpočet takzvaných *blokujúcich miest*, ktoré sú do pôvodnej siete pomocou syntézy pridané a ktoré zablokujú nežiadúce správanie definované cez počty transakcií.

V dizertačnej práci sme ďalej predstavili takzvané (umelé) kontrolné transakcie, ktoré umožňujú dodatočné jemnejšie rozdelenie správania siete.

4 Literatúra

[1] U.S./Canada Power System Outage Task Force: *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*; United States Department of Energy; April 2004.

[2] K. Barkaoui and L. Petrucci. Structural analysis of workflow nets with shared resources. In *Workflow management: Net-based Concepts, Models, Techniques and Tools (WFM'98)*, volume 98/7 of *Computing science reports*, pages 82–95. Eindhoven University of Technology, 1998.

[3] K. van Hee, N. Sidorova, and M. Voorhoeve. Resource-constrained workflow nets. In G. Lindemann, editor, *Proc. of Concurrency Specification and Programming, CS&P'2004*, Informatik-Bericht Nr. 170, pages 166–177. Humboldt-Universität zu Berlin, 2004.

[4] Kees van Hee, Natalia Sidorova, and Marc Voorhoeve. 2006. Resource-Constrained Workflow Nets. *Fundamenta Informaticae*, Volume 71, Issue 2,3 (2006), pages 243-257.

[5] J. Desel and G. Juhás. What is a Petri Net? In H. Ehrig, G. Juhás, J. Padberg, G. Rozenberg (Eds.): *Unifying Petri Nets*, LNCS 2128, Springer, pp. 1–25, 2001.

[6] K. M. van Hee, A. Serebrenik, N. Sidorova and M. Voorhoeve. *Soundness of Resource-Constrained Workflow Nets.* ICATPN 2005, LNCS 3536, Springer, pp. 250-267, 2005.

[7] J. Colom. The resource allocation problem in flexible manufacturing systems. In W. van der Aalst and E. Best, editors, *Application and Theory of Petri Nets 2003, ICATPN'2003*, volume 2679 of Lecture Notes in Computer Science, pages 23–35. Springer-Verlag, 2003.

[8] J. Ezpeleta. Flexible manufacturing systems. In C. Girault and R. Valk, editors, *Petri nets for systems engineering.* Springer-Verlag, 2003.

[9] J. Ezpeleta, J. M. Colom, and J. Martínez. A Petri net based deadlock prevention policy for flexible manufacturing systems. *IEEE Transactions on Robotics and Automation*, 11(2):173–184, 1995.

[10] M. Silva and E. Teruel. Petri nets for the design and operation of manufacturing systems. *European Journal of Control*, 3(3):182–199, 1997.

[11] M. Silva and R. Valette. Petri nets and flexible manufacturing. In G. Rozenberg, editor, *Applications and Theory of Petri Nets*, volume 424 of Lecture Notes in Computer Science, pages 374–417. Springer, 1990.

[12] Bergenthum, R., Desel, J., Lorenz, R., Mauser, S.: Process mining based on regions of languages. In: Alonso, G., Dadam, P., Rosemann, M. (eds.) BPM 2007. LNCS, vol. 4714, pp. 375–383. Springer, Heidelberg (2007)

5 Výber publikovaných prác dizertanta

G. Juhás, I. Kazlov, A. Juhásová: Instance deadlock: A mystery behind frozen programs. In: Lilius, J., Penczek, W. (eds.) *PETRI NETS 2010*. LNCS, vol. 6128, pp. 1–17. Springer, Heidelberg (2010)

I. Kazlov, I. Miňo: Petri Nets Synthesis Using Genetic Programming. In *Application of Region Theory (ART)*: 3rd Workshop Proceedings; Barcelona, 2013, pp. 31–40.

G. Juhás, I. Kazlov: Process discovery = Reconstruction of behavior from logs + Model synthesis from behavior. In *Petri Net Newsletter*, 84., 2015 s. 13–25.

A. Juhásova, I. Kazlov, G. Juhás, L. Molnár: How to model curricula and learnflows by petri nets – a survey, In *14th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, pp. 147-152, 2016.

6 Citácie prác dizertanta

Van Der Aalst WM, Van Hee KM, Ter Hofstede AH, Sidorova N, Verbeek HM, Voorhoeve M, Wynn MT. Soundness of workflow nets: classification, decidability, and analysis. *Formal Aspects of Computing*. 2011 May 1;23(3):333-63.

Rosa-Velardo F., de Frutos-Escrig D. Decidability and complexity of Petri nets with unordered data. *Theoretical Computer Science*. 2011 Aug 5;412(34):4439-51.

Bergenthum R, Desel J, Harrer A, Mauser S. Modeling and mining of learnflows. In *Transactions on Petri Nets and Other Models of Concurrency* V 2012 (pp. 22-50). Springer, Berlin, Heidelberg.

Martos-Salgado M, Rosa-Velardo F. Dynamic soundness in resource-constrained workflow nets. In *Formal Techniques for Distributed Systems* 2011 Jun 6 (pp. 259-273). Springer, Berlin, Heidelberg.

Wang J, Li D. Resource oriented workflow nets and workflow resource requirement analysis. *International Journal of Software Engineering and Knowledge Engineering*. 2013 Jun; 23(05):677-93.

Sidorova N, Stahl C. Soundness for resource-constrained workflow nets is decidable. *IEEE Transactions on Systems, Man, and Cybernetics Systems*. 2012 Sep

12;43(3):724-9.

Solé M, Carmona J. Light region-based techniques for process discovery. *Fundamenta Informaticae*. 2011 Jan 1;113(3-4):343-76.

Martos-Salgado M, Rosa-Velardo F. Cost soundness for priced resource-constrained workflow nets. In *International Conference on Application and Theory of Petri Nets and Concurrency* 2012 Jun 25 (pp. 108-127). Springer, Berlin, Heidelberg.

Wang J, Tepfenhart B, Li X. Analysis of minimum workflow resource requirement. In *International Workshop on Process-Aware Systems* 2015 Oct 30 (pp. 53-66). Springer, Singapore.

Martos-Salgado M, Rosa-Velardo F. Safety and Soundness for Priced Resource-Constrained Workflow Nets. *Fundamenta Informaticae*. 2014 Jan 1;131(1):55-80.

Bergenthum R, Desel J, Mauser S. Workflow Nets with Roles. *Enterprise modelling and information systems architectures (EMISA 2011)*. 2011.

Li X, Liu G, Wang J, Wang J. Resource requirement analysis for cyclic workflows. In 2016 *IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC)* 2016 Apr 28 (pp. 1-6). IEEE.

Ramezani E, Sidorova N, Stahl C. Interval soundness of resource-constrained workflow nets: decidability and repair. In *International Conference on Fundamentals of Software Engineering* 2013 Apr 24 (pp. 150-167). Springer, Berlin, Heidelberg.

Wang J, Li X, Liu G. Cyclic workflow resource requirement analysis and application in healthcare. In 2016 *13th International Workshop on Discrete Event Systems (WODES)* 2016 May 30 (pp. 291-297). IEEE.

Wang J.: Petri net based resource modeling and analysis of workflows with task failures. In 2013 *10th IEEE International Conference on Networking, Sensing and Control (ICNSC)* 2013 Apr 10 (pp. 655-659). IEEE.

7 Summary

The dissertation thesis is dealing with the analysis of work-flow event systems called *resource constrained work-flow nets* (RCWF nets). RCWF nets provide the means to model and simulate multiple concurrent instances / cases, within one process, sharing the same set of resources. Even if the work-flow process is sound for one instance, deadlock can occur while running multiple concurrent instances and is called *dynamic deadlock*. We do not place any restrictions on number of concurrent instances, nor the number of type of shared resources. We first define the concept of so-called *dangerous places* (and markings) which we use to create finite representation of unbounded state space. The representation is used by our algorithm to detect reachable deadlock. The next part of our thesis deals with *algorithmic process rectification*. To preserve soundness property, we define so-called *resource transaction* – our smallest "unit" used to partition a state space of the process. The algorithmic process rectification problem is solved by application of region theory (Petri nets synthesis) at the very end of the thesis to modify the net. The deadlock states are unreachable after the modification (net is sound) and we show that with respect to our resource transaction partitioning, the set of unreachable states is the smallest.

Key words: **Petri nets, work-flow, soundness, deadlock, resources, synthesis, region**