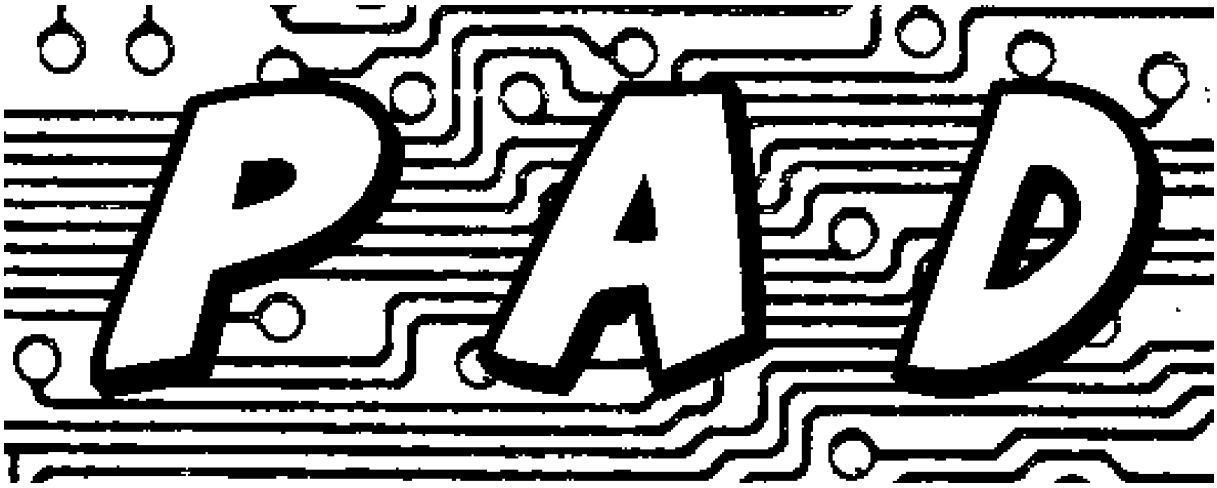
Sborník příspěvků PAD 2021

Počítačové architektury & diagnostika

Česko-slovenský seminář pro studenty doktorského studia



Online seminář 12. 1. 2022
Technická univerzita v Liberci, FMMIS

Sborník příspěvků PAD 2021

Počítačové architektury & diagnostika

Elektronická verze

Martin Rozkovec a Zdeněk Plíva, editoři

Technická univerzita v Liberci

Fakulta mechatroniky, informatiky a mezioborových studií

Ústav informačních technologií a elektroniky

Úvodní slovo

PAD 2021 je osmnáctým pokračováním československého doktorského semináře, původně zaměřeného na prezentování nových myšlenek v oboru architektur a diagnostiky počítačů. Osmnáctý PAD 2021 se měl původně jmenovat PAD 2020 a měl se pořádat pod záštitou Fakulty mechatroniky a Technické univerzity v Liberci. Konal by se v obci Bedřichov. V samotném srdci Jizerských hor.

V roce 2020 zasáhla celý svět pandemie koronaviru a seminář byl přesunut na rok 2021. I v roce 2021 jsme ho po zralé úvaze zrušili jako prezenční událost a uspořádali jej formou online semináře. Seminář se konal 12. 1. 2022, zúčastnili se jej, jak tomu tradičně bývá, doktorandi a školitelé z České a Slovenské republiky. Předneslo se sedm příspěvků a ke každému proběhla diskuse s oponentem, tak jak by tomu bylo, kdybychom se sešli v chatě na Bedřichově.

Osmnáctý PAD byl však jiný v tom, že po samotném semináři nenásledovaly vzrušené neformální diskuse při obědě, společný výletech nebo seznamování se večer nad sklenkou něčeho dobrého. Doktorandům chyběly neformální zpětné vazby oproštěné od konferenčních svázaností, rady od školitelů, připomínky kolegů. Školitelé, kdysi dávno či nedávno v roli studentů se po roce nepotkali a nesdělili si novinky z profesního nebo i soukromého života. Je to škoda, zamrzí to, ale nedá se s tím nic dělat. Doufám, že v dalších letech bude tradice PAD obnovena. V časech, které budou o něco příznivější.

Na tomto místě bych chtěl poděkovat sponzorům - Fakultě mechatroniky, informatiky a mezioborových studií a firmě ČEZ, bez jejichž podpory by se akce nekonala.

Martin Rozkovec

Vážené kolegyně, vážení kolegové, mám rád Jizerské hory, zejména za podzimních mlh a prvních mrazíků a těšil jsem se, že v rámci social-eventu se budeme moci o toto kouzlo podělit. Bohužel, epidemická situace, resp. následně vyvolaná omezení zabránila pořádání "řádného" PADu v roce 2020, a na rozdíl od olympijských her jsme neuspěli ani v roce 2021. Chápu že se sedmi příspěvky nedává smysl pořádat tradiční prezenční workshop, se sekcemi, s vložným a trmácet se až na sever Čech a proto jsem vděčný i za letošní velmi komorní formu. A tak mi nezbývá než poděkovat studentům za zaslané příspěvky, jejich školitelům za spolehlivé vedení i oponentům za vypracování posudků. A v neposlední řadě děkuji Martinovi Rozkovcovi za uspořádání celé akce - mohlo by se zdát, že půldenní akce se zvládne hravě, ale jsem přesvědčen, že uspořádání "normálního" PADu by spotřebovalo méně času i sil. Ale věřím, že jste si šetřili síly na další ročníky.

Zdeněk Plíva

Ocenění studenti PAD 2021

I letos proběhla volba nejlepšího příspěvku v rámci semináře.

Cenu obdržel student 2. ročníku doktorského studia pan:

Alexandr Valach, FIIT, STU, Bratislava, SR

Řídící výbor PAD 2021

prof. Ing. Viera Stopjaková, PhD., FEI STU Bratislava (předsedkyně RV)
doc. Ing. Vladimír Drábek, CSc., FIT VUT v Brně
Ing. Katarína Jelemenská, PhD., FIIT STU v Bratislave
doc. Ing. Richard Růžička, Ph.D., MBA, FIT VUT v Brně
Ing. Robert Kvaček, ASICentrum Praha
prof. Ing. Róbert Lórencz, CSc., FIT ČVUT v Praze
prof. Ing. Ondřej Novák, CSc., FMIMS TU v Liberci
doc. Ing. Tomáš Koutný, PhD., FAV ZČU v Plzni

Programový výbor PAD 2021

Daniel Arbet, FEI STU v Bratislave
Jiří Buček, FIT ČVUT v Praze
Pavel Čičák, FIIT STU v Bratislave
Vladimír Drábek, FIT VUT v Brně
Karel Dudáček, FAV ZČU v Plzni
Miloš Drutarovský, FEI TU v Košiciach
Petr Fišer, FIT ČVUT v Praze
Jiří Jaroš, FIT VUT v Brně
Katarína Jelemenská, FIIT STU v Bratislave
Jan Kořenek, FIT VUT v Brně
Tomáš Koutný, FAV ZČU v Plzni
Ivan Kotuliak, FIIT STU v Bratislave
Robert Kvaček, ASICentrum Praha
Hana Kubátová, FIT ČVUT v Praze
Robert Lórencz, FIT ČVUT v Praze
Ondřej Novák, FMIMS TU v Liberci
Martin Novotný, FIT ČVUT v Praze
Zdeněk Plíva, FMIMS TU v Liberci
Martin Rozkovec, FMIMS TU v Liberci
Richard Růžička, FIT VUT v Brně
Jan Schmidt, FIT ČVUT v Praze
Vladimír Smotlacha, FIT ČVUT v Praze
Viera Stopjaková, FEI STU v Bratislave
Josef Strnadel, FIT VUT v Brně
Karel Vlček, UTB ve Zlíne
Tomáš Zahradnický, 1stplugins s.r.o. Praha
Marcela Zachariášová, FIT VUT v Brně

Organizační výbor PAD 2021

Martin Rozkovec, FMIMS TU v Liberci
Ondřej Novák, FMIMS TU v Liberci
Zdeněk Plíva, FMIMS TU v Liberci
Radana Jedličková, FMIMS TU v Liberci

Obsah

Příspěvky doktorandů

Cryptanalysis With Aid of Passive and Active Combined Attacks

Marina Shchavleva
first year, full-time study
Supervisor: prof. Ing. Róbert Lórencz, CSc.
Specialist supervisor: Ing. Jiří Buček, Ph.D.

Department of Information Security
Faculty of Information Technology
Thákurova 9, 160 00 Praha, Czech Republic
shchamar@fit.cvut.cz

***Abstract*—Security of cryptographic algorithms should be studied not only in the context of their resistance to classic cryptanalysis, but also in the context of resistance of their implementation against hardware attacks such as side-channel analysis and fault injection. Future thesis would aim at the combination of the two and how to make it worth the added complexity. As new encryption algorithms are emerging from NIST contests, it is important to investigate how do they stand against combined attacks.**

***Keywords*—side-channel analysis, fault injection, combined attacks**

I. Introduction

Attacks that target hardware running a cryptographic algorithm challenge conditional security of said algorithm. These attacks exploit algorithm's implementation in combination with physical properties of a device.

This paper describes noninvasive attacks, which do not require depackaging of a device. Attack of this kind might be passive, meaning that adversary is observing physical behavior of the device during execution of an algorithm. Or, attack is active and adversary is able to influence function of the device.

The above-mentioned attacks are often considered separately, and countermeasures are devised as such. However, it is possible to design an attack that combines both passive and active approaches.

Combined attacks are the main topic of this paper, which is organised as follows: section II describes what are passive and active attacks, and how are these combined, section III outlines currently open problems in the field of combined attacks, section IV states the goal of the future thesis and the way to approach it, section V presents results that were achieved so far, and section VI concludes the paper.

II. Background

A. Passive attacks

Passive attacks rely on analysis of a device's side-channel like it's power consumption in order to retrieve secret information such as keys used in encryption. Analysis tools vary from calculating difference between two traces of collected data [1] to using machine learning techniques [2].

While a lot of passive attacks require that adversary has the device under attack in their hands, some of newer research allows them to collect EM traces while being several meters away from the device [3], or even conduct power analysis remotely in a software-based attack [4].

Variety of countermeasures to side-channel analysis exist, such as masking, which alters sensitive data as it goes through the algorithm in order to mask their presence in the side-channel, or hiding, where calculations are hidden in time or in noise.

B. Active attacks

In the active attack scenario, adversary aims to introduce an error in algorithm's calculation by manipulating with the device, for example

by disturbing a clock signal, or by manipulating a voltage supply. This creates a faulty output, which is then analyzed in order to extract secret data, such as private keys in RSA [5]. The goal of active attack is to affect the largest part of the output with fault as small as possible.

To counter fault injection, various error detections are implemented such as error detection codes, or double execution of the algorithm (in case of ciphers it might be double encryption or encryption-decryption).

Although both active and passive attacks are essentially side-channel analysis based attacks, to differentiate them in this paper term "side-channel analysis" is used only for passive attacks, while term "fault injection" or "fault analysis" is used for active attacks.

C. Combined passive and active attacks

Combined attacks require utilizing both passive and active techniques, which creates a new type of attack. While being more complex in realization, combined approach might be more effective than any of the attack separately.

There are two main types of combined attacks.

1) Side-channel analysis supported by fault injection: this type of attack uses fault injection as a tool to obtain traces, that could be more easily analysed.

With fault injection such attack could disarm countermeasure such as masking by simply skipping over random number generation [6], or by transforming valid input into faulty (and leaky) input after it had passed a validity check [7].

2) Fault analysis supported by side-channel analysis: this strategy uses side-channel as a source of additional information to fault analysis.

By observing side-channel adversary might obtain fault propagation pattern and determine important parameters such as fault mask or fault location [8], which greatly reduce key's search-space. Some implementations might stop the calculation if fault was detected, so side-channel analysis might give the information that device had not [9].

III. Open problems

In the future work, the following subset of open problems would be explored.

A. New combinations of attacks

As fault injection already proved to be useful as a tool for overcoming various protections [6], [7], there is a potential for other ways of utilising faults in a side-channel context.

As for side-channel assisted fault analysis, it might be beneficial to utilize machine-learning techniques [2].

B. New encryption algorithms emerging

Two important contests for new cryptographic algorithms are currently running: for lightweight cryptography and for post-quantum cryptography. These algorithms should be closely studied in all lights, including hardware attacks and combined attacks specifically. While there is some research around combined attacks for lightweight algorithms [8], and both passive [10] and active [11] attacks against post-quantum cryptography, PQC and LWC algorithms are still new and require thorough investigation.

C. Attack practicality

Practical aspects of combined attacks are important as well, such as complexity of target devices and complexity of attacks that comes with it.

Since combination of attacks is inherently more complex than attacks on their own, the gain from it must be at least in balance with losses, and, ideally, should outweigh them.

IV. Goal

The goal of the dissertation is to devise novel attacks against various algorithms, including post-quantum and lightweight ones.

First steps to achieve this goal would be the following. To get a close acquaintance with the studied algorithms, first it would be necessary to examine state-of-the-art side-channel analysis attacks and fault injection attacks against these algorithms.

From that point a straight-forward approach seems to be to attempt to add side-channel analysis to already known fault injection attacks.

Since physical fault injection might be unpredictable in terms of resulting side-channel traces due to additional noise created by the fault, it might prove useful to use software simulation of the fault which makes the overall setup simpler.

V. Achieved results

As a pilot, fault injection attack against AES state[12] was taken to be combined with side-channel analysis. The idea is very similar to the idea of extracting fault propagation pattern from side-channel presented in [8].

A. Preliminaries

1) AES: the advanced Encryption Standard is a block cipher with block size of 128 bits and key sizes of 128, 192, 256 bits. Internally AES performs 10, 12 or 14 rounds respectively to key sizes. Round transforms internal state, which is presented by 4×4 matrix, with each element containing one byte (8 bits). Each round, except the last one, contains four operations:

1) SubBytes performs a non-liner transformation SubByte on each byte,
2) ShiftRows shifts each row to the left by $roworder - 1$, so first row is not shifted,
3) MixColumns multiplies state matrix modulo irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ by matrix of coefficients,
4) AddRoundKey applies round key to state with xor operation.

Last round does not contain MixColumns operation. Each round key is created from previous round key, first round key is created from initial key. Before first round, initial key is xored with plaintext block.

2) DFA on AES: The above-mentioned fault injection attack against AES targets MixColumns operation. If one byte fault is injected before two latest MixColumns operations, it is then spread across entire column in a linear manner. Fault is visible in ciphertext due to how column values are spread after ShiftRows.

To obtain last round key byte K from correct ciphertext byte C and faulty ciphertext byte C', the following equation should be solved

$$F = S^{-1}(K \oplus C) \oplus S^{-1}(K \oplus C')$$

where F is the fault that appears *after* last MixColumns and S^{-1} is inverse SubByte. There would be four of these equations for each faulty ciphertext byte.

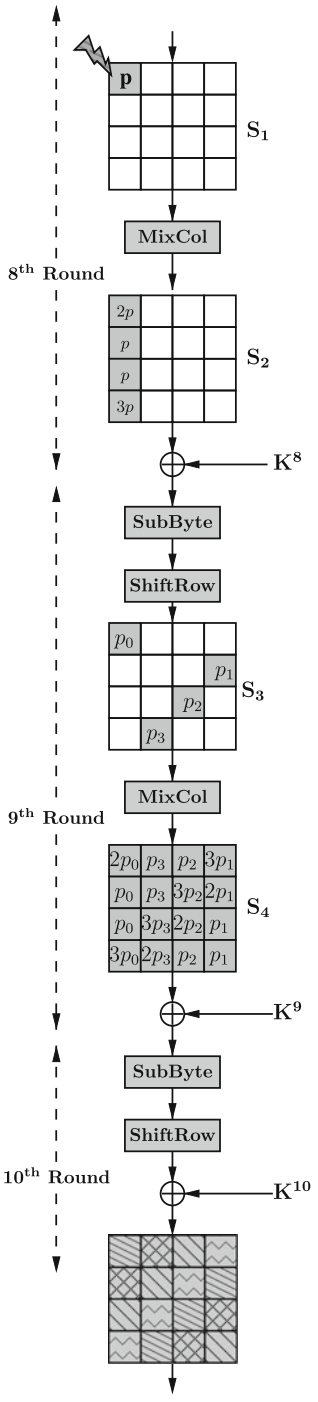


Figure 1. The effect of fault included before penultimate MixColumns[12]

Indices should be added appropriately, with respect that fault values are related between four bytes of ciphertext because of MixColumn's linearity. For fault f, injected in the $(1, 1)$ byte of the state *before* last MixColumns, the coefficients would be $2f, 3f, 1f, 1f$ in order of faulty bytes in the resulting ciphertext.

Improved attack targets the penultimate MixColumns. ShiftRows would transfer the affected column's bytes each to a different column, so after the last MixColumns every byte of ciphertext is affected. Figure 1 shows how are faults spread in this situation.

B. Proposed attack idea

The precise position of fault in a column affects fault coefficients in the above equation. Since this location could not be deduced from ciphertexts only, in order to find a correct key one needs to solve a system of four equations four times for each possible coefficient group.

The idea of proposed attack is to locate where the fault occurred through side-channel. This could be achieved by analysis of difference between two side-channel traces, which are collected during normal execution of AES and during faulty execution. From the differential trace one can deduce which column was affected by the fault in the penultimate MixColumns, which reduces fault analysis complexity four times. The attack assumes unprotected implementation of AES and that every operation processes bytes in their order in memory.

Fault can be detected first by a higher difference in the affected column in MixColumns, and then by a pattern of fault spread by ShiftRows in operations, that process each byte of the state sequentially such as AddRoundKey and SubBytes. Figure 2 shows expected difference pattern.

Proposed idea is similar to the attack presented in [8] because it utilizes side-channel as a source of information on fault propagation pattern. The difference is that in the PRESENT cipher fault propagation pattern is directly influenced by fault value as cipher uses bit permutations, and AES operates on bytes, thus the precise value of the fault can not be deduced from fault propagation pattern only.

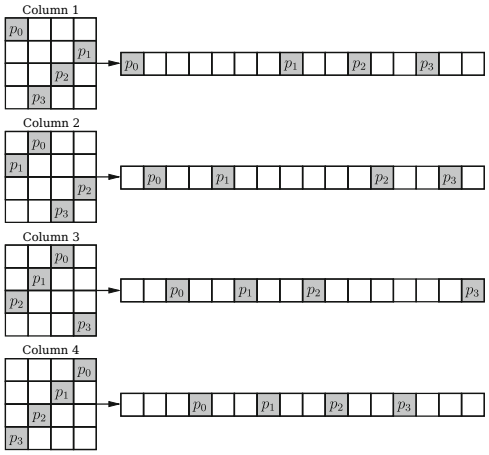


Figure 2. Fault occurrence in the state as bytes in it are processed by operations after ShiftRows.

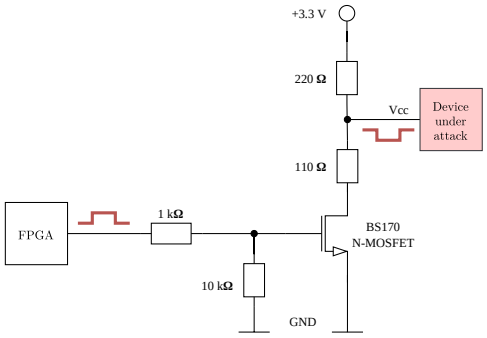


Figure 3. FPGA voltage-drop pulse setup

C. Experiment setup

The aim of the experiment is to determine, whether such faults could be detected through side-channel.

We used ATmega8 as a target device with AES-128, which has both key and plaintext hardcoded. Besides debugging inputs, it receives only reset signal, and outputs ciphertext on UART interface.

Faults were injected through voltage drop, which was controlled through a transistor and FPGA. On the command from PC, FPGA sends a pulse to the processor, see the scheme in figure 3.

Power side-channel was then measured with an oscilloscope.

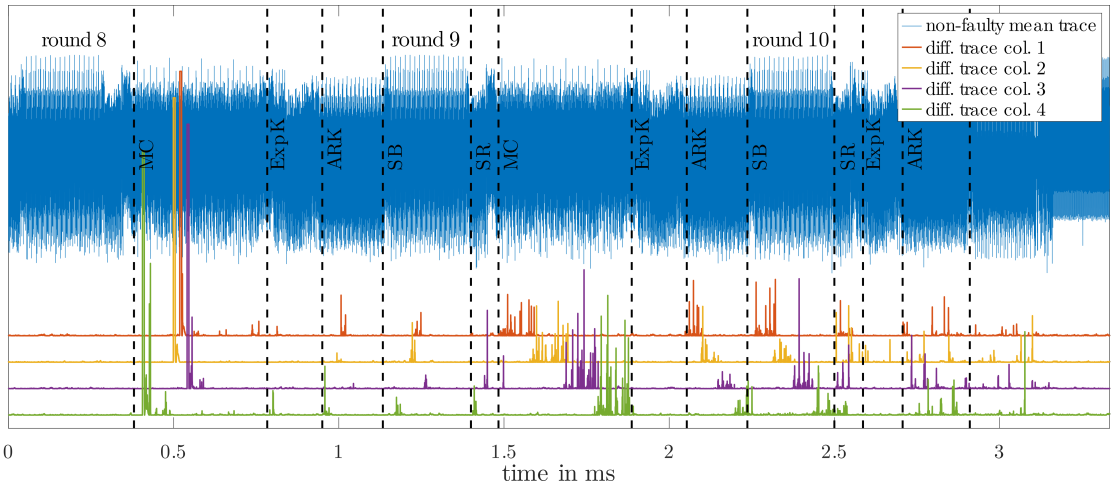


Figure 4. Last rounds of AES-128 with differential traces for each column.

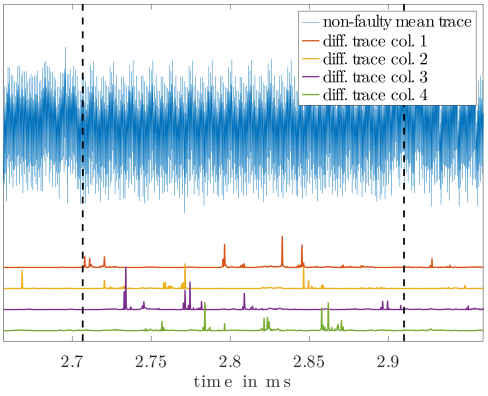


Figure 5. Last AddRoundKey with with differential traces for each column.

D. Experimental results

In order to prove that fault detection is possible, fault was induced before the last MixColumns, so the fault spread pattern is also visible in ciphertext. For each fault spread pattern and also for a normal run ten traces of power consumption were collected, a mean trace of every group was calculated to minimize noise. Fault value was the same inside every group, which is proven by the same faulty ciphertext. Difference with non-faulty mean trace was calculated for traces with each fault pattern. Resulting difference traces were then filtered with a low pass filter in order to further reduce noise.

In figure 4 the non-faulty mean trace is juxtaposed with all four difference traces, so it is easier to locate where each operation is. The difference columns is clearly visible in the last MixColumns.

In figure 5 one can see similar fault spread pattern as in ciphertext (see figure 2).

In the operations before last MixColumns, single byte fault is also visible.

E. Experiment conclusion

In a pilot study it was found that for unprotected AES it is possible to detect fault location. This could lower the complexity of DFA, even though not to a large amount. In the future following topics would be researched:

- possibility of extracting information about fault value,
- further improvements to DFA attack with side-channel knowledge,
- whether there is possibility of mounting the same attack against protected implementations.

VI. Conclusion

Combined passive and active attacks have a potential to be a bigger threat than single attacks on their own. The thesis goal is to study possibilities and feasibility of combined attacks for encryption algorithms.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", in, Springer Berlin Heidelberg, 1999, pp. 388–397.

[2] G. Perin, Ł. Chmielewski, L. Batina, and S. Picek, "Keep it unsupervised: Horizontal attacks meet deep learning", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 1, pp. 343–372, 2020. DOI: 10.46586/tches.v2021.i1.343-372.

[3] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming channels", in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ACM, 2018.

[4] M. Lipp, A. Kogler, D. Oswald, M. Schwarz, C. Easdon, C. Canella, and D. Gruss, "Platypus: Software-based power side-channel attacks on x86", in *2021 2021 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA: IEEE Computer Society, 2021, pp. 1080–1096.

[5] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults", in, Springer Berlin Heidelberg, 1997, pp. 37–51. DOI: 10.1007/3-540-69053-0_4. [Online]. Available: https://doi.org/10.1007%2F3-540-69053-0_4.

[6] Y. Yao, M. Yang, C. Patrick, B. Yuce, and P. Schaumont, "Fault-assisted side-channel analysis of masked implementations", in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, IEEE, 2018.

[7] J. Fan, B. Gierlichs, and F. Vercauteren, "To infinity and beyond: Combined attack on ECC using points of low order", in *Cryptographic Hardware and Embedded Systems – CHES 2011*, Springer Berlin Heidelberg, 2011, pp. 143–159.

[8] S. Patranabis, N. Datta, D. Jap, J. Breier, S. Bhasin, and D. Mukhopadhyay, "Scadfa: Combined sca+dfa attacks on block ciphers with practical validations", *IEEE Transactions on Computers*, vol. 68, no. 10, pp. 1498–1510, 2019.

[9] T. Roche, V. Lomné, and K. Khalfallah, "Combined fault and side-channel attack on protected implementations of aes", in *Smart Card Research and Advanced Applications*, E. Prouff, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 65–83, ISBN: 978-3-642-27257-8.

[10] P. Ravi, S. Sinha Roy, A. Chattopadhyay, and S. Bhasin, "Generic side-channel attacks on cca-secure lattice-based pke and kems", 3, vol. 2020, 2020, pp. 307–335. DOI: 10.13154/tches.v2020.i3.307-335.

[11] P. Ravi, D. B. Roy, S. Bhasin, A. Chattopadhyay, and D. Mukhopadhyay, "Number "not used" once - practical fault attack on pqm4 implementations of NIST candidates", in *Constructive Side-Channel Analysis and Secure Design*, Springer International Publishing, 2019, pp. 232–250.

[12] S. S. Ali, D. Mukhopadhyay, and M. Tunstall, "Differential fault analysis of AES: Towards reaching its limits", vol. 3, no. 2, pp. 73–97, 2012.

Návrh a analýza spotreby energie MPPT kontroléra v 130 nm CMOS technológii

Adam Hudec
2. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

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

***Abstrakt*—Tento príspevok sa zaoberá návrhom číslicového obvodu pre hľadanie bodu maximálneho výkonu MPPT (angl. Maximum Power Point Tracking) zberača energie, a následne najmä analýzou jeho vlastnej spotreby energie. Vyšetrovanie parametrov je vykonávané na najpoužívanejšom priamom MPPT algoritme "Naruš a pozoruj". Tento číslicový obvod bol na medziregistrovej úrovni RTL (angl. Register Transfer Level) navrhnutý pomocou opisného jazyka Verilog. Následná syntéza a proces rozmiestnenia a prepojenia P&R (angl. Place and Route) boli realizované v 130 nm CMOS technológii. V závere príspevku sú zhrnuté výsledky týkajúce sa spotreby energie MPPT kontroléra a taktiež stanovené rámcové ciele dizertačnej práce.**

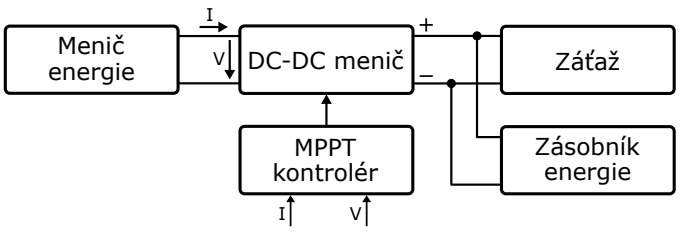
***Kľúčové slová*—Zberače energie, Hľadanie bodu maximálneho výkonu, Naruš a pozoruj, MPPT algoritmy**

I. Úvod

Neustály vývoj a výskum polovodičových materiálov a technológií výroby integrovaných obvodov vedie k zlepšovaniu vlastností a zmenšovaniu rozmerov tranzistora, a zároveň k väčšej integrácii elektronických systémov na čip. Spolu so zmenšovaním tranzistorov klesá aj hodnota napájacieho napätia, čo otvára nové možnosti pre návrh a využitie nízkopríkonových elektronických systémov napájaných z batérie, kde práve spotreba energie sa stáva kľúčovým parametrom. Takýmito systémami sú vo všeobecnosti elektronické obvody, ktoré nemajú možnosť byť pripojené k stálemu zdroju elektrickej energie. Do tejto kategórie spadá napríklad progresívna oblasť internetu vecí – IoT (angl. Internet of Things) [1], kde najčastejším zdrojom energie bývajú práve batérie. Moderné techniky návrhu nízko-príkonovej elektroniky otvárajú priamu cestu k implementácii tzv. zberačov energie (angl. Energy Harvesters) z okolia, ktoré vedia predĺžiť životnosť batérií alebo v istých prípadoch tieto batérie úplne nahradiť. Zberače energie sa tak čoraz častejšie stávajú súčasťou rôznych elektronických obvodov, najmä senzorových systémov [2].

II. Motivácia

Úlohou zberačov energie je konvertovať formu energie dostupnú v okolí (napr. slnečnú, tepelnú alebo mechanickú) na elektrickú energiu. Ich elementárny základ je tvorený meničom energie a následným meničom napätia. Obvod pozostávajúci len zo spomenutých dvoch častí zvyčajne nie je schopný efektívne fungovať z dôvodu fluktuácie vstupných podmienok. Na to, aby bol zabezpečený maximálny prenos energie zo vstupu zberača na jeho výstup, je nevyhnutné pripojiť prídavný riadiaci číslicový obvod tzv. MPPT kontrolér. Jeho implementáciu vo všeobecnom zberači energie môžeme vidieť na Obr. 1.



Obrázok 1. Všeobecná bloková schéma zberača energie.

Schopnosť ladiť zberač energie na maximálny prenos energie umožňujú buď nepriame alebo priame riadiace metódy, ktoré sa od seba líšia zložitosťou, rýchlosťou a presnosťou. Tieto parametre najčastejšie negatívne ovplyvňujú veľkosť využitej plochy na čipe a najmä vlastnú spotrebu elektrickej energie.

Meniče energie akými sú napríklad termoelektrické generátory a hlavne solárne články generujú dostatok energie a spotreba samotného MPPT kontroléra nie je v takýchto prípadoch kritickým parametrom, a preto je tu veľký priestor pre robustnosť algoritmov. Pri iných typoch meničov, akými sú piezoelektrické alebo RF [3] meniče, môže pri zložitých algoritmoch neoptimalizovaných na spotrebu dôjsť k stavu, kedy je hodnota potrebného výkonu blízka alebo prevyšuje hodnotu dodávaného výkonu meničom energie. Netreba zabúdať ani na fakt, že zberač energie nie je tvorený iba meničom napätia a MPPT kontrolérom, ale pozostáva ešte z ďalších nevyhnutných blokov, ktoré majú tiež istú spotrebu energie.

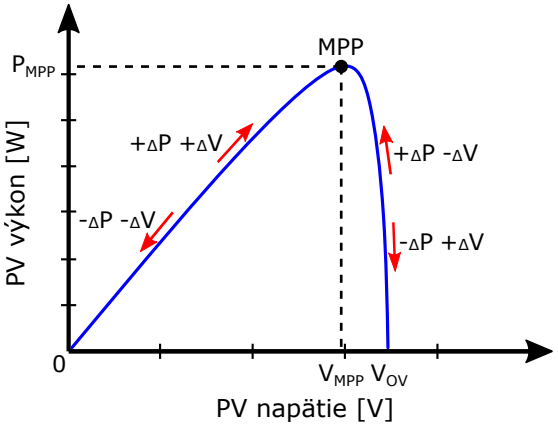
Spomenuté nežiadúce vlastnosti výrazne ovplyvňujú celkovú konverznú účinnosť zberača energie, a preto je nevyhnutné pri samotnom návrhu nájsť kompromis medzi typmi ladiacich metód určených ich zložitosťou a rýchlosťou.

III. Hľadanie bodu maximálneho výkonu

Hľadanie bodu, v ktorom je zberač energie naladený na maximálny prenos energie zo vstupu na jeho výstup, zabezpečuje synchrónny číslicový obvod – MPPT kontrolér. Ide o proces, v ktorom MPPT kontrolér na základe špecifikovaného algoritmu vyhodnotí vstupné dáta získané na meniči energie a následne vygeneruje vhodný riadiaci signál (PWM/PFM), ktorým je ovládaný napríklad výkonový tranzistor v DC-DC meniči regulujúci jeho výstupné napätie [4], [5], [6].

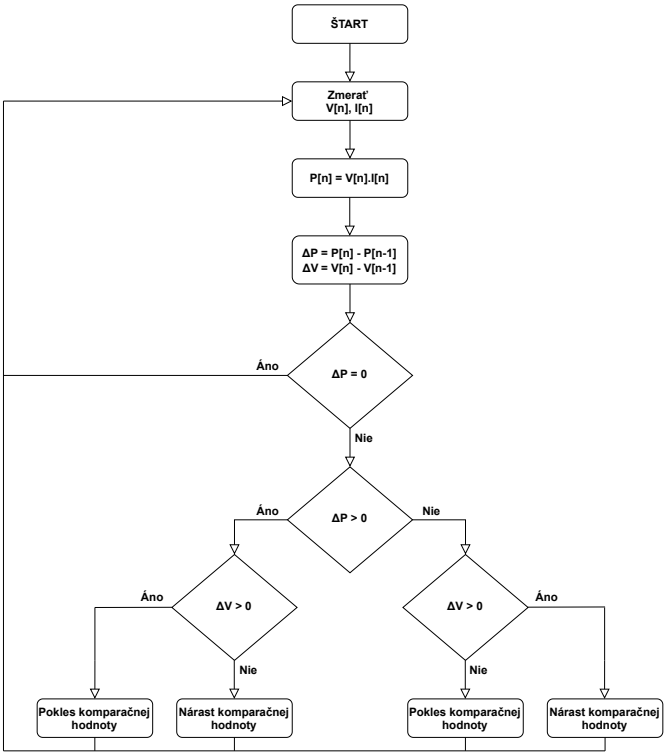
Pre náš návrh a analýzu spotreby elektrickej energie číslicového obvodu sme si zvolili ako zdroj energie slnečnú energiu a vybrali najčastejšie využívanú priamu metódu hľadania bodu maximálneho výkonu "Naruš a pozoruj"[7], [8]. Podstatou tohto algoritmu je riadenie prenosu energie zberačom energie zo vstupu na jeho výstup na základe informácie o vstupnom výkone. To znamená, že je potrebné merať veličiny ako sú napätie a prúd na meniči energie. Pre tento typ algoritmu nie sú podstatné hodnoty vstupných veličín s absolútnou presnosťou, pretože algoritmus vyhodnocuje veľkosť zmeny týchto veličín v aktuálnom kroku voči predošlým krokom merania. Tento fakt je pre analógového návrhára dôležitý, pretože môže viesť napríklad k návrhu menej zložitých analógovo-číslicových prevodníkov, čo tiež pozitívne ovplyvňuje celkovú účinnosť zberača energie.

Samotný algoritmus si na svojom začiatku načíta hodnoty vstupného napätia a prúdu, a vynásobením týchto dvoch veličín získa informáciu o vstupnom výkone v aktuálnom kroku. V nasledujúcej fáze algoritmu dochádza k zisťovaniu veľkosti zmien výkonu a napätia na vstupe. Ak je zmena výkonu nulová, zberač energie je naladený na maximálny prenos energie. V opačnom prípade je nutné vykonať aj vyhodnotenie podmienky pre veľkosť zmeny vstupného napätia. Vyhodnotené podmienky určia relatívnu pozíciu výkonového bodu na výkonovej krivke solárneho článku a smer posunu tohto bodu k bodu maximálneho výkonu (MPP). Pre lepšiu predstavu posunu výkonového bodu po krivke k MPP je tento proces naznačený na Obr. 2.



Obrázok 2. Smer procesu hľadania MPP metódou "Naruš a pozoruj".

Postupnosť krokov, vyhodnotenie podmienok a spôsob regulácie algoritmom "Naruš a pozoruj"je popísané pomocou vývojového diagramu zobrazeného na Obr. 3.



Obrázok 3. Vývojový diagram algoritmu „Naruš a pozoruj".

IV. Analýza spotreby MPPT kontroléra

MPPT kontrolér je sekvenčný synchrónny číslicový obvod, ktorý k svojej funkcii potrebuje hodinový signál. Jeho spotreba nie je zanedbateľná najmä pri zberačoch energie s nízkou hustotou zberanej energie, a preto je nevyhnutné obvod optimalizovať vzhľadom na spotrebu. Tá sa pri číslicových obvodoch skladá zo statickej a dynamickej zložky ako to vyjadruje aj vzťah (1).

$$P = P_s + P_d \tag{1}$$

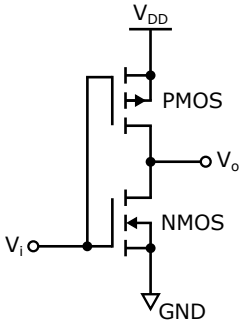
Veľkosť statickej spotreby P_s je najviac ovplyvňovaná počtom hradiel, multiplexorov a preklápacích obvodov, z ktorých sa daný obvod skladá. V štandardných podmienkach, akými sú typický podmienky výrobného procesu TT a izbová teplota 27 °C, má oveľa väčší príspevok k celkovej spotrebe práve dynamická spotreba P_d. Tá je daná nasledujúcim vzťahom:

$$P_d = \alpha C_L V^2 f_{clk}, \tag{2}$$

kde C_L je záťažová kapacita, V je napájacie napätie a f_{clk} reprezentuje pracovnú frekvenciu hodinového signálu. Tieto parametre sú vo veľkej väčšine prípadov statické, ktoré nie je možné dynamicky meniť. Koeficient α vyjadruje pravdepodobnosť zmeny logického stavu daného uzla z *Log 1* do *Log 0* alebo opačne. V prípade samotného CMOS invertora, zloženého z PMOS a NMOS tranzistora, invertujúceho vstupný

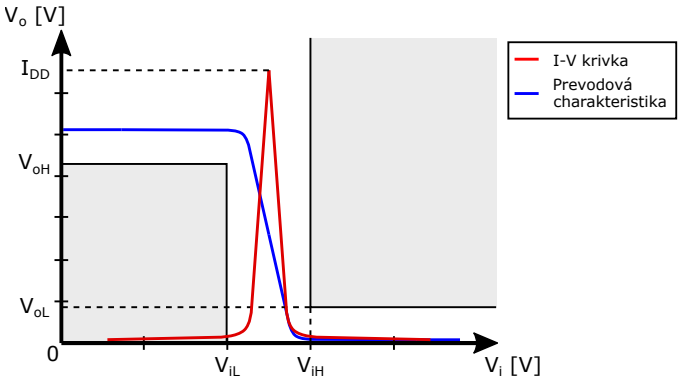
hodinový signál, je táto pravdepodobnosť $0,5$ [9], ale inak je vždy funkciou systému.

Pri CMOS logických obvodoch dominuje z hľadiska spotreby fakt, že aspoň jeden typ tranzistora je vždy zatvorený, čo demonštruje aj invertor na Obr. 4. Privedením *Log 1* na vstup dochádza k zatvoreniu PMOS tranzistora a zároveň k otvoreniu NMOS tranzistora, cez ktorý sa na výstup dostane najnižší potenciál, teda *Log 0*. V opačnom prípade vstupnej hodnoty bude na výstupe hodnota *Log 1* privedená cez otvorený PMOS tranzistor. V ani jednom z prípadov nie sú vodivo prepojené najvyšší a najnižší potenciál, takže spotreba je tvorená iba statickou zložkou, ktorá je veľmi blízka nule. Kritický je však



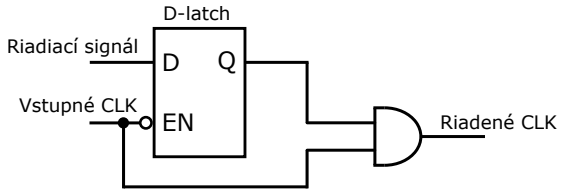
Obrázok 4. CMOS invertor na tranzistorovej úrovni.

prechodový stav prevodovej charakteristiky CMOS invertora, kedy v jednom momente sú oba typy tranzistorov otvorené a je vytvorený vodivý kanál medzi napájaním V_{DD} a zemou GND [10]. Spotreba invertora je v tomto prechodovom stave najvyššia a ním krátkodobo tečie skratový prúd, čo je možné vidieť aj na obr. 5.



Obrázok 5. Prevodová a I-V charakteristika logického invertora.

Z I-V krivky na obr. 5 vyplýva, že pre zníženie dynamickej spotreby P_d je potrebné zamedziť nadmernému a hlavne zbytočnému prepínaniu logických úrovni. V prípade sekvenčných obvodov obsahujúcich preklápacie obvody, je nevyhnutné prijať opatrenia na zamedzenie nadbytočnej aktivity. Vo všeobecnosti je to vykonávané riadiacím signálom, ktorý bráni prístupu hodinového signálu do preklápacieho obvodu. Najdominantnejšou technikou pre riadenie distribúcie hodinového signálu do preklápacieho obvodu je tzv. hradlovanie hodinového signálu (angl. Clock Gating)[11]. Princíp zapojenia hradlovania hodinového signálu môžeme vidieť na Obr 6. Táto technika zamedzuje nadbytočným a nechceným hodinovým pulzom (zápisom) do registrovej banky, kedy nedochádza k žiadnej zmene vstupných dát.



Obrázok 6. Hradlová schéma obvodu riadenia hodín.

V. Dosiahnuté výsledky simulácií

Digitálny obvod MPPT kontroléra bol navrhnutý na vyššej úrovni abstrakcie (RTL úrovni) pomocou opisného jazyka Verilog. Bol syntetizovaný do 130 nm CMOS technológie a prešiel aj procesom P&R s použitím nástroja Cadence. Časové kritéria syntézy sú uvedené v tabuľke I:

Tabuľka I
Parametre syntézy.

Parameter	**Hodnota**
Perióda hodín [ns]	5
Doba nábežnej hrany [ps]	250
Doba dobežnej hrany [ps]	250
Neistota hodín (Jitter) [ps]	70

Navrhnutý digitálny obvod založený na základnom P&O algoritme pozostáva zo 750 štandardných buniek, ktoré zaberajú plochu čipu 10 964 μm^2. Kompletný dizajn obvodu bol následne importovaný do analógového prostredia z dôvodu dosiahnutia čo najpresnejších výsledkov simulácie. V rámci znižovania celkovej spotreby je najdominantnejším parametrom napájacie napätie V_{DD}, pretože s ním sa spotreba digitálneho obvodu mení kvadraticky, čo vyplýva aj zo vzťahu (2). Preto sme sa aj primárne zamerali na tento parameter a celkovú priemernú spotrebu sme vyšetrovali pri napájacom napätí $V_{DD} = 0,4\ V$ v rôznych okrajových podmienkach výrobného procesu a pri zmenách okolitej teploty. Kedže obvod bol pri $V_{DD} = 0,4\ V$ plne funkčný vo všetkých vyšetrovaných prípadoch, tak pri napájaní $V_{DD} = 1,2\ V$ sme spotrebu vyšetrovali pri rôznych teplotách, ale iba v typickom výrobnom procese. Výsledky dosiahnuté v rámci simulácií sú uvedené v tabuľke II.

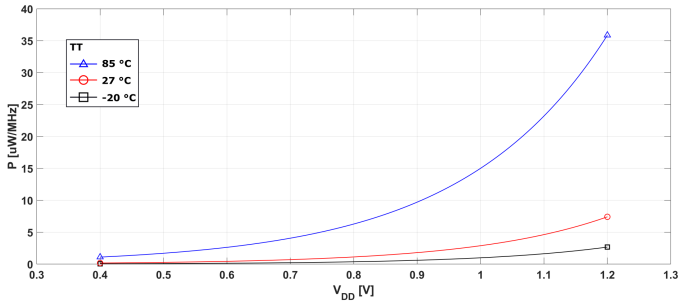
VI. Záver

V tomto príspevku bol predstavený číslicový obvod MPPT kontroléra, ktorý je dôležitou súčasťou zberačov energie. Pri tomto obvode sme vykonali analýzu jeho vlastnej spotreby energie. Všeobecnou analýzou digitálnych obvodov sme dospeli k niekoľkým spôsobom ako minimalizovať spotrebu

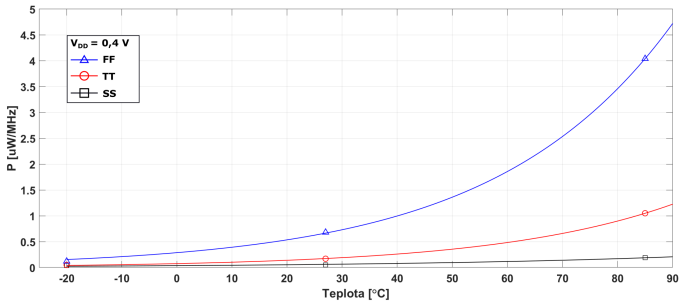
Tabuľka II
SPOTREBA ENERGIE MPPT KONTROLÉRA V OKRAJOVÝCH PODMIENKACH VÝROBNÉHO PROCESU A PRI RÔZNYCH TEPLOTÁCH.

P [μW/MHz]	V_{DD} = 1,2 V			V_{DD} = 0,4 V		
Proces	SS	TT	FF	SS	TT	FF
T = -20 °C	-	2,672	-	0,04	0,054	0,126
T = 27 °C	-	7,406	-	0,053	0,173	0,712
T = 85 °C	-	35,856	-	0,194	1,097	4,256

elektrickej energie obvodu. Ukázalo sa, že zníženie hodnoty napájacieho napätia V_{DD} je najefektívnejším spôsobom znižovania spotreby spomedzi vyššie spomenutých techník. Celková spotreba obvodu ($P_s + P_d$) bola simulovaná vo všetkých procesných a teplotných podmienkach pri $V_{DD} = 0,4\ V$ a $V_{DD} = 1,2\ V$. Výsledné priebehy simulácií je možné vidieť na Obr. 7 a Obr. 8. Znížením hodnoty napájania V_{DD} na



Obrázok 7. Spotreba energie v závislosti od veľkosti napájacieho napätia.



Obrázok 8. Spotreba energie v závislosti od okolitej teploty.

$0,4\ V$ v typických procesných a teplotných podmienkach sme sa dostali so spotrebou na hodnotu $P_{avg} = 0,173\ \mu W/MHz$, čo je takmer 43-násobné zníženie spotreby v porovnaní s prípadom napájania $V_{DD} = 1,2\ V$.

Hlavným zámerom dizertačnej práce je rozvoj metód hľadania maximálneho výkonu zberačov energie. Vyššie spomínané vyšetrovanie spotreby číslicových obvodov a osvojenie si redukčných techník spotreby sú neodmysliteľnou súčasťou tohto zámeru práce.

Ďalšie kroky budú viesť k samotnému vývoju ladiacich metód a optimalizácii s dôrazom na spotrebu, rýchlosť a presnosť. V súčasnosti je zberač energie často navrhovaný tak, aby bol schopný konvertovať energiu z viacerých zdrojov (druhov) energie. A práve tu, v oblasti riadenia/prepínania medzi jednotlivými algoritmami v závislosti od typu meniča energie v zberači alebo od fluktuácie vstupných podmienok, vidíme veľký priestor pre zlepšovanie.

V rámci mojej doterajšej doktorandskej práce a výskumu vznikli 2 publikácie, na ktorých som prvoautorom (oba príspevky boli publikované na medzinárodnej IEEE konferencii Applied Electronics v rokoch 2020 a 2021, ktorá je indexovaná v databáze Scopus).

POĎAKOVANIE

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja v vrámci projektu APVV 19-0392, a projektom VEGA 1/0760/21.

LITERATÚRA

[1] M. Alhawari, B. Mohammad, H. Saleh, and M. Ismail, *Energy harvesting for self-powered wearable devices*. Springer, 2018.
[2] J. E. Salazar-Duque, E. I. Ortiz-Rivera, and J. González-Llorente, "Modified perturb and observe mppt algorithm based on a narrow set of initial conditions," in *2016 IEEE ANDESCON*, 2016, pp. 1–4.
[3] C. M. F. Carvalho and N. F. S. V. Paulino, *CMOS indoor light energy harvesting system for wireless sensing applications*. Heidelberg: Springer, 2015, ISBN: 978-3-319-21616-4.
[4] N. Bizon, N. M. Tabatabaei, F. Blaabjerg, and E. Kurt, *Energy harvesting and energy efficiency*. Švajčiarsko: Springer, 2017, ISBN: 978-3-319-49874-4.
[5] T. J. Kazmierski and S. Beeby, *Energy harvesting systems*. New York: Springer, 2011, ISBN: 978-1-4419-7565-2.
[6] A. Mohapatra, B. Nayak, and C. Saiprakash, "Adaptive perturb observe mppt for pv system with experimental validation," in *2019 IEEE International Conference on Sustainable Energy Technologies and Systems (ICSETS)*, 2019, pp. 257–261.
[7] I. V. Banu, R. Beniugă, and M. Istrate, "Comparative analysis of the perturb-and-observe and incremental conductance mppt methods," in *2013 8TH INTERNATIONAL SYMPOSIUM ON ADVANCED TOPICS IN ELECTRICAL ENGINEERING (ATEE)*, 2013, pp. 1–4.
[8] M. A. Elgendy, B. Zahawi, and D. J. Atkinson, "Evaluation of perturb and observe mppt algorithm implementation techniques," in *6th IET International Conference on Power Electronics, Machines and Drives (PEMD 2012)*, 2012, pp. 1–6.
[9] Y. Zhang, X. Hu, X. Feng, Y. Hu, and X. Tang, "An analysis of power dissipation analysis and power dissipation optimization methods in digital chip layout design," in *2019 IEEE 19th International Conference on Communication Technology (ICCT)*, 2019, pp. 1468–1471.
[10] S. Nikolaidis, "Modeling cmos gates using equivalent inverters," in *2015 IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits Systems*, 2015, pp. 119–122.
[11] T. Chindhu S. and N. Shanmugasundaram, "Clock gating techniques: An overview," in *2018 Conference on Emerging Devices and Smart Systems (ICEDSS)*, 2018, pp. 217–221.

Rozvoj metód merania a vyhodnocovania parametrov prototypových ASIC čipov

Richard Ravasz
2. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

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

***Abstrakt*—Tento príspevok sa zaoberá návrhom komunikačného systému pre ladiacu logiku, ktorá slúži na ladenie parametrov plne diferenciálneho rozdielového zosilňovača (FDDA z angl. Fully Differential Difference Amplifier). Komunikačný systém bol otestovaný pomocou Field programmable gate array (FPGA) vývojovej dosky, kde bola implementovaná samotná ladiaca logika, ďalej mikrokontróler (MCU) slúžiaci ako prevodník komunikácie medzi počítačom a ladiacou logikou. Komunikačný prenos bol odchytávaný pomocou logického analyzátora. Komunikačný systém bude implementovaný na testovaciu dosku spolu s ladeným obvodom na čipe. Taktiež bolo navrhnuté užívateľské rozhranie, ktoré je ovládané pomocou počítača a výrazne zjednoduší a zefektívni ladenie parametrov pri meraní obvodov na spomínanom čipe. V závere príspevku sú stanovené ciele dizertačnej práce.**

***Kľúčové slová*—komunikačný systém, užívateľské rozhranie, ladiaca logika**

I. Úvod

Pri vývoji progresívnej elektroniky integrovanej na čipe sa kladie čoraz väčší dôraz na robustnosť takýchto systémov a na zmenšovanie rozmerov výsledného čipu. Taktiež sa takéto elektronické systémy stávajú súčasťou prenosných zariadení, kde sa kladie hlavný dôraz na spotrebu energie [1]. Avšak počas výrobného procesu môže dôjsť k odchýlkam jednotlivých parametrov obvodov čo môže negatívne ovplyvniť a degradovať funkčnosť celého integrovaného elektronického systému. Aby bola dosiahnutá požadovaná funkcia systému, zvyčajne je nevyhnutná kalibrácia vybraných parametrov [2]. Jednou z možnosti je použiť trimovaciu metódu, pri ktorej sa za pomoci prepálenia tavnej poistky doladia parametre systému. Takéto metódy sú však pre ladiaci systém deštruktívne a nedajú sa vrátiť späť [3]. Ďalšou metódou ladenia parametrov obvodov na čipe je použitie riadiacej logiky, ktorá pripája banku kondenzátorov alebo rezistorov a týmto spôsobom ladí vybrané parametre obvodu. Výhodou takéhoto riešenia je nedeštruktívnosť a opakovateľnosť ladiaceho procesu. Ďalšou výhodou takéhoto riešenia je možnosť ladenia parametrov pomocou počítač čo môže zabezpečiť možnosť vytvorenia automatizovaného meracieho pracoviska pre daný elektronický systém implementovaný s ladiacou logikou.

II. Motivácia

Vývoj integrovaného obvodu (angl. Integrated Circuit, IO) je zložitý proces, ktorý si vyžaduje nemálo znalostí a skúsenosti nielen z oblasti elektroniky, ale aj technológie výroby, aby bol dotiahnutý do úspešného konca. Tento proces by sme mohli rozdeliť do troch disciplín:

- Návrh
- Výroba
- Testovanie

Celý proces zrodu IO začína pri jeho návrhu. Úlohou návrhárov je zvolenie vhodnej topológie, podľa vopred dohodnutých požiadaviek od zákazníka a pretavenie jej do funkčnej schémy. Funkčnosť navrhnutého IO sa verifikuje pomocou numerických simulácií.

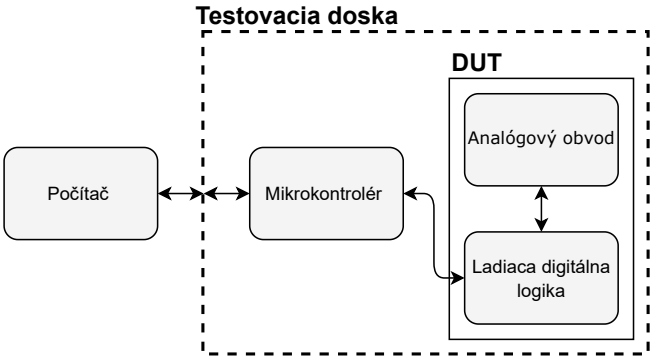
Výrobná činnosť sa týka predovšetkým transformácie navrhnutého IO do fyzickej podoby za pomoci výrobného procesu. Správne zvolený výrobný proces závisí od množstva faktorov vrátane výrobných nákladov, dostupnosti technológie ako aj skúsenosti so zvolenou technológiou. Poznáme mnoho používaných výrobných procesov, ale dominantnou technológiou už niekoľko desaťrocí je technológia CMOS (angl. Complementary Metal Oxide Semiconductor)[4].

Poslednou časťou, ktorú IO musí podstúpiť na svojej výrobnej ceste je testovanie. Až v tejto časti procesu sa ukáže, či navrhnutý IO skutočne spĺňa potrebné požiadavky. Je zrejmé, že v celom procese vývoja IO je nevyhnutná interakcia medzi návrhármi, výrobnou technológiou a testovacími inžiniermi. Mohlo by sa zdať, že pri dokonalom návrhu a dobre zvládnutom výrobnom procese je testovanie IO zbytočné. Pravda je však taká, že i najmenšia chyba pri návrhu alebo nedokonalosť vo výrobe môže spôsobiť disfunkčnosť celého obvodu. A práve preto je nevyhnutné navrhnutý IO podrobiť dôkladnému otestovaniu a overeniu jeho funkčnosti. [5].

Hlavnou motiváciou pri návrhu komunikačného systému pre ladiacu logiku na čipe ako aj pri vývoji grafického užívateľského rozhrania bolo zjednodušenie ovládania ladiacich digitálnych obvodov na čipe, čo výrazne zjednoduší proces testovania a merania prototypových IO.

III. Implementácia komunikačného systému

Navrhnutý komunikačný systém bol použitý pre komunikáciu s digitálnou logikou na čipe, ktorá bola navrhnutá na ladenie parametrov plne diferenciálneho rozdielového zosilňovača. Logika iintegrovaná na čipe zabezpečuje kalibráciu jednotlivých parametrov zosilňovača. Pomocou digitálnych registrov je možné ladiť jednotlivé parametre použitím implementovaného komunikačného protokolu. Digitálne registre je možné ladiť buď pasívne za pomoci tlačidiel alebo rotačných enkóderov, ktoré by boli implementované na testovacej doske. Lepší a efektívnejší spôsob kontroly ladiacich registrov, ktorému sme sa venovali aj my, je použitie počítača s navrhnutým grafickým prostredím. Blokovú schému riadiaceho systému je možné vidieť na Obr.1. Ako prevodník komunikácie medzi počítačom a ladiacou logikou na čipe sme použili mikrokontróler.



Obrázok 1. Bloková schéma riaidaceho systému

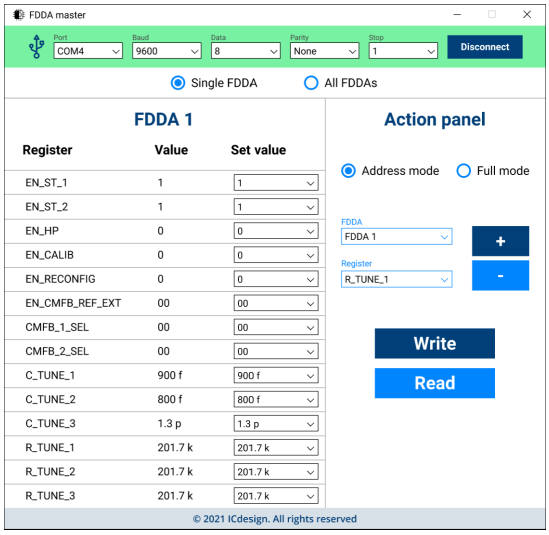
IV. Grafické rozhranie (GUI)

Pre jednoduchšiu ovládateľnosť všetkých 42 ladiacich registrov v digitálnej ladiacej logike na čipe sme navrhli grafické užívateľské rozhranie zobrazené na Obr.2 pomocou programovacieho jazyku Python použitím ThInter knižnice. Grafické rozhranie je rozdelené do troch panelov:

- Komunikačný panel
- Panel s registrami
- Akčný panel

A. Komunikačný panel

Dátovú komunikáciu medzi počítačom a prevodníkom sme zabezpečili pomocou štandardného komunikačného protokolu Universal Asynchronous Receiver-Transmitter (UART) [6]. Pre správne nadviazanie komunikácie je nevyhnutné nastaviť potrebné komunikačné parametre, ktoré tento komunikačný protokol vyžaduje. Ide o tieto parametre: **komunikačný port**, **rýchlosť komunikácie (Baud rate)**, **dátová šírka slova**, **parita** a **počet stop bitov**. Všetky tieto parametre si vieme navoliť pomocou rozbaľovacieho zoznamu (angl. combo box). Po správne nakonfigurovaní komunikácie s požadovaným zariadením a kliknutí na modré tlačidlo pripojiť (*Connect*) je komunikácia spustená. Pomocou tlačidla odpojiť (*Diccon-nect*) komunikáciu prerušíme. Farba pozadia v komunikačnom paneli znázorňuje stav komunikácie. Po pripojení je farba



Obrázok 2. Grafické rozhranie

pozadia komunikačného panelu zelená (Obr. 3) a po odpojení komunikácie je farba pozadia komunikačného panelu červená (Obr. 4).

Obrázok 3. Pripojená komunikácia

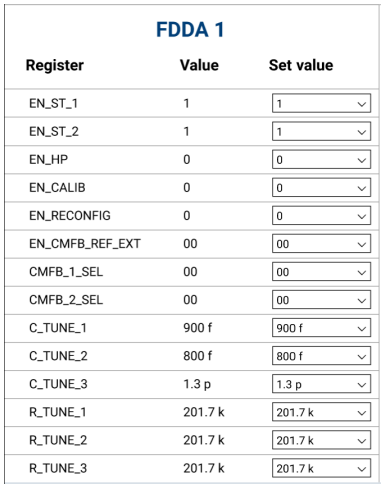
Obrázok 4. Odpojená komunikácia

B. Panel s registrami

Ladiť parametre a kontrolovať hodnoty v registroch ladiacej digitálnej logiky vieme pomocou Panelu s registrami (Obr. 5). Tento panel je rozdelený do troch stĺpcov. Prvý stĺpec pod názvom **Register** znázorňuje názov ladeného parametra. Druhý stĺpec pod názvom **Value** znázorňuje aktuálnu hodnotu príslušného registra. Hodnoty v registroch sa neaktualizujú automaticky. Pre aktualizáciu hodnôt v jednotlivých ladiacich registroch je potrebné vyčítať hodnoty z registrov ladiacej logiky na čipe. Tretí stĺpec nazvaný **Set value** znázorňuje hodnotu, ktorú chceme zapísať do príslušného registra. V hornej časti panela na nachádza názov (FDDA1) určujúci ktorý typ FDDA obvodu ladíme. Keďže na testovanom čipe sa nachádzajú 3 verzie obvodu FDDA, vieme buď každému FDDA ladiť parametre samostane alebo všetkým trom FDDA naraz jednou konfiguráciou. Takúto možnosť si navolíme pod komunikačným panelom označením **Single FDDA** pre ladenie jednotlivých FDDA samostatne alebo **All FDDAs** pre ladenie parametrov všetkých FDDA súčasne.

C. Action panel

Zápis a vyčítavanie dát z ladiacich registrov je zabezpečené pomocou tzv. Akčného panelu (Obr. 6). V hornej časti tohto



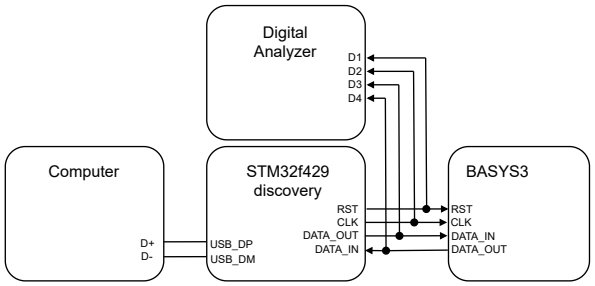
Obrázok 5. Panel s registrami

panelu sa nachádzajú dve možnosti konfigurácie zápisu a čítania dát. Ak použijeme možnosť **Address mode**, vieme zapisovať alebo vyčítavať dáta z jednotlivých ladiacich registrov samostane. Pri použití možnosti **Full mode** vieme zapisovať alebo vyčítavať dáta súčasne zo všetkých ladiacich registrov. V akčnom paneli si taktiež vieme nastaviť, ktorý FDDA obvod chceme konfigurovať. Po nastavení požadovanej konfigurácie sa po stlačení tlačidla *Write* dáta zapíšu do registrov. Pre vyčítavanie dát je potrebné kliknúť na tlačidlo *Read*.

Obrázok 6. Akčný panel

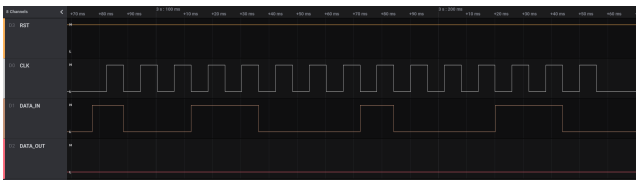
V. Verifikácia komunikačného systému

Experimentálnu verifikáciu komunikačného systému sme realizovali pomocou vývojových dosiek BASYS3 a STM32F429 DISCOVERY. Bloková schéma zapojeného systému je znázornená na Obr. 7. Dátový tok medzi MCU a FPGA sme zachytávali pomocou 8-kanálového logického analyzátora so vzorkovacou frekvenciou 24 MHz. Ladiaca logika je citlivá na nábežnú hranu hodinového signálu a inicializovaná na počiatočnú hodnotu po synchrónnom resete, ktorý je aktívny v logickej nule.



Obrázok 7. Bloková schéma verifikovaného systému

Zachytená komunikácia počas posielania dát do ladiacej logiky na čipe je zobrazená na Obr. 8. V prvom riadku označenom ako **RST** je zobrazený priebeh synchrónneho resetu, ktorý sa nachádza v logickej jednotke. V druhom riadku označenom ako **CLK** môžeme pozorovať priebeh hodinového signálu, ktorý je distribuovaný do všetkých synchrónnych častí ladiacich obvodov tohto integrovaného systému. V treťom riadku označenom ako **DATA_IN** je zobrazený priebeh dát zapisovaných do registrov ladiaceho systému, ktorý nesie informáciu do ktorého registra sa hodnota zapíše ako aj veľkosť samotnej hodnoty. Vo štvrtom riadku označenom ako **DATA_OUT** je zobrazený celý priebeh v logickej nule, nakoľko zápis a čítanie dát nie je možné realizovať súčasne.

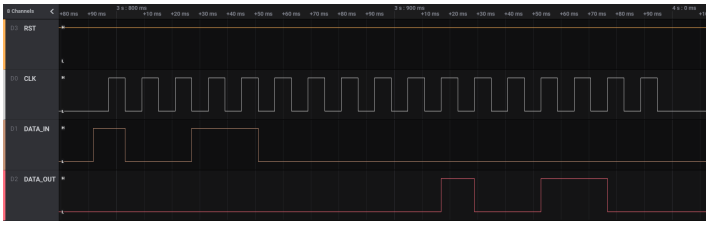


Obrázok 8. Príklad dát posielaných do ladiacej logiky

Zachytená komunikácia pri posielaní dát do ladiacej digitálnej časti na čipe je zobrazená na Obr. 9. Ako si môžeme všimnúť, signály **RST** a **CLK** majú rovnaký priebeh ako pri posielaní dát do čipu. V riadku označenom ako **DATA_IN** si môžeme všimnúť poslané dáta do ladiacich registrov, ktoré nesú príkaz na vyčítanie dát z daného registra a hodnotu vyčítavaného registra. V štvrtom riadku označenom ako **DATA_OUT** si môžeme všimnúť dáta vyčítavané zo zvoleného registra. Vyčítane dáta sa zobrazia v paneli s registrami.

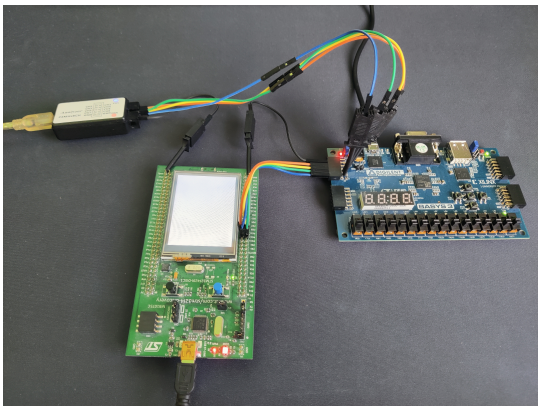
VI. Záver

V rámci dizertačnej práce sme sa v prvom roku zaoberali návrhom a praktickou realizáciou kontrolného systému pre ladiaci digitálny systém implementovaný na čipe. Pre zjednodušenie konfigurácie a samotnej práce s ladiacim systémom sme navrhli grafické rozhranie. Vopred navrhnutý ladiaci systém sme implementovali do FPGA BASYS3 vývojovej dosky, ktorá nám poslúžila ako náhrada za čip. Ako prevodník komunikácie medzi počítačom a BASYS3 sme použili vývojovú



Obrázok 9. Dáta prijaté z ladiacej logiky na čipe

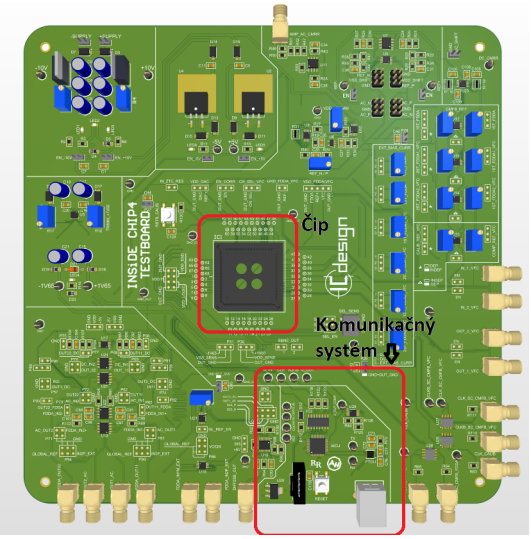
dosku STM32F4 Discovery, pričom sme použili na komunikáciu medzi ladiacou logikou a počítačom komunikačny protokol postavený na metóde *Bit Banging*. Fotka zapojenia pri praktickej verifikácii ladiaceho systému je zobrazená na Obr. 10. Podľa získaných výsledkov môžeme povedať, že navrhnutý komunikačný systém pre ladiacu logiku na čipe funguje správne a bude použitý pri testovaní analógových integrovaných obvodov vyvíjaných na Ústave elektroniky a fotoniky. Počas práce na komunikačnom systéme sme navrhli testovaciu dosku, na ktorej bol náš komunikačný systém implementovaný Obr. 11. Blokovú schému komunikačného systému implementovaného na testovacej doske môžeme vidieť na Obr. 12. Ako prevodník USB na UART sme použili FT234XD. Pre galvanické oddelenie čipu s digitálnou ladiacou elektronikou a mikrokontrólera sme použili optočlen.



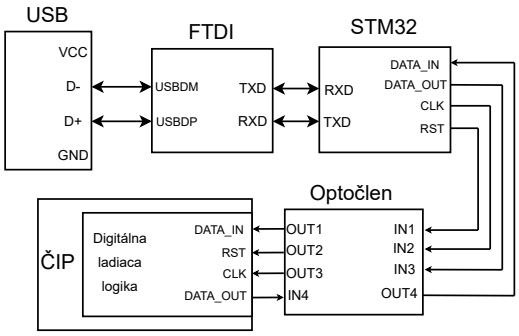
Obrázok 10. Zapojenie verifikovaného systému

VII. Ciele dizertačnej práce

Hlavným zámerom mojej dizertačnej práce je rozvíjať existujúce a vyvíjať nové metódy merania a verifikácie prototypových ASIC z hľadiska zlepšenia efektívnosti merania navrhnutých čipov. Chceme sa zamerať prevažne na návrh metód merania vybraných parametrov analógových IO s ultra nízkou hodnotou napájacieho napätia (pod 1 V), kde vznikla aktuálna potreba vývoja metód na overovanie vyrábaných prototypov. Nasledujúcou dielčou úlohou mojej dizertačnej práce je navrhnúť vhodný spôsob merania prudú na výstupe DC-DC meniča na báze flyback topológie. Pre túto úlohu bude dôležitá analýza dostupných priamych i nepriamych metód merania prúdu, a následná voľba optimálnej metódy. Jednou z nepriamych metód, ktorou sa aktuálne zaoberáme je určenie



Obrázok 11. Navrhnutá testovacia doska



Obrázok 12. Bloková schéma kontrolného systému implementovaného na testovacej doske

hodnoty odoberaného prúdu z konvertora podľa strmosti výstupného napäťového priebehu. Hodnotou výstupneho prúdu bude riadený ovládač samotného napäťového meniča.

VIII. Poďakovanie

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja v vrámci projektu APVV 19-0392, a projektom VEGA 1/0760/21.

Literatúra

[1] M. Alhawari, B. Mohammad, H. Saleh, and M. Ismail, *Energy harvesting for self-powered wearable devices*. Springer, 2018.

[2] M. Šovčík, V. Stopjaková, D. Arbet, M. Kováč, and M. Potočný, "Adverse effects of digital calibration hardware on low-voltage operational amplifiers," in *2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA)*. IEEE, 2018, pp. 1–4.

[3] M. Alafogianni, R. Penlington, and M. Birkett, "Resistor trimming geometry; past, present and future," in *IOP Conference Series: Materials Science and Engineering*, vol. 104, no. 1. IOP Publishing, 2016, p. 012002.

[4] B. a. Razavi, *Design of analog CMOS integrated circuits*. McGraw-Hill, 2001.

[5] I. A. Grout, *Integrated circuit test engineering: modern techniques*. Springer Science & Business Media, 2005.

[6] A. Gupta, *The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things*. Apress, 2019.

Koncept autokalibrácie analógových IO za účelom potlačenia vplyvu okrajových podmienok technológie

David Maljar
2. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

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

***Abstrakt*—Táto práca sa vo svojej podstate zaoberá technikou digitálnej autokalibrácie analógového integrovaného obvodu (IO), konkrétne napäťovej referencie. Článok opisuje všeobecný zmysel a účel kalibrovania IO, na základe ktorého poukazuje na potenciál práve digitálnej kalibrácie. Predstavuje aplikovateľný koncept digitálne autokalibrovanej napäťovej referencie s hodnotou výstupného napätia $96\ mV$, ktorej presnosť závisí najmä od fluktuácie parametrov jednotlivých tranzistorov, ktorá je spôsobená rozptylom výrobného procesu. V rámci predstaveného konceptu je v práci uvedený konkrétny princíp autokalibrovania, ktorého účelom je potlačiť vplyv okrajových podmienok technológie.**

***Kľúčové slová*—digitálna autokalibrácia, fluktuácia parametrov, analýza okrajových podmienok, napäťová referencia, nízkonapäťové obvody**

I. Úvod

Na základe zvyšovania štandardu technologických možností dnešnej doby sa pre ďalší vývoj a výrobu IO determinovali dve základné požiadavky: zvyšovanie výpočtového výkonu a znižovanie spotreby energie. Vďaka pokroku technologického procesu výroby je možné tieto požiadavky spĺňať súčasne. IO sú vyrábané so stále vyššou mierou hustoty integrácie a komplexnosti, čo je zatiaľ v súlade s Moorovým zákonom [1]. Najmenšia doteraz používaná dĺžka hradla tranzistora ($5\ nm$) poskytuje priamy dôkaz tohto pokroku [2].

Technologický proces výroby však nie je ideálny a do IO vnáša isté percento nepresností. To sa prejaví fluktuáciou parametrov obvodových elementov a môže spôsobiť zmenu požadovaných parametrov IO. Medzi fluktuované parametre obvodových elementov patria napríklad hrúbka hradlového oxidu, koncentrácia dopácie polovodiča, geometria obvodových elementov alebo hrúbka izolačnej vrstvy. Dôsledkom tohto vplyvu môžu byť aj parazitné vlastnosti vodivých prepojení: paratizný odpor a parazitná kapacita.

Spomínaná minimálna dĺžka hradla tranzistora sa samozrejme týka využitia v digitálnych IO. Výlučne digitálne IO (bez analógových častí) vo všeobecnosti nie sú tak citlivé na fluktuáciu parametrov spôsobenú technologickým procesom. Táto skutočnosť je zapríčinená najmä povahou digitálnych IO, ktorá spočíva v definovaných úrovniach logickej nuly a logickej jednotky. Keďže definícia jednotlivých logických úrovní zahŕňa celý interval spojitých napäťových hodnôt, tieto obvody dokážu pracovať veľmi spoľahlivo aj pri nízkych hodnotách napájacieho napätia, pričom bývajú vyrábané s veľmi vysokou robustnosťou.

Na druhej strane, analógové a zmiešané IO sú extrémne citlivé ako na nízke hodnoty napájacieho napätia, tak aj na fluktuáciu parametrov spôsobenú výrobným procesom. Existujú motodiky pre návrh analógových IO umožňujúce ich nízkonapäťový návrh prostredníctvom umiestnenia režimu činnosti tranzistorov do tzv. slabej inverzie. Medzi tieto prístupy k návrhu patrí tzv. g_m/I_D metodika a metodika *riadenia tranzistora substrátovou elektródou* (z angl. - *bulk-driven*). Metodika g_m/I_D poukazuje na hodnotu pomeru prenosovej vodivosti g_m a prúdu tečúceho cez tranzistor I_D, ktorý je smerodajným údajom pre stanovenie operačného bodu tranzistora. Riadenie tranzistora substrátovou elektródou priamo ovplyvňuje prahové napätie V_{TH}, čo umožňuje jeho zníženie a zároveň zvýšenie napäťového rozsahu užitočného signálu. Nevýhodou tejto metodiky je zníženie prenosovej vodivosti, ktorá predstavuje približne len 10% pôvodnej hodnoty g_m. Pre potlačenie vplyvu výrobného procesu bývajú používané sofistikované techniky ukladania obvodových elementov na čip, tzv. *layout*.

II. Motivácia

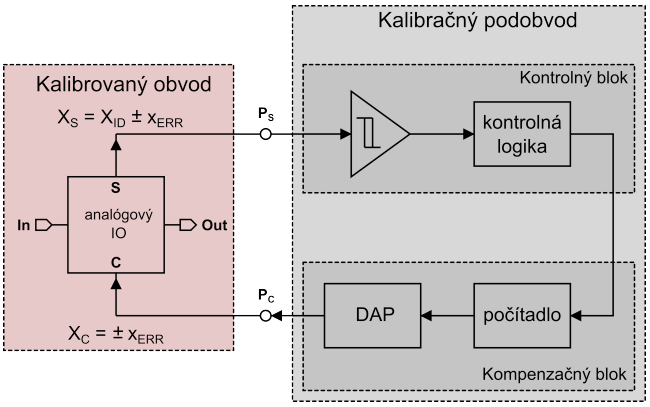
Technika layout-u býva v tomto zmysle kľúčovým činiteľom aby analógový IO mohol byť čo najviac odolný voči nežiaducim dôsledkom výrobného procesu. Vplyv týchto techník však nachádza svoje hranice po ukončení výrobného procesu. Z tohto dôvodu je vhodné túto problematiku riešiť doplnkovými *kalibračnými obvodmi*, ktoré sa v rámci možností s týmito dôsledkami vysporiadajú a konkrétne degradované parametre do značnej miery vykompenzujú. Primárnymi požiadavkami na kalibračné obvody sú ich vysoká odolnosť voči fluktuácii parametrov IO spôsobenej výrobným procesom, nezaťažovanie samotného kalibrovaného analógového IO, čo najnižšia možná spotreba a malá plocha na čipe. Vhodným prístupom k návrhu kalibračných obvodov je prispôsobenie ich všeobecného teoretického konceptu na konkrétnu aplikáciu, čo znamená využitie rôznych techník a metodík návrhu (konvenčných alebo

nekonvenčných). Na základe vyššie uvedených požiadaviek na kalibračné obvody je oproti ostatným technikám [3] práve digitálna kalibrácia tá, ktorá návrhárom otvára brány pre nové možnosti. Práve na základe digitálnej povahy takéhoto obvodu tento nezaťažuje hlavný analógový IO, je extrémne spoľahlivý, rýchly, no najmä vysoko odolný voči spomínanému rozptylu technologických parametrov. Pravdou je, že potrebuje svoje miesto na čipe, no v relatívnom ponímaní s prihliadnutím na jeho univerzálnosť je táto nevýhoda zanedbateľná.

V sekcii III je uvedený teoretický princíp digitálnej kalibrácie. Sekcia IV predstavuje koncept návrhu digitálne autokalibrovanej napäťovej referencie s napájacím napätím $1\ V$ a s výstupným napätím $96\ mV$, ktorej autokalibračný algoritmus pomáha potlačiť vplyv okrajových podmienok technológie.

III. Princíp digitálnej kalibrácie

Podstatou digitálnej kalibrácie je obvod, ktorý dokáže snímať a kompenzovať vybraný degradovaný parameter analógového IO. Na Obr. 1 je uvedený blokový diagram analógového IO s implementovaným digitálnym kalibračným podobvodom. Kalibrovaný obvod je ku kalibračnému podobvodu pripojený prostredníctvom snímacieho portu P_S a kompenzačného portu P_C. Dôležitým aspektom tohto zapojenia je, že oba porty musia byť schopné operovať s kalibrovaným parametrom bez vplyvu na funkčný chod kalibrovaného obvodu. Tieto porty je potrebné určiť veľmi precízne, čo však vo väčšine prípadov nie je možné. Z tohto dôvodu je potrebné už pri návrhu uvažovať nad tým, či bude analógový IO digitálne kalibrovaný a jeho návrh prispôsobiť tomuto účelu.



Obrázok 1. Blokový diagram analógového IO s implementovaným digitálnym kalibračným podobvodom.

Kalibračný podobvod pozostáva z kontrolného a kompenzačného bloku. Kontrolný blok sníma aktuálnu zmenu kompenzovaného parametra, na základe ktorej riadi celý kalibračný proces. Snímaná veličina X_S je privedená na vstup komparátora a môže byť vyjadrená nasledovným vzťahom:

$$X_S = X_{ID} \pm x_{ERR}, \tag{1}$$

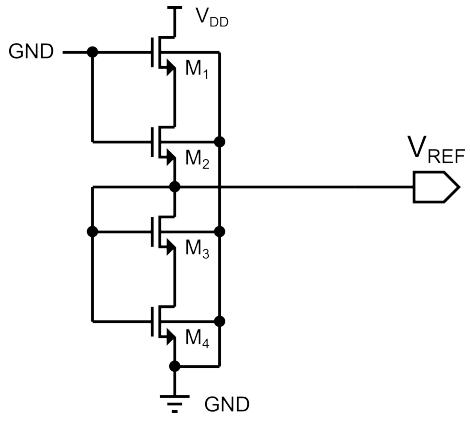
kde X_{ID} predstavuje ideálnu hodnotu kompenzovaného parametra a x_{err} je aktuálna odchýlka X_S od X_{ID}. Komparátor porovná hodnoty X_S a X_{ID}, pričom na základe tohto porovnania kontrolná logika aktivuje kompenzačný blok dovtedy, kým hodnota x_{err} nedosiahne hodnotu minimálneho rozlíšenia (resp. presnosti) - inými slovami, kým je komparátor schopný rozlíšiť hodnoty X_S a X_{ID}. Kompenzačný blok pozostáva z digitálno-analógového prevodníka DAP, ktorý je riadený počítadlom. Počítadlo je ovládané kontrolnou logikou, pričom generuje digitálny kód pre DAP. Výstup DAP je pripojený ku kompenzačnému portu P_C kalibrovaného obvodu a na tento port privádza kompenzovanú hodnotu daného parametra X_C. V celom tomto procese je extrémne dôležitá synchronizácia, pretože zvyšovanie hodnoty X_C musí spôsobovať znižovanie hodnoty x_{err}. V momente, keď x_{err} dosiahne pre komparátor nerozlíšiteľnú hodnotu x_{min}, hodnota kompenzovanej veličiny X_{S_COMP} môže byť vyjadrená vzťahom:

$$X_{S\_COMP} = X_{ID} \pm x_{min}. \tag{2}$$

Keď $x_{err} \cong x_{min}$, kontrolný blok zastaví celý kalibračný cyklus a na port P_C je dodávaná hodnota kompenzovaného parametra X_{S_COMP} a daný analógový IO je možné nazvať nakaliborvaným [3][4][5][6].

IV. Koncept autokalibrovanej napäťovej referencie

Na Obr. 2 je uvedená topológia napäťovej referencie s napájacím napätím $V_{DD} = 1\ V$. Oproti topológii uvedenej v [7] bol pridaný tranzistor M_2 z dôvodu vyššej absolútnej hodnoty parametra $PSRR$ a tranzistor M_4 z dôvodu dosiahnutia nižšej hodnoty teplotného koeficientu. Z hľadiska aplikácie uvedenej topológie bola požadovaná hodnota referenčného napätia $V_{REF} = 96\ mV$ s presnosťou $\pm 1\%$, pričom fluktuácia parametrov obvodových elementov spôsobená technologickým procesom výroby dosahuje odchýlky až $\pm 20\%$.

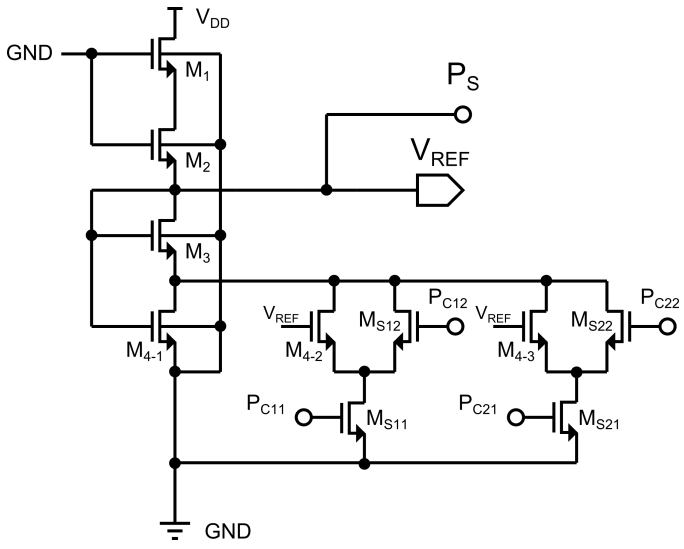


Obrázok 2. Topológia napäťovej referencie.

Požiadavkou na digitálnu kalibráciu bolo kompenzovať zmenu parametrov obvodových elementov prebiehajúcu rovnakým smerom. Táto zmena bola simulovaná prostredníctvom analýzy okrajových podmienok (z angl. *Corner analysis*). Keďže v tomto prípade ide o konkrétnu aplikáciu, na základe navrhovaného kalibračného algoritmu môžeme hovoriť o digitálnej autokalibrácii.

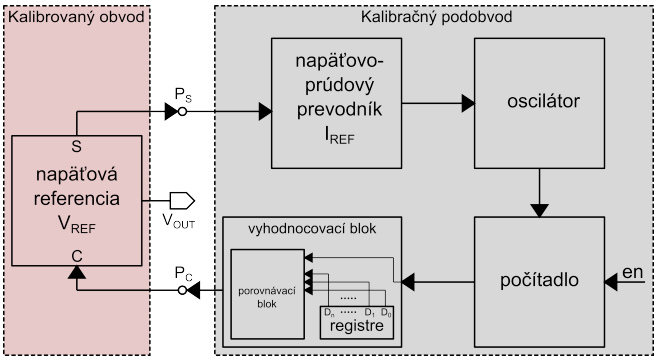
Hodnota prahového napätia tranzistora V_{TH} môže byť vplyvom technologického procesu posunutá do vyšších alebo nižších hodnôt. Pri vyšších (absolútnych) hodnotách prahového napätia reagujú tranzistory na zmeny elektrického signálu pomalšie (z angl. *slow*, ozn. *S*), pri nižších naopak reagujú rýchlejšie (z angl. *fast*, ozn. *F*). Nakoľko PMOS a NMOS tranzistory sa v obvodoch vyskytujú súčasne, okrajové podmienky nadobúdajú štyri kombinácie: FNMOS a FPMOS (FF), FNMOS a SPMOS (FS), SNMOS a FPMOS (SF), SNMOS a SPMOS (SS). V prípade správneho a relatívne presného technologického procesu výroby hovoríme o tzv. typickej podmienke s označením TT.

Veľkou výhodou topológie napäťovej referencie na Obr. 2 je, že pozostáva len z tranzistorov typu NMOS. V takomto prípade má zmysel hovoriť len o okrajových podmienkach, v ktorých sa vyskytuje iba NMOS (napríklad FF a SS) a o typickej podmienke TT. Keďže sme dopredu vedeli, že túto referenciu budeme kalibrovať technikou digitálnej kalibrácie, už počas návrhu obvodu referencie boli určené porty P_S a P_C. Port P_S je v tomto prípade v rovnakom uzle ako výstupný port V_{REF}, pretože z hľadiska kalibračného podobvodu energeticky nezaťažuje daný výstup. Pre vytvorenie portov P_C bol tranzistor M_4 rozdelený na tri časti, ktorých postupné pripájanie prostredníctvom kalibračného podobvodu kompenzuje podmienky v poradí FF, TT a SS. Takto upravený návrh napäťovej referencie je uvedený na Obr. 3.



Obrázok 3. Topológia napäťovej referencie v rámci autokalibrovaného konceptu.

Na Obr. 4 je uvedený koncept autokalibrovanej napäťovej referencie. V tomto štádiu práce sú zatiaľ všetky bloky kalibračného podobvodu uvažované ako ideálne. Princíp autokalibrácie vo všeobecnosti prebieha nasledovným spôsobom. Zo simulačnej analýzy vyplýva, že rozdiel medzi jednotlivými okrajovými podmienkami oproti podmienke TT je $\pm 5\ mV$ (uvedené v Tab. I). Pri zvýšení výstupného napätia V_{REF} dodá napäťovo-prúdový prevodník I_{REF} oscilátoru vyššiu hodnotu prúdu ako nominálnu, v dôsledku čoho oscilátor generuje vyššiu spínaciu frekvenciu pre počítadlo. Uvažovaním ideálneho časového intervalu počas pôsobenia signálu en, vyhodnocovací blok zaznamená hodnotu z počítadla, ktorá bola dosiahnutá v tomto časovom intervale. Túto hodnotu vyhodnocovací blok porovná s predvolenými hodnotami v registroch a na základe tohto porovnania do obvodu prostredníctvom portov P_C na spínačoch M_S pripojí buď tranzistor M_{4-2} alebo oba tranzistory M_{4-2} aj M_{4-3} alebo nepripojí ani M_{4-2} ani M_{4-3}.



Obrázok 4. Koncept autokalibrovanej napäťovej referencie.

Počiatočný stav napäťovej referencie je uložený do predpokladanej okrajovej podmienky FF. Znamená to, že porty P_{C11}, P_{C12}, P_{C21} a P_{C22} sú pred spustením kalibrácie vyhodnocovacím blokom pripojené na potenciály GND, V_{DD}, GND a V_{DD} (tranzistory M_{4-2} sú M_{4-3} sú odpojené). Pokiaľ bude v takomto prípade na výstupe požadovaný potenciál $\approx 96\ mV$, autokalibrácia prebehne s dôsledkom, že ani tranzistor M_{4-2} ani M_{4-3} do obvodu pripojené nebudú. Parametre napäťovej referencie uloženej do okrajovej podmienky FF sú znázornené v Tab. I. Spolu s analýzou okrajových podmienok bol simulovaný aj 10%-ný rozptyl napájacieho napätia V_{DD}. Tento rozptyl je pri každej podmienke označený indexom.

Tabulka I
VZÁJOMNÉ POROVNANIE PARAMETROV OBVODU S ODPOJENÝMI TRANZISTORMI M_{4-2} A M_{4-3}

	$I_{MAX}\ [A]$	$PSRR\ [dB]$	$TC[\frac{ppm}{°C}]$	$V_{REF}\ [V]$
$TT_{0.9\ V}$	3.196n	-43.39	115.9	100.4m
$TT_{1.0\ V}$	3.196n	-43.31	115.6	100.4m
$TT_{1.1\ V}$	3.196n	-43.26	115.4	100.4m
$\mathbf{FF_{0.9\ V}}$	10.2n	-42.62	118.8	95.46m
$\mathbf{FF_{1.0\ V}}$	10.2n	-42.56	118.7	95.46m
$\mathbf{FF_{1.1\ V}}$	10.2n	-42.53	118.6	95.46m
$SS_{0.9\ V}$	1.007n	-44.41	106.0	105.5m
$SS_{1.0\ V}$	1.007n	-44.30	104.9	105.5m
$SS_{1.1\ V}$	1.007n	-44.23	103.7	105.5m

V prípade počiatočnej hodnoty napätia $V_{REF} \approx 100\ mV$ sa obvod nachádza v typickej podmienke TT (uvedené v Tab. I) a vyhodnocovací blok do napäťovej referencie pripojí tranzistor M_{4-2}, čím napätie V_{REF} nakalibruje na hodnotu $\approx 96\ mV$. Parametre autokalibrovanej napäťovej referencie uloženej do typickej podmienky TT sú znázornené v Tab. II.

Tabulka II
VZÁJOMNÉ POROVNANIE PARAMETROV OBVODU S PRIPOJENÝM TRANZISTOROM M_{4-2}

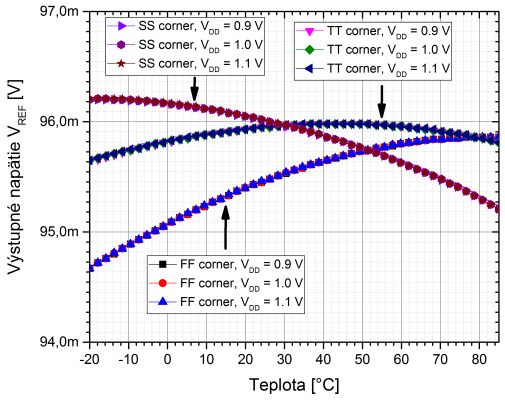
	I_{MAX} [A]	$PSRR$ [dB]	$TC[\frac{ppm}{°C}]$	V_{REF} [V]
$\mathbf{TT_{0.9\ V}}$	3.715n	-49.70	33.61	95.89
$\mathbf{TT_{1.0\ V}}$	3.715n	-49.62	33.41	95.89m
$\mathbf{TT_{1.1\ V}}$	3.716n	-49.57	33.20	95.89m

Ak je na počiatku hodnota referenčného napätia $V_{REF} \approx 105\ mV$, obvod sa nachádza v okrajovej podmienke SS (uvedené v Tab. I). V tomto prípade vyhodnocovací blok do obvodu napäťovej referencie pripojí oba tranzistory M_{4-2} aj M_{4-3}. Parametre kalibrovanej napäťovej referencie uloženej do okrajovej podmienky SS sú znázornené v Tab. III.

Tabulka III
VZÁJOMNÉ POROVNANIE PARAMETROV OBVODU S PRIPOJENÝMI TRANZISTORMI M_{4-2} A M_{4-3}

	I_{MAX} [A]	$PSRR$ [dB]	$TC[\frac{ppm}{°C}]$	V_{REF} [V]
$\mathbf{SS_{0.9\ V}}$	1.349n	-71.98	97.73	96.20m
$\mathbf{SS_{1.0\ V}}$	1.349n	-71.88	98.46	96.21m
$\mathbf{SS_{1.1\ V}}$	1.349n	-75.42	99.19	96.21m

Na Obr. 5 sú uvedené závislosti výstupného napätia V_{REF} od teploty v rozsahu od $-20°$C do $85°$C pre každý prípad okrajovej (resp. typickej) podmienky. Z týchto závislostí je možné pozorovať vysokú teplotnú stabilitu navrhovanej napäťovej referencie.



Obrázok 5. Závislosť napätia V_{REF} od teploty v podmienkach FF, TT a SS.

V. ZÁVER

V uvedenom príspevku bola predstavená digitálne autokalibrovaná napäťová referencia na konceptuálnej úrovni. Uvedené výsledky boli dosiahnuté prostredníctvom simulácií za účelom získania prvotných poznatkov pre ďalšiu prácu. Referencia po simulovaní kalibrácie veľmi spoľahlivo udržiava hodnotu referenčného napätia $V_{REF} = 96\ mV$ s presnosťou $\pm 1\%$. Okrem toho je možné konštatovať, že táto referencia je teplotne nezávislá nielen z hľadiska okrajovej (resp. typickej) podmienky, ale aj z hľadiska zmeny napájacieho napätia.

Ďalším stupňom tejto práce bude návrh samotných blokov uvedených v kalibračnom podobvode. Prvotné problémy môžu nastať už pri návrhu napäťovo-prúdového prevodníka, pretože rozdiel medzi jednotlivými okrajovými podmienkami oproti TT podmienke $\pm 5\ mV$ nemusí byť dostatočný na vyvolanie potrebnej zmeny prúdu. Riešením bude pridanie bloku, ktorý nebude zaťažovať snímací port P_S, no zároveň zmena jeho výstupu v závislosti od okrajových podmienok oproti TT podmienke bude rádovo vyššia, napríklad $\pm 50\ mV$. Očakávané sú taktiež ťažkosti s dosiahnutím požiadavky na veľmi vysokú presnosť týchto blokov, ktorá spočíva vo vysokej odolnosti voči fluktuácii parametrov technologického procesu výroby. Tu bude potrebné zabezpečiť, aby sa požadované operácie kalibračného podobvodu vykonávali na báze digitálnej logiky. V uvedenom algoritme tohto podobvodu je ukrytý vysoký potenciál, pretože ďalším cieľom tejto práce bude prostredníctvom neho vytvoriť tzv. univerzálny *corner detektor*. V takom prípade bude ďalším a vyšším cieľom tejto dizertačnej práce použitie NMOS aj PMOS tranzistorov a následná detekcia všetkých štyroch okrajových podmienok.

Prínos tejto práce ako komplexného celku spočíva v návrhu autokalibračného podobvodu, ktorý dokáže detegovať okrajovú podmienku po výrobe AIO a zároveň daný degradovaný parameter do istej miery kompenzovať. AIO sa totiž veľmi často pohybujú na hranici svojej funkcie v technológii, v ktorej sú vyrobené – kalibračné podobvody v tomto prípade dokážu značne zvýšiť ich spoľahlivosť.

POĎAKOVANIE

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja v vrámci projektu APVV 19-0392, a projektami VEGA 1/0760/21 a VEGA 1/0731/20.

LITERATÚRA

[1] R. R. Tummala, "Moore's law for packaging to replace moore's law for ics," in *2019 Pan Pacific Microelectronics Symposium (Pan Pacific)*, 2019, pp. 1–6.

[2] M.-S. Kim, N. Harada, Y. Kikuchi, J. Boemmels, J. Mitard, T. Huynh-Bao, P. Matagne, Z. Tao, W. Li, K. Devriendt, L.-A. Ragnarsson, C. Lorant, F. Sebaai, C. Porret, E. Rosseel, A. Dangol, D. Batuk, G. Martinez-Alanis, J. Geypen, N. Jourdan, A. Sepulveda, H. Puliyalil, G. Jamieson, M. van der Veen, L. Teugels, Z. El-Mekki, E. Altamirano-Sanchez, Y. Li, H. Nakamura, D. Mocuta, and F. Masuoka, "12-euv layer surrounding gate transistor (sgt) for vertical 6-t sram: 5-nm-class technology for ultra-density logic devices," in *2019 Symposium on VLSI Technology*, 2019, pp. T198–T199.

[3] M. Pastre and M. Kayal, *Methodology for the digital calibration of analog circuits and systems*. Springer, 2006.

[4] M. Šovčík, V. Stopjaková, D. Arbet, and M. Potočný, "Autonomous on-chip digital calibration for analog ics in nanotechnologies," in *2020 30th International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2020, pp. 1–5.

[5] M. Šovčík, V. Stopjaková, D. Arbet, and M. Kováč, "On-chip digital calibration of low-voltage analog ics in nanotechnologies," in *2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2019, pp. 733–738.

[6] M. Šovčík, V. Stopjaková, D. Arbet, M. Kováč, and M. Potočný, "Adverse effects of digital calibration hardware on low-voltage operational amplifiers," in *2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA)*, 2018, pp. 1–4.

[7] M. Seok, G. Kim, D. Blaauw, and D. Sylvester, "A portable 2-transistor picowatt temperature-compensated voltage reference operating at 0.5 v," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 10, pp. 2534–2545, 2012.

Návrh plne integrovaného 3-stupňového boost konvertora so spínanou cievkou

Róbert Ondica
2. ročník, denná prezenčná forma štúdia
Školiteľ: Viera Stopjaková

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

***Abstrakt*—Tento príspevok sa zaoberá návrhom DC-DC boost konvertora so všetkými pasívnymi súčiastkami a výkonovými spínačmi integrovanými na čipe. Pri návrhu štruktúry integrovanej cievky boli použité návrhové techniky zosumarizované v článku, pričom sme sa zamerali na zvýšenie faktora kvality. Medzi najlepšie dosiahnuté výsledky možno považovať indukčnosť $L = 10,91\ nH$, sériový odpor $R_{DC} = 2,71\ \Omega$ a faktor kvality $Q = 9,99\ nH$ pri frekvencii 630 MHz. Topológia konvertora je 3-stupňový boost konvertor (3LBC) a bola vybraná na základe výsledkov predošlého výskumu. Najvyššia dosiahnutá konverzná účinnosť je $\eta_{MAX} = 81,56\ \%$ pri spínacej frekvencii $f_{sw} = 20\ MHz$ a výstupnom výkone $P_{out} = 1,92\ mW$. Výsledky simulácií sú porovnané s výsledkami iných prác.**

***Kľúčové slová*—integrovaná cievka, DC-DC konvertor, nízkonapäťové obvody, 3LBC**

I. Úvod

Dnešný trh s elektronickými zariadeniami sa čoraz viac sústreďuje na mobilné zariadenia. Prenositeľnosť zariadení je veľmi úzko spojená s návrhom nízkonapäťových obvodov, čím sa výrazne mení spotreba energie, čas fungovania zariadenia na jedno nabitie alebo aj životnosť použitých batérií. Cieľom je rovnako aj zmenšovanie rozmerov a hmotnosti celých zariadení a teda aj obvodov nachádzajúcich sa v nich. Úplná integrácia obvodov je jedna z možností ako dosiahnuť všetky tieto ciele. Poslednou bežne používanou pasívnou súčiastkou, ktorej integrácia ešte nie je na takej úrovni ako integrácia odporu alebo kondenzátora je cievka. Jej integrácia je zriedkavá najmä v integrovaných obvodoch s nižšou pracovnou frekvenciou ($< 1\ GHz$), čo priamo súvisí s parametrami integrovanej cievky.

II. Motivácia

Motivácia tejto práce sa odvíja od potreby napäťového manažmentu v širokej škále obvodov, či už v integrovanej alebo diskrétnej forme. Požiadavka na zmenu úrovne napätia na zdroji na úroveň potrebnú pre správne fungovanie obvodu, alebo len jeho časti, stúpa najmä pri zariadeniach napájaných zo zdrojov energie ako sú napríklad batérie alebo zberače energie (EH z angl. Energy Harvester). Zaradenie napäťových meničov do návrhu celého elektronického systému je dnes bežnou praxou.

Práve problémom návrhu napäťového meniča sa zaoberá aj moja dizertačná práca. Pre obvod napájaný fotovoltickým (PV z angl. Photovoltaic) EH je nutné vytvoriť menič jednosmerného napätia, ktorý bude úroveň napätia zvyšovať. Jedná sa teda o DC-DC boost konvertor. Samotnú funkciu obvodu môžu spĺňať rôzne topológie, z ktorých každá bude vlastnosťami vhodnejšia pre inú konkrétnu aplikáciu. Celá topológia musí byť teda vhodná pre plnú integráciu na čip. Nami zvolená podmienka pre topológiu konvertora je implementácia princípu vysokofrekvenčného spínania jednej integrovanej cievky. Tento princíp je ideálne energeticky efektívnejší ako vysokofrekvenčné spínanie kondenzátorov [1]. Vhodne navrhnutá cievka je preto pre tento typ konvertora kritická.

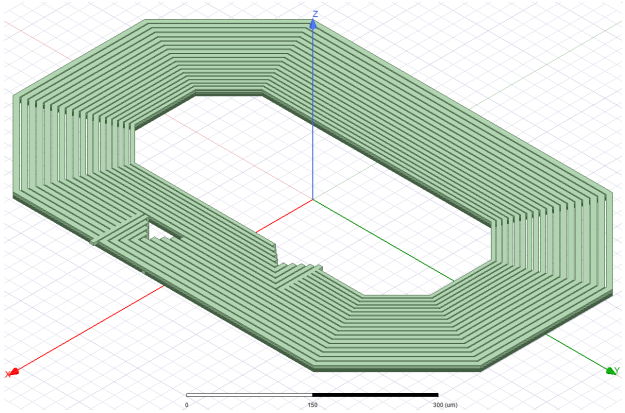
Nežiadúcich vplyvov v štruktúre integrovanej cievky je hneď niekoľko a sú spojené najmä s nízkou indukčnosťou cievky, spôsobenou malou dĺžkou vodiča tvoriaceho cievku a jeho pomerne vysokým odporom. S nízkou indukčnosťou tiež súvisí nutnosť použitia vysokej pracovnej frekvencie, čo ďalej zvyšuje sériový odpor cievky. Ďalšími parazitnými efektami, ktoré zvyšujú energetické straty v cievke sú napríklad vírivé prúdy, kapacitné väzby medzi cievkou a substrátom a medzi jednotlivými závitmi cievky [2]. Tieto nežiadúce vplyvy je možné čiastočne kompenzovať vhodným návrhom samotnej štruktúry cievky. Kapitola III opisuje štruktúru navrhnutej cievky spolu s jej frekvenčnými charakteristikami. Kapitola IV opisuje topológiu napäťového konvertora vybranú pre našu prácu. V časti V sú dosiahnuté výsledky porovnané s inými aktuálnymi prácami. Nakoniec sú v kapitole VI zhrnuté rámcové ciele dizertačnej práce.

III. Integrovaná cievka

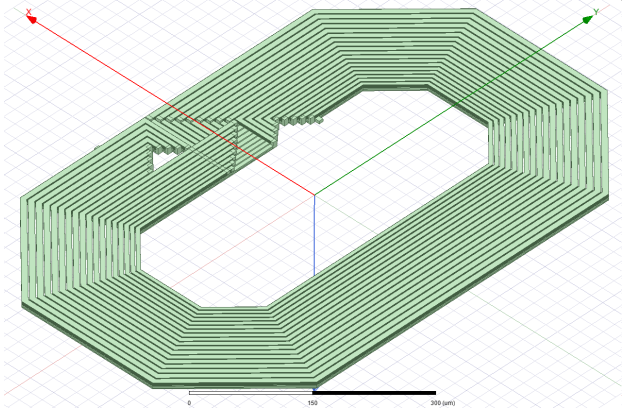
Návrhovými technikami sa snažíme zmeniť tvar cievky tak, aby sme čo najviac znížili vplyv parazitných javov a tak zlepšili požadované parametre. Takéto techniky spočívajú hlavne v rôznom smerovaní, rozdeľovaní a paralelizácii jednotlivých kovových vodivých ciest použitých pri vytváraní štruktúry integrovanej cievky. V tejto práci sme sa zaoberali nasledujúcimi technikami, použitím ktorých sa nám podarilo zlepšiť faktor kvality cievky a potlačiť jej sériový odpor:

- vertikálne paralelizovanie vodivých ciest [3],
- hotizontálne paralelizovanie vodivých ciest (Slicing) [3],

- škálovanie šírky vodivej cesty (Tappering) [4],
- metóda rovnakých dĺžok (EPL z angl. Equal Path Lengths) [5],
- štít pre odtienenie magnetického poľa cievky (PGS z angl. Patterned Ground Shield) [6].



Obrázok 1. Navrhnutá štruktúra integrovanej cievky: pohľad zvrchu

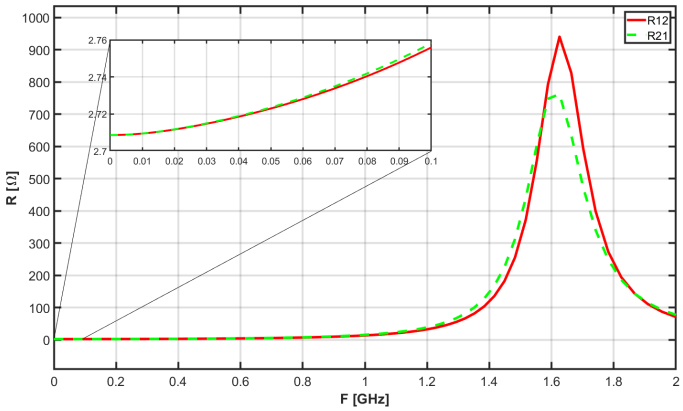


Obrázok 2. Navrhnutá štruktúra integrovanej cievky: pohľad zospodu

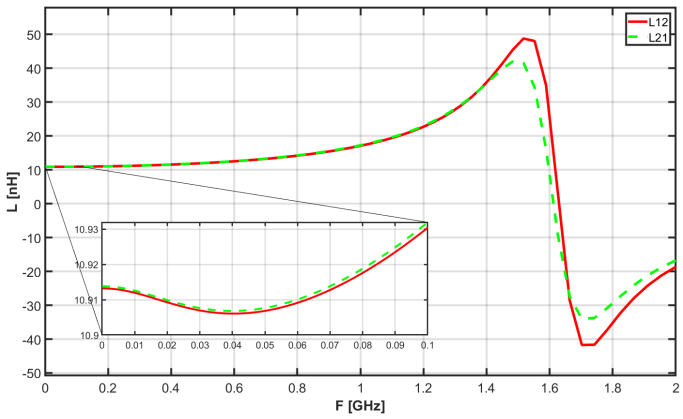
A. *Frekvenčné charakteristiky integrovanej cievky*

Použitím všetkých spomínaných návrhových techník bola vytvorená osemuholníková štvorzávitová (2 vnútorné a 2 vonkajšie závity nad sebou) nesymetrická cievka realizovaná v 7 kovových vrstvách (vertikálna paralelizácia), pri čom každý závit tvorí 9 paralelných vodičov (Slicing), ktoré sú v strede štruktúry prekrížené (EPL). Cievka má rozmery 800 μm x 510 μm a plochu 0,408 mm^2, pričom za účelom kompenzovania vyššej prúdovej hustoty na vonkajšom okraji štruktúry je šírka vonkajšieho závitu 9,8 μm a šírka vnútorného závitu je 5,2 μm (Tappering). Výsledná navrhnutá štruktúra je zobrazená na obrázkoch 1 a 2, a jej charakteristiky boli získané simuláciami v programe ANSYS Electronics Desktop pomocou nástroja ANSYS Electromagnetics Suite 2020 R2.

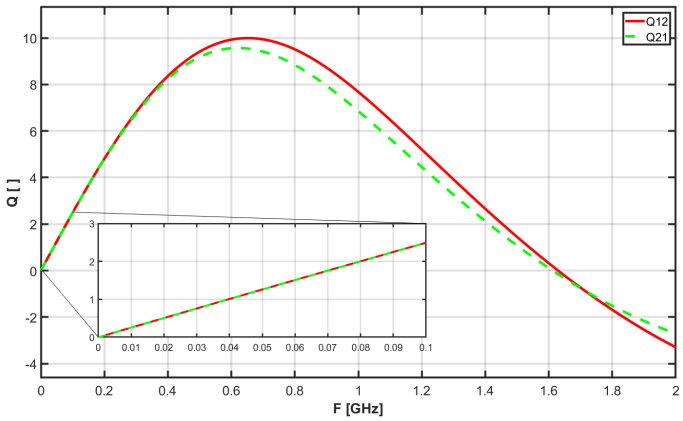
S touto štruktúrou sme dosiahli najvyššiu kvalitu $Q = 9,994$ na frekvencii $632,46$ MHz, indukčnosť $L = 10,913$ nH a sériový odpor $R_{DC} = 2,71$ Ω. Rezonančná frekvencia cievky bola $F_{SR} = 1,59$ GHz. Frekvenčné charakteristiky cievky sú zobrazené na obrázkoch 3, 4 a 5. Pri závislostiach kladieme dôraz na nižšie frekvencie ($<$ 100 MHz), v ktorých bude navrhovaný napäťový konvertor pravdepodobne využívaný.



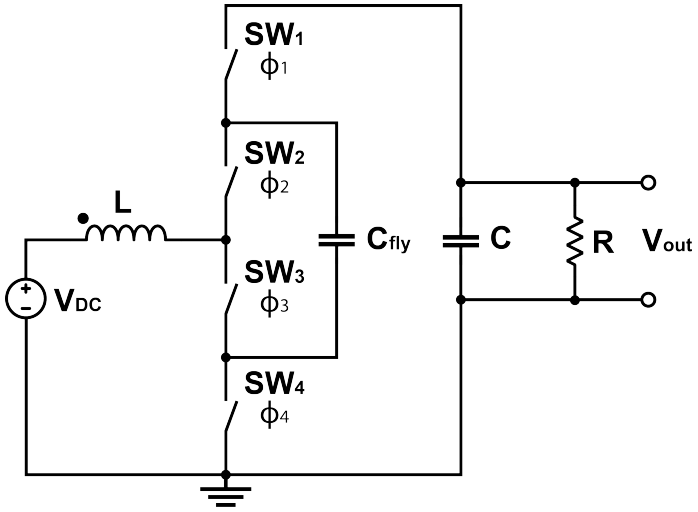
Obrázok 3. Závislosť sériového odporu integrovanej cievky od frekvencie



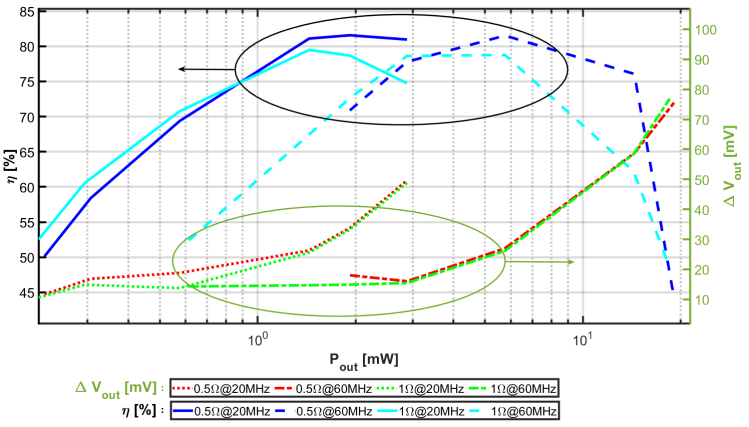
Obrázok 4. Závislosť indukčnosti integrovanej cievky od frekvencie



Obrázok 5. Závislosť faktora kvality integrovanej cievky od frekvencie



Obrázok 6. Ideálna schéma 3-stupňového boost konvertora



Obrázok 7. Závislosť konverznej účinnosti a zvlnenia výstupného napätia od výstupného výkonu 3LBC konvertora

IV. Napäťový menič

Dôležitým krokom je správne vybraná topológia meniča napätia. Tú istú funkciu môže spĺňať niekoľko rôznych topológií, avšak pri dôraze na iné parametre bude výhodnejšia zase iná topológia. Na základe doteraz vykonaného výskumu a predošlých publikovaných prác [7], [8], [9], sme pre naše účely zvolili topológiu 3-stupňového boost konvertora (3LBC z angl. 3-Level Boost Converter). Ideálna schéma tohto meniča je zobrazená na obrázku 6. Menič sa skladá zo štyroch výkonových spínačov $SW1$, $SW2$, $SW3$ a $SW4$, a ooužíva tzv. plávajúci kondenzátor C_{fly}. Taktiež spínače $SW2$ a $SW3$ sú plávajúce. Ostatné použité súčiastky sú integrovaná cievka L, filtračný kondenzátor C a odpor R reprezentujúci záťaž obvodu.

Analýza obvodu prebehla v návrhovom prostredí CADENCE. Obvod aj cievka bola navrhnuté pre štandardnú 130 nm CMOS technológiu. V obvode bola použitá štruktúra cievky predstavená v predošlej časti tohto príspevku, modely reálnych spínačov so sériovým odporom v zopnutom stave $R_{ON_1} = 0,5\ \Omega$ a $R_{ON_2} = 1\ \Omega$, a modely reálnych kondenzátorov s kapacitou $C_{fly} = 0,6\ nF$ a $C = 1\ nF$. Záťažou obvodu je odpor, ktorého hodnota je rozmietaná tak, aby výstupný prúd nadobúdal hodnoty od $I_{MAX} = 0,16\ mA$ do $I_{MIN} = 16\ mA$. Výstupné napätie je regulované ideálnym PWM riadiacim obvodom na hodnotu $V_{out} = 1,2\ V$. Ako zdroj napätia bol použitý ideálny model PV zberača energie s výstupným napätím $V_{DC} = 560\ mV$.

Simuláciami sme overili funkčnosť navrhnutej integrovanej cievky. Maximálna dosiahnutá konverzná účinnosť bola $\eta_{MAX} = 81,56\ \%$ pri spínacej frekvencii $f_{sw} = 20\ MHz$ a výstupnom výkone $P_{out} = 1,92\ mW$. Zvlnenie výstupného napätia je takmer v celom rozsahu pod hodnotou $\Delta V_{out} = 50\ mV$, čo je menej ako $4,2\ \%$ hodnoty výstupného napätia. Závislosti konverznej účinnosti a zvlnenia výstupného napätia pri dvoch pracovných frekvenciách a dvoch odporoch spínačov v zopnutom stave sú zobrazené na obrázku 7.

V. Porovnanie dosiahnutých výsledkov

V tabuľke I sa nachádza porovnanie dosiahnutých výsledkov s výsledkami aktuálnych publikovaných prác s podobným zameraním. Porovnané sú topológie 3LBC s klasickou topológiou boost konvertora (BC z angl. Boost Converter). Výhodou našej práce je dosiahnutie porovnateľnej konverznej účinnosti a výstupného napätia s použitím omnoho nižšej indukčnosti cievky a kapacity kondenzátorov, čo znamená značné ušetrenie plochy na čipe. Dosiahnutý výstupný výkon je však v našom prípade nižší.

VI. Zámer a ciele dizertačnej práce

Hlavným zámerom dizertačnej práce je návrh plne integrovaného DC-DC boost konvertora so všetkými svojimi pasívnymi súčiastkami aj s výkonovými spínačmi. Napäťový menič má pracovať v nízkonapäťovej oblasti ($< 5\ V$) a má byť schopný poskytnúť dostatočný výstupný výkon pre plne autonómne elektronické zariadenie z hľadiska jeho napájania. To znamená použitie fotovoltického zberača energie ako zdroj energie pre celý systém. Samotný konvertor má fungovať na báze vysokofrekvenčného spínania integrovanej cievky, čo má byť najväčším prínosom dizertačnej práce, keďže tento typ obvodu je v plne integrovanej forme zriedkavejší, ako napríklad topológie založené na vysokofrekvenčnom spínaní kondenzátorov (tzv. nábojové pumpy). Princíp spínania cievky z teoretického hľadiska zároveň predpokladá vyššie možné dosiahnuteľné účinnosti konverzie napätia [1].

Keďže topológie napäťových meničov a ich vlastnosti (najmä konverzná účinnosť) je významne ovplyvnená vyhotovením samotnej cievky, čiastkovým cieľom práce bolo navrhnúť vhodnú štruktúru takejto cievky integrovanej na čipe. Pomocou niekoľkých návrhových techník boli zlepšené vybrané parametre dôležité pre správne fungovanie napäťového konvertora.

Nasledujúcim cieľom práce je návrh plne integrovaného napäťového meniča, ktorý bude spĺňať všetky vlastnosti požadované jeho aplikáciou. Dôležitými faktormi pri tom budú pra-

Tabuľka I
POROVNANIE KONVERTOROV VZHĽADOM NA VÝSLEDKY INÝCH PRÁC

Parameter	Jednotka	BC [10]	BC [11]	3LBC [12]	3LBC (Táto práca)
Proces	**[nm]**	130	130	65	130
Spínacia frekvencia	**[MHz]**	0,04	118	100	0,02 - 0,06
Induktor	**[nH]**	220 00	20 + 30 [2]	5	10,9
Výstupný kondenzátor	**[nF]**	2 200	1,08	4	1
Plávajúci kondenzátor	**[nF]**	-	-	2,5	0,6
Maximálna účinnosť	**[%]**	85	77,4	83,2 @ P_{out}=90 mW	81,6 @ P_{out}=1,92 mW
Vstupné napätie	**[mV]**	7,3 - 140	1 - 2,7	1,2	560
Výstupné napätie	**[V]**	1	3,2	1,5 - 2,1	1,2
Zvlnenie výstupného napätia	**[mV]**	-	20,8	85	< 50
Výstupný prúd	**[mA]**	0,47 [1]	6 - 65	5-80	0,16 - 16
Výstupný výkon	**[mW]**	0,47 [1]	19,2 - 208	7,5 - 168	0,192 - 19,2
Metóda hodnotenia	**-**	Fyzická realizácia	Fyzická realizácia	Simulácia	Simulácia
Úroveň integrácie	**-**	Diskrétne pasívne súčiastky	Úplná integrácia	Úplná integrácia	Úplná integrácia
Rok	**-**	2021	2018	2018	2021

[1] **- Približná hodnota** [2] **- Bondwire Induktor**

covná frekvencia obvodu, konverzná účinnosť alebo zvlnenie vstupných aj výstupných signálov. Dôležitým krokom bude aj návrh ďalších pomocných obvodov zabezpečujúcich správne fungovanie celého systému ako aj riadiaci obvod pre všetky výkonové spínače a regulačnú slučku. Overenie ich funkčnosti prebehne opäť v prostredí programu CADENCE.

Posledným krokom v našom výskume bude implementácia celého systému na čip a jeho testovanie. Počas neho bude verifikované správne fungovanie samotného napäťového meniča, pomocných obvodov a charakterizovaná integrovaná cievka.

VII. ZÁVER

Tento príspevok začína prehľadom návrhových techník integrovaných cievok za účelom vytvorenia pasívnej súčiastky pre budúce použitie v obvode napäťového konvertora. Pre účel vyhodnotenia vplyvu metód návrhu a zmien v topológii štruktúry cievky bolo navrhnutých niekoľko cievok tvaru nepravidelného osemuholníka. Nakoniec bola vytvorená výsledná štruktúra s dôrazom na zlepšenie faktora kvality, ktorého maximum bolo $Q = 9,99\ nH$ pri frekvencii $F = 630\ MHz$.

Ďalej sme sa venovali simuláciám topológie 3-stupňového boost konvertora pre zvýšenie úrovne jednosmerného napätia. Výsledky ukazujú porovnateľnú maximálnu konverznú účinnosť ($\eta_{MAX} = 81,56\ \%$) s inými prácami, pri významnom ušetrení plochy čipu potrebnej na realizáciu obvodu.

V rámci mojej doterajšej práce a výskumu vznikli 3 publikácie, ktorých som autorom alebo spoluautorom (2 príspevky na medzinárodných vedeckých konferenciách a 1 príspevok na domácej konferencii).

POĎAKOVANIE

Táto práca bola podporená Agentúrou na podporu výskumu a vývoja v vrámci projektu APVV 19-0392, a projektami VEGA 1/0760/21 a VEGA 1/0731/20.

LITERATÚRA

[1] M. Wens and M. Steyaert, *Design and Implementation of Fully-Integrated Inductive DC-DC Converters in Standard CMOS*, 1st ed. Springer, 2011.

[2] Yue, C. P. and Wong, S. S., "Physical modeling of spiral inductors on silicon" v IEEE Transactions on Electron Devices , 2000, vol. 47, no. 3, 560-568 s. doi: 10.1109/16.824729.

[3] Xu, X. et. al., "Design of Novel High-Q-Factor Multipath Stacked On-Chip Spiral Inductors" v IEEE Transactions on Electron Devices , 2012, vol. 59, no. 8, 2011-2018 s. doi: 10.1109/TED.2012.2197626.

[4] Lopez-Villegas, J.M. et. al., "Improvement of the quality factor of RF integrated inductors by layout optimization" v IEEE Transactions on Microwave Theory and Techniques , 2000, vol. 48, no. 1, 76-83 s. doi: 10.1109/22.817474.

[5] Vanukuru, V. N. R. and Chakravorty, A. "Series Stacked Multipath Inductor With High Self Resonant Frequency" v IEEE Transactions on Electron Devices , 2015, vol. 62, no. 3, 1058-1062 s. doi: 10.1109/TED.2015.2390293.

[6] Seong-Mo Yim et. al., "The effects of a ground shield on the characteristics and performance of spiral inductors" v IEEE Journal of Solid-State Circuits , 2002, vol. 37, no. 2, 237-244 s. doi: 10.1109/4.982430.

[7] Ondica, R.et. al., "Feasibility study towards increasing efficiency of fully on-chip DC-DC boost converter" v 2020 International Conference on Applied Electronics (AE) , 2020, 1-4 s. doi: 10.23919/AE49394.2020.9232811.

[8] Ondica, R. et. al., "Investigation of Inductor-based Fully On-chip Boost Converter" v 2021 28th International Conference on Mixed Design of Integrated Circuits and System , 2021, 115-119 s. doi: 10.23919/MIXDES52406.2021.9497548.

[9] Ondica, R. and Stopjaková, V., "Comparative Study of On-chip Inductive DC-DC Step-up Converters" v 2021 23th Conference of Doctoral Students ELITECH , 2021.

[10] Radin, R. L. et. al., "An Accurate Zero-Current-Switching Circuit for Ultra-Low-Voltage Boost Converters" v IEEE Transactions on Circuits and Systems II: Express Briefs , 2021, vol. 68, no. 6, 1773-1777 s. doi: 10.1109/TCSII.2020.3040501.

[11] Dam, S., Mandal, P., "An Integrated DC–DC Boost Converter Having Low-Output Ripple Suitable for Analog Applications" v IEEE Transactions on Power Electronics 2018, vol. 33, no. 6, 5108-5117 s. doi: 10.1109/TPEL.2017.2735491.

[12] Tan, Y. et. al., "Design and Control of An Integrated 3-Level Boost Converter under DCM Operation" v IEEE International Symposium on Circuits and Systems (ISCAS) , 2018, 1-5 s. doi: 10.1109/ISCAS.2018.8351144.

Zlepšení klasifikace malwarových rodin pomocí naučené vzdálenosti pro nízké dimenze

Mgr. Olha Jurečková
1. ročník prezenčního studia
Studijní obor: Informatika
Vedoucí práce: prof. Ing. Róbert Lórencz, CSc.

FIT ČVUT v Praze
Thákurova 9, 160 00 Praha, Česká republika
jurecolh@fit.cvut.cz

***Abstrakt*—V tomto článku se zabýváme vybranými state-of-the-art technikami pro učení vzdálenosti, které byly použity pro problém klasifikace malwarových rodin, přičemž se zaměřujeme na nízkodimenzionální reprezentace prostoru vstupních příznaků. Cílem algoritmů pro učení vzdálenosti je najít nejvhodnější parametry vzdálenosti s ohledem na dané optimalizační kritérium. Algoritmy pro učení vzdálenosti se v našem výzkumu učí z metadat obsažených v hlavičkách spustitelných souborů v souborovém formátu Portable Executable. Na naší datové sadě bylo provedeno několik experimentů se 14 000 vzorky sestávajícími ze šesti prevalentních malwarových rodin a benigních souborů. Experimentální výsledky ukázaly, že dobré klasifikační výsledky je možné dosáhnout už i pro dvojrozměrné vektory příznaků.**

***Klíčová slova*—Malwarová rodina, PE souborový formát, učení vzdálenosti, strojové učení**

I. Úvod a motivace

Každý den se vytváří velké množství nových škodlivých vzorků, což činí ruční analýzu malware nepraktickou. Většina těchto vzorků je generována generátory malwaru, které definují odpovídající rodiny malwaru. Tvůrci malware neustále obměňují nastavení generátorů, čímž způsobují, že vzorky ze stejné malwarové rodiny generované v jiném časovém období se navzájem liší [1]. Vzorky generované ze stejného generátoru s daným nastavením se mohou navzájem potenciálně podobat (vzhledem k dané podobnosti) a zároveň se mohou lišit od vzorků patřících do jiných malwarových rodin nebo benigních souborů. Tato práce se zaměřuje na využití těchto rozdílů k rozlišení malwarových rodin.

Vzhledem k velkému počtu škodlivých souborů, které přicházejí k antivirovým společnostem, je potřebné automaticky kategorizovat malware do skupin odpovídajících malwarovým rodinám. Vzorky patřící do stejné rodiny jsou si navzájem podobné vzhledem k dané míře podobnosti, která je určená vzdálenostní metrikou. Příslušné rodiny jsou poté distribuovány analytikům malwaru. Praktické použití rozlišování mezi malwarovými rodinami spočívá v tom, že analytici malwaru se lépe můžou vypořádat s velkým počtem vzorků.

Analytici malwaru jsou obvykle specialisté na omezený počet malwarových rodin. Pokud předpokládáme, že vzorky byly klasifikovány správně a vzorky ze stejné rodiny jsou si navzájem podobné a liší se od vzorků jiných rodin, pomocí našeho přístupu se analytici mohou zaměřit pouze na ty vzorky patřící do malwarových rodin, na které jsou analytici specializovaní.

Vhodná míra podobnosti hraje důležitou roli při úspěšnosti klasifikátorů založených na vzdálenosti, jako je k-nejbližších sousedů (KNN). Vzdálenost mezi dvěma vektory příznaků patřící do stejné třídy musí být minimalizována, zatímco vzdálenost mezi dvěma vektory příznaků z různých tříd musí být maximalizována. To je cílem metod učení vzdálenosti (Distance Metric Learning - DML), které se používají k naučení parametrů vzdálenosti z tréninkových dat. V důsledku toho se může potenciálně zlepšit přesnost jednotlivých klasifikátorů.

II. Metody učení vzdálenostní metriky

A. Základní pojmy

Přesnost některých metod strojového učení, jako je KNN, výrazně závisí na vzdálenosti použité k výpočtu míry podobnosti mezi dvěma vzorky. Tyto klasifikátory vycházejí z předpokladu, že vzorky náležející do stejné třídy jsou si navzájem blízké (s ohledem na vzdálenostní metriku) a jsou daleko od vzorků patřících do různých tříd.

Euklidovská vzdálenost je zdaleka nejčastěji používanou vzdálenostní metrikou. Zobecněním euklidovské vzdálenosti je Mahalanobisova vzdálenost, která pro dva n-dimenzionální vektory příznaků $\mathbf{x}$ a $\mathbf{y}$ je definována jako

$$d_{\mathbf{M}}(\mathbf{x}, \mathbf{y}) = \sqrt{(\mathbf{x} - \mathbf{y})^\top \mathbf{M} (\mathbf{x} - \mathbf{y})} \tag{1}$$

kde $\mathbf{M}$ je pozitivně semidefinitní matice. Když $\mathbf{M}$ je jednotková matice, potom $d_{\mathbf{M}}$ v rovnici (1) je redukovaná na euklidovskou vzdálenost.

Cílem učení Mahalanobisovy vzdálenosti je najít vhodnou matici $\mathbf{M}$ s ohledem na nějaké optimalizační kritérium. V kontextu klasifikátoru KNN je cílem najít matici $\mathbf{M}$, která vede k zvýšení přesnosti klasifikátoru KNN. Protože pozitivně semidefinitnou matici $\mathbf{M}$ lze vždy rozložit jako $\mathbf{M} = \mathbf{L}^\top \mathbf{L}$, lze

problém učení vzdálenosti považovat za nalezení buď $\mathbf{M}$ nebo $\mathbf{L} = \mathbf{M}^{\frac{1}{2}}$. Mahalanobisova vzdálenost definovaná v rovnici (1) se může vyjádřit pomocí matice $\mathbf{L}$ jako

$$d_{\mathbf{M}}(\mathbf{x}, \mathbf{y}) = d_{\mathbf{L}}(\mathbf{x}, \mathbf{y}) = \|\mathbf{L}^{\top}(\mathbf{x} - \mathbf{y})\|_2 \tag{2}$$

Matici $\mathbf{L}$ lze použít k transformování původního prostoru příznaků do nového prostoru příznaků. Tato projekce je lineární transformací a je definována pro vektor $\mathbf{x}$ jako

$$\mathbf{x}' = \mathbf{L}\mathbf{x} \tag{3}$$

Mahalanobisova vzdálenost $d_{\mathbf{L}}(\mathbf{x}, \mathbf{y})$ pro dva vektory z původního prostoru příznaků se rovná euklidovské vzdálenosti $d(\mathbf{x}', \mathbf{y}') = \sqrt{(\mathbf{x}' - \mathbf{y}')^{\top}(\mathbf{x}' - \mathbf{y}')}$ v prostore transformovaném pomocí rovnice (3). Tato transformace je užitečná, protože výpočet euklidovské vzdálenosti má nižší výpočtovou složitost než Mahalanobisova vzdálenost.

B. State-of-the-art metody učení vzdálenosti

V této práci se věnujeme třem state-of-the-art metodám pro učení Mahalanobisovy vzdálenosti: Large Margin Nearest Neighbor, Neighborhood Component Analysis a Metric Learning for Kernel Regression.

1) Large Margin Nearest Neighbor: Large Margin Nearest Neighbor (LMNN) [2] je jedním ze state-of-the-art algoritmů pro učení Mahalanobisovy vzdálenosti pro klasifikaci KNN. LMNN se skládá ze dvou kroků. V prvním kroku se pro každý prvek $\mathbf{x}$ identifikuje sada k nejbližších prvků patřících do stejné třídy jako $\mathbf{x}$ (označována jako *cílové sousedy*). Ve druhém kroku přizpůsobíme Mahalanobisovu vzdálenost tak, aby *cíloví sousedé* byly blíže k $\mathbf{x}$ než prvky z různých tříd, které jsou odděleny velkým okrajem (large margin).

Parametr Mahalanobisovy vzdálenosti se odhaduje pomocí řešení problému semidefinitního programování definovaného jako:

$$\min_{\mathbf{L}} \sum_{i,j:j\to i} \Big(d_{\mathbf{L}}(\mathbf{x}_i, \mathbf{x}_j)^2 + \\ + \mu \sum_{k:y_i \neq y_k} \max\Big(0, 1 + d_{\mathbf{L}}(\mathbf{x}_i, \mathbf{x}_j)^2 - d_{\mathbf{L}}(\mathbf{x}_i, \mathbf{x}_k)^2\Big)\Big) \tag{4}$$

Značení $j \to i$ znamená, že $\mathbf{x_j}$ je *cílový soused* prvku $\mathbf{x_i}$ a y_i značí třídu prvku $\mathbf{x_i}$.

2) Neighborhood Component Analysis: Algoritmus Neighborhood Component Analysis (NCA) [3] byl speciálně navržen pro zlepšení klasifikace KNN a můžeme ho definovat následovně.

Nechť p_{ij} je pravděpodobnost, že prvek $\mathbf{x_i}$ je sousedem prvku $\mathbf{x_j}$ patřícího do stejné třídy jako $\mathbf{x_i}$. Tato pravděpodobnost je definována jako:

$$p_{ij} = \frac{\exp(-||\mathbf{L}\mathbf{x}_i - \mathbf{L}\mathbf{x}_j||_2^2)}{\sum_{l\neq i}\exp(-||\mathbf{L}\mathbf{x}_i - \mathbf{L}\mathbf{x}_l||_2^2)}, \qquad p_{ii} = 0 \tag{5}$$

Cílem NCA je najít matici $\mathbf{L}$ která maximalizuje součet pravděpodobností p_i:

$$\arg\max_{\mathbf{L}} \sum_{i=0}^{N-1} \sum_{j:j\neq i, y_j = y_i} p_{ij} \tag{6}$$

K vyřešení tohoto optimalizačního problému se používá známý *gradient ascent* algoritmus. Poznamenejme, že algoritmy LMNN a NCA nevytvářejí žádné předpoklady o rozdělení tříd.

3) Metric Learning for Kernel Regression: Algoritmus Metric Learning for Kernel Regression (MLKR) [4] se zaměřuje na nalezení Mahalanobisovy matice, která minimalizuje následující ztrátovou funkci $\mathcal{L} = \sum_i (y_i - \hat{y}_i)^2$ nad tréninkovými prvky, kde prediktivní třída $\hat{y}_i$ je odvozena z jádrové regrese výpočtem váženého průměru tréninkových prvků:

$$\hat{y}_i = \frac{\sum_{j\neq i} y_j K(\mathbf{x}_i, \mathbf{x}_j)}{\sum_{j\neq i} K(\mathbf{x}_i, \mathbf{x}_j)} \tag{7}$$

MLKR lze použít na mnoho typů funkcí jádra $K(\mathbf{x}_i, \mathbf{x}_j)$ a vzdálenostních metrik $d(\mathbf{x}, \mathbf{y})$.

Zmíněné algoritmy učení vzdálenosti lze použít pro redukci dimenze vektoru příznaků. Když vezmeme v úvahu matici $\mathbf{L} \in \mathbb{R}^{d\times n}$, kde $d < n$, pak dimenze transformovaného vektoru $\mathbf{x}' = \mathbf{L}\mathbf{x}$ je snížena z n na d.

III. Popis navrhovaného řešení

V této kapitole představíme základní kroky navrhovaného postupu pro aplikaci DML algoritmů na problém klasifikace malware do rodin. Prostor transformovaný pomocí DML metod má oproti původnímu prostoru navíc tu vlastnost, že prvky ze stejné třídy jsou k sebe blíž a zároveň dál od prvků z odlišné třídy. Navrhovaný postup se skládá z následujících částí:

1) Z binárních souborů extrahujeme příznaky, které předzpracujeme do podoby vhodné pro algoritmy strojového učení.
2) Vybereme n nejrelevantnějších příznaků pomocí algoritmu pro vyber příznaků.
3) Na trénovací sadě natrénujeme Mahalanobisovu vzdálenost pomocí DML algoritmu.
4) Pomocí rovnice (3) transformujeme původní prostor příznaků do nového prostoru příznaků s dimenzi $d < n$.
5) Na nový prostor příznaků aplikujeme state-of-the-art algoritmy strojového učení, které nakonec vyhodnotíme na testovací sadě.

Podrobnější informace k bodem 1) a 2) jsou uvedeny v kapitole IV-C. Body 3) a 4) jsou stručně diskutovány v kapitole II-B. Nakonec podrobnosti k bodu 5) najdeme v kapitole IV-E.

IV. Experimentální část

V této kapitole představíme dataset, použité metriky pro vyhodnocení, výběr příznaků a nakonec výsledky jednotlivých experimentů.

A. Dataset

Naše experimenty jsou založeny na datové sadě obsahující 14 000 vzorků sestávajících z benigních souborů a ze 6 malwarových rodin. Datová sada je dobře vyvážená, protože každá ze 6 rodin malwaru má stejnou velikost, tj. 2 000 vzorků, a počet benigních souborů je také 2 000. Škodlivé programy

byly získány z online úložiště VirusShare[1] obsahující různé malwarové rodiny. Benigní soubory byly získány z univerzitních počítačů.

V našich experimentech jsme použili následujících šest prevalentních malwarových rodin:

Allaple - polymorfní síťový červ, který se šíří do dalších počítačů a provádí DoS (Denial-of-Service) útoky.

Skeeyah - trojský kůň, který proniká do systémů a krade osobní údaje a přidává infikovaný počítač do botnetu.

Virlock - ransomware, který uzamkne počítač obětí a požaduje platbu za jeho odemčení.

Virut - virus s funkcí backdoor, který operuje přes komunikační protokol založený na IRC.

Vundo - trojský kůň, který zobrazuje vyskakovací reklamy a také vkládá JavaScript do HTML stránek.

Zbot - je trojský kůň, který krade konfigurační soubory, přihlašovací údaje a bankovní údaje.

B. Metriky pro vyhodnocení

V této části uvádíme metriky, které jsme použili k měření přesnosti klasifikačních modelů. V binárním klasifikačním problému se používají následující klasické veličiny: True Positive (TP) představuje počet škodlivých vzorků klasifikovaných jako malware, True Negative (TN) představuje počet benigních vzorků klasifikovaných jako benigní, False Positive (FP) představuje počet benigních vzorků klasifikovaných jako malware, False Negative (FN) představuje počet škodlivých vzorků klasifikovaných jako benigní.

Úspěšnost binárních klasifikátorů uvažovaných v našich experimentech se měří pomocí tří standardních metrik. Nejintuitivnější a běžně používanou hodnotící metrikou je chybovost (error rate - ERR) definována na dané testovací sadě jako procento nesprávně klasifikovaných vzorků. Alternativou pro chybovost je přesnost definovaná jako $1-\text{ERR}$. Dalšími metrikami jsou přesnost (precision) a recall:

$$\text{precision} = \frac{\text{TP}}{\text{TP}+\text{FP}}, \qquad \text{recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \tag{8}$$

Přesnost udává pravděpodobnost, že vzorek označený jako malware, je skutečně škodlivý. Recall odpovídá pravděpodobnosti, že škodlivý soubor bude klasifikátorem detekován.

Protože všechny třídy mají stejný počet vzorků, pro klasifikaci více tříd používáme zprůměrované verze chybovosti, přesnosti a recallu. Průměrná chybovost je definována následovně:

$$\text{(average) ERR} = \frac{1}{N}\sum_{i\leq N} \mathbf{1}_{\text{class}_{\text{pred}} \neq \text{class}_{\text{true}}} \tag{9}$$

kde N je velikost testovací datové sady a $\mathbf{1}$ je charakteristická funkce. Průměrná přesnost, resp. průměrný recall je definován jako průměrná výsledná přesnost, resp. průměrný výsledný recall přes všechny třídy.

[1]http://virusshare.com/

C. Výběr příznaků

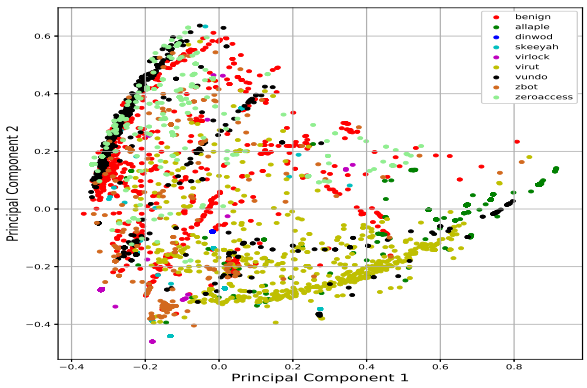
Příznaky použité v našich experimentech byly extrahovány z Portable Executable (PE) souborového formátu[2], což je formát pro spustitelné soubory, DLL knihovny a další soubory používané v 32 a 64 bitových verzích operačního systému Windows. PE formát je nejpoužívanějším souborovým formátem pro malware na platformách stolních počítačů. K extrahování příznaků ze souborů v PE formátu jsme použili Python modul `pefile`[3]. Tento modul extrahuje všechny atributy do objektu, ze kterého jsou snadno přístupné. Extrahovali jsme 358 numerických příznaků, přičemž dimenze je tak vysoká, protože pro každou sekci a pro každý typ charakteristiky (tj. booleovské pole) považujeme každou komponentu pole za jeden příznak.

Před použitím metod výběru příznaků byly všechny příznaky normalizovány pomocí procedury `preprocessing.normalize` z knihovny Scikit-learn[4]. Poté jsme použili šest metod výběru příznaků importovaných také z knihovny Scikit-learn. Klasifikátor k-nejbližších sousedů aplikován na prostor příznaků redukovaný pomocí metody RFE Logistic Regression dosáhl nejnižší chybovost 4.13 % pro 25 vybraných příznaků. Zkratka RFE označuje Recursive Feature Elimination, která je implementována v `feature_selection.RFE` také z knihovny Scikit-learn. Poznamenejme, že klasifikátor k-nejbližších sousedů aplikován na původní prostor (t.j. s 385 příznaky) dosáhl chybovost 4.31%.

D. Reprezentace malwarových rodin ve dvou dimenzích

Dvourozměrná reprezentace vektorů příznaků nám umožňuje zobrazit malwarové rodiny jako body v rovině. Šest prevalentních malwarových rodin a benigní soubory jsou znázorněny na obr. 1. Z každé z těchto tříd bylo náhodně vybráno sto vzorků. Původní prostor příznaku byl transformován pomocí metody analýzy hlavních komponent (Principal component analysis - PCA) do dvou dimenzí.

[2]https://docs.microsoft.com/en-us/windows/win32/debug/pe-format
[3]https://github.com/erocarrera/pefile
[4]https://scikit-learn.org



Obrázek 1. Reprezentace datové sady redukované pomocí metody PCA do dvou dimenzí.

Tabulka I
KLASIFIKAČNÍ VÝSLEDKY PRO DIMENZI $d = 2$ ALGORITMŮ STROJOVÉHO UČENÍ PRO NETRANSFORMOVANÝ (TJ. ORIGINAL) PROSTOR PŘÍZNAKŮ A PRO PROSTORY PŘÍZNAKŮ TRANSFORMOVANÉ POMOCÍ DML ALGORITMŮ (T.J. LMNN, NCA, MLKR).

# dimenzí 2	Average precision [%]						Average recall [%]					
Algoritmus	KNN	LR	NB	DT	RF	MLP	KNN	LR	NB	DT	RF	MLP
original	83.81	37.43	47.05	83.18	84.06	65.19	83.83	42.94	46.8	83.35	84.04	66.62
LMNN	85.63	45.23	49.29	84.23	86.45	**74.33**	85.82	51.97	49.50	84.39	**86.41**	**75.63**
NCA	**85.90**	25.03	**58.65**	84.36	**86.54**	64.56	**85.87**	40.39	**51.13**	84.57	**86.41**	58.19
MLKR	85.39	**46.59**	43.74	**84.76**	86.43	73.63	85.58	**52.58**	43.94	**84.98**	86.21	71.82

Tabulka II
KLASIFIKAČNÍ VÝSLEDKY PRO DIMENZI $d = 25$ ALGORITMŮ STROJOVÉHO UČENÍ PRO NETRANSFORMOVANÝ (TJ. ORIGINAL) PROSTOR PŘÍZNAKŮ A PRO PROSTORY PŘÍZNAKŮ TRANSFORMOVANÉ POMOCÍ DML ALGORITMŮ (T.J. LMNN, NCA, MLKR).

# dimenzí 25	Average precision [%]						Average recall [%]					
Algoritmus	KNN	LR	NB	DT	RF	MLP	KNN	LR	NB	DT	RF	MLP
original	96.15	86.38	**82.98**	94.76	96.44	96.22	96.14	86.17	77.79	94.78	96.41	96.17
LMNN	96.77	89.55	82.02	**95.20**	**97.05**	96.39	96.78	89.27	**81.03**	**95.20**	97.00	96.35
NCA	96.45	**90.78**	78.08	94.87	96.76	95.11	96.46	**90.60**	75.02	94.86	96.72	95.07
MLKR	**97.04**	87.94	77.96	95.15	**97.05**	**96.50**	**97.04**	88.12	75.41	95.13	**97.02**	**96.49**

E. Transformace prostoru příznaků pomocí DML

V následujícím experimentu jsme natrénovali 3 DML metody popsané v kapitole II-B. Výstupem z každé DML metody je pozitivně semidefinitní matice $\mathbf{M}$, kterou jsme rozložili na součin $\mathbf{M} = \mathbf{L}^\top \mathbf{L}$. Matici $\mathbf{L}$ jsme pak použili v lineární projekci, kterou jsme definovali v rovnici (3), pro transformaci původního prostoru příznaků (po výběru relevantních příznaku, tj. s dimenzí $n = 25$) do nového prostoru příznaků s dimenzí $d < n$.

Na původní prostor příznaků a na tři prostory transformované (každý zvlášť) pomocí LMNN, NCA a MLKR jsme aplikovali následující state-of-the-art algoritmy strojového učení: k-nejbližších sousedů ($k = 1$), logistická regrese, (Gaussian) Naive Bayes, náhodný les (počet stromů je 100), a vícevrstvý perceptron (2 skryté vrstvy, maximální počet iterací = 300, aktivační funkce = 'relu', řešení pro optimalizaci = 'adam'). Implementace algoritmů strojového učení, DML algoritmů a klasifikačních metrik vycházela z knihovny Scikit-learn. Pokud není uvedeno, hyperparametry klasifikátorů a DML metod byly nastaveny na jejich výchozí hodnoty, jak jsou uvedeny v knihovně Scikit-learn.

Klasifikační výsledky algoritmů strojového učení pro netransformovaný prostor příznaků a pro prostory příznaků transformované pomocí DML algoritmů jsou uvedeny v tabulce I pro dimenzi $d = 2$ (výběr příznaků se vykonal pomocí metody RFE Logistic Regression) a také pro porovnání v tabulce II pro optimální dimenzi $d = 25$. Z naměřených výsledků vidíme, že pomocí transformaci prostoru příznaků je možné pro některé algoritmy strojového učení zvýšit průměrnou přesnost i průměrný recall. Výsledky z tabulky I také indikují, že některé algoritmy strojového učení dosahují poměrně vysoké průměrné přesnosti a recally i pro dvoudimenzionální vektory příznaků.

V. ZÁVĚR

Naše práce se zaměřuje na problém klasifikace více tříd, kde každá rodina malwaru a benigní soubory mají svou vlastní třídu. Aplikovali jsme tři algoritmy pro naučení Mahalanobisovy vzdálenosti za účelem zlepšení výkonnosti klasifikace prvků z datové sady obsahující šest prevalentních malwarových rodin a benigní soubory. Výsledky klasifikace ukazují, že některé algoritmy strojového učení dosahují lepší výsledky na prostore příznaků transformovaném pomocí DML metod než na původním prostoru. Některé algoritmy strojového učení dosáhli překvapivě dobrých klasifikačních výsledků i pro dvoudimenzionální vektory příznaků.

Za předpokladu, že soubory patřící do stejné rodiny mají podobné chování, které je zachyceno podobnostní metrikou neboli vzdáleností mezi vektory příznaků, tak klasifikace do malwarových rodin může pomoci urychlit další analýzu malware. V budoucí práci by mohly být použity další typy příznaků, jako jsou bajtové sekvence nebo API a systémová volání, které by případně mohli zlepšit výsledky klasifikace.

PODĚKOVÁNÍ

Tento výzkum byl podpořen z projektu SGS21/142/OHK3/2T/18 Českého vysokého učení technického v Praze.

REFERENCE

[1] M. Wadkar, F. Di Troia, and M. Stamp, "Detecting malware evolution using support vector machines," *Expert Systems with Applications*, vol. 143, p. 113022, 2020.

[2] K. Q. Weinberger, J. Blitzer, and L. K. Saul, "Distance metric learning for large margin nearest neighbor classification," in *Advances in neural information processing systems*, 2006, pp. 1473–1480.

[3] J. Goldberger, G. E. Hinton, S. T. Roweis, and R. R. Salakhutdinov, "Neighbourhood components analysis," in *Advances in neural information processing systems*, 2005, pp. 513–520.

[4] K. Q. Weinberger and G. Tesauro, "Metric learning for kernel regression," in *Artificial Intelligence and Statistics*, 2007, pp. 612–619.

Utilization of Reinforcement Learning in Optimization of LoRa Networks

Alexander Valach
Year 2, full-time study
Pavel Čičák and Dominik Macko

Faculty of Informatics and Information Technologies STU in Bratislava
Ilkovičova 2
alexander.valach@stuba.sk

***Abstract*—With the increasing number of devices connected to the Internet of Things a scalable solutions are required. One of the most promising technology for wide-area IoT networks is LoRa. It enables transmission over long distances with minimum power consumption. However, the current solution for network optimization, adaptive data rate, is only able to set the configuration for the stationary environment, where the conditions in the network do not change very frequently. Adaptive data rate is also not able to deal with mobile nodes, which results in a high number of collisions, thus leading to higher power consumption. Some of the devices have only a very limited power supply and needs to prolong the battery lifetime as much as possible. The latest research has shown that using reinforcement learning techniques, especially algorithms for a multi-armed bandit problem, leads to a better power efficiency and higher packet delivery ratio. In this paper, we briefly introduce energy-wise LoRa@FIIT protocol, list and briefly describe the different algorithms for communication parameters selection and propose a network testbed for the performance evaluation of Thompson Sampling.**

***Keywords*—LoRa, LoRa@FIIT, IoT, Low Power, Multi-Armed Bandit, Reinforcement Learning**

I. Introduction

Dictionary of computing defines scalability as a term on how well a solution would sustain even when the problem increases [1]. In the terms of Internet of Things (IoT), it is equivalent to how well would devices be able to transmit and receive messages even when their numbers increase rapidly.

This issue is addressed mainly by the simultaneous existence of heterogenous devices that use different technologies [2], but also similar physical layer frequencies. This results in inter-technology interference [3], and incapability of many protocols (usage of pure ALOHA-based solutions) to listen before transmission [4], [5].

Another issue is a usage of the license-free Industrial Scientific and Medical (ISM) band, which is jammed by many technologies. Two leading low-power wide area network (LPWAN) technologies (LoRa and Sigfox) use the ISM band for communication [6]. This only contributes to higher interference and increases a probability of a packet collision or a channel congestion.

Appropriate tools for the simulation of the physical layer properties are also missing [7], [8]. However, there has been some successful attempts to implement them [9], [10], [11]. They are considered essential building blocks in the deployment of LPWAN networks and a mandatory tool for further research in the field of effective communication and a rapid growth of a number of end devices.

To improve performance, we need to reduce collisions between sent messages, increase the packet delivery ratio (PDR), and ensure that a combination of parameters selection is battery efficient [12]. There can be a situation with a minimal number of collisions and high PDR. However, in the same situation, communication parameters are set to the highest possible values, leading to the battery being drained earlier than expected. In some cases, there is no or limited possibility to recharge the battery, e.g., a sensor is put into an asphalt layer [13].

Effective communication parameters selection does not only refer to transmission in everyday environment with few devices. It is crucial to prepare IoT net-works for rapid increase of connected devices. Semtech, the creator of LoRa, estimates that around 1.6 billion LPWAN devices will be connected in 2026 [14]. It means, we need to evaluate the performance of end devices in a harsh and dense environment, where a risk of collision is increased on purpose.

A node-based machine learning (ML) approach can potentially help to both mitigate collisions and save battery power [7], [15] by using a more effective process of communication parameters selection with only a limited knowledge of the ever-changing environment [8], [16].

The rest of the paper is organized in the following way. Section 2 summarizes the recent research in the field of optimization of LoRa networks using ML algorithms. Section 3 introduces LoRa and LoRa@FIIT essentials focusing on the communication parameters. It further analyzes the different multi-armed bandit algorithms than can aid in mitigating collisions from the perspective of utilization in LoRa technology. Section 4 proposes a network testbed to evaluate a performance of Thompson Sampling algorithm in a switching environment.

II. Related works

One of the current challenges of the deployment of LoRa networks in densely populated urban areas with tall buildings and brick walls is to mitigate collisions. There has been a much research made in this field during the past years [2], [5], [17]. The researchers were focusing on several different aspects like an efficient communication parameters selection [7], [18], [19], [20], [21], designing an energy-wise solution [22], [23], [24], and mitigating or predicting collisions [3], [4], [25], [26], [27].

A field of ML called a reinforcement learning (RL) has been found helpful in process of selecting communication parameters. Even in a dynamic environment where nodes connects to the network and disconnects from it very often [7], [18]. RL is an area where a decision has to be made between an exploration and exploitation with only a limited knowledge of the situation [28].

To simplify evaluation of various RL algorithms in LoRaWAN networks, the LoRa-MAB simulator was developed. It helped to show that the distributed learning outperforms simple heuristics in terms of network throughput [19]. The work [18] showed that even algorithms that do not take a switching environment into account, namely upper confidence bound (UCB) and Thompson sampling (TS), achieve near optimal performance even in non-stationary settings. Every RL algorithms proves to be more energy efficient [7] mainly due to a collision reduction and possibility to adapt to network changes.

A lot of research has been conducted in the recent years considering an optimization of LoRa technology and especially LoRaWAN protocol. However, there are only a few papers addressing a utilization of RL algorithms considering devices that are constantly on the move and thus enforcing a switching environment.

There is almost no paper considering a ML approach with other than LoRaWAN protocol. We proposed our own architecture to simulate a LoRa network and focus on the performance of LoRa@FIIT protocol, which was designed to be more energy-wise than LoRaWAN [29] and can become a promising solution for certain industry use cases, e.g., a quality of service is required.

A. LoRa and LoRa@FIIT

LoRa is a physical layer modulation, also called LoRa PHY. It is a low-power wide area network (LPWAN) technology. It is very popular for battery-constrained devices due to its long-range communication, low power consumption and low deployment cost. It operates in the license-free ISM band [6], [30]. Transmitting in this band is free of charge but it has major regulations. In LoRa, each device can only occupy the medium only for certain time. This time is called a duty cycle (DC) and is set depending on the frequency. In Europe, it is usually 1% of hour, which means a device can only transmit 36 s withing one hour. The DC is refreshed after each hour [30]. The performance of LoRa networks depends on the setting of each device. These settings can be dynamically adjusted and are called communication parameters (CP) [30], [31]:

1) **Carrier Frequency (CF)** is also called a communication channel. When two devices use the same frequency at the same time, a collision occurs. There are also exceptions. When a capture effect (CE) is present [9] a message with higher (+ 6 dB) signal-to-noise ratio (SNR) value can be successfully retrieved [10]. Frequency is expressed in MHz and in Europe uses radio bands near 868 MHz [30].
2) **Transmission Power (TP)** has an impact on a battery lifetime. When an access point receives low-quality signal (below certain threshold), a node should increase its TP. TP is expressed in dBm and can vary from -4 dBm to 20 dBm [17]. In the current implementation of network server, it can only be updated in 1 dBm steps [32].
3) **Spreading Factor (SF)** has the most significant impact on communication efficiency. Lower SF value decreases communication range and time required to transfer message to the receiver (Time on Air, ToA), thus draining less battery power and decreasing a risk of collision, as the medium is occupied only for a short time interval. Higher SF value increases distance, a message can reach with lower SF values, and significantly (twice, by single level SF increment) increases ToA, thus draining more battery power [6], [10].
4) **Coding Rate (CR)** expresses a number of redundant bits in LoRa messages. Possible values are 4/5, 4/6, 4/7 and 4/8. When CR is set to 4/5 a 4-bits are encoded with 5 bits allowing communication to endure a short interference during transmission [30], [31]. A procedure of possible short interference recovery is called Forward Error Correction (FEC). The value of 4/5 is the only possible choice in current LoRa@FIIT implementation [33]. However, it can be dynamically changed by making minor changes to the network server [32].
5) **Bandwidth (BW)** sets up a frequency width (expressed in kHz) for communication channel [29]. LoRa can operate with 125 kHz, 250 kHz, or 500 kHz bandwidth. Higher bandwidth values indicate higher data rates, but lower receiver sensitivity. If not explicitly written, a 125 kHz BW is assumed to be used in the whole paper.

LoRa@FIIT is a Media Access Control (MAC) layer protocol designed to overcome drawbacks of LoRaWAN. It uses Corrected Block Tiny Encryption Algorithm (XXTEA) specifically designed for embedded devices with low memory and computational power [34]. It has a built-in quality of service (QoS) mechanism and supports three different acknowledgement types (no, optional, or mandatory ack). It requires significantly lower (42%) overhead for sending 1 B of data compared to LoRaWAN. However, it does not support roaming, so the owner of the network must be the same as the owner of the end devices [29].

LoRa@FIIT network architecture is derived from Lo-

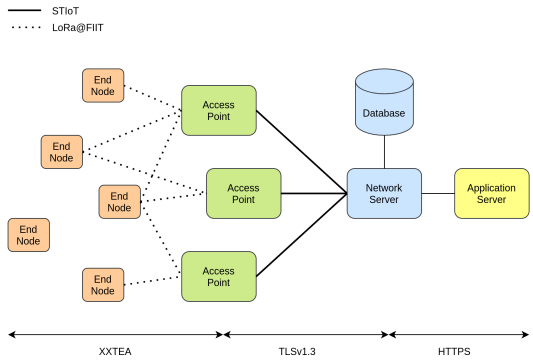


Fig. 1: Typical LoRa@FIIT network architecture derived from LoRaWAN architecture [35]

RaWAN architecture and illustrated in Fig. 1. LoRaWAN is another MAC layer protocol, widely deployed in LoRa networks and maintained by the LoRa Alliance [35], [36], [37], [38]. LoRa@FIIT networks consist of several types of devices:

1) **End node (EN)** is usually a battery-constrained device with limited computational power and memory. It is designed to measure a certain characteristic of an environment, e.g., air quality, humidity, or atmospheric pressure, and send the measured data via LoRa technology to nearest access points.
2) **Access point (AP)** receives LoRa packets from end nodes, extracts the content of the messages and sends it to the network server in a JSON format using Secure TCP for IoT (STIoT) [29].
3) **Network server (NS)** is a central decision-making point of LoRa@FIIT networks. It stores information about device duty cycle and manages communication parameter selection (SF and TP). It processes data from APs and manages end nodes' communication parameters selection process based on previous RSSI and SNR values.
4) **Application server (AS)** displays a collected data from the end nodes to the customers.

LoRa@FIIT introduces several message types that can be processed differently by network components. Message types are listed below:

1) **Data messages** carry an application payload with measured data.
2) **Emergency messages** are sent when critical conditions are measured or the level of the observed characteristics is below or above the acceptable value, e.g., water level too high or a blood oxygen saturation is too low.
3) **Registration messages** are sent when a device wants to join an existing network. They carry a Diffie-Hellman keys to derive a shared secret.
4) **Hello messages** are used as a keepalive mechanism and require an acknowledgement from the network server [29].

The current implementation of LoRaWAN or LoRa@FIIT both uses adaptive data rate algorithm (ADRA) to configure the proper communication parameters on the ENs. CPs are calculated on a network server and distributed to end devices.

The difference between best and worst CP selection combination can lead to 47% battery-life loss due to non-optimal decision making process or lack of information from the network server [15]. The study shows that CP selection is not only crucial for further development, but it is also mandatory to provide long battery-life, in term of several month to years.

B. Multi-Armed Bandit Algorithms

Problem of selecting appropriate communication parameters can be compared to a problem of choosing a right arm with an unknown reward with goal of getting the largest cumulative reward [39]. A bandit, which is pulling arms, is not provided with the reward values and thus is forced to try different arms (exploration) or pull the exact same arm that gave him the largest discovered reward multiple times (exploitation). This problem is called a multi-armed bandit problem (MABP). Algorithms developed to cope with a MABP are called multi-armed bandit algorithms (MABA) [18].

MABAs are the part of a reinforcement learning, a field of machine learning. MABAs have been used to mitigate collisions and make the nodes more independent from network server in various network simulations [7], [8], [18], [40].

In a traditional MABP, we are given several slot machines, also called bandits, with the goal to minimize the cumulative regret [41] with no prior knowledge of which machine produces the highest reward. Depending on the characteristics, we differentiate between several environments [18]:

1) **Stationary environment** where rewards do not change in time. Once an optimal strategy is discovered, the low cumulative regret is achieved. However, this setup is very unrealistic in a dynamic environment of IoT.
2) **Non-stationary (dynamic) environment** where rewards do not change in time. A change point detection mechanism is required, to signal nodes switching to a different environment (change of rewards).
3) **Adversarial environment** where rewards are set by an adversary and change when a new adversary is introduced. It is similar to the dynamic rewards but relies on adversary rather than a change point detection.

1) Stationary Multi-Armed Bandit Algorithms.: These algorithms are designed to deal with a MABP when rewards do not change in time. They are usually easy to implement as there are no additional requirements, only a reward calculation and pick-up of arm.

a) Upper Confidence Bound (UCB).: Defines a confidence level for each arm. It is naive and greedy approach and depends heavily on the first draw [18]. This algorithm is designed for stationary environments. It proves to be the worst algorithm in non-stationary environment, based on the results from mathematical simulations [7]. The cumulative regret also tends to rise with larger number of trials [39].

Require: α, β shape parameters from Beta distribution
Sj=0, Fj=0
for t=1, ..., T **do**
for j=1, ..., N **do**
Draw arm_j according to $Beta(S_j + \alpha, F_j + \beta)$
end for
Select $param_j = argmax_j \theta_j$ and get the reward r
if $r = 0$ **then**
$F_j = F_j + 1$
else
$S_j = S_j + 1$
end if
end for

Fig. 2: Pseudocode for Thompson Sampling

A reward for each arm (combination of communication parameters) is computed based on the following formula:

$$REWARD_i = \mu_i + \sqrt{\frac{2\ln(n)}{n_i}} \quad (1)$$

In the formula above, μ_i represents the current (n^{th} round) average reward returned from arm i, n represents the number of rounds (trials for any arm) so far and n_i represents number of pulls for arm i, e.g., how many times has the combination of communication parameters been selected.

Confidence bound is used as a mean to deal with an exploration versus exploitation dilemma. If multiple arms have the same reward, which is considered an initial state of the network, an arm with a higher confidence bound is drawn. After each draw, the confidence bound is decreased, and the previously unexplored arms are preferred [18]. This strategy follows an optimistic approach in the favor of the uncertainty.

b) Thompson Sampling (TS).: It is a probability matching algorithm [42] that chooses an arm based on the shape parameters: α (successful attempts) and β (failed attempts). It uses Bayesian tools, assuming a prior distribution of each arm [39]. Unlike UCB, this is a sampling based probabilistic approach and proved to achieve smaller cumulative regret than UCB [7], [16], [42].

The TS was designed to deal with a Bernoulli bandit problem where a reward is set to 1 or 0 [39]. Instead of a greedy approach, where a sub-optimal solution is usually found because the algorithm sticks to a local maximum, it uses an theta parameter. This parameter forces selection of a locally sub-optimal solution, which can lead to a globally optimal solution. The fundamentals of a TS algorithm are presented in Fig. 2 [39]:

In the above-mention algorithm, S_j and F_j represent a number of successful draws (a packet was delivered) and failures (a packet was lost), respectively. T is the number of total trials and N represents a number of arms (communication parameters combination) to choose between. θ_j is an array of rewards for each arm [39], which is unknown to the end node. $param_j$ represents arms (combination of SF and TP). Furthermore, a Beta distribution is used to model the mean of each arm. It is considered a standard practice [39].

A search space also has an important role. When it is very expansive, a TS is trying to prove a single option to be more efficient and pulls it several times. On the other hand, UCB uses an optimistic approach and is willing to take a quick but uncertain win option without further investigation.

2) Non-stationary Multi-Armed Bandit Algorithms.: In the non-stationary environment rewards change in time. This is more realistic environment than a stationary one, as it considers the change in the environment, also called a switching. The process of identifying a switching environment is also called a change point detection. We differentiate between two types of switches [7]:

1) **Global switching** where all the rewards are changed. This indicates a change in the environment, e.g., a mobile node moves from one area to another one, where network conditions are different.
2) **Per-arm switching** where only a reward for single arm has changed. It can indicate a congestion on a certain channel (SF). A mechanism to notify all the affected ENs is required [43].

a) Global Switching Thompson Sampling with Bayesian Aggregation (STSBA).: It is a stochastic MABA. To the authors' best knowledge, it has not been evaluated in a real-world environment yet. Only mathematical simulation that take into account several physical modulation constraints were performed, both for LoRa [7] and other wireless networks [16] facing a similar problem. It proved to be the most efficient from the stochastic algorithms, because its adaptability to non-stationary settings and a fast change point detection using a Bayesian aggregation [7].

It is a modified version of TS algorithm designed for non-stationary settings and is combined with a Bayesian online change point detector [42]. It is also an expert-based algorithm, meaning, there is a TS procedure starting at time t. A Bayesian aggregation (BA) is used on the most likely expert (according to its weight) and then a TS is run to choose an arm. After choosing an arm, weight for corresponding arm is updated [7].

In [7], [16] the researchers proved that a STSBA slightly outperformed TS at the cost of higher processor utilization and thus a higher energy consumption. TS performed similarly to STSBA but requires less computational power, which has a significant impact on battery-life for low-power devices.

UCB has also its switching alternative, called Sliding Window UCB (SWUCB). However, it was outperformed by TS (stationary algorithm) and performs similarly to UCB [7], thus we will not examine it closer in this paper.

3) Adversarial Multi-Armed Bandit Algorithms.: Exponential Weights for Exploration and Exploitation (EXP3) is an adversarial MABA. It theoretically performs worse than stochastic bandits (TS and UCB) [16]. However, it can achieve similar results using any settings and thus providing similar results for different environments. It can also handle non-stationary settings [19], [7], which is essential for a real-world

scenario with mobile nodes. EXP3.S is an enhanced version of EXP3 algorithm and performs better than the original one [22].

Disadvantage of these algorithms is the long conversion time. For EXP3 up to 200 kHours and for EXP3.S up to 20 kHours. Each new node should be able to communicate efficiently after conversion time [10]. Therefore, an improved solution is required to shorten the time, as it is not sufficient in dynamic and harsh network environment of license-free LPWANs.

4) Performance of Multi-Armed Bandit Algorithms.: The experiments showed that an ADRA was outperformed by MABAs, both in terms of an energy consumption and PDR. The energy consumption for a single communication parameter selection is lower in ADRA, as no additional overhead is required. However, the overall energy consumption is usually higher due to the node not being able to change CPs without a network server. In MABAs, an overhead is required for a CP selection, but an overall energy consumption can be lower due to an ability to choose alternative CPs without the interception from the network server.

When it comes to a comparison of MABAs, adversarial bandits (EXP3 and EXP3.S) are generally outperformed by the stochastic bandits [7], [16]. This is true especially when mobile nodes are introduced [7]. The stationary bandits (TS and UCB) are outperformed by the switching environment bandit (STSBA, SWUCB). The switching bandits are the most difficult to implement and tune properly, so an additional research in this field is also required.

The experiments also showed that the results of TS, a stationary bandit algorithm, are similar to its switching alternative [7]. This is quite surprising because a TS was not designed for a switching environment [39]. The lowest energy consumption was achieved with UCB and SWUCB. The lowest packet loss and overall total cost compared to ADRA has a STSBA, which is an improved version of TS for switching environments, modified by the researchers in [7]. ADRA naturally has the worst performance in examined scenarios [7], [11].

III. The Proposed Network Testbed

One of the most important aspects before a network is deployed are the performance metrics and ability to perform well even in a harsh real-world environment with densely located nodes and dynamic environment.

To simplify an assertion of different algorithms, we propose our own architecture, illustrated in Fig. 3. We have developed a simple STIoT (protocol for communication between APs and NS) packet generator [36] that simulates an operation of a single AP. This single-AP simulator connects to a deployed remote NS as would be the case in a real-world scenario.

In the simulator, ENs do have their own configuration settings. However, LoRa physical properties are only calculated based on the rules described in the following subsection. As each EN support a communication parameter selection using TS and UCB (bandit algorithms), it is called a bandit node (BN). This term helps to differentiate the traditional ENs, that depend on the decision from NS, from the proposed BNs, which use MABAs.

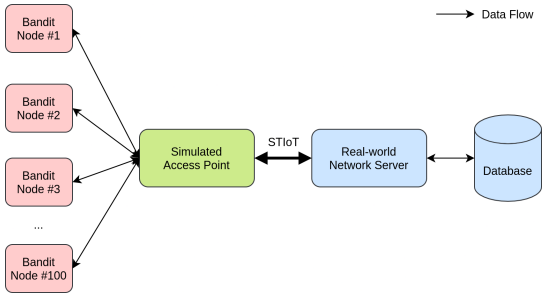


Fig. 3: Network testbed architecture consisting of several ENs, simulated AP and real NS

A. Rules for the STIoT Packet Generator

The experiments will be performed using our own STIoT packet generator [44] and a real LoRa network server [32]. As the results of TS are very promising for mobile nodes, despite being primarily developed for a stationary setting, we will focus on implementing TS in our generator and simulate the process of up to 100 ENs connected to a single AP. Despite being evaluated only using simulations, some aspects from a real-world scenario were also implemented in the simulator and are listed below [44]:

1) **Rules for collisions and packet loss.** There are several types, which we refer to as a collision.
   a) A frame is transmitted on the same SF as another frame at the same time or their receiving times overlap with each other.
   b) When a RSSI value is below the receiver's sensitivity, it is discarded and considered a collision.
   c) SNR value is randomly generated. If it is between certain threshold, it is considered unreadable (too much interference), cannot be demodulated and is discarded.
2) **Movement of the end nodes.** Every second, each of the nodes is moving on the square area of 100 km^2. The signal is weakened by the free-space path loss (FSL) formula presented below. CF is a frequency in Hz and D is a distance in km. When we use Hz and km as units, C becomes close to 32.5:

$$FSL = C + 20 \times \log CF + 20 \times \log D \qquad (2)$$

The directions for horizontal and vertical movements are randomly chosen at the beginning of the experiments and can only be positive or negative. The direction is changed every time a device is getting close to a wall at the edge of the area. Every second, a 0–1 m movement of node can be made in both horizontal and vertical direction, resulting in 8 directions in total. This mechanism was design to force a frequent (but predictable) change of CPs in the environment.

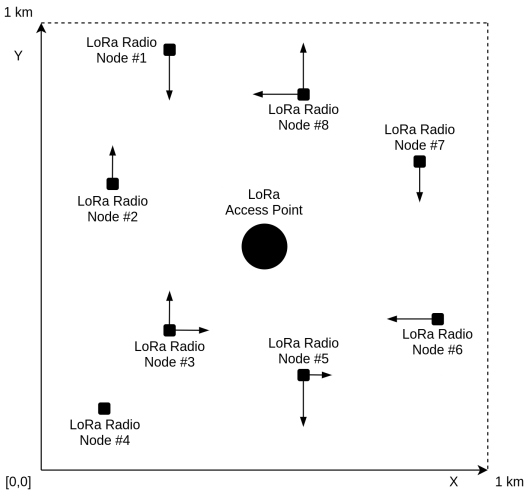


Fig. 4: LoRa access point is placed in the center of the observed area with end nodes moving constantly

3) **Placement of the nodes.** Each EN is placed randomly on the [x, y] coordinates following a uniform distribution. Only a single AP can be found within the area and it is placed in its center at coordinates [5000, 5000]. Distances are calculated in meters. The placement and the movement of the nodes around AP is presented in Fig. 4.
4) **Communication parameters.** Only SF and TP values can be updated by ENs or NS. Other values are fixed (presented in Table **??**) during the experiments to simplify the process, as we focus mainly on the comparison of UCB and TS. The other parameters are CR, BW, and FREQ, which are set to 4/5, 125 kHz, and 866 MHz respectively.
5) **Transmissions.** After sending an uplink message, two receiving windows are subsequently opened. However, only if the message type was set to emergency, a device is waiting for an acknowledgement. Otherwise, it is considered lost and is retransmitted.
6) **Retransmissions.** After three unsuccessful attempts to transmit an important (emergency or registration) message, a device enters a sleep mode. If a message does not require an acknowledgement, a retransmission does not occur. When an important data is being transmitted, a message can be retransmitted till the acknowledgement is received or it is considered lost.
7) **Received Signal Strength Indicator (RSSI)** is calculated based on the following formula, where TP_{TX} is a TP of EN, G_{TX} is a transmitter antenna gain, FSL is a free space loss and G_{RX} is an antenna gain of the receiver.

$$RSSI = TP_{TX} + G_{TX} - FSL + G_{RX} \tag{3}$$

Cable loss at the transmitter and the receiver are both negligible in the case of very short (6 cm) low-loss cable.

8) **Payload.** Each packet contains a base64 encoded string with information about its current position within the simulation area. Those data are decoded and visualized during the evaluation of the experiments.
9) **Duty cycle restrictions.** Only a few papers have considered a duty cycle constraint. Our simulator has a built-in duty cycle management mechanism for each node. It calculates Time on Air [33] for each packet and subtracts this value from the actual duty-cycle. Time on Air (ToA) is calculated using the following equations, where T_S is the time required to send a single symbol and N_{SYM} is number of symbols:

$$ToA = T_S \times N_{SYM} \tag{4}$$

$$T_S = \frac{2^{SF}}{BW} \tag{5}$$

IV. Goals of the Thesis

According to a state of the art and current challenges and research areas, we propose the following goals of the thesis:

1) **Scalable communication parameters selection.** Decentralized solution (semi-autonomous end nodes). All nodes are able to select SF, TP and CF using a computational intelligence. The first step is to experiment only with small set of parameters, preferrably only SF will be considered. This decision-making process should be implemented on both sides of network server and end nodes.
2) **Collision mitigation using a carrier sensing mechanism.** To enhance learning process and mitigate collisions, a preamble detection algorithm will be implemented. This point only makes sense in scenarios when nodes are placed in a close proximity to each other.
3) **Simulators taking into account LoRa limitations and energy restrictions.** Usage of existing simulators to create a tool for reliable scalability tests and energy consumption evaluation of devices supporting LoRa@FIIT protocol.

V. Conclusion

LoRa is an emerging technology that has potential for LPWAN real-world deployment. However, it is not prepared for the harsh network environment of smart cities where hundreds of nodes are connected. Adaptive data rate does not perform well with mobile nodes and as a result a number of collisions in the net-work is rising, which is draining a limited power supply of end nodes. We pro-pose replacing adaptive data rate algorithm with multi-armed bandit alternatives to be more effective both in terms of packet delivery (and overall network reliability) and energy efficiency. We propose a network architecture consisting of a real-world network server and simulated access point with around one hundred end nodes constantly on the move to evaluate simple, yet promising Thompson Sampling algorithm. In the future, we plan to add capture effect and inter-SF collision to make a scenario closer to reality and test other multi-armed bandit

algorithm, not only using a simulator but using a real hardware and physical obstacles.

ACKNOWLEDGMENT

This research was partially supported by the Slovak University of Technology and the Ministry of Education, Science, Research and Sport of the Slovak Repub-lic, within the project ITMS 313021X329, co-funded by the European Regional Development Fund.

REFERENCES

[1] D. Howe, "Foldoc - computing dictionary." [Online]. Available: https://foldoc.org/

[2] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A survey on 5g networks for the internet of things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.

[3] J. Pullmann and D. Macko, "Increasing energy efficiency by minimizing collisions in long-range iot networks," in *2019 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 2019, pp. 178–181.

[4] E. M. Rochester, A. M. Yousuf, B. Ousat, and M. Ghaderi, "Lightweight carrier sensing in lora: Implementation and performance evaluation," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[5] Y. Hou, Z. Liu, and D. Sun, "A novel mac protocol exploiting concurrent transmissions for massive lora connectivity," *Journal of Communications and Networks*, vol. 22, no. 2, pp. 108–117, 2020.

[6] A. Research, "Lorawan® and nb-iot: Competitors or complementary?" [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/cr-lora-102_lorawanr_and_nb-iot.pdf

[7] R. Kerkouche, R. Alami, R. Féraud, N. Varsier, and P. Maillé, "Node-based optimization of lora transmissions with multi-armed bandit algorithms," in *2018 25th International Conference on Telecommunications (ICT)*, 2018, pp. 521–526.

[8] R. M. Sandoval, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "Optimizing and updating lora communication parameters: A machine learning approach," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 884–895, 2019.

[9] T.-H. To and A. Duda, "Simulation of lora in ns-3: Improving lora performance with csma," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[10] D.-T. Ta, K. Khawam, S. Lahoud, C. Adjih, and S. Martin, "Lora-mab: A flexible simulator for decentralized learning resource allocation in iot networks," in *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2019, pp. 55–62.

[11] A. Valach and D. Macko, "Improvement of lora communication scalability using machine learning based adaptiveness," May 2021. [Online]. Available: https://www.techrxiv.org/articles/preprint/Improvement_of_LoRa_Communication_Scalability_using_Machine_Learning_Based_Adaptiveness/14627028/1

[12] M. Bor and U. Roedig, "Lora transmission parameter selection," in *2017 13th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2017, pp. 27–34.

[13] 4TU.Federation, "Smart sensors in asphalt." [Online]. Available: https://www.4tu.nl/bouw/en/Lighthouse/Smart\%20Sensors\%20in\%20Asphalt/

[14] R. Lorrain, "The future of 5g and lorawan." [Online]. Available: https://blog.semtech.com/the-future-of-5g-and-lorawan-friends-or-foes

[15] A. Gupta and M. Fujinami, "Battery optimal configuration of transmission settings in lora moving nodes," in *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, 2019, pp. 1–6.

[16] H. Dakdouk, E. Tarazona, R. Alami, R. Féraud, G. Z. Papadopoulos, and P. Maillé, "Reinforcement learning techniques for optimized channel hopping in ieee 802.15.4-tsch networks," in *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, ser. MSWIM '18. New York, NY, USA: Association for Computing Machinery, 2018, p. 99–107. [Online]. Available: https://doi.org/10.1145/3242102.3242110

[17] R. M. Sandoval, A.-J. Garcia-Sanchez, J. Garcia-Haro, and T. M. Chen, "Optimal policy derivation for transmission duty-cycle constrained lpwan," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 3114–3125, 2018.

[18] R. Bonnefoi, L. Besson, C. Moy, E. Kaufmann, and J. Palicot, "Multi-armed bandit learning in iot networks: Learning helps even in non-stationary settings," in *Cognitive Radio Oriented Wireless Networks*, P. Marques, A. Radwan, S. Mumtaz, D. Noguet, J. Rodriguez, and M. Gundlach, Eds. Cham: Springer International Publishing, 2018, pp. 173–185.

[19] D.-T. Ta, K. Khawam, S. Lahoud, C. Adjih, and S. Martin, "Lora-mab: Toward an intelligent resource allocation approach for lorawan," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[20] E. Sallum, N. Pereira, M. Alves, and M. Santos, "Performance optimization on lora networks through assigning radio parameters," in *2020 IEEE International Conference on Industrial Technology (ICIT)*, 2020, pp. 304–309.

[21] A. Valach and D. Macko, "Optimization of lora devices communication for applications in healthcare," in *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, 2020, pp. 511–514.

[22] Y. Li, J. Yang, and J. Wang, "Dylora: Towards energy efficient dynamic lora transmission control," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 2312–2320.

[23] C. Orfanidis, K. Dimitrakopoulos, X. Fafoutis, and M. Jacobsson, "Towards battery-free lpwan wearables," in *Proceedings of the 7th International Workshop on Energy Harvesting and Energy-Neutral Sensing Systems*, ser. ENSsys'19. New York, NY, USA: Association for Computing Machinery, 2019, p. 52–53. [Online]. Available: https://doi.org/10.1145/3362053.3363488

[24] T. Bouguera, J.-F. Diouris, J.-J. Chaillout, R. Jaouadi, and A. Guillaume, "Energy consumption model for sensor nodes based on lora and lorawan," *Sensors*, vol. 18, p. 2104, 06 2018.

[25] S. Cui and I. Joe, "Collision prediction for a low power wide area network using deep learning methods," *Journal of Communications and Networks*, vol. 22, no. 3, pp. 205–214, 2020.

[26] Y. Ishida, D. Nobayashi, and T. Ikenaga, "Experimental performance evaluation of the collisions in lora communications," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2018, pp. 1032–1035.

[27] C. Moy and L. Besson, "Decentralized spectrum learning for iot wireless networks collision mitigation," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 644–651.

[28] P. Auer, N. Cesa-Bianchi, and P. Fischer, "Finite-time analysis of the multiarmed bandit problem," *Mach. Learn.*, vol. 47, no. 2–3, p. 235–256, May 2002. [Online]. Available: https://doi.org/10.1023/A:1013689704352

[29] O. Perešíni and T. Krajčovič, "More efficient iot communication through lora network with lora@fiit and stiot protocols," in *2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT)*, 2017, pp. 1–6.

[30] Semtech, "What are lora® and lorawan®." [Online]. Available: https://lora-developers.semtech.com/library/tech-papers-and-guides/lora-and-lorawan

[31] K. Hill, K. K. Gagneja, and N. Singh, "Lora phy range tests and software decoding - physical layer security," in *2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)*, 2019, pp. 805–810.

[32] O. Perešíni, K. Cagáň, and A. Valach, "Lora network server." [Online]. Available: https://github.com/alexandervalach/lora-network-server

[33] S. Štefunko, "Lora@fiit arduino library." [Online]. Available: https://github.com/alexandervalach/lorafiit-library

[34] E. M. Galas and B. D. Gerardo, "Feasibility assessment on the implementation of the enhanced xxtea on iot devices," in *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, 2019, pp. 178–182.

[35] L. Alliance, "Lorawan® specification v1.0.4." [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-104-specification-package/

[36] ——, "Lorawan certification protocol specification ts009-1.0.0," 2020.

[37] ——, "Lorawan 1.0.4 end device rf performance for all regions v1.0," 2020.

[38] ——, "Lorawan ts1-1.0.4 l2 specification."

[39] O. Chapelle and L. Li, "An empirical evaluation of thompson sampling," *NIPS*, 01 2011.

[40] A. Gloria, C. Dionisio, G. Simões, and P. Sebastião, "Lora transmission power self con?guration for low power end devices," in *2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2019, pp. 1–6.

[41] R. Alami, O.-A. Maillard, and R. Feraud, "Memory bandits: a bayesian approach for the switching bandit problem," in *NIPS 2017 - 31st Conference on Neural Information Processing Systems*, 12 2017.

[42] J. Mellor and J. Shapiro, "Thompson sampling in switching environments with bayesian online change detection," in *Proceedings of the Sixteenth International Conference on Artificial Intelligence and Statistics*, ser. Proceedings of Machine Learning Research, C. M. Carvalho and P. Ravikumar, Eds., vol. 31. Scottsdale, Arizona, USA: PMLR, May 2013, pp. 442–450. [Online]. Available: http://proceedings.mlr.press/v31/mellor13a.html

[43] R. M. Sandoval, D. Rodenas-Herraiz, A.-J. Garcia-Sanchez, and J. Garcia-Haro, "Deriving and updating optimal transmission configurations for lora networks," *IEEE Access*, vol. 8, pp. 38 586–38 595, 2020.

[44] A. Valach, "Lora@fiit access point and end nodes simulator," 2021. [Online]. Available: https://github.com/alexandervalach/lora-ap-sim

Autorský rejstřík

Název	Sborník příspěvků PAD 2021
Autor	Ing. Martin Rozkovec, Ph.D.
	prof Ing. Zdeněk Plíva, Ph.D.
	Ostatní autoři příspěvků
Vydavatel	Technická univerzita v Liberci
	Studentská 1402/2, Liberec
Schváleno	Rektorátem TUL dne 17. 1. 2022, čj. RE 3/22
Vyšlo	v lednu 2022
Vydání	1.
ISBN	978-80-7494-592-2
Č. publikace	55-003-22

Tato publikace neprošla redakční ani jazykovou úpravou