ŽILINSKÁ UNIVERZITA V ŽILINE
FAKULTA RIADENIA A INFORMATIKY

MANAŽMENT GRIDOVÝCH PROSTRIEDKOV

Dizertačná práca

28360020163001

Študijný program:	9.2.9 aplikovaná informatika
Študijný odbor:	Aplikovaná informatika
Pracovisko:	Katedra informatiky, Fakulta riadenia a informatiky, Žilinská univerzita v Žiline
Školiteľ:	doc. Ing. Penka Martincová, PhD.

Žilina, 2016 **Ing. Slavomír Kavecký**

Venovanie

Prácu venujem svojim rodičom, ktorí sa aj napriek ťažko zažívanému obdobiu snažia uchovať si životný optimizmus.

Poďakovanie

Poďakovať sa chcem svojej školiteľke doc. Ing. Penke Martincovej, PhD. za jej rady, usmernenie ako i slová opory. Veľká vďaka patrí mojim rodičom, ktorí sú mi stálou oporou. Poďakovať sa chcem i priateľom a známym, ktorí mi počas štúdia pomáhali udržať si pozitívnu myseľ a dobrú náladu.

Abstrakt

Ad hoc gridová infraštruktúra umožňuje vykonávať sporadické a krátkodobé kolaborácie medzi používateľmi infraštruktúry a poskytovateľmi zdieľajúcimi svoje prostriedky v rámci infraštruktúry. Práca sa zaoberá problematikou bezpečného vykonávania takto sprostredkovaných kolaborácií. Práca poskytuje rozbor súčasného stavu problematiky a pomenúva nedostatky známych riešení. Práca taktiež obsahuje návrh riešenia problematiky, ktoré je založené na integrácii riadenia dôvery do ad hoc gridovej infraštruktúry. Navrhnuté riešenie je overené pomocou počítačovej simulácie preukazujúcej vhodnosť navrhnutého riešenia. Práca popisuje aj oblasti ďalšieho výskumu zameriavajúce sa na vylepšenie navrhnutého riešenia a jednoduchosť implementácie riešenia existujúcimi ad hoc gridovými infraštruktúrami.

Abstract

Ad hoc grid infrastructure is capable to mediate short-term and sporadic collaborations executed between users and resource providers. The thesis deals especially with a secure execution of those mediated collaborations. The thesis surveys the state of the art in ad hoc grid security provision and identifies shortcomings of current solutions. The thesis also contains a solution proposal based on enhancement of the ad hoc grid infrastructure with trust management. The verification of the proposed solution is carried out by a computer simulation proving the correctness of the solution. The thesis describes also areas for future research dealing with refinement of the proposed solution and ease implementation of the proposed solution in the existing ad hoc grid infrastructures.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam pojmov a skratiek

Pojem / skratka	Význam
P2P	klient-klient (rovný s rovným)
HPC (High Performance Computing)	vysoko výkonné počítanie
CA (Certificate Authority)	certifikačná autorita
AS (Authentication Server)	autentifikačný server
token	autentifikačný kód
AS (Account Server)	server spravujúci používateľské účty
ACL (Access Control List)	zoznam prístupových práv
TI (Trust Index)	index dôvery (veľkosť hodnoty dôvery)
SD (Security Demand)	veľkosť požiadavky na poskytovanie bezpečnosti
Flooding	mechanizmus zasielania správ jedným uzlom všetkým jeho okolitým uzlom
Sandbox	bezpečnostný mechanizmus oddeľujúci vykonávaný program od aktuálneho systému vykonávajúci tento program

Pojem / skratka	Význam
Malware	všeobecné označenie pre škodlivý program
IDS (Intrusion Detection System)	programové alebo technické vybavenie monitorujúce systém pred škodlivými aktivitami
TLS (Transport Layer Security)	protokol slúžiaci na šifrovanie dát
IPsec (Internet Protocol Security)	sada protokolov pre bezpečné komunikovanie prostredníctvom internet protokolu
RAID (Redundant Array of Independent Disks)	súhrnný termín označujúci rôzne schémy ukladania dát na viacero pevných diskov
MIPS (Million Instructions per Second)	jednotka označujúca výkonnosť počítača v miliónoch inštrukcií za sekundu

Kapitola 1

Úvod

Vysoko výkonné počítanie a spracovanie veľkého množstva dát sa v poslednom období začalo využívať širokou verejnosťou v oveľa väčšej miere. Tento trend je dôsledkom najmä lepšej dostupnosti technológií, ktoré toto počítanie a spracovanie dát umožňujú. K popredným technológiám umožňujúcim spomínané funkčné prvky patrí aj Grid[1], ktorého vznik sa datuje na začiatok deväťdesiatich rokov minulého storočia.

Hlavnými charakteristickými črtami gridovej technológie sú rôznorodosť a geografický rozptyl uzlov, ktoré sú súčasťou gridovej infraštruktúry. Tieto uzly slúžia buď ako zdroje potrebné pre uskutočnenie výpočtov a spracovanie dát, alebo ako prístupové body ku gridovej infraštruktúre. Uzly sú poskytované na použitie rôznymi organizáciami, ktoré často využívajú rozdielne výpočtové systémy. Účelom gridovej infraštruktúry je integrácia a správa zdrojov a služieb v rámci distribuovaných, heterogénnych a dynamických virtuálnych organizácií tak, aby sa grid ako technológia z pohľadu jeho používateľov javil ako jeden obrovský výpočtový prostriedok. Umožniť prístup k výpočtovým zdrojom, službám, dátam a iným zdrojom bez ohľadu na ich fyzické umiestnenie si však vyžaduje prekonanie hraníc, ktoré inak bežne oddeľujú rôzne výpočtové systémy jednotlivých organizácií [2].

Tradičná gridová technológia je založená na centralizovanej architektúre, v rámci ktorej sú gridové funkčné prvky (správa zdieľaných zdrojov, ich monitorovanie a dodržia-

vanie kontrolovaného prístupu k nim) vykonávané jednou presne na tento účel vybranou administratívnou autoritou. Avšak existujú také scenáre použitia gridových výpočtov, pre ktoré sa nehodí centralizovaná správa zdrojov aplikovaná tradičnou gridovou technológiou. Ak istá skupina jednotlivcov potrebuje zdieľať prostriedky a vykonávať na nich výpočtové úlohy v rámci krátkodobej alebo jednorázovej spolupráce, tak nadbytočná réžia vyplývajúce zo zriadenia tradičnej gridovej infraštruktúry nie je pre túto skupinu praktická. Takýto typ spolupráce sa vyznačuje dynamickou zmenou členov gridovej komunity a prístupových politík k zdieľaným prostriedkom v rámci tejto komunity[4].

Princíp decentralizácie správy zdrojov sa uplatnil najmä v ad hoc gridovej technológii. Hlavnou motiváciou vývoja ad hoc gridovej technológie je jej schopnosť umožňovať krátkodobé a jednorázové spolupráce medzi dynamicky vznikajúcimi komunitami používateľov. V rámci decentralizovanej architektúry ad hoc gridovej infraštruktúry však nie je možné zveriť správu zdrojov len jednej na tento účel zvolenej administratívnej autorite. I napriek tomu musia byť poskytované zdroje a služby chránené pred neoprávneným použitím alebo úmyselným poškodením.

Problematika rozobratá v práci sa zaoberá špecifikáciou bezpečnosti zdrojov a služieb zdieľaných ad hoc gridovou infraštruktúrou a prepojením bezpečnosti s inými funkčnými prvkami infraštruktúry. Zvyšok práce je členení nasledovne: Kapitola 2 uvádza hlavný cieľ práce; Kapitola 3 popisuje spôsob poskytovania bezpečnosti v tradičnej a ad hoc gridovej infraštruktúre; Navrhované zlepšenie poskytovania bezpečnosti ad hoc gridovou infraštruktúrou uvádza kapitola 4; Overenie navrhnutého riešenia a zhodnotenie dosiahnutých cieľov sú popísané v kapitole 5; a Kapitola 6 uvádza zhrnutie práce.

Kapitola 2

Cieľ práce

Účelom ad hoc gridovej technológie je umožniť vykonávanie výpočtov na zdieľaných výpočtových prostriedkoch. Splnenie tohto účelu si ale vyžaduje, aby ad hoc gridová infraštruktúra podporovala základné funkčné prvky ako riadenie vykonávania úloh, riadenie spracovania dát, vyhľadávanie a správa zdieľaných prostriedkov, bezpečné vykonávanie úloh, bezpečné zdieľanie výpočtových prostriedkov, poskytovanie informácií o zdieľaných prostriedkoch a vykonávaných úlohách a v neposlednej miere i podpora nastaviteľnosti fungovania ad hoc gridovej infraštruktúry [2].

Koncept ad hoc gridovej technológie vznikol začiatkom nového milénia [4] a do dnešných dní vzniklo viacero ad hoc gridových infraštruktúr (OurGrid [5, 3], MoGrid [6]), ktoré sú inšpirované týmto konceptom. Charakteristika vlastná každej ad hoc gridovej infraštruktúre je požiadavka na bezpečné vykonávanie úloh a bezpečné zdieľanie prostriedkov. Avšak do dnešných dní nie je podpora bezpečnosti v prostredí ad hoc gridovej infraštruktúry dostatočne implementovaná. Nedostatky v oblasti bezpečnosti tak neumožňujú viac spopularizovať používanie ad hoc gridovej infraštruktúry.

Hlavným cieľom práce je zlepšenie implementácie poskytovania bezpečnosti v rámci ad hoc gridovej infraštruktúry a je formulovaný nasledovne: **začlenenie konceptu riadenia dôvery do bezpečnostnej infraštruktúry ad hoc gridovej technológie a**

umožniť rozhodovanie o uskutočnení spolupráce medzi entitami a o kontrole prístupu k zdieľaným prostriedkom na základe dôvery medzi entitami. Začlenenie riadenia dôvery do bezpečnostnej infraštruktúry umožní zvýšenú ochranu poskytovateľov zdieľaných prostriedkov ako i používateľov týchto prostriedkov. Predpokladaným dôsledkom začlenenia riadenia dôvery medzi základné funkčné prvky ad hoc gridovej infraštruktúry je väčšia akceptácia tejto technológie zo strany jej používateľov ako i poskytovateľov zdieľaných prostriedkov.

Hlavný cieľ sa skladá z nasledujúcich čiastkových cieľov:

- **Definovať model dôvery.** Dôvera je abstraktný pojem. Pre účely rozhodovania o spolupráci medzi entitami v rámci ad hoc gridovej infraštruktúry je však potrebné kvantifikovať dôveru konkrétnou hodnotou. Model dôvery musí identifikovať všetky relevantné faktory (riziko spojené s každou spoluprácou v distribuovanom systéme, neistota vyplývajúca z nedostatku informácií o spolupracujúcich entitách, vlastnosti systému zdieľaného prostriedka, odpozorované správanie z predošlých spoluprác, atď.) ovplyvňujúce dôveru medzi gridovými entitami, špecifikovať ich vzájomnú závislosť a definovať spôsob ich vzájomnej agregácie do výslednej hodnoty dôvery.
- **Navrhnúť proces riadenia dôvery z pohľadu používateľa ad hoc gridovej infraštruktúry.** Ad hoc gridová infraštruktúra musí byť schopná sprostredkovať vykonanie používateľovej úlohy na takom zdieľanom prostriedku, ktorý je z pohľadu používateľa dostatočne dôveryhodný. Dôveryhodnosť je v tomto prípade chápaná ako ochota poskytovateľa zdieľaného prostriedka poskytnúť všetky dohodnuté zdroje a zabezpečiť prístup k používateľovým dátam len autorizovaným osobám. V rámci procesu riadenia a vykonávania používateľovej úlohy je potrebné navrhnúť začlenenie riadenia dôvery do procesu plánovania úlohy a procesu alokácie zdieľaných prostriedkov.
- **Navrhnúť proces riadenia dôvery z pohľadu poskytovateľa prostriedkov**

zdieľaných v rámci ad hoc gridovej infraštruktúry. Ad hoc gridová infraštruktúra musí umožniť prístup k zdieľaným prostriedkom len takým používateľom, ktorí sú z pohľadu poskytovateľa prostriedkov dostatočne dôveryhodní. Dôveryhodnosť je v tomto prípade chápaná ako ochota používateľa využívať len dohodnuté zdroje v dohodnutom čase, pristupovať len k autorizovaným dátam a vykonávať úlohy neohrozujúce systém zdieľaného prostriedka. V rámci procesu riadenia a vykonávania používateľovej úlohy je potrebné navrhnúť začlenenie riadenia dôvery najmä do procesu plánovania úlohy a procesu alokácie zdieľaných prostriedkov.

- **Overiť správnosť navrhnutého modelu a mechanizmov riadenia dôvery.** Začlenenie riadenia dôvery umožní vykonávať rozhodnutia o vykonávaní spoluprác medzi entitami na základe dôvery. Pre overenie správnosti riešenia je potrebné zvoliť správne prostriedky ako i navrhnúť kvalitatívne a kvantitatívne metriky, s pomocou ktorých sa určí vplyv riadenia dôvery na vlastnosti ad hoc gridového systému. Hlavný dôraz bude kladený predovšetkým na jednoznačné kvantifikovanie celkového prínosu integrácie dôvery do procesu správy a riadenia bezpečného vykonávania úloh.

Kapitola 3

Opis problematiky a súčasný stav

Cieľ práce definuje riadenie dôvery ako prostriedok umožňujúci používateľom ad hoc gridovej infraštruktúry a poskytovateľom zdieľaných prostriedkov rozhodovať sa o vykonaní potencionálnych kolaborácií. Nasledujúce sekcie popisujú tradičné a ad hoc gridové infraštruktúry, špecifikujú proces riadenia dôvery, definujú riešenú problematiku a popisujú súčasný stav integrácie riadenia dôvery do gridových infraštruktúr.

3.1 Dôvera a modelovanie dôvery

Význam pojmu dôvera je značne vágny a je ťažké ho presne zadefinovať. Našťastie, význam pojmu dôvera môže byť zredukovaný iba na oblasť, v rámci ktorej sa tento pojem týka iba online prostredí ako je internet ale distribuované online systémy. Nasledujúce sekcie sa zaoberajú špecifikovaným pojmu dôvera, popisom dôvery ako obojstranného vzťahu medzi entitami a definovaním procesu riadenia dôvery.

3.1.1 Definícia dôvery

Pojem **dôvera** je v kontexte distribuovaných online prostredí bežne definovaný v odbornej literatúre dvoma definíciami [7, 8]:

- **kontextovo nezávislá dôvera**, ktorá je definovaná nasledovne: dôvera je subjektívna pravdepodobnosť, s ktorou jednotlivec A očakáva od iného jednotlivca B správne vykonanie istej akcie, pričom blaho jednotlivca A je závislé na výsledku vykonanej akcie.
- **kontextovo závislá dôvera**, ktorá je definovaná nasledovne: dôvera predstavuje mieru, do akej je jednotlivec A ochotný spoľahnúť sa na iného jednotlivca B v istej situácii s pocitom relatívnej bezpečnosti a to aj v prípade, že sa môžu vyskytnúť negatívne následky spôsobené spoľahnutím sa na jednotlivca B.

Kontextovo nezávislá dôvera medzi dôverovaným a dôverujúcim jednotlivcom popisuje dôveru ako vzťah založený na pravdepodobnosti, kde dôverujúci jednotlivec očakáva správne vykonanie akcie dôverovaným jednotlivcom s istou pravdepodobnosťou. Avšak, škoda v prípade vzniku chyby (zlyhanie akcie z ľubovoľného dôvodu) môže byť taká veľká, že nie je možné spoľahnúť sa na vykonanie akcie dôverovaným jednotlivcom a to nezávisle od pravdepodobnosti vzniku chyby a od zisku, ktorý vykonanie akcie prináša.

Kontextovo závislá dôvera definuje kontext ako súčasť hodnoty dôvery a prepája odhad spoľahlivosti dôverovaného jednotlivca s rizikom, ktoré vyplýva z neistého výsledku spolupráce medzi dôverujúcim a dôverovaným jednotlivcom. Z tohto dôvodu sa kontextovo závislá dôvera javí byť viac vhodná pre modelovanie hodnoty dôvery.

3.1.2 Dôvera ako obojstranný vzťah

Dôvera predstavuje obojstranný vzťah medzi jednotlivcami, ktorí vzájomne spolupracujú prostredníctvom distribuovaného systému akým je aj grid. Dôvera v tomto prípade je použitá ako prostriedok, na základe ktorého sa obe kolaborujúce strany rozhodujú, či sú alebo nie sú ochotné vzájomne spolupracovať na základe vzájomnej dôvery.

Obojstranný vzťah dôvery v rámci distribuovaného systému je možné rozdeliť do viacerých tried dôvery nasledovne [8]:

- **Dôvera v poskytované služby**. Táto trieda dôvery popisuje dôveru používateľa vkladanú do zdieľaných prostriedkov poskytovateľa. V tomto prípade sa používateľ snaží chrániť pred nespoľahlivým alebo nezodpovedným poskytovateľom prostriedkov.
- **Dôvera v prístupovú kontrolu**. Táto trieda dôvery popisuje dôveru poskytovateľa zdieľaných prostriedkov voči používateľovi, ktorý žiada o službu alebo zdroj. Trieda dôvery zodpovedá paradigme prístupovej kontroly, ktorá je elementárnym základom počítačovej bezpečnosti (ochrana voči nepovolenému prístupu k zdieľaným prostriedkom).
- **Dôvera pri delegácii**. Táto trieda dôvery popisuje dôveru, ktorú jednotlivec (používateľ alebo agent) vkladá do delegovaného agenta vykonávajúceho činnosti a rozhodnutia v mene jednotlivca. Táto trieda dôvery sa môže chápať ako špeciálny prípad dôvery v poskytované služby.
- **Dôvera v identitu**. Táto trieda dôvery predstavuje presvedčenie, že identita jednotlivca (používateľ alebo poskytovateľ zdieľaných prostriedkov), ktorou sa daný jednotlivec prezentuje, je skutočne pravá identita daného jednotlivca.
- **Dôvera v kontext**. Táto trieda dôvery popisuje presvedčenie jednotlivca (používateľ, poskytovateľ alebo delegovaný agent), že existujúce systémy a inštitúcie podporia priebeh vykonania úlohy a poskytnú potrebnú podporu v prípade, že pri vykonávaní úlohy nastanú nežiadané okolnosti. Kontextom sa v tomto prípade chápe napríklad očakávaný zisk ako i možná strata a dodatočné náklady spojené s vykonaním úlohy.

3.1.3 Definícia riadenia dôvery

Úspešnosť a prežitie jednotlivca v spoločnosti je závislé na ochote iných jednotlivcov spolupracovať s ním. Vo všeobecnosti majú ľudia tendenciu spolupracovať iba s dôvery-

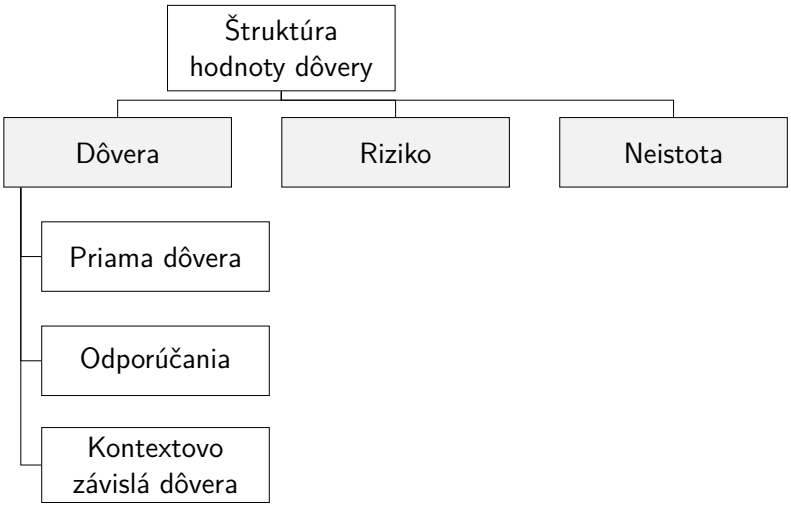
hodnými jednotlivcami. Získanie dôvery iných jednotlivcov v spoločnosti je teda dôležitá schopnosť. Ľudia majú viacero geneticky určených a kultúrne získaných stratégií, ktoré im umožňujú javiť sa ako dôveryhodní a spoľahliví jednotlivci. Najjednoduchšia a pravdepodobne aj najčastejšie používaná metóda získavania dôvery je skutočne správať sa spoľahlivo a dôveryhodne. Žiaľ, snaha o nepravdivé prezentovanie vlastnej dôveryhodnosti za účelom získania osobného profitu nie je žiadnou výnimkou. Dôležitou ľudskou vlastnosťou teda nie je iba schopnosť prezentovať svoju vlastnú dôveryhodnosť a spoľahlivosť, ale aj schopnosť správne ohodnotiť dôveryhodnosť a spoľahlivosť iných jednotlivcov.

Schopnosť prezentovať vlastnú dôveryhodnosť a zároveň i schopnosť ohodnotiť dôveryhodnosť iných jednotlivcov sa označuje ako **riadenie dôvery**. V kontexte online distribuovaných systémov, ktoré je možné definovať ako distribuované systémy vzájomne prepojené počítačovou sieťou, sa riadenie dôvery definuje nasledovne [7]: riadenie dôvery označuje aktivity a metódy, ktoré:

- umožňujú entitám vykonávať rozhodnutia o možných transakciách spojených s istou mierou rizika na základe ohodnotenia dôveryhodnosti spolupracujúcich entít,
- a zároveň umožňujú vlastníkom a správcom systémov správne prezentovať a zväčšovať ich vlastnú dôveryhodnosť ako i dôveryhodnosť ich systémov.

3.1.4 Štruktúra hodnoty dôvery

Dôvera medzi dvoma entitami v online distribuovanom systéme je určovaná na základe ich doterajšej vzájomnej interakcie. Každá udalosť, ktorá je schopná ovplyvniť hodnotu dôvery, je vnímaná dôverujúcou entitou buď ako negatívna skúsenosť alebo ako pozitívna skúsenosť. Ak je udalosť vnímaná ako negatívna skúsenosť, tak dôveryhodnosť hodnotenej entity je znížená. A naopak, ak je udalosť vnímaná ako pozitívna skúsenosť, tak je dôveryhodnosť entity zvýšená o istú mieru [9]. Vplyv na dôveru medzi dvoma



Obrázok č. 1: Štruktúra hodnoty dôvery

entitami majú aj odporúčania od iných entít v systéme. Tieto odporúčania zodpovedajú hodnote dôvery, ktorá je výsledkom odpozorovaných výsledkov interakcií entít s danými entitami. Výsledná hodnota dôvery je taktiež ovplyvnená aj aktuálnym stavom systému spolupracujúcich entít a od kontextu aktuálnej situácie, ktorá predchádza vzájomnej spolupráci entít. Vo všeobecnosti je dôvera medzi entitami určovaná na základe priamej dôvery, odporúčaní a kontextovo závislej dôvery (ako je zobrazené na obrázku č.1).

Priama dôvera ako súčasť celkovej hodnoty dôvery je použitá vo väčšine modelov dôvery (prehľad posudzovaných modelov je uvedený v tabuľke č.3), ktoré začleňujú riadenie dôvery do procesu rozhodovania o vykonaní alebo nevykonaní možných spoluprác medzi entitami v online distribuovanom systéme. Priama dôvera medzi entitami je odvodená najmä od výsledkov interakcií, ktoré entity mali v minulosti. Posudzované modely sa však líšia v spôsobe výpočtu priamej dôvery. Song et al. [10, 11] v navrhnutom modeli určujú priamu dôveru na základe predošlej úspešnosti vykonávania úloh, vlastností ochrannej brány firewall, vlastností a schopností antivírusového programu a na základe schopností systému detekovať nepovolený vstup. Azzedin a Maheswaran [12] vypočítavajú priamu dôveru na základe správania sa ohodnocovanej entity. Správanie sa entity je vyjadrené ako ochota entity dodržať požiadavky stanovené hodnotiacou entitou. Do-

držiavanie pravidiel dôverovanou entitou má za vplyv zvýšenie priamej dôvery, avšak každé porušenie týchto požiadaviek sa prejaví ako penalizácia priamej dôvery.

Odporúčania ako súčasť dôvery sa označujú aj ako reputácia dôverovanej entity a predstavujú všetko, čo sa pripisuje entite na základe jej charakteru alebo povesti. Ak si je dôverujúca entita vedomá reputácie dôverovanej entity, tak dôverujúca entita môže určiť dôveru voči dôverovanej entite práve na základe reputácie (napr. dôverovaná entita je dôveryhodná vďaka dobrej reputácii). Na druhej strane ak má dôverujúca entita súkromnú znalosť o dôverovanej entite (napr. prostredníctvom priamej skúsenosti s entitou), tak privátna znalosť má väčší vplyv ako ľubovoľná reputácia dôverovanej entity (napr. dôverovaná entita môže byť dôveryhodná aj napriek zlej reputácii). Súčasné modely dôvery definujú viacero spôsobov určovania reputácie v prostredí online distribuovaných systémov. Ding et al. [13] určujú reputáciu na úrovni virtuálnych organizácií a nie na úrovni používateľov a poskytovateľov zdrojov, ktorí sú združení v rámci virtuálnych organizácií. Takýto postup je zvolený pre lepšiu škálovateľnosť systému. Ryutov et al. [14] vo svojom modeli stanovujú reputáciu monitorovaním správania sa entít. Ak niektorá z entít vykoná akciu, ktorá je považovaná za nebezpečnú, tak systém rozposiela varovné hlásenia iným podobným entitám hneď potom, ako bola hrozba spozorovaná.

Kontextovo závislú dôveru ako zložku dôvery je možné popísať pomocou nasledovného príkladu [7]: *Predstavme si osobu, ktorá má použiť staré lano na útek z tretieho poschodia domu počas požiarneho cvičenia. Počas cvičenia táto osoba samozrejme neverí, že by toto lano bolo použiteľné na útek. Teraz si predstavme tú istú osobu uväznenú v tom istom dome počas skutočného požiaru a jedinú únikovú cestu z domu predstavuje to isté staré lano, ktoré bolo použité pri požiarnom cvičení. V prípade skutočného požiaru by väčšina ľudí dôverovala lanu ako prostriedku na únik z budovy.* V uvedenom príklade je kontextovo nezávislá dôvera v staré lano počas požiarneho cvičenia rovná kontextovo nezávislej dôvere v staré lano počas skutočného požiaru: lano je staré a teda nie je

možné ho použiť na útek z budovy. Kontextovo závislá dôvera sa v prípade skutočného požiaru odlišuje od kontextovo nezávislej dôvery: v prípade požiaru je staré lano dostatočne dôveryhodné ako prostriedok na únik z budovy. Na základe uvedeného príkladu je teda zrejmé, že kontext vplýva na celkovú hodnotu dôvery významným spôsobom.

Každá spolupráca vykonávaná prostredníctvom online distribuovaného systému je nevyhnutne spojená s nebezpečenstvom vzniku neočakávanej udalosti, ktorá môže spôsobiť ujmu spolupracujúcim entitám. Čím viac je potrebné bezchybné vykonanie úlohy, tak tým závažnejšia škoda môže nastať v prípade vzniku zlyhania vykonávania. Explicitné uvažovanie o možných nebezpečenstvách spojených s vykonávaním úlohy sa stáva dôležitým už počas rozhodovania o uskutočnení alebo neuskutočnení možnej budúcej spolupráce. V rámci procesu rozhodovania sa v online distribuovanom systéme o vykonaní kolaborácie sú pravdepodobnosť výskytu chyby a náklady s ňou spojené označované ako **riziko**. Riziko a dôvera sú vzájomne previazané v tom slova zmysle, že ak nie je súčasťou spolupráce aj riziko, tak potom nie je nutné vykonávať rozhodnutia o spolupráci na základe dôvery. V literatúre sa popisujú dve rôzne relácie medzi dôverou a rizikom [15]: riziko určujúce úroveň dôvery a dôvera určujúca úroveň rizika. Riziko určujúce úroveň dôvery je možné popísať nasledovne: počas istej situácie alebo počas vykonávania istej akcie so známou úrovňou rizika by mala byť entita dostatočne dôveryhodná, aby jej bolo povolené ocitnúť sa v danej situácii alebo vykonať danú akciu (t. j. úroveň rizika určuje minimálnu úroveň požadovanej dôveryhodnosti). Dôveru určujúcu úroveň rizika je možné popísať nasledovne: počas istej situácie alebo počas vykonávania istej akcie, ktorá sa týka entity so známou úrovňou dôveryhodnosti, riziko by malo byť dostatočne nízke, aby entite bolo povolené ocitnúť sa v danej situácii alebo vykonať danú akciu (t. j. úroveň dôveryhodnosti určuje maximálnu úroveň akceptovateľného rizika).

Neistota pri spolupráci sprostredkovanej prostredníctvom online distribuovaného systému vzniká vtedy, keď dôverujúca entita si nie je úplne istá presnosťou svojho rozhodnu-

tia o uskutočnení alebo neuskutočnení možnej budúcej spolupráce. Táto neistota vzniká ako dôsledok absencie informácií, ktoré majú vplyv na výsledné rozhodnutie. Chýbať môžu buď všetky relevantné informácie (v prípade, kedy spolupracujú dve navzájom neznáme entity bez predošlých skúseností a nie sú dostupné ani odporúčania) alebo len časť informácií (v prípade, kedy spolupracujú dve navzájom neznáme entity bez predošlých skúseností, ale odporúčania od iných entít sú dostupné). Vznik neistoty z dôvodu nedostatku informácií nemusí mať nevyhnutne vplyv na hodnotu dôvery. Ak sa však miera neistoty výrazne zmení, tak sa automaticky zmení aj dôvera entity v spolupracujúcu entitu [15].

3.2 Popis gridovej infraštruktúry

Funkčnosť a použiteľnosť gridovej infraštruktúry je závislá od miery implementácie základných funkčných prvkov, medzi ktoré patrí riadenie vykonávania úloh, riadenie spracovania dát, vyhľadávanie a správa zdieľaných prostriedkov, bezpečné vykonávanie úloh, bezpečné zdieľanie výpočtových prostriedkov, poskytovanie informácií o zdieľaných prostriedkoch ako i vykonávaných úlohách a v neposlednej miere i podpora nastaviteľnosti fungovania ad hoc gridovej infraštruktúry. Tradičné gridové infraštruktúry (Globus Toolkit [16], Gridbus Middleware [17] a UNICORE [18]) implementujú spomínané funkčné prvky vo veľmi dobrej miere. V prípade ad hoc gridových infraštruktúr je situácia ale rozdielna. Jeden z hlavných nedostatkov ad hoc gridových infraštruktúr je napríklad ich nedostatočná implementácia bezpečnosti. Nasledujúce sekcie bližšie popisujú charakter gridových infraštruktúr a poskytujú porovnanie ich základných charakteristických vlastností.

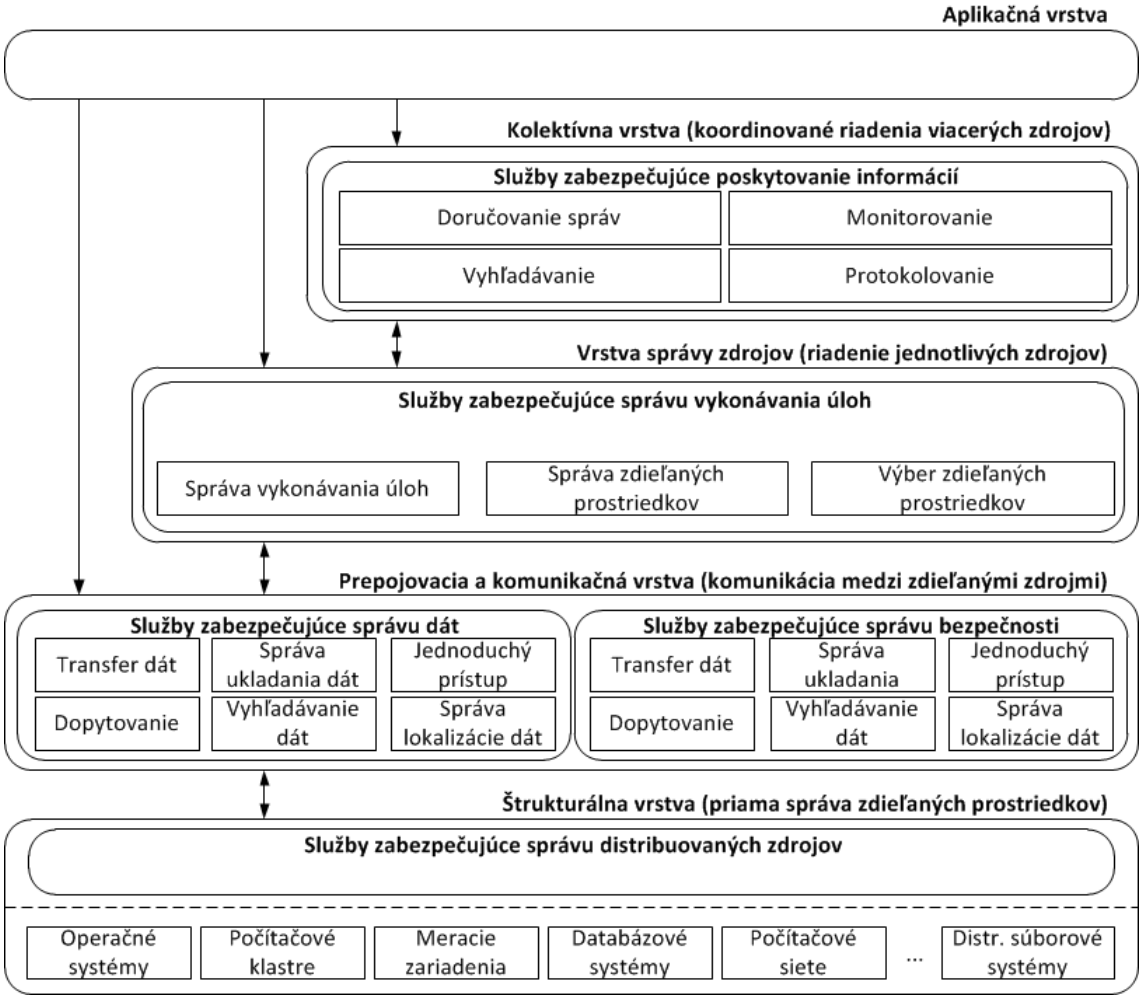
3.2.1 Tradičný grid

Tradičná gridová technológia vznikla spojením existujúcich technológií ako sú distribuované počítanie, virtualizácia, webové služby, internet a rôzne kryptografické techniky. Tieto technológie existovali už istý čas a slúžili na rôzne účely. Gridová infraštruktúra prebrala funkčné prvky týchto technológií a vytvorila tak systém poskytujúci výpočtové zdroje pre vysoko výkonné počítanie.

Virtualizácia je jedna zo základných vlastností príznačných pre každú gridovú infraštruktúru a zodpovedá integrácií geograficky rozptýlených a heterogénnych systémov. Virtualizácia umožňuje, aby používatelia abstrahovali od reálnej implementácie prístupu k zdieľaným prostriedkom (nemusia vedieť nič o skutočnom umiestnení zdrojov, prístupových protokoloch, atď.) a pristupovali k distribuovaným systémom prostredníctvom jedného prístupového bodu. Z pohľadu používateľov existuje iba jeden výpočtový systém, ktorému môžu zaslať svoje žiadosti o poskytnutie služby. Vyhľadanie a lokalizovanie vhodných zdieľaných prostriedkov schopných spracovať žiadosť o službu je už zodpovednosťou príslušnej gridovej infraštruktúry.

Gridová infraštruktúra kombinuje služby, ktoré umožňujú prístup k zdieľaným prostriedkom, prístup k dátam, manipuláciu dát, poskytovanie bezpečnosti, plánovanie vykonávania úloh a vykonávanie úloh. Tieto služby sú podporované informačnými službami, ktoré zabezpečujú vyhľadávanie dostupných prostriedkov, monitorovanie používania prostriedkov, protokolovanie atď. Architektúra tradičnej gridovej infraštruktúry, ktorú prvýkrát navrhli Foster, Kesselman a Tuecke [1], je členená do vrstiev zobrazených na obrázku č. 2. Každá vrstva obsahuje množinu služieb a funkcií poskytovaných vyššej vrstve a využíva služby a funkcie nižšej vrstvy. Najnižšia vrstva spravuje prístup k zdieľaným prostriedkom, nástrojom a ostatným entitám integrovaných do gridovej infraštruktúry.

Skupina organizácií využívajúca gridovú infraštruktúru ako nástroj pre dosiahnutie spoločného cieľa (vykonanie určitej množiny úloh, spracovanie jedinečných dát, vytvore-



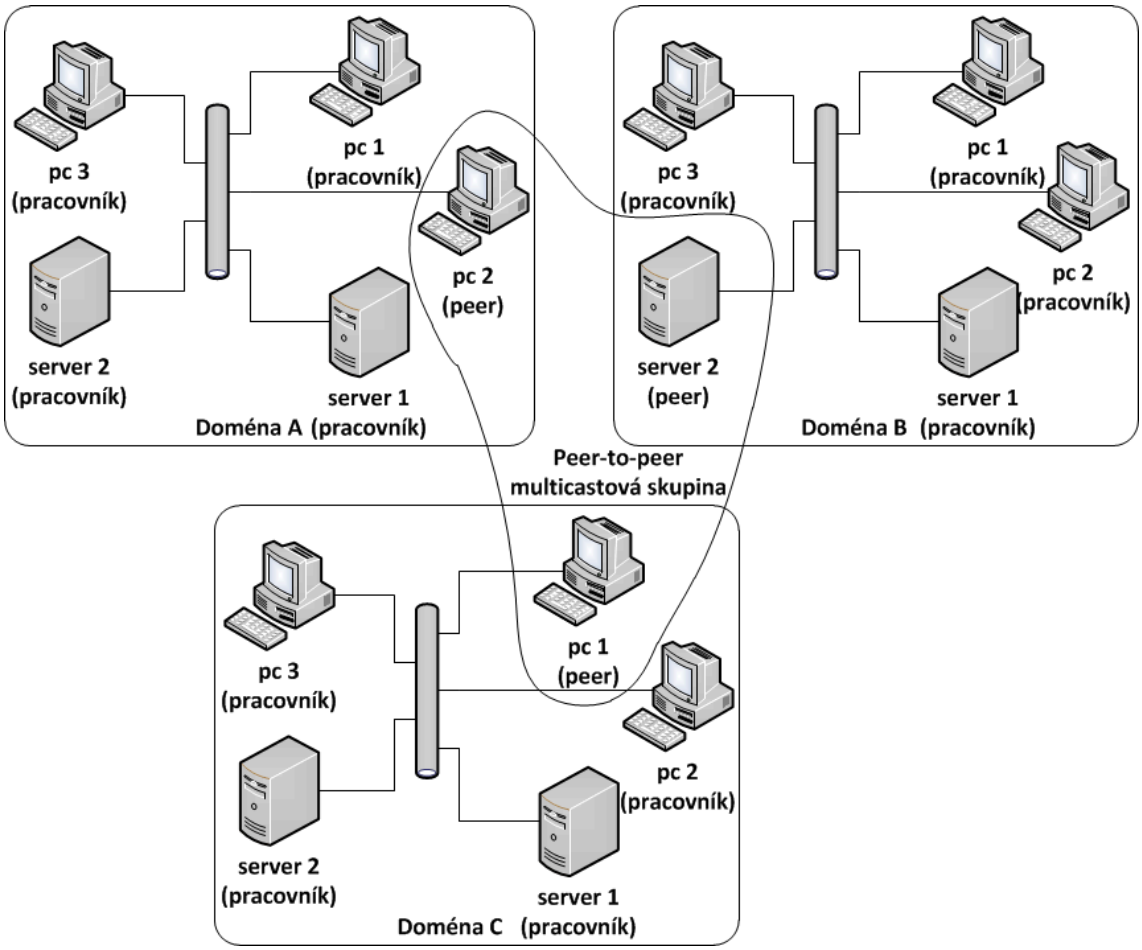
Obrázok č. 2: Architektúra tradičnej gridovej infraštruktúry [1, 2]

nie špecifických služieb poskytovaných gridovou infraštruktúrou, atď.) je označovaná ako virtuálna organizácia. Virtuálna organizácia môže mať záujem o prostriedky alebo služby poskytované aj inými gridovými aplikáciami. Avšak spolupráca medzi aplikáciami implementovanými na báze rôznych gridových infraštruktúr si vyžaduje poskytovanie služieb týmito infraštruktúrami štandardizovaným spôsobom. Neoficiálna množina štandardov a odporúčaní zhrnutá v štandarde OGSA (Open Grid Services Architecture) [2] definuje, že gridové služby musia byť schopné preklenúť hranice, ktoré ich zvyčajne izolujú v rámci gridovej aplikácie. Narozdiel od vyššie spomenutej architektúry definuje OGSA štandardné služby, ktoré nie sú rozčlenené do vrstiev. Štandard však umožňuje vytváranie nových služieb vzájomným kombinovaním a interakciou definovaných služieb. Táto schopnosť OGSA služieb umožňuje ich rozčlenenie do jednotlivých vrstiev definovaných architektúrou tradičnej gridovej infraštruktúry tak ako je to znázornené na obrázku č. 2.

Virtuálne organizácie sú charakteristické svojou dynamickosťou - nová organizácia sa môže pripojiť alebo existujúca členská organizácia môže opustiť virtuálnu organizáciu hocikedy v závislosti od svojich potrieb. Tento dynamický charakter virtuálnych organizácií sa prejavuje štrukturálnou decentralizáciou tradičnej gridovej technológie. Avšak je nutné si uvedomiť, že tradičná gridová infraštruktúra poskytuje svoje služby centralizovane.

3.2.2 Ad hoc grid

Tradičné gridové infraštruktúry sú založené na centralizovanej architektúre, v rámci ktorej sú riadenie zdieľaných prostriedkov, ich monitorovanie a zabezpečenie prístupovej kontroly k zdieľaným prostriedkom vykonávané jednou a presne na tento účel určenou administratívnou autoritou. Všetci účastníci gridovej komunity zdieľajú spoločný cieľ a pri vzájomnej spolupráci rešpektujú dohodnuté pravidlá používania gridovej infraštruktúry. Hlavnou motiváciou vývoja ad hoc gridovej technológie je jej schopnosť podpory krátkodobých a sporadických kolaborácií. Ak by skupina jednotlivcov chcela vzájomne



Obrázok č. 3: Topológia ad hoc gridovej infraštruktúry [3]

zdieľať prostriedky a vykonávať na týchto prostriedkoch krátkodobé výpočtové úlohy, tak nadbytočná réžia vyplývajúca zo zriadenia tradičnej gridovej infraštruktúry nie je praktická pre tento typ spolupráce. Zároveň nie je ani možné delegovať správu zdieľaných prostriedkov na jednu administratívnu autoritu tak ako je to v prípade tradičnej gridovej infraštruktúry.

Ad hoc gridová infraštruktúra zlučuje geograficky rozptýlené zdieľané prostriedky s rôznymi pravidlami prístupu definovanými vlastníkmi týchto prostriedkov. Toto platí aj o tradičnej gridovej infraštruktúre, ale v prípade ad hoc gridovej infraštruktúry absentuje centralizovaná prístupová kontrola. Ad hoc grid je možné definovať nasledovne: *distribuovaná výpočtová architektúra poskytujúca gridové riešenia podporujúce krátkodobé a sporadické kolaborácie, pričom tieto riešenia sa vyznačujú štrukturálnou, technologickou a riadiacou nezávislosťou*. Štrukturálna nezávislosť ad hoc gridovej infraštruktúry poskytuje niekoľko výhod. Umožňuje vyvarovať sa stavu, kedy zlyhanie jedného funkčného prvku vedie k zlyhaniu celého systému. Taktiež umožňuje členom gridovej komunity začať vzájomnú spoluprácu bez potreby riadenia ich spolupráce externou autoritou. Technologická nezávislosť ad hoc gridovej infraštruktúry zodpovedá schopnosti infraštruktúry integrovať rôznorodé gridové technológie a protokoly. Nezávislosť v oblasti riadenia zodpovedá schopnosti ad hoc gridovej infraštruktúry podporovať bezpečnú kolaboráciu medzi účastníkmi gridovej komunity bez prítomnosti centralizovanej administratívnej autority.

Vykonávanie výpočtov prostredníctvom ad hoc gridovej infraštruktúry nepredstavuje iba jednoduché P2P počítanie, ale obsahuje aj integráciu ad hoc paradigiem. Táto skutočnosť je viditeľná napríklad v OurGrid infraštruktúre, ktorá sa zameriava viac na ad hoc charakter gridovej infraštruktúry ako na mobilitu zariadení pripojených do infraštruktúry. Pre ad hoc grid technológiu nevznikli žiadne štandardy, ktoré by presne špecifikovali jej architektúru. Implementácia jednotlivých funkčných prvkov jednotlivými ad hoc gridovými

infraštruktúrami sa môže výrazne líšiť. Všetky dnešné ad hoc gridové infraštruktúry sú schopné vykonať používateľské úlohy nezávisle od nejakej externej infraštruktúry alebo externých služieb. Idea nezávislého vykonávania úloh uzlami ad hoc gridovej infraštruktúry je implementovaná napríklad v OurGrid infraštruktúre zobrazenej na obrázku č. 3.

Ad hoc grid technológia vznikla relatívne nedávno. Existujúce gridové infraštruktúry implementujú v dostatočnej miere zatiaľ len niektoré základné funkčné prvky ako vyhľadávanie a alokovanie zdieľaných prostriedkov, riadenie vykonávania úloh a poskytovanie informácii o vykonávaných úlohách a zdieľaných prostriedkoch. Zvyšné funkčné prvky stále čakajú na plnohodnotnú implementáciu.

3.2.3 Porovnanie tradičného a ad hoc gridu

Tradičná gridová infraštruktúra je už značný čas používaná najmä pre účely vysoko výkonného počítania a dlhotrvajúce kolaborácie. Ad hoc gridová infraštruktúra vznikla začiatkom tohto milénia a postupne sa začína presadzovať ako nástroj pre podporu krátkodobých a sporadických kolaborácií. Základné funkčné prvky ako správa zdieľaných prostriedkov, plánovanie a správa vykonávania úloh sú ad hoc gridovými infraštruktúrami implementované. Chýba im však plnohodnotná implementácia iných základných funkčných prvkov ako je napríklad podpora bezpečného vykonávania úloh. Táto skutočnosť aktuálne bráni prijatiu a akceptácii ad hoc gridovej technológie vo väčšej miere.

V rámci tradičnej gridovej infraštruktúry je proces plánovania úloh zodpovedný za priradenie úloh na dostupné zdieľané prostriedky. Proces plánovania úloh získava informácie o dostupnosti prostriedkov a o iných charakteristikách týchto prostriedkov prostredníctvom centralizovaného informačného systému. Podobne, gridové služby zabezpečujúce bezpečné vykonávanie úloh zdieľanými prostriedkami sú podporované dôveryhodnou treťou stranou, ktorá slúži ako prostredník medzi spolupracujúcimi entitami. Plánovanie úloh a zaistenie bezpečnej spolupráce medzi kolaborujúcimi entitami je v ad hoc

Charakteristika	**Typ gridovej infraštruktúry**	
	Tradičný	Ad hoc
Štandardy	Neoficiálna množina štandardov a odporúčaní zhrnutá v OGSA štandarde.	Žiadne štandardy a ani odporúčania.
Štruktúra gridovej infraštruktúry	Štrukturálna decentralizácia spôsobená dynamickým vstupovaním a vystupovaním organizácii do a z virtuálnej organizácie a funkčná centralizácia zodpovedajúca centralizovanému spôsobu poskytovania a organizácie gridových služieb.	Úplná decentralizácia. Služby sú poskytované decentralizovane a jednotlivé uzly sú sami zodpovedné za svoje aktivity.
Typ zdieľaných prostriedkov	HPC počítače, meracie zariadenia a senzory.	Osobné počítače a mobilné zariadenia (ale i HPC počítače)
Cieľ účastníkov gridovej komunity	Jeden spoločný cieľ zdieľaný všetkými účastníkmi.	Účastníci sú zameraní na dosiahnutie svojich vlastných cieľov.
Použitie gridovej infraštruktúry	Vysoko výkonné počítanie a dlhodobé kolaborácie.	Krátkodobé a sporadické kolaborácie.
Implementácia základných gridových funkcií	Dnešné tradičné gridové infraštruktúry zabezpečujú všetky základné funkcie definované OGSA štandardom.	Podpora vykonávania používateľských úloh je zabezpečená prostredníctvom funkcií ako alokácia prostriedkov, plánovanie úloh, poskytovanie informácií o dostupných prostriedkoch a vykonávaných úlohách. Iné základné funkcie (napr. poskytovanie bezpečnosti) nie sú ešte plnohodnotne implementované.

Tabuľka č. 1: Porovnanie tradičnej a ad hoc gridovej infraštruktúry

gridovej infraštruktúre zabezpečované samotnými kolaborujúcimi entitami bez podpory tretej strany.

Tradičná a ad hoc gridová infraštruktúra jednoznačne zdieľajú veľa spoločných charakteristických znakov čo sa týka spôsobu vykonávania úloh na zdieľaných prostriedkoch. Vzájomne sa však odlišujú v architektúre a implementácii poskytovaných služieb, type zdieľaných prostriedkov, atď. Najvýznamnejšie charakteristické črty, v ktorých sa tieto dve infraštruktúry odlišujú, sú uvedené v tabuľke č. 1.

3.3 Definícia riešeného problému

Veľký dôraz pri spolupráci sprostredkovanej gridovou infraštruktúrou sa kladie na bezpečnosť. Tradičné gridové infraštruktúry majú túto problematiku dobre zanalyzovanú a zaisťujú bezpečnosť v adekvátnej miere tak ako je to možno vidieť v sekcii 3.4.1.1. Ad hoc gridová infraštruktúra zatiaľ neposkytuje bezpečnosť v takej miere, ako si prípadní používatelia vyžadujú. Riešením tohto problému nie je ani integrácia existujúcich bezpečnostných infraštruktúr, ktoré sú súčasťou tradičných gridových infraštruktúr. Integráciu neumožňuje decentralizácia architektúry ad hoc gridovej infraštruktúry a nezávislosť gridových uzlov od centralizovanej kontroly riadenia. Avšak najväčším nedostatkom stávajúcich bezpečnostných infraštruktúr je ich neschopnosť pokryť všetky bezpečnostné potreby spolupracujúcich entít tak ako je to možno vidieť v sekcii 3.4.1.2.

V poslednom období sa čoraz častejšie používa dôvera a riadenie dôvery ako prostriedok umožňujúci lepšie poskytovanie bezpečnosti. Začlenenie dôvery a riadenia dôvery do riadenia vykonávania úloh si vyžaduje splnenie nasledovných požiadaviek: *(i)* určiť parametre slúžiace na odvodenie hodnoty dôvery, *(ii)* stanoviť spôsob výpočtu a odvodenia hodnoty dôvery z nameraných hodnôt parametrov *(iii)* a vykonávať rozhodovanie o vykonaní kolaborácie na základe dôveryhodnosti používateľa v poskytovateľa prostried-

kov a dôveryhodnosti poskytovateľa prostriedkov v používateľa. Tejto problematike sa venovalo už viacero odborníkov, ktorí navrhli matematické modely integrujúce dôveru a riadenie dôvery ako prostriedok lepšieho zaistenia bezpečnosti (prehľad modelov sa nachádza v sekcii 3.4.2). Riešenia prezentované v týchto modeloch však nespĺňajú všetky menované požiadavky na začlenenie riadenia dôvery do riadenia vykonávania úloh.

3.4 Súčasný stav

Gridová infraštruktúra poskytuje viaceré funkcie a služby, ktoré umožňujú vykonávať používateľské úlohy na zdieľaných prostriedkoch. Medzi poskytovanými funkciami a službami musí existovať vzájomná súhra, aby vykonanie úlohy mohlo prebehnúť úspešne. Popis súčasného stavu sa zameriava v závislosti od stanoveného cieľa popísaného v kapitole 2 a riešeného problému definovaného v sekcii 3.3 najmä na poskytovanie bezpečnosti a plánovanie vykonávania úloh.

3.4.1 Bezpečnosť gridovej infraštruktúry

Účelom každej bezpečnostnej gridovej infraštruktúry je ochrana zdieľaných prostriedkov pred nekalou činnosťou používateľov a ochrana dát proti neautorizovanému prístupu. Medzi bežné bezpečnostné mechanizmy používané za účelom poskytovania bezpečnosti patria proces autentifikácie a proces autorizácie. Požiadavky na bezpečnosť v ad hoc gridovej infraštruktúre sa však líšia od požiadaviek na bezpečnosť v tradičnej gridovej infraštruktúre. Tieto rozdiely sú dôsledkom rozdielnej štruktúry a architektúry oboch infraštruktúr. Spôsob poskytovania bezpečnosti oboma infraštruktúrami, ich spoločné črty, rozdiely a ich porovnanie je bližšie popísané v sekciách 3.4.1.1 - 3.4.1.3.

3.4.1.1 Bezpečnosť tradičnej gridovej infraštruktúry

Dnes už tradičná gridová infraštruktúra bola spočiatku používaná iba malou skupinou používateľov, medzi ktorými existovali nepomenované vzťahy dôvery. Skupina používateľov však postupne narastala a objavila sa potreba zabezpečiť prístup k zdieľaným prostriedkom a dátam ako i potreba zabezpečiť komunikáciu sprostredkovanú gridovou infraštruktúrou. Vývojári tradičnej gridovej infraštruktúry postupom času navrhli a implementovali viacero autentifikačných a autorizačných infraštruktúr ako reakcia na vzniknutú potrebu poskytovania bezpečnosti.

Autentifikačné infraštruktúry. Proces autentifikácie je zameraný na overenie identity entity, t. j. či entita sa prezentuje svojou skutočnou totožnosťou. Pravdepodobne najznámejšou autentifikačnou infraštruktúrou je **Public Key Infrastructure** [19], ktorá je založená na princípe kryptografického šifrovania kľúčov. Dôvera v používateľovu identitu je sprostredkovávaná dôveryhodnou treťou stranou, pričom sa predpokladá existencia vzťahov dôvery medzi treťou stranou, používateľmi a poskytovateľmi zdieľaných prostriedkov. Dôveryhodná tretia strana vystupuje ako mediátor medzi používateľmi a poskytovateľmi prostriedkov a označuje sa ako certifikačná autorita (CA). Úlohou CA je mapovanie používateľovej doménovej identity na identitu v rámci gridovej infraštruktúry. CA taktiež zabezpečuje vydávanie certifikátov používateľovi s priradenou identitou. Tieto certifikáty potom používatelia používajú za účelom prístupu k zdieľaným prostriedkom.

Kerberos [20] je ďalšia infraštruktúra, ktorá je založená na existujúcich vzťahoch dôvery. Úlohu dôveryhodnej tretej strany v rámci tejto infraštruktúry zastáva autentifikačný server (AS). AS ako mediátor medzi používateľmi a poskytovateľmi prostriedkov vykonáva autentifikáciu používateľov. V prípade úspešnej autentifikácie obdrží používateľ špeciálny token, ktorým žiada o pridelenie prístupových práv k zdieľaným prostriedkom alebo službám. Tieto povolenia sú priradené používateľovi formou dočasných kľúčov a

tiketu, ktorý používateľ zasiela spolu zo žiadosťou o prístup k zdieľanému prostriedku alebo poskytovanej službe.

Athens [21] je autentifikačná infraštruktúra, ktorá bola vytvorená za účelom prístupovej kontroly k veľkému množstvu rôznych zdieľaných prostriedkov. Pre prístup k zdieľanému prostriedku musí mať používateľ vytvorený svoj používateľský účet. Takýto účet musí mať používateľ pre každý zdieľaný prostriedok zvlášť. Používateľské účty sú spravované prostredníctvom servera používateľských účtov (AS). Každý uzol, ktorý spravuje a poskytuje prostriedky na zdieľanie, má nainštalovaného softvérového agenta zabezpečujúceho dodržiavanie prístupovej kontroly. Používateľ musí poskytnúť svoje používateľské meno a heslo ak chce získať prístup k prostriedku. Tento postup používateľ opakuje vždy, keď chce získať prístup k nejakému dostupnému prostriedku. Možnosť jednorázového prihlásenia nie je infraštruktúrou podporovaná.

Autorizačné infraštruktúry. S narastajúcou popularitou tradičnej gridovej infraštruktúry a rastúcim počtom členov gridovej komunity vznikla potreba kontrolovať prístup k zdieľaným prostriedkom aj na základe ďalších pravidiel. Kontrola prístupu založená na kontrole používateľskej identity už nebola dostačujúca. Pre lepšiu prístupovú kontrolu bol vytvorený proces autorizácie, ktorý určuje komu je umožnené získať prístup k prostriedkom a za akých podmienok. **Grid-Map Files** (GMF) [22] bola prvá autorizačná infraštruktúra, ktorá bola v gridovej infraštruktúre použitá. GMF je založená na princípe kontroly prístupu prostredníctvom zoznamu prístupových práv (ACL). ACL je spravovaný každým zdieľaným prostriedkom, ktorý je súčasťou gridovej infraštruktúry. Zoznam obsahuje jedinečné mená gridových používateľov a ich používateľské účty, ktoré sú im priradené v rámci lokálnych domén zdieľaných prostriedkov. Prístupová kontrola zodpovedajúca lokálnemu používateľskému účtu je potom prenechaná lokálnemu operačnému systému zdieľaného prostriedka. Tento spôsob autorizácie bol veľmi rýchlo prijatý

gridovou komunitou vďaka jednoduchosti jeho implementácie.

Virtual Organization Membership Service (VOMS) [23] spravuje informácie o prístupových právach používateľov na úrovni virtuálnych organizácií. Všetky potrebné informácie o používateľoch sú udržiavané centralizovane na VOMS serveri. Používateľ musí najskôr obdržať z VOMS servera informácie o jeho atribútoch a až potom môže požiadať o prístup k zdieľaným prostriedkom. Používateľ obdrží informácie o jeho atribútoch vo forme atribútového certifikátu. Pri žiadosti o prístup k prostriedku predloží používateľ tento certifikát. Lokálna prístupová kontrola implementovaná zdieľaným prostriedkom vyhodnotí atribúty obsiahnuté v tomto certifikáte a umožní prístup k zdieľanému prostriedku alebo prístup zamietne.

Akenti [24] používa digitálne certifikáty, ktoré sú schopné prenášať identitu používateľa, požiadavky na použitie zdieľaných zdrojov, atribútové certifikáty a informácie potrebné pre delegáciu autorizácie. V Akenti je prístupová kontrola distribuovaná a skladá sa z dvoch častí: certifikát podmienok použitia a certifikát prístupovej politiky. Certifikát podmienok použitia kladie požiadavky na atribútové certifikáty, ktoré používateľ musí mať pre získanie prístupu k zdieľanému prostriedku. Tieto certifikáty majú právo vydávať dôveryhodné tretie strany a to nezávisle jedna od druhej. Jeden zdieľaný prostriedok tak môže mať priradených hneď niekoľko certifikátov podmienok použitia. Certifikát prístupovej politiky kladie nároky na celkovú prístupovú kontrolu k zdieľanému prostriedku.

PrivilEdge and Role Management Infrastructure Standard (PERMIS) [25] je ďalší typ autorizačnej infraštruktúry. Ak chce používateľ získať prístup k zdieľanému prostriedku chráneného PERMIS infraštruktúrou, tak najskôr musí obdržať svoj atribútový certifikát a zoznam priradených rôl. Certifikáty sú schopné vydávať dôveryhodné tretie strany pomenované ako zdroje autority. PERMIS umožňuje distribuovanú správu rôl a atribútov. Vydané certifikáty totiž môžu byť uložené a spravované autoritami, ktoré

ich vydali. Predtým ako je vykonané rozhodnutie o povolení alebo zakázaní prístupu používateľa k zdieľanému prostriedku, tak lokálna prístupová kontrola implementovaná zdieľaným prostriedkom skontroluje používateľove roly, atribúty a či certifikát bol vydaný dôveryhodným zdrojom autority.

3.4.1.2 Bezpečnosť ad hoc gridovej infraštruktúry

Poskytovanie bezpečnosti v rámci gridovej infraštruktúry je bežne zamerané na ochranu zdieľaných prostriedkov pred nekalou činnosťou zo strany používateľov. Bezpečnosť sa taktiež zameriava na ochranu prostriedkov pred inými entitami schopnými poškodiť tieto prostriedky alebo znehodnotiť integritu dát uložených na týchto prostriedkoch. Takáto bezpečnosť sa uplatňuje najmä v prostredí tradičných gridových infraštruktúr, ktoré za účelom poskytovania bezpečnosti integrujú proces autentifikácie a autorizácie. Existujú však situácie, kedy je v prostredí ad hoc gridovej infraštruktúry potrebné chrániť používateľov pred poskytovateľmi zdieľaných prostriedkov alebo služieb [8]. Bezpečnostné infraštruktúry popísané v sekcii 3.4.1.1 však nedokážu poskytovať tento druh ochrany.

Proces autentifikácie a proces autorizácie (často označované aj ako tvrdé bezpečnostné mechanizmy) nepovoľujú žiadny výskyt rizika a neistoty v procese prístupovej kontroly, t. j. používateľ buď je autentifikovaný a autorizovaný, alebo nie je. Avšak kolaborácia sprostredkovávaná prostredníctvom ľubovoľného distribuovaného systému je nevyhnutne spätá aj s potencionálnym nebezpečenstvom, ktoré si vyžaduje začlenenie rizika a neistoty do procesu prístupovej kontroly. Dôvera je v súčasnej dobe uznávaná ako dôležitý prvok rozhodovacieho procesu v mnohých distribuovaných systémoch. V týchto systémoch je dôvera používaná ako mechanizmus pre vedomé narábanie s potencionálnym nebezpečenstvom a ako mechanizmus pre učenie sa z minulých kolaborácií. Dôvera teda umožňuje vystavovať sa riziku v oveľa menšej miere.

Systémy reputácie podporujú vykonávanie rozhodnutí o dôveryhodnosti poskytovateľov služieb v prostredí internetu na základe hodnotení, ktoré používatelia zanechávajú po ukončení poskytovania služby. Iní používatelia môžu použiť takto nahromadené hodnotenie a reputáciu pre vlastné účely rozhodovania o dôveryhodnosti poskytovateľov služieb. Riadenie dôvery predstavuje v kontexte distribuovaných systémov (a teda i v kontexte ad hoc gridových infraštruktúr) snahu o zmenu absolútnej ochrany pred potenciálnym nebezpečenstvom na akceptovanie nebezpečenstva ako neoddeliteľnej súčasti každého globálneho počítania [7, 15]. Techniky a postupy integrovania riadenia dôvery do bezpečnostnej infraštruktúry ad hoc gridovej infraštruktúry sú bližšie popísané v sekcii 3.4.2.

3.4.1.3 Porovnanie bezpečnosti tradičnej a ad hoc gridovej infraštruktúry

Bezpečnostné infraštruktúry tradičných gridových infraštruktúr implicitne integrujú dôveru ako súčasť rozhodovania o uskutočnení kolaborácie. Z tried dôvery implementujú tieto infraštruktúry dôveru v identitu, prístupovú kontrolu a dôveru pri delegovaní vo forme procesu autentifikácie, autorizácie a delegovaním prístupových práv medzi jednotlivými entitami. Explicitná implementácia dôvery v poskytované služby a kontext chýba. Čestné správanie používateľov a poskytovateľov zdieľaných prostriedkov je sprostredkovávané prostredníctvom dôveryhodnej tretej strany. Dôveryhodná tretia strana nemá ale žiadne donucovacie mechanizmy, ktorými by čestné správanie poskytovateľov prostriedkov dokázala vynútiť.

V rámci tradičnej gridovej infraštruktúry je dôvera naviazaná na samotné zostavenie tejto infraštruktúry a je vnímaná ako implicitná súčasť kolaborácií. V ad hoc gridovej infraštruktúre žiadne takéto implicitné vzťahy dôvery medzi jednotlivými entitami neexistujú. V budúcnosti by sa riadenie dôvery mohlo stať mechanizmom umožňujúcim vykonávanie kolaborácií v prítomnosti vzájomnej dôvery medzi spolupracujúcimi entitami.

Charakteristika	**Typ gridovej infraštruktúry**	
	Tradičný	Ad hoc
Účel bezpečnostnej infraštruktúry	Ochrana zdieľaných prostriedkov a dát proti neautorizovanému prístupu.	Ochrana zdieľaných prostriedkov pred nekalou činnosťou zo strany používateľov a ochrana používateľov pred nekalou činnosťou zo strany poskytovateľov.
Predpoklady pre poskytovanie bezpečnostných služieb	Autentifikácia používateľa, bezpečná komunikácia a prenos dát založený na rôznych kryptografických metódach.	Autentifikácia kolaborujúcich entít, bezpečná komunikácia a prenos dát založený na rôznych kryptografických metódach.
Spôsob poskytovania bezpečnostných služieb	Poskytovanie bezpečnosti je založené na procese autentifikácie a procese autorizácie.	Poskytovanie bezpečnosti je založené na riadení dôvery.
Integrácia dôvery	Implicitné a nepomenované vzťahy dôvery medzi členmi gridovej komunity sprostredkovávané dôveryhodnou treťou stranou.	Explicitné vzťahy dôvery medzi účastníkmi gridovej komunity spravované každým účastníkom samostatne.
Implementácia tried dôvery	Dôvera v identitu ako autentifikácia, dôvera v prístupovú kontrolu ako autorizácia a dôvera pri delegovaní ako delegovanie prístupových práv medzi entitami.	Obojstranný vzťah dôvery medzi kolaborujúcimi entitami vyžaduje implementáciu všetkých tried dôvery.

Tabuľka č. 2: Porovnanie charakteristík poskytovania bezpečnosti v tradičných a ad hoc gridových infraštruktúrach

Poskytovanie bezpečnosti v tradičnej a ad hoc gridovej infraštruktúre má niekoľko spoločných znakov. Napríklad, v oboch infraštruktúrach je autentifikácia entitít nevyhnutným predpokladom pre poskytovanie ostatných služieb v oblasti bezpečnosti. Poskytovanie bezpečnosti v oboch infraštruktúrach sa pochopiteľne aj odlišuje z dôvodu rozdielov v architektúre infraštruktúr a rozdielnych požiadaviek členov gridovej komunity kladených na bezpečnosť. Najvýznamnejšie charakteristické črty, v ktorých sa poskytovanie bezpečnosti v gridových infraštruktúrach odlišuje, sú uvedené v tabuľke č. 2.

3.4.2 Popis modelov integrujúcich dôveru

Jeden z prvých modelov, ktoré integrujú riadenie dôvery ako súčasť gridového počítania, navrhli Azzedin a Maheswaran [12]. Autori vo svojom modeli delia dôveru do dvoch zložiek: dôvera v identitu (zodpovedá procesu autentifikácie a procesu autorizácie) a dôvera v správanie sa entity (zodpovedá pozorovanému správaniu sa entít počas viacerých kolaborácií). Výpočet hodnoty dôvery a jej aktualizácia (operácie vyplývajúce z riadenia dôvery) sú v modeli vykonávané len pre dôveru v správanie sa entity. Pre účely riadenia dôvery nie je dôvera v identitu zohľadnená. Model vynecháva z procesu riadenia dôvery aj riziko a neistotu. Hlavným prínosom modelu je určenie dôvery medzi kolaborujúcimi entitami ako obojstranného vzťahu, t. j. dôvera jednej entity v druhú entitu je odlišná od dôvery druhej entity v prvú entitu. Pokiaľ sa teda obe entity navzájom nevnímajú ako dôveryhodné entity, tak kolaborácia medzi entitami nie je uskutočnená.

Song et al. [10, 11] navrhli model dôvery, ktorý určuje dôveryhodnosť entity na základe jej schopnosti ochrany pred nepovoleným prístupom a na základe jej reputácie odvodenej od správania sa danej entity počas viacerých kolaborácií. Odvodená hodnota dôvery sa v modeli označuje ako index dôvery (Trust Index - TI). Autori v modeli definujú aj hodnotu požiadaviek používateľa na poskytovanie bezpečnosti poskytovateľmi zdieľaných prostriedkov (Security Demand - SD). Tieto požiadavky sa môžu vyskytovať

Model dôvery	**Charakteristika**				
	Dôvera	Riziko	Neistota	Vzťah dôvery	Inicializačná dôvera
Azzedin a Maheswaran [12]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií.	Bez integrácie rizika.	Bez integrácie neistoty.	Obojstranný vzťah dôvery, t. j. dôvera jednej enity v druhú entitu sa líši od dôvery druhej entity v prvú entitu.	Bez integrácie inicializačnej dôvery.
Song et al. [10, 11]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií a systémových charakteristík entity.	Bez integrácie rizika.	Neistota integrovaná len implicitne prostredníctvom fuzzy logiky.	Dôvera je určovaná iba z pohľadu používateľa.	Bez integrácie inicializačnej dôvery.
Lin et al. [26]	Dôvera určená na základe spoľahlivosti a kompetencie používateľa a poskytovateľa prostriedkov.	Bez integrácie rizika.	Neistota integrovaná ako doplnok pre presvedčenie a pochybnosť o dôveryhodnosti hodnotenej entity.	Obojstranný vzťah dôvery.	Bez integrácie inicializačnej dôvery.
Shi et al. [9]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií a odporúčaní iných entít.	Bez integrácie rizika.	Neistota integrovaná len implicitne ako súčasť inicializačnej dôvery v prípade kolaborácie s neznámou entitou.	Obojstranný vzťah dôvery.	Inicializačná dôvera integrovaná a určuje do akej miery je entita schopná dôverovať neznámej entite.

Model dôvery	**Charakteristika**				
	Dôvera	Riziko	Neistota	Vzťah dôvery	Inicializačná dôvera
Papalilo a Freisleben [27]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií.	Bez integrácie rizika.	Bez integrácie neistoty.	Obojstranný vzťah dôvery.	Bez integrácie inicializačnej dôvery.
Kavitha a Sankaranarayanan [28]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií, systémových charakteristík entity a spôsobu určovania identity entity.	Bez integrácie rizika.	Bez integrácie neistoty.	Dôvera je určovaná iba z pohľadu používateľa.	Bez integrácie inicializačnej dôvery.
Kaur a Sen-Gupta [29]	Dôvera určená na základe správania sa entity počas predošlých kolaborácií a charakteristík potencionálnej kolaborácie.	Bez integrácie rizika.	Bez integrácie neistoty.	Dôvera je určovaná iba z pohľadu používateľa.	Bez integrácie inicializačnej dôvery.
Kumar a Ramachandram [30]	Dôvera určená na základe dostupnosti a spoľahlivosti poskytovateľa prostriedkov a odporúčaní iných entít.	Bez integrácie rizika.	Neistota integrovaná len implicitne prostredníctvom fuzzy logiky.	Dôvera je určovaná iba z pohľadu používateľa.	Bez integrácie inicializačnej dôvery (v modeli je považovaná za nepotrebnú).

Tabuľka č. 3: Porovnanie modelov dôvery integrujúcich riadenie dôvery

vo forme požiadaviek na autentifikáciu, bezpečnú komunikáciu, prístupovú kontrolu, atď. Pre vykonanie úloh na zdieľanom prostriedku musí byť splnená podmienka $SD \leq TI$, t. j. požiadavky používateľa na poskytovanie bezpečnosti sú menšie alebo rovné dôveryhodnosti poskytovateľa zdieľaného prostriedku. TI priradený poskytovateľovi prostriedkov je určený na základe jeho správania sa počas viacerých kolaborácií a na základe systémových charakteristík zdieľaných prostriedkov. Ani v tomto modeli nie je riziko a neistota zohľadnená ako súčasť hodnoty dôvery. Najväčším nedostatkom tohto modelu je určovanie vzťahu dôvery iba z pohľadu používateľov. Poskytovatelia zdieľaných prostriedkov nemajú žiadnu modelom definovanú možnosť ako rozhodovať o uskutočnení alebo neuskutočnení kolaborácie na základe dôvery v používateľov.

Lit et al. [26] navrhli model, ktorý definuje neistotu ako explicitnú súčasť hodnoty dôvery. Hodnota dôvery v entitu je určená ako kombinácia presvedčenia a súčasne pochybnosti v dôveryhodnosť hodnotenej entity. Neistota je v modeli požitá na vyplnenie priestoru medzi presvedčením a pochybnosťami. Dôveryhodnosť entity sa určuje z pohľadu používateľov ako i z pohľadu poskytovateľov zdieľaných prostriedkov. Autori v modeli taktiež definujú, že používatelia a poskytovatelia majú určenú dôveryhodnosť odlišne. Používatelia vnímajú dôveryhodnosť poskytovateľov prostriedkov prostredníctvom ich schopnosti zodpovedne alokovať zdieľané prostriedky a umožniť tak úspešné vykonanie používateľovej úlohy. Poskytovatelia vnímajú dôveryhodnosť používateľov prostredníctvom ich schopnosti vytvárať vykonávateľný program nepoškodzujúci zdieľané prostriedky počas jeho vykonávania.

Model navrhnutý autormi Shi et al. [9] obsahuje niekoľko inovatívnych prvkov, ktoré v predošlých modeloch neboli zohľadnené. Dôveryhodnosť entity, ktorá je v modeli určená na základe priamej dôvery a reputácie, je ovplyvnená aj kontextom kolaborácie pred jej vykonaním, t. j. autori modelujú dôveryhodnosť ako kontextovo závislú dôveru. Ďalšia novota modelu je stanovenie inicializačnej dôvery medzi entitami, ktorá definuje

do akej miery je kolaborujúca entita ochotná dôverovať neznámym entitám. Inicializačná dôvera je určená na základe všetkých skúseností entity s inými entitami a vo všetkých situáciách. Napriek viacerým novotám má tento model aj niekoľko nedostatkov. Autori vynechávajú integráciu rizika ako súčasti hodnoty dôvery a neistota je použitá v modeli len nepriamo ako súčasť inicializačnej dôvery.

Papalilo a Freisleben [27] navrhli model definujúci vzťahy dôvery z pohľadu používateľov ako i poskytovateľov zdieľaných prostriedkov. Priama dôvera medzi entitami je v modeli určená na základe presvedčenia dôverujúcej entity v korektné správanie sa druhej entity. Dôvera v správanie sa kolaborujúcej entity je určená prostredníctvom rôznych parametrov odvodených od požiadaviek na poskytovanie bezpečnosti a kvality samotnej kolaborácie. Tieto parametre je možné merať buď priamo, alebo je možné ich rozčleniť na merateľné prvky. Hlavným prínosom modelu je vylúčenie nekorektne sa správajúcich účastníkov kolaborácie z budúcich ale i aktuálne prebiehajúcich kolaborácií. Medzi nedostatky modelu patrí vynechanie rizika a neistoty ako súčasti modelovanej hodnoty dôvery. Model taktiež neponúka žiadny postup určenia dôvery medzi entitami, ktoré vzájomne ešte nikdy nespolupracovali.

V poslednom období vzniklo viacero modelov [31, 28, 29, 30], ktoré určujú hodnotu dôvery na základe pozorovaného správania sa entity, charakteristík popisujúcich spôsob vykonávania autorizácie a autentifikácie, schopnosti entity chrániť sa proti nepovolenému prístupu, atď. Správne určenie hodnoty dôvery je však závislé aj od integrácie rizika, neistoty, inicializačnej dôvery, odporúčaní ako i ďalších zložiek hodnoty dôvery. Prehľad vyššie popísaných modelov, ich charakteristík a významných čŕt je zobrazený v tabuľke č. 3.

Integrácia riadenia dôvery do ad hoc gridovej infraštruktúry umožňuje určovať dôveryhodnosť spolupracujúcich účastníkov kolaborácie a vykonávať rozhodnutia o uskutočnení alebo neuskutočnení kolaborácie. Modely popísané v tejto sekcii určujú hodnotu

dôvery na základe systémových vlastností, pozorovaných formách správania sa, rizika a neistoty. Existujú však i iné postupy určovania dôveryhodnosti účastníkov kolaborácie. Huraj et al. [32] definujú mechanizmus, ktorý umožňuje vytvorenie vzťahu dôvery medzi poskytovateľom zdieľaných prostriedkov a používateľom na základe prieniku virtuálnych organizácií. Mechanizmus je vhodný na použitie najmä v prípade zlyhania ostatných mechanizmov autorizácie. Hodnota dôveryhodnosti používateľa sa určuje na základe dôveryhodnosti virtuálnych organizácií používateľa. Dôveryhodnosť virtuálnych organizácií sa buduje prostredníctvom existujúcich autorizačných informácií o členoch týchto organizácií. Používateľ sa stáva dôveryhodný z pohľadu poskytovateľa zdieľaných prostriedkov vtedy, ak členovia používateľových virtuálnych organizácií sú zároveň aj členmi virtuálnych organizácií poskytovateľa prostriedkov. Ďalšie mechanizmy zaoberajúce sa problematikou autorizácie v prostredí ad hoc gridovej infraštruktúry navrhli Kerschbaum et al. [33] a Zhao et al [34].

3.4.3 Plánovanie úloh

Proces plánovania vykonávania úloh na zdieľaných prostriedkoch v gridových infraštruktúrach je možné definovať ako proces priraďovania používateľských úloh na jednotlivé zdieľané prostriedky rozptýlené vo viacerých administratívnych doménach. Plánovanie úloh sa na základe architektúry jeho vykonávania delí na tri typy [35]: *(i)* centralizované plánovanie, *(ii)* decentralizované plánovanie *(iii)* a hybridné plánovanie.

Architektúra **centralizovaného plánovania** vykonávania úloh je založená na jednom centrálnom kontrolnom prvku, ktorý je zodpovedný za vykonávanie a riadenie plánovania. Prostriedky zdieľané v rámci gridovej infraštruktúry musia informovať tento centrálny kontrolný prvok o ich nemenných vlastnostiach a aktuálnom stave ich systému. Hlavným nedostatkom tejto architektúry je existencia jedného miesta zlyhania, ktoré predstavuje centralizovaný kontrolný prvok. Nedostatkom architektúry sú aj problémy

so škálovateľnosťou systému, ktoré sú dôsledkom veľkého množstva zdieľaných prostriedkov. Architektúra **decentralizovaného plánovania** úloh prenecháva zodpovednosť za plánovanie úloh na jednotlivé uzly gridovej infraštruktúry. Každý uzol však musí obsahovať na tento účel stanovený modul, ktorý rozhoduje o priradení používateľskej úlohy na konkrétny zdieľaný prostriedok. Architektúra **hybridného plánovania** kombinuje techniky centralizovaného a decentralizovaného plánovania. V rámci tejto architektúry jeden modul vykonávajúci plánovanie spravuje viacero zaregistrovaných uzlov. Tento modul komunikuje s ďalšími modulmi vykonávajúcich plánovanie úloh, ktoré spravujú vlastné registrované uzly. Ak takýto modul nedokáže naplánovať používateľskú úlohu v rámci lokálne spravovaných uzlov, tak deleguje používateľskú úlohu spolupracujúcim modulom plánovania.

Integrácia riadenia dôvery do tradičnej a ad hoc gridovej infraštruktúry si vyžaduje spoluprácu služieb poskytujúcich gridovú bezpečnosť a služieb zaoberajúcich sa plánovaním vykonávania používateľských úloh. Služby poskytovania bezpečnosti sú zodpovedné za identifikáciu dôveryhodnosti entít a proces plánovania úloh je zodpovedný za vytvorenie plánu vykonávania úloh na dôveryhodných zdieľaných prostriedkoch. Popis procesu plánovania a spôsob integrácie riadenia dôvery do tohto procesu je bližšie popísaný v sekciách 3.4.3.1 a 3.4.3.2.

3.4.3.1 Plánovanie úloh v tradičnej gridovej infraštruktúre

V tradičnej gridovej infraštruktúre je plánovanie úloh bežne vykonávané jedným gridovým modulom plánovania úloh a viacerými lokálnymi modulmi plánovania úloh. Gridový a lokálny modul plánovania sa líšia v tom, že gridový modul plánovania nemá žiadnu priamu kontrolu nad zdieľanými prostriedkami. Tento modul vyžaduje spoluprácu vzdialených uzlov a ich lokálnych modulov plánovania úloh. Gridový modul plánovania deleguje požiadavky na vykonanie plánovacieho procesu modulom na hierarchicky nižšej úrovni.

Tieto moduly buď majú už priamu kontrolu nad zdieľanými prostriedkami, alebo majú nejakú inú možnosť prístupu k prostriedkom. Koncept gridového plánovania úloh sa neohraničuje iba na dve úrovne. Moduly plánovania na nižšej úrovni totiž môžu byť reprezentované buď lokálnymi modulmi plánovania s prístupom k prostriedkom, alebo sú reprezentované systémovými modulmi plánovania spolupracujúcimi s viacerými lokálnymi modulmi plánovania.

Proces plánovania úlohy je vykonávaný v troch fázach [36]: *(i)* vyhľadávanie zdieľaných prostriedkov, *(ii)* voľba systému *(iii)* a vykonanie úlohy. **Vyhľadávanie zdieľaných prostriedkov** zisťuje dostupnosť týchto prostriedkov a vytvára množinu prostriedkov spĺňajúcich minimálne požiadavky na vykonanie úlohy. Fáza **voľby systému** zabezpečuje výber konkrétneho zdieľaného prostriedka z množiny dostupných prostriedkov. Fáza **vykonania úlohy** je zodpovedná za predanie úlohy zvolenému prostriedku a spustenie vykonávania samotnej úlohy.

I keď v súčasnej dobe neexistuje ešte žiadny generický gridový modul plánovania, tak je možné nájsť niekoľko spoločných aspektov plánovania rozborom známych scenárov vykonávania plánovania [37]. Na základe spoločných aspektov je možné rozdeliť fázy plánovania úlohy do nasledovných krokov [36, 38]:

1. **Filtrovanie na základe autorizácie** zodpovedá faktu, že nemá zmysel naplánovať vykonanie úlohy na neautorizovaný zdieľaný prostriedok. Tento krok je zodpovedný na vyhľadanie takých prostriedkov, ktoré je používateľ oprávnený používať.
2. **Definovanie požiadaviek** je zodpovedné za vytvorenie definície minimálnych požiadaviek na vykonanie používateľskej úlohy. Definícia môže obsahovať nemenné vlastnosti zdieľaných prostriedkov (napr. typ operačného systému) ako i dynamicky sa meniace vlastnosti (napr. veľkosť dostupnej RAM pamäte). Vo všeobecnosti platí, že čím viac požiadaviek definícia obsahuje, tým lepší bude výber prostriedkov.
3. **Filtrovanie na základe definície požiadaviek** vykonáva ďalšiu selekciu takých

zdieľaných prostriedkov, ktoré spĺňajú minimálne požiadavky na vykonanie úlohy.

4. **Zber dynamických informácií** zabezpečuje obdržanie detailných informácií o zdieľaných prostriedkoch za účelom čo najlepšieho priradenia používateľskej úlohy na zdieľaný prostriedok.
5. **Voľba systému** vykonáva výber zdieľaného prostriedka, na ktorom bude naplánované vykonanie úlohy. Výber prostriedka zahŕňa vytvorenie plánu optimalizujúceho čas vykonania úlohy alebo iné kritérium zodpovedajúce používateľovým požiadavkám.
6. **Predbežná rezervácia** je voliteľný krok a jeho účelom je (ak to zdieľaný prostriedok umožňuje) rezervovať si istý časový interval na danom prostriedku, počas ktorého úloha bude vykonaná. Keď nastane čas vykonania úlohy, tak zdieľaný prostriedok je vyžiadaný pre rezervované vykonanie úlohy.
7. **Predloženie úlohy na vykonanie** je proces prenosu používateľovej úlohy na zdieľaný prostriedok spolu so spustiteľným zdrojovým kódom a príslušnými dátami.
8. **Prípravné úlohy** pred spustením používateľskej úlohy predstavujú akcie, ktoré musia byť vykonané pred samotným vykonaním úlohy (napr. vyžiadanie si zdieľaného prostriedka, inštalácia úlohy a dodatočných knižníc, prenos dát, atď.).
9. **Monitorovanie priebehu vykonávania** úlohy je potrebné pre prípad, že nastane jav spôsobujúci prerušenie vykonávania úlohy a opätovné naplánovanie danej úlohy. Monitorovanie je potrebné aj v prípade, že sa používateľ sám rozhodne premiestniť úlohu na iný dostupný prostriedok.
10. **Dokončenie vykonávania úlohy** zodpovedá za informovanie používateľa o ukončení vykonávania úlohy, ktorý si následne môže prevziať výsledky vykonanej úlohy.
11. **Ukončovacie úlohy** slúžia na prenos vypočítaných dát zo zdieľaného prostriedka, odstránenie dočasných nastavení, atď.

3.4.3.2 Plánovanie úloh v ad hoc gridovej infraštruktúre

V sekcii 3.2.2 je ad hoc gridová infraštruktúra definovaná ako distribuovaná výpočtová architektúra vyznačujúca sa štrukturálnou nezávislosťou. Táto nezávislosť umožňuje účastníkom gridovej komunity kolaborovať bez potreby riadenia ich spolupráce externou infraštruktúrou. Centralizovaná architektúra plánovania úloh je preto nevhodná na implementáciu v prostredí ad hoc gridovej infraštruktúry.

Hybridná architektúra plánovania úloh je v ad hoc gridovej infraštruktúre implementovaná ako zoskupenie uzlov začlenených do infraštruktúry formou clusterov [3, 5, 39]. Cluster tvoria buď geograficky vzájomne si blízke uzly [3, 5], alebo uzly patriace do jednej lokálnej siete umožňujúcej im priamo komunikovať prostredníctvom lokálneho riadiaceho uzla [39].

Na rozdiel od centralizovanej a hybridnej architektúry plánovania úloh sú v decentralizovanej architektúre plánovania úloh proces vyhľadávania dostupných zdieľaných prostriedkov a informačné služby implementované samostatne každým uzlom gridovej infraštruktúry [6, 40, 41, 42]. Pre účely plánovania používateľskej úlohy vyžaduje modul plánovania úlohy informácie o dostupných prostriedkoch a o aktuálnom stave ich systému. Ad hoc gridová infraštruktúra MoGrid využíva pre tento účel mechanizmus nazvaný flooding [6, 40]. Uzol hľadajúci dostupné zdieľané prostriedky zasiela správy všetkým susedným uzlom. Uzol prijímajúci takúto správu taktiež propaguje prijatú správu svojim susedom. Tento postup sa opakuje kým nie je dosiahnutá istá maximálna hodnota propagácie. Uzly, ktoré prijali rozposlanú správu, odpovedajú na základe ich ochoty kolaborovať ako poskytovateľ zdieľaného prostriedka. Iný postup vyhľadania dostupného zdieľaného prostriedka v zmysle decentralizovanej architektúry plánovania úloh predstavujú mobilní agenti [41] a zdieľaná virtuálna pamäť [42].

Kapitola 4

Navrhované riešenie

Kolaborácia v ad hoc gridovej infraštruktúre je bežne vykonávaná medzi dvoma typmi entít: používatelia a poskytovatelia zdieľaných prostriedkov. Používatelia a poskytovatelia vyžadujú poskytovanie ochrany zo strany gridovej infraštruktúry voči nekalému správaniu sa kolaborujúcich entít, ktoré môže nadobúdať formu zámerne škodlivého zdrojového kódu obsiahnutého v používateľskej úlohe. Nekalé správanie môže nadobúdať aj formu zdieľaného prostriedka schopného poškodiť vykonávanie používateľskej úlohy alebo schopného alternovať používateľove dáta [26].

Bezpečnostná infraštruktúra integrujúca riadenie dôvery musí byť založená na modeli schopného podporiť a zároveň i vylepšiť vykonávanie funkčných prvkov implementovaných gridovou infraštruktúrou. Model musí byť tiež schopný transformovať formy správania sa entít pozorovaných počas predošlých kolaborácií, relevantné parametre popisujúce schopnosti entít a stav ich systému, riziko, neistotu a ostatné významné zložky dôvery do výslednej hodnoty dôvery. Určenie výslednej hodnoty dôvery musí byť model schopný vykonať z pohľadu používateľa ako i z pohľadu poskytovateľa zdieľaných prostriedkov. Používatelia a aj poskytovatelia prostriedkov môžu potom na základe hodnoty dôvery vykonávať rozhodnutie o uskutočnení potencionálnej kolaborácie. Navrhnutý model spĺňajúci uvedené požiadavky je popísaný v sekcii 4.1. Navrhnutá integrácia ria-

denia dôvery do ad hoc gridovej infraštruktúry založená na určovaní hodnoty dôvery je popísaná v sekcii 4.2.

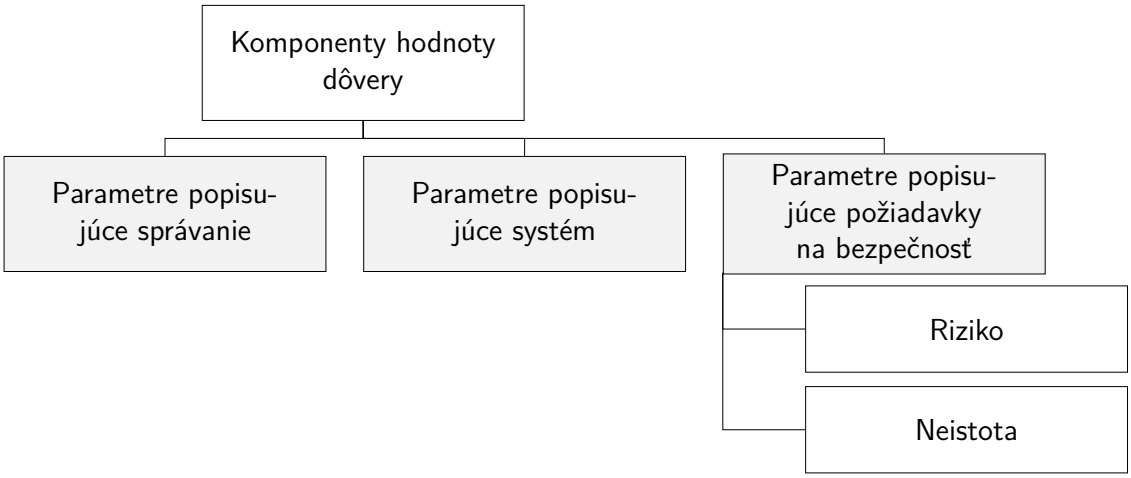
4.1 Model dôvery

Model dôvery transformuje viaceré zložky dôvery do výslednej hodnoty, ktorú používatelia a poskytovatelia zdieľaných prostriedkov využívajú ako prostriedok pre vykonanie rozhodnutia o uskutočnení potencionálnej kolaborácie. Navrhovaný model dôvery definuje v sekcii 4.1.1 klasifikáciu parametrov obsiahnutých vo výslednej hodnote dôvery. Model dôvery tiež popisuje metódu výpočtu výslednej hodnoty dôvery z nameraných hodnôt parametrov v sekcii 4.1.2. Metóda merania parametrov je popísaná v sekcii 4.1.3.

4.1.1 Klasifikácia parametrov

Používatelia a poskytovatelia zdieľaných prostriedkov majú odlišné požiadavky na bezpečnosť poskytovanú gridovou infraštruktúrou. Používatelia vyžadujú od infraštruktúry, aby zabezpečila kompetentné vykonanie úloh na zdieľaných prostriedkoch a ochránila spravované dáta pred nepovoleným prístupom a modifikáciou. Používatelia taktiež vyžadujú, aby infraštruktúra zabezpečila integritu dát uložených na zdieľaných prostriedkoch. Poskytovatelia zdieľaných prostriedkov vyžaduje od infraštruktúry, aby sprostredkovávala úlohy iba od autentifikovaných a autorizovaných používateľov.

Každý účastník kolaborácie sprostredkovanej prostredníctvom ad hoc gridovej infraštruktúry má vlastnú množinu požiadaviek na kvalitu a priebeh kolaborácie. Účastník kolaborácie je spokojný s uskutočnenou kolaboráciou iba vtedy, ak boli splnené všetky jeho požiadavky. Dôvera v tomto prípade predstavuje presvedčenie účastníka kolaborácie, že kolaborujúca entita skutočne splní stanovené požiadavky. Požiadavky na kvalitu a



Obrázok č. 4: Komponenty hodnoty dôvery

priebeh kolaborácie sa dajú transformovať na parametre popisujúce systémové vlastnosti a schopnosti kolaborujúcej entity. Na základe abstrakcie daných parametrov je možné definovať nasledujúcu klasifikáciu parametrov (viď obrázok č. 4): *(i)* parametre popisujúce správanie, *(ii)* parametre popisujúce systém *(iii)* a parametre popisujúce požiadavky na bezpečnosť.

Parametre popisujúce správanie sa účastníka kolaborácie predstavujú formy správania sa tohto účastníka, ktoré boli pozorované počas predošlých kolaborácií. Medzi tieto parametre patrí napríklad dostupnosť, prístupnosť, kompetencia a spoľahlivosť. Na základe analýzy histórie pozorovaného správania sa a aplikovaným personalizovaných preferencií o korektnom a nekalom správaní dokážu účastníci kolaborácie predikovať výsledok tejto kolaborácie.

Parametre popisujúce systém predstavujú technické parametre a schopnosti systému účastníka kolaborácie. Medzi tieto parametre patria napríklad aplikované mechanizmy autentifikácie a autorizácie, používané bezpečnostné mechanizmy, spôsob zabezpečenia integrity dát, atď. Parametre popisujúce systém účastníka kolaborácie sú typické pre svoju nemennosť, t. j. tieto parametre sa postupom času menia len zriedka. Zmena prichádza náhle a je nápadne veľká.

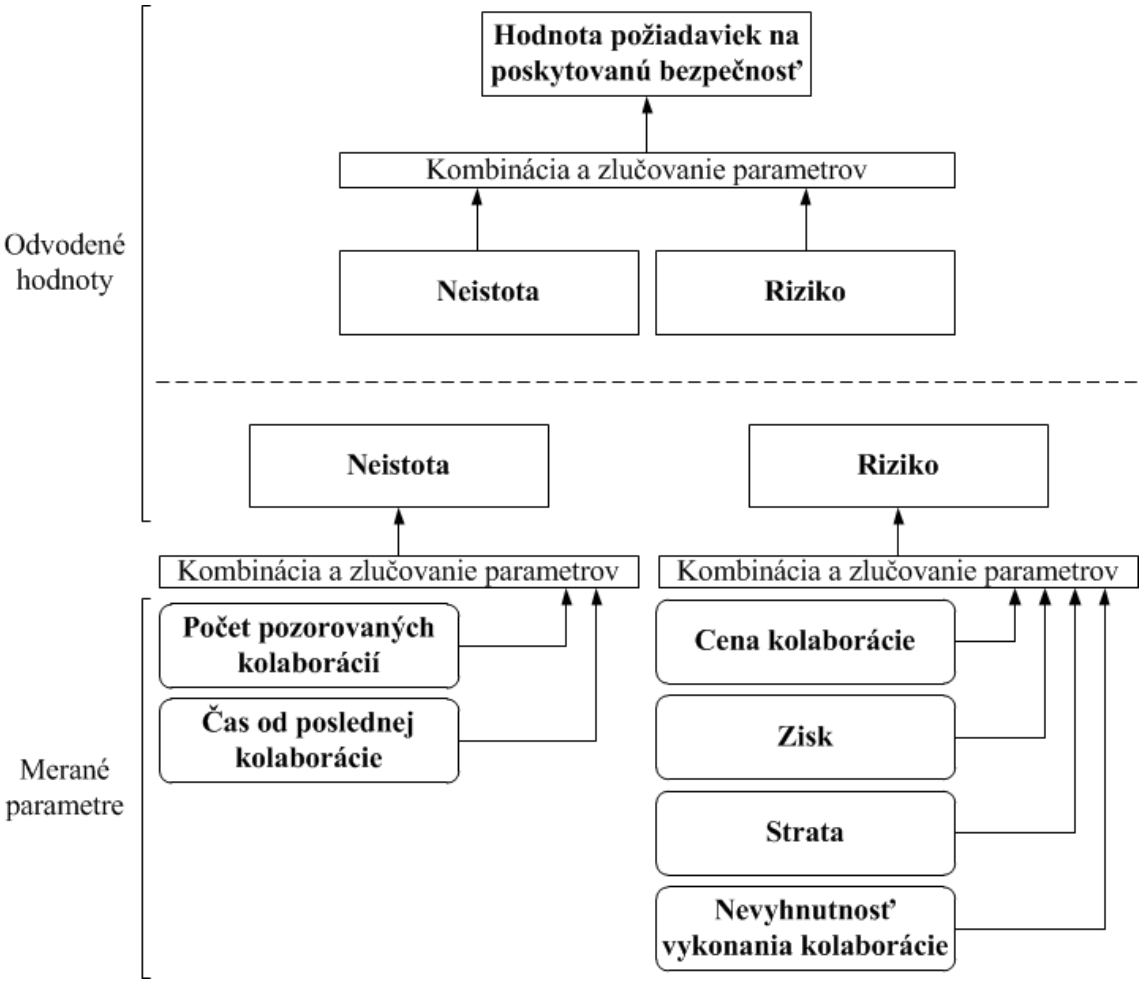
Parametre popisujúce požiadavky na bezpečnosť neslúžia na určovanie vzájomnej dôveryhodnosti účastníkov kolaborácie, ale určujú požiadavky na úroveň bezpečnosti implementovanej účastníkmi kolaborácie. Medzi tieto parametre patrí napríklad zisk a strata spojená s kolaboráciou, čas od poslednej vzájomnej kolaborácie, dostupnosť evidencie o pozorovaných formách správania sa, atď. V rámci istej kolaborácie predstavujú požiadavky na bezpečnosť požadovanú dôveryhodnosť účastníkov kolaborácie

4.1.2 Výpočet hodnoty dôvery

Kolaborácia medzi používateľom a poskytovateľom zdieľaných prostriedkov je vykonaná len v prípade, že obaja účastníci kolaborácie súhlasia s jej uskutočnením. Vykonanie rozhodnutia si ale vyžaduje stanoviť požiadavky oboch účastníkov na poskytovanú bezpečnosť (označme ako SD) a index dôvery predstavujúci vnímanú úroveň dôveryhodnosti (označme ako TI). Kolaborácia sa uskutoční len vtedy, ak z pohľadu oboch účastníkov kolaborácie je splnená podmienka $SD \leq TI$ (podmienku definovali vo svojej práci Song et al. [10, 11]).

4.1.2.1 Výpočet hodnoty požiadaviek na poskytovanú bezpečnosť

Hodnota **požiadaviek na poskytovanú bezpečnosť** sa stanovuje na základe rizika a neistoty vnímaných účastníkmi potencionálne vykonanej kolaborácie. Tento vzťah je znázornený na obrázku č. 5. V prípade kolaborácie spojenej s veľkou mierou rizika vnímaného účastníkom kolaborácie má tento účastník veľké požiadavky na bezpečnosť poskytovanú druhým účastníkom kolaborácie. Ak je miera vnímaného rizika malá, tak sa zmenšuje aj celková hodnota požiadaviek na poskytovanú bezpečnosť. Obdobne ovplyvňuje hodnotu požiadaviek na poskytovanú bezpečnosť aj neistota. Čím väčšia je neistota účastníka kolaborácie, tým menej si je účastník istý výsledkom kolaborácie. V tomto prípade hodnota požiadaviek na poskytovanú bezpečnosť bude rásť.



Obrázok č. 5: Hodnota požiadaviek na poskytovanú bezpečnosť odvodená z komponentov hodnoty dôvery

Čím viac potrebné je bezchybné vykonanie potencionálnej kolaborácie, tým väčšia škoda vznikne účastníkom kolaborácie v prípade jej zlyhania. Pravdepodobnosť vzniku takéhoto zlyhania a ním spôsobené škody sa označujú ako **riziko**. Hodnota rizika pre účely výpočtu hodnoty požiadaviek na poskytovanú bezpečnosť je určená odvodením z nasledujúcich merateľných parametrov [7, 15, 43] (viď obrázok č. 5):

- **Cena kolaborácie** predstavuje náklady (napr. poplatky za použitie zdieľaného prostriedka), ktoré účastník kolaborácie bude musieť zaplatiť druhej kolaborujúcej entite v prípade spustenia vykonávania potencionálnej kolaborácie. Vo väčšine prípadov nie je účastník kolaborácie ochotný investovať veľký obnos peňažných prostriedkov. Investovať takýto väčší obnos peňažných prostriedkov je účastník ochotný len v prípade vysokej miery bezpečnosti poskytovanej druhým kolaborujúcim účastníkom. Z uvedeného vyplýva, že riziko vnímané účastníkom kolaborácie vzrastá s rastúcou sumou investovaných peňažných prostriedkov.
- **Zisk** predstavuje odhadovaný prínos (napr. výsledok spracovania dát, poplatky za použitie zdieľaného prostriedka, atď.) účastníka kolaborácie, ktorý získa po úspešnom dokončení kolaborácie. Čím je odhadovaný prínos väčší, tým viac je aj účastník kolaborácie motivovaný túto kolaboráciu úspešne vykonať. Z uvedeného vyplýva, že s rastúcim odhadovaným prínosom vykonanej kolaborácie riziko vnímané účastníkom kolaborácie klesá.
- **Strata** predstavuje obnos peňažných prostriedkov, o ktoré účastník kolaborácie príde v prípade zlyhania počas vykonávania kolaborácie. Stratené peňažné prostriedky nezodpovedajú iba zaplatenej cene kolaborácie. Strata zahŕňa aj stratený odhadovaný zisk z úspešne vykonanej kolaborácie, čas investovaný do vykonávanie kolaborácie, dôležitosť dát získaných prostredníctvom kolaborácie, zlepšenie reputácie úspešným dokončením kolaborácie, atď. Vo väčšine prípadov nie je účastník kolaborácie ochotný vykonať kolaboráciu spojenú s vysokou odhadovanou

stratou. Účastník je ochotný zúčastniť sa takejto kolaborácie iba vtedy, ak je miera bezpečnosti poskytovanej druhým účastníkom kolaborácie vysoká. Z uvedeného vypláva, že riziko vnímané účastníkom kolaborácie vzrastá s rastúcou mierou odhadovanej straty.

- **Nevyhnutnosť vykonania kolaborácie** predstavuje situáciu, v rámci ktorej účastník potencionálnej kolaborácie potrebuje zabezpečiť jej vykonanie z dôvodu vyvarovania sa vzniku veľmi pravdepodobných strát. Účastník má túto potrebu vykonania kolaborácie i napriek tomu, že môžu nastať negatívne následky spojené s jej vykonaním. Čím je nevyhnutnosť vykonania kolaborácie väčšia, tým menšie požiadavky má účastník kolaborácie na poskytovanú bezpečnosť druhým účastníkom. Z uvedeného vyplýva, že riziko vnímané účastníkom kolaborácie klesá s rastúcou mierou nevyhnutnosti vykonania kolaborácie.

Rozhodovanie účastníka potencionálnej kolaborácie o jej vykonaní počas situácie, kedy si nie je istý jej výsledkom z dôvodu nedostatočného počtu relevantných informácií, sa označuje ako rozhodovanie počas **neistoty**. Hodnota neistoty pre účely výpočtu hodnoty požiadaviek na poskytovanú bezpečnosť je určená odvodením z nasledujúcich merateľných parametrov (viď obrázok č. 5):

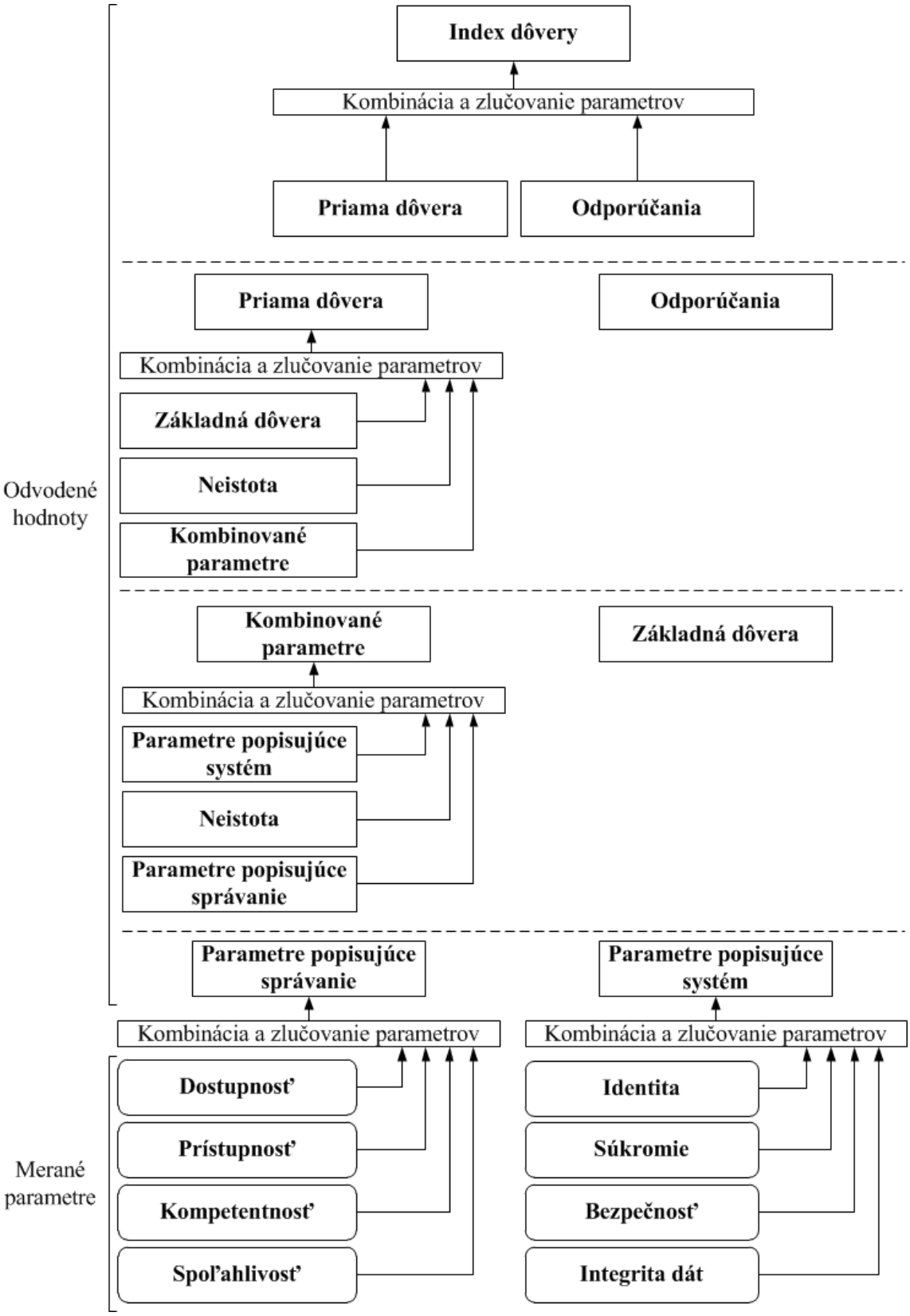
- **Počet pozorovaných kolaborácií** predstavuje všetky historické dáta o pozorovaných formách správania sa, ktoré účastník kolaborácie eviduje o druhom účastníkovi kolaborácie. Čím viac historických dát má účastník k dispozícií, tým lepšie dokáže tento účastník odhadnúť budúce správanie sa druhého účastníka. Z uvedeného vyplýva, že s rastúcim počtom dostupných historických dát o formách správania sa klesá miera neistoty vnímanej účastníkom kolaborácie.
- **Čas od poslednej kolaborácie** predstavuje veľkosť časového intervalu od poslednej interakcie účastníka kolaborácie s druhým účastníkom. Ak posledná kolaborácia bola vykonaná relatívne dávno, tak istota účastníka o výsledku potencionálne

vykonanej kolaborácie klesá. Ak bola posledná kolaborácia vykonaná len nedávno, tak istota o výsledku potencionálnej kolaborácie narastá.

4.1.2.2 Výpočet indexu dôvery

Index dôvery určovaný pre účely rozhodovania účastníkov potencionálnej kolaborácie o jej vykonaní sa stanovuje na základe priamej dôvery a odporúčaní. Tento vzťah je znázornený na obrázku č. 6. **Odporúčania** zodpovedajú reputácii člena gridovej komunity, ktorú nadobudol počas kolaborácie s inými členmi komunity. Reputáciu v kontexte spolupráce sprostredkovanej prostredníctvom ad hoc gridovej infraštruktúry je možné definovať ako všeobecný názor členov gridovej komunity o charaktere posudzovaného člena komunity. Ak má účastník potencionálnej kolaborácie znalosť o dobrej reputácii druhého účastníka, tak druhý účastník kolaborácie je dôveryhodný z pohľadu prvého účastníka práve na základe tejto dobrej reputácie. V prípade zlej reputácie je ale tento druhý účastník kolaborácie nedôveryhodný z pohľadu prvého účastníka. Z uvedeného vyplýva, že čím je reputácia posudzovaného účastníka kolaborácie lepšia, tým viac dôveryhodným sa tento účastník stáva.

Priama dôvera predstavuje vlastnú znalosť účastníka potencionálnej kolaborácie o druhom účastníkovi. Táto znalosť sa určuje na základe histórie dát o pozorovaných formách správania sa druhého účastníka, kontexte potencionálne vykonanej kolaborácie a atribútov popisujúcich technické parametre a schopnosti systému druhého účastníka. Priama dôvera a odporúčania majú odlišný vplyv na výslednú hodnotu indexu dôvery. Vlastná znalosť účastníka kolaborácie vo forme priamej dôvery má výraznejší vplyv na index dôvery. V prípade dostatočne veľkej priamej dôvery je druhý účastník kolaborácie dôveryhodný z pohľadu prvého účastníka aj napriek jeho zlej reputácií. V prípade značne malej priamej dôvery je druhý účastník kolaborácie nedôveryhodný aj napriek jeho dobrej reputácii. Schopnosť priamej dôvery ovplyvniť index dôvery vo väčšej miere ako



Obrázok č. 6: Index dôvery odvodený z komponentov hodnoty dôvery

odporúčania je závislá na váhach, ktoré sú týmto dvom parametrom priradené v rámci rozhodovacieho procesu. Hodnota priamej dôvery je určená odvodením z nasledujúcich parametrov (viď obrázok č. 6):

- **Základná dôvera** prestavuje hodnotu dôvery jedného účastníka kolaborácie v druhého účastníka. Ak má byť potencionálna kolaborácia vykonaná medzi vzájomne si neznámymi účastníkmi (t. j. títo účastníci spolu ešte nikdy nespolupracovali), tak základná dôvera je nastavená na hodnotu inicializačnej dôvery. Inicializačná dôvera charakterizuje neznámeho účastníka ako napoly dôveryhodného a napoly nedôveryhodného. Po ukončení každej kolaborácie je hodnota základnej dôvery nastavená na novú hodnotou, ktorá je rovná hodnote indexu dôvery vypočítanej po kolaborácii. Základná dôvera sa mení aj s plynúcim časom. Čím viac času uplynulo od poslednej vzájomnej kolaborácie medzi dvoma účastníkmi, tým viac sa základná dôvera približuje hodnote inicializačnej dôvery.
- **Kombinované parametre** združujú všetky relevantné vlastnosti systému účastníka kolaborácie. Tieto vlastnosti sú vzájomnou kombináciou a zlučovaním spojené do jednej výslednej hodnoty. Táto hodnota zodpovedá kvalite technických vlastností systému účastníka kolaborácie ako i pozorovaným formám správania sa tohto účastníka.
- **Neistota** predstavuje počet dostupných informácií, ktoré účastník potencionálnej kolaborácie potrebuje na čo najpresnejšie vykonanie rozhodnutia o uskutočnení alebo neuskutočnení kolaborácie. Neistota neovplyvňuje priamu dôvery priamo. V rámci vykonávania rozhodnutia vystupuje skôr v úlohe váhy, ktorá určuje významnosť vplyvu základnej dôvery a kombinovaných parametrov na odvodenú hodnotu priamej dôvery. V prípade malej miery neistoty vnímanej účastníkom kolaborácie má väčší vplyv na rozhodnutie základná dôvera. V prípade vysokej miery neistoty ovplyvňujú priamu dôveru vo väčšej miere kombinované parametre.

Kombinované parametre sú odvodené vzájomnou kombináciou **parametrov popisujúcich systém** účastníka kolaborácie a **parametrov popisujúcich pozorované formy správania sa** tohto účastníka. Nepriamy vplyv na výslednú hodnotu kombinovaných parametrov má aj neistota vnímaná účastníkom potencionálnej kolaborácie. Pri kombinácii parametrov slúži neistota ako váha určujúca významnosť vplyvu jednotlivých parametrov na výslednú hodnotu kombinovaných parametrov. V prípade malej miery neistoty majú parametre popisujúce správanie sa účastníka kolaborácie väčší vplyv na hodnotu kombinovaných parametrov. Pri vysokej miere neistoty väčší vplyv na hodnotu kombinovaných parametrov majú parametre popisujúce systém účastníka kolaborácie.

Výslednú hodnotu kombinovaných parametrov je možné odvodiť z nasledovných parametrov popisujúcich systém účastníka potencionálnej kolaborácie (viď obrázok č. 6):

- **Identita** ako parameter popisuje kvalitatívne vlastnosti mechanizmu, ktorý používatelia a poskytovatelia zdieľaných prostriedkov používajú pri autentifikácií členov kolaborácií sprostredkovávaných ad hoc gridovou infraštruktúrou.
- **Súkromie** ako parameter popisuje kvalitatívne schopnosti poskytovateľov zdieľaných prostriedkov povoliť prístup iba k takým dátam, na ktoré majú autentifikovaní používatelia právo prístupu.
- **Bezpečnosť** ako parameter popisuje schopnosť poskytovateľov zdieľaných prostriedkov zaistiť bezpečný prenos dát a ochrániť svoje prostriedky pred škodlivým zdrojovým kódom obsiahnutým v používateľských úlohách, vírusmi, malware programami, atď.
- **Integrita dát** ako parameter popisuje schopnosť používateľov a poskytovateľov zdieľaných prostriedkov zabezpečiť prenášané dáta a správy pred ich nežiadúcim pozmenením treťou stranou. Integrita dát popisuje najmä kvalitatívne vlastnosti mechanizmov chrániace komunikačné linky ako i využívané kryptografické techniky chrániace dáta pred nechceným pozmenením.

Výslednú hodnotu kombinovaných parametrov je možné odvodiť z nasledovných parametrov popisujúcich správanie sa účastníka potencionálnej kolaborácie (viď obrázok č. 6):

- **Dostupnosť** ako parameter popisuje pripravenosť prostriedkov zdieľaných poskytovateľmi vykonávať používateľské úlohy, ukladať a spravovať dáta používateľov alebo poskytovať iné služby ponúkané poskytovateľmi prostriedkov.
- **Prístupnosť** ako parameter popisuje schopnosť prostriedkov zdieľaných poskytovateľmi reagovať na dopyty týkajúce sa informácií popisujúcich stav prostriedkov a vykonávaných používateľských úloh alebo na dopyty týkajúcich sa informácií o iných poskytovaných službách ponúkaných poskytovateľmi prostriedkov.
- **Kompetentnosť** z pohľadu používateľov popisuje ochotu a pripravenosť prostriedkov zdieľaných poskytovateľmi poskytnúť všetky dohodnuté systémové prostriedky, ktoré sú potrebné pre vykonanie používateľskej úlohy. Z pohľadu poskytovateľov zdieľaných prostriedkov predstavuje kompetentnosť ochotu používateľov používať dohodnuté systémové prostriedky a to počas dohodnutého časového intervalu.
- **Spoľahlivosť** z pohľadu používateľov popisuje korektné fungovanie prostriedkov zdieľaných poskytovateľmi alebo iných služieb ponúkaných poskytovateľmi. Z pohľadu poskytovateľov prostriedkov popisuje spoľahlivosť korektné vykonanie používateľských úloh, ktoré nepoškodzujú prostriedky prostredníctvom škodlivého zdrojového kódu a zároveň ani nepristupujú k neautorizovaným dátam.

4.1.3 Metóda merania parametrov

Hodnota požiadaviek na poskytovanú bezpečnosť a hodnota indexu dôvery slúžia na vykonávanie rozhodnutí o uskutočnení alebo neuskutočnení potencionálnych kolaborácií. Uvedené hodnoty sa odvodzujú z merateľných parametrov a odvodených parametrov (viď obrázok č. 5 a obrázok č. 6). Medzi merané parametre sa radia parametre

slúžiace na odvodenie parametrov popisujúcich systém, parametrov popisujúcich pozorované formy správania a parametrov popisujúcich riziko a neistotu. Ostatné parametre sú odvodené na základe parametrov z nižšej úrovne (výnimku tvoria iba odporúčania a základná dôvera, ktorých hodnoty sa získavajú odlišným spôsobom).

Merateľné parametre sú merané buď priamo alebo môžu byť rozčlenené na merateľné prvky. Parametre slúžiace na odvodenie hodnoty parametrov popisujúcich správanie sa členov gridovej komunity sú merané priamo. Označme účastníka kolaborácie X ako účastníka určujúceho dôveryhodnosť druhého účastníka. Zároveň označme druhého účastníka kolaborácie Y ako hodnoteného účastníka. Výsledná hodnota parametrov V_X popisujúcich správanie sa hodnoteného účastníka kolaborácie určenej na základe všetkých N pozorovaných parametrov je vyjadrená formulou 1:

$$V_X = \frac{\sum_{i=1}^{N} E(Y)_i}{N} \tag{1}$$

kde $E(Y)_i$ predstavuje hodnotu priradenú i-tému pozorovanému parametru. Každý pozorovaný parameter je určený ako podiel počtu "pozitívnych" pozorovaní korektného správania sa a celkového počtu pozorovaní. Tento vzťah je vyjadrený formulou 2:

$$E(Y)_i = \frac{\begin{array}{c}\text{"}pozitívne\text{"}\ pozorovania\ i\text{-}tého \\ parametra\end{array}}{všetky\ pozorovania\ i\text{-}tého\ parametra} \tag{2}$$

Niektoré parametre slúžiace na odvodenie parametrov popisujúcich systém členov gridovej komunity sú merané priamo. Iné parametre sú zasa rozčlenené na merateľné prvky [31, 44]. Parameter identita je meraný priamo na základe mechanizmu, ktorý je použitý príslušným členom gridovej komunity na autentifikovanie iných členov komunity. Medzi používané mechanizmy patrí autentifikácia na základe používateľského mena a

hesla, autentifikácia založená na X.509 certifikátoch alebo autentifikácia prostredníctvom Kerberos infraštruktúry. Čím dômyselnejší je použitý mechanizmus autentifikácie, tým väčšia hodnota je priradená meranému parametru. V tomto prípade je hodnota meraného parametra rovná hodnote 1, 2 alebo 3 v závislosti od použitého mechanizmu autentifikácie.

Parameter súkromie je meraný priamo na základe mechanizmu, ktorý je použitý príslušným poskytovateľom zdieľaných prostriedkov pre účely autorizácie prístupu k prostriedkom a dátam. Medzi používané mechanizmy patrí autorizácia na základe identity, autorizácia založená na roli používateľa a autorizácia na základe atribútov používateľa. Čím dômyselnejší je použitý mechanizmus autorizácie, tým väčšia hodnota je priradená meranému parametru. V tomto prípade je hodnota meraného parametra rovná hodnote 1, 2 alebo 3 v závislosti od použitého mechanizmu autorizácie.

Parameter bezpečnosť je meraný na základe nasledujúcich merateľných prvkov: *(i)* zabezpečenie vlastnej ochrany zdieľaným prostriedkom, *(ii)* zabezpečenie komunikačných liniek *(iii)* a vykonávanie používateľských úloh na zdieľanom prostriedku v prostredí sandbox. Zabezpečenie vlastnej ochrany zdieľaným prostriedkom je merané na základe mechanizmov používaných zdieľaným prostriedkom pre ochranu proti vírusom, malware programom a inej nekalej činnosti zo strany používateľov. Medzi používané mechanizmy patria napríklad antivírusové programy, brána firewall, IDS, atď. Čím viac mechanizmov zdieľaný prostriedok používa, tým väčšia je hodnota zabezpečenia vlastnej ochrany zdieľaným prostriedkom. Hodnota meraného prvku je v tomto prípade zväčšená o hodnotu 1 pre každý použitý mechanizmus. Zabezpečenie komunikačných liniek je merané na základe použitého typu komunikačného protokolu, medzi ktoré patrí napríklad TLS alebo IPsec. Čím dômyselnejší je použitý typ protokolu, tým väčšia je hodnota priradená meranému prvku. V tomto prípade je hodnota meraného prvku rovná hodnote 1 alebo 2 v závislosti od použitého typu protokolu. Vykonávanie používateľských úloh na zdieľanom

prostriedku v prostredí sandbox je merané na základe schopnosti zdieľaného prostriedku tento výpočtový sandbox poskytovať. Hodnota meraného prvku je rovná hodnote 1 ak prostriedok sandbox poskytuje, v opačnom prípade je hodnota prvku rovná hodnote 0.

Parameter integrita dát je meraný na základe nasledujúcich merateľných prvkov: *(i)* ochrana proti chybám dát *(ii)* a zabezpečenie komunikačných liniek. Ochrana proti chybám dát je meraná na základe mechanizmov použitých na vyvarovanie sa nechcenej zmeny dát, ktorá sa môže vyskytnúť počas zapisovania, čítania alebo spracovania týchto dát. Medzi používané mechanizmy patrí vytváranie kontrolných súm dát a metadát ako i hardvérové riešenie RAID. Čím viac mechanizmov systém zdieľaného prostriedku alebo používateľa používa, tým väčšia je hodnota ochrany proti chybám dát. Hodnota meraného prvku je v tomto prípade zväčšená o hodnotu 1 pre každý použitý mechanizmus. Zabezpečenie komunikačných liniek je merané rovnakým spôsobom ako je to v prípade parametru bezpečnosť (t. j. na základe použitého typu protokolu).

Označme účastníka kolaborácie X ako účastníka určujúceho dôveryhodnosť druhého účastníka. Zároveň označme druhého účastníka kolaborácie Y ako hodnoteného účastníka. Výsledná hodnota parametrov V_X popisujúcich systém hodnoteného účastníka kolaborácie určenej na základe všetkých N meraných parametrov je vyjadrená formulou 1, kde $E(Y)_i$ predstavuje hodnotu priradenú i-tému meranému parametru. Pre hodnoty parametrov identity a súkromia platí, že hodnota $E(Y)_i$ je určená ako podiel hodnoty priradenej parametru a maximálne možnej hodnoty príslušného parametra. Tento vzťah je generalizovaný formulou 3:

$$E(Y)_i = \frac{hodnota\ priradená\ i\text{-}tému\ merateľnému\ parametru}{maximálna\ možná\ hodnota\ i\text{-}tého\ merateľného\ parametra} \quad (3)$$

Pre hodnoty parametrov bezpečnosti a integrity dát platí, že hodnota $E(Y)_i$ je určená

ako podiel súčtu n hodnôt priradených jednotlivým merateľným prvkom prislúchajúcich nepriamo merateľnému parametru a maximálne možnej hodnoty tohto parametra. Tento vzťah je generalizovaný formulou 4:

$$E(Y)_i = \frac{\sum_{j=1}^{n} \begin{array}{c} j\text{-tá } hodnota\ merateľnoho\ prvku\ prislúchajúca \\ i\text{-tému } nepriamo\ merateľnému\ parametru \end{array}}{\begin{array}{c} maximálna\ možná\ hodnota \\ i\text{-tého } nepriamo\ merateľného\ parametra \end{array}} \tag{4}$$

Parametre slúžiace na odvodenie hodnoty neistoty sú merané priamočiaro, tak ako je popísané v sekcii č. 4.1.2.1. V prípade parametrov slúžiacich na odvodenie hodnoty rizika je určovanie ich hodnôt odlišné od všetkých ostatných metód popísaných vyššie. Používatelia ako i poskytovatelia zdieľaných prostriedkov definujú očakávania, ktoré môžu dosiahnuť vykonaním potencionálnej kolaborácie. Tieto očakávania sú vyjadrené formou očakávaných nákladov, predpokladaného zisku, predpokladaných strát v prípade zlyhania kolaborácie a aktuálnej nutnosti vykonania kolaborácie. Z uvedeného vyplýva, že hodnoty týchto parametrov sú merané ako osobné preferencie používateľov a poskytovateľov zdieľaných prostriedkov.

Hodnoty parametrov odvodených z meraných parametrov sú normalizované tak, aby tieto hodnoty patrili do intervalu $< 0, 1 >$. Dôvod pre transformáciu hodnôt do tohto intervalu je ten, že hodnoty odvodených parametrov nadobúdajú rôzne maximálne hodnoty. Po normalizácii hodnôt je možné potom jednotlivé parametre zlučovať do výslednej hodnoty indexu dôvery a hodnoty požiadaviek na poskytovanú bezpečnosť prostredníctvom lineárnej kombinácie alebo aplikovaním logických fuzzy pravidiel v prípade fuzzy odvodzovacieho systému. Konkrétne váhy, ktoré môžu byť aplikované pre jednotlivé hodnoty parametrov, je možné potom stanoviť podľa požiadaviek a preferencií používateľov

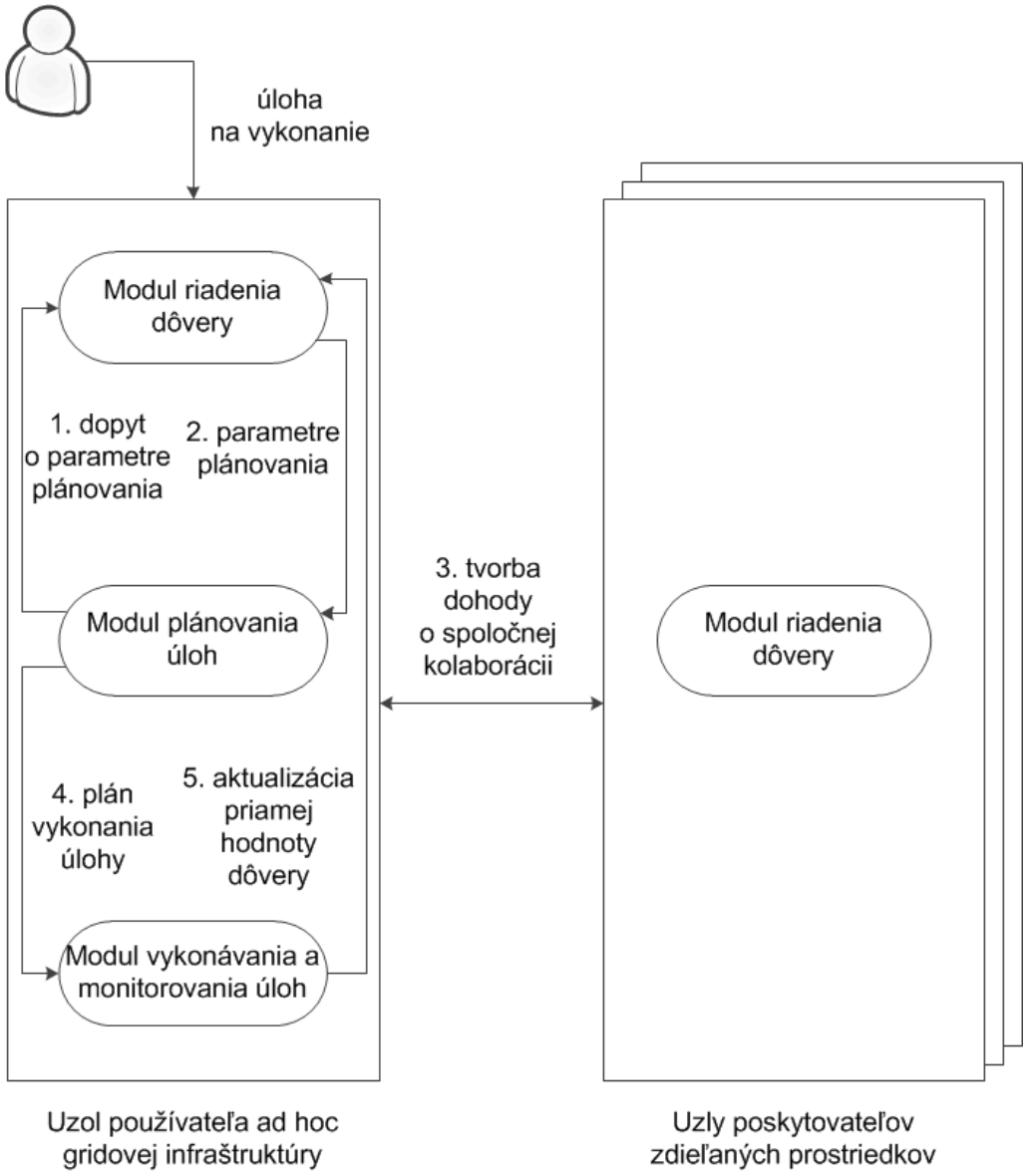
a poskytovateľov zdieľaných prostriedkov. Tieto váhy by však mali zohľadňovať vzťahy medzi parametrami popísanými v sekcii 4.1.2.

4.2 Integrácia riadenia dôvery do ad hoc gridovej infraštruktúry

Integrácia riadenia dôvery do ad hoc gridovej infraštruktúry si nevyhnutne vyžaduje úpravu a rozšírenie viacerých fáz, ktoré sa vykonávajú počas plánovania vykonávania úloh. Fáza vyhľadávania dostupných zdieľaných prostriedkov, fáza výberu vhodného systému a fáza vykonávania úloh musia byť rozšírené o nasledovné kroky: *(i)* určenie požiadaviek na poskytovanú bezpečnosť, *(ii)* stanovenie indexu dôvery *(iii)* a aktualizácia základnej dôvery po ukončení kolaborácie. Vykonanie týchto dodatočných krokov nie je možné bez úpravy architektúry ad hoc gridovej infraštruktúry. Úprava architektúry spočíva v rozšírení ad hoc gridovej infraštruktúry o nový modul nazvaný modul riadenia dôvery. Integrácia tohto modulu je načrtnutá na obrázku č. 7.

Počas uskutočňovania fázy vyhľadávania vhodných zdieľaných prostriedkov definuje používateľ okrem svojej úlohy aj systémové požiadavky, ktoré zdieľaný prostriedok musí spĺňať pre jej úspešné vykonanie. Modul plánovania úloh vykonaním filtrovania dostupných zdieľaných prostriedkov na základe autorizácie a stanovených požiadaviek vyberie také zdieľané prostriedky, ktoré spĺňajú minimálne požiadavky na vykonanie úlohy. Po výbere zdieľaných prostriedkov spĺňajúcich systémové požiadavky zabezpečí modul plánovania úlohy zber dynamických informácií o vybraných zdieľaných prostriedkoch prostredníctvom informačných služieb ad hoc gridovej infraštruktúry. V tomto okamihu začne prebiehať voľba systému, t. j. výber konkrétneho zdieľaného prostriedka.

V prostredí ad hoc gridovej infraštruktúry je používateľ ochotný uskutočniť svoju úlohu iba na zdieľanom prostriedku patriaceho dôveryhodnému poskytovateľovi zdieľa-



Obrázok č. 7: Schéma integrácie riadenia dôvery do ad hoc gridovej infraštruktúry

ných prostriedkov. Modul plánovania najskôr zvolí prostriedok, ktorý čo najviac optimalizuje čas vykonania úlohy alebo iné kritérium podľa požiadaviek používateľa. Pre takto zvolený zdieľaný prostriedok si následne vyžiada modul plánovania úlohy dodatočné parametre plánovania od modulu riadenia dôvery vo forme požiadaviek na poskytovanú bezpečnosť (SD) a index dôvery (TI). Parameter SD je určovaný na základe predpokladaných nákladov kolaborácie, predpokladaného zisku, možnej straty a aktuálnej nutnosti vykonania kolaborácie. Špecifikáciu týchto očakávaní definuje používateľ súčasne s definíciou úlohy a definíciou systémových požiadaviek. Parameter SD je tiež určovaný aj na základe dát popisujúcich správanie sa daného zdieľaného prostriedka, ktoré používateľ pozoroval počas predošlých vzájomných kolaborácií s daným prostriedkom. Za správu historických dát je pritom zodpovedný modul riadenia dôvery. Parameter TI je určovaný na základe historických dát ako i dynamických informácií bližšie špecifikujúcich vlastnosti zdieľaného prostriedka. Získavanie týchto informácií uskutočňuje modul riadenia prostredníctvom rovnakých informačných služieb ako modul plánovania. Modul plánovania vykoná na základe hodnôt SD a TI rozhodnutie, či je zdieľaný prostriedok dôveryhodný na vykonanie používateľovej úlohy, t. j. musí platiť podmienka $SD \leq TI$. Ak prostriedok nie je dostatočne dôveryhodný, tak modul plánovania úloh vykoná rozhodnutie o dôveryhodnosti ďalšieho prostriedka optimalizujúceho kritérium plánovania. Tento proces (kroky 1 a 2 na obrázku č.7) sa opakuje tak dlho, kým nie je nájdený dôveryhodný zdieľaný prostriedok.

Poskytovateľ zdieľaných prostriedkov je ochotný poskytnúť svoje prostriedky na zdieľanie len dôveryhodným používateľom. Modul plánovania úloh môže teda zaslať používateľskú úlohu na spracovanie zdieľanému prostriedku iba vtedy, ak tento prostriedok súhlasí s vykonaním kolaborácie. Modul plánovania úloh po nájdení dôveryhodného zdieľaného prostriedka požiada tento prostriedok o súhlas s kolaboráciou. Zdieľaný prostriedok vykonáva rozhodnutie na základe hodnôt SD a TI, ktorých hodnoty určí pomocou

svojho modulu riadenia dôvery. Parameter SD z pohľadu poskytovateľa prostriedka je určovaný taktiež na základe nákladov kolaborácie, predpokladaného zisku, možnej straty a nutnosti vykonania kolaborácie. Špecifikáciu týchto očakávaní musí definovať poskytovateľ najneskôr od okamihu začatia zdieľania prostriedka, alebo je určovaná automaticky na základe poskytovateľom definovaných pravidiel. Parameter SD je tiež určovaný aj na základe dát popisujúcich správanie sa systému používateľa, ktoré zdieľaný prostriedok pozoroval počas predošlých vzájomných kolaborácií. Parameter TI je určovaný na základe historických dát a dynamických informácií o systéme používateľa. Zdieľaný prostriedok vykoná rozhodnutie, či je používateľ dôveryhodný pre vykonanie jeho úlohy, t. j. musí platiť podmienka $SD \leq TI$. Ak prostriedok odmietne zúčastniť sa na kolaborácii, tak používateľov modul plánovania úloh vyberie ďalší dostatočne dôveryhodný zdieľaný prostriedok, ktorý požiada o súhlas s kolaboráciou. Tento proces (krok 3 na obrázku č.7) sa opakuje tak dlho, kým modul plánovania nenájde zdieľaný prostriedok súhlasiaci s účasťou na kolaborácií.

Modul plánovania úloh zabezpečí odoslanie používateľovej úlohy na vybraný zdieľaný prostriedok prostredníctvom modulu vykonávania a monitorovania úloh (krok 4 na obrázku č. 7). Po ukončení úlohy musí prebehnúť aktualizácia základnej dôvery. Táto aktualizácia prebieha na uzle používateľa ako i na uzle poskytovateľa zdieľaného prostriedka. Používateľov modul riadenia dôvery stanoví novú hodnotu základnej dôvery voči poskytovateľovi ako TI zohľadňujúci priebeh ukončenej kolaborácie (krok 5 na obrázku č. 7). Podobne, modul riadenia dôvery poskytovateľa zdieľaného prostriedka určí novú hodnotu základnej dôvery voči používateľovi ako TI taktiež zohľadňujúci priebeh ukončenej kolaborácie.

Kapitola 5

Overenie riešenia a zhodnotenie dosiahnutých výsledkov

Účelom integrácie riadenia dôvery do ad hoc gridovej infraštruktúry je zlepšenie bezpečnosti poskytovanej infraštruktúrou jej používateľom ako i poskytovateľom zdieľaných prostriedkov. Sekcia 5.1 popisuje spôsob overenia integrácie riadenia dôvery navrhnutej v kapitole 4. Sekcia 5.2 sa zaoberá hodnotením dosiahnutia cieľov stanovených v kapitole 2 a zároveň popisuje oblasti ďalšieho výskumu.

5.1 Overenie riešenia

Metodika overenia navrhovaného riešenia sa skladá z určenia metódy overenia, stanovenia metrík, uskutočnenia overenia a zhodnotenia výsledkov overenia pomocou zvolených metrík.

5.1.1 Metóda overenia

Navrhnuté riešenie integrácie riadenia dôvery do ad hoc gridovej infraštruktúry je overené pomocou počítačovej simulácie. V rámci simulácie sa reálny systém ad hoc gri-

dovej infraštruktúry nahradil jej počítačovým modelom. Simulácia sa zameriavala najmä na dopad integrácie riadenia dôvery na správanie sa simulovaného systému.

Na vykonanie simulácie ad hoc gridovej infraštruktúry rozšírenej o riadenie dôvery bol použitý simulačný nástroj GridSim[45]. Tento nástroj bol vyvinutý za účelom návrhu a vyhodnotenia algoritmov plánovania úloh v tradičnej gridovej infraštruktúre. Úpravou a rozšírením zdrojového kódu nástroja bolo však možné rozšíriť tento nástroj o schopnosť simulovania ad hoc gridovej infraštruktúry vykonávajúcej proces plánovanie úloh v súčinnosti s riadením dôvery.

Popis simulácie. Simulovaný počítačový model obsahuje desať entít predstavujúcich používateľov ad hoc gridovej infraštruktúry a desať entít predstavujúcich poskytovateľov zdieľaných prostriedkov. Simulovaní používatelia majú priradené viaceré systémové charakteristiky a formy správania sa (uvedené v tabuľke č. 4 a 5). Simulovaní poskytovatelia zdieľaných prostriedkov majú tiež priradené viaceré charakteristiky a formy správania sa (uvedené v tabuľke č. 6 a 7). Systémové charakteristiky ako i formy správania sa predstavujú parametre, ktoré slúžia na výpočet hodnoty požiadaviek na poskytovanú bezpečnosť a hodnoty indexu dôvery.

Priebeh simulácie vykonanej pomocou nástroja GridSim začína vytvorením entít predstavujúcich používateľov ad hoc gridovej infraštruktúry a poskytovateľov zdieľaných prostriedkov. Každému používateľovi sú priradené jeho systémové charakteristiky a očakávané formy správania sa. Entity používateľov sú po spustení simulácie zodpovedné za generovanie používateľských úloh, ktorým je priradená veľkosť dát určených na spracovanie a časová náročnosť vykonania úlohy. Entity používateľov generujú nové úlohy nezávisle od aktuálne naplánovaných a vykonávaných úloh. Nové úlohy sú generované aj vtedy, ak používateľove úlohy neboli ešte dokončené. Systémové charakteristiky, očakávané formy správania sa a výpočtový výkon zdieľaného prostriedka sú priradené aj en-

Charakteristika	**Používateľ**				
	1	2	3	4	5
Antivírusová ochrana	Áno	Áno	Áno	Áno	Áno
Firewall	Áno	Áno	Áno	Áno	Áno
IDS	Nie	Nie	Nie	Nie	Nie
TLS	Áno	Áno	Áno	Áno	Áno
IPsec	Nie	Nie	Nie	Nie	Nie
Výskyt chybných úloh	Žiadny výskyt	Takmer žiadny výskyt	Zriedkavý výskyt	Zriedkavý výskyt	Bežný výskyt

Tabuľka č. 4: Charakteristiky používateľov (1 - 5) simulovanej ad hoc gridovej infraštruktúry

Charakteristika	**Používateľ**				
	6	7	8	9	10
Antivírusová ochrana	Áno	Áno	Áno	Áno	Áno
Firewall	Áno	Áno	Áno	Áno	Áno
IDS	Nie	Nie	Nie	Nie	Nie
TLS	Áno	Áno	Áno	Áno	Áno
IPsec	Nie	Nie	Nie	Nie	Nie
Výskyt chybných úloh	Bežný výskyt	Častý výskyt	Častý výskyt	Veľmi častý výskyt	Veľmi častý výskyt

Tabuľka č. 5: Charakteristiky používateľov (6 - 10) simulovanej ad hoc gridovej infraštruktúry

Charakteristika	**Poskytovateľ zdieľaných prostriedkov**				
	1	2	3	4	5
Antivírusová ochrana	Áno	Áno	Áno	Áno	Áno
Firewall	Áno	Áno	Áno	Áno	Áno
IDS	Nie	Nie	Nie	Nie	Nie
TLS	Áno	Áno	Áno	Áno	Áno
IPsec	Nie	Nie	Nie	Nie	Nie
Sandbox	Nie	Nie	Nie	Nie	Nie
Typ autentifikácie	X509 certifikát	X509 certifikát	X509 certifikát	X509 certifikát	X509 certifikát
Typ autorizácie	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa
MIPS	2700	2350	2000	2350	2350
Výskyt nedostupnosti prostriedka	Žiadny výskyt	Žiadny výskyt	Žiadny výskyt	Veľmi zriedkavý výskyt	Zriedkavý výskyt
Výskyt zlyhania vykonávania úlohy	Žiadny výskyt	Žiadny výskyt	Žiadny výskyt	Bežný výskyt	Bežný výskyt

Tabuľka č. 6: Charakteristiky poskytovateľov zdieľaných prostriedkov (1 - 5) v simulovanej ad hoc gridovej infraštruktúre

Charakteristika	**Poskytovateľ zdieľaných prostriedkov**				
	6	7	8	9	10
Antivírusová ochrana	Áno	Áno	Áno	Áno	Áno
Firewall	Áno	Áno	Áno	Áno	Áno
IDS	Nie	Nie	Nie	Nie	Nie
TLS	Áno	Áno	Áno	Áno	Áno
IPsec	Nie	Nie	Nie	Nie	Nie
Sandbox	Nie	Nie	Nie	Nie	Nie
Typ autentifikácie	X509 certifikát	X509 certifikát	X509 certifikát	X509 certifikát	X509 certifikát
Typ autorizácie	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa	Autorizácia na základe roly používateľa
MIPS	2350	2700	2000	2700	2000
Výskyt nedostupnosti prostriedka	Bežný výskyt	Častý výskyt	Častý výskyt	Veľmi častý výskyt	Veľmi častý výskyt
Výskyt zlyhania vykonávania úlohy	Bežný výskyt	Častý výskyt	Častý výskyt	Veľmi častý výskyt	Veľmi častý výskyt

Tabuľka č. 7: Charakteristiky poskytovateľov zdieľaných prostriedkov (6 - 10) v simulovanej ad hoc gridovej infraštruktúre

titám predstavujúcich poskytovateľov zdieľaných prostriedkov. Po spustení simulácie sú tieto entity zodpovedné za vykonávanie používateľských úloh v závislosti od špecifikácie časovej náročnosti úlohy a veľkosti dát určených na spracovanie.

Nástroj GridSim neumožňuje, aby entity predstavujúce používateľov plánovali generované úlohy vlastným modulom plánovania. Tento nástroj definuje len jednu špeciálnu entitu, ktorá preberá zodpovednosť za plánovanie a vykonanie úloh. Simulačný model vykonáva plánovanie úloh teda len prostredníctvom jedného modulu plánovania úloh. Účelom simulačného modelu je však pozorovať dopad riadenia dôvery na správanie sa systému. Existencia iba jediného modulu plánovania úloh nijakým spôsobom neobmedzuje vykonanie samotnej simulácie.

Po vytvorení entít používateľov a poskytovateľov zdieľaných prostriedkov simulovaný modul plánovania úloh preberá od entít používateľov požiadavky na naplánovanie vykonania generovaných úloh. Plánovanie úloh sa uskutočňuje na základe postupu definovaného v sekcii 4.2. Modul plánovania úloh najskôr vyhľadá dostupné zdieľané prostriedky. Algoritmus plánovania úloh aplikovaný modulom plánovania má za cieľ optimalizovať čas vykonania plánovanej úlohy. Modul vyberie z dostupných prostriedkov ten, ktorý najviac optimalizuje čas vykonania. Pre tento zdieľaný prostriedok určí modul plánovania v spolupráci s modulom riadenia dôvery používateľa hodnotu požiadaviek na poskytovanú bezpečnosť a index dôvery zvoleného zdieľaného prostriedka. Tento postup opakuje modul plánovania tak dlho, kým nenájde dostatočne dôveryhodný zdieľaný prostriedok. Po nájdení dôveryhodného zdieľaného prostriedka je tento simulovaný prostriedok zodpovedný za určenie hodnoty jeho požiadaviek na bezpečnosť a index dôvery voči používateľovi. Ak je aj simulovaná entita používateľa dôveryhodná z pohľadu zdieľaného prostriedka, tak úloha je priradená modulom plánovania úloh tomuto prostriedku na vykonanie.

Stanovenie metrík. Stanovenie kvality navrhnutého riešenia overeného prostredníctvom počítačovej simulácie je uskutočnené na základe viacerých kvantitatívnych metrík. Metriky hodnotia najmä dve charakteristiky simulovanej ad hoc gridovej infraštruktúry: *(i)* kompetencia infraštruktúry *(ii)* a spoľahlivosť infraštruktúry.

Kompetencia infraštruktúry charakterizuje schopnosť simulovanej ad hoc gridovej infraštruktúry vykonávať úlohy generované entitami používateľov. Táto metrika má za cieľ zhodnotiť, akým spôsobom vplýva integrácia riadenia dôvery na proces plánovania úloh a na proces rozhodovania o vykonaní potencionálnych kolaborácií. Predpokladá sa, že integrácia riadenia dôvery neovplyvní zásadným spôsobom priepustnosť systému a ani celkový počet spracovaných úloh. Tento predpoklad je správny ale iba vtedy, ak systém obsahuje aj entity poskytovateľov zdieľaných prostriedkov správajúcich sa vždy kompetentne. Ako je uvedené v tabuľke č. 6, simulovaná ad hoc gridová infraštruktúra obsahuje hneď niekoľko takto kompetentne sa správajúcich entít. Hodnota kvantitatívnej metriky kompetencia sa určuje na základe celkového počtu vykonaných úloh uskutočnených počas počítačovej simulácie.

Spoľahlivosť infraštruktúry charakterizuje schopnosť simulovanej ad hoc gridovej infraštruktúry zabezpečiť bezpečné vykonávanie úloh generovaných entitami používateľov. Táto metrika má za cieľ zhodnotiť, akým spôsobom ovplyvní riadenie dôvery úspešnosť vykonávania úloh. Predpokladá sa, že integrácia riadenia dôvery do procesu rozhodovania o uskutočňovaní potencionálnych kolaborácií zlepší spoľahlivosť systému vykonávať používateľské úlohy. Tento predpoklad je správny ale iba vtedy, ak systém obsahuje entity poskytovateľov ako i používateľov správajúcich sa vždy korektne. Ako je uvedené v tabuľkách č. 6 a 4, simulovaná ad hoc gridová infraštruktúra obsahuje hneď niekoľko takto korektne sa správajúcich entít. Hodnota kvantitatívnej metriky spoľahlivosť sa určuje za základe celkového počtu neúspešne vykonaných úloh zaznamenaných počas počítačovej simulácie.

5.1.2 Priebeh overenia

Počítačová simulácia uskutočnená na základe simulačného modelu abstrahujúceho reálny systém umožňuje odhadnúť správanie sa reálneho systému. Simulácia modelovanej ad hoc gridovej infraštruktúry poskytuje informácie o trende správania sa entít používateľov, entít poskytovateľov zdieľaných prostriedkov a dopade riadenia dôvery na celkové fungovanie infraštruktúry. Počítačová platforma použitá pre vykonanie simulácie je charakterizovaná nasledovnými parametrami: operačný systém – *Windows Home Premium*, procesor – *Intel(R) Core(TM) i3-2310M @ 2.10GHz*, pamäť RAM - *4,00GB*.

Overenie navrhnutého riešenia pomocou počítačovej simulácie na základe navrhnutých metrík si vyžaduje vykonanie viacerých experimentov. Každému experimentu zodpovedá uskutočnená simulácia s rozdielnymi vstupnými parametrami simulačného modelu. Vykonané boli experimenty s dvoma typmi infraštruktúr: *(i)* ad hoc gridová infraštruktúra bez integrácie riadenia dôvery *(ii)* a ad hoc gridová infraštruktúra s integráciou riadenia dôvery. Porovnaním výsledkov oboch simulačných behov je možné určiť dopad riadenia dôvery na funkčnosť ad hoc gridovej infraštruktúry. Zároveň je možné stanoviť i kvalitu navrhnutého riešenia pomocou definovaných metrík.

Experiment č.1 - ad hoc gridová infraštruktúra bez integrácie riadenia dôvery. Experiment č. 1 je vykonaný ako počítačová simulácia, ktorá je uskutočnená na základe simulačného modelu nezahrňujúceho riadenie dôvery ako súčasť modelovanej ad hoc gridovej infraštruktúry. Simulácia poskytuje referenčné dáta o vlastnostiach ad hoc gridovej infraštruktúry, voči ktorým sú porovnané dáta získané z iných experimentov. Počas simulácie bolo uskutočnených 1000 simulačných behov. **Hodnoty namerané počas týchto behov sú uvádzané pre každý typ nameranej hodnoty (počet vykonaných, úspešných a neúspešných úloh) ako aritmetický priemer zaokrúhlený na dve desatinné miesta.**

Celkový počet uskutočnených úloh simulovanou ad hoc gridovou infraštruktúrou, počet úspešných úloh ako i počet neúspešne vykonaných úloh je uvedený v tabuľke č. 8. V danej tabuľke je uvedené aj percentuálne zastúpenie úspešne a neúspešne vykonaných úloh. Celkový počet uskutočnených úloh je 5833,10, úspešne vykonaných úloh je 4800,36 (83,67% zo všetkých úloh) a neúspešne vykonaných úloh je 952,74 (16,33% zo všetkých úloh). Neúspešne vykonané úlohy nastali z dôvodu výskytu viacerých druhov chýb. Počet neúspešných úloh podľa jednotlivých kategórií chýb ako i percentuálne zastúpenie týchto úloh z celkového počtu neúspešne vykonaných úloh sú uvedené v tabuľke č. 9.

Typ úlohy	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
Všetky uskutočnené úlohy	5833,10	100,00
Úspešne vykonané úlohy	4880,36	83,67
Neúspešne vykonané úlohy	952,74	16,33

Tabuľka č. 8: Počet všetkých úloh vykonaných bez integrácie riadenia dôvery

Typ úlohy	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
Žiadny zdieľaný prostriedok k dispozícii	0,00	0,00
Zdieľaný prostriedok nedostupný	238,90	25,00
Zlyhanie zdieľaného prostriedka	568,95	60,00
Chyba vykonávanej úlohy	144,90	15,00

Tabuľka č. 9: Počet neúspešných úloh podľa kategórie vyskytnutej chyby vykonaných bez integrácie riadenia dôvery

Tabuľky č. 10 až 12 popisujú charakteristiky používateľov simulovanej ad hoc gridovej

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
1	582,90	9,99
2	581,71	9,97
3	583,56	10,00
4	583,77	10,01
5	584,41	10,02
6	584,28	10,02
7	583,75	10,01
8	582,72	9,99
9	583,98	10,01
10	582,05	9,98

Tabuľka č. 10: Počet všetkých používateľských úloh vykonaných bez integrácie riadenia dôvery

infraštruktúry. Ako vidno v tabuľke č. 10, počet používateľských úloh spracovaných ad hoc gridovou infraštruktúrou je takmer rovnaký pre každého používateľa. Jednotliví používatelia sa ale odlišujú v počte úloh vykonaných úspešne a neúspešne (tabuľky č. 11 a 12). Rozdiely medzi používateľmi sú dôsledkom určeného správania sa týchto používateľov popísaného v tabuľkách č. 4 a 5 (charakteristika "výskyt chybných úloh"). Čím viac chybných úloh entita používateľa generuje, tým viac neúspešne vykonaných úloh používateľ aj zaznamená. Najmarkantnejší rozdiel v tomto prípade badať medzi používateľmi 1 a 10, kde je rozdiel v počte úspešných úloh 51,37 a neúspešných úloh 50,52.

Charakteristiky poskytovateľov zdieľaných prostriedkov sú uvedené v tabuľkách č. 13 až 15. Ako vidno v tabuľke č. 13, v prípade entít poskytovateľov zdieľaných prostriedkov je možné badať značný rozdiel medzi počtom úloh spracovaných jednotlivými zdieľanými prostriedkami. Tieto rozdiely medzi prostriedkami sú dôsledkom určeného správania sa týchto prostriedkov popísaného v tabuľkách č. 6 a 7 (charakteristika "MIPS"). Čím viac inštrukcií za sekundu dokáže zdieľaný prostriedok vykonať, tým viac úloh počas simulácie tento prostriedok aj spracoval. Najviac úloh spracovali prostriedky 9, 7 a 1. Najmenej

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet úspešných úloh	Podiel z úspešných úloh [v %]
1	503,00	10,31
2	493,98	10,12
3	493,91	10,12
4	496,56	10,17
5	491,69	10,07
6	495,32	10,15
7	491,34	10,07
8	488,62	10,01
9	474,32	9,72
10	451,63	9,25

Tabuľka č. 11: Počet úspešných používateľských úloh vykonaných bez integrácie riadenia dôvery

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
1	79,90	8,39
2	87,73	9,21
3	89,65	9,41
4	87,21	9,15
5	92,72	9,73
6	88,96	9,34
7	92,41	9,70
8	94,10	9,88
9	109,66	11,51
10	130,42	13,69

Tabuľka č. 12: Počet neúspešných používateľských úloh vykonaných bez integrácie riadenia dôvery

Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
1	762,68	13,07
2	570,79	9,79
3	321,17	5,51
4	571,81	9,80
5	554,21	9,50
6	553,22	9,48
7	775,88	13,30
8	322,48	5,53
9	1004,85	17,23
10	396,03	6,79

Tabuľka č. 13: Počet všetkých úloh vykonaných zdieľaným prostriedkom bez integrácie riadenia dôvery

úloh spracovali prostriedky 3, 8 a 10. Zdieľaný prostriedok 9 zaznamenal veľký počet spracovaných úloh z dôvodu vysokej hodnoty charakteristiky "MIPS" a zároveň z dôvodu aplikovaného algoritmu plánovania úloh. Algoritmus plánovania optimalizuje čas vykonania plánovanej úlohy. Algoritmus vyberá pri plánovaní taký zdieľaný prostriedok, ktorý je schopný vykonávať vysoký počet inštrukcií za sekundu a zároveň nie je zaťažený úlohami čakajúcimi vo fronte pripravených úloh. Fronta pripravených úloh je ale v prípade výpadku prostriedka vyprázdnená. Po skončení výpadku sa prostriedok stáva atraktívny pre modul plánovania úloh vďaka vysokej hodnote charakteristiky "MIPS" a prázdnemu frontu pripravených úloh. Tabuľky č. 14 a 15 uvádzajú počet úspešne a neúspešne vykonaných úloh spracovaných jednotlivými zdieľanými prostriedkami. Najviac úspešných úloh spracovali prostriedky 1 a 7, najmenej úspešných úloh spracovali prostriedky 10, 8 a 3. Najviac neúspešných úloh bolo zaznamenaných na zdieľaných prostriedkoch 9 a 10, čo zodpovedá forme správania sa popísanej v tabuľke č. 6 a 7 (charakteristiky "výskyt nedostupnosti prostriedka" a "výskyt zlyhania vykonávania úlohy").

Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet úspešných úloh	Podiel z úspešných úloh [v %]
1	742,30	15,21
2	554,91	11,37
3	311,25	6,38
4	552,38	11,32
5	532,98	10,92
6	526,09	10,78
7	690,33	14,15
8	278,26	5,70
9	548,42	11,24
10	143,46	2,94

Tabuľka č. 14: Počet úspešných úloh vykonaných zdieľaným prostriedkom bez integrácie riadenia dôvery

Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
1	20,38	2,14
2	15,88	1,67
3	9,92	1,04
4	19,43	2,04
5	21,24	2,23
6	27,13	2,85
7	85,56	8,98
8	44,22	4,64
9	456,43	47,91
10	252,57	26,51

Tabuľka č. 15: Počet neúspešných úloh vykonaných zdieľaným prostriedkom bez integrácie riadenia dôvery

Experiment č.2 - ad hoc gridová infraštruktúra s integrovaným riadením dôvery. Experiment č. 2 je vykonaný ako počítačová simulácia, ktorá je uskutočnená na základe simulačného modelu zahrňujúceho riadenie dôvery ako súčasť modelovanej ad hoc gridovej infraštruktúry. Počas simulácie bolo uskutočnených celkovo 1000 simulačných behov. **Hodnoty namerané počas týchto behov sú uvádzané pre každý typ nameranej hodnoty (počet vykonaných, úspešných a neúspešných úloh) ako aritmetický priemer zaokrúhlený na dve desatinné miesta.**

Celkový počet uskutočnených úloh simulovanou ad hoc gridovou infraštruktúrou, počet úspešných úloh ako i počet neúspešne vykonaných úloh je uvedený v tabuľke č. 16. V danej tabuľke je uvedené aj percentuálne zastúpenie úspešne a neúspešne vykonaných úloh. Celkový počet uskutočnených úloh je 5829,20, počet úspešne vykonaných úloh je 5292,12 (90,79% zo všetkých úloh) a počet neúspešne vykonaných úloh je 537,09 (9,21% zo všetkých úloh). Neúspešne vykonané úlohy nastali z dôvodu výskytu viacerých druhov chýb. Počet neúspešných úloh podľa jednotlivých kategórií chýb ako i percentuálne zastúpenie týchto úloh z celkového počtu neúspešne vykonaných úloh sú uvedené v tabuľke č. 17. V prípade experimentu s integráciou riadenia dôvery nastalo niekoľko prípadov, kedy nebol nájdený žiadny zdieľaný prostriedok pre spracovanie úlohy z dôvodu nedôvery medzi používateľom a poskytovateľom zdieľaného prostriedka.

Typ úlohy	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
Všetky uskutočnené úlohy	5829,20	100,00
Úspešne vykonané úlohy	5292,12	90,79
Neúspešne vykonané úlohy	537,09	9,21

Tabuľka č. 16: Počet všetkých úloh vykonaných s integráciu riadenia dôvery

Typ úlohy	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
Žiadny zdieľaný prostriedok k dispozícii	1,12	0,21
Zdieľaný prostriedok nedostupný	109,05	20,03
Zlyhanie zdieľaného prostriedka	274,07	51,03
Chyba vykonávanej úlohy	152,86	28,46

Tabuľka č. 17: Počet neúspešných úloh podľa kategórie vyskytnutej chyby vykonaných s integráciou riadenia dôvery

Tabuľky č. 18 až 20 popisujú charakteristiky používateľov simulovanej ad hoc gridovej infraštruktúry. Ako vidno v tabuľke č. 18, tak počet používateľských úloh je takmer rovnaký pre každého používateľa. Používatelia sa znova odlišujú v počte úspešne a neúspešne vykonaných úloh (tabuľky č. 19 a 20). Najmarkantnejší rozdiel nameraný počas experimentu č. 2 vidno medzi používateľmi 1 a 10, kde je rozdiel v počte úspešných úloh 53,51 a neúspešných úloh 50,58.

Charakteristiky poskytovateľov zdieľaných prostriedkov sú uvedené v tabuľkách č. 21 až 23. Ako vidno v tabuľke č. 21, v prípade entít poskytovateľov zdieľaných prostriedkov je možné badať značný rozdiel medzi počtom úloh spracovaných jednotlivými zdieľanými prostriedkami. Tieto rozdiely medzi zdieľanými prostriedkami sú dôsledkom určeného správania sa týchto prostriedkov popísaného v tabuľkách č. 6 a 7 (charakteristika "MIPS"). Čím viac inštrukcií za sekundu dokáže zdieľaný prostriedok vykonať, tým viac úloh počas simulácie tento prostriedok aj spracoval. Najviac úloh spracovali prostriedky 9, 7 a 1. Najmenej úloh spracovali prostriedky 10, 3 a 8. I v prípade experimentu č. 2 platí, že zdieľaný prostriedok 9 zaznamenal taký veľký počet spracovaných úloh z dôvodu vysokej hodnoty charakteristiky "MIPS" a zároveň z dôvodu aplikovaného algo-

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
1	582,19	9,99
2	582,24	9,99
3	578,09	9,92
4	591,44	10,15
5	586,79	10,07
6	583,83	10,02
7	578,83	9,93
8	582,73	10,00
9	583,82	10,02
10	579,27	9,94

Tabuľka č. 18: Počet všetkých používateľských úloh vykonaných s integráciou riadenia dôvery

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet úspešných úloh	Podiel z úspešných úloh [v %]
1	541,23	10,23
2	537,61	10,16
3	533,93	10,09
4	549,24	10,38
5	538,39	10,17
6	536,08	10,13
7	530,75	10,03
8	519,31	9,81
9	517,89	9,79
10	487,72	9,22

Tabuľka č. 19: Počet úspešných používateľských úloh vykonaných s integráciou riadenia dôvery

Používateľ	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
1	40,97	7,63
2	44,63	8,31
3	44,16	8,22
4	42,20	7,86
5	48,41	9,01
6	47,75	8,89
7	48,08	8,95
8	63,43	11,81
9	65,93	12,28
10	91,55	17,05

Tabuľka č. 20: Počet neúspešných používateľských úloh vykonaných s integráciou riadenia dôvery

ritmu plánovania úloh. Algoritmus vyberá pri plánovaní taký zdieľaný prostriedok, ktorý je schopný vykonávať vysoký počet inštrukcií za sekundu a zároveň tento prostriedok nie je zaťažený úlohami čakajúcimi vo fronte pripravených úloh. Fronta pripravených úloh je ale v prípade výpadku prostriedka vyprázdnená. Po skončení výpadku sa prostriedok stáva atraktívny pre modul plánovania úloh vďaka vysokej hodnote charakteristiky "MIPS" a prázdnemu frontu pripravených úloh. Tabuľky č. 22 a 23 uvádzajú počet úspešne a neúspešne vykonaných úloh spracovanými jednotlivými zdieľanými prostriedkami. Najviac úspešných úloh spracovali prostriedky 1 a 7, najmenej úspešných úloh spracovali prostriedky 10, 8 a 3. Najviac neúspešných úloh bolo zaznamenaných na zdieľaných prostriedkoch 9 a 7, najmenej neúspešných úloh bolo zaznamenaných na zdieľaných prostriedkoch 3, 2, 1 a 5.

Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet vykonaných úloh	Podiel z vykonaných úloh [v %]
1	786,36	13,49
2	583,57	10,01
3	325,84	5,59
4	595,13	10,21
5	588,81	10,10
6	598,62	10,27
7	844,78	14,49
8	354,53	6,08
9	955,31	16,39
10	195,16	3,35

Tabuľka č. 21: Počet všetkých úloh vykonaných zdieľaným prostriedkom s integráciou riadenia dôvery

Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet úspešných úloh	Podiel z úspešných úloh [v %]
1	761,93	14,40
2	567,60	10,73
3	317,16	5,99
4	572,72	10,82
5	563,36	10,65
6	564,38	10,66
7	726,99	13,74
8	303,74	5,74
9	765,45	14,46
10	148,81	2,81

Tabuľka č. 22: Počet úspešných úloh vykonaných zdieľaným prostriedkom s integráciou riadenia dôvery

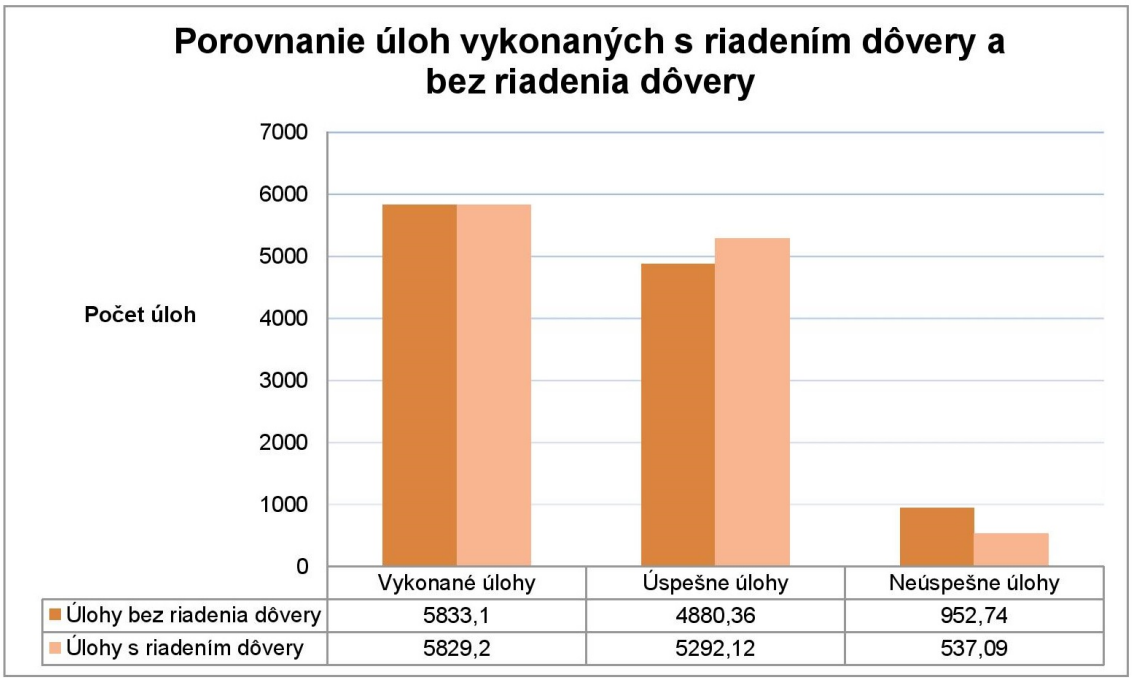
Zdieľaný prostriedok	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
1	24,43	4,55
2	15,97	2,95
3	8,68	1,62
4	22,41	4,17
5	25,45	4,74
6	32,24	6,38
7	117,79	21,93
8	50,80	9,46
9	189,86	35,35
10	46,35	8,63

Tabuľka č. 23: Počet neúspešných úloh vykonaných zdieľaným prostriedkom s integráciou riadenia dôvery

5.1.3 Výsledky overenia

Zhodnotenie kvality navrhnutého riešenia je vykonané na základe metrík, ktorých hodnoty boli namerané počas experimentov popísaných v sekcii 5.1.2. **Kompetencia** ako metrika hodnotiaca schopnosť simulovanej ad hoc gridovej infraštruktúry vykonávať úlohy je meraná ako celkový počet úloh vykonaných počas počítačovej simulácie. V rámci experimentu č. 1 bez integrácie riadenia dôvery do ad hoc gridovej infraštruktúry bol zistený nasledovný 95% interval spoľahlivosti pre celkový počet vykonaných úloh (5826,77;5839,43). V rámci experimentu č. 2 s integráciou riadenia dôvery do ad hoc gridovej infraštruktúry bol zistený nasledovný 95% interval spoľahlivosti pre celkový počet vykonaných úloh (5823,06;5835,34). Porovnaním stredných hodnôt týchto intervalov (viď graf na obrázku č. 8) je zrejmé, že kompetencia ad hoc gridovej infraštruktúry ostáva aj pri integrácii riadenia dôvery nepozmenená.

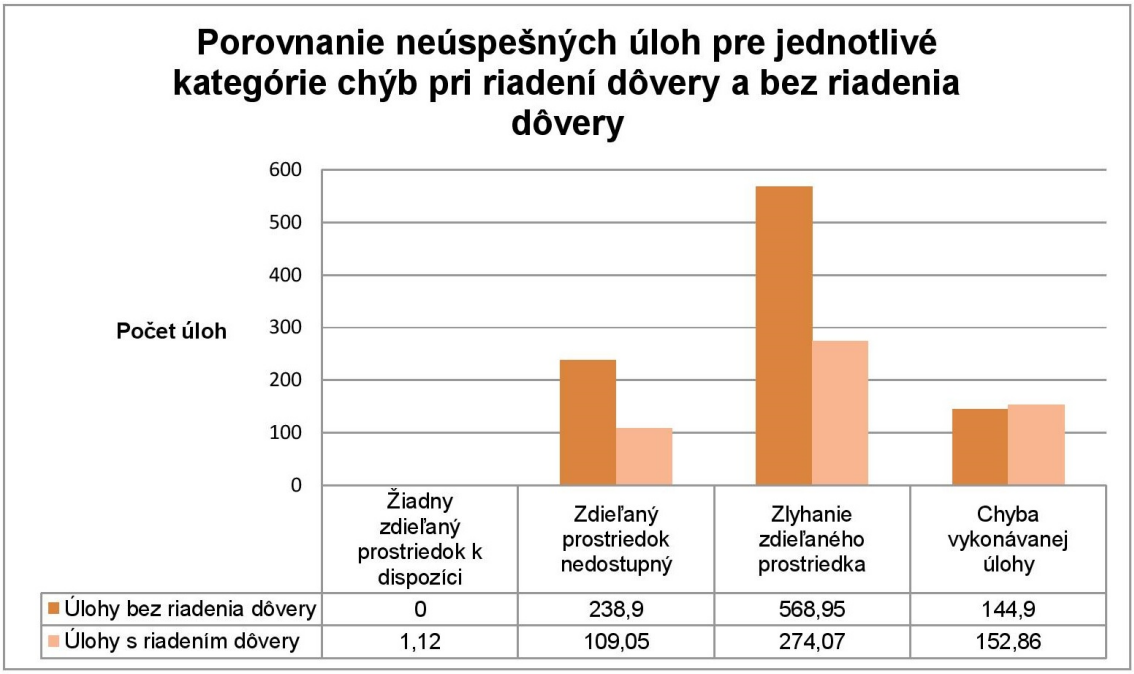
Spoľahlivosť ako metrika hodnotiaca schopnosť simulovanej ad hoc gridovej infraštruktúry zaistiť bezpečné vykonávanie úloh je meraná ako počet neúspešných úloh



Obrázok č. 8: Kompetencia a spoľahlivosť ad hoc gridovej infraštruktúry vyjadrená počtom vykonaných úloh bez riadenia dôvery a s riadením dôvery

zaznamenaných počas počítačovej simulácie. V rámci experimentu č. 1 bez integrácie riadenia dôvery do ad hoc gridovej infraštruktúry bol zistený nasledovný 95% interval spoľahlivosti pre počet neúspešne vykonaných úloh (923,74;981,74). V rámci experimentu č. 2 s integráciou riadenia dôvery do ad hoc gridovej infraštruktúry bol zistený nasledovný 95% interval spoľahlivosti pre počet neúspešne vykonaných úloh (527,38;546,80). Porovnaním stredných hodnôt týchto intervalov (viď graf na obrázku č. 8) je zrejmé, že spoľahlivosť ad hoc gridovej infraštruktúry sa integráciou riadenia dôvery zlepší. Počet neúspešných úloh bez integrácie riadenia dôvery bol 952,74, v prípade integrácie riadenia dôvery bol počet neúspešných úloh 537,09. Spoľahlivosť simulovanej ad hoc gridovej infraštruktúry sa integráciou riadenia dôvery zlepšila o 43,62%.

Vyhodnotenie metrík jednoznačne ukázalo, že navrhované riešenie zachováva kompetenciu ad hoc gridovej infraštruktúry a zároveň zlepšuje spoľahlivosť danej infraštruktúry. Zlepšenie spoľahlivosti sa prejavilo v poklese počtu neúspešných úloh. Porovnanie výskytu neúspešných úloh podľa jednotlivých kategórií chýb je znázornené grafom

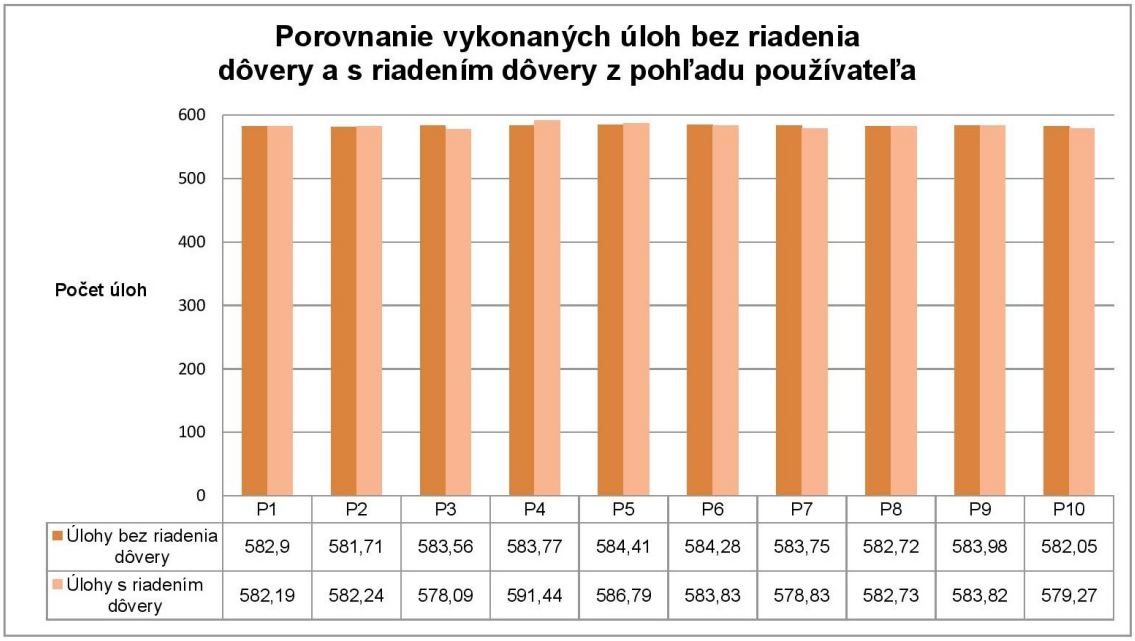


Obrázok č. 9: Porovnanie neúspešných úloh pre jednotlivé kategórie bez riadenia dôvery a s riadením dôvery

na obrázku č. 9. Značný pokles výskytu chýb bol zaznamenaný pre nedostupnosť zdieľaného prostriedka a zlyhanie zdieľaného prostriedka. Mierny nárast zaznamenali chyby spojené s nenájdením dôveryhodného zdieľaného prostriedka a chyby spôsobené chybnými používateľskými úlohami.

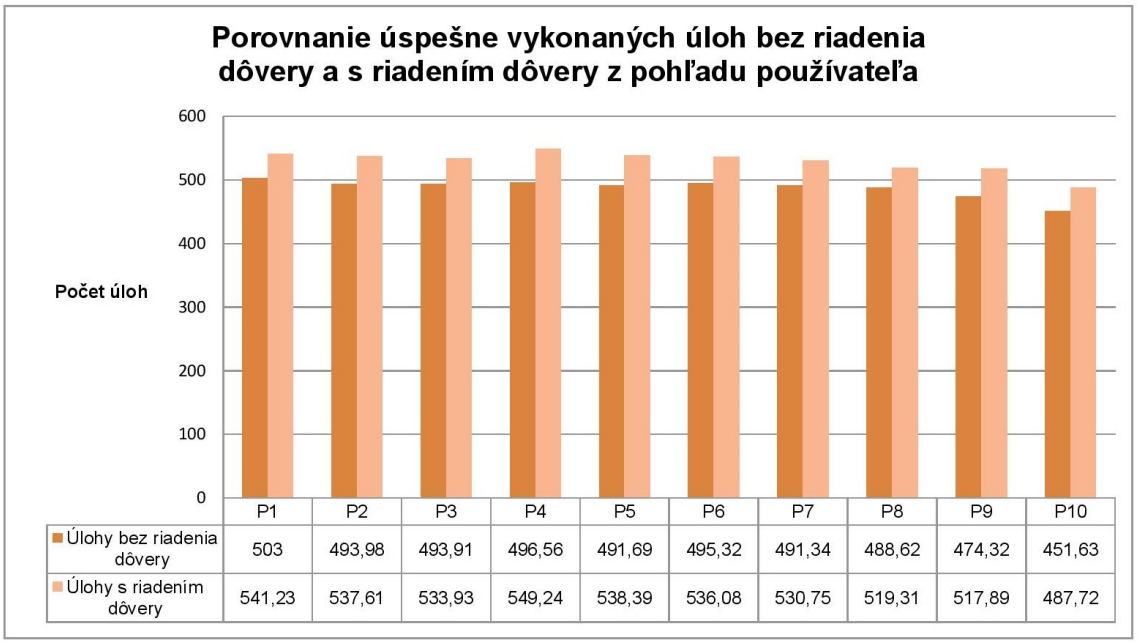
Grafy na obrázkoch č. 10 až 12 zobrazujú porovnanie počtu vykonaných, úspešných a neúspešných úloh z pohľadu používateľov ad hoc gridovej infraštruktúry. Graf zobrazený na obrázku č. 10 znázorňuje, že celkový počet spracovaných úloh pre každého používateľa je takmer totožný pre oba vykonané experimenty. Kompetencia ad hoc gridovej infraštruktúry je teda z pohľadu používateľov rovnaká aj v prípade integrácie riadenia dôvery. Graf na obrázku č. 11 znázorňuje, že používatelia zaznamenali v prípade integrácie riadenia dôvery väčší počet úspešných úloh ako v prípade bez integrácie riadenia dôvery. Spoľahlivosť ad hoc gridovej infraštruktúry vyjadrená počtom neúspešných úloh je v prípade časti používateľov lepšia približne o polovicu (viď graf na obrázku č. 12).

Grafy na obrázkoch č. 13 až 15 zobrazujú porovnanie počtu vykonaných, úspešných



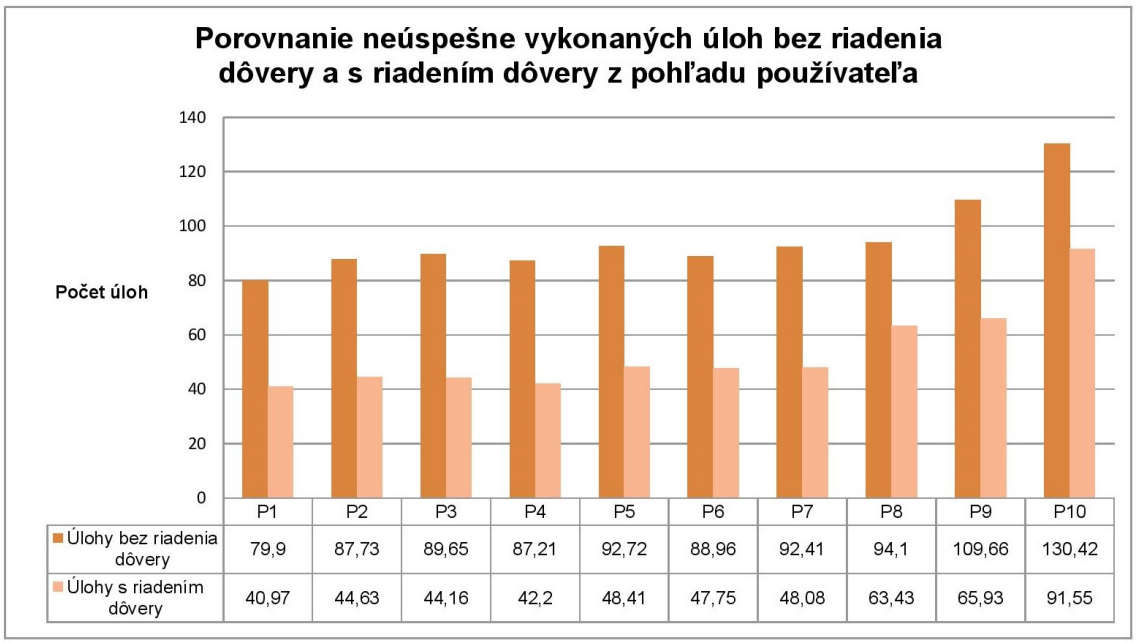
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Úlohy bez riadenia dôvery	582,9	581,71	583,56	583,77	584,41	584,28	583,75	582,72	583,98	582,05
Úlohy s riadením dôvery	582,19	582,24	578,09	591,44	586,79	583,83	578,83	582,73	583,82	579,27

Obrázok č. 10: Porovnanie úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu používateľa ad hoc gridovej infraštruktúry



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Úlohy bez riadenia dôvery	503	493,98	493,91	496,56	491,69	495,32	491,34	488,62	474,32	451,63
Úlohy s riadením dôvery	541,23	537,61	533,93	549,24	538,39	536,08	530,75	519,31	517,89	487,72

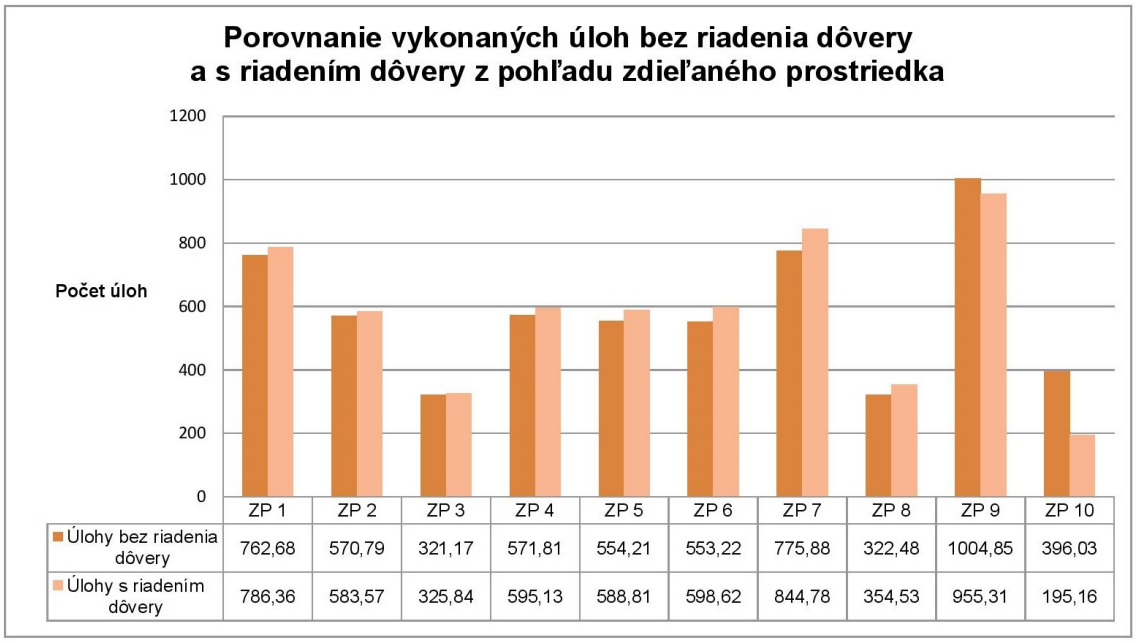
Obrázok č. 11: Porovnanie úspešných úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu používateľa ad hoc gridovej infraštruktúry



	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Úlohy bez riadenia dôvery	79,9	87,73	89,65	87,21	92,72	88,96	92,41	94,1	109,66	130,42
Úlohy s riadením dôvery	40,97	44,63	44,16	42,2	48,41	47,75	48,08	63,43	65,93	91,55

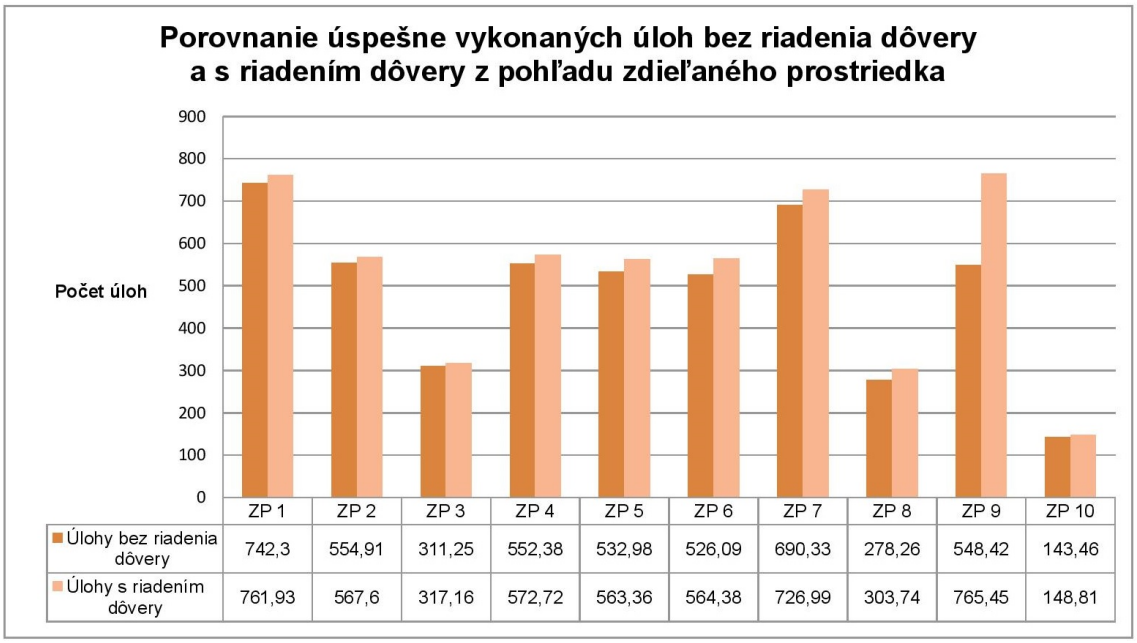
Obrázok č. 12: Porovnanie neúspešných úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu používateľa ad hoc gridovej infraštruktúry

a neúspešných úloh z pohľadu jednotlivých zdieľaných prostriedkov ad hoc gridovej infraštruktúry. Ako vidno na grafe zobrazenom na obrázku č. 13, tak v prípade prostriedkov (1 až 8) so žiadnym alebo menším výskytom chýb a zlyhaní vzrástol počet celkovo spracovaných úloh. V prípade zdieľaných prostriedkov (9 a 10) s väčším výskytom chýb a zlyhaní celkový počet spracovaných úloh poklesol. Graf na obrázku č. 14 znázorňuje počet úspešných úloh spracovaných jednotlivými zdieľanými prostriedkami. Každý zdieľaný prostriedok zaznamenal v prípade integrácie riadenia dôvery väčší počet úspešných úloh ako v prípade bez integrácie riadenia dôvery. Ako vidno na grafe zobrazenom na obrázku č. 15, spoľahlivosť jednotlivých zdieľaných prostriedkov sa zhoršila v prípade integrácie riadenia dôvery u niektorých prostriedkov len minimálne. Toto zhoršenie je spôsobené nárastom celkového počtu úloh, ktoré tieto zdieľané prostriedky spracovali. Najväčšie zlepšenie zaznamenali tie zdieľané prostriedky, ktoré sa vyznačujú častým výskytom chýb z dôvody nedostupnosti zdieľaného prostriedka alebo zlyhania zdieľaného prostriedka.



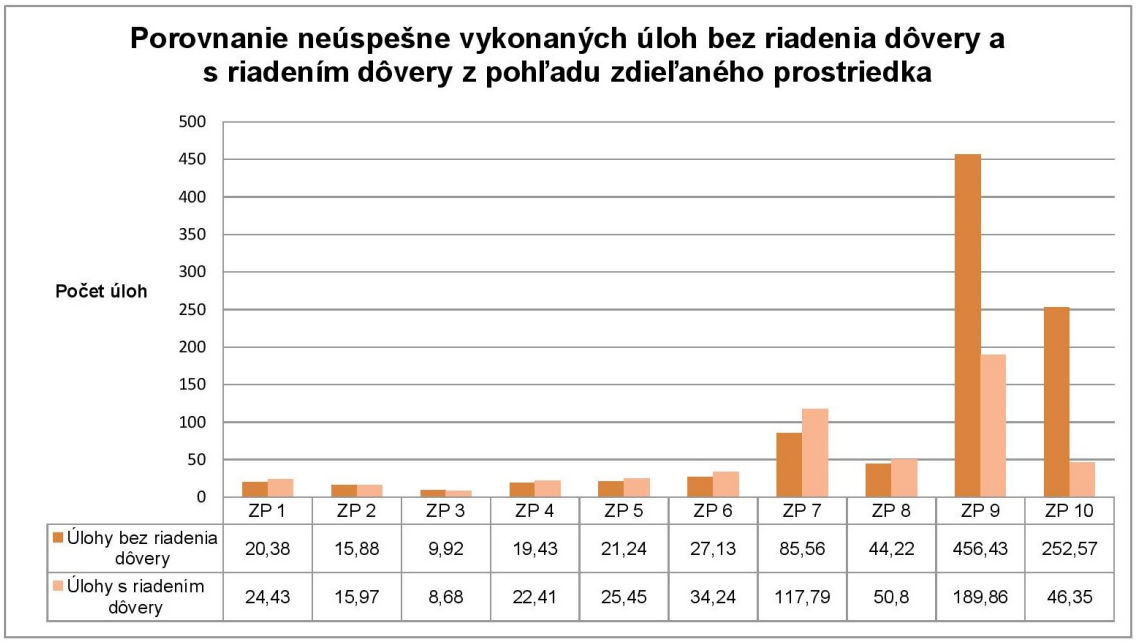
	ZP 1	ZP 2	ZP 3	ZP 4	ZP 5	ZP 6	ZP 7	ZP 8	ZP 9	ZP 10
Úlohy bez riadenia dôvery	762,68	570,79	321,17	571,81	554,21	553,22	775,88	322,48	1004,85	396,03
Úlohy s riadením dôvery	786,36	583,57	325,84	595,13	588,81	598,62	844,78	354,53	955,31	195,16

Obrázok č. 13: Porovnanie úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu prostriedkov zdieľaných v ad hoc gridovej infraštruktúre



	ZP 1	ZP 2	ZP 3	ZP 4	ZP 5	ZP 6	ZP 7	ZP 8	ZP 9	ZP 10
Úlohy bez riadenia dôvery	742,3	554,91	311,25	552,38	532,98	526,09	690,33	278,26	548,42	143,46
Úlohy s riadením dôvery	761,93	567,6	317,16	572,72	563,36	564,38	726,99	303,74	765,45	148,81

Obrázok č. 14: Porovnanie úspešných úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu prostriedkov zdieľaných v ad hoc gridovej infraštruktúre



	ZP 1	ZP 2	ZP 3	ZP 4	ZP 5	ZP 6	ZP 7	ZP 8	ZP 9	ZP 10
Úlohy bez riadenia dôvery	20,38	15,88	9,92	19,43	21,24	27,13	85,56	44,22	456,43	252,57
Úlohy s riadením dôvery	24,43	15,97	8,68	22,41	25,45	34,24	117,79	50,8	189,86	46,35

Obrázok č. 15: Porovnanie neúspešných úloh vykonaných s integráciou riadenia dôvery a bez integrácie riadenia dôvery z pohľadu prostriedkov zdieľaných v ad hoc gridovej infraštruktúre

5.2 Zhodnotenie dosiahnutých výsledkov

Bezpečnosť poskytovaná ad hoc gridovou infraštruktúrou jej používateľom ako i poskytovateľom zdieľaných prostriedkov je jedným zo základných faktorov akceptácie tejto infraštruktúry širokou verejnosťou. Cieľom práce je rozšírenie poskytovanej bezpečnosti prostredníctvom riadenia dôvery. Nasledujúce sekcie sa venujú zhodnoteniu dosiahnutia stanoveného cieľa, ale i zhodnoteniu vedeckého prínosu práce a načrtnutiu nevyriešených otázok a problémov ponechaných pre ďalší výskum.

5.2.1 Splnenie stanovených cieľov

Cieľ práce bol definovaný ako požiadavka na integráciu riadenia dôvery do bezpečnostnej infraštruktúry ad hoc gridovej technológie. Toto rozšírenie bezpečnosti malo umožniť používateľom ad hoc gridovej infraštruktúry ako i poskytovateľom zdieľajúcich svoje prostriedky v rámci infraštruktúry vykonávať rozhodnutia o uskutočnení potencionálnych

kolaborácií.

Práca obsahuje v sekcii 4.2 návrh modulu riadenia dôvery, ktorý spolu s modulom plánovania úloh integrujú rozhodovanie o vykonaní potencionálnej kolaborácie na základe dôveryhodnosti medzi účastníkmi tejto kolaborácie. Účastníci potencionálnej kolaborácie určujú dôveryhodnosť na základe rôznych systémových parametrov a parametrov popisujúcich správanie sa účastníkov kolaborácie. Práca v sekcii 4.1 klasifikuje parametre, ktoré sú súčasťou výslednej hodnoty dôvery. Táto sekcia taktiež popisuje jednotlivé parametre, udáva vzťahy medzi parametrami a špecifikuje spôsob výpočtu dôveryhodnosti účastníka potencionálnej kolaborácie.

Vhodnosť navrhnutého riešenia zodpovedajúceho stanovenému cieľu bola overená experimentálne pomocou počítačovej simulácie. Vyhodnotenie experimentov metrikami určenými v sekcii 5.1.3 ukázalo, že navrhnutá integrácia riadenia dôvery do ad hoc gridovej infraštruktúry zachováva kompetenciu infraštruktúry vykonávať používateľské úlohy. Vyhodnotenie zároveň preukázalo, že spoľahlivosť ad hoc gridovej infraštruktúry sa navrhnutou integráciou riadenia dôvery zlepší. **Hlavný cieľ práce a čiastkové ciele práce boli splnené**.

5.2.2 Vedecký prínos

Problematika poskytovania bezpečnosti v rámci ad hoc gridovej infraštruktúry rozšírenej o riadenie dôvery je známa, ale v súčasnosti ešte nie je dobre špecifikovaná a ani popísaná. Prínos práce spočíva práve v rozsiahlom súhrne súčasného stavu poskytovania bezpečnosti, popísaní rozdielov medzi riešeniami uplatňovanými tradičnou a ad hoc gridovou infraštruktúrou ako i v definovaní pojmu dôvera v kontexte ad hoc gridovej technológie.

Hlavným prínosom práce je návrh riešenia vyvarujúceho sa nedostatkov súčasných modelov výpočtu hodnoty dôvery medzi účastníkmi kolaborácie. Navrhované riešenie rešpektuje právo používateľov ako i poskytovateľov zdieľaných prostriedkov vykonávať

rozhodnutia o vykonaní alebo nevykonaní kolaborácií. Tieto rozhodnutia sú pritom vykonané na základe dôveryhodnosti medzi účastníkmi vypočítanej z viacerých parametrov. Navrhované riešenie na rozdiel od súčasných modelov dôvery poskytuje rozsiahlu špecifikáciu parametrov tvoriacich súčasť výslednej hodnoty dôvery. Riešenie taktiež definuje vzťahy medzi parametrami a poskytuje popis metódy výpočtu hodnoty dôvery.

5.2.3 Pokračovanie vo výskume

Navrhované riešenie definuje, že dôveryhodnosť účastníkov kolaborácií sprostredkovaných ad hoc gridovou infraštruktúrou sa určuje na základe viacerých typov parametrov. Na prvý pohľad sa môže zdať, že určovanie hodnôt týchto parametrov je pre používateľov a poskytovateľov zdieľaných prostriedkov zložité. Ako vidno na obrázkoch č. 5 a 6, veľkú časť uvažovaných parametrov je možné získať odvodením z meraných parametrov. V prípade výpočtu hodnoty indexu dôvery sú hodnoty meraných parametrov určené priamočiaro na základe parametrov zodpovedajúcich pozorovaným formám správania sa účastníkov kolaborácie a parametrov popisujúcich systém týchto účastníkov. Meranie hodnôt týchto parametrov je ponechané na ad hoc gridovú infraštruktúru. Úlohou pre ďalší výskum je definovanie mechanizmu, ktorým infraštruktúra zabezpečí meranie systémových informácií a informácií o pozorovaných formách správania sa. V prípade výpočtu hodnoty požiadaviek na poskytovanú bezpečnosť sú hodnoty meraných parametrov určované na základe preferencií samotných používateľov a poskytovateľov zdieľaných prostriedkov. Túto problematiku riešia do istej miery už Dionysiou a Gjermundrod vo svojej práci [44]. Pre účely navrhovanej integrácie riadenia dôvery je úlohou pre ďalší výskum definovanie mechanizmu, ktorým ad hoc gridová infraštruktúra zabezpečí jednoduché a používateľsky priateľské definovanie preferencií zodpovedajúcich hodnotám parametrov definujúcich riziko a neistotu.

Graf na obrázku č. 9 zobrazuje, že integrácia riadenia dôvery má pozitívny dopad

na zníženie počtu chýb súvisiacich so zlyhaním zdieľaných prostriedkov. Integrácia riadenia dôvery však nezabezpečila zníženie počtu chýb spôsobených chybnými používateľskými úlohami. Úlohou pre ďalší výskum je určiť príčiny tohto nedostatku riešenia a vyriešiť ho buď doplnením definovaných parametrov alebo zmenou váh určujúcich veľkosť vplyvu parametrov na dôveryhodnosť používateľov. Úlohou pre ďalší výskum je zároveň aj úprava váh parametrov majúcich vplyv na dôveryhodnosť poskytovateľov zdieľaných prostriedkov. Úprava váh má za úlohu ešte vo väčšej miere zlepšiť spoľahlivosť ad hoc gridovej infraštruktúry.

Kapitola 6

Zhrnutie a záver

Ad hoc gridová infraštruktúra bola navrhnutá ako prostriedok podporujúci krátkodobé a sporadické kolaborácie. Prijatie tejto infraštruktúry širokou verejnosťou ako výpočtového prostriedka je však podmienené implementáciou nevyhnutných funkčných prvkov ako sú správa zdieľaných prostriedkov, plánovanie vykonávania úloh, monitorovanie vykonávania úloh, zabezpečenie bezpečného vykonania úloh ako i zabezpečenie sprostredkovanej kolaborácie. Práca rozoberá súčasný stav poskytovania bezpečnosti ad hoc gridovou infraštruktúrou a pomenúva nedostatky známych riešení. Práca taktiež obsahuje návrh riešenia, ktoré má za cieľ zlepšiť poskytovanie bezpečnosti ad hoc gridovou infraštruktúrou prostredníctvom integrácie riadenia dôvery. Navrhnuté riešenie bolo overené pomocou počítačovej simulácie jednoznačne preukazúcej vhodnosť navrhnutého riešenia. Nasadenie navrhnutého riešenia v praxi si vyžaduje i napriek vhodnosti riešenia ďalšie pokračovanie vo výskume. Oblasť ďalšieho výskumu sa pritom zameriava na vylepšenie navrhnutého riešenia a jednoduchosť implementácie riešenia existujúcimi ad hoc gridovými infraštruktúrami.

Zoznam použitej literatúry

[1] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *Int. J. High Perform. Comput. Appl.*, vol. 15, pp. 200–222, Aug. 2001.

[2] I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam, J. Treadwell, and J. Von Reich, "The open grid services architecture, version 1.5," July 2006.

[3] P. G. S. Tiburcio and M. A. Spohn, "Ad hoc grid: An adaptive and self-organizing peer-to-peer computing grid.," in *IEEE 10th International Conference on Computer and Information Technology (CIT)*, pp. 225–232, IEEE Computer Society, 2010.

[4] K. Amin, G. von Laszewski, and A. R. Mikler, "Toward an architecture for ad hoc grids," in *12th International Conference on Advanced Computing and Communications (ADCOM 2004), Ahmedabad*, pp. 15–18, 2004.

[5] N. Andrade, L. Costa, G. Germóglio, and W. Cirne, "Peer-to-peer grid computing with the ourgrid community," in *23rd Brazilian Symposium on Computer Networks (SBRC 2005) - 4th Special Tools Session*, 2005.

[6] A. Gomes, A. Ziviani, L. Lima, and M. Endler, "Performance evaluation of a discovery and scheduling protocol for multihop ad hoc mobile grids," *Journal of the Brazilian Computer Society*, vol. 15, no. 4, pp. 15–29, 2009.

[7] A. Jøsang, C. Keser, and T. Dimitrakos, "Can we manage trust?," in *Trust Management*, vol. 3477 of *Lecture Notes in Computer Science*, pp. 93–107, Springer Berlin Heidelberg, 2005.

[8] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, pp. 618–644, mar 2007.

[9] J. Shi, G. v. Bochmann, and C. Adams, "A trust model with statistical foundation," in *Formal Aspects in Security and Trust*, vol. 173 of *IFIP International Federation for Information Processing*, pp. 145–158, Springer US, 2005.

[10] S. Song, K. Hwang, and M. Macwan, "Fuzzy trust integration for security enforcement in grid computing," in *Network and Parallel Computing*, vol. 3222 of *Lecture Notes in Computer Science*, pp. 9–21, Springer Berlin Heidelberg, 2004.

[11] S. Song, K. Hwang, and Y.-K. Kwok, "Trusted grid computing with security binding and trust integration," *Journal of Grid Computing*, vol. 3, no. 1-2, pp. 53–73, 2005.

[12] F. Azzedin and M. Maheswaran, "Evolving and managing trust in grid computing systems," in *Canadian Conference on Electrical and Computer Engineering, 2002.*, vol. 3, pp. 1424–1429, 2002.

[13] C. Ding, Y. Fu, Z. Hu, and P. Xiao, "A novel trust model based on bayesian network for service-oriented grid," in *Eighth IEEE/ACIS International Conference on Computer and Information Science, 2009.*, pp. 494–499, June 2009.

[14] T. Ryutov, L. Zhou, C. Neuman, N. Foukia, T. Leithead, and K. E. Seamons, "Adaptive trust negotiation and access control for grids," in *GRID*, pp. 55–62, IEEE, 2005.

[15] C. English, S. Terzis, and W. Wagealla, "Engineering trust based collaborations in a global computing environment," in *Trust Management*, vol. 2995 of *Lecture Notes in Computer Science*, pp. 120–134, 2004.

[16] "Globus toolkit." `http://www.globus.org/toolkit/`. [Online; posledný prístup 1.3. 2016].

[17] "Gridbus." `http://www.cloudbus.org/`. [Online; posledný prístup 1.3. 2016].

[18] "Uniform interface to computing resources." `http://www.unicore.eu/`. [Online; posledný prístup 1.3. 2016].

[19] J. Weise, "Public key infrastructure overview." `http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf`, 2001. [Online; posledný prístup 1.3. 2016].

[20] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, pp. 33–38, Sept. 1994.

[21] "Athens." `http://www.openathens.net/`. [Online; posledný prístup 1.3. 2016].

[22] W. Jie, J. Arshad, R. Sinnott, P. Townend, and Z. Lei, "A review of grid authentication and authorization technologies and support for federated access control," *ACM Computing Surveys*, vol. 43, pp. 12:1–12:26, Feb. 2011.

[23] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Gianoli, F. Spataro, F. Bonnassieux, P. J. Broadfoot, G. Lowe, L. Cornwall, J. Jensen, D. P. Kelsey, k. Frohner, D. L. Groep, W. S. de Cerff, M. Steenbakkers, G. Venekamp, D. Kouril, A. McNab, O. Mulmo, M. Silander, J. Hahkala, and K. Lörentey, "Managing dynamic user communities in a grid of autonomous resources," *CoRR*, vol. cs.DC/0306004, 2003.

[24] "Akenti." http://dst.lbl.gov/ACSSoftware/Akenti/. [Online; posledný prístup 1.3. 2016].

[25] D. W. Chadwick, A. Otenko, and E. Ball, "Role-based access control with x.509 attribute certificates," *IEEE Internet Computing*, vol. 7, pp. 62–69, Mar. 2003.

[26] C. Lin, V. Varadharajan, Y. Wang, and V. Pruthi, "Enhancing grid security with trust management," in *Proceedings of the 2004 IEEE International Conference on Services Computing, 2004.*, pp. 303–310, Sept 2004.

[27] E. Papalilo and B. Freisleben, "Managing behaviour trust in grid computing environments," *Journal of Information Assurance and Security*, vol. 3, pp. 27–37, March 2008.

[28] G. Kavitha and V. Sankaranarayanan, "Secure resource selection in computational grid based on quantitative execution trust," *International Science Index*, vol. 4, no. 12, pp. 112 – 118, 2010.

[29] D. Kaur and J. SenGupta, "A trust model based on p2p trust models for secure global grids," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 1103–1108, June 2012.

[30] P. Suresh Kumar and S. Ramachandram, "User satisfaction based quantification of direct trust in t-grid computational model," in *Computer, Communications, and Control Technology (I4CT), 2014 International Conference on*, pp. 438–442, Sept 2014.

[31] P. Manuel, S. Thamarai Selvi, and M.-E. Barr, "Trust management system for grid and cloud resources," in *First International Conference onAdvanced Computing, 2009.*, pp. 176–181, Dec 2009.

[32] L. Huraj, V. Siládi, J. Škrinárová, and V. Bojdová, "Towards a vo intersection trust model for ad hoc grid environment: Design and simulation results," *IAENG International Journal of Computer Science*, vol. 40, no. 2, pp. 53–61, 2013.

[33] F. Kerschbaum, J. Haller, Y. Karabulut, e. K. Robinson, Philip", W. H. Winsborough, F. Martinelli, and F. Massacci, *Trust Management: Proceedings of the 4th International Conference, iTrust 2006, Pisa, Italy, May 16-19, 2006.*, ch. PathTrust: A Trust-Based Reputation Service for Virtual Organization Formation, pp. 193–205. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006.

[34] S. Zhao, A. Aggarwal, and R. D. Kent, "Pki-based authentication mechanisms in grid systems," in *International Conference on Networking, Architecture, and Storage, 2007. NAS 2007.*, pp. 83–90, July 2007.

[35] R. Ranjan, A. Harwood, and R. Buyya, "Peer-to-peer-based resource discovery in global grids: A tutorial," *Communications Surveys and Tutorials*, vol. 10, pp. 6–33, Apr. 2008.

[36] J. M. Schopf, "Ten actions when grid scheduling: The user as a grid scheduler," in *Grid Resource Management*, pp. 15–23, Kluwer Academic Publishers, 2004.

[37] C. Grimme, J. Lepping, A. Papaspyrou, P. Wieder, R. Yahyapour, A. Oleksiak, O. Wäldrich, and W. Ziegler, "Towards a standards-based grid scheduling architecture," in *Grid Computing*, pp. 147–158, Springer US, 2008.

[38] R. Yahyapour and P. Wieder, "Grid scheduling use cases." `http://www.ogf.org/documents/GFD.64.pdf`, March 2006. [Online; posledný prístup 1.3. 2016].

[39] H. Morsy and H. El-Rewini, "Adaptive scheduling in a mobile ad-hoc grid for time-sensitive computing," in *2013 ACS International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–8, May 2013.

[40] L. dos S. Lima, A. T. A. Gomes, A. Ziviani, M. Endler, L. F. G. Soares, and B. Schulze, "Peer-to-peer resource discovery in mobile grids," in *Proceedings of the 3rd International Workshop on Middleware for Grid Computing*, MGC '05, pp. 1–6, ACM, 2005.

[41] Z. Wang, Q. Chen, and C. Gao, "Implementing grid computing over mobile ad-hoc networks based on mobile agent," in *Fifth International Conference on Grid and Cooperative Computing Workshops, 2006. GCCW '06.*, pp. 321–326, Oct 2006.

[42] K. Hummel and G. Jelleschitz, "A robust decentralized job scheduling approach for mobile peers in ad-hoc grids," in *Seventh IEEE International Symposium on Cluster Computing and the Grid, 2007. CCGRID 2007.*, pp. 461–470, May 2007.

[43] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in *Trust Management*, vol. 2995 of *Lecture Notes in Computer Science*, pp. 135–145, Springer Berlin Heidelberg, 2004.

[44] I. Dionysiou and H. Gjermundrod, "sguts: Simplified grid user trust service for site selection," in *The Seventh International Conference on Internet Monitoring and Protection, 2012*, pp. 40–46, May 2012.

[45] R. Buyya and A. Sulistio, "Service and utility oriented distributed computing systems: Challenges and opportunities for modeling and simulation communities," in *Simulation Symposium, 2008. ANSS 2008. 41st Annual*, pp. 68–81, April 2008.