

Používateľská dokumentácia

GUI

Vypracoval: Bc. Veronika Satinová

Obsah

Zoznam obrázkov	3
1 Ako obsluhovať GUI?	5
1.1 Časť pre načítanie, spracovanie a uloženie dát	5
1.1.1 Zobrazené načítané a navzorkované vstupné dáta.....	8
1.1.2 Možnosť uloženia si načítaných a spracovaných dát	9
1.1.3 Upravenie vstupu pre IMPORT.....	11
1.2 Funkcie	13
1.3 Funkcie 3D	15
1.4 Testovanie metód	16
2 Predikčné tunely	18
2.1 Implementácia	18
2.2 Načítanie vstupného súboru	18
2.3 Výber nastavení pre výpočet niektorého z tunelov	20
2.3.1 Výber tunela	20
2.3.2 Nastavenie stupňa polynómu.....	20
2.3.3 Kalibrácia	21
2.3.4 Vyhľadanie.....	21
2.3.5 Zvyšné nastavenia	21
2.3.6 Vypočítať	22
2.4 Vyhodnotenia	22
2.5 Vypočítaný tunel	22

Zoznam obrázkov

Obrázok 1 Náhľad prvej časti GUI.....	5
Obrázok 2 Nastavovanie hodnoty pre vzorkovacie okno	6
Obrázok 3 Informačný banner pri načítavaní vstupného súboru	6
Obrázok 4 Proces vzorkovania načítaných vstupných dát.....	7
Obrázok 5 Načítané dáta z PCAP súboru	8
Obrázok 7 Informácie pred načítaním a spracovaním vstupného súboru.....	8
Obrázok 7 Zobrazené informácie o načítaných dátach.....	8
Obrázok 8 Tlačidlá pre uloženie vstupných dát pre ich opätovné použitie	9
Obrázok 9 Tlačidlá pre uloženie navzorkovaných dát pre ich opätovné použitie	9
Obrázok 10 Možnosť si zobrazit' histogram	10
Obrázok 11 Spôsob ako si uložiť graf	10
Obrázok 12 Funkcionalita pre úpravu dát.....	11
Obrázok 13 Okno pre editovanie dát	11
Obrázok 14 Okno s načítanými dátami pre editovanie.....	12
Obrázok 15 Menu s funkciami.....	13
Obrázok 16 Okno pre výpočet funkcie	13
Obrázok 17 Prenásobený parameter koeficientom 2	14
Obrázok 18 Menu pre Funkcie 3D	15
Obrázok 19 3D graf s vypočítanými hodnotami parametra entropia.....	15
Obrázok 20 Položka v MENU: Testovanie metód	16
Obrázok 21 Okno pre testovanie metód	16
Obrázok 22 Metódy pre testovanie	16
Obrázok 23 Prepočítané parametre: variabilnosť, šikmosť, špicatosť.....	17
Obrázok 24 3. časť GUI – predikčné tunely	18
Obrázok 25 Panel pre načítanie vstupného súboru pre tunely	19
Obrázok 26 Načítaný parameter s časom útoku	19
Obrázok 27 Zobrazené tlačidlo „Vypočítat“	20
Obrázok 28 Voľba tunelu	20
Obrázok 29 Šírka predikčného intervalu	20
Obrázok 30 Kalibrácia	21
Obrázok 31 Vyhladenie	21

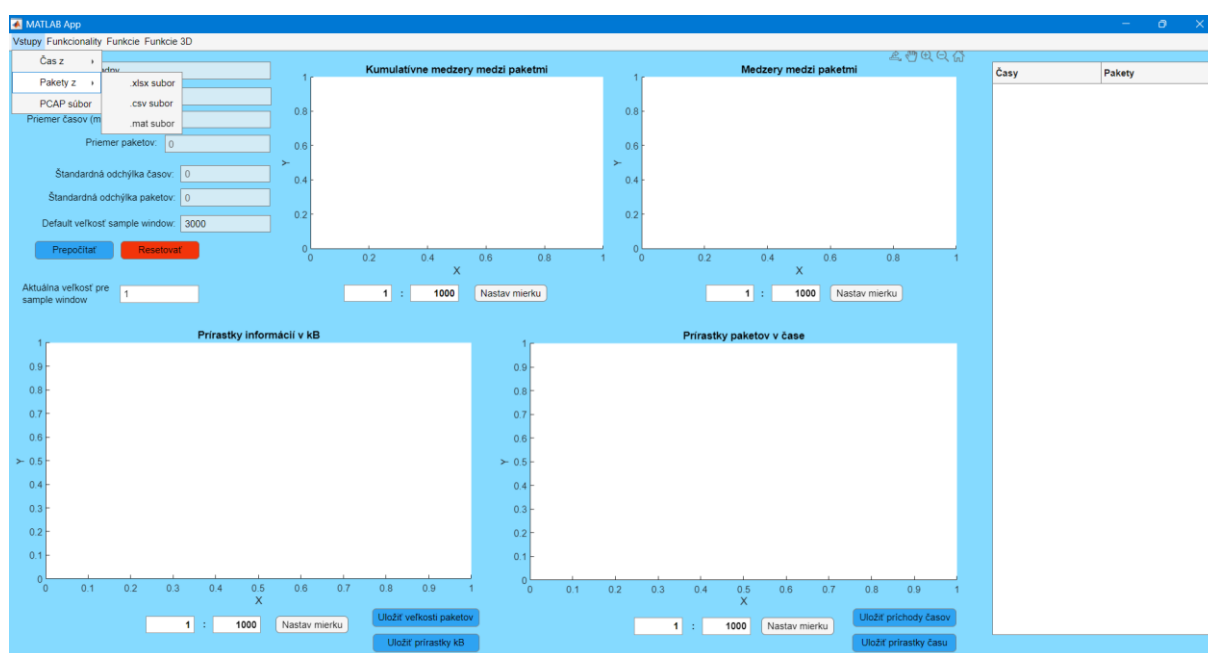
Obrázok 32 Ďalšie nastavenia.....	21
Obrázok 33 Vyhodnotenie tunela	22
Obrázok 34 Vykreslené tunely pri použití metódy AR(m,n).....	22

1 Ako obsluhovať GUI?

V ZIP súbore sa nachádza všetko potrebné pre spustenie GUI. Spustíte ho po kliknutí na „app.mlapp“ súbor a pokiaľ nemáte spustený Matlab po kliknutí na tento súbor sa vám automaticky spustí.

Používateľské grafické prostredie sa skladá z 3 hlavných častí:

1.1 Časť pre načítanie, spracovanie a uloženie dát



Obrázok 1 Náhľad prvej časti GUI

Ako môžete vidieť v časti hlavného menu pod položkou **Vstupy** si môžete načítať vaše dáta. **Pozor:** tieto dáta sa myslia tie nespracované, nenavzorkované. Ako vstup môžete použiť priamo PCAP súbor, MAT súbor, XLSX súbor alebo CSV súbor.

POZOR: pri načítaní času z (MAT, CSV alebo XLSX) súboru musia byť dáta v správnom formáte. Správny formát pre načítanie času sa myslí stĺpec prichádzajúcich časov pod sebou v riadkoch.

Ďalej ak načítavam pakety, správny formát sa myslia 2 stĺpce, z toho 1. stĺpec sú prichádzajúce časy a 2. stĺpec sú už veľkosti paketov v kB. **Nemôže to byť opačne!**

Na ukážku sme pripravili vstupné dáta vo všetkých formátoch, takže ak by bol nejaký problém pri načítavaní vstupných dát, upriamte prosím svoju pozornosť na tieto

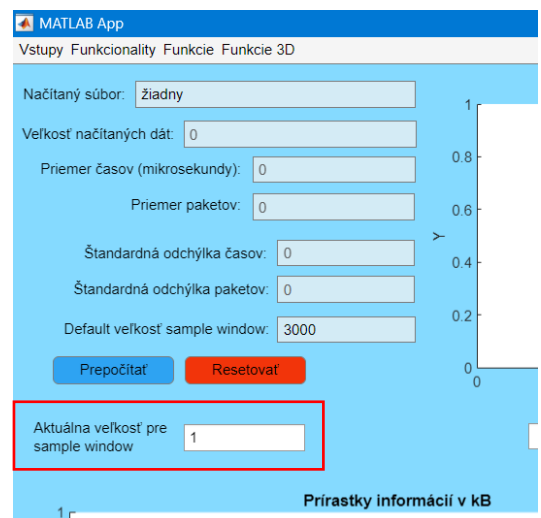
vybrané súbory a na formát s ktorým chcete pracovať. Sú uložené v priečinku GUI/ukážkové_vstupné_dáta.

Ak chcete načítať celý PCAP súbor, všetky grafy budú obsahovať dáta, rovnako ak by ste načítali aj pakety. Ak načítate iba časy, dáta budú zobrazené na všetkých grafoch okrem grafu **Prírastky informácií v kB**.

Vpravo sa nachádza tabuľka, ktorá bude zobrazovať vaše načítané dáta, aby ste vedeli, čo sa vám načítalo a taktiež je to pomôcka toho, aby ste vedeli aké veľké vzorkovacie okno zvoliť pre správne zobrazenie vašich načítaných dát. Ak by ste na začiatku zvolili nevhodné vzorkovacie okno je možné zvoliť nové a ak stlačíte tlačidlo „**Prepočítať**“ tak sa vám dáta znovu načítajú s novým vzorkovacím oknom.

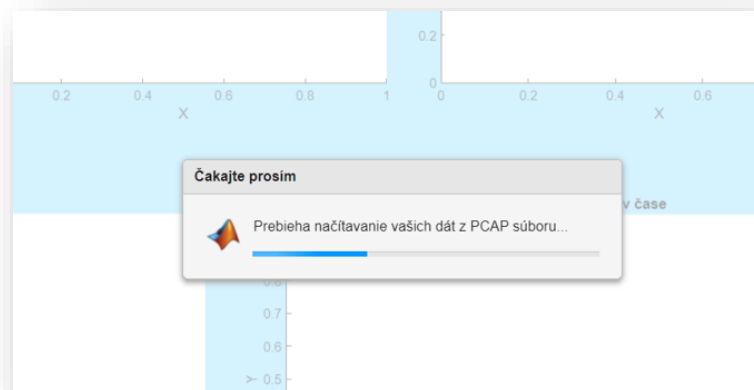
Po načítaní prebehne slotovanie dát.

Pred tým ako načítate vstup sa ubezpečte, že ste zadali hodnotu pre vzorkovacie okno v tomto Edit Fielde:



Obrázok 2 Nastavovanie hodnoty pre vzorkovacie okno

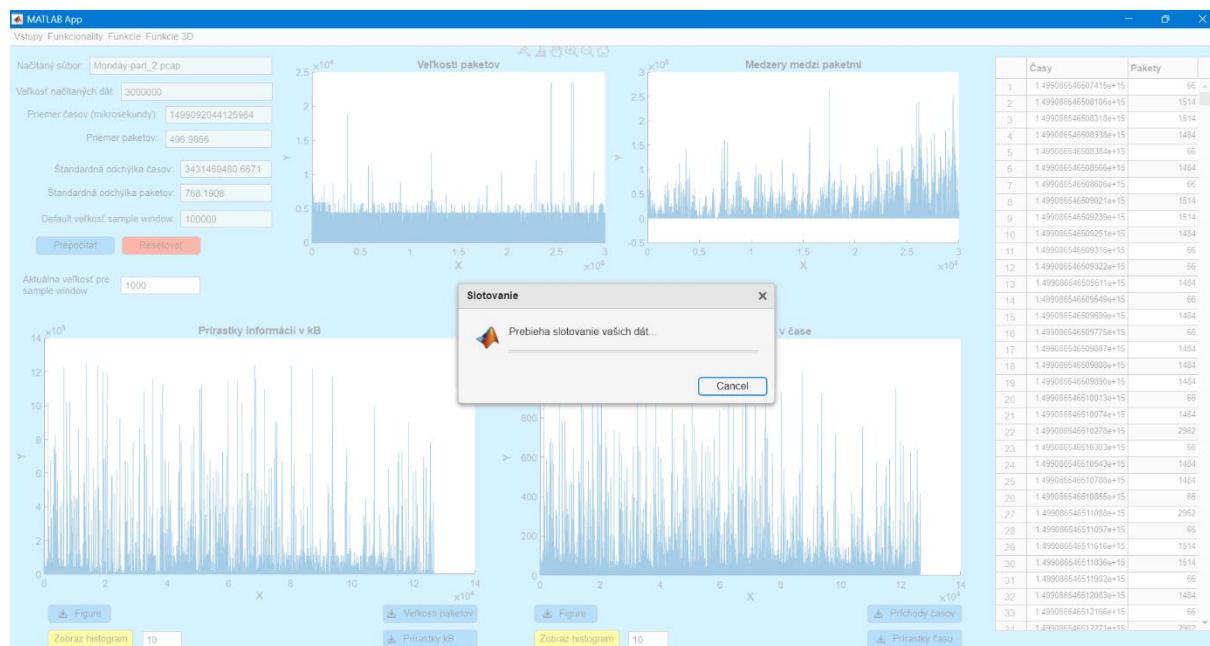
GUI vás bude sprevádzať počas všetkých operácií, kde vás upozorní čo sa práve deje. Ak zvolíte ako vstupný súbor napríklad PCAP, GUI vám zobrazí, že prebieha načítavanie vašich dát z PCAP súboru:



Obrázok 3 Informačný banner pri načítavaní vstupného súboru

Načítavanie väčších vstupných súborov môže zaberať niekoľko minút, takže pokiaľ sa vám stále zobrazuje banner nezúfajte, dáta sa totiž stále načítavajú a je potrebné počkať. Táto doba čakania závisí najmä od výkonu vášho zariadenia, veľkosti RAM a hlavne veľkosti zvoleného vstupného súboru. Počas testovania GUI sme skúšali vložiť PCAP súbory, ktoré boli veľké cez 3 Giga a Matlab nám ich v poriadku načítal za zhruba 15-20 minút. Ubezpečíme vás, že len načítanie takéhoto veľkého súboru trvá dlhšie. Už samotné vzorkovanie dát trvá zlomok sekundy oproti načítavaniu tak veľkého vstupného súboru. Pre tých, ktorým sa nechce tak dlho čakať pre načítanie vstupného súboru, odporúčame si PCAP rozkúskovať na menšie súbory.

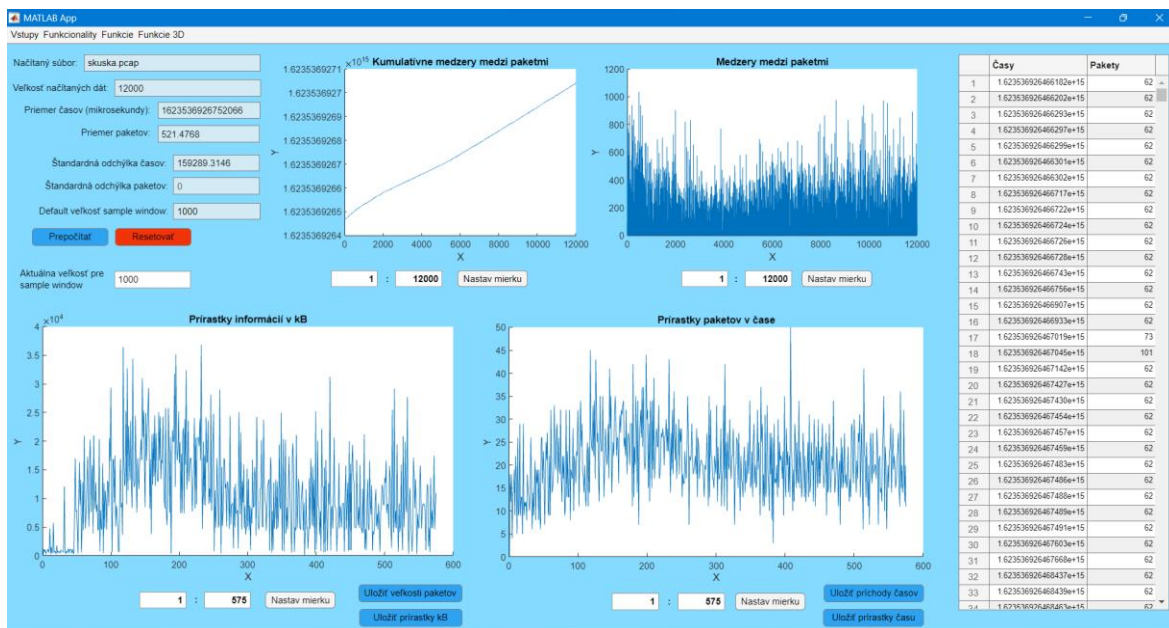
Ak sa vám už načítali dáta zo vstupného súboru, GUI vás ďalej upozorní, že sa začalo vzorkovanie vašich načítaných dát. Trvanie vzorkovania trvá iba pár sekúnd:



Obrázok 4 Proces vzorkovania načítaných vstupných dát

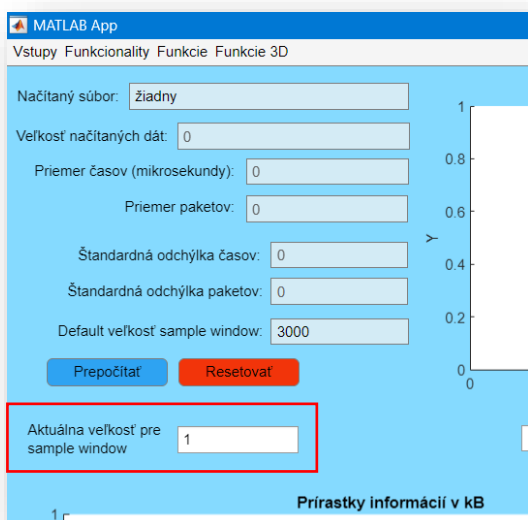
Tak tiež odporúčame si načítané dáta ukladať (spôsob ich ukladania ukážeme v nasledujúcich krokoch), aby ste už druhýkrát nemuseli načítavať veľký vstupný súbor a v pokoji ste si mohli znovu načítať dáta v podobe časov alebo paketov.

1.1.1 Zobrazené načítané a navzorkované vstupné dáta

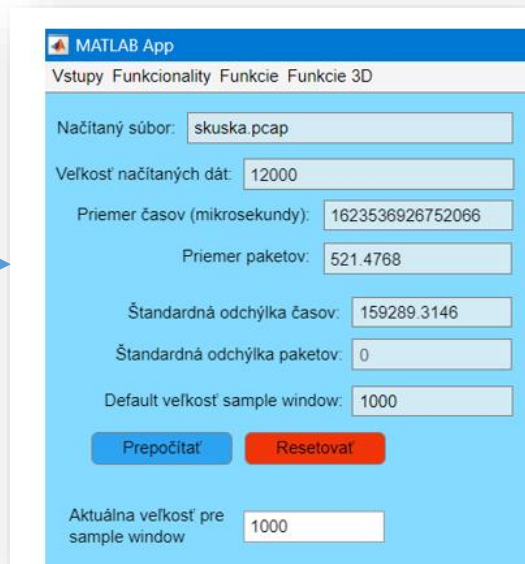


Obrázok 5 Načítané dáta z PCAP súboru

Po načítaní vstupu budete v tejto časti vidieť základné informácie o dátach, ktoré ste načítali:



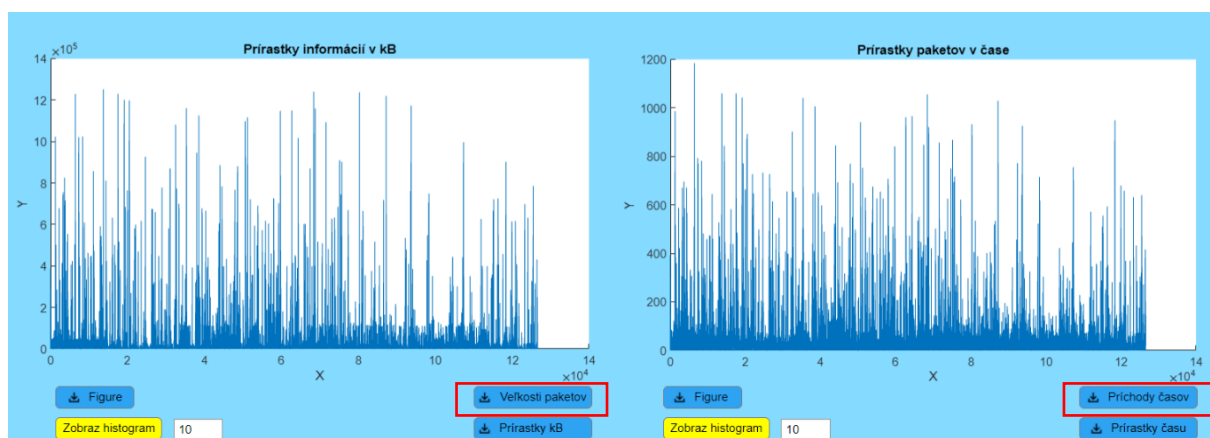
Obrázok 7 Informácie pred načítaním a spracovaním vstupného súboru



Obrázok 7 Zobrazené informácie o načítaných dátach

1.1.2 Možnosť uloženia si načítaných a spracovaných dát

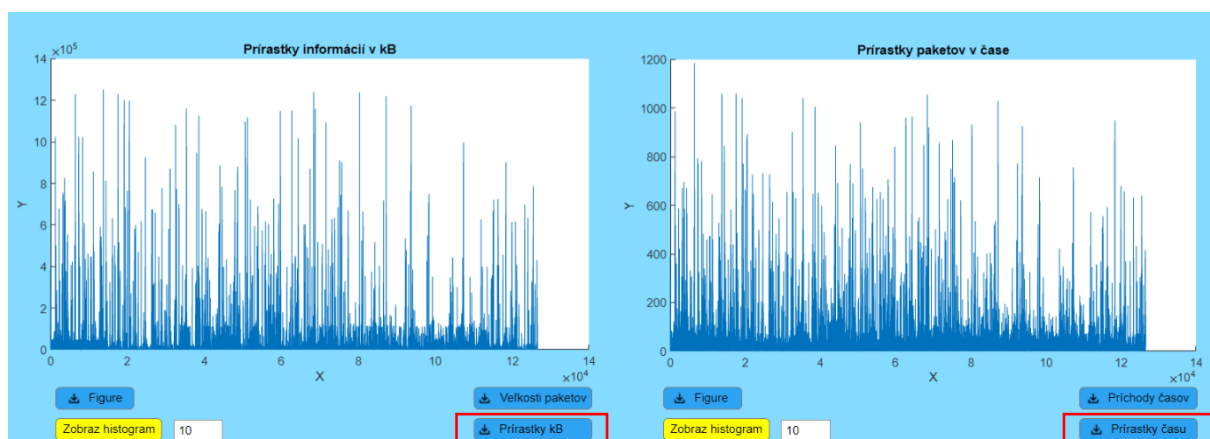
Ak máte ako používateľ zobrazené načítané dáta, môžete si ich stiahnuť cez červenou farbou vyznačené tlačidlá. Stiahnete si cez ne načítané vstupné dáta, ktoré nie sú spracované, čiže nie sú navzorkované a ak si ich stiahnete potom ich môžete znovu použiť, napríklad pre znovu načítanie dát s inou veľkosťou vzorkovacieho okna bez toho, aby ste znovu načítavali veľký PCAP súbor.



Obrázok 8 Tlačidlá pre uloženie vstupných dát pre ich opätovné použitie

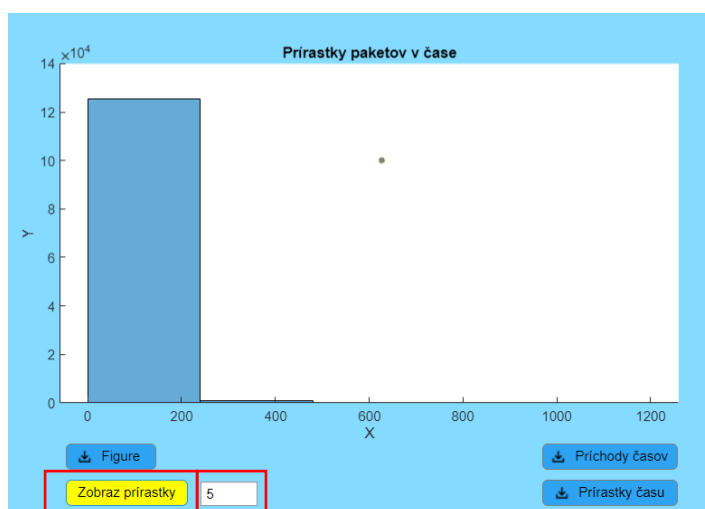
Takéto uložené dáta sa ukladajú vo formáte MAT.

Vďaka nasledujúcemu obrázku, kde sú zobrazené zvýraznené ďalšie 2 tlačidlá si ako používateľ stiahnete už navzorkované/naslotované dáta (spracované), ktoré potom budete používať v ostatných častiach, napr.: v časti Parametre, kde uvidíte ako vám zvolený parameter reaguje na vaše navzorkované dáta.



Obrázok 9 Tlačidlá pre uloženie navzorkovaných dát pre ich opätovné použitie

Cez tlačidlo **Zobraz histogram** je možnosť si zobrazit' dáta ako histogram. Ak kliknete na toto tlačidlo automaticky sa vám zobrazí histogram z dát a toto tlačidlo sa premenuje na **Zobraz prírastky**, aby ste sa vedeli prepínať medzi prírastkami a histogramom. Je tiež možné si zvolit' koľko tried má histogram zobrazit' cez Edit Field hneď vedľa tohto tlačidla:



Obrázok 10 Možnosť si zobrazit' histogram

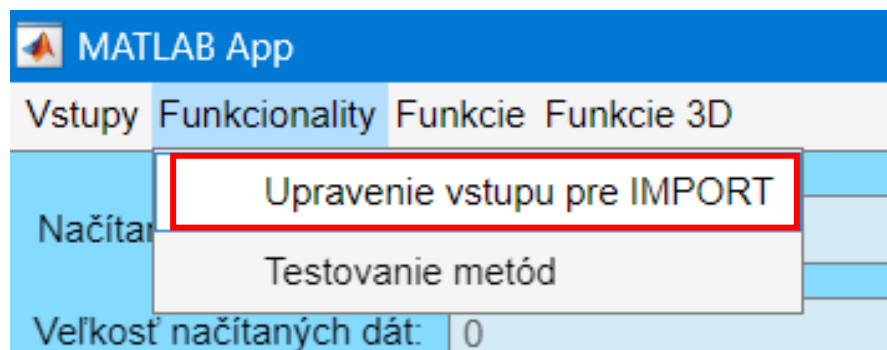
Pomocou tlačidla **Figure** si viete zobrazený graf uložit' vo formáte .fig :



Obrázok 11 Spôsob ako si uložit' graf

1.1.3 Upravenie vstupu pre IMPORT

V tejto časti je dôležitá práve úprava vstupu pre import. Pomocou tejto funkcionality si môžete načítať **iba MAT** súbor a ten si potom strihať na menšie časti alebo odstrihnúť nepotrebnú časť a vytvoriť tak nový súbor.



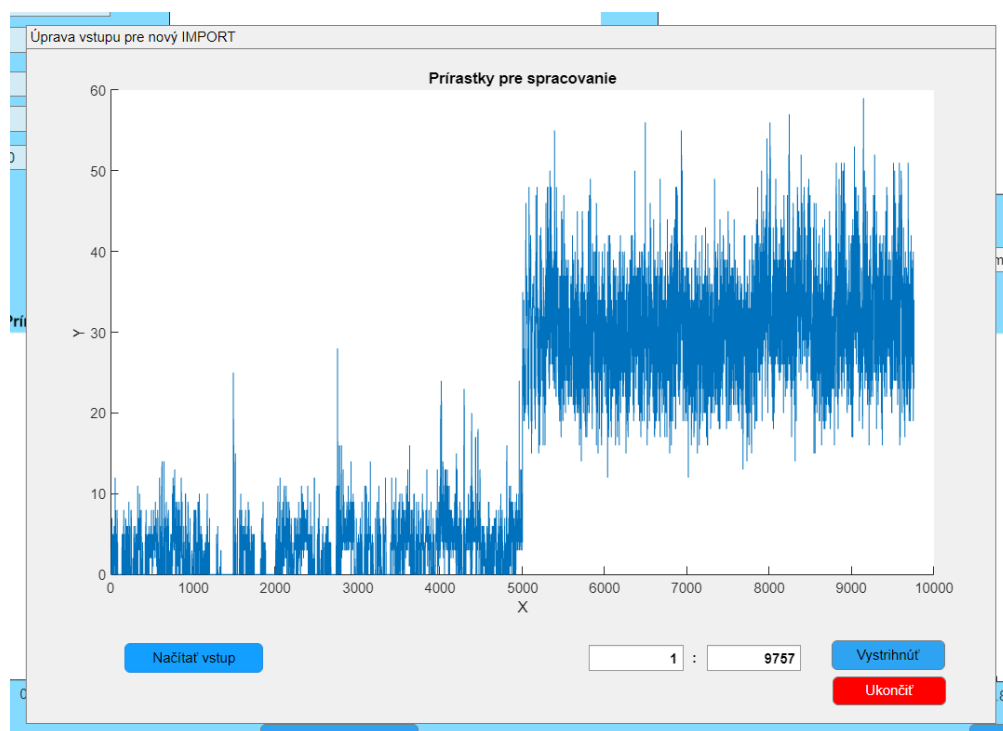
Obrázok 12 Funkcionalita pre úpravu dát

Po kliknutí v menu na: **Upravenie vstupu pre IMPORT** sa vám otvorí nasledujúce okno:



Obrázok 13 Okno pre editovanie dát

Cez tlačidlo **Načítať vstup** si vložíte dáta pre editovanie (pozor: iba MAT súbor sa dá načítať) a potom sa vám zobrazí nasledujúci graf:



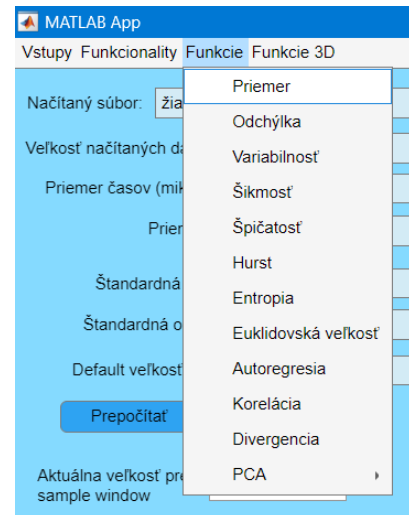
Obrázok 14 Okno s načítanými dátami pre editovanie

Ako ste si mohli všimnúť dole pod grafom sú hodnoty od 1 po 9757. Je to dĺžka na osi X, po ktorú môžete strihať tieto načítané dáta. Ak do týchto okien zadáte napr. 200:6000 a následne kliknete na tlačidlo **Vystrihnúť** zobrazí sa vám prehľadavacie okno kam chcete, aby sa vám tieto vystrihnuté dáta potom v podobe MAT súboru uložili. Ak vyberiete priečinok, do ktorého sa vám to uloží, môžete toto okno zavrieť a pracovať potom s novým mat súborom.

1.2 Funkcie

Vďaka tejto ponuke v menu sa presuniete na nové okno, kde bude treba načítať vstup, v podobe MAT súboru, kedy načítavate už naslotované/navzorkované dáta.

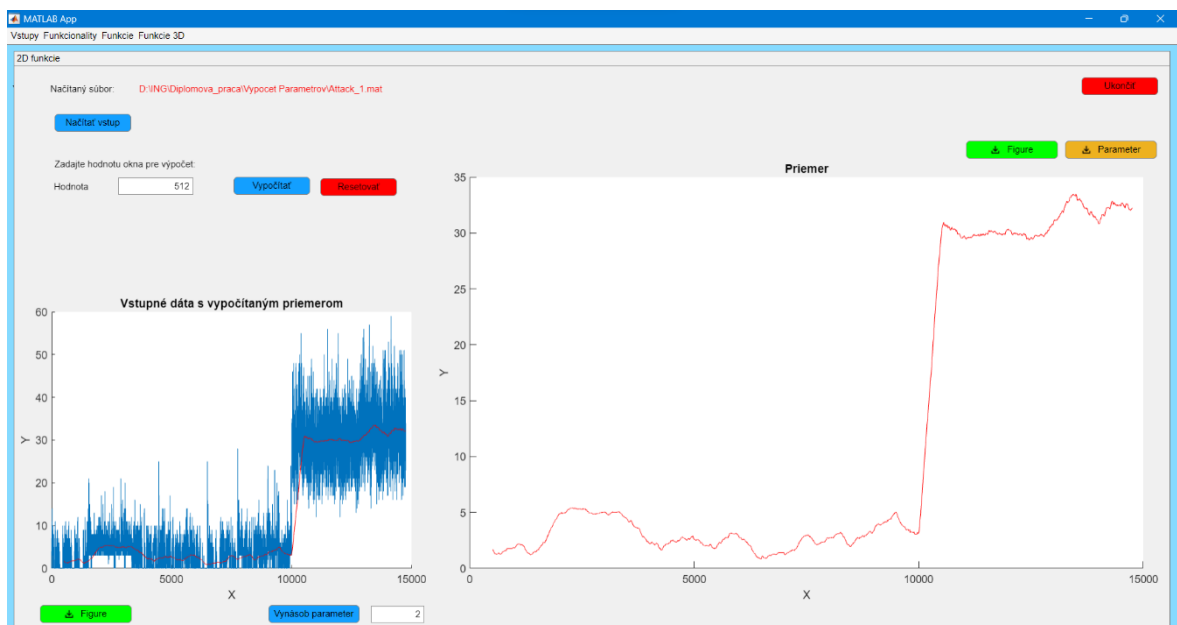
Pripravili sme pre vás aj vzorky navzorkovaných dát, ktoré sa nachádzajú v priečinku „*GUI/Naslotované_dáta_útoky*“.



Obrázok 15 Menu s funkciami

Po tom ako si zvolíte, s ktorou funkciou si chcete zobraziť dáta sa vám zobrazí nasledujúce okno:

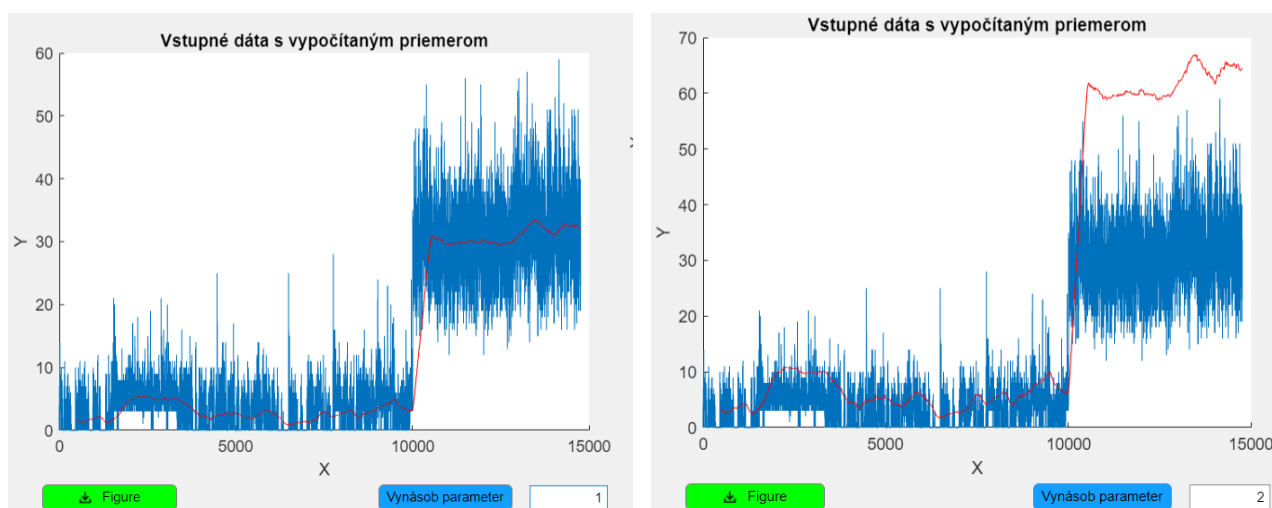
Pre príklad sme zvolili funkciu priemer. Vľavo hore je tlačidlo **Načítať vstup**, cez ktoré si načítate vstupné dáta (**pozor:** dáta musia byť naslotované/navzorkované v formáte MAT).



Obrázok 16 Okno pre výpočet funkcie

Ďalej sa tu nachádza Edit Field, v ktorom je počiatočná hodnota výpočtového okna pre funkciu 512, ale viete si ju samozrejme aj zmeniť. Potom už len kliknete na tlačidlo **Vypočítat'** a po chvíli sa vám zobrazia prepočítané dáta cez funkciu priemer. Vypočítané hodnoty si viete zmazať cez tlačidlo **Resetovať'** a následne môžete opäť vykonať výpočet s napríklad iným výpočtovým oknom, ktoré zadáte cez Edit Field. Rovnako si viete uložiť, či už grafy v podobe figure alebo aj hodnoty vypočítaného parametra cez oranžové tlačidlo **Parameter**.

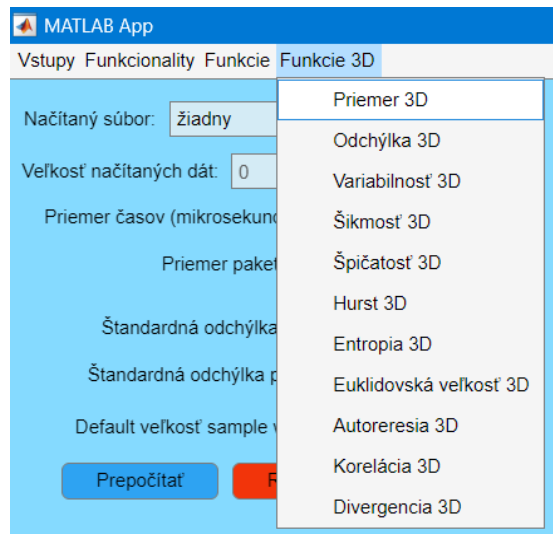
Pre lepšiu vizualizáciu dát a vypočítaného parametra slúži menší graf vľavo, ktorého hodnoty parametra sa dajú prenásobiť ľubovoľným koeficientom, aby bolo zrejmé ako parameter reagoval na dáta.



Obrázok 17 Prenásobený parameter koeficientom 2

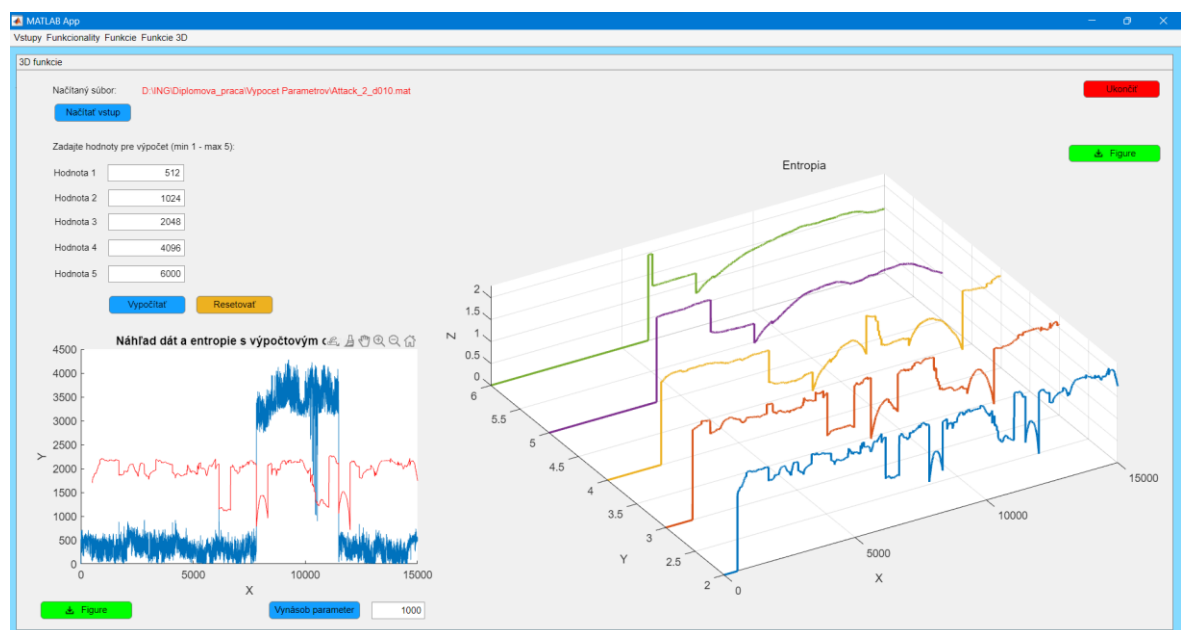
1.3 Funkcie 3D

Táto časť funguje principiálne rovnako ako predošlá časť Funkcie, akurát sa tu nenachádza možnosť si uložiť hodnoty vypočítaného parametra. Po kliknutí na konkrétnu funkciu sa vám zobrazí okno a môžete naraz zadávať viacero vstupných hodnôt pre parameter *výpočtové okno* na vypočítanie danej funkcie.



Obrázok 18 Menu pre Funkcie 3D

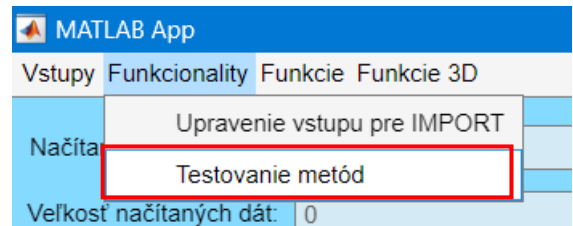
Po kliknutí v časti menu Funkcie 3D sa vám zobrazí nasledujúce okno, kde si zadáte vstup (**naslotované/navzorkované dáta v podobe MAT súboru**), zvolíte si vstupné parametre pre výpočtové okno pre danú funkciu a následne kliknete na tlačidlo **Vypočítať**. Po chvíli sa vám zobrazí 3D graf, s ktorým môžete hýbať a otáčať ho do ľubovoľného smeru a ktorý obsahuje prepočítané dáta. Vľavo je opäť menší graf, ktorý vám ukáže aj ako táto funkcia reaguje na vašich dátach, na ktoré bolo použité výpočtové okno s hodnotou 512.



Obrázok 19 3D graf s vypočítanými hodnotami parametra entropia

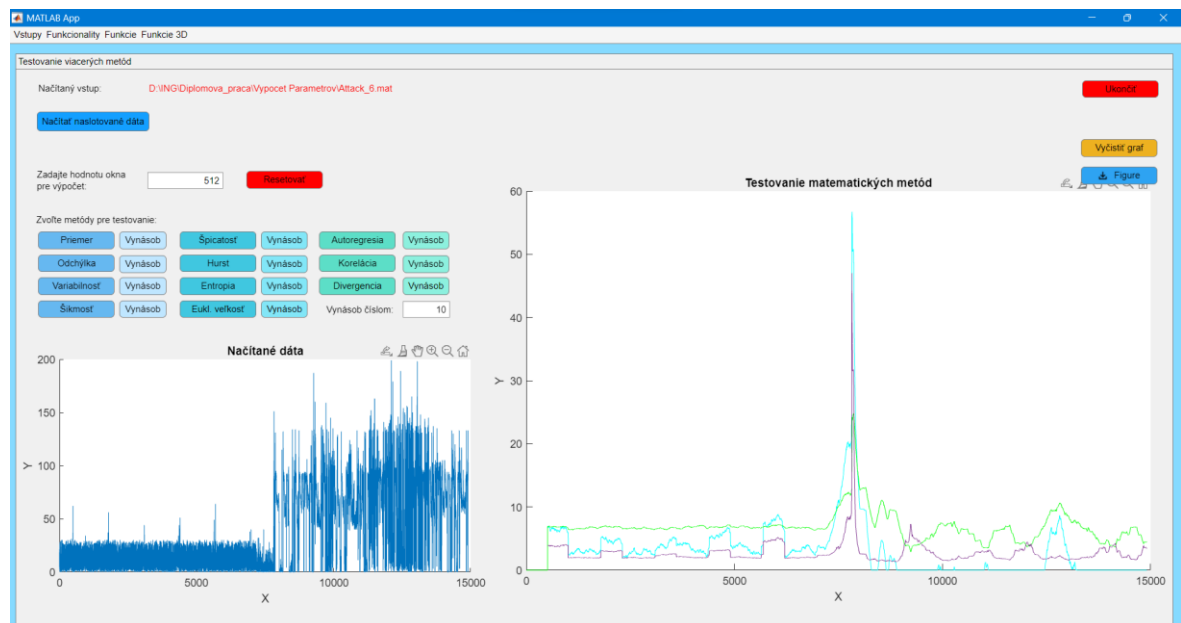
1.4 Testovanie metód

V rámci GUI sme vytvorili pre používateľa možnosť si vizualizovať reakciu viacerých parametrov súčasne. Pre takúto funkcionality slúži položka v menu **Testovanie metód**.



Obrázok 20 Položka v MENU: Testovanie metód

Po kliknutí na túto položku sa používateľovi zobrazí nasledujúce okno:



Obrázok 21 Okno pre testovanie metód

Používateľ postupuje rovnakým spôsobom ako v predošlých prípadoch. Je potrebné si načítať naslotované/navzorkované dáta cez tlačidlo **Načítať naslotované dáta**. Následne sa zvolí veľkosť výpočtového okna cez Edit Field a potom sa klikne na niektorú z funkcií:



Obrázok 22 Metódy pre testovanie

Akonáhle sa klikne na niektoré z tlačidiel, z ktorých každé tlačidlo predstavuje výpočet niektorej z metód, na grafe sa zobrazí vypočítaný parameter v závislosti od vložených vstupných navzorkovaných dát. Ďalej môžeme kliknúť na tlačidlo s inou metódou a do grafu sa pridá ďalší prepočítaný parameter ako to môžeme vidieť na nasledujúcom obrázku:



Obrázok 23 Prepočítané parametre: variabilnosť, šikmosť, špicatosť

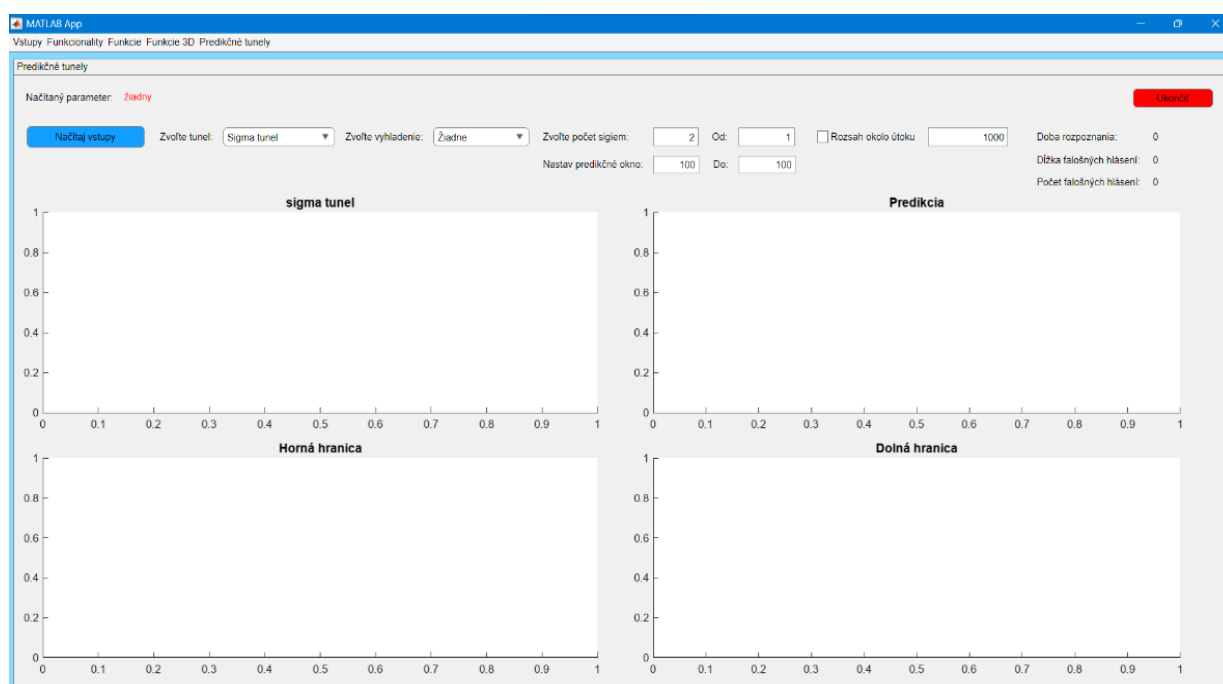
Opäť je možnosť si vynásobiť vypočítaný parameter ľubovoľným koeficientom, aby sme boli schopní lepšie vizualizovať dáta. Pokiaľ je graf zahltený rôznymi parametrami je možné si graf vyčistiť cez tlačidlo **Vyčistiť graf** a následne si znovu vykresliť vypočítané parametre.

2 Predikčné tunely

Táto časť bola implementovaná do GUI vďaka Eve Haluškovej a slúži na experimentovanie s predikčnými tunelmi.

2.1 Implementácia

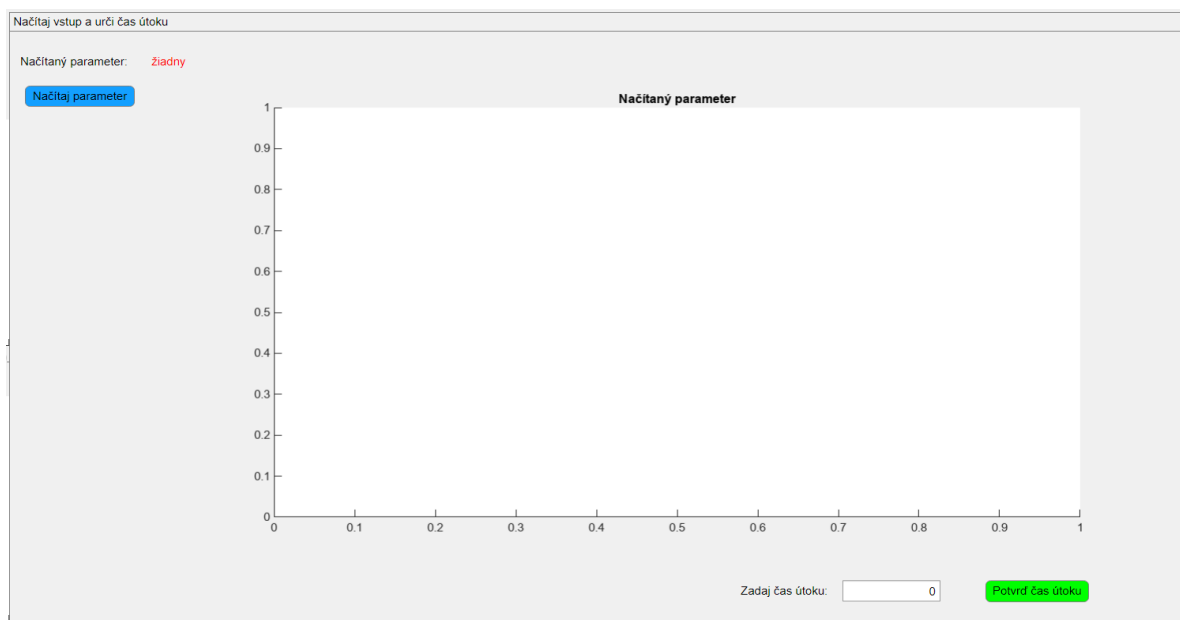
Celkový pohľad na túto časť vyzerá nasledovne a postupne v príručke preberieme všetky nastavenia.



Obrázok 24 3. časť GUI – predikčné tunely

2.2 Načítanie vstupného súboru

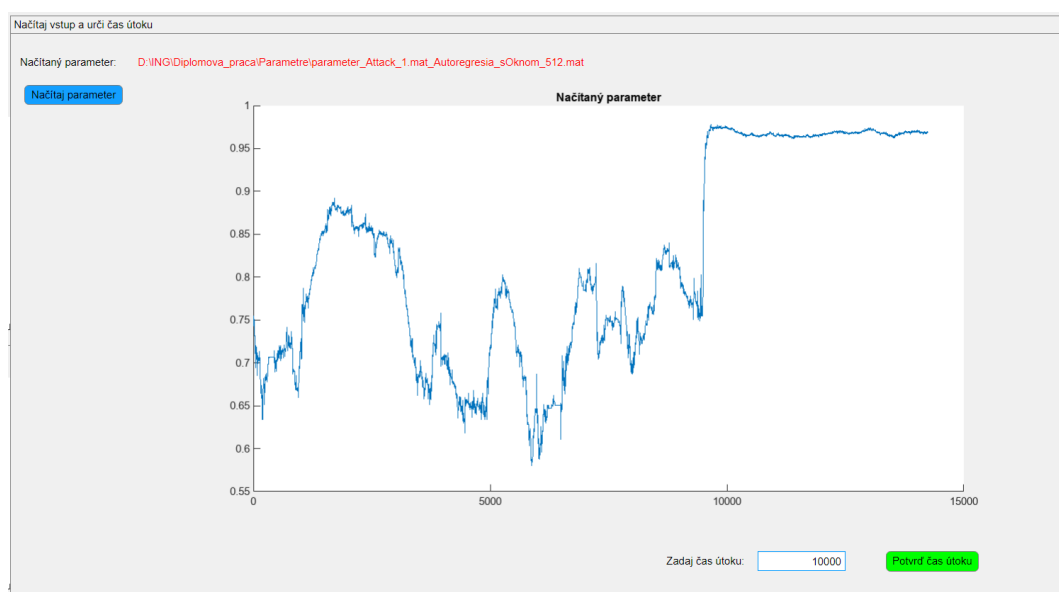
Vstupné dáta si používateľ môže načítať pomocou tlačidla „Načítaj vstupy“ a zobrazí sa mu nasledujúci panel:



Obrázok 25 Panel pre načítanie vstupného súboru pre tunely

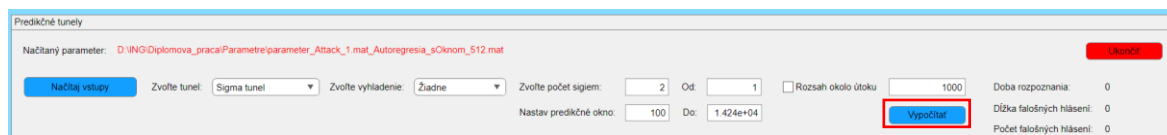
Po zobrazení tohto panelu musí používateľ vložiť vstupný súbor vo formáte .mat, cez tlačidlo „Načítaj parameter“. Načítané dáta musia byť dáta, ktoré sme získali z druhej časti GUI výpočtom skúmaného parametra. Po úspešnom načítaní dát sa v grafe „Načítaný parameter“ zobrazia načítané dáta a používateľ musí zadať čas útoku do edit fieldu „Zadaj čas útoku:“. Následne po zadaní hodnoty musí používateľ kliknúť na tlačidlo „Potvrď čas útoku“ a znovu sa mu otvorí predchádzajúci panel už s možnosťou si vypočítať niektorý z tunelov.

Pre príklad sme načítali autoregresný parameter a ako čas útoku sme zadali hodnotu 10000:



Obrázok 26 Načítaný parameter s časom útoku

Ak sa používateľovi podarí správne načítať súbor a zadať čas útoku vysvieti sa tlačidlo „Vypočítať“ modrou farbou:

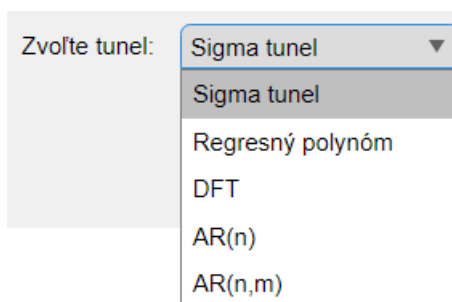


Obrázok 27 Zobrazené tlačidlo „Vypočítať“

2.3 Výber nastavení pre výpočet niektorého z tunelov

2.3.1 Výber tunela

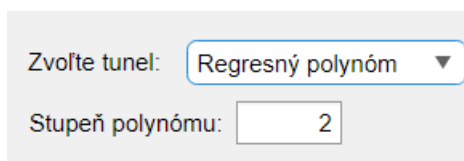
Používateľ si vyberá, ktorý predikčný tunel chce vytvoriť. Na výber má z niekoľkých možností: Sigma tunel, tunel tvorený pomocou regresného polynómu, tunel využívajúci diskretnú Fourierovu transformáciu a dva autoregresné tunely.



Obrázok 28 Voľba tunelu

2.3.2 Nastavenie stupňa polynómu

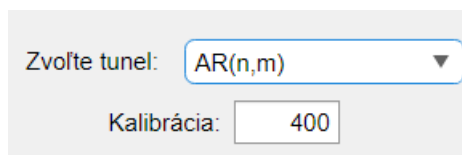
Používateľ si môže zvoliť stupeň polynómu pri počítaní regresného modelu, defaultne je táto hodnota nastavená na 2:



Obrázok 29 Šírka predikčného intervalu

2.3.3 Kalibrácia

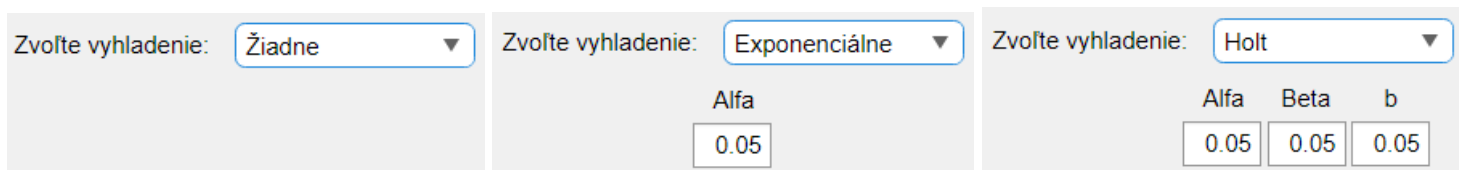
Pri autoregresnom tunely $AR(m,n)$ má používateľ možnosť dodatočne si zvoliť dĺžku radu na natréňovanie. Defaultne je táto hodnota nastavená na 400. Rada by som upozornila na to, že tvorba tunelu pomocou DFT a $AR(m,n)$ trvá o niečo dlhšie ako ostatné tunely, preto treba chvíľku počkať, kým sa načítajú obrázky.



Obrázok 30 Kalibrácia

2.3.4 Vyhladenie

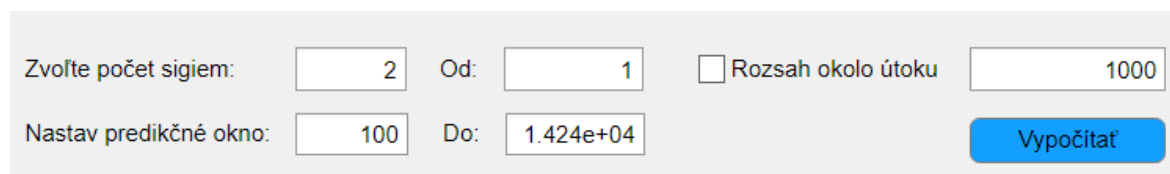
Používateľ si môže navoliť, či a aké vyhladenie chce na parameter použiť ešte pred vytvorením tunela – žiadne, exponenciálne alebo Holtovo. Pri rôznych vyhladeniach má používateľ možnosť navoliť si rôzne parametre:



Obrázok 31 Vyhladenie

2.3.5 Zvyšné nastavenia

Ako ďalšie si používateľ môže navoliť ako chce, aby sa mu tunel vykreslil. Pokiaľ zaškrtnie políčko „Rozsah okolo útoku“, tunel za vykresli zvolenú šírku okolo útoku a tak môže používateľ lepšie vidieť, ako zareagoval tunel pri útoku. Hodnota je defaultne nastavená na 1000. Pokiaľ toto políčko ostane nezaškrtnuté, používateľ si môže zvoliť rozsah, ktorý chce vykresliť. Hodnota je automaticky nastavená od začiatku až po koniec.



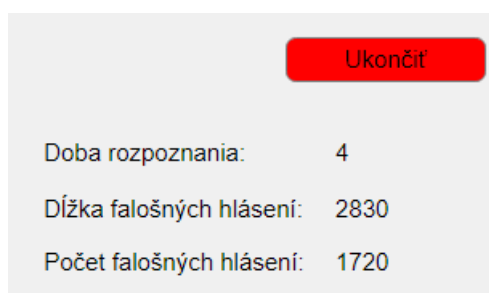
Obrázok 32 Ďalšie nastavenia

2.3.6 Vypočítat'

Ak má používateľ už všetky nastavenia navolené, stačí stlačiť tlačidlo „Vypočítat“ a začne sa vytvárať tunel.

2.4 Vyhodnotenia

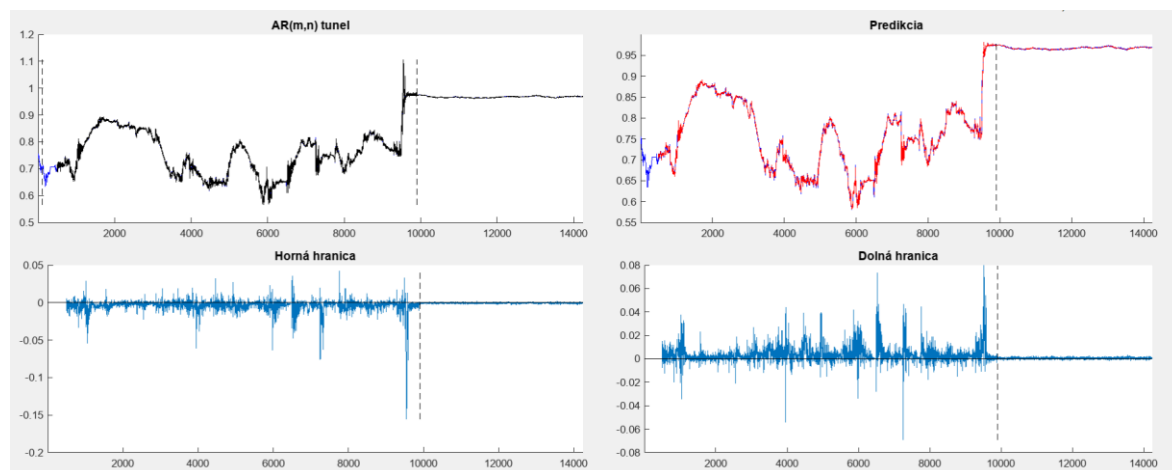
Úplne na konci sú vyhodnotenia, ako dobre daný tunel rozpoznal útok. Je tam vypísaná doba rozpoznania útoku daným tunelom, dĺžka falošných hlásení tunela a počet falošných hlásení.



Obrázok 33 Vyhodnotenie tunela

2.5 Vypočítaný tunel

Pri zvolení tunela „Sigma tunel“ uvidíme ako výstup vykreslené iba 3 grafy zatiaľ, čo pri ostatných tuneloch uvidíme všetky grafy vykreslené:



Obrázok 34 Vykreslené tunely pri použití metódy AR(m,n)