ŽILINSKÁ UNIVERZITA V ŽILINE

AUTOREFERÁT
DIZERTAČNEJ PRÁCE

Žilina, apríl 2016

Ing. Slavomír Kavecký

Žilinská univerzita v Žiline
Fakulta riadenia a informatiky

Ing. Slavomír Kavecký

Autoreferát dizertačnej práce

Manažment gridových prostriedkov

na získanie akademického titulu **„philosophiae doctor“ (v skratke PhD.)**

v študijnom programe doktorandského štúdia:
aplikovaná informatika

v študijnom odbore:
9.2.9 aplikovaná informatika

Žilina, apríl 2016

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia alebo v externej forme doktorandského štúdia **na katedre informatiky, Fakulte riadenia a informatiky, Žilinskej univerzity v Žiline**

Predkladateľ: **Ing. Slavomír Kavecký**
Katedra informatiky
Fakulta riadenia a informatiky
Žilinská univerzita v Žiline

Školiteľ: **doc. Ing. Penka Martincová, PhD.**
Katedra informatiky
Fakulta riadenia a informatiky
Žilinská univerzita v Žiline

Oponenti:

Autoreferát bol rozoslaný dňa: .....

Obhajoba dizertačnej práce sa koná dňa ..... o ..... h. pred komisiou pre obhajobu dizertačnej práce schválenou odborovou komisiou v študijnom odbore **9.2.9 aplikovaná informatika**, v študijnom programe **aplikovaná informatika**, vymenovanou dekanom Fakulty riadenia a informatiky Žilinskej univerzity v Žiline dňa .....

prof. Ing.Martin Klimo, PhD.
predseda odborovej komisie
študijného programu **aplikovaná informatika**
v študijnom odbore **9.2.9 aplikovaná informatika**
Fakulta riadenia a informatiky
Žilinská univerzita
Univerzitná 8215/1
010 26 Žilina

Obsah

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 dodržiavanie 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[3].

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 zdroje a služby poskytované ad hoc gridovou infraštruktúrou 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 následovne: Sekcia 2 uvádza hlavný cieľ práce; Sekcia 3 popisuje spôsob poskytovania bezpečnosti v tradičnej a ad hoc gridovej infraštruktúre; Navrhované zlepšenie poskytovania bezpečnosti ad hoc gridovou infraštruktúrou uvádza sekcia 4; Overenie navrhovaného riešenia a zhodnotenie dosiahnutých cieľov sú popísané v sekcii 5; a Sekcia 6 uvádza zhrnutie práce.

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 [3] a do dnešných dní vzniklo viacero ad hoc gridových infraštruktúr (OurGrid [4, 5], MoGrid [6]), ktoré sú inšpirované týmto konceptom. Jednou zo základných čŕt každej ad hoc gridovej infraštruktúry je požiadavka na bezpečné vykonávanie úloh a 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**. Za-

členenie 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.

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 riešený problém 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, rozsah významu 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 popisuje dôveru ako vzťah medzi dôverovaným a dôverujúcim jednotlivcom 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 vymožiteľnosť práva, poistenie a pod.

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 dôveryhodnými 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 ako i ohodnotiť dôveryhodnosť iných jednotlivcov sa označuje ako **riadenie dôvery**, ktoré sa v kontexte online distribuovaných systémov 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.

3.2 Popis gridovej infraštruktúry

Funkčnosť a použiteľnosť gridovej infraštruktúry je závislá od miery implementácie základných funkčných prvkov, medzi ktoré nevyhnutné 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 [9], Gridbus Middleware [10] a UNICORE [11]) 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 viacerých vrstiev. 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, vytvorenie 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.

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. Zo spomenutého teda vyplýva, že tradičná gridová infraštruktúra nie je centralizovaná štrukturálne ale funkčne.

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 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, avšak v prípade ad hoc gridovej infraštruktúry absentuje centralizovaná prístupová kontrola. Ad hoc grid je možné definovať ako: *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 infraštruktúrou. 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 štruktúry 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 teda 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.

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.

3.3 Definícia problému

Veľký dôraz pri spolupráci sprostredkovanej prostredníctvom gridovej infraštruktúry sa kladie na bezpečnosť. Tradičné gridové infraštruktúry majú túto problematiku dobre zanalyzovanú a zabezpečujú bezpečnosť v adekvátnej miere tak ako je to možno vidieť v sekcii 3.4.1. 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 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.

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 prostriedkov 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 poskytovania bezpečnosti. 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 funkčné prvky, ktoré umožňujú vykonávať používateľské úlohy na zdieľaných prostriedkoch. Medzi funkčnými prvkami musí existovať vzájomná súhra, aby vykonanie úlohy mohlo prebehnúť úspešne. Popis súčasného stavu sa zameriava v závislosti od stanoveného cieľa popísaného v sekcii 2 a definovaného problému 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 používateľských 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. Popis poskytovania bezpečnosti oboma infraštruktúrami, ich spoločné črty, rozdiely a ich porovnanie je bližšie popísané vo zvyšku sekcie.

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, prístup k dátam ako i potreba zabezpečiť komunikáciu sprostredkovanú gridovou infraštruktúrou. Vývojári tradičnej gridovej infraštruktúry postupom času navrhli a implementovali viacero autentifikačných a autorizačných infraštruktúr ako reakciu 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** [12], 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. 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 [13] 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 [14] 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) [15] 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 prostriedku. Tento spôsob autorizácie bol veľmi rýchlo prijatý gridovou komunitou vďaka jednoduchosti jeho implementácie.

Virtual Organization Membership Service (VOMS) [16] 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 [17] 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) [18] 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 zdrojmi autority, 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.

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 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 teda 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, 19].

3.4.2 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 [20]: *(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.

Plánovanie úloh v tradičnej gridovej infraštruktúre. V tradičnej gridovej infraštruktúre je plánovanie úloh bežne vykonávané jedným gridovým modulom plánovania úloh a viacerými lokálnymi modulmi plánova-

nia 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 [21]: *(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.

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 [5, 4, 22]. Cluster tvoria buď geograficky vzájomne si blízke uzly [5, 4], alebo uzly patriace do jednej lokálnej siete umožňujúcej im priamo komunikovať s operátorom lokálneho zoskupenia [22].

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, 23, 24, 25]. 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, 23]. 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 [24] a zdieľaná virtuálna pamäť [25].

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 menované požiadavky je popísaný v sekcii 4.1. Navrhnutá integrácia riadenia 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.

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 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: *(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 minimálnu úroveň dôveryhodnosti 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. [27, 28]).

Výpočet hodnoty požiadaviek na poskytovanú bezpečnosť. Hodnota **požiadaviek na poskytovanú bezpečnosť** sa stanovuje na základe rizika a neistoty vnímaných účastníkmi potencionálne vykonanej kolaborácie. 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.

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, 19, 29]:

- **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:

- **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.

Výpočet indexu dôvery. Index dôvery určovaný pre účely rozhodovania účastníkov potencionálnej kolaborácie o jej vykonaní sa stanovuje na základe priamej dôvery a odporúčaní. **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 po-

hľadu 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 odporúčania je závislá na váhach, ktoré sú týmto dvom parametrom priradené v rámci rozhodovacieho procesu. Hodnota priamej dôvery je určená odvodením z nasledujúcich parametrov:

- **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 hodnota kombinovaných parametrov je možné odvodiť z nasledovných parametrov popisujúcich systém účastníka potencionálnej kolaborácie:

- **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 zabezpečiť 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 hodnota kombinovaných parametrov je možné odvodiť z nasledovných parametrov popisujúcich správanie sa účastníka potencionálnej kolaborácie:

- **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.

4.2 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.

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 zdieľaných 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 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 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. Po ukončení úlohy musí prebehnúť aktualizácia základnej dôvery. Táto aktualizácia prebieha na uzle používateľa ako i na uzle poskytovateľa zdieľaného prostriedku. Používateľov modul riadenia dôvery stanoví novú hodnotu základnej dôvery voči poskytovateľovi ako TI zohľadňujúci priebeh ukončenej kolaborácie. Podobne, modul riadenia dôvery poskytovateľa zdieľaného prostriedku určí novú hodnotu základnej dôvery voči používateľovi ako TI taktiež zohľadňujúci priebeh ukončenej kolaborácie.

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 sekcii 4. Sekcia 5.2 sa zaoberá hodnotením dosiahnutia cieľov stanovených v sekcii 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 gridovej 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[30]. 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. Simulovaní poskytovatelia zdieľaných prostriedkov majú tiež priradené viaceré charakteristiky a formy správania sa. 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 entitám 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.

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 korektne. Simulovaná ad hoc gridová infraštruktúra obsahuje hneď niekoľko takto korektne 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. 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.

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 dva experimenty: *(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. Uskutočnená simulácia poskytuje referenčné dáta o vlastnostiach ad hoc gridovej infraštruktúry, voči ktorým sú porovnané dáta získané z iných experimentov. Počas simulácie bolo uskutočnených celkovo 1000 simulačných behov. Hodnoty namerané počas týchto jednotlivých behov sú uvádzané pre každý typ nameranej hodnoty 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. 1. 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. 2.

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. 1: 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	25,0
Zlyhanie zdieľaného prostriedka	568,95	60,0
Chyba vykonávanej úlohy	144,90	15,00

Tabuľka č. 2: Počet neúspešných úloh podľa kategórie vyskytnutej chyby vykonaných 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 jednotlivých behov sú uvádzané pre každý typ nameranej hodnoty 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. 3. 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. 4. 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 prostriedku.

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. 3: Počet všetkých úloh vykonaných s integráciu riadenia dôvery

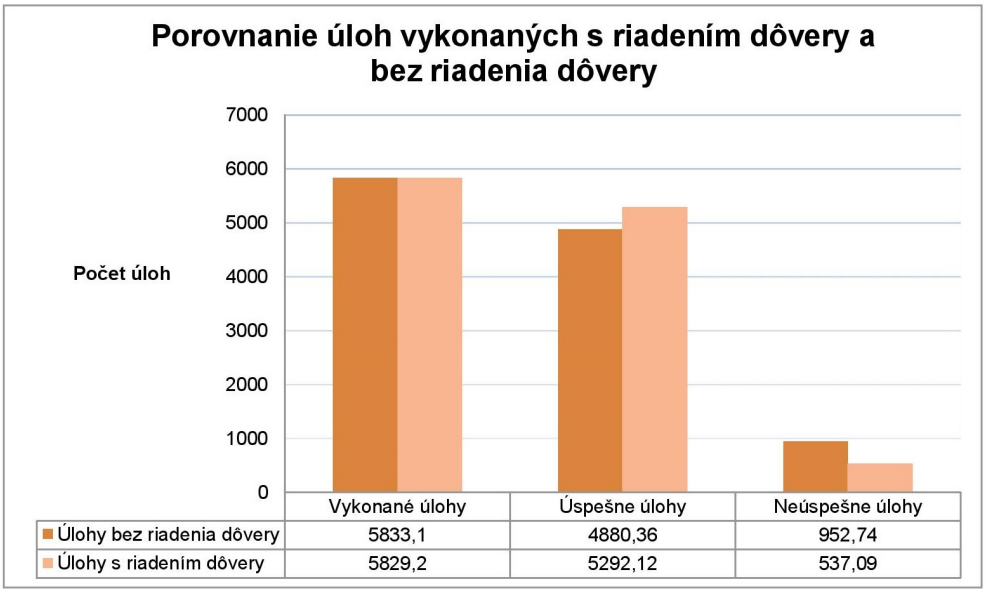
Typ úlohy	**Namerané hodnoty** [s presnosťou na dve desatinné miesta]	
	Počet neúspešných úloh	Podiel z neúspešných úloh [v %]
Žiadny zdieľaný prostriedok k dispozícii	1,12	0,21
Zdieľaný prostriedok nedostupný	109,05	20,03
Zlyhanie zdieľaného prostriedka	274,07	51,03
Chyba vykonávanej úlohy	152,86	28,46

Tabuľka č. 4: Počet neúspešných úloh podľa kategórie vyskytnutej chyby vykonaných s integráciou riadenia dôvery

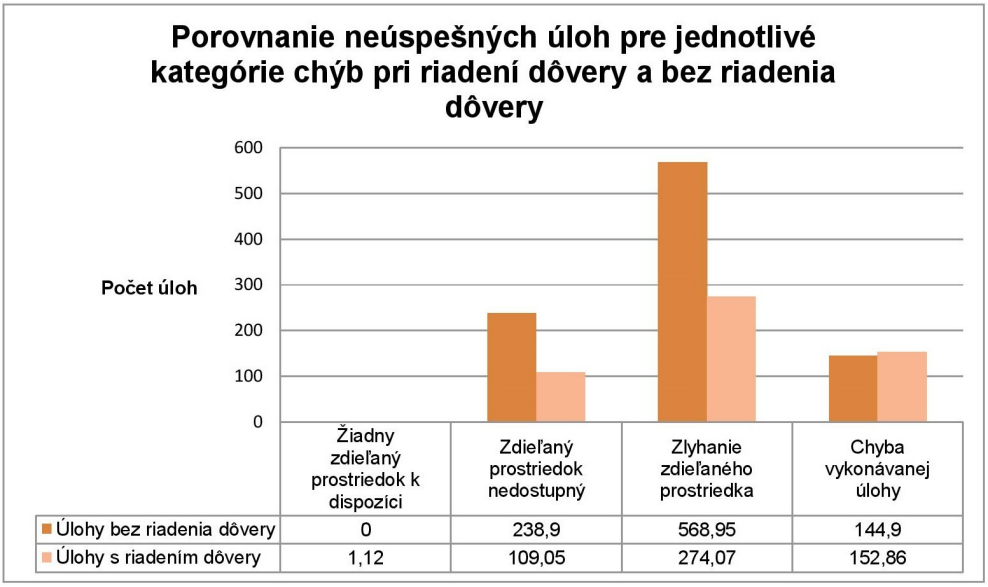
5.1.3 Výsledky overenia

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. 1) je zrejmé, že kompetencia ad hoc gridovej infraštruktúry ostáva aj pri integrácii riadenia dôvery takmer rovnaká. Riadenie dôvery teda nemá žiadny negatívny dopad na schopnosť ad hoc gridovej infraštruktúry vykonávať úlohy.

Spoľahlivosť ako metrika hodnotiaca schopnosť simulovanej ad hoc gridovej infraštruktúry zabezpečiť bezpečné vykonávanie úloh je meraná ako počet neúspešných úloh 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. 1) 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



Obrázok č. 1: Porovnanie úloh vykonaných bez riadenia dôvery a s riadením dôvery



Obrázok č. 2: Porovnanie neúspešných úloh pre jednotlivé kategórie bez riadenia dôvery a s riadením dôvery

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 nemá negatívny vplyv na kompetenciu ad hoc gridovej infraštruktúry a taktiež zlepšuje spoľahlivosť danej infraštruktúry. Zlepšenie spoľahlivosti sa prejavilo v poklese počtu neúspešných úloh. Porovnanie výskytu neúspešných úloh podľa jednotlivých kategórií chýb je znázornené grafom na obrázku č. 2. 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.

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 určenými metrikami v sekcii 5.1.3 ukázalo, že navrhnutá integrácia riadenia dôvery do ad hoc gridovej infraštruktúry neznižuje 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 teda 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. 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 prenechaná 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 [31]. 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. 2 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.

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] 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.

[4] 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.

[5] 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.

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

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

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

[12] 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].

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

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

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[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] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

Zoznam vlastnej publikačnej činnosti

1. S. Kavecký, "Trust based grid security and security models", in International journal on information technologies and security, ISSN 1313-8251, vol. 4, no. 3, pp. 81-91, 2012.
2. S. Kavecký, "Ad hoc grid trust management architecture", in International journal on information technologies and security, ISSN 1313-8251, vol. 5, no. 3, pp. 21-30, 2013.
3. S. Kavecký, "Grid security and trust management overview", in IJCSI International journal of computer science issues, ISSN 1694-0784, vol. 10, iss. 3, no. 3, pp. 225-233, 2013.
4. S. Kavecký, P. Martincová, "Overview of trust models integrating trust management into grid computing", in International journal of computer applications", ISSN 0975-8887, ISBN 973-93-80889-96-8, vol. 129, no. 7, pp. 1-6, 2015, online: http://www.ijcaonline.org/research/volume129/number7/kaveck%C2%B4-2015-ijca-906657.pdf.
5. S. Kavecký, P. Martincová, "Specification of parameters relevant for trust evaluation in an adhoc grid environment", in International journal of computer applications", ISSN 0975-8887, ISBN 973-93-80889-96-8, vol. 132, no. 11, pp. 1-8, 2015, online: http://www.ijcaonline.org/research/volume132/number11/kaveck%C2%B4y-2015-ijca-907586.pdf.
6. S. Kavecký, P. Martincová, "A survey on trust aware security and scheduling in traditional and ad hoc grids", in International journal of computer applications", ISSN 0975-8887, ISBN 973-93-80889-96-8, vol. 133, no. 12, pp. 1-13, 2016, online: http://www.ijcaonline.org/research/volume133/number12/kaveck%C3%BD-2016-ijca-908058.pdf.