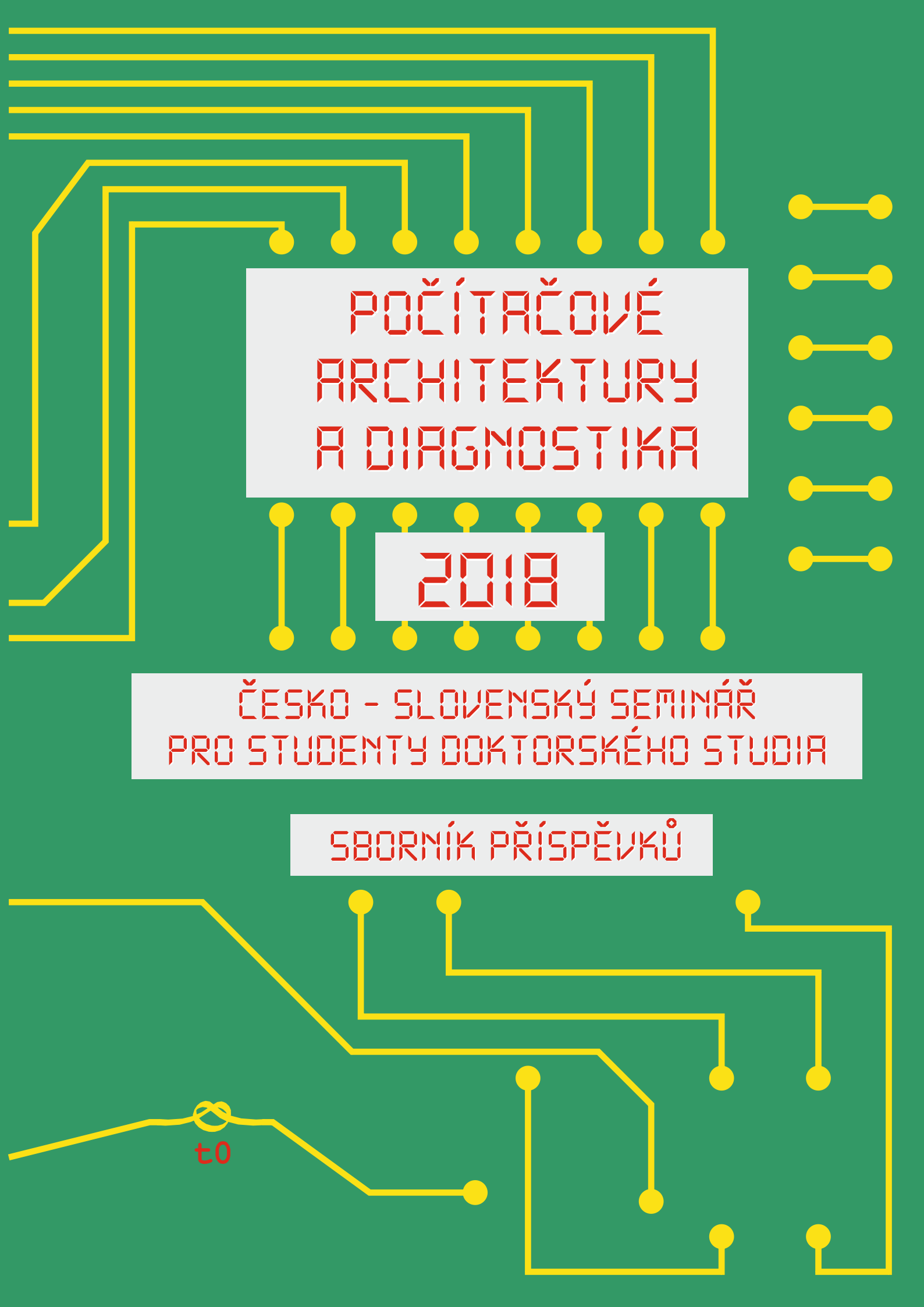

POČÍTAČOVÉ
ARCHITEKTURY
A DIAGNOSTIKA
2018
ČESKO - SLOVENSKÝ SEMINÁŘ
PRO STUDENTY DOKTORSKÉHO STUDIA
SBORNÍK PŘÍSPĚVKŮ
t0

Počítačové architektury a diagnostika PAD 2018

Pracovní seminář pro studenty doktorského studia

Hotel Churáňov, Stachy, Zadov, 5. – 7.9. 2018

Sborník příspěvků

ISBN 978-80-261-0814-6

Vydala Západočeská univerzita v Plzni 2018

Katedra informatiky a výpočetní techniky

Programový výbor:

Daniel Arbet	FEI STU v Bratislave
Jiří Buček	FIT ČVUT v Praze
Vladimír Drábek	FIT VUT v Brně
Karel Dudáček	FAV ZČU v Plzni
Petr Fišer	FIT ČVUT v Praze
Jiří Jaroš	FIT VUT v Brně
Katarína Jelemenská	FIIT STU v Bratislavě
Jan Kořenek	FIT VUT v Brně
Tomáš Koutný	FAV ZČU v Plzni
Štefan Krištofík	UI SAV v Bratislavě
Hana Kubátová	FIT ČVUT v Praze
Robert Kvaček	ASICentrum spol. s r.o.
Róbert Lórencz	FIT ČVUT v Praze
Dominik Macko	FIIT STU v Bratislavě
Ondrej Novák	FMIMS TU v Liberci
Zdeněk Plíva	FMIMS TU v Liberci
Stanislav Racek	FAV ZČU v Plzni
Martin Rozkovec	FMIMS TU v Liberci
Richard Růžička	FIT VUT v Brně
Jan Schmidt	FIT ČVUT v Praze
Vladimir Smotlacha	FIT ČVUT v Praze
Viera Stopjaková	FEI STU v Bratislave
Josef Strnadel	FIT VUT v Brně
Vlastimil Vavřička	FAV ZČU v Plzni
Karel Vlček	UTB ve Zlíně
Tomáš Zahradnický	Boxtrap security, spol. s r.o.

Organizační výbor:

Vlastimil Vavřička	FAV ZČU v Plzni
Stanislav Racek	FAV ZČU v Plzni
Karel Dudáček	FAV ZČU v Plzni
Tomáš Koutný	FAV ZČU v Plzni
Helena Ptáčková	FAV ZČU v Plzni

Obsah

Monitorace koncentrace glukózy pomocí nositelných zařízení

Martin Úbl
0. ročník, prezenční studium
školitel: Doc. Ing. Tomáš Koutný, Ph.D.

Katedra informatiky a výpočetní techniky, Fakulta aplikovaných věd Západočeské univerzity v Plzni
Technická 8, 301 00 Plzeň
Email: ublm@kiv.zcu.cz

***Abstrakt*—Diabetes mellitus je heterogenní skupina onemocnění, která má společný znak – zvýšenou koncentraci glukózy v krvi. Tělo zdravého člověka je schopno tuto koncentraci udržovat v únosné míře, tělo diabetika však ne a v dlouhodobém měřítku tato skutečnost vede až k trvalému poškození některých orgánů. Pacient si proto musí pravidelně měřit koncentraci glukózy a na základě této hodnoty pak dávkovat hormon inzulin, který tuto koncentraci snižuje. Měření může v běžných „domácích" podmínkách probíhat buď sporadicky ze vzorku krve, nebo kontinuálně senzorem zavedeným v podkožní tkáni. Tento příspěvek se zabývá měřicími přístroji, jejich komunikačními možnostmi a dalšími zařízeními, se kterými se mohou spojit a přenášet do nich naměřená data. Také se zabývá realizací simulační platformy, která simuluje kompletní softwarový zásobník systému pro měření koncentrace glukózy.**

***Keywords*—glukóza, diabetes, cgms, monitoring pacienta**

I. Úvod

Diabetes mellitus, česky *úplavice cukrová*, hovorově také *cukrovka*, je heterogenní skupina onemocnění, která sdílí společný znak – zvýšenou koncentraci glukózy v krvi. Jde o poruchu homeostázy glukózy, při které mohou v krátkodobém měřítku vzniknout komplikace zvané hypo- a hyperglykémie, tedy snížená, respektive zvýšená koncentrace glukózy v krvi. Neléčený diabetes vede k trvalé hyperglykemii a v dlouhodobém měřítku tato skutečnost vede k nefropatii (poškození jater), neuropatii (poškození nervů), retinopatii (poškození oční sítnice) a dalším trvalým poškozením orgánů.

Nejrozšířenějšími typy diabetu jsou typ 1 (T1D), typ 2 (T2D) a gestační diabetes. T1D je autoimunitním onemocněním, při kterém imunitní systém postiženého likviduje Langerhansovy ostrůvky slinivky břišní, které produkují mj. hormony inzulin a glukagon. Ty se starají o regulaci koncentrace glukózy v těle – inzulin tuto koncentraci snižuje a glukagon naopak zvyšuje. Při T2D vzniká tzv. inzulinová rezistence, tedy snížená schopnost glukózy pronikat přes buněčnou membránu, a tak zásobovat buňky energií. Dlouhodobě se pak může vyvinout v T1D. Gestační diabetes je typ, který vzniká během těhotenství v těle matky a přímo ohrožuje zdraví matky i plodu[1].

Diabetik tedy musí pravidelně koncentraci glukózy v krvi měřit a podle toho dodávat tělu potřebné dávky inzulinu a v některých případech i glukagonu. Pro orgány a vlastní regulaci je rozhodující koncentrace glukózy v krvi, glukóza se ale v určité koncentraci vyskytuje i v tzv. tkáňovém moku (intersticiální tekutině), tedy mezibuněčné výplni, přes kterou musí projít, aby se k buňkám dostala. Měření proto může využít vzorky z obou těchto prostředí, ovšem koncentrace v intersticiální tekutině není stejná, jako v krvi. Má však tendenci se vlivem difúze vyrovnávat.

II. Měření koncentrace glukózy

Měření koncentrace v krvi probíhá typicky píchnutím do bříška prstu, extrakcí kapky krve na testovací proužek, který je následně vložen do měřicícho přístroje, takzvaného glukometru. Ten vzorek analyzuje a zobrazí výslednou koncentraci na displeji. Tento způsob měření je ale pro pacienta nepříjemný a lze ho provádět pouze sporadicky – typicky nejvýše desetkrát denně, prakticky se však provádí 2 až 3 měření.

Koncentraci v intersticiální tekutině je možné měřit systémem, který se označuje jako CGMS[1]. Jedná se o minimálně invazivní způsob měření, kdy je pacientovi do podkoží zaveden senzor, který kontinuálně měří koncentraci glukózy a připojeným vysílačem komunikuje s dalším zařízením, do kterého hodnoty odesílá.

A. Glukometr

Glukometr je přístroj pro měření koncentrace glukózy v krvi pomocí testovacích proužků. Tyto proužky jsou vybaveny elektrodami a chemickou sloučeninou, která po kontaktu s glukózou v krvi reaguje a vytváří elektrický proud mezi elektrodami [2].

Roztokem, který je na proužek aplikován, nemusí nutně být krev. Toho se využívá i při prvotní kalibraci přístroje, kdy je připraveno několik různých roztoků glukózy o známých koncentracích, které jsou postupně přístrojem měřeny a je zaznamenáván naměřený proud [3]. Tato sada hodnot je pak použita pro zjištění parametrů jednoduchého modelu, kterým typicky bývá obyčejná lineární regrese – obecně lze předpokládat, že závislost naměřeného proudu na skutečné koncentraci glukózy v roztoku bude lineární.

[1]Continuous Glucose Monitoring System

V takovém případě lze například metodou nejmenších čtverců získat dva parametry – posunutí a směrnici. Ty poté slouží k transformaci každého dalšího naměřeného elektrického proudu na číselnou reprezentaci koncentrace glukózy.

B. Kontinuální měření v podkoží

Zařízení pro kontinuální měření se skládají ze dvou částí – ze senzoru a z vysílače. Senzor je zaveden do podkožní tkáně pacienta typicky v podbřišku, případně na jiném dostupném místě, kde nenarušuje komfort pacienta. K vysílači je připojen velmi těsně přes proprietární konektor. Celá tato soustava je typicky zajištěna často voděodolnou náplastí.

Jedno měření má trvání typicky do 10 dnů. Během této doby je nutné přístroj pravidelně kalibrovat zadáváním koncentrace glukózy zjištěné sporadickým měřením v krvi. Jehla senzoru je totiž lidským tělem vnímána jako cizí těleso a imunitní reakce postupně degradují přesnost měření nepředvídatelným způsobem. Princip kalibrace je de-facto stejný jako u kalibrace glukometru při výrobě, pouze je spoléháno na přesnost glukometru při poskytnutí referenční hodnoty. Vnitřně senzor měří hodnotu elektrického proudu – tato hodnota je nazývána zkratkou *ISig*[2]. Ta je za předpokladu, že byl přístroj zkalibrován, převedena jednoduchým lineárním modelem na číselnou reprezentaci koncentrace glukózy v podkožní tkáni.

III. Komunikace senzoru

Komunikační modul připojený k modernímu senzoru využívá technologie Bluetooth Low-Energy (BLE). Komerčně dostupné senzory pak implementují vlastní proprietární profil, ovšem se standardizací protokolu IEEE 11073-10425 pro kontinuální měření koncentrace glukózy [4] lze očekávat, že se situace změní.

A. CGM profil

CGM profil pro Bluetooth Low-Energy adaptovaný organizací Bluetooth SIG [5] definuje tyto charakteristiky:

1) CGM Measurement: hodnota naměřené koncentrace glukózy – obsahuje příznaky měřicího sezení (zda data obsahují informace o trendech, odhad kvality, apod.), naměřenou hodnotu ve formátu SFLOAT (IEEE 11073) a časovou značku měřené hodnoty relativní vůči *CGM Session Start Time* ve vteřinách

2) CGM Feature: obsahuje informace o dostupných funkcích senzoru, zdroji naměřených hodnot a umístění senzoru.

3) CGM Status: obsahuje aktuální časovou značku relativní vůči *CGM Session Start Time* ve vteřinách a stav senzoru (chybové kódy, příznak nízkého stavu baterie, ...).

4) CGM Session Start Time: obsahuje časovou značku začátku měření. Tuto hodnotu nastavuje první připojené zařízení ihned po navázání komunikace, senzor hodnotu při zápisu upraví dle relativního času, který uběhl od skutečného zapnutí.

[2]Interstitiary signal

5) CGM Session Run Time: obsahuje zbývající čas, po který senzor bude poskytovat relevantní hodnoty. Tato hodnota je odhadem na základě konstrukce a vlastností senzoru a je specifická pro každou implementaci. Hodnota je ve vteřinách.

6) Record Access Control Point (RACP): řídicí pole, do kterého řídicí zařízení (mobilní telefon, koncentrátor, ...) zapisuje požadavky pro vyzvednutí a vymazání hodnot z historie. Po zápisu je do této charakteristiky indikován návratový kód (úspěch, chyba) a v případě úspěchu jsou do charakteristiky *CGM Measurement* postupně indikovány vyžádané hodnoty.

7) CGM Specific Ops Control Point (SOCP): řídicí pole pro operace specifické pro CGM přístroj. Zápisem do této charakteristiky lze senzor kalibrovat, nastavovat prahové hodnoty koncentrace glukózy (a trendů), při kterých je vyvolán alarm, nastavuje se komunikační interval a také je tímto možné spustit nebo ukončit sezení.

Integrita dat může být navíc v rámci každé charakteristiky zabezpečena pomocí E2E-CRC. I přes to, že jde o přenos medicínských dat, standard neukládá zvýšenou úroveň zabezpečení.

B. Průběh měřicího sezení

Po spuštění senzoru začne čítání reálného času a senzor je inicializován – to obnáší prvotní pokusy o měření, které ověří, zda je správně zaveden a zda není například poškozen. Následně vyčkává, až se k němu připojí řídicí stanice. Ta do SOCP zapíše příkaz pro započetí sezení a do *CGM Session Start Time* zapíše aktuální časovou značku. Senzor dopočte skutečnou časovou značku odečtením hodnoty, kterou do této doby načítal a měření započne. Senzor však neposkytuje hodnoty koncentrace glukózy, dokud není patřičně zkalibrován. Metoda kalibrace a rozestupy se různí v implementacích různých výrobců, typicky je však senzor kalibrován na začátku měření a poté ještě několikrát v několika následujících hodinách. Po této kalibrační rutině začne poskytovat měřené hodnoty notifikací charakteristiky *CGM Measurement*.

Senzor si během sezení vyžádá kalibraci ještě několikrát, a to pravidelně v řádech jednotek hodin (6 a více hodin), případně v posledních dnech životnosti senzoru o něco častěji. Konec své životnosti senzor oznamuje jak stále aktualizovanou hodnotou *CGM Session Run Time*, tak hodnotou v charakteristice *CGM Status*.

C. Ukládání hodnot

Senzor interně ukládá hodnoty do vestavěné paměti, která může být volatilní. Vnitřně se jedná o kruhový buffer s omezenou kapacitou v řádu desítek až stovek měření. Z této „databáze“ lze hodnoty vyzvedávat zpětně zápisem do charakteristiky *Record Access Control Point* – senzor poté postupně notifikuje charakteristiku *CGM Measurement* se všemi dostupnými hodnotami, které vyhovují filtru.

Tento mechanismus dovoluje vyrovnat krátké výpadky spojení s řídicí stanicí – senzor si pamatuje časové značky a hodnoty, řídicí stanice si po delší odmlce může vyžádat všechny hodnoty od časové značky, kterou jako poslední obdržela.

IV. Řídicí stanice

Řídicí stanicí může být libovolný přístroj, který implementuje stejný protokol. Typicky jím je buď specializované zařízení výrobce (inzulinová pumpa, koncentrátor hodnot) nebo například mobilní telefon. Také mohou být do řetězu zpracování zapojeny „chytré“ hodinky, které od mobilního telefonu data přijímají v odděleném datovém toku a zobrazují informace v omezené formě.

Inzulinová pumpa je zařízení, které je vybaveno systémem pro dávkování inzulinu a je schopné na základě čtených hodnot ze senzoru inzulin dávkovat přímo do pacientova těla. Tato regulace se děje buď automaticky podle měřených hodnot a jejich trendů, nebo manuálně na pacientův podnět.

Koncentrátorem hodnot se rozumí takové zařízení, které kromě kalibrace senzoru a řídicích zpráv měřené hodnoty přijímá a ukládá. Pacient po ukončení měřicího sezení tento koncentrátor předá specialistovi, který hodnoty z přístroje vyzvedne, analyzuje a podle nich určí další směr léčby.

V neposlední řadě lze jako řídicí zařízení použít mobilní telefon s potřebným programovým vybavením a podporou komunikačního zásobníku Bluetooth Low-Energy. Vzhledem k faktu, že tzv. „chytrý“ mobilní telefon dnes vlastní drtivá většina populace vyspělých zemí, je jeho použití i logickým krokem k minimalizaci dodatečných nákladů a zvýšení komfortu pacienta – není třeba nosit s sebou další zařízení.

Aplikační vybavení mobilního telefonu pak musí umožňovat analogické funkce koncentrátoru hodnot. Mobilní telefon není vybaven systémem pro dávkování inzulinu, takže ho nelze využít přímo k aktivní regulaci koncentrace glukózy.

V. Další náležitosti

Pro další vylepšení systémů pro monitoraci koncentrace glukózy na straně pacienta je nutné uvažovat ještě další náležitosti. První jsou modely dynamiky glukózy pro přepočet dostupných signálů na relevantní hodnoty, eventuálně s možností predikce. Dále musíme uvažovat algoritmy pro hledání jejich parametrů a příslušné metriky, které jsou použity pro odhad kvality parametrů. Celý systém je pak vhodné koncipovat tak, aby bylo možné provádět jak měření na straně pacienta, tak simulace pro potřeby výzkumu a vývoje modelů dynamiky glukózy a souvisejících náležitostí.

A. Modely dynamiky glukózy

Jak bylo zmíněno v kapitole I, koncentrace glukózy v podkožní tkáni (intersticiální tekutině) a v krvi se neshodují, ale lze jejich vztah popsat matematickým modelem. Na dostupných signálech, tedy signálu sporadického měření v krvi a kontinuálního měření v podkožní tkáni, staví dva hlavní modely: model Steil-Rebrinové [6] a model difúzní [7].

B. Algoritmy pro výpočet parametrů modelu

Problém nalezení optimálních parametrů modelu je problémem optimalizačním. Proto je možné použít například genetický algoritmus nebo některou z vybraných deterministických metod. Školitelem jsou v současné době používány algoritmy dva: NEWUOA z knihovny NLopt pro nelineární optimalizace [8] a metadiferenciální evoluce [9].

C. Metriky

Pro ohodnocení kvality nalezených parametrů v průběhu výpočtu jsou použity metriky. Tyto metriky jsou počítány na základě rozdílů naměřených a vypočtených hodnot, volitelně jsou pak použity jejich druhé mocniny, případně odchylky relativní místo absolutních.

Použít lze libovolnou ze standardních statistických metrik: maximální chybu, průměrnou chybu nebo například standardní odchylku. Ty ale neuvažují časové uspořádání hodnot a tak je vysoce pravděpodobné, že pro dvě rozdílně kvalitní řešení poskytnou velmi blízkou hodnotu metriky.

Metrika která takové uspořádání respektuje je například metrika Crosswalk [10]. Pravděpodobnost podobného ohodnocení velmi kvalitativně odlišných řešení stále není nulová, ale tato metrika ji výrazně minimalizuje.

V průběhu výpočtu parametrů jde vždy o minimalizaci hodnoty metriky – menší hodnota metriky odpovídá lepšímu řešení.

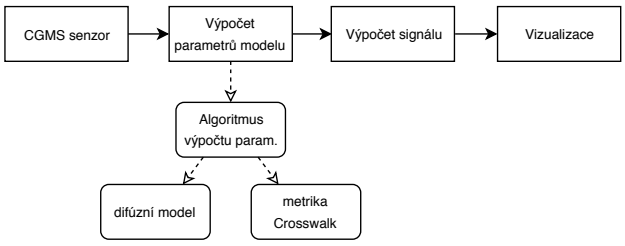
D. Softwarová architektura

Celé řešení musí být vhodně navrženo a implementováno tak, aby bylo možné simulovat kompletní softwarový zásobník řešení pro měření koncentrace glukózy. Také by mělo být možné beze změny kódu přenést celou architekturu například na mobilní telefon, který může být součástí systému pro měření na straně pacienta.

VI. Dosavadní práce

Na základě těchto znalostí byla v rámci předcházející diplomové práce implementována aplikace SmartCGMS, a to ve dvou variantách: aplikace pro mobilní telefon a „chytré“ hodinky a aplikace pro osobní počítač.

Obě varianty sdílí společný základ *fall-through* architektury, která vychází z High-Level Architecture [11], podporuje simulace, ale je možné ji rekonfigurovat tak, aby byla schopná fungovat v režimu pro měření v reálném čase a s reálným senzorem. Aplikace se liší pouze uživatelským rozhraním, a to zejména z důvodu odlišných požadavků na ovládací prvky a funkce. Rozhraní je pro desktopovou aplikaci implementováno knihovnou Qt a mobilní aplikace je realizována užitím technologie Xamarin a Xamarin.Forms.



Obrázek 1. Zjednodušené schéma architektury v konfiguraci pro měření na straně pacienta

Architektura se skládá z tzv. filtrů, které představují jednotlivé objekty simulace a každý plní oddělenou specifickou funkci. Jedná se o architekturu lineární, kdy je každý

filtr propojen komunikačním kanálem, tzv. rourou, s filtrem předcházejícím a následujícím. Tímto kanálem jsou dopředně šířeny zprávy různých typů obsahující například měřenou hodnotu, parametry modelu, informační zprávy a další. Každá entita (filtr, model, metrika, ...) je identifikována unikátním GUID. Zjednodušené schéma použité v mobilní aplikaci lze vidět na obrázku 1.

Rovněž byl v rámci dosavadní práce implementován simulovaný senzor s podporou podmnožiny funkcí standardu IEEE 11073-10425, a to jako firmware pro vývojovou desku Texas Instruments LAUNCHXL-CC2650. Ten je schopen přehrávat již naměřené hodnoty z minulosti, které jsou do jeho paměti nahrány v čase kompilace, a chová se jako reálný senzor.

VII. Navazující práce

Tento základ otevírá možnosti širokému spektru směrů, kterými se lze v rámci dizertační práce vydat. Aplikační zásobník bude v první řadě nutné rozšířit o simulátor lidského těla (diabetického pacienta) – lze zmínit například modely fyziologických procesů lidského těla vyvíjené v rámci projektu HumMod, resp. jeho moderní adaptace Physiomodel [12].

Vzhledem k velmi omezenému přísunu testovacích a validačních dat lze tyto modely použít pro generování signálů, které by za normálních okolností měřil a poskytoval senzor – koncentrace glukózy v krvi a intersticiální tekutině. Model také odbourává nutnost omezovat se na sporadicky měřené koncentrace v krvi – simulaci lze jednoduše parametrizovat tak, aby poskytovala hodnoty v intervalech např. 5 minut. Model dynamiky glukózy ale musí stále počítat pouze se sporadickým měřením, protože to je v praktických aplikacích na straně pacienta dostupné. Modely lidského těla tedy bude možné použít například k verifikaci.

Dalším směrem je bez pochyby oblast hledání parametrů modelů. Z této oblasti lze uvažovat zejména o stochastických optimalizačních algoritmech, tedy například o již zmíněné metadiferenciální evoluci, která poskytuje přijatelné výsledky [9]. Jednou z hlavních nevýhod této metody je však doba běhu, která v případě mobilního zařízení není uspokojivá. Doba běhu společně s využitím všech procesorových jader pak jde ruku v ruce se spotřebou elektrické energie, která v případě mobilního telefonu nebo jiného zařízení s omezeným zdrojem napájení musí být co možná nejnižší. Cílem je tedy najít takový optimalizační algoritmus, který nalezne alespoň srovnatelně kvalitní řešení, jako metadiferenciální evoluce, ale spotřeba elektrické energie bude výrazně nižší. Zde je možné soustředit se na optimalizaci existujícího algoritmu, tedy jeho jednotlivých částí (strategie křížení, mutace, ...) a implementační aspekty, nebo na možnosti použití jiných, existujících algoritmů. Z těch se nabízí například bayesovská optimalizace. Mimo to se v tomto stádiu vývoje nabízí ještě možnost *offloadingu*, tedy odesílání dat ke zpracování a výpočtům na vzdálený server, což pochopitelně implikuje zvýšený důraz na bezpečnost komunikačního kanálu a cílového serveru – jedná se o citlivá medicínská data.

V neposlední řadě je tu směr budoucí integrace do přístrojů pro monitoring a dávkování inzulinu na straně pacienta v módu „closed loop“, tedy v podstatě umělé slinivky břišní, respektive její části, která se stará o homeostázu glukózy. Tomu ale předchází nutnost mít kompletní simulační prostředí, co nejpřesnější model dynamiky glukózy a takové algoritmy, které je možné provozovat na nízkopříkonovém zařízení odolném proti poruchám.

Využití mobilního telefonu v řetězu zpracování signálu také otevírá dveře monitoringu na dálku, kterým se momentálně věnuje hlavně projekt Nightscout [13]. To je užitečné zejména pro monitoring diabetických dětí.

VIII. Závěr

Tento příspěvek shrnuje způsoby měření koncentrace glukózy v těle pacienta, měřicí přístroje k tomuto účelu používané, komunikační protokol, který senzory používají, zařízení, která slouží jako řídicí stanice a další související náležitosti. Také byla stručně představena předcházející diplomová práce, na kterou bude práce dizertační navazovat.

Acknowledgment

Tato práce byla podpořena (1) projektem LO1506 Ministerstva školství, mládeže a tělovýchovy České republiky a (2) Institucionální podporou na dlouhodobý koncepční rozvoj výzkumné organizace.

Reference

[1] J. Hall, *Guyton and Hall Textbook of Medical Physiology E-Book*, ser. Guyton Physiology. Elsevier Health Sciences, 2015. [Online]. Available: https://books.google.cz/books?id=krLSCQAAQBAJ

[2] J. Bronzino, *Medical Devices and Systems*, ser. The Biomedical Engineering Handbook, Fourth Edition. CRC Press, 2006. [Online]. Available: https://books.google.cz/books?id=OQjO-iecCkQC

[3] N. Dalvi, *Glucose Meter Reference Design*, Microchip Technology Inc., 2013, dokument číslo: 00001560A.

[4] “Health informatics–personal health device communication - part 10425: Device specialization–continuous glucose monitor (cgm),” *IEEE Std 11073-10425-2017 (Revision of IEEE Std 11073-10425-2014)*, pp. 1–83, Leden 2018.

[5] R. Hughes, R. Strickland, R. Schmitz, F. Bootz, W. Heck, K. Shingala, L. Richardson, L.-A. Aschehoug, S. Larvenz, N. Hamming, M. Yeung, and J. Hartmann. (2014) Continuous glucose monitoring service. Verze 1.0.1. [Online]. Available: https://www.bluetooth.com/specifications/gatt

[6] K. Rebrin and G. M. Steil, “Can interstitial glucose assessment replace blood glucose measurements?” *Diabetes Technology & Therapeutics*, vol. 2, no. 3, pp. 461–472, 2000, pMID: 11467349.

[7] T. Koutny, “Glucose predictability, blood capillary permeability, and glucose utilization rate in subcutaneous, skeletal muscle, and visceral fat tissues,” *Computers in Biology and Medicine*, vol. 43, no. 11, pp. 1680 – 1686, 2013.

[8] M. J. D. Powell, *The NEWUOA software for unconstrained optimization without derivatives*. Boston, MA: Springer US, 2006, pp. 255–297.

[9] T. Koutny, “Using meta-differential evolution to enhance a calculation of a continuous blood glucose level,” *Computer Methods and Programs in Biomedicine*, vol. 133, pp. 45–54, 2016.

[10] ——, “Crosswalk – a time-ordered metric,” in *EMBEC & NBC 2017*. Singapore: Springer Singapore, 2018, pp. 884–887.

[11] O. Topçu and H. Oğuztüzün, “Guide to distributed simulation with hla,” in *Simulation Foundations, Methods and Applications*. Springer International Publishing, 2017, pp. 1–307.

[12] M. Mateják and J. Kofránek, “Physiomodel - an integrative physiology in modelica,” in *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, Aug 2015, pp. 1464–1467.

[13] J. M. Lee, E. Hirschfeld, and J. Wedding, “A patient-designed do-it-yourself mobile technology system for diabetes: Promise and challenges for a new era in medicine,” vol. 315, p. 1447, 04 2016.

Automatizace návrhu spolehlivých systémů a její dílčí komponenty

Jakub Lojda
3. ročník, prezenční studium,
Školitel: Doc. Ing. Zdeněk Kotásek, CSc.

Fakulta informačních technologií Vysokého učení technického v Brně,
Centre of Excellence IT4Innovations
Božetěchova 1/2, 612 66 Brno, Czech Republic
Email: {ilojda, kotasek}@fit.vutbr.cz

***Abstrakt*—Vyšší úroveň integrace umožňuje implementovat stále složitější systémy. Vyšší integrace však zvyšuje riziko vzniku poruchy. Riziko je možno minimalizovat použitím technik odolnosti proti poruchám a maskování poruch. Vyšší složitost ale značně komplikuje vývoj takových systémů, který se do značné míry opírá o zkušenosti návrháře. Cílem našeho výzkumu je navrhnout metodu automatické konverze systémů neodolných na systémy odolné proti poruchám, která by uměla pracovat na téměř libovolné úrovni abstrakce. Tento článek je věnován dvěma podstatným částem výzkumu automatizace návrhu odolných systémů, tj. vkládání redundance a akceleraci vyhodnocení výsledků. Stěžejní částí článku je prezentace výsledků získaných během posledního roku výzkumu.**

***Klíčová slova*—Automatizace návrhu, HLS, vysokoúrovňová syntéza, odhad odolnosti, systém odolný proti poruchám.**

I. Úvod a Cíle výzkumu

Zvyšování integrace na čipu umožňuje realizovat složitější obvody, ale také vede na vyšší náchylnost k poruchám. Např. u hradlových polí dochází ke zvýšení jevů typu *Single Event Upset* (SEU). Obecným cílem našeho výzkumu je navrhnout metodu pro automatizovanou konverzi systému neodolného na systém odolný proti poruchám (OPP). Cílem je, aby metoda byla schopna pokrýt jak nové metody návrhu, např. vysokoúrovňovou syntézu, z angl. *High-Level Synthesis* (HLS), která pracuje na úrovni popisu algoritmu (např. C++), tak konvenční přístupy. Naše snaha vychází z obecného návrhu systémů OPP:

1) definovat zamýšlené parametry výsledného řešení,
2) vložit (modifikovat) architekturu pro dosažení OPP,
3) vyhodnotit zvažované parametry,
4) pokud řešení nesplňuje parametry, pokračovat bodem 2.

Tento článek pokrývá výzkum spojený s automatizací návrhu OPP a věnuje se především bodům 2 a 3. Sekce II cituje některé ze souvisejících výzkumů. Sekce III popisuje v úvodu využívanou platformu pro verifikaci OPP. Následují stěžejní Sekce IV a V, jež se zabývají zaváděním OPP do systémů vyvíjených pomocí HLS. Zavádění OPP je představeno v kontextu výzkumu dosavadního a také v kontextu posledního roku. Stěžejní je rovněž Sekce VI, jež je zaměřena na aktuální výsledky v oblasti urychlení a odhadu parametrů odolnosti. Sekce VII uvádí obecné cíle disertace a závěrečné zhodnocení.

II. Související práce

Následující část textu je věnována popisu aktuálních metod zavádějících OPP a rovněž akcelerujících vyhodnocení OPP.

A. Odolnost pro HLS

Autoři frameworku, který nazývají HLShield [2], představují přístup, při kterém je vstupní algoritmus označkován v profilovacím SW a následně zpracován upravenou variantou HLS, která podporuje vkládání redundance dle značek. Autoři příspěvku [14] představují manuální modifikaci algoritmu násobení matic pro získání spolehlivosti ve spojení se syntézou pomocí nástroje Vivado HLS. Na zvoleném algoritmu dokazují efektivitu jejich řešení, nicméně samotná modifikace kódu je ponechána na vývojáři.

B. Vyhodnocení odolnosti

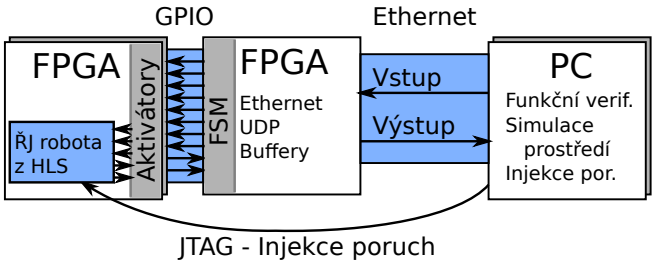
Vyhodnocení dopadu poruch je aktuálním problémem a není možné vyjmenovat všechny publikace na toto téma. Z vybraných se vyhodnocením OPP zabývají např. autoři článku [11], jenž je zaměřen na test implementací na úrovni RTL a netlist. Autoři příspěvku [13] navrhli nástroj pro injekci poruch, který ale vyžaduje modifikaci cílové implementace. Podporují mnoho syntetizovatelných modelů poruch, autoři navržené řešení implementovali v jazyce VHDL. Autoři v [10] se rovněž zaměřují na rychlost verifikace a představují řešení, kde je injekce poruch řešena přímo na čipu FPGA.

III. Verifikační prostředí s řadičem robota

V úvodu akademického roku ještě nebyl dokončen nástroj pro akceleraci vyhodnocení citlivých bitů (bude prezentován dále). Z tohoto důvodu jsme v úvodu práce využívali verifikační prostředí, jenž slouží pro finální, důkladné, ohodnocení systému i se zvážením mechanické části, což je ovšem časově mnohem náročnější. Proto přikládáme stručný popis tohoto verifikačního prostředí, jenž bylo v rámci naší skupiny již dříve publikováno v [12]. Verifikační prostředí je zaměřeno na vyhodnocení elektromechanických aplikací a je složeno ze dvou částí: 1) elektronického přípravku (kit s FPGA, do kterého jsou injektovány poruchy, zde ML506 založený na FPGA řady Virtex 5); 2) mechanického prostředí, které je simulováno na PC (zde aplikace Player/Stage [3]), implementace verifikace a injektoru poruch [15], rovněž běžících na PC. Schéma experimentálního prostředí ukazuje Obrázek 1. Pomocí injektoru poruch je možno cíleně vkládat poruchy do využitých bitů *Look-up* tabulek (LUT) a to zároveň pouze do těch, které jsou součástí specifikovaného bloku, tj. výhradně do verifikovaného obvodu.

IV. Vkládání redundance: Současný stav výzkumu

V našem předchozím výzkumu jsme se zabývali návrhem prostředků pro vkládání redundance do systémů popsaných na úrovni algoritmu a syntetizovaných pomocí HLS před průběhem samotné syntézy a bez zásahu do samotného procesu syntézy. Pro vkládání byla navržena metoda umožňující cílit redundanci za pomocí modifikovaných datových typů a s



Obrázek 1: Struktura experimentálního verifikačního prostředí.

nimi sémanticky spjatých modifikovaných operací nad těmito typy. Tyto prostředky jsme pracovně nazvali Redundantní Datové Typy (RDT). Pro každou metodu OPP je navržen příslušející RDT, který ji vkládá do algoritmu na místa, v nichž je instanciována proměnná daného datového typu, případně na místa, na kterých probíhají operace s instancí daného RDT. Tím je zajištěna automatická modifikace sémantiky operací, přičemž pro její dosažení je třeba modifikovat pouze onen datový typ proměnné. RDT jsou parametrizovatelné, každý RDT zahrnuje minimálně jeden parametr, jenž obsahuje jméno původně využitého datového typu, jehož funkci RDT zastoupí. RDT je pak možno v algoritmu používat ekvivalentním způsobem, jako typ původní, přičemž pomocí RDT je zajištěna jeho odolná implementace ve výsledné realizaci.

Pro účely experimentální implementace byl zvolen jazyk C++ v kombinaci s využitím tzv. systému *šablon*, které pro jazyk C++ umožňují efektivně realizovat koncept RDT. Koncept RDT pro syntézu systémů OPP jsme prezentovali v [9]. Jeho podrobnější vyhodnocení s využitím na řadiči robota je prezentováno v [8]. V minulosti jsme zkoumali i možnost vyhodnocení *důležitosti* jednotlivých operací v obvodové realizaci za pomocí HLS a RDT, jež se ovšem v publikaci [6] ukázala jako náročná na analýzu a interpretaci výsledků a rovněž na časové zdroje.

V. Vkládání redundance: Aktuální výsledky

Aktuální výsledky výzkumu v oblasti vkládání redundance spočívají především ve zlepšení vlastností systémů generovaných s využitím RDT a jsou publikovány v [7]. V následujícím experimentu je zkoumán vliv míry redundance a volby majoritní funkce v hlasovacím členu na výslednou odolnost systému. Ke dříve prezentovanému RDT *triple*, jenž implementuje známou architekturu TMR, jsme přidali rovněž RDT *quadruple* (4MR) a *quintuple* (5MR). Dále jsme přidali varianty s bitovou majoritou, jejichž názvy končí *_bit*. Využíváme platformy pro finální verifikaci, která zvažuje též vlivy poruchy na řízenou mechanickou část.

Redundance v obvodu ve smyslu nadbytečného využití zdrojů nemusí nutně implikovat jeho OPP. Z tohoto důvodu jsme zaměřili pozornost na definici jednotky *Intenzity Injektáže Poruch* (IIP), která je vztažena k velikosti obvodu. Velikost obvodu zde reprezentujeme počtem bitů bitstreamu, do kterých násobné poruchy injektujeme. Výsledná jednotka je tedy $injekce/s/bit$, tj. počet injekcí během jedné sekundy na jeden bit bitstreamu. Pro naše experimenty jsme zvolili IIP rovnu $2,6e$-6. Tuto volbu jsme učinili na základě experimentu s jednotkou *quintuple*. Kritériem byla výše střední doby do poruchy, tj. *Mean Time To Failure* (MTTF), a procentuální zastoupení poruchových běhů. Z důvodu rozlišení pozorovaných veličin bylo pro tuto největší z jednotek třeba volit kompromis mezi nejvyšším MTTF a nejnižší procent. chybovostí běhů.

A. Vliv míry redundance a majoritní funkce

Pro každý RDT jsme vytvořili ŘJ robota, v jejímž popise jsou všechny proměnné ošetřeny daným RDT. Počet verifikačních běhů jsme stanovili pro každou z jednotek u na $0.1 \times bity\_LUT_u$, tak, aby rozsáhlejší jednotka byla testována důkladněji. Injekce poruch probíhaly náhodně do všech bitů LUT jednotek dle *uniformního* rozdělení a dle zvolené IPP = $2.0e$-6 inj/s/bit. Počty běhů, testovaných bitů, výsledky procent. selhání a MTTF každé jednotky uvádí Tabulka I.

Tabulka I: Přehled parametrů testů společně s výsledky procent. selhání běhů a MTTF.

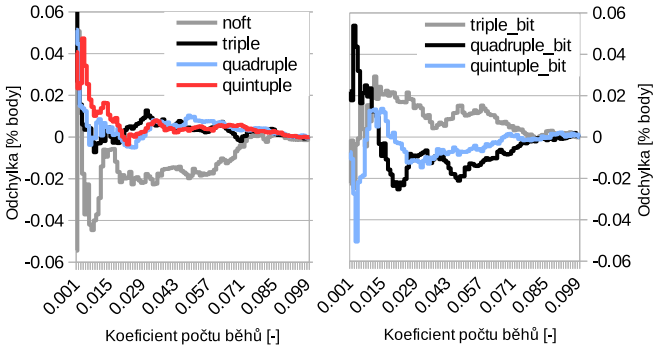
RDT aplikovaný na ŘJ robota		Parametry testů: bity LUT [b]	Počet běhů [-]	Intenz. poruch [inj/s/bit]	Obdržené výsledky: Selhané běhy[%]	MTTF [s]
noft (bez RDT)		19392	1940	2e-6	21.24	131.05
Slovní maj.	triple	48704	4871	2e-6	18.99	139.40
	quadruple	73216	7322	2e-6	20.88	138.14
	quintuple	122880	12288	2e-6	21.34	141.06
Bitová maj.	triple_bit	24480	2448	2e-6	18.91	128.68
	quadruple_bit	26784	2679	2e-6	20.87	132.88
	quintuple_bit	37632	3764	2e-6	25.05	130.08

Můžeme vidět, že aplikace *triple* snížila počet selhání, což je očekávaný stav. Pro *quadruple* se počet selhání snížil oproti nezabezpečené variantě, ale oproti *triple* došlo ke zhoršení. Předpokládáme, že tento fenomén je způsoben tím, že 4MR zabírá více plochy, zatímco pro bezporuchovou funkčnost je vyžadována funkčnost tří jednotek (tj. majorita). Tento výsledek potvrzuje fakt, že sudý počet jednotek v nMR parametry ve skutečnosti zhoršuje. Toto naznačuje i MTTF, které je pro *triple* a *quadruple* téměř ekvivalentní. Nicméně, pro *quintuple* dochází ke zvýšení procentuálního počtu selhání. Vyšší MTTF, které je s tímto údajem v rozporu ale naznačuje, že se je toto měření pravděpodobně ovlivněno vyšším rozptylem hodnot Jednotka s *triple_bit* dosáhla nejlepšího výsledku procentuálního zastoupení selhaných běhů, tj. $18.91\,\%$. V kontrastu, MTTF se snížilo. Pro tento jev opět předpokládáme vliv rozptylu MTTF. Pro *quadruple_bit* můžeme pozorovat obdobný fenomén, jako u *quadruple*. Pro *quintuple_bit* se procentuální zastoupení chybných běhů zvýšilo a MTTF snížilo. V tomto případě nepřinesla bitová majoritní funkce zlepšení, nicméně pokud zvážíme spotřebované zdroje (a to i u všech ostatních jednotek), jedná se stále o výrazně účinnější variantu při spotřebované ploše na čipu oproti slovní majoritě.

B. Počet verifikačních běhů

Protože jsme počet běhů zvolili čistě empiricky na základě předchozích zkušeností, uvádíme zde ještě retrospektivní vyhodnocení. Předpokládejme, že vyšší počet verifikačních běhů vede na přesnější výsledek a rovněž, že aritmetický průměr těchto výsledků konverguje k ideální hodnotě. Za ideální hodnoty tedy prohlasme původně vypočtené hodnoty procentuálního selhání jednotek. Za pomocí detailních záznamů pak následně simulujeme stav ohodnocení pro případ, že bychom jako počet verifikačních běhů volili koeficienty počtu běhů od 0.001 do $0.099 \times bity\_LUT_u$, namísto původních $0.1 \times bity\_LUT_u$. Referenční hodnota byla odečtena od hodnot obdržených výše popsaným způsobem. Takto jsme obdrželi graf na Obrázku 2.

Jak je možno pozorovat, od koeficientu 0.073 téměř nedochází ke změnám výsledků. Usuzujeme tedy, že počet běhů $0.1 \times bity\_LUT_u$ je pro naše ohodnocení obvodů dostačující.



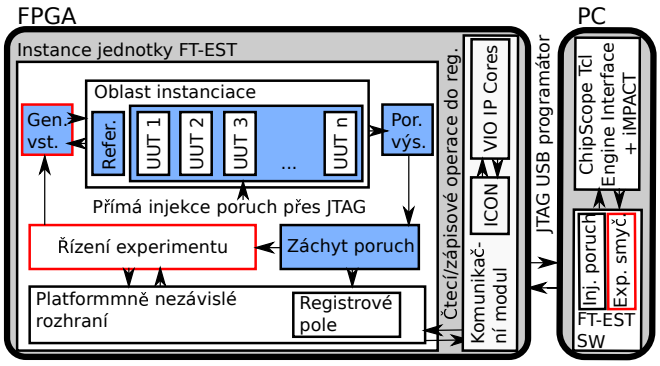
Obrázek 2: Zpětně vypočtené odchylky v procentních bodech selhaných běhů v závislosti na počtu testovaných běhů.

VI. Odhad spolehlivosti: Aktuální výsledky

Pro návrh systémů OPP je nutné mít možnost relativně rychlé verifikace obvodu. Často se stává, že aplikovaná metoda nevede správným směrem, jakým by se vývoj měl ubírat. Z tohoto důvodu je žádoucí možnost obvod otestovat s nižší přesností výsledku s cílem urychlit odhad. Závěrečná verifikace je poté provedena s vyšší přesností, případně s využitím odlišného verifikačního nástroje.

A. Struktura nástroje FT-EST

Pro tyto účely byl během posledního roku vyvinut nástroj, který umožňuje akceleraci odhadu spolehlivosti. Nástroj jsme nazvali Fault Tolerance ESTimation (FT-EST) framework. Výsledky z této části byly publikovány v [4]. Akcelerace spočívá mj. v možnosti autonomního testu, generování stimulů v rámci FPGA a možnosti paralelního spouštění testů. Míra akcelerace je pak dána velikostí testovaného obvodu. Nástroj zohledňuje možnost spouštět testy automatizovaně bez nutnosti zásahu návrháře, nicméně možnost modifikace parametrů testu je ponechána. Struktura nástroje je shrnuta na Obrázku 3.



Obrázek 3: Zjednodušená architektura nástroje FT-EST; části zvýrazněné modře jsou dynamicky generovány; části vyznačené červeně, které určují význam experimentu, volí vývojář.

Jednotka *generování vstupů* generuje stimuly do *oblasti instanciace*. V oblasti instanciace se nachází samotné instance testované jednotky, z angl. *Unit Under Test* (UUT) a také jednu instanci referenční jednotky, jež není předmětem injektáže poruch. Odtud jdou výstupní porty UUT do jednotky *porovnání vstupů* a následně jednotky *záchytu poruch*. Jednotka *řízení experimentu* zajišťuje řízení průběhu experimentu v HW části. Oddělený *komunikační modul* umožňuje snazší přenos frameworku na jiné platformy. SW část obsahuje opět komunikační modul a dříve prezentovaný injektor poruch [15], který umožňuje specifikaci injektáže do konkrétního bloku na FPGA. Výsledky o tom, který bit je pro funkčnost kritický jsou poté zaznamenávány do záznamového souboru na PC.

B. Vliv aplikace RDT na jednotlivé operace

Rozhodli jsme se využít FT-EST k odhalení slabin metody RDT. Pro tyto účely jsme zvolili tři jednoduché algoritmy. Algoritmy realizují součet dvou 16 bitových ne-znaménkových čísel a odečet dvou znaménkových 16 bitových čísel, přičemž výsledek je reprezentován rovněž na 16 bitech. Dále realizaci výpočtu CRC-8 s výstupem 8 bitů a vstupní šířkou dat 32 bitů. Na každý z těchto popisů jsme aplikovali metodu RDT a to na všechny proměnné, které byly v popisu využity vč. těch, které slouží jako vstupní parametry (tj. po syntéze jako rozhraní obvodu). Během vyhodnocení jsme k obvodům přidali ještě externí hlasovací člen, jenž byl implementován ve VHDL. Pro férové srovnání byla injektáž poruch prováděna rovněž do externího hlasovacího členu. Syntézu jsme provedli i pro obvody bez RDT. Porovnání výsledků je v Tabulce II.

Tabulka II: Využité a citlivé bity vč. jejich procent. zastoupení.

Algoritmus	metoda OPP	bity LUT [b]	Počet injekcí [-]	Počet poruch [-]	Citlivé bity [%]
Součet	bez (simplex)	4288 b	4288	890	20.76 %
Součet	TMR	8320 b	8320	225	2.70 %
Odečet	bez (simplex)	4288 b	4288	178	4.15 %
Odečet	TMR	8320 b	8320	278	3.34 %
CRC-8	bez (simplex)	4800 b	4800	1658	34.54 %
CRC-8	TMR	6592 b	6592	879	13.33 %

Výsledky naznačují obecnou funkčnost konceptu RDT, ale zároveň indikují místa, kde by mělo dojít ke zlepšení. Pro operaci odečtu došlo k procentuálnímu snížení citlivých bitů, ale z celkového pohledu je jejich počet navýšen, což není dobrý stav. Jeho řešení bude předmětem dalšího vývoje.

C. Vliv pokrytí na přesnost odhadu

V rámci experimentální činnosti s nástrojem FT-EST jsme vyhodnotili rovněž zrychlení odhadu vlivem neúplného pokrytí bitů na přesnost odhadu. Výsledky z Tabulky III ukazují, že pro zvolené obvody byl v případě 30% pokrytí poruch (tj. přibližně trojnásobného zrychlení odhadu) rozdíl v odhadech procent. zastoupení kritických bitů maximálně 3.6% bodů.

Tabulka III: Odchylka pro různé rychlosti odhadu dle pokrytí.

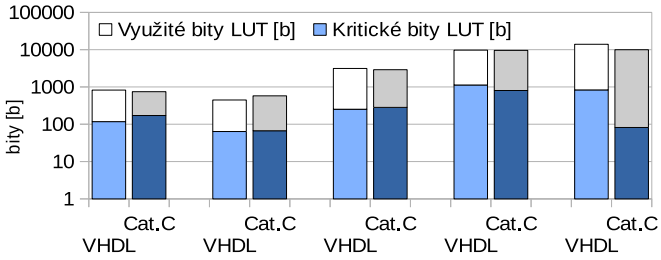
Pokrytí SEU [%]	Rozsah odchylky při odhadu [% body] Součet simplex	Součet TMR	Odečet simplex	Odečet TMR	CRC-8 simplex	CRC-8 TMR
60 %	1.63 – -1.63	0.46 – -0.40	0.70 – -0.89	0.63 – -0.46	1.71 – -1.94	1.1 – -0.97
30 %	2.57 – -2.47	0.98 – -0.78	1.91 – -1.20	0.91 – -1.1	3.38 – -3.64	1.99 – -2.46
10 %	6.06 – -5.36	1.74 – -1.50	2.61 – -2.52	1.71 – -1.9	6.29 – -6.21	4.26 – -3.78
5 %	11.0 – -9.6	2.58 – -1.98	4.71 – -3.69	3.15 – -2.62	9.63 – -9.54	5.78 – -5.14
1 %	16.6 – -16.1	6.91 – -2.7	12.2 – -4.15	8.68 – -3.34	21.7 – -19.96	18.5 – -11.8

Výsledky naznačují, že i tímto postupem je možno odhad akcelerovat a snížit tak čas potřebný k automatickému návrhu, resp. ve stejném čase prozkoumat více konfigurací a obdržet tak kvalitnější výsledek systému OPP.

D. Vliv použití HLS na spolehlivost

V publikaci [5] prezentujeme vliv použití HLS na spolehlivost syntetizovaného obvodu. Cílem experimentu bylo potvrzení předpokladu, že změna jazyka popisu výrazně neovlivní výslednou spolehlivost, pakliže porovnáváme systémy funkčně

ekvivalentní. Z testovací sady *ITC'99* [1] bylo vybráno 5 obvodů, jejichž VHDL implementace byla manuálně převedena do jazyka C++. Převod byl uskutečněn bez úmyslného vkládání optimalizací. Protože jsme záměrně vybrali implementačně nenáročné obvody, posun úrovně abstrakce popisu nebyl příliš patrný přímo z kódu, který odpovídal téměř 1:1 kódu VHDL. Výsledky byly syntetizovány pomocí nástroje Catapult C a Xilinx ISE. Původní VHDL varianty byly rovněž syntetizovány. Z výsledků zobrazených v grafu na Obrázku 4 plyne, že využití C++ pro popis nemělo výrazný vliv na měřené parametry.



Obrázek 4: Graf porovnání úrovně kritických bitů pro jednotky syntetizované z VHDL a z C++ pomocí HLS.

VII. Cíle disertační práce a závěr

Cílem disertační práce je navrhnout metodu pro automatizaci návrhu systémů OPP, pro jeho dosažení byly stanoveny tři hlavní podcíle: 1) vybudovat prostředky pro automatické vkládání redundance; 2) zvolit vhodnou variantu ohodnocení odolnosti; 3) navrhnout metodu automatické volby zabezpečení ve vztahu k vlastnostem dané komponenty (příp. části algoritmu) při zohlednění optimalizačních parametrů.

Pro podcíl 1) byly navrženy a implementovány prostředky pro selektivní vkládání OPP do algoritmu zapsaného v jazyce C++, jenž jsme nastínili v [9]. Prostředky využívají možnosti moderních programovacích jazyků vytvářet, případně modifikovat, definice datových typů a s nimi spojených operací. Pro náš výzkum jsme prostředky implementovali v C++. Dále jsme ověřili funkčnost představené metody rovněž ve vztahu k nastavení zvolených parametrů syntézy [8]. V publikaci [6] jsme ověřili možnost použití selektivního zabezpečení dílčích částí algoritmu k sestavení koeficientu *důležitosti* konkrétních instancí operací v algoritmu. Dále jsme se zabývali rozšířením o nové RDT, jež využívaly různé úrovně redundance a odlišný typ majoritní funkce [7]. V publikaci [5] jsme zkoumali vliv použití HLS a tedy i odlišného jazyka popisu na spolehlivost syntetizovaného obvodu. Výsledky naznačují velmi dobrou použitelnost HLS a rovněž nezávislost dosažené spolehlivosti na volbě jazyka vyšší úrovně abstrakce.

Pro účely podcíle 2) byl vyvinut framework FT-EST pro odhad během vývoje, jenž je popsán v [4]. V téže publikaci jsme prezentovali rovněž možnost snížení pokrytí poruch za účelem nadále až trojnásobné akcelerace odhadu (tj. bez započítání akcelerace dosažitelné použitím FT-EST) při minimálním vlivu na jeho přesnost.

V rámci podcíle 3) bude zkoumána možnost využití existujících algoritmů pro průzkum stavového prostoru s důrazem na minimalizaci počtu ohodnocení obvodů. Algoritmy vyberou z dostupných metod vkládání redundance (např. TMR, 5MR, *kódy oprav chyb*) a provedou ohodnocení takto získané pracovní verze obvodu. Mezi rozhodující parametry zprvu zařadíme samotnou spolehlivost při statickém omezení implementačního prostoru. S využitím konfigurovatelnosti FT-EST bude možno přiřadit různým typům výstupních dat (příp. operačních transakcí) odlišnou důležitost. V další fázi by mohlo být jistě zajímavé zakomponovat další možnosti omezení, např. možnost omezení spotřeby elektrické energie. V rámci bodu 3) bychom dále rádi realizovali metodu vkládání OPP pro některý konvenční jazyk popisu HW realizace (pravděpodobně VHDL) a i na tomto jazyce ukázali možnosti automatické volby OPP.

Poděkování

Tato práce byla podporována Ministerstvem školství, mládeže a tělovýchovy z Národního programu udržitelnosti (NPU II), projektu IT4Innovations excellence in science – LQ1602, projektem řešeným na VUT v Brně pod číslem FIT-S-17-3994 a projektem JU ECSEL SECREDAS (Product Security for Cross Domain Reliable Dependable Automated Systems), grantová dohoda č. 783119.

Reference

[1] Corno, F.; Reorda, M.; Squillero, G.: RT-level ITC'99 benchmarks and first ATPG results. *Design Test of Computers, IEEE*, ročník 17, č. 3, červenec 2000: s. 44–53, ISSN 0740-7475, doi:10.1109/54.867894.

[2] Fibich, C.; Horauer, M.; Obermaisser, R.: HLshield: a reliability enhancement framework for high-level synthesis. *2017 12th IEEE International Symposium on Industrial Embedded Systems (SIES)*, červen 2017, s. 1–10, doi:10.1109/SIES.2017.7993378.

[3] Gerkey, B.; Vaughan, R.; Howard, A.; aj.: The Player/Stage Project. *přístupné z http://playerstage.sourceforge.net*, 2003.

[4] Lojda, J.; Podivinsky, J.; Cekan, O.; aj.: FT-EST Framework: Reliability Estimation for the Purposes of Fault-Tolerant System Design Automation. *Článek přijat k prezentaci na: Digital System Design (DSD), 2018, 21st Euromicro Conference.*

[5] Lojda, J.; Podivinsky, J.; Kotasek, Z.: Fault Tolerance Properties of Systems Generated with the Use of High-Level Synthesis. *Článek přijat k prezentaci na: 16th IEEE East-West Design & Test Symposium (EWDTS-2018).*

[6] Lojda, J.; Podivinsky, J.; Kotasek, Z.: Redundant Data Types and Operations in HLS and their Use for a Robot Controller Unit Fault Tolerance Evaluation. *2017 IEEE East-West Design & Test Symposium (EWDTS)*, září 2017, s. 359–364, doi:10.1109/EWDTS.2017.8110127.

[7] Lojda, J.; Podivinsky, J.; Kotasek, Z.; aj.: Majority Type and Redundancy Level Influences on Redundant Data Types Approach for HLS. *Článek přijat k prezentaci na: 16th Biennial Baltic Electronics Conference (BEC), 2018.*

[8] Lojda, J.; Podivinsky, J.; Kotasek, Z.; aj.: Data Types and Operations Modifications: A Practical Approach to Fault Tolerance in HLS. *2017 IEEE East-West Design & Test Symposium (EWDTS)*, září 2017, s. 273–278, doi:10.1109/EWDTS.2017.8110113.

[9] Lojda, J.; Podivínský, J.; Krčma, M.; aj.: HLS-based Fault Tolerance Approach for SRAM-based FPGAs. *Proceedings of the 2016 International Conference on Field Programmable Technology*, IEEE Computer Society, 2016, ISBN 978-1-5090-5602-6, s. 297–298.

[10] López-Ongil, C.; Garcia-Valderas, M.; Portela-García, M.; aj.: Autonomous Fault Emulation: A New FPGA-based Acceleration System for Hardness Evaluation. *IEEE Transactions on Nuclear Science*, ročník 54, č. 1, 2007: s. 252–261.

[11] Nidhin, T.; Bhattacharyya, A.; Behera, R.; aj.: Verification of Fault Tolerant Techniques in Finite State Machines Using Simulation based Fault Injection Targeted at FPGAs for SEU Mitigation. *2017 4th International Conference on Electronics and Communication Systems (ICECS)*, IEEE, 2017, s. 153–157.

[12] Podivinsky, J.; Cekan, O.; Lojda, J.; aj.: Verification of Robot Controller for Evaluating Impacts of Faults in Electro-mechanical Systems. *2016 19th Euromicro Conference on Digital System Design (DSD)*, IEEE, 2016, s. 487–494.

[13] Rudrakshi, S.; Midasala, V.; Bhavanam, S.: Implementation of FPGA based Fault Injection Tool (FITO) for Testing Fault Tolerant Designs. *IACSIT International Journal of Engineering and Technology*, ročník 4, č. 5, 2012: s. 522–526.

[14] dos Santos, A. F.; Tambara, L. A.; Kastensmidt, F. L.: Evaluating the Efficiency of using TMR in the High-level Synthesis Design Flow of SRAM-based FPGA. *2017 IEEE 8th Latin American Symposium on Circuits Systems (LASCAS)*, únor 2017, s. 1–4, doi: 10.1109/LASCAS.2017.7948064.

[15] Straka, M.; Kastil, J.; Kotasek, Z.: SEU Simulation Framework for Xilinx FPGA: First Step Towards Testing Fault Tolerant Systems. *14th EUROMICRO Conference on Digital System Design*, IEEE Computer Society, 2011, ISBN 978-0-7695-4494-6, s. 223–230.

Zpracování hyperspektrálních dat pomocí neuronových sítí

Jiří Čech
3. ročník, prezenční studium
Školitel: Martin Rozkovec

Technická Univerzita v Liberci
Studentská 1402/2, 461 17 Liberec, ČR
jiri.cech@tul.cz

***Abstrakt*—Ve svém studiu jsem se zaměřil na využití neuronových sítí pro vyhodnocování hyperspektrálních dat, která získávám z vytvořené hyperspektrální kamery v rámci projektu robustního detekčního systému (RODES). Pro plánovanou implementaci vyhodnocování v programovatelném hradlovém poli (FPGA) kamery je vhodné využít konvoluční neuronové sítě (CNN), které umožňují extrémní paralelizaci výpočtu a vyžadují nižší datové přenosy. Navrhuji jednotlivé struktury CNN a metody, které ověřuji na několika rozdílných vzorcích s cílem nalézt snadno implementovatelnou jednoduchou strukturu.**

Klíčová slova—Konvoluční neuronové sítě, Hyperspektrální zobrazování, Dlouhovlná infračervená kamera, FPGA

I. Úvod

Pro bezdotykovou detekci různých látek na delší vzdálenosti se využívají kamery se speciální optikou, které dokáží snímat scénu v různých vlnových délkách. Podle počtu detekovaných vlnových délek je dělíme na Multispektrální (cca 10) nebo Hyperspektrální (cca 100 a víc). Podle použité optiky, optických materiálů a detekčního senzoru může kamera operovat v některé části elektromagnetického spektra: Ultrafialové, Viditelné, Blízké nebo Vzdálené infračervené.

Systém RODES pracuje v dlouhých infračervených (LWIR) vlnových délkách. Využívá levný nechlazený bolometrický senzor (FPA)[1] osazený v infračervené kameře (IRCA) se speciálním optickým systémem. Jeho rozsah spektrální citlivosti je od 7,5 do 11,5 µm rozprostřené na 300 z celkových 480 pixelů FPA. Takovýto spektrální rozklad je aplikován na sloupec scény s rozlišením 640 pixelů, který je po scéně posouván otočným zrcadlem. Data z FPA se pro laboratorní účely posílají přes gigabit ethernet do počítače. V něm se jednotlivé snímky skládají do tzv. Hyperspektrální kostky, což je datová struktura se kterou pracují vyhodnocovací algoritmy [2].

Centrální procesní jednotkou systému RODES je programovatelný modul APSoC se Zynq 7020 [3], který se skládá z vícejádrového SoC (systém na čipu, 2x 32bit ARM Cortex A9 a 1GB DDR3) a programovatelné logiky, která vychází z rodiny Artix-7 (nízkonákladové produkty 7 série Xilinx FPGA s nízkou spotřebou).

Neuronové sítě díky rostoucímu výpočetnímu výkonu počítačů mají stále širší možnosti uplatnění. Umožňují řešit i náročné problémy jako jsou vyhodnocení obrazu či zvuku, odstranění šumu, zvýšení kvality obrazu. Dále pak dokáží vyhledávat informace podle klíčových slov, autonomně řídit vozidlo a jiné. Tyto problémy zpravidla vedou na rozsáhlé a komplexní struktury neuronových sítí, které pro výpočet v reálném čase vyžadují extrémní výkon.

Trénování neuronových sítí lze provádět v mnoha prostředích např. Matlab, a v mnoha jazycích např. C++, Python, Lua. Mezi nejrozšířenější prostředí patří Caffe, Theano a Torch [4]. U nás je rozšířené prostředí Torch [5], které se jednoduše programuje jazykem Lua a dosahuje vysokých rychlostí výpočtu na GPU s modulem CUNN. Výpočty probíhají na stolním PC s operačním systémem Linux. Ve finální fázi projektu se pravděpodobně převedou už natrénované sítě do prostředí Caffe a pomocí dostupných nástrojů reVISION [6] se implementují do FPGA.

Neuronová síť je tvořena z několika vrstev, z nichž první vrstva je vstupní a poslední je výstupní. Jim odpovídá velikost vstupního a výstupního vektoru. Mezi nimi je množství tzv. skrytých vrstev proložených přechodovou funkcí. Nejčastější typ vrstvy je Lineární, dalšími typy vrstev jsou různé matematické operace jako: přičítání, násobení, výběr maxima, prahování a jiné. Přechodová funkce bývá nejčastěji: hyperbolická funkce (sinh, tanh) nebo Rectified Linear Unit (ReLU).

Pro klasifikaci do *n* výstupních tříd je vhodná kriteriální funkce ClassNLLCriterion, která ovšem potřebuje přidání vrstvy LogSoftMax. Ta transformuje výstup sítě na pravděpodobnost v logaritmickém měřítku. Pokud nechceme do struktury sítě přidávat další vrstvu, existuje rozšířená funkce CrossEntropyCriterion, které transformaci LogSoftMax provádí interně. Při trénování je kritériem porovnáván aktuální a očekávaný výstup pro daný vstup, kterým v tomto případě je vektor vah k jednotlivým třídám.

Pro trénování neuronových sítí je zapotřebí velký soubor dat, a pro jejich testování další jiný soubor dat. Pro urychlení výpočtu se trénování neprovádí po jednotlivých vstupních vektorech ale ve větších dávkách, kde až po jejich vypočtení se aktualizují váhy sítě. Trénování se několikrát opakuje na stejném souboru dat a poté se otestuje „úspěšnost“ tj. průměr podílů úspěšných

klasifikací jednotlivých tříd. Tento cyklus se opakuje, dokud není dosaženo dostatečné úspěšnosti nebo daného počtu cyklů.

Zvláštním případem neuronových sítí jsou již zmíněné CNN [7, 8]. Tyto sítě obsahují konvoluční vrstvy, které provádí konvoluci s jednorozměrným (Temporal), dvourozměrným (Spatial) nebo třírozměrným (Volumetric) jádrem. Bývají nejvýše tři konvoluční vrstvy za sebou a poté následuje vrstva pro podvzorkování, většinou výběr maxima (MaxPooling). Posledními vrstvami je NN síť, jejíž struktura je zpravidla výrazně menší než při řešení čistě pomocí hlubokých NN. Konvoluční vrstva může mít více výstupů, tj. více konvolučních jader. Konvoluce nemusí být prováděná souvisle s celou vstupní maticí, ale lze posouvat o *n* pozic.

Velké úspěchy mají CNN zejména při detekci objektů v obraze. Využívají se i rozsáhlejší paralelní struktury, binarizované váhy, rekurentní propojení vrstev nebo společné váhy mezi vrstvami. Struktura CNN nejen že umožňuje vysoké míry paralelismu, ale díky principu výpočtu konvoluce za pomocí Winograd algoritmu [8], lze snížit počet potřebných operací násobení a optimalizovat tak výpočet na FPGA.

II. Motivace

Účastním se na probíhajícím projektu vývoje systému RODES firmou APPLIC s.r.o. ve spolupráci s Technickou Univerzitou v Liberci a s výzkumným centrem TOPTEC Ústavu fyziky plazmatu AVČR, v.v.i.. Systém by měl umět detekovat různé těkavé látky a výbušné plyny. Využívá levné, moderní a prostorově nenáročné komponenty, proto je cenově dostupný a snadno přenositelný.

Běžné metody vyhodnocování hyperspektrálních dat vyžadují rychlé připojení ke kameře a zpracování na výkonném počítači, často doplněném o specializované akcelerátory. Naše řešení plánuje integrovat zpracování obrazu přímo do kamery a jejího řídícího modulu. Navázáním paralelního zpracování dat přímo na jejich výčet ze senzoru odpadá zpoždění dané záznamem, předzpracováním a přenosem dat do PC.

Laboratorně získané vzorky se od reálných měření liší v různorodosti pozadí a intenzitě. Porovnávám navržené sítě a metody na několika různých typech vzorků: pomocí systému RODES naměřený primitivní průběh filtrů (Filtry), ideální průběh testovaných plynů (Chem) vůči černému tělesu [9] a dva online dostupné reálné referenční hyperspektrální satelitní záznamy (IndiaPines, PaviaU) [10].

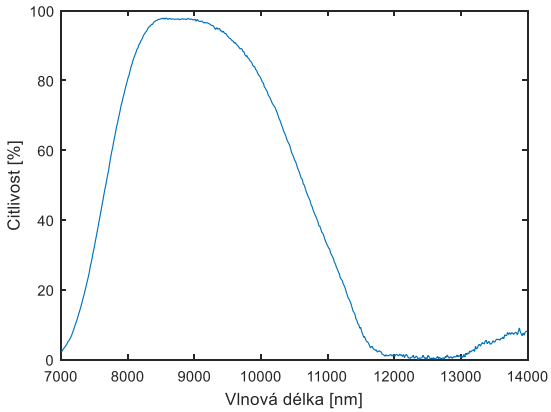
Cílem porovnávání sítí na různorodých vzorcích je otestování, zda daná struktura sítě nevyhovuje pouze ideálním, početně omezeným laboratorním vzorkům, ale je vhodná i pro předpokládané reálné využití. Limitujícím faktorem je spektrální rozlišení vzorku, počet a podobnost jednotlivých tříd a zahrnutí okolí daného pixelu. Sítě naučené na ideálních průbězích z laboratorního měření, lze později dotrénovat na datech získaných z polních měření.

III. Měření

Pro naměření laboratorních vzorků k testování jsme nejprve nastavili pracovní rozsah kamery [11]. Ten je závislý nejen na napětí jednotlivých vstupů senzoru, ale i na jeho teplotě. Aby bylo možné stabilizovat teplotu kamery na libovolné hodnotě 10-60 °C byl k senzoru přidán externě napájený Peltierův článek.

A. Frekvenční citlivost

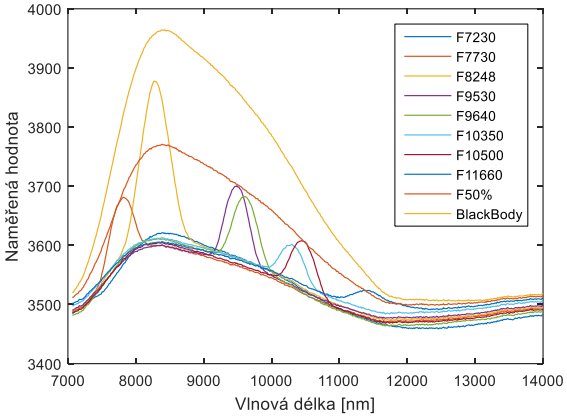
Frekvenční citlivost hyperspektrální kamery získáme jako poměr záznamu černého tělesa o dané teplotě a odpovídajícího průběhu daným Planckovým zákonem, viz Obrázek 1. Přesnost změřené charakteristiky je dána přesností černého tělesa (v teplotě a ve frekvenci) a vlivem šumu, který s klesajícím signálem roste.



Obrázek 1. Frekvenční citlivosti hyperspektrální kamery

B. Vzorek Filtry

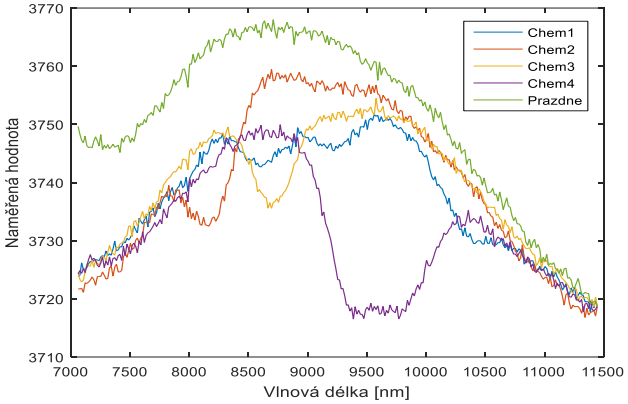
Primitivní průběhy filtrů jsou záznamy černého tělesa skrz sadu osmi úzkopásmových filtrů a polopropustného filtru pořízené hyperspektrální kamerou, viz Obrázek 2. Na průbězích je znatelný energetický vzestup odpovídající propustné frekvenci filtru. Znatelný je i zeslabený průběh podobný průběhu černého tělesa daný vlivem okolí. Jednotlivé průběhy se od sebe jasně lišší, tudíž jejich rozeznání by mělo být jednoduché.



Obrázek 2. Průběhy filtrů

C. Vzorek Chem

Obdobně byly pořízeny záznamy několika těkavých látek, viz Obrázek 3. (prozatím naměřené 4 látky) Místo filtrů byla použita průhledná nádoba naplněná měřenou látkou. Charakteristika byla oříznuta na 300 hodnot, kvůli nízké citlivosti systému na délky vyšší než 12000 nm, viz Obrázek 1. Zde je také snadné rozlišit jednotlivé průběhy, i když jsou zatíženy vyšším šumem a nižší citlivostí systému.

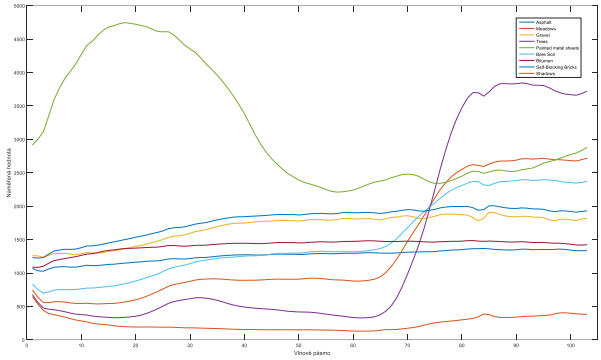


Obrázek 3. Průběhy chemických látek

D. Vzorek PaviaU a IndiaPines

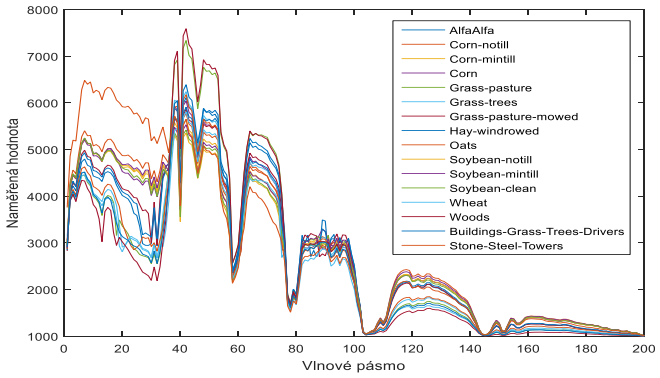
Vzorky jsou získané pomocí snímání povrchu země z letadel či satelitů, což je jedno z běžných použití hyperspektrálních kamer. Takové záznamy se oproti našim liší v kvalitě a vlnové délce. Jeden pixel odpovídá výrazně větší ploše a naměřená data se ořezávají o pásma, kde je voda či atmosféra neprůhledná.

Vzorek PaviaU [10] obsahuje snímek Univerzity Pavia pomocí sensoru ROSIS, má rozměry 610x610 pixelů a 103 vlnových pásem a obsahuje 9 různých tříd, viz Obrázek 4. Průběhy jednotlivých tříd jsou až na výjimky snadno rozlišitelné neměly by být výsledky o tolik horší, než u předchozích dat.



Obrázek 4. Průběhy vzorku PaviaU

Vzorek IndiaPines [10] obsahuje snímek polí získané pomocí senzoru AVIRIS, má rozměry 145x145 pixelů a 200 vlnových pásem a obsahuje 16 různých tříd, viz Obrázek 5.



Obrázek 5. Průběhy vzorku IndiaPines

IV. Vyhodnocení

Celý komplexní systém trénování byl ověřován na trénování klasických (NN) a hlubokých (DNN) neuronových sítí. Z jednotlivých vzorků se náhodně vybrali trénovací (5 %) a testovací (30 %) data. Zbytek dat byl použit pro výsledné otestování sítě. V Tabulce I. jsou vybrané výsledky pro NN s vnitřními lineárními vrstvami [vrstva1][vrstva2][vrstva3] pro jednotlivé vzorky, kde vstupem je záznam spektra z daného pixelu.

TABULKA I. Výsledky NN a DNN sítí

Vzorek		Filtry	Chem	IndiaPines	PaviaU
Síť	***Velikost sítě***	***Úspěšnost [%]***			
Model1L1	[0]	85,9	**96,0**	38,2	74,3
Model1L2	[5000]	92,7	95,8	57,0	83,7
Model2L1	[10][10]	88,9	91,1	39,2	81,2
Model2L2	[5000][5000]	**93,5**	94,2	**64,7**	**85,9**
Model3L1	[10][10][10]	86,9	81,3	39,278	76,0

Pro zvýšení kvality rozpoznání byl použit jako vstup do NN vektor složený i z okolních pixelů, naskládaných za sebe. Výsledky pro vstup 3x3 pixely je v Tabulce II. a pro vstup 7x7 pixelů v Tabulce III.

TABULKA II. Výsledky NN a DNN sítí pro okolí 3x3

Vzorek		Filtry	Chem	IndiaPines	PaviaU
Síť	***Velikost sítě***	***Úspěšnost [%]***			
Model1L1	[0]	93,5	99,9	12,5	88,0
Model1L2	[5000]	95,3	99,9	62,9	90,8
Model2L1	[10][10]	64,6	75,9	36,9	86,4
Model2L2	[5000][5000]	**96,0**	**99,9**	**66,7**	**91,6**
Model3L1	[10][10][10]	88,3	77,3	43,3	88,2

TABULKA III. Výsledky NN a DNN sítí pro okolí 7x7

Vzorek		Filtry	Chem	IndiaPines	PaviaU
Síť	***Velikost sítě***	***Úspěšnost [%]***			
Model1L1	[0]	**94,0**	**83,6**	**61,8**	86,7
Model1L2	[5000]	10,0	20,0	6,3	23, 2
Model2L1	[10][10]	11,4	21,0	12,5	87,1
Model2L2	[5000][5000]	35,4	23,4	25,0	88,1
Model3L1	[10][10][10]	38,5	56,5	29,8	**89,3**

Na stejná vstupní data jako pro NN byla aplikována jednorozměrná konvoluční vrstva s rozdílným počtem jader, velikostí jader a posunem s jednoduchou výstupní vrstvou. Vybrané výsledky jsou v Tabulce IV. a pro vstupy s okolím 3x3 v Tabulce V. Velikost sítě popisuje nastavení konvoluční vrstvy [počet jader, velikost jádra, posouvání jádra].

TABULKA IV. VÝSLEDKY CNN SÍTÍ

Vzorek		Filtry	Chem	IndiaPines	PaviaU
Síť	***Velikost sítě***	***Úspěšnost [%]***			
ModelC1	[5,10,10]	**91,6**	91,6	53,0	80,8
ModelC2	[5,20,20]	89,9	91,0	42,4	**81,8**
ModelC3	[5,30,30]	88,9	92,3	**54,1**	80,1
ModelC4	[10,10,10]	88,9	93,1	51,4	81,1
ModelC5	[10,30,30]	89,8	**93,8**	41,5	81,5

TABULKA V. VÝSLEDKY CNN SÍTÍ PRO OKOLÍ 3X3

Vzorek		Filtry	Chem	IndiaPines	PaviaU
Síť	***Velikost sítě***	***Úspěšnost [%]***			
ModelC1	[5,10,10]	93,6	**99,9**	**63,0**	90,1
ModelC2	[5,20,20]	92,4	99,3	59,0	87,0
ModelC3	[5,30,30]	94,1	67,4	60,9	87,4
ModelC4	[10,10,10]	**94,8**	99,9	51,6	**90,7**
ModelC5	[10,30,30]	94,0	68,4	60,4	89,6

V. CÍLE

Tímto měřením došlo k ověření funkčnosti testovací platformy, která trénuje sítě různých struktur na prezentovaných vzorcích. Různorodost jednotlivých vzorků umožňuje porovnání navržených struktur a metod pro vhodnost detekce podobných tříd, vyššího počtu tříd či různého spektrálního rozlišení.

Pomocí laboratorních měření zjistit a ověřit vlastnosti kamery. Vytvořit kalibrační matici pro převod naměřených hodnot na fyzikální jednotky a porovnat s databázovými vzorky.

Navrhnout a otestovat různé NN pro „čistá“ data z kamery po korekci a pro data bez korekce. Navrhnout a otestovat sériové i paralelní struktury s využitím vrstev s binárními vahami. Otestovat odolnost proti šumu a změně teploty kamery.

Navrhnout navázání procesu výpočtu dané sítě na proces sestavování hyperspektrální kostky a následného vytvoření vyhodnoceného obrazu. Upravit vybrané struktury pro výpočet na dostupné FPGA platformě (plně využít dostupných násobiček a ostatních zdrojů)

VI. ZÁVĚR

Byly porovnány čtyři vzorky hyperspektrálních kostek s rozdílným počtem klasifikovaných tříd (Filtry 10 a PaviaU 9, Chem 4 a IndiaPines 16). Při porovnání klasifikací pomocí NN se nejlépe osvědčila struktura Model2L2 s dvojicí vnitřních vrstev po 5000 neuronech, ve které 3 ze 4 vzorků dosáhly nejvyšší úspěšnosti. Nejlépe byl rozpoznán vzorek Chem a nejhůře IndiaPines, což přisuzuji rozdílnému počtu tříd.

Poté bylo testováno, jak zahrnutí okolí pixelu vylepší úspěšnost rozpoznání. Při zahrnutí okolí pixelu 3x3 se zlepšila úspěšnost v průměru o 3 %, přičemž všechny vzorky dosáhly maxima ve stejné již zmíněné struktuře Model2L2. Při zahrnutí okolí 7x7 došlo jen u dvou vzorků ke zlepšení a průměrné zlepšení (zhoršení) je -2,8 % pro strukturu Model1L1 bez vnitřních vrstev. Na zhoršení úspěšnosti může mít vliv i nedostatečné množství trénovacích vzorků, kterých je s velikostí sítě potřeba značně více.

Využitím CNN se průměrná úspěšnost zhoršila o 4,7 % a struktura sítě s dosaženým maximem byla pro každý vzorek různá. S využitím CNN a okolím pixelu 3x3 se průměrná úspěšnosti oproti NN zlepšila o 2 %, což je pouze o 1 % méně než NN síť se stejným vstupem.

PODĚKOVÁNÍ

Tato práce byla podpořena Studentskou Grantovou Soutěží 2018 Technické Univerzity v Liberci. Dále byla podpořena firmou APPLIC s.r.o. a Regionálním centrem speciální optiky a optoelektronických systémů TOPTEC Ústavu fyziky plazmatu AVČR, v.v.i.

LITERATURA

[1] L. J. Tissot, P. Robert, A. Durand, S. Tinnes, E. Bercier, A. Crastes, “Status of uncooled infrared detector technology at ULIS,” France, Defence Science Journal, vol. 63, no. 6, pp. 545-549, 2013.

[2] F. Zhu, Y. Wang, B. Fan, G. Meng, Ch. Pan, “Effective Spectral Unmixing via Robust Representation and Learning-based Sparsity,“ CoRR, 2014, online <arxiv.org/abs/1409.0685>.

[3] Xilinx Inc., „Zynq-7000 All Programmable SoC,“ online <http://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html>, 2017.

[4] S. Bahrampour, N. Ramakrishnan, L. Schott, M. Shah, “Comparative Study of Deep Learning Software Frameworks,” arXiv:1511.06435v3 [cs.LG], 2016.

[5] R. Collobert, C. Farabet, K. Kavukcuoglu, A. Chintala, “Torch,” online <torch.ch, github.com/torch/nn, github.com/torch/cunn>, 2017.

[6] Xilinx Inc., “Responsive and Reconfigurable Vision Systems,” online <www.xilinx.com/products/design-tools/embedded-vision-zone.html>, 2018.

[7] A. Podili, C. Zhang, V. Prasanna, “Fast and efficient implementation of Convolutional Neural Networks on FPGA,” 2017 IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP), Seattle, WA, 2017, pp. 11-18. doi: 10.1109/ASAP.2017.7995253.

[8] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, A. Rabinovich, “Going deeper with convolutions,” Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 1, 2015.

[9] E. Theocharous, P. N. Fox, I. V. Sapritsky, N. S. Mekhontsev, P. S. Morozova, “Absolute measurements of black-body emitted radiance, Metrologia,” vol. 35, no. 4, pp. 549-554, 1998.

[10] L. Sun, „Datasets for classification,“ 2018, online <http://lesun.weebly.com/hyperspectral-data-set.html>.

[11] J. Čech, M. Rozkovec, „Selection of Ideal Operating Point for Infrared Camera System,“ unpublished, accepted but not printed

DNSSEC in the networks with a NAT64/DNS64

Martin Huněk
3. ročník, prezenční studium
Supervisor: Zdeněk Plíva

Technická univerzita v Liberci
Studentská 2, 461 17 Liberec 1, ČR
martin.hunek@tul.cz

***Abstract*—This paper describes the problems with using both DNSSEC (security extension to domain name system) validating DNS resolvers and NAT64/DNS64 transition mechanism. In this paper we also propose a solution how to solve the problem of such combination. The foreign (synthesized) AAAA record as well as the broken trust chain in such records in secure way which doesn't breach DNSSEC.**

As the DNSSEC requires uninterrupted trust chain from the root authority, all the way down to every signed DNS record or the signed record that the sub-zone is not signed (NSEC or NSEC3), the DNS64 fabricated AAAA record could not have such signature. This triggers an error in the DNSSEC validation so the client after the DNSSEC validating resolver does not receive such DNS record. This result in broken DNS system and every DNSSEC secured domain without AAAA record to every corresponding A record would be subjected to these failures.

A current widely used solution comes from RFC 7050 [1] with conjunction with RFC 6146 [2] and RFC 6147 [3]. In such case the end node will detect DNS64 by asking for well-known IPv4 only domain, if detected end node would disable DNSSEC validation. This solves previously mentioned problem of foreign AAAA record and such domain would be reachable. However this also brakes DNSSEC validation and it does not allow operator to control over the prefix preference.

Our proposed solution supplies the end node with secondary DNSSEC chain to validate DNS64 synthesized records from information already presented to the node by neighbor discovery or DHCPv6 protocol, in the way that network operator can have a control over the prefixes and DNS resolvers used by the end node for NAT64/DNS64 transition mechanism.

***Index Terms*—IPv6, NAT64, DNS64, DNSSEC.**

I. Introduction

This paper deals with conjunction of two technologies. One is the security extension to domain name system – DNSSEC [4], the second is a transition mechanism between internet protocol version 4 and version 6 – the NAT64 [2] and its integral part DNS64 [3].

The main problem of such conjunction is the DNS64 part of the transition mechanism. Due to its nature the DNS64 synthesize IPv6 (AAAA) record for domain name which has got only IPv4 (A) record, is effectively pointing the communication towards the network address translation node – the NAT64.

On the other hand the DNSSEC is preventing undetected manipulation to the zone which may get manipulated by synthesized AAAA records produced by DNS64. In other words these technologies are effectively working against each other. Usual way to handle this situation is to disable one of them, either loosing ability of communication between IPv4 and IPv6 nodes by disabling DNS64 or by loosing security aspects of a DNS by disabling DNSSEC validation.

II. Theoretical background

When the internet protocol version 6 has been designed, It has been decided that instead of just expanding IP address space by extending the IP header, entirely new protocol should be designed. This let to inability of IPv4 only node in communication directly with IPv6 node and vice versa. Due to this limitation, the tunneling and translation mechanisms has been invented.

One of the translation mechanisms is the NAT64/DNS64, which consists of two components. The first component is the NAT64, which stands for Network Address Translation IPv6 to IPv4. It basically does the same thing as the NAT44 or NAT [5] in short. It extracts the IP header and replaces it by new one. In this case the transformation is between two different protocols. The second part – DNS64 is responsible for pointing the end nodes to use NAT64 gateway. If the target does have only IPv4 (A) record in DNS, the DNS64 resolver synthesize an IPv6 (AAAA) record which point to network prefix used by NAT64. This effectively point end node to NAT64 and whole communication in the infrastructure of operator network would go through the IPv6 protocol (due to its priority over older IPv4). After the transition on the NAT64 L4, data would be transported over IPv4 to target IPv4 node. Vice versa, the data from target to end node would be transported over IPv4 to the NAT64 box to its IPv4 address and then the response would be translated back to IPv6 and send to the originating end node.

Because the NAT64/DNS64 is based on the modification of DNS responses - effectively working on the same schema as the Man in the Middle (MitM) attack, it opens some security vulnerabilities. These include Denial of Service (DoS), end node flooding and MitM attacks. To overcome this problem the DNSSEC must be used and for DNSSEC usage, the node must

know the trusted domain list. Standard does not specify the correct way how the trusted domain list should be determined, however it might use some of these sources:

- End user maintained list.
- ISP maintained list.
- Auto-configuration via SLAAC - DNSSL option
- Auto-configuration via DHCPv6 - option 24
- Auto-configuration via DHCPv4

III. Current solution

Current solution outlined by the RFC 7050 [1], use well-known domain "*ipv4only.arpa.*" which has got only two A records *192.0.0.170* and *192.0.0.171*. However when the end node asks the DNS64 enabled resolver, the response would be a IPv6 AAAA record pointing to NAT64 pool ending by hexadecimal representation of above mentioned addresses (*C000:AA* or *C000:AB*). By this way the end node knows, that network uses DNS64 and should use NAT64.

This also should trigger either DNSSEC enabled end node stub resolver or the DNSSEC enabled caching resolver to keep the "Checking Disabled" flag set to zero. This action informs the DNS64 resolver to synthesize AAAA record which otherwise would be enabled. So the IPv6 only nodes would not be able to access the IPv4 only nodes - they would not receive the AAAA record opining to the NAT64 box.

To overcame possible security vulnerabilities, introduced by this "legal" modification of DNS records. The RFC 7050 [1] came up with DNSSEC validation of provided NAT64 prefix. However method proposed by RFC 7050 [1] is quite complex in the sense of number of needed steps and phases and it also has got a lower manageability.

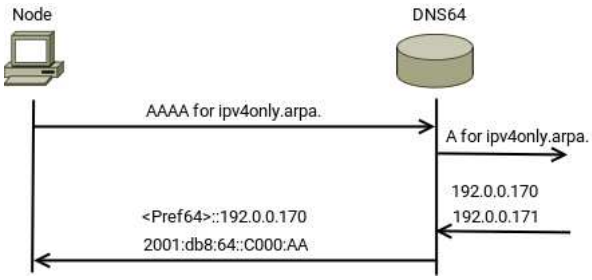


Figure 1. Detection of NAT64 prefix according to RFC 7050 [1]

First stage of NAT64/DNS64 discovery is the detection of NAT64 prefix. This is shown in the figure 1. In this figure it can be seen, that method proposed by current RFC does not require the node to have any specific knowledge about its network. This is the bright side of current approach, however the the well-known address has to be served in the arpa domain. The rest of this part of this process is quite straight forward. The DNS64 box translates the well-known address to the NAT64 prefix according to RFC 6147 [3]. The address received from the arpa domain had to match with the standard, otherwise record received by the node would have been ignored. By this step, the detection of NAT64 prefixes ends. The non-validating node can start to use received prefix for accessing IPv4 only nodes, however the DNSSEC would not be available and the end node could be subjected to the race condition type of DoS attack, MitM attack or can participate on flooding attack. To leverage DNSSEC for protection against such attack the end node must verify all of the received NAT64 prefixes.

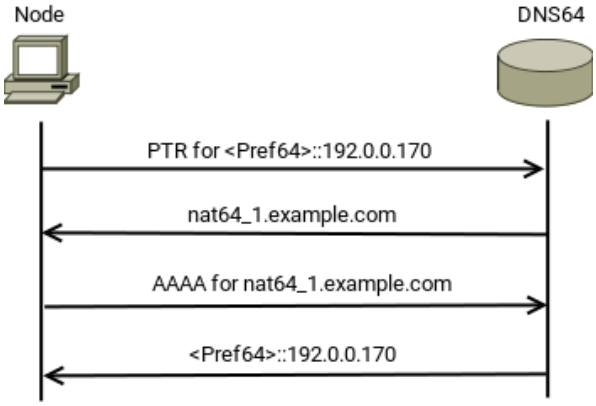


Figure 2. Validation of NAT64 prefix according to RFC 7050 [1]

The DNSSEC validating node continues in the process according to the figure 2. In the first step the node asks for the reverse record (PTR) for every detected prefix – well-known encoded address outside of well-known NAT64 prefix (that can't be validated by DNSSEC and it is supposed to be safe). When the node receives the PTR reply, it had to compare the received domain name with the list of trusted domains. This require the end node knowledge about its network prior to successful validation. The RFC 7050 [1] does not explicitly describe the way for the node how to acquire such a list but it is supposed to be either set by user/operator or by auto-configuration (SLAAC or DHCPv6).

If the domain in PTR record matches a domain from the trusted list, node have to ask for an AAAA record of every matching PTR. After that the node must validate every response and the address in an AAAA response must match the previously discovered ones. If everything checks out fine, the discovery has been successfully completed and validated prefix is marked as trusted.

IV. Proposed solution

In the contrast with the RFC 7050 [1] solution of this problem, we propose to reverse its logic for faster and simpler process of NAT64/DNS64 discovery. Supposing that the node has got the trusted domain list and that it would be able to get an "active" domain list by auto-configuration (e.g. SLAAC – DNS Search List or DHCPv6 option 24). Then the node can match those lists and start asking for proposed SRV records.

The node would have to ask first for SRV for *_nat64._ipv6* in trusted and active domains as it is shown in the figure 3. As a response, the node would receive a list of all prefixes with their priorities and weights. This is one of the major differences between proposed solution and the RFC 7050 [1], which does

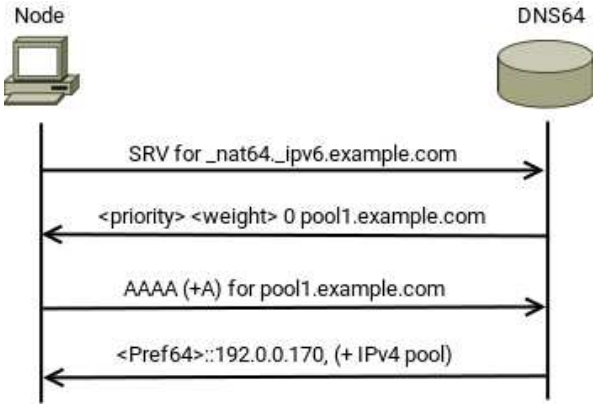


Figure 3. Proposed NAT64 SRV record and NAT64 discovery

not provide a way for network operator to specify NAT64 pool priorities. The number reserved for port number can then be optionally used for indicating pool sizes both for IPv6 and IPv4 or set to zero. When it is non-zero it must indicate the length of network masks for both protocols, IPv4 appended decadically after IPv6 (for example 09632 – meaning NAT64 IPv6 prefix has length 96 bits and it is translated to single IPv4 address). Then the node might additionally ask for A record of such pool, determining its public IPv4 address (or size of dynamic pool), if needed by application. Otherwise only AAAA record would be needed to determine NAT64 IPv6 pool.

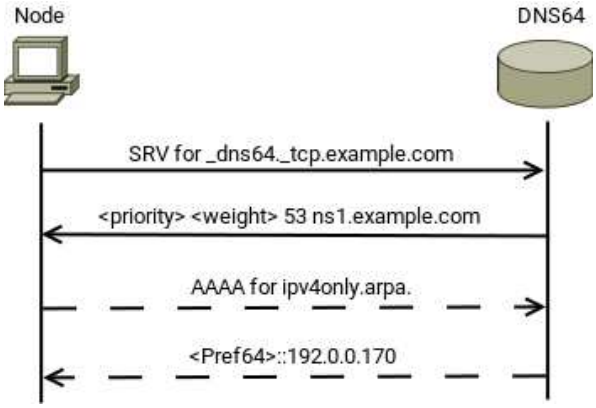


Figure 4. Proposed DNS64 SRV record and DNS64 discovery

In addition to the NAT64 SRV records, we also propose the DNS64 SRV record. This adds the possibility for network operator to run DNS64 service outside of the primary DNS infrastructure. This way the network operator might choose to provide DNS64 service only to this new standard capable nodes. By this way operator may effectively solve possible problems with old DNSSEC implementations. The process of the DNS64 server detection is shown in the figure 4.

The above mentioned figure also shows optional validation of DNS64 box function. However subsequent query and DNSSEC validation of PTR records is not necessary due to the signature of SRV record. If the DNS64 SRV record is not present the node should fall back to process outlined by the RFC 7050 [1].

Of course the whole proposed solution requires the same prerequisites as the RFC 7050 [1] does. The domain used for NAT64 prefix discovery must be DNSSEC secured and the DNSSEC validating node must ensure that all responses are valid. The PTR records should still match corresponding AAAA records, however it is not required by proposed method so there is also no requirement concerning DNSSEC deployment in reverse zone. Due to the absence of PTR record queries, there is no difference between processing network specific NAT64 prefixes and well-known NAT64 prefix. All of them are validated by signatures of SRV and AAAA records in the trusted domain. Secure transmission of trusted domains and security of routing NAT64 prefixes remains within responsibility of network operator and it is out of scope of proposed NAT64 prefix discovery method.

V. Conclusion

Our proposed method of NAT64 prefix discovery extends the current standard in use (the RFC 7050 [1]) by adding alternative means of secure prefix discovery. It utilizes the well-known IPv4 only record in ARPA domain as well as the well-known IP address and provides compatibility with above mentioned standard as a fallback option. Node, unaware of this method, would not be impacted by the proposed method. Network not utilizing the new method would make penalty to method aware nodes in total length of processing one SRV query and corresponding NODATA and NSEC(/NSEC3) response.

When implemented, our proposed method should be used before the method outlined in the RFC 7050 [1]. The first query should be for NAT64 SRV record, then the node may ask for DNS64 SRV record or continue with AAAA query for *ipv4only.arpa* for current resolver and fallback to SRV record method only if its current resolver does not provide DNS64 service.

Main contribution of proposed method lays in the added possibility of network operator to provide sorted list of NAT64 prefixes by their priority. This allows network operator controlled load balancing which is not possible with current standard. The same applies to DNS64 service record which also provides a possibility to run DNS64 service outside of main DNS infrastructure. This might help to overcome possibly broken implementations of current standard in DNSSEC validating nodes.

Further work should be focused on achieving standardization of our proposed method in IETF. Target would be a level of Best Current Practice (BCP) or Internet Standard. After the standardization process, consequent research might be based on method's impact. Impact might be evaluated both resource-wise and time-wise.

Acknowledgment

This paper has been supported by Student Grant Scheme (SGS 2018) at Technical University of Liberec.

References

[1] T. Savolainen, J. Korhonen, and D. Wing, "Discovery of the IPv6 Prefix Used for IPv6 Address Synthesis", RFC Editor, RFC 7050, Nov. 2013, pp. 1–22. DOI: 10.17487/RFC7050. [Online]. Available: https://www.rfc-editor.org/rfc/rfc7050.txt.

[2] M. Bagnulo, P. Matthews, and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC Editor, RFC 6146, Apr. 2011, pp. 1–45. DOI: 10.17487/RFC6146. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6146.txt.

[3] M. Bagnulo, A. Sullivan, P. Matthews, and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC Editor, RFC 6147, Apr. 2011, pp. 1–32. DOI: 10.17487/RFC6147. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6147.txt.

[4] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements", RFC Editor, RFC 4033, Mar. 2005, pp. 1–21. DOI: 10.17487/RFC4033. [Online]. Available: https://www.rfc-editor.org/rfc/rfc4033.txt.

[5] P. Srisuresh and K. B. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC Editor, RFC 3022, Jan. 2001, pp. 1–16. DOI: 10.17487/RFC3022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3022.txt.

Extrakcia parametrov EKV modelu MOS tranzistora pre návrh nízko-napäťových IO

Matej Rakús
3. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

Fakulta elektrotechniky a informatiky, Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava, SR
matej.rakus@stuba.sk

***Abstrakt*—Tento príspevok sa zaoberá extrakciou základných parametrov intrinzického modelu EKV2.6 z modelu BSIM3v3 (ktorý je priemyselným štandardom) v 130 nm CMOS technológii. Presnosť extrahovaných parametrov je následne zvýšená zjemnením na charakteristiky získané pomocou meraní a charakterizácie testovacích tranzistorov vyrobených v uvedenej technológii prostredníctvom experimentálneho čipu. Takto získaný EKV model potvrdzuje svoju výhodu pri návrhu analógových obvodov pomocou metodiky návrhu využívajúcej účinnosť prenosovej vodivosti MOS tranzistorov. 130 nm technológia bola zvolená z dôvodu jej stále častejšieho využitia v priemysle práve pri návrhu analógových obvodov.**

***Kľúčové slová*—BSIM, EKV, analógový návrh, koeficient inverzie, technologický prúd**

I. Úvod

Postupné zmenšovanie minimálneho rozmeru technológií (až do nm) skomplikovalo návrh integrovaných obvodov (IO) hlavne z dôvodu zvýšeného vplyvu sekundárnych parazitných javov [1]. Modely MOS tranzistorov BSIM3v3 a BSIM4, ktoré boli dlhodobo priemyselnými štandardmi, sú postupne nahradzované kompaktnejšími modelmi pre nanometrové technológie. Model BSIM6 je najnovšou generáciou BSIM modelov. Tento model je spojitý cez všetky oblasti inverzie tranzistora, avšak nevýhodou je jeho zložitosť, ktorá komplikuje jeho použitie pri výpočte kolektorových prúdov tranzistorov. Zaužívaná Vittoz-ová metóda výpočtu náboja, ktorú využíva model EKV2.6 je jednoduchšia a často uprednostňovaná analógovými návrhármi vďaka intuitívnejšiemu návrhu a kompaktnosti modelu. Model EKV2.6 je taktiež spojitý cez všetky oblasti inverzie MOS tranzistora [2]. Nevýhodou tohto modelu je však jeho obmedzené použitie v nanometrových technológiách, nakoľko zohľadňuje iba niektoré parazitné javy spojené s krátkym kanálom. Model EKV2.6 však stále ponúka výhody pre prvotné určenie rozmerov MOS tranzistorov pri návrhu vďaka jednoduchším analytickým rovniciam. Novšia generácia modelu EKV3.0 je vhodná pre návrh v technológiách do $65\ nm$, avšak s výrazne vyšším počtom parametrov [3].

II. Parametre modelu EKV2.6

Intrinzický model EKV2.6 obsahuje 18 základných parametrov, ktoré sú uvedené v tabuľke I [4]. Prvé štyri parametre sú viazané na technologický proces a sú extrahované zo špecifikácie technológie. Extrakcia ďalších jedenástich parametrov spolu s technologickým prúdom I_s je opísaná nižšie. Nakoniec zostávajú posledné tri parametre, ktoré nemajú konkrétnu metodiku extrakcie a sú len prispôsobovacie a zatiaľ im bude ponechaná pôvodná hodnota.

Tabuľka I
Základné parametre modelu EKV2.6

#	Param.	Opis
1	COX	Kapacita hradlového oxidu
2	XJ	Hĺbka vniku
3	DL	Korekcia dĺžky kanála
4	DW	Korekcia šírky kanála
5	$VT0$	Prahové napätie veľkého MOS tranzistora
6	$GAMMA$	Substrátový koeficient
7	PHI	Fermiho potenciál substrátu
8	KP	Vodivostný koeficient
9	$E0$	Koeficient redukcie pohyblivosti nábojov
10	$LAMBDA$	Koeficient modulácie dĺžky kanála
11	$UCRIT$	Kritické pozdĺžne pole
12	$LETA$	Koeficient efektu krátkeho kanála
13	$WETA$	Koeficient efektu úzkeho kanála
14	$Q0$	Maximálna hustota náboja reverzného efektu krátkeho kanála
15	LK	Charakteristická dĺžka reverzného efektu krátkeho kanála
16	IBA	Prvý koeficient nárazovej ionizácie
17	IBB	Druhý koeficient nárazovej ionizácie
18	IBN	Činiteľ saturačného napätia pre nárazovú ionizáciu

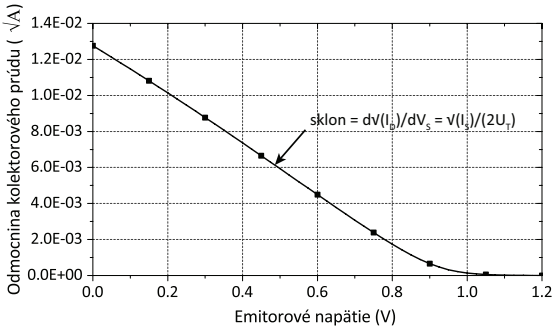
III. Hierarchická extrakcia parametrov

Model EKV2.6 má všetky parametre navzájom hierarchicky zviazané, a tak ich extrakcia je systematická a časovo relatívne nenáročná [5].

A. Extrakcia technologického prúdu

Technologický prúd I_s je prúd, pri ktorom MOS tranzistor pracuje v strednej inverzii ($i_c = 1$). Technologický prúd môže

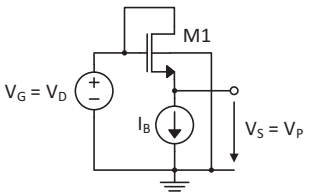
byť vypočítaný zo sklonu závislosti odmocniny kolektorového prúdu $\sqrt{I_D}$ od emitorového napätia V_S MOS tranzistora v silnej inverzii a saturácii (Obr. 1) [6], [7]. V praxi tento sklon nie je konštantný, preto treba technologický prúd vypočítať z jeho maximálnej hodnoty.



Obr. 1. Závislosť odmocniny kolektorového prúdu od napätia na emitore

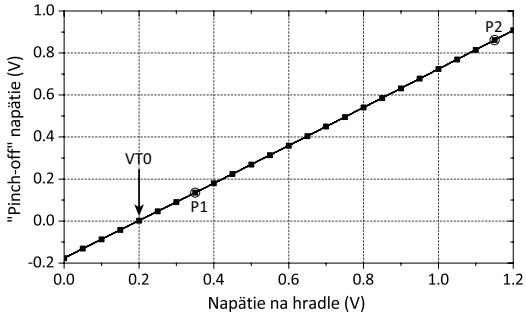
B. Extrakcia parametrov $VT0$, $GAMMA$ a PHI

Parameter $VT0$ možno extrahovať zo závislosti tzv. „pinch-off“ napätia V_P od napätia na hradle V_G MOS tranzistora s dlhým a širokým kanálom (šírka $W = 10\ \mu m$, dĺžka $L = 10\ \mu m$). Napätie V_P zodpovedá potenciálu kanála, pri ktorom sa inverzné náboje v nerovnovážnom stave rovnajú nule. Zapojenie obvodu pre simuláciu tejto charakteristiky sa nachádza na obr. 2.



Obr. 2. Schéma merania „pinch-off“ napätia

Prúd I_B sa rovná približne polovici technologického prúdu, čo zabezpečí činnosť tranzistora v strede oblasti strednej inverzie. Parameter $VT0$ sa potom rovná napätiu V_G, pri ktorom je $V_P = 0\ V$ (Obr. 3).



Obr. 3. Závislosť „pinch-off“ napätia od napätia na hradle

Zvolením dvoch bodov na tejto charakteristike, pre ktoré platí $V_G > VT0$, možno vypočítať parametre $GAMMA$ a PHI pomocou nasledujúceho systému rovníc:

$$V_{Pn} = V'_{Gn} - PHI - GAMMA\cdot \left[\sqrt{V'_{Gn} + \left(\frac{GAMMA}{2}\right)^2} - \frac{GAMMA}{2}\right], \quad (1)$$
$$V'_{Gn} = V_{Gn} - VT0 + PHI + GAMMA\sqrt{PHI},$$

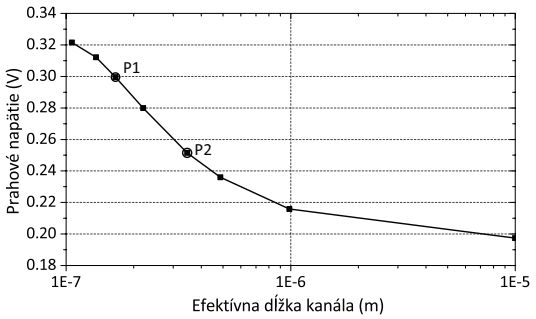
kde V'_G je efektívne napätie na hradle MOS tranzistora a γ je substrátový efekt. Dosadenie týchto dvoch bodov do systému rovníc (1) potom možno vypočítať oba parametre $GAMMA$ a PHI súčasne.

C. Extrakcia parametrov $LETA$ a $WETA$

Na extrakciu parametrov $LETA$ a $WETA$ je možne využiť rovnaké zapojenie ako pri extrakcii parametrov $VT0$, $GAMMA$ a PHI. Parameter $LETA$ opisuje javy spojené s krátkym a širokým kanálom MOS tranzistora. Stanovením rozmerov hradla na dĺžku $L = L_{min} = 120\ nm$ a šírku $W = 10\ \mu m$ je možné považovať parameter $WETA$ za rovný nule. Dosadením do systému rovníc (1), ktoré rozšírime o javy spojené s krátkym a úzkym kanálom [8], môžeme vypočítať parameter $LETA$. Rovnaký princíp platí pre extrakciu parametra $WETA$ ($L = 10\ \mu m, W = W_{min} = 160\ nm$).

D. Extrakcia parametrov LK a $Q0$

Parametre LK a $Q0$ opisujú jav, ktorý spôsobuje nárast prahového napätia V_{TH} pri MOS tranzistoroch s krátkym kanálom ($L \approx L_{min}$). Tieto parametre môžu byť opäť extrahované pomocou rovnakého zapojenia, ako predchádzajúce parametre, avšak tentokrát so sadou MOS tranzistorov s hradlom so šírkou $W = 10\mu m$ a rôznymi malými dĺžkami L. Na extrakciu sa využíva rovnaké zapojenie ako na extrakciu parametra $VT0$. Nájdením prahového napätia všetkých použitých tranzistorov je možné vykresliť závislosť prahového napätia V_{TH} od efektívnej dĺžky kanála $L_{eff} = L + DL$ (Obr. 4).



Obr. 4. Závislosť prahového napätia od efektívnej dĺžky kanála

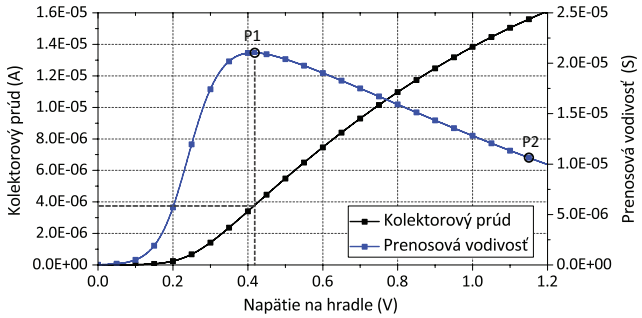
Z tejto závislosti je jasne badateľný nárast prahového napätia pri poklese dĺžky kanála. Na extrakciu parametrov LK a $Q0$ je potrebné zvoliť dva body (P1 a P2) z lineárnej závislosti získanej charakteristiky a dosadiť do zjednodušenej rovnice

$$V_{TH} = VT0 + \Delta V_{RSCE} + \gamma'\sqrt{V_S} - GAMMA\sqrt{PHI} \quad (2)$$

Z rovnice 2 je možné pre každý bod vypočítať hodnotu ΔV_{RSCE} a dosadením do systému rovníc publikovaných v [8] extrahovať oba uvedené parametre.

E. Extrakcia parametrov KP a $E0$

Parametre KP a $E0$ sa extrahujú z prevodovej charakteristiky veľkého MOS tranzistora pracujúceho v lineárnom režime. Parameter KP sa počíta z bodu (P1), pri ktorom prenosová vodivosť g_m dosahuje najvyššie hodnoty (Obr. 5).



Obr. 5. Prevodová charakteristika NMOS tranzistora v lineárnom režime

Parameter KP je následne možné vypočítať pomocou vzťahu (3), kde μ je pohyblivosť voľných nosičov náboja.

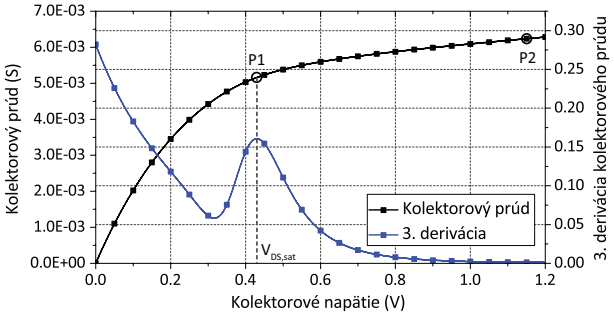
$$KP = \mu COX = \frac{I_D}{\frac{W}{L} \cdot V_D(V_G - VT0)}, \tag{3}$$

Maximálna pohyblivosť voľných nosičov náboja je v bode P1, v ktorom MOS tranzistor dosahuje najvyššiu vodivosť. Od tohoto bodu g_m a μ klesajú s relatívne konštantným sklonom. Tento sklon je definovaný ako koeficient redukcie pohyblivosti voľných nosičov náboja θ. Zvolením si druhého bodu (P2) z tejto lineárnej časti závislosti možno vypočítať koeficient $E0$ zo sady rovníc (4), kde bod s maximálnou prenosovou vodivosťou reprezentuje μ_0, pohyblivosť v druhom bode (P2) je μ a TOX je šírka hradlového izolačného oxidu.

$$\frac{\mu_0}{\mu} = 1 + \theta(V_G - VT0), \quad E0 = \frac{0,2}{\theta TOX} \tag{4}$$

F. Extrakcia parametra UCRIT

Parameter $UCRIT$ je možné extrahovať z výstupnej charakteristiky MOS tranzistora (Obr. 6) s minimálnou dĺžkou a veľkou šírkou kanála tranzistora pracujúceho v silnej inverzii. Ako prvé treba nájsť saturačné napätie tranzistora $V_{DS,sat}$ (P1) pomocou tretej derivácie výstupnej charakteristiky a nájdením jej lokálneho maxima (Obr. 6).



Obr. 6. Výstupná charakteristika NMOS tranzistora v silnej inverzii

Následne je možné vypočítať parameter $UCRIT$ s chybou menšou ako 5% pomocou systému rovníc nachádzajúcich sa v literatúre [8].

G. Extrakcia parametra LAMBDA

Parameter $LAMBA$ je možné extrahovať z rovnakej charakteristiky ako parameter $UCRIT$, avšak je potrebné zvoliť druhý bod P2, ktorý sa bude nachádzať blízko napájacieho napätia ($V_D \approx V_{DD}$). Pri extrakcii tohto parametra treba najskôr vypočítať hodnotu zmeny dĺžky kanála ΔL spôsobenú zväčšením ochudobnenej oblasti pomocou vzťahu (5):

$$\Delta L = L\left(1 - \frac{I_{DS,sat}}{I_{DS}}\right), \tag{5}$$

kde $I_{DS,sat}$ je kolektorový prúd v prvom bode a I_{DS} je kolektorový prúd v druhom bode. Hodnota zmeny dĺžky kanála umožňuje vypočítať hľadaný parameter $LAMBDA$ pomocou súboru rovníc nachádzajúcich sa v literatúre [8].

IV. Experimentálne výsledky

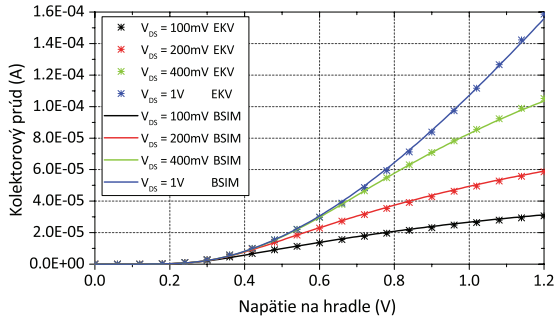
Pomocou vyššie opísaného postupu bola vyextrahovaný súbor základných parametrov pre model EKV2.6. Hodnoty všetkých parametrov sú zhrnuté v tabuľke II.

Tabuľka II
EXTRAHOVANÉ PARAMETRE PRE EKV MODEL

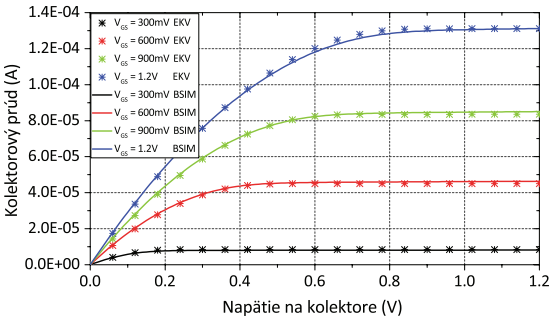
Typ	Parameter	Hodnota
Technologické parametre	COX	1,12e-2
	XJ	1,05e-7
	DL	-2,82e-8
	DW	-7e-8
Parametre súvisiace s dopáciou a pohyblivosťou	$VT0$	1,97e-1
	$GAMMA$	2e-1
	PHI	8,44e-1
	KP	4,65e-4
	$E0$	9,16e7
	$UCRIT$	2,29e6
Parametre spojené s krátkym a úzkym kanálom	$LAMBDA$	3,66
	$LETA$	1,14e-1
	$WETA$	-9,52e-2
	$Q0$	1,3e-2
	LK	1,06e-7
Parametre spojené so substrátovým prúdom	IBA	0
	IBB	3e9
	IBN	1

Korelácia medzi pôvodným modelom BSIM3V3 a extrahovaným EKV2.6 bola overené simuláciami základných charakteristík MOS tranzistora. Porovnanie prevodových a výstupných charakteristík NMOS tranzistora s rozmermi kanála 10 μm x 10 μm sa nachádza na obr. 7.

Dôkazom toho, že EKV model vychádza z metodiky využívajúcej parameter g_m/I_D je porovnanie závislostí tohoto parametra od koeficientu inverzie, ktoré je znázornené na obr. 8. Z tohto grafu možno pozorovať, že charakteristika modelu má podobný trend ako analytické vyjadrenie tohoto



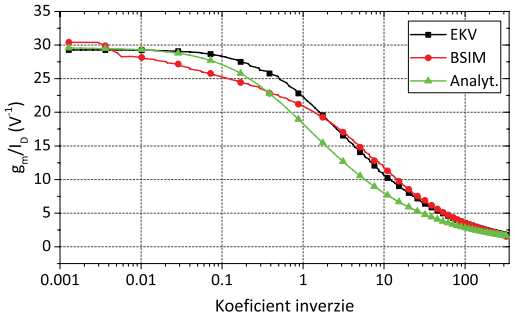
(a)



(b)

Obr. 7. Porovnanie základných charakteristík MOS tranzistora: (a) prevodové charakteristiky; (b) výstupné charakteristiky

parametra [9]. Posun medzi týmito dvomi charakteristikami je spôsobený relatívne veľkou chybou pri extrakcii parametrov EKV modelu. Tato chyba je systematická a je spôsobená tým, že extrakcia slúži na prvotný nástrel parametrov. Zároveň ju mohol spôsobiť aj malý počet nameraných vzoriek a posun technologického procesu meraných tranzistorov. Zvýšenie presnosti môže byť dosiahnuté ďalším prispôsobením ("zjemnením") parametrov hlavne pre oblasť strednej inverzie ($0,1 < i_c < 10$), čo aj jedným z nasledujúcich cieľov v rámci dizertačnej práce. Charakteristika BSIM modelu dokazuje vysokú nepresnosť modelovania činnosti MOS tranzistora v oblasti slabej ($i_c < 0,1$) a strednej inverzie [10].



Obr. 8. Závislosť efektivity prenosovej vodivosti od koeficientu inverzie

V. Ciele dizertačnej práce

- ✓ Analýza techník vhodných pre návrh nízko-napäťových IO a získanie najnovších poznatkov o vlastnostiach MOS tranzistorov riadených substrátovou elektródou.
- ✓ Návrh testovacích štruktúr a vytvorenie návrhu topografie testovacieho čipu.
- ✓ Charakterizácia testovacích tranzistorov vyrobených na prototypovom čipe pomocou meraní pre návrh nízko-napäťových IO.
- ✓ Extrakcia parametrov pre EKV model.
- Spresnenie extrahovaných parametrov pomocou nameraných charakteristík testovacích štruktúr.
- Overenie presnosti a použiteľnosti spresneného modelu pre návrh nízko-napäťových IO pomocou meraní navrhnutých a vyrobených štruktúr a obvodov.
- Uprava parametrov EKV modelu opisujúcich substrátový prúd pre návrh obvodov využívajúcich tranzistory riadené substrátovou elektródou.

VI. Záver

V tomto príspevku bol analyzovaný EKV model a spôsob extrakcie jeho základných parametrov. Zo získaných parametrov bol zostavený model EKV2.6. Simulácie parametra g_m/I_D dokazujú vhodnosť EKV modelu pre návrh IO využívajúcich tranzistory pracujúce v slabej a strednej oblasti inverzie.

V rámci mojej doterajšej práce a výskumu vzniklo 13 publikácií (4 články v impaktovaných vedeckých časopisoch, 7 príspevkov na medzinárodných konferenciách - DDECS, ICETA a ADEPT, a 2 príspevky na doktorandskom seminári PAD).

Poďakovanie

Táto práca bola podporená projektami APVV-15-0254 a VEGA 1/0905/17.

Literatúra

[1] K. Bult, "Analog design in deep sub-micron CMOS," in *26th European Solid-State Circuits Conference*, Sept 2000, pp. 126–132.

[2] C. C. Enz, F. Krummenacher, and E. A. Vittoz, "An analytical mos transistor model valid in all regions of operation and dedicated to low-voltage and low-current applications," *Analog Integr. Circuits Signal Process.*, vol. 8, no. 1, pp. 83–114, Jul. 1995. [Online]. Available: http://dx.doi.org/10.1007/BF01239381

[3] W. Grabinski, "EKV v2.6 parameter extraction tutorial," in *ICCAP Web Conference (webcast)*, Dec 2001.

[4] L. Faria and R. d'Amore, "A physics-oriented parameter extraction method for MOSFET libraries generation," *Journal of Integrated Circuits and Systems*, vol. 11, no. 2, pp. 121–131, 2016.

[5] K. Singh and P. Jain, "BSIM3v3 to EKV2.6 model parameter extraction and optimisation using LM algorithm on 0.18μ technology node," *International Journal of Electronics and Telecomunications*, vol. 64, no. 1, pp. 5–11, 2018.

[6] M. Bucher, C. Lallement, and C. C. Enz, "An efficient parameter extraction methodology for the EKV MOST model," in *Proceedings of International Conference on Microelectronic Test Structures*, Mar 1996, pp. 145–150.

[7] D. Stefanovic and M. Kayal, *Structured Analog CMOS Design*, 1st ed. Springer Science+Business Media B.V: Springer Netherlands, 2008.

[8] M. Bucher, C. Lallement, C. Enz, F. Theodolz, and F. Krummenacher, *The EPFL-EKV MOSFET Model Equations for Simulation*. EPFL-DELEG, 1998.

[9] D. M. Binkley, *Tradeoffs and Optimization in Analog CMOS Design*, 1st ed. Cambridge (UK): Cambridge University Press, 2010.

[10] V. Stopjakova, M. Rakus, M. Kovac, D. Arbet, L. Nagy, M. Sovcik, and M. Potocny, "Ultra-low voltage analog IC design: Challenges, methods and examples," *Radioengineering*, vol. 27, no. 1, pp. 171–185, 2018.

Metodika návrhu řadiče rekonfigurace pro Systémy odolné proti poruchám

Richard Pánek
2. ročník, prezenční studium
školitel: Doc. Ing. Zdeněk Kotásek, CSc.

Fakulta informačních technologií Vysokého učení technického v Brně
Božetěchova 2, 612 66 Brno, Česká republika
Tel.: +420 54114-{1362, 1223}
Email: {ipanek, kotasek}@fit.vutbr.cz

***Abstrakt*—Programovatelná hradlová pole (FPGA) jsou v dnešní době populární nejen pro vestavěné systémy. Jejich nevýhodou je náchylnost na sluneční aktivitu, která díky radioaktivnímu záření způsobuje poruchy konfigurační paměti známé jako SEU. Ty mohou způsobit selhání celého systému. Proto je vyvíjena řada metod pro zvýšení odolnosti proti poruchám. Pro FPGA je typické využití prostorové redundance např. TMR, která ale poruchy pouze maskuje. Proto je velmi vhodné využít klíčové schopnosti FPGA – rekonfigurace a tudíž moci poruchy opravit. Vše potřebné k opravě pomocí rekonfigurace musí zajistit její řadič. Ovšem existuje mnoho přístupů jak jej implementovat a proto se v rámci disertační práce zabývám jeho návrhem. Dále je představen nástroj pro odhad spolehlivosti systému založeného na TMR a rekonfiguraci. Nástroj je založený na simulaci systému s parametry MTTF a dobou rekonfigurace.**

***Klíčová slova*—Řadič rekonfigurace, systémy odolné proti poruchám, částečná dynamická rekonfigurace, FPGA.**

I. Úvod

Nejen pro implementaci vestavěných systému jsou velmi populární programovatelná hradlová pole (*angl. Field Programable Gate Arrays*, FPGAs). Důvodem je cenová dostupnost při výrobě malých sérií oproti aplikačně specifickým integrovaným odvodům (*angl. Application-Specific Integrated Circuits*, ASICs) a vyšší rychlost výpočtu v porovnání s procesorovou implementací. Využití FPGA přináší i další výhody, těmi jsou flexibilita, možnost přeprogramování a tudíž změna funkcionality, nebo jednoduché prototypování apod. Klíčovou vlastností je možnost změnit konfiguraci i za běhu aplikace a tím docílit buď přizpůsobení se měnícím se podmínkám nebo možnost odstranění za běhu objevených poruch. Současná konfigurace daného FPGA je dána bitstreamem uloženým v jeho konfigurační paměti. Bitstream tedy určuje využití a propojení zdrojů FPGA, jako jsou vyhledávací tabulky LUT, flip-flops registry, paměti BRAM, atd. Ty jsou organizovány do programovatelných logických bloků (*angl. Configurable Logic Blocks*, CLBs) a propojeny pomocí programovatelné propojovací sítě. Nejpoužívanější jsou tzv. SRAM FPGA, jejichž konfigurační paměť je založena na paměťových buňkách SRAM. Ovšem díky tomu jsou náchylná na radioaktivní záření např. v podobě nabitých částic, které způsobuje překlopení bitů konfigurační paměti a tudíž poškození implementovaného obvodu. Tyto poruchy jsou známé pod pojmem *Single Event Upset* (SEU) a je potřeba s nimi počítat obzvláště při návrhu vesmírných aplikací, protože ty budou pod vlivem slunečního záření [11].

Existuje mnoho metod na zajištění zvýšení odolnosti proti poruchám a tedy dopadům SEU. Značná část z nich je založena na prostorové redundanci, ovšem je možné využít i časovou nebo datovou redundanci. Patrně nejznámější metodou je tří-modulová redundance (*angl. Triple Modular Redundancy*, TMR), která je základem pro značnou část dalších metod jako např. [1], kde byl navržen spolehlivější prvek určující majoritu. Autoři článku [4] kombinují prostorovou a časovou redundanci, tudíž redukovali prostorovou náročnost na úkor potřebného času na maskování poruchy. Článek [15] dělí využité LUT na SEU-senzitivní a SEU-nesenzitivní. Pak aplikuje TMR pouze na SEU-senzitivní LUT a tím zajistí snížení prostorové náročnosti na úkor nepatrného zhoršení spolehlivosti.

Samotná TMR je schopná poruchy pouze maskovat, tudíž při nashromáždění více poruch časem dojde k selhání celého systému. Proto je vhodné využít rekonfiguraci, která je schopná chybu opravit [14]. V takovém případě mluvíme o systému řízení odolnosti proti poruchám (*angl. Fault-tolerant Control System*, FTCS). Ten je složen ze tří základních částí:

- rekonfigurovatelného řízení – v našem případě FPGA,
- detekce a diagnostiky poruch,
- řadiče rekonfigurace (*angl. Reconfiguration Controller*, RC), který za základě diagnostických dat zajistí opravu poruchy.

Pro detekci je možné využít právě TMR s tím, že prvek určující majoritu musí být schopen informovat řadič částečné dynamické rekonfigurace o modulu s poruchou, který bude následně opraven pomocí rekonfigurace [3]. I tento model je předmětem dalšího zkoumání. Např. v článku [8] se věnovali plánování ověřování majority TMR a rekonfigurace detekovaných poruch s upřednostněním kritických prvků, aby zvýšili celkovou spolehlivost. Ovšem i samotný řadič rekon-

figurace lze implementovat různými způsoby. Autoři článku [5] využívají procesorovou implementaci řadiče rekonfigurace. Dále pro úsporu energie je detekce poruch zajištěna časovou redundancí. Článek [2] popisuje FTCS rozprostřený na více FPGA. Řadič rekonfigurace je v systému také několikrát. Jedná se buď o soft-core procesor na každém využitém FPGA, nebo externí komponentu. Tímto modelem je možné rekonfigurovat i samotné řadiče rekonfigurace v případě jejich poruchy. Další možností je implementace řadiče rekonfigurace přímo v hardware. Příkladem je řadič popsaný v článcích [6], [13]. Takový řadič může být buď na stejném FPGA jako zabezpečovaný obvod nebo na jiném.

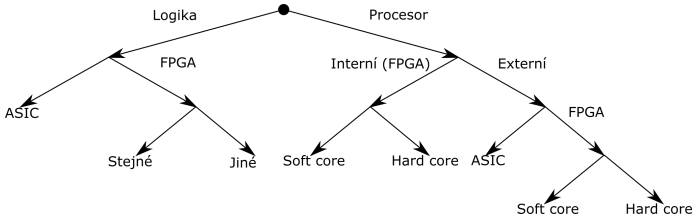
Tento článek je dále uspořádán následovně. Sekce II se věnuje definování řešené problematiky. V sekci III je popsáno vyhodnocení odhadu spolehlivosti systému odolného proti poruchám umístěného do FPGA a využívajícího částečnou dynamickou rekonfiguraci. Pro výpočet odhadované spolehlivosti je využita simulace. V sekci IV jsou rozpracovány cíle disertační práce. Závěrečné shrnutí je v sekci V.

II. Zaměření výzkumu

V rámci výzkumu se zaměřuji na návrh řadiče částečné dynamické rekonfigurace. Již z úvodu je patrné, že existuje mnoho způsobů jak jej implementovat:

- v logice nebo na procesoru,
- do FPGA (společně s obvodem nebo externí) nebo na ASIC,
- soft-core nebo hard-core procesor na FPGA.

Přehledné znázornění je na obrázku 1. Samozřejmě takových zobrazení může být více, záleží na volbě kořenového atributu. Jedná se o binární stromové uspořádání, kdy v kořenu je počáteční dělení a na listech konečné způsoby implementace. Ty dále mohou být na poruchy náchylné, nebo proti nim odolné.



Obrázek 1. Dělení způsobů implementace řadiče částečné dynamické rekonfigurace.

V rámci disertační práce budou diskutovány výhody a nevýhody jednotlivých přístupů. Z nich by mělo vyplynout, který přístup je vhodnější pro konkrétní navrhovaný systém odolný proti poruchám.

III. Simulační vyhodnocení odhadu spolehlivosti systému odolného proti poruchám na FPGA s využitím částečné dynamické rekonfigurace

Nástroj pro rychlé vyhodnocení využití rekonfigurace pro zajištění odolnosti proti poruchám byl představen v [10]. Zajímal nás dopad střední doby do výskytu poruchy (*angl. Mean Time To Failure*, MTTF) a doby potřebné pro opravu modulu pomocí rekonfigurace na celkovou spolehlivost celého systému. MTTF je dán prostředím, pro které je systém navrhován. Čas rekonfigurace lze ovlivnit velikostí rekonfigurovatelných modulů a také technologií (zvolením konkrétního FPGA).

Pro rychlé vyhodnocení byl vytvořen simulační nástroj postavený na knihovně *SimPy* [12], což je simulační framework založený na procesech a diskrétních událostech pro jazyk Python.

Pro experimentální systém jsme zvolili přístup TMR s rekonfigurací porouchaných jednotek. Každá jednotka může být v jednom ze dvou stavů: v poruchovém nebo bezporuchovém. Systém pracuje správně, pokud aspoň dvě jednotky TMR jsou v bezporuchovém stavu. V opačném případě dochází k selhání systému. Stav každé jednotky je možné změnit rekonfigurací nebo zásahem poruchy. V naší simulaci každá jednotka přejde do poruchového stavu v závislosti na MTTF. Konkrétní doba je určena normálním rozdělením, které je charakterizováno dvěma parametry [7]: *střední hodnota* (μ) a *rozptyl* (σ^2). Střední hodnotě odpovídá MTTF a rozptyl je dán na základě předchozích experimentů empiricky zjištěnou rovnicí 1.

$$\sigma^2 = \frac{\mu}{10} + 1\,[-] \tag{1}$$

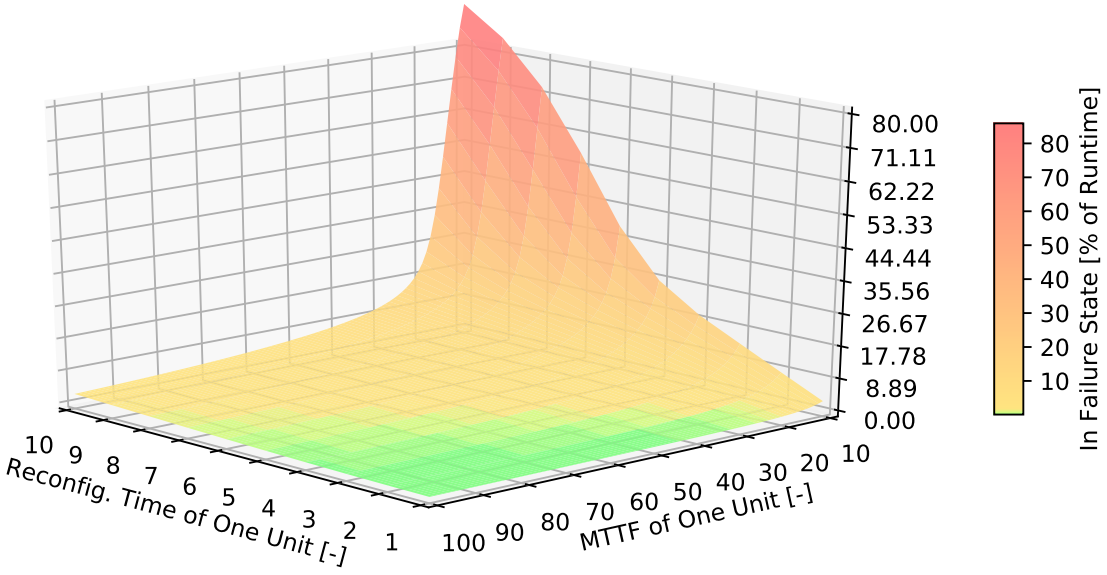
Výsledky experimentů s výše popsaným vyhodnocovacím prostředím jsou shrnuty v tabulce I. Doba potřebná k rekonfiguraci byla zvolena z intervalu $\langle 1, 10\rangle$. MTTF byla vybrána z intervalu $\langle 10, 100\rangle$. Tyto hodnoty byly zvoleny na základě monitorování skutečného experimentování s naším experimentálním elektromechanickým systémem (robotem v bludišti) [9]. Hodnoty jsou bezrozměrné, konkrétní rozměr záleží na výsledném systému, pro který budou využity. Čas běhu byl nastaven na 1000 jednotek a počet běhů jednoho scénáře byl 10 000. Jedním scénářem je myšlena jedna kombinace MTTF a doby rekonfigurace jednotky (jedna buňka tabulky).

Z výsledku v tabulce I je patrné, že největší pravděpodobnost selhání systému je při krátkém MTTF a dlouhé době rekonfigurace. Na opačné straně dlouhá MTTF a krátká doba rekonfigurace vede k nízké pravděpodobnosti selhání systému. Tyto výsledky byly očekávány, ovšem díky našemu simulačnímu nástroji mohou vývojáři snáze odhadnout, jak se jejich systém bude chovat i v jiném prostředí. Dále si mohou určit, jaká pravděpodobnost selhání je pro ně kritická a tudíž se rozhodnout, zda jimi navrhovaný systém se do nastavených hranic vejde. Výsledky mohou sloužit i jako základ pro rozhodnutí, zda snaha o zrychlení rekonfigurace bude mít dostatečný účinek na snížení pravděpodobnosti selhání.

Získané výsledky jsou také znázorněné v grafu na obrázku 2. Jedná se o znázornění totožných dat z tabulky I, ovšem z jiného pohledu. Z něj je patrný nelineární růst pravděpodobnosti selhání. Tudíž v určitých případech by bylo možné přijmout nepatrné zhoršení pravděpodobnosti selhání, ale zato využít méně náročný způsob rekonfigurace.

Tabulka I
PROCENTUÁLNĚ VYJÁDŘENÁ DOBA SELHÁNÍ SYSTÉMU BĚHEM PROVOZU ZÍSKANÁ POMOCÍ SIMULACE.

Failure State Representation [%]	Time To Reconfigure One Unit [-]									
MTTF of One Unit [-]	10.00	9.00	8.00	7.00	6.00	5.00	4.00	3.00	2.00	1.00
10.0	91.93	84.43	72.91	56.81	38.70	25.91	18.67	13.23	7.84	2.55
15.0	50.27	36.78	26.31	20.04	16.14	13.11	10.26	7.26	4.04	1.20
20.0	20.91	17.18	14.60	12.55	10.70	8.85	6.86	4.69	2.47	0.70
25.0	13.61	12.07	10.70	9.38	8.03	6.57	4.98	3.29	1.67	0.46
30.0	10.60	9.57	8.55	7.49	6.36	5.13	3.80	2.43	1.20	0.32
35.0	8.83	8.00	7.14	6.21	5.20	4.12	2.98	1.87	0.90	0.24
40.0	7.61	6.88	6.10	5.26	4.35	3.39	2.41	1.48	0.70	0.18
45.0	6.68	6.01	5.29	4.52	3.70	2.84	1.99	1.20	0.56	0.15
50.0	5.94	5.31	4.64	3.92	3.17	2.40	1.66	0.99	0.46	0.12
55.0	5.33	4.74	4.10	3.44	2.75	2.06	1.41	0.84	0.39	0.10
60.0	4.80	4.24	3.65	3.03	2.40	1.79	1.21	0.71	0.33	0.08
65.0	4.35	3.82	3.26	2.69	2.12	1.56	1.05	0.61	0.28	0.07
70.0	3.97	3.46	2.93	2.40	1.88	1.38	0.92	0.54	0.25	0.06
75.0	3.63	3.15	2.65	2.16	1.68	1.22	0.81	0.47	0.22	0.05
80.0	3.33	2.87	2.41	1.95	1.50	1.09	0.72	0.42	0.19	0.05
85.0	3.06	2.63	2.20	1.77	1.36	0.98	0.65	0.37	0.17	0.04
90.0	2.82	2.41	2.01	1.61	1.23	0.88	0.58	0.34	0.15	0.04
95.0	2.61	2.22	1.84	1.47	1.12	0.80	0.53	0.30	0.14	0.03
100.0	2.42	2.05	1.69	1.34	1.02	0.73	0.48	0.27	0.12	0.03



Obrázek 2. Graf doby selhání systému vyjádřené v procentech v závislosti na MTTF a době rekonfigurace každého jednotky.

IV. CÍLE DISERTAČNÍ PRÁCE

V rámci disertační práce se zaměřuji na vypracování metodiky návrhu a využití řadiče částečné dynamické rekonfigurace pro systémy odolné proti poruchám. Především se zaměřuji na dvě hlavní alternativy implementace řadiče v FPGA. První z nich je obvodová realizace a druhou pak program pro procesor, který je v FPGA. Dále budou vytvořena kritéria pro návrh, implementaci a samotné používání řadiče rekonfigurace. Ten bude následně implementován, aby s ním mohlo být experimentováno s cílem vyhodnotit míru splnění příslušných kritérií. Zatím známá kritéria pro posuzování jsou:

- Spolehlivost – odolnost proti poruchám, což je zásadní požadavek, protože o zvyšování odolnosti nám jde především.
- Rychlost a zpoždění, což souvisí s negativními dopady, které by mohlo přinést zvyšování odolnosti. Zajímá nás především, jestli využití rekonfigurace a potažmo jejího řadiče nebude mít za následek zvětšení zpoždění zabezpečované aplikace. I samotná rychlost rekonfigurace by mohla ovlivnit zabezpečovaný systém.
- Spotřeba, protože přidáním dalších komponent s velikou pravděpodobností naroste, ovšem záleží do jaké míry.

Obzvláště důležité je toto kritérium pro mobilní zařízení, které musí být napájené z baterií. V takovém případě úzce souvisí i s životností systému, protože i míra zabezpečení závisí na době, po kterou musí zařízení být plně funkční. Pokud by se měla energie, která je pro systém vyhrazená, vyčerpat dříve, než nastane jistá porucha, pak je zbytečné mít zabezpečení, které je na ni připravené a současně spotřebovává další energii.

- Zabraná plocha na FPGA se také zvětší, ale bude zkoumáno do jaké míry. Samozřejmě čím více FPGA zdrojů bude zapotřebí, tím větší a také dražší FPGA bude vyžadováno. Další možností může být využití více FPGA čipů. Vše povede na nárůst ceny. Zvětšení využité plochy FPGA také může zvýšit pravděpodobnost, že bude systém poruchou zasažen.
- Zabezpečení samotného řadiče, aby byl odolný proti poruchám. S tím souvisí vyhodnocení, jaké jsou možnosti pro zabezpečení řadiče a jaké budou dopady na zabezpečovaný systém. Bude zapotřebí vyhodnotit také všechna ostatní kritéria, protože i ta budou ovlivněna.

Další kritéria mohou být identifikována v průběhu výzkumu. Je zřejmé, že jsou vzájemně protichůdná a tak předpokládám vznik různých paretooptimálních řešení, která budou v rámci metodiky diskutována. Zejména jejich přínos pro různé požadavky aplikací.

V rámci výzkumné skupiny byly již mými předchůdci položeny základy pro využití rekonfigurace pro systémy odolné proti poruchám. Mým cílem je využití těchto základů pro moji práci a dále je rozvíjet. Pokračuji proto s vývojem řadiče částečné dynamické rekonfigurace GPDRC [6], [13]. Tento řadič budu dále zabezpečovat pomocí TMR a také budu zkoumat možnosti auto-rekonfigurace, tedy možnosti, že by se řadič dokázal po poruše sám opravit pomocí rekonfigurace. Dále pro porovnání počítám také s vytvořením implementace pro procesor a jejím zabezpečením stejnými postupy jako předchozí verzi. Všechny tyto přístupy budou podrobeny experimentům a budou diskutovány přínosy a úskalí, které budou potřeba pro vypracování metodiky.

Uvažovaná metodika má za cíl pomoci s výběrem ideálního řadiče rekonfigurace FPGA pro zajištění odolnosti proti poruchám výsledné aplikace tak, aby byly požadavky na ni kladené splněny co nejlépe.

V. Závěr

V rámci tohoto článku byla nastíněna problematika řešená v moji disertační práci. Jedná se metodiku návrhu řadiče rekonfigurace pro systémy odolné proti poruchám. Samotný řadič částečné dynamické rekonfigurace je klíčová komponenta pro zvýšení odolnosti proti poruchám. Ovšem může být implementována různými způsoby jako např. v FPGA (logika, procesor – sof-core, hard-core), nebo externí součástka: procesor, jiné FPGA atd. V rámci zamýšlené metodiky budou jednotlivé přístupy porovnány, aby bylo jednodušší rozhodnout, jaký typ řadiče zvolit při návrhu nového systému odolného proti poruchám.

Dále byl představen nástroj na vyhodnocení přínosu rekonfigurace založený na simulaci. Díky němu je možné odhadnout pravděpodobnost selhání konkrétního systému. Náš nástroj může být užitečný pro návrháře, protože budou moci odhadnout, zda jimi navrhované řešení je dostatečně spolehlivé pro dané prostředí.

Poděkování

Tato práce byla podporována projektem JU ECSEL SECREDAS (Product Security for Cross Domain Reliable Dependable Automated Systems), grantová dohoda č. 783119 a projektem řešeným na FIT VUT v Brně pod číslem FIT-S-17-3994.

Reference

[1] Afzaal, U.; Lee, J. A.: FPGA-based design of a self-checking TMR voter. *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, Sept 2017, s. 1–4, doi:10.23919/FPL.2017.8056811.

[2] Bolchini, C.; Fossati, L.; Codinachs, D. M.; aj.: A Reliable Reconfiguration Controller for Fault-Tolerant Embedded Systems on Multi-FPGA Platforms. *2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems*, Oct 2010, ISSN 1550-5774, s. 191–199.

[3] Bolchini, C.; Miele, A.; Santambrogio, M. D.: TMR and Partial Dynamic Reconfiguration to Mitigate SEU Faults in FPGAs. *22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems (DFT 2007)*, Sept 2007, ISSN 1550-5774, s. 87–95.

[4] Bělohoubek, J.; Fišer, P.; Schmidt, J.: Error masking method based on the short-duration offline test. *Microprocessors and Microsystems*, ročník 52, 2017: s. 236 – 250, ISSN 0141-9331, doi: https://doi.org/10.1016/j.micpro.2017.06.007.

[5] Frenkel, C.; Legat, J. D.; Bol, D.: A Partial Reconfiguration-based Scheme to Mitigate Multiple-Bit Upsets for FPGAs in Low-cost Space Applications. *2015 10th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*, June 2015, s. 1–7.

[6] Miculka, L.; Kotasek, Z.: Generic partial dynamic reconfiguration controller for transient and permanent fault mitigation in fault tolerant systems implemented into FPGA. *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, duben 2014, s. 171–174, doi:10.1109/DDECS.2014.6868784.

[7] Natrella, M.: *NIST/SEMATECH e-handbook of statistical methods*. NIST/SEMATECH, 2010.

[8] Nguyen, N. T. H.; Agiakatsikas, D.; Cetin, E.; aj.: Dynamic scheduling of voter checks in FPGA-based TMR systems. *2016 International Conference on Field-Programmable Technology (FPT)*, Dec 2016, s. 169–172, doi:10.1109/FPT.2016.7929525.

[9] Podivinsky, J.; Lojda, J.; Cekan, O.; aj.: Reliability Analysis and Improvement of FPGA-Based Robot Controller. *Digital System Design (DSD), 2017 Euromicro Conference on*, IEEE, 2017, s. 337–344.

[10] Pánek, R.; Lojda, J.; Podivínský, J.; aj.: Partial Dynamic Reconfiguration in an FPGA-based Fault-Tolerant System: Simulation-based Evaluation. *Submitted to: IEEE East-West Design & Test Symposium*, 2018.

[11] Siegle, F.; Vladimirova, T.; Ilstad, J.; aj.: Mitigation of Radiation Effects in SRAM-Based FPGAs for Space Applications. *ACM Comput. Surv.*, ročník 47, č. 2, leden 2015: s. 37:1–37:34, ISSN 0360-0300, doi: 10.1145/2671181.
URL http://doi.acm.org/10.1145/2671181

[12] Team SimPy: SimPy: Discrete Event Simulation for Python. https://simpy.readthedocs.io/, 2017, accessed: 2018-06-10.

[13] Straka, M.; Kastil, J.; Kotasek, Z.: Generic partial dynamic reconfiguration controller for fault tolerant designs based on FPGA. *NORCHIP 2010*, listopad 2010, s. 1–4, doi:10.1109/NORCHIP.2010.5669477.

[14] Zhang, Y.; Jiang, J.: Bibliographical Review on Reconfigurable Fault-tolerant Control Systems. *Annual Reviews in Control*, ročník 32, č. 2, 2008: s. 229 – 252, ISSN 1367-5788, doi: https://doi.org/10.1016/j.arcontrol.2008.03.008.

[15] Zheng, M. S.; Wang, Z. L.; Tu, J.; aj.: Reliability Oriented Selective Triple Modular Redundancy for SRAM-Based FPGAs. *Applied Mechanics and Materials*, ročník 713, Trans Tech Publ, 2015, s. 1127–1131.

Scientific Workflows Management

Marta Jaros
2nd year, full-time study
Supervisor: Jiri Jaros

Centre of Excellence IT4Innovations, Faculty of Information Technology, Brno University of Technology
Bozetechova 1/2, 612 66 Brno, Czech Republic
icudova@fit.vutbr.cz

***Abstract*—Scientific workflows provide a formal way to define, automate and repeat multi-step computational procedures. Existing tools, providing workflows creation, execution and sharing, focus mainly on expert users. Tuning and organizing the workflow computation effectively in order to minimize the cost while meeting given time constrains is very challenging and almost unfeasible even for expert users. This work shows the approach and tool providing effective planning, executing and monitoring many cooperating tasks in a sense of individual tasks and the workflow as a whole. The designed tool is suitable for both expert and regular users.**

***Keywords*—scientific workflow management system, high performance computing, distributed computing, automation, service**

I. Introduction

Scientific workflows are meant to improve the reproducibility of scientific applications by making it easier to share and reuse workflows between scientists. Unfortunately, this is not happening and scientists often find reusing difficult. As a reaction to this problem, a framework for facilitating the reproducibility of scientific workflows at the task level was proposed in [1]. The framework integrated execution environment specifications into scientific workflow systems. Scientists were given a complete control over the execution environment of individual tasks and their integration into scientific workflow systems. [1]

However, a regular researcher might not have enough background knowledge to configure and tune the system appropriately. Thus, the presented approach is built on predefined workflows and optimized programs prepared by expert users. A workflow is defined as a cyclic or acyclic directed weighted graph $G = (V, E)$ where V is a set of v weighted nodes representing tasks, and E is a set of e weighted edges representing data flow and dependency relationship. Weights on nodes represent the simulation time (i.e. elapsed time, disk processing time). Weights on edges represent an amount of data generated or copied by the task and needed time. The main feature of this approach is the ability to tune each task in the workflow individually (i.e. selection of HW resource, binary, number of processor cores or an environment variables setting), and to tune the workflow as a whole. Optimization decision will be based on the measured profiled data updated after each run. However, it is unfeasible to hold data for all possible input data sizes. Thus, a convenient method to get or estimate the run configuration needs to be used, e.g., an interpolation or machine learning methods. Optimalization of workflow execution planning should also minimize the time spent in computational queues. This problem is not usually solved by any scheduler used in high performance computing (HPC) environment.

The idea of this system is to enable researchers and regular users to use and compose complex workflows without a high level knowledge. This paper focuses on *k-Dispatch*, a workflow management system dedicated mainly to medical usage, however, easily extensible in more general way. Its fundamental architecture and example usecases were introduced last year [2]. Thus, this paper presents the state of the art in the scientific workflows management systems and schedulers used in HPC environment, introduces challenges for the k-Dispatch development, goals and key characteristics to be implemented.

II. State of the Art

Since the last year when *k-Dispatch* was firstly introduced, I have done a deeper research in the state of the art into scientific workflows management systems and HPC schedulers. The key findings coming from this research are important for the development of *k-Dispatch* and are summarized.

Over the last more than a decade, there have been developed manifold middle-ware projects focusing on running computational tasks on high performance facilities to automate and accelerate scientific projects, for example, grid frameworks [3] like Globus [3], [4] or gLite [5]. They serve scientists to share computing power, databases, tools, etc. Workflow tools offer a formal way to define, automate, and repeat multi-step computational procedures. Such tools usually provide services for resource monitoring and management, security and file management. Workflows supported by those tools are usually defined as directed acyclic graphs (DAGs).

Taverna [6] and Kepler [7], [8] provide graphical environment to help users to perform complex simulation workflows, design, execute or share with other people. Taverna enables to run workflows on a user computer, Taverna server, clouds and grids, using its own Workflow Management System. Kepler allows computations over computer clusters and grids. Both, Taverna and Kepler, focus on researchers and well-informed users. They are widely used in bioinformatics, ecological

and environmental research, weather and climate analysis, astronomy, and so on.

FabSim [9] shares functionality with mentioned middleware toolkits, however, it is aimed at the experienced computational scientists. Command line is the only supported interface which is easy to extend by developers. The key strength of FabSim is its focus on simplifying and accelerating development activities. FabSim does not provide decision-making in terms of planning and monitoring. Its main goal is to simplify researchers' daily tasks.

Next, HyperLoom [10] is a platform for defining and executing scientific workflows in large-scale high performance computing (HPC) systems. Its goal is to minimize the overall workflow execution time by respecting tasks and environment resource constraints. HyperLoom implements an optimized dynamic scheduler that schedules tasks reactively with low overhead since the execution time of individual tasks is not known in advance. Each task is considered to run only on one computation node. Thus, the only supported paralellism is the inter-node one. Its scheduler respects task dependencies and prioritizes placements that induce the smallest possible inter-node data transfer. Data produced by tasks are kept directly in memory and can be accessed by any other task without additional overhead. HyperLoom enables users to define and execute workflows using its client application. It is focused on experienced users as well. Although HyperLoom was originally designed to be used within HPC infrastructures, these infrastructures may be unavailable or too expensive especially for small to medium workloads. Therefore, HyperLoom developers started to aim at public cloud providers since the performance of their machines is comparable to those in HPC systems. However, network solutions used in HPC systems offer incomparably higher inter-node throughput.

Effective workflow scheduling is the key but challenging issue in heterogeneous environments due to heterogeneity and dynamism. A workflow, usually modeled as a DAG, consists of several tasks that need to be scheduled. However, these tasks differ in their demands. Task scheduling strongly affects the waiting time, efficiency, throughput and the total time needed to finish the whole workflow. The guarantee of the calculation completed in a specified time is very crucial and required. Task scheduling problems with the smallest parallel execution time have been shown to be NP-complete in a strong sense, even for an unbounded number of processors, and present an efficient scheduling algorithm which is close to optimal in practice [11].

Supercomputing facilities use commercial or open-source job schedulers that contain job scheduling algorithms developed in the past, e.g., backfilling, first come first served (FCFS), etc. For instance, Portable Batch System (PBS)[1] uses the backfilling scheduling algorithm, and considers user and group priorities, and fair-share cluster policy[2].

The IT4Innovations[3] supercomputing centre's PBS scheduler gives each job an execution priority first, and then uses this job execution priority to select which job(s) to run. Job execution priority is determined by the queue priority, fair-share priority and eligible time where the queue priority has the biggest impact. Fair-share priority is calculated on the recent usage of resources per project. Eligible time is an amount of eligible time the job accrued while waiting to run and has the least impact on execution priority. Therefore, jobs with higher eligible time gains higher priority. Therefore, it is very beneficial to specify the walltime when submitting jobs which enables better scheduling and better resource usage. *Backfilling* is an FCFS improved by increasing the utilization of the system resources and by decreasing the average waiting time in the queue. *Backfilling* fits smaller jobs in front of the higher-priority jobs if it is possible, in such a way that the higher-priority jobs are not delayed. This allows to keep resources from becoming idle when the top job (job with the highest execution priority) cannot run. [12] Backfilling scheduling algorithm is used by IT4Innovations' clusters.

Another widely employed workload manager is Slurm[4] used by, e.g., Chinese Sunway TaihuLight or Swiss Piz Daint. Slurm performs always a best-fit algorithm based on the Hilbert curve scheduling or fat tree network topology in order to optimize locality of task assignments on parallel computers [13].

However, as mentioned before, developers of workflow management systems sometimes implement their own schedulers, e.g., HyperLoom, operating above those used in supercomputing centers. Another example is NCSA (National Center for Supercomputing Applications at the University of Illinois) scheduler tool [14] designed for Blue Waters and other HPC systems. Many HPC facilities limit the number of jobs per user to prevent queues from becoming cumbersome. NCSA scheduler allows users to aggregate single-core jobs as a single batch and job share the node between applications using a simple configuration file. Scheduler allows queuing jobs and manages efficiently independent single-core jobs, can bundle OpenMP (Open Multi-Processing) single-node jobs but cannot bundle MPI (Message Passing Interface) jobs.

III. Hypothesis

Contemporary complex HPC systems do not allow users from industry or clinics to use them efficiently and easily without proper and deep knowledge. An appropriate interface and simulation planning (involves a creation of a task graph) is supposed to (a) increase the processing efficiency since the execution is based on the task graph and current HPC system status, and (b) save resources, reduce the price of calculation or decrease computational time by an appropriate choice of the job configuration. Moreover, this may bring HPC and the latest technologies to industry and enable new methods to emerge and gain new knowledge in a medical practice. The workflow management software allows more users to cooperate and implement a level of fault tolerance, i.e., faulty

[1] pbspro.org

[2] nas.nasa.gov/hecc/support/kb/how-pbs-schedules-jobs_179.html

[3] docs.it4i.cz

[4] schedmd.com/fair_tree.html

tasks are executed repeatedly with respect to dependencies to calculate the simulation workflow correctly.

IV. Open problems

In this section, selected open problems and challenges are depicted.

- **Selection of the most convenient computational resource.** There are several factors that influence the resource choice, e.g., allocation size, machine availability, machine workload, workflow demands, required time, price, etc. If there is more than one suitable machine, it is needed to run benchmarks corresponding to the planned workflow and based on this knowledge choose the appropriate machine.
- **Run configuration.** A run configuration can be set to meet time or price constraints. To find the most appropriate configuration for each program, it is necessary to hold information about settings on each machine, data size, elapsed time and spent corehours in a data structure. This data structure can be updated after each run. However, this data structure does not hold all possible options. Thus, it is necessary to use a convenient method to get or estimate the run configuration. For instance, a linear interpolation can be applied on the measured data and obtained result can be adjusted to the concrete cluster. Problem of a proper run configuration finding has a potential in machine learning methods such as neuron nets. However, these methods require a big amount of measured data to learn the model.
- **Heterogeneous architectures support.** Modern supercomputers usually provide nodes with CPUs and some nodes with accelerators as GPUs, MICs or FPGAs. In many cases, the usage of an appropriate accelerator can be beneficial. The complexity is increased since the selection and configuration need to be done globally, i.e. for the workflow as a whole.
- **Data transfers.** Demanding simulations process and produce huge data files. Since simulations consist of several steps, the same files may be required in multiple steps. This might cause problems with a lack of storage. There are two possible solutions; the first one is to generate data files every time they are required and delete them immediately after the computation finished. This can be more computationally intensive process. The second approach is to generate data files only once, copy them if needed, and delete them after the whole computation of the simulation has finished. The shortage of this solution is a storage requirement.
- **Workflows with tightly coupled tasks and dynamic number of task instances.** These worklows contain unknown numbers of cyclic dependencies among tasks in the task graph. The execution of workflows that exclude these dependencies is quite clear since identifiers are known at the moment the tasks are submitted to the queues. However, in the case we do not know number of task instances (iterative calculations with thresholds), we need to find an appropriate way how to discover identifiers of these jobs, send them back and store in the database in order to monitor them. Another practical example where we have this problem is the checkpoint-restarting. Checkpoint-restart is a useful way to continue in a calculation of a suspended job. It is useful in cases, e.g., the job calculation is too long and the CPU time limit in the queue is going to be exceeded. Checkpoint restart enables to recover its calculation without data loss. However, this job receives a new identifier which is unknown for the workflow management software.

Other open problem is the implementation of an efficient model coupling interface, which is crucial for reducing the total computational time, better resources utilization, minimizing disk operations, and increasing the computational accuracy in some cases [2].

V. Thesis goals

Thesis goals have been selected from the open problems and challenges described in Sec. III. Their possible solutions are evaluated in the previous section as well. Selected goals of this thesis are:

1) Create a prototype of the software providing planning, executing and monitoring cooperation computations on HPC systems.
2) Investigate convenient heuristics and description formalisms. Workflows might be described using scale separation map and multiscale modelling languages [15].
3) Support heterogeneous architectures (CPUs, GPUs, other accelerators) within the same cluster.
4) Implement a logic responsible for choosing the most appropriate computational machine and an optimal task run configuration.
5) Provide an effective workflow planning with the throughput maximalization or the latency minimalization.
6) Test this software on two selected medical applications, i.e, women breast cancer diagnosis and HIFU[5] surgery.
7) Evaluation and benefits.

VI. Work progress

The basic concept of *k-Dispatch* was presented in [2]. This concept is listed in Fig. 1, and for detailed description of its modules see Fig. 2.

k-Dispatch shares functionality with tools like Taverna and is highly inspired by FabSim, but it is aiming at users who are not IT experts. The process of simulation planning, monitoring and executing is fully automated. Although, *k-Dispatch* was designed mainly for medical use, its design is generic and modular. So, it can be extended to support new workflows as well as provide functionality to enable users to create and modify their own workflows including computational machine specifics.

[5]High Intensity Focused Ultrasound

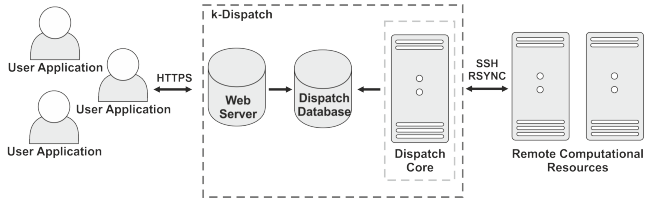


Fig. 1. Simple overview of *k-Dispatch*. Communication with user applications is based on standard web services, i.e., *HTTPS*. Communication with computational machines is based on SSH. *k-Dispatch* consists of the Web server, the Dispatch database and the Dispatch core where the main logic part is hidden.

At this time, *k-Dispatch*'s design does not involve its own scheduler. Instead, *k-Dispatch* relies on remotely installed schedulers such as PBS Pro to manage jobs on remote machines. Support for newly released schedulers can be easily added by adjusting the machine-specific configurations and creating a template file for the job submission script.

However, if we consider dedicated cluster or its queues, it would be very desirable to design and implement our own scheduler to plan computations more effectively.

k-Dispatch is being implemented in Python because of a variety of available modules, rapid prototyping and coding, and easy extensibility. A set of unit tests was created for each implemented component and module. Its Web server and the Dispatch database were tested locally. A connection and transfers between *k-Dispatch* and remote machines have been tested on IT4Innovations cluster Anselm.

In recent time, the Monitor module has been finished and tested using a set of unit tests. Those tests include workflows, e.g., trees of three to five tasks with and without dependencies. Except the workflow deletion at a user request and non-problematic workflows, errors were injected and the ability to restart has been successfully tested.

At this moment, workflows are formally defined only by directed acyclic graphs. The mapping problem is defined as tasks mapping onto available resources and available time slots aiming at minimizing the total computation time. Such a mapping Q might be defined as a projection $Q \rightarrow (T_i \times R_i)$ where T_i is a subset of a finite set T of time slots, and R_i is a subset of a finite set R of all computational resources.

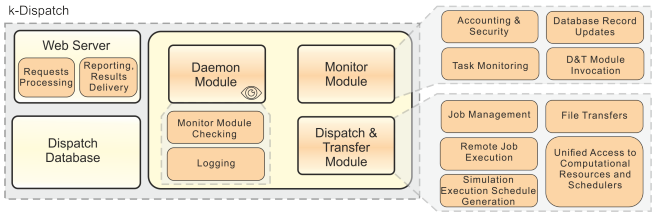


Fig. 2. Architecture of *k-Dispatch*. This figure shows modules of *k-Dispatch* in detail and their functionality.

VII. Conclusions

The state of the art in workflow management systems and HPC schedulers has been presented. k-Dispatch is a platform trying to fill shortages of existing tools that are considered to be important.

Goals 1) and 2) are almost finished. The defined formalism is sufficient at this time and may be extended later. The developed prototype is being tested right now. For advanced testing, *k-Dispatch* is now going to be moved onto our faculty server to the docker container[6]. Testing workflows consisting of real simulations will be created. After this phase, some refactoring and small improvements are supposed to be done and my research can move to another goal, e.g., a support of heterogeneous architectures implementation.

Acknowledgment

This work was supported by the FIT-S-17-3994 Advanced parallel and embedded computer systems project.

References

[1] H. Meng and D. Thain, "Facilitating the Reproducibility of Scientific Workflows with Execution Environment Specifications," *Procedia Computer Science*, vol. 108, pp. 705 – 714, 2017.

[2] M. Cudova, "Framework for Planning, Executing and Monitoring Cooperating Computations," in *Počítačové architektúry & diagnostika PAD 2017*, 15th ed. Bratislava: Slovenská technická univerzita v Bratislavě, 2017, pp. 20–23.

[3] I. Foster, C. Kesselman, and S. Tuecke, "The Anatomy of the Grid," *Hand clinics*, vol. 17, no. 4, pp. 525–532, 2001.

[4] I. Foster, "Globus Toolkit Version 4: Software for Service-Oriented Systems," *Journal of Computer Science and Technology*, vol. 21, no. 4, pp. 513–520, jul 2006.

[5] "glite–introduction," http://grid-deployment.web.cern.ch/grid-deployment/glite-web/introduction, (Accessed on 01/11/2018).

[6] "Apache taverna–apache taverna (incubating)," https://taverna.incubator.apache.org/, (Accessed on 01/10/2018).

[7] "Kepler 2.5 released–kepler," https://kepler-project.org/users/whats-new/kepler-2.5-released, (Accessed on 01/15/2018).

[8] B. Ludäscher, I. Altintas, C. Berkley, D. Higgins, E. Jaeger, M. Jones, E. A. Lee, J. Tao, and Y. Zhao, "Scientific workflow management and the Kepler system," *Concurrency and Computation: Practice and Experience*, vol. 18, no. 10, pp. 1039–1065, aug 2006.

[9] D. Groen, A. P. Bhati, J. Suter, J. Hetherington, S. J. Zasada, and P. V. Coveney, "FabSim: Facilitating computational research through automation on large-scale and distributed e-infrastructures," *Computer Physics Communications*, vol. 207, pp. 375–385, 2016.

[10] V. Cima, J. Thomas, and V. Chupakhin, "HyperLoom Possibilities for Executing Scientific Workflows on the Cloud," in *Complex, Intelligent, and Software Intensive Systems (AISC, Vol.611)*, L. Barolli and O. Terzo, Eds. Springer International Publishing, 2017.

[11] V. Sarkar, *Partitioning and Scheduling Parallel Programs for Multiprocessors*. MIT Press, Cambridge, 1989.

[12] P. Singh, Z. Quadri, and A. Kumar, "Comparative Study of Parallel Scheduling Algorithm for Parallel Job," *International Journal of Computer Applications*, vol. 134, no. 10, pp. 10–14, 2016.

[13] J. A. Pascual, J. Navaridas, and J. Miguel-Alonso, "Job Scheduling Strategies for Parallel Processing," in *JSSPP 2009. Lecture Notes in Computer Science, vol. 5798*, U. Frachtenberg, Eitan Schwiegelshohn, Ed. Berlin, Heidelberg: Springer, 2009.

[14] "Github - ncsa/scheduler: The aggregate job launcher of single-core or single-node applications on hpc sites," https://github.com/ncsa/Scheduler, (Accessed on 01/29/2018).

[15] B. Chopard, J. Borgdorff, and A. G. Hoekstra, "A framework for multi-scale modelling," *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences*, vol. 372, 2014.

[6] https://www.docker.com/what-docker

Mnohokanálový softwarový FHSS přijímač na Cortex-M

Tomáš Jakubík
V průběhu 2. ročníku, prezenční studium
Jiří Jeníček

Technická univerzita v Liberci
Fakulta mechatroniky, informatiky a mezioborových studií
Studentská 1402/2, 461 17 Liberec
Email: tomas.jakubik@tul.cz, jiri.jenicek@tul.cz

***Abstrakt*—Tento článek pojednává o návrhu speciálního softwarového přijímače pro řídící prvek sítě senzorů. Přijímač naslouchá najednou na 64 Gaussian Minimal Shift Keying (GMSK) kanálech v 868 MHz bezlicenčním pásmu. Navržený koncept bezdrátové Frequency Hopping Spread Spectrum (FHSS) komunikace umožňuje s pomocí představeného přijímače zachovat velmi nízkou spotřebu senzorů i při zavedení Spread Spectrum komunikace. Přijímač je navržen, simulován a otestován na RTL-SDR a Matlab Simulink. Nakonec je uveden nástin miniaturizace výsledného přijímače do mikroprocesoru LPC4370.**

***Klíčová slova*—FHSS, SDR, Cortex-M, sensor network**

I. Úvod

Většina typů bezdrátové komunikace se těší rychlému rozvoji, ať už jde o mobilní komunikaci nebo internet věcí. Existují ale oblasti, kde počet vyrobených kusů neodpovídá nákladům na vývoj. Komunikace malých bateriemi napájených senzorů s nadřízeným prvkem tak většinou používá již překonané technologie. Příchod levných Software Defined Radio (SDR) by mohl v dohledné době situaci změnit.

A. Bateriemi napájené senzory

Pro malé jednoduché senzory vznikají sítě internetu věcí. Ty se ale vyznačují nespolehlivostí a velmi pomalou odezvou. Pro senzory týkající se bezpečnosti nebo uživatelské interakce jsou tyto sítě nepoužitelné. Do této kategorie můžeme zařadit detektory pohybu, otevření oken nebo dveří, kouřová čidla, ale i termostaty nebo vypínače světel. Všechna tato zařízení musí reportovat události do nadřízeného prvku bez většího zpoždění a s minimálními nároky na energii. Pro představu, běžný detektor otevření okna zabezpečovacího systému musí vyžít s průměrnou spotřebou $5\,\mu\mathrm{A}$ při napájení $3.3\,\mathrm{V}$. To by z baterie mobilního telefonu stačilo zhruba na 50 let provozu. Přenesení informace musí být hotovo ve zlomcích sekundy, tak aby uživatel při zapnutí světel nepoznal zpoždění a aby zničení senzoru nestihlo komunikaci přerušit.

Komunikace je zde nejčastěji řešena jednofrekvenčním systémem. Nadřízený prvek neustále naslouchá a senzory jsou uspané. Jakmile je detekována událost, senzor se probouzí a ihned začíná vysílat. Nadřízený prvek informaci zachytí a může dále jednat. Běžná modulace je Gaussian Frequency Shift Keying (GFSK) v sub-GHz pásmu, které je méně zarušené a umožňuje mnohem delší dosah než pásmo $2.4\,\mathrm{GHz}$.

B. Spread Spectrum

Spread Spectrum je technologie, která se už dostala téměř do všech odvětví elektromagnetické komunikace. Rozprostření spektra velmi napomáhá komunikaci, která je potom více odolná proti rušení a lépe se skloubí s ostatní komunikací ve stejném pásmu [1]. Nejjednodušší a jednou z nejstarších Spread Spectrum technologií je FHSS [2]. Použije se pouze jeden úzký komunikační kanál, ale v průběhu komunikace se frekvenční kanál mění. Pokud se kanál změní mezi jednotlivými pakety, pak je možné použít stávající jednofrekvenční hardware, který se v prodlevě mezi pakety stihne přeladit.

Nevýhodou je zde skloubení s používaným systémem komunikace, kdy senzory spí. Senzory musí vědět jaký kanál je zrovna použitý. K tomu je potřeba buď udržovat senzory synchronizované, což spotřebuje mnoho energie, nebo je synchronizovat před každým spojením, což zpozdí přenesení události. Obě řešení mají nedostatky, které vylučují například Bluetooth z použití v této situaci [3].

Problém už jsme se pokusili vyřešit navržením FHSS sítě na míru [4]. Takové řešení má také své nevýhody.

II. Mnohokanálový přijímač

Jedna z možností jak problém vyřešit je použít přijímač, který bude poslouchat na všech kanálech najednou. Senzor bude moci spát, tak jako doposud. Po detekování události se probudí, vybere náhodný frekvenční kanál a začne vysílat. Speciální mnohokanálový přijímač se postará o zbytek.

Jedním řešením by mohlo být 47 standardních přijímačů (47 je nejmenší počet kanálů pro FHSS [5]), ale to by znamenalo velkou a drahou desku nebo návrh vlastního drahého čipu. Zbývá pouze softwarové rádio, které je zatím také drahé, pokud není jednoúčelové a vyráběné ve velkých množstvích. Při investici do softwarového rádia by bylo možné využít zbývající výkon pro komunikaci s vícero senzory najednou na rozdílných frekvencích nebo pro komunikaci s datově náročnějšími zařízeními. Zatímco nadřízený prvek komunikuje na jedné frekvenci se senzorem, mohl by stahovat videozáznam

z kamery na dalších frekvencích. Synchronizace v jednom zařízení by vyřešila rušení dvou rozdílných systémů, tak jako se děje například mezi WiFi a Bluetooth [6].

V nejjednodušší konfiguraci by nadřízenému prvku přibyl pouze jeden mnohokanálový přijímač ke stávajícímu jednofrekvenčnímu hardware. Většina komunikace by probíhala standardním FHSS a pouze prvotní navázání spojení by vyřešil přidaný speciální přijímač v nadřízeném prvku. Senzor by se mohl probudit, odvysílat událost na náhodném kanálu a čekat na odpověď. Nadřízený prvek by speciálním přijímačem vyslechl informaci, přeladil by obyčejný vysílač na stejný kanál a odpověděl by. V odpovědi by mohly být informace potřebné k okamžitému připojení do FHSS nebo příkaz, který senzor opět uspí.

První krok je tedy navrhnout přijímač všech FHSS kanálů. Na rozdíl od plnohodnotného SDR bude samotný přijímač dostatečně levný, aby byl dostupný pro domácí automatizaci a zabezpečení.

III. Implementace na RTL-SDR a Simulink

Běžný DVB-T přijímač je v základu SDR, který je vyráběn masově a tedy cenově přijatelně. Projekt RTL-SDR odemyká možnosti běžných USB DVB-T zařízení, tak aby šly použít k libovolným účelům. Zakoupit lze i RTL-SDR přijímač, který je navíc upravený pro potřeby SDR.

RTL-SDR přijímač se skládá z demodulátoru R820T2 a DVB-T dekodéru RTL2832U. S pomocí správného software lze dekodér přepnout aby vracel surové IQ vzorky. Tyto vzorky lze potom zpracovávat například v programech GNU Radio nebo Matlab Simulink. Pro vývoj mnohokanálového přijímače jsem zvolil Matlab Simulink.

A. Příjem

Pro příjem mnoha kanálů najednou se hodí FFT. Výstupem je informace o amplitudě a fázi pro každý kanál. FSK signál je tvořen frekvencí o málo vyšší nebo nižší než frekvence samotného kanálu. Na výstupu FFT se toto projeví jako lineárně se měnící fáze. Stačí tedy fázi derivovat (v nejjednodušším případě odečíst předchozí vzorek) a výsledkem je odchylka přijaté frekvence (Obrázek 1, blok *diff & wrap*).

Z maximálních hodnot fáze lze odvodit maximální detekovatelný rozdíl frekvence

$$max(F_{dev}) = \frac{1}{2T_c} \tag{1}$$

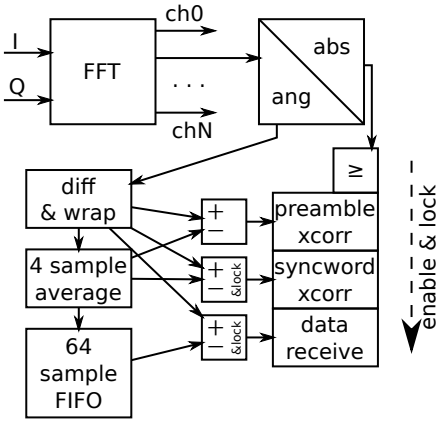
kde T_c je délka jednoho vzorku na výstupu FFT. Při použití GMSK (GMSK je zvláštní případ GFSK s minimálním F_{dev}) platí

$$F_{dev} = \frac{1}{4T_s} \qquad T_s \geq \frac{T_c}{2} \tag{2}$$

kde T_s je délka symbolu. Minimum je jeden symbol na jeden vzorek signálu, takže podmínka je pro GMSK splněna.

Carsonovým pravidlem lze i odhadnout šířku pásma (BW) jednoho kanálu a omezit symbolovou rychlost, aby se nepřeléval do kanálů sousedních. Pro GMSK to lze vyjádřit jako

$$F_{bw} \approx \frac{1.5}{T_s} \qquad T_s \geq 1.5T_c \tag{3}$$



Obrázek 1. Zjednodušené schéma přijímače.

Zvolením $T_s = 2T_c$ je s malou rezervou splněna i tato podmínka a bude možné zjednodušit symbolovou synchronizaci na výběr ze dvou vzorků.

Minimum potřebných kanálů splní velikost 64, nejbližší vyšší mocnina 2. RTL-SDR dovede posílat vzorky maximálně $2.4\,\mathrm{MHz}$ a to je i jeho maximální BW. Z toho vyplývá šířka jednoho kanálu $\frac{1}{T_c} = 37.5\,\mathrm{kHz}$ a rychlost komunikace $\frac{1}{T_s} = 18.75\,\mathrm{kBaud/s}$.

B. Zpracování vzorků

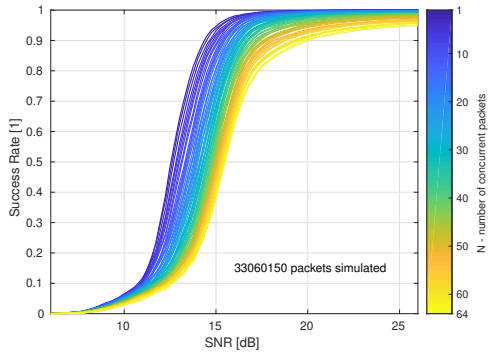
První vyhodnocení kanálu se provádí ze vzorků amplitudy (blok $\geq$). Amplituda musí být vyšší než nastavená konstanta a skokově narůst, aby začaly signál zpracovávat další části přijímače.

Pokud amplituda souhlasí, pokračuje se filtrováním stejnosměrné složky signálu (blok *4 sample average*) a hledáním preambule ze signálu frekvenční odchylky (blok *preamble xcorr*). Vysílače nejsou většinou přesně frekvenčně sladěny takže se spočítá průměr ze dvou symbolů v průběhu preambule a ten se od signálu odečte. Preambule je sekvence jedniček a nul sloužící pro nastavení přijímačů.

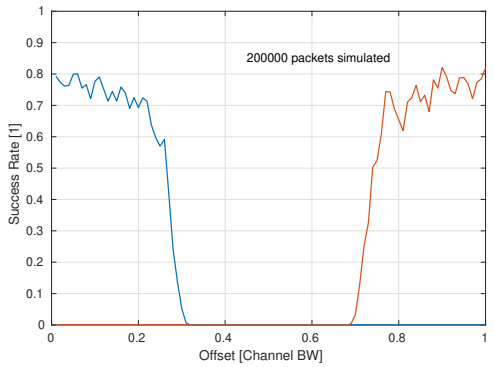
Na rozdíl od běžných způsobů [7] byla zde symbolová synchronizace zjednodušena na nejnutnější minimum. Mezi preambulí a daty paketu je poslán syncword, který se v přijímači koreluje (blok *syncword xcorr*) a podle špičky se rozhodne zda symbol začíná lichým nebo sudým vzorkem. Jakákoliv jiná synchronizace by byla nepraktická nebo velmi výpočetně náročná, protože sladění s jedním vysílačem by rozsynchronizovalo všechny ostatní. Při přesnosti krystalu $30\,\mathrm{ppm}$ se synchronizace posune o jednu polovinu vzorku T_c za 8333 symbolů T_s respektive $1042\,\mathrm{B}$. To je násobně více než je délka běžného paketu v těchto sítích, takže synchronizace ze začátku paketu stačí až do jeho konce.

Zbývá už pouze skládání bitů, bajtů a kontrolní CRC (blok *data receive*). Pro odečet stejnosměrné složky se zde používá hodnota z konce preambule (blok *64 sample FIFO*).

Jednotlivé části přijímače se zapínají pouze pokud jsou potřeba. Například korelace syncword běží pouze mezi detekcí preambule a ihned po detekování syncword se opět vypíná.



Obrázek 2. Simulace přijímače pro vícero paketů.



Obrázek 3. Simulace příjmu při frekvenční odchylce.

C. Výsledky

Přijímač byl otestován simulací. Ačkoliv je možná častější simulovat Bit Error Rate (BER), zde byly simulovány celé pakety pro ověření celého přijímače. V paketech nebyl použit opravný kód a jediný chybně přijatý bit znamená neúspěch.

Vygenerované pakety obsahovaly $20\,\mathrm{B}$ užitečných dat, respektive $31\,\mathrm{B}$ celkem. Před signál byl vložen náhodný počet prázdných vzorků k otestování synchronizace symbolů. Výsledný signál prošel přes Additive White Gaussian Noise (AWGN) kanál jehož Signal to Noise Ratio (SNR) bylo upraveno o

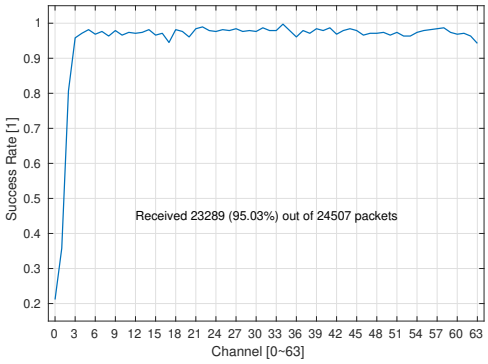
$$SNR_{offset} = 10 \cdot log_{10}\left(\frac{1}{64}\right) \approx -18\,\mathrm{dB} \tag{4}$$

tak aby se eliminoval zisk samotného FFT.

Obrázek 2 ukazuje závislost úspěšnosti příjmu na šumu a počtu najednou přijímaných paketů. Jednotlivé pakety byly náhodně vzájemně posunuty až o $16\,\mathrm{B}$, podobně jako při skutečném příjmu. Z grafu je vidět, že příjem na všech kanálech najednou zhoršuje úspěšnost, ale přijímač je stále funkční. Pro předpokládanou situaci kdy se potkají maximálně jednotky paketů je zhoršení zanedbatelné.

Úspěšnost příjmu při rozladění nosných frekvencí ukazuje Obrázek 3. Simulovaný signál byl při náhodném SNR mezi $12\,\mathrm{dB}$ a $16\,\mathrm{dB}$ frekvenčně posunut o zlomek šíře kanálu. Přijímač přestává pracovat při posunu o

$$0.2 \cdot \frac{1}{T_c} = 0.2 \cdot 37.5\,\mathrm{kHz} = 7.5\,\mathrm{kHz} \tag{5}$$



Obrázek 4. Skutečný test na hraně dosahu CC1200.

To je možná méně než by zvládl hardwarový GFSK přijímač [8], ale pro základní kompenzaci nezkalibrovaného vysílače to dostačuje. Křivka na pravé straně grafu znázorňuje přijetí paketu na sousedním kanálu.

Testy na skutečném hardware byly provedeny ve staré univerzitní budově. Pakety byly vysílány z jednoduché desky s transceiverem CC1200 a mikroprocesorem STM32 a přijímány na RTL-SDR napojeném na Matlab Simulink v nekonečné simulaci.

Při pokusu na vzdálenost zhruba $1\,\mathrm{m}$ bylo přijato $99.90\,\%$ vyslaných paketů. Přebuzení přijímače a deformace signálu způsobily příjem několika paketů na vícero kanálech najednou. Důvodem je opět nepřizpůsobovat se jednomu blízkému vysílači čímž by byly utlumeny ostatní.

Při vzdálenosti zhruba $30\,\mathrm{m}$ a jedno podlaží byla úspěšnost příjmu ještě vyšších $99.98\,\%$. Obrázek 4 ukazuje pokus příjmu přes dvě podlaží, vzdálenost zhruba $50\,\mathrm{m}$ a za několika zdmi. Při tomto umístění už vysílání přestával přijímat stejný transceiver CC1200. V této situaci bylo přijato $95.03\,\%$ paketů. Pakety byly popořadě vysílány na různých kanálech, aby šlo jednoduše odvodit, na kterých kanálech nebyl paket přijat. Na grafu je vidět propad na nejnižších kanálech, který se na simulacích neprojevil. Důvodem bude nejspíš charakteristika přijímače.

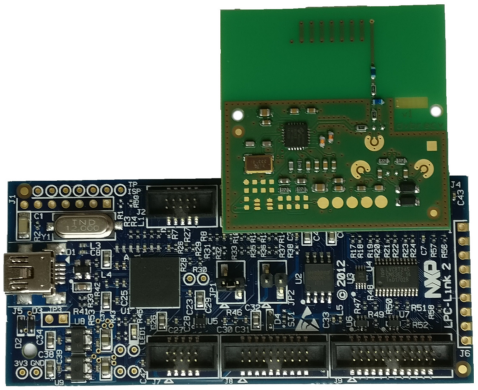
Až potud bude přijímač dokumentován přijatým, ale zatím nepublikovaným, článkem [9].

IV. Zmenšení do Cortex-M mikroprocesoru

Navržený přijímač je sice funkční a vyrovná se i komerčnímu transceiveru, ale není příliš praktický. Použitý Matlab Simulink cenou zastiňuje levný hardware a i pokud by byl provozován na Raspberry-Pi, celý přijímač je příliš velký.

Potřebný výpočetní výkon je na hraně dnešních Cortex-M procesorů. Pro další práci byl zvolen LPC4370, který sice nyní už není nejvýkonnější, ale obsahuje rychlý ADC. Existující vývojová deska LPC-Link 2 usnadní práci s BGA čipem. Na připravené konektory bylo potřeba navrhnout vlastní desku s demodulátorem a anténou.

Jako demodulátor byl použit R820T2, který je použitý i v RTL-SDR. Většina těchto součástek nemá vůbec zveřejněnou dokumentaci, což je velký problém a důvod proč R820T2 je i s velmi omezenou dokumentací tak oblíbený. Diferenciální



Obrázek 5. LPC-Link 2 s deskou demodulátoru.

Tabulka I
ČAS POTŘEBNÝ PRO VYBRANÉ VÝPOČTY

Výpočet	**Čas [µs]**
Bitový posun	1.34
Roznásobení cos a -sin	1.42
Decimace a FIR	5.66
Komplexní FFT, 64 prvků	13.46
Reálné FFT, 128 prvků	21.46
Druhá mocnina magnitudy	2.67

výstup demodulátoru byl bez zesílení napojen na diferenciální AD převodník v procesoru. Výslednou desku plošných spojů zobrazuje Obrázek 5.

Mikroprocesor LPC4370 obsahuje jedno jádro Cortex-M4 a dvě Cortex-M0 běžící na 204 MHz. Na téměř všechny výpočty lze použít CMSIS-DSP knihovnu, která je vysoce optimalizovaná pro Cortex-M procesory. Výpočet FFT téměř úplně zaneprázdní jádro M4 a zbytek přijímače tak připadne na dvě slabší jádra.

První pokus bylo nasnímaný signál frekvenčně posunout o čtvrtinu vzorkovací frekvence, filtrovat, decimovat a spočítat 64 vzorkové FFT. Decimování a FIR filtrace je potřeba provést dvakrát a součtem podle Tabulky I se ihned dostaneme přes 26.67 µs, což je čas dostupný při zachování komunikační rychlosti z předchozí implementace.

Celý proces lze zjednodušit použitím většího reálného FFT. Nasnímaný signál lze po bitovém posunu ihned vložit do FFT, které je optimalizováno pro reálný vstup. Nevýhodou je, že několik nejnižších kanálů nebude použitelných, protože demodulátor nejnižší frekvence filtruje. Nakonec je použit výpočet druhé mocniny magnitudy. Druhá mocnina magnitudy bude možná komplikovat vyhodnocení, ale ušetří spoustu odmocnin. Výpočty celkem trvají 25.47 µs a to už se s malou rezervou vejde do časového limitu.

V. Závěr a cíle

Zatím se podařilo navrhnout přijímač umožňující zavedení Spread Spectrum do oblastí kde zatím převládají jednofrekvenční sítě. Řešení umožní navrhnout senzorovou síť využívající FHSS i při zachování spotřeby srovnatelné se stávajícím řešením. Přijímač je zatím nepraktický a další prací bude dokončit miniaturizaci přijímače do mikroprocesoru LPC4370. Výsledek by už mohl být cenově i velikostně zajímavý pro výrobce zabezpečovací techniky a domácí automatizace. Hotový přijímač bude potřeba podložit základním měřením, i když od prototypu nejsou očekávány oslnivé parametry. Běžné komunikační desky plošných spojů se ještě dlouho a jemně dolaďují, tak jako je jistě i RTL-SDR, ale nikoliv mnou navržený prototyp.

Následující výzkum bude směřovat k výkonnějšímu softwarovému rádiu. K dispozici jsou moduly rádia a FPGA s mnohem větším výpočetním výkonem a lepším analogovým koncem. Zatím jsou tyto moduly příliš drahé pro použití v malé elektronice, ale během několika let se mohou objevit, stejně jako donedávna nepředstavitelné přímé softwarové rádio [10]. Výkonnější elektronika v některých prvcích sítě navíc umožní paralelizaci, vyšší datové toky nebo zjednodušení komunikace pro bateriemi napájené senzory. Další cíle disertační práce:

- Miniaturizovat popsaný přijímač do LPC4370.
- Navrhnout složitější metody komunikace při využití FPGA. Použít kombinaci FHSS a Orthogonal Frequency Division Multiplex (OFDM) v jedné asymetrické komunikační síti na zařízeních z nichž některá mohou používat softwarové rádio.
- Ověřit metody implementací a porovnat výsledky.

Uznání

Příspěvek byl částečně podpořen Studentskou Grantovou Soutěží 2018 na FM TUL.

S návrhem a výrobou části hardware pomohla společnost JABLOTRON ALARMS a.s..

Poděkování si zaslouží i projekt Airspy jehož otevřené zdrojové kódy velmi pomohly s nastavením nezdokumentovaných částí demodulátoru.

Reference

[1] N. H. Motlagh, “Frequency Hopping Spread Spectrum: An Effective Way to Improve Wireless Communication Performance,” *Advanced Trends in Wireless Communications*, 2011.
[2] N. Tesla, “Method of signaling,” U.S. Patent 723 188, 1903.
[3] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, “Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario,” in *2013 IEEE International Wireless Symposium*, 2013.
[4] T. Jakubík and J. Jeníček, “Asymmetric Low-power FHSS Algorithm,” in *Proceedings of the IEEE 13th International Workshop On Electronics, Control, Measurement, Signals and their Application in Mechatronics*, 2017.
[5] *EN 300 220-2*, ETSI Std., Rev. 3.1.1, 2017.
[6] J. So and Y. Kim, “Interference-aware frequency hopping for Bluetooth in crowded Wi-Fi networks,” *Electronics Letters*, 2016.
[7] M. Rice, *Digital Communications: A Discrete-Time Approach*. Pearson Education, Inc., 2009.
[8] *CC120X Low-Power High Performance Sub-1 GHz RF Transceivers*, Texas Instruments Incorporated, 2013.
[9] T. Jakubík and J. Jeníček, “SDR All-channels Receiver for FHSS Sensor Network,” in *2018 International Conference on Applied Electronics (AE)*, 2018.
[10] A. Collins, *All Programmable RF-Sampling Solutions*, Xilinx, 2017.

Dummy Rounds jako opatření proti DPA v hardwaru

Stanislav Jeřábek
Druhý ročník, prezenční studium
Jan Schmidt, Martin Novotný

České vysoké učení technické v Praze, Fakulta Informačních technologií
Thákurova 9, 160 00 Praha 6
jerabst1@fit.cvut.cz

***Abstrakt*—Tato práce popisuje techniku Dummy Rounds jako protiopatření vůči DPA v hardwarových implementacích rundovních šifer. Princip je inspirován dobře známými metodami používaných v hardwaru jako skrývání a dynamická rekonfigurace stejně jako metodami z softwarových implementací jako nadbytečné cykly, náhodné provádění instrukcí nebo skrývání v čase. Tato metoda inspirovaná dynamickou rekonfigurací kombinuje skrývání spotřeby se skrýváním v čase. V této práci také diskutujeme množství náhodnosti dostupné pro kontrolu výpočtu.**

***Klíčová slova*—dynamická rekonfigurace, skrývání, FPGA, DPA, skrývání v čase, dummy rounds.**

I. Motivace

Požadavky na spolehlivost stále rostou. Jedno z možných kritických ohrožení, kterým musí být v moderních číslicových systémech zabráněno, je únik dat. Některé z klasických *útoků postranními kanály* jsou založeny na měření spotřeby [1] nebo elektromagnetického záření [2]. Napadané šifry jsou většinou iterativní. Nejběžnějšími třídami iterativních šifer jsou Feistelovy šifry [3] jako DES [4], nebo novější Substitučně-permutační šifry [5] jako AES [6] nebo PRESENT [7]. Iterační kroky se jmenují *rundy* a v každé z nich jsou prováděny podobné výpočty. Tato podobnost velmi zjednodušuje implementaci, ovšem jednotlivé iterace mohou být odlišeny a některé okamžiky v průběhu výpočtu pak využity ke kryptoanalýze. Jedna z možností je tyto okamžiky před útočníkem *skrýt*.

Tato práce popisuje použití přidaných rund a randomizace ke skrytí spotřeby jako prevenci před Rozdílovou odběrovou analýzou (DPA) [1]. Technika *Dummy Rounds* se již dříve objevila u SW implementací [8]. Metody Dummy Rounds je podobná také dalším SW protiopatřením jako Dummy Cycles [9], Random Order Execution [10], nebo Shuffling [11]. Dummy Rounds také byla ve spojení s dalšími metodami použita jako ochrana proti útokům s využitím chyb [8] [12] [13]. Jelikož některé z těchto metod selhaly [14] [15], omezili jsme výzkum pouze na ochranu vůči DPA. Dummy Rounds byla také již použita proti DPA [16], nicméně princip v tomto případě zůstává podobný tomu v jiných SW implementacích – vložení dalších rund či jejich částí.

Metoda Dummy Rounds jak ji navrhujeme, kombinuje SW skrývání v čase s běžným skrýváním spotřeby v hardwaru. V hardwaru je implementováno více zřetězených částí (rund), které jsou vždy všechny výpočetně zpracovány, ale v daném hodinovém cyklu je jako výstup použit výstup pouze jedné z nich náhodně určené. Struktura návrhu je tak stejná pro každý hodinová cyklus a spotřeba zůstává stejná, zatímco logická funkce obvodu se mění. Takové chování je možné vnímat jako druh dynamické rekonfigurace, jejíž princip je používán také jinde [17] [18] [19].

Ačkoliv se výpočet v daných cyklech mění, výsledek zůstává správný díky (stále náhodnému) plánování rund. V kapitole II je podrobný popis metody Dummy Rounds, následován případovou studií šifry PRESENT [7] v FPGA a výsledky měření v kapitole III. Úpravy metody Dummy Rounds navrhované na základě výsledků měření jsou popsány jako následný výzkum v kapitole IV.

II. Dummy Rounds jako protiopatření vůči DPA

A. Architektura a fungování

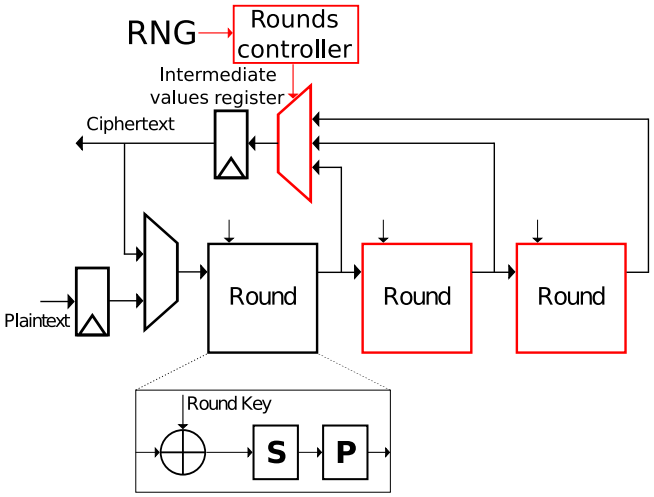
Předpokládejme rundovní šifru s C rundami. Také předpokládejme implementaci, kde může být spočteno v každém taktu nejméně m a nejvýše M rund. Pak použijeme metodu Dummy Rounds z Obrázku 1, kde $m = 1$ a $M = 3$. Použitím čtvrtého vstupu multiplexoru můžeme umožnit $m = 0$. Řízení rund určuje, výsledek kolikáté rundy bude v daném hodinovém cyklu použit. Nepoužité rundy stále spotřebovávají energii, ale jejich výpočty se nikam neuloží. Stálá míra přepínání signálů je také principem protiopatření zvaného skrývání [20] [21]. Metoda Dummy Round je použitelná jak pro Feistelovy šifry [3] tak také Substitučně-permutační šifry [5].

Aplikace metody Dummy Rounds má dva důležité parametry. Maximální počet rund spočtených v jednom hodinovém cyklu M určuje hodinovou frekvenci a ovlivňuje režijní náklady na čas i plochu. Průměrný počet akceptovaných rund pak určuje (konstantní) počet hodinových cyklů celého šifrování a tím i časovou režii.

Konstantním počtem cyklů zamezíme nebezpečí možného úniku informací kvůli extrémním náhodným hodnotám. Bez něj existuje malá pravděpodobnost, že návrh náhodně spočte v každém cyklu jednu rundu (nebo jinou hodnotu m). Tento případ z délky celého šifrování útočník snadno pozná a může na šifru zaútočit jako na nechráněnou. V případě náhodného použití M v každém taktu je situace velmi podobná. S

parametrem konstantního počtu hodinových cyklů a řadičem pro řízení rund dříve popsaná situace nemůže nastat.

Představme parametry na implementaci šifry PRESENT. Šifra má 31 rund a navíc jednu operaci *XOR* s rundovním klíčem, kterou považujeme za další rundu. Předpokládejme, že původní architektura má právě jednu rundu, což je běžné. Dále předpokládejme implementaci s parametrem $M = 3$, což je praktická volba ve většině případů. Takto potřebujeme $N = 16$ hodinových cyklů s průměrně 2 přijatými rundami. Perioda hodinového signálu pak bude zhruba třikrát delší, tedy časová režie přibližně 50 %. Runda je v rámci návrhu stěžejním prvkem, tedy horní hranice prostorové režie je 200 %.



Obrázek 1. Schéma Dummy Rounds metody. Upraven obrázek z [18].

B. Řízení rund

Řadič rund má dva úkoly. Prvním je zajistit provedení správného počtu rund v daném počtu cyklů. Dalším je zabránit jednotným průběhům výpočtu. V našem případě je řízení implementováno v hardwaru a mělo by tak být co nejjednodušší.Pro splnění prvního úkolu musí řadič sledovat počet rund přijatých v jednotlivých cyklech. Nechť c_n je počet rund přijatých od začátku až po krok n, kde $n \leq N$, včetně. Pak

$$c_n \leq Mn \tag{1}$$

$$c_n \geq mn \tag{2}$$

Aby bylo možné dosáhnout spočtení právě C v kroce N, musí platit následující

$$c_n + m(N-n) \leq C \tag{3}$$

$$c_n + M(N-n) \geq C \tag{4}$$

Pro příklad prostoru omezeného těmito nerovnicemi uvádíme Obrázky 2 a 3. Všimněme si, jak malá změna v jednom parametru ($m = 0$ namísto $m = 1$) může způsobit velkou změnu v ohraničení tohoto prostoru.Jakmile se řadič rozhodne v kroku n právě s_n rund v dalším cyklu, musí pro výsledný počet přijatých rund po tomto kroku c_{n+1} platit následující nerovnice 3 a 4

$$s_n \leq C - m(N-n-1) - c_n \tag{5}$$

$$s_n \geq C - M(N-n-1) - c_n \tag{6}$$

Toto jsou minimální požadavky zaručující správnost. Jednoduchý řadič nemusí využít celý prostor ohraničený nerovnicemi 1 až 4. Sofistikovanější řadič může reagovat před použitím nerovnic 3 a 4 a pouze upravit pravděpodobnosti příští náhodné hodnoty pro dosažení lepší náhodnosti.

Pokračujme s příkladem šifry PRESENT, kde $M = 3$. Výstup z náhodně zvolené rundy (1 až 3) je uložen do výstupního registru. Řadič musí zajistit, aby zvolený počet rund c_n během n kroků nevybočil do zakázaného prostoru na Obrázku 2. S parametry zvolenými pro tento příklad existuje 5 196 627 možností, jak během 16 taktů vyhodnotit 32 rund při dodržení všech podmínek. Tento počet byl určen empiricky jako počet řad o 16 přirozených číslech od jedné do tří, kde je jejich součet 32. DPA je nicméně obvykle použito k útoku na první či poslední rundu, takže ne všechny tyto možnosti jsou z pohledu útočníka odlišné.

Naše metoda stejně jako spousta ostatních (například [18]) vyžaduje přítomnost RNG. Jelikož samotný RNG může být zranitelný různými útoky, máme díky HW implementaci možnost použít TRNG.

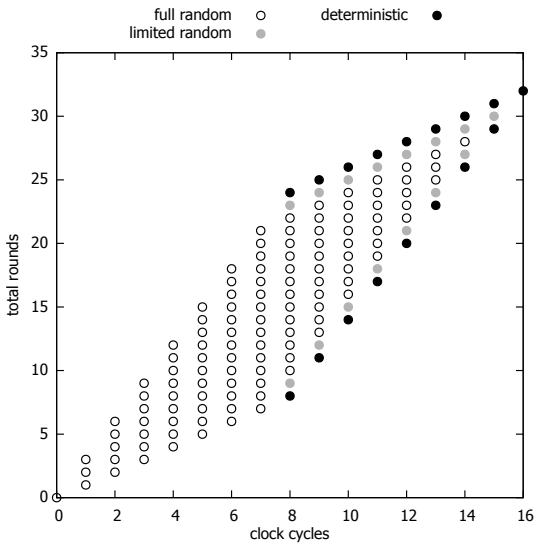
III. Implementace a výsledky

Jako případovou studii pro experimentální vyhodnocení jsme zvolili šifru PRESENT se 3 rundami. Počet hodinových cyklů na jedno šifrování je 16. Jako RNG používáme 64 bitový zpětnovazební posuvný registr s ireducibilním polynomem $g(x) = x^{64} + x^{63} + x^{61} + x^{60} + 1$. Ten je na začátku nastaven samými jedničkami a svoji hodnotu mění v každém hodinovém taktu použitého FPGA.

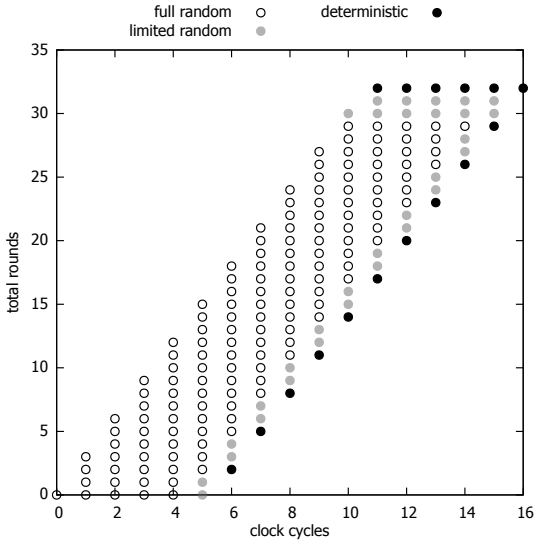
Stav řadiče obsahuje aktuální dosavadní počet cyklů a přijatých rund. V každém stavu řadič zkontroluje soulad přijaté náhodné hodnoty a nerovnic 5 a 6. Hodnoty mimo přípustné rozmezí jsou nahrazeny nejbližšími přípustnými. Stavový prostor je na Obrázku 2. Všimněte si menšího počtu stavů s omezeným připustným rozhodováním než na Obrázku 3.

Návrh popsaný výše byl vyhodnocen na implementaci v FPGA na desce SAKURA-G [22]. Naměřili jsme pro každou variantu 100 000 průběhů spotřeby a vyhodnotili je jednorozměrným nespecifickým Welschovým t-testem prvního řádu, jak je popsán v [23]. T-hodnoty naměřených průběhů spotřeby jsou na Obrázku 4, kde jsou na ose X vyznačeny náběžné hrany hodinového signálu. T-hodnoty pak vyjadřují míru množství informace obsažené ve spotřebě. V našem případě je maximální t-hodnota 346, zatímco je obvykle za hraniční hodnotu pro zabezpečený návrh považováno 4,5.

Největší únik informace je samozřejmě ze začátku šifrování. V prvním cyklu je pravděpodobnost přesně jedna třetina, že po jejím konci registr pro průběžné hodnoty obsahuje výsledek pouze první rundy. Tato průběžná hodnota bude muset být skryta za použití jiné metody nebo alespoň znáhodnění pozice začátku šifrování v čase.



Obrázek 2. Stavový prostor řadiče rund pro $m = 1$ and $M = 3$.

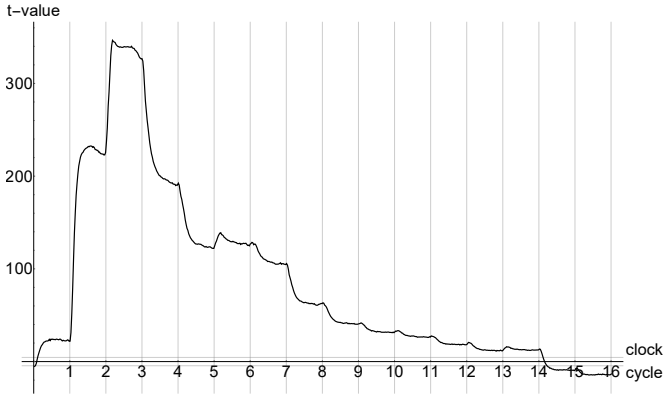


Obrázek 3. Stavový prostor upraveného řadiče rund pro $m = 0$ and $M = 3$.

Také jsme vyhodnotili jak chování návrhu závisí na počtu rund v jednotlivých cyklech. Vedle původní verze s 64 bitovým zpětnovazebním posuvným registrem jsme implementovali tyto verze:

1) Počítající právě 2 rundy v každém taktu.
2) Začínající s 8 takty po jedné rundě a končící 8 takty po třech rundách.
3) Začínající s 8 takty po třech rundách a končící 8 takty po jedné rundě.
4) Střídající takty po jedné a třech rundách, začínající jednou rundou v prvním taktu.
5) Střídající takty po jedné a třech rundách, začínající třemi rundami v prvním taktu.

Nejhůře dopadla verze číslo 3 (maximální t-hodnota 804), zatímco verze číslo 1 má nejlepší výsledky (maximální t-hodnota 267). Vliv *náhodných* hodnot na chování obvodu budeme studovat i nadále.



Obrázek 4. T-hodnoty šifry PRESENT s počátečním Dummy Rounds protiopatřením.

IV. Budoucí výzkum

Obecně jsou výsledky Dummy Rounds metody zatím neuspokojivé. Budeme nadále studovat vliv náhodných hodnot řídících celý návrh. Tato kapitola shrnuje možné cesty.

A. Počet hodinových taktů

Implementovali jsme šifru s konstantním počtem hodinových cyklů. Toto rozhodnutí bylo učiněno z důvodu možného úniku informace způsobeného různou délkou šifrování popsaným v podkapitole II-A.Nicméně tyto architekturní parametry mohou mít nepříznivý vliv na náhodnost. V našem případě (počítáme 32 rund v 16 taktech) víme, že počet taktů s jednou rundou je shodný jako počet taktů se třemi rundami. Navíc víme, že v ostatních taktech jsou spočítány právě 2 rundy.

B. Falešné výpočty

Také bychom mohli prodloužit délku šifrování ukrýt šifrování (teoreticky s proměnnou délkou) uvnitř delšího, částečně falešného výpočtu. DPA útoky obecně cílí na první či poslední rundu, takže prakticky ztížíme útok přítomností náhodně dlouhého falešného šifrování před začátkem a po konci požadovaného výpočtu. Začneme šifrování s nějakou náhodnou hodnotou, poté načteme správný otevřený text, provedeme šifrování, uložíme výsledek do registru, a poté načteme náhodnou hodnotu pro další falešné šifrování na konci výpočtu. Musíme pouze dosáhnou konstantní délky výpočtu z pohledu útočníka.

Rozšíření je také nutné při $m = 0$. Jinak by bylo triviální v průbězích spotřeby najít hodinové cykly bez akceptované rundy díky extrémně nízké spotřebě.

C. Rundovní řadič

Dále zvažujme chování rundovního řadiče. V první verzi zahrnující pouze nezbytné podmínky, řadič mění náhodnou hodnotu v případě potřeby, jak je ukázáno na Obrázcích 2

a 3. Mohli bychom dosáhnout náhodnějšího rozdělení vygenerováním počtů přijatých rund v cyklech předem a následnou permutací. Proti jsou ovšem paměťové nároky.

Samotná metoda Dummy Rounds je ohrožena například lokalizovaným elektromagnetickým útokem [24]. Tím se může útočník zaměřit na spotřebu pouze jedné rundy a získat tak více informace. Také proto je součástí další práce kombinování Dummy Rounds s již známými protiopatřeními popsanými v [18] a vyhodnocení těchto kombinací.

V. Závěr

Protiopatření Dummy Rounds popsané v této práci je snadno aplikovatelné pro každou rundovní šifru. Návrhář musí jen zkopírovat rundu jako takovou a přidat multiplexor řízený řadičem používajícím RNG. Může být kombinováno s dalšími protiopatřeními. Tato metoda je silně závislá na RNG podobně jako další běžně používaná protiopatření.

Výsledky statistického vyhodnocení prvotní implementace t-testem nejsou zatím uspokojivé. Maximální t-hodnota je 346, přičemž za hraniční hodnotu pro zabezpečený návrh je považováno 4,5. Nicméně další experimenty ukazují možná vylepšení řízením náhodnosti, prozatím snižující t-hodnotu na 267. Proto je pro zjištění potenciálu této metody důležité implementovat další navrhované úpravy diskutované v kapitole IV této práce.

Poděkování

Děkuji Prof. Dr.-Ing. Tim Güneysu za přínosné konzultace.

Tento výzkum byl částečně finančně podpořen z grantu GA16-05179S České grantové agentury "Fault Tolerant and Attack-Resistant Architectures Based on Programmable Devices: Research of Interplay and Common Features" (2016-2018), projektu CELSA "DRASTIC: Dynamically Reconfigurable Architectures for Side-channel analysis protection of Cryptographic implementations" (CELSA/17/033) a grantu ČVUT SGS17/213/OHK3/3T/18.

Reference

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side—channel(s)," in *Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, ç. K. Koç, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 29–45.

[3] H. Feistel, "Cryptography and computer privacy," *Scientific american*, vol. 228, no. 5, pp. 15–23, 1973.

[4] D. E. Standard *et al.*, "Federal information processing standards publication 46," *National Bureau of Standards, US Department of Commerce*, vol. 4, 1977.

[5] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[6] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," 1999.

[7] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "Present: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 450–466.

[8] B. Gierlichs, J.-M. Schmidt, and M. Tunstall, "Infective computation and dummy rounds: Fault protection for block ciphers without check-before-output," in *Progress in Cryptology – LATINCRYPT 2012*, A. Hevia and G. Neven, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 305–321.

[9] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Cryptographic Hardware and Embedded Systems — CHES 2000*, Ç. K. Koç and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 252–263.

[10] S. Tillich, C. Herbst, and S. Mangard, "Protecting aes software implementations on 32-bit processors against power analysis," in *Applied Cryptography and Network Security*, J. Katz and M. Yung, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 141–157.

[11] N. Veyrat-Charvillon, M. Medwed, S. Kerckhof, and F.-X. Standaert, "Shuffling against side-channel attacks: A comprehensive study with cautionary note," in *Advances in Cryptology – ASIACRYPT 2012*, X. Wang and K. Sako, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 740–757.

[12] S. Patranabis, A. Chakraborty, and D. Mukhopadhyay, "Fault tolerant infective countermeasure for aes," in *Security, Privacy, and Applied Cryptography Engineering*, R. S. Chakraborty, P. Schwabe, and J. Solworth, Eds. Cham: Springer International Publishing, 2015, pp. 190–209.

[13] S. Patranabis and D. Mukhopadhyay, *Infective Countermeasures Against Fault Analysis*. Singapore: Springer Singapore, 2018, pp. 197–211.

[14] A. Battistello and C. Giraud, "Fault analysis of infective aes computations," in *2013 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Aug 2013, pp. 101–107.

[15] H. Tupsamudre, S. Bisht, and D. Mukhopadhyay, "Destroying fault invariant with randomization," in *Cryptographic Hardware and Embedded Systems – CHES 2014*, L. Batina and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 93–111.

[16] C. Herbst, E. Oswald, and S. Mangard, "An aes smart card implementation resistant to power analysis attacks," in *Applied Cryptography and Network Security*, J. Zhou, M. Yung, and F. Bao, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 239–252.

[17] N. Mentens, B. Gierlichs, and I. Verbauwhede, "Power and fault analysis resistance in hardware through dynamic reconfiguration," in *Cryptographic Hardware and Embedded Systems – CHES 2008*, E. Oswald and P. Rohatgi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 346–362.

[18] P. Sasdrich, A. Moradi, O. Mischke, and T. Güneysu, "Achieving side-channel protection with dynamic logic reconfiguration on modern fpgas," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2015, pp. 130–136.

[19] P. Sasdrich, A. Moradi, and T. Güneysu, "Hiding higher-order side-channel leakage," in *Topics in Cryptology – CT-RSA 2017*, H. Handschuh, Ed. Cham: Springer International Publishing, 2017, pp. 131–146.

[20] J. L. Danger, S. Guilley, S. Bhasin, and M. Nassar, "Overview of dual rail with precharge logic styles to thwart implementation-level attacks on hardware cryptoprocessors," in *2009 3rd International Conference on Signals, Circuits and Systems (SCS)*, Nov 2009, pp. 1–8.

[21] D. Suzuki and M. Saeki, "Security evaluation of dpa countermeasures using dual-rail pre-charge logic style," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 255–269.

[22] H. Guntur, J. Ishii, and A. Satoh, "Side-channel attack user reference architecture board sakura-g," in *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)*, Oct 2014, pp. 271–274.

[23] T. Schneider and A. Moradi, "Leakage assessment methodology," *Journal of Cryptographic Engineering*, vol. 6, no. 2, pp. 85–99, Jun 2016. [Online]. Available: https://doi.org/10.1007/s13389-016-0120-y

[24] F. Unterstein, J. Heyszl, F. D. Santis, and R. Specht, "Dissecting leakage resilient prfs with multivariate localized em attacks - a practical security evaluation on fpga," *IACR Cryptology ePrint Archive*, vol. 2017, p. 272, 2017.

Prijímač pre bezdrôtový prenos energie plne integrovaný na čipe

Miroslav Potočný
2. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

Fakulta elektrotechniky a informatiky, Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava, Slovenská republika
miroslav.potocny@stuba.sk

***Abstrakt*—Tento príspevok sa zaoberá návrhom plne integrovaného prijímača pre bezdrôtový prenos energie v 130 nm CMOS technológii. Rozoberá hlavné problémy a výzvy návrhu takéhoto systému, predovšetkým slabú väzbu medzi vysielačom a prijímačom, ktorá má za následok nízke vstupné výkony a napätia. Preto sme sa najprv venovali návrhu usmerňovača schopného spracovať takýto vstupný signál. Následne sme navrhli plne integrovaný prijímač zložený z trojstupňového usmerňovača, prijímacej cievky a rezonančného obvodu. Rezonančný obvod má za úlohu zvýšiť vstupné napätie usmerňovača. Zahrnutím laditeľnej kapacity do tohto obvodu vieme ovládať vstupné napätie usmerňovača a tým zabezpečiť aj čiastočnú ochranu pred silným magnetickým poľom. V závere príspevku uvádzame tézy dizertačnej práce, ktoré bližšie opisujú budúce smerovanie nášho výskumu.**

***Kľúčové slová*—bezdrôtový prenos energie; zberač energie; implantovateľné medicínske zariadenia.**

I. Úvod

Rozvoj súčasných bezdrôtových aplikácií integrovaných obvodov (IO), napríklad v oblasti implantovateľných medicínskych zariadení (IMD) [1], [2], rádiofrekvenčnej identifikácie (RFID) [3], [4] alebo internetu vecí (IoT) [5], [6] vytvára požiadavku na neustále zmenšovanie ich rozmerov, znižovanie ceny a spotreby energie, ako aj predlžovanie ich životnosti. Rozmery takýchto elektronických systémov sú závislé najmä od použitej antény a batérie.

Ako možné riešenie pre predĺženie životnosti a zmenšenie rozmerov bezdrôtových elektronických systémov sa ukazuje využitie zberu energie z okolitého prostredia. Toto umožňuje výrazne predĺžiť životnosť batérie alebo dokonca jej úplné nahradenie. Pre plne integrované IMD systémy sa dá najjednoduchšie využiť prenos energie blízkym magnetickým poľom, keďže sú umiestnené v ľudskom tkanive [7].

V rámci nášho výskumu sa zaoberáme prenosom VF energie blízkym magnetickým poľom pre napájanie plne integrovaných IMD systémov s prijímacou cievkou na čipe. Takéto systémy však majú značné obmedzenia spojené s realizáciou celého systému v štandardnej CMOS technológii. Za hlavný faktor limitujúci takéto systémy považujeme veľmi slabú väzbu medzi vysielačom a prijímačom. Táto vyplýva z malých rozmerov prijímacej cievky. Nezanedbateľný vplyv má aj tkanivo, ktoré tvorí stratové prostredie pre prenášaný VF signál [8]. Obmedzené je aj použiteľné frekvenčné pásmo, ktoré je zhora ohraničené vlastnou rezonančnou frekvenciou integrovaných cievok. Naopak príliš nízke frekvencie vyžadujú veľké hodnoty pasívnych prvkov, ktoré nie sú prakticky realizovateľné na čipe. Ako najvýhodnejšie sa ukazuje pásmo 150–500 MHz [9], pre ktoré sme teda navrhovali aj prezentovaný prijímač pracujúci na frekvencii 200 MHz.

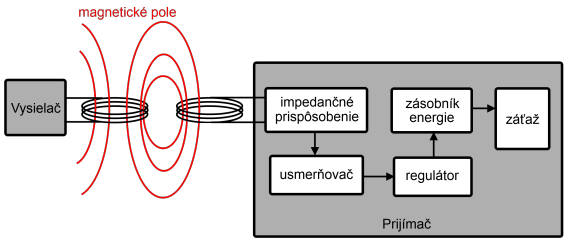
Táto práca je rozdelená nasledovne. Kapitola II opisuje hlavné časti bezdrôtového prijímača energie na systémovej úrovni. Kapitola III je venovaná doterajším výsledkom a je rozdelená na dve časti. Časť III-A je zameraná na návrh jedného stupňa VF usmerňovača a jeho porovnanie s doteraz publikovanými topológiami. Časť III-B je venovaná opisu plne integrovaného prijímača zrealizovaného v 130 nm CMOS technológii. V kapitole IV sú predstavené tézy dizertačnej práce. V kapitola V obsahuje stručné zhrnutie a uzatvára príspevok.

II. Systém bezdrôtového prenosu energie

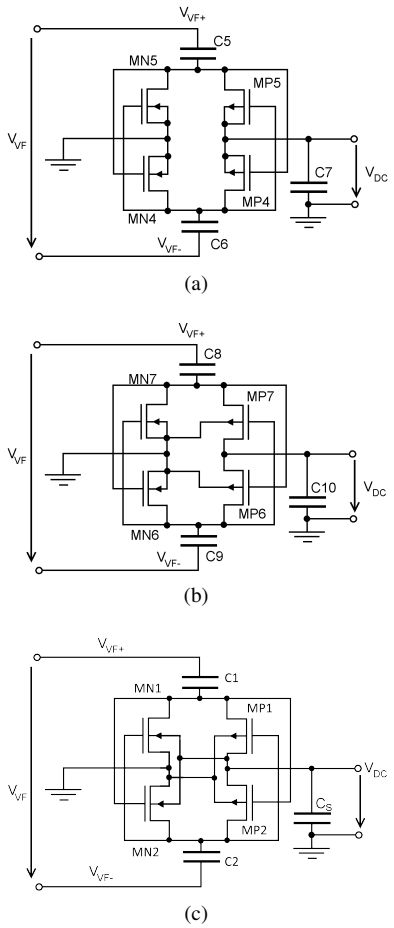
Hlavné časti systému na zber vysokofrekvenčnej energie z okolia sú zobrazené na obrázku 1. Takýto systém sa v súčasnosti využíva napríklad v obvodoch RFID alebo v bezdrôtových senzoroch používaných v zdravotníctve [10]. V tejto práci sa venujeme vysokofrekvenčnej časti prijímača pre takýto systém. Táto sa skladá z prijímacej cievky, obvodu impedančného prispôsobenia a usmerňovača. Zvyšné časti prijímača sú napájané jednosmerným výstupným napätím usmerňovača. Regulátor slúži na upravenie tohto napätia na úroveň vhodnú na napájanie zvyšných častí systému prijímača. Zároveň chráni zvyšok obvodu pred prepätím, ktoré môže vzniknúť pri vystavení prijímača silnému magnetickému poľu. Energia je zhromažďovaná v zásobníku, ktorý môže byť tvorený batériou alebo kondenzátorom. Ostatné obvody v tomto systéme sú napájané z tohto zásobníka, a teda tvoria záťaž pre systém prenosu energie.

Pre zamýšľanú aplikáciu v IMD systémoch treba uvažovať so špecifickými obmedzeniami. Tieto vyplývajú hlavne z parametrov cievok integrovaných na čipe [11], ale aj z parametrov biologického tkaniva v prenosovom kanáli [8]. V dôsledku týchto vplyvov je väzba medzi vysielačom a prijímačom veľmi slabá, čo má za následok malé vstupné výkony. Na zvýšenie efektivity usmerňovača sa v prijímači často využíva paralelný

rezonančný obvod, ktorý zvyšuje vstupné napätie prijímača. Táto funkcia je daná hlavne kvalitou cievky, ktorá je pre cievky integrované na čipe vo všeobecnosti nízka. Preto sme sa najprv zamerali na návrh usmerňovača pre veľmi malé vstupné výkony a napätia.



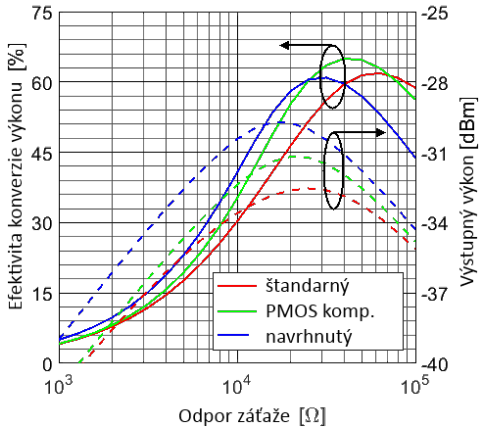
Obr. 1. Bloková schéma systému bezdrôtového prenosu energie.



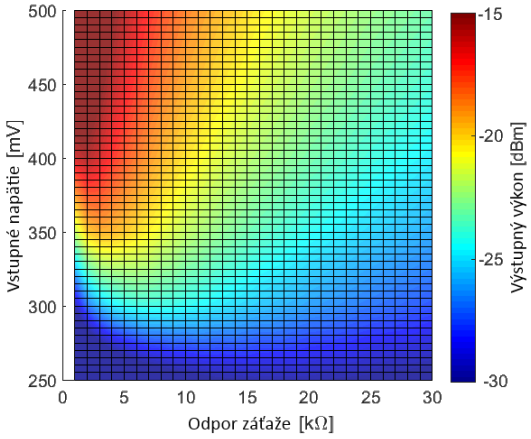
Obr. 2. Zapojenia VF usmerňovačov: štandardný [13] (a), PMOS kompenzovaný [14] (b), a nami navrhnutý (c).

III. Výsledky

Táto kapitola je venovaná doteraz dosiahnutým výsledkom. Najskôr budeme prezentovať návrh jedného stupňa pre integrovaný usmerňovač. Cieľom bolo vylepšiť vlastnosti doteraz publikovaných riešení pre nízke vstupné výkony a napätia. Na tento účel bol využitý prístup riadenia MOS tranzistorov substrátovou elektródou.



Obr. 3. Porovnanie usmerňovačov pri vstupnom napätí 250 mV. Plné čiary znázorňujú efektivitu konverzie výkonu, kým prerušované výstupný výkon.



Obr. 4. Výstupný výkon jedného stupňa navrhnutého usmerňovača v závislosti od amplitúdy vstupného signálu a odporu záťaže.

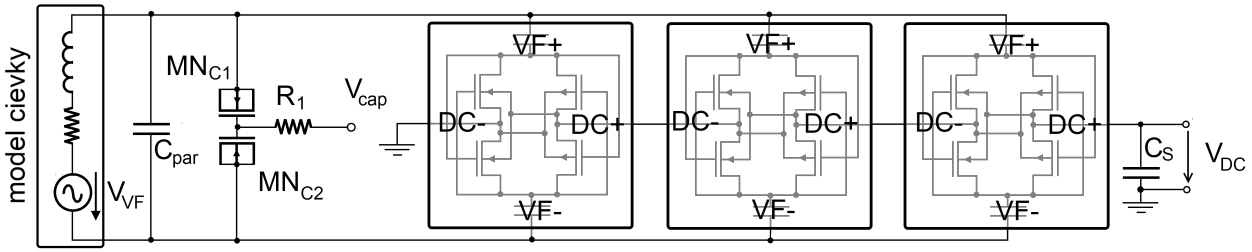
A. Usmerňovač

Hlavné zdroje strát v usmerňovačoch vyplývajú z vlastností spínacích elementov. Keďže nami navrhnutý usmerňovač má byť kompatibilný s CMOS výrobným procesom, tieto sú tvorené MOSFET tranzistormi. Dva parametre tranzistora, ktoré najviac ovplyvňujú efektivitu usmerňovača sú záverný prúd I_r a prahové napätie V_{TH} [12], definované rovnicami (1) a (2). Pre malé vstupné výkony má väčší vplyv V_{th}, preto sme sa zamerali na kompenzáciu vplyvu tohto parametra. Toto sa dá dosiahnuť práve pomocou riadenia substrátovej elektródy. Z rovníc (1) a (2) je možné pozorovať že, tieto parametre sú navzájom zviazané, takže znížením V_{th} dôjde k zvýšeniu I_r. Preto sa dá očakávať, že pri vysokých vstupných výkonoch, bude efektivita takto kompenzovaného usmerňovača nižšia.

$$I_r = I_0 \frac{W_g}{L_g} \exp\left(\frac{V_{GS} - V_{TH}}{n_s V_T}\right)\left(1 - \exp\left(\frac{-V_{DS}}{V_T}\right)\right) \quad (1)$$

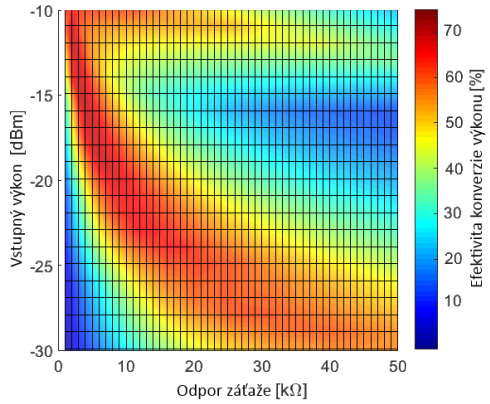
$$V_{TH} = V_{TH0} \pm \gamma\left(\sqrt{|2\Phi_F \pm V_{SB}|} - \sqrt{|2\phi_F|}\right) \quad (2)$$

Základ nášho usmerňovača tvorí štruktúra z [13]. Vylepšenie z [14], ktoré je založené na kompenzácii V_{TH} PMOS



Obr. 5. Schéma zapojenia navrhnutého prijímača energie.

tranzistorov sme rozšírili aj na NMOS tranzistory. Toto si vyžiadalo využitie izolovaných NMOS tranzistorov v trojitej jame. Schémy týchto zapojení sú na obrázku 2.



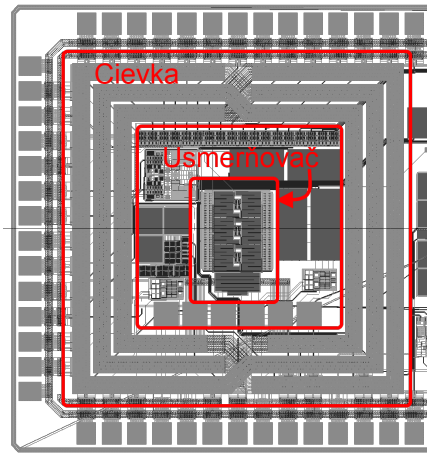
Obr. 6. Efektivita konverzie výkonu jedného stupňa navrhnutého usmerňovača v závislosti od amplitúdy vstupného signálu a odporu záťaže.

Nakoľko výsledky publikované v [13], [14] boli dosiahnuté pre rôzne vstupné výkony, v rôznych technológiách a pracovných frekvenciách, rozhodli sme sa ich porovnávať na základe simulácie pre podmienky špecifické pre uvažovanú aplikáciu. Tieto tri verzie usmerňovača boli analyzované pomocou obvodovej simulácie v prostredí Cadence Virtuoso za rovnakých podmienok a s rovnakými rozmermi prvkov. Porovnanie výstupných výkonov a efektivity konverzie výkonu (EKV) sú zobrazené na obrázku 3. V porovnaní s ostatnými riešeniami dosahuje nami navrhnutý usmerňovač najvyšší výstupný výkon. Je približne o 40 % vyšší ako u ostatných zapojení. Jeho EKV je však o niečo nižšia, čo je pravdepodobne spôsobené vyššími stratami v NMOS tranzistoroch v dôsledku zvýšeného zvodového prúdu.

Parametre usmerňovačov v takýchto aplikáciách sú závislé od vstupného signálu ako aj od zaťažovacieho odporu. Závislosť výstupného výkonu od týchto dvoch premenných je zobrazená na obrázku 4. Z grafu vyplýva, že pre danú vstupnú amplitúdu VF signálu existuje ideálna záťaž, pri ktorej dodáva usmerňovač najvyšší výkon. Podobný graf, ale s EKV usmerňovača je zobrazený na obrázku 6, kde môžeme pozorovať ideálnu hodnotu záťaže, tentoraz ale pre dosiahnutie maximálnej účinnosti konverzie energie.

B. Integrovaný prijímač

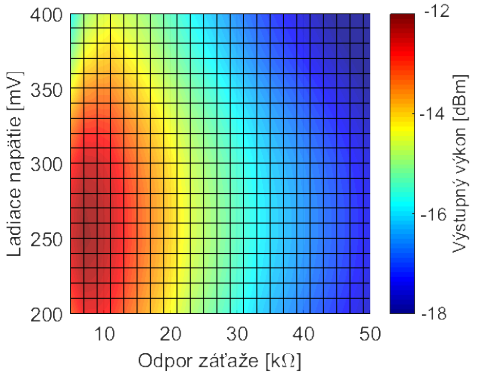
Schéma zapojenia integrovaného prijímača je na obrázku 5. Na základe vyššie opísaného návrhu jedného stupňa sme



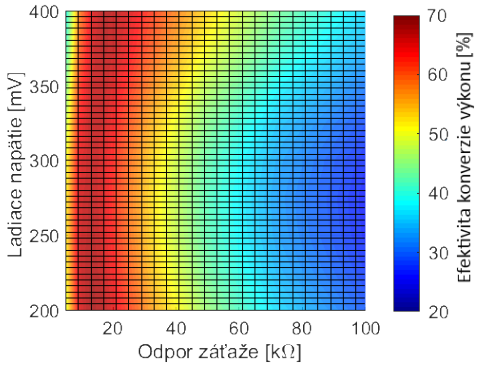
Obr. 7. Topológia časti prototypu čipu s prijímacou cievkou a usmerňovačom.

následne zrealizovali 3-stupňový usmerňovač v 130 nm CMOS technológii. Týmto sme dosiahli zvýšenie výstupného napätia, za cenu mierne nižšej efektivity. Zároveň bola na čipe integrovaná aj prijímacia cievka. Na zvýšenie vstupného napätia usmerňovača bol vytvorený paralelný rezonančný obvod pridaním napätím laditeľného kondenzátora paralelne s pevným kondenzátorom C_{par}. Tento bol realizovaný pomocou dvoch NMOS tranzistorov MN_{C1} a MN_{C2}, zapojených anti-sériovo ako kapacitné diódy. Ladiace napätie je privádzané na hradlá týchto tranzistorov cez oddeľovací rezistor R_1. Toto nám dovoľuje prelaďovať rezonančný obvod v rozsahu približne 190–230 MHz. Topológia testovacieho čipu s vyznačeným usmerňovačom a prijímacou cievkou je zobrazená na obrázku 7. Jednotlivé stupne usmerňovača sú tvorené zapojením z obrázku 2 (c).

Paralelný rezonančný obvod je použitý na zvýšenie vstupného napätia usmerňovača, ako bolo uvedené v predchádzajúcich kapitolách. Využitie laditeľnej kapacity v tomto obvode nám dovoľuje regulovať toto napätie, a tým aj výstupný výkon usmerňovača. Túto vlastnosť sme overili simuláciami celého zapojenia prijímača pri vstupnom napätí na cievke 150 mV a frekvencii vstupného signálu 200 MHz. Závislosť výstupného výkonu od ladiaceho napätia a odporu záťaže je zobrazená na obrázku 8. Účinnosť konverzie prijímača je zobrazená na obrázku 9, kde oblasť vysokej efektivity celého prijímača v ľavej časti grafu sleduje vysokú účinnosť usmerňovača z obrázku 6. Ak však tento trend porovnáme s grafom na obrázku 8, je zjavné, že sa v tomto pásme výrazne mení



Obr. 8. Výstupný výkon navrhnutého prijímača v závislosti od ladiaceho napätia a odporu záťaže.



Obr. 9. Efektivita konverzie výkonu navrhnutého prijímača v závislosti od ladiaceho napätia a odporu záťaže.

výstupný výkon. Efektivita sa príliš nemení, nakoľko dochádza aj k zmene vstupného výkonu. Preto je dôležité sledovať obe veličiny. Oblasť nízkej účinnosti v pravej časti grafu na obrázku 8 zodpovedá oblasti s vysokým vstupným napätím, kde narastajú straty v usmerňovači. Tieto zistenia budú použité v budúcnosti pri skúmaní možností riadenia prijímača. V súčastnosti sa venujeme návrhu vysielacej časti systému a meracieho pracoviska na overenie parametrov prijímača.

IV. Tézy dizertačnej práce

- Preskúmať prenosovú cestu systému na bezdrôtový prenos energie pre medicínske aplikácie s pomocou 3D simulácií elektromagnetického poľa, so zameraním na vplyv strát v tkanive.
- Navrhnúť a optimalizovať systém prijímača vysokofrekvenčnej energie integrovaného na čipe.
- Vyhodnotiť možnosti implementácie riadenia kapacity rezonančného obvodu prijímača na zabezpečenie ochrany systému proti silnému magnetickému poľu.
- Preskúmať možnosti riadenia zaťažovacieho odporu a rezonančnej kapacity na sledovanie bodu maximálneho dodaného výkonu pre rôzne vstupné výkony.
- Implementovať a experimentálne overiť integrovaný systém prijímača vysokofrekvenčnej energie.

V. Záver

Počas druhého ročníka štúdia bol navrhnutý a zrealizovaný plne integrovaný prijímač pre systém bezdrôtového prenosu energie. Jeho hlavnou časťou je nami modifikovaný usmerňovač, ktorý vďaka kompenzácii prahového napätia tranzistorov dosahuje vyššie výstupné výkony pri veľmi nízkych vstupných napätiach. Ďalšími časťami prijímača sú prijímacia cievka a laditeľná kapacita, ktorá slúži na ovládanie vstupného napätia usmerňovača. Pri overovaní sme sa zamerali na efektivitu ako aj výstupný výkon prijímača. V súčastnosti sa venujeme príprave meracieho pracoviska na overenie vyrobených vzoriek. Náš ďalší výskum bude zameraný na preskúmanie možností riadenia rezonančnej kapacity v prijímači za účelom regulácie jeho výstupného výkonu.

Poďakovanie

Táto práca bola podporená projektami APVV-15-0254 a VEGA 1/0905/17.

Literatúra

[1] F. Inanlou and M. Ghovanloo, "Wideband near-field data transmission using pulse harmonic modulation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 1, pp. 186–195, Jan 2011.

[2] R. R. Harrison, P. T. Watkins, R. J. Kier, R. O. Lovejoy, D. J. Black, B. Greger, and F. Solzbacher, "A low-power integrated circuit for a wireless 100-electrode neural recording system," *IEEE Journal of Solid-State Circuits*, vol. 42, no. 1, pp. 123–133, Jan 2007.

[3] A. Shameli, A. Safarian, A. Rofougaran, M. Rofougaran, J. Castaneda, and F. D. Flaviis, "A uhf near-field rfid system with fully integrated transponder," *IEEE Transactions on Microwave Theory and Techniques*, vol. 56, no. 5, pp. 1267–1277, May 2008.

[4] A. Radecki, H. Chung, Y. Yoshida, N. Miura, T. Shidei, H. Ishikuro, and T. Kuroda, "6w/25mm2 inductive power transfer for non-contact wafer-level testing," in *2011 IEEE International Solid-State Circuits Conference*, Feb 2011, pp. 230–232.

[5] S. Dey and N. C. Karmakar, "An iot empowered flexible chipless rfid tag for low cost item identification," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, Dec 2017, pp. 179–182.

[6] R. W. Porto, V. J. Brusamarello, I. Müller, F. L. C. Riaño, and F. R. D. Sousa, "Wireless power transfer for contactless instrumentation and measurement," *IEEE Instrumentation Measurement Magazine*, vol. 20, no. 4, pp. 49–54, August 2017.

[7] K. Fotopoulou and B. W. Flynn, "Wireless powering of implanted sensors using rf inductive coupling," in *2006 5th IEEE Conference on Sensors*, Oct 2006, pp. 765–768.

[8] S. Gabriel, R. W. Lau, and C. Gabriel, "The dielectric properties of biological tissues: Ii. measurements in the frequency range 10 hz to 20 ghz," *Physics in Medicine & Biology*, vol. 41, no. 11, p. 2251, 1996. [Online]. Available: http://stacks.iop.org/0031-9155/41/i=11/a=002

[9] A. S. Y. Poon, S. O'Driscoll, and T. H. Meng, "Optimal frequency for wireless power transmission into dispersive tissue," *IEEE Transactions on Antennas and Propagation*, vol. 58, no. 5, pp. 1739–1750, May 2010.

[10] K. Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication.*, 3rd ed. Hoboken, NJ: Wiley, 2010.

[11] M. Zargham and P. G. Gulak, "Maximum achievable efficiency in near-field coupled power-transfer systems," *IEEE Transactions on Biomedical Circuits and Systems*, vol. 6, no. 3, pp. 228–245, June 2012.

[12] B. Razavi, *Design of Analog CMOS Integrated Circuits*, ser. McGraw-Hill higher education. Tata McGraw-Hill, 2002.

[13] K. Kotani, A. Sasaki, and T. Ito, "High-efficiency differential-drive cmos rectifier for uhf rfids," *IEEE Journal of Solid-State Circuits*, vol. 44, no. 11, pp. 3011–3018, Nov 2009.

[14] A. K. Moghaddam, J. H. Chuah, H. Ramiah, J. Ahmadian, P. I. Mak, and R. P. Martins, "A 73.9 %-efficiency cmos rectifier using a lower dc feeding (ldcf) self-body-biasing technique for far-field rf energy-harvesting systems," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 4, pp. 992–1002, April 2017.

Zvyšování spolehlivosti a bezpečnosti číslicových obvodů na úrovni mikroarchitektury

Jan Bělohoubek
4. ročník, prezenční studium
Školitel: doc. Ing. Petr Fišer, Ph.D.
Školitel specialista: doc. Ing. Jan Schmidt, Ph.D.

Fakulta informačních technologií ČVUT v Praze
Thákurova 9, 160 00 Praha 6
jan.belohoubek@fit.cvut.cz

***Abstrakt*—Spolehlivost a bezpečnost jsou důležité vlastnosti vyžadované od mnoha zařízení. Zvýšení spolehlivosti a bezpečnosti systému lze dosáhnout mimo jiné vhodnou mikroarchitekturou. Dokončený výzkum se věnoval právě zvyšování spolehlivosti číslicových systémů na úrovni mikroarchitektury. Výzkum na něj bezprostředně navazující cílí na řešení spojující přístupy zajišťující zároveň bezpečnost i spolehlivost dílčích částí číslicových systémů. Velká část příspěvku je věnována rešerši, jež se váže k navrhovanému konceptu μTMR.**

***Klíčová slova*—Spolehlivost, bezpečnost, Time-Extended Duplex, dvoudrátová logika, monotónní obvod, postranní kanál**

I. Úvod

Spolehlivost a bezpečnost jsou důležité vlastnosti vyžadované od mnoha zařízení. Vzhledem k širokému použití číslicových (digitálních) systémů v různých podmínkách se stále zvyšují nároky kladené na spolehlivost (*dependability*, *reliability*, *safety*) a bezpečnost (*security*) těchto systémů.

Vysoká spolehlivost a bezpečnost zařízení (při zvážení provozních podmínek a konkrétního nasazení) je podmíněna dobrým návrhem architektury celého systému. Zvýšení spolehlivosti a bezpečnosti systému lze však dosáhnout i na úrovni mikroarchitektury – např. použitým návrhovým stylem, či speciálních logických prvků zaručujících určité vlastnosti. V některých případech je dokonce nutné použít speciální návrhové postupy na úrovni mikroarchitektury, aby bylo možné zajistit požadované vlastnosti na makroúrovni.

Některé prvky systému, např. kryptografické obvody, mohou vyžadovat zvýšenou úroveň zabezpečení proti možnému odcizení tajného klíče (příkonová charakteristika zařízení musí být nezávislá na zpracovávaných datech). Jiné části systému, např. řídící systém musí být schopen celý systém uvést při poruše do bezpečného stavu, apod.

Příspěvek je členěn takto: ve zbytku úvodní kapitoly jsou shrnuty cíle dizertační práce a současný stav jejího řešení. Kapitola II slouží jako stručná rešerše, ve které je shrnut současný stav problematiky okolo útoků na kryptografická zařízení se zaměřením na oblast současné výzkumné aktivity. V kapitole III je rozebrán současný stav řešení dosud rozpracované části práce.

Příspěvek se věnuje výhradně tématům výzkumu souvisejícím s dizertační prací. Ostatní aktivity a publikace jsou uvedeny na webu autora[1].

A. Cíle dizertační práce

V rámci výzkumu vedoucího k vypracování dizertační práce jsem se zaměřil na návrhové postupy na úrovni mikroarchitektury číslicových systémů, tj. na úrovni hradel a obvodů, vedoucí ke zvýšení spolehlivosti dílcích částí číslicového systému.

Vzhledem k důležitosti problematiky bezpečnosti, a s přihlédnutím k zaměření výzkumného pracoviště (*Digital Design research Group na FIT ČVUT*) a řešeným výzkumným grantům, se významná pozornost výzkumu soustředila také na hodnocení bezpečnosti kryptografických zařízení a jejího možného zvýšení právě z pohledu mikroarchitektury.

Oba cíle dizertační práce jsou vzájemně komplementární vzhledem k použitým metodám, simulačním a vývojovým prostředkům.

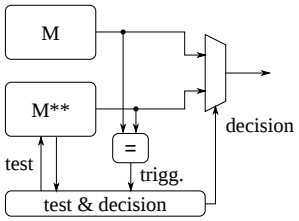
B. Dokončený výzkum: Time-Extended Duplex

Výzkum na nějž jsem se soustředil v prvních třech letech doktorského studia se zabýval návrhem spolehlivé architektury číslicových systémů – *Time-Extended Duplex (TED)* – kombinující redundanci v ploše a v čase, tak aby se minimalizovaly náklady na takové řešení (*area overhead*, *time overhead*). Konceptuální schéma výsledného řešení, které je hlediska plochy pro skupinu obvodů výhodnější než TMR (*Triple Modular Redundancy*), ale zároveň poskytuje srovnatelnou odolnost proti poruchám (*fault-tolerance*), je na obrázku 1.

Modul $\mathtt{M}^{\star\star}$ na obrázku 1 je testovatelný pomocí rychlého testu se 100% pokrytím poruch vzhledem k modelu poruch *trvalá 1/trvalá 0* (*stuck-at model*). Díky tomu je v případě poruchy možno lokalizovat poruchu a vybrat tak správný ze dvou výstupů duplexu.

Vzhledem ke speciálním vlastnostem umožňujícím rychlý test číslicového obvodu (jednotky cyklů) byly navrženy

[1] http://users.fit.cvut.cz/~belohja4/



Obrázek 1. Konceptuální schéma TED – jedná se o duplex se schopností opravy jedné chyby

speciální hradla inspirovaná metodami asynchronního návrhu [1]. Testovatelný obvod je navíc navržen jako modifikovaná $\mathtt{M}^{**}$ verze dvoudrátové logiky a je tedy monotónní [1].

Obdobnou problematikou se zabývali i Vierhaus [2], Kubalík [3], Borecký [4] nebo Baláž a Krištofík [5].

Dílčí výstupy výzkumu byly publikovány na řadě lokálních i mezinárodní workshopech a konferencích [JBn1], [JBn2], [JBn3], [JBn4], [JBr1], [JBr2].

Všechny výsledky, experimentální vyhodnocení a podrobný popis architektury a návrhového stylu byl publikován jako součást zprávy o průběhu doktorského studia (tzv. *minimum*) [JBn5] a v článku publikovaném v žurnálu *Microprocessors and Microsystems* [JBr3].

Do odevzdání dizertační práce bude ještě potřeba věnovat pozornost zobecnění podmínek umožňujícím krátký test číslicových obvodů s vysokým pokrytím poruch, případně možnostem realizace krátkého testu s vysokým pokrytím poruch při použití realističtějších poruchových modelů.

II. Útoky na kryptografická zařízení

I když jsou dnešní šifrovací algoritmy, např. AES s dostupnou technikou z principu neprolomitelné, tajný klíč, uložený v zařízení, je možno získat v reálném čase útokem na implementaci šifrovacího algoritmu v HW nebo v SW. Útokem se rozumí manipulace se zařízením, která má za cíl extrakci tajného klíče pomocí tzv. *postranního kanálu* (*side-channel*). Formálně řečeno: postranní kanál je sekundární projev zařízení umožňující kritické snížení entropie tajného klíče [6], [7].

Postranním kanálem může být jakýkoli proměnlivý (datově závislý) projev, např. čas výpočtu, odběr, EM vyzařování nebo dokonce chování při chybě. Podmínkou pro vedení útoku na HW kryptografické zařízení je (zpravidla) fyzický přístup k zařízení. Fyzický přístup je u některých zařízení omezen, avšak s rostoucím počtem *smart karet* nebo *IoT zřízení* (zařízení tzv. internetu věcí) se množství potenciálně zranitelných zařízení stále zvětšuje [8].

Útoky na kryptografická zařízení postranním kanálem můžeme rozdělit na [9]:

1) neinvazivní (non-invasive attack): měření běžných projevů zařízení: časová [10] a odběrová analýza – *Simple Power Analysis* (SPA) a *Differential Power Analyzis* (DPA) [11], [12], [9] – nebo analýza EM vyzařování, tj. *EM radiation*

2) poloinvazivní (semi-invasive attack): injekce přechodných poruch – EM impulzem nebo laserovým paprskem

3) invazivní (invasive attack): injekce trvalých poruch

A. Hodnocení útoků postranními kanály

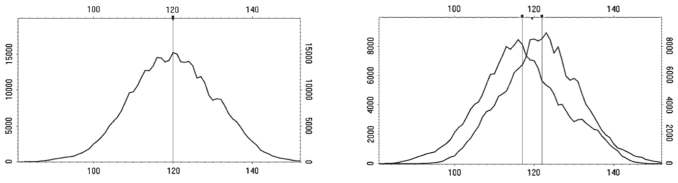
Závažnost různých typů útoku na kryptografické zařízení se obecně vyjadřuje náklady, které je nutné vynaložit k úspěšnému provedení útoku (*attack cost*), přičemž nejnebezpečnější útoky jsou takové, které lze provést s minimálním technickým vybavením, v minimálním čase a s minimálními znalostmi.

B. Neinvazivní útoky na základě příkonové analýzy

Z výše uvedeného důvodu jsou útoky na základě příkonové analýzy nejzkoumanější skupinou útoků a také skupinou útoků, kterým věnují největší pozornost výrobci HW. Postranním kanálem je zde příkonová charakteristika obvodu.

Útoky na kryptografická zařízení pomocí *příkonové analýzy* (*Simple Power Analyzis* (SPA) a *Differential Power Analyzis* (DPA)) byly představeny ve 2. pol. 90 let Kocherem a kol. [11], [12] z firmy Cryptography Research, Inc. (CRI) (od roku 2011 Rambus Inc.). Od té doby se intenzivní výzkum soustředil na jedné straně na metody útoků na kryptografická zařízení a na straně druhé na metody obrany (*countermeasures*). Společnost Rambus je dnes předním dodavatelem certifikovaných řešení odolných proti SPA/DPA [13].

Odběrová analýza pracuje s faktem, že odběr IC je datově závislý. Pouhým pohledem na odběrovou charakteristiku IC, v případě SPA, nebo pomocí matematické statistiky a za předpokladu velkého množství provedených měření, v případě DPA, lze odvodit tajný klíč používaný kryptografickým zařízením. Datovou závislost příkonové charakteristiky lze demonstrovat pomocí metody *rozdílu středních hodnot* [14] – viz obrázek 2.



Obrázek 2. Distribuce průběhu příkonové charakteristiky IC – pro směs všech průběhů a pro dvě směsi rozlišené dle hodnoty LSB (LSB = 0, resp. LSB = 1); převzato z [14]

C. Ochrany proti analýze odběru

Ochrany můžeme rozdělit i) na ty, které jsou aplikovány na úrovni mikroarchitektury – na úrovni tranzistorů a hradel, případně logického obvodu, rep. návrhového stylu a ii) na ochrany, které jsou aplikovány na úrovni algoritmu.

Na úrovni mikroarchitektury je cílem ochrany proti prosáknutí informace postranním kanálem snížením poměru signál/šum (*Signal to Noise Ratio (SNR)*. Toho lze dosáhnout zvýšením šumu (změna pořadí vykonávání nebo generování nekorelovaného šumu) nebo zmenšením signálu, tj. zvýšení nezávislosti mezi zpracovávanými daty a spotřebou.

Pro snížení závislosti průběhu příkonové charakteristiky na zpracovávaných datech se často používá *dvoudrátová logika*

(*Dual-Rail Precharge Logic*) v synchronní nebo asynchronní variantě, která je *monotónní* a pro každý signál pracuje zároveň s jeho komplementem. Upřednostňují se pak takové návrhové styly, které umožňují využít standardních knihovních buněk (*standard cells*) a nevyžadují tak tvorbu speciální knihovny pro každou technologii. Nejznámější takovou metodou je *Wave Dynamic Differential Logic (WDDL)* [15], [16], poměrně zajímavou alternativu představuje metoda *Dual Spacer Dual-Rail*, která umožňuje teoreticky dosáhnout naprosté nezávislosti zpotřebované energie na zpracovávaných datech (v průběhu jednoho cyklu) [17]. Další široce používanou metodou je *Masked Dual-rail with Pre-charge Logic (MDPL)* [13], [18], která vychází z dvoudrátové logiky, ale navíc přidává maskování na úrovni logických buněk.

Maskování na úrovni algoritmu je v principu silnější [16]. Používá se k odstranění závislosti odběru na zpracovávaných datech. Místo toho je odběr IC závislý na maskovaných datech. Nevýhodou těchto metod, např. *Boolean masking* [16] nebo *Threshold Implementation* je velmi výrazná penalizace v oblasti plochy, spotřeby a výkonu – např. $\approx$ 5x větší plocha u (velice efektivní) implementace od A. Moradiho a kol. [19].

Z důvodu obecně menší složitosti metod, větší přímočarosti implementace a zejména pak nižší penalizace v oblasti plochy, výkonu a spotřeby a zároveň uspokojivé bezpečnosti je v průmyslu preferována první skupina ochran proti analýze odběru [13]. De-fakto standardem jsou tak metody maskování založené na dvoudrátové logice.

D. Poloinvazivní a invazivní útoky na základě injekce poruch

Další široce zkoumanou skupinou útoků na kryptografická zařízení jsou útoky využívající injekce (trvalých nebo přechodných) poruch. Tyto metody lze kategorizovat dle způsobu injekce poruch, např.: optická injekce, glitch na hodinovém signálu, rušení napájení, elektromagnetický impulz, apod. Jejich historie sahá do roku 1996, kdy byla představena metoda *Differential Fault Analyzis (DFA)* [20].

Metoda DFA používá výstupy šifrovacího algoritmu bez přítomnosti poruchy a za přítomnosti poruchy pro totožný klíč. Na základě diferencí je pak možno výrazně zmenšit počet kandidátů tajného klíče nebo dokonce klíč přesně určit.

Další metodou je *Fault Sensitivity Analyzis (FSA)* [21], jejíž princip spočívá ve vyžití závislosti délky faktické kritické cesty v kryptografickém obvodu na zpracovávaných datech.

Velmi zajímavou metodou je *Safe-Error Attack (SEA)*, kde k určení tajného klíče postačuje informace o tom, zda injekce poruchy způsobila změnu hodnoty na výstupu, či nikoli [22].

E. Ochrany proti (polo)invazivním útokům

Základní ochranou proti útokům založeným na injekci poruch je detekce projevu poruchy, tj. chyby, založená na duplexní architektuře [23]. Je-li detekována chyba, vystaví se na výstup obvodu definovaná (neplatná) data – u dvoudrátové logiky typicky `NULL`, tj. `(0, 0)`.

Pro některé typy útoků, např. *Safe-Error Attack (SEA)*, však nemusí být detekce chyby dostatečná, protože stačí informace, zda injekce poruchy způsobila např. změnu hodnoty v registru – chybu je potřeba opravit, ne pouze detekovat.

F. Kombinované útoky

Z hlediska zranitelnosti kryptografických obvodů je velmi problematická skupina tzv. *kombinovaných útoků*, kde se pro získání tajného klíče využívá nejen znalost chybového/bezchybného výstupu, ale také jiného postranního kanálu, např. příkonové charakteristiky [24].

Takové útoky jsou potenciálně velmi nebezpečné, protože znamenají nutnost integrace ochran pro různé typy útoků tak, aby informace pokud možno neunikla žádným postranním kanálem.

III. Koncept μTMR pro kryptografické aplikace

Jako ochranu proti kombinovaným útokům a zároveň jako spolehlivostní řešení navrhuji koncept *μTMR*. Cílem μTMR je zvýšení odolnosti proti přirozeným zdrojům poruch i proti útokům injekcí poruch. Zároveň by μTMR mělo minimalizovat množství informace potenciálně dostupné přes všechny možné postranní kanály. To vše při co nejmenším nárůstu plochy a spotřeby a ideálně za použití standardních buněk.

Návrhový styl využívající μTMR použije tzv. *μ-voterů* rozprostřených v celém obvodu tak, aby detekce a oprava chyb (vniklých vlivem přirozených nebo nebo injektovaných poruch) probíhala co nejblíže místu poruchy (lokalita), a tak byl projev poruchy v postranních kanálech co nejmenší.

Podobný koncept byl zkoumán na platformě FPGA, avšak pouze z hlediska spolehlivosti [25], [26].

A. Otevřené problémy

V rámci práce na tématu μTMR budu řešeny následující otevřené problémy (klesající priorita):

- Efektivní implementace μ-voteru ze standardních buněk
- Rozmístění μ-voterů v obvodu a jeho vliv na požadované vlastnosti systému založeného na konceptu μTMR: vliv na zranitelnost útoky postranními kanály, realistický model injekce poruch a spolehlivostní parametry
- Optimální implementace μ-voterů v technologii CMOS (nehledě na standardní buňky)
- Simulace velkých (komb.) obvodů s podporou SPICE

B. Metodologie

Na základě předchozích zkušeností z práce na spolehlivostních architekturách, monotónních, synchronních i asynchronních obvodech a jejich mikroarchitektuře a vzhledem k návrhovým stylům preferovaných průmyslem bude μTMR stavět na variantě dvoudrátové logiky od Sokolova a kol. [17], s tím, že v úvahu bude vzato maskování mezivýsledků [13].

Na sadě benchmarků bude provedeno hodnocení ceny (plocha, rychlost), zranitelnosti a spolehlivosti obvodů. Malé benchmarkové obvody budou ověřeny v systému SPICE (ngSPICE) pro relevantní CMOS technologie. Pro větší obvody bude použit méně přesný simulátor, nebo rychlejší simulace s podporou SPICE (ve vývoji).

C. Přípravné práce – μTMR

Výsledky týkající se hodnocení zranitelnosti obvodů na základě simulace (ngSPICE, IRSIM) byly publikovány na workshopu CryptArchi 2017 [JBn6] a výsledky týkající se kvality dat použitých pro realizaci DPA byly prezentovány na workshopu Trudevice 2018 [JBn7].

Na základě zkuseností získaných z experimentů prezentovaných v [JBn7] lze pomocí simulace provést férové zhodnocení zranitelnosti systému založeného na µTMR.

IV. Závěr

Příspěvek shrnuje současný stav řešení dizertační práce. Část práce týkající se zvyšování spolehlivosti číslicových obvodů na úrovni mikroarchitektury je již dokončena.

Většina příspěvku je věnována probíhajícímu výzkumu spolehlivých a bezpečných mikroarchitektur, zejména rešerši. Dokončení druhé části výzkumu a doktorského studia je plánováno na následující rok.

Poděkování

GAČR GA16-05179S, ČVUT SGS17/213/OHK3/3T/18.

Reference

[1] J. Sparsø and S. Furber, *Principles of Asynchronous Circuit Design: A Systems Perspective*, 1st ed. Kluwer Academic Publishers, Boston, 2001.

[2] T. Koal, M. Scholzel, and H. Vierhaus, "Combining fault tolerance and self repair at minimum cost in power and hardware," in *17th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, April 2014, pp. 153–158.

[3] P. Fiser, P. Kubalik, and H. Kubatova, "An Efficient Multiple-Parity Generator Design for On-Line Testing on FPGA," in *11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools, 2008, DSD'08*, Sept 2008, pp. 96–99.

[4] J. Borecký, "Dependable Systems Design Methods for FPGAs," Ph.D. dissertation, the Faculty of Information Technology, Czech Technical University in Prague, 8 2015.

[5] M. Balaz and S. Kristofik, "Generic Self Repair Architecture with Multiple Fault Handling Capability," in *Euromicro Conference on Digital System Design (DSD), 2015*, Aug 2015, pp. 197–204.

[6] L. T. L. M. T. W. . W. G. Killmann, W., "Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations." BSI, Jul 2011. [Online]. Available: http://www.bsi.bund.de

[7] K. Lemke-Rust, "Models and Algorithms for Physical Cryptanalysis." Dissertation, Europäischer Universitätsverlag, 2007.

[8] T. Snyder and G. Byrd, "The Internet of Everything," *Computer*, vol. 50, no. 6, pp. 8–9, 2017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/MC.2017.179

[9] Y. Li, M. Chen, and J. Wang, "Introduction to side-channel attacks and fault attacks," in *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, vol. 01, May 2016, pp. 573–575.

[10] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Annual International Cryptology Conference*. Springer, 1996, pp. 104–113.

[11] P. Kocher, J. Jaffe and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," 1998, technical report. [Online]. Available: http://www.cryptography.com/dpa/

[12] ——, "Differential power analysis," in *Annual International Cryptology Conference*. Springer, 1999, pp. 388–397.

[13] "Security: DPA Countermeasures," 2018. [Online]. Available: https://www.rambus.com/security/dpa-countermeasures/

[14] L. V. Lu Zhang and M. Taylor, "Power Side Channels in Security ICs: Hardware Countermeasures." arXiv, 2016.

[15] Y. Li, K. Ohta, and K. Sakiyama, "Revisit fault sensitivity analysis on wddl-aes," in *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*, June 2011, pp. 148–153.

[16] V. Lomné, T. Roche, and A. Thillard, "On the Need of Randomness in Fault Attack Countermeasures - Application to AES," in *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2012 Workshop on*, Sept 2012, pp. 85–94.

[17] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 449–460, April 2005.

[18] A. Moradi and M. Kirschbaum and T. Eisenbarth and C. Paar, "Masked Dual-Rail Precharge Logic Encounters State-of-the-Art Power Analysis Methods," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 9, pp. 1578–1589, Sept 2012.

[19] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang, "Pushing the limits: a very compact and a threshold implementation of AES," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2011, pp. 69–88.

[20] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Annual international cryptology conference*. Springer, 1997, pp. 513–525.

[21] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis," in *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer, 2010, pp. 320–334.

[22] S.-M. Yen and M. Joye, "Checking before output may not be enough against fault-based cryptanalysis," *IEEE Transactions on Computers*, vol. 49, no. 9, pp. 967–970, Sep 2000.

[23] S. Bhasin, J. L. Danger, F. Flament, T. Graba, S. Guilley, Y. Mathieu, M. Nassar, L. Sauvage, and N. Selmane, "Combined SCA and DFA Countermeasures Integrable in a FPGA Design Flow," in *2009 International Conference on Reconfigurable Computing and FPGAs*, Dec 2009, pp. 213–218.

[24] F. Amiel, K. Villegas, B. Feix, and L. Marcel, "Passive and active combined attacks: Combining fault attacks and side channel analysis," in *Fault Diagnosis and Tolerance in Cryptography, 2007. FDTC 2007. Workshop on*, Sept 2007, pp. 92–102.

[25] G. L. Nazar, "Fine-grained error detection techniques for fast repair of FPGAs," 2013.

[26] M. Niknahad, *Using Fine Grain Approaches for Highly Reliable Design of FPGA-based Systems in Space*. KIT Scientific Publishing, 2013, vol. 9.

Recenzované publikace autora

[JBr1] J. Bělohoubek, P. Fišer, and J. Schmidt, "Novel C-Element Based Error Detection and Correction Method Combining Time and Area Redundancy," in *Euromicro Conference on Digital System Design (DSD), 2015*, Aug 2015, pp. 280–283.

[JBr2] J. Belohoubek, P. Fišer, and J. Schmidt, "Error Correction Method Based on the Short-Duration Offline Test," in *2016 Euromicro Conference on Digital System Design (DSD)*, Aug 2016, pp. 495–502.

[JBr3] J. Bělohoubek, P. Fišer, and J. Schmidt, "Error masking method based on the short-duration offline test," *Microprocessors and Microsystems*, vol. 52, pp. 236–250, 2017.

Ostatní publikace autora

[JBn1] J. Bělohoubek, "Fully asynchronous QDI implementation of DES in FPGA," Annency, France, 2014. [Online]. Available: https://labh-curien.univ-st-etienne.fr/cryptarchi/workshop14/presentations.html

[JBn2] ——, "Novel gate design methodology for short-duration test," Prague, Czech Republic, 2015.

[JBn3] ——, "Novel Error Detection and Correction Method Combining Time and Area Redundancy," Zlín, Czech Republic, 2015.

[JBn4] ——, "Využití rychlého offline testu v systému se schopností maskování jedné chyby," Kraví Hora - Bořetice, Czech Republic, 2016.

[JBn5] ——, "Error Correction Method Based on the Efficient Offline Test," Czech Technical University in Prague, Faculty of Information Technology, Tech. Rep., 05 2016.

[JBn6] ——, "The Design-Time Side-Channel Information Leakage Estimation," Smolenice, Slovakia, 2017. [Online]. Available: https://labh-curien.univ-st-etienne.fr/cryptarchi/workshop17/presentations.html

[JBn7] ——, "Effect of Power Trace Set Properties to Differential Power Analysis," Dresden, Germany, 2018.

Satelitní lokalizace SSR transpondérů

Luděk Dudáček
4, prezenční studium
doc. Ing. Jiří Masopust, CSc.

Katedra aplikované elektroniky a telekomunikací
dudacekl@kae.zcu.cz

***Abstrakt*—Tato práce se zabývá možnostmi využití satelitů pro multilateraci signálů z odpovídačů sekundárních přehledových radarů (SSR) a signálů ADS-B (Automatic Dependant Surveillance – Broadcast) vysílačů.**

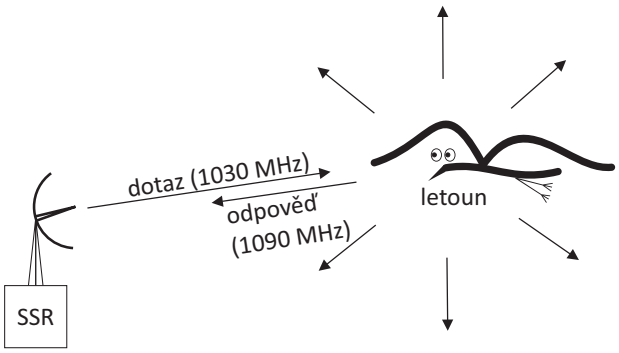
V současné době je většina letounů vybavena odpovídačem SSR nebo systémem ADS-B pracujícím v pásmu 1090 MHz. Tyto systémy potřebují pro zajištění správné funkce řízení letového provozu (ATC) síť pozemních stanic umožňujících příjem a případně i dotazování transpondérů umístěných v letounech. Tato koncepce však omezuje možnosti využití těchto systémů v oblastech, ve kterých není možné z technických důvodů vybudování pozemních stanic (např.: oceány, pouště, arktické oblasti).

Jednou z moderních možností pro zajištění pokrytí nad těmito nehostinnými oblastmi je využití satelitů na nízkých oběžných drahách země (LEO) pro příjem signálů ADS-B spolu s následným dekódováním datového obsahu zprávy. Druhou možností je zjištění pozice ADS-B transpondéru bez dekódování datového obsahu pomocí multilaterace s využitím několika satelitních přijímačů.

***Klíčová slova*—Sekundární přehledový radar, Automatic Dependent Surveillance – Broadcast, transpondér, satelit, radiolokace, satelitní navigace, TDOA.**

I. Úvod

Vzdušný prostor je na celém světě hojně využíván pro leteckou dopravu osob a materiálu. Pro získání informací o aktuálních pozicích letounů slouží několik vzájemně se doplňujících systémů: primární přehledové radary PSR (Primary Surveillance Radar), sekundární přehledové radary SSR (Secondary Surveillance Radar), Automatic Dependent Surveillance – Broadcast (ADS-B) a Automatic Dependent Surveillance – Contract (ADS-C). Pokud nebudeme uvažovat speciální vojenské aplikace jsou primární a sekundární přehledové radary z hlediska ATC výhradně pozemními zařízeními. Získání informace o pozici letounu je v těchto případech zajištěno respektive iniciováno pozemním zařízením, kdy pro činnost PSR není ze strany letounu vyžadována žádná „spolupráce“ a v případě SSR je letounem odeslána odpověď na výzvu vyslanou pozemním zařízením. Na rozdíl od PSR a SSR jsou systémy ADS-B a ADS-C schopné pracovat nezávisle na pozemním segmentu. Přesněji řečeno vyslání informace o pozici je iniciováno zařízením umístěným v letounu a nevyžaduje žádnou výzvu od pozemní části. Díky tomu jsou tyto systémy vhodné pro využití v oblastech, kde není možné z technických důvodů budovat strukturu pozemních zařízení zajišťující pokrytí příslušné oblasti.



Obrázek 1: Princip činnosti sekundárního přehledového radaru.

Jednou z možností jak zajistit příjem ADS-B vysílání v nepřístupných oblastech je využití satelitních přijímačů [1], [2], [3]. Rozvoj malých satelitů výrazně podpořil vývoj satelitních ADS-B přijímačů.

Dalšímy systémy pro určování pozice letounů jsou systémy pracující na principu multilaterace (MLAT), nebo pro rozsáhlejší oblasti WAM (Wide Area Multilateration). Přehledové systémy ATM, pracující na principu MLAT respektive WAM pro svoji činnost s výhodou využívají právě signálu SSR a ADS-B [4].

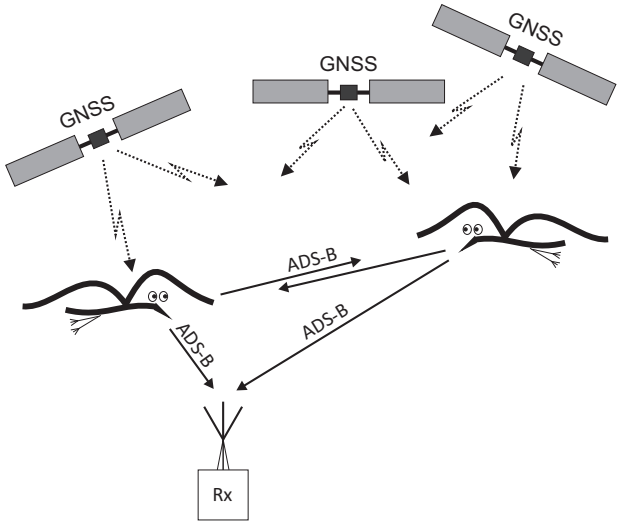
A. Princip činnosti sekundárních přehledových radarů

Sekundární přehledový radar (SSR) historicky vychází ze systému rozlišení přátelských a nepřátelských letounů IFF (Identification Friend or Foe). Jeho činnost je založena na principu dotaz-odpověď. První částí SSR je pozemní dotazovač, který zahajuje celý proces lokalizace letounu vysláním dotazu (výzvy) do určitého prostoru směrovou anténou. Druhou částí SSR je odpovídač (transpondér) umístěný v letounu. V případě, že transpondér zachytí výzvu, reaguje na ni odesláním své odpovědi se stanoveným zpožděním ($3\mu s \pm 0.5\mu s$). Princip činnosti SSR je znázorněn na obrázku 1.

Podle směru, ze kterého byla zachycena odpověď a ze zpoždění mezi vysláním dotazu a zachycením odpovědi je následně pozemní částí vyhodnocena pozice detekovaného letounu.

B. Princip činnosti systému Automatic Dependent Surveillance – Broadcast

Princip činnosti Automatic Dependent Surveillance – Broadcast je znázorněn na obrázku 2. Technické požadavky na tento systém jsou stanoveny v dokumentu [5].



Obrázek 2: Princip činnosti systému ADS-B

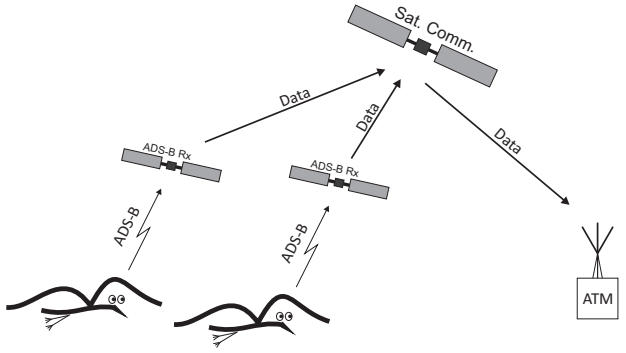
Systém ADS-B se skládá ze dvou subsystémů: *ADS-B Out* a *ADS-B In*. Úkolem subsystému ADS-B Out je vysílat v pravidelných intervalech informace o pozici, rychlosti, směru letu letounu. Zprávy obsahující tyto informace jsou označovány jako *Squitter*. Na rozdíl od SSR není vyslání informace iniciováno žádným vnějším zařízením, díky tomu je možné tento systém provozovat i v oblastech, kde není vybudováno radarové pokrytí. Informace vysílané prostřednictvím ADS-B Out jsou získávány z palubních systémů letounu a pozice je určována prostřednictvím GNSS (Global Navigation Satellite Systems). ADS-B vysílání využívá zprávy ve zvláštním formátu zpráv módu-S využívaného systémy SSR.

II. Definice řešeného problému

Systémy pro MLAT lokalizaci letounů jsou však zatím běžně využívány pouze v pozemním provedení, a neumožňují tedy určování pozic letounů v odlehlých oblastech. Pokud by byly odlehlé oblasti vhodně pokryty satelitními přijímači těchto signálů, mohla by být určována pomocí multilaterace i pozice letounů pohybujících se mimo dosah standardních multilateračních systémů.

Cíle práce jsou stanoveny takto:

1) Analýza současného stavu leteckých přehledových systémů.
2) Analýza možnosti příjmu SSR signálů pomocí malých satelitů.
3) Návrh systému umožňujícího multilateraci SSR signálů s využitím přijímačů na nízkých oběžných drahách.
4) Volba a řešení konkrétní oblasti související s činností navrženého systému.



Obrázek 3: Dvouúrovňový systém satelitního příjmu ADS-B

III. Hotové analýzy možných řešení

První část této kapitoly bude věnována popisu možné konfigurace satelitního WAM systému (SWAM). Druhá část nastíní možná řešení synchronizace jednotlivých MLAT přijímačů. V dalších částech bude řešena energetické bilanci rádiového spoje letoun–satelit, daný systém bude analyzován z pohledu hromadného přístupu k satelitnímu přijímači a na závěr bude analyzován modelový případ konstelace satelitních přijímačů z pohledu pokrytí zemského povrchu.

A. Možné konfigurace satelitních WAM systému

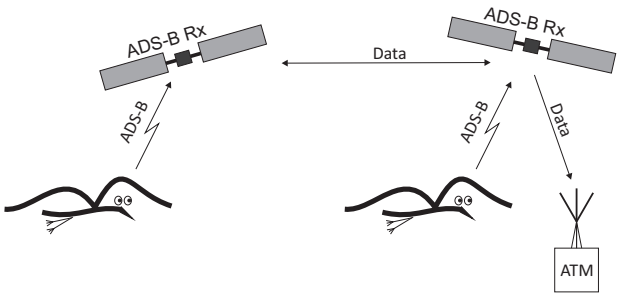
Principiálně je možné k satelitnímu příjmu přistupovat několika způsoby podle metody zpracování přijatého signálu.

Možné topologie systému vhodného pro satelitní příjem a multilateraci ADS-B signálu se liší ve způsobu předávání dat pozemní stanici. První metoda vychází z návrhu uvedeného v [6] je znázorněna na obrázku 3. V tomto případě jsou satelitní přijímače rozmístěné na LEO. Přijatý signál je dekódován a následně vhodným přenosovým kanálem předáván komunikačním satelitům na geostacionární oběžné dráze, koncentrujícím ADS-B data z více satelitních ADS-B přijímačů a zajišťujícím předání dat pozemním stanicím. Tímto přístupem je zajištěno nepřetržité předávání dat ze satelitních ADS-B dat pozemním stanicím a efektivnější využití přenosových kanálů. Nevýhodou však může být větší latence celého systému.

Další možný přístup je použit v systému společností Aireon a Iridium a je zachycen na obrázku 4. V tomto případě spojení s pozemní stanicí není realizováno prostřednictvím komunikačních satelitů na GEO, ale pomocí datové sítě vytvořené mezi jednotlivými satelitními přijímači. V případě, že není ADS-B přijímač v dosahu pozemní stanice, jsou jím přijatá ADS-B data předána pozemní stanici prostřednictvím jednoho nebo více sousedních satelitů. Tím je zajištěno globální pokrytí a nejmenší možná latence celého systému.

B. Metody synchronizace WAM přijímačů

Přesnost MLAT měření polohy je závislá zejména na přesnosti měření časových zpoždění mezi příjmem daného signálu jednotlivými senzory, respektive na přesnosti určení TOA. Z této skutečnosti vyplývá požadavek na co nejpřesnější znalost zpoždění způsobených jednotlivými senzory.



Obrázek 4: Jednoúrovňový systém satelitního příjmu ADS-B

	$\mathbf{h_S = 300}$ km		$\mathbf{h_S = 790}$ km		
	min.	max.	min.	max.	
$EIRP$	15,45	18,45	15,40	18,45	dBW
C	-167,34	-146,37	-172,32	-154,35	dBW
N_0	-180,00	-185,50	-180,00	-185,50	dBW
C/N_0	12,65	39,13	4,60	31,15	dB

Tabulka I: Energetické bilance rádiového spoje letoun–satelit pro ADS-B třídy A0 a B0

(EIRP - efektivní isotropně vyzářený výkon, C - úroveň signálu na vstupu přijímače, N_0 - úroveň šumu na vstupu přijímače, C/N_0 - odstup signál-šum na vstupu přijímače)

Pro přesné určení časových zpoždění je nezbytné aby časové základny všech senzorů byly synchronní. Synchronizaci těchto obvodů lze zajistit několika způsoby. Z principu činnosti a struktury SWAM systému však připadají v úvahu pouze synchronizační metody využívající časových signálů GNSS.

C. Energetická bilance rádiového spoje letoun-satelit

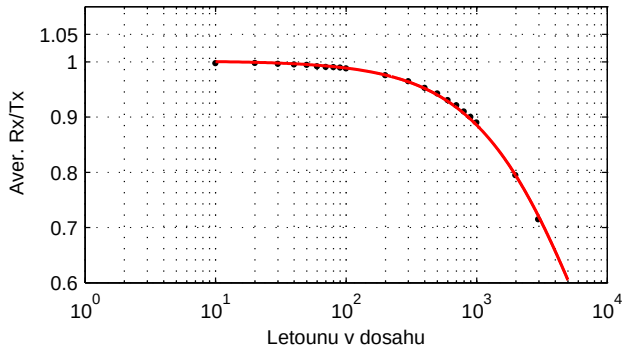
Výkonová úroveň na vstupu satelitního přijímače je obecně závislá na mnoha faktorech. Podrobný rozbor energetické bilance a jejích jednotlivých faktorů je proveden například v [7] nebo [8].

V tabulce I je vyčíslena konkrétní energetické bilance pro orbitální dráhy 300 km a 790 km a pro různé třídy ADS-B vysílání. Zde sloupeček *„max“* odpovídá maximálním hodnotám C/N_0. Pro výpočty hodnoty maximálního C/N_0 byly použity hodnoty minimálního útlum, minimálního N_0 a maximálního EIRP.

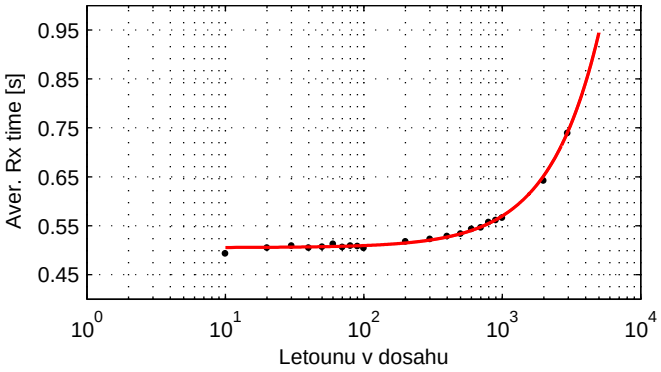
D. Vytížení satelitního přijímače

Standardní ADS-B přijímač provádějící signálové zpracování podle [5] vyhodnocuje pro každý zachycený rámec (respektive pro každou identifikovanou hlavičku rámce) referenční úroveň výkonu. V případě, že jsou zachyceny dva alespoň částečně se překrývající rámce, jsou porovnány tyto referenční úrovně a dále je zpracováván pouze rámec jehož referenční výkonová úroveň je alespoň o 3 dB větší než referenční úroveň druhého z kolidujících rámců. Ve všech ostatních případech dojde ke ztrátě obou zachycených rámců.

Na obrázcích 5 a 6 jsou uvedeny vysledky simulací vyhodnocující vytížení přijímače ve výšce 1000 km. Obrázek 5 zobrazuje závislost poměru přijatých a vyslabých rámců v závislosti na počtu letounů v dosahu přijímače. Obrázek 6 pak znázorňuje závislost průměrného času mezi příjmem dvou rámců stejného letounu na počtu letounů v dosahu.



Obrázek 5: Závislost poměru přijatých a vyslaných ADS-B rámců na počtu letounů v dosahu přijímače.



Obrázek 6: Závislost průměrného času mezi zachycením dvou ADS-B rámců jednoho letounu na počtu letounů v dosahu přijímače.

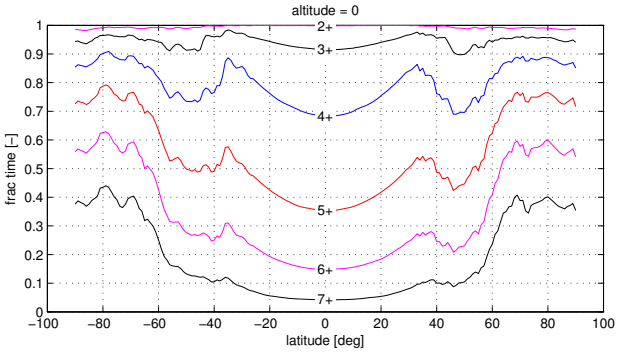
E. Analýza pokrytí satelity Iridium

Pokud budeme chtít realizovat systém umožňující multilateraci pomocí přijímačů rozmístěných na LEO je nutné zajistit v jednom okamžiku viditelnost minimálně 4 satelitů při požadavku na kompletní informaci o poloze vysílače. Tento požadavek vychází z principu funkce systémů MLAT.

S ohledem na to, že v posledních letech jsou nové satelity společnosti Iridium vybavovány ADS-B přijímači, byla provedena analýza možnosti využít takto rozmístěné přijímače pro účely multilaterace. Pro účely vytvoření modelu byla využito knihoven *SGP4*, které realizují výpočty polohy satelitu na orbitální dráze definované pomocí TLE (Two Line Elements). Analýza pokrytí byla provedena pro tři možné konstelace satelitů: úplná konstelace (bylo použito 64 aktivních satelitů), poloviční počet drah (byly použity pouze satelity na drahách 1,3 a 5), poloviční počet pozic (na každé dráze byl použit pouze každý druhý satelit). Na obrázku 7 je znázorněna poměrná doba mezvyditelnosti daného počtu satelitů v závislosti na zeměpisné šířce.

IV. Závěr

Dosavadní výsledky naznačují, že systém satelitní multilaterace je s jistými omezeními realizovatelný.



Obrázek 7: Poměrný čas viditelnosti více satelitů současně v závislosti na zeměpisné šířce při plném obsazení drah.

Při požadavku na provozování systému ve všech zeměpisných šířkách se jako kritický bod se ukazuje konstelace satelitů zajišťující dostatečné pokrytí sledovaného území.

Z analýzy vytížení satelitního přijímače také vyplývá, že v oblastech s vysokou hustotou provozu může v některých případech docházet k zahlcení přijímače a ztrátám datových rámců.

V. Plán další práce

Další směřování práce bude zaměřeno na podrobnější analýzu NLOS komunikačního kanálu mezi letounem a satelitním přijímačem s ohledem na využití v systému satelitní multilaterace. Dále bude analyzován vliv Dopplerova posuvu na přesnost SWAM systému. Zásadním bodem určujícím použitelnost SWAM, kterému je zapotřebí věnovat pozornost, je přístup k synchronizaci jednotlivých satelitních přijímačů a jeho přesnost.

Body 1 a 2 uvedené v kapitole II již byly realizovány. Pro realizaci bodů 3 a 4 z kapitoly II bude postupováno podle následujícího harmonogramu, který pokrývá klíčové části systému satelitní multilaterace SSR a ADS-B signálů:

1) Volba topologie systému pro kosmickou multilateraci SSR a ADS-B signálů.
2) Konstelace satelitů:
   a) volba vhodné konstelace,
   b) model pokrytí zemského povrchu při zvolené konstelaci,
   c) vliv zvolené konstelace na přesnost SWAM systému.
3) Volba vhodné metody synchronizace hodinových signálů.
4) Požadavky na přenosové kanály mezi satelitními přijímači a centrální jednotkou:
   a) potřebné komunikační rychlosti,
   b) energetická bilance.

VI. Publikační činnost autora

[i] Dudáček, L., Vertat, I.: Multidimensional Parity Check codes with short block lengths. In *E2016 24th Telecommunications Forum (TELFOR)*, 2016, doi: 10.1109/TELFOR.2016.7818772.

[ii] Dudáček, L.: Porovnání kódů MDPC a LDPC. In *Elektrotechnika, elektronika, elektroenergetika*, 2015, ISBN 978-80-261-0514-5, s. 145–148.

[iii] Dudáček, L.: Realizace hybridních modulací DM-FSK/DQPSK. In *Elektrotechnika, elektronika, elektroenergetika*, 2014, ISBN 978-80-261-0366-0, s. 21–24.

[iv] Dudáček, L.: *Hybridní modulace pro komunikační systém pikosatelitů*. Diplomová práce, Západočeská univerzita v Plzni, Fakulta elektrotechnická, Katedra aplikované elektroniky a telekomunikací, 2014, vedoucí práce: Ivo Veřtát.

[v] Vertat, I.; Linhart, R.; Dudacek, L.; aj.: Hybrid modulation as beacon replacement in CubeSat picosatellites. In *2013 23rd International Conference Radioelektronika (RADIOELEKTRONIKA)*, April 2013, s. 297–301, doi: 10.1109/RadioElek.2013.6530935.

[vi] Dudáček, L.: *Radarové měření vzdáleností*. Bakalářská práce, Západočeská univerzita v Plzni, Fakulta elektrotechnická, Katedra aplikované elektroniky a telekomunikací, 2012, vedoucí práce: Jiří Masopust.

[vii] Dudáček, L. Model vytížení přijímače ADS-B na nízkých oběžných drahách. In *Elektrotechnika a informatika 2016. Elektrotechnika, elektronika, elektroenergetika.* Plzeň: Západočeská univerzita v Plzni, 2016. s. 105-108. ISBN: 978-80-261-0516-9

[viii] Vertat, I.; Linhart, R.; Masopust, J.; Vobornik, A.; Dudacek, L.: *Earth's thermal radiation sensors for attitude determination systems of small satellites*, Contributions of the Astronomical Observatory Skalnaté Pleso, vol. 47, no. 2, p. 157-164.

Reference

[1] A. Parkinson, "Space-based ads-b: A small step for technology a giant leap for atm?" in *2011 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles*, Sept 2011, pp. 159–164.

[2] M. A. Garcia, J. Stafford, J. Minnix, and J. Dolan, "Aireon space based ads-b performance model," in *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*, April 2015, pp. C2–1–C2–10.

[3] H. Blomenhofer, A. Pawlitzki, P. Rosenthal, and L. Escudero, "Space-based automatic dependent surveillance broadcast (ads-b) payload for in-orbit demonstration," in *2012 6th Advanced Satellite Multimedia Systems Conference (ASMS) and 12th Signal Processing for Space Communications Workshop (SPSC)*, Sept 2012, pp. 160–165.

[4] W. Neven, T. Quilter, R. Weedon, and R. Hogendoorn, "Wide area multilateration report on eatmp trs 131/04 version 1.1," National Aerospace Laboratory NLR, August 2005.

[5] "Rtca do-260b – minimum operational performance standards for 1090 mhz extended squitter automatic dependent surveillance – broadcast (ads-b) and traffic information services – broadcast (tis-b)," RTCA, Inc., 2009.

[6] K. F. Trillingsgaard, A. Alcindor, N. B. Thomsen, and M. B. Eriksen, "Space based ads-b," Bachelor Thesis, Aalborg University, 2011, supervisor: Henrik Schiøler.

[7] M. B. Gérard Maral, *Satellite communications systems*. John Wiley & Sons Ltd, 2009.

[8] I. Veřtát, "Efektivní komunikační systém pikosatelitů," Disertační práce, Západočeská univerzita v Plzni, Fakulta elektrotechnická, Katedra aplikované elektroniky a telekomunikací, 2011, vedoucí práce: Doc. Ing. Jiří Masopust, CSc.

Challenges In the Computer Photoacoustic Tomograpy Using the k-Wave Toolbox

Gabriel Bordovsky
1st year, full-time study
Supervisor: Jiri Jaros

Brno University of Technology, Faculty of Information Technology
Bozetechova 2, 612 66 Brno, Czech Republic
ibordovsky@fit.vutbr.cz

***Abstract*—The goal of the photoacoustic tomography (PAT) is to create a 3D image of the tissue from the ultrasound pulses measured on the surface of the tissue. The contrast of the image is based on the optical absorption in the tissue. This article describes a study of photoacoustic tomography on human breast phantoms and challenges in the implementation of the Normal Adjoint Operator (NOA) required for the reconstruction.**

***Keywords*—photoacoustic tomography, ultrasound simulation, high-performance computing, parallel systems**

I. Introduction

The photoacoustic tomography is based on the fact that the chromophones in specific tissue [1],[2], such as hemoglobin in veins and tumors, absorbs the laser light. The absorbed light is transformed into heat and cause thermoelastic expansion. This generates broadband ultrasonic waves in the tissue that can be captured by the ultrasound sensors. The tumor tissue is rich on hemoglobin which leads to a stronger absorption of the near-infrared light than in the surrounding tissue. This provides a promising base for a real application and is a strong advantage against the X-ray screening such as mammography.

Current experiments are driven by the work on the European project H2020 PAMMOTH, that aims for developing of a diagnostic machine for detection of breast tumors. This machine, including developed image reconstruction algorithms should be ready to undergo clinical tests in 2020.

Our experiments are based on the proposed specification of the diagnostic machine. Those specification are not fixed yet. Our expectation are that the machine should be composed of 512 evenly distributed ultrasound sensors with central frequency of $1\,\mathrm{MHz}$. The sensors will be placed on the surface of a bowl with radius $25\,\mathrm{cm}$. The bowl should rotate around the breast continuously and take $1000\,\mathrm{measurements}$. A membrane should fixate the breast in place, which allows to combine all measurements by $512\,\mathrm{sensors}$ and treat them as single measurement by $512\,000\,\mathrm{sensors}$. The spatial resolution required by the project is $500\,\mu\mathrm{m}$ and $1\,\mathrm{mm}$.

This article studies an implementation of the adjoint operator to the forward wave propagation presented in [3], and deducted NOA for the image reconstruction. The used computational model has its limitation that has to be compensated for real application in the photoacoustic tomography [4].

II. Photoacoustic tomography

The expansion of the hemoglobin in veins and the tumors forms a pressure field p_0 inside the tissue. The process of ultrasound measurement during the PAT can be described as Eq. (1). In this linear system, A models the propagation of the ultrasound waves through the tissue and the measurement process itself. We will call A the forward operator which maps initial p_0 from domain pressure distribution $\mathcal{P}$ into signal f from domain of time-varying pressure on sensors $\mathcal{F}$.

$$f = Ap_0 + \epsilon \tag{1}$$

The problem of obtaining the initial pressure distribution p_0 in form of the reconstructed image, can be described as an inversion of Eq. (1). For that we would need inverse operator to A. Since A is linear operator, one possible representation would be matrix mapping inputs to outputs. This matrix would have high memory requirements due high count of sensors and domain voxels and would be challenging to construct. To such matrix, the inverse may be constructed as:

$$A^{-1} = \frac{1}{detA}A^* \tag{2}$$

Where A^* would be adjoint to A constructed as transposed cofactor matrix of A. Construction of the adjoint to the forward operator A and it's discretization may be found in [3].

Part information about the original pressure distribution p_0 is lost (ϵ) due limited position and size of the sensors, subsampling and other factors. Therefore, we may not use the inversion directly [5]. Instead, we may look at the PAT as an optimization problem where we search for such a pressure distribution that produces signal on the sensors as close as possible to the measured one.

$$p := \underset{p_0}{\operatorname{argmin}} \left\{ \tfrac{1}{2} ||Ap_0 - f||_2^2 \right\} \tag{3}$$

The Equation 3 may be solved by *first order method* [6] such as gradient descent [7]. For that we need to know difference of minimization criteria $Ap_0 - f$ in domain of

pressure distribution $\mathcal{P}$. It is sufficient to use adjoint operator A^* to transform the result from domain $\mathcal{F}$ to $\mathcal{P}$.

$$\nabla \tfrac{1}{2}||Ap_0 - f||_2^2 = A^* \left(Ap_0 - f\right) \tag{4}$$

The gradient descent algorithm may be then written in form of iterative scheme in Eq. (5) respective Eq. (6).

$$p^{k+1} = p^k - \eta A^* \left(Ap^k - f\right), \tag{5}$$

$$p^{k+1} = p^k - \eta A^* A p^k + \eta A^* f \tag{6}$$

The pair of operators A^*A in Eq. (6) forms the normal PA operator and will be discussed further on. The η represents step of the gradient descent method, and to ensure convergence to p with minimal error against f, it has to be chosen from interval $(0, 2/\theta)$ where θ is the largest singular value, eigenvalue, of the A^*A operator.

This eigenvalue has to be evaluated for each patient, as it is expected to depend on speed of sound map of the patients tissue. In current experiments it is required to evaluate A^*A 30-50 times to find θ using power iteration method.

III. Discretization

The above proposed solution of the PAT problem calls for an effective and fast model of the ultrasound propagation in tissue. One of the possible discrete numerical realizations is the k-Wave toolbox for Matlab [8]. K-Wave is designed for time domain acoustic and ultrasound simulation in complex media and is widely used. The the numerical solution is based on the k-space pseudospectral method. The toolbox also provides binary files to offload the computation to GPUs or distributed clusters. This solver will be further referenced as the operator K. Disadvantage of the k-Wave is the requirement to use Matlab to preprocess and postprocess data. Each call of forward PA operator A or adjoint PA operator A^* requires preprocessing in Matlab, storing data in the input file, running the optimized parallel solver which stores results in the output file and that is read back into Matlab. Whole normal PA operator A^*A is called as one in gradient descent iterative solver, and the dependence on the Matlab represent unnecessary overhead.

Another disadvantage is missing support for realistic sensors in a high resolution grid. The k-Wave solves the wave propagation on a uniform staggered grid, and is only able to record pressure at selected voxels. Fine resolution of the simulation causes, that single signal of f is composed of pressure sampled at several voxels. This calls for a mapping function C capable to gather sampled pressure into sensor channels. Moreover, the recorded signal is not simply the pressure at voxels, but it is also influenced by the characteristics of the sensor itself. To bring the simulated output closer to the recorded signal, it is required to apply a frequency impulse response filter F on given separated channels. Two other functions are used to improve the image quality. First is the region of interest R that removes residual acoustic pressure in the simulation domain, e.g. behind the sensors or in the coupling acoustic media. Second is spectral smoothing function S removing high frequencies from the domain [9].

The functions for pre-processing and post-processing of data for the k-space solver K may be applied on resulted data in Matlab environment. This is a common case when the K needs to be evaluated only once. The functions are usually more memory consuming than computationally, so there was no need for fast parallel implementation as with k-space solver. However, for the effective iterative solver using normal PA operator, it is necessary to come with efficient implementation inside parallel application.

A. Forward PA Simulation

The application of the forward PA operator A on the acoustic pressure distribution p may be rewritten as a consecutive application of those previously mentioned functions:

$$Ap = F(C(K(S(R(p))))) \tag{7}$$

B. Adjoint PA Simulation

For each part of the forward PA simulation has to be found adjoint function to simulate overall adjoint of the forward PA operator A^*. Some of the functions in the forward simulation are self-adjoint or trivial to create adjoint.

$$C^* = C^T \tag{8}$$

$$S^* = S \tag{9}$$

$$R^* = R \tag{10}$$

Since F is a signal filter, its adjoint F^* is *Adjoint signal filter*. This filter may be created by reverting the time order of the elements in signal filter mask h and use of complex conjugated elements to the original mask h. For a symmetrical mask with only real values the filter function F is also self-adjoint.

$$A^*(f) = R(S(K^*(C^T(F(f))))) \tag{11}$$

Derivation of the adjoint for K and its discretization in k-Wave may be found in [3].

IV. Integrated execution of the normal operator

The original structure is composed only of *pre-processing*, *simulation loop* and *post-processing* functions. The *pre-processing* loads data from the input file, initializes required matrices and computes values constant within the simulation. The *simulation loop* updates acoustic velocity of the particles and pressure inside the computational domain. During the simulation loop, the sensor data is also stored. The *post-processing* stores other data into files. To compute the normal operator A^*A, the steps of applying ROI on the input and the output pressure have to be added as well as computation of the adjoint source signal before the second simulation loop.

All required data is stored in the input HDF5 file. To be able to run the simulation in one binary, the input file had to be extended by required data. Namely by the sensor frequency response, the region of interest mask and sensor-voxel mapping C.

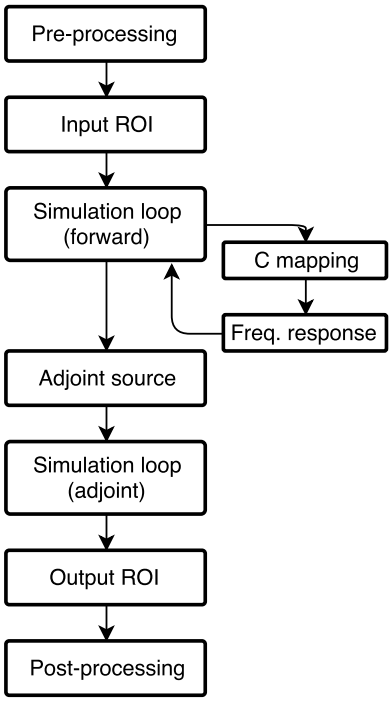


Fig. 1. Structure of the normal operator execution

A. Sensor data recording

K-Wave computes on a uniform cubical grid, an 3D matrices containing current acoustic pressure. Some of the voxels of the grid are referenced by array of indexes and inside those is the pressure measured. Since the sensors are on the surface of the bowl the spacing between voxels that are referenced is random. This has to be extended by mapping function C, that may be described as matrix where one side represents N_r realistic sensors and second side represents N_v sensor voxels. In current experiments we use simplified model of sensors which expects, that each sensor always occupies only four voxels, in $1\,\mathrm{mm}$ resolution. (This simplification will not hold for the real case.) Since the number of sensors is rather high in the current setup, some of them covers the same voxels. In our experiments, size of such matrix would be $512\,000 \times 142\,343$, taking $\sim$270 GB of memory in single precision. Fortunately, the matrix is rather sparse since each row has only several non-zero values, where the value is the ratio of how much space of the voxel is occupied by a given sensor. Matlab provides a solution for such sparse matrices, where each nonzero element of sparse matrix is transformed into source index from N_v, destination index from N_r and value V. Resulting representation is formed by three vectors and the size may be reduced, in our case to $33\,\mathrm{MB}$.

In the future it is expected that different and complex sensor models will occupy different number of voxels depending on the angle between sensor and the domain axis. This could lead into unaligned reads and unaligned writes in the computational domain and negatively influence runtime due to cache miss ratio.

```
for (i=0,i< C_length,i++) {
  sensor[C_i[i]] +=
    pressure[vox_s[C_j[i]]] *
    C_v[i];
}
```

Listing 1. Standard sensor-voxel mapping. Array vox_s list indexes of voxels in which we want to sample. Array C_i provides destination sensor channel, C_j source sampled voxel and C_v the value of sparse matrix C.

One of possible solutions seams to be rather simple for systems with uniform memory access, UMA. The mapping could be ordered, by dimension in which writes are done, and then split between cores. If two cores has to write into same sensor channel, one does so in beginning of the processing, and the second at the end.

B. Frequency response

The sampled and mapped signal represents only the pressure in simulation domain during the wave propagation. The real measured signal is influenced by characteristic of the used sensors. Our current experiments applies the frequency impulse response, FIR, on the measured signal after is the forward simulation finished. The application is multiplication of signals spectrum with mask representing the sensor's FIR. Since real application expects up to 1 TB of data to by produced by the forward simulation it is cumbersome to store data to disc [10] and then apply the filter, or to hold whole data in memory [11]. We decided to use the FIR filter during the sampling phase. This solution should provide possibility for trade-off between memory requirements and accuracy depending on size of used buffer.

C. Region of interest

The function R (the region of interest mask), which is composed of logical true and false values. Unfortunately, the HDF5 does not provide a direct logical or boolean data type. The k-Wave normally uses only two data types in HDF5 files, *float* for real numbers and unsigned long integer *size_t* for indexes. Float data type was chosen for logical mask because it is applied to the pressure in the domain which is also stored as *float*, therefore it does not require second type cast. In future, this is planned to be changed to form a logical mask in form of bit-field, stored as integer. The vector instruction ware planned to do the masking based on ROI in form this mask.

V. Testing

The testing is was done on two six-cored Intel XEON processors. Two configuration of the Matlab framework for PAT were used. First used unmodified execution scheme, where the forward and the adjoint simulations represents separate solver calls. The second run used single call of the modified k-space solver described in Sec. IV. The used metric is average time needed to evaluate single normal PAT operator during twenty iterations of gradient solver.

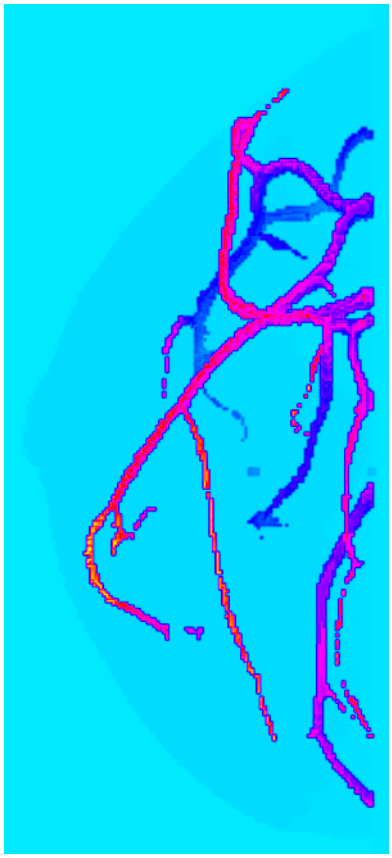


Fig. 2. Pressure(low-light-blue, medium-dark blue, high-red/yellow) in healthy breast phantom[12] after optical simulation. Energy is absorbed mostly by the veins.

TABLE I
AVERAGE TIME REQUIRED TO EVALUATE NOA

Configuration	Runtime	Speedup
Split	963 s	1.000×
Integrated	822 s	1.171×

VI. Future Research

In near future it is necessary to move remaining parts of normal PA operator into distributed codes. Mainly the FIR filter and smooth function. Current codes works well on UMA machines, but due to size of the expected data the effort in following work will be aimed into NUMA systems and/or GPGPUs.

In the more distant future we want to investigate possibilities of heterogeneous computational systems for PAT. Current supercomputer clusters are composed from several nodes containing both CPU and GPU or FPGA accelerator. The applications usually does not use both resources, which leads to ineffective usage of the computational node. Such task as the splitting of the application evenly on different architectures with different access to files or memories is challenging.

VII. Conclusion

This article describes some of the current problems with use of the k-space pseudospectral solver for the photoacoustic tomography and suggest some solution. The image reconstruction used for the PAT uses the normal photoacoustic operator, which depends on two consecutive simulations of the ultrasound propagation through heterogeneous media. Integrating both simulation to single parallel k-space solver was proposed and first results shows speedup by 17%.

Acknowledgment

This work was supported by The Ministry of Education, Youth and Sports from the National Programme of Sustainability (NPU II) project IT4Innovations excellence in science – LQ1602" and by the IT4Innovations infrastructure which is supported from the Large Infrastructures for Research, Experimental Development and Innovations project IT4Innovations National Supercomputing Center – LM2015070".

This work was supported by the FIT-S-17-3994 Advanced parallel and embedded computer systems project.

References

[1] A. C. Tam, "Applications of photoacoustic sensing techniques," *Reviews of Modern Physics*, vol. 58, no. 2, p. 381, 1986.

[2] P. Beard, "Biomedical photoacoustic imaging," *Interface focus*, p. rsfs20110028, 2011.

[3] S. R. Arridge, M. M. Betcke, B. T. Cox, F. Lucka, and B. E. Treeby, "On the adjoint operator in photoacoustic tomography," *Inverse Problems*, vol. 32, no. 11, p. 115012, 2016.

[4] S. Arridge, P. Beard, M. Betcke, B. Cox, N. Huynh, F. Lucka, O. Ogunlade, and E. Zhang, "Accelerated high-resolution photoacoustic tomography via compressed sensing," *Physics in Medicine & Biology*, vol. 61, no. 24, p. 8908, 2016.

[5] Z. Belhachmi, T. Glatz, and O. Scherzer, "A direct method for photoacoustic tomography with inhomogeneous sound speed," *Inverse Problems*, vol. 32, no. 4, p. 045005, 2016.

[6] M. Burger, A. C. Mennucci, S. Osher, and M. Rumpf, *Level Set and PDE Based Reconstruction Methods in Imaging: Cetraro, Italy 2008, Editors: Martin Burger, Stanley Osher*. Springer, 2013, vol. 2090.

[7] M. Hanke, *Conjugate Gradient Type Methods for Ill-Posed Problems*. CRC Press, 1995, vol. 327.

[8] B. E. Treeby and B. T. Cox, "k-wave: Matlab toolbox for the simulation and reconstruction of photoacoustic wave fields," *Journal of biomedical optics*, vol. 15, no. 2, p. 021314, 2010.

[9] M. Burger, A. Sawatzky, and G. Steidl, "First order algorithms in variational image processing," in *Splitting Methods in Communication, Imaging, Science, and Engineering*. Springer, 2016, pp. 345–407.

[10] H. Luu, M. Winslett, W. Gropp, R. Ross, P. Carns, K. Harms, M. Prabhat, S. Byna, and Y. Yao, "A multiplatform study of i/o behavior on petascale supercomputers," in *Proceedings of the 24th International Symposium on High-Performance Parallel and Distributed Computing*. ACM, 2015, pp. 33–44.

[11] J. Nieplocha, R. J. Harrison, and R. J. Littlefield, "Global arrays: A nonuniform memory access programming model for high-performance computers," *The Journal of Supercomputing*, vol. 10, no. 2, pp. 169–189, 1996.

[12] Y. Lou, W. Zhou, T. P. Matthews, C. M. Appleton, and M. A. Anastasio, "Generation of anatomically realistic numerical phantoms for photoacoustic and ultrasonic breast imaging," *Journal of biomedical optics*, vol. 22, no. 4, p. 041015, 2017.

Rozvoj digitálnych metód kalibrácie analógových integrovaných obvodov v nanotechnológiách

Michal Šovčík
1. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

Fakulta elektrotechniky a informatiky, Slovenská technická univerzita v Bratislave
Ilkovičova 3, 812 19 Bratislava, SR
michal.sovcik@stuba.sk

***Abstrakt*—Táto práca pojednáva o metódach kalibrácie analógových integrovaných obvodov (IO) realizovaných v nanotechnológiách. V úvodnej časti je predstavená motivácia pre predmetný výskum. Ďalej sú v práci v krátkosti analyzované existujúce techniky kalibrácie analógových IO. V ďalšej časti je predstavená implementácia digitálnej metódy kalibrácie zosilňovača s variabilným zosilnením (VGA) v $130\ nm$ CMOS technológii. Navrhnutý obvodový systém je zameraný na redukciu vstupného napäťového ofsetu (V_{IOFF}) predmetného zosilňovača a je navrhnutý pre napájacie napätie (V_{DD}) $0,6\ V$. V nasledujúcej časti príspevku sú uvedené štatistické výsledky Monte Carlo analýzy V_{IOFF} kalibrovaného VGA v rozsahu teplôt od $-20°C$ až $60°C$. Stredná hodnota μ rozdelenia výsledkov V_{IOFF} kalibrovaného VGA sa pohybuje v rozsahu od $273\ \mu V$ do $413\ \mu V$. Smerodajná odchýlka σ rozdelenia ofsetu sa pohybuje v rozsahu od $356\ \mu V$ do $802\ \mu V$. Pre porovnanie sú uvedené výsledky experimentálnych meraní prototypovej série čipov VGA, ktorý bol vyrobený samostatne v rovnakej technológii. Štatistické výsledky V_{IOFF} získané použitím 60 vzoriek dosahujú $\mu = -1,01\ mV$ a $\sigma = 3,45\ mV$.**

***Kľúčové slová*—rozptyl parametrov technológie, napätia a teploty; digitálna metóda kalibrácie; vstupný napäťový ofset**

I. Úvod

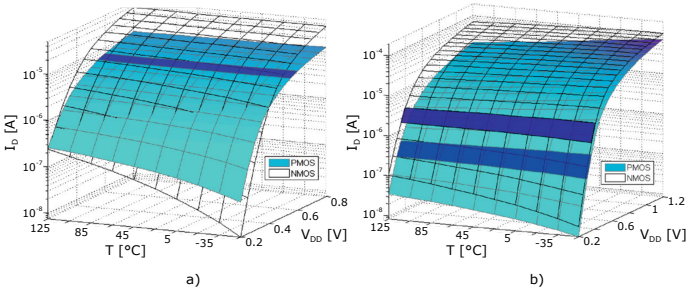
Neustále narastajúci funkčný výkon súčasných elektronických systémov ako aj ich cenová dostupnosť sú výsledkom enormného rozvoja v oblasti návrhu a technológií výroby IO, kde je snahou zmenšovať minimálny rozmer výrobnej technológie. Tento progres v technológii však na druhej strane prináša náhodnú a významnú fluktuáciu elektrických parametrov obvodových elementov. Klesá totiž schopnosť výrobnej technológie zabezpečiť rovnaké technologické parametre pre väčší počet obvodových elementov na čipe, či sériu obvodov. Vzniknuté odchýlky sú značné už v rámci substrátu jedného čipu.

II. Motivácia

Fluktuácia elektrických parametrov obvodových elementov následne vplýva na funkciu či spoľahlivosť IO. Okrem toho, parametre IO dynamicky fluktuujú so zmenou teploty, napájacieho napätia V_{DD} a vplyvom starnutia materiálu. Súhrnne to nazývame PVT (z angl. *process, voltage, temperature*) rozptyl. Na obr. 1 je znázornený vplyv zmeny teploty a napájacieho napätia na hodnotu prúdu tranzistora v diódovom zapojení I_D pre dve technológie CMOS [1]. Z grafov je možné pozorovať, že prúd tranzistora dosahuje väčší rozptyl pri zmene teploty a napájacieho napätia v menšej technológii (obr. 1b). Vzhľadom na výsledky dostupné v práci [1] nebolo možné bližšie kvantifikovať rozptyl I_D v závislosti od technológie, prípadne veľkosti tranzistorov.

Aktuálne dôležitým trendom v návrhu IO je minimalizácia spotreby energie. Túto požiadavku je možné realizovať aj prostredníctvom návrhu IO s nízkym napájacím napätím. Z grafov na obr. 1 je zjavné, že so znižovaním hodnoty V_{DD} rozptyl I_D narastá jednak so zmenou teploty a tiež s variáciou napätia. Navyše táto tendencia je výraznejšia v menšej technológii. Aby bolo možné zabezpečiť optimálnu činnosť IO v nanotechnológiách, je z uvedených dôvodov nutné použiť metódy kompenzácie PVT fluktuácií pomocou kalibrácie IO.

Napríklad, u operačných zosilňovačov (OZ), obvodovým parametrom reprezentujúcim mieru vplyvu PVT rozptylu je V_{IOFF}, ktorý je možné kompenzovať práve použitím vhodnej metódy kalibrácie obvodu. Doposiaľ najširšie používanými metódami kalibrácie analógových IO sú trimovanie, *chopper* stabilizácia a auto-nulovanie (z angl. *auto-zero*).



Obrázok 1. Závislosť prúdu MOS tranzistora od zmeny teploty a napájacieho napätia pre a) 22 nm a b) 90 nm CMOS technológiu [1].

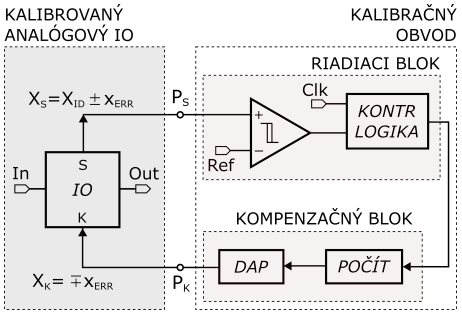
III. Porovnanie metód kalibrácie AIO

Trimovanie prostredníctvom poistiek je jednorazová metóda kompenzácie vplyvu rozptylu technologických parametrov po výrobe IO [2], [3]. Touto metódou nie je teda možné zamedziť spomenutým dynamickým faktorom, ktoré vplývajú na IO

počas jeho dlhodobého využitia v aplikácii. Na druhej strane techniky *chopper* stabilizácia a auto-nulovanie kompenzujú odchýlky elektrických parametrov súbežne s riadnou činnosťou IO (bližšie popísané v [4], [5], [6]). V porovnaní s laserovým trimovaním teda eliminujú aj vplyv teploty a starnutia na parametre IO. Výhodou *chopper* stabilizácie je veľmi nízka hodnota reziduálneho V_{IOFF}, ktorý zostáva prítomný po použití kalibrácie. Na druhej strane táto metóda výrazne obmedzuje šírku pásma OZ a teda aj možnosti jeho použitia.

Metóda auto-nulovania nevnáša do kalibrovaného systému tento nedostatok. Je založená na sekvenčnej dvojfázovej činnosti. V prvej fáze je kalibrovaný OZ v modifikovanej topológii, a kompenzovaný parameter (napr. V_{IOFF}) je zosnímaný. V nasledujúcej fáze je OZ v riadnej činnosti a uchovaná hodnota V_{IOFF} je odčítaná od vstupu. Nevýhodou metódy auto-nulovania je pomerne veľký vplyv presakovania náboja, ktorý vzniká prepínaním režimov zapojenia kalibrovaného obvodu. Tento nedostatok je možné odstrániť implementáciou digitálneho spôsobu kompenzácie snímaného parametra. Avšak digitálne auto-nulovanie naďalej využíva periodickú modifikáciu topológie kalibrovaného OZ za účelom vzorkovania. Táto metóda pomerne účinne eliminuje okrem vplyvu PVT variácií aj šum [4], [5]. Frekvencia spínania topológií musí byť však pomerne vysoká a výstup zosilňovača je teda nespojitý.

V prípade, že vstupný šum nie je pre systém s OZ kritický, je výhodné vynechať vzorkovaciu fázu tejto metódy. Eliminuje sa tak rušivá modifikácia vstupu OZ a proces kalibrácie sa stane plne digitálnym. Na obr. 2 je zobrazená bloková schéma nami navrhovaného systému digitálnej kalibrácie analógových IO, konkrétne OZ.



Obrázok 2. Bloková schéma analógového IO s kalibračným obvodom.

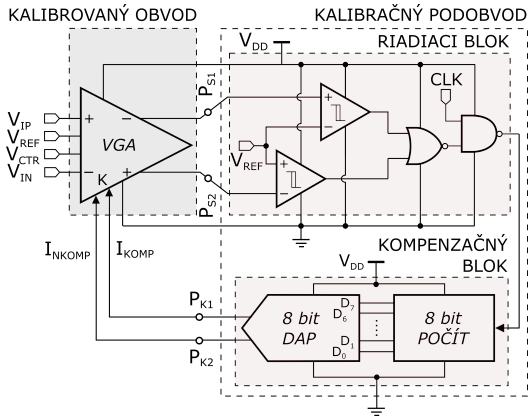
Táto metóda je predmetom nášho výskumu a jej podrobný opis bol publikovaný v prácach [7] a [8]. V nasledujúcej časti preto iba stručne zhrnieme podstatu činnosti navrhovaného systému pre účel súvislosti s jeho implementáciou, ktorá bude opísaná v ďalšej časti príspevku.

Kalibračný obvod na obr. 2 pozostáva z dvoch podblokov, plniacich dve hlavné funkcie. Riadiaci blok sníma úroveň kompenzovaného parametra X_S a podľa tejto informácie riadi dĺžku kalibračného cyklu. Kompenzačný blok generuje analógový kompenzačný signál X_K v závislosti od času trvania cyklu. V okamihu, keď X_S presiahne referenčnú úroveň, riadiaci blok zastaví cyklus a kalibrovaný IO je uvedený do riadnej činnosti. Na kompenzačný port IO je naďalej privádzaná posledne nastavená hodnota parametra X_K.

Kalibračný cyklus OZ je založený na úprave prúdovonapäťových podmienok OZ prostredníctvom jeho kompenzačného portu signálom X_K. Čiže dochádza tiež k narušeniu spracovania signálu zosilňovačom. Tento nedostatok je možné minimalizovať vhodnými technikami. Jednou z nich je známa metóda *"ping-pong"* [9]. Taktiež je možné vďaka digitálnemu prístupu uchovať hodnotu kompenzovaného parametra po skončení posledného cyklu kalibrácie a ďalší cyklus vykonať v skrátenom rozsahu okolo naposledy nastavenej hodnoty X_K. Táto technika si vyžaduje ďalšiu analýzu vplyvu na skreslenie výstupného signálu OZ.

IV. Implementácia digitálnej kalibrácie pre diferenciálny zosilňovač

V rámci nášho výskumu bola zrealizovaná implementácia digitálnej metódy kalibrácie pre zosilňovač s variabilným zosilnením (VGA z angl. *Variable Gain Amplifier*). Návrh topografie OZ a výroba prototypovej série čipov sa uskutočnili v štandardnej $130\ nm$ CMOS technológii. Momentálne prebieha testovanie implementovaného systému kalibrácie, ktorého blokova schéma je zobrazená na obr. 3.

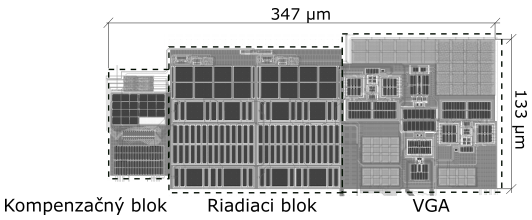


Obrázok 3. Implementácia metódy digitálnej kalibrácie ofsetu pre VGA.

Z porovnania obr. 2 a obr. 3 je možné pozorovať koreláciu jednotlivých blokov systému. Kalibrácia je zameraná na kompenzáciu V_{IOFF} VGA zosilňovača. Nominálna hodnota napájacieho napätia zvolenú technológiu je $1,2\ V$, ale z dôvodu cieľovej aplikácie VGA je celý systém navrhnutý pre $V_{DD} = 600\ mV$. Kalibrovaný zosilňovač dosahuje magnitúdu napäťového zisku $33\ dB$ a šírku pásma $20\ kHz$ (pri záťaži $10\ pF$). Referenčné napätie V_{REF} bude neskôr realizované na čipe pomocou *bandgap* referencie. Jeho hodnota je zvolená ako polovica V_{DD} pre maximálny výstupný rozsah OZ.

A. Topografia

Topografická štruktúra navrhnutej implementácie digitálne kalibrovaného VGA je zobrazená na obr. 4. V štruktúre sú vyznačené hlavné bloky z obr. 3. Plocha kalibračného obvodu dosahuje cca. $0,023\ mm^2$ a kalibrovaný VGA predstavuje plochu približne $0,018\ mm^2$.



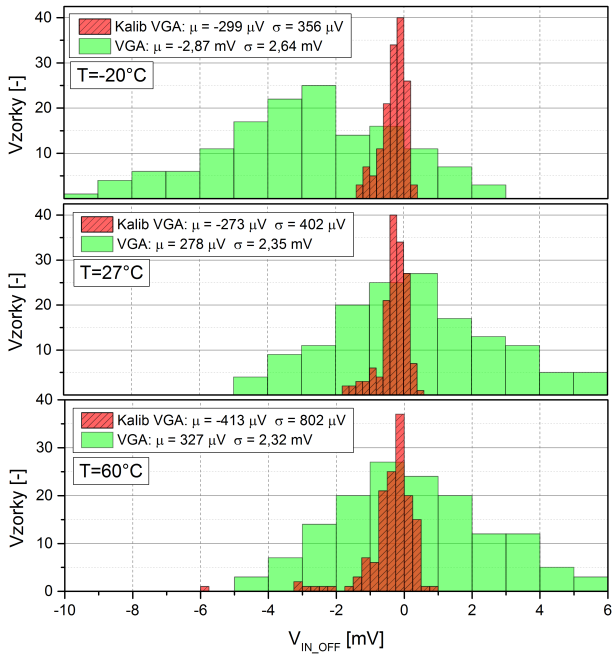
Obrázok 4. Topografia systému digitálne kalibrovaného VGA.

V. Overenie metódy

Navrhnutá metóda kalibrácie bola overená prostredníctvom Monte Carlo (MC) analýzy pri teplotách v rozsahu od $-20°C$ do $+60°C$. Bolo použitých 150 vzoriek a bol uvažovaný vplyv rozptylu technologických parametrov a taktiež rozptyl geometrických rozmerov obvodových elementov.

A. Redukcia vstupného ofsetu

Grafy na obr. 5 zobrazujú porovnanie výsledkov MC analýzy V_{IOFF} zosilňovača VGA bez použitia a s použitím metódy kalibrácie v spomínanom rozsahu teplôt. Jednotlivé histogramy potvrdzujú z hľadiska redukcie V_{IOFF} pomerne úspešne splnený zámer kalibrácie VGA.



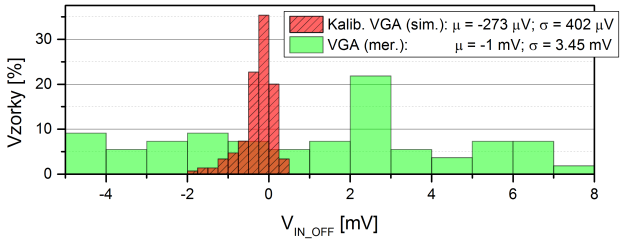
Obrázok 5. Porovnanie výsledkov MC analýzy V_{IOFF} VGA bez použitia a s použitím kalibrácie pri zmene teploty.

V tab. I je uvedený koeficient zmeny μ a σ rozdelenia výsledkov MC analýzy V_{IOFF} VGA pri rôznych teplotách. Tento koeficient predstavuje podiel hodnoty daného ukazovateľa s použitím kalibrácie a hodnoty bez použitia kalibrácie. Ako je možné pozorovať, μ rozdelenie V_{IOFF} s použitím kalibrácie pri teplote približne nad $30°C$ nežiadúco narastá nad 100%. Magnitúda ofsetu však zostáva rádovo na úrovni stoviek μV a preto považujeme tento výsledok za akceptovateľný. Na druhej strane, hodnota σ s použitím kalibrácie značne klesá, v uvedenom rozsahu teplôt na $13,5\%$ až 35%. V tab. I sú uvedené tiež hodnoty μ a σ ofsetu kalibrovaného VGA v rámci 10 % variácie napájacieho napätia. Je možné vidieť že metóda kalibrácie je pomerne stabilná.

Tabuľka I
Koeficient zmeny ukazovateľov rozdelenia výsledkov MC analýzy V_{IOFF} pri použití kalibrácie v rôznych teplotách.

	Koeficient zmeny [%] (V=0.6 V)				**Odchýlky vplyvom zmeny V_{DD} [μV] (T=27°C)**		
	Teplota [°C]				**V_{DD} [V]**		
	-20	**27**	**40**	**60**	**0.54**	**0.60**	**0.66**
μ	11	98	158	126	-312	-273	-263
σ	14	17	19	35	541	402	541

V minulosti bolo vykonané experimentálne meranie V_{IOFF} nekalibrovaného VGA, ktorý bol skoršie vyrobený taktiež v rovnakej technológii. Meranie prebehlo pri teplote približne $27°C$ s použitím 60 nezapuzdrených vzoriek. Na obr. 6 je znázornené porovnanie výsledkov meraní s výsledkami MC analýzy kalibrovaného VGA (totožné s histogramom pre $27°C$ na obr. 5). Zlepšenie ukazovateľov rozdelenia V_{IOFF} je zjavné. Stredná hodnota je znížená na 27% a smerodajná odchýlka na 12%.

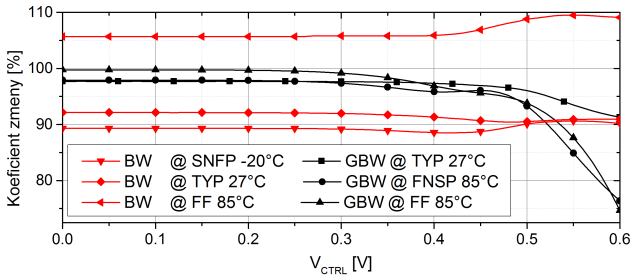


Obrázok 6. Porovnanie výsledkov MC analýzy V_{IOFF} kalibrovaného VGA a experimentálnych výsledkov nekalibrovaného VGA.

B. Nežiaduci vplyv obvodov kalibrácie na VGA

Ako vyplýva z kapitoly IV, aby bolo možné kalibračným obvodom modifikovať prúdovo-napäťové podmienky VGA, topológia zosilňovača bola upravená. V uzloch VGA, kde sa pripája vstup a výstup kalibračného obvodu vzniká dodatočná kapacita, ktorá mení pôvodnú prenosovú funkciu VGA. Následkom toho sa zmenia frekvenčné vlastnosti zosilňovača. Preto bola vykonaná simulačná analýza šírky pásma zisku (GBW) a pásma prenosu (BW). Na obr. 7 je znázornený koeficient zmeny týchto parametrov po pripojení kalibračného obvodu (rovnako ako v prípade koeficientu zmeny μ a σ v tab. I) v závislosti od riadiaceho napätia (V_{CTR}) VGA. V simulácii bol uvážený rozptyl parametrov výrobnej technológie a tiež rozsah teplôt $-20°C$ až $85°C$. Jednotlivé priebehy predstavujú najväčšie odchýlky od nominálnych priebehov. Hodnoty GBW sú mierne redukované v rozsahu V_{CTR} $0 - 0,45$ V, tzn. pri vyššom zisku VGA. Pre vyššie hodnoty V_{CTR} GBW klesá v najhoršom prípade na 75% pôvodnej hodnoty, pričom tento

rozsah korešponduje s nízkym ziskom VGA. Priebeh BW je oveľa menej závislý od V_{CTR}. V najhorších prípadoch sa BW mení vplyvom pripojenia kalibračného obvodu na 88% a 109% pôvodnej hodnoty.



Obrázok 7. Závislosť koeficientu zmeny BW a GBW zosilňovača v najhorších prípadoch okrajových podmienok.

VI. Zámer a rámcové ciele dizertačnej práce

Medzi tézy dizertačnej práce patrí určenie podmienok pri, ktorých bude použitie digitálnej kalibrácie výhodnejšie ako iné metódy kompenzácie vplyvu PVT z hľadiska náročnosti (náklady, spotreba energie, a pod.). Pre objektívne porovnanie metód kalibrácie, vyhodnotenie získaných výsledkov a prínosu nášho výskumu bude preto užitočné zaviesť merateľný ukazovateľ (FOM z angl. *Figure of merit*). Tento FOM je tvorený nasledovnými zložkami:

- $K(\mu, \sigma)$ - kompenzačný koeficient, kvantifikujúci výsledok kalibrácie prostredníctvom zmeny strednej hodnoty a smerodajnej odchýlky súboru kalibrovaných vzoriek,
- $\prod_{i=1}^{n} R_i(P_{AIO\_i})$ - produkt koeficientov zmeny n sledovaných parametrov kompenzovaného obvodu (P_{AIO_i}),
- A_{KPO}/A_{KO} - pomer plochy prídavných obvodov kalibračnej techniky k ploche kalibrovaného obvodu,
- N_{DOD} - dodatočné náklady po výrobe IO vplyvom použitia danej kalibračnej metódy.
- P_{SUP} - príkon prídavných obvodov pre realizáciu kalibrácie.

Najbližším cieľom dizertačnej práce je experimentálna verifikácia činnosti navrhnutého systému kalibrácie VGA, kde chceme overiť simulované parametre a optimalizovať pôvodné atribúty návrhu.

Z hľadiska použitia kalibrovaného VGA v komplexnejšom systéme bude potrebné vytvoriť automatické riadenie kalibračného cyklu. Za účelom kompenzácie vplyvu nielen statických faktorov, ale aj vplyvu teploty a zmeny napájacieho napätia je potrebné kalibračný cyklus vykonávať súbežne s činnosťou VGA. Táto požiadavka predstavuje však nespojitosť, respektíve skreslenie výstupného signálu VGA. Cieľom dizertačnej práce je preto tiež návrh riešenia súbežnej kalibrácie VGA počas jeho činnosti. Pre tento účel bude možné vďaka digitálnemu prístupu ľahko uchovať informáciu o výsledku posledného cyklu kalibrácie a skrátiť tak ten nasledovný.

Z hľadiska nežiaduceho spätného vplyvu kalibračného obvodu na frekvenčné vlastnosti VGA bude v budúcnosti charakterizovaný vplyv na prenosovú funkciu zosilňovača s cieľom jeho minimalizácie. Súčasťou tejto tézy práce bude analýza viacerých konfigurácií pripojenia kalibračného obvodu k VGA.

Za účelom efektívnejšej činnosti obvodov kalibračnej techniky pri nízkom napájacom napätí budú v budúcnosti analyzované možnosti použitia prístupu *bulk-driven*.

Pre zefektívnenie algoritmu kalibrácie bude použité spojenie dvoch DA prevodníkov s rôznymi veľkosťami plného výstupného rozsahu.

VII. Záver

V tomto príspevku bola analyzovaná digitálna metóda kalibrácie analógových integrovaných obvodov v porovnaní s alternatívnymi metódami. Ďalej bol opísaný všeobecný princíp tejto metódy a jej implementácia v $130\ nm$ CMOS technológii pre kompenzáciu ofsetu vstupného napätia VGA. Účinnosť metódy bola overená pomocou Monte-Carlo analýzy v rozsahu teplôt $-20°C$ až $60°C$. Vzhľadom na výsledky je možné tvrdiť, že analyzovaná metóda je schopná značne potlačiť vplyv rozptylu výrobnej technológie a teploty na vlastnosti VGA.

V rámci mojej doterajšej práce a výskumu vzniklo 12 publikácií, ktorých som prvoautorom alebo spoluautorom (2 príspevky v zahraničných karentovaných časopisoch, 1 príspevok v zahraničnom časopise registrovanom v databázach Web of Science alebo SCOPUS, 8 príspevkov na medzinárodných konferenciách a 1 príspevok na domácej konferencii).

Poďakovanie

Táto práca bola podporená projektami APVV-15-0254, VEGA 1/0762/16 a VEGA 1/0905/17.

Literatúra

[1] D. Wolpert and P. Ampadu, *Managing Temperature Effects in Nanoscale Adaptive Systems*. Springer New York, 2011. [Online]. Available: https://books.google.sk/books?id=iju-fRTmX10C

[2] T. He, F. Zhang, S. Bhunia, and P. X. L. Feng, "Silicon carbide (sic) nanoelectromechanical antifuse for ultralow-power one-time-programmable (otp) fpga interconnects," *IEEE Journal of the Electron Devices Society*, vol. 3, no. 4, pp. 323–335, July 2015.

[3] Synopsis, "Antifuse-based split-channel 1t-fuse bit cell for otp nvm ip," https://www.synopsys.com/dw/ipdir.php?ds=nvm˙1t-bit-cell, accessed Januar 3, 2018.

[4] M. Pastre and M. Kayal, *Methodology for the digital calibration of analog circuits and systems*. Springer, 2006.

[5] C. C. Enz and G. C. Temes, "Circuit techniques for reducing the effects of op-amp imperfections: autozeroing, correlated double sampling, and chopper stabilization," *Proceedings of the IEEE*, vol. 84, no. 11, pp. 1584–1614, Nov 1996.

[6] P. Godoy and J. L. Dawson, "Chopper stabilization of analog multipliers, variable gain amplifiers, and mixers," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 10, pp. 2311–2321, Oct 2008.

[7] M. Šovčík, V. Stopjaková, D. Arbet, M. Kováč, and M. Potočný, "Digital methods of calibration for analog integrated circuits in nanotechnologies," in *2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Oct 2017, pp. 1–6.

[8] M. Šovčík, V. Stopjaková, D. Arbet, L. Nagy, and M. Kováč, "Digital methods of calibration for analog integrated circuits in nanotechnologies," in *23rd International Conference on Applied Electronics 2018 [to be published]*, 2018.

[9] M. Kayal, R. T. L. Saez, and M. Declercq, "An automatic offset compensation technique applicable to existing operational amplifier core cell," in *Proceedings of the IEEE 1998 Custom Integrated Circuits Conference (Cat. No.98CH36143)*, May 1998, pp. 419–422.

Počítačové architektury a diagnostika PAD 2018
Pracovní seminář pro studenty doktorského studia

Editoři sborníku: Vlastimil Vavřička, Stanislav Racek, Karel Dudáček

Grafický návrh přebalu: Karel Dudáček

Vydala Západočeská univerzita v Plzni, Univerzitní 8, 306 14Plzeň

1. vydání

56 stran

Plzeň 2018

ISBN 978-80-261-0814-6