

Slovenská technická univerzita v Bratislave  
Fakulta informatiky a informačných technológií

Bc. Matúš Cimerman

**Analýza prúdu prichádzajúcich udalostí  
použitím rôznych metód pre analýzu údajov**

*Diplomová práca*

Vedúci práce: Ing. Jakub Ševcech

máj, 2016



Slovenská technická univerzita v Bratislave  
Fakulta informatiky a informačných technológií

Bc. Matúš Cimerman

# Analýza prúdu prichádzajúcich udalostí použitím rôznych metód pre analýzu údajov

*Diplomová práca*

Študijný program: Informačné systémy

Študijný odbor: 9.2.6 Informačné systémy

Miesto vypracovania: Ústav informatiky, informačných systémov a softvérového inžinierstva,  
FIIT STU v Bratislave

Vedúci práce: Ing. Jakub Ševcech

máj, 2016



## Návrh zadania diplomovej práce

Finálna verzia do diplomovej práce<sup>1</sup>

### Študent:

**Meno, priezvisko, tituly:** Matúš Cimerman, Bc.  
**Študijný program:** Informačné systémy  
**Kontakt:** matus.cimerman@gmail.com

### Výskumník:

**Meno, priezvisko, tituly:** Jakub Ševcech, Ing.

### Projekt:

**Názov:** Analýza prúdu prichádzajúcich udalostí použitím rôznych metód pre analýzu údajov  
**Názov v angličtine:** Stream analysis of incoming events using different data analysis methods  
**Miesto vypracovania:** Ústav informatiky a softvérového inžinierstva, FIIT STU, Bratislava  
**Oblast problematiky:** analýza dát, prúd udalostí

### Text návrhu zadania<sup>2</sup>

Analýza údajov v sebe spája rôzne techniky z rôznych oblastí štatistiky, strojového učenia a dolovania v údajoch v spojení so znalosťou domény. Každá z týchto domén vyžaduje netriviálne znalosti potrebné pre preloženie otázky do analytickej úlohy, výberu analytickej metódy, vykonanie analýzy a interpretovanie výsledkov. Častokrát je veľmi náročné nájsť experta, ktorý by vedel prepojiť všetky tieto oblasti a s ďalším rozvojom analytickej metód bude tento problém ďalej rásť.

Priestor na zmiernenie tohto problému je napríklad v návrhu nástrojov, ktoré pomáhajú v tomto procese a umožňujú používanie a interpretovanie pokročilých modelov doménovým expertom bez potreby detailných znalostí o fungovaní modelu. Podobné prístupy sme mohli vidieť v podobe rôznych populárnych nástrojov na spracovanie statických kolekcií údajov pomocou metód ako sú lieviková analýza (angl. funnel analysis) alebo vnáranie sa (angl. drill down). V súčasnosti sa však do pozornosti dostáva analýza údajov v čase ich vzniku, kde hovoríme o analýze prúdu prichádzajúcich udalostí.

Analyzujte možnosti použitia známych metód na analýzu statických kolekcií údajov a existujúcich metód na analýzu prúdov údajov. Vyberte a aplikujte metódu na analýzu údajov v doméne spracovania prúdov údajov. Sústredte sa pritom na použiteľnosť metódy, jej jednoduchosť a interpretateľnosť poskytnutých výsledkov používateľom, ktorí nemajú detailné znalosti o fungovaní modelu. Navrhnuté riešenie overte pomocou softvérovej súčiastky implementovaním vybranej metódy vhodnej pre analýzu prúdu udalostí vo zvolenej doméne.

<sup>1</sup> Vytlačiť obojstranne na jeden list papiera

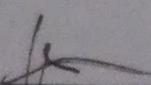
<sup>2</sup> 150-200 slov (1200-1700 znakov), ktoré opisujú výskumný problém v kontexte súčasného stavu vrátane motivácie a smerov riešenia

### Literatúra<sup>3</sup>

- KREMPL, Georg, et al. Open challenges for data stream mining research. ACM SIGKDD Explorations Newsletter, 2014, 16.1: 1-10.
- GABER, Mohamed Medhat; ZASLAVSKY, Arkady; KRISHNASWAMY, Shonali. Mining data streams: a review. ACM Sigmod Record, 2005, 34.2: 18-26.

Vyššie je uvedený návrh diplomového projektu, ktorý vypracoval(a) Bc. Matúš Cimerman, konzultoval(a) a osvojil(a) si ho Ing. Jakub Ševcech a súhlasí, že bude takýto projekt viesť v prípade, že bude pridelený tomuto študentovi.

V Bratislave dňa 12.1.2016



---

Podpis študenta



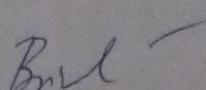
---

Podpis výskumníka

### Vyjadrenie garanta predmetov Diplomový projekt I, II, III

Návrh zadania schválený: áno / nie<sup>4</sup>

Dňa: ..... 15.2.2016 .....



---

Podpis garanta predmetov

<sup>3</sup> 2 vedecké zdroje, každý v samostatnej rubrike a s údajmi zodpovedajúcimi bibliografickým odkazom podľa normy STN ISO 690, ktoré sa viažu k téme zadania a preukazujú výskumnú povahu problému a jeho aktuálnosť (uvedte všetky potrebné údaje na identifikáciu zdroja, pričom uprednostnite vedecké príspevky v časopisoch a medzinárodných konferenciách)

<sup>4</sup> Nehodiace sa prečiarknite

## Zadanie diplomovej práce

**Meno študenta:** Bc. Matúš Cimerman

**Študijný program:** Informačné systémy

**Študijný odbor:** Informačné systémy

**Názov práce:** **Analýza prúdu prichádzajúcich udalostí použitím rôznych metód pre analýzu údajov**

Samostatnou výskumnou a vývojovou činnosťou v rámci predmetov Diplomový projekt I, II, III vypracujte diplomovú prácu na tému, vyjadrenú vyššie uvedeným názvom tak, aby ste dosiahli tieto ciele:

**Všeobecný cieľ:**

Vypracovaním diplomovej práce preukážte, ako ste si osvojili metódy a postupy riešenia relativne rozsiahlych projektov, schopnosť samostatne a tvorivo riešiť zložité úlohy aj výskumného charakteru v súlade so súčasnými metódami a postupmi študovaného odboru využívanými v príslušnej oblasti a schopnosť samostatne, tvorivo a kriticky pristupovať k analýze možných riešení a k tvorbe modelov.

**Specifický cieľ:**

Vytvorte riešenie zodpovedajúce návrhu textu zadania, ktorý je prílohou tohto zadania. Návrh bližšie opisuje tému vyjadrenú názvom. Tento opis je záväzný, má však rámcový charakter, aby vznikol dostatočný priestor pre Vašu tvorivosť.

Riadťe sa pokynmi Vášho vedúceho.

Pokiaľ v priebehu riešenia, opierajúc sa o hlbšie poznanie súčasného stavu v príslušnej oblasti, alebo o priebežné výsledky Vášho riešenia, alebo o iné závažné skutočnosti, dospejete spoločne s Vaším vedúcim k presvedčeniu, že niečo v texte zadania a/alebo v názve by sa malo zmeniť, navrhnite zmenu. Zmena je spravidla možná len pri dosiahnutí kontrolného bodu.

**Miesto vypracovania:** Ústav informatiky a softvérového inžinierstva, FIIT STU Bratislava

**Vedúci práce:** Ing. Jakub Ševcech

**Termíny odovzdania:**

Podľa harmonogramu štúdia platného pre semester, v ktorom máte príslušný predmet (Diplomový projekt I, II, III) absolvovať podľa Vášho študijného plánu

**Predmety odovzdania:**

V každom predmete dokument podľa pokynov na [www.fiit.stuba.sk](http://www.fiit.stuba.sk) v časti:  
home > Informácie o > štúdiu > organizácia štúdia > diplomový projekt.

V Bratislave dňa 15. 2. 2016



prof. Ing. Pavol Návrat, PhD.  
riaditeľ Ústavu informatiky a softvérového  
inžinierstva



# Anotácia

**Fakulta Informatiky a Informačných Technológií  
Slovenská Technická Univerzita**

Meno:

Bc. Matúš Cimerman

Vedúci diplomovej práce:

Ing. Jakub Ševcech

Diplomová práca:

Analýza prúdu prichádzajúcich udalostí použitím rôznych metód pre analýzu údajov

Študijný program:

Informačné systémy

Máj 2016

Dnes môžeme pozorovať narastujúcu potrebu analyzovať dátá počas ich vzniku. Spracovanie a analýza prúdov dát predstavuje komplexnú úlohu, pričom je dôležité poskytnúť riešenie s nízkou odozvou, ktoré je odolné voči chybám.

V našej práci sa sústredíme na návrh súboru nástrojov, ktoré pomôžu doménovému expertovi počas analýzy dát. Doménový expert nepotrebuje mať detailné znalosti o fungovaní analytického modelu. Podobný prístup je podobný, ak chceme analyzovať statické kolekcia dát napríklad lievikovou analýzou. Študujeme možnosti použitia tradičných metód pre statické údaje v doméne analýzy prúdov dát. Našim cieľom je aplikovať metódu pre analýzu v doméne prúdu dát. Zameriavame sa pritom na jednoduchosť vybranej metódy a interpretovateľnosť výsledkov. Pre doménových expertov je nevyhnutné aby boli tieto požiadavky splnené, pretože nebudú potrebovať detailné znalosti z domén ako strojové učenie sa alebo štatistika. Naše riešenie vyhodnocujeme implementovaním softvérovej súčiastky a vybranej metódy.



# Annotation

**Faculty of Informatics and Information Technologies  
Slovak University of Technology**

Name:	Bc. Matúš Cimerman
Supervisor:	Ing. Jakub Ševcech
Diploma thesis:	Stream analysis of incoming events using different data analysis methods
Course:	Information systems
2016, May	

Nowadays we can see emerging need for data analysis as data occur. Processing and analysis of data streams is a complex task, first, we particuraly need to provide low latency and fault-tolerant solution.

In our work we focus on proposal a set of tools which will help domain expert in process of data analysis. Domain expert do not need to have detailed knowledge of analytics models. Similar approach is popular when we want analyse static collections, eg. funnel analysis. We study possibilities of usage well known methods for static data analysis in domain data streams analysis. Our goal is to apply method for data analysis in domain of data streams. This approach is focused on simplicity in use of selected method and interpretability of results. It is essential for domain experts to meet these requirements because they will not need to have detailed knowledge from such a domains as machine learning or statistics. We evaluate our solution using software component implementing chosen method.



# Pod'akovanie

Na prvom mieste vyslovujem pod'akovanie vedúcemu mojej diplomovej práce, Ing. Jakubovi Ševcechovi, za všetky jeho odborné rady, odovzdané skúsenosti a usmernenie pri tvorení práce.

Tento cestou taktiež vyslovujem pod'akovanie všetkým výskumníkom zo skupiny PeWe, za prínosné diskusie a ich spätnú väzbu týkajúcu sa mojej práce. V neposlednom rade ďakujem celej mojej rodine a priateľom.

Matúš Cimerman



# Obsah

<b>1</b>	<b>Úvod</b>	<b>1</b>
<b>2</b>	<b>Analytické úlohy nad prúdom dát</b>	<b>3</b>
2.1	Dopyty nad prúdom dát . . . . .	7
2.2	Detekcia zmien . . . . .	8
2.3	Detekcia anomálií . . . . .	11
2.4	Zhlukovanie . . . . .	14
2.5	Klasifikácia . . . . .	14
2.6	Evaluácia . . . . .	16
2.7	Zhodnotenie . . . . .	16
<b>3</b>	<b>Existujúce nástroje pre analýzu prúdu udalostí</b>	<b>17</b>
3.1	MOA . . . . .	17
3.2	WEKA . . . . .	18
3.3	RapidMiner Streams-Plugin . . . . .	20
3.4	StreamBase . . . . .	21
3.5	Spark . . . . .	23
<b>4</b>	<b>Klasifikácia prúdu dát použitím rozhodovacích stromov</b>	<b>25</b>
<b>5</b>	<b>Zhodnotenie a budúca práca</b>	<b>27</b>

<b>Literatúra</b>	<b>29</b>
<b>Prílohy</b>	<b>33</b>
A Plán na Letný semester 2016/2017 . . . . .	33
B Plán na zimný semester 2016/2017 . . . . .	33

---

# 1. Úvod

V súčasnosti pozorujeme zvýšený záujem o oblast analýzy a dolovania dát. Vhodné použitie a výber metód pre spracovanie dát prináša hodnotné výstupy a náhľady pre používateľa. Výstupy môžu byť použité pre strategické rozhodnutia v podnikoch. Najčastejší postup je aplikovaním metód ako napríklad lieviková analýza alebo rozhodovacie stromy nad statickou kolekcii dát. Tento prístup má niekoľko problémov a to najmä: všetky trénovacie dátá musia byť uložené v pamäti alebo na disku, spracovanie a výpočtová náročnosť a vysporiadanie sa s trendami a zmenami v dátach. Nutnosť dátaj nájskôr zozbierať a uložiť, čo je dnes, kedy vznikajú milióny záznamov za deň, či hodinu, predstavuje rovnako veľký problém.

Pod pojmom spracovanie v reálnom čase myslíme spracovanie v takmer reálnom čase, tzv. jemné (angl. soft) spracovanie v reálnom čase. Jemné spracovanie v reálnom čase znamená, že systém negarantuje spracovanie a odpoveď v stanovenom časovom limite, pričom niektoré vzorky sa môžu omeškať alebo úplne vynechať (Stankovic and Zhao, 1988). Presné limity, do kedy sa spracovanie považuje za reálny čas závisí od problému. Niekde to môže predstavovať rádovo stotiny sekundy, v inej úlohe rádovo sekundy. V tejto práci budeme pracovať s pojmom spracovanie v reálnom čase chápajúcich ako jemné spracovanie v reálnom čase.

Pri dolovaní v prúde dát čelíme niekoľkým výzvam: objem, rýchlosť (frekvencia) a rozmanitosť. Veľký objem dát, ktoré vznikajú veľmi rýchlo je potrebné spracovať v ohraničenom časovom intervale, často v reálnom čase. Pričom sa objem dát neustále zväčšuje, potenciálne narastá až do nekonečna. Identifikujeme niekoľko najviac zasiahnutých oblastí, ktoré sú združení týchto dát: počítačové siete, sociálne siete, Webové stránky (sledovanie správania používateľa na stránke) a Internet Vecí (angl. Internet of Things). Na informácie generované z takýchto zdrojov sa často pozerať ako na neohraničené a potenciálne nekonečné prúdy údajov.

---

Spracovanie, analýza a dolovanie v týchto prúdoch je komplexná úloha. Pre aplikácie je kritické spracovať údaje s nízkou odozvou, pričom riešenie musí byť presné, škálovateľné a odolné voči chybám. Nakoľko sú prúdy neohraničené vo veľkosti a potenciálne nekonečné, môžeme spracovať len ohraničený interval prúdu. Potom hovoríme, že dátá musia byť spracované tak ako vznikajú. Tradičné metódy a princípy pre spracovanie statickej kolekcie údajov nie sú postačujúce na takéto úlohy (Krempl et al., 2014; Han et al., 2011).

## 2. Analytické úlohy nad prúdom dát

Spracovanie, analýza a dolovanie dát predstavuje vo všeobecnosti výzvu. Zvláštnu pozornosť si tieto úlohy vyžadujú pri spracovaní, analýze a dolovaní z prúdu prúdu udalostí. Prúd udalostí je často nazývaný *prúd dát* alebo *údajov*, či len skrátene *prúd*. V tomto texte budeme pre jednoduchosť používať najmä termín *prúd* a *prúd dát* (Tran et al., 2014). Avšak môžu sa vyskytnúť aj terminy ako *prúd udalostí*, *sekvencia udalostí*, či *elementov*, pričom všetky termíny majú v tomto teste rovnaký význam.

**Definícia 2.0.1** *Prúd je potenciálne nekonečná sekvencia elementov (Tran et al., 2014).*

$$S = \{(X_1, T_1), \dots, (X_j, T_j), \dots\}$$

*Kde každý element je pári  $(X_j, T_j)$  kde  $X_j$  je  $d$ -dimenzionálny vektor  $X_j = (x_1, x_2, \dots, x_d)$  prichádzajúci v čase  $T_j$ .  $T_j$  je často nazývaný aj časová pečiatka, existujú dva typy časovej pečiatky: explicitná je generovaná ked' dát dorazia, implicitná je priradená vektoru v čase ich vzniku.*

Takmer každé odvetvie dnes generuje masívne množstvo dát. Vzhľadom na ich veľký objem analytici a doménový experti často strácajú schopnosť dolovať v celej sade dát. Stáva sa preto častým zvykom, že sa vyberie reprezentujúca vzorka, ktorej spracovanie predstavuje menšiu časovú a pamäťovú výzvu. Pri pamäťovej náročnosti hovoríme o limitoch počítača, pričom ak hovoríme o časovej náročnosti hovoríme o limitovanom čase doménového experta (čakanie na výsledok analýzy) (Hulten et al., 2001). Predpokladajme, že bude pre doménového experta vysokým prínosom možnosť vykonávať analýzy nad prúdom v reálnom čase. Výstupy z takejto analýzy sú na rôznej granularite a úrovni, pričom môžu byť neskôr použité na ďalšie spracovanie alebo na priame

prezentovanie výsledkov.

Analýza a spracovanie prúdov dát pridáva viaceré otvorené výzvy a možnosti pre výskum (Krempl et al., 2014):

- *Ochrana súkromia a dôvernosti* pri analýze a dolovaní v prúde dát. Hlavným cieľom je vyvinúť metódy a techniky, ktoré neodhalia informácie a vzory, ktoré by kompromitovali potreby dôvernosti a ochrany súkromia. Dve hlavné výzvy pri analýze a dolovaní v prúdoch dát sú: *vysporiadanie sa s neúplnými dátami* a *uchovanie zmien* (angl. *concept drift*) v prúde dát.
- *Predspracovanie* dát je dôležitou súčasťou každej reálnej aplikácie, najmä tých pre analýzu dát. Zatiaľ čo pri tradičnej analýze dát je predspracovanie vykonané jednorázovo, zvyčajne doménovým expertom, ktorý rozumie dátam. Pri prúde dát toto nieje prijateľné, pretože dáta nepretržite prichádzajú. Okrem niekoľkých štúdií (Zliobaite and Gabrys, 2014; Anagnostopoulos et al., 2008) tejto problematike nebola venovaná dostatočná pozornosť ako pri tradičnom spracovaní dát. Hlavné výzvy, ktorým treba čeliť pri predspracovaní prúdu dát sú: *hluk v dátach*, *outliers* a *adaptívny výber vzorky*.
- *Načasovanie a dostupnosť informácie*, väčšina algoritmov robí jednoduchý predpoklad, že prijatá informácia je kompletná, ihneď dostupná, prijatá pasívne a zadarmo. Viaceré výzvy spojené s načasovaním a dostupnosťou informácie sú formulované a nepreskúmané: *spracovanie nekompletívnych dát*, *vysporiadanie sa so skreslenou* (angl. *skewed*) *distribúciou dát* a *spracovanie oneskorených dát*.
- *Dolovanie entít a udalostí* kde entity predstavujúce prúd sú spojené do viacerých inštancií resp. štruktúrovaných informácií (napr. agregácie). Tieto entity môžu byť niekedy spojené s výskyтом udalostí resp. v prúde dát.
- *Evaluácia algoritmov pre prúdy dát* predstavuje úplne novú výzvu v porovnaní s tradičnými metódami. Pri evaluácii v prúde dát sa musíme vysporiadať s problémami ako: *zmeny* (angl. *concept drift*, *limitovaný čas pre spracovanie vzorky*, *vyvíjajúce sa skreslenie tried dát*, či *oneskorenie*

---

*overenia.* Tejto problematike sa v poslednej dobe venuje vyššia pozornosť, ako napríklad pre evaluáciu klasifikátorov nad prúdmi dát (Bifet et al., 2015).

- Špecializované, reaktívne a jednoduché modely na pochopenie pre doménového experta. Tieto tri výzvy v sebe ukrývajú potrebu pre minimálizáciu závislosti na nastavení parametrov metódy, kombinácia online a offline modelov a riešenie správneho problému (zmeny v prúdoch).

**Model prúdu dát** môže byť jeden z nasledujúcich: model časových radov, pokladničný model a model turniketu. Podľa modelu prúdu dát existujú príslušné algoritmy, ktoré boli vytvorené pre daný model (Tran et al., 2014). Majme prúd dát  $a_1, a_2, \dots$ , ktorý prichádza sekvenčne za sebou a popisuje podstaný signál  $A$ . V modeli časových radov každá vzorka  $a_i$  sa rovná  $A[i]$  pričom vzorky prichádzajú v vzostupnom poradí. Tento model je vhodný pre prúdy dát, ktoré nesú v sebe časovú postupnosť alebo je ich poradie určované časovou pečiatkou (Muthukrishnan, 2005). Pri pokladničnom modeli môžeme považovať množinu  $U = 1, 2, \dots, n$  za element z prúdu dát. Ak uvažujeme sekvenciu 2, 1, 2, 5 ako príklad, potom hovoríme o pokladničnom modeli. Tento model je často používaný v praxi, napríklad v prípadoch kde sled IP adres pristupuje na Web server (Ikonomovska and Zelke, 2013; Muthukrishnan, 2005). Model turniketu je veľmi podobný pokladničnému modelu. Rozdiel je v tom, že vzorka môže predstavovať aj zápornú hodnotu - analógia z reálneho sveta kedy niektorí ľudia prichádzajú a vychádzajú turniketom, počet ľudi sa mení (napr. na zjazdovke) (Ikonomovska and Zelke, 2013; Muthukrishnan, 2005).

**Predspracovanie prúdu** Predspracovanie je azda najdôležitejším krokom v aplikáciach reálneho sveta a časovo najnáročnejšou úlohou pre každého analyтика. Nakoľko dáta prichádzajú z nehomogénneho sveta, môžu byť zašumené, nekompletné, duplicitné alebo často obsahovať hodnoty, ktoré sa značne líšia od ostatných. Predspracovanie prúdiach údajov je potrebné čo najviac automatizovať. Existuje niekoľko známych metód a techník, ktoré sú používané pri predspracovaní prúdov dát:

- *Vzorkovanie*, napríklad podľa pravdepodobnostného modelu.

- *Zahadzovania potenciálne nepotrebných vzoriek*, ak je spracujúci proces príliš zaťažený. Tu môže nastať problém, že práve zahodená vzorka bola dôležitá (zmena v dátach).
- *Agregácia údajov* môže značne znížiť objem dát, ale môže spôsobiť problém pri potrebe pohľadu do minulosti.
- *Approximačné algoritmy* a ich použitie má za následok podstatné zrýchlenie spracovania a analýzy prúdov za predpokladu istej chybovosti. Chybovosť je zvačsa ohraničená.
- *Posuvné okno*, tento prístup vznikol s potrebou analýzy definovaného časového okna z prúdiacich údajov.

**Spracovanie, dolovanie a analýza informácií** Problematika spracovania, dolovania a analýzy bola študovaná niekoľko dekád. Zvýšenú pozornosť začala odborná verejnosť venovať pri aplikovaní týchto úloh na prúdy dát. Týmto úlohám sa venujeme podrobne v nasledujúcich podkapitolách:

- *Klastrovanie*, existuje niekoľko výskumov, ktoré sa venovali špeciálne klastrovaniu implementovaním napríklad k-mediánu a inkrementálnych algoritmov.
- *Klasifikácia*, táto úloha je dlho skúmaná s použitím rôznych metód roz-hodovacích stromov.
- *Počítanie frekvencie a opakovanie*, použitím posuvných okien a inkrementálnych algoritmov na detekciu vzorov v prúde.
- *Analýza časových radov použitím symbolickej reprezentácie časových radov* v prúde dát. Takáto reprezentácia nám umožňuje redukciu veľkosti prenášaných dát. Táto technika pozostáva z dvoch hlavných krokov, approximácia po častiach a následná transformácia výsledku do diskrétnych veličín.

## 2.1 Dopyty nad prúdom dát

Vyhodnocovaniu dopytov nad statickou kolekciovou dát bola venovaná značná pozornosť, ak však hovoríme o prúdoch dát dopyty musia byť vyhodnocované kontinuálne (Babu and Widom, 2001; Babcock et al., 2002). Vzniká teda nová paradigma pre interakciu s dynamicky sa meniacimi dátami, ktorú nazývame kontinuálne dopyty (angl. continuous queries) (Babu and Widom, 2001). Výsledky kontinuálnych dopytov sú produkované dynamicky v čase vzniku nových dát. Príkladom použitia takýchto dopytov je napríklad sledovanie vývoja akcií burzy. Problém môže nastať pri jednorázových dopytoch, ktoré obsahujú agregačné funkcie. Pri tradičnom spracovaní dát kde sú všetky dáta uložené ako statická kolekcia, je dopyt vykonaný nad celou kolekciovou. V prípade kontinuálneho dopytu je problém získať predchádzajúce dáta za predpokladu, že dáta niesú ukladané. Môžu potom nastať dva scenáre:

1. agregačná funkcia je prepočítaná nad kolekciovou dát, za predpokladu, že boli historické dáta ukladané.
2. agregačná funkcia je počítaná od momentu zadania dopytu.

Kontinuálne dopytovanie do prúdu dát nesie so sebou nieľko výziev (Babcock et al., 2002):

- *Limitované pamäťové požiadavky* na algoritmy spracujúce dopyty, pretože prúd dát predstavuje potenciálne nekonečný prúd udalostí.
- *Približné odpovede na dopyty* sú niekedy postačujúce za predpokladu, že odpoveď je dostatočne rýchla a používateľ rozumie v akej presnosti mu bola odpoveď poskytnutá. Techniky pre redukciu dimenzionality a objemu dát zahŕňajú napríklad: histogramy, náhodné vzorkovanie, symbolické vzorkovanie apod.
- *Dopytovací jazyk* by mal byť podobný štandardu jazyka SQL. Jazyk SQL je známy deklaratívny jazyk, je široko používaný so zavedením štandardom, ktorý poskytuje flexibilitu a optimálnu evaluáciu dopytu a vykonanie nad prúdom, či datasetom.

Výskumné práce sa tiež venovali adaptívnym kontinuálnym dopytom nad prúdmi dát. Bolo ukázané, že takýto prístup môže mať značný prínos v oblasti výkonnosti systému vďaka jeho schopnosti adaptácie na zmeny v prúde dát. Tieto vlastnosti sú dosiahnuté aplikovaním zoskupovania indexov filtrov na priebežný výber predikátov (Madden et al., 2002).

Ďalší priestor na zlepšenie výkonnosti kontinuálnych dopytov nad prúdmi dát predstavujú adaptívne filtre. Pri dopytovaní sa takmer vždy vykonáva filtrovanie dát v nejakej podobe. Tento krok filtrovania je obvykle implementovaný v systéme na spracovanie dopytov. Pre zvýšenie výkonnosti dopytov je preto možné tieto filtre presunúť priamo do zdrojov dát. Ukázalo sa, že takýto prístup môže mať pozitívny dopad na výkonnosť (Olston et al., 2003). Tento prístup prinesie najmä redukciu prenášaných dát výmenou za ich nepresnosť. Problémom tejto techniky je, že je aplikovateľná len v prostredí, ktoré máme plne pod kontrolou a vieme zasahovať do všetkých jeho súčastí.

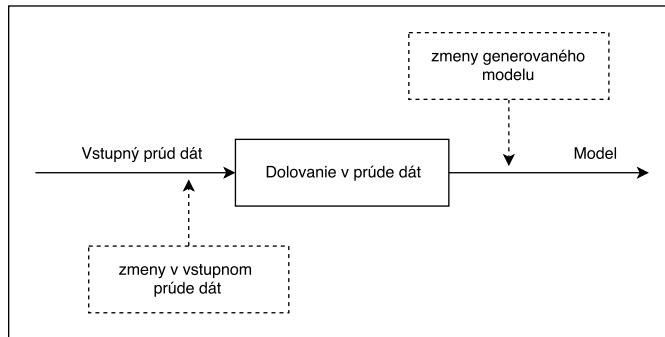
## 2.2 Detekcia zmien

Detekcia zmien (angl. concept drift) zohráva, v dnešnom rýchlo sa meniacom svete, dôležitú úlohu. Zmeny nastávajú veľmi rýchlo a nečakane. Preto stúpa potreba detektie zmeny a následná správna reakcia, ktorá vyplynie z detektovanej zmeny. Na to aby sme boli schopní na tieto zmeny adekvátnie reagovať je potrebné dátá spracovávať tak ako vznikajú a pozerať sa na ne ako na prúd udalostí. Tradičné metódy pre paralelné spracovanie uvažujú len statickú kolekciu dát (Tran et al., 2014).

Detekcia zmeny predstavuje proces identifikácie zmeny aktuálneho stavu modelu voči predchádzajúcemu. Na tento objekt sa pozéráme v rôznom čase. Dôležitý rozdiel medzi zmenou a rozdielom je, že zmena hovorí o prechode modelu do iného stavu, zatiaľ čo rozdiel znamená nepodobnosť v atribútoch dvoch objektov. V kontexte prúdu, detekovanie zmeny je proces segmentácie prúdu udalostí do rôznych segmentov a identifikovanie miest kde sa zmení dynamika prúdu (Ross et al., 2009). Metóda pre detekciu zmien musí riešiť nasledujúce úlohy (Tran et al., 2014): *detekcia zmeny* znamená správnu identifikáciu zmeny a *lokálizácia zmeny* hovorí o identifikovaní momentu kedy

zmena nastala. Týmto úloh je potrebné venovať dostatočnú pozornosť, pretože zmeny môžu byť falošné alebo dočasné čo so sebou prináša problém lokalizácie danej zmeny. Ďalší rozdiel, ktorý je potrebné zdefinovať, je medzi rozdiel detekovaním posunu pojmu (angl. concept drift). Pre lepšiu čitateľnosť tohto textu budeme pod pojmom detekcia zmeny, zmena rozumieť posun pojmu. Detekcia concept drift-u sa sústredí na označkované dátá, zatiaľ čo detekcia zmeny pracuje s označkovanými rovnako ako s neoznačkovanými dátami. Posun pojmu nazývame tiež časté zmeny v účelovej funkcií modelu, ktorý sa učí online.

Metódy pre detekovanie zmien môžme klasifikovať do nasledujúcich prístupov (Liu et al., 2010): *metódy založené na stave*, *metódy sledujúce trend* a *prahové metódy*. Algoritmus pre detekciu zmien by mal spĺňať aspoň nasledovné požiadavky: *presnosť*, *rýchlosť* a *odpoved v reálnom čase*. Algoritmus by tiež mal detektovať čo najmenej chybných zmien a čo najviac správnych presných miest zmeny. Algoritmy by mali byť prispôsobené reálnemu prostrediu a spracovaniu prúdov vysokých objemov a rýchlosťi. Na obrázku 2.2 je zobrazený všeobecný diagram pre detekciu zmeny v prúde udalostí.



**Obrázok 2.1:** Všeobecný diagram zobrazujúci detekciu zmeny v prúde udalostí (Tran et al., 2014).

Pre detekciu zmeny v prúdoch dát bolo vyvinutých niekoľko techník a metód. Niektoré z nich nižšie podrobnejšie popisujeme.

**Charakteristika dát** Metódy pre detekciu zmien môžu byť klasifikované na základe charakteru dát, s ktorými pracujú. Najčastejšie môžme prúdy klasifikovať do kategorických alebo numerických prúdov. Ak hovoríme o kategorických prúdoch, dáta obsiahnuté v prúde majú kategorický charakter, napríklad rôzny

výrobcovia áut:  $x \in \{Volvo, Toyota\}$ . Pri numerických prúdoch dáta predstavujú numerické hodnoty  $x \in \mathbb{R}$ . Pre každý takýto prúd boli vyvinuté príslušné algoritmy. Problém nastáva pri aplikáciach s dátami reálneho sveta kde prúdy často obsahujú numerické aj kategorické dáta. V takýchto situáciach má zmysel dáta rozdeliť rovnomenných skupín obsahujúce dáta rovnakého typu. Na tieto skupiny sú následne použité príslušné algoritmy. Prúdy dát sa ďalej môžu klasifikovať do označkovaných a neoznačkovaných prúdov. Neoznačkované prúdy obsahujú dáta, ktoré niesú zaradené do žiadnej triedy. Naopak označkované prúdy nesú v sebe informáciu o tom, do ktorej triedy patrí vybraný element. Rôzny charakter prúdu predstavuje rôzne zmeny a prístup na ich riešenie pri detekcii zmien v prúde (Tran et al., 2014).

**Metóda pre detekciu zmeny** V skratke DDM z anglického Drift Detection Method. Táto metóda sa zaoberá detekciou zmeny modelu. Majme prúd dát  $(x_i, y_i)$  kde  $x_i$  predstavuje atribúty a  $y_i$  triedu vzorky. Model sa potom snaží predikovať skutočnú triedu  $y_i + 1$  novej vzorky. Gama a spol. založili DDM na fakte, že každá iterácia klasifikátora predikuje triedu vzorky. Klasifikátor je binárny, takže trieda môže byť len *pravda* alebo *nepravda*. Potom, pre množinu vzoriek, chyba predstavuje náhodnú premennú z Bernoulliho pokusov (angl. Bernoulli trials). Vďaka tomu môžeme chybu modelovať s bínomickým rozdelnením. Nech  $p$  je pravdepodobnosť zlej predikcie a  $s_i$  je štandardná odchýlka vypočítaná nasledovne:

$$s_i = \sqrt{\frac{p_i(1-p_i)}{i}}$$

Pre každú vzorku z prúdu sú udržiavané dve premenné,  $p_{min}$  a  $s_{min}$ . Ich hodnoty sú použité na výpočet varovnej hodnoty, ktorá slúži na definovanie optimálnej velkosti kontextového okna. Kontextové okno si udržiava staré vzorky, ktoré obsahujú nový kontext resp. zmenu, či posun pojmu, a minimálny počet elementov zo starého konextu. Ak sa následne zníži množstvo chybne predikovaných vzoriek, okno je zahodené ako zle identifikovaná zmena (false alarm). Naopak, ak je dosiahnutá dostatočná varovná úroveň, predtým naučený model je zahodený a vytvorený nový, ale iba zo vzoriek ktoré boli uložené do kontextového okna (Gama et al., 2004; Brzeziński, 2010).

Existuje tiež rozšírenie EDDM, ktoré je modifikáciou DDM. Tento algoritmus

používa rovnakú techniku varovných alarmov, ale namiesto klasifikácie chyby používa metriku množstva rozdielnych chýb. EDDM metóda dosahuje lepšie výsledky pri postupných zmenách, ale je citlivejšia na hluk v dátach (Wadewale and Desai, 2015).

**ADWIN** je skratka pre algoritmus s názvom adaptívne posuvné okno (angl. adapting sliding window). Tento algoritmus je vhodný je prúdy s náhlymi zmenami. Algoritmus si udržiava okno  $W$  s najnovšími vzorkami. Okno  $W$  je automatický zväčšované, ak nie je detekovaná žiadna výrazná zmena v prúde a naopak zmenšované, ak bola zmena detekovaná. Obmedzenie nárastu okna do nekonečna (žiadna zmena v prúde) je možné parametrom algoritmu, ktorý bude limitovať dĺžku okna  $W$ . ADWIN taktiež poskytuje ohraničenie výkonu na základe množstva falošne pozitívne a falošne negatívnych vzoriek (Wadewale and Desai, 2015). Základná verzia algoritmu ADWIN je vhodná pre 1-dimenzionálne dátá. Ak je potrebné detektovať zmeny pre viac-dimenzionálne dátá, potom sa vytvára paralelne niekoľko okien pre každú dimenziu dát (Brzeziński, 2010).

Existuje mnoho ďalších prístupov ako sa vysporiadať so zmenami v prúde, napríklad: exponenciálne váhovaný posuvný priemer, štatistické testovanie rovnomeného podielu, súborové (angl. ensemble) metódy. Popis všetkých metód je nad rámec tejto práce.

## 2.3 Detekcia anomálií

Detekcia anomálií (angl. anomaly detection) predstavuje proces identifikácie dát, ktoré sa význačne odchyľujú (angl. deviate) od historických vzorov (Hodge and Austin, 2004). Anomálie môžu spôsobovať chyby v meraní senzorov, nezvyčajné správanie systému alebo chyba pri prenose dát, či zámerné vytváranie anomálií v používateľmi generovanom obsahu. Takže detekcia anomálií má veľa praktického použitia napríklad v aplikáciach, ktoré dohliadajú na kvalitu a kontrolu dát (Hill et al., 2007) alebo adaptívne monitorovanie sietí (Hill and Minsker, 2010). Tieto aplikácie často kladú požiadavku aby boli anomálie detekované v čase ich vzniku, teda v reálnom čase. Potom metódy pre detekciu

anomálií musia byť rýchle vo vykonávaní a mať inkrementálny charakter.

V minulosti sa obvykle anomálie detekovali manuálne s pomocou vizualizačných nástrojov, ktoré doménovým expertom pomáhali v tejto úlohe. Manuálne metódy avšak zlyhávajú pri detekcii anomálií v reálnom čase. Výskumníci navrhli niekoľko metód, ktoré majú myšlienku v prístupoch strojového učenia sa a automatizovaného štatistického vyhodnocovania (Hill and Minsker, 2010): *minimálny objem elipsoidu, konvexný zvon, najbližší sused, zhľukovanie, klasifikácia neurónovou sieťou, klasifikácia metódou podporných vektorov a rozhodovacie stromy*. Tieto metódy sú pochopiteľne rýchlejšie než manuálna detektia, avšak jeden význačný nedostatok, bez úpravy niesú vhodné pre prúdové spracovanie v reálnom čase. Existujú napríklad rozhodovacie stromy, ktoré si dokážu budovať model inkrementálne, avšak sa líšia od dobre známych algoritmov. Táto metóda je podrobne popísana ďalej v texte.

**Dátovo riadená metóda** (angl. data-driven), ktorú navrhli (Hill and Minsker, 2010), využíva dátovo riadený jednorozmerný autoregresívny model prúdu dát a predikčný interval (ďalej len PI) vypočítaný z posledných historických dát na identifikáciu anomálií v prúde. Dátovo riadený model časového radu je použitý, pretože je jednoduchší na implementáciu a použitie v porovnaní s ostatnými modelmi časových radov. Tento model tiež poskytuje rýchle a presné prognózy. Dáta sú potom klasifikované ako anomálie na základe toho, či sú spadnú do zvoleného intervalu PI. Metóda teda poskytuje principiálny rámc pre výber hraničného prahu kedy majú byť anomálie klasifikované. Výhoda metódy je, že nevyžaduje žiadne vzorky dát, ktoré sú vopred označkované alebo klasifikované. Je veľmi dobre škálovateľná na veľké objemy dát a vykonáva inkrementálne počítanie tak ako dátá vznikajú. Metóda pozostáva z nasledujúcich krokov so začiatkom v čase  $t$ :

1. použi model na predikciu o krok vpred (angl. one-step-ahead), ktorý má ako vstup  $D^t = \{x_{t-q+1}, \dots, x_t\}$   $q$  je rôzne meranie  $x$  v čase  $t$  a  $D^t$  je model predikcie. Tento model je použitý na predikovanie hodnoty  $\bar{x}_{t+1}$  ako očakávaná hodnota v čase  $t+1$ .
2. výpočet hornej a spodnej hranice kam by malo spadnúť pozorované meranie s pravdepodobnosťou  $p$ .

3. porovnaj pozorovanie v čase  $t+1$ , či spadá do určeného intervalu. Ak spadne mimo intervalu, objekt je klasifikovaný ako anomália.
4. (a) pri stratégii metódy detekcie anomálií a zmiernenia (angl. anomaly detection and mitigation) ADAM, ak je pozorovaný objekt klasifikovaný ako anomália, modifikuj  $D^t$  odstránením  $x_{t-q+1}$  z konca pozorovaného okna a pridaním  $\bar{x}_{t+1}$  na začiatok okna, čím vytvoríme  $D^{t+1}$ .  
(b) pri jednoduchej stratégii detekcie anomálií (angl. anomaly detection) AD, modifikuj  $D^t$  odstránením  $x_{t-q+1}$  z konca okna a pridaj  $x_{t+1}$  na začiatok okna čím vznikne  $D^{t+1}$ .
5. opakuj kroky 1-4

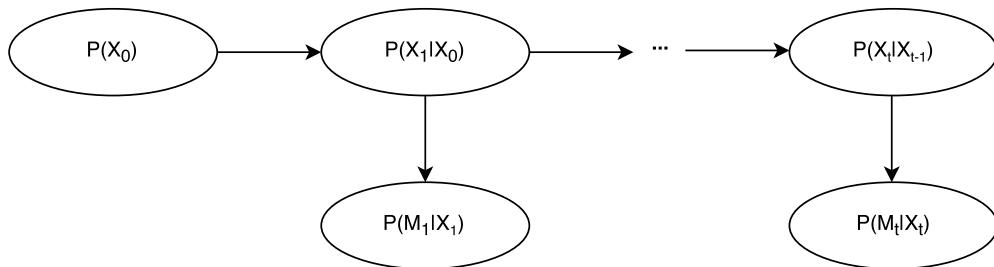
**Metóda dynamických bayesových sietí** (angl. Dynamic Bayesian Networks) (Hill et al., 2007) bola vytvorená pre detekciu anomálií v prúdoch zo senzorov, ktoré sú umiestnené v životnom prostredí. Bayesové siete predstavujú acyklický orientovaný graf, zobrazené na obrázku 2.3, v ktorom každý uzol obsahuje pravdepodobnosť informáciu v súvislosti k všetkým možným stavom, v ktorých sa môže premenná nachádzať. Táto informácia spolu s topológiou bayesovej siete, špecifikuje úplné spojenie distribúcie stavu premennej, pričom sada známych premených môže byť použitá na odvodenie hodnoty neznámych premených. Dynamické bayesové siete s topológiou, ktorá sa vyvýja v čase, pridáva nové stavové premenné pre lepšiu reprezentáciu stavu systému v aktuálnom čase  $t$ . Stavové premenné môžeme kategorizovať ako *neznáme*, ktoré predstavujú skutočný stav systému a *merané*, ktoré sú nedokonalé merania. Tieto premenné môžu byť naviac diskrétny alebo spojité. Nakoľko sa veľkosť siete zväčšuje s časom, vytváranie záverov použitím celej siete by bolo neefektívne a časovo náročné. Preto boli vyvinuté aproximačné algoritmy ako *Kalmanové filtrovanie* alebo *Rao-Blackwellized časticové filtrovanie*.

Hill et al. navrhli v (Hill et al., 2007) dve stratégie pre detekovanie anomálií v prúde dát:

- *Bayesov dôveryhodný interval* (angl. Bayesian credible interval - BCI), ktorý sleduje viacrozmernú gausovskú distribúciu lineárneho stavu pre-

mennej, ktorý korešponduje s neznámym stavom systému a jej meraným náprotivkom.

- *Maximálne posteriori meraný status* (angl. Maximum a posteriori measurement status - MAP-ms) používa komplexnejšiu dynamickú bayseovú sieť. Princíp je rovnaký ako pri BCI, pričom MAP-ms metóda je naviac rozšírená o status (napr. anomália áno/nie), ktorý je reprezentovaný distribúciou diskrétnej premennej každého merania senzoru.



**Obrázok 2.2:** Štruktúra dnmickej bayseovej siete. Vektor  $X$  reprezentuje spojité zložky, neznáme alebo tiež nazývané skryté premenné systému a vektory  $M$  predstavujú spojité pozorované premenné v čase  $t$ .

## 2.4 Zhlukovanie

## 2.5 Klasifikácia

**Multinomiálny Naive Bayes** je klasifikátor najčastejšie používaný na klasifikáciu dokumentov, ktorý obvykle poskytuje dobré výsledky aj čo sa týka presnosti výsledku aj rýchlosťi. Túto metódu je jednoduché aplikovať v kontexte prúdu dát (Bifet and Frank, 2010). Multinomiálny naivný Bayes sa pozera na dokument ako na zhluk slov. Pre každú triedu  $c$ ,  $P(w|c)$ , pravdepodobnosť, že slovo  $w$  patrí do tejto triedy je odhadovaná z trénovacích dát jednoducho vypočítaním relatívnej početnosti každého slova v trénovacej sade pre danú triedu. Klasifikátor potrebuje naviac nepodmienenú pravdepodobnosť  $P(c)$ . Za predpokladu, že  $n_{wd}$  je počet výskytov slova  $w$  v dokumente  $d$ , pravdepodobnosť triedy  $c$  z testovacieho dokumentu je nasledovaná:

$$P(c|d) = \frac{P(c) \prod_{w \in d} P(w|c)^{n_{wd}}}{P(d)}$$

Kde  $P(d)$  je normalizačný faktor. Aby sme sa vyhli problému kedy sa trieda nevyskytuje v datasete ani jeden krát, je bežné použiť Laplacovej korekcie a nahradenie nulových početností jednotkou, resp. inicializovať početnosť každej triedy na 1 namiesto 0.

**Stochastický gradientný zostup** (angl. Stochastic Gradient Descent, SGD). Bifet and Frank v ich práci použili implementáciu tzv. vanilla stochastický gradientný zostup s pevnou rýchlosťou učenia, optimalizujúc stratu s  $L_2$  penalizáciou.  $L_2$  penalizácia je často používaná pri podporných vektorových strojoch (angl. support vector machines). Lineárny stroj, ktorý je často aplikovaný na problémy klasifikácie dokumentov, optimalizujeme funkciu straty nasledovne:

$$\frac{\lambda}{2} \|w\|^2 + \sum [1 - (yxw + b)]_+$$

kde  $w$  je váhovaný vektor,  $b$  je sklon,  $\lambda$  regulačný parameter a označenie triedy  $y$  je z intervalu  $\{+1, -1\}$ .

**Hoeffdingov strom** (angl. Hoeffding tree) je najznámejšia implementácia rozhodovacích stromov v použití prúdového spracovania. Hoeffdingov algoritmus implementuje stratégiu pred-prerezávania, ktorá je založená na Hoeffdingovom ohraničení. Toto umožňuje inkrementálne budovanie rozhodovacieho stromu. Uzol stromu je rozvinutý hned ako obsahuje dostatočne silnú štatistickú informáciu. Existujú ďalšie sofistikované implementácie Hoeffdingových stromov, ktoré implementujú rýchlejšie a efektívnejšie algoritmy, napr. VFDT - Very Fast Decision Trees (Domingos and Hulten, 2000) alebo CVFDT - Concept adapting Very Fast Decision Trees (Hulten et al., 2001)

## 2.6 Evaluácia

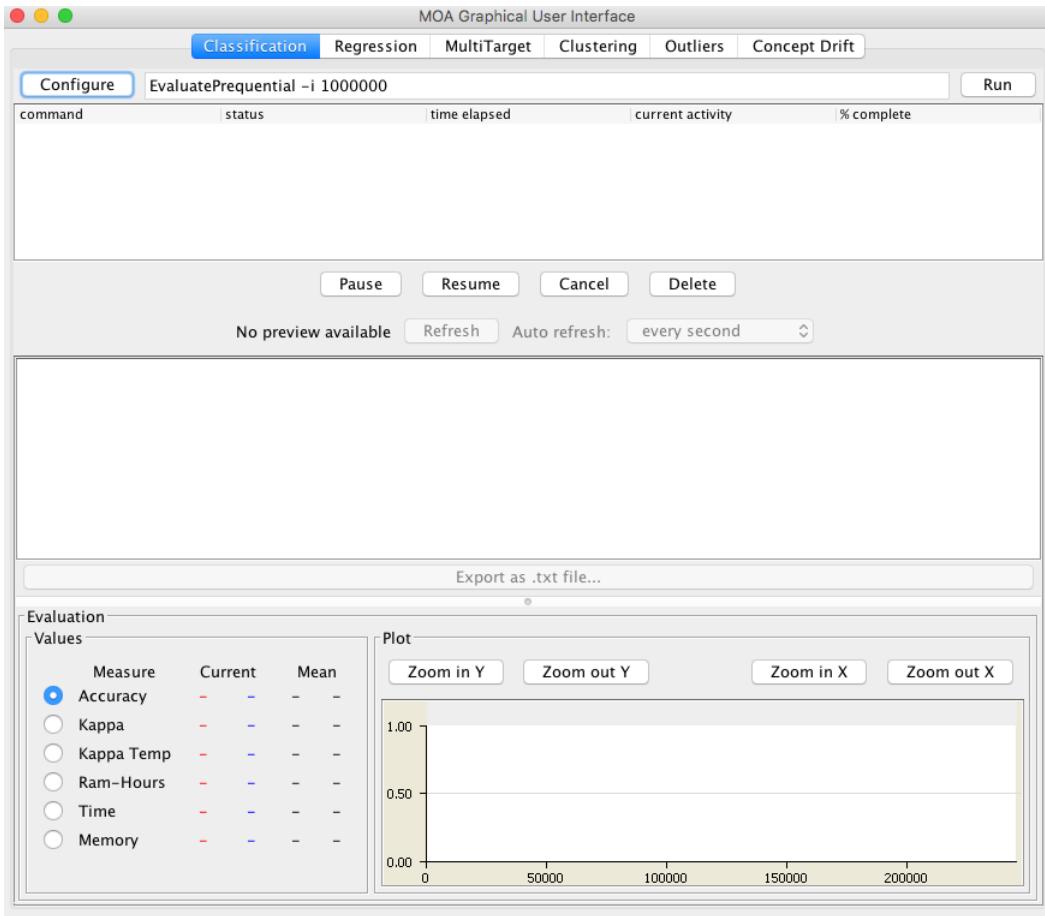
## 2.7 Zhodnotenie

### 3. Existujúce nástroje pre analýzu prúdu udalostí

#### 3.1 MOA

Masívny online analyzátor (z angl. Massive Online Analysis - MOA, ďalej len MOA) je softvérové prostredie pre implementáciu algoritmov a vykonávanie experimentov pre online učenie sa z vyvýjajúcich sa prúdov dát (Bifet et al., 2010). MOA pozostáva z kolekcie offline a online metód a tiež nástrojov pre evaluáciu týchto metód. MOA implementuje metódy a algoritmy pre klasifikáciu, zhľukovanie prúdu, detekciu inštancií, ktoré sa vymykajú prahovým hodnotám a tiež odporúčacie systémy. Presnejšie MOA implementuje napríklad nasledujúce: stupňovanie (angl. boosting), vrecovanie (angl. bagging) a Hoeffdingove stromy, všetky metódy s a bez Naive Bayes klasifikátorom na listoch. MOA podporuje obojsmernú interakciu s nástrojom WEKA, ktorý je detailne opísaný v nasledujúcej kapitole.

MOA je implementovaná v programovacom jazyku Java. Za hlavný benefit implementácie v Java považujú autori jej platformová nezávislosť. MOA obsahuje tiež generár prúdu dát, vie dobre modelovať concept drift. V aplikácií je možné definovať pravdepodobnosť, že inštancia prúdu patrí do nového concept drift-u. Sú dostupné nasledovné generátory prúdu (Bifet et al., 2010): *Random Tree Generator, SEA Concepts Generator, STAGGER Concepts Generator, Rotating Hyperplane, Random RBF Generator, LED Generator, Waveform Generator, and Function Generator*.



Obrázok 3.1: Hlavná obrazovka GUI nástroja MOA.

## 3.2 WEKA

The Wakaito Enviroment for Knowledge Analysis (ďalej len Weka) vznikol s jednoduchým cieľom poskytunúť výskumníkom unifikovanú platformu pre prístup k state-of-the-art technikám strojového učenia sa (Hall et al., 2009). Weka vznikla na University of Waikato na Novom Zélande v roku 1992, pričom je aktívne vyvýjaná posledných 16 rokov. Weka poskytuje kolekciu algoritmov strojového učenia sa pre úlohy dolovania v dátach. Algoritmy môžu byť priamo aplikované na datasety prostredníctvom aplikácie alebo použiť vo vlastných aplikáciach volaním Java kódu. Weka obsahuje tiež nástroje na predspracovanie dát, klasifikáciu, regresiu, zhlukovanie, asociačné pravidlá a vizualizáciu. Nástroj je tiež vhodný pre návrhovanie a vývoj nových schém pre strojové učenia sa v kontexte dolovania dát. Zaujímavosťou je tiež, že

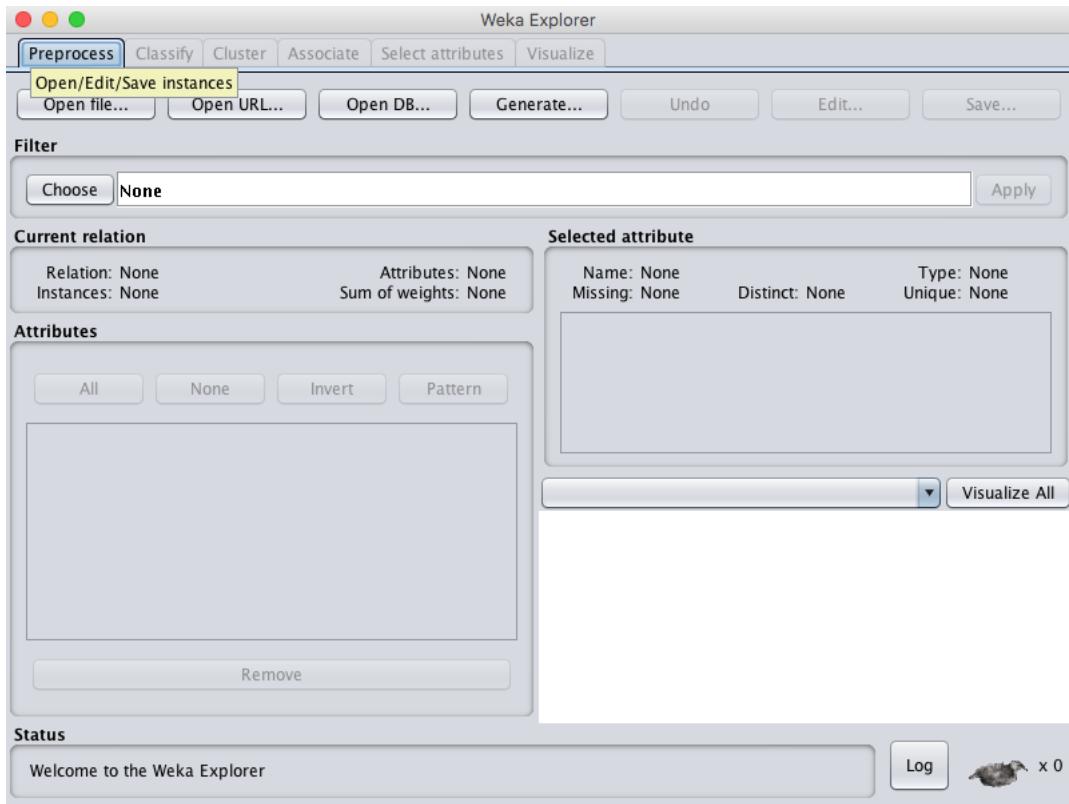
Weka je nelietajúci vták, ktorý žije len na ostrove Nového Zélandu.

Vieľom nástroja je poskytnúť pracovný nástroj pre výskumníkov. Poskytuje napríklad (nástroj ich obsahuje omnoho viac, vymenované sú len vybrané) tieto algoritmy určené pre klasifikáciu dát:

- *Bayesová logistická regresia* (angl. Bayesian logistic regression), pre kategorizáciu textu s Gausovským a Laplacovým apriori.
- *Najlepší prvý rozhodovací strom* (angl. Best-first decision tree), konštrukcia rozhodovacieho stromu so stratégiou najlepší prvý.
- *Hybridná rozhodovacia tabuľka a naivný Bayes* (angl. Decision table native Bayes hybrid) hybridný klasifikátor, ktorý kombinuje rozhodovacie tabuľky a metódu Naivný Bayes.
- *Funkčné stromy* sú rozhodovacie stromy s lomeným rozdelením a lineárnymi funkiami v listoch.

Weka poskytuje tiež nástroje pre predspracovanie dát, zoznam niektorých filtrov (vymenované sú len vybrané základné filtre):

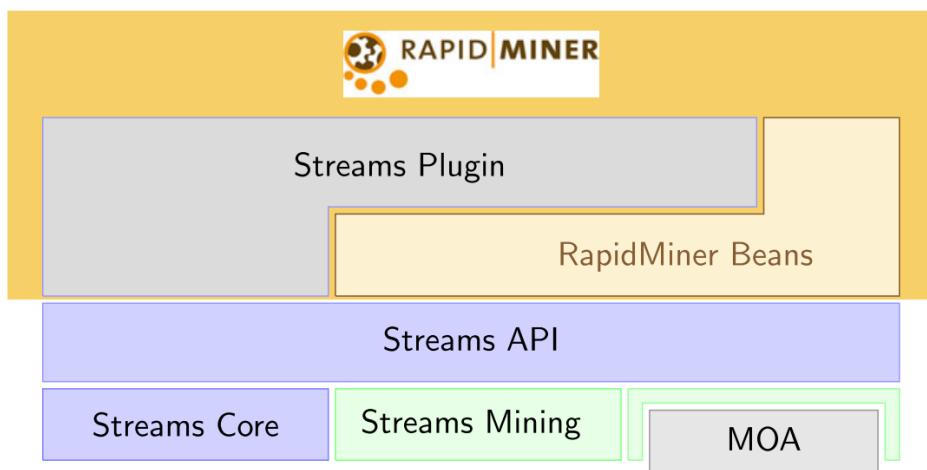
- *Pridanie klasifikátora*, pridá predikcie klasifikátora do datasetu.
- *Pridanie ID* ako nového atribútu pre každý záznam datasetu.
- *Pridanie hodnoty* chýbajúcim hodnotám z poskytnutého zoznamu.
- *Preskupenie atribútov* preusporiadanie poradia atribútov.
- *Numerické hodnoty na nominálne*, konverzia numerických hodnôt na nominálne.



Obrázok 3.2: Hlavná obrazovka GUI nástroja WEKA.

### 3.3 RapidMiner Streams-Plugin

Streams plugin poskytuje operátory RapidMiner-u pre základné budovanie blokov Streams API použitím obaľovača (angl. wrapper) na priame použitie implementácie, ktorú poskytuje Streams balík. Operátory Streams Plugin-u sú automaticky vytvorené pomocou procesora a použitím knižnice RapidMiner Beans (Bockermann and Blom, 2012). Architektúra Streams Plugin-u je postavená na Streams API, ktoré bolo navrhnuté v práci Bockermann a Bloma.



**Obrázok 3.3:** Architektúra RapidMiner Stream Plugin-u a ďalších potrebných častí.

## 3.4 StreamBase

StreamBase<sup>1</sup> je platforma pre spracovanie udalostí, ktorá poskytuje vysoko-výkonný softvér pre budovanie a nasadanie systémov, ktoré analyzujú a reagujú (napr. akciami) na prúdiace dátu v reálnom čase. StreamBase poskytuje prostredie pre svižný vývoj, server pre spracovanie udalostí s nízkou odozvou a vysokou prieplustnosťou a zároveň integráciu do podnikových nástrojov, napríklad pre spracovanie historických údajov. Server analyzuje prúdiace dátu a poskytuje výsledky a odpovede v reálnom čase s extrémne nízkou odozvou. Toto je dosiahnuté maximalizáciou využitia hlavnej pamäte a ostatných prostriedkov servera, zatiaľ čo sa eliminujú závislosti na ostatné aplikácie. Integrované vývojové prostredie - StreamBase Studio umožňuje programátorom jednoducho a rýchlo vytvoriť, testovať a debugovať StreamSQL aplikácie použitím grafického modelu toku vykonávania. StreamBase aplikácie sú potom skompilované a nasadené za behu servera.

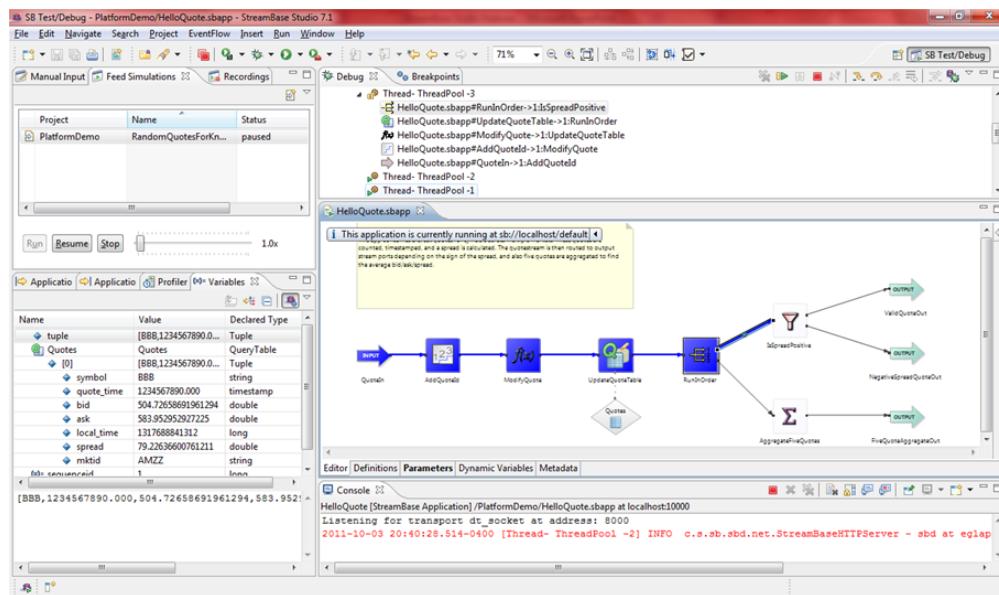
StreamSQL je dopytovací jazyk, ktorý rozširuje štandard SQL. StreamSQL umožňuje spracovanie prúdov v reálnom čase a dopytovanie sa do nich. Základná myšlienka jazyka SQL je možnosť dopytovať sa do uložených

<sup>1</sup><http://www.streambase.com/>

statických kolekcií dát, StreamSQL umožňuje to isté, ale do prúdov dát. Teda, StreamSQL musí zvládnuť spracovať kontinuálny prúd udalostí a časovo orientované záznamy. StreamSQL zachováva schopnosti jazyka SQL zatiaľ čo pridáva nové možnosti ako napríklad: bohatý systém posuvných okien, možnosť miešania prúdiacich dát a statických dát a tiež možnosť pridať vlastnú logiku vo forme analytických funkcií.

StreamBase EventFlow je jazyk pre prúdove spracovanie vo forme tokov a operátorov ako grafických elementov. Používateľ má možnosť spájať tieto grafické elementy a vytvárať tak jednoducho topológiu pre prúdové spracovanie bez nutnosti programovania. EventFlow integruje všetky možnosti StreamSQL.

Použitie StreamBase sa výborne hodí pre štrukturované aplikácie "reálneho času", ktoré majú za cieľ rýchle spracovanie spolu s rýchlym prototypovaním a nasadením nových funkcionalít.



Obrázok 3.4: Vývojové prostredie nástroja StreamBase.

## 3.5 Spark

Spark je klastrový výpočtový systém. Kombinuje spracovanie uložených dát v dávkovom móde so spracovaním prúdu údajov v reálnom čase (Cimerman and Ševcech, 2015). Cieľom Spark-u je poskytnúť rýchlu výpočtovú platformu pre analýzu dát. Spark poskytuje všeobecný model výkonávania ľubovoľných dopytov, ktoré sú výkonávané v hlavnej pamäti (pokiaľ ide o prúdové spracovanie). Tento model je nazvaný *Pružný distribuovaný dataset*, skr. RDD (angl. Resilient Distributed Dataset), čo je dátova abstrakcia distribuovanej pamäti. Keďže výpočet beží v hlavnej pamäti (pri prúdovom spracovaní), nie je potrebné vykonávať zápisu na disk, vďaka čomu môže byť dosiahnuté spracovanie v reálnom čase. Výpočet prebieha vo veľkom klastri uzlov s dosiahnutím odolnosti voči chybám za použitia RDD. RDD sídli v hlavnej pamäti, ale môže byť periodicky ukladaný na disk. Vďaka distribuovanej povahе RDD môže byť stratená časť RDD obnovená z pamäti iného uzla. Samotné prúdové spracovanie nie je vykonávané správa po správe (angl. message by message), ale v mikro dávkach, ktoré môžu byť automaticky paralelne distribuované v strapci. Spark Streaming<sup>2</sup> alebo tiež, prúdové spracovanie, si v poslednej dobe vyžiadalo špeciálnu pozornosť od tvorcom programovacieho rámca. Reagujú tým na vysoký dopyt odbornej verejnosti po prúdovom spracovaní dát, ktoré chýbalo v Spark-u. Spark Streaming poskytuje integrované rozhranie API pre rôzne programovacie jazyky, pričom v budúcnosti je snaha toto rozhranie úplne integrovať s dávkovým spracovaním, aby mohli vývojári používať rovnaké dátové typy pre rôzne typy úloh. Poskytuje tiež aspoň raz (angl. at least once) schému doručenia správ a zaručuje tak odolnosť voči chybám a prípadnej strate správy. Prúdové spracovanie v Spark-u je jednoduché integrovať spolu s dávkovým spracovaním, ktoré poskytuje, či použiť spolu s knižnicou pre strojové učenie sa.

---

<sup>2</sup><http://spark.apache.org/streaming/>



## 4. Klasifikácia prúdu dát použitím rozhodovacích stromov

Teda, kladieme nasledujúce hypotézy:

**Hypotéza 4.0.1** *Naše riešenie detektuje trendy v prúde dát s istou pravdepodobnosťou použitím polo-automatického výberu vhodnej metódy pre detekciu trendov a zároveň poskytuje výsledky v reálnom čase*

**Hypotéza 4.0.2** *Metóda je ľahká na použitie a interpretované výsledky sú jednoduché na pochopenie pre doménového experta bez detailnej znalosti o fungovaní modelu.*

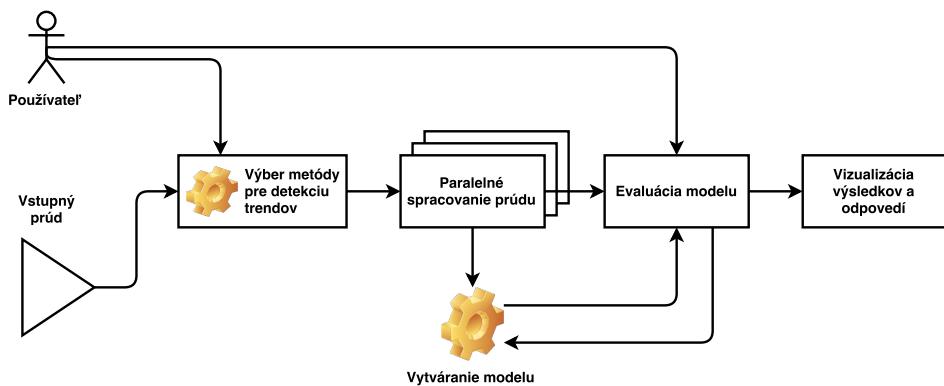
Pri detekcii trendu bude nutné zohľadniť nasledujúce elementy:

- anomálie, chyby a spam,
- sezónnosť dát,
- concept drift a zmeny,

V situácii keď potrebuje doménovy expert analyzovať trend v dátach reálneho sveta, je často potrebná najprv detailná znalosť dát, ktorú doménový expert, predpokladáme má. Potom, pre to, aby vedel správne analyzovať trend, sa potrebuje oboznámiť s viacerými modelmi a následne ich vyhodnotiť. Práve túto činnosť chceme uľahčiť doménovým expertom našou metódou. Nami navrhovaná metóda, schematicky zobrazená na 4 pozostáva z nasledujúcich krokov:

1. Používateľ vyberie metódu, ktorú chce aplikovať na analýzu trendu v prúde dát. Používateľ môže metódu vybrať sám, alebo nechá aplikáciu aby mu odporučila podľa vzorky dát vhodnú metódu.

2. Paralelne sa nepretržite spracuje a analyzuje prúd údajov. Zároveň je vytváraný model.
3. Po každej spracovanej správe je model vyhodnotený viacerými metrikami. Podľa výsledku evaluácie sa upraví aktuálny model.
4. Posledným krokom je prezentácia výsledkov používateľovi vo forme vizualizácie.



**Obrázok 4.1:** Schematický návrh metódy pre semi-automatickú analýzu trendov.

## 5. Zhodnotenie a budúca práca



# Literatúra

- Anagnostopoulos, C., Adams, N. M., and Hand, D. J. (2008). Deciding what to observe next: adaptive variable selection for regression in multivariate data streams. In *Proceedings of the 2008 ACM symposium on Applied computing*, pages 961–965. ACM.
- Babcock, B., Babu, S., Datar, M., Motwani, R., and Widom, J. (2002). Models and issues in data stream systems. In *Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 1–16. ACM.
- Babu, S. and Widom, J. (2001). Continuous queries over data streams. *ACM Sigmod Record*, 30(3):109–120.
- Bifet, A., de Francisci Morales, G., Read, J., Holmes, G., and Pfahringer, B. (2015). Efficient online evaluation of big data stream classifiers. In *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 59–68. ACM.
- Bifet, A. and Frank, E. (2010). Sentiment knowledge discovery in twitter streaming data. In *Discovery Science*, pages 1–15. Springer.
- Bifet, A., Holmes, G., Kirkby, R., and Pfahringer, B. (2010). MOA: massive online analysis. *Journal of Machine Learning Research*, 11:1601–1604.
- Bockermann, C. and Blom, H. (2012). Processing data streams with the rapidminer streams-plugin. In *Proceedings of the 3rd RapidMiner Community Meeting and Conference*.
- Brzeziński, D. (2010). *Mining data streams with concept drift*. PhD thesis, Master’s thesis, Poznan University of Technology.
- Cimerman, M. and Ševcech, J. (2015). *Analýza prúdu údajov*.

- Domingos, P. and Hulten, G. (2000). Mining high-speed data streams. In *Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 71–80. ACM.
- Gama, J., Medas, P., Castillo, G., and Rodrigues, P. (2004). Learning with drift detection. In *Brazilian Symposium on Artificial Intelligence*, pages 286–295. Springer.
- Hall, M., Frank, E., Holmes, G., Pfahringer, B., Reutemann, P., and Witten, I. H. (2009). The weka data mining software: an update. *ACM SIGKDD explorations newsletter*, 11(1):10–18.
- Han, J., Pei, J., and Kamber, M. (2011). *Data mining: concepts and techniques*. Elsevier.
- Hill, D. J. and Minsker, B. S. (2010). Anomaly detection in streaming environmental sensor data: A data-driven modeling approach. *Environmental Modelling & Software*, 25(9):1014–1022.
- Hill, D. J., Minsker, B. S., and Amir, E. (2007). Real-time bayesian anomaly detection for environmental sensor data. In *Proceedings of the Congress-International Association for Hydraulic Research*, volume 32, page 503. Citeseer.
- Hodge, V. J. and Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review*, 22(2):85–126.
- Hulten, G., Spencer, L., and Domingos, P. (2001). Mining time-changing data streams. In *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 97–106. ACM.
- Ikonomovska, E. and Zelke, M. (2013). Algorithmic techniques for processing data streams. *Dagstuhl Follow-Ups*, 5.
- Krempl, G., Žliobaite, I., Brzeziński, D., Hüllermeier, E., Last, M., Lemaire, V., Noack, T., Shaker, A., Sievi, S., Spiliopoulou, M., et al. (2014). Open challenges for data stream mining research. *ACM SIGKDD Explorations Newsletter*, 16(1):1–10.
- Liu, X., Wu, X., Wang, H., Zhang, R., Bailey, J., and Ramamohanarao, K. (2010). Mining distribution change in stock order streams.

- Madden, S., Shah, M., Hellerstein, J. M., and Raman, V. (2002). Continuously adaptive continuous queries over streams. In *Proceedings of the 2002 ACM SIGMOD international conference on Management of data*, pages 49–60. ACM.
- Muthukrishnan, S. (2005). *Data streams: Algorithms and applications*. Now Publishers Inc.
- Olston, C., Jiang, J., and Widom, J. (2003). Adaptive filters for continuous queries over distributed data streams. In *Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, pages 563–574. ACM.
- Ross, G. J., Tasoulis, D. K., and Adams, N. M. (2009). Online annotation and prediction for regime switching data streams. In *Proceedings of the 2009 ACM symposium on applied computing*, pages 1501–1505. ACM.
- Stankovic, J. A. and Zhao, W. (1988). On real-time transactions. *ACM Sigmod Record*, 17(1):4–18.
- Tran, D.-H., Gaber, M. M., and Sattler, K.-U. (2014). Change detection in streaming data in the era of big data: models and issues. *ACM SIGKDD Explorations Newsletter*, 16(1):30–38.
- Wadewale, K. and Desai, S. (2015). Survey on method of drift detection and classification for time varying data set.
- Zliobaite, I. and Gabrys, B. (2014). Adaptive preprocessing for streaming data. *IEEE transactions on knowledge and data Engineering*, 26(2):309–321.



# Prílohy

## A Plán na Letný semester 2016/2017

- TODO
- TODO

## B Plán na zimný semester 2016/2017

- Rozšírenie analýzy o ďalšie metódy a celkovo zpresnenie, zprehľadnenie a orezanie analýzy.
- Dokončenie návhu vlastnej metódy.
- Implementácia metódy.
- Evaluácia metódy - toto je priamo súčasťou navrhovanej metódy.
- Príprava článku na nejakú konferenciu, napr. IIT.SRC.
- Prvý experiment s použitím Eye Tracker-a na evaluáciu vizualizácie výsledkov.



