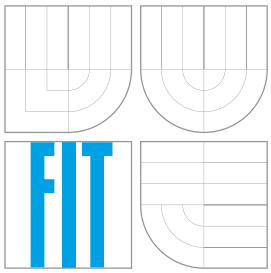
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

MODELY DŮVĚRY V POČÍTAČOVÝCH SYSTÉMECH

TRUST MODELS IN COMPUTER SYSTEMS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

LUKÁŠ GALBIČKA

VEDOUCÍ PRÁCE
SUPERVISOR

Doc. Ing. FRANTIŠEK ZBOŘIL, Ph.D.

BRNO 2016

Zadání bakalářské práce/18317/2015/xgalbi01

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2015/2016

Zadání bakalářské práce

Řešitel: **Galbička Lukáš**
Obor: Informační technologie
Téma: **Modely důvěry v počítačových systémech**
Trust Models in Computer Systems
Kategorie: Umělá inteligence

Pokyny:

1. Seznamte se s pojmem důvěra při použití v počítačových aplikacích. Dále se seznamte s pojmy agent, norma a závazek.
2. Navrhněte model, ve kterém by bylo možné sledovat důvěru mezi jednotlivými prvky a její vývoj během jednání těchto prvků v systému. Pro tyto účely do modelu zahrňte právě normy a závazky.
3. Ve vhodně zvoleném implementačním nebo simulačním nástroji realizujte tento model pro nějakou reálnou aplikaci (P2P sítě, bezdrátové sítě, komunitní weby).
4. Sledujte chování modelu během jeho vykonávání a zhodnoťte jeho validitu.
5. Diskutujte přínos modelování důvěry a možné využití při návrhu a realizaci reálných počítačových systémů.

Literatura:

- Plánování a komunikace

Pro udělení zápočtu za první semestr je požadováno:

- První dva body zadání

Podrobné závazné pokyny pro vypracování bakalářské práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva bakalářské práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap (20 až 30% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Zbořil František, doc. Ing., Ph.D.**, UITS FIT VUT
Datum zadání: 1. listopadu 2015
Datum odevzdání: 18. května 2016

L.S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Táto bakalárska práca sa zaoberá problematikou modelovania dôvery a reputácie v multiagentných sustémoch. Práca oboznamuje so základnými pojmami týkajúcich sa dôvery medzi agentmi. Predstavuje niekoľko modelov založených na dôvere a následne zameriava svoju pozornosť na jeden konkrétny, nad ktorým sú vykonané merania za účelom preskúmania praktickej funkčnosti modelu a jeho prípadného zlepšenia

Abstract

This bachelor's thesis deals with modeling of trust and reputation in multi-agent systems. It provides information about the basic concepts related to trust between agents. Several models based on trust are presented, one of which is chosen as a subject of measurements verifying its functionality. Possibilities for the model's improvement are explored based on the results of the measurements.

Klíčová slova

agent, dôvera, záväzok, norma, reputácia, model, odporúčanie

Keywords

agent, trust, obligation, norm, reputation, model, recommedation

Citace

GALBIČKA, Lukáš. *Modely důvěry v počítačových systémech.* Brno, 2016. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Zbořil František.

Modely důvěry v počítačových systémech

Prohlášení

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Doc. Ing. Františka Zbořila, Ph.D.. Uviedol som všetky literárne pramene a publikácie, z ktorých som čerpal

. . . . . .
Lukáš Galbička
16. května 2016

Poděkování

Ďakujem Doc. Ing. Františkovi Zbořilovi, Ph.D. za vedenie mojej bakalárskej práce

© Lukáš Galbička, 2016.
Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

Seznam obrázků

Kapitola 1

Úvod

V dnešnom svete hraje pojem dôvera kľúčovú rolu. Tento pojem má svoj pôvod v sociológii, no dnes je využívaný v rade iných vedných oborov, ako psychológií, ekonomike či v informatike.

Dôveru si budujeme k našej rodine a najbližším v našom okolí. Tento kruh dôvery sa však väčšmi rozširuje a je potreba si dôveru budovať v celej spoločnosti, v ktorej žijeme. Vďaka internetu a globalizácii je potreba vytvárať dôverné vzťahy naprieč ľudmi, skupinami a inštitúciami nielen v rámci regiónu, ale aj celosvetovo. Každá naša interakcia so svetom vôkol nás vyvoláva odozvu, ktorá môže mať za následok posilnenie dôvery, či jej prepad.

Výskum dôvery v oblasti informatiky so zameraním na umelú inteligenciu je zameraný predovšetkým na jej prevedenie z reálneho sveta do prostredia virtuálnych distribuovaných agentných systémov. Cieľom je vývoj metód a algoritmov, ktoré umožnia dosiahnutie väčšej racionality umelých agentov z pohľadu ich rozhodovania v zložitých sociálnych interakciách.

V tejto bakalárskej práci sa najskôr pozrieme na základné pojmy, ktoré s dôverou bezprostredne súvisia, ako sú norma, záväzok, reputácia či odporúčanie. Následne si predstavíme tri modely dôvery a reputácie, ktoré si zakladajú na vzájomných vzťahov agentov. Oboznámime sa s ich princípom fungovania a ich prípadnými slabosťami.

Druhá časť práce sa zameriava na výber jedného z predstavených modelov, nad ktorým vykonané merania preukážu jeho praktickosť a flexibilitu v rámci agentného systému. Výsledky budú porovnávané s modelom, pri ktorom budú hodnoty dôvery a reputácie vypočítavané v celku jednoduchým spôsobom a to aritmetickým priemerom hodnotení. Zistíme v čom spočíva robustnosť zložitého modelu a naopak, v ktorých prípadoch model celkom zlyháva. Následne sa pokúsime nedostatky odhalené pri meraní čiastočne vylepšiť. Samotná tvorba modelov dôvery a reputácie nie je súčasťou tejto bakalárskej práce.

Kapitola 2

Základné pojmy

2.1 Agent

V oblasti umelej inteligencie je agenta možno chápať, ako „zariadenie“, ktoré reaguje na podnety zo svojho prostredia. Môže nastať mylná predstava, že agent je výhradne stroj, akoby robot. Agentom však môže byť takisto bezpilotné auto, postava vo videohre či proces komunikujúci s inými procesmi. Agent sa vyznačuje vlastnosťami ako autonómnosť, nezávislosť (koná samostatne na základne vnútorných pravidiel), adaptívnosť(schopnosť učiť sa a prispôsobovať sa) [11], jedná lokálne (nepozná stav celého systému) a dokáže komunikovať s ostatnými. Týmito vlastnosťami sa agenti odlišujú od programov, ktoré väčšinou z uvedených vlastností nedisponujú.

Väčšina agentov má senzory, ktorými získavajú informácie zo svojho okolia a výkonné jednotky, ktorými ich ovplyvňujú. V prípade reálneho sveta medzi senzory môžu patriť mikrofóny, kamery, detektory pohybu a v prípade agenta pracujúceho ako proces sa jedná skôr o vstupné parametre či informácie hlásené inou výpočtovou jednotkou. Príkladom výkonnej jednotky (tiež nazývané *efektory*) môžu byť kolesá, krídla či ohybné rameno s klepetom.

Vlastnosti a reakcie agenta sa môžu zlepšovať s tým, ako sa agent učí. Toto učenie môže rozvíjať *procedurálne znalosti* (odpovede na otázky „ako?“) alebo ukladať *deklaratívne znalosti* (odpovede na otázky „čo?“). Procedurálne znalosti sa väčšinou nadobúdajú formou pokusov a omylov. Tento prístup umožnil vyvinúť agentov, ktorí postupne zlepšujú svoje schopnosti v kompetitívnych hrách, ako sú napríklad šachy. Učením deklaratívnych znalostí agent obvykle upravuje získané „fakty“ vo svojom úložisku informácií.

Riešenie problému

Bez znalosti cieľa agenti iba reagujú na podnety, no nedokážu plánovať svoje konanie. Pozrime sa na túto vec trochu abstraktnejšie.

Agent vychádza z prostredia, v ktorom sa nachádza. Prostredie je jeho „svetom“, ktorý sa mení aj jeho vlastným pôsobením. Stavy prostredia určujú aký bol, je a aký bude. V abstraktnej množine môžeme opísať svet pomocou množiny všetkých jeho možných stavov. Abstraktný priestor stavov sveta je miesto, v ktorom dochádza k riešeniu problémov. Agent vždy smeruje za určitým cieľom. Ten môže byť splnený, alebo nesplnený. Vyjadrením cieľa je množina všetkých stavov, v ktorých je cieľ splnený. Cieľ je možno dosiahnuť aj bez potreby riešiť problémy. Taká situácia je však zriedkavá, pretože problém nastane vtedy, keď aktuálny stav, nespadá do cieľovej množiny. Problém je teda rozpor medzi tým, čo je a tým, čo si agent želá. Vtedy je potrebné riešiť problém v procese riešenia problémov. [8]

Proces riešenia problémov už potom závisí od konkrétneho problému, ktorému agent čelí.

2.2 Objekt a subjekt

Pred definovaním pojmov, ktoré súvisia s medziagentnými vzťahmi, je potreba si najskôr definovať dva pojmy, ktoré budú v nasledujúcich podkapitolách používané.

Pojem *objekt* označuje nejaký prvok či entitu systému, pre ktorú je dôvera či reputácia stanovená. Je to teda cieľ dôvery. Objekt nemusí byť „inteligentná“ entita. Môže sa jednať napríklad o softvér či súbor. V anglickom jazyku je tomuto pojmu ekvivalent *trustee*.

Pojem *subjekt* označuje entitu, z ktorej pohľadu je dôvera či reputácia vyhodnocovaná vzhľadom k objektu. Subjekt teda musí byť určitým spôsob „inteligentný“, aby mohol objekt zmysluplne ohodnotiť. V niektorých modeloch dôvery je explicitne definované či je dôvera stanovená medzi subjektom a subjektom, a či medzi subjektom a objektom. V anglickom jazyku je tomuto pojmu ekvivalent *trustor*, niekedy *truster*. Vzťah medzi týmito entitami by sa teda dal popísať ako „dôvera subjektu v objekt“ prípadne „dôvera subjektu v objekt na základe reputácie objektu“.

2.3 Norma a Záväzok

Napriek poradí pojmov v názve sekcií, sa najskôr zoznámime s pojmom záväzok a až následne s normou.

> *„Záväzok, alebo obligácia, znamená vzťah medzi dvoma ľudmi či skupinami, z ktorých jednej plynie povinnosť v budúcnosti niečo dať,urobiť či nerobiť, zatiaľčo druhej oprávnenie splnenie záväzku očakávať, prípadne vymáhať.“*

Týmito slovami záväzok formuluje staroveké rímske právo [7]. Je jasné, že definícia záväzku sa od staroveku nijak nezmenila a teda platnosť tohto tvrdenia trvá do dnes.

Forma záväzku sa môže výrazne líšiť v pravidlách aj závažnosti. Napríklad, osoba spravujúca pozíciu politika má vo všeobecnosti ďaleko viac záväzkov, než priemerný dospelý občan, ktorý ich má zas viacej, ako neplnoleté dieťa. Možno povedať, že záväzok je určitá forma zodpovednosti plniť svoje povinnosti, ktoré nám boli pridelené niekym iným či samými sebou a my sme sa ich rozhodli, aj nedobrovoľne, prijať. Je však potreba si význam záväzku premietnuť do oblasti umelej inteligencie a ujasniť si, ako záväzok chápeme v multiagentných sieťach.

Prostredníctvom záväzkov vyjadrujú agenti vôľu spolupracovať. Záväzkom jeden agent utvrdzuje druhého v tom, že prijal nejaký mentálny postoj a že jeho zámerom je tento mentálny postoj udržovať. Obecne agent, ktorý záväzok prijal, má vykonať nejakú službu, ktorú po ňom žiada iný agent. Táto služba môže byť taktiež podmienená. Teda agent sa zaviaže, že splní sľúbený úkon len v prípade ak bude splnená určitá, predom stanovená podmienka. [21]. Vo väčšine prípadov sú medzi agentmi zjednávané záväzky podmienené. Výnimku tvoria práve *normy* definované v rámci skupiny.

Môžeme tvrdiť, že normy sú mechanizmy, ktoré si spoločnosť vytvorila, aby ovplyvnila správanie agentov v nej samej. Normy môžu byt tvorené z rôznych zdrojov, od pevne vstavaných noriem po jednoduché dohody medzi agentmi. Môžu trvať rôzne dlhú dobu, do doby kedy agent vystúpi zo spoločnosti, dokedy sa nesplní určitá stanovená podmienka či kým nenastane ďalšia najbližšia časové jednotka.

Norma je teda záväzok, ktorý je spoločne prijatý a dodržiavaný vrámci celej skupiny. Podľa definovaných noriem sú agentom špecifikované určité „normatívne ciele“. Tie môžu byť priamo určené alebo je ich úlohou zabrániť naplneniu iných cieľov (ako prípad prohibície). Normy nemusia byť vždy aplikovateľné a ich aktivácia závisí od kontextu, v ktorom sa agent nachádza. Taktiež môžu nastať výnimočné stavy, v ktorých agenti nie sú zaviazaní konať v zhode s normami. Pri definovaní noriem môže existovať predpis pre udeľovanie trestov a odmien, v závislosti od plnenia normatívnych cieľov, ktoré sa agenta týkajú [10].

2.4 Dôvera

V tejto podkapitole si definujeme pojem *dôvera*. Najskôr zo všeobecného hľadiska, následne z hľadiska informatiky.

Dôveru možno chápať ako vzťah, kedy vkladáme nádej do inej osoby, inštitúcie či veci. Najpriaznivejšie hľadisko pre skúmanie dôvery je ak si ju rozdelíme podľa jednotlivých konceptov. Oblasti, ktorých sa dôvera priamo či nepriamo dotýka je mnoho. Medzi najvýraznejšie možno zaradiť napríklad dôveru z oblasti politologických a sociologických štúdií.

Sociologický pohľad podľa Anthonyho Giddensa [4] vraví, že dôvera je :

> *„dôverčivosť v, či spoliehanie sa na, určitú vlastnosť alebo atribút osoby alebo veci, či pravdivosť tvrdenia“*

Veľký sociologický slovník [20] zase definuje dôveru nasledovne :

> *„Dôvera je typ postoja a zároveň medziľudského vzťahu, ktorý vyvoláva pocit istoty plynúci z presvedčenia, že partner komunikácie (osoba, inštitúcia) splní určité očakávania.“*

Možností ako vysvetliť tento pojem je viacero. Všetky sa ale zhodujú na tom, že sa jedná o poctivý vzťah k okoliu, ktorý sa zakladá na predpoklade, že okolie dodrží očakávané modely chovania a konania vo vzťahu k nám. Dôveru teda možno brať, ako akt spojený s budúcimi rozhodnutiami, ktoré ovplyvnia náš vzťah s okolím. Jedná sa teda o pomerne riskantný krok konania, pretože nemožno zaručiť, že dôvera nebude zneužitá druhou stranou.

Vzhľadom k tomu, že existuje celá rada vedeckých prací rôznych autorov zaoberajúcich sa popisom dôvery, možno odvodiť vlastnosti, ktoré sú pre dôveru charakteristické.

1. Dôvera je reflexívna, teda A dôveruje samému sebe.
2. Dôvera nie je obecne tranzitívna, teda ak A dôveruje B a B dôveruje C, A nemusí dôverovať C.
3. Dôvera je asymetrická, teda keď A dôveruje B, B nemusí (rovnakou mierou) dôverovať A.
4. Dôvera je individuálna, teda A a B dôverujú C rôznou mierou.
5. Dôvera je dynamická, teda sa v čase mení.
6. Dôvera je kontextová, teda A dôveruje B na základe kontextu x.

2.5 Reputácia

V tejto podkapitole sa pozrieme na pojem *reputácia*. Čo ho definuje a ako súvisí s dôverou. Reputácia je jedným z hlavných mechanizmov, pomocou ktorého môžeme získať ďalšie informácie pri budovaní dôvery voči danému objektu. Podobne ako pri dôvere, jedná sa o abstraktný pojem, teda jeho definícia môže byť miestami sporná. V odbornom článku *Can We Manage Trust?* od autorov *Audun Jøsang*, *Claudia Keser* a *Theo Dimitrakos* [5] je reputácia definovaná nasledovne:

> *„Reputácia je to, čo je obecne známe o charaktere či postoji ľudí, či vecí.“*

Tento opis ilustrujú vetami: *„Verím ti na základe tvojej dobrej reputácie.“*, alebo *„Verím ti napriek tvojej zlej reputácii.“* Prvá veta vypovedá o tom, že subjekt dôveruje objektu na základe verejne známom kontexte. Druhá veta zas predstavuje situáciu, kedy je medzi subjektom a objektom nejaká dôverná znalosť, ktorá nie je verejne známa a nepodieľa sa na vytváraní celkovej reputácie, ktorou daný objekt oplýva pre ostatné subjekty.

Reputácia môže byť chápaná skrz spoločenský alebo osobný názor na objekt a aj napriek tomu, že sa jedná o skupinový názor, je vnímanie reputácie vždy subjektívne. Možno ju teda považovať za prognostiku budúceho správania objektu na základe jeho minulých činov. Reputácia môže byť založená na základe dôvery rovnako tak, ako dôvera založená na reputácii. Pre prvý prípad by sa dal uvažovať príklad:

> Adam by rád využil služieb Cyrila. Adam nemá s Cyrilom žiadne osobné skúsenosti, preto sa spýta Borisa na jeho odporučenie na Cyrila. Adam si z Borisovej odpovede vytvorí názor na Cyrila. Z príkladu vidieť, že Adamova dôvera voči Cyrilovi bola založená na základe Cyrilovej reputácii u Borisa.

Pre druhý prípad by sa dal uvažovať príklad:

> Boris má stanovenú mieru dôvery voči Cyrilovi, len na základe vlastných skúseností. Ak sa Adam spýta na Borisov názor na Cyrila, tak Boris poskytne odporúčanie stanovené na základe miery dôvery vzhľadom ku Cyrilovi. Toto odporúčanie si Adam agreguje s prípadnými ďalšími odporúčaniami a vzniká tým reputácia Cyrila.

2.5.1 Reputácia ako výsledok dodržiavania noriem

V podkapitole 2.3 sme sa zoznámili s pojmami záväzok a norma. Bolo povedané, že normy môžu mať definovaný systém odmien a trestov v závislosti od toho, ako ako agent dodržuje stanovené normy, respektíve ako sa snaží plniť normatívne ciele. Agent môže byť odmeňovaný práve tým spôsobom, že povesť o jeho dobrej povahe sa rozšíri medzi ostatných agentov. Tí mu tým pádom budú viac naklonení dôverovať. Naopak, ako trest sa bude šíriť informácia o jeho zlej povahe a tým sa dá ostatným agentom na známosť, aby sa vyvarovali interakcii s týmto agentom, pretože tento agent nie je ochotný dodržiavať stanovené normy a plniť si svoje záväzky. A práve takéto šírenie informácii predstavuje reputáciu tohto agenta. Reputácia je teda výsledok dodržiavania noriem a plnenia svojich záväzkov. Vo výsledku nám reputácia plne nahradzuje pojmy norma a záväzok. Preto sa nimi viac nebudeme zaoberať a pozornosť zameriame výhradne na reputáciu a jej vzťah k dôvere.

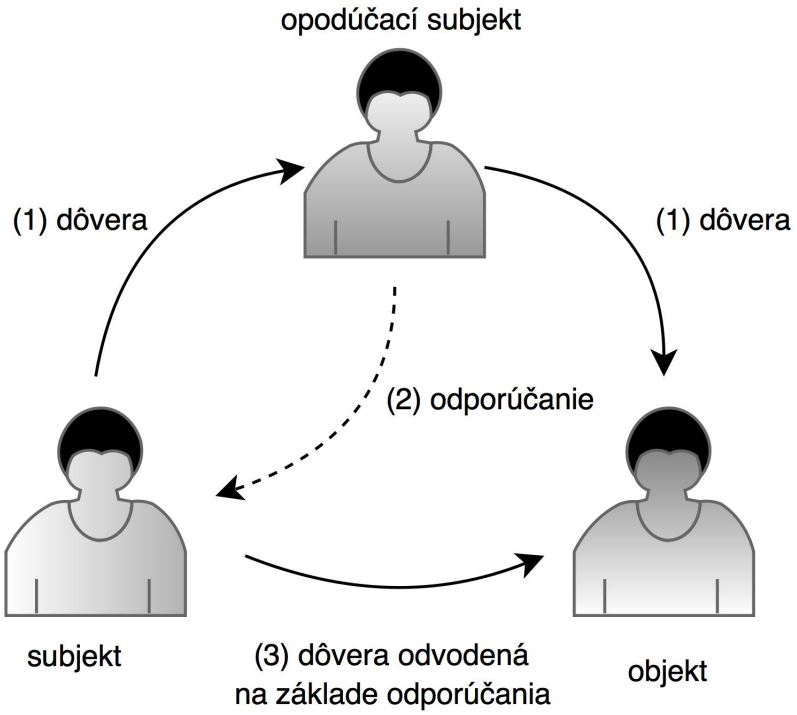
2.6 Odporúčanie

Vo vyššie písanom texte sa vyskytol pojem *odporúčať*. Tento výraz popisuje faktor, ktorý je pri budovaní verejnej reputácie veľmi dôležitý.

Jan Samek, autor svojej dizertačnej práce *Důvěra a reputace v distribuovaných systémech* [19], definoval odporúčanie nasledovne:

> *„Odporúčanie je predávanie subjektívnej informácie (názoru) alebo znalosti medzi dvoma subjektmi vzhľadom k nejakému aspektu (alebo aspektom, vlastnostiam) konkrétneho objektu“*

Teda aby odporúčajúcí subjekt mohol o objektu odporúčanie vykonať, musí mať o objekte nejakú znalosť. Odporúčanie je prevažne vykonávané na základe dôvery medzi odporúčajúcím subjektom a objektom. Obrázok 2.1 popisuje tento potrebný vzťah. Medzi odporúčacím subjektom a subjektom , ktorý si odporúčanie vyžiadal musí existovať nejaký dôverný vzťah (1). Medzi odporúčacím subjektom a objektom rovnako tak (1). Odporúčací subjekt vykoná odporúčanie na objekt (2), následkom čoho si subjekt vytvorí dôveru voči objektu - vzniká reputácia (3).



Obrázok 2.1: Princíp odporúčania

Kapitola 3

Modely založené na dôvere a reputácii

Modely simulujúce dôveru a reputáciu medzi agentmi sú mnohé. Stali sa doménou výskumu širšieho zamerania ako len sociológie. Prenikajú do mnohých oborov, pričom výrazným podielom práve k informatike. V oblasti informačných technológii by sa dali neformálne rozdeliť na modely teoretické a praktické. Medzi teoretické možno zaradiť modely sofistikované a veľmi zložité, ktoré sa pohybujú prednostne v akademickej sfére. Ich popis je skôr formálny a matematicky definovaný. V reálom svete ich je často veľmi ťažko implementovať. Praktické modely sú opakom teoretických a ich zložitosť je podstatne menšia. Ich autormi bývajú skôr programátori než vedci a často si nájdu uplatnenie v reálnom svete. Príkladom veľmi jednoduchého modelu je systém hodnotenia predávajúcich na Amazon [1], kde sa počíta priemerné hodnotenie zo všetkých hodnotení, ktoré boli predávajúcemu od kupujúcich udelené. Takéto modely však nie sú príliš efektívne. Dajú sa ľahko obalamutiť a výsledné hodnotenie je potom skreslené a nepravdivé.

Návrh vlastného modelu

Zadanie práce vraví, aby bol vytvorený vlastný model, ktorý by sledoval dôveru medzi jednotlivými prvkami. Avšak tomuto kroku zadaniu nebola v tejto práci venovaná veľká pozornosť. Takéto modely, ktoré pracujú s dôverou a reputáciou medzi agentmi sú totižto voľne dostupné ako open source algoritmy a skôr ako vytvárať vlastný jednoduchý model, ktorý by v konečnom dôsledku postrádal väčší význam, je lepšie zamerať sa na už vytvorené modely, zistiť ich skutočnú funkčnosť a prípadne sa pokúsiť o ich zlepšenie. V nasledujúcich sekciách sa preto pozrieme na už navrhnuté modely, ktoré sú postavené na rozdielnych princípoch a majú mnohé ošetrenia voči zlomyseľným agentom, snažiacim sa systém rozvrátiť.

3.1 RATEWeb

Reputation Assessment for Trust Establishment among Web services (skrátene *RATEWeb*) [12] je systém pre budovanie dôvery v servisne–orientovanom prostredí. RATEWeb podporuje kooperatívny model, v ktorom webové služby (teda subjekty) zdieľajú svoje skúsenosti o poskytovateľoch služieb (teda objektoch) medzi sebou skrz spätno-väzobné hodnotenia (anglicky *feedback ratings*). Zo zozbieraných hodnotení sa odvodzuje celková reputácia konkrétneho poskytovateľa služieb. Cieľom je poskytnúť úplné riešenie pre tvorbu reputácie poskytovateľov služieb presným, spoľahlivým a decentralizovaným spôsobom. Navrhovaný

model berie tiež v úvahu prítomnosť zlomyseľných hodnotiacich, ktorí môžu striedavo poskytovať pravdivé a nepravdivé hodnotenia za účelom pošpiniť poskytovateľa služieb [1].

3.1.1 Entity modelu

V tejto sekcii si popíšeme kľúčové komponenty, z ktorých model pozostáva a ako sú tieto komponenty prepojené medzi sebou. Typické interakcie zahrňujú štyri entity: webové služby, poskytovateľov služieb, registre služieb a konzumentov služieb.

- *Webové služby* (anglicky *Web services*, skrátene *WS*) môžu byť braté ako kolekcia operácií, kde každá operácia je výpočtová jednotka, ktorá prijíma vstupné hodnoty (parametre) a generuje výstupné hodnoty (výsledky). Pre jednoduchosť uvažujeme vždy jednu operáciu na jednu službu.

- *Poskytovatelia služieb* (anglicky *Service providers*, skrátene *SP*) sú entita, ktorá poskytuje služby, teda robí ich dostupné pre konzumentov. Z fyzického hľadiska, SP môže byť napríklad firma, vládna agentúra alebo akademická inštitúcia. SP môže poskytovať jednu či viacero služieb, majú verejne známe identity a môžu či nemusia požadovanú službu spravovať. SP môže napríklad prenechať spracovanie konkrétnej služby tretej strane. Konzument služby potom môže či nemusí byť schopný rozoznať všetky strany podieľajúce sa na doručení konkrétnej služby. V tomto modely sa nečinia rozdiely medzi pojmom poskytovateľ služieb a poskytnutá webová služba. Teda ak hovoríme o nejakom SP, v skutočnosti sa jedná o WS, ktorá je poskytovaná.

- *Registre služieb* (anglicky *Service registries*, skrátene *SR*) je prehliadateľný adresár, ktorý obsahuje kolekciu popisov jednotlivých WS. SR má dva komponenty: repozitár popisu služieb a engine, ktorý odpovedá na požiadavky prijaté od SP a konzumentov služieb. SR môže byť verejný, alebo privátny. Každý SP môže inzerovať svoje schopnosti zverejnením WS vo verejnom SR. Privátny SR môže využiť len obmedzený počet vybraných SP na zverejnenie WS. V tomto modely sa zameriavame na využitie len verejných registrov a len za účelom lokalizovania odpovedajúcich SP. SR taktiež neukladajú žiadne dodatočné informácie spojené s reputáciou.

- *Konzumenti služieb* (anglicky *Service consumers*, skrátene *SC*) je entita, ktorá sa dožaduje WS, teda inteligentný agent, webová aplikácia, alebo iná webová služba. Ľudský užívateľ sa taktiež môže dožadovať WS, no predpokladáme, že každý užívateľ je v systéme reprezentovaný softvérovým komponentom (proxy). Proxy je zodpovedná za komunikáciu všetkých užívateľov a spravovanie požiadavkou užívateľa. To, ako je toho dosiahnuté, nie je súčasťou tohto modelu ani práce.

Budeme predpokladať symetrický interaktívny model, kde typická interakcia zahrňuje dve WS: jedna, SP, ktorá poskytuje nejakú funkcionalitu druhej, SC, ktorá sa prvej pre túto funkcionalitu dožaduje.

3.1.2 Interakcia služieb: rozšírenie skrz ontológie pre RATEWeb

Model predstavuje koncept *komunity*. Komunita je „kontajner“, ktorý zhlukuje WS, ktoré sú rovnakej oblasti záujmu. Komunity poskytujú popisy týchto služieb všeobecne bez odkazovania sa na konkrétnu službu z danej oblasti (teda na konkrétneho SP). Obrázok 3.1

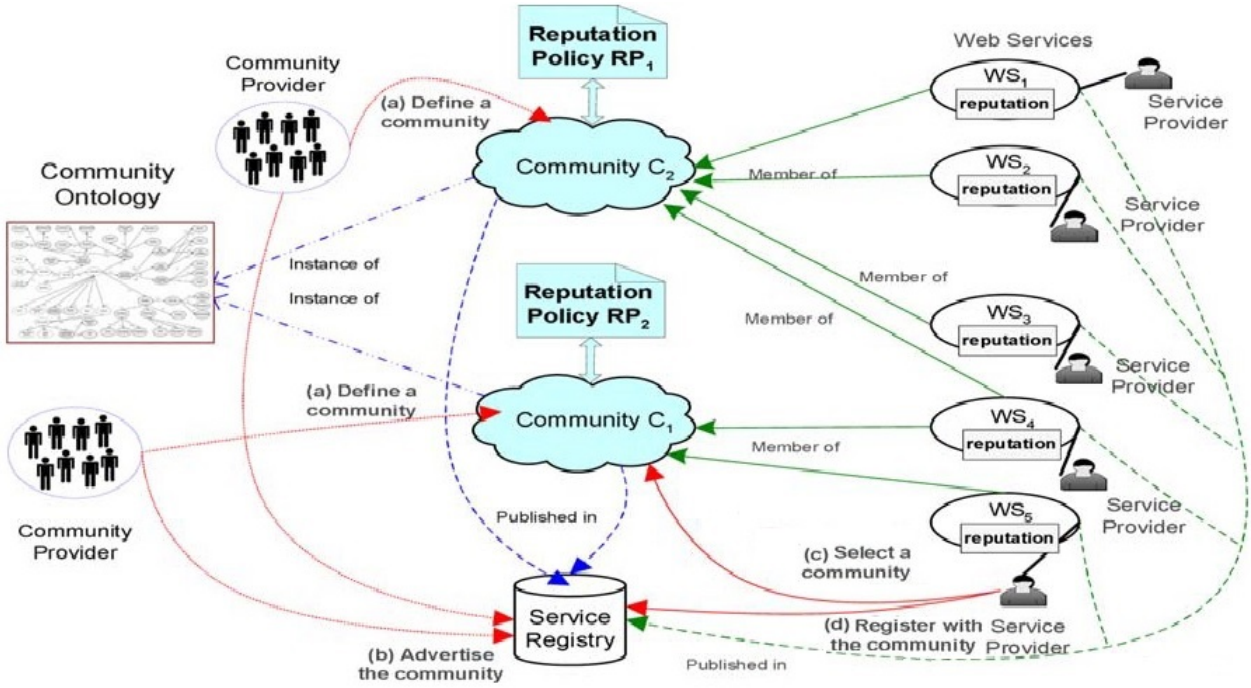
[1] Je treba podotknúť, že väčšina nasledujúceho textu vysvetľujúc princíp RATEWeb bola prebraná a preložená z odborného článku [12], ktorý tento model plne predstavuje.

vykresľuje proces vytvárania komunity a registrovania WS do nej. Komunity sú definované poskytovateľmi komunít (anglicky *Community providers*, skrátene *CP*) ako inštancia komunitnej ontológie. Fyzickým CP sú spravidla štátne agentúry, neziskové organizácie a firmy ktoré zdieľajú spoločnú oblasť záujmu. Ďalšou povinnosťou CP môže byť definovať politiku reputácie. Môžu byť stanovené pravidlá ako :

I stanoviť hraničné hodnoty reputácie pre členov, ktorých sa musia držať

II určiť, čo sa má stať, ak reputácia člena komunity klesne pod danú hraničnú hodnotu

III definovať požiadavky na nových členov



Obrázok 3.1: Tvorba komunity a registrácia služby v RATEWeb

Komunita C_i je formálne definovaná n-ticou ($Identifikátor_i, Kategória_i, G-operácia_i$, $Členovia_i$). $Identifikátor_i$ obsahuje unikátne meno a textový popis vlastností C_i. $Kategória_i$ opisuje oblasť záujmu danej komunity. Všetky WS, ktoré spadajú do jedného C_i majú rovnakú kategóriu ako toto C_i. C_i je dostupná skrz set operácii zvaných generické operácie. Tie sú špecifikované v $G-operácii_i$ klauzuly. Generické operácie sú „abstraktné operácie“, ktoré zhrňujú hlavné funkcie potrebné členmi C_i. Pojem „abstraktné“ znamená, že žiadna implementácia nie je pre generické operácie poskytnutá. CP definujú len rozhranie pre každú generickú operáciu ako op_{ik}.

V RATEWeb je samotná komunita službou, ktorá je inzerovaná, objavovaná a volaná ako bežná WS. CP najskôr definujú komunitu podľa konceptu komunitnej ontológie (3.1, krok a) a následne ju publikujú v registroch (3.1, krok b). SP tieto registre prezerajú pričom si zvolia komunitu (3.1, krok c), do ktorej by svoje služby chceli zaregistrovať. (3.1, krok d). Samotné priradenie WS do komunity je definované politikou reputácie. Registrované WS

daných SP nemusia spĺňať všetky operácie definované konkrétnou komunitou. Nakoniec, aby boli služby dostupné pre všetkých SC, SP ich musí publikovať v SR. SP môže publikovať svoju WS v jednom či viacerých registroch. Napríklad WS 4 môže poskytovať služby rôznych domén záujmu (napr. finančníctvo a predaj automobilov), teda svoje služby registruje vo viacerých komunitách a to za predpokladu, že spĺňa politiku reputácie všetkých týchto komunít.

SC pristupujú k SR pre zistenie ponuky komunít a poskytovateľov. Konzumentov dopyt môže pozostávať z operácii, ktoré by rád invokoval. Môže sa stať, že požadované operácie sa budú zhodovať s ponukou viacerých rozdielnych komunít. Každá táto komunita vytvorí list poskytovateľov, ktorí majú u nej tieto operácie registrované. Predpokladá sa, že komunity a registre sú neutrálne, teda majú nestrannú politiku pre poskytovateľov rôznych služieb. SC potom vyberie najlepšiu službu z poskytnutého listu. Výber je založený na reputácii každého poskytovateľa respektíve služby jednotlivo. Predpokladá sa, že pri poskytnutí tohto listu bude pri každom SP mimo „bežných" detailov dostupný zoznam konzumentov, ktorý v minulosti s týmto SP vykonali interakcie a poskytli spätnú väzbu. Komunita sa teda chová len ako adresár hodnotiacich, nie ako centrálny repozitár hodnotení. Hodnotenia sú teda držané lokálne u hodnotiacich. Konzument môže teda kontaktovať týchto peerov a dožadovať sa ich hodnotení. SC potom invokujú WS skrz jednu z vypísaných operácií. Konzument teda poskytne vybraným operáciám odpovedajúce vstupné hodnoty načo služba následne vráti výsledné hodnoty. Na konci interakcie konzument ohodnotí poskytovateľa na základe definovaných atribútov kvality. Konzument taktiež oznámi komunite, že u seba uchováva hodnotenia poskytovateľov, s ktorými vykonali interakcie. Tieto hodnotenia služieb sa primerane použijú na výpočet celkovej reputácie poskytovateľa.

3.1.3 Parametre vyjadrujúce kvalitu webovej služby

V kontexte servisne-orientovaného prostredia rozoznávame tri typy kvality WS ($QRef$): poskytovateľom-sľúbená $QRef$ ($QRef_p$), konzumentom-očakávaná $QRef$ ($QRef_r$) a službou-doručená $QRef$ ($QRef_d$). $QRef_p$ hodnoty sú tie, ktoré SP uverejnil cez SR. $QRef_r$ reprezentuje preferencie konzumenta pre každý parameter kvality. $QRef_d$ reprezentuje skutočnú kvalitu služby, ktorá je odhalená až po interakcii SC s SP. Mnohé $QRef_d$ parametre závisia na rozdielnych faktoroch, preto rôzni SC môžu vnímať kvalitu rôzne, dokonca aj keď sa poskytovateľ správa dôsledne ku všetkým SC.

3.1.4 Reputácia webovej služby

V RATEWeb modely reputácie žiadna samostatná entita nie je zodpovedná za zber, aktualizáciu a šírenie reputácie WS. Každý SC má vlastné záznamy reputácií služieb, s ktorými vykonal interakciu. Tento záznam sa volá *osobné ohodnotenie*. Pre každú službu s_j, s ktorou SC t_x vykonal interakciu si SC udržuje p-element vektor $PerEval_j^x$ reprezentujúci vnímanie správania služby s_j konzumentom t_x. Osobné ohodnotenie $PerEval_j^x$ reprezentuje vnímanie len jedného konzumenta t_x. Ohodnotenia iných CS sa môžu s týmto konzumentom zhodovať alebo môžu byť rozdielne. SC, ktorý sa na reputáciu SP táže ostatných SC, môže prijať rôznorodú spätnú väzbu. Aby bol odhad správania služby korektný, všetky osobné ohodnotenia pre s_j sa musia agregovať. Agregácia všetkých osobných ohodnotení pre výpočet jednej hodnoty reputácie je definovaná ako *odhadová reputácia* poskytovateľa služieb v očiach konzumenta. Každý konzument môže aplikovať inú techniku agregovania reputácie. Preto môže byť odhadovaná reputácia poskytovateľa pre každého zákazníka iná. Takéto poňatie odhadovanej reputácie sa pomerne líši od definície globálnej reputácie, pretože táto

reputácia nie je zhodná pre všetky služby. Je to agregovanie všetkých osobných ohodnotení čisto z pohľadu konzumenta t_x.

Definícia 3.1.1. Nech L značí skupinu konzumentov, ktorí v minulosti interagovali so s_j a želajú si zdieľať svoje osobné ohodnotenie pre s_j. Predpokladáme, že L nie je prázdne. Teda platí, že $L \subseteq T$, pričom $L \neq 0$ a každá služba x v L má $PerEval_j^x$ hodnôt pre s_j. Potom reputácia pre s_j z pohľadu konzumenta je definovaná ako:

$$Reputation(s_j) = \bigwedge_{x \in L} (PerEval_j^x) \tag{3.1}$$

kde $\bigwedge$ predstavuje funkciu agregácie. Rovnica 3.1 predstavuje prvú aproximáciu výpočtu reputácie. Avšak výpočet udelenej reputácie zahrňuje rôzne faktory, ktoré musia byť presne definované a merané.

3.1.5 Metriky pre výpočet reputácie

Metriky RATEWebu sú definované tak, aby zachytili väčšinu (ak nie všetky) aspekty sociálnej reputácie. Sú to:

1. *Vierohodnosť hodnotiaceho*: Model umožňuje SC, aby učinil svoje rozhodnutia na základe vierohodnosti hodnotiacich. Vierohodnosť hodnotiaceho vyjadruje, že ako veľmi môžu ostatní SC veriť jeho hodnoteniu vzhľadom na reputáciu WS, ktorej sa dožadovali. Toto umožňuje činiť rozdiely medzi dôverou v službu a dôverou v spätnú väzbu. Napríklad služba, ktorá nemá vysokú reputáciu ako poskytovateľ (malá dôvera v služby) môže byť hodnotný zdroj (veľká dôvera v spätnú väzbu) pri posudzovaní správania iných SP a naopak.

2. *Hodnotenie väčšiny*: Odhadovaná reputácia SP nie je čistá agregácia ohodnotení, ale je vypočítavané na základe väčšiny. Čím viac sa hodnotenie nejakého konzumenta líši od názoru väčšiny, tým menej je brané v úvahu pre výpočet celkovej reputácie SP.

3. *História hodnotení*: Model umožňuje, aby vierohodnosť hodnotiacich bola aktualizovaná na základe jeho histórie hodnotení.

4. *Osobná skúsenosť pre zváženie vierohodnosti*: Model berie do úvahy možnosť, že hodnotiaci sa môže mýliť. SC môžu zvážiť pravdivosť spätnej väzby podľa rozdielu medzi ich osobnou skúsenosťou a hodnotením, nahláseným ostatnými konzumentmi.

5. *Osobné preferencie*: Model poskytuje osobné vyhodnotenie reputácie, kde konzumenti môžu zvážiť rôzne atribúty $QRef$ vzhľadom na ich vlastné preferencie.

6. *Osobná skúsenosť pre odhad reputácie*: Väčšina SC, ktorá inteagovala s určitým SP v minulosti a bola spokojná, uprednostní tohto SP aj pri ďalších podobných službách. No ak SC vykonáva interakcie len s vybratým poskytovateľom, môže prísť o poskytovateľa s lepšou $QRef$. V RATEWeb modely sú nahlásené hodnotenia kombinované s *„first-hand“* skúsenosťou pre výpočet výslednej reputácie.

7. *Dočasná senzitivita*: Všetky hodnotenia majú dočasnú váhu dôležitosti, teda starším hodnoteniam sú dávané na menšiu zreteľ ako novšie.

3.1.6 Vierohodnosť hodnotiacich

Hlavnou nevýhodou feedback-only systémov je ich predpoklad, že všetky hodnotenia budú pravdivé a nezaujaté. Avšak v reálnom svete rozlišujeme medzi výpoveďou našich vlastných zdrojov a iných dôveryhodných zdrojov v systéme. Webová služba ktorá poskytuje uspokojivé služby (v súlade so sľúbenou kvalitou ($QRef_p$)) môže dostať nesprávne či falošné hodnotenie od rôznych hodnotiacich skrz niekoľko *zlomyseľných motívov*. Kvôli takýmto *„zlomyseľným“* hodnotiacim systém správy reputácie by mal zvážiť hodnotenie viacej dôveryhodných hodnotiacich viac, než hodnotiacich s nízkou vierohodnosťou. Pri RATEWeb, hodnota reputácie daného SP je vypočítaná na základe vierohodnosti hodnotiacich ako:

$$Reputation(s_j) = \frac{\sum_{x=1}^{L}(PerEval_j^x * C_r(x))}{\sum_{x=1}^{L} C_r(x)} \tag{3.2}$$

kde $Reputation(s_j)$ je hodnota reputácia pre s_j z pohľadu daného SC a $C_r(x)$ vierohodnosť hodnotiaceho x z pohľadu daného SC. Dôveryhodnosť hodnotiacich leží vždy v intervale $[0, 1]$, kde 0 predstavuje najnižšiu a 1 najvyššiu hodnotu dôveryhodnosti.

Vyhodnotenie dôveryhodnosti hodnotiaceho: Existuje niekoľko online systémov ako je eBay, Amazon, Yahoo! Auction a pod. ktoré používajú centralizovaný systém reputácie. Mnohé z týchto systémov sa spoliehajú výhradne na číselnú hodnotu obdržanú od rôznych užívateľov ako mieru reputácie. Hodnota reputácie je vypočítaná ako jednoduchý agregácia obdržaných hodnotení, ktoré nemusia úplne vystihovať dôveryhodnosť daného SP. Ku príkladu na eBay môže nakupujúci a predávajúci hodnotiť jeden druhého pozitívne (+1), neutrálne(0) alebo negatívne(-1). Centralizovaný systém reputácie vypočíta výslednú reputáciu ako sumu týchto hodnotení. Užívateľ s hodnotou 50 pozitívnej spätej odozvy bude mať potom rovnakú hodnotu reputácie ako užívateľ, ktorý obdrží 300 pozitívneho a 250 negatívneho hodnotenia. Iné systémy (napríklad Amazon) vypočítavajú celkovú reputáciu ako priemer všetkých hodnotení. Vezmime v úvahu sériu hodnotení: 9, 9, 9, 1, 1, 1, 1, 1. Hodnota reputácie takéhoto užívateľa bude 3,7. Je zrejmé, že tieto systémy hodnotenia sú zavádzajúce, nepresné a môžu byť ľahko zmanipulované. Preto navrhnúť systém hodnotenia, ktorý bude dostatočne robustný na detekciu a zmenšenie vplyvu nepravdivých hodnotení je základným problémom.

RATEWeb implementuje vlastný systém pre výpočet dôveryhodnosti užívateľov, pričom využíva schému hodnotenia väčšiny. Základná myšlienka je nasledujúca: Ak nahlásené hodnotenie súhlasí s názorom väčšiny, potom vierohodnosť užívateľa je zvýšená, v opačnom prípadne znížená. RATEWeb využíva techniku zhlukovania dát pre definovanie názoru väčšiny, teda podobné hodnoty spätnej odozvy sú zgrupované dohromady. Na vytvorenie „klastrov“ všetkých nahlásených hodnotení sa využíva $k--$mean klastrovací algoritmus. Klaster s najväčším počtom hodnotení ja potom braný ako „majoritný klaster“ a ťažisko tohoto klasteru je brané ako *názor väčšiny* (značené ako M):

$$M = \text{centroid}(\max(\mathcal{R}_k)) \quad \forall k$$

kde k predstavuje počet klasterov, $\max(x)$ vracia klaster $\mathcal{R}$ s najväčším počtom hodnotení a $\text{centroid}(x)$ vracia ťažisko klasteru x. Euklidova vzdialenosť medzi hodnotením väčšiny (M) a nahláseným hodnotením (V) potom určuje vierohodnosť hodnotiaceho. Zmena vo vierohodnosti skrz hodnotenie väčšiny, značená ako Mf, je definovaná ako:

$$Mf = \begin{cases} 1 - \frac{\sqrt{\sum_{k=1}^{n}(M-V_k)^2}}{\sigma} & \text{ak } \sqrt{\sum_{k=1}^{n}(M-V_k)^2} < \sigma \\ 1 - \frac{\sigma}{\sqrt{\sum_{k=1}^{n}(M-V_k)^2}} & \text{v opačnom prípade} \end{cases} \tag{3.3}$$

kde σ je štandardný odklon pre všetky nahlásené hodnotenia. Je potreba si uvedomiť, že Mf nepredstavuje hodnotu vierohodnosti hodnotiaceho ako takú, ale definuje efekt ktorý ovplyvňuje vierohodnosť skrz súhlas/nesúhlas s hodnotením väčšiny. Môžu nastať prípady, kedy väčšina hodnotiacich sa zhodne na poskytovaní falošného hodnotenia danému poskytovateľovi služieb. A čo viac, títo okrajoví hodnotiaci (tí, ktorí nespadajú do majoritného klasteru) môžu byť prví, ktorí budú s SP vykonávať interakciu. Je teda jasné, že samotná schéma hodnotenia väčšiny nie je spôsobilá, aby presne určila reputáciu danej webovej služby.

Schéma hodnotenia väčšiny je doplnená o určenie vierohodnosti hodnotiaceho na základe jeho minulého správania. Dôveryhodnosť je teda počítaná na základe „poslednej udelenej hodnoty reputácie“, súčasnom hodnotení väčšiny a aktuálnom hodnotení udelené hodnotiacim. Vierohodný hodnotiaci je teda ten, ktorý koná rozhodne, presne a preukázal sa byť užitočný naprieč časom.

Konzistencia je definované správanie služby, ktorá vykazuje podobné výsledky v ustálených podmienkach. To znamená, že pri kontrolovaných situáciach by sa vnímanie webovej služby konzumentom nemalo príliš odchyľovať, ale zostať konzistentné naprieč časom. RATEWeb predpokladá, že interakcia medzi službami nastane v čase t a konzument služieb má záznam o predchádzajúcich udelených hodnoteniach (značené ako A), čo je definované ako:

$$A = \bigsqcup_{t-1}^{t-k} \text{Reputation}(s_j)^t \tag{3.4}$$

kde Reputation(s_j) je definované ako v rovnici 3.1 pre každý časový prípad t, $\bigsqcup$ predstavuje operátor agregácie a k je doba času definovaná každým konzumentom služieb. Môže sa meniť od jednej doby času po kompletný záznam minulých hodnotení pre s_j. Všimnime si, že A nie je „osobné vyhodnotenie“ konzumenta alebo poskytovateľa služieb, ale je to „udelená reputácia“ vypočítaná konzumentom služieb v predchádzajúcich časových jednotkách. Ak sa správanie poskytovateľa služieb naprieč časom príliš nemení, A a aktuálne udelené hodnotenie V by malo byť podobné. Preto efekt vierohodnosti skrz súhlas/nesúhlas s posledným udeleným hodnotením (značené ako Af) je definované podobne ako v prípade rovnice 3.3, teda :

$$Af = \begin{cases} 1 - \frac{\sqrt{\sum_{k=1}^{n}(A-V_k)^2}}{\sigma} & \text{ak } \sqrt{\sum_{k=1}^{n}(A-V_k)^2} < \sigma \\ 1 - \frac{\sigma}{\sqrt{\sum_{k=1}^{n}(A-V_k)^2}} & \text{v opačnom prípade} \end{cases} \tag{3.5}$$

V reálnych situáciach je ťažké určiť rôzne faktory, ktoré spôsobujú zmenu v stave webovej služby. Hodnotiaci môže hodnotiť rovnakú službu rôznym hodnotením bez zlomyseľného motívu. Preto vierohodnosť hodnotiaceho sa môže výrazne meniť v závislosti od hodnôt V, Mf, a Af. Hlavná formula je:

$$C_r(x) = C_r(x) \pm \mathcal{N} * \Upsilon \tag{3.6}$$

kde $\mathcal{N}$ predstavuje normalizovaný faktor vierohodnosti a Υ reprezentuje veľkosť zmeny vierohodnosti skrz zhodu či rozdiel hodnoty V s M a A.

Na hodnotenia udelené v aktuálnej časovej jednotke je braná väčšia zreteľ ako na tie minulé, preto zhoda či rozdiel V s M má väčšiu prioritu ako V s A. Toto môže byť vidieť

z rovnice 3.6 kde znamienko + s $\mathcal{N}$ indikuje $V \cong M$, kým znamienko − s $\mathcal{N}$ znamená, že $V \neq M$. $\mathcal{N}$ je definované ako:

$$\mathcal{N} = C_r(x) \times (1 - |V_x - M|) \tag{3.7}$$

Rovnica 3.7 vraví, že hodnota normalizovaného faktoru $\mathcal{N}$ závisí od vierohodnosti hodnotiaceho a absolútneho rozdielu medzi aktuálnou spätnou väzbou a hodnotenia väčšiny. Vynásobenie tejto hodnoty vierohodnosťou hodnotiaceho umožňuje čestným hodnotiacim mať väčší vplyv na proces agregácie hodnotení a nečestných hodnotiacich odsúdi na rýchlu stratu vierohodnosti v prípade ich nepravdivého či zavádzajúceho hodnotenia. Rozdielne hodnoty pre Υ sú popísané nižšie. *Regulovanie vierohodnosti hodnotiacich:* Υ tvorí Mf a/alebo Af a „faktor pesimizmu“ (ρ). Presná hodnota ρ závisí od opatrnosti konzumenta s výnimkou, že jeho minimálna hodnota by mala byť 2. Čím nižšia hodnota ρ je, tým viac optimistickým sa konzument stáva a so stúpajúcou hodnotou ρ sa naopak zvyšuje jeho pesimizmus. Pesimistický konzument je taký, ktorý nedôveruje ľahko iným konzumentom, a ich vierohodnosť v jeho očiach sa po nepravdivej spätnej väzbe drasticky znižuje. Optimistický konzument naopak krátku nepravosť ľahko odpúšťa (dlhodobá nepravdivosť je taktiež trestaná) a ľahko si buduje dôveru voči iným na základe pravdivej spätnej väzby. V, M a A môžu byť vo vzájomnom vzťahu jedným zo štyroch spôsobov a každý z nich špecifikuje ako sú Mf a Af použité v modely.

1. Nahlásená hodnota reputácie je podobná hodnoteniu väčšiny a predchádzajúcej udelenej reputácii, teda ($V \cong M \cong A$). Rovnosť $M \cong A$ predpokladá, že väčšina hodnotiacich verí, že $QoWS$ poskytovateľa s_j sa nezmenila. Vierohodnosť hodnotiaceho služby je aktualizovaná ako:

$$C_r(x) = C_r(x) + \mathcal{N} * \left(\frac{|Mf + Af|}{\rho} \right) \tag{3.8}$$

2. Nahlásená hodnota reputácie je podobná hodnoteniu väčšiny, no líši sa od tej predchádzajúcej, teda ($V \cong M$) $\wedge$ ($V \neq A$). V takomto prípade zmena v hodnotení mohla nastať z dvoch dôvodov. Prvý, že hodnotiaci môže byť dohodnutý s inými konzumentmi na zvýšení/znížení reputácie pre s_j. Druhý, že $QoWS$ pre s_j sa mohlo zmeniť odkedy A bolo naposledy vypočítané. Vierohodnosť hodnotiaceho služby je aktualizovaná ako:

$$C_r(x) = C_r(x) + \mathcal{N} * \left(\frac{Mf}{\rho} \right) \tag{3.9}$$

3. Nahlásená hodnota reputácie je podobná hodnotiaceho poslednému nahlásenému hodnoteniu, ale líši sa od názoru väčšiny, teda ($V \neq M$) $\wedge$ ($V \cong A$). V sa môže od väčšiny líšiť skrz nasledovné. Za prvé, V môže poskytovať hodnotenie, ktoré je zastaralé. Po druhé, V sa snaží poskytnúť „falošné“ negatívne/pozitívne hodnotenie pre s_j. Treťou možnosťou je, že V poskytuje pravdivé hodnotenie, zatiaľčo ostatní konzumenti spadajúci pod M môžu spoločne zvyšovať/znižovať reputáciu pre s_j. Ani jedna z týchto možností by nemala byť prehliadaná. Vierohodnosť hodnotiaceho služby je aktualizovaná ako:

$$C_r(x) = C_r(x) - \mathcal{N} * \left(\frac{Af}{\rho} \right) \tag{3.10}$$

4. Nahlásená hodnota reputácie nie je podobná jak hodnoteniu väčšiny, tak ani predchádzajúcemu hodnoteniu, teda ($V \neq M$) $\wedge$ ($V \neq A$). Takáto situácie môže nastať

z viacerých dôvodov. V môže prvýkrát interagovať so zmeneným správaním s_j, V nemusí poznať aktuálnu hodnotu $QRef$ alebo V môže klamať za účelom zvýšenia/zníženia reputácie pre s_j. Vierohodnosť hodnotiaceho služby je aktualizovaná ako:

$$C_r(x) = C_r(x) - \mathcal{N} * \left(\frac{|Mf + Af|}{\rho} \right) \tag{3.11}$$

Pri RATEWeb, po každej interakcii, bokom od hodnotenia poskytovateľa s_j, Konzument služieb ohodnotí užitočnosť ostatných hodnotiacich, ktorí poskytli svoje hodnotenie služieb od s_j. Ak sa Euklidova Vzdialenosť medzi vlastnou skúsenosťou konzumenta a V_i poskytnuté od iného hodnotiaceho líšia viac ako o zadanú hranicu, V_i je brané ako neužitočné, inak je brané ako užitočné. Užitočnosť služby je požadovaná na výpočet tendencie hodnotiacich poskytovať nepravdivé hodnotenia. Môžu tiež nastať prípady, kedy hodnotiaci menia svoj postoj užitočnosti naprieč časom. Aby sme teda správne vyhodnotili konzumentov sklon k podvádzaniu, vypočítame *pomer* počtu užitočných hodnotení (k) ku celkovému počtu hodnotení (n). Tento pomer značíme ako u_f.

$$u_f = \frac{\sum_{i=1}^{k} U_i}{\sum_{X=1}^{n} V_x} \tag{3.12}$$

kde U_i je prípad hodnotenia, kedy bol konzument vzatý ako „užitočný“ a V_x značí celkový počet hodnotení, ktoré konzument poskytol. Vierohodnosť hodnotiaceho je vyhodnotená ako:

$$C_r(x) = C_r(x) * u_f \tag{3.13}$$

3.1.7 Osobné preferencie

Konzumenti služieb sa môžu líšiť vo vyhodnotení reputácie poskytovateľov skrz rozdiely v ich $QRef$ preferenciami nad webovými službami. Napríklad, ak niektorí konzumenti dávajú prednosť webovým službám s vyššou kvalitou, kým iní preferujú nízko–cenové služby. RATEWeb umožňuje konzumentom služieb výpočet hodnoty reputácie webových služieb podľa ich vlastných preferencií. Každý konzument si ukladá svoj vlastný atribút preferencií $QRef$ vo *vektore preferenčných hodnôt* (anglicky *reputation significance vector* (RSV). Keďže konzumenti môžu svoje preferencie meniť naprieč transakciami, RSV je vyvolané pri každom ohodnotení. Konzumenti služieb si potom môžu zvoliť či budú akceptovať vyhodnotenie reputácií inými hodnotiacimi, alebo, v prípade že majú rozdielne RSV, si vypočítajú túto hodnotu sami. V neskoršom prípade je od hodnotiaceho požadovaná skôr hodnota atribútu $QRef$ ako vyhodnotenie osobných preferencií. Pri takejto metóde majú konzumenti schopnosť zvažovať rôzne atribúty vzhľadom na vlastné preferencie.

Definícia 3.1.2. Nech $\phi_h(s_j, u)^x$ značí hodnotenie pridelené atribútu h od hodnotiaceho x pre poskytovateľa služieb s_j v transakcii u. m značí celkový počet atribútov a RSV_h predstavuje preferencie konzumenta služieb pre atribút h. Potom lokálna reputácia pre s_j od hodnotiaceho x je definovaná ako:

$$PerEval_j^x = \frac{\sum_{h=1}^{m} (\phi_h(s_j, u)^x * \mathrm{RSV}_h)}{\sum_{h=1}^{m} \mathrm{RSV}_h} \tag{3.14}$$

3.1.8 Dočasná dôležitosť

Konzumenti služieb predpokladajú, že poskytovatelia služieb budú jednať férovo a nemenne. Môže sa však stať, že poskytovateľ menil naprieč časom svoje správanie. Ku príkladu, webová služba, ktorá v minulosti jednala neférovo sa mohla trvalo polepšiť. Naopak poskytovateľ sa mohol od svojho bývalého dobrého správania prejsť k poskytovaniu zlých služieb. Môže teda nastať prípad, kedy zvažovanie všetkých historických dát môže poskytnúť nesprávnu hodnotou reputácie. Pre ošetrenie takýchto záležitostí RATEWeb má v sebe zakomponovanú dočasnú dôležitosť. Hodnotené interakcie sú teda označené časovou známkou aby sa aktuálnejším hodnoteniam prikladala väčšia váha ako tým minulým. Hodnotu reputácie teda počítame ako:

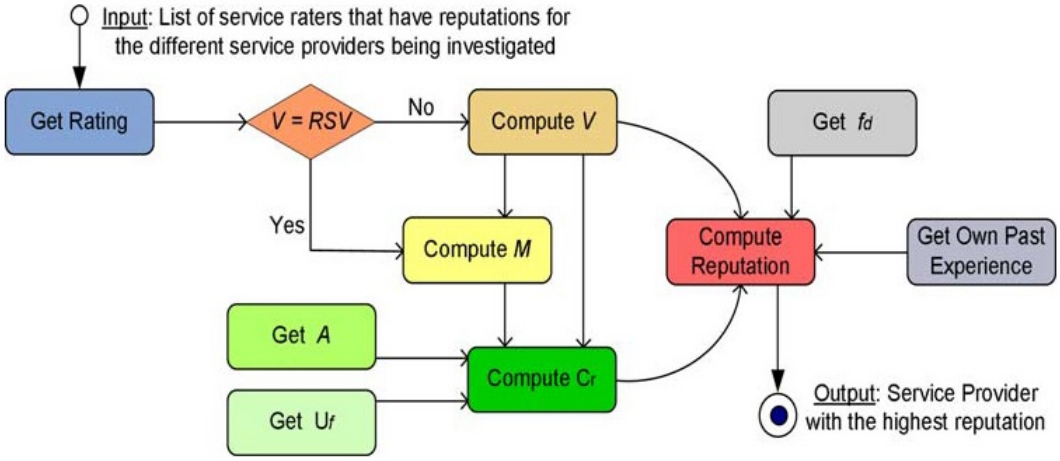
$$PerEval_x^j = PerEval_x^j * f_d \quad f_d \in [0,1] \tag{3.15}$$

Kde $PerEval_x^j$ je hodnotenie poskytnuté konzumentom služieb a f_d je faktor dôležitosti reputácie. Najnovšie hodnotenie má hodnotu f_d rovnú 1, kým staršie hodnotenia majú každou časovou jednotkou faktor dôležitosti znížený. Keď f_d dosiahne hodnoty 0, hodnotenie konzumenta nie je viac braté v úvahu. „Jednotka času“ je v tomto prípade chápaná ako akákoľvek hodnota, ktorá sa môže pohybovať od jednej transakcie, cez desať a viac. Všetky transakcie, ktoré sú poznačené rovnakou časovou známkou majú rovnakú hodnotu faktoru dôležitosti. Jedným zo spôsobov ako počítať f_d môže byť: $f_d = \frac{1}{P_u}$, kde P_u je celkový počet minulých transakcií, z ktorých je konkrétna reputácia počítaná.

3.1.9 Osobná skúsenosť pre odhad reputácie

Väčšina konzumentov služieb, ktorá interagovala s poskytovateľom služieb a bola uspokojená, bude naďalej preferovať interakciu s touto službou. V reálnych situáciach užívatelia nezvyknú meniť svojich základných poskytovateľov kvôli strachu zo zníženia kvality. Webové služby sú však plne dynamické a teda nové služby (s lepšou hodnotou $QRef$) môžu vstúpiť do systémy kedykoľvek. A čo viac, služby s nízkou hodnotou kvality sa môžu naprieč časom výrazne zlepšiť. Avšak ak konzument služieb vykonáva interakcie výhradne s *dôvernými* webovými službami, môže prísť o možnosť interakcie s ďaleko lepšími službami s lepšou hodnotu $QRef$. Model preto poskytuje konzumentovi zahrnúť do výpočtu finálnej hodnoty reputácie osobnú skúsenosť „z prvej ruky“. Finálna rovnica pre výpočet udelenej reputácie bude vyzerať:

$$\text{Reputation}(\text{s}_\text{j}) = \frac{\sum_{x=1}^{L} \left[\frac{\sum_{h=1}^{m} (\phi_h(s_j,u)^x * \text{RSV}_h)}{\sum_{h=1}^{m} \text{RSV}_h} * f_d * C_r(x) \right]}{\sum_{x=1}^{L} C_r(x)} \tag{3.16}$$



Obrázok 3.2: Metriky vyhodnotenia reputácie

Obrázok 3.2 zobrazuje vytvorený algoritmus, ktorý využíva všetky vyššie spomínané metriky. Vstupom je list hodnotiacich, ktorí majú hodnotenie reputácie pre poskytovateľov webových služieb, s ktorými v minulosti vykonali interakciu. Pre úplnosť, algoritmus iteruje nad kompletným listom potenciálnych poskytovateľov služieb obdržaný z UDDI registra. Výstupom každej invokácie algoritmu je poskytovateľ s najvyššou hodnotou reputácie. Avšak pre zjednodušenie, obrázok 3.2 neznázorňuje slučky či aktualizáciu procesov.

Na začiatku algoritmus iteruje nad listom hodnotiacich s osobným vyhodnotením reputácie pre poskytovateľa s_j a zbiera tieto hodnotenia. Hodnotiaci teda vracia vektor, ktorý obsahuje skalárne hodnotenie reputácie, RSV hodnotiaceho, hodnotenie pre jednotlivé atribúty a časovú známku pre výpočet tohto hodnotenia. RSV hodnotiaceho je potom porovnané s RSV konzumenta. Ak sú hodnoty podobné, skalárne hodnotenie reputácie je akceptované. V prípade, že sa tieto dve RSV líšia, hodnotenie reputácie je vypočítané na základe konzumentových vlastných preferencií. Následne sú všetky hodnotenia použité pre výpočet názoru väčšiny M. Vierohodnosť hodnotiaceho (Cr) je vypočítaná vzhľadom na názor väčšiny, poslednú vypočítanú hodnotu reputácie a hodnotenie jednotlivých hodnotiacich, pričom sa berie v úvahu faktor užitočnosti U_f. Nahlásené reputácie (V_i) a vierohodnosť každého hodnotiaceho (C_{r_i}) sa použijú pre výpočet „váženého hodnotenia reputácie“. Hodnota reputácie je taktiež ovplyvnená faktorom dôležitosti f_d. Ak je takto vypočítaná hodnota reputácie vyššia než tá pre predchádzajúceho poskytovateľa, aktuálne s_j je (z pohľadu konzumenta) braté ako služba s najvyššou hodnotou reputácie. Keď sú vyhodnotené reputácie pre všetkých s_j, s_j s najvyššou hodnotou je identifikovaný.

3.2 EigenTrust

The EigenTrust Algorithm for Reputation Management in P2P Networks (skrátene *EigenTrust*) [6] opisuje algoritmus slúžiaci na zníženie počtu sťahovaní nedôveryhodných súborov v peer-to-peer zdieľanej sieti, ktorý pridelí každému tzv.*peerovi* unikátnu hodnotu globálnej dôvery založenú na peerovej histórii uploadov. Na základe tejto hodnoty dôvery si peeri určujú s kým budú vykonávať interakcie, čím sa taktiež identifikujú nedôveryhodní peeri a izolujú

sa od siete [2]. Existuje päť problémov, ktoré zahrňujú každý P2P systém reputácie:

1. Systém by mal byť *self-policing*. To znamená, že etika užívateľov je definovaná a dodržiavaná peermi samotnými a nie nejakou centrálnou autoritou

2. Systém by mal udržiavať *anonymitu*. To znamená, že peerova reputácia by mala byť spojená s nezistiteľným identifikátorom, než byť združená s presnou identitou.

3. Systém by nemal prideľovať žiadny *prospech novopríchodzím*. To znamená, že dobrá reputácia by mala byť udeľovaná len za dobré správanie pri transakciách a nezvýhodňovať nepoctivých peerov so zlou reputáciou, ktorí by pravidelne menili svoje ID pre získanie statusu novopríchodzieho.

4. Systém by mal mať *minimálne režijné náklady* vo vzťahu ku výpočtom, infraštruktúre, úložisku a komplexnosti správ.

5. Systém by mal byt *robustný voči zlomyseľným kolektívom* peerov, ktorí sa navzájom poznajú a snažia sa spoločne rozvrátiť systém.

3.2.1 Reputačný systém

V distribuovanom prostredí sa peeri môžu navzájom hodnotiť po každej jednej transakcii. Napríklad, vždy keď peer i stiahne súbor od peera j, môže ohodnotiť transakciu pozitívne ($tr(i,j) = 1$) alebo negatívne ($tr(i,j) = -1$). Hodnota lokálnej dôvery (anglicky *local trust value*) s_{ij} je definovaná ako suma hodnotení individuálnych transakcií , ktoré peer i vykonal s peerom j: $s_{ij} = \sum tr_{ij}$.

Rovnako tak, každý peer i si môže uložiť počet uspokojivých transakcií s peerom j ako $sat(i,j)$ a neuspokojivých ako $unsat(i,j)$. s_{ij} je potom definované ako

$$s_{ij} = sat(i,j) - unsat(i,j) \tag{3.17}$$

Výzvou pre systém reputácie v distribuovanom prostredí je ako agregovať hodnoty lokálnej dôvery s_{ij} bez potreby centralizovaného úložiska a riadiaceho zariadenia. EigentTrust agreguje hodnotu lokálnej dôvery všetkých užívateľov s minimálnou komplexnosťou správ. Spôsob poňatia je založený na tranzitívnej dôvere: Teda peer i bude mat dobrý názor o tých peeroch, ktorí dokážu poskytnúť autenticitu ich súborov. Navyše, peer i je viac naklonený dôverovať názoru týchto peerov, pretože peeri, ktorí sú úprimní ohľadne súborov, ktoré poskytujú, zvyknú byť úprimní aj v nahlasovaní ich hodnoty lokálnej dôvery. V EigenTrust je globálna reputácia každého peera i daná hodnotou lokálnej dôvery ostatných peerov voči nemu, pričom názor každého peera je braný v úvahu natoľko, na koľko je vysoká jeho vlastná globálna reputácia.

3.2.2 Normalizované hodnoty lokálnej dôvery

Za účelom agregácie hodnôt lokálnej dôvery, je potreba ich nejakým spôsobom normalizovať. Inak by hrozilo, že zlomyseľní peeri by udeľovali ľubovoľnú hodnotu lokálnej dôvery iným

[2] Je treba podotknúť, že väčšina nasledujúceho textu je prebraná a preložená z odborného článku [6], kde je popísaná kompletná funkcionalita EigenTrust algoritmu

zlomyseľným peerom a znižovali hu dôveryhodným peerom. Preto je treba hodnotu lokálnej dôvery normalizovať. Normalizovaná hodnota lokálnej dôvery c_{ij} je definovaná ako:

$$c_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)} \tag{3.18}$$

Tento vzťah zaistí, že všetky hodnoty budú medzi 0 a 1. (V prípade, že $\sum_j \max(s_{ij}) = 0$, potom c_{ij} je nedefinované. Táto situácia je ďalej prebraná v 3.2.5). Pri normalizácii týmto spôsobom vznikajú určité nedostatky. Jeden z nich je, že normalizované hodnoty dôvery nerozlišujú medzi peerom s ktorým peer i nevykonal interakciu a peerom, s ktorým má peer i slabé skúsenosti. Taktiež , ak $c_{ij} = c_{ij}$, vieme, že peer j má v očiach peera i rovnakú reputáciu ako peer k, ale nevieme či obaja sú veľmi dôverní, alebo skôr priemerní peeri. Avšak pri normalizácii týmto spôsobom je zaistené, že hodnota globálnej reputácie nemusí byť nanovo normalizovaná pri každej iterácii (čo by mohlo byť v rozsiahlom distribuovanom prostredí výpočtovo veľmi nákladné).

3.2.3 Agregácia hodnôt lokálnej dôvery

Prirodzenou cestou, ako agregovať normalizované hodnoty lokálnej dôvery v distribuovaných prostrediach je, že peer i sa pýta okolitých peerov na ich skúsenosti s inými peermi. Je pochopiteľné, že názory ostatných peerov majú takú váhu, ako veľmi im peer i dôveruje, teda:

$$t_{ik} = \sum_j c_{ij} c_{jk} \tag{3.19}$$

kde t_{ik} reprezentuje dôveru peera i v peera k založenú na dotazoch jeho „priateľov“ (teda peerov j). Tento vzťah možno vyjadriť v maticovej notácii: Ak definujeme C ako maticu $[c_{ij}]$ a $\vec{t_i}$ ako vektor obsahujúci hodnoty t_{ik}, potom $\vec{t_i} = C^T \vec{c_i}$. (Snahou je, aby $\sum_j t_{ij} 1 =$). Toto je užitočný spôsob ako zaistiť, aby každý peer mal prehľad o sieti, ktorá je väčšia, ako pokrýva jeho vlastná skúsenosť. Avšak, hodnoty dôvery uložené peerom i odrážajú len skúsenosti jeho vlastné a jeho známych. Za účelom získania väčšieho prehľadu, peer i sa môže pýtať na názory známych jeho známych ($\vec{t} = (C^T)^2 \vec{c_i}$). Týmto spôsobom možno pokračovať na ďalšie kontakty ako: $\vec{t} = (C^T)^n \vec{c_i}$. Teda peer i bude mať kompletný prehľad o celej sieti po n iteráciách. Ak je n dosť veľké, vektor dôvery $\vec{t_i}$ bude konvergovať k rovnakému vektoru pre všetkých peerov i. Inými slovami, $\vec{t_i}$ je vektor globálnej dôvery, kde jeho elementy, t_j, určujú ako veľmi systém, ako taký, dôveruje peerovi j.

3.2.4 Pravdepodobnostná intrepretácia

Je užitočné si povšimnúť, že existuje presná pravdepodobnostná interpretácia tejto metódy. Teda ak sa agent rozhodne vyhľadať hodnoverných peerov, môže prehľadávať sieť použitím nasledujúceho pravidla: každý peer i bude prechádzať na ďalších peerov skrz peera j s pravdepodobnosťou c_{ij}. Po určitom čase prechádzania siete týmto spôsobom sa agent s väčšou pravdepodobnosťou vyskytne medzi hodnovernými a peermi než nedôveryhodnými.

3.2.5 Základný EigenTrust

V tejto sekcii budeme uvažovať základný EigenTrust algoritmus,pre teraz ignorujúci distribuovanú podstatu P2P siete. To znamená, že predpokladáme existenciu nejakého centrálneho servera majúceho znalosti všetkých c_{ij} hodnôt a vykonávajúcich výpočty nad nimi.

Naším cieľom je vypočítať $\vec{t} = (C^T)^n \vec{e}$, pre n = veľké, kde $\vec{e}$ je $m-$vector reprezentujúci rovnomerné rozdelenie pravdepodobnosti nad všetkými m peermi,$e_i = 1/m$. (Vyššie bol spomenutý výpočet $\vec{t} = (C^T)^n \vec{c_i}$, kde $\vec{c_i}$ je normalizovaná hodnota lokálnej dôvery nejakého peera i. Avšak keďže obe hodnoty konvergujú k rovnakému vektoru, budeme uprednostňovať $\vec{e}$.)

3.2.6 Praktické problémy

Prednostný výber dôvery: Často sa stáva, že v sieti sa nachádzajú peeri, o ktorých sa vie, že budú vždy dôveryhodní. Napríklad, prvých pár peerov, ktorí sa pripoja do siete sa dajú považovať za dôveryhodných, keďže návrhári siete a prví užívatelia, ktorí sa do nej pripojili nemajú tendenciu rozvrátiť sieť, ktorú sami vytvorili. Takýchto peerov, ktorým sa dá dôverovať od chvíle ich pripojenia hovoríme *pre-trusted peeri*. Tento fakt je vhodné zakomponovať do modelu. To je docielené definovaním distribúcie $\vec{p}$ nad pre-trusted peermi. Ak je nejaká skupina peerov P známa ako dôveryhodná, môžeme definovať $p_i = 1/|P|$ ak $i \in P$,inak $p_i = 0$. Toto rozdelenie $\vec{p}$ je možné využiť tromi spôsobmi. Za prvé, v prítomnosti nedôveryhodných peerov, $\vec{t} = (C^T)^n \vec{p}$ bude spravidla konvergovať rýchlejšie ako $\vec{t} = (C^T)^n \vec{e}$, preto $\vec{p}$ je použité ako štartovací vektor. Ďalšie spôsoby využitia sú popísané nižšie.

Neaktívny peeri: Ak peer i nesťahuje od žiadneho iného užívateľa, alebo má nulové hodnotenie voči všetkým ostatným peerom, c_{ij} z rovnice 3.18 bude nedefinované. V takom prípade je $c_{ij} = p_j$. Takže c_{ij} je predefinované ako:

$$c_{ij} = \begin{cases} \frac{max(s_{ij},0)}{\sum_j max(s_{ij})} & \text{ak } \sum_j max(s_{ij},0) \neq 0 \\ p_j & \text{v opačnom prípade} \end{cases} \tag{3.20}$$

Teda ak peer i nikoho v systéme nepozná, alebo nikomu neverí, zvolí si dôverovať pre-trusted peerom.

Zlomyseľné kolektívy: V peer-to-peer sieťach sa zvyknú formovať zlomyseľné kolektívy. Zlomyseľný kolektív je skupina peerov, ktorí sa navzájom poznajú, navzájom si udeľujú vysoké hodnoty lokálnej dôvery a ostatným peerom zase nízke za účelom rozvrátiť systém. Aby sa dalo takému niečomu zabrániť, je treba aby každý peer mal aspoň nejakú dôveru v pre-trusted peerov, ktorí nie sú súčasťou žiadneho kolektívu. Toho možno docieliť vzťahom:

$$\vec{t}^{(k+1)} = (1-a)C^T \vec{t}^{(k)} + a\vec{p} \tag{3.21}$$

kde a je nejaká konštanta menšia než 1. Tento vzťah je ekvivalentný nastaveniu vektora $\vec{c_i} = (1-a)\vec{c_i} + a\vec{p}$, čo naruší tvorenie zlomyseľných kolektívov vložením aspoň nejakej dôvery v peerov P, ktorí nie sú súčasťou žiadneho takého kolektívu. Inými slovami, agent, ktorý prechádza sieťou na základe vyššie spomínaného pravdepodobnostného modelu, má menšiu šancu prechádzať zlomyseľným kolektívom, pretože pri každom kroku existuje istá pravdepodobnosť, že bude smerovaný k pre-trusted peerovi. Pre-trusted peeri sú teda pre tento prístup kľúčoví, lebo garantujú určitú konvergenciu a rozvracajú zlomyseľné kolektívy. Preto je výber pre-trusted peerov dôležitý, obzvlášť, aby neboli súčasťou žiadneho takéhoto zlomyseľného kolektívu.

3.2.7 Distribuovaný EigenTrust

V distribuovanom EigenTrus systéme všetci peeri kooperujú pri výpočte a uložení vektora globálne dôvery, pričom výpočet, uskladnenie a zasielanie správ je u každého peera minimálne. Otázka, ktorá sa naskytá, je ako uložiť C a $\vec{t}$. Budeme uvažovať, že každý peer si

u seba môže uložiť svoj vektor lokálnej dôvery $\vec{c_i}$ a tie hodnotu globálnej dôvery t_i.(Pre prezentačný účel budeme zatiaľ ignorovať záležitosť bezpečnosti a povolíme peerom, aby si ukladali ich vlastné hodnoty dôvery) Každý peer si môže vypočítať svoju hodnotu globálnej dôvery ako:

$$t_i^{(k+1)} = (1-a)(c_{1i}t_1^{(k)} + \ldots + c_{ni}t_n^(k)) + ap_i \tag{3.22}$$

Treba podotknúť dve veci. Prvá, že len pre-trusted peeri potrebujú vedieť ich p_i. To znamená, že pre-trusted peeri môžu zostať anonymní. Nikto iný nemusí vedieť, že práve oni sú pre-trusted. Za druhé, vo väčšine P2P sieťach má každý peer obmedzený počet interakcií s inými peermi. To znamená, že pri výpočte $t_i^{(k+1)}$ je väčšina hodnôt c_{ij} nulová a tiež, že počet zaslaných správ medzi A_i (peeri, ktorí sťahujú súbory od peera i) a B_i (peeri, od ktorých peer i sťahoval súbory) nie je tak vysoký.

3.2.8 Zabezpečený EigenTrust

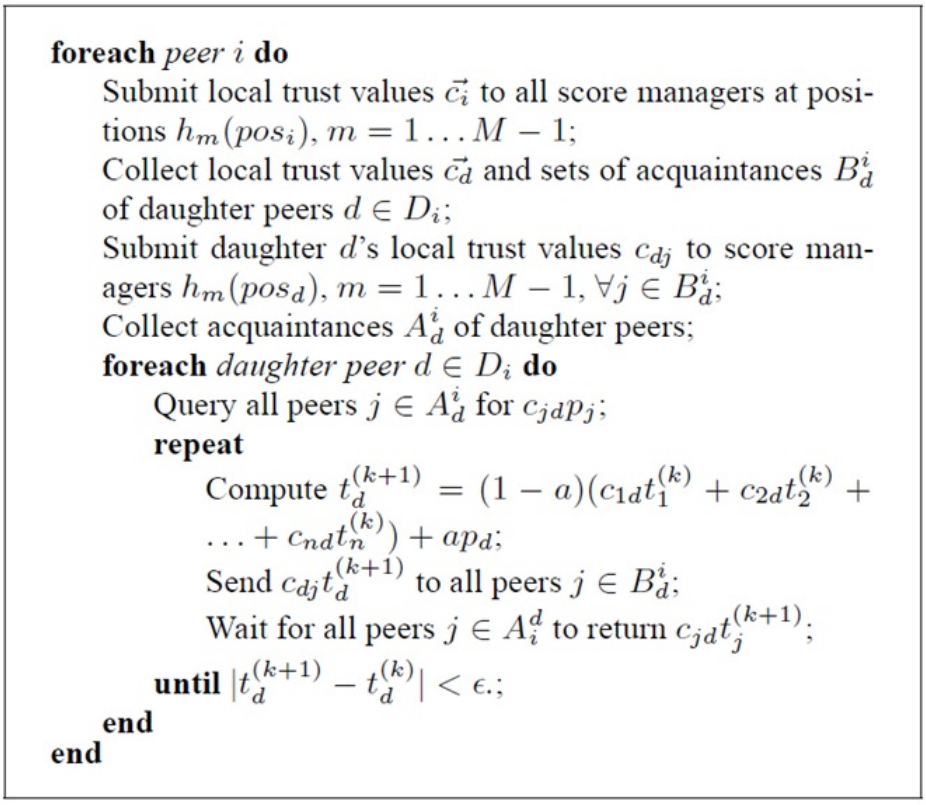
V sekcii vyššie si každý peer i počítal a nahlasoval svoju vlastnú hodnotu dôvery t_i. Také niečo by však zlomyseľní peeri mohli ľahko zneužiť a nahlásiť falošnú hodnotu dôvery.

Proti takémuto zneužitiu sa dajú aplikovať dve idey. Prvá, že aktuálna hodnota dôvery daného peera nemôže byť vypočítavaná ním a uložená u neho samého. Preto dôveru tohto peera bude počítať nejaký iný peer. Druhá sa týka situácie, kedy výpočet dôvery nejakého peera môže pripadnúť za úlohu peerovi, ktorý jedná nečestne a mal by tendenciu nahlásiť klamlivú hodnotu dôvery. Z toho dôvodu je hodnota dôvery jedného peera vypočítavaná viacerými peermi. V zabezpečenej verzii distribuovaného algoritmu teda M peerov (takzvaných *score manažérov* peera i) počíta hodnotu dôvery peera i. Ak nejaký ďalší peer bude chcieť vedieť hodnotu dôvery peera i, môže sa dotazovať všetkých M score manažérov.

Pre určenie score manažérov sa využíva distribuovaná hashovacia tabuľka (DHT). V EigenTrust je peerov score manažér určený hashovaním jeho ID (ako je IP adresa a TCP port) do určitého bodu v DHT hashovaciom priestore. Peer, ktorý aktuálne pokrýva tento bod ako časť jeho DHT regiónu je určený ako score manažér tohto peera. Každý peer v systéme, ktorý pozná toto ID daného peera môže teda lokalizovať jeho score manažéra.Ak score manažér opustí systém, jeho úloha prejde na jeho suseda v DHT. DHT tiež zabezpečuje pred stratou dát ich replikáciou v prípade, že score manažér zlyhá.

3.2.9 Popis algoritmu

Popíšeme si teraz algoritmus, ktorý vypočítava vektor globálnej dôvery. Každý peer má M score manažérov, ktorých DHT súradnice sú dané aplikovaním sériou one-way hash funkcií $h_0, h_1, \ldots, h_{M-1}$ na peerov jedinečný identifikátor. pos_i predstavujú súradnice peera i v hashovanom priestore. Keďže každý peer môže jednať aj ako score manažér, je vytvorená skupina dcér D_i. D_i obsahuje adresy peerov, ktorých výpočet hodnoty dôvery je vykonávaný mimo iných aj peerom i. Score manažér si taktiež drží vektor názorov c_d^i jeho dcéry peera d, pričom $d \in D_i$. Peer i je taktiež oboznámený s A_d^i, čo je skupina peerov, ktorí sťahovali súbory od peera d. Od A_d^i potom peer i obdrží hodnotenie dôvery jeho dcéry, peera d. Nakoniec peer i bude oboznámený s B_d^i - skupina peerov, od ktorých sťahoval peer d.



Obrázok 3.3: Zabezpečený EigenTrust algoritmus (tento obrázok bol prebratý z [6])

Výhody algoritmu v prípade zvýšenej spoľahlivosti a zabezpečenia sú:

I *Anonymita.* Peer nie je schopný zistiť ID iného peera, ktorému má za úlohu vypočítať hodnotu dôvery. Preto zlomyseľní peeri nemôžu cielene zvyšovať reputáciu iných zlomyseľných peerov.

II *Náhodnosť.* Peer, ktorý vstúpi do systému si nemôže zvoliť na akých súradniciach hashovacieho priestoru chce byť umiestnený. Peer si teda nemôže vypočítať hashovnú hodnotu jeho vlastného ID a umiestniť sa na vybranú pozíciu hashovacieho priestoru, kde by bol schopný počítať si vlastnú hodnotu dôvery.

III *Redundancia.* Viacero score manažérov počíta hodnotu dôvery jedného peera. Pre pridelenie viacerých score manažérov jednému peerovi sa využíva niekoľko multi-dimenzionálnych hashovacích (MDH) funkcií. Peer v systéme stále zaberá presnú polohu v súradnicovom priestore, avšak tentoraz je priestorov viacero, pričom každý bol vytvorený práve jednou MDH funkciou. Peerove ID je teda mapované do iného bodu v každej MDH.

3.2.10 Využitie hodnôt globálnej dôvery

V poslednej sekcii o EigenTrust si povieme ako možno využiť hodnoty globálnej dôvery v peer-to-peer systéme. Spôsoby sú dva. Prvým je izolovať zlomyseľných peerov zo siete podnetom užívateľov sťahovať od dôveryhodných peerov a druhým je motivovať peerov zdieľať súbory ich odmeňovaním.

Izolovanie zlomyseľných peerov. Keď peer i podá dotaz, systém môže využiť hodnoty dôvery t_j, pre odklon užívateľa k sťahovaniu od viacej dôveryhodných peerov. Jeden spôsob by bol sťahovať výhradne od tých najdôveryhodnejších. Takýto prístup by však viedol k preťaženiu vysoko dôveryhodných peerov. A čo viac, novopríchodzí by si v systéme nedokázali vybudovať žiadnu reputáciu.

Iná stratégia by bola vyberať peerov na interakciu podľa určitej pravdepodobnosti, založenej na hodnote dôvery. Takýto prístup s malou toleranciou obmedzuje počet neuspokojivých interakcií v sieti pričom udržuje rovnomerné vyťaženie siete a umožňuje novopríchodzím si vybudovať reputáciu.

Peerom by malo taktiež byť umožnené učiniť svojrázne rozhodnutie výberu kombináciou hodnôt globálnej dôvery a ich vlastných odhadov lokálnej dôvery voči ostatným peerom, teda využiť hodnoty dôvery dané vektorom $\vec{t}_{personal} = b\vec{t} + (1-b)\vec{c}$, kde b je konštanta medzi 0 a 1. Týmto spôsobom sa peer môže vyhnúť interakcii s peerom, ktorý mu poskytol zlé služby, napriek tomu, že zvyšku siete poslúžil dobre.

Motivácia k zdieľaniu. Systém môže odmeňovať peerov, ktorí majú vysokú hodnotu dôvery. Napríklad, cenený peer môže byť odmeňovaný vyššou rýchlosťou pripojenia k iným ceneným peerom či zvýšením šírky prenosového pásma. Odmeňovanie vysoko dôverných peerov má dvojaký efekt. Po prvé, dáva to peerom podnet zdieľať súbory, keďže vysokú hodnotu globálnej dôvery sa dá dosiahnuť len zdieľaním autentických súborov. Druhý efekt je, že odmeňovaním vysoko dôveryhodných peerov dáva iným poctivým peerom podnet na odstránenie neautentických súborov, ktoré mohli nedopatrením stiahnuť od zlomyseľných peerov. Sťažuje sa teda šanca šírenia neautentických súborov naprieč systémom.

3.3 Model dôvery a reputácie inšpirovaný prírodou

V nasledujúcej sekcii si v krátkosti predstavíme model dôvery a reputácie inšpirovaný prírodou (anglicky *Bio-inspired Trust and Reputation Model*, skrátene *BTRM*) [13].

BTRM zakladá výber najviac dôveryhodného uzlu skrz cestu s najlepšou reputáciou poskytujúcou zaručenú službu. Je založený na algoritme inšpirovaný prírodou, nazvaný *systém mravčej kolónie* (anglicky *Ant Colony System*, skrátene *ACS*), v ktorej mravce budujú feromónové cesty za účelom dosiahnutia určitých cieľov. Tieto feromónové stopy pomáhajú mravcom nájsť optimálnu cestu riešenia, keďže cesta s najsilnejšou feromónovou stopou je považovaná za najlepšiu. Keď aplikujeme tento ACS algoritmus na systém dôvery a reputácie, pojem „hodnota feromónu“ bude reprezentovať dôveryhodnosť uzlov (*senzorov*). Každý uzol v BRTM obsahuje feromónovú trasu ku všetkým jeho susedom ($\tau \in [0,1]$), ktorá určuje mravcovu pravdepodobnosť pre výber cesty, ako aj cieľový senzor, ku ktorému cesta smeruje. Inými slovami, τ môže byť brané ako dôvera, ktorú jeden senzor vkladá do iného.

Bližší popis BTRM algoritmu je nasledujúci: Je vytvorená skupina „umelých mravcov“, ktorí opúšťajú klientský senzor. Keď sa mravec pohne zo senzoru i k senzoru j, vydá rozkaz nad týmito dvoma senzormi, aby zmenili hodnotu feromónu medzi nimi podľa rovnosti:

$$\tau_{ij} = (1-\varphi) * \tau_{ij} + \varphi * \Omega \tag{3.23}$$

$$\Omega = 1 + (1-\varphi) * (1-\tau_{ij}) * \eta_{ij} \tag{3.24}$$

pričom τ_{ij} predstavuje hodnotu feromónu medzi senzorom i a j, Ω hodnotu konvergencie τ_{ij}, φ parameter kontrolujúci množstvo feromónu, ktoré mravci zanechávajú a η_{ij} značí „viditeľnosť“ miest i a j, ktorá je nepriamo úmerná ich vzdialenosti d_{ij} (teda $\eta_{ij} = 1/d_{ij}$).

Každý mravec pri svojom hľadaní najviac dôveryhodnej cesty k senzoru poskytujúcemu dobré služby musí rozhodnúť či má zastaviť a vrátiť riešenie klientovi, a či pokračovať v hľadaní iného riešenia na základe reputácie senzoru, ktorý práve našiel. Keď mravec k dorazí k senzoru s, môžu nastať dve situácie. V prípade prvej, senzor s poskytne svoje služby. Ak má senzor s viacero susedov, ktorých mravec k zatiaľ nenavštívil, potom k vypočíta priemernú hodnotu feromónu ($\bar{\tau_k}$) cesty vedúcej od klienta k senzoru s. Ak $\bar{\tau_k}$ je väčšie než definovaná hraničná hodnota, potom sa mravec k zastaví a vráti riešenie. V opačnom prípade pokračuje ďalej. Druhá možná situácia znie, že senzor s žiadne služby neposkytuje. Ak senzor s má viacero susedov, ktorých mravec k zatiaľ nenavštívil, posunie sa k ďalšiemu uzlu. Ak senzor s nemá žiadnych ďalších susedov, ktorí by už neboli mravcom k navštíveni, potom k dosiahlo mŕtveho konca. V takom prípade musí k putovať späť po tej istej trase ku zdroju, pokým nenarazí buď na senzor, ktorý poskytuje požadované služby, alebo senzor neposkytujúci tieto služby, no majúci stále nejakých susedov, ktorých ešte stále nenavštívil.

Klient následne preverí a uloží riešenia, ktoré mu boli vyslanými mravcami navrátené a vyhodnotí celkovú kvalitu danej cesty. Kvalita môže byť počítaná ako:

$$Q(S_k) = \frac{\bar{\tau_k}}{\text{Length}(S_k)^{\text{PLF}}} * \%A_k \tag{3.25}$$

kde S_k značí riešenie poskytnuté mravcom k, teda cestu vedúcu k vybratému senzoru, $Q(S_k)$ kvalitu danej S_k, $\bar{\tau_k}$ priemernú hodnotu feromónu cesty S_k, PLF(*path length vector*) vektor dĺžky cesty, pričom PLF $\in [0, 1]$ a $\%A_k$ percento mravcov, ktorí zvolili rovnakú cestu, ako mravec k.

Po výpočte kvality všetkých riešení, ktoré mravce klientovi poskytli, si klient zvolí cestu s najvyššou hodnotou a uloží ho ako svoje najlepšie aktuálne riešenie. Potom klient porovná kvalitu tohto riešenia s najlepším globálnym riešením. Ak je aktuálne riešenie lepšie ako to globálne, nahradí globálne s aktuálnym a vyšle jedného extra mravca, ktorý modifikuje hodnotu feromónu aktuálneho globálneho riešenia.

Transakcia a Ohodnotenie: Po tom, ako si klient zvolí najlepšie globálne riešenie, vykoná transakciu so zvoleným senzorom. Po prijatí služby udelí klient senzoru ohodnotenie na základe kvality služby, ktorú mu senzor poskytol. V prípade uspokojivých služieb klient udelí senzoru hodnotu uspokojenia ako náhodné číslo medzi δ a 1, pričom δ predstavuje preddefinovanú hranicu hodnotenia senzora. V opačnom prípade, kedy klient nie je uspokojený so službami senzoru dostane senzor hodnotenie ako náhodné číslo medzi 0 a δ. Trest či odmena budú udelené všetkým spojom na tejto ceste v závislosti uspokojenia klienta. Tým je myslené zníženie, či zvýšenie hodnoty feromónu tejto cesty.

Kapitola 4

Meranie

V predchádzajúcej kapitole boli predstavené tri modely dôvery a reputácie, pričom princíp fungovania každého z nich sa značne líšil od toho druhého. V nasledujúcej časti budú opísané vykonané merania nad jedným z týchto modelov, overenie popisovanej funkcionality, prípadne jej zlepšenie.

4.1 Výber modelu

Výber modelu bol viac-menej intuitívny. Z uvádzaných modelov bol ako prvý vylúčený model inšpirovaný prírodou (BTRM), pretože princíp jeho fungovania nie je pre multiagentné siete celkom vyhovujúci. V prípade výberu vhodnejšieho modelu medzi EigenTrust a RATEWeb poslúžil odborný text *RATEWeb: Reputation Assessment for Trust Establishment amongWeb services* [12] v ktorom autori *Zaki Malik* a *Athman Bouguettaya* v krátkosti porovnávajú tieto modely. Uvádzajú, že EigenTrust sa sústredí na myšlienku tranzitívnej dôvery, kde dôvera v spätnú väzbu a dôvera v poskytované služby sú spojené v jedno. Teda ak je agent považovaný za dôveryhodný v zdieľaní zdrojov, ich informácie so hodnotení sú brané rovnako vierohodné. Toto je vec, v ktorej je EigenTrust v nevýhodne oproti RATEWeb, kde táto myšlienka tranzitívnej dôvery je považovaná za chybnú a teda rozlišuje u jedného agenta rôzne hodnoty vierohodnosti podľa daného kontextu. Druhou nevýhodou EigenTrust je, že predpokladá existenciu pre-trusted agentov. Predpoklad, že v sieti sa budú nachádzať agenti, ktorých možno vždy považovať za dôveryhodných môže byť zásadnou slabinou.

Nutno podotknúť, že pri výbere modelu taktiež zavážila dostupnosť zdrojových kódov a aplikácií pre beh programu (použitá aplikácia je opísaná v nasledujúcej sekcii)

4.2 EStarMom

Spôsob akým je funkčnosť RATEWeb modelu otestovaná je zvoliť vhodný spôsob simulácie. Keďže RATEWeb bol opisovaný na základe interakcie medzi predajcami a kupcami, je na mieste zvoliť simulované prostredie práve medzi týmito dvoma entitami. Teda agenti, ktorí figurujú ako nakupujúci, vykonávajú interakcie s agentmi predstavujúci kupcov a na základe spokojnosti s poskytnutou službou vytvárajú spätnú väzbu, z ktorej si budujú dôveru v predávajúcich pre budúce interakcie a dôveru vzájomnú.

Prostredie pre takýto typ simulácie plne poskytuje *Extendable Simulator for Trust and Reputation Management in Online Marketplaces*, skrátene EStarMom. EStarMom [15] je

aplikácia, ktorej autorkou je *Thao P. Nguyen*

EStarMom je voľno-šíriteľný program, ktorý predstavuje simulačné prostredie, v ktorom kupci s určitým počtom požiadavok si vyberajú predajcu pre využitie jeho poskytovaných služieb, na základe jeho hodnoty reputácie. Simulácia končí, keď žiadny z kupcov nemá žiadnu požiadavku, ktorá by čakala na uspokojenie, alebo keď všetci predajcovia vyčerpajú svoje zásoby, alebo ak žiadny z predajcov nesplňuje kupcove požiadavky. Program je písaný v jazyku Java a sú dostupné všetky jeho zdrojové kódy ako open-source softvér.

4.2.1 Parametre simulátora

EStaRMom oplýva mnohými vstupnými parametrami pre nastavenie simulácie podľa vlastných potrieb.

- *Užívateľský model.* Jednotlivci zúčastnení simulácie sú v EStarMom modelovaní ako *užívatelia*. Skupina užívateľov, ktorí majú rovnaké parametre, teda rovnaké správanie, sa nazýva užívateľský model. Užívateľský model je definovaný ako štvorica: (názov modelu, typ užívateľa, počet žiadostí/zásob, model správania kupca/predajcu). Užívateľské modely sú vytvárané koncovým užívateľom aplikácie EStarMom a držané v súbore na disku užívateľa. „Typ užívateľa“ môže byť buďto „kupec“ či „predajca“. Ak je zvolený typ kupca, tak nasledujúce parametre sú „počet žiadostí“ a „model správania kupca“. V opačnom prípade, kedy je vybraný typ predajcu je to „počet zásob“, ktoré má predajca na sklade a „model správania predajcu“ určujúci jeho stratégiu predaja. Konkrétny model správania oboch typov užívateľov je možné zvoliť z odpovedajúcej knižnice. Táto knižnica môže byť tiež rozšírená o nové modely správania. Výber konkrétneho užívateľského modelu pre danú skupinu, počet žiadostí/zásob a počet užívateľov spadajúcich pod túto skupinu si volí koncoví užívateľ (Obrázok: 4.1, 1). Zvolené skupiny užívateľov, ktoré sa budú simulácie účastniť sú vyobrazené v tabuľke (Obrázok: 4.1, 2).

- *Algoritmus dôvery a reputácie.* Každý užívateľ si pred transakciou vypočítava hodnoty reputácie pre každého predajcu. O tento výpočet sa stará zvolený „algoritmus dôvery a reputácie“ (*ADR*) (Obrázok:4.1, 3). Podľa zvoleného ADR sú na jeho vstupe vybraté zaznamenané údaje z predchádzajúcich transakcií. Z nich je vypočítaná hodnota dôvery a reputácie, ktoré je pridelená odpovedajúcemu užívateľovi. Jednotlivé ADR môžu mať dodatočné parametre, ktoré si môže koncoví užívateľ navoliť v *detailoch algoritmu.*

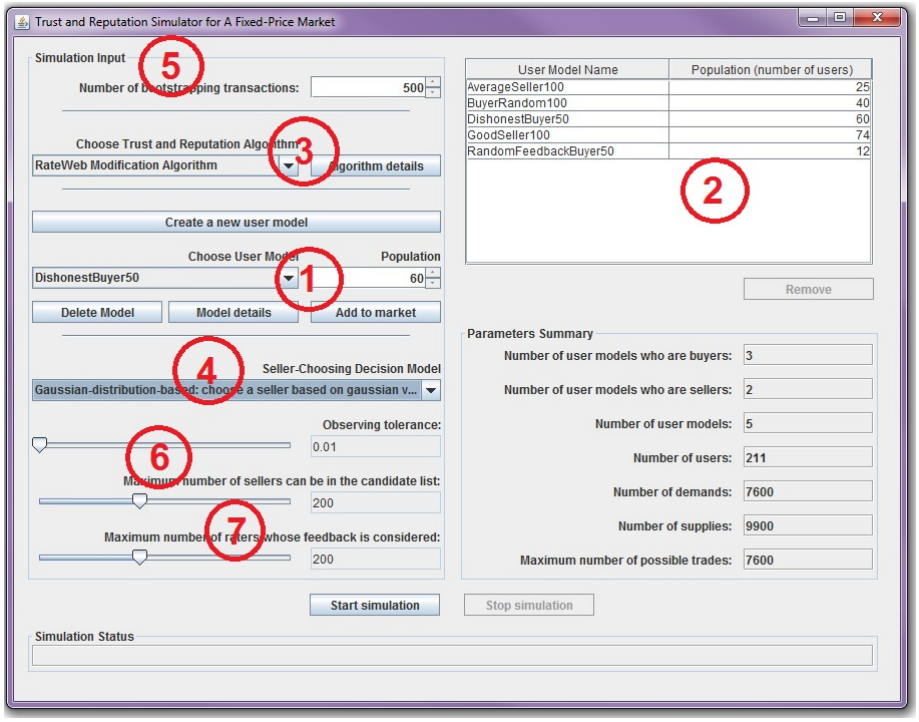
- *Rozhodovací model pre výber predajcu.* Po tom čo je vypočítaná hodnota reputácie pre každého predajcu sa kupec musí rozhodnúť pre jedného konkrétneho predajcu, s ktorým vykoná interakciu a využije jeho ponúkané služby. O túto záležistosť sa stará rozhodovací model pre výber predajcu (*RMVP*). Rozhodovacích modelov môže byť viacero a koncový užívateľ si volí jeden konkrétny ktorým sa budú riadiť všetci kupci počas celého behu simulácie (Obrázok: 4.1, 4). RMVP je častokrát nemenej dôležitý ako ADR a má tiež značný vplyv na celý systém dôvery a reputácie, a tiež konečné výsledky simulácie.

- *Bootstrap transakcie.* Keď užívateľ vstúpi na trh, nemá v systéme žiadnu zaznamenanú históriu, teda žiaden existujúci užívateľ nemá hodnotenie o tomto užívateľovi. Problém pridelenia hodnoty dôvery a reputácie novopríchodzím je nazývaný ako problém „bootstrap reputácie“. V EStarMom sú všetci účastníci simulácie bratí ako novopríchodzí

a teda všetci vstupujú na trh v rovnakom čase. Preto na začiatku každej simulácie prebehne bootstrap perióda. V tejto perióde sa každému predajcovi pridelí predvolená hodnota reputácie a prebehne daný počet bootstrap transakcií, behom ktorých kupci vykonávajú interakcie s predajcami, ohodnocujú ich služby a budujú si vzájomnú dôveru. Rozdiel oproti bežnej transakcii spočíva v tom, že pri bootstrap transakciách kupcom neklesá počet žiadosti a predajcom počet zásob. Počet bootstrap transakcií si určuje koncoví užívateľ (Obrázok: 4.1, 5). Čím viac bootstrap transakcií sa pred prechodom do skutočnej simulácie vykoná, tým viac budú hodnoty dôvery a reputácie jednotlivých užívateľov presnejšie.

- *Tolerancia pozornosti.* V reálnom svete existuje mnoho prípadov, kedy užívateľ správne neodhadne kvalitu služby, ktorú mu iný užívateľ poskytol. Akýkoľvek faktor, ktorý môže spôsobiť chybu v užívateľovom vnímaní služby je potreba zahrnúť medzi hlavné okolnosti. Iný možný dôvod rozdielu medzi kupcovým odhadom a skutočnou kvalitou služby sú praktické vlastnosti služby. Rôznemu užívateľovi sa môže zdať rôzna praktickosť služby. Tá sa môže vplyvom okolia meniť naprieč časom. Všetky tieto faktory sú simulované v parametre tolerancie pozornosti (Obrázok: 4.1, 6). Tento parameter reprezentuje maximálnu možnú chybu v kupcovom odhade s ohľadom na reálnu hodnotu služby. Platí teda vzťah,že $|PercievedQ - RealQ| \in |0, ObservedTol|$, kde $PercievedQ$ vyjadruje obdržanú kvalitu z pohľadu kupca, $RealQ$ skutočnú kvalitu danej služby a $ObservedTol$ hranicu tolerancie definovanú koncovým užívateľom.

- *Maximálny počet užívateľov braných v úvahu.* Môžu nastať prípady, kedy si koncový užívateľ nepraje, aby ADR bol vypočítavaný nad všetkými kupcami či aby sa kupcovi vykonávajúcemu transakciu dostávala spätná väzba od všetkých kupcov v systéme. Dôvod môže byť napríklad zvýšenie prehľadnosti výsledkov či výpočtový výkon stanice. EStarMom teda umožňuje definovať maximálny počet predajcov, ktorí budú v liste kandidátov v danej transakcii a maximálny počet hodnotiacich, ktorých spätná väzba bude bratá v úvahu (Obrázok: 4.1, 7).



Obrázok 4.1: GUI pre simulátor EStarMom

4.3 Praktické merania

V nasledujúcej časti si popíšeme priebeh a výsledky vykonaných meraní. Ako bolo spomenuté, model dôvery a reputácie, na ktorý sa budú merania sústrediť je RATEWeb. Pre porovnanie kvality výsledkov budú merania vykonané nad druhým modelom a to *Avegrage DoubleScore* modelom (*AVG*). AVG funguje na jednoduchom princípe aritmetického priemeru. Reputácia každého predajcu je teda vypočítavaná ako priemerná hodnota všetkých hodnotení, ktoré boli po aktuálnu transakciu predajcovi udelené.

Hodnotenie, ktoré mohli užívatelia udeľovať sa pohybovalo na škále od 0 do 1, v závislosti od spokojnosti obdržanej služby. Reputácia predajcu mala teda v najhoršom prípade hodnotu 0 a v najlepšom 1.

4.3.1 Inštalácia

Bolo vytvorené simulačné prostredie, v ktorom 100 kupcov vykonáva interakcie so 100 predajcami. Každý kupec má rovnaký počet požiadavok (10) a každý predajca má rovnaký počet zásob (1000). Všimnime si, že celkový počet zásob je razantne vyšší ako počet všetkých žiadostí. Je to z dôvodu, aby rôzne skupiny predajcov zúčastnených každej simulácie neminuli svoje zásoby na nulu, ale zotrvali v simulácii po celú dobu jej behu. Hodnota tolerancie pozornosti bola nastavená na 1%. Obe hodnoty, maximálny počet predajcov v liste kandidátov a maximálny počet spätných väzieb od hodnotiacich, boli nastavené na takú hodnotu, aby vždy boli všetci predajcovia v liste kandidátov a tiež sa brala v úvahu spätná väzba všetkých hodnotiacich nachádzajúcich sa v systéme. Počet transakcií behom ktorých budú kupci vykonávať interakcie s predajcami bol nastavený počtom požiadavok na 1000

transakcií. Po 1000. transakcii budú všetky požiadavky kupcov splnené. Počet bootstrap transakcií bol nastavený na 500. Polovica transakcií celkového behu simulácie by mala byť dostatočná na to, aby si kupci medzi sebou vytvorili dôveru a predajcom bola pridelená zaslúžená reputácia.

4.3.2 Užívateľské modely

V každej simulácii sa nachádzal rôzny počet rôznych užívateľských modelov. Pri každej simulácii je uvedený presný počet užívateľov, ktorý pod daný užívateľský model spadá. Užívateľské modely kupcov, ktoré sa v modely vyskytovali, boli:

- *Čestná spätná väzba.* Predajca vždy dodá hodnotenie pre predajcu také, akej kvality službu obdržal, teda $Rating = PercievedQ$.
- *Nečestná spätná väzba.* Hodnotenie sa líši o 0,5 od skutočného názoru kupca, teda $|Rating - PercievedQ| = 0,5$.
- *Dohodnutá spätná väzba.* Kupci generujú najvyššie hodnotenie ($Rating = 1$) predajcom, ktorí sú v rovnakej dohodnutej skupine a najnižšie ($Rating = 0$) všetkým ostatným predajcom.

Užívateľské modely predajcov, ktoré sa v meraniach vyskytovali, boli:

- *Zlá kvalita.* Predajca vždy poskytuje služby so stálou hodnotou nízkej kvality, teda $RealQ \in [0,01; 0,4]$
- *Priemerná kvalita.* Predajca vždy poskytuje služby so stálou hodnotou priemernej kvality, teda $RealQ \in [0,41; 0,7]$.
- *Dobrá kvalita.* Predajca vždy poskytuje služby so stálou hodnotou vysokej kvality, teda $RealQ \in [0,71; 1]$.
- *Zlá zmenená v dobrú.* V prvej polovici simulácie predajca poskytuje služby s hodnotou $RealQ \in [0,01; 0,4]$, následne zmení kvalitu služby na $RealQ \in [0,71; 1]$. Tento typ užívateľského modelu by sa v reálnom prípade dal chápeš ako predajca, ktorý sa poučil zo svojich minulých chýb a rozhodol sa poskytovať služby vyššej kvality.
- *Dobrá zmenená v zlú.* V prvej polovici simulácie predajca poskytuje služby s hodnotou $RealQ \in [0,71; 1]$, následne zmení kvalitu služby na $RealQ \in [0,01; 0,4]$. Tento typ modelu zase možno chápať ako zlomyseľného predajcu, ktorý sa v zo začiatku snaží vybudovať si dobrú povesť, načo následne začne poskytovať nekvalitné služby za účelom rozvrátenia systému.
- *Dohodnutá zlá kvalita.* Predajca vždy poskytuje služby zlej kvality, pričom je v dohode s kupcami poskytujúcimi dohodnutú spätnú väzbu.

4.3.3 Rozhodovací model pre výber predajcu

EStarMom oplýva dvoma hlavnými RMVP a to *TopTrust* a *Gaussovo rozdelenie pravdepodobnosti*. V prípade TopTrust, RMVP náhodne vyberie predajcu spomedzi tých s najvyššou hodnotou reputácie v danom okamihu. V prípade, že taký predajca je len jeden, zvolí práve toho. Pri Gaussovom rozdelení je výber mierne zložitejší. Najprv RMVP pridelí predávajúcim kandidátom určitý stupeň na základe ich hodnoty reputácie tak, aby sa vytvoril

usporiadaný zoznam o veľkosti N. Za druhé, Gaussovo rozdelenie využíva štandardnú odchýlku $\sigma = \sqrt{N}$ a stred hodnoty $a = 0$ pre výpočet „Gassovej náhodnej hodnoty“ (G_s) pre všetkých kandidátov. G_s každého predajcu závisí od veľkosti N a jeho prideleného stupňa, teda nie výhradne od jeho hodnoty reputácie. Nakoniec RMVP zvolí predajcu náhodne, s pravdepodobnosťou primeranou k jeho hodnote G_s. Cieľom tejto schémy je, že predajcom s vyššou hodnotou a teda s vyšším prideleným stupňom budú mať vyššiu no nie úplnú pravdepodobnosť výbery. Táto schéma nie je taká striktná ako TopTrust, kde vyberaní kandidáti boli len tí s najvyššou hodnotou reputácie, ale dáva šancu aj horším kandidátom, aby boli zvolení.

4.3.4 Oprava bugov a modifikácie

Počas práce s EStarMom bolo odhalených niekoľko bugov, ktoré bolo treba opraviť. Model nepracoval správne s užívateľmi, ktorí menili kvalitu svojich služieb počas simulácie. Taktiež bol úplne zanedbaný model dohodnutých užívateľov, ktorý bolo potreba takmer celý implementovať.

Čo sa týka už zakomponovaných úprav, tie sa dotkli implementácie RATEWeb ADR. Pri opise jeho fungovania sme si predstavili systém komunít, ktoré poskytovali užívateľovi list určitých predajcov podľa toho, aké služby daný užívateľ požadoval. V EStarMom všetci predávajúci užívatelia poskytujú služby síce rôznej kvality, no všetky rovnakého druhu. Tým pádom systém komunít odpadá a nie je v RATEWeb pre EStarMom implementovaný. Metriky pre výpočet reputácie sú však všetky plne zakomponované [1].

Princíp transakcií v bootstrap perióde sme si už predstavili. Teda funguje rovnako ako bežná transakcia, ibaže kupcom sa neplnia požiadavky a predajcom sa nemíňajú zásoby. Táto idea sa však ukázala ako nepraktická. Napríklad, pri použití TopTrust RMVP bola všetkým predajcom pridelená hodnota reputácie 0,5. Teraz ak bol pre transakciu vybraný užívateľ, ktorého hodnota reputácie po interakcii s kupcom stúpne nad 0,5, bude tento predajca vyberaný po celú dobu bootstrap periódy. Tým pádom všetci ostatní užívatelia vstúpia do normálneho behu simulácie s predvolenou hodnotou 0,5, čo je veľmi nepresné. Podobné správanie nastalo pri Gaussovom rozdelení. Je jasné, že toto správanie je nesprávne a bootstrap perióda neplní svoju úlohu. Preto bola implementácia pozmenená tak, že bez ohľadu na použitý RMVP budú v bootstrap perióde vyberaní kupci pre interakciu vždy náhodne. S týmto prístupom boli výsledky ďaleko presnejšie.

EStarMom po každej ukončenej simulácii generuje dva **.xls* súbory, v ktorých sú popísané štatistiky transakcií a presný zoznam vykonaných transakcií a udelených hodnotení. Tieto súbory neboli pri merania príliš používané, pretože neobsahovali dáta, ktoré boli požadované. Všetky uvádzané štatistické údaje boli zachytené výstupom na konzolu, ktoré bol dodatočne implementovaný priamo do zdrojového kódu.

4.4 Výsledky simulácií

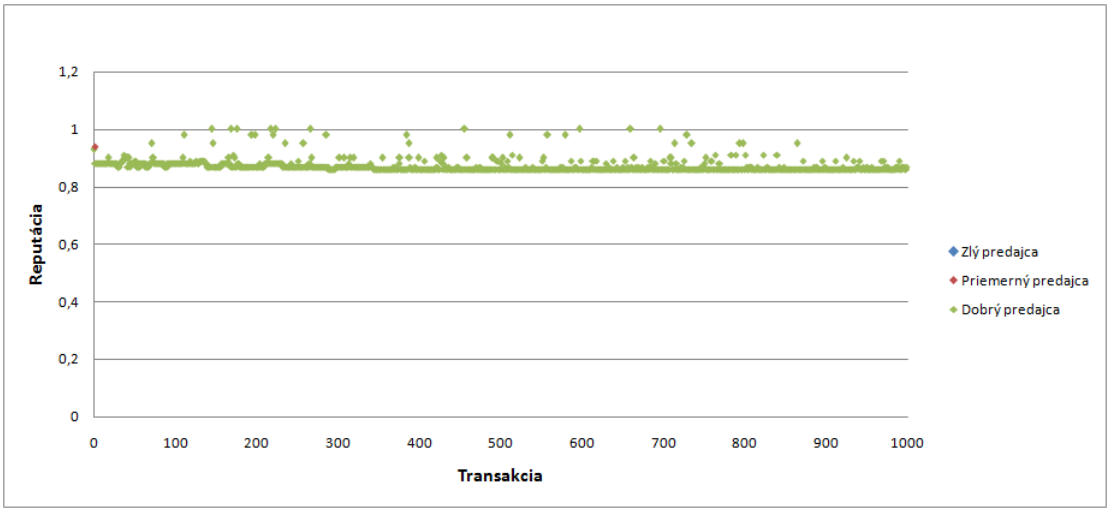
Pre nasledujúce merania platilo niekoľko spoločných nastavení, a to:

Parameter	**Počet**
Počet zlých predajcov	40
Počet priemerných predajcov	20

[1] Treba podotknúť, že mimo úprav a rozšírení, ktoré budú neskôr spomenuté, sú autormi EStarMom aplikácie spolu s implementáciou RATEWeb ADR Thao P. Nguyen a Brain J. d'Auriol

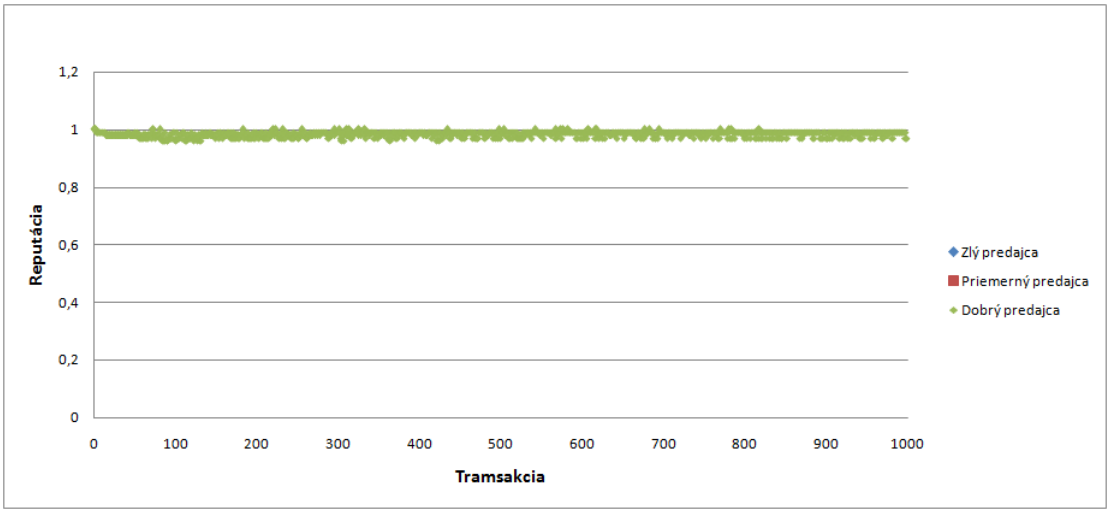
Ďalej, použitý výberový model je TopTrust V prvom meraní bol použití AVG model reputácie a stanovený pomer čestných a nečestných predajcov v pomere 4:1, teda 80 čestných a 20 nečestných. Použitý RMVP bol TopTrust.

Z grafu (4.2) možno vidieť, že pri pomere stanovenom čestných a nečestných kupujúcich AVG model zvláda výber vhodného sellera bez ťažkostí. Počas celého algoritmu sa medzi vyberanými predajcami držali tí s dobrou kvalitou služieb.



Obrázok 4.2: Meranie 1 – AVG:TopTrust kupci: 80 čestných, 20 nečestných

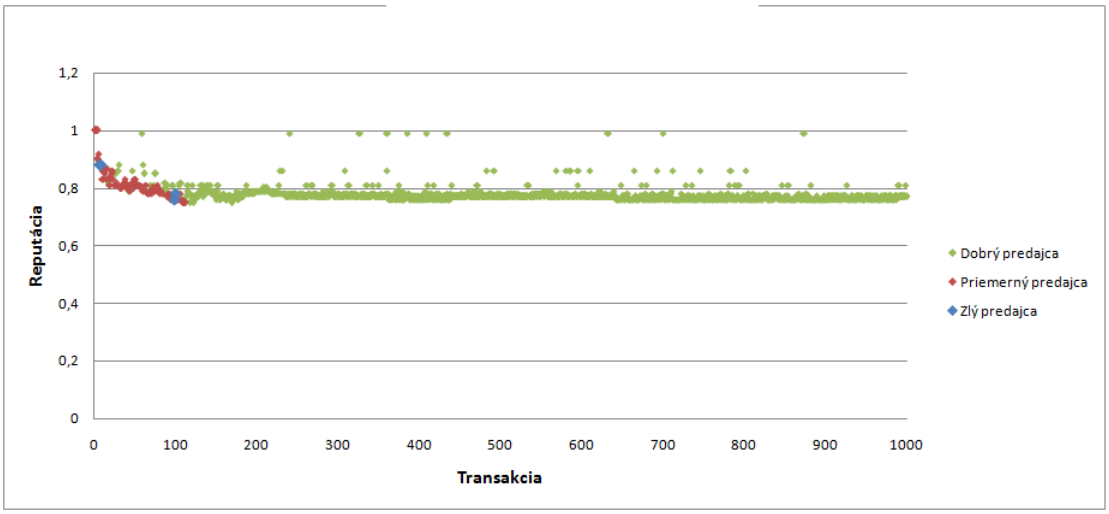
Pri druhom meraní (4.3) bol AVG model nahradení RATEWeb modelom. Pri použití RATEWeb výberového modelu je pri takom množstve čestných kupcov výsledok takmer identický s AVG modelom. Výsledky sú lepšie z toho hľadiska, že RATEWeb model dokázal lepšie rozoznať predajcov s dobrou kvalitou a udržať ich reputáciu na maximálnej hodnote. Teda nečestní kupci tento systém ani v najmenšom neohrozili.



Obrázok 4.3: Meranie 2 – RATEWeb:TopTrust kupci: 80 čestných, 20 nečestných

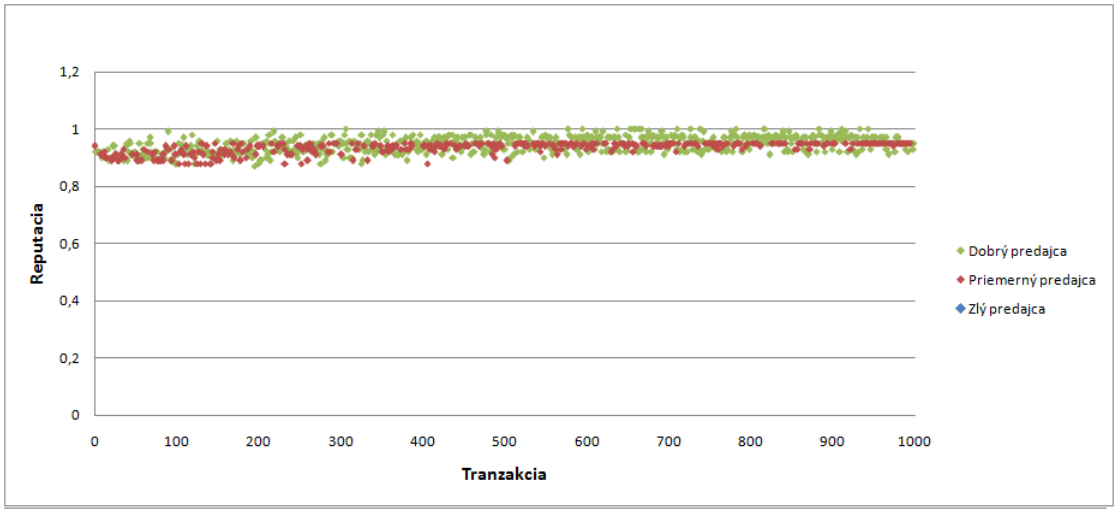
Pre ďalšie dve merania s AVG a následne RATEWeb ADR bol pomer čestných a nečestných kupcov upravený na 1:1, teda 50 čestných a 50 nečestných.

Pri tomto pomere kupcov sa vyskytnú prípady (4.4), kedy je vybraný predajca so zlou či priemernou kvalitou služieb, ktorý sa dostal na vrchol výberu práve skrz nepravdivé hodnotenia nečestných kupujúcich. Takáto situácia však nastala ojedinele a len pri začiatku simulácie. Stalo sa tak hlavne skrz bootsrapping transakcie, kedy sa predajca na interakciu vyberá náhodne. V prípade kedy nečestný kupujúci náhodne vyberie zlého predajcu, udelí mu vysoké hodnotenie, čím ho dostane vyššie pre neskoršiu selekciu. Akonáhle simulácia prejde od bootstrapping transakcií k normálnym, výberový model sa zmení z náhodného na TopTrust. Od tohto okamžiku sú vyberaný predajcovia s najvyššou hodnotou reputácie. V takom prípade sú zlí a priemerní predajcovia čestnými kupujúcimi pomerne rýchlo vypudení z výberu, ktorému budú opäť dominovať predajcovia s dobrou kvalitou služieb. Teda napriek jednoduchosti AVG výberového modelu a veľkému množstvu nečestných hodnotiacich model nebol nijak veľmi rozvrátený. Všimnime si, že jediný väčší vplyv nečestných kupujúcich bol, že priemerná hodnota reputácie oproti predošlej simulácii klesla pod 0,8.



Obrázok 4.4: Meranie 3 – AVG:TopTrust kupci: 50 čestných, 50 nečestných

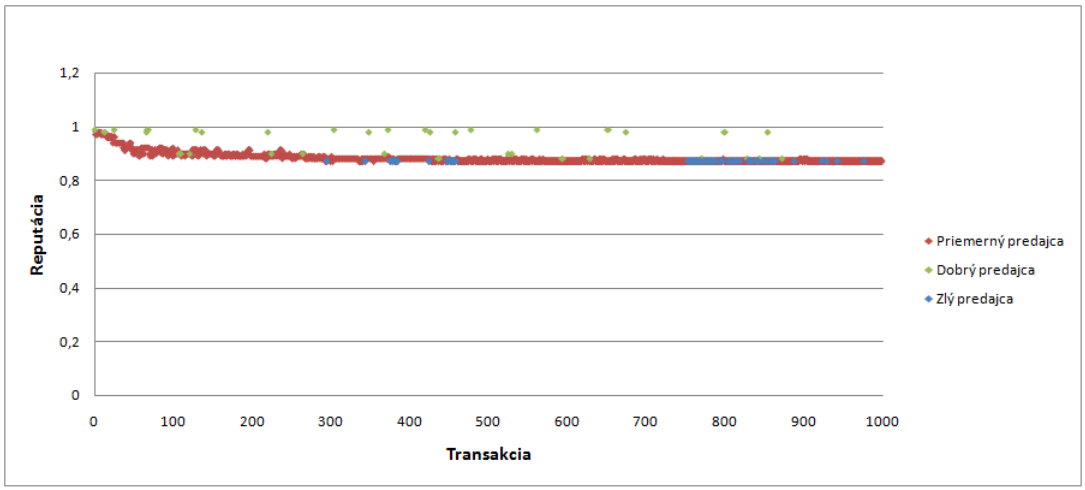
Pri rovnakom počte čestných aj nečestných kupujúcich je vyberaný predajca s dobrou kvalitou služieb približne rovnako často, ako ten s priemernou kvalitou, pričom priemerná hodnota reputácie sa drží na hodnote 0,9 až 1 (4.5). Napriek tomu, že si RATEWeb drží lepšiu priemernú hodnotu reputácie predajcov možno povedať, že RATEWeb je menej robustný oproti jednoduchému AVG modelu.



Obrázok 4.5: Meranie 4 – RATEWeb:TopTrust kupci: 50 čestných, 50 nečestných

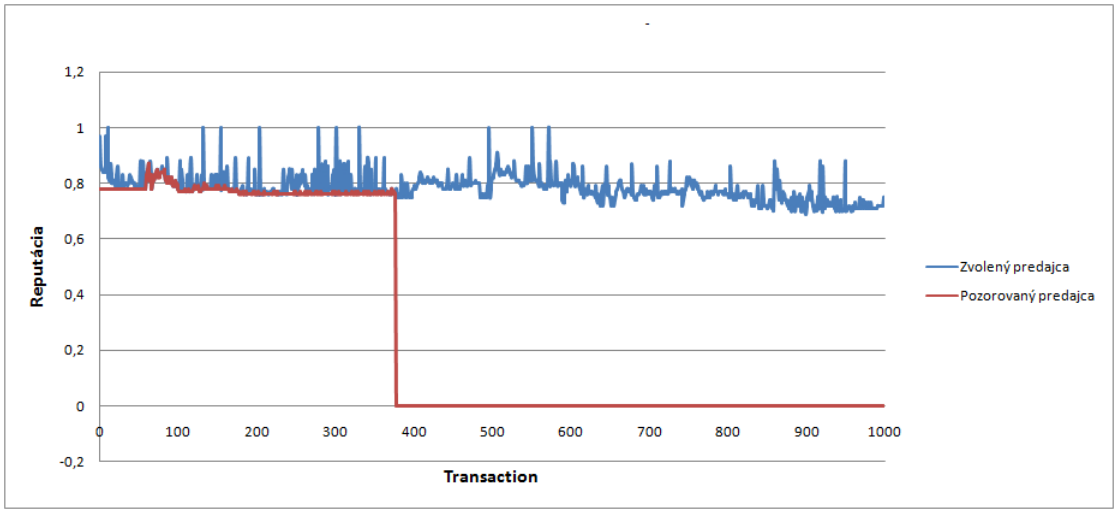
Ďalšie meranie slúži skôr ako demonštračný príklad. Pre toto meranie bol totižto pomer čestných a nečestných kupcov 1:4, teda 20 čestných a 80 nečestných. Jedná sa o prípad, ktorý je v reálnych modeloch dôvery a reputácie v podstate nereálny, pretože také množstvo zlomyseľných agentov by v podstate tvorilo vlastný nefunkčný model. Teda taký model by sa dal považovať za celkom rozvrátený. V prípade, kedy nečestní kupujúci dominujú nad čestnými sú predajcovia s dobrou kvalitou služieb zrazení dole mimo výber (4.6). Je treba si uvedomiť, že nečestní kupujúci poskytuje nie vždy zlé hodnotenie. Ak je jeho

„reálny“ názor d na službu väčší ako 0,5 udelí hodnotenie $d - 0,5$. Ak je menší, tak $d + 0,5$. Predajcovia s nízkou kvalitou služieb majú priemernú kvalitu okolo 0,2 a s tak malou hodnotu sa nemôžu dostať na vrchol pre výber (výnimkou sú práve zlí predajcovia, ktorí sú tesne pod hranicou priemerných kvality). Priemerní predávajúci užívatelia majú zato kvalitu služieb oscilujúcu okolo hodnoty 0,5. Ak je teda kvalita ich služieb málo pod 0,5, ľahko môžu byť nečestnými kupujúcimi vynesení na vrchol výberu. Malé množstvo čestných kupujúcich je pochopiteľne s priemernými službami spokojnejšia ako so zlými a preto ich po vzájomnej interakcii nezrážajú priveľmi dole. V modely kde je prevažujúci počet nečestných nad čestnými sa teda na vrcholu výberu usadia priemerní predajcovia s vysokou hodnotou reputácie ako tí zlí. (Je však dôležité si uvedomiť ako chápeme nečestných predajcov. Ak bude jednanie nečestného kupujúceho modelované inak ako v tomto prípade, výsledky sa môžu radikálne líšiť.)



Obrázok 4.6: Meranie 5 – AVG:TopTrust kupci: 20 čestných, 80 nečestných

Z doposiaľ opísaných meraní je možno vidieť, že aj tak jednoduchý ADR ako je AVG dokáže konkurovať zložitým mechanizmom RATEWeb modelu. Nutno však treba podotknúť, že RMVP, ktorý bol doteraz používaný bol výhradne TopTrust a ten disponuje jednou zásadnou nevýhodou – výrazne vyťažuje najlepších predajcov. Tento model totižto vždy volí predajcu s najvyššou hodnotou reputácie a to je zväčša vždy jeden konkrétny predajca. Tento predajca je potom vyberaný pre interakciu v každej jedenej transakcii po dobu, kým nečestní kupci nezrazia jeho reputáciu aspoň o toľko nižšie, aby padol na druhé miesto najlepšieho predajcu na trhu. Tento problém znázorňuje nasledujúci graf (4.7), kde je vidieť reputáciu predajcu, ktorý bol zvolený pre interakciu a aktuálnu reputáciu pozorovaného predajcu. Pre tento graf bol upravený počet zásob predajcov z 1000 na 100. V prípade že zásoby predajcu klesnú na 0, predajca opúšťa systém a jeho hodnoty dôvery a reputácie klesnú na 0. Ako možno vidieť, pozorovaný predajca sa dostane asi v 100. transakcii na vrchol výberu a je neustále vyberaný pre interakciu až po 100 transakciách vyčerpá všetky svoje zásoby.

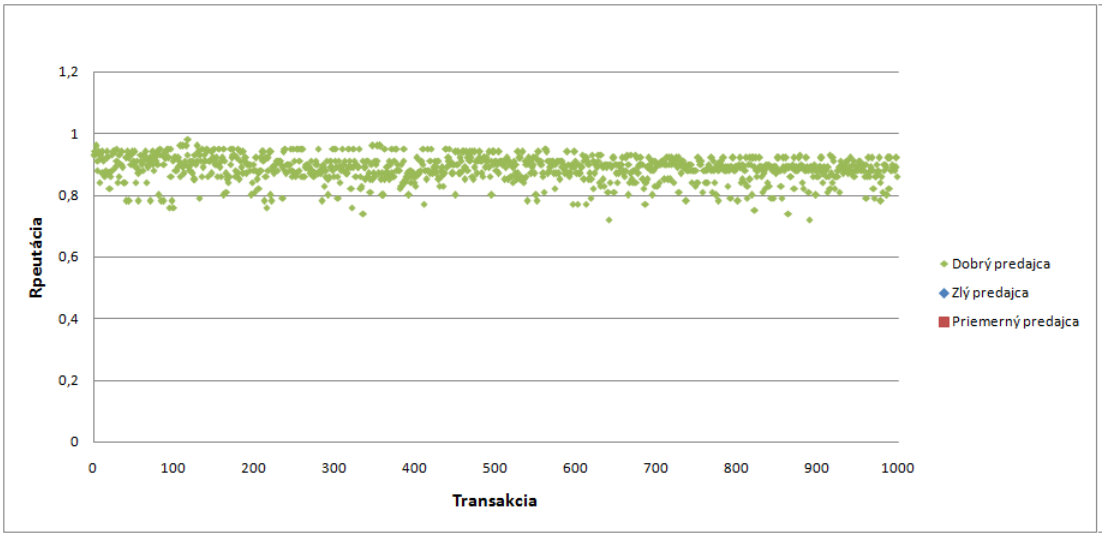


Obrázok 4.7: Meranie 6 – AVG:TopTrust kupci: 50 čestných, 50 nečestných; ukážka vyťaženia kupcov pri použití TopTrust RMVP

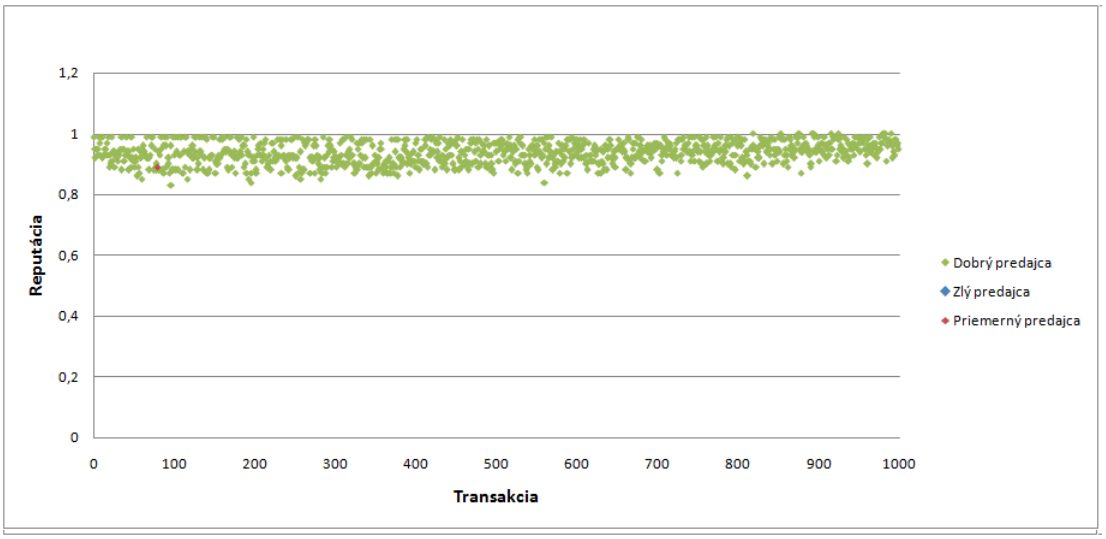
Je teda zrejmé, že RMVP nemožno plne uplatniť v reálnych multiagentných sieťach, pretože by až príliš vyťažovala najlepších agentov a nedala žiadnu šancu čiastočne horším agentom, ktorí pritom môžu ponúkať služby takmer identickej kvality.

V nasledujúcich meraniach zachováme všetky nastavenia parametrov, no ako RMVP bude stanovené Gaussovo rozdelenie pravdepodobnosti.

Výsledky sú pri AVG (4.8) aj RATEWe b(4.9) ADR pomerne rovnaké. V oboch prípadoch Gaussovo rozdelenie spôsobilo, že predajcovia s najvyššou kvalitou tovaru nie sú kompletne vyťažení požiadavkami kupcov, ale sú rozložené medzi všetkých predajcov pomerne rovnako dobrej kvality služieb. Pri RATEWeb je priemerná hodnota reputácie o niečo vyššia ako pri AVG.



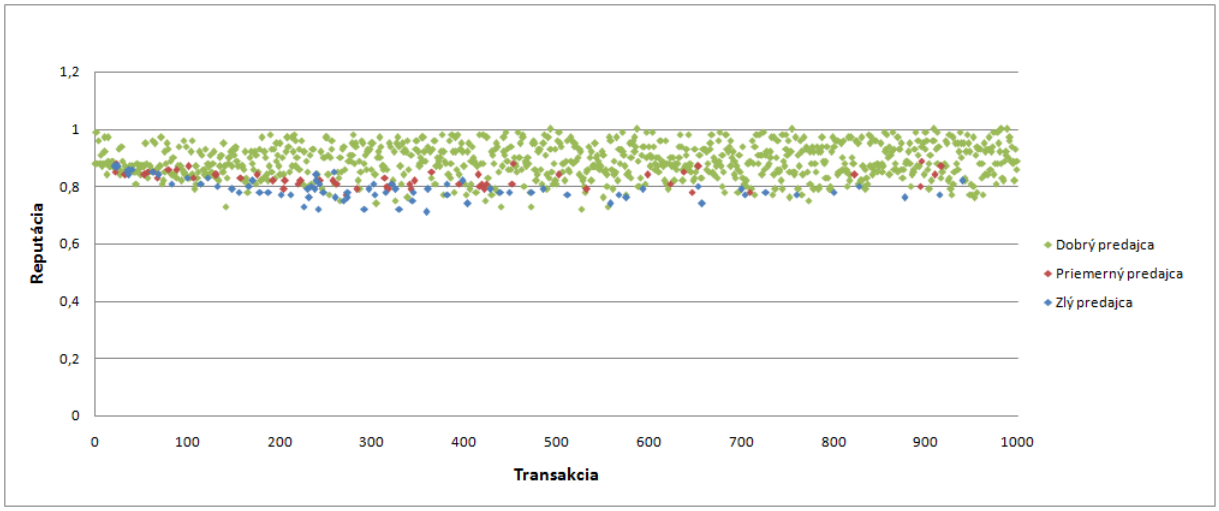
Obrázok 4.8: Meranie 7 – AVG:Gaussian kupci: 80 čestných, 20 nečestných



Obrázok 4.9: Meranie 8 – RATEWeb:Gaussian kupci: 80 čestných, 20 nečestných

Ak v simulácii stanovíme rovnaký počet nečestných kupcov ako čestných, model RATEWeb začína byť viditeľne lepší. Pri AVG (4.10) je priemerná hodnota reputácie okolo 0,7, pričom značné zastúpenie výberu majú aj predajcovia s priemernou či zlou kvalitou tovaru. Pri RATEWeb (4.11), naproti tomu, sa priemerná hodnota drží v hodnotách okolo 0,9. Napriek veľkému zastúpeniu nečestných kupcov sa výber drží prednostne u predajcov s dobrou kvalitou služieb, pričom k zlým či priemerným kupcom výber poklesne len príležitostne, keď Gaussovo rozdelenie vygeneruje malú hodnotu G_s. Možno teda povedať, že čím viac reálny model vytvoríme, tým lepším ADR sa RATEWeb oproti AVG stáva.

Obrázok 4.10: Meranie 9 – AVG:Gaussian kupci: 50 čestných, 50 nečestných



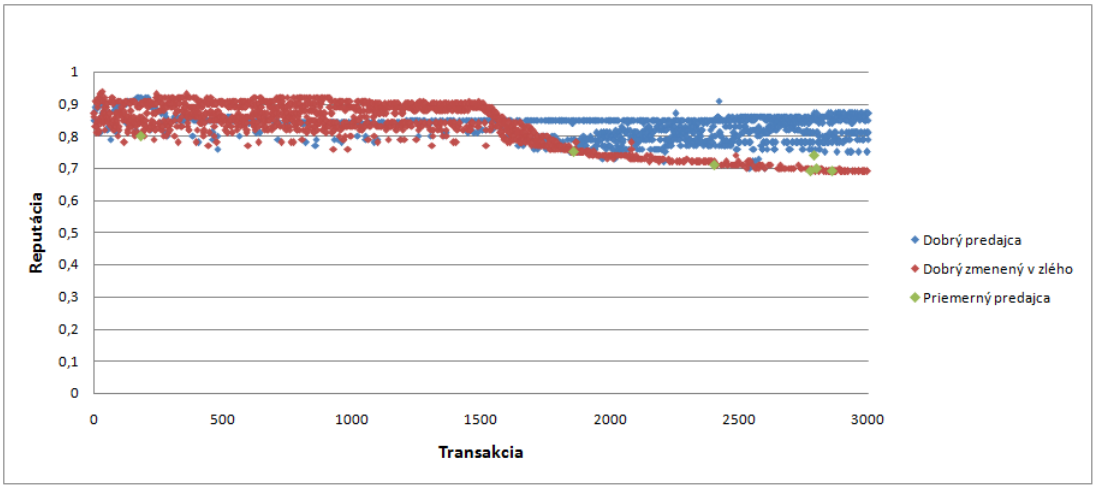
Obrázok 4.11: Meranie 10 – RATEWeb:Gaussian kupci: 50 čestných, 50 nečestných

Predajcovia so zmenou kvality

V nasledujúcich prípadoch sa v modely budú vyskytovať predajcovia, ktorí kvalitu svojich služieb menia počas simulácie. Presné počty predajcov sú:

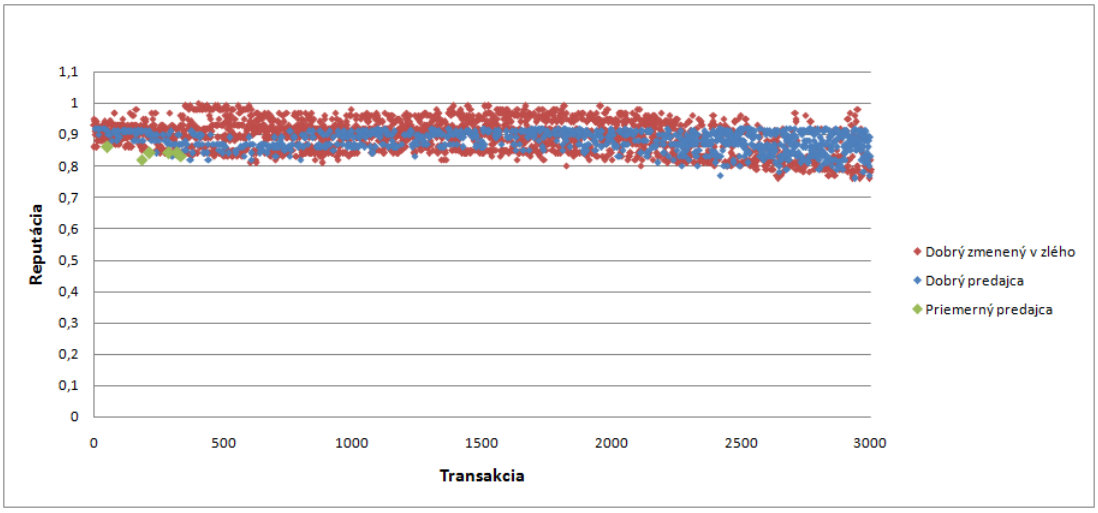
Parameter	**Počet**
Počet dobrých predajcov	10
Počet dobrých predajcov zmenených v zlých	30
Počet priemerných predajcov	30

Pre názorné účely bol počet kupcov trojnásobne zvýšený a tým pádom počet transakcií zmenený z 1000 na 3000. Pomer čestných a nečestných kupcov je 4:1, teda 240 čestných a 60 nečestných. Tri štvrtiny kupcov poskytujúcich služby dobrej kvality zmenia svoju kvalitu na zlú v polovici celkovo vykonaných transakcií. Pri použití metódy AVG je vidieť (4.12) že akonáhle si kupec zvolil interakciu s pozmeneným predajcom, jeho zlá skúsenosť sa započíta do priemerných hodnôt spolu s predajcovi doteraz udelenými. Každou transakciou je teda celková reputácia zmeneného kupca nižšia. Postupom času sa týmto spôsobom pozmenení predajcovia vyradia z výberového modelu.



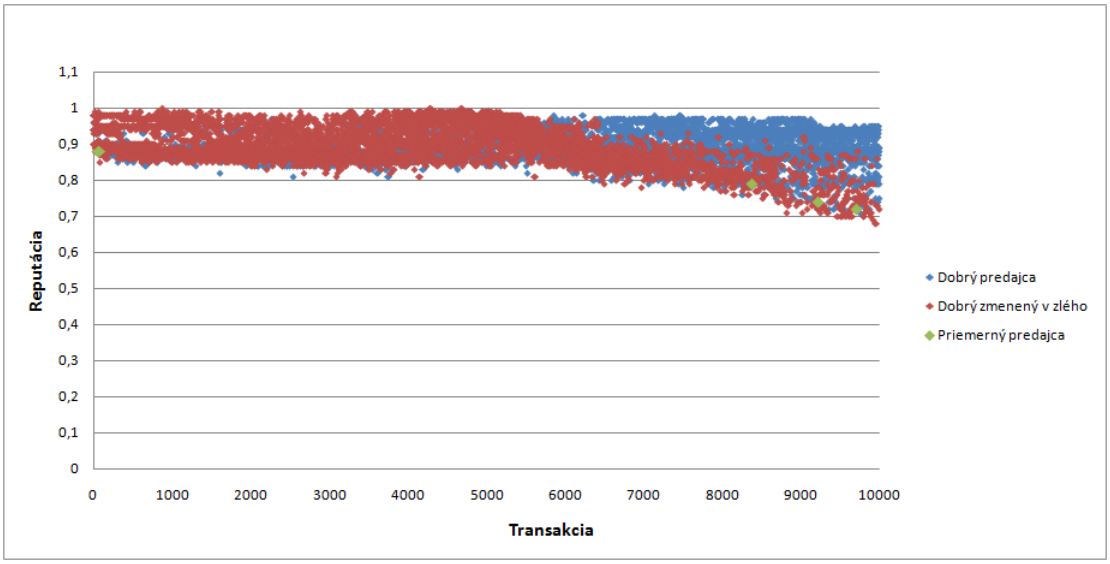
Obrázok 4.12: Meranie 11 – AVG:Gaussian kupci: 240 čestných, 60 nečestných; ukážka schopnosti AVG ADR vysporiadať sa so zmenou kvality služieb vybraných predajcov

Pri RATEWeb ADR sa však situácia vyvíja horšie (4.13). Po tom ,čo sa predajcom v polovici simulácie zmení kvalita služieb je viditeľný minimálny rozdiel. Dôvod je ten, že než sa predajcom zmenila kvalita služieb, model sa naučil brať týchto predajcov ako dôveryhodných a zdráhal sa uveriť novo hláseným hodnoteniam. Zmeníme teda počet transakcií z 3000 na 10000 (teda počet kupcov z 300 na 1000) pre zistenie či sa postoj modelu voči týmto predajcom zmení.



Obrázok 4.13: Meranie 12 – RATEWeb:Gaussian kupci: 240 čestných, 60 nečestných; ukážka zlyhania RATEWeb ADR spracovať zmenu kvality služieb vybraných predajcov

Pri tejto simulácii je postoj predajcov zmenení po 5000. transakcii (4.14). Je vidieť, že model opäť odmieta uveriť radikálnej zmene postoja predajcov. Po ďalších asi 3000 transakciách, kedy väčšina kupujúcich nahlasuje zlé hodnotenia, reputácia zmenených predajcov začína postupne klesať. Táto doba je však hrozne dlhá a za ten čas by zlomyseľní predávajúci užívatelia stihli narobiť veľké škody.

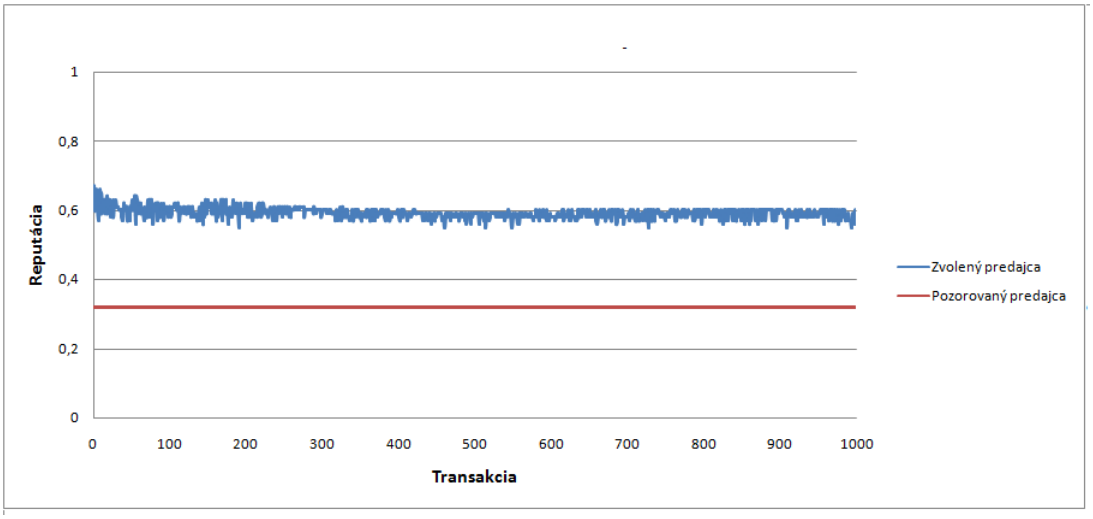


Obrázok 4.14: Meranie 13 – RATEWeb:Gaussian kupci: 800 čestných, 200 nečestných; ukážka dlhej doby spracovania zmeny kvality služieb vybraných predajcov

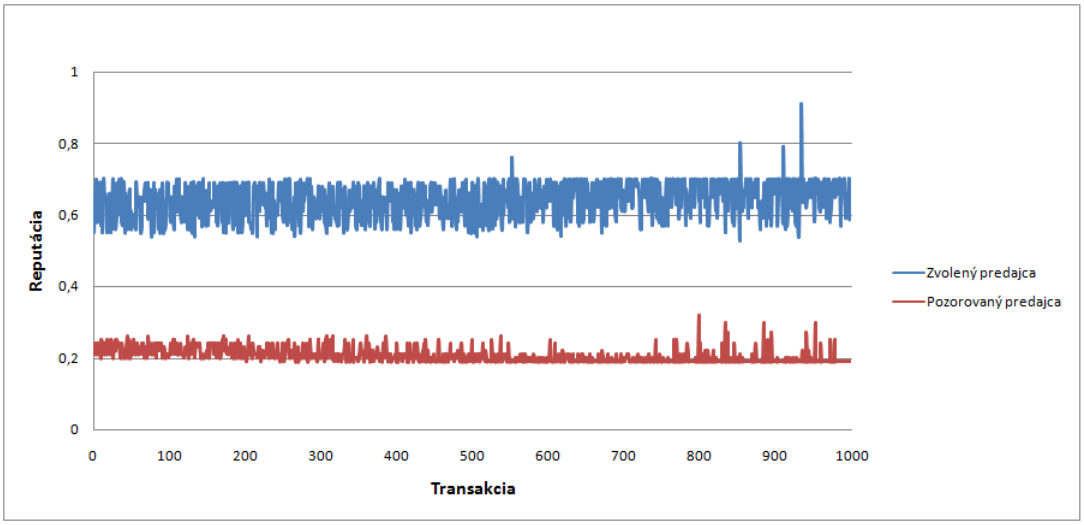
V prípade opačnej zmeny správania predajcu, teda zo zlého v dobrého chybujú oba modely. Dokazuje to 14.(4.15) a 15.(4.16) meranie, kde je v každej transakcii vyobrazená reputácia zvoleného predajcu a aktuálna reputácia pozorovaného predajcu. Pre meranie boli na trh umiestnení predajcovia:

Parameter	**Počet**
Počet zlých predajcov	5
Počet priemerných predajcov	20
Počet zlých predajcov zmenených v dobrých	1

, pričom predajca čo mení svoje správanie je práve pozorovaný užívateľ.



Obrázok 4.15: Meranie 14 – AVG:Gaussian kupci: 80 čestných, 20 nečestných; schopnosť Gaussian RMVP pri AVG ADR zaregistrovať zmenu správania predajcu zo zlého v dobrého

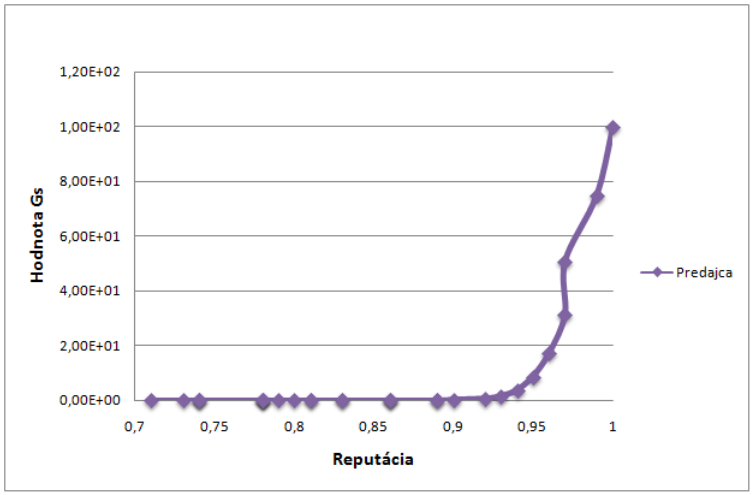


Obrázok 4.16: Meranie 15 – RATEWeb:Gaussian kupci: 80 čestných, 20 nečestných; schopnosť Gaussian RMVP pri RATEWeb ADR zaregistrovať zmenu správania predajcu zo zlého v dobrého

V oboch prípadoch začal pozorovaný užívateľ ako zlý predajca. Svoju hodnotu reputácie získal behom bootstrap transakcií, kedy boli predajcovia vyberaní náhodne a teda aj zlí predajcovia boli volení pre interakcie. Počas reálnych transakcií však RMVP začal využívať Gaussovo rozdelenie, ktoré sa ani raz nedostalo k výberu zlého predajcu. Pozorovaný predajca zmenil kvalitu svojich služieb na dobrú, teda $RealQ \in [0,71; 1]$, no keďže RMVP ho nikdy nevybralo, nemal šancu sa presadiť a trhu dominovali výhradne priemerní užívatelia.

Dôvod prečo sa pozorovaný predajca nemohol presadiť tkvie v implementácii Gassuovho rozdelenia. Totižto pri pozorovaní správania Gaussovho rozdelenia vyplynulo, že sic vyberá z väčšieho množstva užívateľov a každému užívateľovi určí hodnotu G_s, no predajcovia

s nižšou kvalitou služby ako má skupina najlepších majú výrazne nižšie hodnoty G_s a ich pravdepodobnosť výberu je takmer nulová. Vidieť to z nasledujúceho grafu (4.18), kde je vyobrazené Gaussovo rozdelenie z prostriedku simulácie nad 30 užívateľmi s dobrou kvalitou.



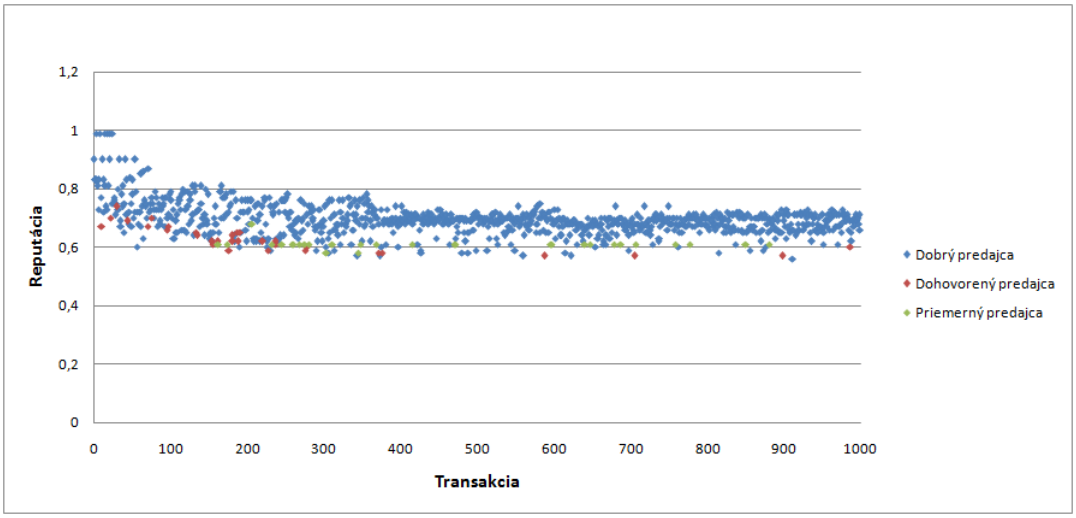
Obrázok 4.17: Gaussovo rozdelenie nad predajcami dostupnými na trhu

Dohovorené skupiny užívateľov

Pri tomto meraní bola do modelu zakomponovaná idea dohovorených užívateľov. Ten funguje na princípe, že ak dohovorenému kupcovi RMVP zvolí predajcu, ktorý nepatri do jeho skupiny dohovorených členov, udelí predajcovi najnižšie možné hodnotenie, teda 0. V opačnom prípade udelí svojmu kupcovi najvyššie možné, teda 1. Simulovaná bola výhradne situácia odpovedajúca reálne možným prípadom, teda v simulácii figurovalo 70 čestných a 30 nečestných kupcov. Väčšie počty dohovorených užívateľov by predstavovalo skôr model, v ktorom agenti spolupracujú vrámci vlastného uzavretého trhu, než užívateľov, ktorí sa snažia rozvrátiť verejný model. Ďalej, počty predajcov boli nasledovné:

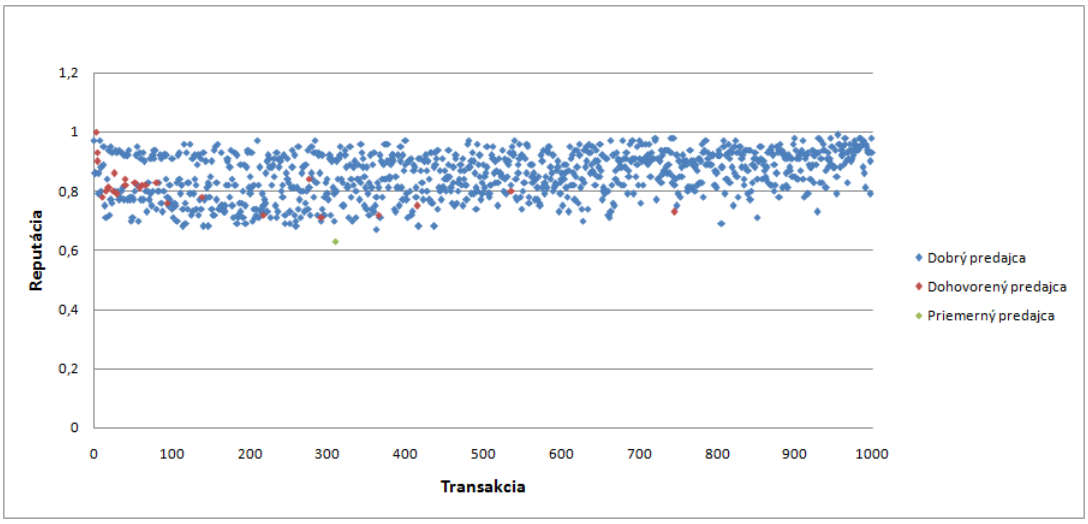
Parameter	**Počet**
Počet zlých predajcov	20
Počet priemerných predajcov	20
Počet dobrých predajcov	20
Počet dohovorených predajcov	20

Ako možno vidieť (4.18), pri použití AVG modelu sú prednostne vyberaní predajcovia s dobrou kvalitou služieb a tí dohovorení sú vybraní len ak RMVP klesne s výberom veľmi nízko. Avšak vinou dohodnutej skupiny predajcov a kupcov je priemerná hodnota reputácie všetkých užívateľov výrazne nižšia ako by mala byť.



Obrázok 4.18: Meranie 16 – AVG:Gaussian kupci: 70 čestných, 30 nečestných; Robustnosť AVG ADR voči dohovorenej skupine užívateľov

V prípade RATEWeb AVR je situácia viditeľne lepšia (4.19). Predajcovia dohovorenej skupiny sú vyberaní len zo začiatku simulácie, čo je zrejme spôsobené nízkym počtom bootstrap transakcií. Následne model odfiltruje falošných predajcov a počas simulácie sú v drvivej väčšine vyberaní užívatelia dobrej kvality. Priemerná hodnota reputácie dobrých predajcov sa taktiež drží v číslach, ktoré si títo poskytovatelia služieb skutočne zaslúžia.



Obrázok 4.19: Meranie 17 – RATEWeb:Gaussian kupci: 70 čestných, 30 nečestných; Robustnosť RATEWeb ADR voči dohovorenej skupine užívateľov

4.4.1 Rozšírenie rozhodovacieho modelu

V poslednej časti sa pozrieme na RMVP, ktorý bol implementovaný za účelom „dať šancu napraveným predajcom“, teda presadiť v systéme predajcov, ktorí sa „poučili“ zo svojho

zlého správania a rozhodli sa poskytovať služby dobrej kvality.

Návrh

MyRMVP, ako je tento RMVP pomenovaný, pracuje na nasledujúcom princípe: Algoritmus náhodne zvolí jedného predajcu zo všetkých, ktorí sa v systéme nachádzajú. Ďalej vygeneruje náhodné číslo od 0 po 100. Ak je toto číslo menšie ako 30, zdvojnásobí jeho hodnotu. Toto číslo predstavuje minimálnu hodnotu reputácie, ktorou musí zvolený predajca oplývať, aby bol vybraný pre interakciu. Následne sa pozrie na hodnotu reputácie vybraného predajcu a porovná hu s vygenerovanou hodnotou. Ak je reputácia predajcu menšia, celý proces sa opakuje. Ak je vyššia, predajca je vybraný pre interakciu s kupcom v danej transakcii. Tento algoritmus je znázornený na obrázku 4.20[2].

Algoritmus 1: *MyRMVP*

Input: $listOfSellers$
Output: $choosenSeller$

```
1  if listOfSeller.size > 0 then
2:     while loop++ < 500 do
3:         choosenSeller = listOfSellers[Random(0, listOfSeller.size)]
4:         if (theEdge = Random(0,1)) < 0,3 then
5:             theEdge* = 2
6:         end if
7:         if choosenSeller.reputationValue > theEdge then
8:             return choosenSeller
9:         end if
10:    end while
11:    return listOfSellers[Random(0, listOfSeller.size)]
12 end if
13 return null
```

Obrázok 4.20: Algoritmus MyRMVP

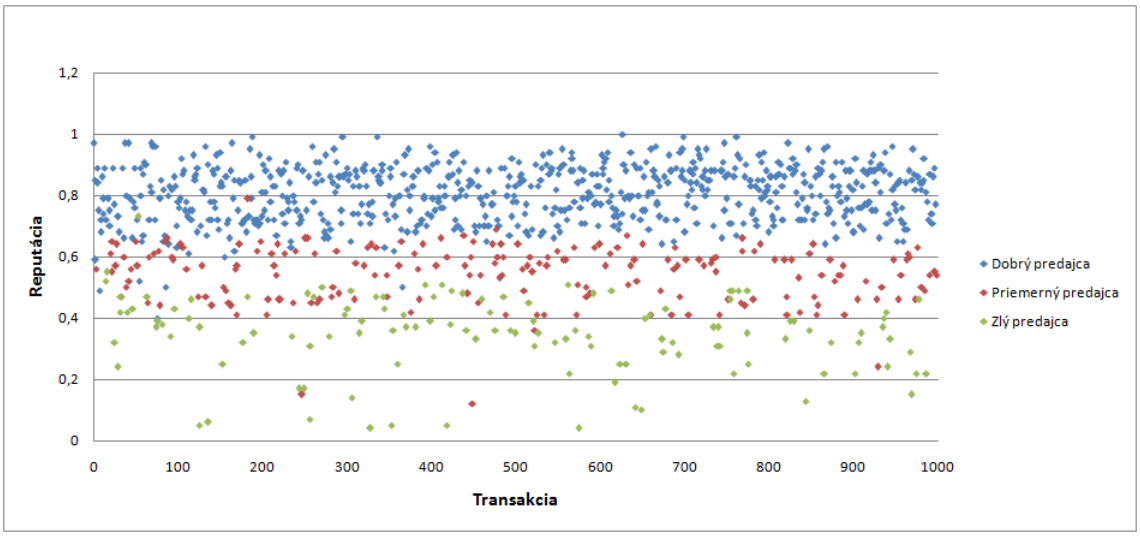
Tento princíp algoritmu umožňuje zlým predajcom aby dostali šancu preukázať, že sa ich správanie zmenilo k lepšiemu a môžu na trh ponúknuť služby dobrej kvality. Napriek tomu je treba zabezpečiť, aby zlí predajcovia neboli príliš často vyberaní pre interakciu. O to sa stará spomenutá podmienka $if(Edge < 30 then Edge = Edge * 2)$. Tá v prípade vygenerovania nízkej hodnoty požadovanie hranice zaistí aby predajcovia s kvalitou služieb menšou ako 0,3 mali dvakrát menšiu šancu pre výber ako ostatní.

Výsledky

Pre nasledujúce meranie boli použité podobné princípy ako v predchádzajúcich meraniach, teda v simulácii o 500 bootstrap a 1000 normálnych transakciách 100 čestných a nečestných predajcov v pomere 4:1 vykonávali interakcie so 100 predajcami, pričom počet dobrých a

[2]Podmienka cyklusu ($while loop++ < 500$) zabezpečuje aby algoritmus, aj keď s veľmi malou pravdepodobnosťou, necyklil príliš dlho. Ak sa vyber predajcu vykoná viac ako 500-krát, bude zvolený náhodný predajca

zlých predajcov bol 40 a počet priemerných 20. Použitý ADR bol RATEWeb a použitý RMVP, bol novovytvorený MyRMVP. Z výsledkov (4.21) možno vidieť, že použitý RMVP vyberá zo všetkých skupín užívateľských modelov, no napriek tomu uprednostňuje tých viac dôveryhodných. MyRMVP nerozlišuje striktné hranice medzi dobrou ($RealQ \in [0,7;1]$), priemernou ($RealQ \in [0,41;0,7]$) a zlou ($RealQ \in [0,01;0,4]$) kvalitou služieb. Pravidelnosť výberu užívateľa sa teda zvyšuje s jeho rastúcou reputáciou a nie na základe jeho skupiny. Inými slovami, užívateľ s väčšou reputáciou bude mať väčšiu šancu,že bude vybraný, ako užívateľ s menšou reputáciou, napriek tomu, že obaja spadajú do rovnakého užívateľského modelu.



Obrázok 4.21: Meranie 18 – RATEWeb:MyRMVP kupci: 80 čestných, 20 nečestných; Výber predajcov s použitím MyRMVP RMVP nad RATEWeb ADR za bežných podmienok

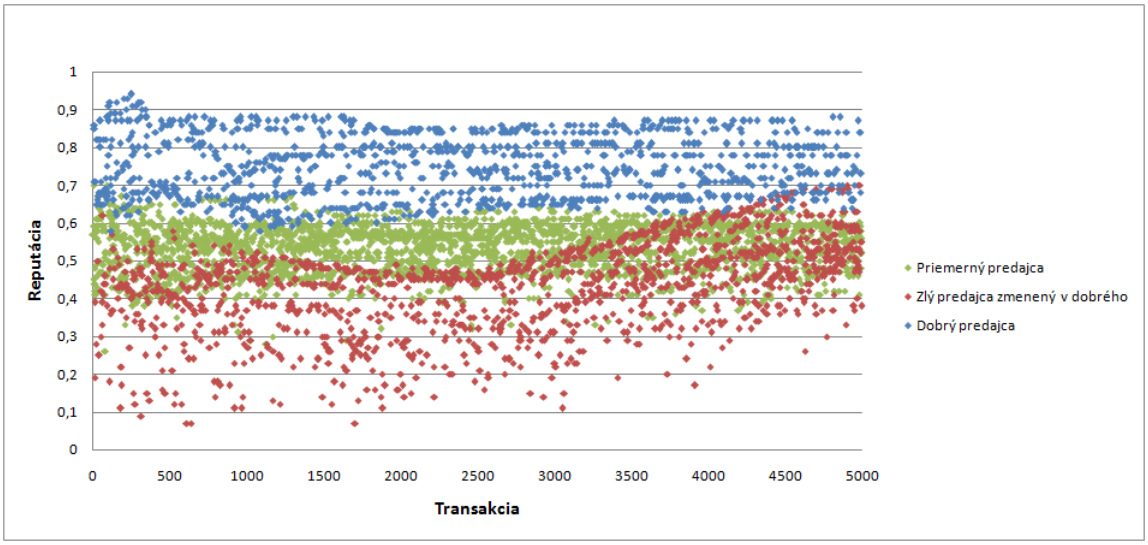
Pozrime sa teraz, ako MyRMVP dokázal začleniť napravených predajcov medzi dôveryhodnú skupinu užívateľov. Bude teda simulovaný model, v ktorom skupina užívateľov bude poskytovať služby zlej kvality, ktorú následne v polovici simulácie zmení v dobrú. Parametre pre simuláciu sú:

Parameter	**Hodnota**
Počet priemerných predajcov	30
Počet dobrých predajcov	10
Počet zlých predajcov zmenených v dobrých	30
Počet čestných kupcov	400
Počet nečestných kupcov	100
Počet bootstrap transakcií	500
Počet transakcií	5000
Počet zásob na predajcu	1000
Počet požiadavok na kupca	10

Ako ADR bol v prvom meraní použitý AVG.

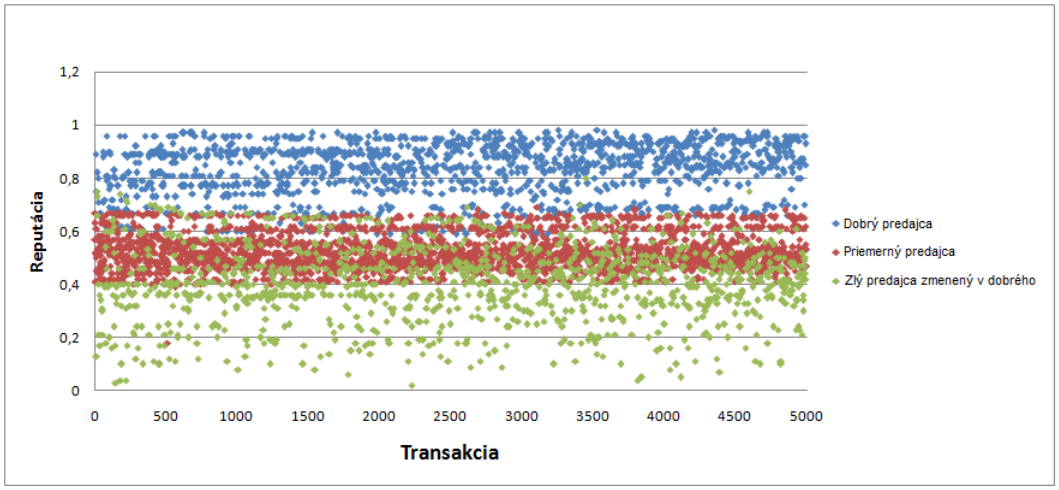
Zlí predajcovia boli príležitostne vyberaní pre interakciu s kupcom (4.22) ,pričom čím vyššiu kvalitu tovaru poskytovali, tým častejšie vyberaní boli. Od polovice simulácie, kedy

užívatelia zmenili kvalitu svojich služieb k lepšiemu, sa reputácia predajcov začala viditeľne zvyšovať. Ku koncu behu simulácie mala väčšina napravených užívateľov rovnakú reputáciu, ako priemerní predajcovia, pričom táto hodnota by sa naďalej zvyšovala, pokým by nedosiahla hodnotu najlepšie odpovedajúcu kvalite ich služieb (s ohľadom na počet čestných/nečestných kupcov).



Obrázok 4.22: Meranie 19 – AVG:MyRMVP kupci: 400 čestných, 100 nečestných; Schopnosť AVG ADR rozoznať zmenenú kvalitu služieb vybraných predajcov za použitia MyRMVP RMVP

Avšak pri použití RATEWeb ADR je situácia viditeľne horšia (4.23). ADR sa zachoval podobne ako v prípade simulácie dobrých predajcov zmenených v zlých (4.13). Teda model si opäť navykol na správanie jednotlivých užívateľov a zdráhal sa uveriť ich náhlej zmene správania napriek tomu, že väčšina kupujúcich poskytovala čestné hodnotenia. Predajcovia boli teda naďalej braní ako nedôveryhodní a ich reputácia sa počas celého behu simulácie takmer vôbec nezlepšila.



Obrázok 4.23: Meranie 20 – RATEWeb:MyRMVP kupci: 400 čestných, 100 nečestných; Schopnosť RATEWeb ADR rozoznať zmenenú kvalitu služieb vybraných predajcov za použitia MyRMVP RMVP

4.4.2 Zhrnutie

Na základe výsledkov prezentovaných vyššie možno konštatovať, že pri použití zložitého ADR, akým je napríklad RATEWeb, sa výsledky môžu len čiastočne zlepšiť či v niektorých prípadoch aj zhoršiť, oproti jednoduchej metóde výpočtu hodnoty reputácie aritmetickým priemerom, akou disponuje AVG. Sila RATEWebu evidentne tkvie v zabezpečení trhu pred dohodnutými skupinami užívateľov, ktorí by chceli model rozvrátiť. Avšak jeho neschopnosť vysporiadať sa s náhlou zmenou správania užívateľov je veľmi citeľná. Ďalej je treba konštatovať, že správny chod modelu nespočíva len v silnom ADR, ale závisí aj od voľby vhodného RMVP. Experimenty jasne ukázali, že pri použití nesprávneho RMVP môžu nastať problémy, ako priveľké vyťaženie užívateľov či neschopnosť modelu zachytiť zmenu v chovaní užívateľov. Je preto dôležité, aby voľba RMVP odpovedala použitému ADR a naopak.

Kapitola 5

Záver

Cieľom tejto práce bolo vykonať rešerš ohľadom existujúcich modelov dôvery a reputácie pre multiagentné siete. Za týmto účelom bolo nevyhnutné zoznámiť sa so základnou teóriou okolo pojmov agent, dôvera, reputácia a ďalšími v úzkom vzťahu k nim. Práca sa zaoberá tým, ako tieto pojmy zaradiť do oboru umelej inteligencie a ako simulovať ich význam v multiagentných sieťach.

Ďalej práca predstavuje tri rozličné modely, ktoré simulujú dôveru a reputáciu medzi agentmi. Z predstavených modelov je najväčšia pozornosť venovaná RATEWeb modelu, nad ktorým je v štvrtej kapitole vykonaná väčšina meraní. Z meraní vystáva, že napriek komplexnosti a uvádzanej robustnosti modelu, má model značné nedostatky, a nie úplne zvláda všetky situácie, ktoré v multiagentnej sieti môžu nastať.

Preto ďalšie smerovanie tejto práce môže byť zvýšenie robustnosti skúmaného modelu, prípadne nájsť lepšie konštantné hodnoty pre parametre modelu ako tolerancia pozornosti, pesimizmus užívateľov či dočasná senzitivita hodnotení.

Literatura

[1] adaptic: Amazon:About Comments, Feedback and Ratings. online, [navštívené 12.1.2016].
URL http://www.amazon.com/gp/help/customer/display.html?nodeId=537806

[2] Bordini, R. H.; Hübner, J. F.; Wooldridge, M.: *Programming multi-agent systems in AgentSpeak using Jason*, ročník 8. John Wiley & Sons, 2007.

[3] Davidson, S.: How to Make a Chart or Graph in Excel. online, [navštívené 12.3.2016].
URL http://blog.hubspot.com/marketing/how-to-build-excel-graph#sm.0001il5ouneiidxapje104qatbzjc

[4] Giddens, A.: *Sociologie*. Argo, 2000, ISBN 8072031244.

[5] Jøsang, A.; Keser, C.; Dimitrakos, T.: Can we manage trust? In *Trust management*, Springer, 2005, s. 93–107.

[6] Kamvar, S. D.; Schlosser, M. T.; Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, ACM, 2003, s. 640–651.

[7] Kincl, J.: *Gaius- učebnice práva ve čtyřech knihách*. Aleš Čeněk, 2007, ISBN 9788073800543.

[8] Lažanský, J.; Mařík, V.; Štěpánková, O.: *Umělá inteligence (1)*. Praha:Academia, 1993, ISBN 80-200-0502-1.

[9] Lucina, R.: Reputácia verzus Obchodná značka a konsekvencie. online, [navštívené 14.12.2016].
URL https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=32363

[10] Luck, M.; d'Inverno, M.; aj.: Constraining autonomy through norms. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 2*, ACM, 2002, s. 674–681.

[11] Macy, M. W.; Willer, R.: From factors to actors: Computational sociology and agent-based modeling. *Annual review of sociology*, 2002: s. 143–166.

[12] Malik, Z.; Bouguettaya, A.: Rateweb: Reputation assessment for trust establishment among web services. *The VLDB Journal—The International Journal on Very Large Data Bases*, ročník 18, č. 4, 2009: s. 885–911.

[13] Mármol, F. G.; Pérez, G. M.: Providing trust in wireless sensor networks using a bio-inspired technique. *Telecommunication systems*, ročník 46, č. 2, 2011: s. 163–180.

[14] ORSAVA, T.: Multiagentový simulační model vybraného trhu [online]. 2013 [cit. 2016-05-10].
URL http://is.muni.cz/th/323016/prif_b/

[15] P Nguyen, T.; J d'Auriol, B.: EStarMom: Extendable Simulator for Trust and Reputation Management in Online Marketplaces. 2015.

[16] Pecinovský, R.: *Myslíme objektově v jazyku Java*, ročník 2. Grada Publishing, 2008, ISBN 9788024726533.

[17] Rybička, J.: *LaTeX pro začátečníky*. Konvoj, 1999, ISBN ISBN 80-85615-77-0.

[18] Rábová, Z.; Hanáček, P.; Peringer, P.; aj.: *Užitečné rady pro psaní odborného textu*. FIT VUT v Brně, 2016-03-09, [Online; navštívené 15.4.2016].
URL http://www.fit.vutbr.cz/info/szz/psani_textu.html.cs

[19] Samek, J.: *Dúvěra a reputace v distribuovaných systémech*. Disertační práce, Vysoké učení technické v Brně, Fakulta informačních technologií, Brno, 2011.

[20] Vodáková, A.; Petrusek, M.: *Velký sociologický slovník*. Praha: Karolinum, 1996, ISBN 80-7184-310-5.

[21] Zbořil, F.: *Plánování a komunikace v multiagentních systémech*. Disertační práce, Vysoké učení technické v Brně, Fakulta informačních technologií, Brno, 2004.

Príloha A

Obsah CD

Priložené dátové médium obsahuje:

- Zdrojové kódy aplikácie
- Spustiteľný JAR súbor
- Technickú správu vo formáte pdf
- Zdrojové súbory technickej správy pre LaTeX
- README súbor
- Prezentačný plagát